Computers, Materials & Continua
DOI: 10.32604/cmc.2023.034773
Article

Tech Science Press

Enhanced Energy Efficient with a Trust Aware in MANET for Real-Time Applications

M. V. Narayana[1], Vadla Pradeep Kumar[2], Ashok Kumar Nanda[2,*], Hanumantha Rao Jalla[3] and Subba Reddy Chavva[4]

[1]Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad, Ranga Reddy District, Telangana, 501506, India
[2]Department of CSE, B V Raju Institute of Technology, Narsapur, Medak, Telangana, 502313, India
[3]Department of CSE, T.R.R. Government Degree College Kandukur, Kandukur, A.P., 523105, India
[4]Department of IT, VFST& Research (Deemed to be University), Vadlamudi, A.P., 522213, India
*Corresponding Author: Ashok Kumar Nanda. Email: ashokkumarnanda2022@gmail.com
Received: 27 July 2022; Accepted: 04 November 2022

Abstract: Mobile ad hoc networks (MANETs) are subjected to attack detection for transmitting and creating new messages or existing message modifications. The attacker on another node evaluates the forging activity in the message directly or indirectly. Every node sends short packets in a MANET environment with its identifier, location on the map, and time through beacons. The attackers on the network broadcast the warning message using faked coordinates, providing the appearance of a network collision. Similarly, MANET degrades the channel utilization performance. Performance highly affects network performance through security algorithms. This paper developed a trust management technique called Enhanced Beacon Trust Management with Hybrid Optimization (EBTM-Hyopt) for efficient cluster head selection and malicious node detection. It tries to build trust among connected nodes and may improve security by requiring every participating node to develop and distribute genuine, accurate, and trustworthy material across the network. Specifically, optimized cluster head election is done periodically to reduce and balance the energy consumption to improve the lifetime network. The cluster head election optimization is based on hybridizing Particle Swarm Optimization (PSO) and Gravitational Search Optimization Algorithm (GSOA) concepts to enable and ensure reliable routing. Simulation results show that the proposed EBTM-HYOPT outperforms the state-of-the-art trust model in terms of 297.99 kbps of throughput, 46.34% of PDR, 13% of energy consumption, 165.6 kbps of packet loss, 67.49% of end-to-end delay, and 16.34% of packet length.

Keywords: MANET; malicious nodes; clustering; trust management; beacon message

1 Introduction

A Mobile Ad-hoc Network (MANET) comprises self-governing wireless sensor nodes [1,2]. The MANET network does not require any particular infrastructure for the dynamic changes in the network. The designed model comprises the self-governance and infrastructure-less environment for the MANET boon and curse. On the other hand, the sensor nodes are self-governed with the requirements of the central government in the classic network and infrastructure–less network for the deployed network node without any arrangements. Conversely, MANET networks are subjected to various challenges due to their dynamic nature and mobility [3]. The MANET mobile nature generates a tougher routing process and consumes an extensive range of energy. Hence, the sensor node energy needs to be effectively utilized with a reasonable sensor lifetime.

The higher the sensor lifetime, the better the network performance is fulfilled. The MANET is also defined as the Wireless Sensor Network (WSN). The construction of the routing protocol is unsuitable for the MANET network, similar to the WSN. In the MANET network, the dynamic nature is unsuitable for the network topology and the active sensor node mobility pattern [4]. With a decrease in network reliability, the nature of mobile performance in MANET exhibits a significant advantage in various applications. The performance metrics have been highly affected by the network routing technique. For instance, packet transmission between source and destination reaches its destination without interference. However, in MANET, the data packet forwarding fails to reach the destination due to different techniques such as congestion, mobility, etc. Through improved network reliability, packet delivery rates are minimal for the latency. An efficient routing algorithm achieves a higher packet delivery rate [5]. The MANET routing protocol is divided into reactive, hybrid, and proactive. With the proactive routing protocol in the sensor node, the routing table is maintained, establishing the route between the senders and the destination node. On the other hand, the reactive routing protocol attempted to develop the routes actively engaged in the maintenance of the routing table [6]. The hybrid routing protocol integrates proactive and reactive routing protocols for optimal path establishment with high value, energy level, and distance.

In the network environment, the services are presented and configured ad hoc for information transmission. In the MANET environment, the infrastructure supports the susceptible wireless links to prevent attacks. Security leads to inherent weakness. For an ad hoc infrastructure to work well, the nomadic node environment must ensure that the radio link has common access. Secure communication between nodes is involved in providing a secure communication link between nodes [7]. With a secure communication link establishment between nodes, it needs to identify the node. The resultant node must provide the identity with the associated credentials between the nodes [8]. The node in the receiver questions the integrity of the authentication identity and credentials in the protected integrity for the delivery. Each compromised node is responsible for providing an effective identity for packet and recipient delivery. It is necessary to establish a secure architecture in the ad hoc network. Conventional attacks need to be evaluated with standard features classified into different attacks; those differences are minimal. The process can be categorized based on data traffic attack and control attack traffic. This involved the construction of a secure scheme for the broader categories and mitigation [9]. Through various attacks, MANET suffers. The following subsections classify different types of attacks [10]:

1. Denial of Service Attack: the most adverse effects of the MANETs are the types of attacks. The users exchange information jammed by the attacker of the main communication medium. The users cannot access the medium further because of this.
2. Distributed Denial of Service (DDOS) attack: these attacks are caused from various locations in distributed form by one attacker. Within different time durations, an attacker might transmit

the messages. There is a difference in the nature and the duration within which the message is to be transmitted based on the nodes presented by the attacker. This attacker's objective is the same as the DOS attack [11].

3. Sybil attack: The attacker transmits multiple messages. In every message in the network, several sources of identity are present. The attacker sends incorrect messages to nodes to confuse and jam the traffic. The nodes are forced to follow the next path to communicate with each other. Therefore, the attacker's primary objective is to forcefully choose another route to generate the illusion of multiple nodes.
4. Node Impersonation Attack: vehicular networks use a unique identifier to verify the messages. When any accident occurs, the wrong messages are sent to various nodes [12].
5. Application Attack: Various applications are attacked mainly by the attacker in this type of attack of information relevant to safety and non-safety. With the help of safety applications, warning messages are provided to users. The attacker alters the information present within the actual message in this attack, which results in sending the wrong information to other nodes.
6. Non-Safety Application Attack: Within the journey and the safety applications not disturbed, the types of attacks are concerned with the user's comfort. The traffic system is enhanced, and comfort is provided to the passengers by the non-safety applications. Passengers are discomforted by the generation of attacks in such scenarios where data cannot be received at the required time and, within the complete network, there is a delay in occurring. The apps are unsafe because they don't have the information to be warned if there is a delay in the apps [13].

The challenges associated with the MANET deployment are security and privacy. The nodes in the MANET transmit messages to each other to get the latest information about road conditions and traffic. The messages are defined as Cooperative Awareness Messages (CAMs) and are shared regularly. The developed messages include parameters such as speed, position, and so on for data transmission between nodes to broadcast information to nodes within the range [14]. Therefore, security is crucial for decision-making based on information transmission between the other nodes.

Similarly, the user who is not tracked or identified at the same interval of time needs to be accountable for the user's network responsibility. In the MANET environment, the researcher for attack identification responsible for the MANET misconduct develops different misbehaviour detection schemes. The device's precautionary measurement detects abnormal detection and is used to identify malicious activity in the network. This paper proposed a trust management protocol, Enhanced Beacon Trust Management with Hybrid Optimization (EBTM-Hyopt), to effectively detect malicious, dropped, or duplicate packets in the node with the monitoring approach. The simulation analysis is based on different attack models such as timing, node impersonation, and Sybil attack. This, in turn, increases the network's performance with the requirements of the complex security schemes in MANETs.

The present paper is organized as follows: Section 2 provides the different malicious detection node schemes in MANETs. Section 3 presents a protocol for those designs that are explained in detail. Section 4 provides the evaluation of the proposed protocol performance through comparative analysis. Section 5 provides the overall conclusion and future work.

2 Literature Review

In [15] constructed a malicious node detection and monitoring termed QoS and Monitoring of Malicious Nodes in Mobile ad hoc networks protocol (QMM-MANET). The proposed QMM-MANET protocol is based on three parts, such as (i) the computing in the node with QoS and election

of the cluster-head trustier node, (ii) with proper selection of the neighboring nodes for the packet retransmission, and (iii) utilizing the recovery algorithm for the failure in the gateway node. The simulation results showed that the proposed QMM-MANET exhibits suitable performance for the highway scenario compared with the existing protocol, with an increased packet delivery rate of 12% and a reduced end-to-end delay of 45%. The limitations associated with the dataset educate the test leads to false positives and environmental factors. In [16] introduced an Intelligent Black hole Attack Detection scheme (IBAD) integrated with the Autonomous and Connected Nodes (ACV) based on the consideration of the four parameters such as destination sequence number, hop count, End-to-end delay (E2E), and Packet Delivery Ratio (PDR). It exhibits significant performance in the neighboring node through the malicious node and data packet dropping in the emergency alarms. However, the developed protocol design shows a more time-consuming process.

In [17], the authors proposed a Hybrid Wormhole Attack Detection (HWAD) protocol for the detection of wormholes with Round Trip Time (RTT) estimation of the hop count and packet delivery ratio (PDR). Additionally, the wormholes out of the band exhibit the successive node for the transmission range in a lively manner compared with the existing algorithm. The proposed HWDA minimizes the delay and energy for wormhole detection for different network nodes. However, the proposed HWAD does not rely on specific middleware or hardware. In [18], the authors constructed a Genetic Algorithm with Hill Climbing (GAHC) for the optimal route selection in a multipath environment. Initially, the proposed improved fuzzy C-means algorithm exhibits higher peak density and Cluster Head (CH) selection in the predicted manner based on consideration of direct, indirect, and recent trust. In [19], the authors developed a model for dual attack prevention for the Black Hole Attack (BHA) and Gray Hole Attack (GHA) with the utilization of the Artificial Neural Network (ANN) integrated deep learning model for swarm-based Artificial Bee Colony (ABC) algorithm optimization. In [20], the authors constructed an optimal routing model for energy-efficient communication in MANET with a trust-based protocol. The proposed model is termed the Bacteria for Aging Optimization Algorithm (BFOA) and is based on a trusted and energy-efficient algorithm.

In [21], the authors developed a trust-based reasoning model with Fuzzy Petri Net (FPN) is presented to evaluate the node's credibility. The developed routing algorithm is estimated based on the trust entropy with the computation of the selected trust entropy in the routing table. The developed routing algorithm reflects the comprehensive performance in the route hop and trust value of nodes for the route selection to increase the MANET QoS.

In [22], the authors constructed a Certificateless Key-Encapsulated Signcryption (CL-KESC) scheme integrated with the (CL-PKC). The immune key escrow model, which is seen as a big problem with Identity-based Public Key Cryptography (ID-PKC), has been built into the CL-PKC model. The existing CL-KESC model relies on the elliptic curve operation for the higher computation expense in small UAVs. They developed a CL-KESC construction model termed Hyperelliptic Curve Cryptography (HECC) to overcome the limitation.

The approaches discussed above are suitable solutions for strengthening the AODV routing protocol against Distributed Denial of Service (DDOS) attacks; under these schemes, misbehaving nodes may be recognized and blacklisted, resulting in increased network throughput and decreased end-to-end latency. The network's overall performance has improved. Unfortunately, these techniques for defending against a unique assault offer to secure AODV with no performance analysis and only pay attention to one attack, which may not support security in the face of all other attacks with energy conservation. The Enhanced Beacon Trust Management with Particle Swarm Optimization (EBTM-PSO) solution is proposed to deal with these problems.

3 Research Methodology

In this EBTM-HYOPT model, optimization of the cluster head is based on incorporating the principle of particle swarm optimization to enable and ensure reliable routing. The malicious node can transmit false safety in the network for the computation of malicious behavior or selfishness. In an ad-hoc network, false messages are altered based on the behavior and formulation of the disastrous network situation [23–27]. Therefore, it is important to evaluate the wrong messages in the system through the Enhanced Beacon Trust Management scheme. With a beacon-based trust management scheme, the verification and estimation are based on the node's constants, such as direction, position, and velocity. The similarity index values are computed based on the estimated angle and vector based on the direction, position of nodes, and velocity [28–30]. The proposed trust-based energy-efficient MANET architecture is shown in Fig. 1.

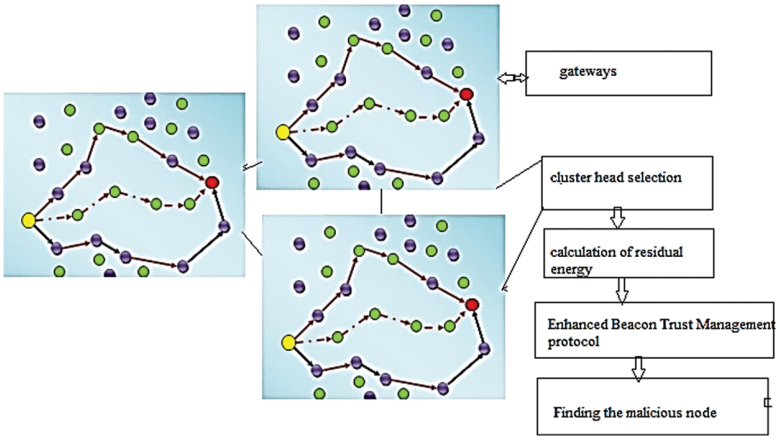

Figure 1: System architecture of the proposed method

3.1 Cluster Head Selection

The cluster head election process is performed in five steps (i) Fuzzy clustering, (ii) Calculating total clusters, (iii) Joint Resource allocation, (iv) Particle swarm optimization for the improvement of energy consumption, (v) Information gathering between nodes, (vi) Residual energy calculation.

In this fuzzy clustering model for CH election, 's' sensor nodes denoted as k_1, $k_2 \ldots$., k_s are clustered into 'm' clusters represented as $N_{1,}$ $N_2 \ldots$., N_m. Hence, the clustering state is given by a matrix whose size is $t \times s$ with mapping degree T_{ij} quantifying the degree of relation between the members of the cluster and its head. This clustering based on fuzzy minimizes the distance of the cluster members to the center of the cluster, ensuring the degree of mapping of sensor node K_i to cluster N_j. The fuzzy clustering model uses a degree of mapping, and its expression is given below in Eq. (1)

$$DoM\left(T_{ij}\right) = \frac{1}{dist(k_i, T_j)^2} \tag{1}$$

The normalized degree of mapping is represented in Eq. (2)

$$T_{ij} = \frac{\frac{1}{dist(k_i,T_j)^2}}{\sum_{i=1}^{k} \frac{1}{dist(k_i,T_j)^2}} \tag{2}$$

The clustering process is achieved by using Eq. (3)

$$T_j = \frac{\sum_{i=1}^{s} T_{ij} \cdot k_i}{\sum_{i=1}^{s} T_{ij}} \tag{3}$$

This clustering method is termed soft clustering because every node can act as a member of numerous clusters.

3.2 Number of Clusters Calculation

In the network, fuzzy clustering requires a precise number of clusters to control clustering granularity and reliably balance compressibility and precision [31–35]. Thus, the number of clusters is determined based on the Sum of Squared Error (SSE) parameter, and the within-cluster sum of square (W_{SS}) is given in Eq. (4)

$$T_j^{SSE} = \sum_{i=1}^{s} W_{ss} dist(k_i, T_j)^2 \tag{4}$$

where k_i and T_j describe the position of every member and to which cluster it is assigned. Moreover, SSE helps to estimate the feasibility of data fitting as indicated in Eq. (5)

$$T_j^{SSE}(m) = \sum_{i=1}^{s} \sum_{j=1}^{m} W_{ss} dist(k_i, T_j)^2 \tag{5}$$

DFLCHES uses the Elbow method to estimate the total clusters; when cluster count increases, the degree of SSE reduces with every cluster. Here, several clusters are based on SSE calculation and inflection point defined by a curve drawn with estimated SSE obtained for 'm' clusters.

3.3 Particle Swarm Optimization (PSO)

Optimal routing is obtained through several iterations after PSO is randomly assigned to a set of particles [36–40]. By the decision made through fitness function, every CH must be optimized, and for which speed must be estimated using distance and the direction of flight. After then, the best CH is found with the best location [36–40]. Two extremes are tracked, and they update the best CHs in each iteration. One extreme is CH, which finds the optimal routing O_{id}; the other is the optimal result of the current population P_{pd}. The formula for updating is shown in Eqs.(6) and (7).

$$p_{id}(t+1) = wp_{id} - [a_1 r_1 (k_{id} - O_{id}(t)) - a_2 r_2 \left(P_{pd} - k_{id}(t)\right)] \tag{6}$$

$$k_{id}(t+1) = k_{id}(t) - p_{id}(t+1) \tag{7}$$

where the number of iterations is denoted by t, p_{id} represents the CH's speed and k_{id} indicates the CH location. A random number between 0 and 1 is represented by r_1 and r_2. a_1 and a_2 is the accelerating factor, and w is the weighting coefficient.

3.4 Gravitational Search Optimization Algorithm (GSOA)

The Gravitational Search Optimization Algorithm (GSOA) is a stochasticity population with the meta-heuristics algorithm operating based on Newton's law of motion gravity. Originally, the GSOA module focused on identifying the continuous optimization problem solution [41–46]. The developed optimization approach involves a set of objects or agents introduced with search space to determine the optimal dimension solution with the principle of Newton's law. The candidate solution X_i is evaluated based on the search space. The performance of the agent is higher with the gravitational mass those have a higher attraction gain radius. With GSOA lifespan, the successive agent is adjusted with X_i by the agent with the best KGSOA agent with Newton's laws. To evaluate in detail, the agent system is assumed to have the agent position defined as

$$X_i = \left(x_i^1, \ldots, x_i^d, \ldots, x_i^n\right); i = 1, 2, \ldots, s \tag{8}$$

where x_i^d presented the agent i position with the search space of n with dimension d. For each agent, the estimated mass with the gravitational current data fitness is computed using the Eqs. (9) and (10) as follows:

$$q_i(t) = \frac{fit_i(t) - \text{worst}(t)}{\text{best}(t) - \text{worst}(t)} \tag{9}$$

$$M_i(t) = \frac{q_i(t)}{\sum_{j=1}^{s} q_j(t)} \tag{10}$$

where, $M_i(t)$ and $fit_i(t)$ are denoted as i^{th} agent fitness value gravitational mass at respective time t. In this, the best(t) and worst(t) are defined as

$$\text{best}(t) = \min_{j \in \{1,\ldots,s\}} fit_j(t) \tag{11}$$

$$\text{worst}(t) = \max_{j \in \{1,\ldots,s\}} f_{it_j}(t) \tag{12}$$

Agent acceleration of an is computed based on every agent force in the set KGSA using the gravitational law given in Eq. (6) with estimated acceleration agent using motional law

$$F_i^d(t) = \sum\nolimits_{j \in K\,\text{best}, j \neq i} \text{rand}_j\, G(t) \frac{M_j(t) M_i(t)}{R_{ij}(t) + \varepsilon} \left(x_j^d(t) - x_i^d(t)\right) \tag{13}$$

$$a_i^d(t) = \frac{F_i^d(t)}{M_i(t)} = \sum\nolimits_{j \in K\,\text{best}, j \neq i} \text{rand}_j\, G(t) \frac{M_j(t)}{R_{ij}(t) + \varepsilon} \left(x_j^d(t) - x_i^d(t)\right) \tag{14}$$

where r and j are defined as the distributed random number between the range of [0,1],

- ε, represented as a minimal value with the zero-error division when R_{ij} (t) is computed as zero,
- R_{ij} (t) denoted as the agent i and j Euclidean distance indicated as $kX_i(t), X_j(t)k_2$
- K_{best} represents the KGSOA first agent best fitness value with the higher gravitational mass, where the initial value $K_{initial}$ is assigned with the reduction with the time.
- G(t) is denoted as the initial gravitational constant $G_{initial}$, which decreases with time till the process of G_{end} reaches.

$$G(t) = G\left(G_{\text{initial}}, G_{\text{end}}, t\right) \tag{15}$$

The velocity and next position of the agent is estimated using the Eqs. (9) and (10)

$$v_i^d(t+1) = \text{rand}_i * v_i^d(t) + a_i^d(t) \tag{16}$$

$$x_i^d(t+1) = x_i^d(t) + v_i^d(t+1) \tag{17}$$

Fig. 2 presents the flow of the proposed energy conservation model.

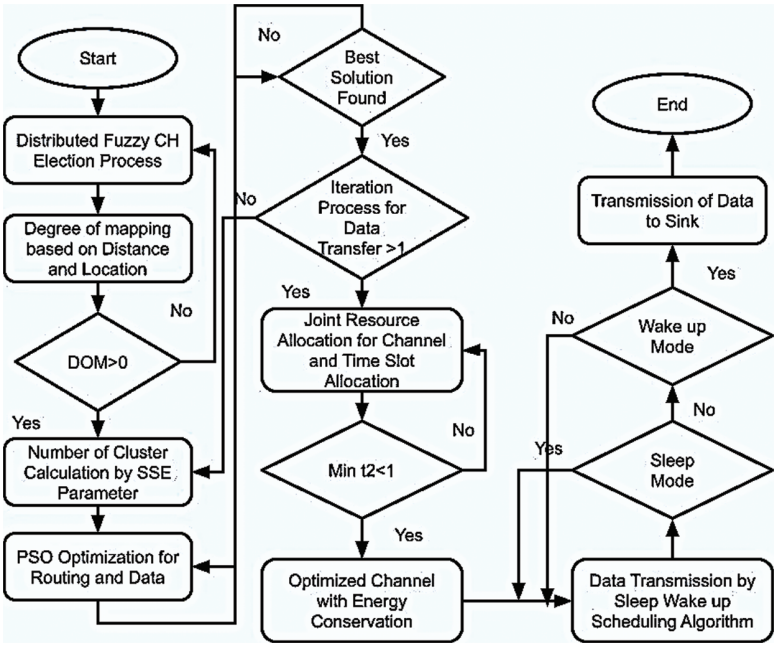

Figure 2: Flowchart of the proposed energy conservation architecture

3.5 Joint Resource Allocation

The complex resource allocation is solved by optimizing joint resource allocation, power control, and time slot assignment.

All the links are scheduled for frame length minimization while ensuring conflicts are free for the entire network, thus time slot for joint resource allocation is obtained by

$$h: E_s\{1, 2, 3 \ldots\} \tag{18}$$

$$\min t_3 = \| sE_s \| \tag{19}$$

$$\sum e_{ij}(T) \leq N_i \vee_i \in h(E_s) \tag{20}$$

$$\begin{cases} e_{ij}(T) = 1 \ \textit{Time slot assigned } T \textit{ for all links} \\ e_{ij}(T) = 0 \ \textit{others} \end{cases} \tag{21}$$

where Ni represents several interfaces N_i. The set of neighbors for nodes i and j is given by e_{ij}. T is the time slot, concluding with the collision-free transmission.

Joint optimization of resource allocation and power control is defined as a multi-objective problem with constraints. Thus, the multi-objective optimization problem for resource allocation is as follows

$$\min t_1 = \max((Y_i)) \tag{22}$$

where the network energy consumption is optimized by the min-max method, in which the maximum node energy consumption is minimized

$$\min t_2 = -\sum\nolimits_{d_{ij} \in E} W_{ij} \tag{23}$$

Cooperative communication in the network highly enhances transmission efficiency and maximizes network capacity, given by $\sum_{d_{ij} \in E} W_{ij}$. But network interference is also increased. To ensure the quality of the communication for every link, a constraint is framed as in Eq. (23) which helps guarantee that every link in the network satisfies SINR criteria.

$$\gamma_{ij} > \gamma_{th} \vee_{ij} \in E_s \tag{24}$$

where γ_{th} represents the threshold of SINR and γ_{ij} indicates the threshold value of the i^{th} and j^{th} node, and the threshold value of the system is given by

$$\eta \leq \delta \tag{25}$$

where η is the criterion for load balance, δ is the threshold value of the network, and the balanced power level for joint resource allocation is expressed

$$p_{ij} = P_{ij} \tag{26}$$

where p_{ij} denotes the balanced load power level and P_{ij} is the optimized channel level power. The power level, as well as the channel lying in the optional range, is ensured by

$$d_{ij} \in E_c \tag{27}$$

where d_{ij} *is* the optimized power and channel level, and E_c is the consumed energy.

3.6 Information Gathering between Nodes

Generally, the MANET environment comprises information gathering with trust classified under two categories, such as direct and indirect. Consider the nodes involved in network communication with uncertain communication in the node. In a homogeneous MANET communication structure, the nodes are allowed to move without any knowledge platform for free movement and join using different lanes until the recent neighbor evaluation of trust level. The relationship between direct trust is allowed with the neighboring nodes for information exchange. The presence of the intermediate node 'A' the platoon involved in RREQ based on the repository certificate on the roadside in the neighbor for the data forward request. With the presence of the certificate, the self-certificate is exchanged between node 'A' and its neighbor based on a unicast message. Similar to establishing direct trust, node A searches the originator certificate. In case the certificate is not observed in node 'A' with unicast certificate CetA in the neighbor. The indirect trust certificate requires originator A for the destination certificate possession CetB. Through the transmission of the reply message, indirect trust is established completely. The data transmission is transmitted with the guided conditions, first with the head estimation and second with the identification of the route head. It comprises the platoon head CertB with the piggy backend with the route reply message RREP towards node B. Every intermediate

node stores the CertB with the certificate repository. Based on the second condition, the fresh routes are identified with the intermediate node P and destination B between routes P to A. Each node is localized with direct trust in the two routes with the certificate chains. The RREP is propagated towards B with the appended CertA towards A with the appended CertB. A data transmission schedule is necessary to avoid collisions during data transmission among nodes in a cluster that includes CH. This scheduling process is divided into frequently run rounds to assign transmission slots. Every round comprises three phases that, in turn, are divided into three time slots.

The nodes whose hop distance is three use identical time slots to communicate with no disturbance among one another. For every node, the start and end phases are definite, thus, the start of every time node estimates the slot. The start time of mini slot i at round k is given by

$$T_{sm}\left(m_{i,k}\right) = T_{sm}\left(m_{i,k-1}\right) + 3 * (T_m + T_u + T_t) \tag{28}$$

$$T_{sm}\left(m_i, 0\right) = (T_{NDC} + T_D + T_{ST} + ((h+2)\, mod 3) * T_m \tag{29}$$

Here, T_m, T_u, and T_t represent the time of every time slot in scheduling assignments, updates, and data transmission. T_{NDC}, T_D, and T_{ST} indicate the time required to initially collect neighborhood data, gather data for scheduling, and construct steps of spanning trees, respectively. Likewise, starting time for transmitting data $T_{st}\left(S_{i,k}\right)$ and update scheduling time slot $T_{su}\left(f_{i,k}\right)$ are as follows

$$T_{st}\left(S_{i,k}\right) = T_{st}\left(S_{i,k-1}\right) + 3 * (T_m + T_u + T_t) \tag{30}$$

$$T_{st}\left(S_i, 0\right) = (T_{NDC} + T_D + T_{ST}) + 3T_m + ((h+2)\, mod 3) * T_t \tag{31}$$

$$T_{su}\left(f_{i,k}\right) = T_{su}\left(f_{i,k-1}\right) + 3 * (T_m + T_u + T_t) \tag{32}$$

$$T_{su}\left(f_i, 0\right) = (T_{NDC} + T_D + T_{ST}) + 3(T_m + T_t) + ((h+2)\, mod 3) * T_t \tag{33}$$

The slots assigned to a node are made available in the next round. A node that has transmitted data in the previous round remains awake, and the node which has to send data continuously uses the same slots for transmitting data in the next round. The nodes, which have to transfer data, are activated when slot assignment scheduling is processed and is awake until data for transmission is received. These active nodes forward the data to CH in time slots while other nodes are idle, preserving energy. When a parent node in any round has data for transmission, it goes to a waking state. When no child node is waking or has no data for information, it switches to either a receiving or sleeping state. Before trading, nodes inform their CH about their state change through a message in their respective update time slot.

3.7 Estimation of Residual Energy

The total energy consumed by the network at every round is given by

$$E_{net-sum} = \sum\nolimits_{i=1}^{k} (E_{REQ-CLUST} + \sum\nolimits_{j=1}^{N_j} E^{ij}{}_{CLUST-MEMB}) \tag{34}$$

The residual energy (REQ) for every node (N_j) is estimated

$$RE_i = IE - (TE + RE) \tag{35}$$

where IE, TE, and RE indicate starting energy and energy utilized to transmit and receive data, respectively.

3.8 Algorithm

1. Estimate the number of clusters using the Elbow method

   T_{ij} = PSO_CLUSTER_PROCESS(s,m)

2. Find the location of the cluster head concerning m

   For j = 1; to m do

3. Define the number of sensor nodes in a cluster
4. Optimize CH based on its position by using PSO

   $K_{id}(t+1)$;

5. Information gathering between nodes
6. Calculate residual energy.

$$RE_i = IE - (TE + RE)$$

End

3.9 Enhanced Beacon Trust Management Protocol

Estimate the node constant in the beacon-trust system while confirming the direction, velocity, and position. With the transmission of the beacon signal to the nodes, the trust worth value is calculated by calculating the similarity between the estimated values for location, direction, and velocity. This paper provides a Zijdenbos similarity that considers direction, velocity, and position variables and is used to compute the angle between the claimed vector. With the Zijdenbos similarity zij(sim), via angular metric inner products are calculated using the Eq. (36)

$$\text{zij(sim)[a, b]} = \frac{2(a.b)}{/a/ + /b/} = \frac{x\,(a)\,x\,(b) + y\,(a)\,y\,(b) + z\,(a)\,z(b)}{\sqrt{x\,(a)^2 + y\,(a)^2 + z\,(a)^2}.\sqrt{x\,(b)^2 + y\,(b)^2\,z\,(b)^2}} \tag{36}$$

The estimated vector a is defined as the latest observation, and the claimed vector for the beacon messages is represented as b. Let's assume that b = (xb, yb, vb) and a = (xa, ya, va), which comprises the three components such as *(x, y, v)* those are estimated based on the coordinates *x* and *y* are xy for the node movement velocity of *v*. In Eq. (1) the received beacon signal coordinates are computed as *x*b, *y*b; the latest received beacon signal velocity is denoted as *v*b; and the estimated coordinates in the received beacon message is represented as *xa, y*a. The computed function range between variables is denoted as zero and one based on the Jaccard coefficient. In the Jaccard index, the function corresponding difference is not computed based on the distance metric without satisfying the triangle inequality. The simple counter-example is defined as in three different sets, such as {a}, {b}, and {a, b}, for the difference between the first two sets, I, and the difference between each set is defined as one-third. To satisfy the inequality of the triangle, any two sets need to be sum those need to be higher or equal to the other remaining side. However, the distance between sets are stated as {a} and {a, b} plus the distance between sets {b} and {a, b} need to be equal to 2/3 those need to be less than the distance between sets {a} and {b} those need to be 1. The proposed scheme uses the time-based weighted model to compute the trusted beacon messages to estimate the historical beacon trust information between neighboring

nodes. In (4), the neighboring node comprises the beacon trust value denoted as Tbea, and I stated those need to be considered as the beacon. The larger the I value, the longer the beacon message time that influences the trust

$$\mathrm{T\ (beacon)} = \frac{\sum_{t=1}^{n} Zij\ (sim)\ [a, b]\ (Wi)}{\sum_{t=1}^{n} (wi)\ .n} \tag{37}$$

where wi stated as the weights in the beacons in i and

n represented as the exponent value.

Using the n value, the similarity between the variables is computed over time.

3.10 Peer-to-Peer Trust Evaluation

The trust evaluation process in the two-level need to be evaluated based on the consideration of the four trust components: honesty, intimacy, unselfishness, and energy. The node i trust value is assessed based on node j for the time instance denoted as t, $T_{ij}(t)$ indicated the real value range of [0,1] with a total trust value of 0.5 and distrust value of 0. The equation $T_{ij}(t)$ is represented as

$$T_{ij}\ (t) = w_1 T_{ij}^{intimacy}\ (t) + w_2 T_{ij}^{honesty}\ (t) + w_3 T_{ij}^{energy}\ (t) + w_4 T_{ij}^{unselfishness}\ (t) \tag{38}$$

where $w1, w2, w3$, and $w4$ denote the associated weights in the trust components represented as $w1 + w2 + w3 + w4 = 1$. The peer-to-peer evaluation of the trust is computed based on the SNs peer between CHs peer value. The trusted node i is evaluated based on the trustee node j for the time t and updated as $T_{ij}^{x}\ (t)$ represents the trust component X represented as follows:

$$T_{ij}^{x}\ (t) = \begin{cases} (1- \propto)\ T_{ij}^{x}\ (t - \Delta t) + \alpha T_{ij}^{x,direct}\ (t)\ if\ i\ and\ j\ are\ 1 - hop\ neighbours \\ avg\{(1 - \gamma)\ T_{ij}^{x}\ (t - \Delta t) + \gamma\, T_{ij}^{x,recomm}\ (t)\} \end{cases} \tag{39}$$

The node with the 1-hop in the neighbor is computed for the node i and j, based on the new trust value based on the direct observation $T_{ij}^{x,direct}\ (t)$, and old trust value in the past is denoted as $T_{ij}^{x}\ (t - \Delta t)$, where Δt updates the trust interval between the node j with the updated value of T_{ij}^{x}. The parameter $\propto$ is represented as the weights for the two trust values that decay over time. The old trust decay based on the contribution of the new trust value. The higher trust value relies on the observation of direct trust, where $T_{ij}^{x,direct}\ (t)$ denotes the trust value of node i towards node j using accumulated direct value in period for node i with node j for the 1-hop neighbor. The experience on the trust for the node i is denoted as $T_{ij}^{x}\ (t - \Delta t)$ for the neighbor with 1-hop is defined as $T_{ij}^{x,recomm}\ (it)$ with the recommender k value is updated as $T_{ij}^{x}\ (t)$. The neighbors in node i uses the 1-hop recommender energy level for conservation and scalability. The recommender energy conservation is based on node i with a 1-hop neighbor in the empty set for node I as an orphan for the case $\gamma = 0$ for node i contributing effective trust management with the peer-to-peer process. The estimated γ uses the recommendation in weight level with experience with the trust decay over time defined as follows:

$$\gamma = \frac{\beta T_{ij}^{x}(t)}{1 + \beta T_{ij}^{x}(t)} \tag{40}$$

In the above equation, indirect recommendations are represented as the specified parameter β based on the weighted assigned value of $T_{ij}^{x}\ (t)$ for indirect recommendation is normalized with the $\beta T_{ij}^{x}(t)$ based on the relative experience 1. Essentially, the recommended trust increases proportionally with the increases in β.

Instead of the fixed weight ratio of β to 1, the estimation is based on the adjusted value ratio and value for the testing effect in the resiliency in the slandering attacks in the network for the good

and bad-mouthing attacks. In the WSN model m, the energy in the selfish model is computed based on the reading data and packet drop in the receiver. Every trust value is evaluated with an unselfish node based on the remaining energy and the unselfish neighbors. The selfish node redeems to achieve service availability to sense the selfish neighbor SNs to balance the welfare *vs.* system individual. The node with selfishness can achieve service availability by sensing the SNs neighbor to balance individual interest vs system welfare. The model behavior comprises the token in the SN place with a transition with triggered T_SELFISH and the elimination of the SN token with T_REDEMP triggered. The SN is placed to exhibit the selfish node.

3.11 Finding the Malicious Node

On reception of the accusation of the beacon message (beaAccus_meg), the node immediately receives the node for the accused node's query and the other node's charge of the message. With statistics of the packet for the route, in the end, the statistics are received based on the query. The determined node receives the accused node for malicious activity or not. Upon receiving the node, the accusation is upheld based on the blacklist node movement. Without the party's concurrence, the charge is dropped by terminating the process. The time-limited entries are blacklisted based on the policy set based on the redemption of the node possibility. The access for the offender is defined with a unique identifier based on the entry timestamp until it expires. Additionally, with the unique identifier for the data transmission between sources and destinations based on the public key, a digital signature for the blacklist entry for every included node is created.

4 Performance Analysis

We compared our scheme to the present method in terms of performance metrics like throughput, packet delivery ratio, energy consumption, packet loss, end-to-end delay, and path length. To verify our EBTM-Hyopt to be more efficient than the existing techniques, such as QoS and Monitoring of Malicious nodes in mobile ad hoc networks (QMM-MANET) and QoS Optimized Link State Routing protocol (QOLSR), the graphs are given here.

4.1 Throughput

It refers to the data flow rate of a communication channel. In a MANET environment, throughput is an essential measurement while the nodes move simultaneously without traffic.

$$\text{Throughput (bits/ sec)} = \sum \frac{(\text{number of successful packets}) * (\text{average packet size})}{\text{Total Time sent in delivering that amount of data}} \tag{41}$$

Fig. 3 depicts the network throughput comparison of existing QMM-MANET, QOLSR, and proposed EBTM-Hyopt. The X and Y axes show the number of nodes and the values obtained in percentage, respectively. The blue and red colors indicate the existing QMM-MANET and QOLSR, whereas the green color indicates the proposed EBTM-Hyopt, respectively. When compared, existing QMM-MANET and QOLSR methods achieve 71.99 and 197.48 kbps of network throughput, while the proposed EBTM-Hyopt method achieves 297.99 kbps of network throughput, which is 226 kbps better than the QMM-MANET and 100.51 kbps better than the QOLSR method.

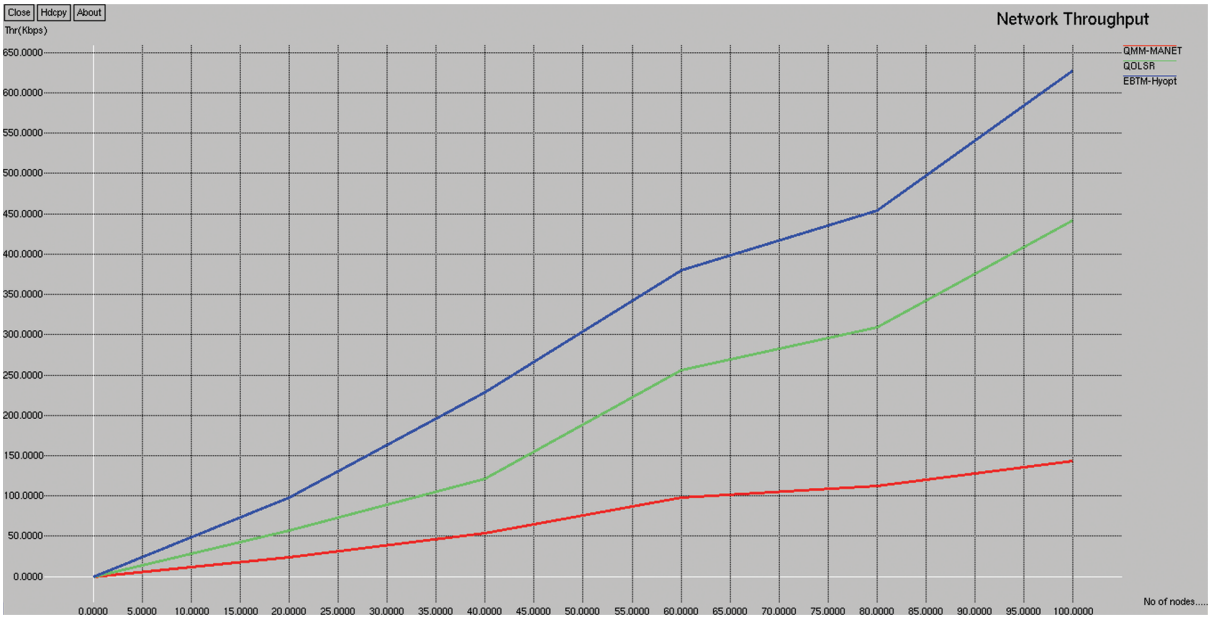

Figure 3: Network throughput

4.2 Packet Delivery Ratio (PDR)

The packet ratio transferred from the source node to the destination in the network successfully.

$$PDR = \frac{number\ of\ packet\ received\ succesfully}{Total\ number\ of\ packets\ forwarded} \tag{42}$$

Fig. 4 depicts the network packet delivery ratio comparison of the existing QMM-MANET, QOLSR, and proposed EBTM-Hyopt. The X and Y axes show the number of nodes and the values obtained in percentage, respectively. The blue and red colors indicate the existing QMM-MANET and QOLSR, whereas the green colors indicate the proposed EBTM-Hyopt. When compared, the existing QMM-MANET and QOLSR methods achieve 39.18% and 42.55% of packet delivery ratios. The proposed EBTM-Hyopt method achieves a 46.34% packet delivery ratio, which is 7.2% better than the QMM-MANET, and 4.21% better than the QOLSR method.

4.3 Energy Consumption

This is measured as the total energy of all hops and is computed as

$$Energy = \frac{1}{p}\sum_{n}^{p} E_n \tag{43}$$

where p denotes the hops in multihop routing and E_n is the energy of n^{th} hop.

Fig. 5 depicts the energy consumption comparison of the existing QMM-MANET, QOLSR, and proposed EBTM-Hyopt. The X and Y axes show the number of nodes and the values obtained in percentage, respectively. The blue and red color indicates the existing QMM-MANET and QOLSR, whereas the green color indicates the proposed EBTM-Hyopt, respectively. When compared, the existing QMM-MANET and QOLSR methods achieve 23% and 19% of energy consumption, while

the proposed EBTM-Hyopt method achieves 13% of energy consumption, which is 10% less than the QMM-MANET and 5% less than the QOLSR method.

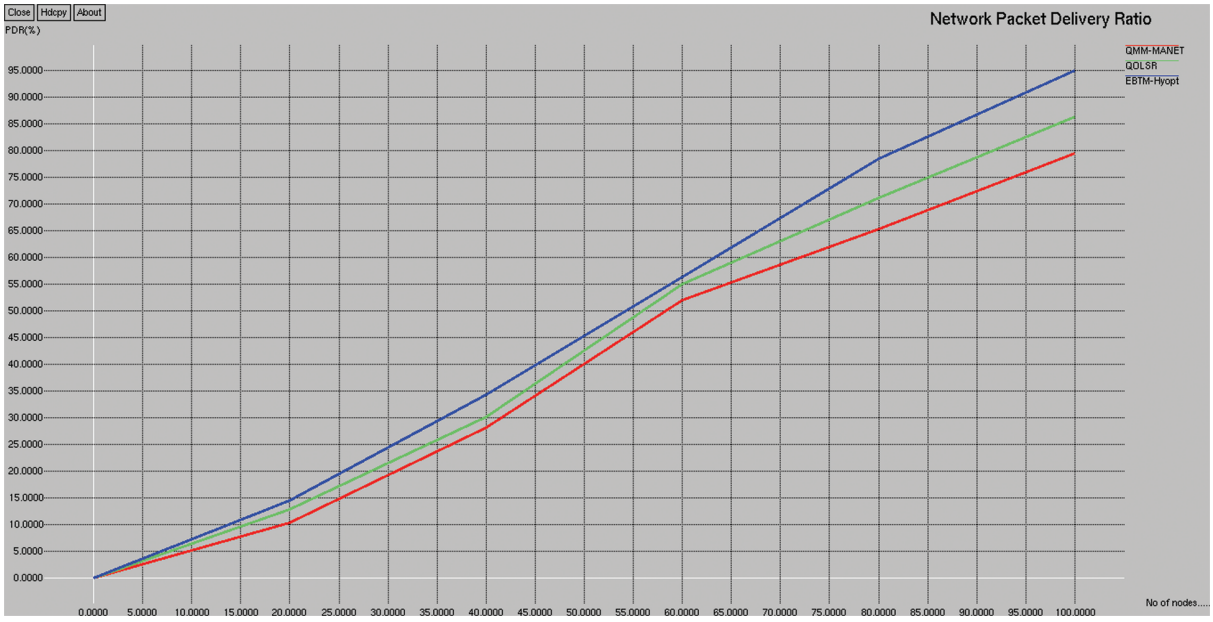

Figure 4: Packet delivery ratio

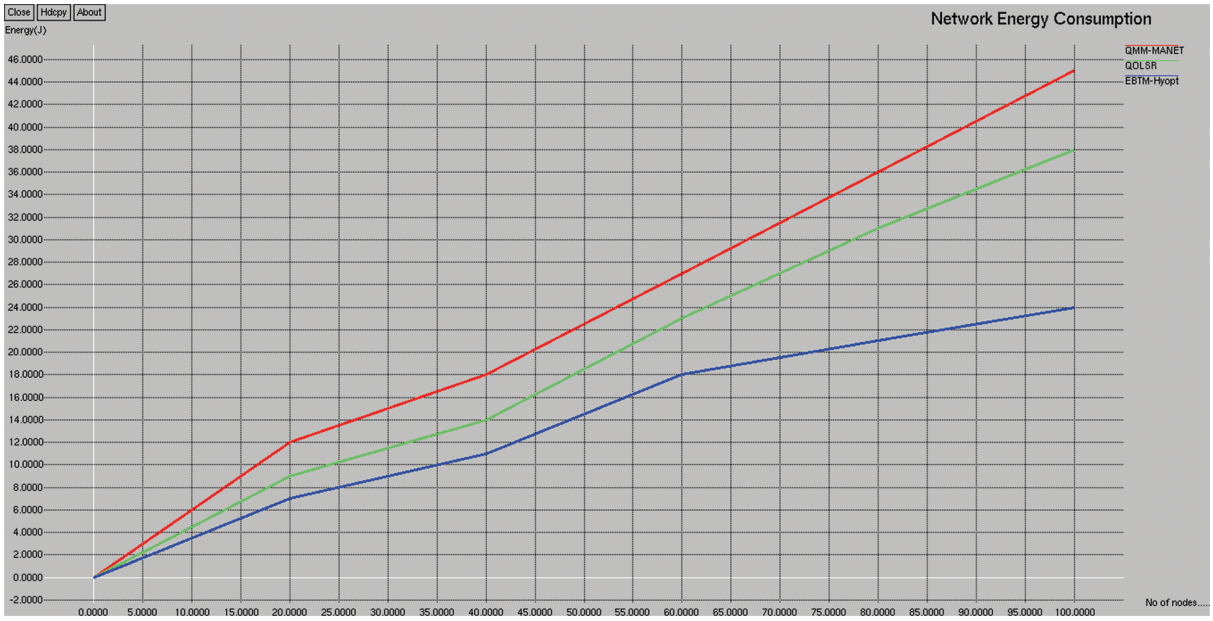

Figure 5: Energy consumption

4.4 Packet Loss

It is defined as the variance of packet arrival times at the end-user buffer. It occurs when packets travel on different network paths to reach the same destination. Fig. 6 depicts the packet loss comparison of the existing QMM-MANET, QOLSR, and proposed EBTM-Hyopt. The X and Y axes show the number of nodes and the values obtained in percentage, respectively. The blue and red colors indicate existing QMM-MANET and QOLSR, whereas the green color indicates the proposed EBTM-Hyopt, respectively. When compared, the existing QMM-MANET and QOLSR methods achieve 243.3 and 205.5 kbps of packet loss, while the proposed EBTM-Hyopt method achieves 165.6 kbps of packet loss which is 101 kbps better than the QMM-MANET and 25% better than the QOLSR method.

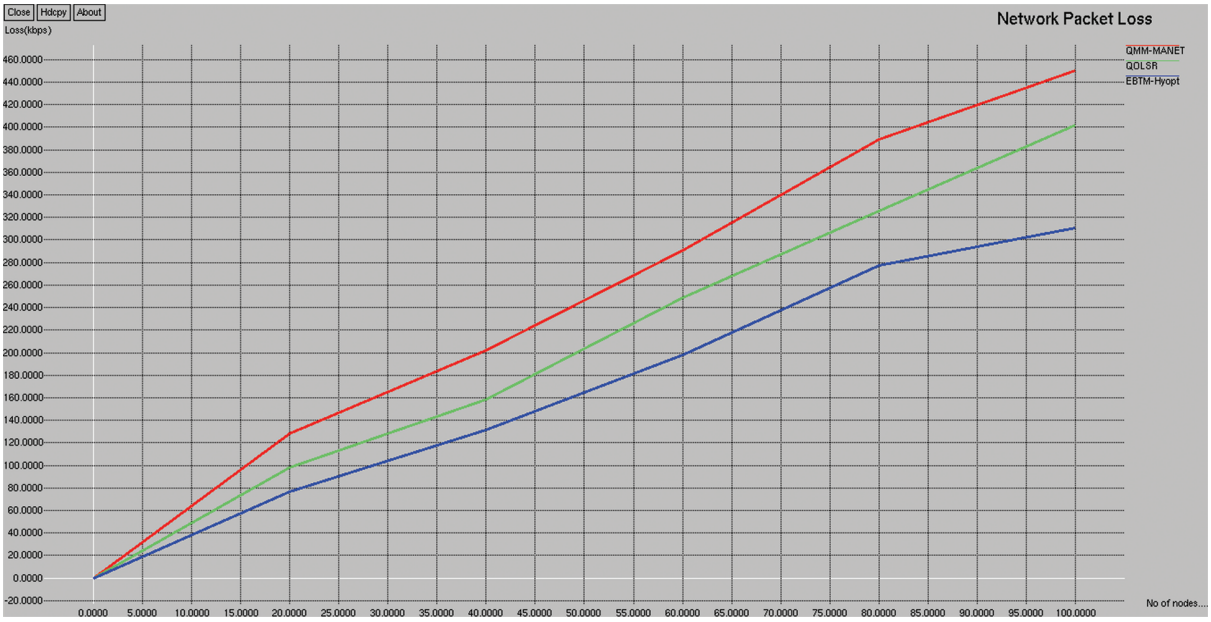

Figure 6: Packet loss

4.5 End-to-End Delay

This is the ratio of total hops (p) essential for routing to the full nodes (t_n) in the network, which is given by

$$Delay = \frac{p}{tn} \tag{44}$$

Fig. 7 depicts the end-to-end delay comparison of the existing QMM-MANET, QOLSR, and proposed EBTM-Hyopt. The X and Y axes show the number of nodes and the values obtained in percentage, respectively. The blue and red colors indicate existing QMM-MANET and QOLSR, whereas the green color indicates the proposed EBTM-Hyopt, respectively. When compared, existing QMM-MANET and QOLSR methods achieve 94.55% and 80.4% of end-to-end delay, while the proposed EBTM-Hyopt method achieves 67.49% of end-to-end delay, which is 24% better than the QMM-MANET and 13% better than the QOLSR method.

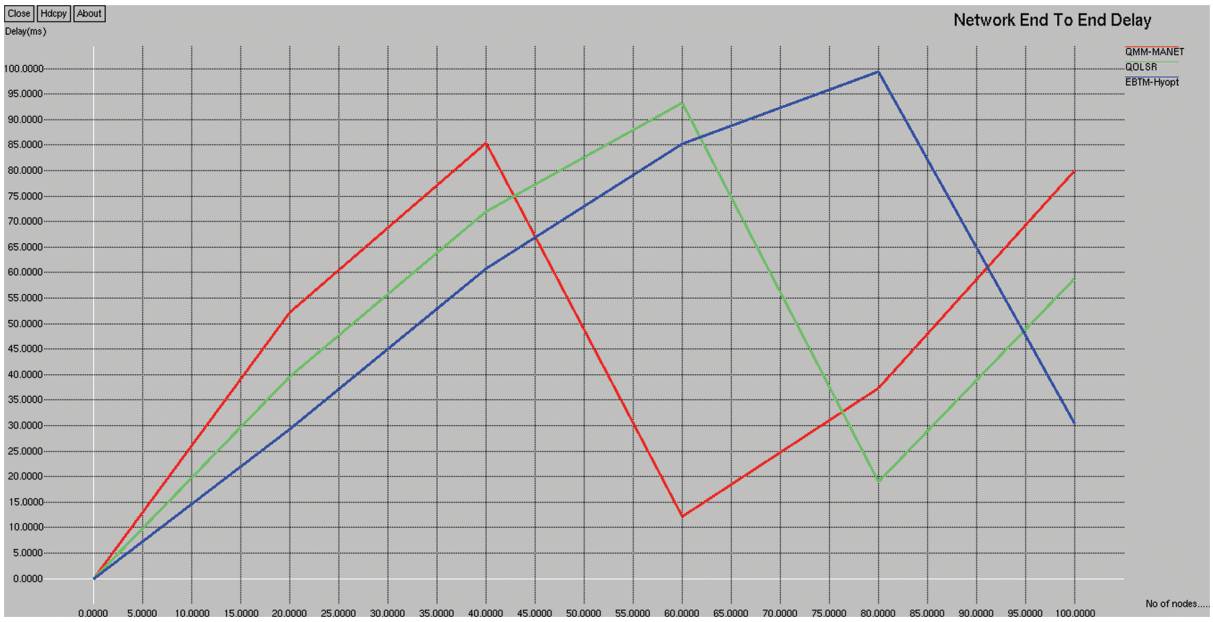

Figure 7: End-to-end delay

4.6 Path Length

Total path length specifies the length of the entire IP packet, including both the header and data segments, in bytes.

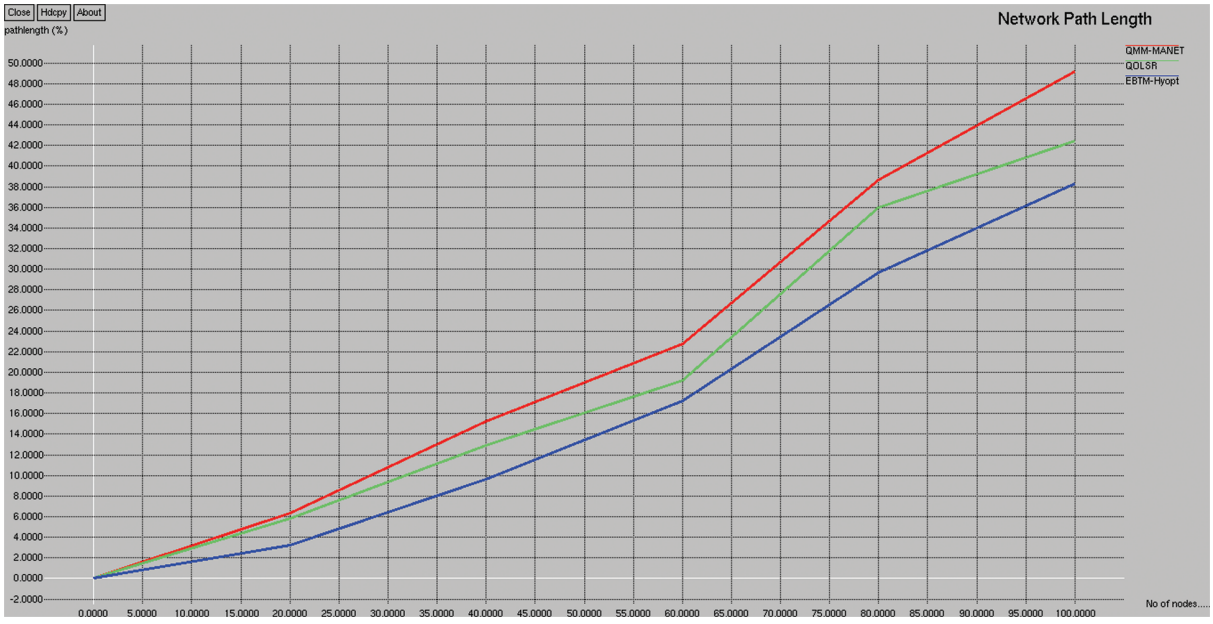

Figure 8: Path length

Fig. 8 depicts the path length comparison of the existing QMM-MANET, QOLSR, and proposed EBTM-Hyopt. The X and Y axes show the number of nodes and the values obtained in percentage, respectively. The blue and red color indicates existing QMM-MANET and QOLSR, whereas the green color indicates the proposed EBTM-Hyopt, respectively. When compared, the existing QMM-MANET and QOLSR methods achieve 22.04% and 19.40% of path length, while the proposed EBTM-Hyopt method achieves 16.34% of path length is 6.3% better than the QMM-MANET and 3.14% better than the QOLSR method.

5 Conclusion

A novel approach is proposed in this research work that may effectively classify attackers and separate malicious nodes in MANETs by combining a clustering mechanism with a trust mechanism. The analysis indicates that the proposed trust model is simple enough to meet the requirement for fast trustworthiness evaluation. Moreover, Particle Swarm Optimization with Cluster Head Election Scheme (DFLCHES) is proposed in this paper, which categorizes and removes packets from nodes having the least feasibility of becoming a cluster head that enables and ensures reliable routing. A sleep-wake-up approach is efficiently used to aggregate data, and intra and inter-cluster collisions are avoided using a TDMA transmission schedule. Thus, the election process of a gateway node using a threshold mechanism is enhanced, and cluster head selection is made by higher residual energy calculation. Simulation results suggest that EBTM-Hyopt is an attack-resistant trust model that provides high accuracy in detecting trust content in the presence of malicious nodes. Moreover, the performance of EBTM-Hyopt is compared with QoS and Monitoring of Malicious Nodes in Mobile Ad Hoc Networks (QMM-MANET) and QoS Optimized Link State Routing protocol (QOLSR), which clearly shows that Enhanced Beacon Trust Management with Hybrid Optimization (EBTM-Hyopt) performs better by achieving 297.99 kbps of throughput, 46.34% of PDR, 13% of energy consumption, 165.6 kbps of packet loss, 67.49% of end-to-end delay, and 16.34% of packet length. Future studies are required to enhance this model and develop a systematic algorithm appropriate for multi-interface and multi-channel MANET, to enhance the feasibility of the algorithm.

Acknowledgement: The authors would like to thank the R&D departments of Guru Nanak Institutions, B V Raju Institute of Technology, T. R. R. Government Degree College, and VFST& Research (Deemed to be University) for supporting this work.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Surendran and S. Prakash, "An aco look-ahead approach to QoS enabled fault-tolerant routing in manets," *China Communications*, vol. 12, no. 8, pp. 93–110, 2015.

[2] R. Cai, X. J. Li and P. H. J. Chong, "An evolutionary self-cooperative trust scheme against routing disruptions in manets," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 42–55, 2019.

[3] B. Paramasivan, M. Johan, V. Prakash and M. Kaliappan, "Development of a secure routing protocol using game theory model in mobile ad hoc networks," *Journal of Communications and Networks*, vol. 17, no. 1, pp. 75–83, 2015.

[4] J. Bai, Y. Sun, Ch. Phillips and Y. Cao, "Toward constructive relay-based cooperative routing in manets," *IEEE Systems Journal*, vol. 12, no. 2, pp. 1743–1754, 2018.
[5] O. Oyakhire and K. Gyoda, "Improved proactive routing protocol considering node density using game theory in dense networks," *Future Internet*, vol. 12, no. 3, pp. 47, 2020.
[6] K. Rajakumari, P. Punitha, L. Kumar and C. Suresh, "Improvising packet delivery and reducing delay ratio in mobile ad hoc network using neighbour coverage-based topology control algorithm," *International Journal of Communication Systems*, vol. 35, no. 2, 2022.
[7] J. Shanthini, P. Punitha and S. Karthik, "Improvisation of node mobility using cluster routing-based group adaptive in manet," *Computer Systems Science and Engineering*, vol. 44, no. 3, pp. 2619–2636, 2023.
[8] K. Lakshmanna, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalaf *et al.,* "Improved metaheuristic-driven energy-aware cluster-based routing scheme for IoT-assisted wireless sensor networks," *Sustainability*, vol. 14, no. 13, pp. 7712, 2022.
[9] U. Sri Lakshmi, S. Alghamdi, V. V. Ankalu, N. Veeraiah and Y. Alotaibi, "A secure optimization routing algorithm for mobile ad hoc networks," *IEEE Access*, vol. 10, pp. 14260–14269, 2022.
[10] S. Michael and M. Imad, "Spatial distribution and channel quality adaptive protocol for multihop wireless broadcast routing in vanet," *IEEE Trans Mobile Computing*, vol. 12, no. 4, pp. 722–734.
[11] S. Sennan, K. Gopalan, Y. Alotaibi, D. Pandey and S. Alghamdi, "EACR-LEACH: Energy-aware cluster-based routing protocol for wsn based IoT," *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2159–2174, 2022.
[12] U. Khan, S. Agrawala and S. Silakari, "Detection of malicious nodes (DMN) in vehicular ad-hoc networks," *Procedia Computer Science*, vol. 22, no. 46, pp. 965–972, 2015.
[13] O. A. Wahab, H. Otrok and A. Mourad, "A cooperative watchdog model based on dempster-shafer for detecting misbehaving vehicles," *Computer Communications*, vol. 41, no. 5, pp. 43–54, 2014.
[14] M. Ghosh, A. Varghese, A. Gupta, A. A. Kherani and S. N. Muthaiga, "Detecting misbehaviors in vanet with integrated root-cause analysis," *Ad Hoc Network*, vol. 8, no. 7, pp. 778–790, 2010.
[15] H. Fatemidokht and M. K. Rafsanjani, "MM-VANET: An efficient clustering algorithm based on QoS and monitoring of malicious vehicles in vehicular ad hoc networks," *Journal of Systems and Software*, vol. 165, pp. 110561, 2020.
[16] Z. Hassan, A. Mehmood, C. Maple, M. A. Khan and A. Aldegheishem, "Intelligent detection of black hole attacks for secure communication in autonomous and connected vehicles," *IEEE Access*, vol. 8, pp. 199618–199628, 2020.
[17] M. Tahboush and M. Agoyi, "A hybrid wormhole attack detection in mobile ad-hoc network (manet)," *IEEE Access*, vol. 9, pp. 11872–11883, 2021.
[18] U. Sri Lakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf *et al.,* "An improved hybrid secure multipath routing protocol for manet," *IEEE Access*, vol. 9, pp. 163043–163053, 2021.
[19] P. Rani, S. Verma and G. N. Nguyen, "Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network," *IEEE Access*, vol. 8, pp. 121755–121764, 2020.
[20] U. Sri Lakshmi, 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.
[21] X. Wang, P. Zhang, Y. Du and M. Qi, "Trust routing protocol based on cloud-based fuzzy petri net and trust entropy for mobile ad hoc network," *IEEE Access*, vol. 8, pp. 47675–47693, 2020.
[22] M. A. Khan, I. Ullah, S. Nisar, F. Noor, I. M. Qureshi *et al.,* "An efficient and provably secure certificateless key-encapsulated signcryption scheme for flying ad-hoc network," *IEEE Access*, vol. 8, pp. 36807–36828, 2020.
[23] M. Chatterjee, S. K. Das and D. Turgut, "WCA: A weighted clustering algorithm for mobile ad hoc networks," *Cluster Computing*, vol. 5, no. 2, pp. 193–204, 2012.
[24] Y. Alotaibi, "A new meta-heuristics data clustering algorithm based on tabu search and adaptive search memory," *Symmetry*, vol. 14, no. 3, pp. 623, 2022.

[25] D. Anuradha, N. Subramani, O. Khalaf, Y. Alotaibi, S. Alghamdi *et al.,* "Chaotic search-and-rescue-optimization-based multihop data transmission protocol for underwater wireless sensor networks," *Sensors*, vol. 22, pp. 2867, 2022.
[26] P. Mohan, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalaf *et al.,* "Improved metaheuristics-based clustering with multihop routing protocol for underwater wireless sensor networks," *Sensors*, vol. 22, no. 4, pp. 1618, 2022.
[27] N. Veeraiah and B. T. Krishna, "Intrusion detection based on piecewise fuzzy c-means clustering and fuzzy Naïve Bayes rule," *Multimedia Research*, vol. 1, no. 1, pp. 27–32, 2018.
[28] N. Veeraiah and B. T. Krishna, "Trust-aware fuzzyclus-fuzzy nb: Intrusion detection scheme based on fuzzy clustering and bayesian rule," *Wireless Networks*, vol. 25, no. 7, pp. 4021–4035, 2019.
[29] N. Veeraiah and B. T. Krishna, "Selfish node detection IDSM based approach using individual master cluster node," in *2018 2nd Int. Conf. on Inventive Systems and Control (ICISC)*, Coimbatore, India, pp. 427–431, 2018.
[30] K. Pradeep and N. Veeraiah, "VLSI implementation of euler number computation and stereo vision concept for cordic based image registration," in *2021 10th IEEE Int. Conf. on Communication Systems and Network Technologies (CSNT)*, Bhopal, India, pp. 269–272, 2021.
[31] Y. Alotaibi, "A new database intrusion detection approach based on hybrid meta-heuristics," *CMC-Computers, Materials & Continua*, vol. 66, no. 2, pp. 1879–1895, 2021.
[32] N. Subramani, P. Mohan, Y. Alotaibi, S. Alghamdi and O. I. Khalaf, "An efficient metaheuristic-based clustering with routing protocol for underwater wireless sensor networks," *Sensors*, vol. 22, no. 2, pp. 415, 2022.
[33] S. Bharany, S. Sharma, S. Badotra, O. I. Khalaf, Y. Alotaibi *et al.,* "Energy-efficient clustering scheme for flying ad-hoc networks using an optimized leach protocol," *Energies*, vol. 14, no. 19, pp. 6016, 2021.
[34] N. Veeraiah, O. I. Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani *et al.,* "Trust aware secure energy-efficient hybrid protocol for manet," *IEEE Access*, vol. 9, pp. 120996–121005, 2021.
[35] S. Arun and K. Sudharson, "DEFECT: Discover and eradicate fool around node in emergency network using combinatorial techniques," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 10, pp. 1–12, 2020.
[36] K. Sudharson, M. Akshaya, M. Lokeswari and K. Gopika, "Secure authentication scheme using CEEK technique for trusted environment," in *Int. Mobile and Embedded Technology Conf. (MECON)*, Noida, India, pp. 66–71, 2022.
[37] K. Sudharson and S. Arun, "Security protocol function using quantum elliptic curve cryptography algorithm," *Intelligent Automation & Soft Computing*, vol. 34, no. 3, pp. 1769–1784, 2022.
[38] B. Murugeshwari, D. Selvaraj, K. Sudharson and S. Radhika, "Data mining with privacy protection using precise elliptical curve cryptography," *Intelligent Automation & Soft Computing*, vol. 35, no. 1, pp. 839–851, 2023.
[39] S. N. Pari and K. Sudharson, "Hybrid trust-based reputation mechanism for discovering malevolent node in manet," *Computer Systems Science and Engineering*, vol. 44, no. 3, pp. 2775–2789, 2023.
[40] B. Murugeshwari, S. Rajalakshmi and K. Sudharson, "Hybrid approach for privacy enhancement in data mining using arbitrariness and perturbation," *Computer Systems Science and Engineering*, vol. 44, no. 3, pp. 2293–2307, 2023.
[41] S. Neelavathy Pari and K. Sudharson, "An enhanced trust-based secure route protocol for malicious node detection," *Intelligent Automation & Soft Computing*, vol. 35, no. 2, pp. 2541–2554, 2023.
[42] S. Palanisamy, B. Thangaraju, O. I. Khalaf, Y. Alotaibi and S. Alghamdi, "Design and synthesis of multi-mode bandpass filter for wireless applications," *Electronics*, vol. 10, no. 22, pp. 2853, 2021.
[43] S. R. Akhila, Y. Alotaibi, O. I. Khalaf and S. Alghamdi, "Authentication and resource allocation strategies during handoff for 5G IoVs using deep learning," *Energies*, vol. 15, no. 6, pp. 2006, 2022.

[44] A. Alsufyani, Y. Alotaibi, A. O. Almagrabi, S. A. Alghamdi and N. Alsufyani, "Optimized intelligent data management framework for a cyber-physical system for computational applications," *Complex & Intelligent Systems*, vol. 17, no. 4, pp. 1–13, 2021.
[45] S. Rajendran, O. I. Khalaf, Y. Alotaibi and S. Alghamdi, "Map reduce-based big data classification model using feature subset selection and hyperparameter tuned deep belief network," *Scientific Reports*, vol. 11, no. 1, pp. 1–10, 2021.
[46] A. Alsufyani, Y. Alotaibi, A. O. Almagrabi, S. A. Alghamdi and N. Alsufyani, "Optimized intelligent data management framework for a cyber-physical system for computational applications," *Complex & Intelligent Systems*, vol. 17, no. 4, pp. 1–13, 2021.