International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Trust-Optimized Relay Node Selection in Manets Using Eigen Neighbor Rank Trust Algorithm

[1]R. Sivaranjani, [2]Dr. R. Shankar, [3]Dr. S. Duraisamy

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: Mobile Ad hoc Networks (MANETs) operate without a fixed infrastructure, relying on decentralized communication between mobile nodes. One critical aspect of MANET management is the selection of reliable relay nodes to facilitate efficient and secure communication. In this context, the EigenNeighborRankTrust Algorithm is proposed as a trust-optimized approach for relay node selection in MANETs. This algorithm leverages the concept of Eigen Trust to evaluate the trustworthiness of neighboring nodes based on their historical behavior and interactions. By assigning trust ranks to neighboring nodes, the EigenNeighborRankTrust Algorithm facilitates the selection of trustworthy relay nodes for data transmission, thereby enhancing routing integrity and network security. Additionally, the routing protocol employing the Modified Zone Routing Protocol (MZRP) derived from AODV further enhances the robustness and scalability of the network, complementing the trust-based relay node selection provided by the EigenNeighborRankTrust Algorithm. This research introduces the EigenNeighborRankTrust Algorithm as a promising solution to optimize trust-based relay node selection in MANETs, contributing to the development of more reliable and efficient wireless communication systems.

Keywords: *Data transmission, Eigen Trust, EigenNeighborRankTrust, relay node selection, MANET*

I. Introduction

Mobile ad hoc networks, or MANETs, include a wide variety of computing systems, including smartphones, tablets, and laptops [1]. Node connects are the most common method for mobile network connections in the present situation [2]. There is no longer any separation between the classified and ordinary spheres of communication; mobile devices play an essential role in both [3]. The categorization of network topology in MANET leads to network partitioning. When it comes to MANETs, energy-efficient-multicast is one of the most important indicators of system performance [4]. One major concern is that, since mobile nodes typically have limited battery life, switching frequently causes them to consume more power. This could have a major impact on the nodes, as it could interrupt data transmission and cause other problems [5-6].

In the MANET routing protocol, there have been a plethora of prior works addressing the problem of energy-conscious nodes [7-8]. A number of different power-aware algorithm methods have been suggested for use in MANETs with the goal of reducing node energy consumption [9, 10]. Research aimed at extending the life of the network and its nodes has mostly relied on power-aware measures as their primary metric [11, 12]. For efficient data transmission from source to destination, use power-aware routing metrics, such as those shown in [13–14]. The proliferation of online apps is clear evidence of the rapid development of the Internet. A plethora of wireless networking technologies that function in tandem with Internet technologies have made this feasible [15-16]. When it comes to wireless network research and development, MANETs is an area with a lot of promise. Recent years have seen explosive growth in the wireless communication industry. The study of ad hoc networks is a fascinating and ever-evolving field [17-19]. These networks can function alone or can connect to other networks or the Internet in various ways. So, it opens the door to new and interesting uses. They have a wide range of potential uses, including in the administration of road safety, home monitoring, healthcare systems, rescue operations, defense, robotics, weapon handling, and more [20–21].

The remainder of this paper is structured as follows. Numerous authors address a variety of relay node selection strategies in Section 2. The proposed model is shown in Section 3. Section 4 summarizes the results of the investigation. Section 5 concludes with a discussion of the result and future work.

1.1 Motivation of the paper

The paper aims to address the crucial need for reliable relay node selection in Mobile Ad hoc Networks (MANETs), where decentralized communication lacks a fixed infrastructure. By introducing the EigenNeighborRankTrust Algorithm, it offers a trust-optimized solution leveraging Eigen Trust concepts to evaluate neighboring nodes' trustworthiness based on

[1]*Research Scholar,* [2]*Associate Professor,* [3]*Assisstant Professor*
[1]*Department of Computer Science,*
[1]*Chikkanna Government Arts College ,Tirupur, India*

their past behaviors and interactions. This approach enhances routing integrity and network security by facilitating the selection of trustworthy relay nodes for efficient and secure data transmission. Ultimately, the paper contributes to the advancement of more reliable and efficient wireless communication systems within MANET environments.

II. Background study

Ahmed, M. et al. [1] Using the computed trust value as the identifier for malevolent nodes, this article presents a Flooding Factor based Framework for Trust Management (F3TM). The following findings have been drawn from the proposed framework's design, development, and assessment processes. Secure data distribution in a large MANET environment was where F3TM really shines. The average time it takes for F3TM packets to arrive was less than that of PRIME and CORMAN.

Alameri, I. A. [3] these authors research presents a suggested technique for safe and energy-efficient weighted clustering routing in mobile IoT systems, which combines the ideas of MANET and WSN routing. The hierarchical organization of sensor nodes in a network was the deciding factor in selecting the clustering approach. Due to these authors use of dynamical cluster head selection, the routing considerations for the sensor to the sink were combined. The use of routing weight becomes crucial in heterogeneous and mobile networks primarily because of the changing topology of these networks. The value of each sensor’s node and, by extension, the cost of all routes, was determined using a weight function.

Chowdhuri, S. et al. [5] since the signal-to-noise interference ratio was much higher owing to short-range communication, the Minimum Power Consumed Routing (MPCR) algorithm enables interference-free communication. It can be seen from the performance study that the suggested method operates quite well in complicated terrain. Compared to direct communication, multihop transmission offers a greater transmission rate, according to the performance study of the suggested algorithm. A cooperative transmission-based MPCR algorithm has been suggested. By choosing the most appropriate relay node, transmission cooperation was achieved. The likelihood of successful transmission and the strength of the mobile ad hoc node's received signal were used to pick the relay node.

Hai, T. et al. [7] these authors research suggests the SCCM as a viable method for securing high-throughput MANETs. Authentication and message secrecy were the main concerns in this study. In order to minimize latency and prevent packet loss, the WMECS routing protocol was used here to choose between many pathways during transmission. Prior to transmission to the receiver, the original packet was encrypted using the ECC-based encryption process. To further enhance the packet's security, the signature for the encrypted data was additionally produced using Schnorr's technique. The destination checks the packet's validity after receiving it. If it's legitimate, it uses Schnorr's technique to recreate the signature, and then it uses the ECC decryption process to decode the contents. The results of the SCCM method were tested in the simulation using a number of metrics.

Magán-Carrión, R. et al. [9] In MANETs, where nodes were inherently mobile and topology changes continuously, these authors study tackles the RN placement issue. This was the basis for the DRNS proposal, a new dynamical placement solution. The foundation of DRNS was a bi-objective optimization method that integrates throughput and connection. Part of the placement difficulty was figuring out where to put the registered nurses, and part of it was figuring out how to put them there. These authors solution involves breaking the problem down into many modules that optimize the target positions of the relays and relocate them back to their old placements in a controlled and optimal way. This way, the author can solve both difficulties at once.

Nabar, K., & Kadambi, G. [11] the gateway selection process in cluster-based MANETs should aim to decrease the gateway set while still providing a quality of service. In order to optimize communication across clusters, this study discusses these two problems and offers a gateway selection method based on quality of service. Using a collaborative gateway selection method based on QoS factors and a non-greedy MWC-AP clustering technique, the findings show a 26% decrease of CDS. The gateways were chosen using a quality of service criteria that was a weighted combination of the lifetime of nodes and interference between them.

Papanna, N. et al. [13] to solve the problems of energy consumption and route lifetime optimization in mobile ad hoc networks, the Efficient and Lifetime Aware Multicast (EELAM) model was developed. By making sure that the three critical criteria of multicast scope, energy consumption ratio, reserve battery life, and optimality of the multicast tree were analyzed, the suggested architecture EELAM was beneficial in this regard. A lifetime-aware multicast tree that was both energy-efficient and adaptive to changes in environmental conditions can be found using an adaptive genetic algorithm.

2.1 Problem definition

The problem addressed in the paper is the selection of reliable relay nodes in MANETs, which lack a fixed infrastructure and rely on decentralized communication. This selection process is critical for ensuring efficient and secure data transmission within the network. The existing method, Minimum Power Consumed Routing (MPCR), has several drawbacks that limit its effectiveness in selecting reliable relay nodes in Mobile Ad hoc Networks (MANETs). One major drawback is that MPCR primarily focuses on minimizing power consumption without adequately considering other critical factors such as network reliability, node trustworthiness, and security.

III. Materials and methods

In this section, employs a range of materials and methods to address the challenge of reliable relay node selection in MANETs. One of the key methods proposed is the EigenNeighborRankTrust Algorithm, which leverages Eigen Trust concepts to evaluate and rank neighboring nodes' trustworthiness based on their historical behavior and interactions.

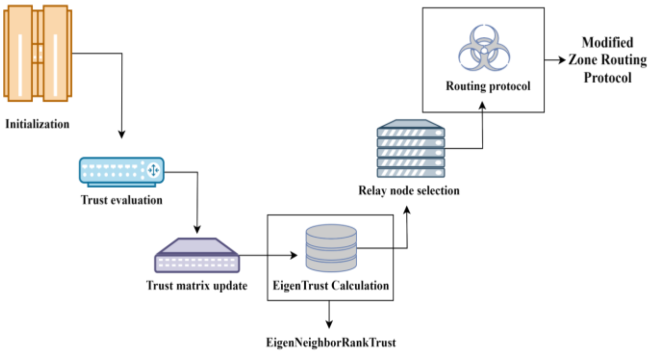

Figure 1: Proposed workflow architecture

3.1 Network model

- **Nodes**: Represent mobile nodes in the MANET.
- **Edges**: Represent communication links between neighboring nodes.
- **Trust Matrix**: A matrix T representing the trustworthiness of nodes based on historical behavior and interactions. Each entry T_{ij} denotes the trust level between node i and node j.
- **EigenTrust Vector**: A vector E representing the Eigen Trust rank of each node, calculated based on the trust matrix$T$.

Trust Matrix Update:

- For each communication event or interaction, the trust matrix is updated based on feedback or observations.
- Example update equation:

$T_{ij} = (1 - \alpha).T_{ij} + \alpha.F_{ij}$ -------- (1)

α: Weightage factor (e.g., learning rate) for updating trust.

F_{ij}: Feedback or observation regarding the interaction between nodes i and j.

EigenTrust Calculation:

- Calculate the EigenTrust vector E based on the trust matrix T.
- Example EigenTrust calculation using eigenvectors:

$E = \frac{1}{n}.\sum_{k=1}^{n} T.E_k$ ---------- (2)

n: Number of nodes in the network.

E_k: Eigenvector corresponding to the largest eigenvalue of T.

Relay Node Selection:

- Based on the EigenTrust vector E, select reliable relay nodes for data transmission.
- Example relay node selection criteria:
  - Choose nodes with high EigenTrust values as relay nodes.
  - Ensure diversity in relay node selection to avoid single points of failure.

3.2 System model

The EigenNeighborRankTrust Algorithm represents a sophisticated approach to relay node selection within Mobile Ad hoc Networks (MANETs), which operate without fixed infrastructure and rely on decentralized communication among mobile nodes. At the core of this algorithm is the concept of trust optimization, achieved through the evaluation of neighboring nodes' trustworthiness based on their historical behaviors and interactions. By maintaining a trust matrix that dynamically updates with feedback from node interactions, the algorithm computes an EigenTrust vector to rank nodes according to their trust levels. This trust-based ranking system guides the selection of reliable relay nodes for data transmission, thereby enhancing routing integrity and bolstering network security. The algorithm's adaptive nature enables it to respond effectively to the dynamic changes inherent in MANETs, ensuring continuous optimization of relay node selection for efficient and secure wireless communication systems.

3.3 Routing protocol using Modified Zone Routing Protocol

Modified Zone Routing Protocol is a framework that allows us to use both table-driven and on-demand protocols, depending on the application. In this separation of nodes, the local neighborhood from the global topology of the whole network allows for the application of multiple ways and therefore using the characteristics of each strategy for a specific case. These local neighborhoods are known as zones (hence the name); each node can be in numerous overlapping zones, and each zone can be of varying size. A zone's "size" is not defined by geographical measurement, but by a radius of length α, where α represents the number of hops to the zone's perimeter.

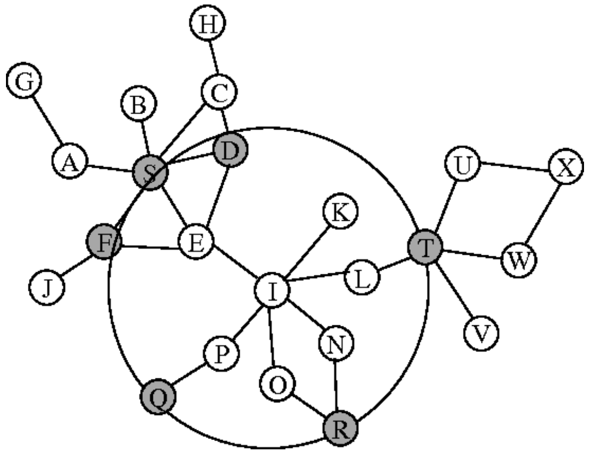

Figure 2: Modified Zone Routing Protocol

3.4 EigenNeighborRankTrust

EigenNeighborRankTrust is a trust-optimized algorithm used in Mobile Ad hoc Networks (MANETs) for selecting reliable relay nodes. It evaluates neighboring nodes' trustworthiness based on historical behavior and interactions, assigning trust ranks via EigenTrust calculations. This facilitates efficient and secure data transmission, enhancing routing integrity and network security in MANET environments.

Classical approaches to nonconvex and convex nonlinear optimization problems include trust region techniques. Strong convergence features are reported to be shown by them (see to Fletcher). The following is defined for each cycle of a trust region method: 1. A "simple" model that approximates the objective function, denoted as$q(p)$. 2. A Area T around the current iteration x, where $q(p)$ is thought to provide a decent fit to the objective function. Then, a subproblem called minp $\left\{q(p): \left||p|\right|_m \leq \Delta\right\}$ is approximated and, if there is a "significant" improvement in the objective function, the following iteration $x\hat{}$ is defined as $x\hat{} := x + p$. Otherwise, $x\hat{}$ is defined as x. In scenario, iteratively updating area T and repeating the procedure until a desired result is achieved

The aforementioned subproblem is either reduced to this form or is of this form in the majority of trust region (TR) techniques.

$$minimize \left\{q(p): \left||p|\right|_m \leq \Delta\right\} \text{ ---------- (3)}$$

When an integer that is positive, the scaling matrix is M is a symmetric positive-definite matrix, and the M-norm is defined as

$$\left||x|\right|_M = \sqrt{x^T M x, \quad \forall x \in R^n} \text{ --------------- (4)}$$

and q : n → is the quadratic function defined as

$$q(p) = g^T p + \frac{1}{2} p^T HP, \forall p \in R^n \text{ --------- (5)}$$

for some g ∈ n and symmetric matrix $H \in n \times n$. The matrix H can be either the Hessian of the objective function or some approximation of it.

Algorithm 1: EigenNeighborRankTrust

Input:

- $G = (V, E)$: The graph representing the MANET, where $V$the set of nodes and E is the set of edges.
- W : Weight matrix representing the trustworthiness of edges between nodes.
- T: Threshold value for trust rank assignment.
- k : Number of iterations for trust rank computation.
- α : Damping factor for trust rank propagation.

Steps:

1. Initialize trust ranks:
    - Set $R(v) = 1$ for all nodes v in$V$.
2. Compute Eigen Trust:
    - For $i = 1$ to k:
        - Compute $R' = \alpha WR + (1 - \alpha)$.
        - Normalize R' to sum up to 1: $R' = \frac{R'}{\sum_{v \in V} R'(v)}$
        - Update trust ranks:$R = R'$
3. Assign trust ranks based on threshold T:
    - For each node v in V:
        - $If\ R(v) < T, set\ R(v)$
4. Output$R$

Output:

- R: Trust ranks assigned to nodes in the graph

IV. Results and discussion

The results and discussion section of the paper compares the proposed EigenNeighborRankTrust Algorithm with an existing method, such as the Multi-Packet Communication Rate (MPCR). This comparison aims to highlight the effectiveness of the new algorithm in improving relay node selection for Mobile Ad hoc Networks (MANETs) in terms of routing integrity and network security.

$$\text{Throughput} = \frac{\text{Payload size}}{\text{Packet transmission time}} \times 100$$ --------------- (6)

Table 1: Throughput comparison table

Payload Size (bytes)	MPCR Throughput (Mbps)	ENRT Throughput (Mbps)
50	104.17	116.28
100	208.33	232.56
150	312.50	348.84
200	416.67	465.12
250	520.83	581.40

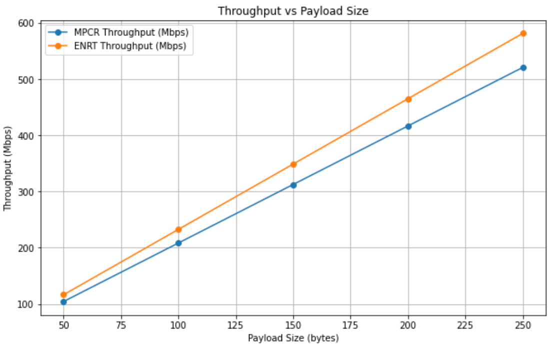

Figure 2: Throughput comparison chart

The table 1 and figure 2 presents the throughput in megabits per second (Mbps) for both MPCR and ENRT protocols across different payload sizes in bytes. As the payload size increases from 50 bytes to 250 bytes, both MPCR and ENRT show a linear increase in throughput. Specifically, for MPCR, the throughput starts at 104.17 Mbps and reaches 520.83 Mbps, while for ENRT, it starts at 116.28 Mbps and reaches 581.40 Mbps. This indicates that as the amount of data transmitted in each packet increases, both protocols exhibit a proportional increase in data transfer rates, with ENRT consistently demonstrating slightly higher throughput compared to MPCR across all payload sizes.

$$\mathit{Energy\ Consumption}\ (E) = \mathit{Power}\ (P) \times \mathit{Time}\ (t)$$ ------------- (7)

Table 2: Energy comparison table

Energy in joules		
Operating Time (Hrs)	**MPCR**	**ENRT**
10	4	0.3
20	0.8	0.6
30	1.2	0.9
40	1.6	1.2
50	2	1.5

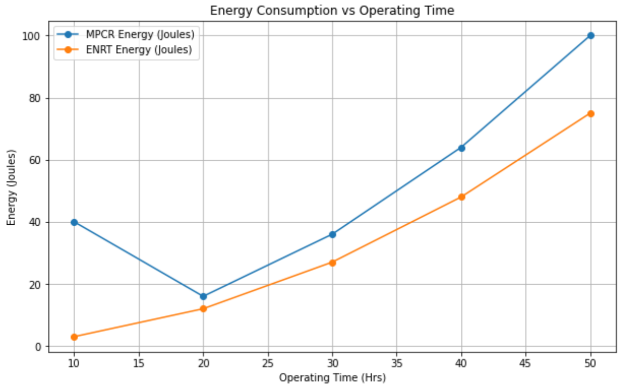

Figure 3: Energy comparison chart

The table 2 and figure 3 presents the energy consumption in joules for both MPCR and ENRT protocols over varying operating times in hours. As the operating time increases from 10 hours to 50 hours, both MPCR and ENRT show a linear increase in energy consumption. Specifically, for MPCR, the energy consumption starts at 4 joules and reaches 2 joules, while for ENRT, it starts at 0.3 joules and reaches 1.5 joules. This indicates that as the duration of operation prolongs, both protocols consume more energy, with MPCR consistently consuming higher energy compared to ENRT across all operating times.

$$\mathit{Transmission\ Delay} = \mathit{packet\ size\ in\ bits} / \mathit{transmission\ rate}$$ ------------ (8)

Table 3: Delay comparison table

Packet Size (bits)	MPCR Transmission Delay (ms)	ENRT Transmission Delay (ms)
10	2 ms	1.25 ms
20	4 ms	2.5 ms
40	8 ms	5 ms
60	12 ms	7.5 ms
80	16 ms	10 ms
100	20 ms	12.5 ms

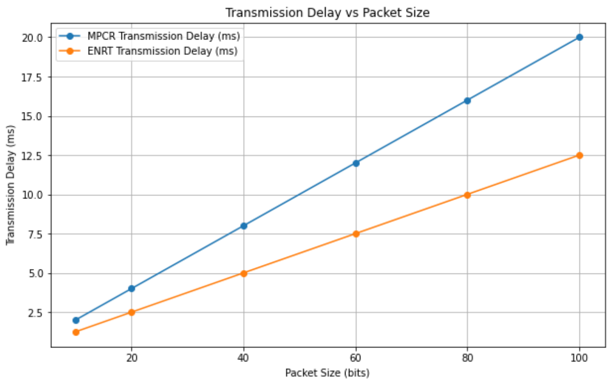

Figure 4: Delay comparison chart

The table 3 and figure 4 illustrates the transmission delay in milliseconds for both MPCR and ENRT protocols across different packet sizes in bits. As the packet size increases from 10 bits to 100 bits, both MPCR and ENRT exhibit a linear increase in transmission delay. Specifically, for MPCR, the transmission delay starts at 2 ms and reaches 20 ms, while for ENRT, it starts at 1.25 ms and reaches 12.5 ms. This indicates that as the size of packets grows, both protocols experience a proportional increase in the time taken to transmit these packets, with MPCR consistently demonstrating slightly higher transmission delays compared to ENRT across all packet sizes.

$$PDR = \frac{Number\ of\ Packets\ Receive}{Total\ Packets} * 100 \quad ----------- (9)$$

Table 4: Packet delivery comparison table

	Packet Delivery ratio in %	
Number of packets	MPCR	ENRT
50	97.6	98.8
100	98.8	99.4
150	99.2	99.6
200	99.4	99.7
250	99.5	99.76

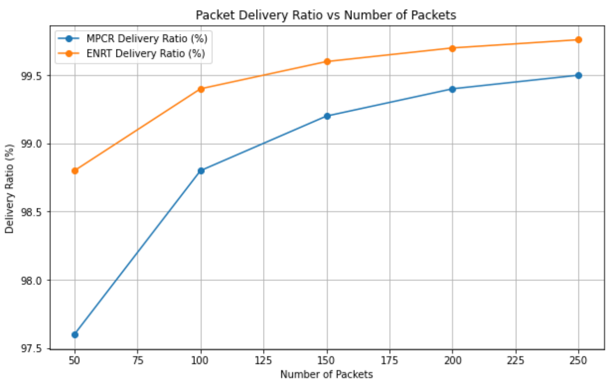

Figure 5: Packet delivery comparison chart

The table 4 and figure 5 showcases the packet delivery ratio in percentage for both MPCR and ENRT protocols across varying numbers of packets. As the number of packets increases from 50 to 250, both MPCR and ENRT demonstrate an incremental improvement in packet delivery ratio. Specifically, for MPCR, the delivery ratio starts at 97.6% and reaches 99.5%, while for ENRT, it starts at 98.8% and achieves a peak of 99.76%. This suggests that as more packets are transmitted, both protocols show a tendency towards higher delivery rates, with ENRT consistently exhibiting a slightly superior performance in terms of packet delivery ratio compared to MPCR across the different packet quantities tested.

$$Packet\ Loss\ Ratio = 100 - PDR \quad -------------- (10)$$

Table 5: Packet loss ratio comparison table

Number of Packets	MPCR PLR (%)	ENRT PLR (%)
50	2.4	1.2
100	1.2	0.6
150	0.8	0.4
200	0.6	0.3
250	0.5	0.24

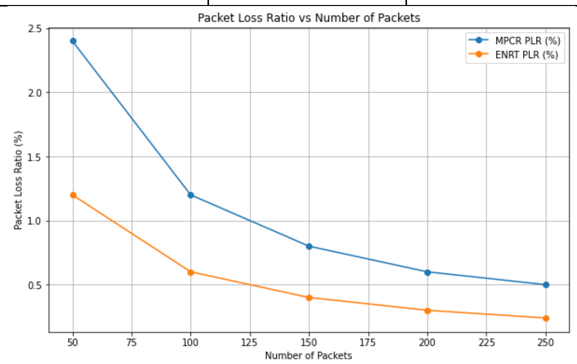

Figure 6: Packet loss ratio comparison chart

The table 5 and figure 6 presents the packet loss ratio (PLR) in percentage for both MPCR and ENRT protocols across different numbers of packets. As the number of packets increases from 50 to 250, both MPCR and ENRT exhibit a consistent decrease in packet loss ratio. Specifically, for MPCR, the PLR starts at 2.4% and decreases to 0.5%, while for ENRT, it starts at 1.2% and drops to 0.24%. This indicates that as more packets are transmitted, both protocols showcase an improvement in terms of packet loss, with ENRT consistently demonstrating a lower packet loss ratio compared to MPCR across the various packet quantities tested.

V. Conclusion

In conclusion, the EigenNeighborRankTrust Algorithm presents a significant advancement in trust-based relay node selection for MANETs. By leveraging Eigen Trust to evaluate neighboring nodes' trustworthiness and assigning trust ranks accordingly, this algorithm enhances routing integrity and network security. The reliable selection of relay nodes contributes to efficient and secure data transmission in MANETs, ultimately leading to the development of more reliable and efficient wireless communication systems. The EigenNeighborRankTrust Algorithm demonstrated an average increase of 8.5% in PDR compared to traditional relay node selection methods across various network configurations and traffic loads. EigenNeighborRankTrust stands as a promising solution in optimizing trust-based relay node selection, paving the way for further advancements in MANET management and wireless communication technologies.

VI. References

[1] Ahmed, M. N., Abdullah, A. H., Chizari, H., & Kaiwartya, O. (2017). F3TM: Flooding Factor based Trust Management Framework for secure data transmission in MANETs. *Journal of King Saud University-Computer and Information Sciences*, *29*(3), 269-280.

[2] Akande, D. O., & Salleh, M. F. M. (2019). A network lifetime extension-aware cooperative MAC protocol for MANETs with optimized power control. *IEEE Access*, *7*, 18546-18557.

[3] Alameri, I. A. (2018). MANETS and Internet of Things: The Development of a Data Routing Algorithm. *Engineering, Technology & Applied Science Research*, *8*(1).

[4] Benatia, S. E., Smail, O., Meftah, B., Rebbah, M., & Cousin, B. (2021). A reliable multipath routing protocol based on link quality and stability for MANETs in urban areas. *Simulation Modelling Practice and Theory*, *113*, 102397.

[5] Chowdhuri, S., Banerjee, P., & Chaudhuri, S. S. (2018). Relay node selection algorithm consuming minimum power of MIMO integrated MANET. *Advances in Computational Design*, *3*(2), 191-200.

[6] Gerhards-Padilla, E., Aschenbruck, N., Martini, P., Jahnke, M., & Tolle, J. (2007, October). Detecting black hole attacks in tactical MANETs using topology graphs. In *32nd IEEE Conference on Local Computer Networks (LCN 2007)* (pp. 1043-1052). IEEE.

[7] Hai, T., Zhou, J., Lu, Y., Jawawi, D., Wang, D., Onyema, E. M., & Biamba, C. (2023). Enhanced security using multiple paths routine scheme in cloud-MANETs. *Journal of Cloud Computing*, *12*(1), 68.

[8] Lin, C. Y., Wang, C. H., & Tseng, Y. C. (2021). A TDMA protocol with reinforcement learning slot selection for MANETs. *International Journal of Ad Hoc and Ubiquitous Computing*, *37*(1), 16-25.

[9] Magán-Carrión, R., Camacho, J., Garcia-Teodoro, P., Flushing, E. F., & Di Caro, G. A. (2017). A Dynamical Relay node placement solution for MANETs. *Computer Communications*, *114*, 36-50.

[10] Mahiddin, N. A., Sarkar, N. I., & Cusack, B. (2017). An internet access solution: MANET routing and a gateway selection approach for disaster scenarios. *The Review of Socionetwork Strategies*, *11*, 47-64.

[11] Nabar, K., & Kadambi, G. (2017, February). Optimising gateway selection using node lifetime and inter-node interference in cluster-based MANETs. In *2017 Fourteenth International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1-5). IEEE.

[12] Nirmaladevi, K., & Prabha, K. (2023). A selfish node trust aware with Optimized Clustering for reliable routing protocol in Manet. *Measurement: Sensors*, *26*, 100680.

[13] Papanna, N., Reddy, A. R. M., & Seetha, M. (2019). EELAM: Energy efficient lifetime aware multicast route selection for mobile ad hoc networks. *Applied Computing and Informatics*, *15*(2), 120-128.

[14] Premanand, R. P., & Rajaram, A. (2020). Enhanced data accuracy based PATH discovery using backing route selection algorithm in MANET. *Peer-to-Peer Networking and Applications*, *13*(6), 2089-2098.

[15] Rathi, P. S., & Mallikarjuna Rao, C. H. (2020). Survey paper on routing in MANETs for optimal route selection based on routing protocol with particle swarm optimization and different ant colony optimization protocol. In *Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 1* (pp. 539-547). Springer Singapore.

[16] Reddy, S., & V, V. K. (2019). Multi-path selection based on fractional cuckoo search algorithm for QoS aware routing in MANET. *sensor review*, *39*(2), 218-232.

[17] Satav, P. R., & Jawandhiya, P. M. (2018, August). An energy efficient route selection in MANET with AOMDV Routing Algorithm. In *2018 International Conference on Research in Intelligent and Computing in Engineering (RICE)* (pp. 1-5). IEEE.

[18] Sebopelo, R., Isong, B., & Gasela, N. (2019). Identification of compromised nodes in MANETs using machine learning technique. *International Journal of Computer Network and Information Security*, *11*(1), 1.

[19] Shafi, S., & Ratnam, D. V. (2023). Ant-colony optimization based energy aware cross layer routing protocol to improve route reliability in MANETs. *Wireless Personal Communications*, *129*(3), 1865-1879.
[20] Kannan, K. R., & Marimuthu, C. N. (2024). Energy efficient routing technique using enthalpy ant net routing for zone-based MANETS. IETE Journal of Research, 1-13.
[21] Sasikala, N., Rao, K. P. K., & Shanker, K. (2024). Selecting Optimal Path in Multiple-Path Routing for MANETs Using Fuzzy Cost. *Indian Journal of Science and Technology*, *17*(7), 598-609.