SSRG International Journal of Electrical and Electronics Engineering
ISSN: 2348-8379/ https://doi.org/10.14445/23488379/IJEEE-V12I7P103

Volume 12 Issue 7, 18-33, July 2025

Original Article

ETPA: Energy, Throughput, Privacy Aware Multipath Routing with Intrusion Avoidance for Reliable MANET System

Nirmala Bai K.S[1*], M.V. Subramanyam[2]

[1]*JNTUACEK, Kalikiri. Annamayya, AP, India.*
[2]*Santhiram Engineering College, Nandyal, AP, India.*

**Corresponding Author : nirmala.lalitha@gmail.com*

Received: 03 May 2025 Revised: 05 June 2025 Accepted: 04 July 2025 Published: 31 July 2025

Abstract *- One of the power consumption issues in MANET networks is a major continuous problem, and it is of great importance to develop an energy-efficient routing architecture to prolong the operation of the network. Therefore, it is also claimed that the more mobility of the nodes in MANETs results in more network traffic and delays. Reducing such delays is still a major focus of study using optimization techniques. This work proposes the energy-aware multipath routing model applied to the clustering system using a Genetic Algorithm-Based Lion Optimization (GALO) AOMDV model. To prevent intrusions through clustering, Adaptive Ensemble Tree Learning (AETL), clubbed with the best machine learning technique, Hybrid Dual Optimization of Machine Learning Model (HDOMLM), is chosen by this study to choose cluster heads. The GALO algorithm aims to enhance network lifespan and generic Quality of Service (QoS) by lowering link failures using appropriate data transmission path identification. It would leverage the proposed GALO model for the networks to find shorter networks and thus improve the packet delivery ratio, throughput, packet loss, Delay, and energy depletion. Running the simulations, with our proposed ETPA system, we were able to attain 71% more energy from previous routing algorithm-based implementations and an increase of 50.12% on network lifetime.*

Keywords *- CH nodes, Clustering, Intrusion avoidance, MANET, Multi-path routing, Network lifetime, Shortest path selection.*

1. Introduction

Mobile Ad Hoc Networks (MANETs) are a new form of wireless networking; they are self-configuring networks independent of fixed infrastructure [1]. Compared to popular networks such as conventional base stations and wired networks, MANETs are self-organizing networks built of nodes that communicate wirelessly. The ad hoc network is created where the nodes can dynamically create and sustain links between each other. Due to the lack of infrastructure, MANETs are especially appropriate for applications where establishing or supporting fixed infrastructure is impossible, uneconomical, or unavailable. Due to the fact that MANETs are often deployed in military operations, disaster conditions, and remote areas with no conventional network infrastructure, there are many channels of peer-to-peer communication. The main difference between MANETs and conventional network types is that MANETs have specific features. One very important aspect of MANETS is that their topology is dynamic [2]. Because nodes are mobile, there is a lack of established infrastructure, security, and energy efficiency, which are the key issues in MANETs. Creating a communication pathway among nodes in MANETs is necessary; routing methods are used to ensure that data is transmitted to any part of the network [4]. In MANETs, data must be exchanged, and other resources must be shared between nodes to coordinate actions among nodes. For such methods to be efficient, they must adapt to the dynamic nature of MANETs to maintain connections between nodes that move around and generate connection changes. The routing methods are difficult to use due to the fluctuating topology of MANETs. Nodes continually relocate and through this process, form, sever, or modify connections between these nodes. Routing protocols must detect changes, and routing tables must be changed in accordance with the new information. To satisfy this requirement, reactive or hybrid routing protocols need to be implemented to find new routes and continue with the old routes in the presence of node mobility. Since these routing methods demand a large number of resources and a long time to adjust, proactive methods to keep the routing information of all the network nodes are unsuitable for MANETs. Due to the limited battery capacity in mobile nodes becomes a key issue in increasing the energy efficiency in MANETs to increase the lifetime [1]. MANETs usually consist of mobile nodes operating on constrained

battery power; hence, energy efficiency is an important design factor. As with most networks, throughput is a critical performance metric for MANETs, which is defined as the rate of successful message transmission, implying the network's capacity to deal with the data load [7]. Throughput, in simple terms, is the amount of data that is transmitted over an effective network within some given time frame. Since MANETs must accommodate diverse applications and high throughput, which is crucial for making effective data transfer possible, they must deliver high throughput. MANETs are becoming more and more aware of the importance of protecting the privacy of their communication and, as a result, require privacy-supporting routing techniques that prevent eavesdropping and unwanted sharing of sensitive information [8]. Since MANETs are being used more and more in sensitive applications, such as military communications and personal data sharing, privacy has become a major issue.

To decrease energy consumption, energy-aware routing protocols try to select paths that either prolong the operation life of nodes or the network. The finite battery resources of the mobile nodes [10] translate into a need to extend the network's lifespan. However, effective energy management is critical to ensure the connectivity and reliability of the network in a highly volatile MANET environment [11].

They create energy-centric trees with the objective of reducing energy consumption [12]. An energy-efficient routing method, DTOEO, is presented, which uses the generation of energy-based trees to minimize the use of Energy in MANETs. In this technique, we build a tree-like structure that conveys the data transmission on the nodes with the highest energy levels and located at small inter-node distances. In addition, hybrid methodologies that employ AHP, EWM, and AODV can obtain Energy efficient routing [13]. The hybrid routing methodologies blend the characteristics of proactive and reactive routing approaches to achieve energy efficiency.

In the MANET environment, privacy-conscious routing methods are formulated to protect sensitive information and to deliver secure data [14]. In MANETs, user trust and safe applications are essential; therefore, user data and secrecy should be safeguarded [15]. MANET routing incurs energy efficiency, throughput optimization, and privacy preservation as vital factors [16]. These three aspects are important for MANETs to be usable, performable, and secure in the face of different applications. These difficulties must be tackled to implement networking protocols successfully. However, in the case of MANETs, the problem is further complicated by the fact that the topology of the networks is fluctuating, and nodes in the network are mobile [17]. Furthermore, since nodes move, network connections change, and so do traffic patterns and resource utilization, it can be quite difficult to distinguish between typical variations and malicious actions [18].

1.1. Problems Identified

Trust forms a basic part of the successful development and sustainability of MANETs. In MANETs, it is guaranteed that if users can ensure their data and conversation secrecy, users are more affected and depend on MANETs. Assuming some routes are stale, one can have many routes and use table-driven protocols or proactive multipath routing methods to keep multiple routes. The trailing protocols keep their routing tables updated regularly. Consequently, there are many feasible routes that the data will travel through and that can facilitate changes to the architecture of the network. Proactive systems give quick access because the routing data is maintained immediately, but there can be considerable expenses in the constant maintenance of routing data. Being a distributed topology, nodes of the MANET share the intrusion detection capabilities, i.e. a distributed Intrusion Detection System (IDS) is to be used in MANETs.

1.2. Motivation for the Proposed Work

- Without a doubt, MANET nodes have very limited resources, such as processor capacity and battery life. Safe routing strategies for optimizing resource utilization are what we need to develop.
- For the MANETs, node failures and connection interruptions are caused by mobility and limited resources. The structure of the network takes part then. Multipath routing has several other alternatives, rather than a single path, so the chance for successful data transfer increases.
- The MANET is sensitive to a variety of hazards, such as routing attacks, data integrity attacks, and node intrusion. Authenticating and encrypting between paths on each Path makes secure multipath routing an ideal way to guarantee that data is kept confidential and intact on its way to the destination.
- Multipath routing helps to lower congestion and improve network efficiency via better use of the capacity that is on hand, distributing traffic over several channels.
- In particular, multipath routing boosts the network's lifetime when MANETs are run on batteries using load distribution and efficient routing techniques.

1.3. Outline and Major Contributions of the Proposed Work

The Energy, Throughput, and Privacy Aware (ETPA) algorithms are designed for secure multi-path routing, efficient intrusion avoidance, and low-cost clustering in this proposed system. The nodes are predicted as malicious or normal in the intrusion avoidance algorithm of Adaptive Ensemble Tree Learning (AETL) based on three terms: Energy, routing overhead, and Packet Delivery Ratio (PDR). After this identification, the network is clustered, and the leading agents for each cluster are identified using the optimized machine learning method of Hybrid Dual Optimization of Machine Learning Model (HDOMLM). The main contribution of the proposed model is given as follows:

- Multipath routing redeems itself with redundancy by providing several paths between the source and destination nodes. However, the proposed GALO does yet transport data across other pathways despite one connection not working, thus increasing the network resilience and decreasing the packet loss.
- Reducing the amount of traffic over each Path enables several channels to share data. Distributing the traffic load fairness between the nodes aids in the improvement of the efficiency of the entire network and prevents congestion.
- Using many secure routes allows the network to resist many security risks, including eavesdropping. Intrusion avoidance is implemented using AETL, and different simulation scenarios of different attack levels are evaluated in the performance analysis.
- Evaluation of the proposed models with various aspects and environment configurations is measured and analyzed to show the proposed model's ETPA efficiency.

1.4. Paper Organization

The remaining paper sections are structured as follows: related and earlier implementations in section 2, methodology of the proposed model of ETPA and its mathematical derivations in section 3, simulation experiments and performance analysis in section 4, and conclusion in section 5.

2. Related Works

The high throughput is necessary for MANETs to support appropriate data transfer speed and various applications. Throughput is the term used to describe the rate at which data can be transmitted from a source to a destination over a link. In MANETs, higher throughput is crucial to allow huge file transfers, video streaming, online gaming, etc. Network overload will be averted, and good throughput in MANETs will be provided by congestion control strategies [19]. Consequently, if the demand for network resources exceeds the network's capacity, congestion will arise, causing delays, packet loss, and reduced throughput.

The method used by AIACOAR is inspired by the way ants find paths to discover the best routes that decrease the transmission time and energy consumption. Ant colony optimization is used in AIACOAR to find the shortest transmission time and energy consumption for the optimal routes. Data packets are secured by using encryption methods such as Elliptic Curve Cryptography (ECC). Also, from illegal access [18], in the case of encryption, data is transformed into a gibberish form, which unauthorized people cannot comprehend. One of the popular encryption algorithms used today is called elliptic curve cryptography (ECC), which provides high security with low computation power required for the encryption, making it suitable for the resource-constrained Mobile Ad Hoc Network (MANET). The authentication systems ensure that data can only be accessed by the authorized device [8], thereby ensuring data integrity and reliability. Authentication means determining or proving who you are so that a resource on a network gives you access. It prevents unauthorized nodes from obtaining confidential information and disrupting the network's operations. The routing protocols based on the trust route are based on the reliable node. Then they have some trust metrics based on which they quantify the dependability and security of a particular node. Typically, such protocols give trust levels to nodes depending on their past behavior, reputation, and transactions on other nodes [5]. Therefore, routing decisions are driven by prioritizing paths containing nodes with high trust, thereby increasing the chances of eliminating hostile nodes from the routing path. Secure multipath routing schemes apply cryptographic techniques to secure data transmission to ensure data transmission confidentiality, integrity, and authenticity [20]. Encryption methods are used during these protocols to safeguard data packets and prevent the individual from gaining unauthorized access to sensitive information.

To create such routing protocols while adding security, security should be added without hampering the network performance, considering some important factors [21]. The main aspect is scalability. In other words, a routing protocol has to be able to accommodate many nodes and changing networks. To diminish this problem, scalable routing methods must minimize routing overhead, shorten path discovery time, and deal well with routing information [22].

Message delivery in Mobile Ad hoc Networks (MANETs) relies on Energy efficient methods, as it has been observed that the nodes in MANETs usually have a limited amount of battery power [23]. Hence, we need to engineer routing protocols to maximize energy efficiency by minimising control message transmissions, using energy-conserving routes, and applying power-aware routing metrics. To reduce the cost of energy expenditure on security operations, energy efficient intrusion detection systems are required. In Mobile Ad Hoc Networks (MANETs), diverse trust metrics and models are used to evaluate nodes' reliability; each is unique in its strengths and weaknesses [24]. Metrics based on reputation measure a node’s historical behavior, i.e. how compliant they are with the network protocols and whether they tend to collaborate and be reliable. Generally, these metrics are derived from previous data, namely, packet forwarding rates, response times, and behavioral consistency.

The latter work investigates using reputation-based metrics that provide a longitudinal measure of the reliability of a node but behave sluggishly. From the standpoint of energy metrics, a node’s level of energy is a factor in its reliability, so nodes with lower energy levels are more likely to behave selfishly or maliciously [25]. It is assumed that nodes with limited energy resources may choose their privilege at the expense of network collaboration. This will

degrade the performance or even lead to malicious behavior. However, energy-based indicators provide a dynamic evaluation of the node's reliability, but on some occasions, they are not accurate. QoS-based metrics evaluate a node by its ability to provide service quality, which in this case implies its efficiency in transmitting data with an acceptable level of packet loss, throughput, and latency [26]. The metrics for such performance, such as Latency, Bandwidth, and error rates, are generally provided by real-time network performance assessments. However, the QoS-based metrics are dynamic and evaluate a node's reliability with respect to external variables such as network congestion and interference. Using the benefits of each indicator, hybrid models combine different measures to provide a complete trust assessment by taking advantage of their strengths to give a more precise and resistant estimate of node trustworthiness [27]. These can then utilize weighted averaging or fuzzy logic to combine data from different sources such as reputation scores, energy levels, and quality of service measures. However, the idea of combination models gives a holistic view of node reliability, although it might come with more complexity in implementation and operation. The comparison of performance for recent works of secure multi-path routing in MANET is listed in Table 1.

Table 1. Recent works of secure multi path routing in MANETs

Ref	Methodology	Key Findings	Limitations
[28]	Centralized and new smart controller that changes the rates, a mix of ambient intelligence methods such as ant colony optimization and use of elliptic curve cryptography, to secure the communications, and a multi-hop quality of service scheduler.	The proposed method yields an improved PDR over currently available AIFSORP and LF-SSO methods.	The high energy consumption in dynamic environments is utilized in this paper algorithm.
[29]	An optimized Ad hoc On-Demand Distance Vector (AODV) routing protocol, utilizing Improved Chicken Swarm Optimization (ICSO), is employed.	MANET routing protocol combined with an energy conservation strategy using a clustering hierarchy to maximize network lifespan. Fire Hawk Optimization (FHO) is used for Cluster Head (CH) selection.	MANETs' changeable topology can negatively impact system performance, and limited battery power makes energy consumption a major challenge, particularly affecting network lifetime and throughput.
[30]	The paper proposes a "MANET-ESO IoT" method to improve security and energy efficiency in IoT-based wireless sensor networks by leveraging MANET routing principles.	Simulation results show improved performance in terms of node alive counts, residual energy, throughput, delivery ratio, and reduced routing overhead.	Challenges arise from the combination of MANET and IoT characteristics, specifically moderate security and high packet loss in IoT networks compared to MANETs, and the need to balance energy saving with frequent data forwarding to the internet gateway.
[31]	The paper proposes two improved routing protocols, PLA-AOMDV and ELA-AOMDV, building upon FF-AOMDV.	ELA-AOMDV is experimentally shown to outperform PLA-AOMDV in throughput, packet drop rate, energy consumption, and network lifetime.	Needs enhancements in addressing link breakage and utilization.
[32]	The paper proposes a modified AODV routing protocol for MANETs that uses a combination of the Analytic Hierarchy Process (AHP) and Entropy Weight Method (EWM) to select routes based on energy, congestion, and hop count.	Simulations demonstrate improved performance in terms of end-to-end delay, energy consumption, and network lifetime.	The vanilla AODV protocol, which uses hop count as the sole metric, suffers from network congestion and energy exhaustion, limiting its use in resource-constrained applications.

3. Proposed Secure Multi-Path Routing using Optimization of Genetic Algorithm and Lion Optimization (GALO)

Before starting the real transmission in the network, intrusion detection is performed using the proposed Adaptive Ensemble Tree Learning (AETL). In this method, the characteristics of each node in the network are gathered and decided as normal or malicious. After detecting and recovering a malicious intrusion in the Network, the Leading Agent (LA) Node prediction is implemented using a Hybrid Dual Optimization of Machine Learning Model (HDOMLM).

The clustering and the Selection of LA nodes play a crucial role in the MANET routing. This is done by integrating PSO-based clustering and Optimized ML-based detection of LA nodes. Because of the perpetual mobility of nodes, the topology of the MANET is subject to changes that are neither predicted nor anticipated. When relay nodes are not in a direct link for transmission, the means of routing are utilized by the nodes to facilitate transmission. For the sole purpose of propagating the data, relay nodes are accountable. The prediction of the shortest Path between the source node and destination is decided with the optimization using the Genetic Algorithm Lion Optimization (GALO). Secure Multi-Path routing is implemented in this proposed work using GALO with the decision metrics of Energy, Throughput, and Privacy (ETPA). The overall proposed workflow is portrayed in Figure 1.

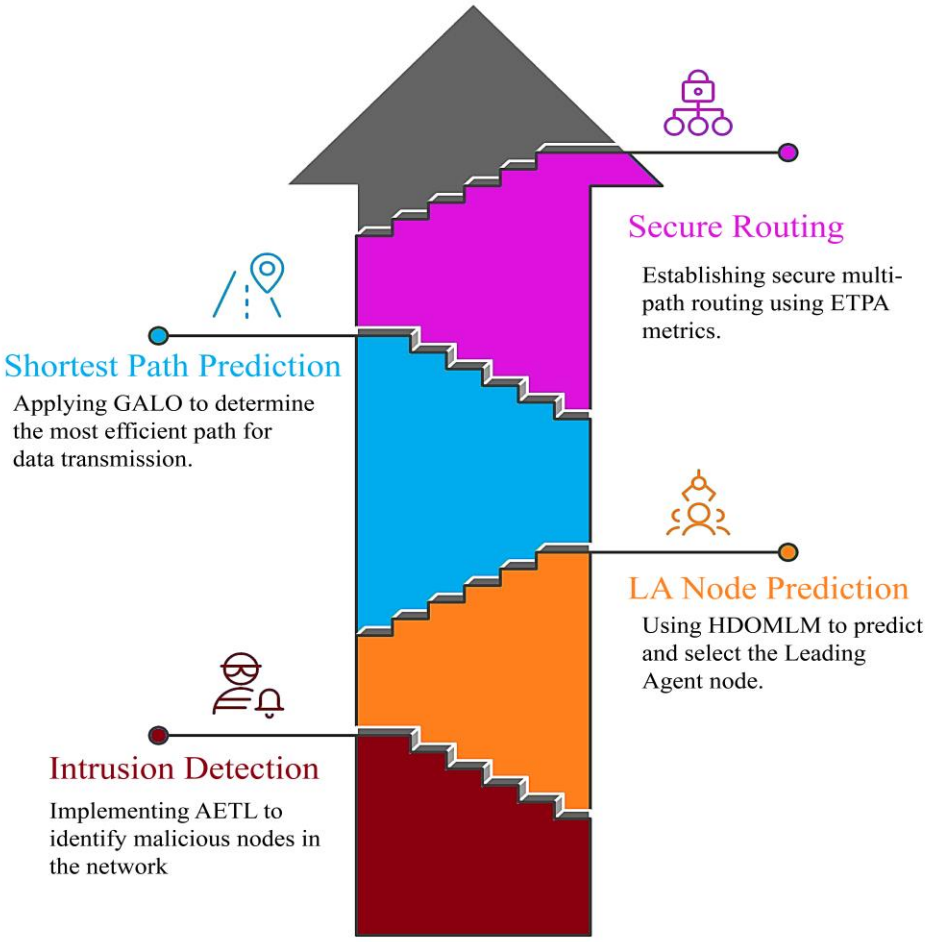

Fig. 1 Proposed ETPA system model block diagram

3.1. Energy Model of MANET

The issue of energy efficiency is very important for the communications between nodes in Mobile Ad Hoc Networks (MANETs) and for power utilization.

Together with the fact that batteries are the main power supply for data transmission, and since nodes are consuming energy in the states of sending, receiving, sleeping, or idle, this rather significantly impacts how the network performs [33].

Different energy-saving measures are used to minimise energy consumption under different network conditions and attributes when implementing routing protocols.

3.1.1. Transmission Mode

In the transmission mode, nodes send data packets for energy level estimation based on the transmitting nodes, and this versatility in ad hoc routing is applied as,

$$E_{Trans} = \frac{E_{Transmission}}{E_t} \quad (1)$$

3.1.2. Receiving Mode

When we are in receiving mode, the energy consumed is not significantly more than the acceptable level of packet reception at the sender, as given by,

$$E_{Rec} = \frac{E_{receive}}{E_t} \quad (2)$$

Power transmission in Equation (2) speaks of the power consumed in transmission mode. $E_{receive}$ and E_t Receive is assumed to be the energy consumed for reception and the total energy of the node, respectively.

3.1.3. Idle Mode

While not sending data, nodes consume energy in idle mode due to the status table constantly being checked and refreshed for added nodes.

In this mode, the energy consumption is essentially the combination of getting mode operations. The communication model for the idle mode of the network is represented as,

$$E_{idle} = E_{receive} \quad (3)$$

3.1.4. Overhearing Mode

In the overhearing stage, the nodes consume energy even for the packets they are not interested in, resulting in a waste of power. The power overhearing component used to model this energy consumption is defined as,

$$\mathrm{E}_{\text{ overhearing}} = \mathrm{E}_{\text{ receive}} \quad (4)$$

The $\mathrm{E}_{\text{ receive}}$ represents the power consumed during normal packet reception. Finally, the total energy consumed in the network is calculated considering the energy consumed for packets being overheard, idle states, and transmission and reception energy. To maximize the network lifetime, we have to minimize the overall energy consumption so that the power is available to all the nodes in the network.

3.2. Intrusion Detection using AETL

In particular, Adaptive Ensemble Tree Learning (AETL) is a special machine learning method used in our proposed intrusion detection system to classify nodes into two classes: malicious and normal. This work discusses several forms of attacks in MANET: black hole attack, cooperative black hole, grey hole attack, wormhole attack, Sybil attack, and jellyfish attack. The proposed method tries to detect attacks in mobile ad hoc networks by keeping track of unequal utilization of the transmission channel.

Attack typical behaviors according to [34] are Active Time Deviation (forcing a node to exhaust its battery), Malicious Flooding (sending a huge amount of control packets either within the network or directed to the target nodes), and Disregarding the MAC protocol, which is the case when a noncompliant node generates RTS/CTS at an inappropriate frequency so that it does not play with the backoff mechanism and blocks the surrounding nodes from having fair access to the transmission channel.

The three main aspects of many attacks contribute to increased energy consumption from Active Time Deviation, increased routing overhead due to malicious flooding, and decreased packet delivery ratio due to neglect of the MAC protocol. At the stage of network acquisition, we could evaluate the three main characteristics, namely energy consumption, routing, overhead, and packet delivery ratio for every node. In AETL, we included bagging and boosting techniques on the decision tree classifier. An ensemble learning approach is used first to find the fundamental models to be merged. A single basic learning algorithm is used, usually integrating the most frequently used bagging and boosting techniques, resulting in homogeneous weak learners being taught in different ways [35].

$X, Y, \hat{Y}$ are random variables describing the distribution of values for instances x, and their ground truth and predicted values f(x) and h(x). $h(X)$is an estimator (hypothesis) of the true(unknown) function$f(X)$, which is generated by some model Y as given by,

$$Y = f(X) + \varepsilon \; y \in Y \quad (5)$$

If the ensemble method is optimized as boosting, the AdaBoost classifier is utilized, while bagging refers to using the random forest classifier [41]. Assume that the cost of classification for a classifier with Z features is,

$$Cost_L = weight \times Z + bias \quad (6)$$

The algorithm of AETL is described in Algorithm 1 below.

3.3. Recovery of Compromised Nodes

An area of the recovery process will commence should the database not meet security standards. As less than 10–15% of the nodes are impacted, the program loaded recovery method is used. Next, we fix all compromised nodes by restoring the software on each compromised node so they return quickly. Quickly, we should repair the nodes that were compromised.

This allows us to update the deviations by comparing the current block picture with the previous block picture. When it detects a failure, the AETL sends a fetch checkpoint message that triggers the state's recovery.

A Fetch Checkpoint Reply [36] contains the most recent database checkpoint. The disk and database in this control will restore the base station's most recent image under AETL. The procedure allows any false or corrupted data to be removed.

3.4. Clustering and Leading Agent Selection using HDOMLM

In this cluster head selection algorithm, we optimise cluster formation and LAn selection using PSO and O-MLM, respectively. The workflow of HDOMLM is shown in Figure 2.

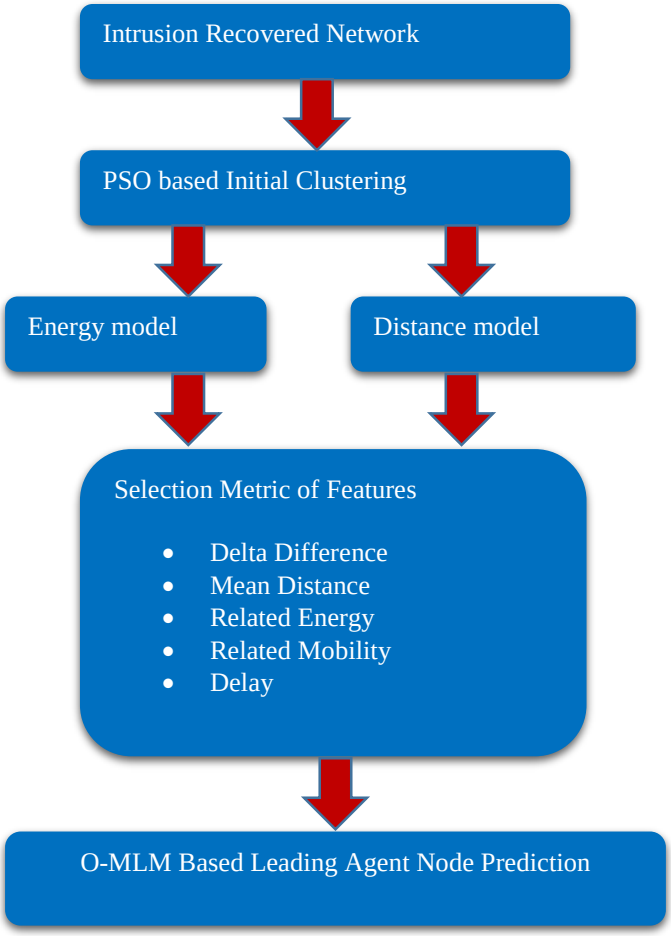

Fig. 2 HDOMLM based cluster head selection

Algorithm 1: Adaptive Ensemble Tree Learning (AETL)

Input: Data for training, Features f_1, f_2, f_3Number of layers, False Positive Rate μ. Maximum iteration I_{max}number of folds N_{fold}

Output: AETL learned model

- ✓ Perform linear regression using the algorithm of least-squares for the validation database, then predict the results of β_1 and β_2 With reference to a fitting algorithm.
- ✓ The features of the layers f_1, f_2, f_3 are calculate.
- ✓ $for\ iterations\ = 1\ to\ I_{max}\ do$
  - Randomly permute the actual dataset
  - $for\ j\ = 1\ to\ N_{fold}\ do$
    - ➢ Extract the training subset from an overall dataset.
    - ➢ Recursively train the left and right subtrees of the binary tree to obtain the AETL model.
    - ➢ Exploit $AETL$ to conduct analysis on several subsets and compute the AUC values and F-measures
  - end
- ✓ end

The aim is to reduce the average distance between member nodes of the cluster so that the fitness value of the particle is set to F_c To make the distance of the member nodes between the cluster average small. The particle's fitness value is determined by calculation,

$$F_c = \frac{\sum_{j=1}^{n} d(i,j)}{n} \quad (7)$$

One of the basic features of this Optimized Machine Learning Model (O-MLM) supports the generation of selection metrics as a feature for the machine learning model. The elements applied to the learning model are delta difference, average distance, related energy, related mobility, and average transmission delay.

These measurements were developed as shown in Table 2. So, in this paper, we have classified nodes (conventional nodes or Leading Agent nodes, i.e., LAns) using Machine Learning (ML) in Mobile Ad Hoc Networks (MANETs), thus providing a novel approach to clustering in MANETS. It is classified as per certain criteria applied as a feature.

High classification accuracy can be produced using machine learning methods such as Support Vector Machines (SVM), decision trees, neural networks, ensemble learning, etc., using K Nearest Neighbors (KNN), naïve Bayes, etc. The O-MLM model has been used. This approach specifies that an ML model is chosen by tweaking hyperparameters such that the classification accuracy is maximized without loss [37]. Given the different ML models available for being employed and depending on the chosen machine learning model and matching hyperparameters, the O-MLM technique will choose one for training the process.

The system uses Bayesian optimization to select models and the associated hyperparameter values. For each model, the cross-validation classification error is computed. Once the optimization process is finished, we will show the model we have learned on the whole dataset and try to predict new data.

3.5. GALO-based Multi-Path Routing

In this work, the routing algorithm is developed based on estimating the optimal Path between the sender and destination node using trust parameter values. To select the best route from available options, the Genetic-Based Lion Optimization Algorithm (GALO) is used. The routing process consists of three main phases: route establishment, trust computation, and optimal route estimation. The standard Ad Hoc on Demand Distance Vector (AODV) routing protocol is used in the route establishment phase to find multiple paths between the source and destination.

For each route in the network, the trust metrics are computed for each node [38, 39]. Last, GALO is applied to find an optimal route out of all possible routes.

3.5.1. Route Establishment Phase

Once data transmission is established from the sender node to the desired node, the source node sends a 'Route Request' (RREQ) broadcast message to its neighboring nodes of the MANET. These neighboring nodes send back RREP to the sender that they received RREQ from. The result of this process is the potential creation of multiple routes for the source and destination nodes to communicate. It uses a route establishment process similar to the Ad hoc On-Demand Distance Vector routing (AODV). Then the nodes in the considered route compute metrics and select the best route according to the chosen metrics.

Table 2. O-MLM features of decision metrics

O-MLM Feature Types	Expression	Remarks
Delta difference Δ_d	$\Delta_d = \frac{\lvert I_\theta - N_\theta \rvert}{360}$ (8)	I_θ is ideal degree of the nodes in MANET set as 45° and N_θ is individual nodes's mobility degree from RWP model.
Average distance A_d	$A_d = \frac{\sum_{m=1}^{M} D_m}{M}$ (9)	M is the aggregate count of neighboring nodes inside the respective cluster and D_m is distance in the middle of neighbor node and LAn of the same cluster.
Related energy E_R	$E_R = \frac{Q_{energy}}{P_{energy}}$ (10)	$Q_{energy} = \sum_{j=1}^{K} \Phi_{E,j}$ (11) $\Phi_{E,j} = \sum_{i=1}^{M} (1 - [E_i - E_{C,j}])$ (12) $P_{energy} = K * \max_{i=1:M} E_i * \max_{j=1:K} E_{c,j}$ (13) K represents the number of clusters in the network
Related mobility M_R	$M_R = \frac{Q_{mobility}}{P_{mobility}}$ (14)	$Q_{mobility} = \sum_{i=1}^{M} \sum_{j=1}^{K} \lVert DLA_{j,i} \rVert + \lVert LAB_j \rVert$ (15) $P_{mobility} = \sum_{i=1}^{M} \sum_{j=1}^{K} \lVert d_{i,j} \rVert$ (16) The variable $DLA_{j,i}$ represents the distance between the i-th member node and the j-th leading agent and LAB_j is the distance in the middle of j-th leading agent node to BS. $d_{i,j}$ is the distance between to member nodes in each cluster.
Average delay $Delay_j$	$Delay_j = \frac{\max_{i=1\ to\ M} \tau_{i,j}}{M}$ (17)	$\tau_{i,j}$ is the maximum delay of all i-th member nodes in the j-th cluster.

3.5.2. Trust Metric Computation Phase

The Selection of backup energy nodes, packet delivery rate, and queue length in a network are greatly influenced by the trust scheme metrics. The availability of backup Energy in network nodes is one of the factors improving network lifetime. As the nodes have sufficient energy levels, they can efficiently offer services. On the contrary, the lifespan for nodes with lower energy is also shorter. If there is a node in the route that is very low in energy, then this route will fail and cause congestion or packet loss. Thus, it is necessary to evaluate trust metrics.

Another important trust metric, packet delivery rate, is based on incoming and outgoing packets at each node. A node is deemed reliable if it matches its incoming and outgoing messages so that data is effectively delivered. Finally, we estimate the message queue length at each node to reflect the queuing delay of the algorithm at a node, where longer queues suggest longer wait times and higher latency, which in turn results in degradation of the routing algorithm performance. Excessive messages can also cause congestion. In particular, this paper deals with backup Energy, packet delivery rate, and node queue length in certain routes.

This paper uses these metrics to determine the shortest Path in the network. Someone choosing message routes based on the shortest Path and seemingly relatively 'safe' nodes would cause congestion and latencies. Hence, this paper focuses on selecting the trust metrics to set up reliable routes and energy-efficient communication [40, 41].

Each deployed node in a Mobile Ad-hoc Network (MANET) has an initial energy level ranging from 0 to 1. The full energy level is represented by 1, and no energy level is represented by 0. Partial energy levels, like half or a quarter, have values between 0 and 1. The packet delivery rate, the ratio between incoming and outgoing messages, is also computed for each node.

In this case, nodes that forward all incoming messages are called fully trustworthy. However, if a node forwards just half of the incoming messages, this node could be termed selfish or malicious. They consider the nodes that forward reliable messages; they are treated as trusted, and thus, they contribute to finding the shortest and most efficient route within the network. The assigned delivery rates to the nodes of the network are shown in Table 3.

The parameter estimated for outgoing packets is denoted using φ in Table 3, and τ does the same for incoming packets. The values of each node are computed. If a node forwards all or none of its messages, it is assigned 1 or 0. The value between 0 and 1 denotes the intention at which a node forwards data. In that case, nodes with a higher message forwarding ability are chosen to improve their reliability.

Table 3. PDR assignment in trust computation

PDR Value	Node type
0	$\emptyset = 0$
0.5	$\emptyset = \tau/2$
0.75	$\emptyset = 4\tau/3$
1	$\emptyset = \tau$

The node Queue Length is finally computed by dividing the message queue length by the node route, and it is denoted as,

$$QL = \frac{M_C}{TN_R} \tag{18}$$

The normalized queue length (QL) for the computed values is determined by,

$$QL_N = \frac{(QL - o_l) \times (n_h - n_l)}{o_h - o_l} \tag{19}$$

where o_h is the highest node Queue length and o_l This work considers the lowest queue length of a node, respectively. n_h & n_l Are the normalized high and low Queue ranges with the values of 1-0, correspondingly?

The overall trust metric is computed as,

$$T_C = \sum_{i=1}^{N} \frac{E + PDR + QL}{3} \tag{20}$$

The GALO algorithm utilizes these computed trust metrics of nodes to pick the optimal route out of the available routes in the network. In this GALO, three implementation phases occur: detection of routes, Selection of optimal routes, and congestion control. The detection of routes is described in Algorithm 2.

Algorithm 2: Detection of route and computation of trust metric

Input: Adhoc Nodes Data Gathered
Output: Predicted Routes

For every source node in the network
  Broadcast the message RREQ to neighborhood nodes in the network.
  Receive the RREP in the nodes.
  Detect all available routes in the network between the source and destination;
End for

For every returned route in the network
Do
Compute T_c By eqn. 20 for every route in the node;
Save T_c;
End do
End for

3.5.3. Optimal Route Selection

The GALO algorithm chooses the best accessible connection from all routes that exist between a starting point and a destination. A biological routing process that operates similarly to lions enables it to simulate these group formations using Lion Optimization (LO).

A lion pride includes two types of members: resident adults and nomadic adults, and between four and five cubs. The development of young lions leads their pride to force their departure, turning them into roaming animals. Nomadic young lions reside close to their pride territory yet occasionally consider striking against the area. To work together, the LO algorithm distributes its population into two groups, including resident pride members and nomadic members. The algorithm computes how many nomadic lions exist while controlling specific regions of the pride.

The algorithm regulates gender proportion but focuses on hunting abilities to develop optimal solutions by determining the fitness values of nomadic lions. The fitness evaluation determines both a pride membership selection among hopeful lions and new calculations for fitness-based eligibility within the existing pride, where uncompetitive lions lose their position. The algorithm completes its process once it discovers the best possible solution. The fitness function of LO is defined for the route selection problem as,

$$F_v = \sum_{i=1}^{N} \frac{\left(T_{c_1}, T_{c_2}, \ldots T_{c_N}\right)}{N} \quad (21)$$

The Lion Optimization (LO) algorithm performs route selection by evaluating the fitness function of Equation (21). The solution technique targets both reliable performance and energy-efficient communication, along with optimal results. The LO-based route selection is mentioned in Algorithm 3.

Algorithm 3: Selection of Optimal Route using LO

Input: Predicted routes from algorithm 1
Output: Optimal Secured Route

For every lion, those are the residents
  Do
  Randomly selects the lions for the hunting process
  Compute the lion fitness function using Equation (21)
  Evaluate the fitness value in ascending order
  Eliminate the least valuable of the lions as F_v
  End do;
End for;

For every nomadic lion
  Follow a similar process to resident lions;
  Compute Fv,
    If (F_v (nomadic lion) $< F_v$ (resident lion)
      Include the lion pride in the group.
      Eliminate the minimal F_v of the lions;
      Compare the swap and solution values necessary.
      Store the best solution
    End if
  End for

Congestion Control

In this work, congestion control is implemented using the GA algorithm. The three elements are considered for the fitness in congestion control of selected optimal routes using Genetic algorithm-based optimization of energy, distance, and queue length. The fitness function of the congestion-controlled route in GA is represented as,

$$F_{GA} = \frac{(F_e + F_d + F_L)}{3} \quad (22)$$

$$F_e = \frac{S_{RE}}{D_{RE}} \quad (23)$$

$$F_d = \frac{D_{n,n}}{D_{s,d}} \quad (24)$$

$$F_L = (RTT - T_{min}) * \Upsilon \quad (25)$$

where, S_{RE} is the residual energy of the source node and D_{RE} is the residual energy of the destination node, $D_{n,n}$ is the intra-node link distance and $D_{s,d}$ The link distance between source and destination nodes, RTT, is the trip time, and T_{min} is the minimum round-trip time, and Υ is the Bandwidth of the transmission.

The congestion evaluation depends on TCP Congestion Control Enhancement for Random Loss (CERL). The TCP sender employs T as the minimum Round Trip Time value recorded, and L represents the current RTT measurement that includes updates from received packets. The CERL queue length F_L Serves as the basis to check link congestion by Eq. (25). The dynamic queue length threshold, which is represented as Q_n is given by,

$$Q_n = A * L_{\max} \quad (26)$$

The transmitter records the maximum observed F_L value as $L_{\max}$ while the constant factor A lies within the range of 0 to 1. Network congestion evaluation under the proposed CERL happens through F_L and Q_n Variables. The condition where F_{GA} oversteps Q_n Points to network congestion across different nodes. The optimal route calculation requires the removal of this pathway since additional packet drops would occur through it. A route with F_{GA} values between 0 and Q_n It will be incorporated into evaluating potential best routes for fitness function calculations. Any random packet drop on this route minimises the impact on fitness evaluation and congestion window size because it does not affect network throughput. The effectiveness judgment for routes in CERL

depends on maintaining accurate constants from F_{GA} and Q_n Together with derived inequalities based on these constants. Correctly evaluating BW as a critical factor enables CERL to pinpoint its most effective communication pathways.

4. Results And Discussion

This section presents the performance evaluation of the proposed GALO for multi Path routing with security awareness in MANET with intrusion avoidance-based clustering using AETL+HDOMLM. The simulation environment we used is MATLAB version R2022a. The network is configured with a 350mx350m area, and the number of nodes ranges from 50 to 400. The mobility of MANET nodes is defined with a speed of 20 ms^{-1}.

Out of the nodes in the network, 10% will be leading agents while clustering, and 20% will be intrusion nodes. For training of AETL, the number of scenarios with different node configurations is considered, and the generated database in the dimension of 5000 has three attributes of energy, routing overhead, and PDR. For HDOMLM learning database creation, the 5000 different nodes' data is aggregated with five decision metrics of delta difference, related energy, related mobility, average Delay, and average distance. The optimization methods of PSO with 100 iterations, 50 populations, local and global learning coefficients of 1.5, and an inertia weight of 0.8.

4.1. Performance of Network Lifetime, Energy, Throughput and Delay

Figure 3 shows the network topology of the number of nodes with the indication of source and destination. For this network, how the routing is performed is analyzed in the following sections. Figure 4 illustrates the predicted Path using the optimization of the GALO with security concerns in multi-path routing. This figure highlights the source and destination as black circle markers and the predicted Path as green connective lines. The intermediate relay nodes are shown as red colored triangle markers.

Figure 5 depicts the performance network lifetime with the evaluations of the number of alive nodes in each round of execution. Conventionally, as the number of rounds increases, the energy exhaustion in each node will be greater and wash out the node's lifetime. Hence, the number of alive nodes will decrease as the number of rounds increases, as shown in Figure 5. Compared with other existing implementations of ANFIS-EESC, CCCH, our proposed algorithms provide a higher network lifetime, as shown in Figure 5 with malicious presence and absence. Without considering the malicious, the HDOMLM-based clustering and CH selection provide the network lifetime with more than 900 rounds.

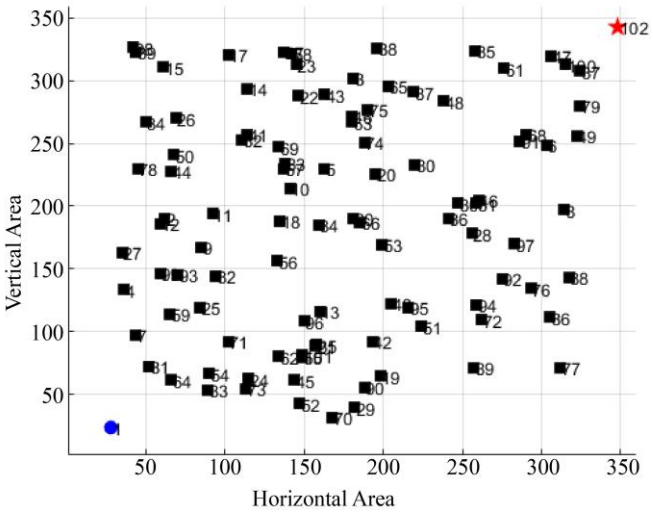

Fig. 3 Network formation with source and destination

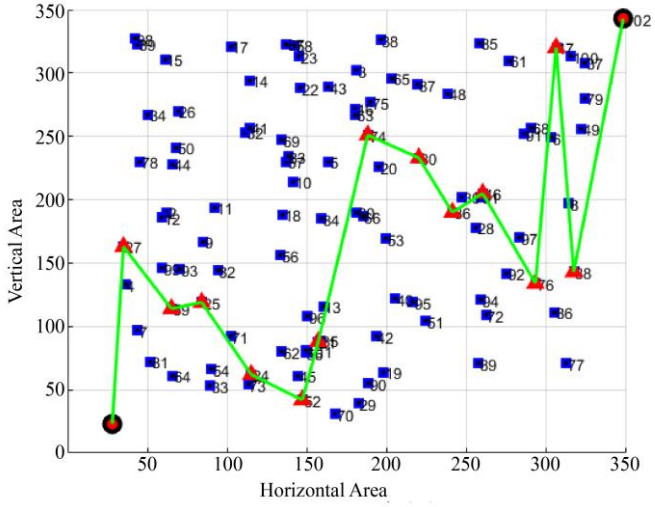

Fig. 4 The detected optimal path using the proposed GALO

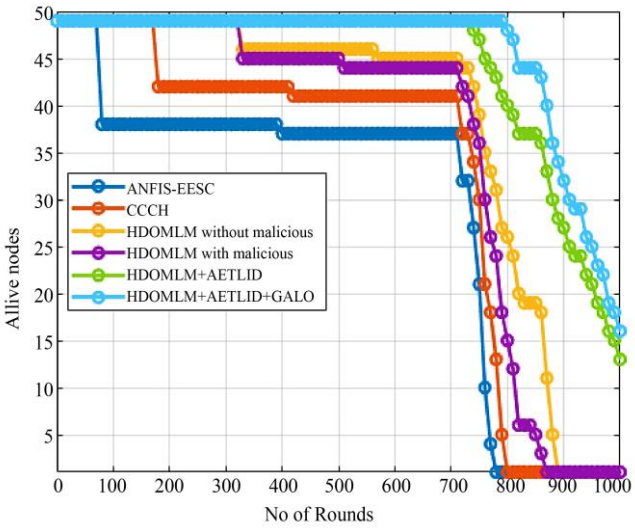

Fig. 5 Network lifetime comparison for nodes of 50

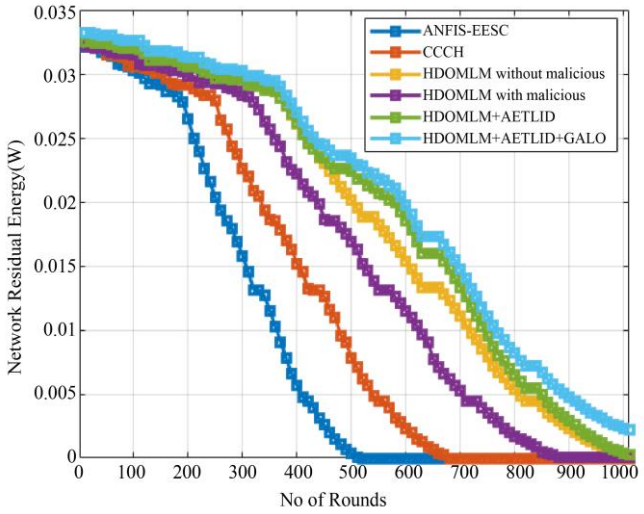

Fig. 6 Network residual energy Vs Number of rounds with nodes 50

For the same methodology of HDOMLM, involved with intrusion attacks, it degraded to less than 900 rounds. When intrusion avoidance using AETL is integrated with the HDOMLM, the performance is improved and it does not attain the zero energy nodes at rounds of 1000; it has alive nodes of 13. In this work, the improvement of AETL+HDOMLM is further enhanced using GALO. At the round of 1000, the alive nodes will be 17.

As the number of rounds increases, the energy must be reduced due to a number of processes like transmission, reception, data gathering, node association, routing, and intrusion avoidance. The energy performance of the proposed system is shown in Figure 6. The complete energy is dropped as these processes are repeated for a number of rounds, and with the ANFIS-EESC algorithm, it is achieved with 500 rounds. In our proposed model of HDOMLM+AETL+GALO, the nil energy is not attained, and still, some energy of 0.0023W is presented as shown in Figure 6.

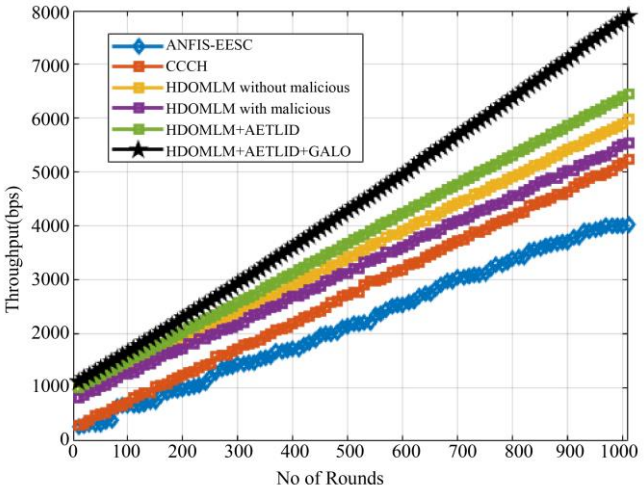

Fig. 7 Throughput Vs Number of rounds with nodes 50

Figure 7 shows the system's throughput with 50 nodes in the network. As the number of rounds in the processing of routing increases, the throughput will increase as the packets transmitted increases in each communication slot. From Figure 7, it is clearly shown that compared to the earlier implementation of ANFIS-EESC, CCCH, our proposed models of only HDOMLM, HDOMLM+AETL, and HDOMLM+AETL+GALO achieved the best throughput of more than 5Kbps. Applying efficient ETPA routing into the MANET network improves the throughput to 8Kbps, 38% and 19% higher than HDOMLM and HDOMLM+AETL, respectively.

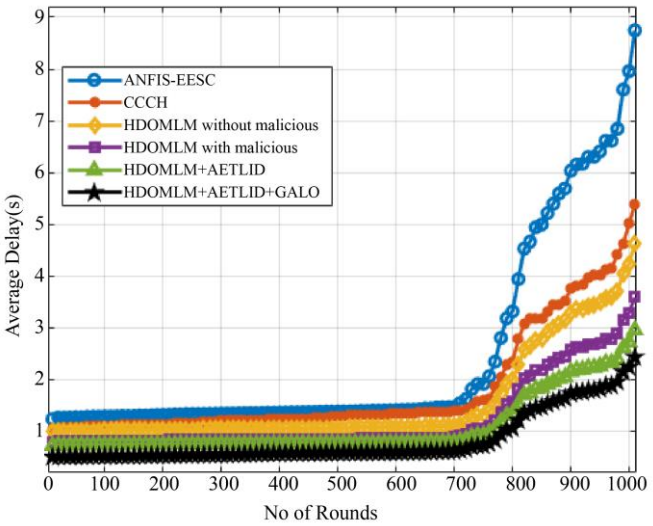

Fig 8. Average delay for the number of nodes of 50

Figure 8 illustrates the average Delay performance for each round of the process with network nodes 50. Delay is increased as the number of rounds increases, as shown in Figure 8. Up to the round of 700, the Delay is gradually increasing. After that round, it suddenly increased with high Delay for all the methods. This scenario occurs due to the fact that with an increased number of rounds, the number of alive nodes will be reduced. Hence, the search for CH nodes and route prediction will take some more time than the search for the higher available nodes. Nearly 9s if the Delay is obtained from the ANFIS-EESC algorithm, which is 4 times higher than our proposed method, HDOMLM+AETL+GALO.

4.2. Performance Evaluations for Scalability Measure

The performance of the network lifetime with an increasing number of nodes from 50 to 400 is shown in Figure 9. In this evaluation, the number of alive nodes increases as the network nodes increases. The proposed model of HDOMLM+AETL+GALO attains significantly higher alive nodes than other methodologies, as shown in Figure 9. The scalability of nodes in the network is highly impacted in real-time scenarios, and it is proven using our proposed models of HDOMLM+AETL+GALO.

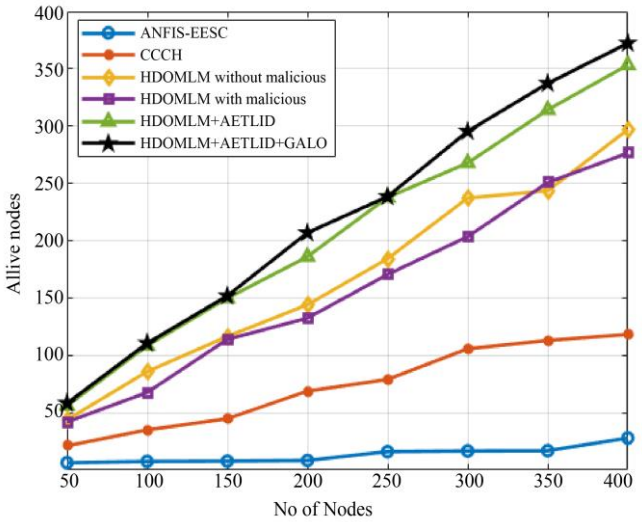

Fig. 9 Network lifetime comparison for nodes 50-400

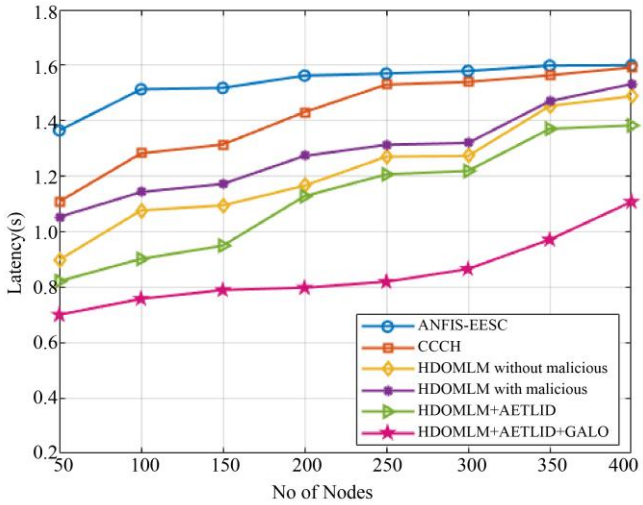

Fig. 10 Scalability analysis for latency

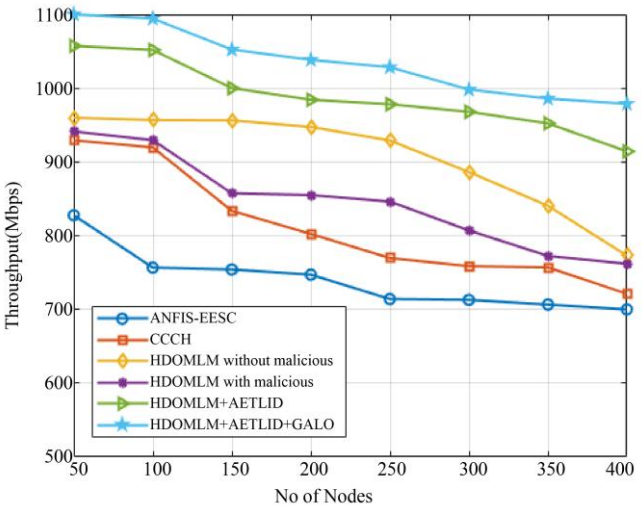

Fig. 11 Scalability analysis for throughput

In Figure 12, the latency performance is shown as a function of the number of nodes. With effective proposed ETPA multi-path routing, the prediction of paths between source and destination is reduced to 0.7s in HDOMLM+AETL+GALO, which is 13%, 30%, 37%, and 47% less than HDOMLM+AETL, only HDOMLM, CCCH and ANFIS-EESC, respectively.

Figure 13 depicts the scalability performance through evaluations. As the number of nodes increases, the throughput decreases due to high intermediate communications and losses of packets between each relay communication.

The proposed ETPA method achieved a high throughput of 1100 Mbps at a 50 50-node configuration, which is 5%, 15%, 16% and 25% higher than HDOMLM+AETL, only HDOMLM, CCCH and ANFIS-EESC, respectively.

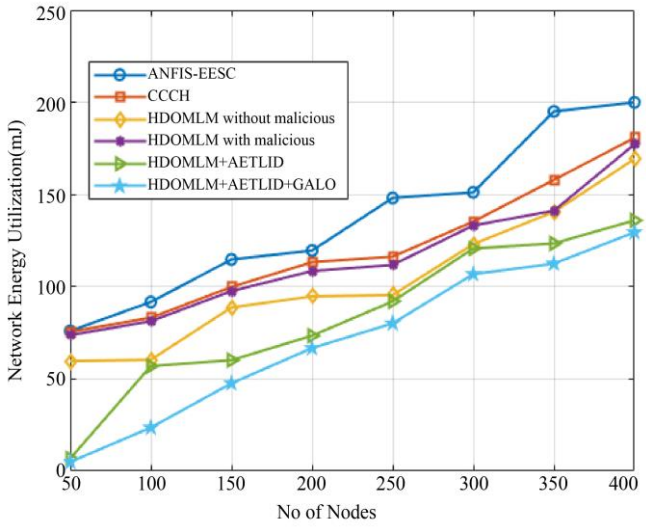

Fig. 12 Scalability analysis for network energy utilization

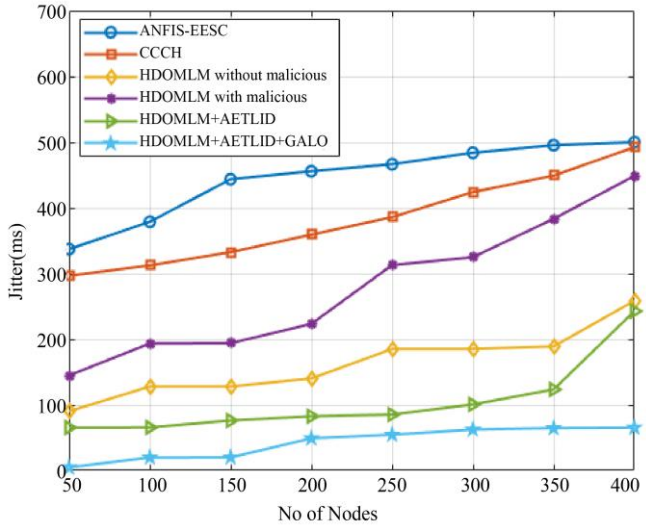

Fig. 13 Scalability analysis for jitter

Figure 12 shows the performance of the network energy utilization as the number of nodes increases from 50 to 400. In the Energy efficient system, the network energy utilization will be low. The same we achieved using our proposed model of ETPA of 129.51mJ, and it is 6.97mJ, 40.71mJ, 51.36mJ, and 69.22mJ less than HDOMLM+AETL, only HDOMLM, CCCH, and ANFIS-EESC, respectively. In Figure 13, the jitter performance for different numbers of nodes in the network is shown. As the number of nodes increases, the Jitter will increase. The arrival time deviation increases while the number of nodes increases, as shown in Figure 13. All methods in Figure 13 show the minimal Jitter at nodes of 50, and it increased to high ranges from 500ms to 50ms for ANFIS-EESC and proposed HDOMLM+AETL+GALO, respectively.

4.3. Performance Evaluations for Reliability Measure

In this section, the reliability of the proposed system is compared with various aspects of MANET design. Table 4 provides the performance evaluations of reliability regarding different intrusions, MANET mobility, and node density rates.

The QoS value is evaluated for these scenarios and compared with our proposed models. ETPA provides a higher QoS in three different aspects and six parameter settings than the other two methods.

Table 4. QoS performance for different scenarios of the network

Methods		HDOMLM+ AETLID + GALO	HDOMLM + AETLID	HDOMLM
Attacker Rate	<15%	0.9091	0.8849	0.8471
	>15% & <50%	0.6937	0.6512	0.5887
Nodes Mobility	Low speed (20m/s)	0.9102	0.8917	0.7945
	High speed (200m/s)	0.7361	0.7083	0.6523
Nodes Density	Nodes=50	0.9388	0.9141	0.9013
	Nodes=500	0.9059	0.8764	0.8436

5. Conclusion

This work proposes a new routing system for MANET based on a Genetic Algorithm based on Lion Optimization (GALO) to be more efficient with regard to energy consumption, enhance the data flow, and address privacy issues. Security is guaranteed over the phases of route discovery and maintenance over the proposed routing system. To do this, we refined the GALO into an optimal result. Introducing a new objective function aids in equilibrating the load over the network and enhances its performance. Using the GALO protocol reduces the routing-security interdependent loop, and the protocol is low in complexity and efficient. A strong contribution of the work here is the integration of intrusion prevention mechanisms within the Adaptive Ensemble Tree Learning (AETL) and Hybrid Dual Optimization Machine Learning (HDOMLM) models during the clustering process. That will help with path prediction, reduce energy usage, improve throughput, and provide more security. Simulation reveals that the system resists localized assaults by malicious nodes who may insert false certificates. It also shows efficacy in cooperative virus attack when some nodes already have a high level of trust before the network construction. Other real-time situations will be combined with the future deep learning model to improve system interoperability.

References

[1] R. Shanmugavalli et al., "Energy Aware Routing Mechanism Using AODV Protocol For Low Energy Consumption in WSN," *2023 IEEE 5th International Conference on Cybernetics, Cognition and Machine Learning Applications*, Hamburg, Germany, pp. 242-247, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[2] R.O. Raji, and A.M. Oyelakin, "Approaches for Solving Routing and Security Issues in Mobile Ad-Hoc Networks (Manets): A Review," *Journal of Information Technology and Computing*, vol. 4, no. 2, pp. 20-30, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Nitesh Ghodichor et al., "Secure Routing Protocol to Mitigate Attacks by Using Blockchain Technology in MANET," *International Journal of Computer Networks & Communications*, vol. 15, no. 2, pp. 127-146, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[4] Suraj Patel, "Performance Analysis of Routing Protocols in Mobile Ad-hoc Networks (MANETs) Using NS2: A Comparative Study of AODV, DSR, and DSDV," *International Journal of Scientific Research in Engineering and Management*, vol. 8, no. 9, pp. 1-7, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Tao Hai et al., "Enhanced Security Using Multiple Paths Routine Scheme in Cloud-MANETs," *Journal of Cloud Computing*, vol. 12, pp. 1-23, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[6] Y.M. Mahaboob John, and G. Ravi, "Cooperative Self-Scheduling Secure Routing Protocol for Efficient Communication in MANET," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 4S, pp. 232-241, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[7] Lavanya Nagichetty Lakshminarayana, Shashi Rekha Gangadharaiah, and Madhushree, "Trust Based Multi Objective-Pelican Optimization Algorithm for Mobile Ad Hoc Networks," *International Journal of Intelligent Engineering & Systems*, vol. 16, no. 6, pp. 590-599, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] KDV Prasad et al., "A Novel Method of Enhancing Security Solutions and Energy Efficiency of IoT Protocols," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 4S, pp. 325-335, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[9] Uma Maheswari Arumugam, and Suganthi Perumal, "Trust Based Secure and Reliable Routing Protocol of Military Communication on MANETs," *Journal of Machine and Computing*, vol. 3, no. 1, pp. 47-57, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ali Alzahrani, and Nigel Thomas, "Analysing the Performance of a Trust-Based AODV in the Presence of a Flooding Attack," *Applied Sciences*, vol. 14, no. 7, pp. 1-16, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Vasantha Kumara Mahadevachar, and Naveen Thimmahanumaiah Hosur, "Metaheuristic Based Energy Efficient Routing Protocol in MANET Using Battle Royale Optimization," *International Journal of Intelligent Engineering & Systems*, vol. 16, no. 4, pp. 1-11, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Satyanand Singh, Joanna Rosak-Szyrocka, and Balí zs Lukí cs, "Design and Analysis of a Bandwidth Aware Adaptive Multipath N-Channel Routing Protocol for 5G Internet of Things (IoT)," *Emerging Science Journal*, vol. 8, no. 1, pp. 251-269, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Manikandan Rajagopal et al., "Minimizing Energy Depletion Using Extended Lifespan: QoS Satisfied Multiple Learned Rate (ELQSSM-ML) for Increased Lifespan of Mobile Adhoc Networks (MANET)," *Information*, vol. 14, no. 4, pp. 1-14, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Priyanka Kaushik, "Congestion Articulation Control Using Machine Learning Technique," *Amity Journal of Professional Practices*, vol. 3, no. 1, pp. 1-7, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Qahtan M. Yas, and Abdulbasi Alazzawi, "Integrating Intelligent Systems in MANET-IoT Environment Based on Subjective Context," *Iraqi Journal for Computer Science and Mathematics*, vol. 5, no. 2, pp. 26-35, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Raneen I. Al-Essa, and Ghaida A. Al-Suhail, "AFB-GPSR: Adaptive Beaconing Strategy Based on Fuzzy Logic Scheme for Geographical Routing in a Mobile Ad Hoc Network (MANET)," *Computation*, vol. 11, no. 9, pp. 1-27, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] H.K. Sampada, and K.R. Shobha, "Co-Ordinated Blackhole and Grayhole Attack Detection Using Smart & Secure Ad Hoc On Demand Distance Vector Routing Protocol in MANETs," *International Journal of Computer Networks and Applications*, vol. 11, no. 1, pp. 13-28, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Nikitina Vlada et al., "Enhancing Security in Mobile Ad Hoc Networks: Enhanced Particle Swarm Optimization-driven Intrusion Detection and Secure Routing Algorithm," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 14, no. 3, pp. 77-88, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[19] Anita R. Patil, and Gautam M. Borkar, "Node Authentication and Encrypted Data Transmission in Mobile Ad Hoc Network Using the Swarm Intelligence-Based Secure Ad-Hoc on-Demand Distance Vector Algorithm," *IET Wireless Sensor Systems*, vol. 13, no. 6, pp. 201-215, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[20] Jayantkumar A. Rathod, and Manjunath Kotari, "TriChain: Kangaroo-Based Intrusion Detection for Secure Multipath Route Discovery and Route Maintenance in MANET Using Advanced Routing Protocol," *International Journal of Computer Networks and Applications*, vol. 11, no. 1, pp. 61-81, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[21] Veeramani Ramasamy, Madhan Mohan Ramalingam, and Mahesh Chitraivel, "Energy Efficient Secured-Quality of Service Routing Protocol for Mobile Ad Hoc Network Using Multi-Objective Optimization," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, pp. 1486-1495, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Khaled Ahmed Abood Omer, "Impact of Jellyfish Attack on Routing Protocols in TCP-Based MANETs," *University of Aden Journal of Natural and Applied Sciences*, vol. 27, no. 1, pp. 139-150, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[23] Versha Matre, and Pradnya A. Vikhar, "Trust-Based Routing Selection Policy on Mobile Ad-Hoc Network Using Aodv Routing Protocol," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 9, pp. 4575-4580, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[24] G.R. Rama Devi, M. Swamy Das, and M.V. Ramana Murthy, "Secure Cross-Layer Routing Protocol with Authentication Key Management Scheme for Manets," *Measurement: Sensors*, vol. 29, pp. 1-9, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[25] V. Anjana Devi et al., "An Energy Efficient Routing Establishment (EERE) Mechanism for MANET-IoT Security," *Franklin Open*, vol. 8, pp. 1-10, 2024 [CrossRef] [Google Scholar] [Publisher Link]

[26] S. Agnes Shifani et al., "MANET: A Secured and Logical Routing Protocol Development over Mobile AdHoc Networks for Intelligent Data Communication," *2024 5th International Conference on Electronics and Sustainable Communication Systems*, Coimbatore, India, pp. 741-748, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[27] Mohamad T. Sultan, Hesham El Sayed, and Manzoor Ahmed Khan, "An Intrusion Detection Mechanism for Manets Based on Deep Learning Artificial Neural Networks (Anns)," *International Journal of Computer Networks & Communications*, vol. 15, no. 1, pp. 1-15, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[28] S. Mohan, and P. Vimala, "Enhancing Congestion Control and QoS Scheduling Using Novel Rate Aware-Neuro-Fuzzy Algorithm in MANET," *Wseas Transactions on Communications*, vol. 22, pp. 58-74, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[29] Shridhar Sanshi, N. Karthik, and Ramesh Vatambeti, "IoT Energy Efficiency Routing Protocol Using FHO-Based Clustering and Improved CSO Model-Based Routing in MANET," *International Journal of Communication Systems*, vol. 37, no. 9, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[30] Vinoth Kumar Krishnamoorthy et al., "Energy Saving Optimization Technique-Based Routing Protocol in Mobile Ad-Hoc Network with IoT Environment," *Energies*, vol. 16, no. 3, pp. 1-16, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[31] R. Praba et al., "Enhanced Hybrid Routing Protocol for Energy-Efficient Multipath Routing in Manets," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 10, no. 3, pp. 619-623, 2024. [CrossRef] [Publisher Link]

[32] Yi Jiang, Hui Sun, and Muyan Yang, "AODV-EOCW: An Energy-Optimized Combined Weighting AODV Protocol for Mobile Ad Hoc Networks," *Sensors*, vol. 23, no. 15, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[33] Tribhuvan Singh et al., "Data Clustering Using Moth-Flame Optimization Algorithm," *Sensors*, vol. 21, no. 12, pp. 1-19. [CrossRef] [Google Scholar] [Publisher Link]

[34] Mohamed Elhoseny, and K. Shankar, "Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique," *IEEE Transactions on Reliability*, vol. 69, no. 3, pp. 1077-1086, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[35] Uppalapati Srilakshmi et al., "An Improved Hybrid Secure Multipath Routing Protocol for MANET," *IEEE Access*, vol. 9, pp. 163043-163053, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[36] Neenavath Veeraiah et al., "Trust Aware Secure Energy Efficient Hybrid Protocol for MANET," *IEEE Access*, vol. 9, pp. 120996-121005, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[37] L. Ellen Funderburg, and Im-Yeong Lee, "A Privacy-Preserving Key Management Scheme with Support for Sybil Attack Detection in VANETs," *Sensors*, vol. 21, no. 4, pp. 1-17, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[38] K. Vinoth Kumar et al., "SDARP: Security Based Data Aware Routing Protocol for Ad Hoc Sensor Networks," *International Journal of Intelligent Networks*, vol. 1, pp. 36-42, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[39] Thippaluru Umamaheswari, and Y. Murali Mohan Babu, "ViT-MAENB7: An Innovative Breast Cancer Diagnosis Model from 3D Mammograms Using Advanced Segmentation and Classification Process," *Computer Methods and Programs in Biomedicine*, vol. 257, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[40] Jinghui Zhong et al., "A Hyper-Heuristic Framework for Lifetime Maximization in Wireless Sensor Networks with a Mobile Sink," *IEEE/CAA Journal of Automatica Sinica*, vol. 7, no. 1, pp. 223-236, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[41] D.V. Sai Kishore et al., "Fuzzy C-Means Based Medical Image Retrieval for Identifying Most Clinically Relevant Images," *Multimedia Tools and Applications*, vol. 83, pp. 55283-55303, 2024. [CrossRef] [Google Scholar] [Publisher Link]