Received: December 13, 2022. Revised: February 28, 2023. 532

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

A Secure and Energy Efficient Cluster Based Routing Using Energy and Trust Aware - Multi Objective African Vultures Optimization for MANET

Shalini Sharma[1]* **Syed Zeeshan Hussain[1]**

[1]*Department of Computer Science, Jamia Millia Islamia University New Delhi, India*
* Corresponding author's Email: shalinisharma1980@gmail.com

Abstract: A mobile Ad Hoc network (MANET) is a dynamic wireless network developed using wireless nodes without using any infrastructures. The wireless nature of mobile networks causes several challenges in secured communication which makes it susceptible to malicious attacks. Therefore, security is a very essential factor in facilitating a secured message transmission among mobile nodes in the wireless medium. The energy and trust aware - multi objective african vultures optimization (ETA-MAVO) method is used in this paper to provide high security for the data packets, thereby preventing malicious attacks. Using the ETA-MAVO algorithm, the network nodes' energy efficiency and trust value are calculated. For choosing the best cluster heads (CHs), ETA-MAVO considers fitness functions, namely: trust value, energy ratio, communication cost, the total number of gateway hops, and network load. To discover malicious nodes in the network and minimize packet loss, the trust value of a node is calculated from its neighbours. Because of trust value, updating routing information is simpler and increases network throughput. The results obtained from the simulation show that the proposed ETA-MAVO achieved better performance with respect to parameters such as delay, energy consumption, throughput, and detection rate when compared with the existing cat slap single-play algorithm (C-SSA) and data-driven zone based routing protocol (DD-ZRP), angular based energy proficient trusted routing (ACEPTR) protocol and aquila optimizer (AO) and puzzle optimization algorithm (POA). The proposed method achieved a detection rate of 93% while the existing C-SSA, DD-ZRP, ACEPTR, AO and POA achieved a detection rate of 90%, 68%, 72%, 91% and 90% respectively.

Keywords: Energy efficiency, Malicious nodes, Mobile Ad Hoc networks, Multi-objective african vulture optimization, Trust value.

1. Introduction

MANET is a collection of mobile nodes which establishes communication without using the fixed physical infrastructure. MANET has different prominent characteristics such as rapid setup, varying topology, and multi-hop wireless communication. [1]. The collection of nodes present in the MANET creates a cluster that has the ability to move on any route. The nodes present in the MANET form dynamic networks without utilizing the network infrastructures. The nodes of MANET consist of wireless interfaces which use radio channels to perform communication with each other without the help of a centralized management [2, 3]. Moreover, the communication nodes present in the MANET track the nodes in the intermediate stage and generate a communication channel [4]. The nodes present in MANET are collected randomly and they can travel at any speed in any direction. Moreover, the MANET consists of execution limits which are combined along with multi-hop correspondence [5]. The nodes which are in a particular range can communicate with each other immediately whereas the nodes at a farther range require an intermediate node to perform communication. There is a need for intermediate nodes to deliver the packets from the node at the source to the node at the destination. So, the nodes in the MANET should cooperate between them to perform multi-hop communications [6, 7]. The application of MANET is widely utilized in the fields of military-related operations, meetings or

conferences, as well as for search and rescue operations [8].

The security provided by the MANET mainly depends on the existence of a reliable layer for communication. However, the mobility of the nodes in MANET changes since it is dynamic and highly vulnerable to attacks [9, 10]. Changing and discharging the batteries requires more time and prevents the MANET from providing energy efficiency, as it causes energy constraints and reduces the packet delivery ratio at the node of the destination [11]. Clustering is considered one of the significant processes in maintaining route stability in networks. The cluster head functions present in the clustering-based frameworks offer secure communication in inter and intra-cluster routing [12]. In cluster-based routing, the sensor nodes are categorized into groups known as clusters. There are cluster heads present in each cluster that collect data from the sensor nodes, process it, and then send it to the receiver node. Lightweight key management algorithms are needed for the cluster head to manage the group's cluster members [13, 14]. Various methods of conventional mechanisms are used for this goal, but they suffer from increased computing complexity, network overhead, ineffective security, unreliability, and decreased network throughput [15]. To overcome these problems, this paper develops a secure clustering-based method to improve the efficiency of the MANET.

The main contributions of the paper are provided as follows:

1. A secure cluster head selection is achieved using ETA-MAVO, wherein it is optimized by using trust value, energy ratio, communication cost, the total number of gateway hops, and network load.
2. Moreover, a secure routing path is developed by using the ETA-MAVO based on the trust value, energy ratio and communication cost.
3. A secure and energy-efficient cluster-based routing is constructed for attaining reliable communication.

The remaining paper is organized as follows: section 2 represents the related works of the paper. The proposed method is discussed in section 3. The results and discussion are provided in section 4. Finally, section 5 presents the overall summary of the paper.

2. Related works

Srilakshmi [16] introduced a secure bacteria foraging optimization algorithm (BFOA) for routing in mobile Ad Hoc networks (MANET). The proposed algorithm was considered ideal for routing and offered trust basis protection and energy efficiency in MANET. The fuzzy clustering algorithm was initiated and CHs were chosen depending on the direct, indirect and recent trust in cluster heads. The proposed method consisted of a faster rate of convergence and it optimized the storage and limitations in connection of routes.

However, the indirect trust value utilized in this method lacked in providing the witness variable which helps in the security and authentication of the node.

Veeraiah [17] introduced a hybrid algorithm called the cat slap single-player algorithm (C-SSA) to address the lack of efficacy in energy and security on a trust based routing in MANET. The hybrid algorithm was able to enhance the routing. At first, the fuzzy clustering was set up and CHs were selected on basis of direct, indirect and recent trust. The proposed C-SSA optimization was utilized to perform significant leaps during the process of routing. However, the hybrid C-SSA algorithm faced difficulties in the process of route linking.

Merlin and Ravi [18] introduced a trust based energy aware routing (TEAR) mechanism for MANET. The TEAR mechanism mitigated the black hole by generating dynamic detection routes to identify the black hole quickly and offered better security by calculating the trust of the nodes. The TEAR mechanism utilized data routing protocol to select the trusted node from the set of candidate nodes near the sink. The TEAR mechanism was created by using the energy from non-hotspots to increase the efficiency and security of the data. However, the TEAR mechanism lacked in detecting the node's trust and reduced the probability of providing successful routing.

Rajashanthi and Valarmathi [19] introduced a multipath routing system in MANET which offered a better quality of service (QoS) along with the encryption technique. The multipath routing system utilized the grey wolf optimization method to select the optimal path for the data. The encryption system based on Homomorphism was utilized in recognizing routers to shelter the management of data keys and for security purposes. The level of energy consumption of the proposed routing system was very low when compared with other systems. However, there was a delay in the communication of nodes which lowered the overall performance of the system.

Chugh [20] introduced a new hybrid method known as Data Driven Zone-based Routing Protocol (DD-ZRP) for constraining resources present in the networks of MANET. The introduced DD-ZRP method was integrated along with schemes of

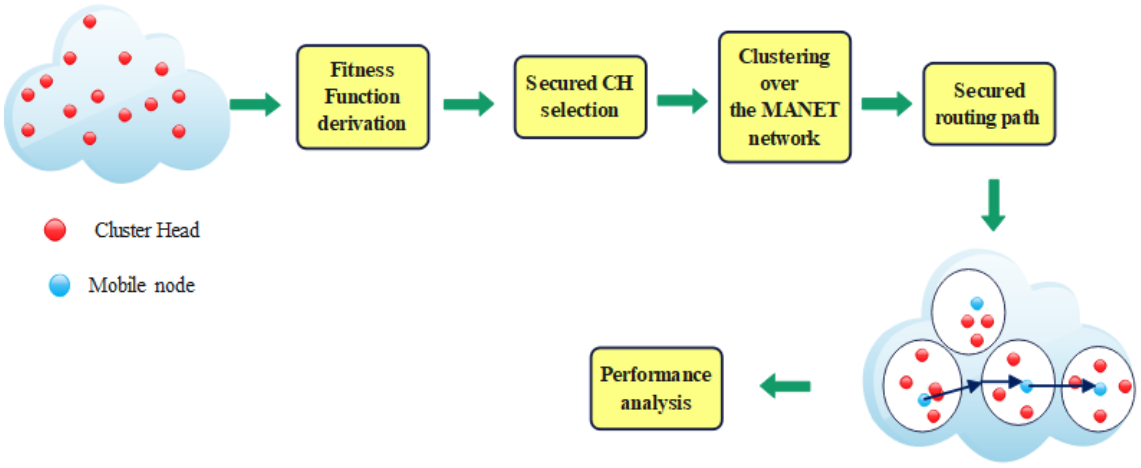

Figure. 1 Block diagram of ETA-MAVO method

anomaly detection for trust and energy awareness of MANET using network simulator 3. The resource-constrained key utilized in the DD-ZRP efficiently detected the outliers and built primitives to enhance the security of the system. The DD-ZRP had the ability to utilize past data and detect repeated intrusive activities. However, the DD-ZRP was not robust when unknown vulnerabilities were introduced into the system.

Thirunavukkarasu [21] introduced cluster and angular based energy proficient trusted routing (ACEPTR) protocol for MANET. In the initial stage, the node credit score (NCS) was computed to determine the nodes' trust ratio. Both Self-Trust computation and Joint-Trust computation were factors in the credit score calculation. ACEPTR protocol performed the process of conventional communication control which helped to detect the transmission range of nodes. However, the rapid increase of nodes presents in cluster affected the reliability of the system.

The recent optimization techniques such as Aquila Optimizer (AO) [22], Guided pelican algorithm (GPA) [23] and Puzzle Optimization Algorithm (POA) [24]. AO is based on optimal allocation of soft open points for multi-objective operation in Electric Vehicles (EV) integrated active distribution networks. GPA was utilized to optimize the networks by three stages such as selection of target, location replacement and use multi candidate to deal with real world optimization problems. The POA was introduced by Fatemeh Ahmadi Zeidabadi and Mohammad Dehghani which was based on simulation process of solving the puzzles and POA has no control parameters and it is not limited by any parameters. However, the discussed algorithms such as AO, GPA and POA was not suited to solve the problems related to multi-objective fitness functions.

3. ETA-MAVO method

In the ETA-MAVO method, trust based and energy-efficient routing is developed based on clustering to increase the life span of the network and the ratio of packet delivery. The positioning of sensors, selection of Secure Cluster Head (SCH), and generating the paths for clustering and routing, are all significant processes in the accomplishment of ETA-MAVO. The nodes which are noticed as malicious are neglected during the process of selecting SCH and routing is performed by evaluating the trust value present in nodes. The block diagram of the ETA-MAVO method is represented in Fig. 1.

3.1 Initializing the sensors

This stage is the foremost stage based on deploying the nodes of the sensors in the MANET. The selection of SCH and generation of routes utilizing the ETA-MAVO method is described in the following section.

3.1.1. Selection of SCH using ETA-MAVO

During this phase, the selection process of secure cluster heads is performed to make advancements in the security system of the network and to improve the energy efficiency of the network. The selection phase of SCH is mainly utilized in the process of avoidance of malicious nodes during the time of communication among the nodes.

The ETA-MAVO algorithm is developed from the behaviour of African vultures and they are generally categorized into two classes. The ETA-MAVO algorithm computes the fitness function of the individuals to categorize the eagles into classes. In ETA-MAVO algorithm, the following stages, which are performed to identify the best vulture in the

group, are being explained in the upcoming sections by calculating the starvation rate and the weakest one.

3.1.2. Determination of best vultures

At this stage, the fitness rate of the population of the individuals (vulture) is calculated. The vulture which has a high starvation rate and survives till last is considered the best vulture belonging to the first class and the second best one belongs to the second class. The remaining vultures join with the first and second class, as represented in Eq. (1).

$$R(i) = \begin{cases} best\ vulture_1, & if\ P_i = L_1 \\ best\ \ vulture_2, & if\ P_i = L_2 \end{cases} \quad (1)$$

Where $best\ vulture_1$ and $best\ \ vulture_2$ are denoted as the best vultures of the first and second class respectively. The probability of selection is denoted as P_i , the values between $[0, 1]$ are denoted as L_1 and L_2 and their sum is unity. The Roulette wheel is a method that is used to select the best vulture and it is represented by Eq. (2).

$$P_i = \frac{F_i}{\sum_{i=1}^{n} F_i} \quad (2)$$

Where the fitness value of i^{th} vulture in the search space is denoted as F_i and n is number of populations.

3.1.3. Finding starvation rate of vultures

When the vultures feel overfilled and have more energy, they go in search of food for a longer distance. But, when they feel hungry they can't fly for long distances during food search, therefore during the time of starvation, they become violent and this violent behavior is represented using Eq. (3) and Eq. (4)

$$t = h \times \left(sin^w \left(\frac{\pi}{2} \times \frac{iter}{iter_{max}} \right) + cos\left(\frac{\pi}{2} \times \frac{iter}{iter_{max}} \right) - 1 \right) \quad (3)$$

$$F = (2r_1 + 1) \times z \times \left(1 - \frac{iter}{iter_{max}} \right) \quad (4)$$

The satisfied status of the vulture is represented by F, the value of the current iteration, and the maximum iteration is represented by $iter$ and $iter_{max}$ respectively. The random number in the range [-1, 1] is denoted as h and the random number present in the range [-2, 2] is denoted as z. The random number between 0 and 1 is denoted as r_1. When the vulture is in starvation, the value of z becomes less than 0, and when the value of z increases the vulture becomes satisfied. By using Eq. (4), the transportation of AVO takes place from the phase of exploration until the phase of exploitation. On other hand, the performance of the optimizer to solve the problem is improved using Eq. (3). When the value of w gets increased, the exploration stage probability gets increased at the last stage and by decreasing the w, entry into the exploration phase also gets decreased. Moreover, when the F value becomes less than 1, the algorithm directly jumps to the phase of exploitation rather than going through the exploration phase.

3.1.4. Stage of exploration

The vultures have a highly sharp vision that helps them in identifying the food and have the prediction power to detect dying animals. The identification of food for a vulture is not an easy task, it needs to search in their surrounding for a long time and travel long distances in search of food. The vultures use their visual capability to detect the prey in various areas. Likewise, in the AVO algorithm the parameter P_1 is utilized to choose two strategies. The value of P_1 lies within 0 and 1. The selection of this strategy takes place by utilizing Eq. (5).

$$P_i(t+1) = \begin{cases} R(i) - |X - R(i) - P(i)| \times FP_1 \geq r_{P_1} \\ R(i) - F + r_2 \times \left((u_b - l_b) \times r_3 + l_b \right) P_1 < r_{P_1} \end{cases} \quad (5)$$

Where the best vulture is denoted as $R(i)$, The distance located by the vulture to save their food from others is denoted as X, and the random numbers present in the range [0, 1] are denoted as r_2 and r_3. The limits present in upper and lower limits are denoted as u_b and l_b respectively. When the value of r_3 becomes unity the capability to search various search areas gets increased.

3.1.5. Stage of exploitation

The exploitation phase is the final stage employed in AVO algorithm and there are two strategies followed in this phase, each strategy is selected based on two parameters known as P_2 and P_3.

The first strategy is implemented in the first stage using the parameter P_2 and the second strategy is implemented in the second stage using the parameter P_3. The exploitation phase at the first stage is taken into consideration whenever the value of F lies

between 0.5 and 1. When the value of F becomes greater or equals 0.5, the AVO algorithm executes the process of food competition. When more vultures aim for the same source of food, it leads to severe conflicts and struggles in attaining the food. During that time, the vultures having high capability and strength won't share their food source while the vultures with lower physical strength try to take away the food source from the capable vultures. The first phase takes place in the stage of exploitation which is represented in Eq. (6).

$$P_i(t+1) = \begin{cases} |X - R(i) - P(i)|(F + r_4) \\ \quad \ldots - \big(R(i) - P(i)\big)P_2 \geq r_{P_2} \\ R(i) - R(i) \times \left(\frac{P(i)}{2\pi}\right)(r_5 \times cos\big(P(i)\big) \\ \quad \ldots + r_6\ sin\big(P(i)\big)P_2 < r_{P_2} \end{cases} \quad (6)$$

In the above Eq. (6), the random numbers between the range $[0, 1]$ are represented as r_4, r_5, r_6. During the time of the second stage in the phase of exploitation, the travel of two vultures for the source of food is noticed by more vultures and conflicts start in order to gain that food. The second stage that takes place in the stage of exploitation is represented in Eq. (7).

$$P_i(t+1) = \begin{cases} 0.5 \left(\begin{matrix} best\ vulture_1(i) + best\ vulture_2(i) - \\ \left(\frac{best\ vulture_1(i) \times P_i}{best\ vulture_1(i) - P(i)^2} + \frac{best\ vulture_2(i) \times P_i}{2(i) - P(i)^2}\right) \times F \end{matrix} \right) P_3 \\ \geq r_{P_3} \\ R(i) - |R(i) - P(i)| \times F \times Levy\big(R(i) - P(i)\big)P_3 < r_{P_3} \end{cases} \quad (7)$$

In Eq. (7) the representation of the levy flight function is denoted as $Levy$. AVO algorithm has clearer procedures for the exploration and exploitation phases than other optimization systems. A balance between diversity and resonance is established in the AVO algorithm using the two most optimal solutions as a representation of the two groups of eagles that are more powerful than the rest and this process helps in improving the overall performance of the AVO algorithm. Additionally, the AVO algorithm carries out space searches using different mechanisms in the phases of exploration and exploitation. The AVO algorithm encounters low-level computational difficulties and is more flexible when compared with other algorithms, thereby signifying its power.

3.2 Multi-objective fitness function formulation for selection of CH

The fitness functions considered in ETA-MAVO for selecting the optimal CHs are trust value, energy ratio, communication cost, the total number of gateway hops, and network load. The fitness function is represented using the overall formula which is shown in Eq. (8).

$$F = \alpha_1 \times F_1 + \alpha_2 \times F_2 + \alpha_3 \times F_3 + \alpha_4 \times F_4 + \alpha_5 \times F_5 \quad (8)$$

In Eq. (8), the weighted parameters assigned to each fitness parameter are represented as α_1, α_2, α_3, α_4 and α_5. Moreover, the trust value of the node is represented as F_1, energy ratio of the node is represented as F_2, the communication cost of the node is represented as F_3, the total number of gateway hops is represented as F_4 and the network load is represented as F_5.

- The primary fitness function considered in ETA-MAVO is the trust value of each node. The degree of confidence one node has in another node to be assigned for work within a given time frame is known as trust. Based on the details of previous communications, one node can estimate the trust value of another node. This value is time-dependent and changes based on observations from trusted neighbour nodes. By utilizing the packet forwarding behaviour that assesses each neighbour's packet forwarding performance, the trust metrics are calculated. This could be the proportion of packets successfully received and routed by a node. The trust value calculation between nodes i and j is represented in Eq. (9).

$$F_1 = \frac{U_{i,j}(t)}{V_{i,j}(t)} \quad (9)$$

In Eq. (9), $U_{i,j}(t)$ represents the number of packets transferred by node j at the time t and likewise $V_{i,j}(t)$ represents the total received packets at node j. The occurrence of a malicious node is easily identified using the trust value. When the malicious node is present in the network, the trust value gets reduced so it is easily detected and successfully neglected from the network route.

- One of the most important issues for cluster-based systems is energy. According to the suggested methodology, the most crucial factor in CH appointment process is energy. For the CH nomination process, the suggested approach makes use of the initial energy to residual energy ratio of

nodes. The fitness function of the suggested scheme's energy ratio makes the CH selection process energy-dependent. The node with the highest level of residual energy has a greater chance of winning the CH contest. The parameter for the energy ratio present in the fitness function is represented in Eq. (10) and Eq. (11).

$$F_2 = \sum_{i=1}^{N} \frac{Initial\ energy}{Residual\ energy} \tag{10}$$

The Eq. (12) can be written as,

$$F_2 = \sum_{i=1}^{N} \frac{E_0}{E_0 - S(i).E} \tag{11}$$

Where the total number of nodes is represented as N, the energy at the initial stage is represented as E_0 and the energy of the nodes in the current situation is represented as $S(i).E$. The goal is to reduce the energy ratio of nodes to a minimum so that total energy costs can be kept to a minimum. The value of the energy ratio gets decreased if the node's remaining energy is high. The fitness function seeks to improve network performance and lifetime by selecting nodes with higher residual energy for the CH job. The network performance may be directly impacted if the lower energy node is chosen to be the CH.

- Data is transmitted using the power that is directly proportional to the square of the distance between candidate nodes and the source node. The communication cost is computed using Eq. (12).

$$F_3 = \frac{d_{avg}^2}{d_0^2} \tag{12}$$

Where, the average distance between the nodes and the neighbours is represented by d_{avg} and the distribution radius of the node is represented by d_0.

- The total number of gateway hops present in the network node is represented using the following Eq. (13).

$$F_4 = \sum_{i=1}^{m} NextGCount(g_i) \tag{13}$$

Where, amount of gateways necessary for reaching to BS from gateway (g_i) is denoted as $NextGCount(g_i)$ and total amount of gateways is denoted as m. The minimal number of hops and the minimum traversal distance are taken into account during routing. Therefore, the solution's fitness value increases as there is decrease in total distance travelled and the number of hops. That is, the amount of travel time and the number of hops are inversely related to the routing fitness. The optimal option among the node population is the one with the highest fitness value.

- In the final fitness function, network load balancing is utilized to manage the load from CH and the high amount of loads in CH can be minimized using the Eq. (14).

$$F_5 = \frac{max(|CN_q|)}{\frac{1}{R}\sum_{q=1}^{R}(|CN_q|)} \tag{14}$$

Where, the number of nodes present in the cluster q is represented as $|CN_q|$ and the total number of clusters is represented as R.

The above-mentioned fitness functions namely: trust value, energy ratio, communication cost, the total number of gateway hops, and the network load, are employed in the detection of malicious nodes, which enhances the energy efficiency of the MANET.

3.3 Formation of cluster

In the stage involving creation of clusters, the normal sensors are consigned to choose the CHs. Here, the creation of clusters takes place by energy and distance. The equational representation used to form the cluster function is represented in the Eq. (15).

$$Sensor\ potential\ (s_i) = \frac{E_{CH}}{dis(s_i, CH)} \tag{15}$$

Where, energy of CH is denoted as E_{CH} and distance between ith sensor and CH is denoted as $dis(s_i, CH)$.

3.4 Generation of routing path using ETA-MAVO

The path for routing is created using the proposed ETA-MAVO method. In the scenario of path generation, the CH near to sink node is considered the final gateway. There are five optimal fitness functions known as trust value, energy ratio, communication cost, total number of gateway hops and network load, for optimizing the transmission path generation. The following steps are processed during the phase of the routing stage,

1. At first, the vultures are initialized with the possible paths from the source CH to the receiver node. Each vulture's dimension is equal to the number of intermediate nodes that exist in the path.
2. Next, the stage of exploration and exploitation are updated according to the fitness of each path. The information about the stage of exploration and exploitation is already explained in the previous sections.

Table 1. Simulation parameters

Parameters	Values
Area of simulation	1000 m × 1000 m
Simulation time	800 (sec)
Total number of nodes	1000 nodes
Size of the data packet	512 byte
Bandwidth	2 Mb/sec

3. The fitness considered while generating the transmission path is trust, energy ratio, and communication cost. Eq. (16) denotes the fitness utilized in ETA-MAVO-based route generation.

$$Fitness = \gamma_1 \times \frac{U_{i,j}(t)}{V_{i,j}(t)} + \gamma_2 \times \sum_{i=1}^{N} \frac{E_0}{E_0 - S(i).E} + \gamma_3 \times \frac{d_{avg}^2}{d_0^2} \quad (16)$$

In the above Eq. (16), γ_1, γ_2, and γ_3 are known as weighted parameters assigned to each objective of route generation. This helps in identifying the routing path with high trust value, energy ratio, and less cost for communication. Therefore, the consumption of energy at the node is reduced by utilizing the ETA-MAVO based routing which aids in enhancing the lifespan of the network.

4. Results and discussion

The results and discussion of the ETA-MAVO are explained in this section. The design and implementation of reliable transmission using ETA-MAVO are performed using MATLAB R2018a. The features of the system, comprise an i5 processor with 6GB RAM. The major part of the ETA-MAVO method is to attain high security and energy efficiency for the MANET. The simulation parameters of ETA-MAVO are represented in Table 1.

4.1 Performance analysis

The performance of the ETA-MAVO is evaluated in terms of delay, energy consumption, throughput and detection rate. In this paper, the overall performance of ETA-MAVO is evaluated along with the hybrid cat slap single-play algorithm (C-SSA) [12], data driven zone based routing protocol (DD-ZRP) [15], angular based energy proficient trusted routing (ACEPTR) protocol [21]. Further, the recent optimization techniques such as AO used for multi-objective operation in electric vehicles (EV) [22] and POA used for optimization of networks [24] are developed for performing clustering and routing to evaluate the performance of ETA-MAVO. The

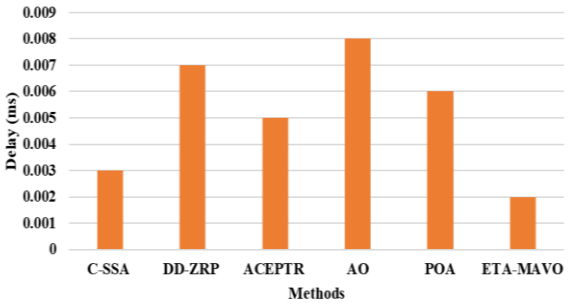

Figure. 2 Graphical representation of delay

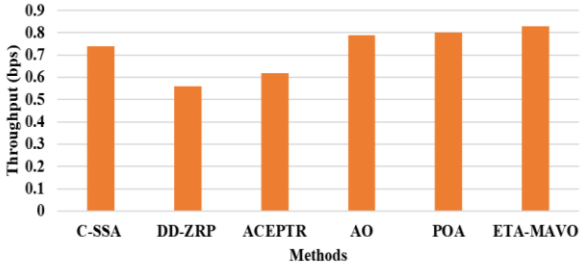

Figure. 3 Graphical representation of throughput

aforementioned approaches are implemented with the same specifications as shown in Table 1.

4.1.1. Delay

Delay time is represented as the time between change of component measured at the source point and the destination point of the system. The time delay obtained by C-SSA, DD-ZRP, ACEPTR, AO, POA and ETA-MAVO algorithms are graphically represented in the Fig. 2. The time period on delay of C-SSA, DD-ZRP, ACEPTR, AO, POA and ETA-MAVO algorithms are 0.003, 0.007, 0.005, 0.008, 0.006 and 0.002 msec respectively. The results obtained from the simulation show that the suggested ETA-MAVO acquired the minimum delay of 0.002 msec when compared with the existing techniques.

4.1.2. Throughput

The network throughput is defined as the amount of data shifted effectively from one node to another in a particular period. The network throughput obtained by C-SSA, DD-ZRP, ACEPTR, AO, POA and ETA-MAVO algorithms are graphically represented in Fig. 3. The throughput values of C-SSA, DD-ZRP, ACEPTR, AO, POA and ETA-MAVO algorithm are 0.74, 0.56, 0.62, 0.79, 0.80 and 0.83 bps respectively. The results obtained from the simulation show that the suggested ETA-MAVO acquired high network throughput and shifted more data during the transmission when compared with the existing techniques C-SSA, DD-ZRP, ACEPTR, AO and POA.

Table 2. Comparative analysis

Parameter	C-SSA [12]	DD-ZRP [15]	ACEPTR [21]	AO [22]	POA [24]	ETA-MAVO
Delay(ms)	0.003	0.007	0.005	0.008	0.006	0.002
Energy consumption (mJ)	0.11	0.08	0.1	0.09	0.08	0.07
Throughput (bps)	0.74	0.56	0.62	0.79	0.80	0.83
Detection rate (%)	90	68	72	91	90	93

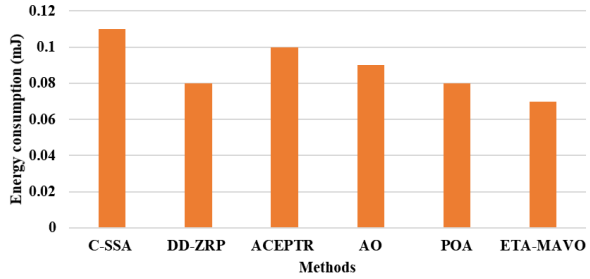

Figure. 4 Graphical representation of energy consumption

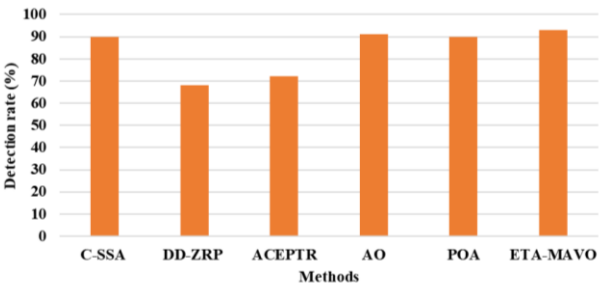

Figure. 5 Graphical representation of detection rate

4.1.3. Energy consumption

The consumption of energy in the network is defined as the quantity of consumed energy during the time of receiving and broadcasting packets that contain data. The energy consumed by C-SSA, DD-ZRP, ACEPTR, AO, POA and ETA-MAVO algorithms are graphically represented in Fig. 4. The energy consumption of the C-SSA, DD-ZRP, ACEPTR, AO, POA and ETA-MAVO algorithms are 0.11, 0.08, 0.1, 0.09, 0.08 and 0.07 mJ respectively. The results obtained from the simulation show that the suggested ETA-MAVO consumed less amount of energy during the process when compared with the existing techniques.

4.1.4. Detection rate

The detection of malicious nodes present in the network within a particular time period is referred to as detection rate. The detection rate of C-SSA, DD-ZRP and ETA-MAVO, ACEPTR, AO and POA algorithms are graphically represented in the Fig. 5. The detection rate of C-SSA, DD-ZRP, ACEPTR, AO, POA and ETA-MAVO algorithm is 90%, 68%, 72%, 91%, 90%and 93% respectively. The results obtained from the simulation show that the suggested ETA-MAVO has higher rate of detection during the process while compared with the rest of the existing techniques.

4.2 Comparative analysis

The comparative analysis of the ETA-MAVO with existing researches is provided in this section. The existing C-SSA, DD-ZRP, ACEPTR, AO and POA are used for comparison with ETA-MAVO to evaluate its efficiency. This analysis amongst the C-SSA, DD-ZRP, ACEPTR, AO, POA and ETA-MAVO algorithm, is represented in Table 2. The results obtained from Table 2 show that ETA-MAVO attains better performance when compared with the existing methods due to the selection of optimal fitness function. The derived multi-objective fitness function is utilized in achieving secure and energy-efficient data transmission over the networks in MANET. The trust value considered in the ETA-MAVO is used to improve the detection rate of malicious attackers which helps to enhance the throughput. Moreover, the combination of CH selection and multipath routing using ETA-MAVO is used to minimize the energy consumption. The clustering performed in the ETA-MAVO is used to minimize overhead which resulted in lesser delay.

5. Conclusion

Mobile ad hoc networks have sparked a keen interest among researchers due to their potential applications. Despite this, these networks are vulnerable to a variety of attacks due to their inherent characteristics. Broad deployment of these wireless networks is still significantly hampered by their energy and security constraints. A safe energy-efficient routing protocol addresses both the energy crisis as well as the security concerns. A successful routing approach is employed using the multi objective African vulture optimization calculations. The effective leaps for innovative routing are performed in MANET using the proposed ETA-MAVO method. The selection of CH and generation of routing path using ETA-MAVO increasingly involves the utilization of parameters related to

fitness such as trust value, energy ratio, communication cost, the total number of gateway hops, and network load. The trust value obtained from ETA-MAVO is utilized for mitigating malicious attacks during the stage of data transmission. The results obtained from the comparative analysis show that ETA-MAVO attained high performance when compared with other existing methods. Moreover, the performance of ETA-MAVO is compared with the existing C-SSA, ACEPTR, AO, POA and DD-ZRP. Overall the proposed method achieves better results. In the future, the proposed method can be tested under more security attacks to evaluate its efficiency and performance metrics.

Nomenclature

Parameter	Description
$best\ vulture_1$ and $best\ \ vulture_2$	Best vultures of the first and second class
$R(i)$	The remaining vultures joins with the first and second class
P_i	Probability of selection
L_1 and L_2	Values between $[0, 1]$
F_i	Fitness value of i^{th} vulture
n	Number of populations
$iter$	Current iteration
$iter_{max}$	Maximum iteration
h	Random number in the range [-1, 1]
z	Random number present in the range [-2, 2]
r_1, r_2, r_3, r_4, r_5 and r_6	Random number between 0 and 1
w	Value set before the optimization
X	Distance located by the vulture to save their food from others
u_b	Upper limits
l_b	Lower limits
$Levy$	Levy flight function
$\alpha_1, \alpha_2, \alpha_3, \alpha_4, and\ \ \alpha_5$	Weighted parameters assigned for each fitness parameter
F_1	Trust value of the node
F_2	Energy ratio
F_3	Communication cost
F_4	Total number of gateway hops
F_5	Network load
$U_{i,j}(t)$	Number of packets transferred by node j
$V_{i,j}(t)$	Total received packets at node j
t	Time
N	Total number of nodes
E_0	Energy at the initial stage
$S(i).E$	Energy of the nodes in the current situation
d_{avg}^2	Average distance between the nodes and the neighbours
d_0	Distribution radius of the node
$NextGCount(g_i)$	Amount of gateways necessary for reaching to BS from gateway (g_i)
m	Total amount of gateways
$\lvert CN_q \rvert$	Number of nodes present in the cluster q
R	Total number of clusters
E_{CH}	Energy of CH
$dis(s_i, CH)$	Distance between ith sensor and CH

Conflicts of interest

The authors declare no conflict of interest.

Author contributions

The paper conceptualization, methodology, software, validation, formal analysis, investigation, resources, data curation, writing—original draft preparation, writing—review and editing, visualization, have been done by 1st author. The supervision and project administration, have been done by 2nd author.

References

[1] S. S. Jamaesha and S. Bhavani, "A secure and efficient cluster based location aware routing protocol in MANET", *Cluster Computing*, Vol. 22, No. 2, pp. 4179-4186, 2019.

[2] N. S. S. S. Farheen, V. K. Sharma, and A. Jain, "An optimized Energy efficient cluster based routing in MANET", *Journal of Xi'an University of Architecture & Technology*, Vol. 12, No. 5, pp. 109-117, 2020.

[3] M. A. Mahdi, T. C. Wan, A. Mahdi, M. A. G. Hazber, and B. A. Mohammed, "A Multipath Cluster-Based Routing Protocol for Mobile Ad Hoc Networks", *Engineering, Technology & Applied Science Research*, Vol. 11, No. 5, pp. 7635-7640, 2021.

[4] V. Alappatt and P. M. J. Prathap, "Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E", *International Journal of Computer Networks and Applications*, Vol. 8, No. 4, pp. 400-411, 2021.

[5] M. Rajashanthi and K. Valarmathi, "Energy-efficient multipath routing in networking aid of clustering with OGFSO algorithm", *Soft Computing*, Vol. 24, No. 17, pp. 12845-12854, 2020.

[6] W. Alnumay, U. Ghosh, and P. Chatterjee, "A Trust-Based predictive model for mobile ad hoc network in internet of things", *Sensors*, Vol. 19, No. 6, p. 1467, 2019.

[7] G. Husnain and S. Anwar, "An intelligent cluster optimization algorithm based on Whale Optimization Algorithm for VANETs (WOACNET)", *Plos one*, Vol. 16, No. 4, p. e0250271, 2021.

[8] R. Raja and P. Ganeshkumar, "QoSTRP: A trusted clustering based routing protocol for mobile ad-hoc networks", *Programming and Computer Software*, Vol. 44, No. 6, pp. 407-416, 2018.

[9] V. S. Devi and N. P. Hegde, "Multipath security aware routing protocol for MANET based on trust enhanced cluster mechanism for lossless multimedia data transfer", *Wireless Personal Communications*, Vol. 100, No. 3, pp. 923-940, 2018.

[10] S. S. Sefati and S. G. Tabrizi, "Detecting sybil attack in vehicular ad-hoc networks (vanets) by using fitness function, signal strength index and throughput", *Wireless Personal Communications*, Vol. 123, No. 3, pp. 2699-2719, 2022.

[11] C. G. 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.

[12] S. Sennan, S. Ramasubbareddy, S. Balasubramaniyam, A. Nayyar, C. A. Kerrache, and M. Bilal, "MADCR: mobility aware dynamic clustering-based routing protocol in Internet of Vehicles", *China Communications*, Vol. 18, No. 7, pp. 69-85, 2021.

[13] D. R. Edla, M. C. Kongara, and R. Cheruku, "A PSO based routing with novel fitness function for improving lifetime of WSNs", *Wireless Personal Communications*, Vol. 104, No. 1, pp. 73-89, 2019.

[14] P. Mohan, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalaf, and S. Ulaganathan, "Improved metaheuristics-based clustering with multihop routing protocol for underwater wireless sensor networks", *Sensors*, Vol. 22, No. 4, p. 1618, 2022.

[15] A. R. Mohindra and C. Gandhi, "A secure cryptography based clustering mechanism for improving the data transmission in MANET", *Walailak Journal of Science and Technology (WJST)*, Vol. 18, No. 6, p. 8987, 2021.

[16] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah, and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks", *IEEE Access*, Vol. 10, pp. 14260-14269, 2022.

[17] N. Veeraiah, O. I. Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, and N. Alsufyani, "Trust aware secure energy-efficient hybrid protocol for manet", *IEEE Access*, Vol. 9, pp. 120996-121005, 2021.

[18] 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.

[19] 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.

[20] N. Chugh, G. S. Tomar, R. S. Bhadoria, and N. Saxena, "A novel anomaly behavior detection scheme for mobile ad hoc networks", *Electronics*, Vol. 10, No. 14, p. 1635, 2021.

[21] V. Thirunavukkarasu, A. S. Kumar, and P. Prakasam, "Cluster and angular based energy proficient trusted routing protocol for mobile ad-hoc network", *Peer-to-Peer Networking and Applications*, Vo. 15, No. 5, pp. 2240-2252, 2022.

[22] N. K. CH, S. R. Inkollu, R. Patil, and V. Janamala, "Aquila Optimizer Based Optimal Allocation of Soft Open Points for Multi Objective Operation in Electric Vehicles Integrated Active Distribution Networks", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 4, 2022, doi: 10.22266/ijies2022.0831.25.

[23] P. D. Kusuma and A. L. Prasasti, "Guided Pelican Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 6, pp. 179-190, 2022, doi: 10.22266/ijies2022.1231.18.

[24] F. A. Zeidabadi and M. Dehghani, "POA: Puzzle Optimization Algorithm", *International Journal of Intelligent Engineering and Systems*, Vol. 15, No. 1, pp. 273-281, 2022, doi: 10.22266/ijies2022.0228.25.