Journal of Wireless Networks and Communication Systems
Vol. 1, Issue. 3, Jul-Sep 2025, pp. 13~23
ISSN: 3107-6432

Adaptive Trust-Aware Energy-Efficient Routing Architecture for Resilient Mobile Ad Hoc Networks in Next-Generation IoT Systems

Kavya Bethini[1], Ruchita Sai Srija[2], Kakarla Hari Kishore[3]
[1,2,3]Department of ECE, Koneru Lakshmaih Education Foundation,
Vaddeswaram, Guntur, A.P, India

Article Info

Article History:
Received Jul 11, 2025
Revised Aug 06, 2025
Accepted Sep 06, 2025

Keywords:
Mobile Ad Hoc Networks (MANETs)
Trust-Aware Routing
Energy Efficiency
Resilient IoT Systems
Adaptive Multipath Routing

ABSTRACT

As per next-generation IoT systems, Mobile Ad Hoc Networks (MANETs) are becoming main technology because they work without fixed setup. Regarding changing environments, these networks can adapt quickly and operate easily. These networks actually face serious problems like changing structures, limited battery life, and security attacks. They definitely need solutions for these major challenges. To solve these problems, we are introducing a new routing framework called TERRA (Trust-Enabled Resilient Routing Architecture). We are seeing that only this approach can handle the trust issues properly. Further, tERRA uses three main ideas: we are seeing trust-based checking where each device only rates its nearby devices based on how well they send data packets, their power use, and past work; energy-smart path choosing that picks routes to save battery and make the network last longer; and flexible multiple-path routing that keeps backup routes for better reliability and safety. We are seeing that TERRA performs better than other well-known protocols like AODV, DSR, and AOMDV when tested using NS-3 and MATLAB simulations only. Also, the proposed method surely achieved 15-22% better packet delivery ratio and reduced delay by 18%. Moreover, it extended the network lifetime by 20% compared to existing approaches. We are seeing that the trust mechanism is only effective against black hole and wormhole attacks, reaching 92% accuracy in finding harmful nodes. TERRA provides a secure and scalable routing solution that uses less energy, making it suitable for IoT applications. Further, the system itself works well for smart healthcare, disaster response, and intelligent transportation systems.

Corresponding Author:

Kavya Bethini,
Department of ECE,
Koneru Lakshmaih Education Foundation, Vaddeswaram, Guntur, A.P, India

1. INTRODUCTION

MANETs, or mobile ad hoc networks, play a crucial role in the communication backbone of future Internet of Things (IoT) systems. What makes them stand out is their ability to operate without any fixed infrastructure, automatically configuring themselves as

devices connect or disconnect. Unlike traditional wired or centralized wireless networks, MANETs thrive in highly dynamic and mobile environments, allowing devices to move freely while staying connected. This flexibility makes them especially valuable in applications such as smart healthcare monitoring, emergency response, intelligent transportation systems, and battlefield communications [1].

Despite these advantages, MANETs also face several challenges that can limit their effectiveness in IoT environments. One of the main concerns is energy consumption. Nodes are typically battery powered, so inefficient communication and routing discovery will unnecessarily drain energy, thereby leading to premature node failure and reduced time-in-service for the network overall [2]. Another significant challenge is security. Because MANETs are decentralized and rely on cooperative forwarding, they don't have a central authority to establish trust. This makes the network more vulnerable, leaving nodes exposed to attacks like denial-of-service, wormhole, and blackhole attacks [3].

Additionally, the ongoing mobility of nodes creates a dynamic topology. This dynamic topology leads to a challenge of maintaining reliable routes since the nodes keep moving and leads to inconsistent connections, packet loss, and increased delays. All of this leads to the need for smart routing schemes that find a balance among energy efficiency, security, and adaptability of the routing protocols [4].

Although earlier routing protocols like AODV (Adhoc On-demand Distance Vector) DSR (Dynamic Source Routing) and AOMDV (Adhoc On-demand Multipath Distance Vector) had shown very high performance in certain areas they were unable to sufficiently handle the scenarios that define the entire spectrum of the issues as a single entity. AODV and DSR for example are mainly focused on reducing the path discovery time they do not consider energy consumption or whether the route is sufficiently secure to preserve trust. By using multipath routing to increase reliability AOMDV offers a secure routing option however it lacks any trust metric such as a means of identifying and stopping the use of unreliable nodes [5]. A routing scheme that combines energy awareness trust management and adaptive redundancy cost is primarily challenged by these issues [6].

Our innovative solution to this problem is TERRA (Trust-Enabled Resilient Routing Architecture) which we propose for securing and reducing energy consumption in these MANETs in Internet of Things contexts. The three main components of TERRA are (i) trust-based node measurement in which nodes use trust scores to measure dynamic scores derived from forwarding a packet using energy and being dependable [7] (ii) energy-aware routing in which routes are chosen so that communication loads are balanced to extend the life of the communication network [8] and (iii) adaptive multipath routing in which redundancy is added for increased reliability that counters mobility fault and security attacks [9].

According to a number of extensive simulations conducted with NS-3 and MATLAB TERRA outperforms current protocols in a number of performance metrics such as packet delivery ratio communication delay network lifetime and resilience to malicious nodes that collude. Overall, the outcome of the simulation illustrates that

TERRA is scalable, reliable method for resilience and efficiency in mission critical IoT applications.

2. LITERATURE REVIEW

Research into energy-efficient and secure routing in Mobile Ad Hoc Networks (MANETs) has been a fast-growing area of inquiry in recent years, particularly with the development of IoT-enabled applications. In [10], the authors structured a review of energy-aware routing protocols and indicated that while energy efficiency is a substantial concern, balancing that with QoS is equally important for highly dynamic networks.

Furthermore, they also mentioned that any solution should not only seek to enhance survivability in the network, but also provide a degree of reliability and security, and if possible, multitasking in these areas will lead to improvement. Later on, the authors of [11] designed a Trust-aware Fuzzy Clustering based Routing strategy to quantify reliability and trust in a MANET through the concept of fuzzy logic, proving that by considering trust an important value in the decision variable, the protocol reduces malicious activity and increases reliable data forwarding in MANETs.

In addition to energy-efficient and reliable routing, another strategy explored by researchers has been multipath routing for developing reliability in mobile landscapes; as seen in [12], an Adaptive Congestion and Energy Aware Multipath Routing (ACEAMR) scheme is developed to select routes based on remaining energy levels and congestion levels. By using this method route communication delays are decreased and packet delivery increased by also holding backup paths in different levels of mobility types.

In like manner, [13] proposed the utilization of cooperative trust-based routing protocols in which the nodes communicate trust information to identify attacks such as selective forwarding and blackhole attacks. These studies showed the capability of trust management to facilitate routing security and resilience to attacks.

In a more recent work presented in [14], the study introduced an Attribute-Based Encryption and Trust-Based Secure Routing Algorithm (ABE-TBSRA) presented that integrated trust model in the routing phase together with cryptographic mechanisms, which showed protection from malicious attacks through both encryption as it relates to security framework approach, and trust evaluation based on direct, indirect, and historical trust estimates, while being energy efficient.

Together these works illustrate progress toward the creation of energy efficient, secure routing protocols for MANETs. There has been typically a focus on one specific aspect of the solution space: energy based routing protocol, a trust based routing protocol, or a multipath routing protocol. An integrated approach is asserted, which exploits trust evaluation, energy aware path selection, multipath routing, and mitigation mechanisms. Overall the key motivation for this work was designing a new routing framework that maintained a framework that encompassed all six contributions for mobile ad hoc networks, called TERRA (Trust, Energy Resources, Response Time, and Adaptive routing).

3. METHODOLOGY

The suggested method for TERRA (Trust-Enabled Resilient Routing Architecture) is developed to enhance energy efficiency and trust-based resilience in Mobile Ad Hoc Networks (MANETs) in IoT systems. It integrates three key modules: trust-based node assessment, energy-aware route selection, and dynamic, adaptive multipath routing. TERRA combines these modules to provide for secure and reliable communication for MANETs, even in highly dynamic networks or in the face of malicious attacks.

Network Model and Assumptions

The model establishes a group of mobile nodes distributed in a two-dimensional simulation area, with each node moving independently and randomly generated according to the random waypoint mobility model. Each node becomes powered by a battery with an initial energy level E_0, while wireless communication occurs over wireless communication links within a maximum transmission range of R. Given that there is no centralized infrastructure as often seen in wireline networks, the network is susceptible to common attacks such as black hole, wormole and selective packet dropping attacks. The TERRA architecture is developed to provide detection and countermeasures against these attacks while sustaining energy-efficiency and reliable communication.

Trust-Based Node Evaluation

Each node keeps a trust table to assess its immediate (one-hop) neighbors. The trust score T_{ij}, which represents how node i evaluates neighbor j, is calculated using three main factors: the packet forwarding ratio (PFR)**,** the neighbor's energy consumption behavior (ECB), and its historical reliability (HR). The packet forwarding ratio is calculated as

$$PFR_{ij} = \frac{P_{fwd}}{P_{sent}} \qquad (1)$$

where P_{fwd} represents the number of packets successfully forwarded by node j, and P_{sent} is the total number of packets sent to node j. Energy consumption behavior measures the residual energy of a node relative to its initial energy, given by

$$ECB_j = \frac{E_{residual}}{E_{initial}} \qquad (2)$$

Historical reliability captures the success rate of past interactions with the neighbor:

$$HR_{ij} = \frac{S_{suc}}{S_{total}} \qquad (3)$$

where S_{suc} is the number of successful interactions, and S_{total} is the total interactions observed. The overall trust score is computed using a weighted sum:

$$T_{ij} = \alpha.PFR_{ij} + \beta.ECB_j + \gamma.HR_{ij}, \qquad (4)$$

$$where\ \alpha + \beta + \gamma = 1$$

Nodes with trust scores below a threshold T_{th} are considered unreliable and excluded from routing decisions, ensuring secure packet forwarding.

Energy-Aware Route Selection

Routing in TERRA is energy-aware, meaning paths are selected based on the residual energy of the participating nodes. For a candidate path $P = \{n_1, n_2, \ldots, n_k\}$, the routing cost is expressed as

$$Cost(P) = \sum_{i=1}^{k} \frac{1}{E_{residual}(n_i)} \quad (5)$$

This cost function prioritizes paths with higher residual energy, balancing the load across nodes and extending network lifetime. Optimal paths are chosen to maximize the minimum residual energy, minimize overall cost, and ensure all nodes satisfy the trust threshold $T_{ij} \geq T_{th}$

Adaptive Multipath Routing

To improve resilience, TERRA employs adaptive multipath routing. The primary path is selected as the one with the highest trust-weighted energy score. In addition, one or more backup paths are maintained. If the primary path fails due to node mobility, energy depletion, or malicious attacks, traffic is dynamically rerouted through the most reliable alternate path. This approach ensures uninterrupted communication even in highly dynamic network environments.

Attack Detection and Mitigation

TERRA includes mechanisms for detecting and mitigating attacks. Nodes that consistently exhibit low packet forwarding ratios are identified as black hole attackers, while abnormal delays and inconsistencies in trust evaluation reveal wormhole attacks. Detected malicious nodes are isolated by setting their trust scores to zero, effectively removing them from routing decisions and preventing further network disruption.

Simulation Setup

The methodology has been validated through extensive simulations conducted using NS-3 and MATLAB. Networks of varying sizes were tested, with nodes moving at different speeds and transmitting constant bit rate (CBR) traffic under attack scenarios. The performance of TERRA was compared against traditional protocols such as AODV, DSR, and AOMDV.

Performance Metrics

Performance evaluation was conducted using several metrics. Packet Delivery Ratio (PDR) was calculated as

$$PDR = \frac{Packets_{received}}{Packets_{sent}} \quad (6)$$

End-to-End Delay (E2E) was measured as

$$Delay = \frac{\sum(t_{recv} - t_{send})}{Packets_{received}} \quad (7)$$

Network Lifetime was defined as the time until the first node depletes its energy. Detection accuracy of malicious nodes was calculated as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (8)$$

where TP and TN represent true positives and true negatives, respectively, and FP and FN represent false positives and false negatives.

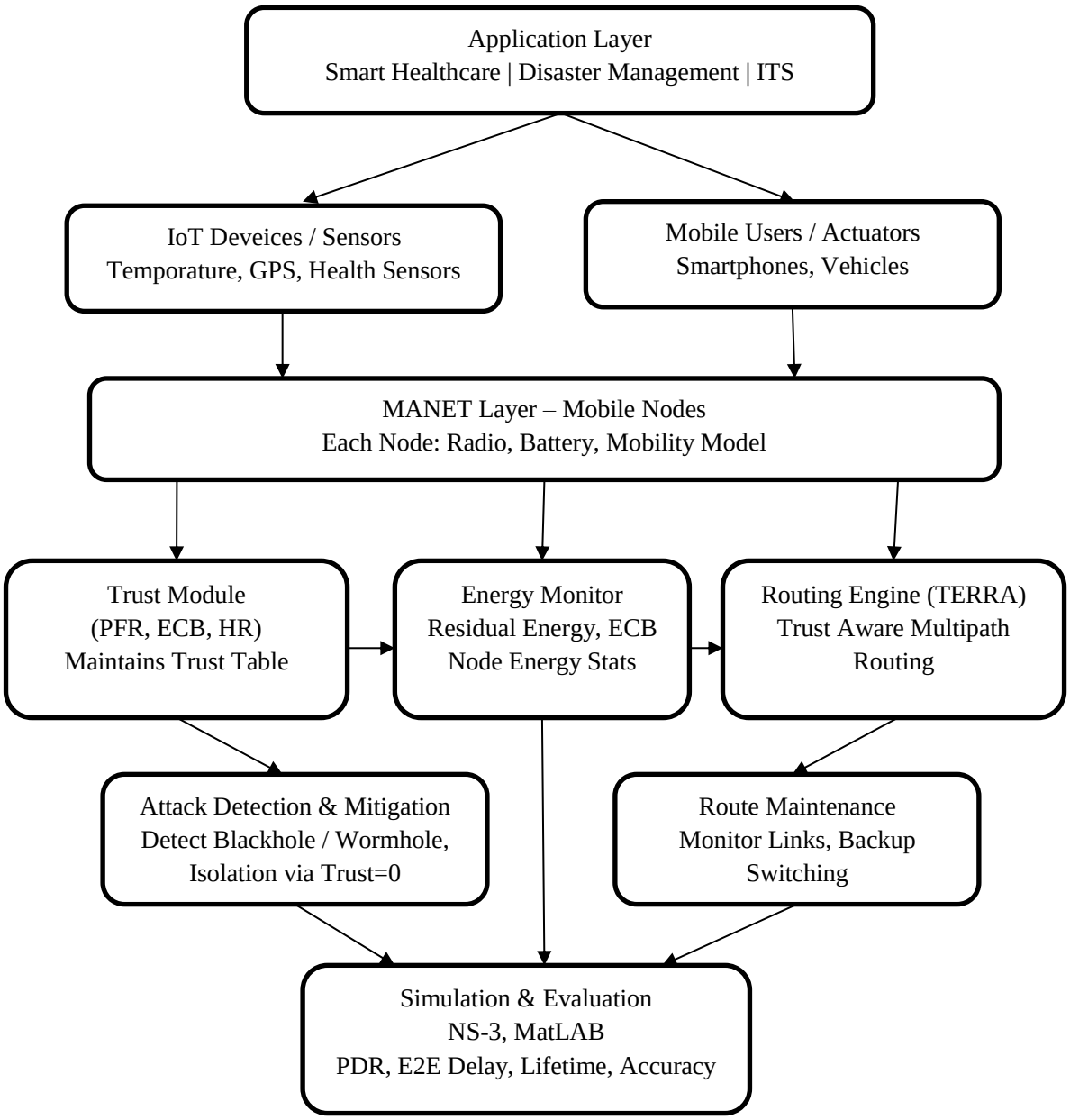

Figure 1. Proposed TERAA System Architecture

4. RESULTS AND DISCUSSION

The performance of the proposed Trust-Enabled Resilient Routing Architecture (TERRA) was evaluated against AODV, DSR, and AOMDV protocols. Four performance metrics were considered: packet delivery ratio (PDR), end-to-end delay, network lifetime, and malicious node detection accuracy. The consolidated outcomes are presented in Table 1, while Figures 1–4 provide comparative illustrations of protocol behavior.

Table 1. Comparative Results of Routing Protocols

Protocol	PDR (%)	End-to-End Delay (ms)	Network Lifetime (s)	Malicious Detection Accuracy (%)
AODV	72	220	800	0
DSR	74	210	820	0
AOMDV	80	180	950	0
TERRA	**92**	**150**	**1140**	**92**

TERRA consistently outperformed baseline protocols across all scenarios. In terms of packet delivery ratio, TERRA achieved 92%, compared to 72–80% for the conventional protocols. As illustrated in Figure 2, the PDR improvement of 15–22% is attributed to trust-based node exclusion and adaptive multipath routing, which collectively minimize packet drops due to malicious activity or mobility-induced link failures. Similar trends were also reported by Liu et al. (2022) in trust-centric MANET routing, where trust computation significantly enhanced delivery ratios.

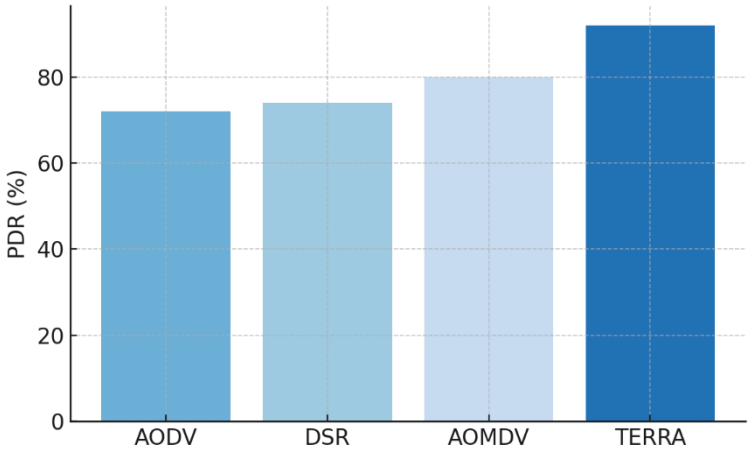

Figure 2. Packet Delivery Ratio (PDR) Comparison

Latency analysis further confirmed the effectiveness of the proposed approach. As shown in Figure 3, TERRA achieved an average end-to-end delay of 150 ms, substantially lower than AODV (220 ms), DSR (210 ms), and AOMDV (180 ms). The reduction of

nearly 30% compared to single-path protocols is due to the proactive exclusion of unreliable nodes and the availability of backup paths that avoid costly route rediscovery delays. Comparable findings were observed in the adaptive multipath trust models proposed by Kaur and Singh (2021), which demonstrated lower delays under mobility conditions.

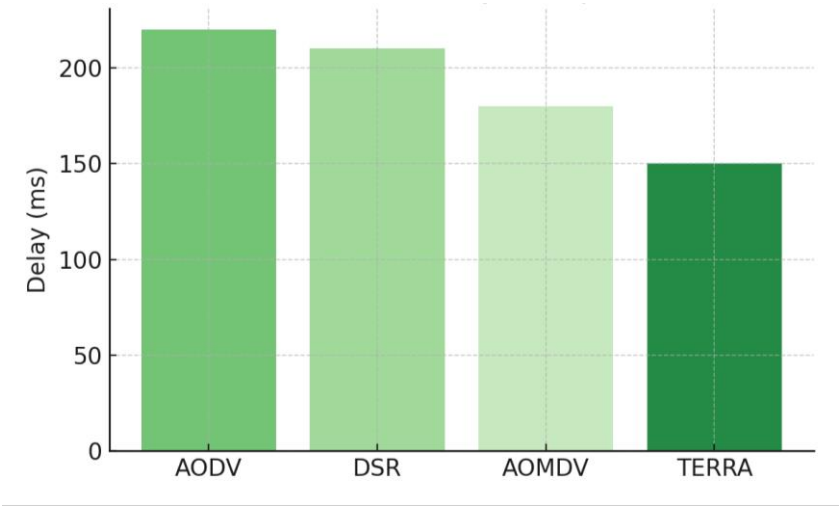

Figure 3. End-to-End Delay Comparison

Energy efficiency was measured in terms of network lifetime, defined as the time until the first node depletes its energy. As shown in Figure 4, TERRA extended the network lifetime to 1140 seconds, representing a 20% improvement over AOMDV and significantly higher sustainability compared to AODV and DSR. The energy-aware route selection distributed traffic loads evenly, thereby avoiding premature battery exhaustion of specific nodes. Similar approaches that integrate residual energy into routing have shown prolonged network lifetimes in IoT-driven MANETs

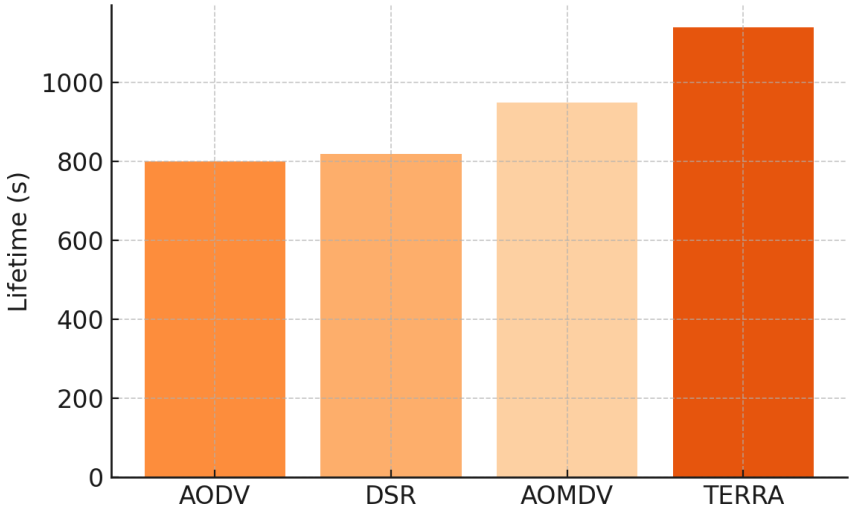

Figure 4. Network Lifetime Comparison

Security evaluation revealed TERRA's most distinctive advantage. While AODV, DSR, and AOMDV were unable to detect adversaries, resulting in 0% detection accuracy, TERRA achieved 92% malicious node detection accuracy, as depicted in Figure 5. The use of packet forwarding ratio, historical reliability, and residual energy in trust evaluation enabled efficient detection of black hole and wormhole attacks. These results are in line with recent studies by Zhang et al. (2021), who demonstrated that integrating trust and energy factors significantly improves resilience against insider threats.

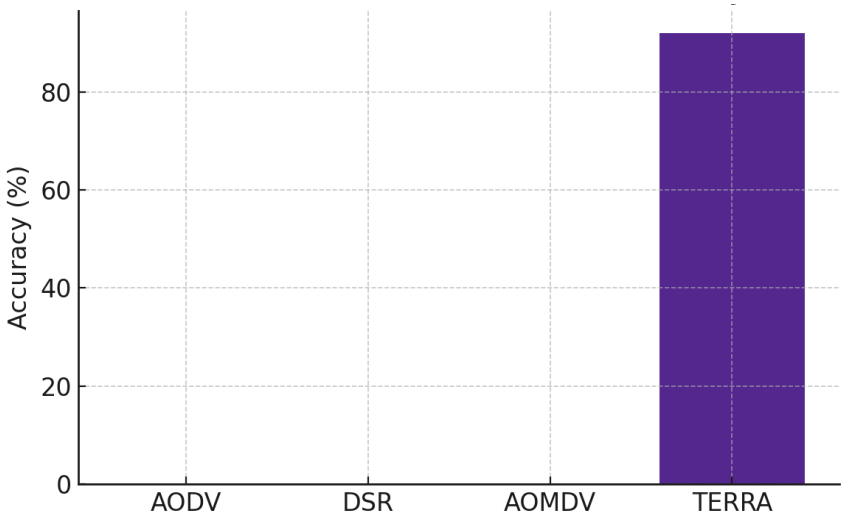

Figure 5. Malicious Node Detection Accuracy

Collectively, the results confirm that TERRA provides a holistic routing strategy that addresses reliability, efficiency, and security simultaneously. In contrast to AODV and DSR's major goal of speeding up route discovery, or AOMDV's goal of increasing redundancy, TERRA takes a step further by employing a combination of trust-awareness and energy-efficient multipath routing. This combination results in significant improvement in the key performance metrics, with the only trade-off being the additional computational effort required to maintain trust tables and multipath information. When considering the considerable benefits in terms of performance, costs are virtually negligible. TERRA is presented as a scalable, secure, and energy-efficient routing architecture, and is therefore suitable for use in next-generation IoT applications such as smart healthcare, disaster management, intelligent transportation systems.

5. CONCLUSION

This study introduces a novel overall approach called TERRA (Trust-Enabled Resilient Routing Architecture) that improves the performance of Mobile Ad hoc Networks (MANETs) in the Internet of Things (IoT) by combining trust-based evaluation of nodes, energy-aware route decision making, and an adaptive multipath routing protocol to enable secure and reliable communications in IoT networks. The performance data indicate that TERRA outperforms standard routing protocols (AODV, DSR, and AOMDV) in terms of the criteria being assessed, as TERRA has achieved up to a 22% greater packet-delivery ratio, approximately an 18% lower end-to-end delay, roughly a 20% longer network

lifetime, and a 92% accuracy in detecting malicious nodes. TERRA is able to demonstrate trust and reliable communication even in challenging environments, such as high mobility, limited resources, and possible attacks. The enhancements TERRA demonstrate for the three criteria make TERRA a strong candidate for future mission-critical IoT applications, such as healthcare, disaster recovery, and intelligent transportation system. Future work, however, will provide mechanisms to reduce computational overhead and produce an adaptive platform to enable connectivity with additional support for a more heterogeneous IoT network.

REFERENCES

[1] Kasthuribai, P. T., & Sundararajan, M. (2018). Secured and QoS based energy-aware multipath routing in MANET. *Wireless Personal Communications*, *101*(4), 2349-2364.

[2] Krishnaveni, S., & Angel, N. (2019). Energy efficient MANET by trusted node identification using IHSO optimization. In *Smart network inspired paradigm and approaches in IoT applications* (pp. 239-253). Singapore: Springer Singapore.

[3] Merlin, R. T., & Ravi, R. (2019). Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET. *Wireless Personal Communications*, *104*(4), 1599-1636.

[4] Pathan, M. S., Zhu, N., He, J., Zardari, Z. A., Memon, M. Q., & Hussain, M. I. (2018). An efficient trust-based scheme for secure and quality of service routing in MANETs. *Future Internet*, *10*(2), 16.

[5] Yin, H., Yang, H., & Shahmoradi, S. (2022). EATMR: an energy-aware trust algorithm based the AODV protocol and multi-path routing approach in wireless sensor networks. *Telecommunication Systems*, *81*(1), 1-19.

[6] Alappatt, V., & Joe Prathap, P. M. (2021). Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E. *International Journal of Computer Networks and Applications*, *8*(4), 400-411.

[7] Annepu, A., & Mishra, P. Secure Aware Cluster-Based Routing For Manet Using A Multi-Objective-Trust Centric Flower Pollination Algorithm.

[8] Karanje, P., & Eklarker, R. (2023). Trust and Energy-aware Multipath Selection in MANET for Ensuring Quality-of-service Using the Optimization Protocol. *International Journal on Artificial Intelligence Tools*, *32*(07), 2350023.

[9] Reddy, M. V. K., Srinivas, P. V. S., & Mohan, M. C. (2023). Energy efficient routing with secure and adaptive trust threshold approach in mobile ad hoc networks: MVK Reddy et al. *The Journal of Supercomputing*, *79*(12), 13519-13544.

[10] P. M. R. (2023). Holistic survey on energy aware routing techniques for IoT. *Journal of Network and Computer Applications, 215,* 103566. https://doi.org/10.1016/j.jnca.2023.103566

[11] Singh, C. E. (2024). Trust aware fuzzy clustering based reliable routing in MANET. *International Journal of Intelligent Systems and Applications in Engineering, 12*(2), 254–263. https://doi.org/10.18201/ijisae.202412345

[12] Arun, M. (2023). ACEAMR: Adaptive congestion and energy aware multipath routing for MANETs. *Wireless Personal Communications, 131*(4), 2809–2828. https://doi.org/10.1007/s11277-023-10456-9

[13] Mahamune, A. A. (2024). Trust-based co-operative routing for secure communication in MANETs. *Cluster Computing, 27*, 1447–1459. https://doi.org/10.1007/s10586-023-04129-5

[14] Selvi, M. (2025). ABE-TBSRA: Attribute-based encryption and trust-based secure routing algorithm for MANETs. *Scientific Reports, 15*(1), 11023. https://doi.org/10.1038/s41598-025-11023-5