International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V70I1P230
Volume 70 Issue 1, 252-258, January, 2022

Secure Aware Cluster-Based Routing For Manet Using A Multi-Objective-Trust Centric Flower Pollination Algorithm

Arudra Annepu[1], Priti Mishra[2]

[1]*Research Scholar, Department of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, R.T Nagar, Bangalore – 560032, India*
[2]*Associate Professor, Department of Computer Science and Engineering, Rajiv Gandhi Institute of Technology, R.T Nagar, Bangalore, 560032*

yarudra@gmail.com

Abstract *- A mobile Adhoc network (MANET) is a system of moveable nodes that are self-configured where the nodes in the network communicate through wireless links. However, the dynamic topology of the network creates route failures, higher energy consumption, and high delays. Moreover, the nodes in the MANE are vulnerable to malicious attacks because of their mobility and lack of solid infrastructure. In order to overcome this, the Multi-objective-Trust Centric Flower Pollination Algorithm (M-TCFPA) is proposed for achieving a safe and dependable network data transfer. This M-TCFPA method is used to perform secure-aware cluster-based routing over the network. The M-TCFPA trust, integrity factor, residual energy, and distance are all taken into account. For selecting a secure optimal cluster head (CH) and determining a secure routing path over the network. Performance of the M-TCFPA technique is evaluated using PDR, PLR, average end-to-end delay (AEED), and throughput metrics.. particularly, the current research, Trust-Based Secure Multipath Routing (TBSMR), is used for evaluating the M-TCFPA method. The PDR of the M-TCFPA method for 100 nodes is 98.85%, which is high when compared to the TBSMR method.*

Keywords — *Cluster-based routing, packet delivery ratio, Integrity factor, Mobile ad-hoc network, multi objective-trust centric flower pollination algorithm, Trust.*

I. INTRODUCTION

Generally, the MANET includes a group of mobile nodes which has a self-configuring and self-organizing architecture [1]. Each sensor in the MANET has behaved either as a router or host; therefore, it is used to transmit the data to the adjacent nodes [2] [3]. The significant merits of the MANET are allowing the data communication inside the network, which has different characteristics and maintaining the dynamic methodology. However, the nodes are limited to the transmission range that specifies the nodes cannot transfer data inside the network [4]. Hence, this network type is applicable for only the temporary communication links because it is infrastructure-less and it doesn't have any centralized control [5]. MANET is used in a variety of contexts, including vehicle networks, forestry, military applications, maritime communications, disaster recovery systems, etc. [6]. Since, the nodes in the network generate the random topology, it adopts multi-hop communication. So, the nodes in the communication range perform the direct data transmission. If the nodes aren't in the communication range, then the source node depends on the intermediate nodes for transmitting the data packets using multi-hop communication [7]. Each node in the MANET should periodically transfer the hello message for maintaining the local connectivity information. This information is essential to develop a dialogue between the parties adjacent nodes and remaining distant nodes [8].

The heterogeneity of the nodes is solved, and the amount of routing information is limited by using cluster-based routing in the MANET. The network is separated into clusters, and CHs are chosen from each cluster to improve the MANET performance. An important advantage of the CH is that it aggregates the data packets acquired from both the cluster members and other CHs [9] [10]. Better broadcasting is achieved by using the cluster-based routing protocol, where it performs the inter-cluster and intra-cluster data transmission [11]. The MANET topology is continually varying due to the random connections and mobile nodes, so the malevolent attacks may target network nodes attacks [12] [13] [14]. The identification of malicious actions over the network is essential for obtaining effective data communication. When the attack is not detected in the MANET, it results in higher packet loss and lower throughput [15]. Therefore, it is required to develop a security-aware cluster-based routing for improving the data delivery of the MANET.

The following is a list of the research's significant contributions:

- A secure optimal CH is selected by using the M-TCFPA method, where it is optimised by considering four distinct trusts, integrity factor, residual energy, and distance are examples of fitness values. Here, the trust and integrity factors are considered important fitness values that are used to ensure the nodes' trustworthiness and data correctness during communication.
- Next, a secure route path from the beginning until the end is discovered by using the M-TCFPA method. The malicious nodes are avoided by considering the trust and integrity factors, which improve the data delivery of the MANET.
- Therefore, the proposed M-TCFPA method achieves an improved PDR while minimizing the lag time between sending and receiving data packets.

The paper's general structure is as follows: An overview of previous studies is provided in Section 2 of this paper. Section 3 explains the M-TCFPA technique in great depth. For the M-TCFPA method's findings and explanation, as well as a comparison to other methods, see Section 4. In Section 5, the conclusion is made.

II. RELATED WORK

To prevent attacks, Sridevi, N., and Nagarajan, V. [16] created the dynamic on-demand protocol and PSO–BAT is a combination of the bat method in addition to particle swarm. The optimization techniques are a set of procedures for maximising efficiency. Both the PSO and BAT considered the location and velocity of their fitness values. This PSO–BAT performed the malicious attack detection without any unwanted energy consumption. However, an inappropriate fitness function derivation affects the network performance.

Xu, H. *et al.* [17] presented the Trust-based Probabilistic Broadcast (TPB) approach that concentrated on the overhead minimization generated by the malicious nodes. The trustworthiness of the nodes was used to compute the rebroadcast probability. In order to find out the node's trust level, we employed a lightweight trust management strategy. Hence, the untrusted nodes were prevented from discovering the route by using the rebroadcast probability. The developed TPB technique was used to reduce the number of repetitive packets that had to be relayed across the internet. This TPB was considered only on the node's trust values, but it failed to consider other optimal parameters such as distance and energy for optimising the path selection.

Usha, M.S., and Ravishankar, K.C. [18] created in place of classic AODV, the Novel Energy Efficient Trust Aware Routing (NETAR) select the most efficient route. In NETAR, the calculation of bandwidth, neighbour-node trust rate evaluation, energy, and malicious attack identification were utilised for enhancing the three trust degrees between the nodes. Here, the trusted neighbour node was chosen based on the higher received signal strength, residual energy, and channel capacity. Accordingly, the trusted node usage in the routing improved the network efficiency. However, this NETAR has its own drawbacks for identifying the absence of errors. If the error was not detected while transmitting the data packets, the packet loss should have occurred over the network.

Biga, M. and Pramila, S.R. [19] presented the stimulated meta heuristics method, namely the emperor penguin optimising algorithm for accomplishing an energy-efficient route over the MANET. Here, three distinct factors, the extent of energy depletion, congestion, and link firmness, were used to perform the secured route over the network. Therefore, the developed emperor penguin approach was used to acquire less delay while transmitting the packets. However, this Emperor Penguin approach ignores clustering, which is critical for effective data transmission over the network in the MANET.

Sirajuddin, M. *et al.* [20] developed the TBSMR algorithm to accomplish secure data transmission over the MANET. To put it another way, this TBSMR is an improved variant of the regular TBSMR procedure. The rogue node is identified by the source node transmitting a bogus RREQ packet. This TBSMR algorithm was used to identify malicious nodes in each stage of communication. However, the developed TBSMR did not consider the distance while transmitting the packets, which may have resulted in a high delay.

III. M-TCFPA METHOD

In this M-TCFPA method, a secure optimal CH and routing path are selected to achieve reliable transmission over the network. This M-TCFPA method has three different phases, such as clustering, CH selection, and routing path selection. Generally, clustering over the network is used to improve energy efficiency while performing data aggregation. Here, the CH selection and routing path generation using M-TCFPA are optimised by using the trust, integrity factor, remaining power, and distance.

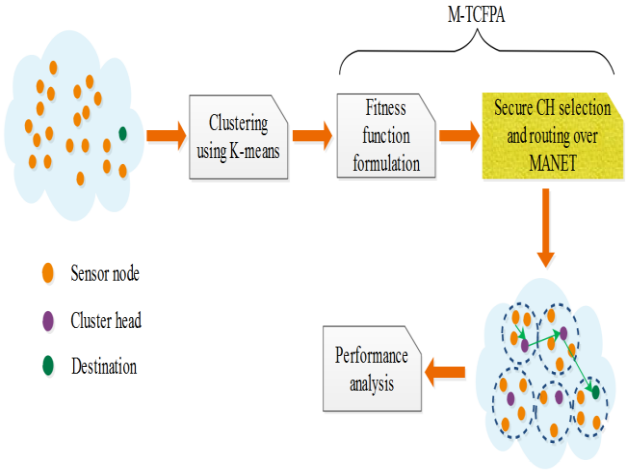

Figure 1. The M-TCFPA method's block diagram

The idea that has been floated M-TCFPA has the capacity to avoid malicious attacks by considering the trust and integrity factors in its fitness function. Figure 1 depicts the M-TCFPA method's block diagram.

A. CLUSTERING PROCESS

The first step is to randomly distribute the nodes in the network region of interest, followed by clustering using the K-means method. Here, the K-means divides the overall network into the number of clusters. Since then, the calculation of Euclidian distances has been mainly used in the K-means clustering process. After clustering the network, optimal CHs is selected from each cluster by using the M-TCFPA, which is explained in the following section.

B. SECURE OPTIMAL CH SELECTION

In the second phase, secure optimal CHs are selected from the clusters for achieving robustness against malicious attacks and for minimising the energy consumption of the nodes. Since Xin-She Yang created the FPA, a population-based optimization technique, this FPA replicates the behaviour of flower pollination. Generally, "pollination" specifies the natural physiological process of plants mating that is related to the pollen transfer accomplished by pollinators (e.g., insects). In this research, the conventional FPA is modified into a Multi-objective-Trust Centric FPA (M-TCFPA) by considering the distinct fitness parameters such as trust, integrity factor, residual energy, and distance. The process of CH selection using the M-TCFPA is explained as follows:

a) Representation and Initialization

The potential solution is represented by using the flower/ pollen of the M-TCFPA. Here, the group of sensor nodes are denoted by the population to select an appropriate candidate node as a CH. CHs are needed in the network in proportion to the population's dimension. Each population receives a unique node ID ranging from 1 to N, where N is the total number of sensor nodes in the network. The initialization of M-TCFPA is expressed in the following equation (1).

$$x_i = (x_{i,1}, x_{i,2}, .., x_{i,NCH}) \quad (1)$$

Where the position of each population $x_{i,d} 1 \leq d \leq NCH$ represents any of the candidate node_ID between all nodes.

b) Iterative process

The pollination accomplished in the M-TCFPA has two types: self-pollination and cross-pollination. In that, self-pollination means a single bloom is pollinated by pollen from a single blossom. If the transferred pollen grain from another plant fertilises the plant, then it is referred to as "cross-pollination." Moreover, there are different ways that the flowers try to distribute their pollen. Abiotic pollination is one of the different pollination methods where the pollen is distributed through the wind. Next, the pollination that happens through birds, bats, insects, and other animals is referred to as "biotic pollination." Additionally, the flower constancy is monitored for insect pollinators, especially honeybees. These types of pollinators move towards a certain flower type and avoid the remaining species, which are used to increase the reproduction of similar flower types. In this iterative process of the M-TCFPA, a variety of factors, including trust, integrity, residual energy, and distance, all play a role, which is used to enhance the search probability during the CH selection. The following four rules are considered in the M-TCFPA:

- Using biotic and cross-pollination as global pollinations, pollinators are carrying pollen travel across large distances, following the Lévy flights (Rule 1).
- Next, local pollinators are biotic and self-pollination (Rule 2).
- Similar to reproduction likelihood, floral constancy is seen as a result of the resemblance of two flowers engaging in pollination (Rule 3).
- The switching probability is considered to obtain the switching between local pollination and global pollination (Rule 4).

The flower constancy specified for the global pollination stage is expressed in equation (2).

$$x_i^{t+1} = x_i^t + \gamma L(\lambda)(g_* - x_i^t) \quad (2)$$

Where the ith pollen at iteration t is denoted as x_i^t; the best solution is denoted as g_*; the scaling factor utilized for controlling the step size is represented as γ; the Lévy flights based step size is represented as $L(\lambda)$, which is related to the pollination's strength. The insects fly through the high distance with the Equation obtained from the Lévy distribution showing the unique distance steps (3).

$$L \sim \frac{\lambda \Gamma(\lambda) \sin\left(\frac{\pi\lambda}{2}\right)}{\pi} \frac{1}{s^{1+\lambda}} \quad (s \gg s_0 > 0) \quad (3)$$

Where the gamma function is specified as $\Gamma(\lambda)$ and In the case of large steps s>0, this dispersion holds true. Flower constancy Rule 2 and (Rule 3) are used to accomplish the local pollination, which is expressed in equation (4).

$$x_i^{t+1} = x_i^t + \varepsilon(x_j^t - x_k^t) \quad (4)$$

Where the pollen obtained from various flowers of the same plant varieties are represented as x_j^t and x_k^tAnd the random number between the range of [0 1] is denoted as ε. The position update is represented as a local random walk when the x_j^t and x_k^t They are taken from the same species or from the same population. Further, pollination has occurred at both the local and global levels (Rule 4).

c) Multi-objective fitness function formulation

In the conventional CH selection process, the CHs are selected mainly based on the residual energy and distance, which leads to decreased performance. But, the designed M-TCFPA considers four optimal fitness function parameters

during the CH selection. The optimal fitness parameters used in the M-TCFPA are defined as follows:

1) Trust

The trust value of each node is regarded to be one of the essential fitness factors in this multi-objective problem. As a result, the mobile nodes in the MANET are connected to one another via the establishment of a mutual trust relationship. The trust value is derived in this case based on direct conversations, while it is tied to the packet forwarding behaviour in the previous case. It is defined as the ratio of broadcast packets to received packets between nodes, and it is expressed as a percentage and is expressed in equation (5).

$$Trust = \frac{Amount\ of\ broadcasted\ packets_{a,b}}{Amount\ of\ received\ packets_{a,b}} \quad (5)$$

2) Integrity factor

When data is transported from one node to another, the integrity factor is used to determine whether or not the transmitted data packets are infected with a virus or not. Moreover, this integrity factor is used to analyse whether the packets are broadcast at a definite time as well as to guarantee integrity. The following equation (6) expresses the integrity factor analysed between the node and

$$IF = \frac{Amount\ of\ correctly\ forwarded\ packets_{a,b}}{Amount\ of\ packets\ not\ forwarded\ yet_{a,b}} \quad (6)$$

Where IF defines the integrity factor, here, the evaluation node is a, and the node is required to be examined in b.

3) Residual energy

The neighbouring node is selected by the source CH as the next-hop node for the purpose of sending packets to the destination. The chosen CH has its own challenging task, i.e., it has to perform the data aggression for the data received from its intra and inter-cluster members. Hence, the nest hop node with a large amount of residual energy is considered the preferred choice while broadcasting the data. The residual energy is expressed in equation (7).

$$RE = \sum_{i=1}^{NCH} E_{CH_i} \quad (7)$$

Where the residual energy is represented as RE and the residual energy of the ith CH is denoted as E_{CH_i}.

4) Distance

The Euclidean distance among the nodes to CH and CH to destination is also considered for the nodes' energy usage should be reduced.

In addition, the weighted sum approach is used for converting the multiple objectives into a single objective function which is expressed in equation (8).

$$Fitness = \beta_1 \times Trust + \beta_2 \times IF + \beta_3 \times RE + \beta_4 \times Distance \quad (8)$$

Where, $\beta_1, \beta_2, \beta_3$ and β_4 represents the weights assigned to each fitness value which are equal to 0.3, 0.3, 0.2 and 0.2, respectively. The optimum CHs are obtained from the cluster using the fitness function that was defined before. The benefits of using derived fitness values are mentioned as follows; the trust value used to M-TCFPA improves the robustness against the malicious attacks; the properties of data correctness and the data packets are forwarded in the definite time or not are evaluated by the integrity factor. Therefore, these trust and integrity factors are used to improve the PDR. The residual energy is used to avoid the node/ link failure during the data transmission. Finally, the distance factored into the fitness values is utilised to find the shortest route to and from the location CH.

C. SECURE ROUTING USING M-TCFPA

After performing the clustering, the phase of the destination node is initiated to identify the secure path. Here, It is identified the secure the route from the origin CH to the endpoint CH. by using the same fitness criterion that was used in the CH selection process. The M-TCFPA is initialised with the most secure routing route from the source to the destination during this phase, which affects each population of M-TCFPA. The M-TCFPA employs the control messages of the AODV, such as the Route Request, Route Reply, Route Error and HELLO, throughout the route discovery portion of the process. Initially, during route discovery, the source node broadcasts the RREQ message to all other nodes in the network. Following that, depending on the RREP message received from the reverse route, the next-hop CH with the best fitness is chosen and used. It is formed by receiving the RREP message from a neighbouring node that the route from the transmitter to the receiver is defined will be created and used. Here, secure data transmission is accomplished by avoiding malicious attacks during communication. On the other hand, route maintenance is accomplished by using the HELLO and RERR messages.

IV. RESULTS AND DISCUSSION OF THE FINDINGS

Discussion of the findings and recommendations made during the M-TCFPA method are explained in this section. For the simulation of the M-TCFPA method, the Network Simulator 2.34 (NS-2.34) is used in the Ubuntu OS along with the 8 GB of RAM and the i5 processor. To perform secure aware data transmission, the M-TCFPA takes four different fitness functions into account: trust, integrity factor, residual energy, and distance. Varying nodes of 10 to 200 nodes are considered in this simulation over the network area of Moreover, the simulation time considered during the simulation is 500 sec, whereas the simulation parameters of the M-TCFPA method are mentioned in Table 1.

Table 1 summarises the parameters used in the simulations.

Parameter	Values
Number of nodes	10, 50, 100, 150 and 200
Area	$500m \times 500m$
Cluster-based routing protocol	M-TCFPA
Mobility model	Random waypoint
Maximum speed	20 m/s
Traffic type	CBR
Packet size	512bytes
Simulation time	500 sec

On the basis of the PDR, the PLR, the AEED, and the throughput, we evaluate the performance of the M-TCFPA technique. For the purpose of evaluating the performance of the M-TCFPA approach, we use an established method, TBSMR [20].

A. PACKET DELIVERY RATIO

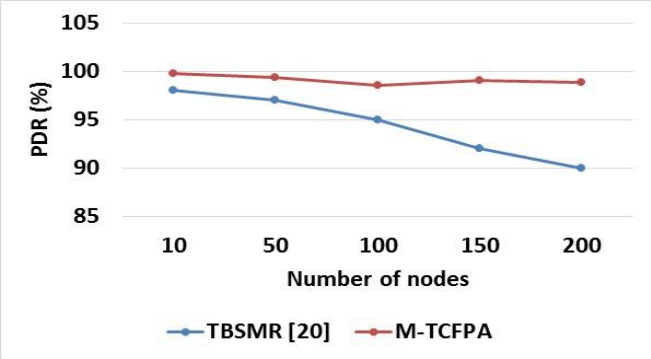

Figure 2. PDR for varying nodes

The packet delivery ratio (PDR), as indicated in equation (9), Received packets are divided by the total number of packets provided by network traffic.

$$PDR = \frac{Total\ amount\ of\ packets\ received}{Total\ amount\ of\ packets\ transmitted} \times 100 \quad (9)$$

The comparison of PDR for TBSMR [20] with the M-TCFPA method is shown in Figure 2. The PDR of the M-TCFPA method **varied from 98.50% to 99.77%.** Based on Figure 2, it can be inferred that the M-TCFPA approach delivers a greater PDR than the TBSMR method [19]. Examples are the M-TCFPA, which has a PDR of 98.85 per cent for 200 nodes, which is excellent when compared to the TBSMR [20] and the TBSMR [21]. i.e., 90%. The M-TCFPA method achieves higher PDR by minimising the packet drops caused by malicious attacks. Here, the trust value and integrity factor considered in the multi-objectives are used to increase the robustness against malicious attackers.

B. PACKET LOSS RATIO

The PLR is a measure of how many data packets are lost during the transmission of data packets across a network connection. In network communications, the PLR is defined as the relationship between the total number of lost packets and the total number of received packets, as given in equation (10).

$$PLR = \frac{Total\ amount\ of\ lost\ packets}{Total\ amount\ of\ packets\ received} \times 100 \quad (10)$$

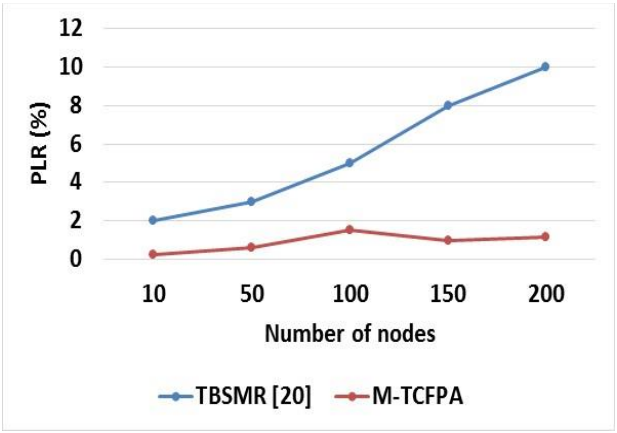

Figure 3. PLR for varying nodes

The findings of the study are shown in Figure 3. PLR analysis for TBSMR. [20] and M-TCFPA. The PLR of the M-TCFPA method varied from 0.22% to 1.49%. Here, the PLR of the M-TCFPA method is less when compared to the TBSMR [20]. For instance, the PLR of the M-TCFPA method is 1.14% for 200 nodes, which is less when compared to the TBSMR [20]. The PLR of the M-TCFPA method is reduced by avoiding malicious attacks during communication. Moreover, this M-TCFPA method performed malicious node monitoring at each stage of the communication to reduce packet loss.

C. THROUGHPUT

The rate of throughput is referred to as the destination collected the data packets in the unit of bits per second.

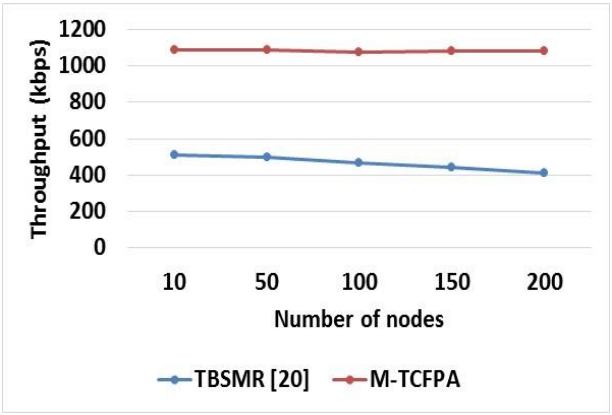

Figure 4. Throughput for varying nodes

The comparison of throughput for TBSMR [20] with the M-TCFPA method is shown in Figure 3. The throughput of the M-TCFPA varies from 1077.85 kbps to 1090.36 kbps. From Figure 3, it is concluded that the M-TCFPA method achieves higher throughput than the TBSMR [20]. For example, the throughput of the M-TCFPA method for 200 nodes is 1083.27 kbps, which is higher than the TBSMR [20]'s throughput, i.e., 410 kbps. The throughput of the M-TCFPA method is improved based on the robustness against the malicious attacks and the elimination of node/ link failure by considering the residual energy in the multi-objectives.

D. AVERAGE END-TO-END DELAY

It is the average amount of time necessary to convey data from a source site to a destination location that is defined by this phrase. This AEED comprises a processing time, transfer time, propagation delay and queuing time.

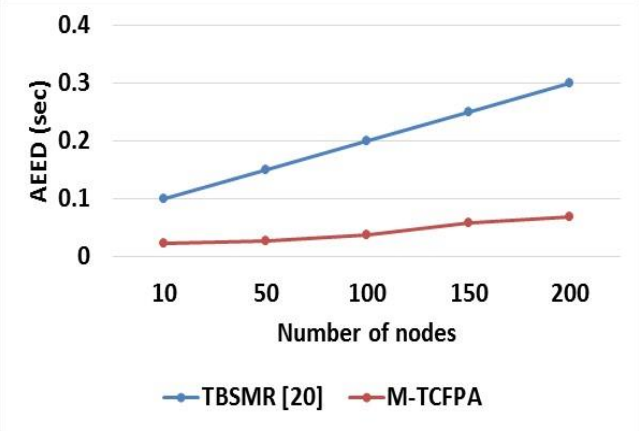

Figure 5. AEED for varying nodes

Figure 5 shows the analysis of the AEED for TBSMR [20] and M-TCFPA. The AEED for the M-TCFPA varied from 0.024 to 0.070 sec. The AEED of the M-TCFPA method is less than the TBSMR [20] while transmitting the packets. For instance, the AEED of the M-TCFPA method for 200 nodes is 0.070 sec. It is less when compared to the TBSMR [20]. The delay of the M-TCFPA method during communication is decreased based on the shortest path identification and fewer control packet transmissions obtained in the route discovery phase.

In a nutshell, the comparative analysis of M-TCFPA with the existing TBSMR [20] is given as follows:

Table 2. Comparative analysis of M-TCFPA

Performances	Method	Number of nodes				
		10	**50**	**100**	**150**	**200**
PDR (%)	**TBSMR [20]**	98	97	95	92	90
	M-TCFPA	99.77	99.37	98.50	99.04	98.85
PLR (%)	**TBSMR [20]**	2	3	5	8	10
	M-TCFPA	0.22	0.62	1.49	0.95	1.14
Throughput (kbps)	**TBSMR [20]**	510	500	470	440	410
	M-TCFPA	1090.36	1086.1	1077.85	1083.72	1083.27
AEED (sec)	**TBSMR [20]**	0.1	0.15	0.2	0.25	0.3
	M-TCFPA	0.024	0.027	0.038	0.060	0.070

Table 2 shows the comparative analysis between the TBSMR [20] and M-TCFPA method. It is possible to compare different numbers of sensor nodes by changing the number of sensor nodes used: 10, 50, 100, 150, and 200. It can be deduced from Table 2 that the M-TCFPA approach outperforms the TBSMR method [20] in terms of performance. The TBSMR [20] considered only the trust, traffic, and residual energy values during the data transmission. This TBSMR [20] doesn't consider the distance while transmitting the data packets. Because of this, the delay of the TBSMR [20] is increased as the data packets are being sent. The M-TCFPA approach, on the other hand, is a noninvasive procedure. Takes into account four ideal fitness values, including trust, integrity factor, residual energy, and distance, among others. The trust and integrity factors considered in the M-TCFPA method are used to ensure the nodes' trustworthiness and data correctness during the communication. Hence, the data delivery of the M-TCFPA method is increased while minimising the delay in the transmission phase.

V. CONCLUSION

The M-TCFPA approach is proposed in this article for developing a secure cluster-based routing system capable of accomplishing effective data transfer. The K-means clustering method is used in this process. Optimise data transmission in the MANET. The secure optimal CH and routing are selected using the M-TCFPA method's four separate fitness parameters: trust, integrity factor, residual energy, and distance. The trust and integrity factors are utilised to boost the robustness of the M-TCFPA against malicious attacks, resulting in a rise in PDR. Additionally, the M-TCFPA method's consideration of residual energy results in the avoidance of node failures along the routing path. As a result, the suggested M-TCFPA approach

achieves a better level of resistance against malicious assaults while decreasing data transmission delay. Based on the results of the performance study, it has been determined that the M-TCFPA technique outperforms the TBSMR approach. When compared to the TBSMR approach, the PDR of the M-TCFPA method is 98.85 per cent for 100 nodes, which is an extremely high percentage.

REFERENCES

[1] Thiyagarajan, P. and Senthilkumar, S., Power-efficient memetic optimized and adjacent exponentially distributed routing in mobile ad hoc networks. Computer Communications, 150 (2020) 209-215.

[2] Rajeswari, A.R., Kulothungan, K., Ganapathy, S. and Kannan, A., A trusted fuzzy-based stable and secure routing algorithm for effective communication in mobile ad-hoc networks. Peer-to-Peer Networking and Applications, 12(5) (2019) 1076-1096.

[3] Robinson, Y.H. and Julie, E.G., MTPKM, Multipart trust-based public key management technique to reduce security vulnerability in mobile ad-hoc networks. Wireless Personal Communications, 109(2) (2019) 739-760.

[4] Krishnan, R.S., Julie, E.G., Robinson, Y.H., Kumar, R., Son, L.H., Tuan, T.A. and Long, H.V., Modified zone-based intrusion detection system for security enhancement in mobile ad hoc networks. Wireless Networks, 26(2) (2020) 1275-1289.

[5] Borkar, G.M. and Mahajan, A.R., A secure and trust-based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Wireless Networks, 23(8) (2017) 2455-2472.

[6] M. Ramesha, K. Jeevan 2020. Implementation of IoT Based Wireless Electronic Stethoscope, Third International Conference on Multimedia Processing, Communication & Information Technology (MPCIT), (2020) 103-106, doi, 10.1109/MPCIT51588.2020.9350476.

[7] Desai, A.M. and Jhaveri, R.H., Secure routing in mobile Ad hoc networks, a predictive approach. International Journal of Information Technology, 11(2) (2019) 345-356.

[8] Bisen, D. and Sharma, S., Enhanced performance through agent-based secure approach for mobile ad hoc networks. International Journal of Electronics, 105(1) (2018)116-136.

[9] Kishore D.V, Shivashankar, and S. Mehta., MANET topology for disaster management using wireless sensor network, in International Conference on Communication and Signal Processing, ICCSP, (2016) 0736–0740, doi, 10.1109/ICCSP.2016.7754242.

[10] Umar, Muhammad &Mehmood, Amjad& Song, Houbing. SeCRoP, secure cluster head centred multi-hop routing protocol for mobile ad hoc networks, SeCRoP. Security and Communication Networks. 9. 10.1002/sec.1544 (2016).

[11] Vatambeti, R., Sanshi, S. and Krishna, D.P., An efficient clustering approach for optimized path selection and route maintenance in mobile ad hoc networks. Journal of Ambient Intelligence and Humanized Computing, (2021) 1-15.

[12] Khalladi, R., Rebbah, M. &Smail, O. A new efficient approach for detecting single and multiple black hole attacks. J Supercomput 77 (2021) 7718–7736. https,//doi.org/10.1007/s11227-020-03596-1.

[13] Raja, R. and Ganeshkumar, P., QoSTRP, A trusted clustering based routing protocol for mobile ad-hoc networks. Programming and Computer Software, 44(6) (2018) 407-416.

[14] Anita, R., Joint cost and secured node disjoint energy-efficient multipath routing in mobile ad hoc network. Wireless Networks, 23(7) (2017) 2307-2316.

[15] Vatambeti, R., A novel wolf based trust accumulation approach for preventing malicious activities in mobile ad hoc networks. Wireless Personal Communications, 113(4) (2020) 2141-2166.

[16] Sridevi, N. and Nagarajan, V., Efficient traffic control and lifetime maximization in mobile ad hoc networks by using PSO–BAT optimization. Wireless Networks, 27(2) (2021) 861-870.

[17] Xu, H., Si, H., Zhang, H., Zhang, L., Leng, Y., Wang, J. and Li, D., Trust-based probabilistic broadcast scheme for mobile ad hoc networks. IEEE Access, 8 (2020) 21380-21392.

[18] Usha, M.S. and Ravishankar, K.C., Implementation of Trust-Based Novel Approach for Security Enhancements in MANETs. SN Computer Science, 2(4) (2021) 1-7.

[19] Thebiga, M. and Pramila, S.R., Adaptable and energy efficacious routing using modified emperor penguin colony optimization multi-faceted metaheuristics algorithm for MANETS. Wireless Personal Communications, 118(2) (2021) 1245-1270.

[20] Sirajuddin, M., Rupa, C., Iwendi, C. and Biamba, C., TBSMR, A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network. Security and Communication Networks, (2021).