Received: January 3, 2023. Revised: April 21, 2023.

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Metaheuristic Based Energy Efficient Routing Protocol in MANET Using Battle Royale Optimization

Vasantha Kumara Mahadevachar[1]* **Naveen Thimmahanumaiah Hosur**[1]

[1]*Department of Computer Science & Engineering, Government Engineering College, Hassan, India*
* Corresponding author's Email: cmn.vasanth@gmail.com

Abstract: Trust based routing with energy efficiency in mobile ad hoc networks (MANET) is a challenging task due to the complex nature of the network. Based on the MANET infrastructure, the interoperability of temporary communication is assured; however, there is no supervisory control process for MANET routing in terms of trust and security. As a result, stability routing is avoided in MANETs which can damage the network's dynamic nature. In this paper, a trust based multi-objective battle royale optimization (T-MOBRO) algorithm is proposed based on the conventional battle royale optimization (BRO) algorithm. To address the limitation of trust based energy efficiency routing in conventional BRO, a novel method T-MOBRO is suggested. The T-MOBRO algorithm establishes trust based routing along with energy efficiency by considering trust, energy, distance as its fitness function. The multi-objectives of the proposed model are said to be distance, energy consumption, packet forwarding rate (PFR), end to end delay (EED), direct trust ($Trust^{DT}$), and indirect trust ($Trust^{IDT}$). The BRO algorithm is based on gameplay that is inspired by battle royale video games. The proposed approach is evaluated using throughput, average energy consumption, packet delivery ratio, end to end delay (EED). The PDR for the developed T-MOBRO method for 10 nodes is 99.58%, throughput is 4032.29 bits/second, end to end delay is less with 0.0070 seconds, and energy consumption of the MANET is less with 1.7Joules for the T-MOBRO method.

Keywords: Battle royale optimization algorithm, Mobile ad hoc networks, Packet forwarding rate, Trust based routing protocol, Wireless sensor networks.

1. Introduction

Infrastructure networks and infrastructure-less networks are two subclasses of wireless networks. A mobile ad hoc network is a wireless network topology that is a part of infrastructure networks with movable communication routes and mobile network nodes. MANETs are a developing area in wireless networking in which mobile nodes communicate in impromptu or ad hoc networks. The node topology of MANET networks is always in an active state due to its node mobility [1, 2]. MANET mobile nodes move randomly and arbitrarily to form a non-permanent and effective topology suitable for sensitive and crucial applications such as military and emergency operations [3]. Routing is regarded as one of the most significant issues in MANETs due to its active and disseminated nature. MANETs routing protocols are vulnerable to several attacks, particularly packet drop attacks. Delivering long-standing routes may help to reduce communication delays between network nodes [4]. Hence, secure and energy-efficient protocols are required. The routing protocols should be designed to reject commonly used attacks such as network data intercepting, hijacking, and jamming. Some of the MANET security services include authentication, confidentiality, integrity, anonymity, and availability which are effective for mobile users. Another significant security attribute that needs to be addressed is QoS (quality of service). The QoS constraints are violated when the network defense mechanism is poor, as it allows unauthorized access to the network [5, 6]. Different applications have different QoS requirements in terms of data loss, postponement, and throughput. QoS management is critical for providing beginning-to-finish QoS guarantees. Routing protocols that are already existed such as ad hoc on-demand distance vector popularly known as AODV, temporally ordered routing algorithm, and dynamic source routing are inadequate for real-time applications. A communication network is required by the application to ensure QoS parameters. [7]. To improve routing efficiency, the organization of MANET into a hierarchy should be improved, which can be achieved through the clustering schemes. The technique of clustering is performed for re-organizing all nodes into small-sized clusters based on their regional proximity and the cluster head, with each cluster determined by the same rule. The task of the cluster head is to supervise cluster operations like cluster process management, routing table updates, and route discovery. Two types of nodes can be observed in the clustering process namely: ordinary nodes and gateway nodes. Ordinary nodes are those in the cluster that are not the cluster head. Gateway nodes are nodes that have inter-cluster links and can communicate with one or more clusters. If the destination is within the cluster, packets are sent to the cluster head; otherwise, they are sent to the gateway node [8, 9]. Numerous routing protocols have been proposed based on different network structures, mobility scenarios, and different programs for ad hoc networks. The mobility of nodes is a difficult task for routing protocol designers [10].

The major contribution of the work is discussed below:

- The trust routing in MANET to a respected destination is generated by using the trust based multi-objective battle royale optimization (T-MOBRO) algorithm. The algorithm considers trust as the primary cost value for avoiding malicious attackers in the route that helps to improve the data delivery over the network.
- The primary objective of this work is to provide trust measurements in the MANET based on trust parameters using a conventional battle royale optimization algorithm. Further, the T-MOBRO algorithm is optimized using a trust, energy, and distance.
- The EED and distance used in the T-MOBRO method are used to minimize the delay during the transmission by selecting the trusted route with less traffic and less distance. The energy consumed in the network is achieved by mitigating malicious nodes.

The rest of the paper is arranged as follows: Section 2 offers the related work accomplished on the routing protocols in MANET. Detailed information about the T-MOBRO method along with its trust factors is given in section 3. The outcomes of the T-MOBRO method are provided in section 4. whereas section 5 provides the conclusion.

2. Literature review

Sathyaraj [11] developed a secure route analysis method for real-time applications that consider the trust of IoT devices and their discovered routes of intermediate nodes for secure routing in MANET. The technique used two approaches in which the first approach involved finding a path list from the source to the destination node. The second approach was implemented to evaluate mobile node secure route support by evaluating IoT device support. The method calculates the data forwarding support value (DFS) by taking the no. of IoT devices in the route for contemplation. Based on the value of DFS, an individual path has been selected to improve MANET's QoS. The proposed method achieved the highest efficiency and increased throughput in secure routing. Alagan Ramasamy Rajeswari [12] developed a new trust-based secure energy aware clustering (TSEAC) model along with two novel algorithms namely: an energy-efficient trust-aware secure clustering algorithm and a filter untrustworthy recommender (FUR) algorithm. The TSEAC method was implemented to build a stable and secure trustworthy cluster head. The proposed approach built the cluster head by reducing malicious nodes. The FUR algorithm was responsible for improving the process of clustering by minimizing distortion attacks. A beta distribution technique was also implemented to predict the value of node trust in both a direct and indirect manner. The proposed TSEAC method outperforms the network lifetime compared to the CBTRP, AOTDV, and CBRP existing methods. Ankita A. Mahamune [13] implemented an Efficient Trust based Routing Scheme (ETRS) to provide secure communication in MANET by detecting, preventing and mitigating malicious nodes. Ad hoc on-demand distance vector was designed and implemented within the context of an inherent dynamic routing protocol (AODV). The proposed scheme's performance was validated by comparing it to the cutting-edge evolutionary self-cooperative trust evolutionary self-cooperative trust (ESCT) scheme and the traditional AODV. The proposed framework is validated using performance metrics such as PDR, EED, throughput, and jitter and other metrics were used to demonstrate the supremacy.

M. S. Usha [14] developed a novel energy efficient trust aware routing protocol novel also known as NETAR for the conventional AODV to improve the three degrees of trust between the nodes in the MANET. The nodes' trust was built by combining the estimation of trust rate of neighbor-node, calculation of bandwidth, energy and prediction of malicious behavior, and performance metrics such as PDR, delay, false positive, and throughput to improve network link life time (NLT). The NS2 simulator was employed where the simulation results outperformed the existing routing protocols with the proposed NETAR framework. Ganesh Kumar Wadhwani [15] developed a trust-based framework to build a flexible network that was adaptable to malicious nodes using the ad hoc on-demand distance vector (AODV) routing protocol as a basic routing protocol. The performance metrics of the proposed framework were measured using packet loss, average packet delay, and varying densities of nodes that are malicious. In presence of malicious nodes, the proposed framework resulted in better performance compared to the basic routing protocol. Mahaboob John [16] proposed a regional mobility energy approximation-based secured routing algorithm to address the inadequacy of QoS performance in MANET for real-time applications. The RRME (real-time regional mobility and energy) estimation routing method divides the complete network into regions, with each node performing approximations in a neighbor selection based on various features such as mobility and energy. As a result, the method computed the QoS, which was a support factor for any route by calculating the data forwarding support, throughput support, and lifetime maximization support (LMS) (QoSSF). Based on the QoSSF value, an individual path has been chosen to conduct routing that maximizes QoS in MANET. Mariappan Rajashanthi [17] developed a secure multipath routing protocol with an encryption technique and optimal fuzzy logic. The proposed framework was dependent on the quality of service which provided a reliable communication of data. grey wolf optimization's adaptive formation approach envisioned the optimal path. Hence, an optimal path was considered from the known routes to protect the techniques of data key management; in this case, the homomorphic encryption method was used. The performance metrics of the proposed framework were EED, PDR, etc. The proposed energy efficient framework resulted in better simulation results along with the network lifetime compared to the existing state-of-the-art methods. Future work can be focused on the communication delay and improve the QoS which is a limitation of this work. Nahid Ebrahimi Majd [18] developed and approach of analysing reactive and pro-active classes which were optimized routing protocols in MANETS. Analysing the effect of various parameters on the performance of the network and its variations were researched in this paper. The reactive classes compared were dynamic source routing (DSR) and ad hoc on-demand distance vector (AODV) and proactive classes compared were destination sequenced distance vector (DSDV) and optimized link state routing (OSLR). The results have shown that OSLR has outperformed in terms of throughput, PDR, EED, and consumed energy. However, OSLR is not suitable for sensor network which is a major drawback of using this algorithm. The future plans of this research were to propose a hybrid protocol with high lifetime of the network. Sreenivasulu Ummadisetty [19] proposed a modified moth flame optimization algorithm which was employed in automatic identification of atrial fibrillation (AF). The proposed approach was deployed for detecting AF in short electrocardiogram (ECG) recordings. Other techniques such as heart rate variability (HRV) and frequency analysis were acquired for extracting features. The obtained results have shown that the HRV technique is efficient for detecting AF from short ECG recordings. The proposed MMFO has a drawback of local optima entrapping, low population diversity, and imbalance between exploitation and exploration phases. The future work of this research is to perform cascading classification to check the performance of the system. N. D. S. S. Kiran Relang [20] proposed an enhanced whale optimization (EWO) algorithm for the classification of ground water quality by considering the real time Indian water quality database. An AlexNet model and KNN were used in classification of optimal features. The proposed optimization algorithm has achieved greater classification results compared to the existing systems. Other databases with large amount of data samples would check the robustness of the classification model, which is a drawback for this work. To further improve the groundwater quality classification, a deep learning based ensemble models can be implemented.

The recent optimization techniques such as grey wolf optimization's (GWO) [17], modified moth flame optimization algorithm (MMFO) [19], and enhanced whale optimization (EWO) [20]. GWO reduces time consuming tasks and reduces operational time for high dimensional data. MMFO is used to solve local optima problem. EWO is used in solving constrained and unconstrained optimizations problem. However, the discussed algorithms such as GWO, MMFO, and EWO was not suited to solve the problems related to trust and security issues in MANETs.

From the observations, the limitations of existing

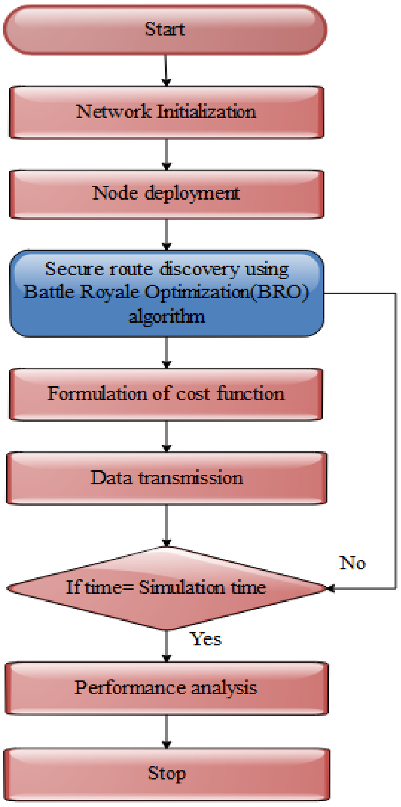

Figure. 1 Flowchart of the proposed MANET model

researches has shown that the lack of finding optimal route, high energy consumption, has decreased the robustness of the network. To overcome this a T-MOBRO method is introduced which enhances and improves robustness of the network by considering multi-objectives.

3. Methodology

In this research, the discovery of routing protocol using the trust based battle royale optimization(T-MOBRO) algorithm is developed for achieving trusted reliable transmission over the MANET, which is shown as a flowchart in Fig. 1. The generation of an energy-efficient trusted route is utilized in mitigating malicious nodes over the network which can also be used to enhance the packet delivery of the network. The BRO algorithm is a last-man-standing gameplay that is inspired by the Japanese film battle royale and the subgenre of the battle royale video game.

3.1 Mobile ad hoc network model

A secure data transmission route path is chosen from the source node (transmitter) to the destination node (receiver) in MANET. To maintain the connectivity of the network, the model measures optimized power even if the nodes' mobility is random. Let $G = (U, V)$ be the graph in MANET with a set of nodes $U = \{u_1, u_2, \dots, u_j, \dots, u_m\}$ where m is the total no. of nodes in MANET. V represents the link set that connects two mobile nodes and is given by $\{v_1, v_2, \dots, v_j, \dots, v_m\}$, where $1 \leq j \leq r \leq m$, and $1 \leq j \leq m$ respectively. Excess energy is required for each node in the model to transmit data from nodes. The distance is considered to be the primary factor in data transmission from the source to the destination node.

3.2 Battle royale optimization (BRO) algorithm

Some video game adaptations of the battle royale genre have players jump out of an aeroplane and land on the map via parachute. Additionally, BRO begins with a random population that is evenly distributed across the problem space, just like other swarm-based algorithms. Next, each person (soldier/player) fires a weapon at the soldier who is closest to them in an attempt to injure them. Therefore, soldiers in better positions harm their closest neighbors. Its damage level rises by one when a soldier is injured by another [21]. The proposed algorithm is diagrammatically represented in Fig. 2.

These interactions are mathematically calculated as $x_i.damage = x_i.damage + 1$ where x_i is the damage level of ith soldiers in the overall population. The $x_i.damage$ can be set to zero if the damaged soldiers can cause harm to their opponents in the next iteration. Additionally, soldiers want to switch positions as soon as they take damage to attack enemies from a different angle. As a result, to concentrate on exploitation, the damaged solder moves in the direction of a position midway between its previous location and the best position (elite) thus far. These interactions are calculated as shown in Eq. (1):

$$x_{dam,d} = x_{dam,d} + r(x_{best,d} - x_{dam,d}) \qquad (1)$$

Where r is a random number from the range [0,1] and $x_{dam,d}$ is the damaged soldier’s position in d(dimension). If a soldier's damage level rises above a predetermined threshold, to concentrate on exploration, the soldier dies, respawns at random from the feasible problem space, and $x_i.damage$ is again set to value zero. We found that a threshold value of 3 was suitable after much trial and error. This action prevents hasty convergence and offers better exploration. The soldier returning to the trouble spot after being killed looks like this:

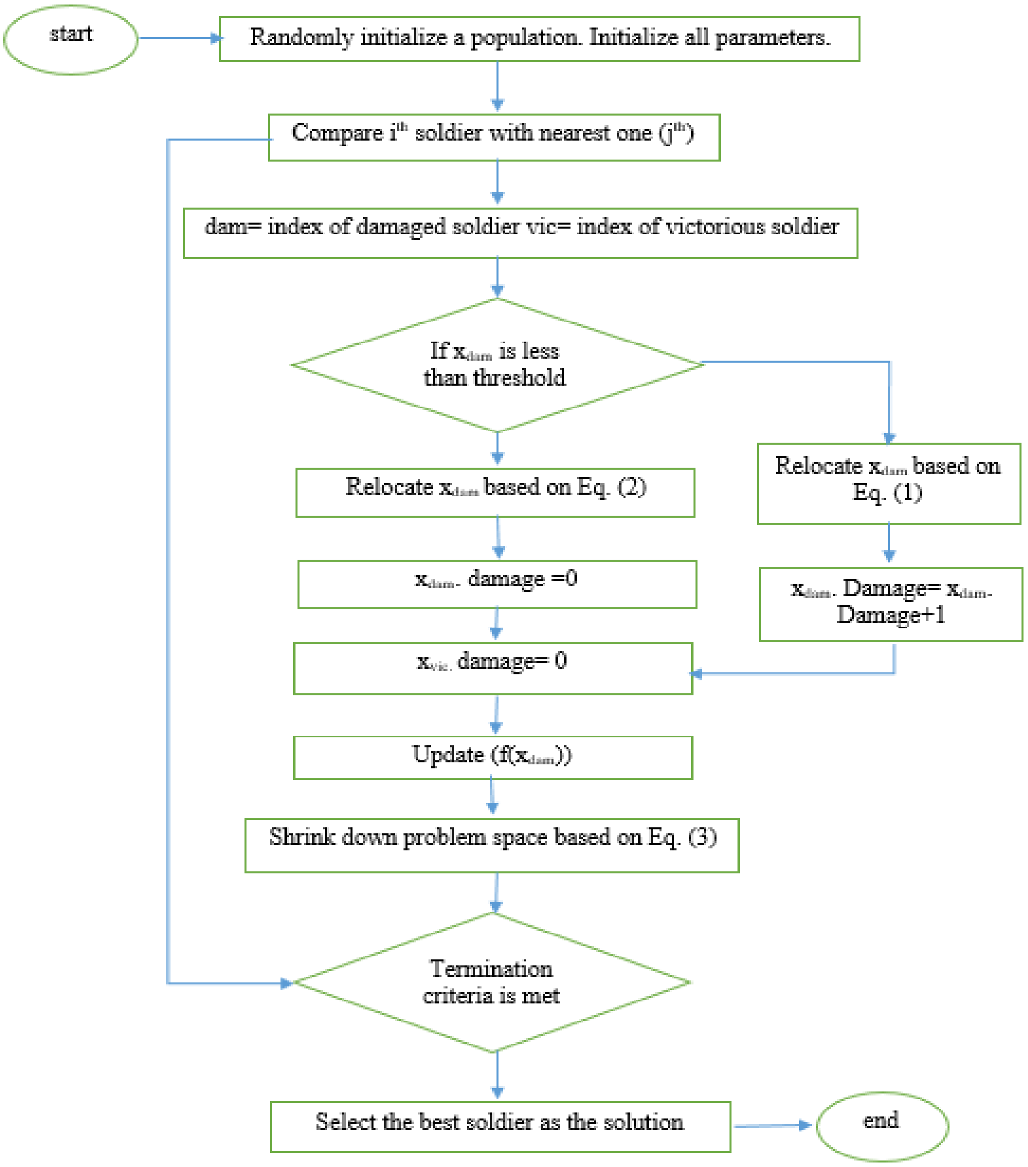
start
Randomly initialize a population. Initialize all parameters.
Compare ith soldier with nearest one (jth)
dam= index of damaged soldier vic= index of victorious soldier
If xdam is less than threshold
Relocate xdam based on Eq. (1)
Relocate xdam based on Eq. (2)
xdam. damage =0
xdam. Damage= xdam. Damage+1
xvic. damage= 0
Update (f(xdam))
Shrink down problem space based on Eq. (3)
Termination criteria is met
Select the best soldier as the solution
end

Figure. 2 Flowchart of battle royale optimization

$$x_{dam,d} = r(ub_d - lb_d) + lb_d \qquad (2)$$

Where, ub_d *and* lb_d are upper and lower bounds of d dimensions in the problem spot. Additionally, in each Δ iteration, the problems attainable search space starts to contract in the direction of the ideal resolution. The initial value was $\Delta = \log_{10}(MaxCircle)$ but it later changed to $\Delta = \Delta + round(\frac{\Delta}{2})$. The maximum number of generations, in this case, is MaxCircle. Exploration and exploitation are both aided by this interaction. The lower/upper boundary will therefore be changed as shown in Eqs. (3) and (4)

$$lb_d = x_{best,d} - SD(\overline{x_d}) \qquad (3)$$

$$ub_d = x_{best,d} + SD(\overline{x_d}) \qquad (4)$$

The standard deviation (SD) of the overall population in the d dimension is represented in this equation by $SD(\overline{x_d})$ and the best solution so far is represented by $x_{best,d}$. As a result, the lb_d/ub_d sets to the original lb_d/ub_d if it surpasses the original lower and upper bound. Additionally, to emphasize elitism, the top player or soldier from every iteration is retained and regarded as elite. Aside from the problem's dimensional area, the proposed approach's computational complexity is also influenced by the overall population and maximum allowed iterations. Considering the total size of the overall population as n, the computing complexity of overall solutions is $O(n^2)$ because every solution should be compared to all others to calculate its distance from all other solutions. Therefore, the computational complexity of BRO is $O(n^3)$ given the number of iterations.

3.3 Energy consumption

One of the most crucial trust metrics is energy because it is the main source of life for the sensor node. Mobile sensor nodes face energy efficiency issues in the network as sensor nodes move at different speeds. A node with insufficient energy backup cannot function effectively in the network, and the network's performance may suffer as a result. A node with no energy backup is denoted by value 0, and a node with full energy backup is denoted by value 1. Consequently, the range of values intended for energy backup is 0 to 1. Clustering manages energy consumption in the network effectively. Mathematically, the energy consumption of a node N_i at Δt time interval is given by:

$$Energy_{consumed}(N_i, \Delta t) = Energy_{res}(N_i, t_0) - Energy_{res}(N_i, t_1) \quad (5)$$

Where $Energy_{res}$ is the residual energy of node N_i at time intervals t_0 and t_1

3.4 Trust model of BRO (T-MOBRO)

Trust is a factor that promotes secure and healthy communication in MANET by preventing malicious nodes to communicate in the network to avoid miscommunication. As a result, the network's transmission and reception are started based on the trust level of each node after the trust of all nodes is measured and analysed. In the developed routing model, the trust model offers security. To assess the collection of trusted nodes, each node trust factor is estimated. The nodes trust value is determined when the transmission range is less distant from the neighbour node. A distance-based RSSI is measured as shown in Eq. (6). The trust value can be determined using Eq. (7) which evaluates direct and indirect trust.

$$Dist_{s,i} = RSSI(N, G_i) \quad (6)$$

Where, N= number of nodes,

$Dist_{s,i}$ is the received signal strength between the nodes of sender node S along with the present neighbor node i.

G_i is the ith node in the graph

$$Trust_{xy}(i) = \omega Trust_{xy}^{DT}(i) + \gamma Trust_{xy}^{IDT}(i) \quad (7)$$

Where, $Trust_{xy}^{DT}(i)$ i is the fundamental trust among the degree for the currently present node and a time i. $Trust_{xy}^{IDT}(i)$, i is the indirect trust that is present to some extent for the neighboring nodes that are present and determined at time ω, i and γ with the fitness factor falling between 0 and 1. so that the $\omega + \gamma = 1$. Some of the direct trust must be considered while calculating a node's degree of trust based on packets received as shown in Eq. 8

$$Trust_{xy}^{DT}(i) = T_{xy}^{RX}(i) + T_{xy}^{SD}(i) \quad (8)$$

Here, $T_{xy}^{RX}(i)$ be the no. of received packets with the use of node x at the time i. The total no. of packets sent by the nodes with the use of y at the time i is represented by $T_{xy}^{SD}(i)$. The transmission of packets in the nearby nodes serves as the basis for the indirect trust degree, which can be defined as shown in Eq. (9):

$$Trust_{xy}^{IDT}(i) = \left(\frac{1}{N_d}\right) * \sum_{d=1}^{N_d} Trust_{dy}^{DT}(i) \quad (9)$$

Where $Trust_{dy}^{DT}(i)$ be the degree of trust that exists for existing works in the nearby neighborhoods at the time i. The N_d represent the neighboring nodes' representational numbers. These factors can raise the level of trust for the detection of malicious nodes that have higher trust values for sending packets with full trust. The detection of malicious nodes determines the trust level in some fundamental ways. With the trust values in the packet transmission, the nodes may have a wider choice. As a result, each iteration is the basis for a model's update.

$$Trust_{xy}^{*}(i+1) = \alpha * Trust_{xy}(i) + (1-\alpha) * Trust_{xy}(i+1) \quad (10)$$

where $Trust_{xy}^{*}(i+1)$ be the degree of trust for the standard measure for a time $i + 1$ and α be the fitness factor that denotes the balanced in the standard measure for the present and previous iterations, with the value the specifically in the range of 0$< \alpha < 1$.

3.5 Formulation of the fitness function

The main goal is to create a set of multiple-layer energy metrics by creating a novel combined energy metric based on the metrics described above and incorporating it into our fitness function. For each metric from the source node N_0 to destination node N_K, a k-hop Path $P = N_0, N_1, \ldots, N_K$ is considered. The above metrics are used to calculate the energy and cost of a node, where each metric is provided with a weight value to adjust the impact of each routing metric, as shown in the Eq. (11). A node's energy fitness function is a single function formed by combining the weighted metrics, and it aims to minimize the weighted sum:

$$C_n(i) = \alpha_1 \left(\frac{P_{T(i)}}{P_{Tmax}} + \frac{P_{R(i)}}{P_{Rmax}}\right) + \alpha_2 \frac{N}{N_{max}} + \alpha_3 \left(1 - \frac{E_{R(i)}}{E_0}\right), \quad (11)$$

$$\begin{cases} \sum_{\mathrm{i}=0}^{3} \alpha_{\mathrm{i}} = 1, \\ 0 \leq \alpha_{\mathrm{i}} \leq 1. \end{cases} \quad (12)$$

Where, $P_{T(i)}$=Tx power of node N_i,
P_{Tmax}= maximum Tx power,
$P_{R(i)}$=Rx power by node N_i,
P_{Rmax}=Maximum Rx power
N=Node Connectivity Index of node N_i,
N_{max}=Number of nodes in the network minus one
$E_{R(i)}$ =Remaining energy capacity of node N_i, E_0= energy capacity of node N_i initially

This method's fundamental goal is to maximize energy efficiency by choosing the smallest Tx and Rx power, node connectivity index, and consumed energy, which is nothing more than the maximum amount of available energy:

$$\frac{E_{cons}(i)}{E_0} = \frac{E_0 - E_r(i)}{E_0} = 1 - \frac{E_r(i)}{E_0} \quad (13)$$

Where, $E_{cons}(i)$ =Consumed energy by node N_i
E_0=energy capacity initially for node N_i, $E_r(i)$= Remaining energy capacity of the node N_i

The optimization metric is the path cost from source to destination nodes. The objective is to find the path that has the lowest total cost. The energy cost function which is represented in Eq. (11) for the new node is used to calculate the path costs between each source to destination nodes. Eq. (14) is the fitness function of this work.

$$Cp(P_i) = \sum_{i=0}^{n} C_n(i) \quad (14)$$

Where $Cp(P_i)$ is the cost of the path (P_i), $C_n(i)$ is the energy cost of the node N_i, n represents a number of nodes in the path.

3.6 Packet forwarding rate (PFR)

By taking into account the packet flow, the PFR is designed to analyze the node's nature. All packets that are meant to be forwarded must be forwarded by a normal node. However, there are instances where the malicious nodes fail to perform the routing task, which causes a serious problem. When a node expresses an interest in forwarding packets, that node can be regarded as reliable. Therefore, it is always best to pick a route with lots of reliable nodes. The packet inflow and outflow are considered when calculating the PDR. Let's say that α and, β respectively, represent the inflow and the outflow. The following condition from Eq. (15) is met by a normal node:

Table 1. Simulation parameters

Parameters	Values
No. of nodes	10 - 50
Initial energy	0.5J
Area size	$1000m \times 1000m$
Range of transmission	$50m$
Packet size	512 bytes
Mobility model	Random waypoint movement

$$\alpha = \beta \quad (15)$$

Assume that the node doesn't show any interest in forwarding packets when its packet outflow is less than half of its packet inflow, or a little plus or minus. The following condition can be used to indicate this:

$$\alpha = \frac{\beta}{2} \quad (16)$$

The node is completely unreliable and unfit to be a part of the network when the β rate is less than half of α. These types of nodes are taken into account when choosing the route, making data routing risk-free and secure. As a result, PFR is yet another crucial node trust metric that can help to improve route reliability.

4. Experimental results

The outcomes of the proposed T-MOBRO method are shown and explained in this section. The implementation and simulation of T-MOBRO method are done in MATLAB R2020a. The T-MOBRO method is used to improve the efficient energy in MANET. The network is initialized with 50 nodes and initial energy of 0.5J are deployed in the area of $1000m \times 1000m$. The range of transmission is $50m$. Table 1 provides the simulation parameters considered while analyzing the T-MOBRO method.

4.1 Performance analysis

The performance of the trust battle royale optimization (T-MOBRO) method is evaluated by using PDR, throughput, EED and energy consumption. The performances are analyzed with conventional optimization namely trust-based secure

Table 2. Comparison of PDR

	PDR (%)				
Number of nodes	TSEAC [12]	ETRS [13]	MMFO [19]	EWO [20]	T-MOBRO
10	90.24	50.00	85.33	82.34	48.49
20	85.45	55.00	80.73	80.23	46.78
30	72.63	65.00	75.52	76.46	44.26
40	65.75	75.00	68.74	74.34	41.63
50	60.93	75.00	64.32	72.55	38.29

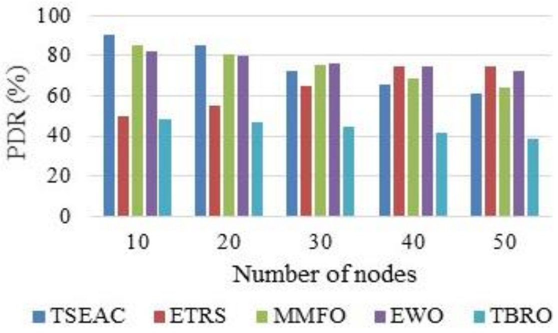

Figure. 3 Analysis of packet delivery ratio

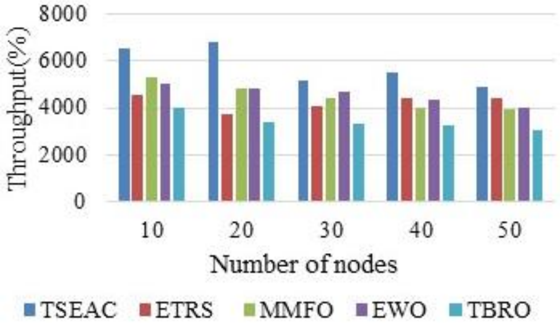

Figure. 4 Analysis of throughput

energy-aware clustering (TSEAC) and efficient trust based routing scheme (ETRS) which provides its energy-efficient routing. The results are analyzed by varying the no. of nodes that exist in the network. The comparative analysis of the T-MOBRO is provided in this section where existing researches such as TSEAC [12] and ETRS [13] is used to perform the comparison. Further, the recent optimization techniques such as MMFO [19], and EWO [20] are developed for performing trust based routing in MANETs to evaluate the performance of T-MOBRO. The aforementioned approaches are implemented with the same specifications as shown in Table 2.

The graphical comparison of PDR, Throughput, EED, and Energy consumption is shown in Figs. 3, 4, 5, and 6. The trust-based energy efficient secure optimal route is implemented to increase the robustness of the network. The energy efficiency is improved along with secure routing with the proposed optimization technique by implementing the T-MOBRO algorithm within the MANET which is the main issue addressed in the literature review section.

4.1.1. Packet delivery ratio

The packet delivery ratio is calculated by dividing the number of packets received at the destination by the number of packets sent by the transmitter node. The comparison of PDR for T-MOBRO with TSEAC [12], ETRS [13], MMFO [19], EWO [20], and T-MOBRO is shown in Table 2 and represented in Fig 3. Fig. 3 shows that the T-MOBRO achieves better PDR than both the methods. For example, the PDR of the T-MOBRO with 10 nodes is 48.49% which is high when compared to the other models. The mitigation of malicious attacks using T-MOBRO is used to avoid data loss while broadcasting the data packets.

4.1.2. Throughput

Throughput is the no. of packets that are successfully received at the destination over the MANET. The comparison of throughput for T-MOBRO with TSEAC [12], ETRS [13], MMFO [19], EWO [20], and T-MOBRO is shown in table 3 and represented in Fig 4. Fig. 4 shows that the T-MOBRO has higher throughput when compared to the all methods. For example, the throughput of the T-MOBRO for 10 nodes is 4032.29 bits/sec which is high when compared to the both the methods. The throughput of T-MOBRO is increased because of avoiding malicious attacks on the route. The development of trust based energy-efficient route over the MANET increases the robustness against malicious attacks that helps to improve the data delivery.

4.1.3. End to end delay

EED is defined as the time taken for packet transmission from the source to the destination. The comparison of EED for T-MOBRO with TSEAC [12], ETRS [13], MMFO [19], EWO [20], and T-MOBRO is shown in Table 3 and represented in Fig. 4 is shown in Table 4 and represented in Fig 5. Fig. 5 shows that the T-MOBRO achieves less EED than all the methods. For example, the EED of the T-MOBRO with 10 nodes is 0.0070S which is less when compared to the other methods. The EED of T-MOBRO is minimized by identifying the path with lesser delay and less transmission distance. Further, the formulated cost function of T-MOBRO is used to

Table 3. Comparison of throughput(bits/sec)

Number of nodes	**Throughput (bits/sec)**				
	TSEAC [12]	**ETRS [13]**	**MMFO [19]**	**EWO [20]**	**T-MOBRO**
10	6560.00	4553.18	5325.26	5034.24	4032.29
20	6800.00	3766.93	4847.34	4839.57	3423.45
30	5160.00	4097.06	4432.36	4677.65	3346.23
40	5520.00	4389.55	4032.17	4338.54	3273.06
50	4860.00	4388.43	3924.32	4033.34	3045.32

Table 4. Comparison of EED

Number of nodes	**EED(Sec)**				
	TSEAC [12]	**ETRS [13]**	**MMFO [19]**	**EWO [20]**	**T-MOBRO**
10	0.29	0.0073	0.0245	0.0372	0.0070
20	0.21	0.0120	0.0226	0.0350	0.0116
30	0.25	0.0115	0.0189	0.0329	0.0102
40	0.22	0.0097	0.0148	0.0298	0.0081
50	0.21	0.0076	0.0125	0.0240	0.0065

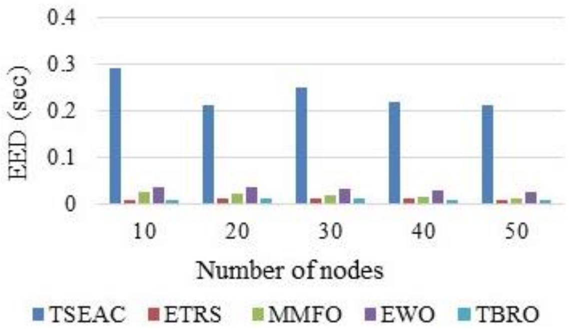

Figure. 5 Analysis of EED

Table 5. Comparison of energy consumption

Number of nodes	**Energy consumption(Joules)**				
	TSEAC [12]	**ETRS [13]**	**MMFO [19]**	**EWO [20]**	**T-MOBRO**
10	2.1	3.2	3.8	3.4	1.7
20	2.9	3.6	4.2	3.7	2.5
30	4	3.9	4.6	3.9	3
40	4.5	4.3	5.1	4.1	4
50	5	4.8	5.4	4.3	4.5

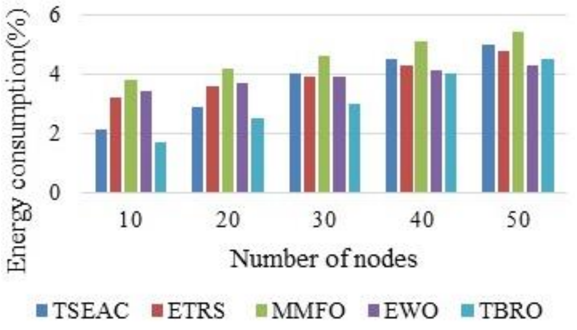

Figure. 6 Analysis of energy consumption

minimize the routing overhead that is further used to minimize the EED.

4.1.4. Energy consumption

Table 5 depict the analysis of the consumption of energy for the proposed T-MOBRO algorithm with existing methods such as TSEAC [12], ETR [13], MMFO [19], EWO [20] for various numbers of nodes considered. Fig. 6 shows that the proposed T-MOBRO consumed less energy compared to all other methods. For example, the energy consumption by T-MOBRO method with 10 nodes is 1.7J which is less when compared to the TSEAC.

5. Conclusion

In this research, the trust based route discovery is performed using the T-MOBRO method. The trust based battle royale optimization algorithm is optimized by using a trust, EED, energy, and distance. The trust value incorporated in the T-MOBRO is used to avoid malicious attacks during route generation. In route discovery, the node failure is avoided using the residual energy whereas the distance and EED are used to identify the route with less distance. The shortest path generation and lesser routing overhead are used to minimize the delay while transmitting the data in MANET. From the results, it is concluded that the T-MOBRO method achieves better performance than the TSEAC, ETRS, MMFO, and EWO. The PDR of the T-MOBRO method for 10 nodes is 48.49% which is high when compared to the TSEAC. The throughput of T-MOBRO method is 4032.29 which is less compared to other methods. End to end delay of the proposed T-MOBRO method is 0.0070seconds which is less compared to the other methods at node 10. Energy consumption achieved at node 10 with the T-MOBRO technique is 1.7J which is less compared to the existing technique. The main aim of this work is to establish a trust based routing protocol. Future research can be focused on establishing a secure routing protocol in MANET by using the proposed optimization method by detecting and mitigating malicious attacks.

Notation table

Parameters	Representation
U	Set of nodes
V	Link set of nodes
m	Total number of nodes
$x_i.damage$	Damage level of ith soldier
$x_{dam,d}$	damaged soldier's position in dimension d
r	random number
ub_d	Upper bounds of dimension d
lb_d	lower bounds of dimension d
$x_{best,d}$	best solution in dimension d
$SD(\overline{x_d})$	Standard Deviation of the overall population in the d dimension
$O(n^3)$	computational complexity overall population
$Energy_{consumed}(N_i, \Delta t)$	residual energy of node N_i at time intervals Δt
$Trust_{xy}^{DT}(i)$	Direct trust of ith node with the use of x and y nodes
$Trust_{xy}^{IDT}(i)$	Indirect trust of ith node with the use of x and y nodes
ω	Time constant
γ	fitness factor
$T_{xy}^{RX}(i)$	Degree of trust from receiver side at time i with the use of x and y nodes
$T_{xy}^{SD}(i)$	Degree of trust from sender side at time i with the use of x and y nodes
$Cp(P_i)$	cost of the path (P_i)

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper background work, conceptualization, methodology, dataset collection, implementation, result analysis and comparison, preparing and editing draft, visualization have been done by first author.

The supervision, review of work and project administration, has been done by second author.

References

[1] V. V. Sarbhukan and L. Ragha, "Establishing secure routing path using trust to enhance security in MANET", *Wireless Personal Communications*, Vol. 110, No. 1, pp. 245-255, 2020.

[2] G. C. Krishnan, A. H. Nishan, S. Gomathi, and G. A. Swaminathan, "Energy and trust management framework for MANET using clustering algorithm", *Wireless Personal Communications*, Vol. 122, No. 2, pp. 1267-1281, 2022.

[3] T. A. N. Abdali, R. Hassan, R. C. Muniyandi, A. H. M. Aman, Q. N. Nguyen, and A. S. A. Khaleefa, "Optimized particle swarm optimization algorithm for the realization of an enhanced energy-aware location-aided routing protocol in MANET", *Information*, Vol. 11, No. 11, p. 529, 2020.

[4] K. Sudhakar, N. Sengottaiyan, and S. Anbukaruppusamy, "A hybrid swarm intelligent framework to support efficient military communication in MANET", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 12, No. 5, pp. 5215-5223, 2021.

[5] K. Ourouss, N. Naja, and A. Jamali, "Defending against smart grayhole attack within MANETs: A reputation-based ant colony optimization approach for secure route discovery in DSR protocol", *Wireless Personal Communications*, Vol. 116, No. 1, pp. 207-226, 2021.

[6] M. Thebiga and S. R. Pramila, "Adaptable and energy efficacious routing using modified emperor penguin colony optimization multi-faceted metaheuristics algorithm for MANETS", *Wireless Personal Communications*, Vol. 118, No. 2, pp. 1245-1270, 2021.

[7] N. Veeraiah and B. T. Krishna, "An approach for optimal-secure multi-path routing and intrusion detection in MANET", *Evolutionary Intelligence*, Vol. 15, No. 2, pp. 1313-1327.

[8] B. K. Tripathy, S. K. Jena, P. Bera, and S. Das, S, "An adaptive secure and efficient routing protocol for mobile ad hoc networks", *Wireless Personal Communications*, Vol. 114, No. 2, pp. 1339-1370, 2020.

[9] K. Karthick and R. Asokan, "Mobility aware quality enhanced cluster based routing protocol for mobile ad-hoc networks using hybrid optimization algorithm", *Wireless Personal Communications*, Vol. 119, No. 4, pp. 3063-3087, 2021.

[10] B. Devika and P. N. Sudha, "Power optimization in MANET using topology management", *Engineering Science and Technology, an International Journal*, Vol. 23, No. 3, pp. 565-575, 2020.

[11] P. Sathyaraj and R. D. Devi, "Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method", *Journal of Ambient*

Intelligence and Humanized Computing, Vol. 12, No. 7, pp. 6987-6995, 2021.

[12] A. R. Rajeswari, S. Ganapathy, K. Kulothungan, and A. Kannan, "An efficient trust-based secure energy-aware clustering to mitigate trust distortion attack in mobile ad-hoc network", *Concurrency and Computation: Practice and Experience*, Vol. 33, No. 13, p. e6223, 2021.

[13] A. A. Mahamune and M. M. Chandane, "An Efficient Trust-Based Routing Scheme Against Malicious Communication in MANET", *International Journal of Wireless Information Networks*, Vol. 28, No. 3, pp. 344-361, 2021.

[14] M. S. Usha and K. C. Ravishankar, "Implementation of trust-based novel approach for security enhancements in MANETs", *SN Computer Science*, Vol. 2, No. 4, p. 257, 2021.

[15] G. K. Wadhwani, S. K. Khatri, and S. K. Mutto, "Trust framework for attack resilience in MANET using AODV", *Journal of Discrete Mathematical Sciences and Cryptography*, Vol. 23, No. 1, pp. 209-220, 2020.

[16] Y. M. M. John and G. Ravi, "Retracted: Real time regional mobility energy feature approximation-based secure routing for improved quality of service in MANET", *International Journal of Communication Systems*, Vol. 35, No. 16, p. e4713, 2022.

[17] M. Rajashanthi and K. Valarmathi, "A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs", *Wireless Personal Communications*, Vol. 112, No. 1, pp. 75-90, 2020.

[18] N. E. Majd, N. Ho, T. Nguyen, and J. Stolmeier, "Evaluation of parameters affecting the performance of routing protocols in mobile ad hoc networks (MANETs) with a focus on energy efficiency", In: *K. Arai, and R. Bhatia (eds), Advances in Information and Communication: Proceedings of the 2019 Future of Information and Communication Conference (FICC)*, San Francisco, USA, Vol. 2, pp. 1210-1219, 2020, Springer Cham.

[19] S. Ummadisetty and M. Tatineni, "Automatic Atrial Fibrillation Detection Using Modified Moth Flame Optimization Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 1, pp. 435-445, 2023, doi: 10.22266/ijies2023.0228.38.

[20] N. D. S. S. K. Relangi, A. Chaparala, and R. Sajja, "Effective Groundwater Quality Classification Using Enhanced Whale Optimization Algorithm with Ensemble Classifier", *International Journal of Intelligent Engineering and Systems*, Vol. 16, No. 1, pp. 214-223, 2023, doi: 10.22266/ijies2023.0228.19.

[21] T. R. Farshi, "Battle royale optimization algorithm", *Neural Computing and Applications*, Vol. 33, No. 4, pp. 1139-1157, 2021.

[22] K. S. Shivakumar and V. C. Patil, "An optimal energy efficient cross-layer routing in MANETs", *Sustainable Computing: Informatics and Systems*, Vol. 28, p. 100458, 2020.