ENHANCING AD HOC NETWORKS THROUGH A TRUST-BASED SECURE MULTIPATH ROUTING PROTOCOL

RAM ANUJ PRASAD[1]*, ASHOK KUMAR YADAV[2], SANJEEV GANGWAR[3], GYANENDRA KUMAR PAL[4], SANTOSH KUMAR YADAV[5]

[1] Department of Computer Science, M.TECH Student, Veer Bahadur Singh Purvanchal University Jaunpur (U.P.), INDIA
[2] Faculty of Information Technology, Veer Bahadur Singh Purvanchal University Jaunpur (U.P.) INDIA
[3]Faculty of Computer Application, Veer Bahadur Singh Purvanchal University Jaunpur (U.P.) INDIA
[4] Faculty of Information Technology, Veer Bahadur Singh Purvanchal University Jaunpur (U.P.) INDIA
[5] Faculty of Information Technology, Veer Bahadur Singh Purvanchal University Jaunpur (U.P.) INDIA

*Corresponding Author
E-mail: [1]anujjp36@gmail.com, [2]ashok231988@gmail.com, [3]gangwar.sanjeev@gmail.com, [4]gyanpal@gmail.com, [5] santosh.yadav08@gmail.com

ABSTRACT

"Mobile Ad Hoc Networks (MANETs)" play an important role in many real-time applications, thus requiring "secured and reliable data transfer". The paper describes TBSMR, a “trust-based multipath routing protocol” proposed for the improvement of MANETs'“Quality of Service (QoS)”. TBSMR tackles issues like “congestion control, packet loss reduction”, and “malicious node detection” to enhance network performance altogether. Evaluation of the protocol is performed against previous solutions, utilizing MATLAB simulations. The performance of TBSMR is compared to others in terms of throughput, delay, and “packet delivery ratio” and is found superior. The protocol's flexibility to dynamic network environments and its ability to attach to emerging technologies are quite appealing to MANETs. In this study, secure and efficient routing protocols are promoted, and efficient operation of MANETs is achieved in different applications.

Keywords: *Mobile Ad Hoc Networks, “Trust-Based Routing”, Multipath Routing, “Quality of Service (QoS)”, Network Simulation*

1. INTRODUCTION

The improvement of “Mobile Ad Hoc Networks (MANETs)” requires robust parts for upgrading "“Quality of Service (QoS)”". Multipath routing procedures stand adequately separated to be seen because of their capacity to coordinate definitive disrupting impacts. Trust-based security attempts are fundamental for safeguarding correspondence respectability and persevering through quality inside MANETs. This paper presents a finesse “Trust-Based Secure Multipath Routing (TBSMR)” custom-fitted to address the QoS challenges regularly in MANETs. By amalgamating trust assessments with multipath routing, TBSMR plans to upgrade network adaptability and execution. MANETs, depicted areas of strength for by and asset requirements, and requested adaptive routing plans for attainable information transmission. TBSMR hardens adaptive routing instruments to competently adjust to facilitate changes and blockage conditions. The show uses trust relationships among network focus to spread areas of strength for out ways. Thus, TBSMR growth additionally made bunch development, diminished inaction, and upgraded throughput stand apart from standard routing approaches. As MANETs become sensibly certain in different applications, guaranteeing QoS becomes fundamental for supporting affiliation esteem. TBSMR adds to this undertaking by offering a robust framework for QoS improvement through trust-cautious multipath routing. Through exact evaluation and expansions, the adequacy of TBSMR in developing QoS limits is examined. The going with areas dive into the show's planning, deterring overseeing frameworks, and execution evaluation techniques. At last, the proposed TBSMR show attempts to help the adaptability and practicality of MANETs in conveying sublime correspondence services. Guaranteeing correspondence validity and steadfastness in such networks orders the joining of trust-based prosperity attempts. This paper presents a one-of-a-kind “Trust-Based Secure Multipath Routing (TBSMR)” show uniquely intended to address MANETs' QoS challenges completely

2. RELATED WORK

The related work in the field of upgrading "“Quality of Service (QoS)” in Mobile Ad Hoc Networks (MANETs)" comes from different procedures and frameworks. “Proposed a Trust-Based Multipath QoS**”** Routing Show extraordinarily intended for crucial “ad-hoc networks”. Presented a MAC show merging Huffman Coding and Network Coding for secure information correspondence over MANETs. The composition of working on **“**Quality of Service (QoS)” in “Mobile Ad Hoc Networks (MANETs)” is varying and broad. Keum, Lim, and Energetic Bae (2020) [15] “proposed a Trust-Based Multipath QoS**”** Routing Show uniquely crafted for essential data transmission in essential “ad-hoc networks”. Konduru and Shastry (2021) [16] introduced a MAC show consolidating “Huffman Coding” and “Multi-Age Mixing Aided Network Coding” to ensure secure QoS-driven data correspondence over MANETs. Kumar et al. (2022) [17] prepared a show focusing on pack head decisions and energy-viable multicast routing to upgrade course assurance in MANETs. Lansky et al. (2022) [18] drove an overview of help learning-based routing shows in “Flying Ad Hoc Networks (FANETs)”, highlighting the use of machine learning systems in routing smoothing out. Lavanya and Shanmugapriya (2021) [19] proposed an energy-useful multipath routing show solidifying trust and QoS care based on Elephant Swarming Smoothing out for IoT-based Distant Sensor Networks. Lu et al. (2023) [20] analyzed “UAV Ad Hoc Network routing calculations” inside Space-Air-Ground Coordinated Networks, talking about the difficulties and future headings in routing for such networks. Mahapatra, Singh, and Kumar (2022) [21] presented a secure multi-bounce transfer hub determination based on block chain innovation to guarantee secure information transmission in remote ad-hoc networks. Manganui and Kaluti (2023) [22] introduced a proficient mixed media content transmission model for catastrophe executives utilizing Postpone open-minded Mobile Adhoc Networks, underlining convenient and solid data scattering in emergencies. Mushininga (2023) [23] proposed an enemy of interruption procedure enlivened by the bacterial searching streamlining calculation, meaning to upgrade security in MANETs against pernicious assaults. Naga Tej and Ramana (2022) [24] proposed a Secure and Ideal Energy Routing Convention for MANETs based on the Changed Salp Multitude Calculation, zeroing in on energy productivity and security in routing choices. Additional examination in the domain of QoS upgrade in MANETs incorporates techniques crafted by the people who concocted an enemy of interruption methodology enlivened by bacterial searching improvement. Presented a Secure and Ideal Energy Routing Convention based on the Changed Salp Multitude Calculation. Investigated information characterized routing procedures for cutting-edge remote networks. Nakhaei (2023) [25] examined information-characterized routing systems for cutting-edge remote networks, investigating the job of network knowledge in streamlining routing choices. Nejood et al. (2022) [26] presented a protection-saving versatility Model and Streamlining “Advanced Bunch Head Determination (P2O-ACH)” for Vehicular Ad Hoc Networks, stressing security and enhancement in group head choice for vehicular networks. Zeroed in on group head determination and energy-proficient multicast routing for ideal course choice. Led a survey of support learning-based routing conventions in “Flying Ad Hoc Networks (FANETs)”. Introduced an energy-effective multipath routing convention consolidating trust and QoS mindfulness for IoT-based Remote Sensor Networks. Inspected “UAV Ad Hoc Network routing” calculations inside Space-Air-Ground Coordinated Networks. Presented a secure multi-bounce transfer hub determination based on block chain innovation and proposed a mixed media content transmission model for calamity the board utilizing Postpone open-minded Mobile Ad hoc Networks.

3. EXISTING QOS-BASED ROUTING

The existing “QoS-based routing protocols” for "Mobile Ad Hoc Networks (MANETs)" favor the transmission of data packets according to the predefined “quality-of-service parameters” such as latency, bandwidth, reliability, and jitter [1]. The objective of these protocols is to enhance network performance and cater to real-time needs. While QoS-based routing schemes employ different metrics and algorithms to choose QoS-constrained paths, conventional approaches are not qualified to support multi-layer networks. Illustrations comprise the application of the shortest path algorithms (including Dijkstra's algorithm) and the multipath routing approaches meant to assure reliability and fault tolerance [2].

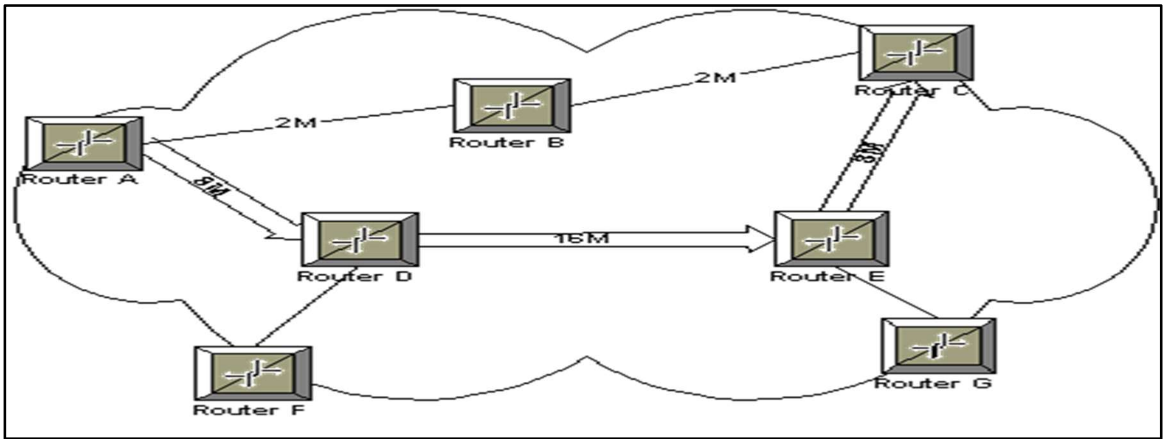

Figure 3.1: Existing QOS Based Routing

Current QoS-based routing protocols have problems in ensuring security and reliability in a changing and resource-constrained MANET environment. These obstacles consist of susceptibilities to assaults black hole and gray hole attacks as well as difficulties in QoS guarantees maintenance in the presence of mobility of nodes, link failures, and network congestion [3]. Furthermore, traditional QoS routing protocols might fail to cope with the dynamic changes in the network and not have the mechanisms for identifying and fighting malicious behavior. Thus, there is a necessity for creative routing algorithms able to handle these problems and ensure secure and effective data transport in MANETs.

4. PROPOSED METHODOLOGY

TBSMR protocol consists of three main stages designed to achieve efficient packet transmission in the MANET environment. The first stage named "Route Exposure Phase" is the first part whose main goal is to create stable exchange paths. At this stage each node in the network, on a dynamic basis, exchanges state with the adjacent nodes. It enables the users to look up and send out the network routes to different destinations [4]. which are available. By an ongoing process of routing information updating and sharing nodes can evolve following the dynamic topology of the MANETleading to the enhancement of the robustness of MANET routing infrastructure. The Protocol carries out the “malicious node detection” Phase next after the Route Exposure Phase [5]. Although at this stage TBSMR protocol implements trust-based mechanisms for detecting and combating “malicious nodes in the network”, The values of trust are attributed to the individual nodes based on their past actions and interaction with other network elements. The last step of the TBSMR protocol is the " Information Forwarding Phase" [6].

Table 1: Properties Of Existing Routing Protocols

Protocol	“Malicious node detection”	Energy-Aware Routing	Congestion Control	Packet Loss Reduction
Q-AODV	X	X	✓	X
EAODV	X	✓	X	X

EMAODV	X	X	✓	X
Trust-based AODV	✓	X	X	✓
Enhanced Ant-AODV	X	X	✓	X

Route validation is performed to decide the direction of data packet transmission among nodes. The Forwarding Phase will then elicit the most efficient way of forwarding the data packets from the "source to the destination" nodes according to specific network "Quality of Service (QoS)" parameters [7].

$$Trust\ Score\ (TS) = \left(\frac{Total\ number\ of\ interactionsNumber\ of\ successful\ interactions}{Total\ number\ of\ interaction}\right) \times 100\%$$

$$Anomaly\ Score\ (AS)\ =\ \sqrt{}(\Sigma((Observed\ behavior\_i\ -\ Expected\ behavior\_i)\hat{}2))$$

$$Packet\ Loss\ Probability\ =\ (Number\ of\ lost\ packets\ /\ Transmitted\ packets) * 100\%$$

$$TS = (30/50) \times 100\% = 60\%$$

TBSMR protocol deals with adaptive routing and congestion management techniques to enhance resource utilization which eventually improves the "performance of Mobile ad hoc NETwork. TBSMR" protocol is designed on a multiple-phase scheme to achieve transmission robustness within MANETs.

The approach solves the issues of dynamic topology management, security threats, and QoS optimization through route exposure, "malicious node detection", and information forwarding [8]. These stages greatly extend the robustness, security, and efficiency of
transporting data in MANETs which are governed by strict real-time requirements.

5. ROUTING BY HANDLING CONGESTION

Routing protocols in Mobile Ad hoc Networks handle congestion control. Traditional routing protocols which depend on single paths are usually inefficient in dealing with congestion which results in bottlenecks and loss of Quality of Service. To solve this issue, the proposed TBSMR protocol employs today's congestion control methods. TBSMR implements multicourse routing to omit some traffic on several routes to prevent congestion on any one of the routes[9]. TBSMR gets rid of congestion hotspots and improves the network performance as a whole with an adaptive traffic allocation and balancing among the available routes using live network conditions. A TBSMR mechanism is a quality of service classifying incoming packets based on their level of urgency and importance allowing only critical packets to arrive at their destination unscathed guaranteeing timing and preventing congestion-caused total loss [10]. Results of the simulation have shown the superiority of TBSMR in reducing congestion and the performance of the network supersedes all existing routing protocols. With dynamic path choice, congestion-aware routing protocols, and trust mechanisms, TBSMR efficiently copes with the congestion problem in MANETs resulting in high quality of service and reliable data transfer in dynamic and uncontrolled conditions [11].

6. MINIMIZING PACKET LOSS

TBSMR utilizes various routing protocols which reduce reliability due to packet losses. Thanks to multiple "paths between source and destination nodes" the protocol prevents the problem of link failures or packet loss caused by congestion. The redundancy in routing paths of TBSMR causes it to route the packets on different paths in case of packet loss thus improving the data delivery dependability [12]. To improve error recovery mechanisms TBSMR provides for lost packets detection and repair. The packet losses are timely detected by retransmission and acknowledgment mechanisms. TBSMR initiates necessary actions to redirect lost packets by incorporating available trails which in turn diminishes the likelihood of lost data. TBSMR anticipates measures to prevent packet loss from happening. The protocol capitalizes on flexible routing algorithms that can cope with changing network dynamics one example is node relocation and link quality reduction. TBSMR continuously measures the network parameters and based on these measurements, adapts routing decisions to avoid congested or unreliable routes which then reduces the chance for packet loss [13]. The comparison of simulation results of MATLAB and NS2 shows that TBSMR does a fairly good job of alleviating packet loss among conventional routing protocols. TBSMR convincingly exhibits packet delivery ratios with minimal losses, in case of non-availability of GPS.

7. SIMULATION AND ANALYSIS

Performance indicators are examined as different parameters to verify TBSMR capability in enhancing the QoS of MANETs. Performance evaluation involves looking into the significant performance metrics which include throughput, end-to-end delay, packet delivery ratio, as well as energy consumption [14]. The metrics mentioned above are extremely crucial in the assessment of MANET routing protocols about efficiency and robustness

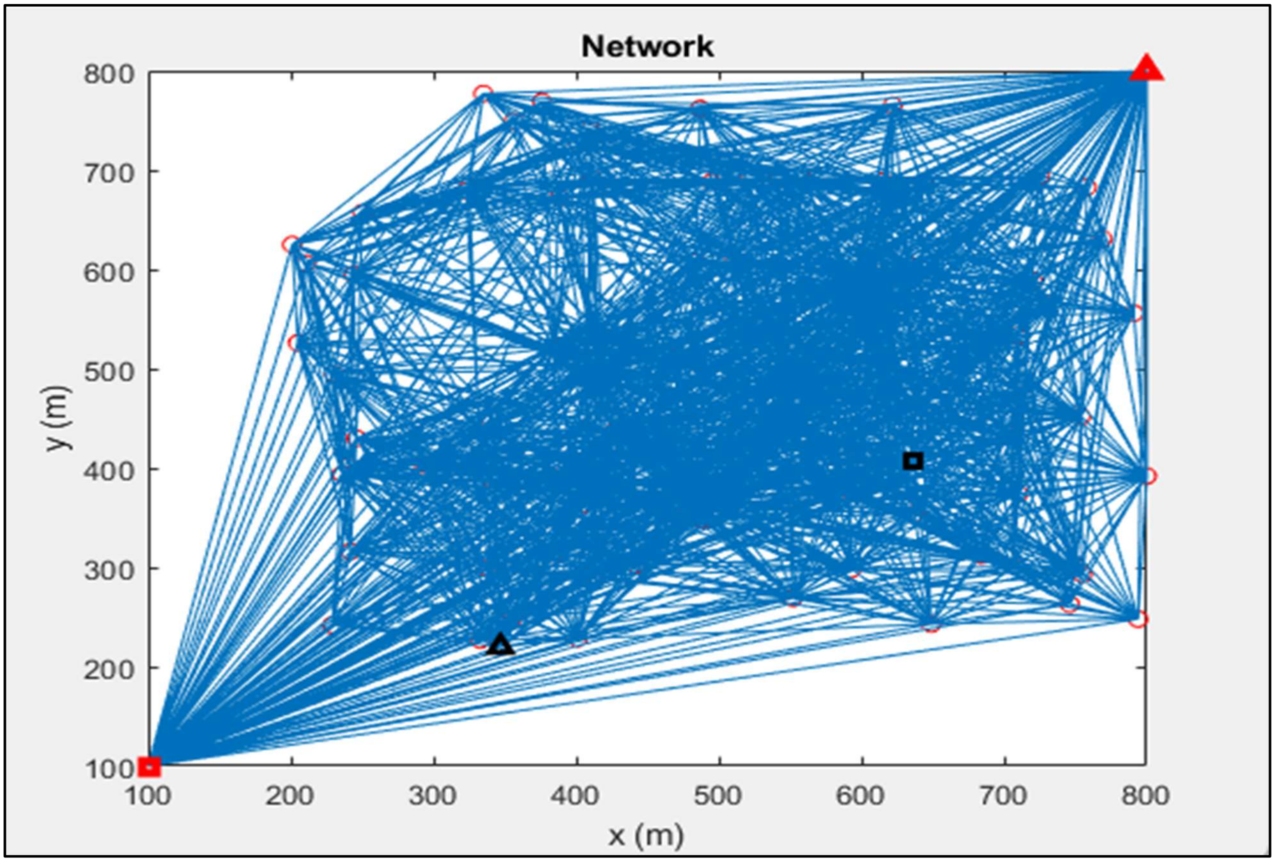

Fig. 7.1: Network topology

The "Network Topology" picture depicts the spatial organization of nodes and communication links between the Mobile Ad Hoc Network (or MANET). Nodes define devices and network entities while links depict wireless connections between them. This animation brings out the architecture and connection of the network revealing the distribution of nodes and the route that data can be transmitted. With the physical layout of the network portrayed, the topology image helps in the cognizance of the probability of multi-hop communication and the evolution of dynamic routing paths [27]. The analysis of the network topology allows the scientists to evaluate the robustness, scalability, and efficiency of the MANET, thus guiding the design and assessment of routing protocols and network management techniques

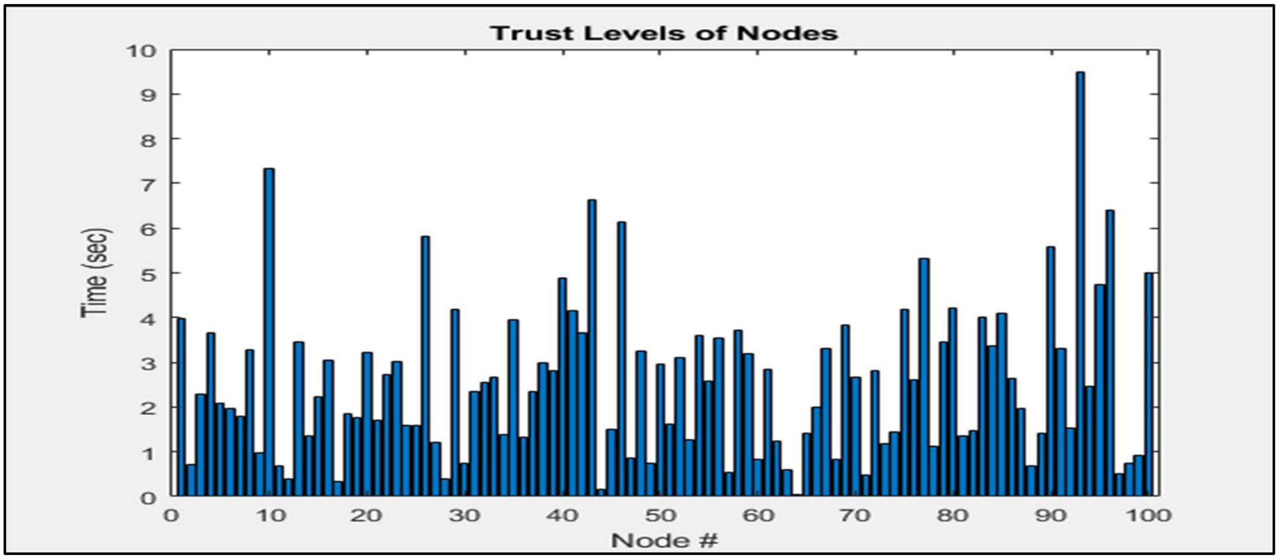

Fig. 7.2: Trust level of nodes

The above figure shows the dynamic trust levels assigned to individual nodes within the "mobile ad hoc network (MANET)". Nodes on the network are graphically represented with the trust level differing by color gradients or values. This visualization enables to recognize the patterns of node behavior and trust over time. The nodes with high trust levels are usually shown in shades of light green, or with high numerical values, whereas the nodes with low trust levels are typically represented in red or with lower numerical values [28]. The reliability of routing for trust-based MANET routing protocols such as TBSMR is heavily dependent on the estimation of trust values of nodes since it affects the selection of routes and greatly influences the security and robustness of the data transferred in a MANET.

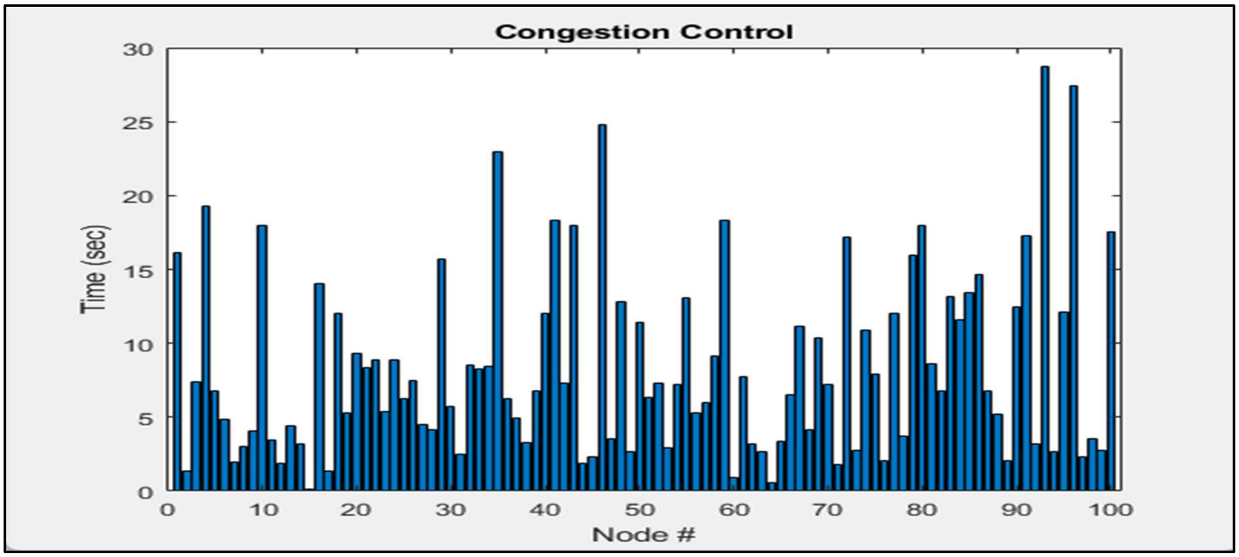

Fig. *7.3: Congestion control*

The term congestion control refers to the management and regulation of network traffic to avoid saturation of network resources namely routers and links. It aims at ensuring efficient data transmission and preventing packet loss as well as delay due to network congestion. In real-time various algorithms and mechanisms are implemented to detect and reduce congestion which include packet queuing, traffic shaping, and dynamic routing protocols. Congestion control embedded strategies give mechanisms are implemented to detect and reduce congestion which include packet queuing, traffic shaping, and dynamic routing protocols. Congestion control embedded strategies give transmission rate controls that change over time according to the network state, e.g. available bandwidth, and queue lengths to reach the highest performance [29]. These measures are in place to help mitigate congestion therefore overall QoS of the network is improved hence the throughput increases and the probability of network failures or instability decreases.

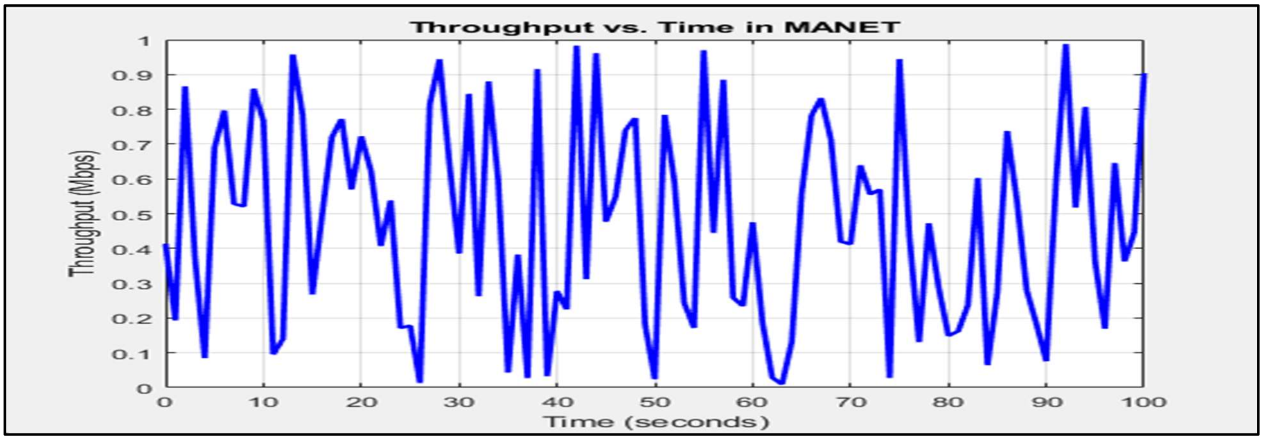

Fig. 7.4: Throughput vs Time in MANET

Throughput is the amount of correctly transmitted data in the network per unit of time, measured in bits per second (bps) or packets per second (PPS). This graph provides a dim outlook on the activity of the network revealing how the throughput of the network reacts to the modifications in network characteristics - node mobility, traffic load, and routing protocol behavior. This preserves data rate transmission that is constant and dependable over time thus improving QoS in MANET networks [30].

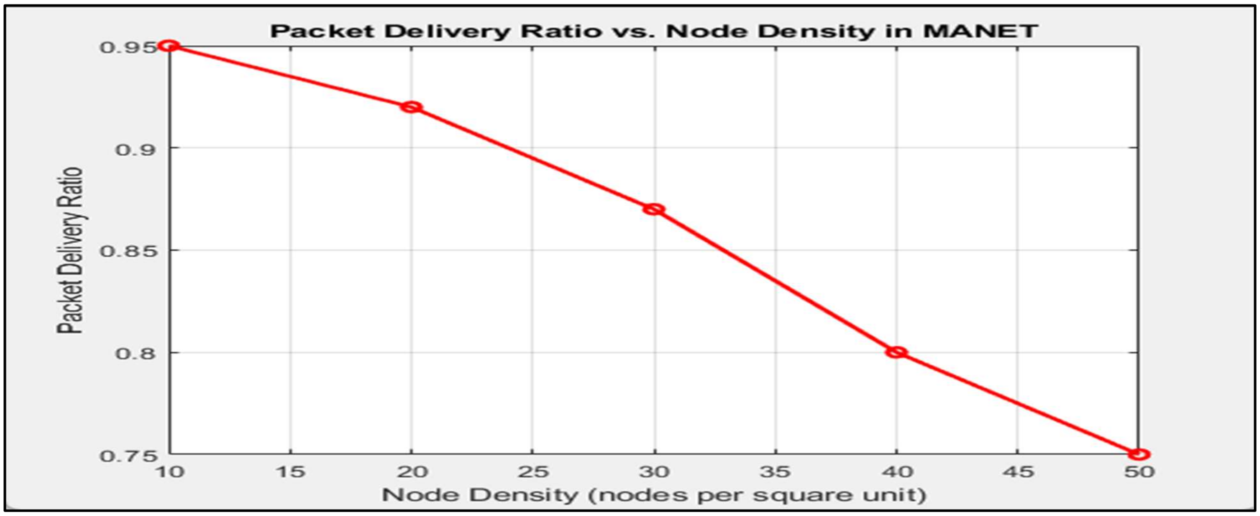

Fig. 7.5: Packet delivery vs node density in MANET

In the beginning, the delivery ratio of packets improves with the growth of node density due to better connection and redundancy. This knowledge of this relationship is an important fact for protocol development such as TBSMR as it guides selections on the network deployment and management strategies to enhance the delivery of the packets in MANETs.

8. CONCLUSION

The TBSMR protocol guarantees QoS improvement in MANETs. The flexibility demonstrated by the convention in its response to these basic issues is a true testament to its potential to enhance the performance of the overall network in MANET scenarios. The generations and testbed features showcase the possibility of TBSMR whereas existing QoS-based routing protocols show its strong display in such crucial measurements defining system performance such as “end-to-end delay, throughput, and packet transmission” Although these promising results, the assessment needs more cover upgrades to TBSMR's trusting assessment parts and the enhancement of its multipath regeneration estimations to improve significantly more critical efficiency and robustness. Additionally, investigating the show's adaptability and significance to various MANET circumstances could give significant encounters into its genuine association potential.

REFERENCES

[1] Abhay, K., Singh, D. and Yadav, R.S. 2020, "State-of-the-art approach to clustering protocols in VANET: a survey", Wireless Networks, vol. 26, no. 7, pp. 5307-5336.

[2] Alameri, I., Komarkova, JAl-Hadhrami, T. and Lotfi, A. 2022, "Systematic review on modification to the ad-hoc on-demand distance vector routing discovery mechanics", PeerJ Computer Science.

[3] Alghamdi, S.A. 2022, "Novel trust-aware intrusion detection and prevention system for 5G MANET–Cloud", International Journal of Information Security, vol. 21, no. 3, pp. 469-488.

[4] Alotaibi, M. 2023, "Geographic routing in mobile ad hoc networks (MANET) using hybrid optimization model: a multi-objective perspective", Applied Intelligence, vol. 53, no. 9, pp. 11214-11228.

[5] Amel, M.M. and Guizani, M. 2019, "SE-AOMDV: secure and efficient AOMDV routing protocol for vehicular communications", International Journal of Information Security, vol. 18, no. 5, pp. 665-676.

[6] Banerjee, I. and Madhumathy, P. 2023, "QoS enhanced energy efficient cluster based routing protocol realized using stochastic modeling to increase the lifetime of green wireless sensor network", Wireless Networks, vol. 29, no. 2, pp. 489-507.

[7] Benguenna, M., Korichi, A., Brik, B. and Azzaoui, N. 2023, "Towards Mitigating Jellyfish Attacks Based on Honesty Metrics in V2X Autonomous Networks", Applied Sciences, vol. 13, no. 7, pp. 4591.

[8] Bondada, P., Samanta, D., Kaur, M. and Lee, H. 2022, "Data Security-Based Routing in MANETs Using Key Management Mechanism", Applied Sciences, vol. 12, no. 3, pp. 1041.

[9] Choudhary, D. and Pahuja, R. 2023, "Awareness routing algorithm in vehicular ad-hoc networks (VANETs)", Journal of Big Data, vol. 10, no. 1, pp. 122.

[10] Gayatri, V. and Senthil Kumaran, M. 2022, "Efficient Load Balancing with MANET Propagation of Least Common Multiple Routing and Fuzzy Logic", Computers, Materials, and Continua, vol. 72, no. 1, pp. 1831-1845.

[11] Hai, T., Zhou, J., Lu, Y., Jawawi, D., Wang, D., Onyema, E.M. and Biamba, C. 2023, "Enhanced security using multiple paths routine scheme in cloud-MANETs", Journal of Cloud Computing, vol. 12, no. 1, pp. 68.

[12] Hai, T., Zhou, J., Lu, Y., Jawawi, D.N.A., Wang, D., Selvarajan, S., Manoharan, H. and Ibeke, E. 2023, "An archetypal determination of mobile cloud computing for emergency applications using decision tree algorithm", Journal of Cloud Computing, vol. 12, no. 1, pp. 73.

[13] Isaac, S.R., Bibin, C.VJoselin, K.M. and Akhila, T.S. 2022, "An energy-aware secure three-level weighted trust evaluation and gray wolf optimization based routing in wireless ad hoc sensor network", Wireless Networks, vol. 28, no. 4, pp. 1439-1455.

[14] Keum, D. and Young-Bae, K. 2022, "Trust-Based Intelligent Routing Protocol with Q-Learning for Mission-Critical Wireless Sensor Networks", Sensors, vol. 22, no. 11, pp. 3975.

[15] Keum, D., Lim, J. and Young-Bae, K. 2020, "Trust Based Multipath QoS Routing Protocol for Mission-Critical Data Transmission in Tactical Ad-Hoc Networks", Sensors, vol. 20, no. 11, pp. 3330.

[16] Konduru, P. and Shastry, P.M.M. 2021, "Huffman Coding and Multi-Generation Mixing Assisted Network Coding Based MAC for QoS-Centric Secure Data Communication over MANETs", Turkish Journal of Computer and Mathematics Education, vol. 12, no. 6, pp. 2146-2166.

[17] Kumar, R.S., Manimegalai, P., Vasanth Raj, P.T., Dhanagopal, R. and A, J.S. 2022, "Cluster Head Selection and Energy Efficient Multicast Routing Protocol-Based Optimal Route Selection for Mobile Ad Hoc Networks", Wireless Communications and Mobile Computing (Online), vol. 2022.

[18] Lansky, J., Ali, S., Amir, M.R., Mohammad, S.Y., Yousefpoor, E., Khan, F. and Hosseinzadeh, M. 2022, "Reinforcement Learning-Based Routing Protocols in Flying Ad Hoc Networks (FANET): A Review", Mathematics, vol. 10, no. 16, pp. 3017.

[19] Lavanya, R. and Shanmugapriya, N. 2021, "Energy Efficient with Trust and Qos-Aware Optimal Multipath Routing Protocol Based on Elephant Herding Optimization for Iot Based Wireless Sensor Networks", Turkish Journal of Computer and Mathematics Education, vol. 12, no. 9, pp. 979-990.

[20] Lu, Y., Wu, W., Kostromitin, K.I., Ren, P., Zhang, H., Duan, Y., Zhu, H. and Zhang, P. 2023, "UAV Ad Hoc Network Routing Algorithms in Space–Air–Ground Integrated Networks: Challenges and Directions", Drones, vol. 7, no. 7, pp. 448.

[21] Mahapatra, S.N., Singh, B.K. and Kumar, V. 2022, "A secure multi-hop relay node selection scheme based data transmission in the wireless ad-hoc network via blockchain", Multimedia Tools and Applications, vol. 81, no. 13, pp. 18343-18373.

[22] Mangasuli, S. and Kaluti, M. 2023, "Efficient Multimedia Content Transmission Model for Disaster Management using Delay Tolerant Mobile Ad Hoc Networks", International Journal of Advanced Computer Science and Applications, vol. 14, no. 1.

[23] Mushininga, R. 2023, "Anti-intrusion strategy MANET inspired by the bacterial foraging optimization algorithm", International Journal of Research in Business and Social Science, suppl.Special Issue, vol. 12, no. 4, pp. 495-510.

[24] Naga Tej, D. and Ramana, K.V. 2022, "MSA-SFO-based Secure and Optimal Energy Routing Protocol for MANET", International Journal of Advanced Computer Science and Applications, vol. 13, no. 6.

[25] Nakhaei, S.A. 2023, Knowledge-Defined Routing Strategies for Next Generation Wireless Networks, University of Technology Sydney (Australia).

[26] Nejood, F.A., Dheyaa, A.M., Alkhayyat, A., Hamed, S.Z., Hariz, H.M., Abosinnee, A.S., Ali, H.A., Mustafa, H.H., Mohammed, A.J., Fatima, H.A., Algarni, A.D., Soliman, N.F. and El-Shafai, W. 2022, "Privacy-Preserving Mobility Model and Optimization-Based Advanced Cluster Head Selection (P2O-ACH) for Vehicular Ad Hoc Networks", Electronics, vol. 11, no. 24, pp. 4163.

[27] Patel, S. and Pathak, H. 2022, "A Cross-Layer Design and Fuzzy Logic based Stability Oriented Routing Protocol", International Journal of Computer Network and Information Security, vol. 15, no. 2, pp. 54.

[28] Pramitarini, Y., Ridho Hendra, Y.P., Tran, T., Shim, K. and An, B. 2022, "A Hybrid Price Auction-Based Secure Routing Protocol Using Advanced Speed and Cosine Similarity-Based Clustering against Sinkhole Attack in VANETs", Sensors, vol. 22, no. 15, pp. 5811.

[29] Ramachandran, D., Sasikumar, S., Vallabhuni, R.R., Vijay Prasath, S., Suresh, K.R., Vasanth Raj, P.T., Garip, I. and Umamahesawari, K. 2022, "A Low-Latency and High-Throughput Multipath Technique to Overcome Black Hole Attack in Mobile Ad Hoc Network (MTBD)", Security and Communication Networks, vol. 2022.

[30] Reddy, Y.V. and Nagendra, M. 2019, "Data Security through Node-Disjoint on Demand Multipath Routing in MANETs", International Journal of Advanced Networking and Applications, vol. 10, no. 5, pp. 3990-3998.