Mobile Networks and Applications
https://doi.org/10.1007/s11036-023-02259-8

Trust Aware Secured Data Transmission Based Routing Strategy Using Optimal Ch Selection in Mobile Ad-Hoc Network

K. Sakthidasan Sankaran[1] · **Seng-Phil Hong**[2]

Accepted: 2 October 2023

Abstract
In Mobile Ad-hoc Network (MANET), the secured means of transferring data over malicious nodes is being considered as a significant aspect. The assurance of trust among the MANET nodes are regarded as an important constraint in providing higher security dynamic network topology deviation & the open wireless constrictions. However, nodes malicious actions decrease the trust level of nodes which may leads to insecure delivery of data. The malicious attacks rise leads to excessive consumption of energy in a network which thereby affects lifetime of network. The nodes should update their positional information which is lacking in traditional methods and it may lead to lowering the level of trust among nodes. Therefore, trust rate computation using mobility models & energy is essential which too needs their update for the secured delivery of data. In this work, a trust-aware ad-hoc route discovery protocol is presented for enhancing trust level among MANET nodes. The neighbor node is estimated using RSSI and the neighbor log collection is carried by means of packet id sequence extraction on trust rate estimation. Then, the optimal selection of cluster head is carried by using multi-faceted cuckoo search optimization approach. The trusted path is estimated by computing trust rate which recognizes the trusted path and discovers better routing path for the secured means of data transmission. Finally, the data is transmitted over trusted and secured path. The performance is estimated for the measures like throughput, routing overhead (RO), packet delivery ratio (PDR), End-to-End delay, & average consumption of energy.

Keywords MANET · Trust estimation · Secured data transmission · Optimal cluster head selection · Multi-faceted cuckoo search optimization

1 Introduction

A number of nodes in a network that has the ability to move in the network involved in change the positions frequently within the network, that displays the active nodes is called a mobile ad hoc network (MANET). In MANET, the nodes interact with other nodes present in the range of communication. The nodes present outside the range of communication interact with other nodes via the middle nodes. MANET is the network to assist any mobile applications in which interaction takes place through any wireless boundaries regardless of the infrastructure. The MANET maintains a routing algorithm which functions on the basis of the aspects like additional network overload, dynamic network topology, energy-conserving ability and the trust of the node. The routing protocols have the capability to handle the restrictions like security, error rate, Quality of Service (QoS), scalability and energy constraint [1].

The classification of the routing protocols is proactive, reactive and multicast. In proactive protocols, the routing table are broadcasted with the adjacent nodes. In reactive protocols, like Ad hoc on-demand distance vector (AODV) and the paths are recognized on demand. The limitations related with routing are confidentiality, authentication and integrity and so on. Optimizations play an important role with the objective to extract trusted secure routing, that offers one or more optimal solutions. Bee colony

✉ Seng-Phil Hong
sengphilhong211@gmail.com; sphong@assist.ac.kr

K. Sakthidasan Sankaran
sakthidasan.sankaran@gmail.com

[1] Department of Electronics and Communication Engineering, Hindustan Institute of Technology and Science, Chennai 603103, Tamil Nadu, India

[2] AI Advanced School, aSSIST University, 46 Ewhayeodae 2-gil, Fintower, Sinchon-ro, Seodaemun-gu, 03767 Seoul, Korea

Published online: 04 November 2023

optimization, Ant colony optimization, particle swarm optimization and genetic algorithm are the major algorithms in finding the optimal paths. MANET is self-organized portable hubs which interact with each other via distant connection. Hub functions as hosts as well as switches to advance posts to one another. BGRP Border Gateway Routing Protocol switches can infer limited QoS data and measurements like transmission capacity and postponement. By using QoS routing information in messages of BGRP, we can differentiate courses with lower traffic burden or higher accessible transmission capacity to advance bundles of information [2].

Mobile Ad hoc Networks MANETs are utilized by a varied types of strategies consisting of smart android phones, laptops and other results of computing. Access and usage are restricted for MANET nodes and privacy and security issue arise due to the wireless communication. Data transfer and interoperability are finished by the open nature of wireless medium. Intruders may get access to interaction in the network by misusing the node mobility, network dynamics and the absence of centralized administrative assistance. A harmful node that intrudes into network transfers has the ability to collect data regarding the nodes. Attacks such as route failure, spoofing of others and packet loss are decided by the aim of interruption into network and the nature. As a result, it leads to resource wastage and deprivation of the functioning of the network. Hence a MANETs routing and technology of attack justification are built [3].

The changes in topology are very often in MANET due to mobility of the nodes. When the node's mobility information is shared with other, the maintenance of topology makes an overhead. To face this overhead issue, cluster-based algorithms is suggested to lower the routing table size. To regulate the network topology updates within the cluster, clusters are formed. A node interacts with other node lies outside the cluster, it interacts only with the cluster head CH. The Cluster Head interacts with another Cluster Head CHs to transfer the data in the direction of the target. Some parameters such as node degree, communication workload, residual energy, neighbor's behavior and relative mobility are needed [4].

MANET is organized by clusters which act as the CH cluster Head and the remaining are members. The clustering method is involved in separation of interrelated sub structures from the whole network. The routing protocol is responsible for interacting on the basis of clustering methods which consists of inter and intra clusters. A huge amount of energy is required for CH than cluster members. MANET network is organized with many nodes which are integrated without wire. The nodes of MANET behave as the router during the transfer of packets in the network as data. These networks have achieved many issues like high energy utilization, low stability and low security. Various routing protocols such as Location Aided Routing (LAR), Zone routing protocol (ZRP), ad hoc on demand distance vector (AODV), Optimized Link State Routing (OLSR) are employed to improve the communication of MANET, but they are achieving the accurate output [5].

The aim of routing protocols in MANET is to find a proper route for the packet between the mobile nodes efficiently and effectively. Two main events of MANET are detecting the optimal path and transmission of information to the target node. In cluster-based Routing Protocol which is a hybrid protocol node are arranged as clusters. Clustering algorithm offers effective utilization of Bandwidth in MANET. One CH Cluster Head interacts with other CH in the network. If Ch is out of the span of communication, then nodes lie in between the clusters behaves as gateway nodes which can forward the data packets instead of CH. In weight-based clustering that includes the weight estimation of nodes with the use of many factors such as mobility, residual energy, node degree and transmission range. Mobility is the main motive for re-clustering [6].

MANETs are susceptible to many attacks and threats. Due to this, diverse information guarantee solutions such as access control, identity management and data protection will require to be employed to protect the network from cyber-attacks. A secure optimization routing algorithm for MANET is developed which is on the basis of BFOA Bacteria for Aging Optimization Algorithm. Routing method depends on Cluster Head Selection and detection of intrude node. The value of threshold is utilized to find the intrude node for efficient routing [7].

The residual part of this paper is structured as follows. Section 2 is the study of different existing methods and reviews enhanced so far. Section 3 represents the detailed description of the proposed work. Section 4 projects performance analysis of proposed work and estimation of the outcomes. Finally, Section 5 shows the conclusion of the work done.

2 Related works

In [8], the author focused to improve the consistent data transmission in the MANET with high security using the technique of optimization. MANET plays a major role such as distributed network, distributed network, quick and fast execution. By using energy efficient routing protocol, the nodes are clustered. Then optimal head of the cluster is chosen using particle swarm optimization. MANET encounters many challenges because of maintenance capabilities and self-configuration. The analysis on the basis of security is done based on energy consumption, delivery ratio, throughput and network lifetime. At last, the output explained that the MANET with optimization technique enhanced the reliable security and attained a high transmission rate.

In [9], the MANET is a self-organized network associated by wireless connection, that is appropriate for temporary interaction as there is less infrastructure and lack of centralized control. In MANET network, the challenging job is to offer security aware routing and QoS because of limited resources and dynamic topology. The main aim is to identify trust based secure route from source to target that assure two or more QoS restriction. The base routing protocol is utilized to compute this model which is an extended form of ad hoc on-demand multi-path distance vector protocol. The projected mesh on the basis of multipath scheme to find all probable secure routes with the use of secure neighboring position trust verification protocol. The Dolphin Echolocation Algorithm is used to find the best ideal path. The recommended routing protocol makes reduced packet delay, packet delivery ratio, provide security against attacks and reduced overheads.

In [10], the authors proposed a CTPS Chunk Top Path Selection using techniques of hybrid meta heuristic and swarm intelligence. Using EMIO Enhanced Monkey inspired optimization the head of the cluster was collected was done. Then with the support of IPS Improved Pattern Search algorithm optimal path has been found. The difficult issue is to transfer a data to a MANET mobile ad-hoc network. To regulate the transfer of data across instinctive hubs, bunching is used. Every group of hubs has one chosen head and all bunch heads are connected to each other. Bunch and idle terminals go through examining energy sooner and minimize the span of the stage. The aim of MANET is to choose reliable cluster heads which offer secure interaction through nodes. NS2 simulation reveals and outperforms methods in constraints of power consumption, performance, pocket delivery speed, pocket overhead and latency.

In [11], Security is a vital factor in which unattainable surroundings leads varied types of intimidations to offer network free of malicious. Game theory plays a vital role in calculating structured secure and safe methods in the network. Here, infinite recurrent game and assistance method is planned to find the harmful nodes and to improve the efficiency. The purpose of infinite recurrent game is to confirm that the hateful node has a long run loss and short run gain. The main aim of the recommended plan is to attack the defense and detection, combating the packet drops. Finally, the recommended method is checked through simulation.

In [12], the author proposed an improved the secure communication in a network called MANET which is declared as a vital and challenging task. A variety of works are implemented for modifying the attacks that lowers the network performance. The links that are faulty are required to be identified for achieving the best output based on the availability and reliability of mobile nodes. In this paper, enhanced IROA-LAFD Improved Rider Optimization Algorithm-based Link Aware Fault Detection is recommended for enabling security by modifying the black and grey hole attacks with improved stability of the connection. IROA-LAFD focuses on effective modification of packet drop on the basis of steps which consists the finding of adjacent and route, analysis of links, detection of attack, link fault detection, transmission of secure packets.

In [13], the authors implemented a survey regarding the techniques utilized for resolving many problems like authentication, routing and security. MANET Mobile ad-hoc network plays a vital role in transferring the packets from origin node to target node. As MANET is highly prone to attacks, it was expected to face the various security needs like anonymity, authentication, integrity, availability and confidentiality. The issue of integrating security into the routing protocols, various algorithms have been implemented to detect the effective and the optimal method. At last, the analysis is done in many prevailing techniques in the MANET.

In [14], the authors offered an algorithm introduces a latest node that behaves as a backup node in the group of nodes. When the actual head of the cluster moves out from the group, the backup node behaves as cluster head CH. Later the head of the cluster reappoint a new backup. This method maintains the accessibility of the network without disturbance. In MANET each node has the ability to send data in a dynamic manner without the need of any infrastructure. The network topology is unstable in MANET, as the mobile nodes often move in a dynamic nature. Here, proposed a stable optimized clustering algorithm that offers high stable network. The backup node and cluster head CH priority is computed on the basis of the residual battery life and the degree of the node for mobile nodes.

In [15], the authors suggested method is a multi-restriction applied energy effective routing method on the basis of Ant Colony Optimization in Mobile Ad-hoc Network. This suggested technique choses the successive node centered on the limits, packets in the route, remaining energy of node that are in motion and topology of movement. A MANET is an associated mobile device that have the ability of self-arrangement. Mobile Ad-hoc Network is facing many problems such as communication issue, management of topology and management of energy because of the unstable nature of devices and connection without wire. By employing ACO, the chances of selecting successive node as advancing node is decided. It is showed that the recommended MCER ACO technique has offered ideal energy effective path when compared with other prevailing techniques.

In [16], the authors proposed a routing method MCLMR (Mobility, Contention window and Link quality sensitive multipath Routing) in Mobile Ad-hoc Network which reflects the contention window size, mobility of the node, computed value of the middle nodes in the selection of the ideal nodes. The nodes mobility, estimation of the quality of the link and traffic congestion are vital aspects in MANET

for launching a consistent route between source and target nodes. The mobility of the nodes and traffic flow of data at a specific node leads to instable network topology and congestion that reduces the output of MANET. Hence link quality routing protocol, reliable mobility has been implemented. The results showed that the recommended MCLMR routing outdoes the MP-OLSR (Multipath Optimized Link State Routing) on the basis of packets loss ratio, end-to-end delay, energy consumption and network throughput.

In [17], the authors suggested an effective way of associated leading set clustering with path selection in MANET to achieve low delay, high packet delivery ratio, low control overhead and low energy consumption. CDS Connected Dominating set has been declared as an effective solution to resolve the issue by creating a virtual network to obtain efficiency and scalability of network. The suggested CRD protocol consists of routing and clustering phases under multichannel cognitive radio strategy. Here, CDS size reduction, CDS selection is recommended in the clustering stage and offer a set of middle nodes that was used as a routing phase. Channel based Focus Selection CFS algorithm is accepted in a dynamic way to create an effective path from a set of nodes.

In [18], the authors proposed and AOMDV protocol for the finding of many routes along with KNN K-Nearest Neighbor for the selection of adjacent neighbor node and FAES (False key-build Advanced Encryption Standard) is used for cryptography technique. FAES algo is engaged to secure the data and IoT devices from the attacks. MANET are accomplishing fame as the users require connection without wire irrespective of the topographical location. MANET need a secure mode of transmission and communication which is a vigorous and challenging problem. Hence a scheme is suggested for reliable and secure transmission in MANET on revised AOMDV Ad hoc On-demand Multipath Distance Vector protocol. The suggested plan output is more stable with advanced throughput. The quality of the scheme is computed on the basis of EE-delay, throughput and energy consumption even in presence of harmful nodes. The output revealed that EE-delay, Variance, throughput and energy consumption of suggested FAES-AOMDV protocol is lesser than the original AOMDV protocol.

In [19], the authors projected a route selection mechanism by integrating Ad-hoc On-Demand Distance Vector protocol (AODV)and Ant Colony Optimization(ACO) to enhance the QoS Quality of Service in Mobile Ad-hoc network MANET. Based on the mechanism of AODV with ant colony, the best path for delivery of data is chosen with the use of pheromone value of the route. In the suggested work, the calculation of pheromone value of a path is done on the basis of hop counts, congestion, remaining energy of the nodes along the route and reliability of the route. The route that has the greatest value of pheromone shows the transfer of packet of data. The output reveals that the recommended plan outdoes DSR Dynamic Source Routing, AODV and improved DSR routing.

In [20], the authors proposed a MEESC (Modified Energy-Efficient Stable Clustering) algorithm in which node mobility is provided higher preference in computation of value for selecting the CH. The suggested algorithm is simulated in NS3 and gave better outputs in selection of CH based on lifetime of the CH and number of clusters. CBRP Cluster-Based Routing Protocol is famous and verified for efficiency in MANET. This protocol splits the network into many clusters. Every cluster consists of CH Cluster head that preserves the formation of cluster. Prevalence of CH enhances the output of routing on the basis of power consumption and low overhead. Due to mobility, members of the cluster, CH movement and re-clustering is needed and this improves the operating cost in the cluster formation. The selection of CH should be done effectively so that CH persists long. Prevailing CH selection algorithms utilize weight-based strategy that uses factors such as mobility, battery power, degree of the node to estimate the weight and residual energy. Mobility is more significant parameter in MANET and has given more significance.

In [21], the authors presented a new quantum worm swarm optimization-based clustering for MANET with a secure routing protocol named QGSOC-SRP that surveys a two-phase process such as route selection and optimal selection of CH. Initially QGSO algorithm determines a fitness function with the use of the distance, energy, trust factor and node degree for selecting the secure CHs. Then the SRP using OGSA oppositional gravitational search algorithm is implemented for selecting the ideal route. MANET consists a group of compact sized, inexpensive, independent sensor nodes that are utilized to identify the factors and transfer them to BS base station. As routing and clustering are energy effective methods, many metaheuristic algorithms have been implemented to regulate optimal CH. To enhance the GSA efficiency, OGSA is implemented on the basis of opposition-based learning concept for generating jumping and initializing the population. To authenticate the outputs with regard to the presented OGSOC-SRP method, experiments done and the result was derived with the use of throughput, network lifetime, energy consumption and E2E delay rate.

The nodes should update their positional information which is lacking in traditional methods and it may lead to lowering the level of trust among nodes. Therefore, trust rate computation using mobility models & energy is essential which too needs their update for the secured delivery of data. For this purpose, the proposed trust based routing scheme is designed.

3 Proposed work

A brief narration on overall working methodology is offered here. The proposed system architecture is shown in Fig. 1 and the complete workflow of anticipated method is shown in Fig. 3.

3.1 System model

At first, formation of network takes place by the initialization of parameters. The distance between user and base station is estimated. After that, information will be collected from the neighbor log reports so as to know the failure/success rates of the packet transmission among the nodes. The value of trust is thus estimated depending on the packet ID sequence matching on comparing the log report of nodes.

Figure 2 shows the system model of MANET. Typically, AODV as reactive routing protocol establishes routes when it is needed on utilizing the sequence number of destination for attaining most recent path. For this reason, the routing protocol AODV is responsible for updating each and every information of routing to destination. However, the estimated destination nodes were not as much of trusted ones because of the malicious activities in the creation of report. Thus, the value of trust is being computed by means of integrated energy estimation, packet delivery success rate, and mobility. After that, the nodes having higher trust value will be selected for transferring packets. By these estimates, discovered routes are reliable, secure, and it possess higher values of trust. The flow of the proposed technique is given in Fig. 3.

3.2 Neighbor node estimation using RSSI

The neighbor node estimation is carried with the RSSI computation. The estimation of distance before the computation of trust value by RSSI guarantees that the trust node nominated must be in the communication range. In MANET, mobile nodes are having the ability for moving in such direction & thus acts as both hosts & routers. As it has not any specific infrastructure, information could be sent from any nodes to the others. The source node is the one that transfers data to others and destination node is the one which receives the data. In case, the trust value of nodes will be higher, then the data transmission among them is highly reliable. The selection of source node and neighbor node will be extracted with the use of RSSI dependent distance estimation. After that, the nodes trust values are updated depending on the computation of energy model and estimation of mobility. A node that has high trust value is chosen as intermediate node to transfer packets to the destination node.

A neighborhood estimation is the first step for computing nodes trust value. The distance estimated among RSSI thus identifies the nodes that are closer to source node. The

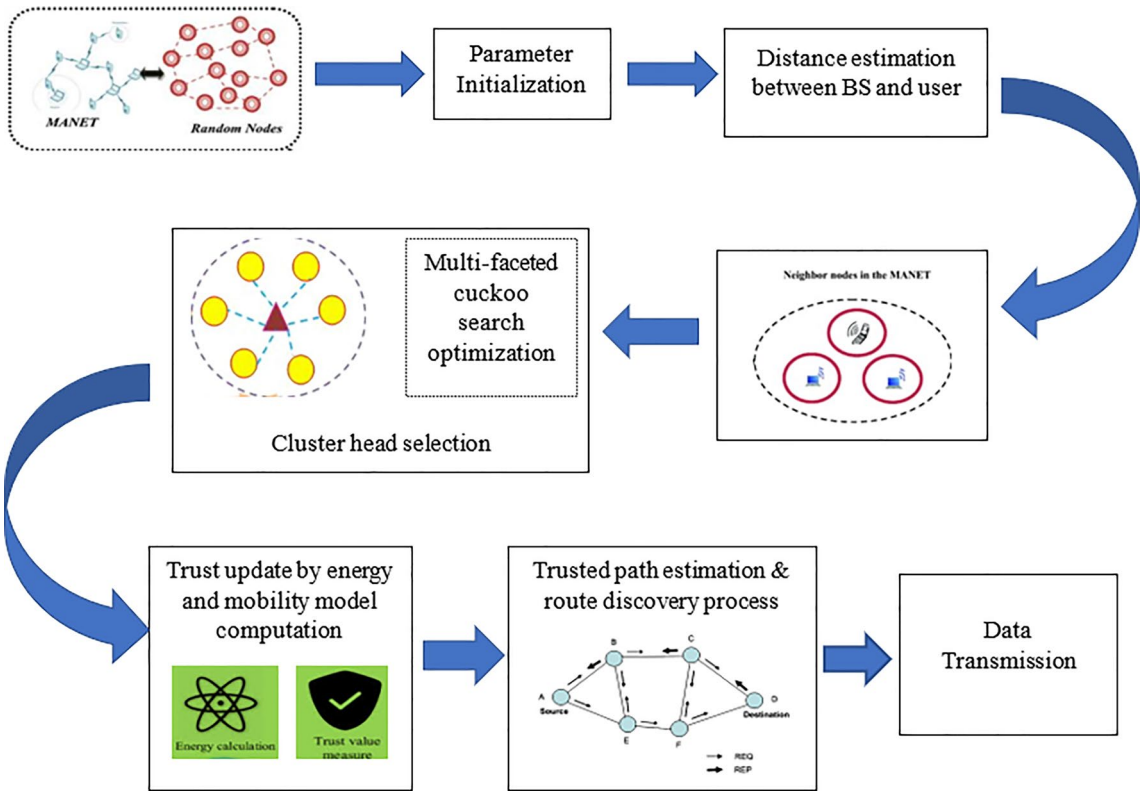

Fig. 1 Architecture of proposed model

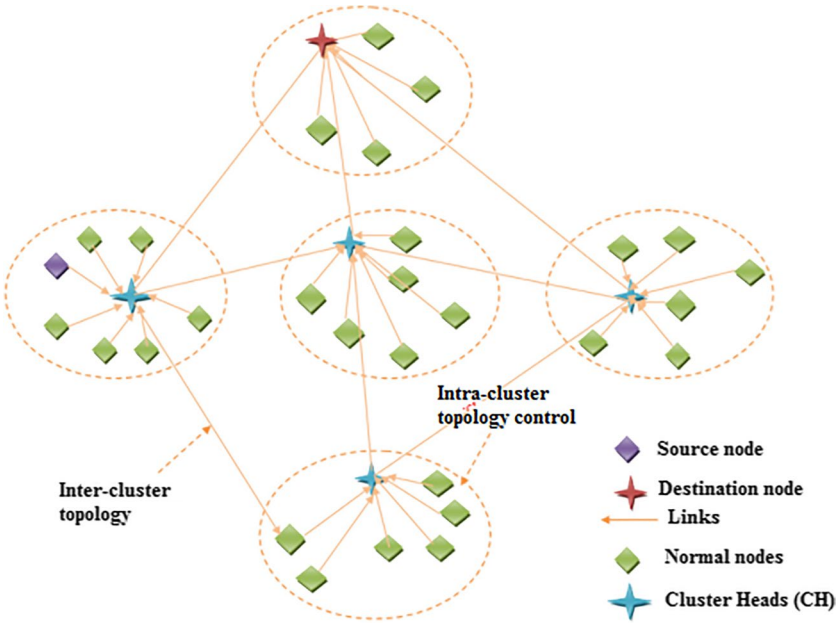

Fig. 2 System model of MANET

neighbor log collection is also done by extraction the packet sequence ID using trust rate.

The distance computed by RSSI is expressed as follows:

$$d_{s,i} = RSSI(N, G_i) \tag{1}$$

Here, $d_{s,i}$ denotes the strength of signal system among source node s & the present node i. G_i signifies the *ith node* of graph.

In case, a computed value of distance is lower than communication range, the packet ID of current node along with next node ID is compared at that time. In case, if these are equal, the respective trust rate is estimated at that time as shown below. The trust rate is provided by means of the prospect for persisting to some time period. The estimation of trust rate is shown by:

$$TR_i = \frac{1}{3}\left(B_{s,i}(H) \times B_{i,s}(H)\right)\left(PS_R + RS_R + RQS_R\right) \tag{2}$$

$$TR_i = \frac{1}{3}\left(B_{s,i}(H) \times B_{i,s}(H)\right)\left(\frac{NP_s}{NP_s + NP_f} + \frac{NRP_s}{NRP_s + NRP_f} + \frac{NR_s}{NR_s + NR_f}\right) \tag{3}$$

Here, the trust rate is indicated by TR_i, packet success rate is represented by PS_R, RS_R denotes reply success rate, RQS_R signifies request success rate.

NR_s – *number of successful requests*
NR_f – *number of failed packet transmission*
NP_f – *number of failed packet transmission*
NP_s – *number of successful packet transmission*
NRP_s – *number of successful reply packets*
NRP_f – *number of failed reply packets*

The belief function $B_{s,i}(H)$ signifies the state of *ith node belief level* since the node of source and vice versa that differs from 0 to 1. The belief level 0 indicates the unidentified condition *and* 1 signifies the condition that are known. The trust rate computation is based on the integration of effective packet transmission rate, effective request rate, and the reply rate that are successful.

The algorithm for this neighbor log collection is shown below:

Input: $Node\ (N), Graph$
Output: $Trust\ rate\ TR_i$
Step 1: The list of neighbor node (NN) is collected from input node (N)
Step 2: The log information of specific NN $(Log_{N(i)})$ is collected
Step 3: From the nodes log report, get the packet sequence IDs
Step 4: **For** $i = 0 \ldots n$ **then**//*here n is the network size*
Step 5: *compute* $d_{s,i}$ *by eqn* 1
Step 6: **if**$(d_{s,i} < range)$ ***then***
Step 7: $Packet_{ID_{N(i)}} = Extract\ packet\ ID\ (Log_{N(i)})$
Step 8: ***if*** $Packet_{ID_{N(i)}} == Packet\_ID_{N(i+1)}$
Step 9: Estimate trust rate by TR_i
Step 10: ***Else***
Step 11: *Goto step* 1
Step 12: ***End if***
Step 13: ***Else***
Step 14: *Go to step* 1
Step 15: ***End if***
Step 16: ***End For***

Algorithm 1 Neighbor log collection

Thus, the neighbor estimation is done by RSSI and the trust rate is thus estimated with neighbor log collection. The, the nodes are clustered and the cluster head selection is made which is described in subsequent section.

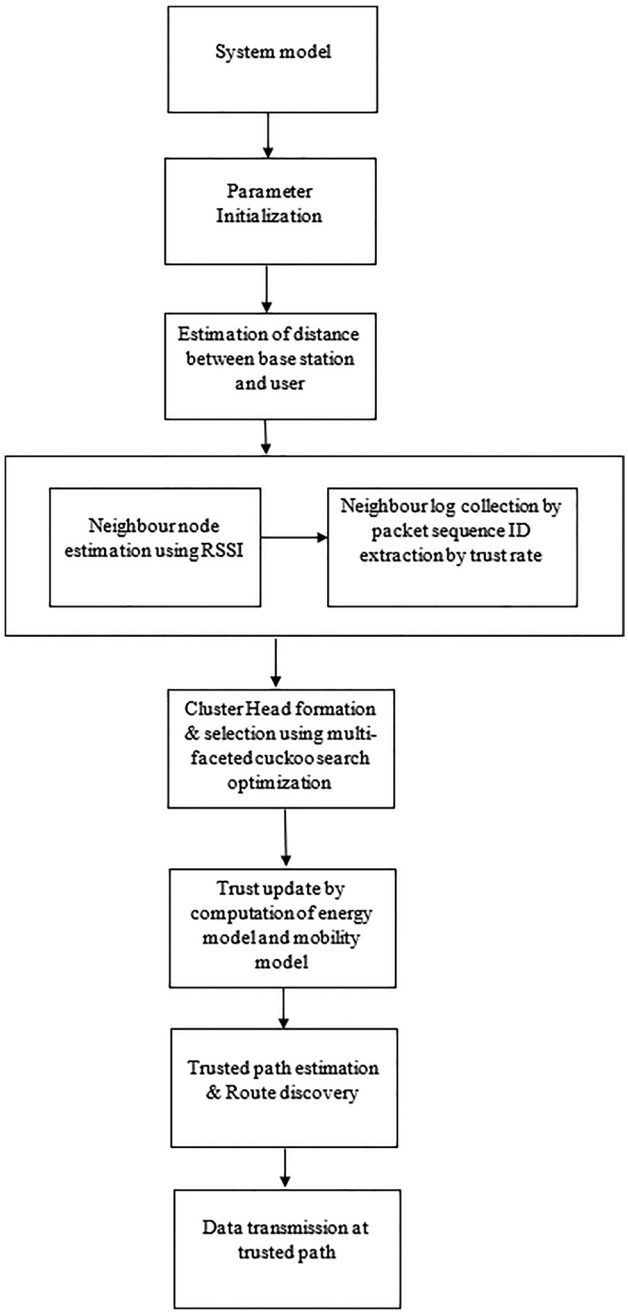

Fig. 3 Flow of the proposed technique

3.3 Cluster head formation and selection using multi-faceted cuckoo search optimization

The process of cluster formation is carried depending on the initial cluster head selection. The addition of node to the cluster group thus mingles or considers the added nodes as a cluster member of that specific cluster group. The new node addition in cluster group depends on 4 control messages like Hello, status, join, and Acknowledgement which too needs the authentication of cluster group. At first, the new node's presence is thus indicated through sending the Hello message by new node. On receiving Hello message, status message is thus forwarded to node by entire surrounding neighbors d as a response. The cluster head n could be identified by node d on checking the mentioned cost value in the status message. If it is not happened, then the status message contains cluster head node ID which shows that the n neighbor node is cluster member. The clustering process's coordinators and the relay routers thus plays a vital part in both routing frameworks of cluster head such that the node in cluster head consumes spare energy on comparing the other nodes which too affects the procedure of routing. This causes re-clustering of group with the use of traditional secure routing approaches which elects other cluster head to avoid loss of packet at the time of data transmission. The issue is that the overall routing process efficiency is thus reduced and thereby the processing time is increased. The group re-clustering is not needed with the use of presented multi-faceted cuckoo search optimization technique, which in turn selects the secondary cluster head in the initially formed group of clusters so as to overcome the issue. the presented optimization approach aids in finding the fitness. In this, cuckoo signifies the source sensor node, data packet sent by source node is represented by cuckoo's egg. By this time, data packets of source node sent via the multi-objective path could be sent to destination node. The data is thus passed over the path of high traffic and unreliable path is thus dropped out.

Figure 4 shows the illustration of cluster head selection. The presented optimization is a metaheuristic technique which is inspired by cuckoo's biological characteristics. Based on the terminologies like randomization search and stochastic search, the technique was developed. At first, the search space exploration for the local optima is carried and is expanded further for deriving the global optima solutions. By modifying the parameter values and step size, the performance of boundary could be personalized dynamically.

The cuckoo shows their oblige behavior and is regarded as a parasitic organism that hinges on other birds for the process of reproduction. This too based on other host birds to raise their younger ones. The activity of cuckoo is initiated by the genetic influence for instance cuckoo foraging. Usually, in the nest of host birds, cuckoo lays their eggs and thereby hatches them. Those hatched younger ones want host attention to attain their nourishment. Similarly, this repeats external host qualities that depends on the exploration and exploitation approaches. The new solution is therefore derived by the technique of levy flight. The technique thus follows few constraints and is provided below. The flow chart of the proposed Multi-faceted cuckoo search optimization algorithm is given in Fig. 5.

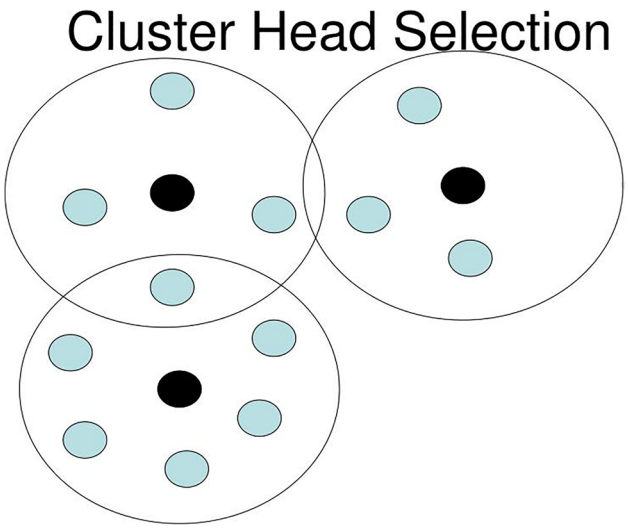

Fig. 4 Cluster head selection illustration

i. At once, one egg was laid by each cuckoo thus leaving them in a randomly chosen nest.
ii. Among them, best ones are grown as a future generation.
iii. There exists some fixed number of nests.

Yet, there is a possibility that the eggs that are unknown could be identified by the host bird. In this condition, the host bird might leave its nest or will discards their eggs accordingly. By this manner, the optimizer selects the optimal CH. The algorithm for this is provided below:

Thus, the optimal cluster heads are chosen by this method which offers best fitness function value. Then, the trusted update is carried by estimating the energy and mobility of network.

3.4 Computation of trust update by energy and mobility computation & trusted path to discover route

The estimation of energy and mobility computation is provided as shown:

(i) Energy computation

Energy is deliberated as a nodes capacity for transferring the data. The energy model's major functions are the sensing of neighbor and maintenance of route. The energy model of proposed technique is computed by:

$$E_{m,n} = \left[\left(Pi_{m,n} \times Ti_{m,n}\right) + \left(Pr_{m,n} \times Tr_{m,n}\right) + \left(Pt_{m,n} \times Tt_{m,n}\right)\right] \tag{4}$$

Afterwards the trusted node selection for the packet transmission, the nodes selected needs to update its energy level for further transmission of packet. The, the overall energy ($Ei_{m,n}$) might be updated on employing following equation as shown below:

$$Ei_{m,n} = Ei_{m,n} = E_{m,n} \tag{5}$$

Here, $Pi_{m,n}$, $Pr_{m,n}$, and $Pt_{m,n}$ refers to the level of power consumed at idle stage, reply, and transmission stage. $Ti_{m,n}$, $Tr_{m,n}$, and $Tt_{m,n}$ signifies the required time for idle stage, reply, and the transmission stage.

(ii) Estimation of mobility function

The function of mobility is defined by movement of mobile nodes which consists of node moving speed, and path. The distance among nodes will be computed with the use of constant k value and required power for the reception or transmission as shown:

$$d = \sqrt{<}spanclass =' \; reftype' > [4] < /span > k.\, Pt/Pr \tag{6}$$

The neighborhood velocity is computed as:

$$\bar{v} = \Delta d/\Delta t \tag{7}$$

The position level of neighbor node is based on the velocity parameter corresponding to the node selected is attained by:

$$Direction = \begin{cases} \bar{v} > 0 & outwards \\ \bar{v} = 0 & static \\ \bar{v} < 0 & inwards \end{cases} \tag{8}$$

The function of mobility is thus attained as;

$$M_i = \bar{V}\, TR_i + d \tag{9}$$

From the computed energy, trust rate and mobility, node's trust value is estimated as shown:

$$TC_{s,i} = E_{s,i} + TR_i - M_i \tag{10}$$

By this estimated trust value, nodes having supreme trust value is selected for packet or data transmission. When the destination is reached, discovery of route was carried. Or else, neighbor estimation should be done once again. The node having higher trust value are chosen and is included to routing path. After that, graph updating takes place with remaining nodes which then decides whether a chosen node is a destination or not. In case, the destination node is found to be equivalent to node that are having maximum trust value, the routing path will be determined and the communication takes place. Thus, the data is conveyed at the

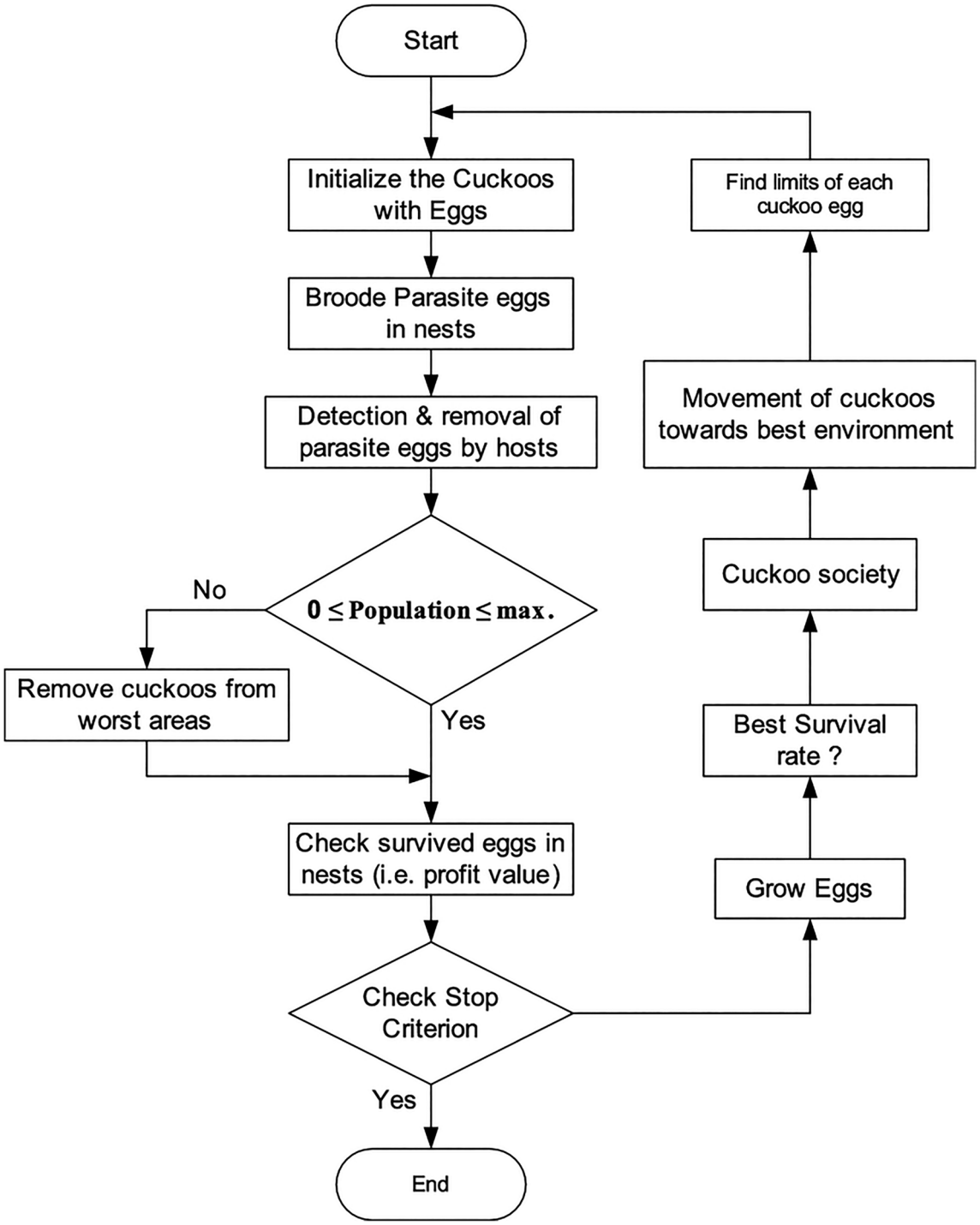

Fig. 5 Flowchart of proposed multi-faceted cuckoo search optimization algorithm

trusted path found satisfying the performance metrics of the network.

The proposed technique employs secured data communication scheme. In this, in spite of sending malicious packets to next hop, those packets are partially transmitted or completely dropped. So as to discover malicious nodes, initial set of communication is carried. For entire node, trust value will be derived through fluctuating criteria that ranges from $0 to 1$. Every node takes a common value of threshold & every node might be recognized on using threshold value in any of two ways: regular node or compromised node. the identified nodes that are malicious are thus removed from network

Algorithm 2 Optimal CH selection by multi-faceted cuckoo search optimization

```
Initialization
create original host nest population as n
objective Function f(y)
Identify eggs of best rank and fit
While (s > MaxProduction) or stop criterion
S = s + 1
        Obtain cuckoo arbitrarily or else create new solution by
levy flights
Identify best fit or quality Qi
Select a nest randomly as k
If (Qi> Qk)
  Swap k by new solution
End if
            With a probability Pe unfit nest is abandoned and
form new nest
             Assess rank and best fit the solution and accept
present as best
End while
  Send process output and visualization
End
```

on changing state power. The source node thus selects the consistent path for their target node in case the malicious nodes among source & destination nodes are removed by now. Thus, from this a secured communication takes place in a trusted path.

4 Performance analysis

The performance metric for evaluating the proposed technique effectiveness is estimated & outcomes accomplished are related to that of the existing models [3, 22] for validating the efficiency of suggested method.

4.1 Performance metrics

(i) Routing overhead

It signifies the control packets that are needed for performing specified number of tasks. Therefore, it also defined as the sum of entire control packets that are sent at a total simulation time and is expressed as follows:

$$RO = \sum_{i}^{N} CP_i \tag{11}$$

Here, CP_i signifies the sent control packets number at every *iteration i* & N signifies the *total number of iterations.*

(ii) Throughput

It is the amount of data that are transferred effectively among the sink and source at a specified time span (sec). This is computed as shown below:

$$TP = \frac{No\ of\ packets\ received\ successfully}{Stop\ time - start\ time} \tag{12}$$

(iii) Packet Delivery Ratio (PDR)

It is the ratio at which data packets are delivered successfully to the destination. This is computed as follows:

$$PD = \frac{\sum_{\forall i \in D} TPR_i}{\sum_{\forall i \in D} \times TPS_k} \times 100 \tag{13}$$

In this, TPR_i signifies the total no of packets that are received by the destination DBR, *i and* TPS_k denotes total no of packets sent by the CBR (constant bit rate) of source node k, S signifies the CBR source collection. D is the CBR destination collections.

(iv) Average E2E delay rate

It is the amount of time in average that are taken for transferring from the node of source to destination. This too covers delay occurred by buffering, re-transmission, and queueing and is computed by:

$$ED = \frac{1}{N \sum_{n=1}^{N} (r_n - s_n)} sec \tag{14}$$

In this, r_n denotes the time period of the sent packet, s_n represents the time period once the packet is received, and N signifies the total packet numbers that are received.

4.2 Performance comparison

The throughput is estimated for the proposed system in terms of number of nodes vs. throughput in kpbs. The

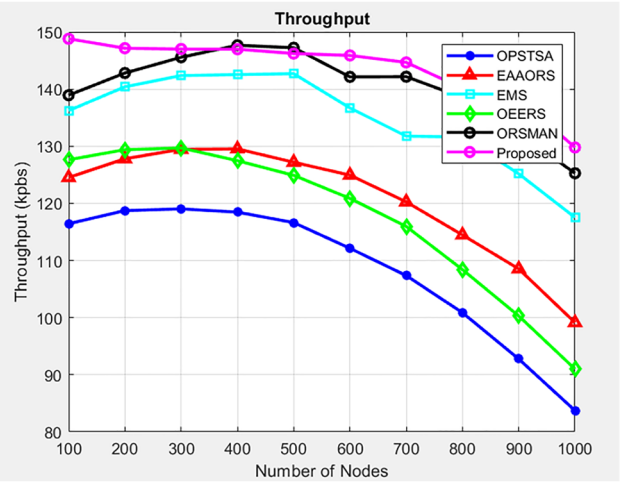

Fig. 6 Comparative estimation of throughput analysis

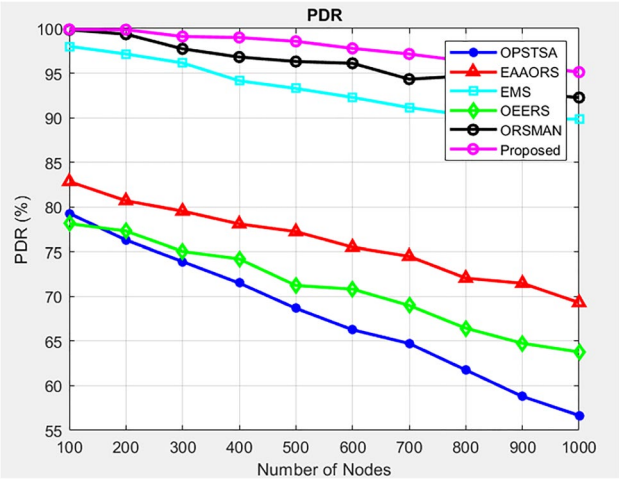

Fig. 8 Comparative estimation of PDR

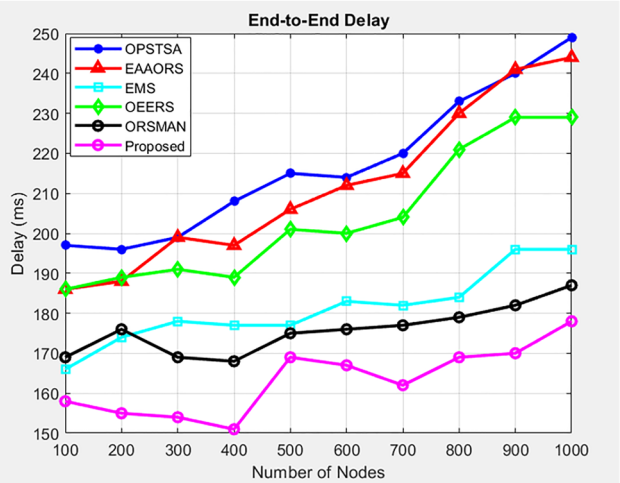

Fig. 7 Comparative estimation of E2E delay

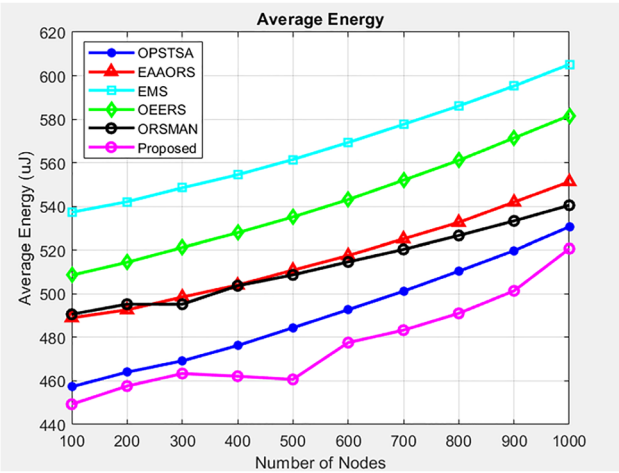

Fig. 9 Comparative estimation of average energy

outcomes are compared with various existing techniques and it is shown below in Fig. 6. The analysis shows that the proposed method offers higher throughput than others.

The average E2E delay rate is estimated for proposed system in terms of number of nodes vs delay in ms. The outcomes are compared with various existing techniques and it is shown below in Fig. 7. The analysis shows that the proposed method offers lower delay rate than others.

The PDR is assessed for the suggested system in terms of number of nodes vs PDR in %. The outcomes are compared with various existing techniques and it is shown below in Fig. 8. The analysis shows that the proposed method offers higher PDR rate than others.

The average energy is assessed for suggested system in terms of number of nodes vs energy in uJ. This is a challenging aspect to retain the energy in network all over the process of transmission and it is considered as an important feature for the network performance. The outcomes are compared with various existing techniques and it is shown below in Fig. 9. The analysis shows that the proposed method offers low consumption energy rate than others.

The routing overhead is estimated for the proposed system in terms of mobile nodes vs. overhead percentage in no. of bits. The outcomes are compared with existing techniques and it is shown in Fig. 10. The analysis reveals that the suggested model offers lower communication RO on comparing other traditional models. Therefore, the proposed system is effectual in providing enhanced performance than the traditional approaches.

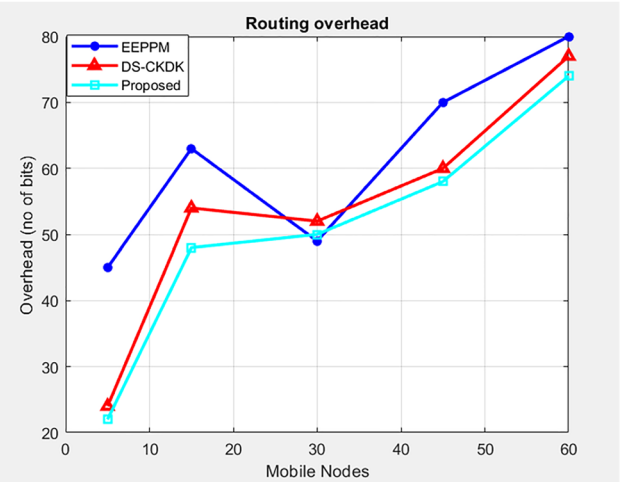

Fig. 10 Comparative estimation of routing overhead [22]

5 Conclusion

A trust-aware mobile ad-hoc route discovery system was presented in this work. The major objective was to enhance the trust level between the nodes in MANET framework. By employing RSSI the neighbor node was estimated and a neighbor log collection was carried using packet id sequence extraction on estimating trust rate. After that, the optimal selection of cluster head was done using multi-faceted cuckoo search optimization approach. The trusted path was estimated by computing trust rate which identifies the trusted path and determines better routing path for the secured data transmission. Lastly, the data was transmitted over secured and trusted path. The performance was estimated in terms of PDR, throughput, RO, E2E delay, and average energy consumption. The estimation was compared with various traditional methods to validate its effectiveness. From the analysis, it was apparent that the proposed model performs well by offering high throughput, PDR, and lower delay, energy usage, and overhead. Thus, the proposed model is improved than the existing schemes.

Acknowledgements This research was supported by AI Advanced School, aSSIST University, Seoul, Korea.

Declarations

Competing interests The authors does not have any conflict of interest.

References

1. Mukhedkar MM, Kolekar U (2019) Trust-based secure routing in mobile ad hoc network using hybrid optimization algorithm. Comput J 62(10):1528–1545
2. Karthick K, Asokan R (2021) Mobility aware quality enhanced cluster based routing protocol for mobile ad-hoc networks using hybrid optimization algorithm. Wirel Pers Commun 119(4):3063–3087
3. Suresh Kumar R, Manimegalai P, Raj V, Dhanagopal R, Johnson Santhosh A (2022) Cluster head selection and energy efficient multicast routing protocol-based optimal route selection for mobile ad hoc networks. Wirel Commun Mob Comput, Article ID 5318136
4. Ahmad M, Hameed A, Ikram AA, Wahid I (2019) State-of-the-art clustering schemes in mobile ad hoc networks: objectives, challenges, and future directions. IEEE Access 7:17067–17081
5. Vatambeti R, Sanshi S, Krishna DP (2023) An efficient clustering approach for optimized path selection and route maintenance in mobile ad hoc networks. J Ambient Intell Humaniz Comput 14(1):305–319
6. Roy A, Deb T (2018) Performance comparison of routing protocols in mobile ad hoc networks. In: Proceedings of the International Conference on Computing and Communication Systems, vol 24. Lecture Notes in Networks and Systems, pp 33–48
7. Srilakshmi U, Alghamdi SA, Vuyyuru VA, Veeraiah N, Alotaibi Y (2022) A secure optimization routing algorithm for mobile ad hoc networks. IEEE Access 10:14260–14269
8. Elhoseny M, Shankar K (2019) Reliable data transmission model for mobile ad hoc network using signcryption technique. IEEE Trans Reliab 69(3):1077–1086
9. Borkar GM, Mahajan AR (2017) A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. Wirel Netw 23(8):2455–2472
10. Saravanan T, Thillaiarasu N (2021) Optimal grouping and belief based CH selection in mobile ad-hoc network using chunk reliable routing protocol. In: 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2021, pp 933–940. https://doi.org/10.1109/ICACITE51222.2021.9404631
11. Balaji S, Julie EG, Robinson YH, Kumar R, Thong PH (2019) Design of a security-aware routing scheme in mobile ad-hoc network using repeated game model. Comput Stand Interfaces 66:103358
12. Janakiraman S, Deva Priya M, Aishwaryalakshmi G, Suganya T, Sam Peter S, Karthick S, Malar CJ (2022) A. Improved rider optimization algorithm-based link aware fault detection (IROA-LAFD) scheme for securing mobile ad hoc networks (MANETs). In: 3rd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing. Springer International Publishing, Berlin, pp 155–169
13. Borkar GM, Mahajan AR (2020) A review on propagation of secure data, prevention of attacks and routing in mobile ad-hoc networks. Int J Commun Netw Distrib Syst 24(1):23–57
14. Pathak S, Jain S (2017) An optimized stable clustering algorithm for mobile ad hoc networks. EURASIP J Wirel Commun Netw 2017:1–11
15. Malar ACJ, Kowsigan M, Krishnamoorthy N, Karthick S, Prabhu E, Venkatachalam K (2021) Multi constraints applied energy efficient routing technique based on ant colony optimization used for disaster resilient location detection in mobile ad-hoc network. J Ambient Intell Humaniz Comput 12:4007–4017
16. Tilwari V, Maheswar R, Jayarajan P, Sundararajan TVP, Hindia MN, Dimyati K, … , Amiri IS (2020) MCLMR: A multicriteria based multipath routing in the mobile ad hoc networks. Wirel Pers Commun 112:2461–2483
17. Tran TN, Nguyen TV, An B (2019) An efficient connected dominating set clustering based routing protocol with dynamic channel selection in cognitive mobile ad hoc networks. Electronics 8(11):1332

18. Singh P, Khari M, Vimal S (2022) EESSMT: an energy efficient hybrid scheme for securing mobile ad hoc networks using IoT. Wirel Pers Commun 126:2149–2173
19. Sarkar D, Choudhury S, Majumder A (2021) Enhanced-Ant-AODV for optimal route selection in mobile ad-hoc network. J King Saud University-Computer Inform Sci 33(10):1186–1201
20. Drishya SR, Vijayakumar V (2019) Modified energy-efficient stable clustering algorithm for Mobile ad hoc networks (MANET). In: Kalita J, Balas V, Borah S, Pradhan R (eds) Recent Developments in Machine Learning and Data Analytics, vol 740. Advances in Intelligent Systems and Computing Springer Singapore, pp 455–465
21. Srinivas M, Patnaik MR (2022) Clustering with a high-performance secure routing protocol for mobile ad hoc networks. J Supercomputing 78(6):8830–8851
22. Bondada P, Samanta D, Kaur M, Lee HN (2022) Data security-based routing in MANETs using key management mechanism. Appl Sci 12(3):1041