ANFIS Based Optimal Routing using Group Teaching and Adaptive Equilibrium Optimization based Trust Aware Routing Protocol in MANET

R. Hemalatha (hemalathar.id@gmail.com)
Anna University Chennai
R Umamaheswari
Loyola Institute of Technology
S Jothi
Anna University Chennai

Research Article

Keywords: MANET, trust-aware routing, ANFIS, group teaching optimization algorithm, adaptive equilibrium optimizer, optimal route selection.

Posted Date: March 31st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-355720/v1

ANFIS based Optimal Routing using Group Teaching and Adaptive Equilibrium Optimization based Trust Aware Routing Protocol in MANET

[1 *] Dr. R. Hemalatha, [2] R. Umamaheswari, [3] Dr .S. Jothi

[1]*Associate Professor, St. Joseph's College of Engineering, Chennai, India.*
[2]*Assistant professor, Loyola Institute of Technology, India.*
[3]*Associate Professor, Department of Computer Science and Engineering*
Anna University, Chennai, India.

*Corresponding Author Email: hemalathar.id@gmail.com

Abstract

Recently, routing is considered the main problem in MANET due to its dynamic nature. The route discovery and the optimal route selection from the multiple routes are established for the efficient routing in MANET. The major objective of this research is to select the optimal route for packet transmission in MANET. In this paper, four stages namely trust evaluation, route discovery, optmal route selection and route maintanance are elucidated. Initially, the trust evaluation is made by using ANFIS where the primary trust values are evaluated. The next stage is the route discovery scheme, in which the routes are established by Group teaching optimization algorithm (GTA). From the route discovery scheme, multiple routes are found. The optimal route for the transmission is selected with the help of the Adaptive equilibrium optimizer (AO) algorithm. Finally, the route maintenance process is established; if any of the routes fails for the broadcast it immediately selects the alternate optimal route from the multi-zone routing table for efficient packet transmission. The proposed approach is evaluated by various performance measures like throughput, energy consumption, packet delivery ratio, end-to-end delay, packet loss rate, detection rate, and routing overhead. This result describes that the proposed approach outperforms other state-of-art approaches.

Keywords: MANET, trust-aware routing, ANFIS, group teaching optimization algorithm, adaptive equilibrium optimizer, optimal route selection.

1. INTRODUCTION

In recent years, Information Technology is a promising field and is expanding everyday. Several efforts were made for establishing secure computations but there are many risks left unevaluated such as integrity, privacy, and security. The mobile ad hoc network (MANET) is the communication system that is described as the assortment of dynamic, wireless, independent, and mobile nodes are created without the assistance of the pre-existing framework [1]. The nodes in the MANET are free to travel inside the network and arranged themselves in the random approach. The important region of the ad hoc network is the setting of the topology of the routing protocol. The entire networks linked with activities such as topology discovery and packet delivery are executed by the nodes only [2].

MANETS are self-governed wireless networks that depend upon the self-directed mobile application structure. In that, each mobile node transmits information from one node to other nodes by equipped wireless interfaces. MANET did not depend upon the static

framework as well as the administrator. The restricted resources are obtained by the wireless sensor network that includes battery capacity, memory, and bandwidth [3]. MANET has various applications like rescue operations, emergency search, military applications, virtual classrooms, data acquisitions in hostile environments, and battlefield meetings. The routing protocol aims to create an perfect and expert route linking the two nodes to send messages on time. The entire network is disintegrated if routing is misdirected that leads to data loss. Hence, routing security is in charge of addressing the security problems created in the entire network [4].

Generally, mobile nodes came with a radio that has an assured transmission range. This limits the nodes is broadcasting the data straight to the destination node or the sink node. Because of this, the mobile nodes participated in helpful communication. By this method, the source nodes choose their path for forwarding the packet via the intermediate nodes in the route. MANETs are created for short-distance communication [5]. The network speed is based on the number of devices. It disintegrates when the number of devices increases because the whole devices are sharing the access network resources. Compared to the traditional wired network, MANET is also used to route packets from the source to the destination. When compared with another network, MANET also has several issues like attacks and threats. The data packets that are forwarded via the intermediate nodes are detained with the malicious nodes and cause various attacks such as modification, sinkhole, eavesdrop, etc [6].

In the MANET, the connections normally have less information measure compared with the wired network. The network management is disseminated to the entire nodes of the network. Hence, these unapproved nodes could become malicious nodes and provide false information to destroy the cluster communication reliableness. This affects the performance of the network [7]. So the security method is required to fight against the changes in the behavior of the nodes and termed as soft security threats to ensure reliableness, access management, and reliableness. Due to the absence of centralized control and infrastructure, security threats are increased in the MANET-IoT environment. MANET is susceptible to security attacks like greyhole attack, Sybil attack, blackhole attack, jamming attack, rushing attack. These attacks decrease the performance of the full network [8].

To cope up with the routing attack, it utilizes the reliability of mobile nodes contributing to routing or includes authentication nodes to the route by providing certificates to mobile nodes. If When several attacks occurred on the route, packets are lost or the link connection fails. This takes a long time to recover a new path from the source to the destination node. If a new route is established, then the control packet number enhances, and also the resulting overhead is also enhanced [9]. Various attacks occurred in the network layer. Even though it is required to establish efficient security solutions that can expose network attackers and there are various MANET security solutions, prevention of attack is more attractive. For decreasing the malicious actions, proficient secure routing methods are required to enhance the MANET reliability, availability, and scalability [10]. This paper proposes the trust aware energy-efficient routing protocol in MANET. The paper uses the GTA algorithm for route discovery and the AO algorithm for the optimal route section for efficient packet transmission. The contribution of the paper is as follows:

- Introducing the ANFIS concept for the evaluation of the trust value of the neighbors for the trust-aware routing protocol.
- Establishing the route discovery scheme by the GTA algorithm
- Selecting the optimal route by adaptive equilibrium optimizer for efficient packet transmission.

The remaining of the paper is arranged as follows. The summary of the exiting works on the trust aware energy-efficient routing protocol in MANETs is discussed in section 2. The proposed methodology for the trust aware energy-efficient routing protocol is described in section 4. The results and discussions are described in section 5. Section 6 states the conclusion and future scope of the work.

2. LITERATURE REVIEW

This section describes the review of some of the existing protocols with the disadvantages of those methods and described in Table 1. Nandgave-Usturge S et al. (2020) proposed Water Spider Monkey Optimization (WSMO) for discovering the optimal path depends on the trust and other parameters such as delay, overhead and distance. The performance of the proposed algorithm was evaluated with the measures such as delay, packet delivery ratio, denial of service, throughput with and without considering the denial of service, black hole attack, etc [11]. Mukhedkar MM and Kolekar U (2019) introduced Advanced Encryption Standard-enabled Trust-based Secure Routing protocol depends upon the projected Dolphin Cat Optimizer (AES-TDCO) with no accurate centralized monitoring process. The measures such as packet drop, delay, detection rate, and throughput were used for the evaluation. This method was difficult to maintain better trust and security-aware routing protocols when dealing with imaginary thoughts [12].

Sun Z et al. (2019) proposed the Secure Routing Protocol based on Multi-objective Ant-colony-optimization (SRPMA) for obtaining the increased network security through low energy consumption. The simulation results were obtained by using measures such as energy consumption, packet loss rate, routing load. This approach has drawbacks like decreased network lifetime as well as reliability [13]. Mukhedkar MM and Kolekar U (2020) designed the routing protocol called Encrypted trust-based dolphin glow-worm optimization (DGO) (E-TDGO) for providing secure routing in MANET. The experimental results were demonstrated with the measures such as packet drop, delay, detection rate, and throughput with considering the attacks [14].

Kanagasundaram H and Ayyaswamy K (2019) proposed a Multi-objective Ant lion optimizer (MALO) for dealing with the routing protocol with energy efficiency and security. The performance of the method was evaluated using measures such as delay, energy consumption, throughput, and network lifetime [15]. To decrease exposure from the malicious nodes and improves security, Alkhamisi AO et al. (2020) proposed an Incorporated Incentive and Trust-based optimal path identification in Ad hoc On-Demand Multipath Distance Vector (IIT-AOMDV). The simulation results were described using measures such as route selection time, throughput, detection accuracy, and overhead [16].

Table 1: Summary of existing routing protocols in MANET

Reference	Method	Purpose	Measures	Demerits
Nandgave-Usturge S et al. (2020)	WSMO algorithm	To find the optimal depends on the trust and other parameters	Delay, packet delivery ratio, denial of service, throughput	Difficult to strengthen the security
Mukhedkar MM and Kolekar U (2019)	AES-TDCO approach	No accurate centralized monitoring process	Packet drop, delay, detection rate, and throughput	Difficult to maintain better trust and security-aware routing protocols when dealing with imaginary thoughts
Sun Z et al. (2019)	SRPMA scheme	To obtain increased network security with low energy consumption	Energy consumption, packet loss rate, routing load	Decreased network lifetime and network reliability
Mukhedkar MM and Kolekar U (2020)	Encrypted trust-based dolphin glow-worm optimization (DGO) (E-TDGO)	To offer secure routing in MANET	Packet drop, delay, detection rate, throughput	Protocol was complex
Kanagasundaram H and Ayyaswamy K (2019)	MALO technique	To offer a secure routing protocol that is energy-efficient	Delay, throughput, energy consumption, and network lifetime	Routing overhead increases
Alkhamisi AO et al. (2020)	IIT-AOMDV approach	To decrease the risks from malicious nodes and improve the network security	Route selection time, throughput, detection accuracy, and overhead	Difficult to imagine direct trust evidence to reduce malicious attacks
Mariadas AE and Madhanmohan R	Hybrid PSO and differential algorithm	To improve the network lifetime	Packet delivery ratio, average delay, packet loss ratio, throughput, energy consumption	Difficult to strengthen the security along with improving network capacity.
Keum D et al. (2020)	Trust-based multipath QoS routing protocol (MC_TQR)	To detect the malicious nodes and also to assure the reliability	End-to-end delay, throughput, Packet delivery ratio	Reliability was low
Kumar R and Shekhar S (2020)	Trust-based fuzzy bat optimization approach	To diminish the consequences of attacks	Network lifetime, throughput, routing overhead, packet delivery ratio, delay	Routing latency increases
Merlin RT and Ravi R (2019)	Trust-based energy-aware routing (TEAR) approach	To provide enhanced route security and also to enhance resource-limited problems	Trust value, energy consumption, Successful routing ratio	Communication overhead was more

Mariadas AE and Madhanmohan R (2020) proposed Hybrid PSO and differential algorithm that concentrates on the lifetime energy based on clustering by the fitness value. The effectiveness of the technique was calculated in terms of the measures namely packet delivery ratio, average delay, packet loss ratio, throughput, and energy consumption [17]. Keum D et al. (2020) proposed a trust-based multipath QoS routing protocol (MC_TQR) for

the ad hoc network for detecting the malicious nodes and also to assure the reliability of the network. The method was evaluated depends on measures namely end-to-end delay, throughput, and packet delivery ratio. The major difficulty was this method has low reliability [18].

Kumar R and Shekhar S (2020) introduced a trust-based fuzzy bat optimization approach for diminishing the consequences of attacks. The results were demonstrated using measures such as network lifetime, packet delivery ratio, throughput, end-to-end delay and routing overhead [19]. Merlin RT and Ravi R (2019) Trust-based energy-aware routing (TEAR) approach for increasing the resourced restricted issues in the network and provides enhanced route security. The measures such as trust value, energy consumption, and Successful routing ratio utilized for the evaluation purposes. This method increases the lifetime of the network by neglecting the black hole attacks and maximizes the successful routing probability [20].

3. SYSTEM DESIGN

This section imagines the important multi-hop MANET in which the nodes are disseminated arbitrarily in the 2D space [21]. Let us consider that there are three cases, where each case comprises of a single channel that are identical to the broadcast range. This paper utilizes directed graph model that are expressed as

$$G_r = \left(V_e , E_l\right) \tag{1}$$

From Eqn.(1), V_e represents the set of the entire nodes and E_l represents the set of the entire edges. Every edge $e_l\,(j,k) \in E_l$ indicates that the two nodes are located inside the broadcast range. In this research the hybrid routing protocol is considered in which the graph G_r is classified into zones. Every node contains only one zone and every zone contains the middle node and few other nodes. The node that corresponds to the zone is classified into interior as well as the boundary nodes individually.

The structure of the hybrid routing protocol consists of trust evaluation and route schemes. Trust evaluation runs for every node to verify the neighbor's behavior in real-time and achieves trust values that are considered as the most significant factors for the hybrid routing protocol. In the majority of the cases, trust contains two sections: direct trust and indirect trust. Due to significant computation cost as well as traffic load, this research considers direct trust. The routing protocol consists of routing within the zone, among the zone, and other fundamental schemes.

3.1 Problem definition

Let us consider the MANET with *n* number of nodes reponsible for sensing and gathering the information related to the environment. Each node lies within the transmission range and the transmission among the source to destination nodes taken place inside the range. If the nodes are moving, they alter their position inside the transmission range, so the new node location is obtained inside the transmission range. Hence to create an effective route for the broadcast, two various factors namely trust and distance are considered. The mobility schemes of the

MANETs determine the nodal movement and it depicts the position, acceleration and velocity of the nodes locations where its positions are updated periodically inside the broadcast range. In addition to this, trust is the main parameter which determines the MANETs security and the nodes determines the trust degree of the network. To overcome these problems, trust-aware routing protocol is proposed that further enhances the trust and security.

4. PROPOSED METHODOLOGY

In this paper, four stages namely trust evaluation, route discovery, optmal route selection and route maintanance are elucidated.Initially, the trust evaluation is made by using ANFIS. In this trust evaluation, the primary trust values are evaluated. The next stage is the route discovery procedure in which the route is discovered by Group teaching optimization algorithm. The third stage is the optimal route selection. Due to the establishment of multiple routes, the optimal route selection is considered as the main problem in the route discovery process, so adaptive equilibrium optimizer is utilized for the optimal route selection procedure. In the route maintenance stage, if any of the routes fails for the broadcast it immediately selects the alternate optimal route from the zone routing table for efficient packet transmission. The route is maintained until the packet reached the destination. The proposed framework for the stable route prediction is described in Fig 1.

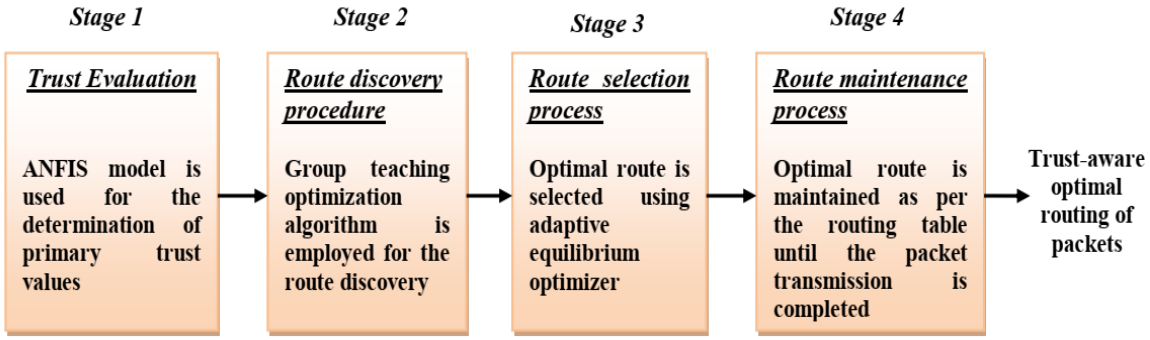

Fig 1: Proposed framework for the trust-aware routing protocol

4.1. Trust evaluation

In the trust aware routing protocol, the analysis of the node's behavior is represented to evaluate whether the node is selfish or the node is acting like the malicious nodes. Each node supervises the behavior of the neighbor nodes in real-time and the trust weights are computed. If the neighbor node *j* links with node *i*, then the node *j* organizes it as the primary trust value. The primary trust value is determined by the ANFIS model.

ANFIS model

The adaptive neuro-fuzzy inference system (ANFIS) is the neural network model that provides the solution of approximation issues. This function provides the mapping link among the input as well as the output data with the deep learning method for determining the best membership function distributions. In this ANFIS structure, five layers are utilized to

build the inference system. Every layer composed of various nodes depicted through the node function [22]. The input of the current layers is achieved from the nodes in the preceding layers. The fuzzy inference system is assumed which consists of 5 layers of the adaptive network with two inputs *(a, b)*, and it has only one output *c*. The ANFIS rule base function is composed of fuzzy if-then rules of Sugeno type [23]. For the first order two-rule Sugeno inference system, the two rules are described as:

Rule 1: If *a* is X_1 and *b* is Y_1 then *c* is F_1 *(a, b)*
Rule 2: If *a* is X_2 and *b* is Y_2 then *c* is F_2 *(a, b)*

Where a and b represent the ANFIS inputs, X and Y represent the fuzzy sets F_1 *(a, b)* indicates the first-order polynomial, indicates the output of the first-order Sugeno fuzzy inference system. The structural design of ANFIS is exposed in Fig 2 and the node functions are determined below. The adaptive nodes are represented using squares that indicate the factor sets which are changeable with the help of the nodes [31]. The fixed nodes are represented by the circles, in which the factor sets are permanent in the system.

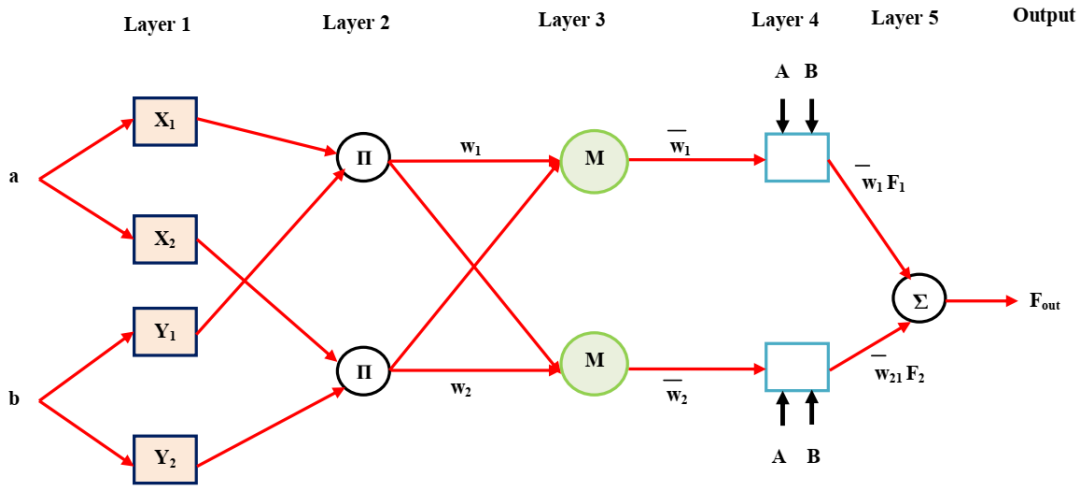

Fig 2: Structural design of ANFIS

<u>*Layer 1:*</u> This layer consists of adaptive nodes and is determined as:

$$Q_{1,j} - \mu_{X_j}(a) \quad for \quad j=1,2 \tag{2}$$

$$Q_{1,j} - \mu_{Y_{j-2}}(b) \quad for \quad j=3,4 \tag{3}$$

From Eqns. (2) and (3), the input nodes are represented as input nodes, X and Y represents the linguistic labels, $\mu(a)$ and $\mu(b)$ represents the membership functions that are typically accepted the bell-shaped function with the highest and lowest value identical to 1 and 0 correspondingly as pursues:

$$\mu(a) = \frac{1}{1 + \left(\frac{a - z_j}{x_j} \right)^{2y_j}} \tag{4}$$

$$\text{Or } \mu(a)=\exp\left\{-\left(\frac{a-z_j}{x_j}\right)^2\right\} \tag{5}$$

From Eqns. (4) and (5), x_j , y_j and z_j represents the factor set. The above-said factors are represented as premise factors.

Layer 2: The nodes in layer 2 is represented as the permanent node, denoted using circle and marked as Π to be multiplied with the input signals to provide the output.

$$Q_{2,j}=w_j=\mu_{X_j}(a)\cdot\mu_{Y_j}(b) \quad for \;\; j=1,2 \tag{6}$$

From Eqn. (6), w_j indicates the rule of the firing strength.

Layer 3: The nodes in layer 2 is represented as the permanent node, denoted using circle and marked as M, to standardize the firing strength. Then it evaluates the proportion of the jth node firing strength with respect to the entire rules as per Eqn. (7)

$$Q_{3,j}=\overline{w}_j=\frac{w_j}{\sum w_j}=\frac{w_j}{w_1+w_2} \quad for \;\; j=1,2 \tag{7}$$

Layer 4: The nodes in layer 4 represent the adaptive nodes, represented by the square with the node function.

$$Q_{4,j}=\overline{w}_j F_j \;\; for\; j=1,2 \tag{8}$$

From Eqn. (8), F_1 and F_2 represents the fuzzy if-then rules

Where l_2 , m_2 and n_2 represents the factor set, mentioned as the resultant factors.

Layer 5: The nodes in layer 5 represent the permanent node using the node function to evaluate the resultant output as Eqn. (9).

$$Q_{5,j}=F_{out}=\sum_j \overline{w}_j F_j = output \tag{9}$$

From the structure of ANFIS described above, the output is described as the linear arrangement of the subsequent factors. The resultant output is written as

$$\begin{aligned} zF_{out}&=\overline{w}_1 F_1+\overline{w}_2 F_2=\frac{w_1}{w_1+w_2}F_1+\frac{w_2}{w_1+w_2}F_2 \\ &=(\overline{w}_1 a)l_1+(\overline{w}_1 b)m_1+(\overline{w}_1)n_1+(\overline{w}_2 a)l_2+(\overline{w}_2 b)m_2+(\overline{w}_2)n_2 \end{aligned} \tag{10}$$

The ANFIS model is utilized for the trust assessment process, in this, the two inputs are represented as trust weight and weight of node j, and the output is termed as trust value. The conditions for the trust value assessment are described as follows.

Rule 1: If the trust weight value is high and the weight of node *j* value is high, then the trust value is high.

Rule 2: If the trust weight value is low and the weight of node *j* value is low, then the trust value is low.

Rule 3: If the trust weight value is medium and the weight of node *j* value is medium, then the trust value is medium.

4.2. Route discovery

The process of route discovery is utilized to establish the optimal route for the packet transfer in the routing protocol in MANET. Here Group teaching optimization algorithm is utilized for the optimal route discovery. The routing process for the trust aware routing protocol consists of two parts: routing within the region and routing between the regions.

Group teaching optimization algorithm

The group teaching optimization algorithm is designed to enhance the entire class knowledge by suggesting the group teaching scheme [24]. To change the group teaching appropriate for employing the optimization technique, first consider the population, fitness value, and decision variables are equivalent to the students, students knowledge, and subjects of the students, correspondingly. This algorithm consists of four phases like teacher allocation phase, teacher phase, capability grouping phase, and student phase. The four phases are explained in detail in the following section.

Capability grouping phase

The information regarding the entire class is considered as the normal distribution. The normal distribution is described as

$$F(a)=\frac{1}{\sqrt{2\pi}\alpha}e^{\frac{-(a-p)^2}{2\alpha^2}} \tag{11}$$

From Eqn. (11), a represents the value of the normal distribution function, p represents the average information of the entire class and α represents the standard deviation. The differences in information between students are represented as the standard deviation α. If the value of the standard deviation is large, then the knowledge differences between the students are also large. The perfect teacher imagines not only enhances the knowledge, also decreases the standard deviation value. For obtaining this objective, the teacher made an appropriate teaching layout for the students.

Teacher phase

The student gained knowledge from the teacher that responds to the described second rule in this phase. The teacher made various layouts for the average group of students and the outstanding group of this algorithm. In the teacher phase I, for the strong capability of the receiving knowledge the teacher aims on enhancing the knowledge of the outstanding student groups as the whole in this algorithm. Particularly, the teacher tries their best for enhancing the mean knowledge of the entire class. Additionally, the differences in receiving knowledge between the students are to be regarded. Hence the outstanding student group attains the knowledge using Eqn. (12).

$$a_{teacher,\,j}^{t+1} = a_j^t + x \times \left(K^t - f \times \left(y \times N^t + z \times a_j^t \right) \right) \tag{12}$$

$$N^t = \frac{1}{M} \sum_{j=1}^{M} a_j^t \tag{13}$$

$$y + z = 1 \tag{14}$$

From Eqn. (14), t represents the present iteration numbers; M represents the number of students, a_j^t represents the student's knowledge, K^t represents the teacher's knowledge at time t, N^t represents the average knowledge of the group at time t, f represents the teaching parameter of the teacher. $a_{teacher,\,j}^{t+1}$ represents the knowledge of the student j, x,y, and z represents the three arbitrary numbers in the interval [0, 1]. The F value is either 1or 2 as made in [25].

In teacher phase II, the teacher provides more concentration for the poor capability of receiving knowledge to the average group than the outstanding group. Hence the students of the average group attain gain their knowledge is described as

$$a_{teacher,\,j}^{t+1} = a_j^t + 2 \times r \times \left(K^t - a_j^t \right) \tag{15}$$

From Eqn. (15), r represents the arbitrary number in the interval [0, 1].

Additionally, the student cannot achieve gain by the teacher phase is addressed as

$$a_{teacher,\,j}^{t+1} = \begin{cases} a_{teacher,\,j}^{t+1}, F\left(a_{teacher,\,j}^{t+1}\right) < F\left(a_j^t\right) \\ a_j^t, F\left(a_{teacher,\,j}^{t+1}\right) \geq F\left(a_j^t\right) \end{cases} \tag{16}$$

Student phase

The student phase contains the student phase I as well as the student phase II respective to the declared third rule. In the extra period, the student attains the knowledge with two various schemes: one via the self-learning and the other via communication among the students that is described as

$$a_{student,\,j}^{t+1} = \begin{cases} a_{teacher,\,j}^{t+1} + d \times \left(a_{teacher,\,j}^{t+1} - a_{teacher,\,k}^{t+1} \right) + h \times \left(a_{teacher,\,j}^{t+1} - a_j^t \right), F\left(a_{teacher,\,j}^{t+1}\right) < F\left(a_{teacher,\,k}^{t+1}\right) \\ a_{teacher,\,j}^{t+1} - d \times \left(a_{teacher,\,j}^{t+1} - a_{teacher,\,k}^{t+1} \right) + h \times \left(a_{teacher,\,j}^{t+1} - a_j^t \right), F\left(a_{teacher,\,j}^{t+1}\right) \geq F\left(a_{teacher,\,k}^{t+1}\right) \end{cases} \tag{17}$$

From Eqn. (17), d and h represent the random numbers in the interval [0, 1]. $a_{student,\,j}^{t+1}$ represents the knowledge of the student j and $a_{teacher,k}^{t+1}$ represents the knowledge of the student k. The second term as well as the third term of Eqn. (17) indicates the right mean learning from the student as well as the self-learning. Additionally, the student cannot achieve knowledge with the student phase that is described as

$$a_j^{t+1} = \begin{cases} a_{teacher,\,j}^{t+1}, F\left(a_{teacher,\,j}^{t+1}\right) < F\left(a_{student,\,j}^{t+1}\right) \\ a_{student,\,j}^{t+1}, F\left(a_{teacher,\,j}^{t+1}\right) \geq F\left(a_{student,\,j}^{t+1}\right) \end{cases} \tag{18}$$

From Eqn. (18), a_j^{t+1} represents the student knowledge at occasion t+1 after the learning cycle.

Teacher allocation phase

Depends upon the described fourth rule, the teacher allocation method is more significant for enhancing the student's knowledge. The teacher allocation scheme is described as

$$K^t = \begin{cases} a_{first}^t, & F\left(a_{first}^t\right) \le F\left(\dfrac{a_{first}^t + a_{second}^t + a_{third}^t}{3}\right) \\ \dfrac{a_{first}^t + a_{second}^t + a_{third}^t}{3}, & F\left(a_{first}^t\right) > F\left(\dfrac{a_{first}^t + a_{second}^t + a_{third}^t}{3}\right) \end{cases} \tag{19}$$

From Eqn. (19), a_{first}^t , a_{second}^t ,and a_{third}^t represents the first, second, and third best students. To speed up the algorithms convergence, the outstanding group, as well as the average group shares the same teacher. By using the value of the teacher phase and student phase, two populations are constructed. These two populations together construct the new population which is the optimal value. So this optimal value is utilized for the efficient route discovery process. Thus by using the algorithm, route discovery is established for efficient data transmission between sources to destination. If the routing protocol is proactive, the routing protocol is classified into two categories: routing inside the zones and routing between the zones.

In the route discovery inside the zones, the central node transmits the route request message from the source to the destination and it discovers the new route or the middle node that routes the packet to the destination node. After the route is established, the destination node transmits the route confirmation message to the source. The route now established is to maintain the optimal path for forwarding the packets from source to destination.

In the route discovery between the zones, when the source sends the data packets to the destination, the node first checks the zone routing table for the route. If there is no existing route, then the route discovery between the zones are triggered. Initially, the source node checks for the multi-zone route table to evaluate if it has any unexpired routes. If the node is established, then the node sets the time and forwards the route request message for establishing the new route. When the node reaches the intermediate node, the node further checks the unexpired route in the multi-zone route table. If there is more than one route, the optimal route is selected and the message is transmitted back to the source node in the optimal path. When the destination node arrives at the intermediate node on the way to the source node, the new route is added to the multi-zone routing table. Hence the multi-zone routing tab contains the new route. When no route is established with the fixed time or threshold, the routing process fails. If there establishes multiple routes, then the adaptive equilibrium optimizer is utilized to find the optimal new route for the transmission of packets.

4.3. Optimal route selection procedure

The route discovery process utilizes the group teaching optimization algorithm. Due to the establishment of multiple routes, the optimal route selection is the main problem in the route discovery process, so adaptive equilibrium optimizer is utilized for the optimal route selection procedure.

Adaptive equilibrium optimizer

The adaptive equilibrium optimizer is proposed for the identification of the optimal route for the packet transmission. The adaptive equilibrium optimizer [26] is the advancement of the equilibrium optimizer [27]. This algorithm depends upon the arbitrary spreading of the search agents within the search space that is chosen from the fitness value. The equilibrium optimizer is encouraged by the equilibrium as well as the dynamic condition that depends upon the mass preservation law through leaving, generating, and entering the control volume.

Let us consider the search agents linked with the search space concentration and the iteration is initialized at $itr = 1$ as pursues:

$$Z_j\,(itr=1) = l_b + rand_j\,(1,e) * (u_b - l_b), \quad j = 1,2,...,M \tag{20}$$

From Eqn. (20), l_b and u_b represents the search space lower as well as the upper bounds, M represents the search agents, e represents the problem dimension, and $rand_j$ represents the 1-D vector that contains the arbitrary number in the interval 0 and 1. The jth search agent location for the control volume C_v in equilibrium optimizer is updated as

$$\overrightarrow{Z}_j\,(new) = \overrightarrow{Z}_{eq}\,(itr) + \left(\overrightarrow{Z}_j\,(itr) - \overrightarrow{Z}_{eq}\,(itr)\right) * \overrightarrow{E}_j\,(itr) + \frac{g_j(itr)}{\overrightarrow{\eta}_j\,(itr) * C_V} \times \left(1 - \overrightarrow{E}_j\,(itr)\right) \tag{21}$$

$\overrightarrow{Z}_{eq}$ determines the arbitrarily selected equilibrium candidate from the pool of equilibrium $\overrightarrow{Z}_{eq\cdot pool}$ of the four best search agents $\overrightarrow{Z}_{eq(1)}, \overrightarrow{Z}_{eq(2)}, \overrightarrow{Z}_{eq(3)}, \overrightarrow{Z}_{eq(4)}$; and the average of the mentioned four search agents is described as $\overrightarrow{Z}_{eq(avg)}$. The values of $\overrightarrow{Z}_{eq(1)}, \overrightarrow{Z}_{eq(2)}, \overrightarrow{Z}_{eq(3)}, \overrightarrow{Z}_{eq(4)}$ are chosen by the fitness values such as $F\left(\overrightarrow{Z}_{eq(1)}\right), F\left(\overrightarrow{Z}_{eq(2)}\right), F\left(\overrightarrow{Z}_{eq(3)}\right)$ and $F\left(\overrightarrow{Z}_{eq(4)}\right)$. For the issue of minimization, the fitness values as well as the equilibrium candidates are determined by the assistance of the sorted list. The value of the fitness of the entire M search agents are described as:

$$F = \left(F_1, F_2, ..., F_3\right) \tag{22}$$

These fitness values are organized in ascending order:

$$\left[sorted\_F, sort\_index\right] = sort\left(F\right) \tag{23}$$

Now the equilibrium candidates, as well as the fitness values, are expressed as:

$$
\begin{aligned}
&F\left(\vec{Z}_{eq(1)}\right)=sorted\_F(1)\ and\ \vec{Z}_{eq(1)}=\vec{Z}\left(sort\_index(1)\right)\\
&F\left(\vec{Z}_{eq(2)}\right)=sorted\_F(2)\ and\ \vec{Z}_{eq(2)}=\vec{Z}\left(sort\_index(2)\right)\\
&F\left(\vec{Z}_{eq(3)}\right)=sorted\_F(3)\ and\ \vec{Z}_{eq(3)}=\vec{Z}\left(sort\_index(3)\right)\\
&F\left(\vec{Z}_{eq(4)}\right)=sorted\_F(4)\ and\ \vec{Z}_{eq(4)}=\vec{Z}\left(sort\_index(4)\right)\\
&\vec{Z}_{eq(avg)}=\frac{1}{4}\left(\vec{Z}_{eq(1)}+\vec{Z}_{eq(2)}+\vec{Z}_{eq(3)}+\vec{Z}_{eq(4)}\right)
\end{aligned}
\tag{24}
$$

Ultimately, the pool of the equilibrium is described as:

$$
\vec{Z}_{eq,pool}=\left\{\vec{Z}_{eq(1)},\vec{Z}_{eq(2)},\vec{Z}_{eq(3)},\vec{Z}_{eq(4)},\vec{Z}_{eq(avg)}\right\} \tag{25}
$$

The exponential factor $\vec{E}_j$ is to help the equilibrium optimizer for the exploitation as well as the exploration is computed for the jth search agents as

$$
\vec{E}_j(itr)=x_1\,sign\left(s_1-0.5\right)\left[e^{-\vec{\eta}_j\left(1-\frac{itr}{\max\_itr}\right)\left(x_2\frac{itr}{\max\_itr}\right)}\right] \tag{26}
$$

From Eqn. (26), the factor x_1 is employed for controlling the exploration function, x_2 is employed for exploitation control, *sign* is for controlling the search direction that depends upon the arbitrary number s_1 in the interval 0 and 1, $\vec{\eta}_j(itr)$ represents the arbitrary vector of dimension *e* in the range 0 and 1 for the jth search agent in itr iterations, itr represents the present iterations and max_ itr represents the highest number of iterations where the equilibrium optimizer go for updating the location.

The generation rate $\vec{g}_j$ assists the exploration stage using participation probability $\vec{Z}_{eq}$. The $\vec{g}_j$ is described as

$$
\vec{g}_j(itr)=\vec{g}_{j,0}(itr)*\vec{E}_j(itr) \tag{27}
$$

The $\vec{g}_{j,0}(itr)$ and $\overline{grc_j}(itr)$ are computed as

$$
\vec{g}_{j,0}(itr)=\overline{grc}_j(itr)\left(\vec{Z}_{eq}(itr)-\vec{\eta}_j(itr)\right) \tag{28}
$$

$$
\overline{grc}_j(itr)=\begin{cases}0.5\,s_1 & s_2\geq g_p\\ 0 & s_2\geq g_p\end{cases} \tag{29}
$$

From the above equations, *grc* represents the control factor of the generation rate and g_p represents the generation probability, s_1 and s_2 represents the arbitrary numbers in the range 0 and 1. The adaptive decision is made by using the present fitness and average fitness of the entire search agents and the minimization issue is described as

$$\overrightarrow{Z}_j(itr+1)=\begin{cases}\overrightarrow{Z}_j(new) & F_j(itr) < F_{avg}(itr)\\ \overrightarrow{Z}_j(new)\otimes(0.5+rand(1,e)) & F_j(itr)\geq F_{avg}(itr)\end{cases} \tag{30}$$

From Eqn. (30), $\otimes$ indicates the component-wise multiplication, $F_j(itr)$ indicates the fitness value at iteration itr and $F_{avg}(itr)$ indicates the fitness value of the entire search agents and is computed as

$$F_{avg}(itr)=\frac{1}{M}\sum_{j=1}^{M}F_j(itr) \tag{31}$$

The adaptive equilibrium optimizer takes over the concepts of memory storage from the equilibrium optimizer. So compare both the fitness values of the present iterations as well as the earlier iteration and then updated once it obtained the optimal fitness value and it is formulated as

$$\overrightarrow{Z}_j(itr)=\begin{cases}\overrightarrow{Z}_j(itr) & itr>1\ and\ F_j(itr)<F_j(itr-1)\\ \overrightarrow{Z}_j(itr-1) & itr>1\ and\ F_j(itr)\geq F_j(itr-1)\\ \overrightarrow{Z}_j(itr) & itr=1\end{cases} \tag{32}$$

$$\text{And } F_j(itr)=\begin{cases}F_j(itr) & itr>1\ and\ F_j(itr)<F_j(itr-1)\\ F_j(itr-1) & itr>1\ and\ F_j(itr)\geq F_j(itr-1)\\ F_j(itr) & itr=1\end{cases} \tag{33}$$

Pseudocode: AO algorithm
Assign the search agents numbers M, maximum iteration numbers max_ itr, search dimensions e, and the free factors like x_1, x_2, g_p, C_V
Initialization: Create the arbitrary location vector Z_j of the jth search agent by Eqn. (20) fir the M search agent for iteration $itr=1$.
for $itr=1$:max_ itr
Compute the fitness value F for the present iteration
Determine the equilibrium candidates $\overrightarrow{Z}_{eq(1)}, \overrightarrow{Z}_{eq(2)}, \overrightarrow{Z}_{eq(3)}, \overrightarrow{Z}_{eq(4)}$ using Eqn. (24)
Create the equilibrium pool $\overrightarrow{Z}_{eq\cdot pool}$ using Eqn. (25)
Achieve memory storage using Eqn. (32) and (33)
for $j=1:M$
Arbitrarily select $\overrightarrow{Z}_{eq}$ from $\overrightarrow{Z}_{eq\cdot pool}$
Create the exponential term $\overrightarrow{E}_j$ by Eqn. (26)
Create the generation rate $\overrightarrow{g}_j$ by Eqn. (27)
Determine the average fitness F_{avg} by Eqn. (31)
Determine the search agent location $\overrightarrow{Z}_j(new)$ by Eqn. (21)
Search agent location is updated $\overrightarrow{Z}_j$ for the subsequent iteration by Eqn. (30)

end for
end for
Return the optimal solution as $\overset{\nu}{Z}_{eq(1)}$ and its best fitness as $F\left(\overset{\nu}{Z}_{eq(1)}\right)$.

The node passing through the multiple zones are described in the route selection process. Let us consider that the source nodes tend to forward the data packets from the source to the destination and the route is selected for the transmission purpose. Initially, the route checks in the zone route tab to know whether there is any local route that matches with the earlier nodes after the source node. If there is more than one local route in the zone then AO is utilized to replace the existing route. This procedure is iterated until the packet arrives at the destination. Thus by the adaptive equilibrium optimizer (AO), the optimal route is explored for the efficient packet data transmission from source to destination.

4.4. Route maintenance procedure

Route maintenance is the process that manages the failures of the route particularly caused due to node mobility or faulty nodes that is more frequent in MANETs. If the damaged route links with the nodes inside the zone, several alternative routes are established in the zone routing table and an alternative route is selected that depends upon the optimization technique. When there is no alternative path, then the path is launched after some time due to the adoption of the proactive routing protocol.

If the damaged path links with the multiple zones, then the upstream node triggers the restricted repair method to establish the new route that is identical to the process of route discovery between the zones. If the alternate route is established, then the communication persists and the warning is forwarded to the source node for updating the multi-zone routing tab for every node on the path. If the error message is received but the source requires transmitting the data packets, then the source selects the alternate unexpired route present in the multi-zone route table and also starts the process of route discovery between the zones.

Table 2: Parameters for the network simulation

Parameter	**Value**
Simulator	NS-3.25
Topology	Arbitrary node placement
Simulation area	1200 x 1200 sq. m
Number of nodes	100
Packet size	256 bytes
Channel type	Wireless
Simulation time	500s
Antenna type	Omni-directional
Initial Energy	75 Joules

5. RESULTS AND DISCUSSIONS

The proposed approach is analyzed using the network simulator ns-3 and compare the simulation results with the other existing approaches like B-iHTRP [21], HyphaNet [28], QNewBee [29], and Crowwhale-ETR [30]. In the simulation environment, 100 nodes are consistently distributed in the area of 1200 x 1200 sq.m. For this scheme, every node moves

in an arbitrary path at a speed uniformly distributed. When the node arrives at the target location, it stops the node for 5s rest and then moves identically. Here in this paper, malicious node detection is considered. The simulation is performed for the pause time ranging from 0 to 50 seconds. Table 2 describes the simulation parameters.

5.1. Performance metrics

The metrics utilized for the examination are packet delivery rate, throughput, packet drop rate, detection rate, routing overhead, delay, and energy consumption [32]. The description of the measures are described below.

Throughput: It describes the total amount of packets distributed to the destination from the source node. It is expressed as

$$Throughput = \frac{packets\ \ delivered}{simulation\ time} \tag{34}$$

Packet delivery rate: It is defined as the proportion of the total amount of effectively distributed to the number of transmitted packets. It is expressed as below

$$Packet\,delivery\,ratio = \frac{\sum packets\,received}{\sum packets\,transmitted} \tag{35}$$

Average delay: It is described as the time dissimilarity among the current packets accepted and the earlier packets accepted, in that *m* represents the node numbers. It is expressed by the below equation.

$$Average\ \ Delay = \frac{\sum packets\,received\,time - packet\,sent\,time}{m} \tag{36}$$

Packet loss rate: It is described as the proportion of the lost packets to the total amount of packets transmitted that is expressed in the Eqn. (37).

$$Packets\,loss\,rate = \frac{\sum packets\,lost}{\sum packets\,transmitted} \tag{37}$$

Detection rate: It is described as the percentage of successfully identified attackers in the network.

Routing overhead: It is the excess data forwarded employed for control. It is described as the proportion of the amount of control information to the total amount of transmitted information.

Energy consumption: The energy consumed by the network is described as the total energy necessitated by the nodes in accepting, broadcasting, and sending the information. Initially, every node assigned the starting energy and each energy level is calculated every time as the simulation measures.

5.2. Performance Analysis

The comparative analyses of the approaches are described in this segment, and the analysis is evaluated that depends upon the performance measures. This analysis is performed in the presence of malicious nodes to express the efficiency of the proposed approach. This section describes the comparative analysis with the help of 100 nodes with the existence of attacks.

Fig 3 shows the comparative analysis of the throughput of the proposed approach with other existing approaches like B-iHTRP, HyphaNet, QNewBee, and Crowwhale-ETR. It is concluded that the throughput of the proposed approach is high when compared to other existing approaches.

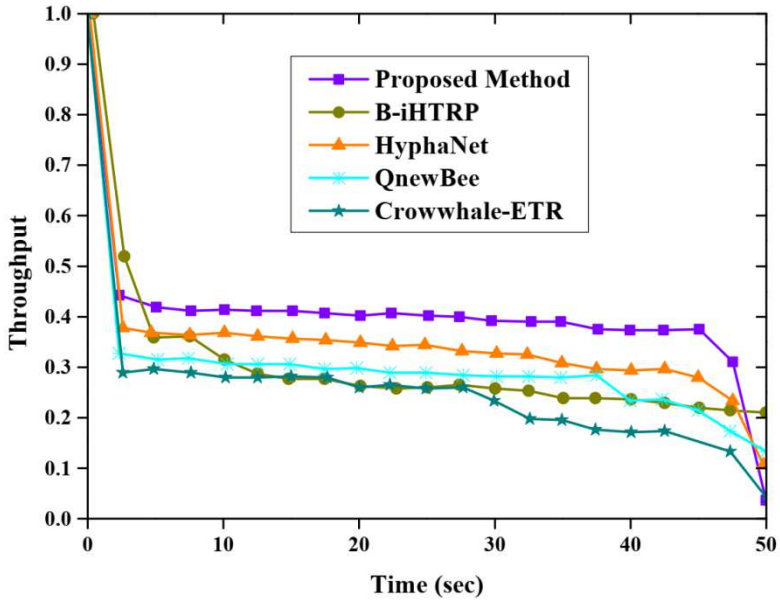

Fig 3: Comparative analysis of throughput

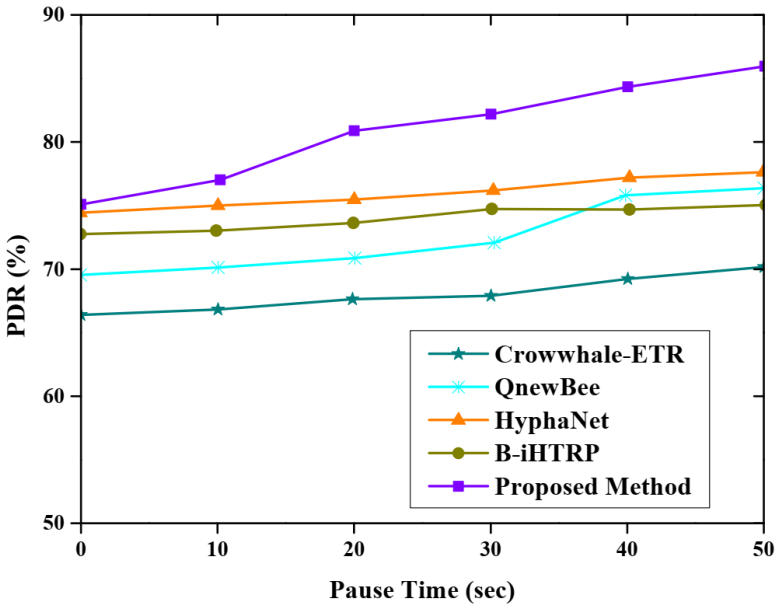

Fig 4: Comparative analysis of packet delivery rate

Fig 4 represents the consequences of changing the pause time on the packet delivery ratio for the proposed approach, B-iHTRP, HyphaNet, QNewBee, and Crowwhale-ETR

routing approaches. When the pause time is maximized, the packet delivery ratio is also increased. The proposed approach achieved better performance concerning the packet delivery ratio than other routing approaches. The results describe that the proposed approach achieved a high packet delivery rate than other state-of-art approaches.

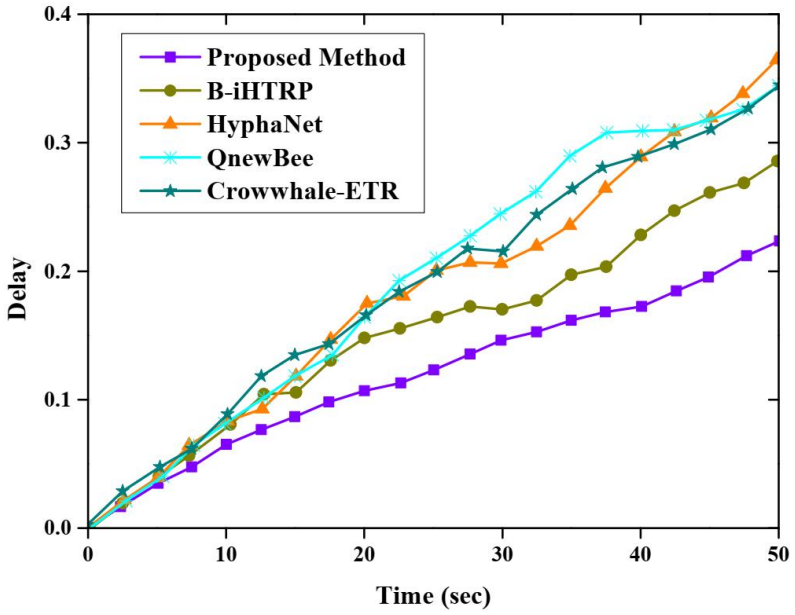

Fig 5: Comparative analysis of the average delay

Fig 5 demonstrates the analysis that depends upon the average delay. In the starting of packet transmission, there is no delay. When the node is moving towards the destination, the delay is increased with an increase in time. From the figure, it is apparent that the proposed approach obtained minimum delay when compared with other approaches like B-iHTRP, HyphaNet, QNewBee, and Crowwhale-ETR.

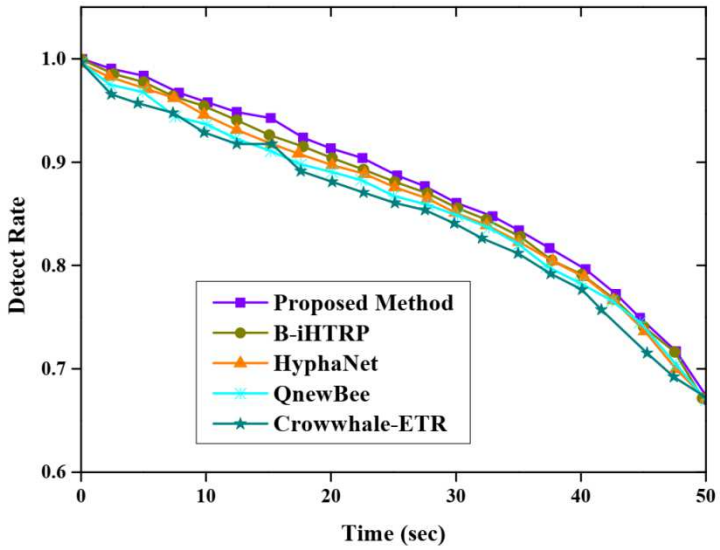

Fig 6: Comparative analysis of the detection rate

The comparative analysis of the detection rate is demonstrated in Fig 6. The efficient approach must provide the largest detection rate that calculates efficient attack detection. From the figure, it is clear that the detection rate decreases with an increase in time but the

proposed approach provides a high detection rate when compared to other existing approaches likeB-iHTRP, HyphaNet, QNewBee, and Crowwhale-ETR. The detection rate launches the opinion that differentiates the normal nodes from the malicious nodes, it detects the malicious nodes with more accuracy.

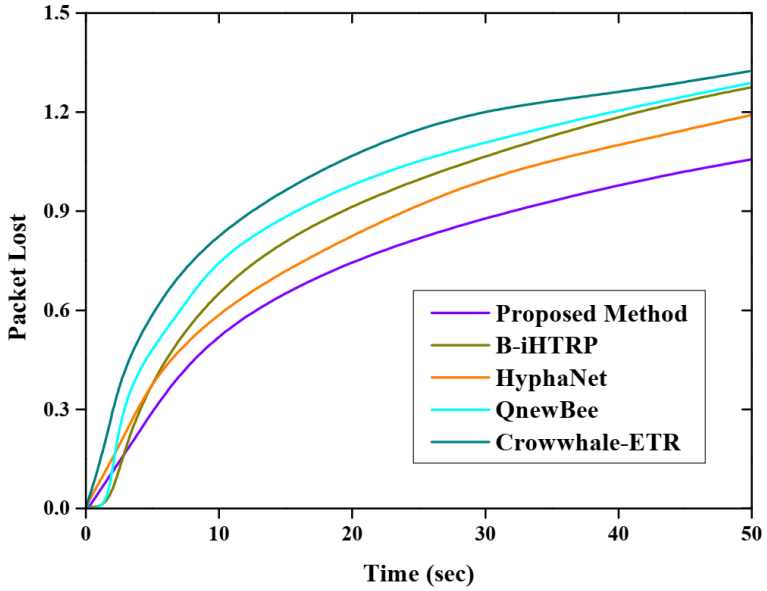

Fig 7: Comparative analysis of the packet loss rate

Figure 7 demonstrates that the comparative analysis of the packet loss rate for the proposed approach with other approaches such asB-iHTRP, HyphaNet, QNewBee, and Crowwhale-ETR. From the figure, it is proved that the proposed approach obtained a low packet loss rate when compared with state-of-art approaches.

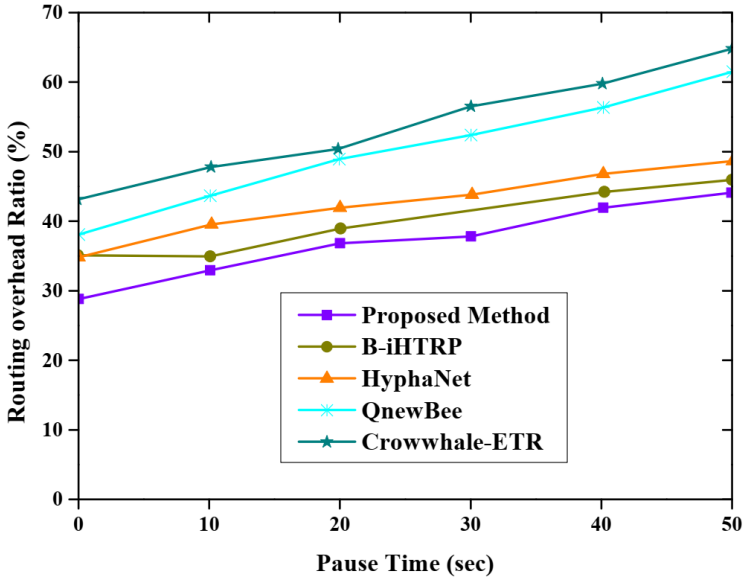

Fig 8: Comparative analysis of the routing overhead ratio

For this simulation, the routing overhead was computed for the proposed approach, B-iHTRP, HyphaNet, QNewBee, and Crowwhale-ETR by changing the time. Figure 8 depicts the routing overhead that happened during the routing process. The proposed approach has the ratio of routing overhead from 29.4% to 34.6%, B-iHTRP achieves from 34.3% to 36.2%, HyphaNet achieves from

34.3% to 38.5%, QNewBee achieves overhead from 38.7% to 61.4% and Crowwhale achieves from 43.4% to 64.4%. It clearly states that the routing overhead for the proposed approach is less when compared to other approaches.

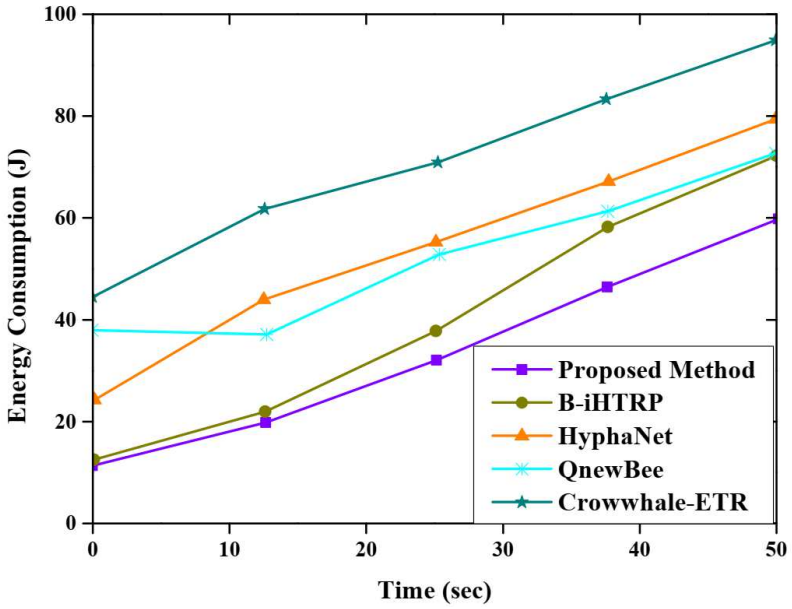

Fig 9: Comparative analysis of the energy consumption

Figure 9 demonstrates the energy consumption of the proposed approach when compared with B-iHTRP, HyphaNet, QNewBee, and Crowwhale-ETR. The energy consumption for the proposed approach is low when compared with other state-of-art methods. The proposed approach consumes 19 Joules in 10 seconds, and in 50 seconds it consumes 59 Joules, whereas B-iHTRP consumes 22 Joules in 10 seconds and in 50 seconds it consumes 66Joules, HyphaNet consumes 42 Joules in 10 seconds and in 50 seconds it consumes 79 Joules, QNewBee consumes 36 Joules in 10 seconds and in 50 seconds it consumes 67 Joules and finally, Crowwhale-ETRconsumes 62 Joules in 10 seconds and in 50 seconds it consumes 87 Joules. The proposed approach has better energy consumption than other approaches.

6. CONCLUSION

The optimal route selection for efficient packet transmission is the most significant issue in MANET. In this paper, the ANFIS model is utilized for the determination of the trust evaluation. The group teaching optimization algorithm (GTA) is proposed for the route discovery scheme. By using this GTA scheme several routes are established. So the optimal route is selected with the help of the adaptive equilibrium optimizer (AO) algorithm. Then the route is maintained for effective packet transmission. This approach increases the trust and security in the packet transmission.Simulation results exposed that the proposed approach outperforms other approaches such as B-iHTRP, HyphaNet, QNewBee, and Crowwhale-ETR in terms of throughput, end-to-end delay, energy consumption, routing overhead, detection rate, packet loss rate, and packet delivery ratio. This approach improves the network throughput by accurate packet distribution, detection rate, decreases the delay, increases the packet delivery rate, reduced energy consumption as well as the packet loss rate via various

paths in the presence of the attacks. The future work is enlarged to implement this approach in real-time experiments and also to test the feasibility of the network.

Funding: Not applicable

Conflicts of interest Statement: Not applicable

Ethics approval:

Compliance with Ethical Standards

Conflict of interest

The authors declare that they have no conflict of interest.

Human and Animal Rights

This article does not contain any studies with human or animal subjects performed by any of the authors.

Informed Consent

Informed consent was obtained from all individual participants included in the study.

Consent to participate: Not applicable

Consent for publication: Not applicable

Availability of data and material: Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Code availability: Not applicable

Authors' contributions

RH agreed on the content of the study. RH, RU and SJ collected all the data for analysis. RH agreed on themethodology. RH, RU and SJ completed the analysis based on agreed steps. Results and conclusions arediscussed and written together. The author read and approved the final manuscript.

REFERENCES

[1] Velagaleti SB, Departmnet IT, GNITS S, Seetha M, Departmnet CS, Raju SV. A Novel Method for Trust Evaluation in a Mobile Ad Hoc Network. International Journal of Computer Science and Information Security (IJCSIS). 2020 Feb; 18(2).

[2] Santhosh RM. Securing Public Key Infrastructure based Manets by using Efficient Trust Computation, International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 05 | May 2019

[3] Srinadh NR, Satyanarayana B. Power-Aware Secure Routing protocol in MANET based on Reputation Model and Optimization. International Journal of Applied Engineering Research. 2019; 14(11):2704-16.

[4] Anjali P, Kallada JJ. Fitness Function As Trust Value Using To Efficient Multipath Routing For Mobile Ad Hoc Network, International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 05 | May 2019
[5] Sathyaraj P, Devi DR. Designing the routing protocol with secured IoT devices and QoS over Manet using trust-based performance evaluation method. Journal of Ambient Intelligence and Humanized Computing. 2020 Jul 30:1-9.
[6] Kausar Fatima S, Gauhar Fatima S, Abdul Sattar S, Srinivasa Rao DD. A Security Scheme Based on Trust Attack in Manet. International Journal of Advanced Research in Engineering and Technology. 2019; 10(2).
[7] Ananthakumaran S, Sathishkumar M, Bhavani R, Reddy RR. Prevention of Routing Attacks using Trust-Based Multipath Protocol. International Journal. 2020 May; 9(3).
[8] Ponguwala M, Rao DS. Secure Group based Routing and Flawless Trust Formulation in MANET using Unsupervised Machine Learning Approach for IoT Applications. EAI Endorsed Transactions on Energy Web. 2019 Oct 1; 6(24).
[9] Yang H. A Study on Improving Secure Routing Performance Using Trust Model in MANET. Mobile Information Systems. 2020 Sep 16; 2020.
[10] Lwin MT, Yim J, Ko YB. Blockchain-Based Lightweight Trust Management in Mobile Ad-Hoc Networks. Sensors. 2020 Jan; 20(3):698.
[11] Nandgave-Usturge S. Water Spider Monkey Optimization Algorithm for Trust-based MANET Secure Routing in IoT, International Journal of Scientific Research & Engineering Trends, Volume 6, Issue 2, Mar-Apr-2020, pp. 980-984.
[12] Mukhedkar MM, Kolekar U. Trust-based secure routing in mobile ad hoc network using hybrid optimization algorithm. The Computer Journal. 2019 Sep 1; 62(10):1528-45.
[13] Sun Z, Wei M, Zhang Z, Qu G. Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks. Applied Soft Computing. 2019 Apr 1; 77:366-75.
[14] Mukhedkar MM, Kolekar U. E-TDGO: An encrypted trust-based dolphin glowworm optimization for secure routing in mobile ad hoc network. International Journal of Communication Systems. 2020 May 10;33(7):e4252.
[15] Kanagasundaram H, Ayyaswamy K. Multi objective ALO based energy efficient and secure routing OLSR protocol in MANET. International Journal of Intelligent Engineering and Systems. 2019; 12(1):74-83.
[16] Alkhamisi AO, Buhari SM, Tsaramirsis G, Basheri M. An integrated incentive and trust-based optimal path identification in ad hoc on-demand multipath distance vector routing for MANET. International Journal of Grid and Utility Computing. 2020;11(2):169-84.
[17] Mariadas AE, Madhanmohan R. Hybrid PSO-DE algorithm-based trust and congestion aware cluster routing algorithm for MANET. International Journal of Cloud Computing. 2020; 9(2-3):330-54.
[18] Keum D, Lim J, Ko YB. Trust Based Multipath QoS Routing Protocol for Mission-Critical Data Transmission in Tactical Ad-Hoc Networks. Sensors. 2020 Jan; 20(11):3330.

[19] Kumar R, Shekhar S. Trust-Based Fuzzy Bat Optimization Algorithm for Attack Detection in Manet. In Smart Innovations in Communication and Computational Sciences 2020 (pp. 3-12). Springer, Singapore.

[20] Merlin RT, Ravi R. Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET. Wireless Personal Communications. 2019 Feb 28; 104(4):1599-636.

[21] Zhang M, Yang M, Wu Q, Zheng R, Zhu J. Smart perception and autonomic optimization: A novel bio-inspired hybrid routing protocol for MANETs. Future generation computer systems. 2018 Apr 1; 81:505-13.

[22] Yi JH, Deb S, Dong J, Alavi AH, Wang GG. An improved NSGA-III algorithm with adaptive mutation operator for Big Data optimization problems. Future Generation Computer Systems. 2018 Nov 1; 88:571-85.

[23] Buragohain, M., & Mahanta, C. (2008). A novel approach for ANFIS modeling based on full factorial design. Applied Soft Computing, 8, 609–625.

[24] Zhang Y, Jin Z. Group teaching optimization algorithm: A novel metaheuristic method for solving global optimization problems. Expert Systems with Applications. 2020 Jun 15; 148:113246.

[25] Rao, R. V., Savsani, V. J., & Vakharia, D. P. (2012). Teaching–Learning-Based optimization: An optimization method for continuous non-linear large scale problems. Information Sciences, 183(1), 1–15.

[26] Wunnava A, Naik MK, Panda R, Jena B, Abraham A. A novel interdependence based multilevel thresholding technique using adaptive equilibrium optimizer. Engineering Applications of Artificial Intelligence. 2020 Sep 1;94:103836.

[27] Faramarzi, A., Heidarinejad, M., Stephens, B., Mirjalili, S., 2020. Equilibrium optimizer: A novel optimization algorithm. Knowl.-Based Syst. 191, 105190.

[28] da Costa Bento CR, Wille EC. Bio-inspired Routing Algorithm for MANETs Based on Fungi Networks. Ad Hoc Networks. 2020 Jun 13:102248.

[29] Labed S, Kout A, Chikhi S. A New Approach based Bee Colony for the Resolution of Routing Problem in Mobile Ad-Hoc Networks. International Journal of Applied Metaheuristic Computing (IJAMC). 2019 Apr 1; 10(2):131-51.

[30] Shende DK, Sonavane SS. CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications. Wireless Networks. 2020 Mar 25:1-9.

[31] Çaydaş U, Hasçalık A, Ekici S. An adaptive neuro-fuzzy inference system (ANFIS) model for wire-EDM. Expert Systems with Applications. 2009 Apr 1;36(3):6135-9.

[32] Jayalakshmi P, Saravanan R. ACO-based enhanced energy-efficient intelligent routing protocol for MANET. International Journal of Grid and Utility Computing. 2020;11(4):435-42.

Figures

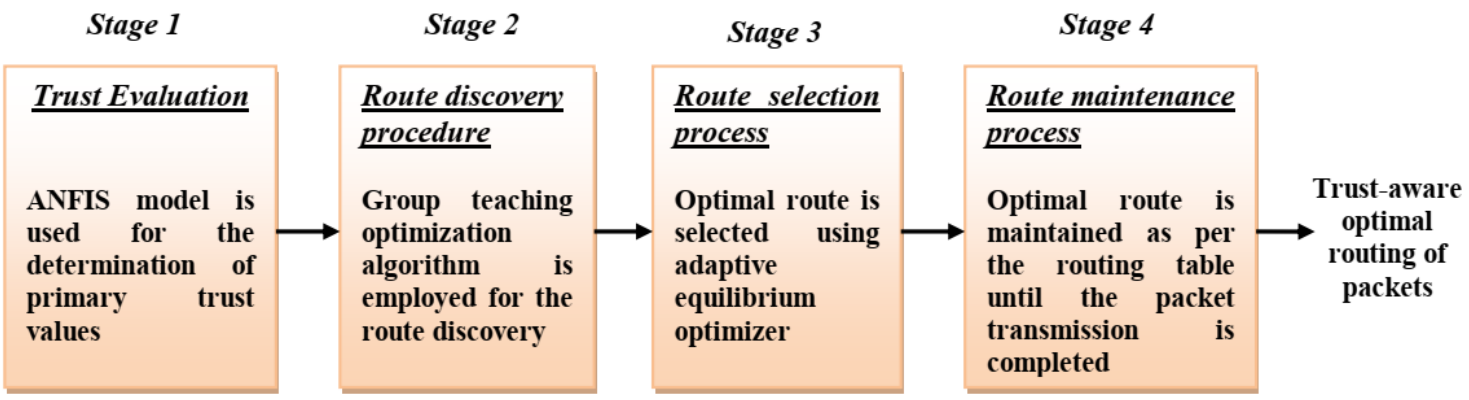

Figure 1

Proposed framework for the trust-aware routing protocol

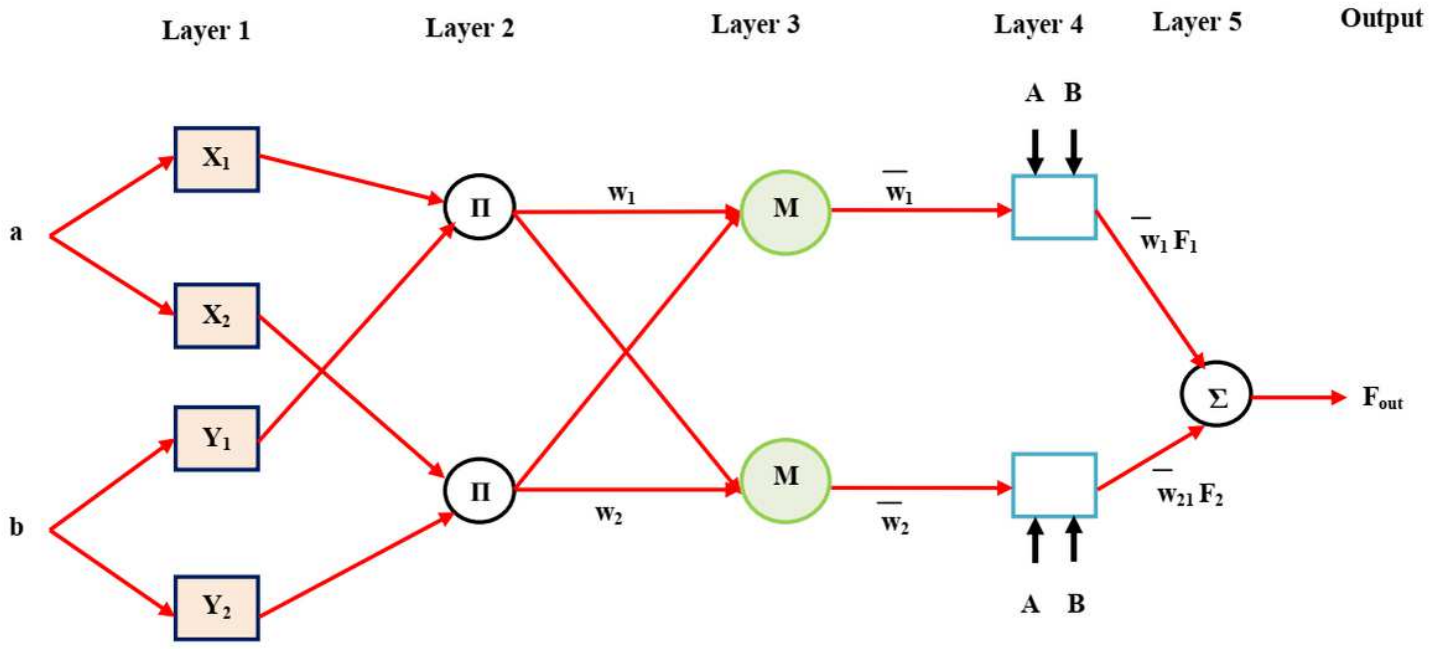

Figure 2

Structural design of ANFIS

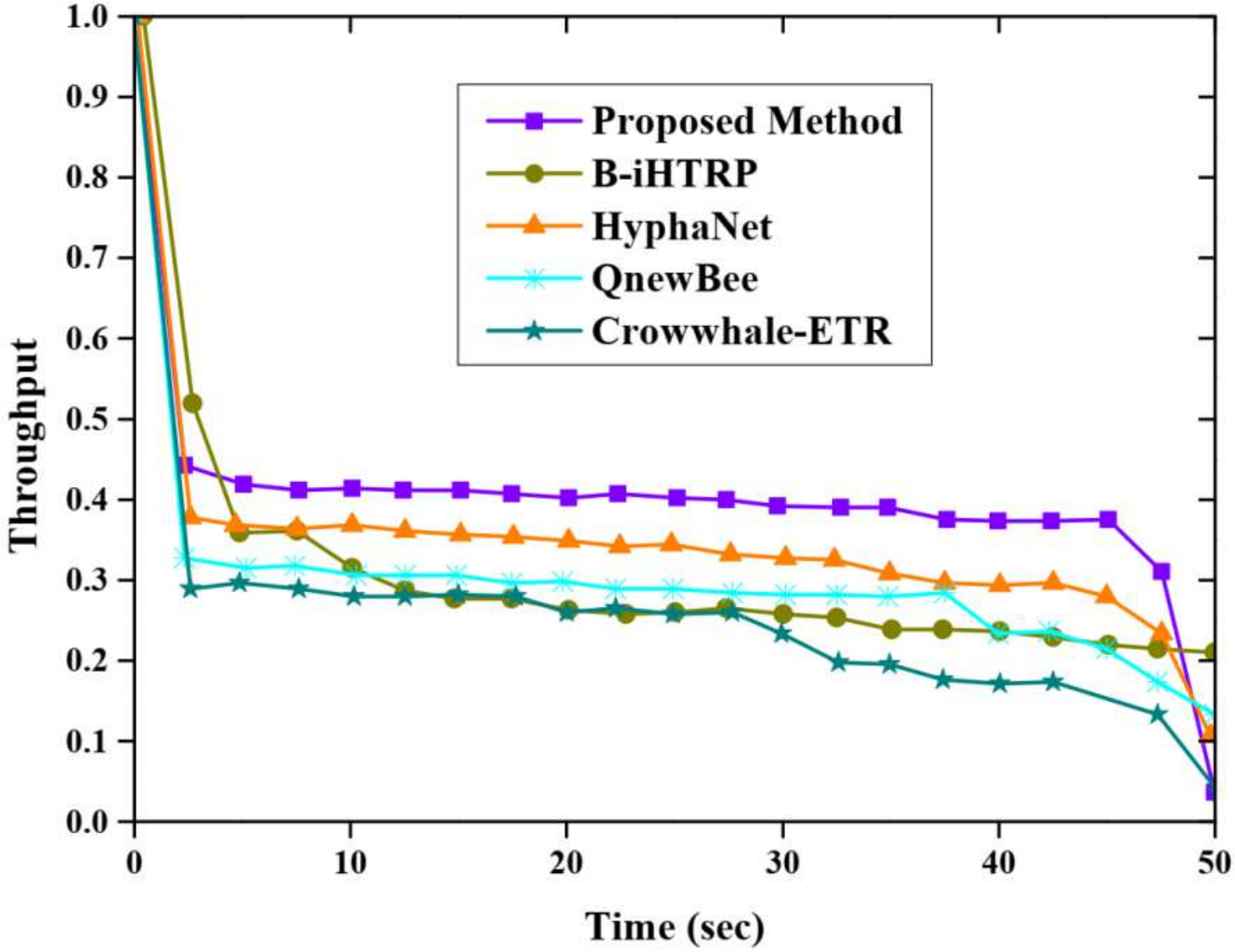

Figure 3

Comparative analysis of throughput

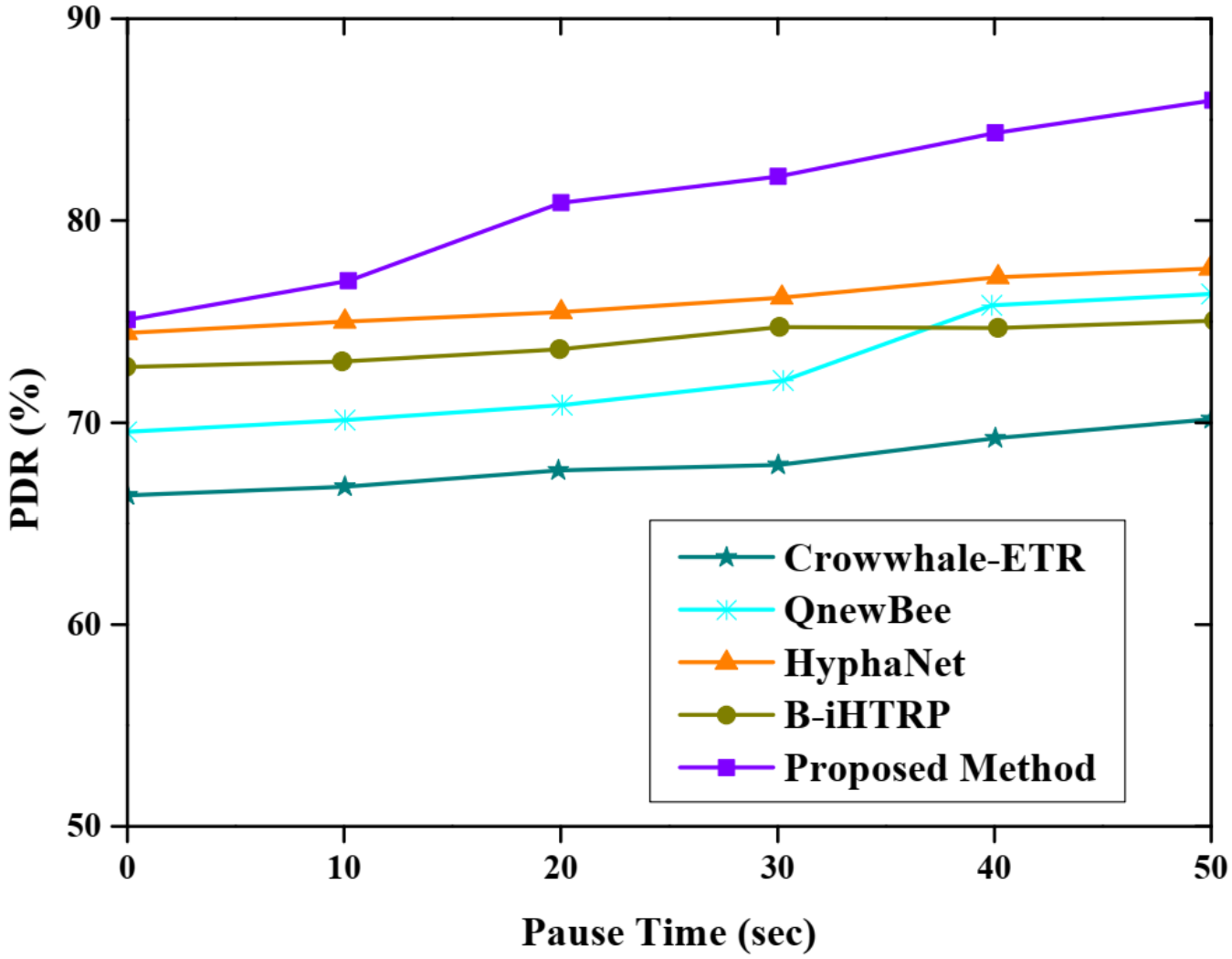

Figure 4

Comparative analysis of packet delivery rate

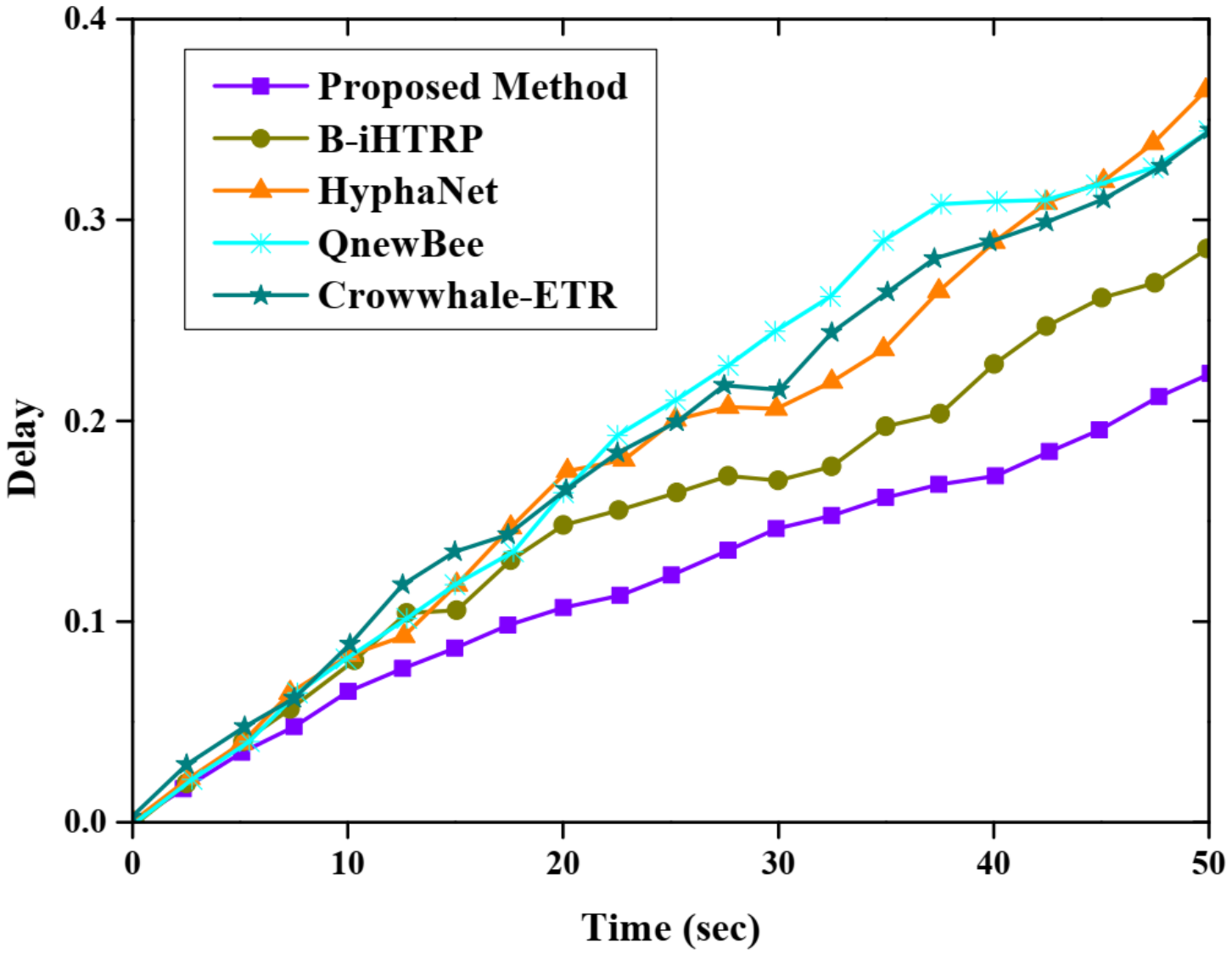

Figure 5

Comparative analysis of the average delay

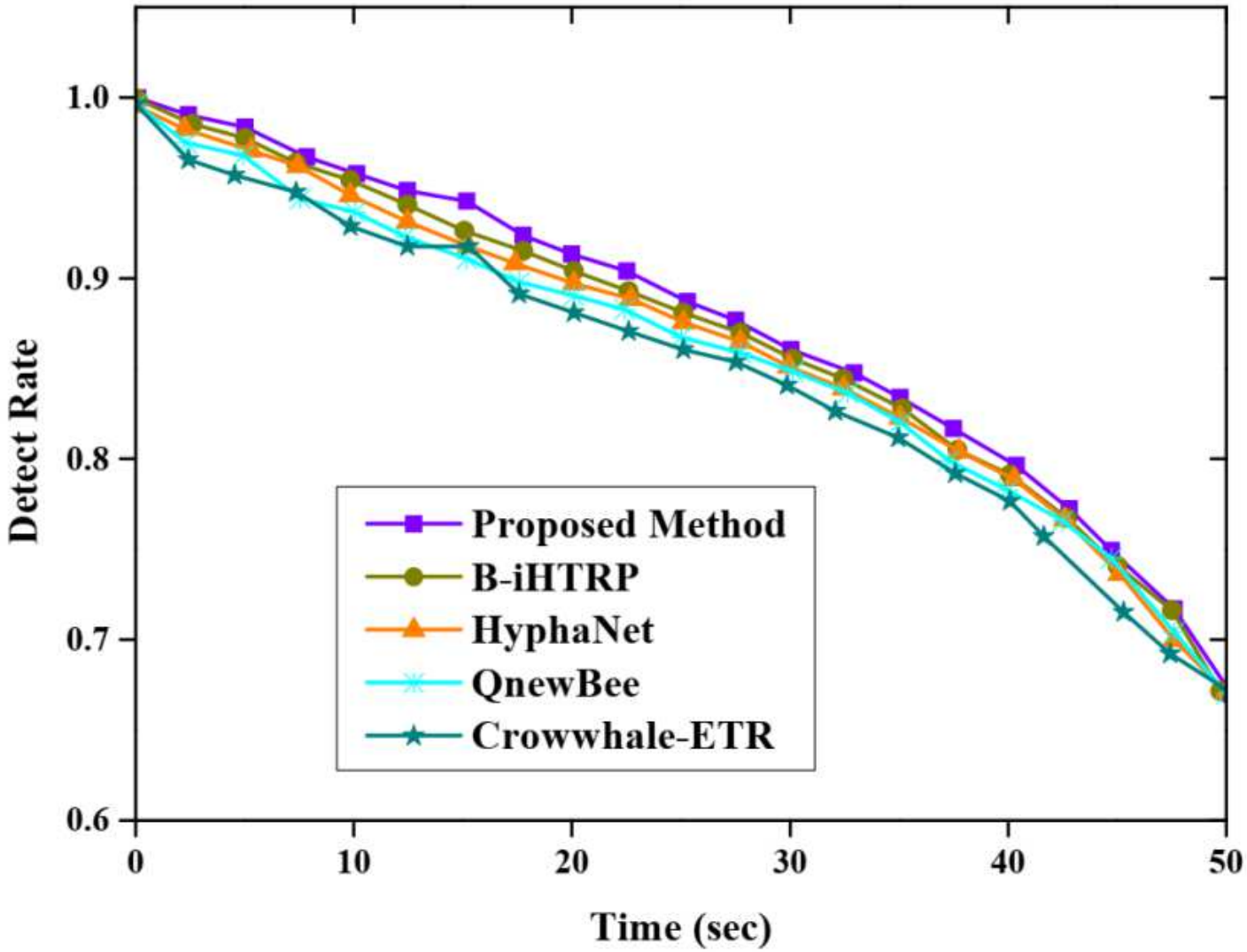

Figure 6

Comparative analysis of the detection rate

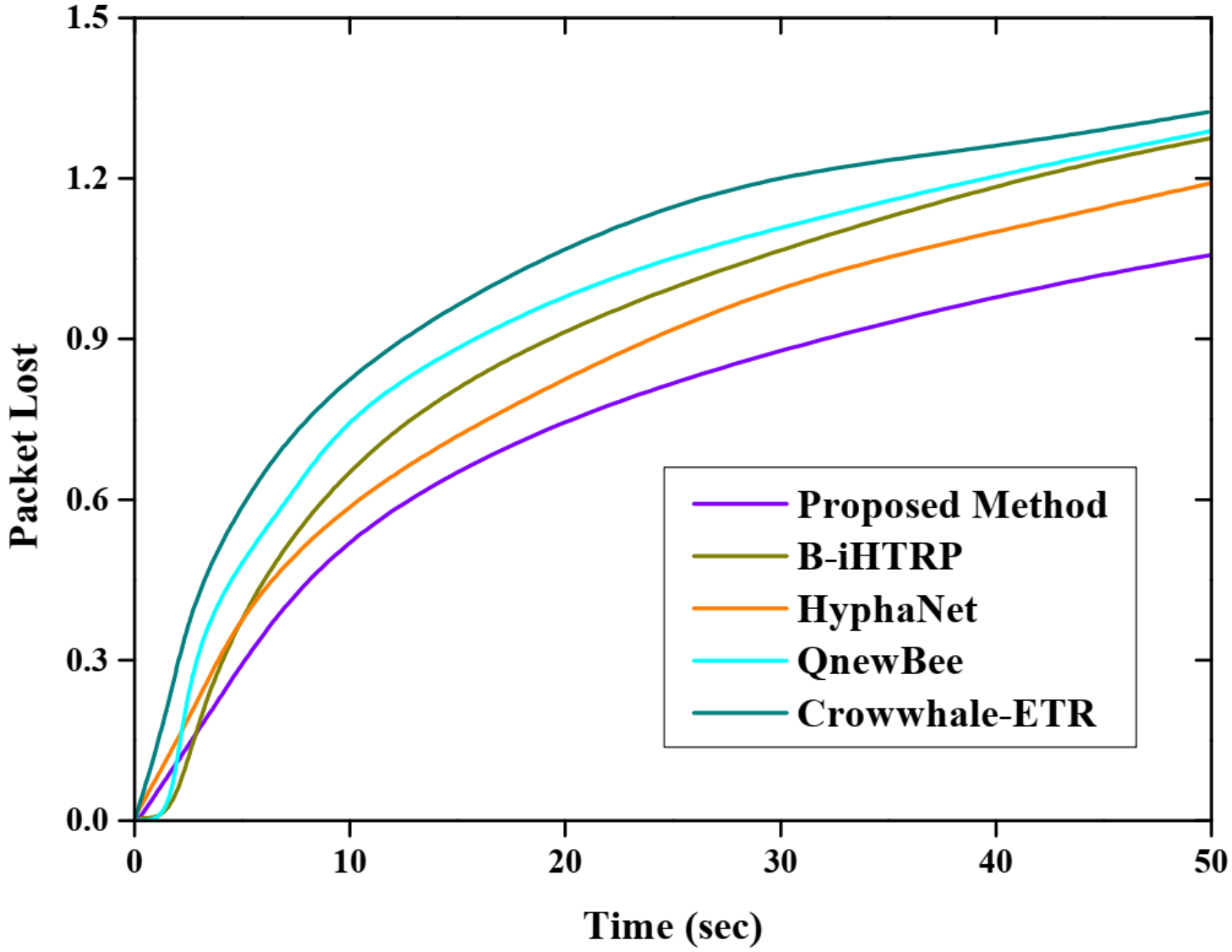

Figure 7

Comparative analysis of the packet loss rate

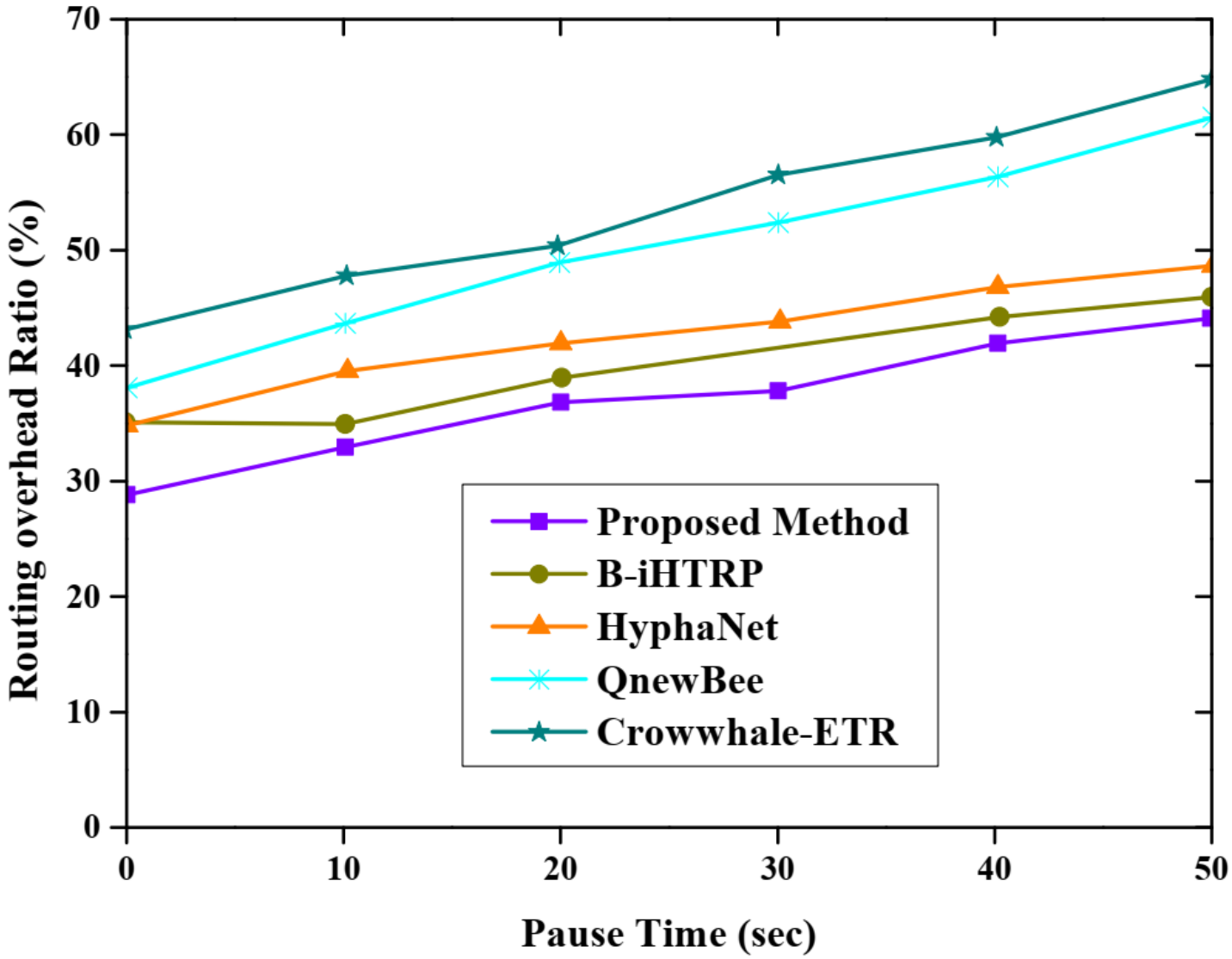

Figure 8

Comparative analysis of the routing overhead ratio

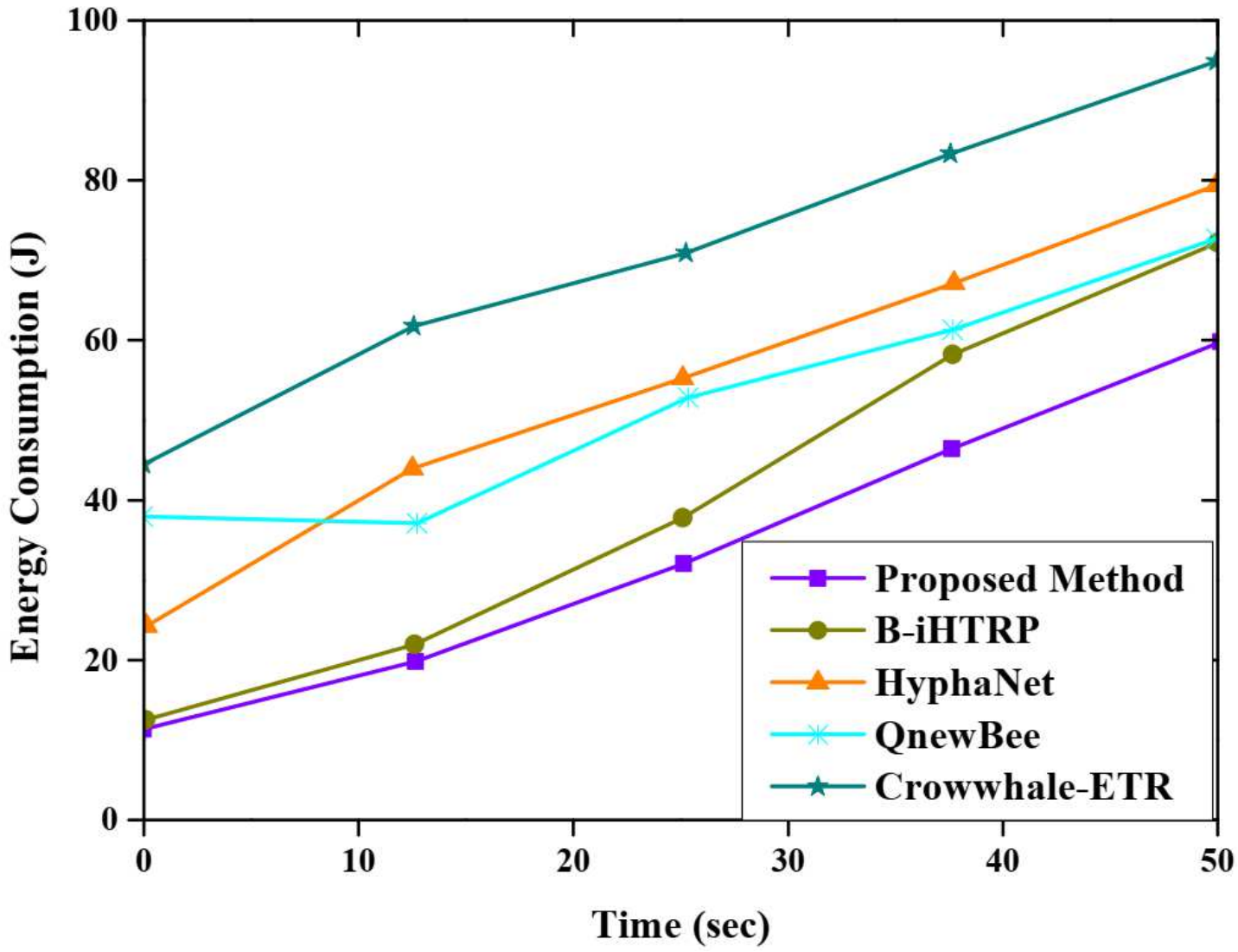

Figure 9

Comparative analysis of the energy consumption