Babylonian Journal of Networking
Vol.2024, **pp**. 78–87
DOI: https://doi.org/10.58496/BJN/2024/009; ISSN: 3006-5372
https://mesopotamian.press/journals/index.php/BJN

Research Article

Secure Routing and Reliable Packets Transmission In MANET Using Fast Recursive Transfer Algorithm

M.Sahaya Sheela[1*], R.Suganthi[2], S.Gopalakrishnan[3], T. Karthikeyan[4], K. Jeevana Jyothi[5], K.Ramamoorthy[6]

[1]Department of Department of Electronics and Communication Engineering , Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, Tamil Nadu, India.

[2]Department of Electronics and Communication Engineering, Panimalar Engineering College, Poonamallee, Chennai-600123, Tamil Nadu, India,

[3]Department of Information Technology, Hindustan Institute of Technology and Science (Deemed To Be University), Kelambakkam, Tamil Nadu 603103, India.

[4]Computing and Information sciences, University of Technology and Applied Sciences - Salalah, Sultanate of Oman.

[5]Department of Electronics and Communication Engineering Ramachandra College of Engineering, Eluru, Andhra Pradesh 534007 ,India

[6]Department of Electronics and Communication and Engineering, PSNA College of Engineering and Technology,Dindigul 624622.Tamil Nadu,India.

ARTICLE INFO

Article History

Received 20 Mar 2024
Accepted 23 May 2024
Published 15 Jun 2024

Keywords

Mobile Ad-hoc Network (MANETs)

Fast Recursive Transmission Algorithm

Collision Detection

Secure Multipath Routing

Secure Location Aware Routing

ABSTRACT

Mobile Ad-hoc Network (MANET) autonomous operation can be multi-hop it is the infrastructure-less wireless network. Security is one of the biggest challenges in Mobile Adhoc Network. The MANETs security there are considerations must be so that the routing protocol in order to protect the secure data transmission. In the routing and security that is an important aspect for in a MANETs, existing method routing protocol, however, is not enough to security requirements. The proposed method using Fast Recursive Transmission Algorithm (FRTA) used designed to maximize the data security, routing optimization, minimizing the impact of malicious attack using Collision Detection Avoid Algorithm (CDAA) activity over the MANET and select the best path. Table-driven routing protocols, also known as proactive routing protocols, mandate that every node on the network keep up-to-date routing data. To maintain consistent routing information for network nodes, these protocols propagate frequent updates to the routing table throughout the network, necessitating changes to the network topology. There's a lot of overhead from these upgrades. The suggested FRTA algorithm lowers node data loss rates and increases network energy efficiency. Table-driven routing protocols, also known as proactive routing protocols, mandate that every node on the network keep up-to-date routing data. To maintain consistent routing information for network nodes, these protocols propagate frequent updates to the routing table throughout the network, necessitating changes to the network topology. There's a lot of overhead from these upgrades. The suggested FRTA algorithm lowers node data loss rates and increases network energy efficiency. The proposed method shows high performance than other existing evaluations of the most advanced security and routing energy, end-to-end delay, packet transfer rate, packet loss

1. INTRODUCTION

Wireless mobile devices serve as nodes in a dynamic, self-configuring network called a mobile ad hoc network (MANET). Applications in both the military and the civilian worlds are still growing. Its open nature and dynamic topology, among other innate features, make it susceptible to security risks. The attacker tampers with the routing mechanism and incites self-centered behavior within the network. Serious security concerns are raised for mobile nodes and their traffic by passive assaults. It is challenging to provide safe and dependable communications in high-stress environments like battlefields.

*Corresponding author. Email: hisheelu@gmail.com

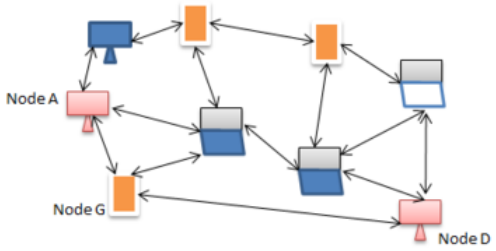

Fig.1. Architecture Diagram for secure routing in MANET

Figure.1 describe secure routing transmission from source node to destination node. In the reliability evaluation hierarchy, a hierarchical structure is adopted to improve the reliability measurement performance of each node. According to Secure Routing, key exchange provides secure communication capabilities and improves the reliability of the routing base and secure routing performance. Reliability evaluation is performed by measuring the packet transmission rate of every node to its neighboring nodes. The trust management node manages the measured trustworthiness of mobile nodes within each cluster, and the measured trustworthiness is used to configure routes between source and destination nodes. Keys are generated and exchanged between nodes without assistance for secure data communication. If the traffic on this route exceeds the cluster's average traffic, the node checks the sending node that transmits data between the source and destination nodes.

2. LITERATURE SURVEY

Gopalakrishnan, S. et al., (2022), discussed security and multi-path data transmission are difficult challenges during multipath routing protocols. To solve this issue, a RREQ packet based secure multipath routing and data transmission was deployed. A queuing-based approach can improve packet delivery rates by reducing delay, packet loss and flexibility.

John et al., (2023), as previously said, packet loss from hostile nodes, high energy consumption, and security are just a few of the issues MANETs face because of the highly dynamic nature of wireless technology. A Cooperative Self-Programming Secure Routing Protocol (CoS3RP) was employed to resolve this issue. Every node in the suggested model forwards packets in accordance with its authentication. In terms of routing performance, security, latency, and throughput, CoS3RP excels.

Thamizhmaran, K., (2023), as previously said, packet loss from hostile nodes, high energy consumption, and security are just a few of the issues MANETs face because of the highly dynamic nature of wireless technology. A Cooperative Self-Programming Secure Routing Protocol (CoS3RP) was employed to resolve this issue. Every node in the suggested model forwards packets in accordance with its authentication. In terms of routing performance, security, latency, and throughput, CoS3RP excels.

Tao et al., (2023), the clustering strategy, which divides the network into smaller networks called clusters, makes the MANETs under discussion extremely vulnerable. There may be nodes in these clusters that overlap and don't intersect. The cluster heads (CHs) are utilized to tackle this problem. System performance is improved and member node overhead is decreased as a result. Multipath routing, or CH for short, enables the network to find different routes that link resources and destinations.

Mahalakshmi, K et al., (2016), discussed that black hole attacks and traffic generation on routes remain unresolved, increasing packet transmission delay. To resolve the challenge, Secure Packet Transmission combining with the Heuristic Path Ranking Geographic Routing Protocol (SPT-HPR) scheme with efficient path ranking was deployed. The SPT-HPR framework captures packet-dropping nodes to reduce traffic rates. Compared to the advanced protocols, the proposed protocol significantly reduces the average delay time of secure path acquisition and improves the packet delivery rate.

Yang et al., (2020), discussed that frequent link failures due to dynamic topology characteristics and node mobility make routing difficult and expose vulnerabilities. To solve the issue. The key exchange between nodes does not need to go through CA, which increases the integrity of data exchange. The deployed protocol ensures node reliability assessment, routing and secure data transmission between nodes, so the network performance is stable even with malicious nodes.

Patil et al., (2018), highlighted how difficult it is to transfer data in a MANET due to its rapid growth and how each node functions as a gateway, making security concerns apparent. A Key Policy-Packet based Encryption (KP-ABE) technique was created in order to address the problem. It offers new-generation adaptive Routing Information Protocol (RIP) to find the best routes between autonomous power-constrained nodes and packet protection against malevolent clients. When

sending packets, it lowers communication costs and routing overhead. The deployed scheme's performance is examined for various evaluation criteria, node density levels, and routing attack types.

S. Gopalakrishnan et al., (2022), discussed that one of the security attacks on MANETs is the packet forwarding malpractice attack, which makes MANETs vulnerable because they exhibit message loss behavior. An Energy Efficient Clustering Protocol (EECP) in conjunction with a CH based on the Radial Basis Function (RBF) approach was implemented to solve the problem. The trust value of a node is determined by looking at its neighbors. This aids in the detection of hostile nodes that use the network to cause power outages and message loss.

Rajashanthi et al., (2020), emphasized that the most crucial component of secure transmission in a MANET is multipath routing, which is accomplished by disregarding egotistical and hostile nodes in the network. A novel secure multipath routing system with a focus on quality of service is implemented to provide dependable data transmission through the use of encryption technology. The suggested protocol's operational effectiveness is assessed using metrics such as packet delivery rate, end-to-end latency, etc.

Keerthika et al., (2018), addressed how open media communications and widespread dissemination expose most protocols to attackers. An upgraded AODV routing protocol using the ABC optimization technique was implemented to address the problem. To achieve the performance, the deployed approach makes use of computing cost, routing overhead, packet success rate, throughput, and parameter thresholds.

Narayana et al., (2018), mentioned that the primary problem is that attackers can readily access the networks because MANET can frame whenever needed without requiring any set infrastructure. A dynamic routing multi-mode routing technique based on cryptography strategy was designed to resolve the problem. The shortest path is found using the I-AODV protocol, which also offers a different approach to lower packet loss by putting forth a plan based on queuing calculations.

T.Chitrae et al., (2022) highlighted that in situations where establishing a fixed cellular communication infrastructure is impractical or practically unfeasible, dynamic networks can be built. A hybrid routing system called SDSR Secure Dynamic Source Routing Protocol was designed to address this problem. Obtain suggestions from nearby nodes to gauge the node's trustworthiness, then use this data to determine the node's trust value. Packet delivery rate, packet loss, and communication overhead measure the performance of SDSR.

Sekar, S et al., (2018), outlined how network overload, node failures, routing failures, and link failures may all cause packet loss in multicast routing. A cross-layer based, lightweight, dependable, and secure multicast routing technique was created to address this problem. When their values go below the minimum threshold, individuals are said to be acting inappropriately.

Jamaesha, S et al., (2019), since mobile nodes might relocate as needed, location-based routing is necessary for the transfer of packets. A Secure Location Aware Routing (SLAR) system was devised to accomplish the procedure. Particle swarm optimization is used in this research to forecast node locations in the future. A node's trust value is determined by its neighbors, which aids in predicting its future location, identifying hostile nodes inside the network, and minimizing packet loss.

Kumar et al., (2019), highlighted that the two primary causes of packet loss in MANETs are malicious packet loss and link problems. The node might act hostilely and negatively impact packet forwarding. A Homomorphism Linear Authenticator (HLA) protocol based on Improved Failure Aware Third Party Auditor (IFTPA) and integrating secured ad hoc on demand distance vector was implemented to address the issue. Malicious nodes and connection problems are the main causes of packet loss, which SAODV can identify.

V. G. Krishnan et al., (2022), talked about the absence of centralized management, the absence of preset devices, integration issues, and the existence of enemies within the network are some of the drawbacks of MANET. An Anonymous Location-Support and Self-reliance Routing (ALsSrR) technique was implemented to address the problem. This protocol's primary goals are to safeguard packets from hostile environments and offer message encryption for safe data transfer.

Samreen et al., (2018), certain basic properties—like its absence of infrastructure, self-organizing nature, and deployment flexibility—have been cited as contributing to its utility; nevertheless, less frequently mentioned features include open communication channels and dynamic topology changes. They are now vulnerable to security breaches. Path Allegiance Metric (PAM) and TMF were implemented in order to overcome these issues.

Hemalatha et al., (2023), highlighted that one of the key things to think about in MANETs is energy-efficient routing. The lifetime of the network is shortened when intermediate nodes lose energy as a result of a control failure. This is due to the fact that it impacts the node's capacity to relay packets on behalf of other nodes in addition to its own system. The

T-test approach was used to address the problem. This technique makes sure that every node taking part in path discovery has enough energy to transmit while iteratively determining the optimal communication strategy between nodes.

3. IMPLEMENTATION OF PROPOSED SYSTEM

The considered FRTA has trusted mobile ad hoc network nodes its public key is a path known to all nodes. Mobile nodes have different routing and security. The network is reliable and has a long lifespan. Nodes have long-term connections with the network therefore, with every in interactions, there is always an expectation of future reactions. Figure 2 explains the proposed diagram.

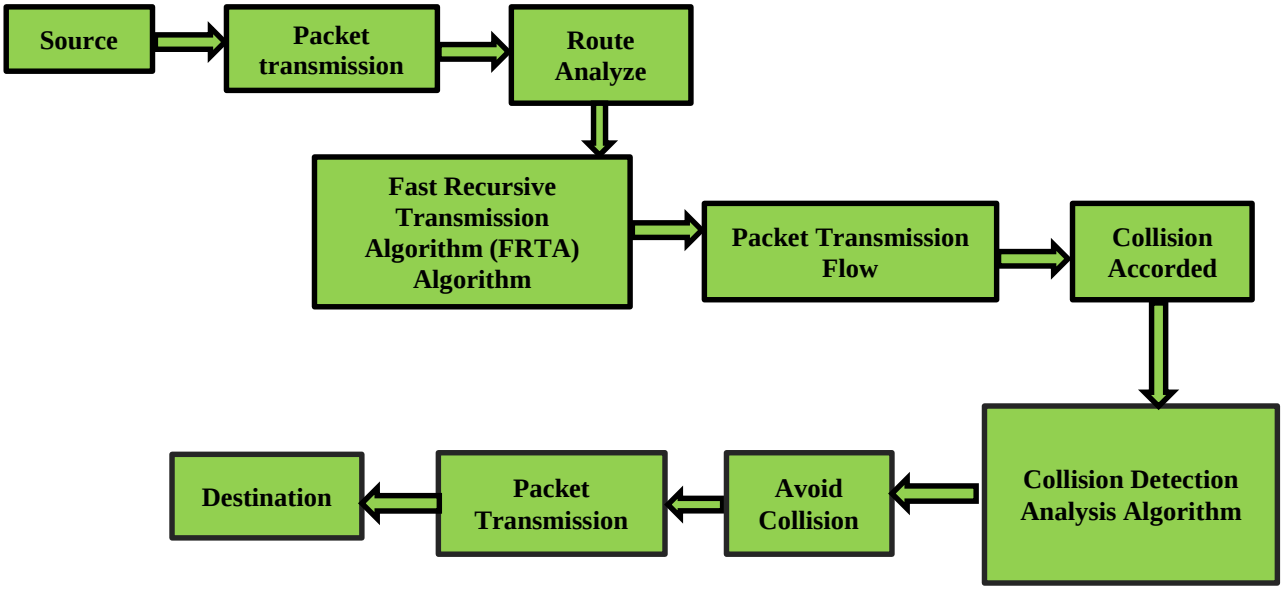

Fig. 2. Proposed diagram

Each node has a unique identity and routing pair a time-limited packet sent from a trusted path. Without a valid identity, nodes cannot communicate Trusted Path (TP) maintains the security and trust value of nodes. Each node contacts the TP to submit and update the number of packets and trust values of the involved nodes.

3.1. Fast Recursive Transmission Algorithm

The implementation of intricate and challenging applications, like packet transmission collision control and monitoring, has been made possible via wireless sensor networks (WSNs). The high-speed ramp path is accessible. The probability optimization method and the high-speed forwarding algorithm (FRDA) are used to determine the optimum node, it has the ability to adjust the search direction and set the automated search location. It offers sophisticated optimization and worldwide search features. When a node or collection of nodes joins a suggested routing-based network, a route is created. A common framework for collisions is provided by conventional partial path planning.

In general, these techniques lessen the standard deviation from the nodes' residual energy and enhance the energy distribution among sensor nodes. It was noted that the new function greatly raised the average energy expenditure while lowering the standard deviation. Consequently, a network's lifetime will rise when energy supply and consumption are properly balanced. Despite the fact that the suggested method has a high average power consumption, we utilized nodes with high energy since we considered their energy when designing the wiring. As a result, this test indicates that the network has a longer lifespan, the new fitness function performs better under conditions of accurate energy consumption distribution, and the harmonic search algorithm use this fitness function to more effectively optimize the trajectory.

Algorithm:

Input:

Number of Nodes, packet Size,

Output: Best path

Begin

Initialize node;

Evaluate path optimization;

While (the stopping criterion is not met)

Select shortest path from current packets;

Apply FRTA to selected paths;

Evaluate node

Set node equal to current packets;

Next generation until avoid collision

End while

End

It gained more importance over wireless networks in the recent decades because of their improved technology. Fast Recursive Transmission Algorithm (FRTA) improves determine the optimal transmission energy of the source and the relay nodes which minimizes the collision area. Because of this, the network's nodes all need to have modest transmission delays in order to reduce the number of lengthy transmission hops. When new routing protocols are introduced, many path collisions occur instead of a single node optimal path, extending the lifetime of wireless sensor networks.

3.2. Collision Detection Avoid Algorithm

Across the globe, wireless technologies are extensively employed to meet end users' communication needs. Nodes in wireless networks use route propagation to send information over the air. Only collisions that occur a specific distance away from the transmitting node can receive a packet that has been transmitted by that node. The transmission range is the term used to describe this distance. The environment, impediments, and the particular strategy employed to transfer the information all affect the transmission range in addition to the power level utilized for transmission. The cost of installing wireless networks has decreased in emerging markets compared to wireless networks of conflict, which is one benefit of using wireless networks.

Algorithm:

Input: Packets

Output: Collision C

Step 1: C £∞; bestc=0;

Step 2: while (fD not empty)

Step 3: for each a € C that appears in fD

Step 4: c = count(a)

Step 5: if (c > bestP)

Step 6: bestc=c; bestAttr a

Step 7: C C a

Step 8: fD Avoid Collision (fD, a)

Step 9: return C

Collision Detection Avoid Algorithm (CDAA) is a reduction of the collision area around sending nodes where a collision may occur, which is used to reduce the probability of a packet collision. This research examines the problem of minimizing collision probability in wireless sensor networks (WSNs) by using cooperative broadcasts and optimal route allocation.

3.3. Packet Transmission Flow

The algorithm starts with initialing the current value of avoid collision, R, to the empty set. Then, heuristic measure is applied to each conditional packet that appearing in the discernibility matrix for evaluation. This is packet a count of the number of appearances in the discernibility function. Packets having higher count is considered as significant. Therefore, the packet with the maximum heuristic value is added to the avoid collision and the remaining packets in the discernibility function are removed. This process is repeated for all packets present in the discernibility function. Finally, the algorithm terminates and returns the reduce Collision.

4. RESULTS AND DISCUSSION

We will present a method for creating a wireless network without the need for established infrastructure. Nodes in this design speak with one another without the assistance of access points. For certain purposes, networks that depend on fixed infrastructure are not always appropriate. For instance, permanent infrastructure may be damaged or rendered useless in remote locations and power zones. Under circumstances, packet transmission might not have enough time to build a reliable infrastructure. When two nodes are within radio range of one another, they can communicate in a distributed fashion. A node first functions as an access point, interacting with other nodes to create a network. Every node in the network is allowed to travel at random along the path.

4.1 Collision Detection

Prior algorithm utilized for both the secure sending and receiving of data, as well as the collision detection procedure IFTPA stands for Enhanced Failure Aware Third Party Auditor. Inadequate detection process performance Low level utilized for anomaly detection. There are three different approaches to collision avoidance: fully reactive, programmable, and path detection via the CDAA algorithm.

TABLE I. COLLISION DETECTION

No. of Packets	IFTPA **in %**	**RPTA in %**	**CDAA in %**
10	5	6	8
30	15	22	25
50	22	33	42
65	33	56	65
80	45	65	85
100	56	75	95

Table 4.1 discuss about the collision detection on network comparing to methods, the proposed systems compared existing system of the networks, the following methods are IFTPA, RPTA, the current methods of CDAA.

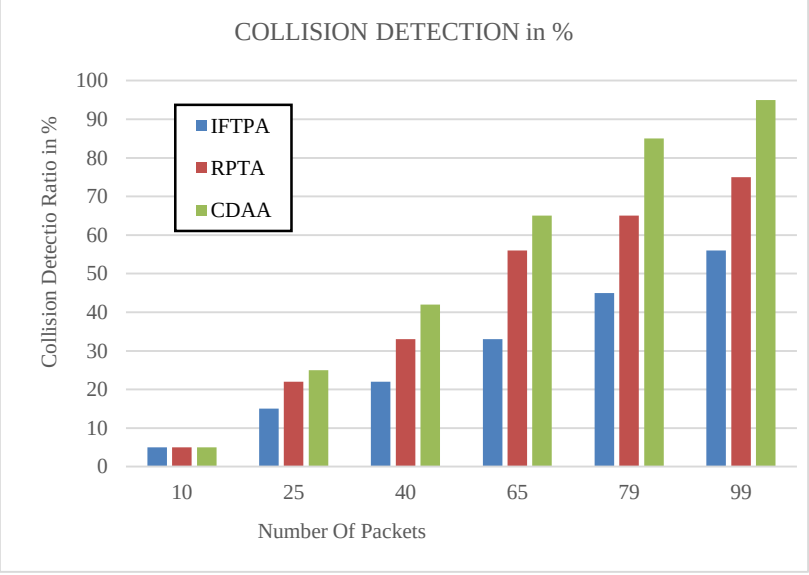

Fig.4. Collision Detection

Figure.4 shows that CDAA is proposed method comparison, IFTPA method 100 packets collision rate is 56%, and RPTA method 100 packets collision rate is 75%, and current method 100 packets collision rate is 95%.

4.2. Packet Transmission rate

The connection can be charged and provided to the MANET as a communication service between the mobile mode and the MANET. In order to simulate and prevent dynamic crashes, this study presents crash trajectory data based on a kinematic model and realistic driving behavior. To control packet travel, it employs strategies including path packet rate association (FRTA) and packet loss avoidance.

TABLE II. PACKET TRANSMISSION RATE

No. of Packets	IFTPA in %	RPTA in %	FRTA in %
10	5	6	8
30	15	22	25
50	22	33	42
65	33	56	65
80	45	63	85
100	50	70	90

Table 2 show discuss about the Packet Transmission rate on network comparing to methods, the proposed systems compared existing system of the networks, the following methods are IFTPA, RPTA, the current methods of CDAA.

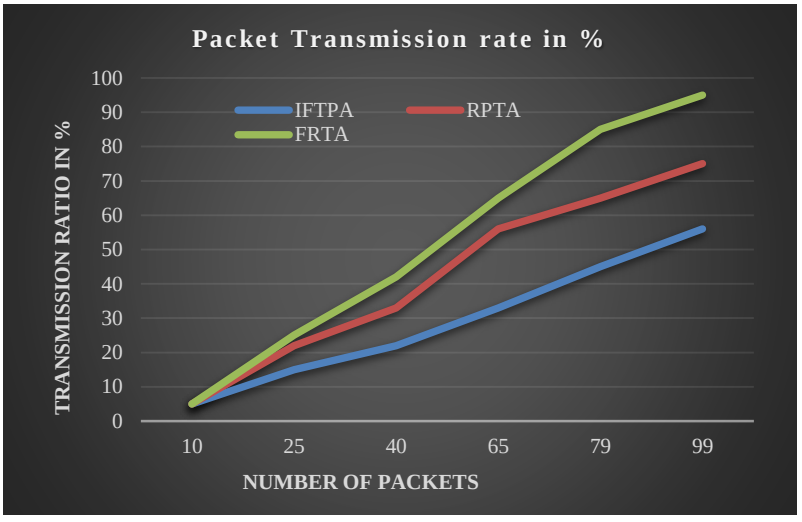

Fig .5. Packet Transmission rate

Figure.5 shows Packet Transmission rate that CDAA is proposed method comparison, IFTPA method 100 packets Packet Transmission rate is 50%, and RPTA method 100 packets Packet Transmission rate is 70%, and current method 100 packets Packet Transmission rate is 90%.

4.3 Transmission Delay in sec

Therefore, it is important to understand the performance of MANETs in line with the packet sending nodes. Unlike other common wireless networks, where the location of nodes is controlled by paths, MANETs have their own paths connected to nodes.

TABLE III. TRANSMISSION DELAY IN SEC

No. of Packets	IFTPA **in sec**	**RPTA in sec**	**CDAA in sec**
10	15	10	5
30	27	22	15
50	38	33	22
65	49	56	33
80	69	63	45
100	80	70	50

Table.3 since discuss about the Transmission Delay in sec on network comparing to methods, the proposed systems compared existing system of the networks, the following methods are IFTPA, RPTA, the current methods of CDAA.

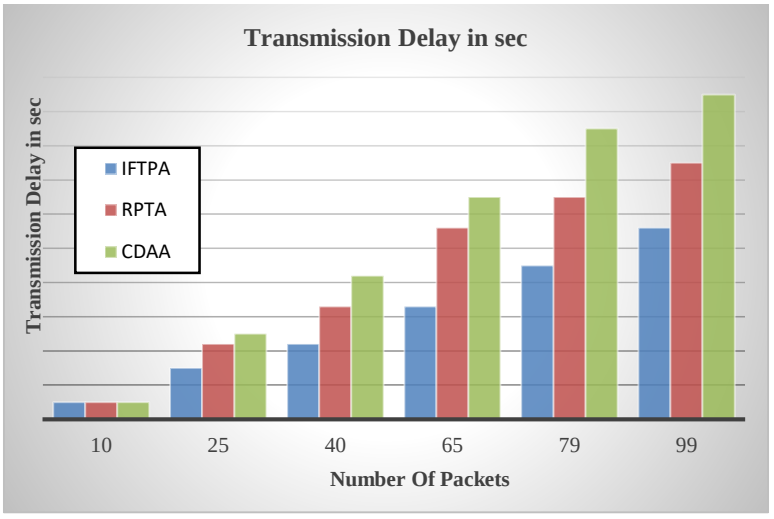

Fig.6. Transmission Delay in sec

Figure.6 shows that Packet Transmission Delay that CDAA is proposed method comparison, IFTPA method 100 packets Packet Transmission rate is 80%, and RPTA method 100 packets Packet Transmission Delay is 70%, and current method 100 packets Packet Transmission rate is 50%.

5. CONCLUSION

The technique seen from above results in the end-to-end transmission delay caused by secure packet transmission and collision avoidance. Neighboring nodes are those that move the sender in the same direction along the path across the receiver and never cause the packet to be delayed during transmission. Certain protocols usually introduce a new round path discovery and discard the entire original path. Even in the case where the root separator has just one connection, this is still valid. When a data packet travels to its destination, the corresponding downstream node along the path checks whether the upstream node has maintained an updated path and identifies the path packet and the risk before sending this field. Enter values in the fields. Optimal transmission path, effective and reliable deep packet inspection technology helps in stream classification. The current packet transmission rate is limited in points, and a possible solution to ensure long distance of nodes is to create multiple mechanisms through wireless relays. Hop transmission links and secure routing are important issues to solve in MANETs. The performance collision rate is 95%**,** and Packet Transmission rate is 90%.

Conflicts Of Interest

The absence of any competing relationships or biases that could affect the research is explicitly mentioned in the paper.

Funding

The author's paper asserts that the research was conducted on a voluntary basis and without any financial backing from institutions or sponsors.

Acknowledgements

I wish to acknowledge the facilities provided by Publishing this Research article by “Centre for Networking and Cyber Défense” (CNCD) - Centre for Excellence, Department of Information Technology, Hindustan Institute of Technology and Science, Kelambakkam, Tamil Nadu -603103, India

References

[1] B. Praveen, D. Samanta, M. Kaur, and H.-N. Lee, "Data Security-Based Routing in MANETs Using Key Management Mechanism," Applied Sciences, vol. 12, no. 3, p. 1041, 2022. [Online]. Available: https://doi.org/10.3390/app12031041
[2] H. Yang, "A Study on Improving Secure Routing Performance Using Trust Model in MANET," Mobile Information Systems, vol. 2020, Article ID 8819587, 17 pages, 2020. [Online]. Available: https://doi.org/10.1155/2020/8819587
[3] B. Rajkumar and N. G., "Secure multipath routing and data transmission in MANET," International Journal of Networking and Virtual Organisations, vol. 16, p. 236, 2016. [Online]. Available: https://doi.org/10.1504/IJNVO.2016.079178
[4] H. D. Reddy et al., "An Intelligent Intrusion Detection and Classification System using CSGO-LSVM Model for Wireless Sensor Networks (WSNs)," International Journal of Intelligent Systems and Applications in Engineering, vol. 10, no. 3, pp. 285–293, 2022. [Online]. Available: https://ijisae.org/index.php/IJISAE/article/view/2167
[5] J. Y. M. and G. Ravi, "Cooperative Self-Scheduling Secure Routing Protocol for Efficient Communication in MANET," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, pp. 232-241, 2023. [Online]. Available: https://doi.org/10.17762/ijritcc.v11i4s.6533
[6] K. Thamizhmaran, "Secure efficient communication in routing protocol in MANETs using ECC-EA3ACKa," i-manager's Journal on Mobile Applications and Technologies, vol. 10, p. 12, 2023. [Online]. Available: https://doi.org/10.26634/jmt.10.1.20125
[7] T. Hai et al., "Enhanced security using multiple paths routine scheme in cloud-MANETs," Journal of Cloud Computing, vol. 12, 2023. [Online]. Available: https://doi.org/10.1186/s13677-023-00443-5
[8] K. Mahalakshmi and D. Sharmila, "A Transmission Efficient Secured Heuristic Path Ranking Geographic Routing Protocol in MANET," Asian Journal of Research in Social Sciences and Humanities, vol. 6, p. 219, 2016. [Online]. Available: https://doi.org/10.5958/2249-7315.2016.00605.5
[9] H. Yang, "A Study on Improving Secure Routing Performance Using Trust Model in MANET," Mobile Information Systems, vol. 2020, pp. 1-17, 2020. [Online]. Available: https://doi.org/10.1155/2020/8819587
[10] L. Patil and G. Borkar, "An Adaptive RIPng Routing Protocol with Secure Packet Transmission in MANETs," Journal of Applied Security Research, vol. 13, pp. 1-27, 2018. [Online]. Available: https://doi.org/10.1080/19361610.2018.1499385
[11] S. Manthandi et al., "Performance analysis of multicast routing using multi agent zone based mechanism in MANET," Accepted: October 2021.
[12] Dr. Shankar, M. Elhoseny, and R. Damasevicius, "Trust Based Cluster Head Election of Secure Message Transmission in MANET Using Multi Secure Protocol with TDES," Journal of Universal Computer Science, vol. 25, pp. 1221-1239, 2019. [Online]. Available: https://doi.org/10.3217/jucs-025-10-1221
[13] P. Satyanarayana et al., "Implementation of Enhanced Energy Aware Clustering Based Routing (EEACBR) Algorithm to Improve Network Lifetime in WSNs," in 2022 IEEE 2nd International Conference on Mobile Networks and Wireless Communications (ICMNWC), Tumkur, Karnataka, India, 2022, pp. 1-6. [Online]. Available: https://doi.org/10.1109/ICMNWC56175.2022.10031991
[14] R. Mariappan and K. Valarmathi, "A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs," Wireless Personal Communications, vol. 112, 2020. [Online]. Available: https://doi.org/10.1007/s11277-019-07016-3
[15] V. Keerthika and M. Nandagopal, "Enhanced AODV protocol to secure routing in MANET with optimization techniques," International Journal of Engineering and Technology (UAE), vol. 7, no. 2, pp. 75-79, 2018. [Online]. Available: https://doi.org/10.14419/ijet.v7i2.19.15052
[16] N. Vejendla and B. Chettiar, "Effective multi-mode routing mechanism with master-slave technique and reduction of packet droppings using 2-ACK scheme in MANETS," Modelling Measurement and Control A, vol. 91, pp. 73-76, 2018. [Online]. Available: https://doi.org/10.18280/mmc_a.910207
[17] M. Balamurugan, S. Mathavan, D. Kumar, and S. Aranganathan, "Anonymous Location-Support and Self-Reliance Routing Protocol For Manet," Indian Journal of Public Health Research & Development, vol. 9, p. 323, 2018. [Online]. Available: https://doi.org/10.5958/0976-5506.2018.00140.7
[18] V. Sesha, M. Seetha, and V. Somalaraju, "SDSR A New Hybrid Secure Routing Protocol using Trust Recommendations in MANET," International Journal of Engineering and Advanced Technology, vol. 9, pp. 1092-1095, 2020. [Online]. Available: https://doi.org/10.35940/ijeat.E1042.069520
[19] P. Satyanarayana et al., "Enhancement of Energy Efficiency and Network Lifetime Using Modified Cluster Based Routing in Wireless Sensor Networks," 2023 International Conference on Intelligent Systems for Communication

IoT and Security (ICISCoIS), Coimbatore, India, 2023, pp. 127-132. [Online]. Available: https://doi.org/10.1109/ICISCoIS56541.2023.10100580

[20] S. Sekar and B. Latha, "Lightweight reliable and secure multicasting routing protocol based on cross-layer for MANET," Concurrency and Computation: Practice and Experience, vol. 32, 2018. [Online]. Available: https://doi.org/10.1002/cpe.5025