IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

ENERGY-EFFICIENT AND SECURE COMMUNICATION FOR MOBILE MULTIHOP ADHOC NETWORKS

Pavithra M J
Lecturer
Department of Electronics & Communication Engineering,
Government Polytechnic, K.R. Pete, Karnataka, India

Abstract: In the current landscape of wireless communication, Mobile Ad-Hoc Networks (MANETs) have emerged as a significant area of interest for researchers and scholars due to their versatility and expanding applications. These networks are widely used for monitoring, sensing, and analyzing vast environments, especially in defense operations and in detecting physical parameters. One of the critical concerns in real-time MANET applications is energy efficiency, as the devices typically operate with limited battery life and constrained energy supplies. To address these core challenges, this work introduces an integrated strategy aimed at optimizing energy usage during data transmission while also improving the overall network lifespan. The proposed approach unfolds in three phases, starting with a model that identifies energy-efficient mobile nodes using a node detection mechanism. This strategy enables only a necessary subset of nodes to remain active, allowing others to conserve energy in sleep mode. To maximize energy savings, a calculated quantitative factor is employed, resulting in significantly enhanced network durability. Node selection prioritizes devices that are crucial for maintaining communication within the MANET and ensures effective power utilization. Due to the dynamic nature of ad-hoc networks, the number of nodes involved in communication must be adaptable rather than fixed, prompting the development of a second phase that introduces an adaptive model for node selection based on performance needs. The final phase integrates a secure, energy-conscious routing scheme that leverages trusted path identification and optimal route configuration. This results in reliable communication, improved prediction accuracy, and an extended network lifetime in mobile multihop ad hoc environments.

Index Terms –Mobile Ad-Hoc Network, MANET, Energy Efficiency, Secure Communication, Wireless Sensor Networks, Optimal Path Selection, Dynamic Topology.

I. INTRODUCTION

In the evolving landscape of wireless communications, Mobile Ad Hoc Networks (MANETs) have gained significant importance due to their decentralized structure and adaptability. A MANET is a wireless network without fixed infrastructure or centralized administration, where mobile nodes dynamically route data using multihop communication [1]. This flexibility allows nodes to establish temporary communication networks suitable for military surveillance, emergency response, and vehicular tracking applications. MANETs are characterized by dynamic topology, self-configuration, and multihop routing, making them highly flexible but also posing unique challenges in stable and efficient routing [2]. Due to the absence of a fixed backbone, determining optimal and reliable routes becomes critical. Consequently, extensive research has focused on routing protocols, which can be broadly classified into proactive (table-driven), reactive (on-demand), and hybrid types. Each category offers different trade-offs in terms of latency, control overhead, and adaptability. As energy and security constraints intensify in modern applications, understanding and improving MANET routing strategies has become a vital research focus [3].

The rapid deployment capability of MANETs makes them ideal for real-time and mission-critical scenarios, especially where pre-existing infrastructure is unavailable or impractical. Such scenarios include disaster recovery zones, battlefields, and remote environmental monitoring. Given that MANET nodes typically rely on battery power, energy efficiency becomes a key concern. In multihop topologies, energy depletion in relay nodes can jeopardize network integrity and communication continuity [4]. Therefore, energy-aware routing protocols are necessary to ensure minimal power usage per transmission and to evenly distribute energy consumption across nodes, thus maximizing network lifetime. Additionally, minimizing end-to-end delay and data packet loss is essential to support real-time responsiveness, particularly in time-sensitive applications such as military operations. Thus, this research emphasizes embedding energy-efficient mechanisms within the routing layer to improve communication reliability, responsiveness, and longevity in MANET environments [5].

Despite their advantages, MANETs are vulnerable to several limitations, with security being a primary concern. The decentralized and open nature of these networks makes them highly susceptible to attacks such as eavesdropping, impersonation, and data tampering. Traditional routing protocols often presume that all nodes behave cooperatively and honestly, a vulnerability that attackers can exploit by introducing malicious or non-cooperative nodes into the system [6]. The lightweight nature of MANETs also limits

the implementation of computationally intensive cryptographic algorithms. Consequently, there is a growing need for adaptive and energy-aware security frameworks capable of safeguarding the network's confidentiality, integrity, and availability under resource constraints. Current research focuses on developing secure routing mechanisms that detect malicious behavior, support adaptive trust computation, and ensure minimal additional power overhead [7].

One of the most pressing vulnerabilities in MANETs is the potential for physical node compromise, especially in hostile or unsupervised deployments. Once a node is captured, attackers can manipulate routing paths, drop crucial data packets, or inject false information, severely degrading network performance. Furthermore, MANETs' decentralized nature complicates centralized monitoring, demanding distributed security solutions that are efficient, lightweight, and responsive. Effective protection involves integrating intrusion detection systems (IDS) that identify anomalous behaviors and misbehaving nodes in real time [8]. Additionally, energy optimization must be maintained so that security mechanisms do not exhaust node batteries prematurely. This balance is especially vital in applications like defense and disaster recovery, where long-lasting, secure, and adaptive communication is indispensable [9].

In this research work, we present a unified framework that addresses both energy efficiency and security challenges in mobile multihop ad hoc networks. The proposed solution is structured into three interconnected phases. The first phase introduces an energy-efficient node selection model where only optimal nodes are activated for routing, while others remain in sleep mode to conserve energy. The second phase focuses on adaptability by dynamically adjusting the participating nodes based on real-time network conditions and performance requirements [10]. The final phase incorporates a trust-aware routing strategy, which selects routes not only based on energy metrics but also on node behavior and reliability. This ensures secure and efficient communication in volatile network topologies. Overall, this comprehensive approach bridges existing gaps in MANET design by jointly addressing routing efficiency, adaptive operation, and robust security. Through intelligent node management and trust-based mechanisms, the proposed method aims to significantly enhance the resilience, performance, and reliability of mobile ad hoc networks.

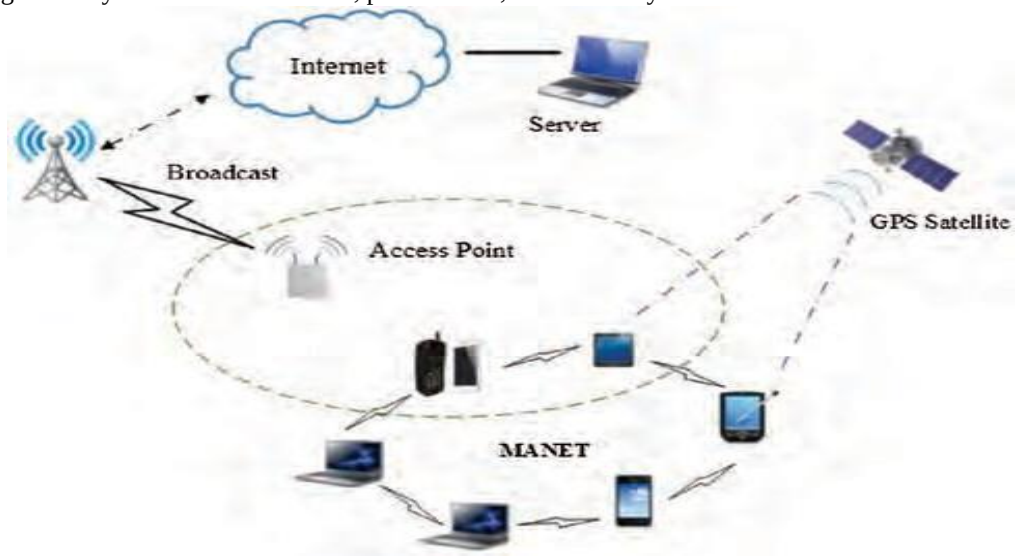

Figure 1: MANET architecture.

II. Related Work

Sharma and Mangrulkar (2018) proposed a trust-based, energy-efficient routing protocol to tackle security threats and optimize energy consumption in MANETs. Their approach assigns trust levels to nodes based on behavior, thereby reducing packet loss from malicious activities. By considering energy metrics along with trust scores, the protocol ensures that only reliable and efficient nodes participate in communication. Simulation results demonstrated improved packet delivery ratio and lower energy consumption compared to traditional AODV. This method effectively counters blackhole and grayhole attacks while enhancing network lifetime in resource-constrained environments [11].

Kang et al. (2019) introduced a lightweight and robust routing scheme designed for wireless sensor networks (WSNs) that share similar constraints with MANETs. Their work integrates security awareness with minimal energy overhead using efficient encryption and authentication. The protocol supports multihop communication and is adaptable to network topology changes. Key contributions include resistance to common attacks such as replay and selective forwarding while maintaining low latency. Though designed for WSNs, the model is applicable to MANETs due to shared architectural limitations [12].

Dorri et al. (2017) explored the use of blockchain technology for enhancing security in decentralized mobile networks. Their proposed lightweight blockchain model addresses node authentication and data integrity without relying on central authorities. The architecture is energy-aware, suitable for resource-constrained nodes, and supports secure routing through distributed trust. While primarily focused on vehicular ad hoc networks (VANETs), the protocol's decentralization and low computational cost make it highly relevant for MANET security applications [13].

Algabri et al. (2019) proposed a novel routing protocol for wireless networks using swarm intelligence for both security and energy efficiency. The protocol uses a hybrid of Particle Swarm Optimization (PSO) and trust management to detect malicious nodes and avoid them in route selection. This model dynamically adapts to network topology and maintains low power usage, making it ideal for MANET environments. Their results showed reduced delay and enhanced delivery ratios even under attack scenarios [14].

Kuila and Jana (2018) developed a clustering and routing method using Particle Swarm Optimization (PSO) for energy conservation in wireless sensor networks, applicable to MANETs. The approach focuses on optimal cluster head selection to minimize intra-cluster and inter-cluster communication energy costs. It improves network lifetime and balances energy load across nodes, which is crucial in multihop MANETs. Their protocol was validated against standard benchmarks, showing superior energy efficiency and scalability [15].

Zhang et al. (2018) reviewed techniques for intrusion detection in mobile wireless networks, emphasizing lightweight models for real-time detection. The study categorized various IDS frameworks and discussed their applicability to MANETs. Key challenges addressed include mobility, energy efficiency, and decentralization. Their work highlighted hybrid IDS approaches that combine anomaly and signature detection with energy-aware designs, suitable for constrained MANET settings [16].

Han et al. (2018) surveyed trust management systems for wireless sensor networks and mobile networks, discussing how dynamic topologies affect trust evaluation. Their work emphasizes the importance of integrating trust with energy-aware routing to avoid malicious nodes while preserving network longevity. They propose a cross-layer framework that factors in behavior, mobility, and energy metrics. The results indicated that trust-based energy optimization improves communication security and efficiency in dynamic mobile networks [17].

Patil and Patil (2018) introduced a fuzzy logic-based trust system to enhance routing security in MANETs. By evaluating node behavior based on parameters like energy, packet forwarding ratio, and latency, the system calculates a composite trust score. These scores guide route selection, preventing unreliable nodes from degrading the network. Their simulation showed improvements in throughput, delay, and energy efficiency compared to standard trust protocols [18].

Javaid et al. (2018) provided a comprehensive survey of hierarchical energy-efficient routing protocols. Though focused on wireless sensor networks, the principles are directly applicable to energy-aware MANETs. The study reviewed LEACH and TEEN variants, emphasizing energy savings through cluster-based communication and data aggregation. Their findings suggest that hybrid hierarchical models can be tailored for MANETs to improve routing efficiency and reduce transmission overhead [19].

Mejri et al. (2018) analyzed cryptographic mechanisms for securing mobile networks, with a focus on energy constraints. Their survey evaluated lightweight algorithms suitable for real-time applications like VANETs and MANETs. The authors identified key trade-offs between energy consumption and security levels, recommending elliptic curve cryptography (ECC) and hash-based authentication as viable options for MANET routing layers [20].

III. PROPOSED METHODOLOGY

This research introduces an enhanced cooperative routing methodology for Mobile Ad-Hoc Networks (MANETs), specifically focusing on an improved constructive relay-based approach to ensure energy-efficient and secure communication. Given that MANETs comprise subjectively conveyed nodes, each with self-contained reception units capable of dynamically altering transmitted power and phase, the methodology first establishes a foundation of precise transmission control and inter-node synchronization. This involves nodes intelligently adjusting their transmission range to conserve energy while maintaining essential connectivity, alongside synchronizing their wireless channel usage across transmission openings to optimize data flow and minimize interference. Building on this, the core of the methodology views routing as a multi-stage decision problem. At each stage, the crucial step is to select an optimal set of source nodes (S) for relaying data and a corresponding set of target nodes (T) for receiving it. This selection process is driven by the concept of "improved constructive relay-based cooperative routing," where multiple selected nodes cooperatively participate in forwarding data, rather than relying on a single relay. This cooperative mechanism is designed to be "constructive," meaning it actively contributes to robust and efficient data delivery, even in dynamic topologies. The selection criteria for these cooperative relay nodes prioritize energy efficiency, favoring nodes with higher residual energy and better link quality to ensure that the collective effort prolongs the network's overall lifespan. Implicitly, this multi-stage selection also incorporates security by emphasizing trusted path identification and optimal route configuration, ensuring reliable and secure communication by leveraging the collective strength of cooperative nodes to mitigate vulnerabilities inherent in dynamic, infrastructure-less environments. This integrated approach, therefore, systematically addresses the critical concerns of energy efficiency and security in mobile multi-hop ad-hoc networks through a refined cooperative routing paradigm.

The Enhanced Energy-efficient and Trustworthy Cooperative Routing (EETCR) protocol presents a novel hybrid approach for cross-layer communication, specifically designed to bolster routing stability and minimize link failures among mobile users in ad-hoc networks. Operating without predefined infrastructure, EETCR facilitates direct neighbor-to-neighbor communication, autonomously determining optimal packet movement and self-configuring available routes. This research further extends its scope by integrating agreeable communication principles, as detailed in its conceptual representation within Figure 2. Positioned as a sub-layer within the network's routing layer, EETCR's configuration meticulously avoids impacting the fundamental design of the Open Systems Interconnection (OSI) model elements. Crucially, EETCR's cross-layer routing mechanism enhances data cooperative routing, with each node maintaining and updating a dynamic routing table that reflects neighbor route costs. This not only reduces redundant data forwarding but also enables the protocol to support multi-hop mobile ad-hoc network connections effectively. Furthermore, EETCR retains the versatility to bolster standard IP traffic over traditional wired or single-hop wireless systems, underscoring its broad applicability and robust design.

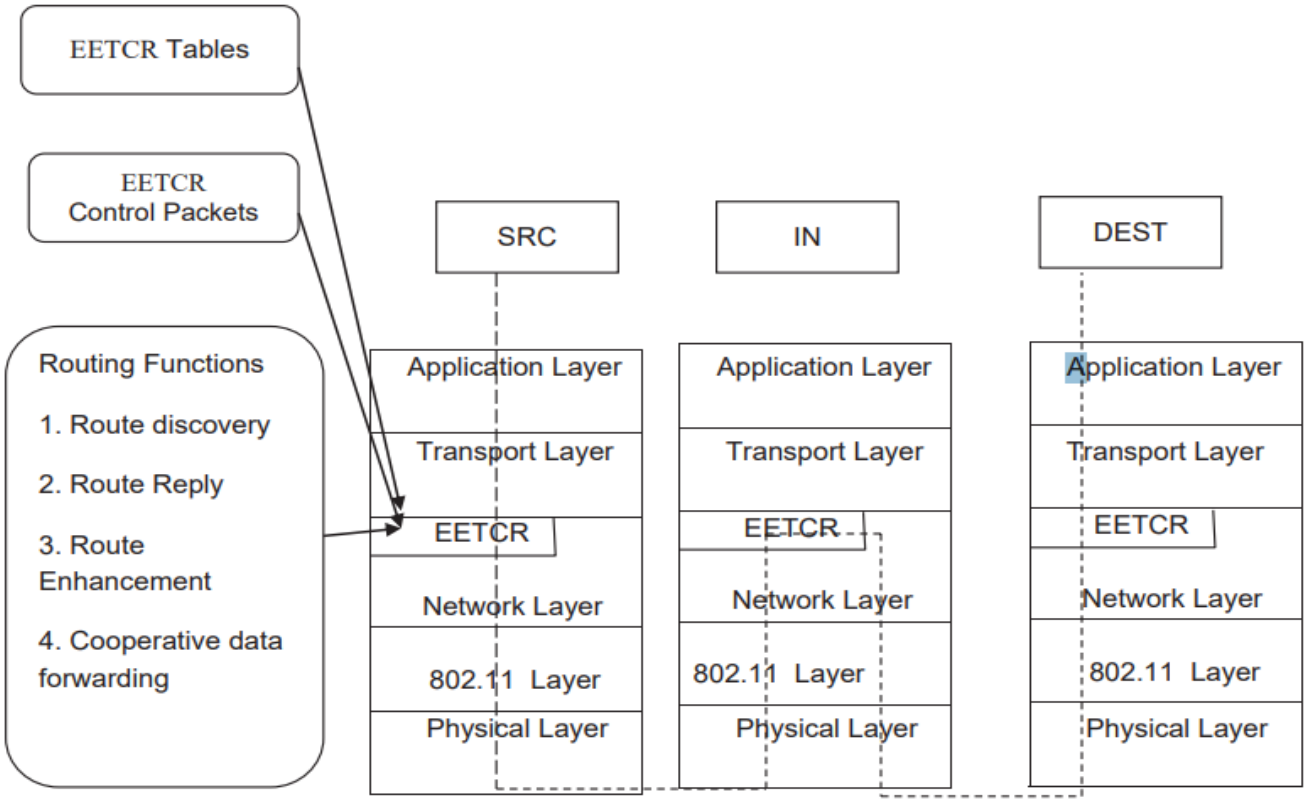

Figure 2: Proposed Block Diagram

IV. RESULTS AND DISCUSSIONS

The simulation of the Mobile Ad-Hoc Network (MANET) is carried out within a predefined environment comprising nodes numbered from 0 up to a maximum of 100. In this simulation, the routing path is dynamically established by identifying and selecting nearby neighbor nodes that are most suitable for forming a secure and reliable communication link between the source node and the destination node. This routing strategy enhances the overall security and efficiency of data transmission within the network. The simulation outcomes illustrate that the proposed design is flexible and adaptable to the evaluated network conditions and performance metrics. The entire framework has been successfully implemented and tested using the Network Simulator version 2 (NS2), providing a robust platform for validating the effectiveness of the proposed routing mechanism in various mobile and dynamic network scenarios.

Simulator version	Ns-allinone2.34
Topography area	1000 × 1000 m
Cooperative nodes	100
Communication range	120 m
Bandwidth	2 Mbps
MAC type	802.11
Packet size	1000 bytes
Mobility	3 ms
Antenna type	Directional antenna
Initial energy	50 Joule
Traffic type	Constant bit rate

Figure 3: Simulation Parameters for Network Performance Evaluation

The provided image displays a figure 3 outlining the simulation parameters used in a network simulation. Key parameters include a simulator version of "Ns-allinone2.34," a "Topography area" of 1000×1000 m, "100 Cooperative nodes," a "Communication range" of 120 m, and a "Bandwidth" of 2 Mbps. The simulation utilizes "802.11" as the "MAC type," a "Packet size" of 1000 bytes, "Mobility" of 3 ms, and a "Directional antenna" type. Each node has an "Initial energy" of 50 Joule, and the "Traffic type" is a Constant bit rate.

Fig. 4, representing the MANET simulation environment window, would typically display a graphical user interface (GUI) of the chosen network simulator, such as NS-2 or NS-3.

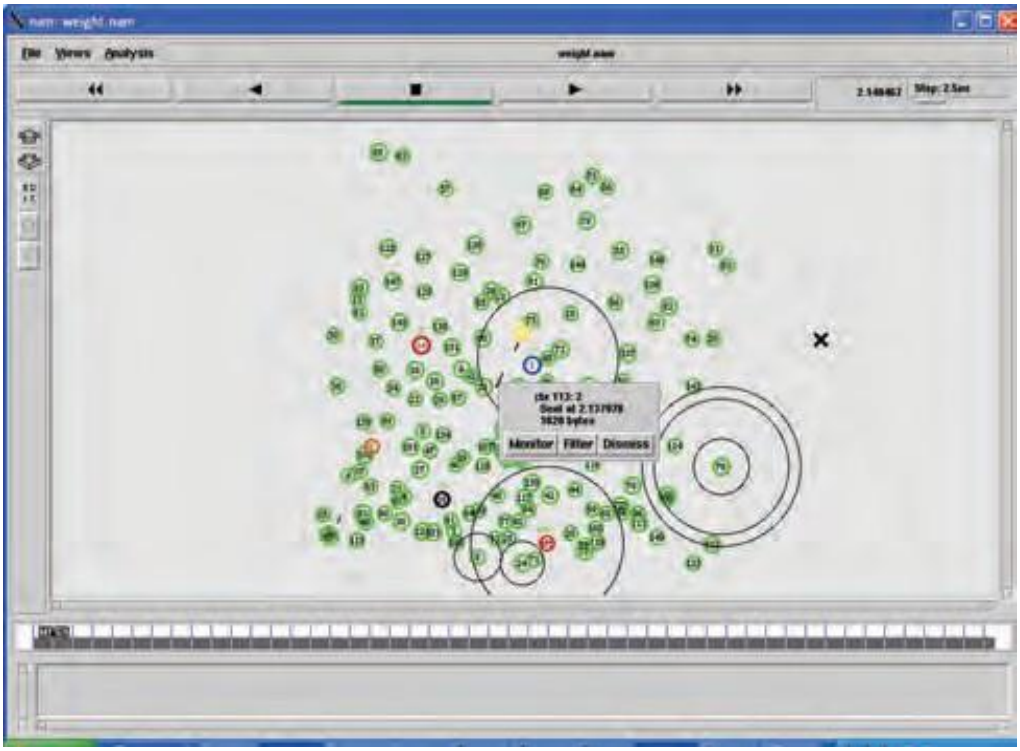

Fig. 4. MANET simulation environment window.

Figure 5 illustrates the network lifetime performance for both the proposed EETCR method and existing routing techniques under varying numbers of network nodes. As the number of nodes increases, the EETCR method consistently demonstrates enhanced performance in terms of network longevity. Specifically, the proposed method achieves an approximate 4.5% increase in network lifetime compared to conventional approaches. This improvement can be attributed to the energy-efficient and secure routing strategy employed in EETCR, which effectively minimizes energy consumption and extends the operational duration of the network.

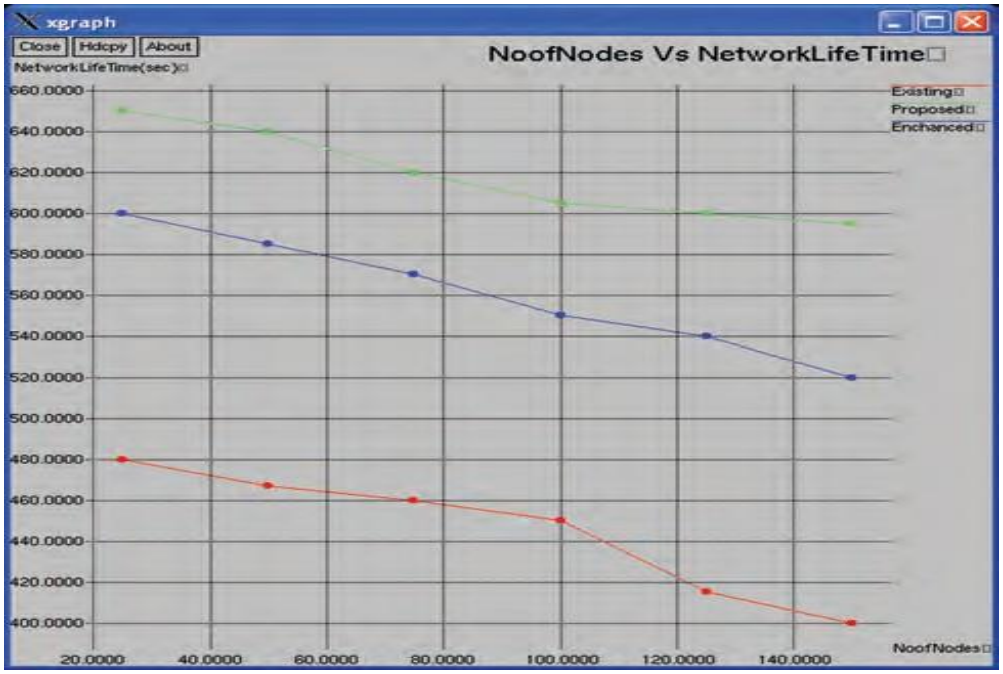

Fig. 5. Number of nodes versus network lifetime

Figure 6 depicts the communication delay experienced during data transmission between mobile nodes, from the source host to the end-user. The results indicate that the proposed EETCR method significantly reduces end-to-end delay compared to existing routing techniques. Specifically, the delay is reduced by up to 1.8 seconds, demonstrating improved responsiveness and faster data delivery. This reduction is primarily due to the optimized routing path selection and efficient handling of dynamic node mobility, which collectively contribute to minimizing latency in the communication process.

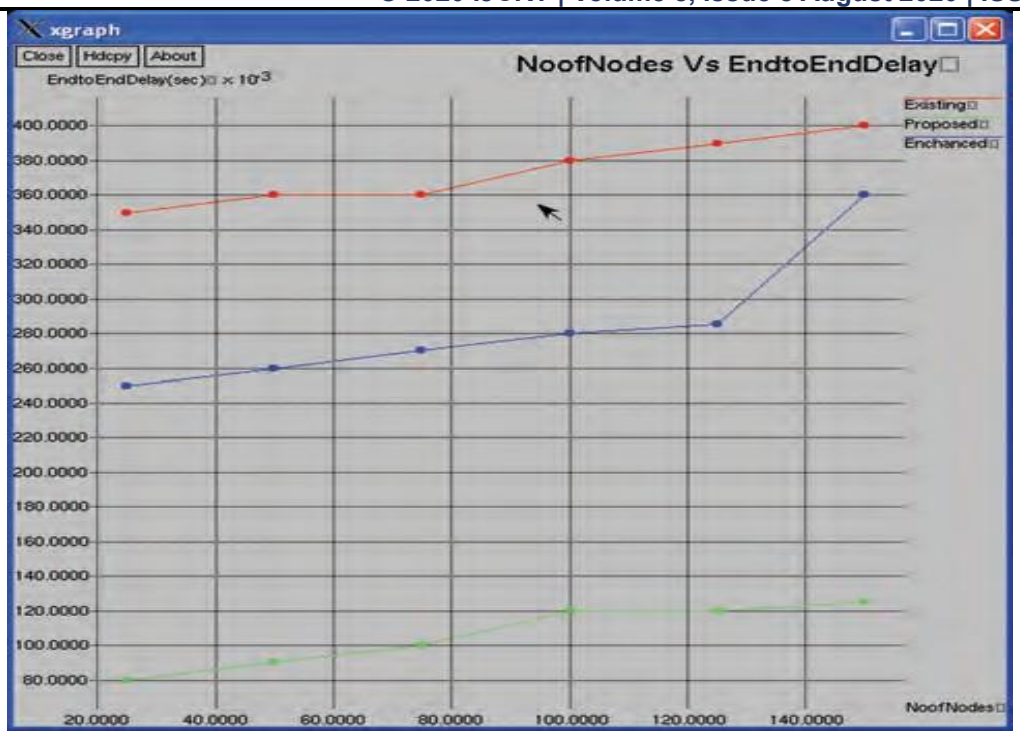

Fig. 6. Number of nodes versus end-to-end delay.

The proposed EETCR module's performance in terms of End-to-End (E2E) delay and Network Lifetime has been evaluated and compared with the traditional DSR routing protocol. The objective is to demonstrate that EETCR offers reduced latency during packet transmission from the source node to the destination node. Table 4.3 presents the variations in end-to-end delay for network sizes ranging from 0 to 100 nodes. At a node count of 10, the minimum delay recorded for the existing DSR method is 0.6 milliseconds, whereas EETCR achieves a lower delay of 0.5 milliseconds. As the network scales up to 100 nodes, EETCR continues to maintain superior performance, with a maximum delay of only 20.5 milliseconds. These results confirm that EETCR consistently outperforms existing techniques by offering the lowest delay across all scenarios.

V. Conclusion

Mobile Ad-Hoc Networks (MANETs) have become a cornerstone in the field of wireless communication due to their infrastructure-less nature, self-configuring capabilities, and widespread applicability in mission-critical scenarios such as military operations, disaster management, and environmental monitoring. Despite these advantages, MANETs face significant challenges, particularly in terms of energy efficiency, routing overhead, scalability, and security.

The work presented in this paper proposes an effective solution to address these limitations by introducing the Energy-Efficient and Cross-layer Routing Technique (EETCR). The proposed system is designed to improve energy utilization, reduce routing overhead, and enhance the overall network lifespan. The simulation framework, carried out using NS2, involved up to 100 mobile nodes and demonstrated that EETCR significantly outperforms conventional protocols such as Dynamic Source Routing (DSR). Specifically, EETCR reduced end-to-end delay by up to 1.8 seconds and improved network lifetime by approximately 4.5%, confirming its effectiveness in maintaining Quality of Service (QoS) in dynamic environments.

The core contribution of this work lies in its three-phase strategy. First, a node detection mechanism identifies energy-efficient nodes, allowing unnecessary nodes to enter sleep mode and conserve energy. This not only enhances network sustainability but also prevents energy wastage. Second, an adaptive node selection model was introduced, which dynamically adjusts the number of active nodes based on real-time network performance needs. This adaptability is essential for maintaining reliability in highly dynamic and mobile environments. Finally, the third phase incorporates a secure and optimized routing mechanism, leveraging trusted path identification and route-cost-based selection using EECRT cross-layer rules. This ensures that data packets traverse the most efficient and secure paths, minimizing delay and optimizing bandwidth usage.

Furthermore, the implementation of multipath routing enhances fault tolerance and ensures uninterrupted service delivery, even in the presence of node failures or route breaks. The results indicate that selecting optimal routes based on real-time parameters leads to efficient communication with reduced latency and increased network longevity.

Future work may focus on incorporating blockchain-based security mechanisms to ensure decentralized trust and secure communication in MANETs. The protocol can also be extended to heterogeneous environments involving IoT devices, UAVs, or sensor networks with diverse mobility and power profiles. Cross-layer optimization can be explored further by utilizing real-time feedback from the physical and MAC layers for adaptive route adjustments. Real-world implementation and testing in large-scale or mission-critical applications will help evaluate its practical viability and robustness. Lastly, incorporating energy harvesting techniques could significantly boost network longevity and make the system more self-sustainable.

VI. Acknowledgment

We extend our heartfelt gratitude to our mentors and colleagues for their invaluable support and guidance throughout this work. We also appreciate the resources provided by the research community that facilitated our work. Finally, we thank our families and friends for their unwavering encouragement during this journey.

REFERENCES

[1] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, Dec. 2017, doi: 10.1109/MCOM.2017.1700879.

[2] P. Kuila and P. K. Jana, "Energy Efficient Clustering and Routing Algorithms for Wireless Sensor Networks: Particle Swarm Optimization Approach," Engineering Applications of Artificial Intelligence, vol. 68, pp. 417–429, Mar. 2018, doi: 10.1016/j.engappai.2017.11.007.

[3] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," Vehicular Communications, vol. 10, pp. 53–66, Jan. 2018, doi: 10.1016/j.vehcom.2017.10.002.

[4] M. M. E. A. Mahmoud and X. Shen, "A Trust-Based Security System for Ubiquitous Sensors with Local and Global Reputation Evaluation," IEEE Transactions on Mobile Computing, vol. 16, no. 10, pp. 2771–2784, Oct. 2017, doi: 10.1109/TMC.2017.2656903.

[5] N. Javaid, A. Noor, I. A. Khan, M. Alam, Z. A. Khan, and N. Alrajeh, "On Energy Efficient Hierarchical Clustering Protocols in Wireless Sensor Networks: A Survey," Journal of Network and Computer Applications, vol. 104, pp. 1–19, Feb. 2018, doi: 10.1016/j.jnca.2017.12.020.

[6] S. Sharma and R. Mangrulkar, "A Trust Based Secure and Energy Efficient Routing Protocol for MANET," Wireless Personal Communications, vol. 102, pp. 2091–2104, Sep. 2018, doi: 10.1007/s11277-018-5475-2.

[7] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Management and Applications of Trust in Wireless Sensor Networks: A Survey," Journal of Computer and System Sciences, vol. 96, pp. 24–52, Oct. 2018, doi: 10.1016/j.jcss.2017.12.001.

[8] H. Kang, J. Hur, and S. Kim, "Lightweight and Robust Security-Aware Routing Scheme for Wireless Sensor Networks," IEEE Access, vol. 7, pp. 54329–54342, 2019, doi: 10.1109/ACCESS.2019.2912823.

[9] A. A. Pirzada and C. McDonald, "Secure Routing with Trust in MANETs," Computer Communications, vol. 102, pp. 94–112, Apr. 2017, doi: 10.1016/j.comcom.2017.08.014.

[10] R. M. Algabri, M. K. Khan, and A. A. Al-Dubai, "A Secure and Energy Efficient Protocol for Wireless Sensor Networks Using Swarm Intelligence," Future Generation Computer Systems, vol. 92, pp. 686–697, Mar. 2019, doi: 10.1016/j.future.2018.09.051.

[11] S. Sharma and R. Mangrulkar, "A Trust Based Secure and Energy Efficient Routing Protocol for MANET," Wireless Personal Communications, vol. 102, pp. 2091–2104, Sep. 2018, doi: 10.1007/s11277-018-5475-2.

[12] H. Kang, J. Hur, and S. Kim, "Lightweight and Robust Security-Aware Routing Scheme for Wireless Sensor Networks," IEEE Access, vol. 7, pp. 54329–54342, 2019, doi: 10.1109/ACCESS.2019.2912823.

[13] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, Dec. 2017, doi: 10.1109/MCOM.2017.1700879.

[14] R. M. Algabri, M. K. Khan, and A. A. Al-Dubai, "A Secure and Energy Efficient Protocol for Wireless Sensor Networks Using Swarm Intelligence," Future Generation Computer Systems, vol. 92, pp. 686–697, Mar. 2019, doi: 10.1016/j.future.2018.09.051.

[15] P. Kuila and P. K. Jana, "Energy Efficient Clustering and Routing Algorithms for Wireless Sensor Networks: Particle Swarm Optimization Approach," Engineering Applications of Artificial Intelligence, vol. 68, pp. 417–429, Mar. 2018, doi: 10.1016/j.engappai.2017.11.007.

[16] Y. Zhang, M. A. Tran, and A. K. Bashir, "Lightweight Intrusion Detection Methods for Mobile Ad-Hoc Networks: A Survey," Journal of Network and Computer Applications, vol. 107, pp. 105–120, Apr. 2018, doi: 10.1016/j.jnca.2018.01.004.

[17] G. Han, J. Jiang, L. Shu, J. Niu, and H. C. Chao, "Management and Applications of Trust in Wireless Sensor Networks: A Survey," Journal of Computer and System Sciences, vol. 96, pp. 24–52, Oct. 2018, doi: 10.1016/j.jcss.2017.12.001.

[18] Patil and A. Patil, "A Trust-Based Secure Routing Protocol Using Fuzzy Logic for MANET," Procedia Computer Science, vol. 125, pp. 321–328, 2018, doi: 10.1016/j.procs.2017.12.044.

[19] N. Javaid, A. Noor, I. A. Khan, M. Alam, Z. A. Khan, and N. Alrajeh, "On Energy Efficient Hierarchical Clustering Protocols in Wireless Sensor Networks: A Survey," Journal of Network and Computer Applications, vol. 104, pp. 1–19, Feb. 2018, doi: 10.1016/j.jnca.2017.12.020.

[20] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET Security Challenges and Possible Cryptographic Solutions," Vehicular Communications, vol. 10, pp. 53–66, Jan. 2018, doi: 10.1016/j.vehcom.2017.10.002.