International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-11 Issue-1, May 2022

Comparative Analysis of Routing Algorithms to Enhance the Quality of Service in MANET

K. Vimala, D. Maruthanayagam

Abstract: ***Mobile Ad hoc Network is a self-organizing, infrastructure-free, distributed wireless networks made up of various mobile devices. Quality-of-Service routing is most difficult task in MANET due to inherent characteristics–for example frequent dynamic topology, node mobility, resource scarcity, absence of centralized control, etc as well. The QoS variables of any MANET routing algorithms determine its performance. QoS routing is process of routing packets from source (S) to destination (D) based on QoS resource constraints such as bandwidth, delay, packet loss rate, cost, security, link stability, and so on. Swarm intelligence, which mimics the collective behaviour of biological organisms to handle routing problems and improve QoS in the network, has been one of most popular studies for network routing in recent years. Particle Swarm Optimization algorithm (PSO), Genetic Algorithm (GA) and Ant Colony Optimization algorithm (ACO) have all been shown to be effective for developing routing algorithms by improving QoS metrics in ad hoc networks using Swarm Intelligence (SI). The primary objective of this comparative study paper is to improve QoS parameters by applying swarm intelligence to MANET routing algorithms. Swarm intelligence-based routing algorithms will be more promising for the specific nature of adhoc networks, outperforming in real scenarios/constraints/environmental conditions and will be tuned and simulated to obtain an efficient and effective MANET routing protocol. This paper investigates four potential pre-existing approaches proposed for MANET routing problems. These routing algorithms are evaluated using various performance metrics such as packet delivery ratio, routing overhead, link failure prevention, energy consumption, accuracy, and throughput, among others.***

Keywords: ***MANET, Routing, Link failure, Security, Swarm Intelligence and Quality of Services.***

I. INTRODUCTION

MANET has received a lot of attention in latest years, owing to the general use of cheaper and more powerful wireless networks [1]. It's composed a collection of wireless mobile nodes, mobile nodes are communicated with each other through one or more connections it does not have any centralized authority [2]. Each mobile node in MANET can acts as both a terminal node and router, which means each mobile node can make its own traffic though also receiving packets from other mobile nodes and sending them to neighbouring nodes.

Manuscript received on 18 April 2022.
Revised Manuscript received on 28 April 2022.
Manuscript published on 30 May 2022.
* Correspondence Author
K. Vimala*, Research Scholar, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri (Tamil Nadu), India.
Dr. D. Maruthanayagam, Professor & Head, PG and Research, Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri (Tamil Nadu), India.

MANET is quick and simple to organizing, making them ideal for real time applications such as environmental monitoring, military surveillance and etc.,[3]. In MANETs, routing for QoS is critical. In further to finding a best route from a source (S) to destination (D), QoS routing must ensure end user quality, usually respecting bandwidth or delay [4].To develop a secure and more efficient routing algorithms, that algorithm can also improve overall quality of network services throughput the routing procedure is a more challenge task for MANETs, because MANET mobile nodes communicate with other nodes only they are inside the communication range. When the receiver mobile node is outlying from the transmitter range, the dynamic behaviour of MANET makes ensuring QoS difficult because the node to node connection and link quality change dynamically, resulting in frequent link failures then affecting nodes to connect with other nodes [5]. Another critical important issue in MANET is security, because malicious nodes can purpose fully misbehave, altering packet information and disrupting packet routing to preferred destinations, dropping packet delivery percentage and reliability. Many MANET routing algorithms, for example (Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV), than Cluster Based Routing (CBRP) already been designed to address link failure and security issues in MANETs. Most solutions, however, are principal effective for a specific type of attack or provide better security at the expense of sacrificing QoS. Until now, no research effort has been able to provide the optimum routing efficiency to ensure high network performance. Because of their self-organizing nature, SI-inspired routing systems have become a research focus in recent years [6], which is very appropriate to routing problems and QoS-related concerns in Mobile Ad hoc Networks (MANETs). Inspired by natural biological swarms, swarm intelligence possesses a number of potent properties for distributed problem solving in more complex real world applications like optimization and control. Natural systems with swarm intelligence assets include ants, bees, and birds, in which unsophisticated agents interact locally with their atmosphere to explore collective problem solving without centralised control. This paper describes and analyses the performance of some existing routing algorithms in order to apply swarm intelligence to routing algorithms used in MANETs to improve QoS.

II. ROUTING ALGORITHMS IN MANET

QoS in MANETs, according to RFC 2386, is an observance requirement that must be met by the MANET network while transporting a data packet flow from the source (S) to its destination (D) [7].

Regards of end-to-end performance, the ad hoc network is expected to provide users with significant pre specified service attributes like bandwidth requirement, data packet damage probability, latency or jitter variation, route acquisition delay, communication overhead, and so on. Finding a feasible route that must satisfies the QoS parameters of a given MANET application is one of the key issues in QoS routing [7]. However, due to node mobility, limited resource constraints, multi-hop communications, channel access contention, and a lack of central coordination, QoS routing in MANETs is extremely difficult. The main QoS issues are link failures, which reduce overall network performance; mobile node movement in network changes the topology, resulting in frequent connection failures. This causes a slew of problems, including data packet loss than packet delay, both are degrade wireless network performance. Link failures between nodes occur when the network structure changes by a no of reasons, including channel interference. One important criterion that will determine service quality is link failure recovery (QoS). Path breaks between neighbouring nodes may occur as a result of the wireless environment's instability. The main causes of unintentional node failure in MANETs are channel quality, link quality, and node energy level. If any established link fails during data transmission, many researchers solve the problems by repaired the route locally or discover a new route, this procedure degrade the performance of network in existing routing algorithms. The QoS is improved by routing algorithms using to find an alternative path or repair local route failure when the link failure time is predicted in advance. The literature discusses various routing techniques for estimating link failure estimated time that are based on statistical, probabilistic, and trigonometric approaches. Furthermore, security is an important QoS factor; however, the network security requirements for QoS provisioning in MANET networks have received little attention, which is a major issue. A secure QoS aware scheme can be used in a variety of real world applications, for example defending any critical network against DoS than fabrication attacks. Data integrity, timely information deliveries are the primary requirements of patient monitoring systems. Recent advancements in MANET research have resulted in methods for mitigating a wide variety of malicious attacks [8]. Earlier research focused on using a variety of security schemes to ensure secure routing performance for Ad hoc. To prevent malicious nodes from entering the network, vast majority of routing approaches employ key management or cryptography techniques [9]. However, these security techniques suffer from a general drawback on key verification process than key exchange, which results in high network traffic. This leads to battery and computational capacity limitations, resulting in bandwidth constraints for MANET nodes and expensive schemes. A bio-inspired model is a novel field influenced by social behaviour. It primarily solves network problems due to its unique natural features and bottom to up approach. Because MANET is a distributed network system, researchers are investigating network best route analysis using bio-inspired methods. Bio-inspired routing protocols employ the swarm intelligence principle, which finds the ideal path to the destination in a distributed and autonomous manner in dynamically changing environments; for that reason, they can maximise routing performance, reduce control overhead, and quickly recover from a path failure due to modifications in network topology [10]. Bio-inspired routing techniques have the following advantages over traditional MANET routing protocols: First, because a swarm of ants or bees finds the optimal route to food in a distributed manner in dynamic environments, a routing protocol inspired by swarm behaviour is suitable for autonomously finding the shortest path to the destination in MANETs. Second, because swarm intelligence maintains the optimal path flexibly in a resource limited environment, the bio-inspired routing protocol can efficiently maintain the shortest path while reducing the occurrence of overhead. Third, because the swarm effectively solves various unpredictable problems in the real world, the bio-inspired routing protocol can quickly repair a link or node failure [6]. Several approaches proposed various routing algorithms with QoS support for MANETs over last decade. However, none of them are sufficient to incorporate all of the available QoS factors for efficient packet routing. The provisioning of QoS is well studied in ad hoc, with the main goal of the research being to improve the QoS factors by recovering link failure than detecting malicious nodes. The following section looks at some of the most recent existing MANET routing algorithms.

A. CBMNDM (Clusters Based Malicious Nodes Detection Methodology in MANET)

For detecting and removing malicious nodes, S. Gopalakrishnan et al [11] proposed a CBMNDM. A cluster key is assigned by cluster head for each node, than the assigned key is used for packet data transmission between the node and cluster head. The CH (cluster head) examines each data transaction from a node to see if it matches the key in their cluster table (CT). If the node is identity is valid the node is recognise as a member of this cluster; otherwise the node determined as a malicious node. In this paper, the author also discussed link failure occurs by the malicious node in MANET and gain of each link. The performance of the proposed method was assessed using the PDR, network life time, and energy consumption.

1. Clusters Based Malicious Nodes Detection

Clusters of nodes are formed by dividing the mobile nodes into smaller regions. Each cluster is led by a (CH) cluster head, which is in charge of controlling all nodes within their capacity. MANET keeps several CHs that are all connected to sink. The packet can be sent directly to sink or through other Cluster Heads by a single Cluster Head. Every CH keeps a CT (cluster table), and every mobile node keeps a NT (neighbour table). The CT includes information about all mobile nodes, distance between the CH and each node within the cluster, and the CK (cluster key). The CH assigns a cluster key to each mobile node in the cluster, which is used for packet data transactions between the CH and the node. The CH examines each data transaction from a node to see if it matches a key in their cluster table.

Algorithm to Remove the Malicious Node:

- **Step 1:** The cluster head locates the malicious node and adds it to the list of malicious nodes in the cluster table.
- **Step 2:** Distribute this malicious node list to all MANET cluster heads.
- **Step 3:** Within the cluster limit, all cluster heads broadcast this information to their corresponding nodes.
- **Step 4:** If the data comes from the malicious node, the cluster nodes do not respond to the malicious node.

Figure 1: Remove Malicious Node

2. Detection of Node Link Faults

Author used a link cost algorithm to detect link failure. For example, the author used three primary source (S) nodes: s_1, s_2, and s_3. All three source nodes (S) send this packet data to the sink node. The Node s_1 connects to the sink node via links l_2 and l_1. Node s_2 connects to the sink via links l_3 and l_1. Node s_3 connects to the sink node via links l_4 and l_1. Node s_3 may also send data to sink node via link l_5. There is a single unit link cost for each network link. Assume that links l_1 and l_5 are both lossy. The link cost algorithm, which is described below, can be used to find these lossy links:

Algorithm for link failure detection

- **Step 1:** Determine the probability of the link to be lossy.
- **Step 2:** Determine the number of possible fault path from source node to sink. Here, have four number of fault path as fp1 = {l_2, l_1}, fp2 = {l_3, l_1}, fp3 = {l_4, l_1} and fp4 = {l_5}.
- **Step 3:** Find the gain of each link in the network using below equation.

$$\Phi_k = p_k.\Phi_{kb} + (1 - p_k).\Phi_{kg} - c_k$$

where, p_k is the probability of a link to be fault.

Φ_{kb} is the cost of the link when the particular link is fault.

Φ_{kg} is the cost of the link when the particular link is not-fault and c_k is the cost of the link to be tested.

- **Step 4:** Find the lowest gain of the link and this link is concluded as a faulty link.

Figure 2: Link Failure Detection

B. Improved Failure Aware Third Party Auditor (IFTPA) Based Homomorphism Linear Authenticator (HLA) Mechanism (IFHM)

Researchers K. Vanitha., et al [12] proposed an (IFTPA) based HLA technique IFHM with SAODV to overcome the problems and have a well-organized malicious mobile node detection process than provide better performances. The proposed method used the trust verification method for data packet damage information and detects malicious node this process are done by using dropping routing, packet identification. In SAODV data packet dropping occurred by link failure or malicious nodes.

The author's primary goal was to locate the malicious node and the network failure link. For verification and linear process homomorphism, the HLA mechanism was used, and for authentication, the FTPA was used. By combining both techniques, the security process was defined as an FTPA based HLA technique IFHM. The FHM method was developed than clearly explained during previous phase of the author's work. Thereby, the proposed research improves the security and the pseudo random function (PRF), these are included in FHM. The PRF process was used to implement the privacy-preserving-public-auditing scheme and to integrate the method as a dynamic and linear process of generating the method in wireless network. In this case, a random process's PRF generator is deterministic than efficient, returning the sequence based on received input. It enables data encryption by utilising the secret key generating process, which is an arbitrary producing procedure. The proposed algorithm is based on FTPA, and HLA is a metadata and data integrity verification process (FTPA). As a result, this method is referred to as FHM, than security is referred to as IFHM. Detection process identifies malicious nodes by correlating lost packets. Following transmission, loss occurrences are identified, and the reason for dropping is specified. As a result of this process, the effects will not be visible in the next communication.

C. Proficient Trusted Node ID Based Resource Reservation Protocol (PT-NIDBRRP)

The PT-NIDBRRP was proposed by G. Jegan, a researcher [13]. Using a weighted end delay based approach, shortest path was found here. Proposed algorithm will find shortest path from starting point to target, potentially increasing detection rate. Sequence numeral and hop address are added to algorithm when route detection process is started. After determining shortest path, failed link was discovered. Link failure localization structure of employed trusted algorithm is better at predicting and resolving link failure issues. Posterior probability assessment was then used to determine the type of attack that caused the link failure.

1. Shortest path selection by weighed end delay technique

To determine shortest path between nodes, the weighed end delay was used. In this case, author relied on the expert trusted Node ID-based (RRP) resource reservation protocol. Proposed weighed end delay method calculated shortest path by determining weightage length of path from the source to each node. Weighed path is shortest path with no link breaks. Following the calculation of the path, information data packets can be sent directly to the destination mobile node. It is a time and energy saving method.

Algorithm: Shortest path prediction

- **Input:** Sequence number and Hops
- **Output:** Shortest path from source to the destination
- **Step 1:** Initialization of the hop parameters such as the communication range and number of the nodes.
- **Step 2:** Obtain the minimal hop count information between each node
- **Step 3:** Calculate average distance between the sensor nodes
- **Step 4:** Calculate of the estimated distance between the nodes
- **Step 5:** Estimation of the nodal location

Figure 3: Shortest Path Prediction

After calculating distance between each node, the nodes must be searched for a link breakage. Because a broken link allows data packets to return to their origin and the process to resume. As a result, the protocol used here was simply modified to find the link breakage, and the author developed a capable trusted Node ID-based RRP for easy prediction of link breakage.

2. Attack Estimation

The attack will be determined using the posterior possibility estimation technique.

This technique a probability distribution method for determining the unidentified prediction of a value, thanthe process is dependent on arbitrary variable selection. Main goal is for it to look for a related experience and arbitrarily observe the relevant data. To achieve goal, it is essential to provide a consistent intervals. Basically put, it can observe the member's possibility and reflect uncertainty value.
Assume that Baye's theorem applied to calculate variable's probability distribution. It is computed by multiplying probability distribution values by normalising constant.

$$P\left(\frac{\emptyset}{x}\right) = \left(P\frac{\left(\frac{x}{\emptyset}\right)}{P(x)}\right)P(\emptyset)$$

Where,

$P(\emptyset)$is the probability distribution function

$P\left(\frac{x}{\emptyset}\right)$is the likelihood function

$P\left(\frac{\emptyset}{x}\right)$is the evidence function

The posterior probability can be directly proportional to likelihood, which is a multiple of previous probability.

$$F(x) = [f(x)(x/y = y(x)/\int_{-\infty}^{\infty} f(x)(u)L(\frac{x}{y} = y(x)(u)du]$$

Where F(x) is the prior density function

f(x) L(x/y=y(x) which is a likelihood function

$f(x)(u)L(\frac{x}{y} = y(x)(u)$is a normalizing constant

The likelihood task was essentially used to map out function's likelihood. After determining previous probability, attack was determined.

D. Trust Path Ant Colony Optimization (TPACO)

The path of Trust S. Sugumaran's (TPACO) algorithm [14] is a swarm intelligent scheme for selecting a trust path from multiple routes between source (S) and destination (D). Proposed algorithm controls the Data Packet dropping occurrence and consent in network by serving as best route. TPACO algorithm, trust mobile node from sender (S) to destination (D) employed with ant colony algorithm, it consists of three steps: (1) discovered potential path, (2) path selection and updating, than (3) trust path selection. In this case, Trust value is calculated by choosing a probable path between the source (S) and destination (D), counting the no of hops, and calculating node's battery deviation in percentage.

1. Discovered Potential Path

Because sources (S) do not have a route to destination (D) at first, the ant's agent initiates the source requested message and distributes it to all the neighbouring nodes in the network. When the Forward ANT reaches a neighbour node that is not a destination node, it proceeds to the next hop with updated information about the neighbour node. Otherwise, Destination destroys Forward ANT requests and provides Backward ANT replay to sources. The Ant pheromone density is being deposited on paths at this time. If the pheromone value is less than the threshold value, the path is unsuitable for data transmission than should be terminated. The density of pheromones between the source and destination, as well as each adjacent node, determines path connectivity. If the Ants arrive at their destination, they must retrace their path to sources and update pheromone level in every node in network. If retraced path fails to reach sources on time due to a lengthy distance, a broken link, or a malicious node, pheromone density is fixed to zero after a time interval, than updated details are stored in the node register.

2. Path selection, Route update

Density of pheromones along the route and probability of periodinterval between the paths determine the path chosen from sender (x) to receiver (y). The time interval indirectly indicates distance of path. Thereby, one of major factors determines best network path. Forward ANTs typically move from sources in all directions around the node. The deposit of forward ANTs is pheromone, than it updates pheromone level in each mobile node. Multiple paths from sender to receiver are generated by the ant colony concept. To determine the best path to take, possibility of shortest paths and pheromone deviation on path are used.

$$Pt_{xy} = \frac{q_{xy}}{p(t)_{xy}}$$

Where $P(t)_{xy}$ represents best path from (x) to(y), $p(t)_{xy}$ represents probability of shortest paths from (x) to(y), than q_{xy} represents pheromone deviation.
Uncertainty malicious nodes are dropped the data packets, the ant agent forwards the data packets that were data dropped by the vulnerable mobile node, and the reduced pheromone density is set to zero, causing a time delay increase. Nonetheless, they only forward a percentage of data packets to next hop, and the pheromone density between two adjacent nodes is reduced compare to a level less than another path density level. Thereby, malicious nodes within network can be easily identified.

E. Trusted path Selection

The three factors such as average deviation of battery level, shortest route path, and lowest hop count between mobile nodes are used in this proposed method. Best path equation probability is regularly used to determine the shortest path (1).When compared to other direction route and battery deviation the trust path is selected by smaller no of hops. Both hop and battery deviation conditions provide a secure communication path while reducing packet drops and selfish attacks caused by vulnerable network nodes. Trust path's conditions are outlined below.

$$T_{path} = \frac{pt_{xy}}{\sum_{xy}(H_{xy}+\%Bat_{devi})} \quad \text{----- (1)}$$

In this case, percentage of node battery of their deviations is shown by below equation,

$$\%Bat_{devi} = \frac{different\ from\ actual\ battery\ level}{actual\ battery\ level} \times 100 \quad \text{----- (2)}$$

Hop count, Pheromone Deviation, and node battery deviation of each mobile node in wireless network is described using secure communication. When the pheromone deviation is lower than forty present the hop count from the total mobile node in the ad hoc network is lower than the threshold,

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

and the battery deviation of each wireless mobile node is lower than fifty present, secure communications is expected. Trusted mobile nodes provides efficient than possible data packet transmission paths. TPACO optimization algorithm is using to implement route protection techniques. The deposit pheromone of choose path was assigned the greatest route for data packet transmission. Where the source chooses the shortest route and other routes are saved for future use. MANET enables a larger number of nodes to enter and exit the network. A transmission delay in this case collapses the wireless network route and depletes node energy. Above this problem is avoided by employing the frequent path selection probability method and choosing the route from wireless network periodicals.

III. EXPERIMENTAL RESULTS

3.1 Simulation Environment

UC Berkeley is working on a discrete even driven simulator called NS2 (Network Simulator). It is a component of the VINT project. NS2 simulation software objective is to support networking investigation and learning. NS2 is an excellent tool for designing different routing algorithms, comparing different protocol algorithms, and evaluating traffic. It has a reputation for being a collaborative environment. It is freely distributed and open source. NS2 is used, maintained, and developed by a large number of organisations and individuals involved in development and research. The simulation environment consists of 50 wireless mobile nodes that form an evenly distributed mobile ad hoc network that travels over a 1500 x 1500 metre area in 500 seconds. The network's mobile nodes are all set up to use pre-existing techniques like CBMNDM, IFHM, PTNIDBRRP, and TPACO.

Table 1: Simulation Environment

Simulation Parameters	
Routing protocols	CBMNDM, IFHM, PT-NIDBRRP, TPACO
Simulation Time	500 sec
No of Nodes	50
Simulation Area	1500 X 1500
Pause Time	10 Sec
Traffic Type	CBR
Packet Size	512 Bytes
Rate	10 Packets/Sec
Number of Runs	5
Node Speed	5 Sec
Queue Size	50 Packets
Mobility Model	Random waypoint
Transmission Range	250 meter

3.2 Performance Parameters

Based on the performance metrics listed below, evaluate the performance of existing routing algorithms.

- **Throughput:** Defined as the amount of data packets transported over the course of the simulation. Routing algorithm proficiency is measured by throughput when receiving packets per destination (D). The following formula is used to calculate throughput: Throughput = number of delivered packets multiplied by packet size multiplied by 8 bits divided by total simulation time.
- **Packet Delivery Ratio (PDR):** The percentage of data packets received by the destination (D) versus data packets sent by the source (S).
- **End-to-End Delay (ETED):** End Delay is the quantity of time it takes to send packets from a source (S) to a destination (D).
- **Routing Overhead (RO):** Overload in the network is proportional to latency and occurs as a result of frequent node movement, network congestion, or high traffic.
- **Link break prediction:** It identifies breakpoints in the overall route.
- **Residual Energy (RE):** The remaining energy of the sensor node can be calculated by adding up the energy consumed while the node is in each state.

1. Packet Delivery Ratio

The delivery ratios of the CBMNDM, IFHM, PT-NIDBRRP, and TPACO methods are shown in Figure 4. When compared to other methods, the TPACO method had a higher packet delivery ratio and higher packet transmission efficiency. TPACO routing could detect congestion quickly and easily find the shortest route. The TPACO protocol was able to detect link breaks easily during the route recovery process prior to data transfer, resulting in gradual data loss reduction and significantly improved packet delivery rate.

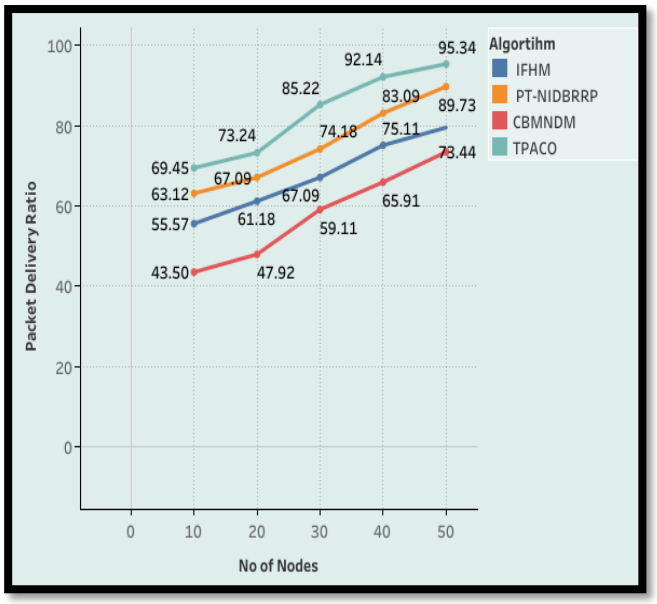


Figure 4: No of Nodes vs. PDR

2. Routing Overhead

Figure 5 compares the performance of the CBMNDM, IFHM, PT-NIDBRRP, and TPACO methods based on their overhead. Despite a slight increase in TPACO, packet receiving efficiency has improved.

The routing balancing of the network's load is causing the overhead promenade. According to the graph, the routing overhead of TPACO is less than that of CBMNDM, IFHM, and PT-NIDBRRP as the network size increases.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

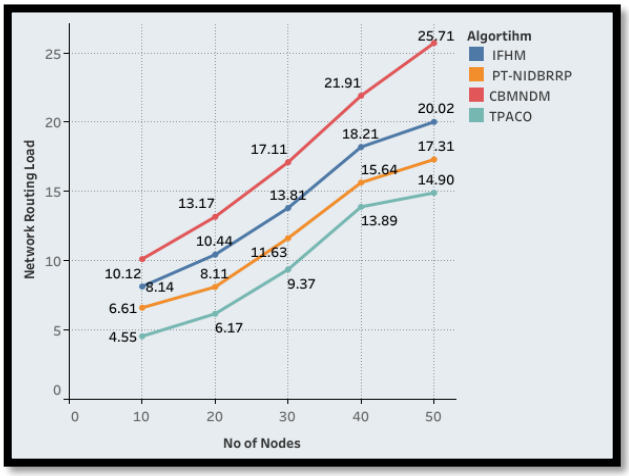


Figure 5: No of Nodes vs. Routing Overhead

3. End to End Delay

The outcome of network mobility of the CBMNDM, IFHM, PT-NIDBRRP, and TPACO algorithms are depicted by Figure 6.The end delay increases as node mobility rises from 10 to 100 metres per second. Higher amount of mobility causes more links halts and frequent redirecting, resulting in longer end delays.

The broken links may require another route recovery and route discovery progression. In every mobility condition, TPACO outperforms the competition.

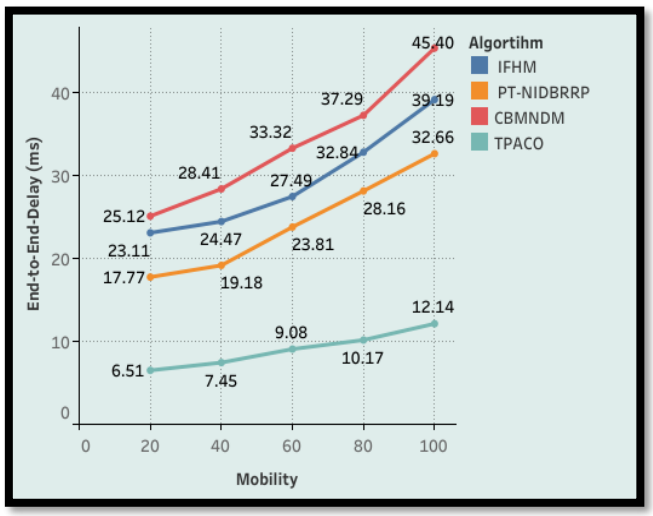
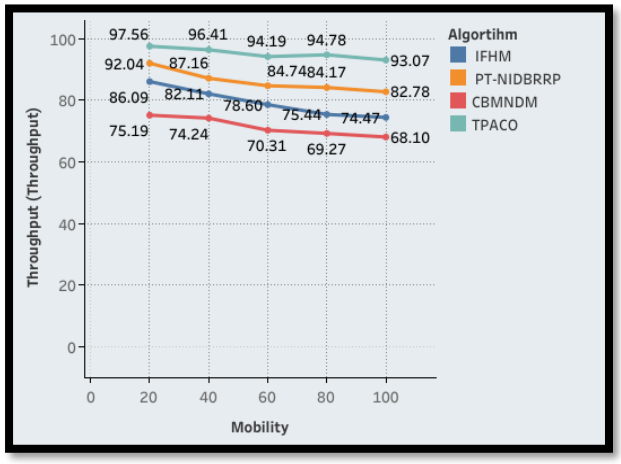


Figure 6: Node Mobility vs. End-to-End delay

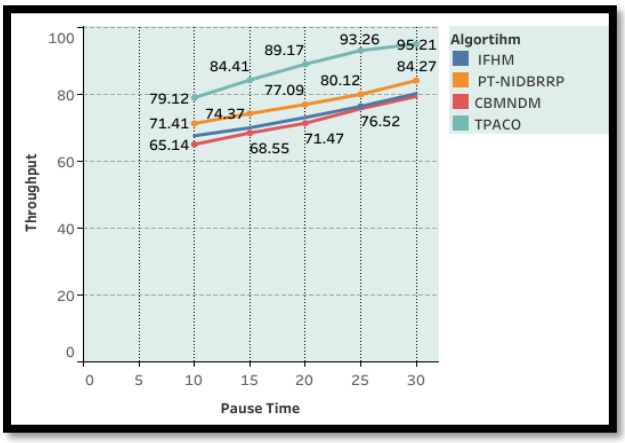
4. Throughput

Figures 7(a) and 7(b) show how mobility and pause time affect throughput for the protocols CBMNDM, IFHM, PT-NIDBRRP, and TPACO. 7(a)-During high mobility, methods such as CBMNDM, IFHM, and PT-NIDBRRP exhibit a small degradation in throughput due to high-link breakage, whereas.

TPACO exhibits a 3% improvement in throughput over other algorithms. Figure 7 (b) shows that there is no difference between algorithms; however, as the pause time increases, the difference between those throughputs grows significantly. Higher throughput is attributed to increased network longevity as a result of proper transmission power adjustment during the link selection phase and energy savings during the sleep scheduling phase.



(a)



(b)

Figure 7: (a) Effect of mobility on throughput, (b) Effect of pause time on throughput

5. Residual Energy

Figure 8 depicts the variation of energy as the amount of nodes increases. The remaining energy drops as the number of nodes increases to 10, 20, 30, and 50. The results show that the number of nodes has a negative effect on the remaining energy for all protocols. The TPACO technique is shown to conserve (save) energy more than other protocols because it establishes an ideal route from the source (S) to the destination (D) node. As a result, this path has the highest energy level; taking this approach reduces the likelihood of exhausting nodes.

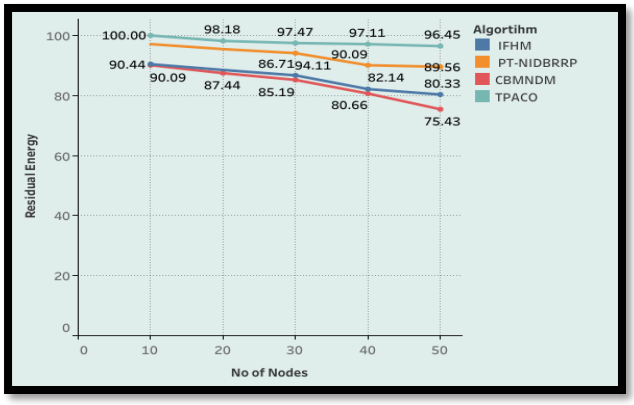


Figure 8: Residual Energy

Retrieval Number: 100.1/ijrte.A69490511122
DOI: 10.35940/ijrte.A6949.0511122
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

6. Link Breakage Prediction

Figure 9 show that the TPACO algorithm has fewer link breaks than all other existing protocols. Before the data communication process begins, the link breakage can be predicted (calculated). The link breaks as the node moves more. So, that was overcome in this case.

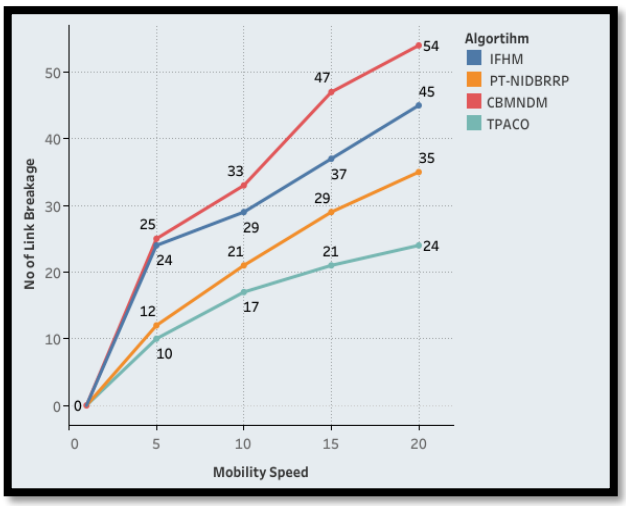


Figure 9: Mobility Speed vs. Link Breakage

7. Accuracy Prediction

The precision of the CBMNDM, IFHM, PT-NIDBRRP, and TPACO methods is depicted in Figure 10. Because the type of attack can be accurately predicted, the TPACO can acquire (obtain) greater accuracy than other existing methods. The attack in this case was determined to be a passive DoS attack, which was difficult to predict but was made possible by the implementation of the probability distribution method. In this experiment the accuracy prediction was determined by passive DoS attack, which attack was more difficult to predict. TPACO algorithms predict DoS attack efficient than other algorithms and also predict link breakage, its provide better results secure data communication.

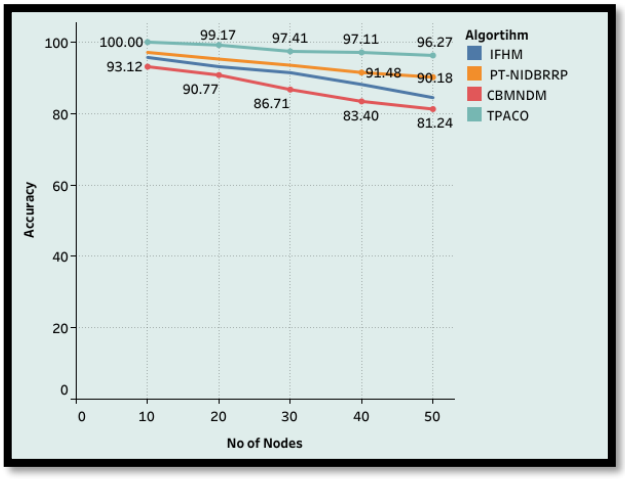


Figure 10: No of Nodes vs. Accuracy

8. Detection Rate

Figure 11 depicts the ability of the TPACO algorithm to detect malicious activity. The detection rate is compared to various scenarios in Fig. 11. Three scenarios were considered with 50 nodes in total. The detection rate decreases as the number of malicious nodes increases due to a decrease in the total number of normal nodes. Figure 11 concluded that swarm intelligence-based routing algorithms have a higher detection rate than other routing algorithms because they solve many optimization problems and provide the best solution.

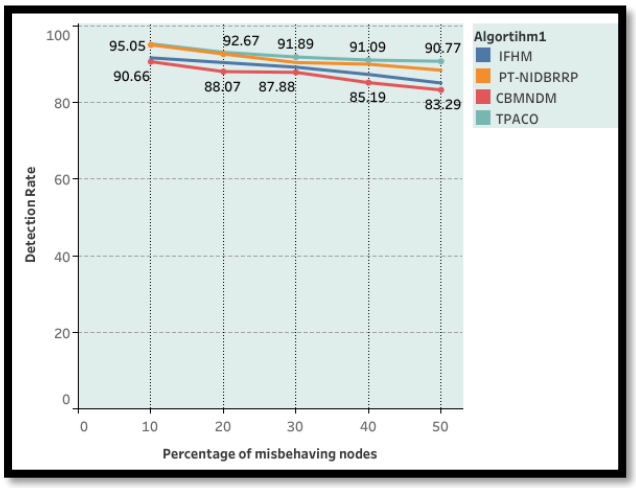


Figure 11: Detection Rate

IV. CONCLUSION

In this paper various routing algorithms for mobile ad hoc networks are compared, including one inspired by bio-inspired. The simulation results concluded the swarm intelligence-based algorithm performs better than others in different types of scenarios involving, for example, data loads, network mobility and network density. In terms of packet delivery ratio, end-to-end delay, throughput, and other quality of service metrics, TPACO algorithms outperform CBMNDM, IFHM, and PT-NIDBRRP routing protocols. TPACO, which is based on swarm intelligence, is found to outperform the competition.

REFERENCES

1. DevarajanJinilErsis, T.Paul Robert, “Review of ad-hoc on-demand distance vector protocol and its swarm intelligent variants for Mobile Ad-hoc NETwork”, The Institution of Engineering and Technology 2017.
2. P. Vijayalakshmi, S. A. J. Francis, and J. A. Dinakaran, ``A robust energy efficient ant colony optimization routing algorithm for multi-hop ad hoc networks in MANETs," Wireless Netw., vol. 22, no. 6, pp. 1_20, 2015.
3. Malathi, M., Jayashri, S. “Robust against route failure using power proficient reliable routing in MANET”. AEJ J. 2016. [CrossRef]
4. Chavhan, S.; Venkataram, P. “Emergent Intelligence Based QoS Routing in MANET”. ProcediaComput. Sci. 2015, 52, 659–664. [CrossRef]
5. S. Kalaivanan, “Quality of service (QoS) and priority aware models for energy efficient and demand routing procedure in mobile ad hoc networks,” Journal of Ambient Intelligence and Humanized Computing, vol. 12, no. 3, pp. 4019–4026, 2021.
6. R. T. Merlin and R. Ravi, “Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET,” Wireless Personal Communications, vol. 104, no. 4, pp. 1599–1636, 2019.
7. Calarany, C., &Manoharan, R. (2019). “An Efficient Evaluation of Bi-Objective Optimization of Path Stability Model for Mobile Ad Hoc Networks Using EN2RP”. Journal of Computational and Theoretical Nanoscience, 16(4), 1454-1464.

8. Khanna, G., Chaturvedi, S. K., &Soh, S. (2019). "Reliability evaluation of mobile ad hoc networks by considering link expiration time and border time". International Journal of System Assurance Engineering and Management, 10(3), 399-415.
9. Kumar, J., &Kathirvel, A. (2019). "Analysis and Ideas for Improved Routing in MANET".
10. Kumar, K. P., &Babu, B. P. (2019, April). "A Simple and Cost-Effective Anomaly Detection Paradigm on the Basis of Computational Intelligence for Mobile Ad-Hoc Networks from a Security Viewpoint". In Computer Science On-line Conference (pp. 78-86). Springer, Cham.
11. S. Gopalakrishnan, P. Mohan Kumar, "Performance Analysis of Malicious Node Detection and Elimination Using Clustering Approach on MANET", Circuits and Systems, 2016, 7, 748-758 Published Online May 2016.
12. Vanitha Kumar, A.M.J.Md.ZubairRahman, "Preventing malicious packet dropping nodes in MANET using IFHM based SAODV routing protocol", The journal of Networks, software tools and applications, ISSN-1386-7857,2019.
13. G. Jegan, D. Kamalakkannan, P. Samundiswary, "A Trusted Method for Early Data Link Failure Prediction", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8 Issue-5, January 2020.
14. S. Sugumaran, P. Venkatesan, "Optimized Trust Path for Control the Packet Dropping and Collusion Attack using Ant Colony in MANET", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249–8958, Volume-8, Issue-6, August 2019.

AUTHOR PROFILE

K.Vimala, received her M.Phil Degree from Bharathidasan University, Tiruchirappalli 2004. She received her M.Sc., Degree from Nehru Memorial College affiliated to Bharathidasan University, Tiruchirapalli in 2001. She is pursuing her Ph.D Degree (Part-Time) in Sri Vijay Vidyalaya College of Arts &Science, Dharmapuri, Tamilnadu, India. She is working as HOD Cum Assistant Professor in Department of Computer Science at Pavai Arts and Science College for Women, Anaipalayam, Rasipuram, Namakkal. Her current research of interests includes Wireless Sensor Network and Computer Networks.

Dr. D. Maruthanayagam, received his Ph.D Degree from Manonmaniam Sundaranar University, Tirunelveli in the year 2014. He received his M.Phil Degree from Bharathidasan University, Trichy in the year 2005. He received his M.C.A Degree from Madras University, Chennai in the year 2000. He is working as HOD Cum Professor, PG and Research Department of Computer Science, Sri Vijay Vidyalaya College of Arts & Science, Dharmapuri, Tamilnadu, India. He has above 21 years of experience in academic field. He has published 6 books, more than 45 papers in International Journals and 30 papers in National & International Conferences so far. His areas of interest include Computer Networks, Grid Computing, Cloud Computing and Mobile Computing.