Wireless Networks (2022) 28:2913–2936
https://doi.org/10.1007/s11276-022-02991-1

ORIGINAL PAPER

Trust-based energy-aware routing using GEOSR protocol for Ad-Hoc sensor networks

Ranjit Kumar[1] · Sachin Tripathi[1] · Rajeev Agrawal[2]

Published online: 14 June 2022

Abstract

The openness nature of the Ad-hoc sensor networks emerged as a security threat in this network environment that leads to packets drop, network overhead, high range energy consumption, and transmission delay. Previous methods such as Trust-Based Malicious Nodes Detection in AD-hoc (TBMND) and Security based Data-Aware Routing Protocol (SDARP) found that this happens due to malicious nodes in the network. A malicious node in a network degrades its efficiency that also affects the routing decision making and also makes error decisions in route selection. Trust vector model and Trust-based Secure Routing (TBSR) have made attempts to evaluate trust nodes via various techniques, but unfortunately, the accuracy level has not been reached to the required range. In this paper, a trust-based energy-aware routing using GEOSR protocol for Ad-hoc sensor networks is presented for providing an energy-efficient and secured routing. In this trust-based energy-aware routing, initially the sensor nodes are deployed in the ad-hoc network. The clustering is performed based on the estimation of distance among the each nodes and the cluster head (CH) is selected based on the threshold value. After CH selection, the trust evaluation is performed for identify the trust and untrusted nodes present in the network. The untrusted node is considered as malicious node which is detected and blocked. The trusted nodes are forwarded to select the optimal routing path for secured transmission. Golden Eagle Optimized Secure Routing (GEOSR) is introduced for selecting the optimal routing path based on the parameters such as distance delay and energy objective function. Thus, energy-efficient and secured routing were done using the GEOSR protocol. GEOSR protocol was then implemented in the NS-2 simulation tool and then compared with existing techniques. GEOSR protocol shows 95% of residual energy for the prediction of two malicious nodes. Thus GEOSR was suitable for real-time applications.

Keywords Energy consumption · Malicious Nodes · Plain text attack · Residual energy and trust evaluation

1 Introduction

Ad-hoc sensor networks are made up of spatially dispersed devices that work together to gather, process, and send physical or environmental data via wireless sensor nodes. Security has been regarded as the most difficult research topic in sensor networks, and security is especially critical in WSNs because the nodes of these networks are deployed in hostile environments [1]. Attackers can quickly capture and turn nodes into malicious nodes due to their small size and unsupervised deployment. Individual sensor nodes collect data of relevance, process it locally for specific purposes, and communicate the processed data directly or indirectly to the base station via intermediate nodes. One of the most essential properties of ad-hoc sensor networks is autonomy, which occurs when each node configures itself

✉ Ranjit Kumar
ranjit_kumaruitbu@yahoo.co.in

Sachin Tripathi
Var_1285@yahoo.com

Rajeev Agrawal
rajkecd@gmail.com

[1] Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, Jharkhand 826004, India

[2] G. L. Bajaj Institute of Technology and Management, Greater Noida 201306, India

without the need for centralized administration [2]. Furthermore, because no pre-existing infrastructure is required for network deployment, ad-hoc sensor networks have been utilized for a number of applications including security monitoring, intrusion detection, disaster management, and animal tracking and so on. With respect to the ad hoc networks [3] that innovate familiar links depend on decompositions that study them with the help of conventional methods like information theory and become interactive ones that result in a little path of the outcome. By gathering, prospects on techniques used to give a dynamical behaviour for multihop networks [4]. Securing basic network operation has become one of the major concerns in Ad-hoc networks that request for most reliable quality of service (QoS) communication in environments that are adversarial. The biggest threat lies in security communication that maintains connectivity in the show of adversaries between unknown as that of frequently changed multihop wireless network topology [5]. To predict this issue and its complexity that provides security at a rich level in two phases of communication as the route discovery must also remain secure.

Security is a critical issue to handle for autonomous and unsupervised ad-hoc sensor networks in order to assure the full functionality of the various applications. This is due to the vulnerability of sensor nodes to attacks such as selective forwarding, Sybil, and wormhole assaults. Most security solutions, such as cryptography, are software-based and are meant to primarily protect traditional networks from outside attacks [6]. However, such soft security is difficult to deploy in sensor nodes to protect against attacks, particularly from inside bad nodes. To deal with the hostile nodes in the network, trustworthy computing has been used to solve the problem [7]. Trust is simply a motivator for nodes to cooperate, and it is calculated depending on a node's action or behavior, such as delivering or discarding data packets in response to a request. Higher trust nodes receive more services from their peers, whereas lower trust nodes receive fewer or no services from their peers [8]. Sensor nodes likewise have a limited power supply and are typically discarded once their batteries have run out [9]. Clustering algorithms are a good way to balance the energy in a sensor network. In a clustering technique, all of the nodes in the network are divided into clusters, which are virtual subnetworks. Cluster Heads are elected by member nodes in each cluster (CHs). The cluster's most significant component, the CH, serves as a local coordinator for data transmission within the cluster and keeps track of the cluster's members and topology.

Securing the basic network operation that becomes one of the major concerns in Ad hoc network that in fact a programmable for its reliable Quality of Service (QOS) that spreads in adversarial communication environments [10]. The idea lies in secured maintenance and communication that connects the presence of adversaries between unknown values by rapidly changing multihop wireless network topology. To find the cause of this issue and give enhanced security levels in both phases of communication that gives route discovery and also data transmission that must be secured [11]. In recent days, a number of works that secure routing mechanisms that protect it against a wide range of attacks below different assumptions of requirements in the system. However, a routing protocol that guarantees an undisruptive and secure delivery of data that made corrections in the route discovery part does not guarantee undisrupted delivery that secures data value. By correcting them up to date route will not be able to be considered automatically for adversaries [12], and an efficient adversary might be able to follow rules that determine the route discovery and also place itself on a route that later started redirecting traffic, forging, dropping and data packet injection [13].

To overcome the problems present in the exiting method, the proposed method designed a Trust-Based Energy-Aware Routing in Ad-Hoc Sensor Networks. The sensor nodes are deployed and begins clustering based on a threshold. Cluster Head (CH) is assigned to the node with the highest energy, while member nodes are assigned to the node with the lowest energy. Each node gathers the behavioural data of its neighbours and transmits it to BS through CH. BS is now assessing the trust computation procedure. Direct trust, indirect trust, packet drop test, attribute test, and total trust value are all part of the trust computation process. The nodes that are trustworthy are forwarded for routing, whereas the nodes that are malevolent are termed malicious nodes. This rogue node's information is disseminated throughout the network, and these nodes are then disconnected from it. Routing was also done by analyzing energy, distance, and latency and then selecting a route using the GEO algorithm, which then processes and transmits the packets via the existing connections. Major contributions of this paper are

- For safe routing, the proposed work seeks to distinguish between antinode and safe-node nodes and also protect routers from stretch attacks and carousel.
- Malicious nodes are detected via a trust-based approach. The child-parent mechanism in the mechanism is based on the trust that examines every impact on a node by the impact.
- In order to further enhance network security by adding attribute trust and packet drop to the present mechanism of direct and indirect trust.
- Through the GEOSR protocol, the node detection is handled by the suggested solution that processes at the

base station. This allows the system to save energy while still maintaining QoS (quality of service).

By developing a trusted node based route selection, a secured ad-hoc network has been ensured in this paper. The rest of the paper is organized as follows. Section 2 is likely to describe related works for routing in Adhoc and their disadvantages. Section 3 explain in detail about GEOSR approach, and Sect. 4 shows the proposed model analysis and its comparative analysis. Section 5 concludes the paper.

2 Literature review

Many energy-efficient routing models have been presented conventionally. Some of them are reviewed, and their drawbacks are given below.

Gong et al. [14] have introduced a trust vector model depend on routing models. Every node that computes its specific trust vector value for about its parameters with respect to its neighbours via neighbouring pattern and its traffic in a network environment. Likewise, trust dynamics have been included in the term of robustness, then an evaluation for each node with its modified behaviour was done. Bertino et al. [15] have presented an architectural framework with respect to assurance of trustworthiness. Computation of data provenance with its trust model that as for estimation for cost level of data and also trust level with data renders. However, data provenance was a policy based query evaluation that does not support all applications. Malar et al. [16] have presented the MCER-ACO method that chosen next-hop node made in the centre on the constraints given. Residual energy for the mobile node, packet number in path and topology movement in dynamic topology movement. An application of ant colony has been used here for selecting the next hop. However, the routing table has been updated periodically, which does not seem able to manage to route efficiently. Poongodi et al. [17] have presented a framework based on trust along with a mechanism that predicts DDOS attacks in VANET. Primary trust elements for the computation of frequency value statistics, residual energy, and data factor and trust hypothesis statistics. However, few nodes in the infrastructure of VANET does not accept message security via time stamp was a drawback of this method.

Gunasekaran et al. [18] have presented a swarm-based defence approach that was used to migrate the faulted channel at a normal operating channel via frequency hop techniques. Analysis was done based on transmission parameters such as false positive, negative rate, transmission efficiency and overhead. However, this method, unfortunately, need more cost for improving its performance. Kim et al. [19] have presented energy-efficient and secure mobile node authentication (ESMR) for wireless networks. Security analysis verified that ESMR meets the security requirements of MWSNs and can prevent relevant security attacks. A maximum network time and low delay value could not be achieved with this approach. Its data collection rate also impacts energy efficiency.

Jhaveri et al. [20] developed an improved trust model for secure routing in mobile ad-hoc networks based on attack pattern discovery. The balance between security and energy efficiency is one of the most important considerations while designing a safe routing system for Mobile Ad-hoc Networks (MANETs). In order to meet Quality-of-Service (QoS) criteria in the network, routing decisions are critical in ensuring secure data transmission and balancing power consumption at the network layer. The goal of this study is to compare the energy efficiency of several secure routing algorithms for dealing with packet forwarding misbehavior in MANETs. The methods are tested in NS-2 against a variety of attackers and under various network conditions. Jhaveri et al. [21] had presented Evaluating Energy Efficiency of Secure Routing Schemes for Mobile Ad-Hoc Networks. This strategy addresses the problem by combining a trust model with an attack pattern finding tool. A designed trust-based approach based on nodes' historical behaviors that uses a pattern discovery mechanism to detect suspicious activity from hostile nodes before they start discarding data packets, extending the Ad-hoc On-demand Distance Vector (AODV) routing protocol. This research also show the detailed activities of three adversary models that initiate various types of packet forwarding misbehavior.

Authors	Title	Methodology	Advantage	Disadvantage
Salam et al. [22]	Bioinspired Mobility-Aware Clustering Optimization in Flying Ad Hoc Sensor Network for Internet of Things: BIMAC-FASNET	Developed a bioinspired mobility-aware clustering optimization technique for routing that takes into account relative mobility, residual energy, degree, and communication load during CH selection and balanced cluster building, based on bee intelligence foraging behavior	Multi-UAVs can be used for remote sensing, tracking, observation, and monitoring. Its nature differs from that of a typical ad hoc network	The speed and different orientations of multi-UAVs make it more difficult to route data in the appropriate direction
Kumar et al. [23]	SDARP: Security based Data	In this method, an unique strategy based on the	This strategy minimized security and	In ad hoc sensor networks, obtaining

Authors	Title	Methodology	Advantage	Disadvantage
	Aware Routing Protocol for ad hoc sensor networks	Security based Data Aware Routing Protocol (SDARP) was designed for high data gathering in order to achieve a balance between security and energy metrics	network traffic problems	sensed data in an energy efficient manner is crucial for the sensor network to operate for a long time
Sajan et al. [24]	Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network	In this method designed Secure Atom Search Routing (SASR) algorithm, which is based on molecular dynamics behavior, is used to give security to the network during data transmission	The method aims to make the battery last longer	Although cryptographic techniques can assist prevent data tampering, they cannot protect against carousal and stretch attacks

From these related works, it has been seen that the drawbacks of previous methods are increased packet drop, network lifetime, security threat and energy consumption. Hence, there was a need for a routing protocol that considers both secure routing and energy consumption.

3 Proposed methodology

Attack affects Ad-hoc network communication in many methods, and it can modify and copy the data packet that is sensed and might result in BS to consider any false routing results. Stretch attack and carousal attack affects the sensor network performance. The proposed design of Golden Eagle Optimized Secure Routing (GEOSR) deploys nodes in sensor space and starts perform clustering with respect to the threshold. The node energy greater than the threshold is designated as Cluster Head (CH), and others are considered as member nodes. Each node gathers the behavioural data of other neighbouring broadcasts and nodes them to BS via CH. Now, BS starts evaluating the trust computation process. The trust computation process involves different types such as direct trust, indirect trust, Packet drop test, attribute test and total trust value. By performing trust evaluation, the nodes that are trustworthy is forwarded for routing, and other nodes are considered as a malicious node. This malicious node and its details are further broadcasted in the network, and these nodes are then disconnected from the network. Further, routing was done by analyzing the energy, distance and delay the route selection is made via GEO algorithm that further process and go ahead to transmit the packets via links that are established.

Figure 1 illustrates the proposed trust-based energy aware routing using GEOSR protocol for Ad-Hoc sensor networks. Initially, the sensor nodes are deployed in Ad-hoc network. After node deployment, the distance and transmission energy among the each nodes are calculated. Then, determine the residual energy of each nodes in the network. If the threshold value is less than 0.05, the nodes are joint as a member node in the network and if the threshold value is grater 0.05 the node is considered as a cluster head. Thus, more effective cluster are selected. Each node gathers the behavioural data of other neighbouring broadcasts and nodes them to BS via CH. Now, BS starts evaluating the trust computation process. The trust computation process involves different types such as direct trust, indirect trust, Packet drop test, attribute test and total trust value. According to the trust evaluation, the trusted and non-trusted nodes are identified. Moreover, the trusted nodes are forwarded for routing and the non-trusted nodes are considered as malicious node. This malicious node and its details are further broadcasted in the network, and these nodes are then disconnected from the network. Further, routing was done by analysing the energy, distance and delay the route selection is made via GEO algorithm that further process and go ahead to transmit the packets via links that are established (Fig. 2).

3.1 Network model

By representing a topology for wireless ad hoc networks with respect to graph $H(\mathbb{W}, \mathbb{E})$ as they were set of nodes that denoted vertices and edges as $\mathbb{W}$ *and* $\mathbb{E}$ respectively. Every node is assigned as an individual integer between 1 and $P = |X|$. Assuming that nodes are powered using a battery. The remaining battery of energy node is $v \in X$ denoted by D_v. While the node battery energy drops under the threshold D_{th} and the node is defined as a dead node. By not considering the loss of generality, the assumption was made as $D_{th} = 0$. By denoting the link in the network as (u, v) as they indicate as sending nodes and receiving nodes further. For the criteria of the link between u *and* v there is a link always with a pre-set value of threshold with respect to received signal strength. Selection of threshold has been made by satisfying the probability of targeted link error. By denoting the probability of free reception, errors consist of packets in a length of x bits, which is transmitted with respect to u and v.

For the necessity of routing via nodes, assumptions have been made that nodes begin to support transmission power. Power is transmitted from node u to v that fits a fixed set of permittable power of transmission. Nodes are assumed to have a pre-programmed set of power ratings. A minimum

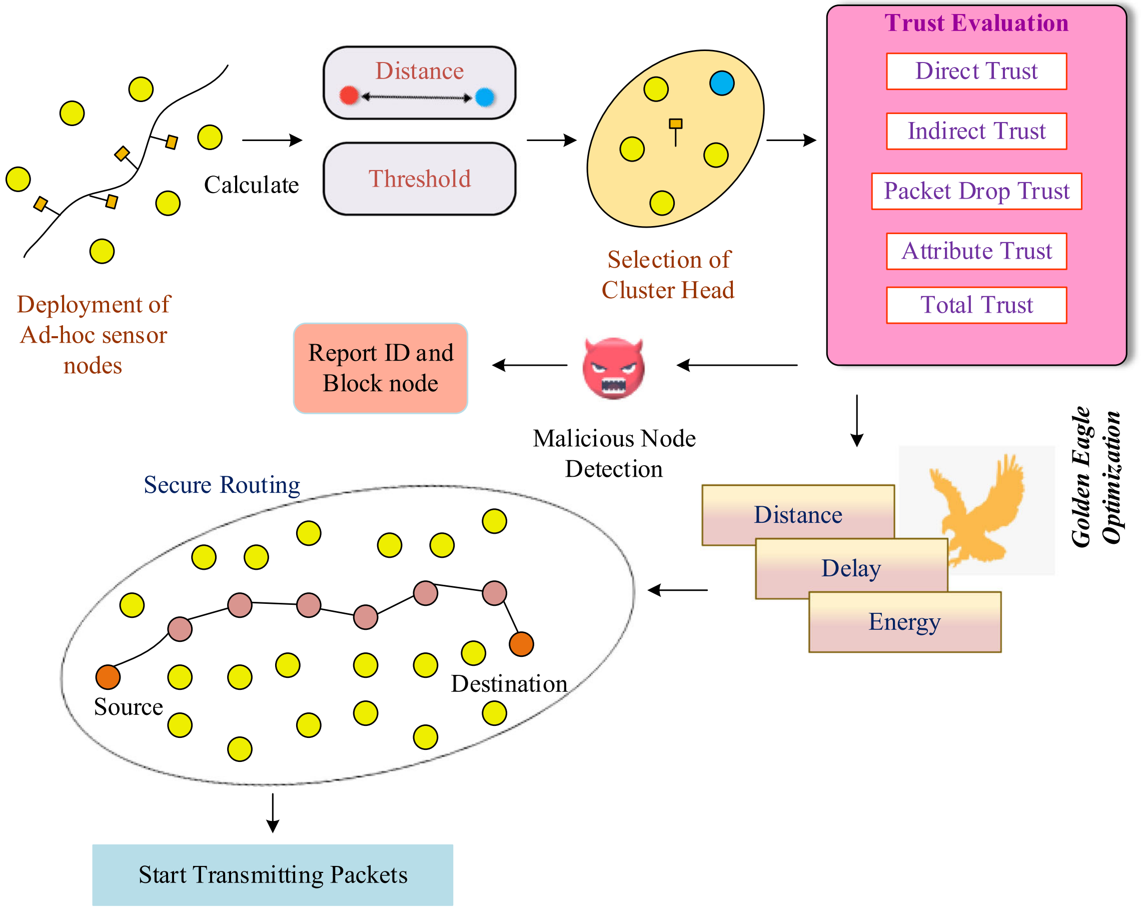


Fig. 1 Overall architecture of the proposed GEOSR model

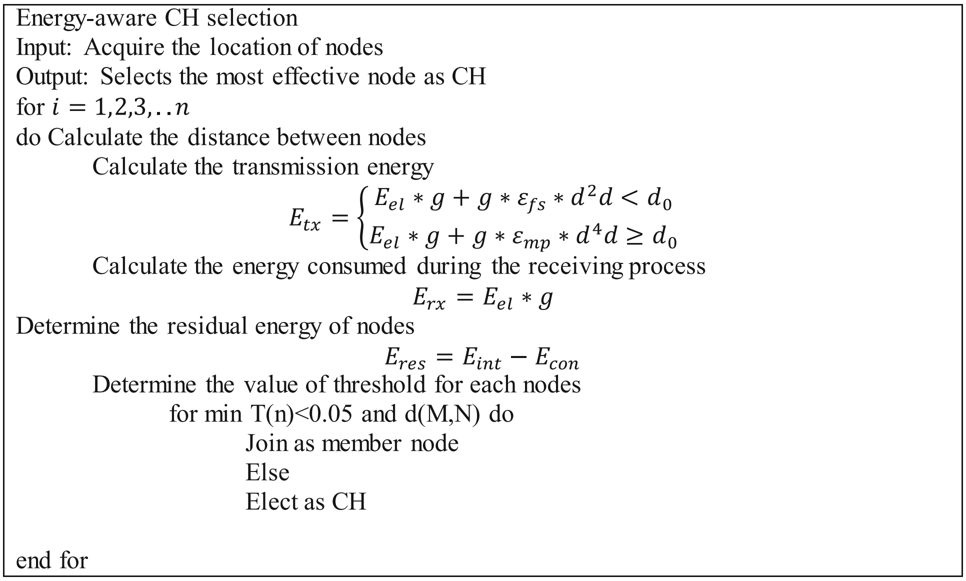
value is assumed as transmission power and also assumed that the physical link contains data rate, which does not change. By representing a network path with h hops among the set of nodes $\mathcal{Q}(\mathfrak{n}_1, \mathfrak{n}_{h+1}) = \{\mathfrak{n}_1, \mathfrak{n}_2, \ldots, \mathfrak{n}_h, \mathfrak{n}_{h+1}\}$ here $n_m \in W$ is given as the selector of the m th node $(m = 1, 2, \ldots., h + 1)$ for every route. By determining the source node as n_1 and its destination node is denoted as n_{h+1}.

3.2 Cluster formation

While implementing sensor nodes in each node of a network that computes its level of energy using derivation (1) by selecting the random number between 0 and 1 that represents their neighbouring value of nodes that contains their ID, the threshold of the smallest value has been set to a value of 0.05, in the process of continuation method nodes that starts to relate this value of threshold with its neighbouring threshold value. When the value is lower than the threshold, all other neighbouring nodes that select themselves as Cluster Head (CH) presents a message to neighbouring nodes. Rather it connects as a member along with a sensor that has a minimum threshold value. Using this approach, the network is partitioned into a various number of clusters, with each cluster that has CH. CH's are required to make a link and share data with neighbouring ones. In order to determine the threshold value, it was done by using the Eq. (1)

$$Z(n) = \begin{cases} \dfrac{S}{1 - S * \left(rmod \dfrac{1}{p}\right)} \times \dfrac{E_{cur}}{E_{int}} ifn \in T \\ 0, Otherwise \end{cases} \tag{1}$$

In Eq. (1), E_{cur} represents current energy of the node, E_{int} denotes primary energy of the node, sensor node percentage is denoted as S rather than selected as CH. By presenting their estimated energy for the entire neighbouring nodes, these nodes consist of a lower value than the threshold as it will be selected as CH from other nodes joined as CH in the member nodes. The selection of CH is done by using the threshold value for each round, as that is based on energy. Implying that the issue for selecting nodes with the minimum amount of residual energy than selected CH.



```
Energy-aware CH selection
Input: Acquire the location of nodes
Output: Selects the most effective node as CH
for $i = 1,2,3,..n$
do Calculate the distance between nodes
        Calculate the transmission energy
            $E_{tx} = \begin{cases} E_{el} * g + g * \varepsilon_{fs} * d^2 d < d_0 \\ E_{el} * g + g * \varepsilon_{mp} * d^4 d \geq d_0 \end{cases}$
        Calculate the energy consumed during the receiving process
            $E_{rx} = E_{el} * g$
Determine the residual energy of nodes
            $E_{res} = E_{int} - E_{con}$
        Determine the value of threshold for each nodes
                for min T(n)<0.05 and d(M,N) do
                        Join as member node
                        Else
                        Elect as CH

end for
```

3.3 Intrusion detection system

Security threats might affect the network by intruding on the first line of defence as that requires a secure intrusion detection system. It is left as a silent guard behind the first line that predicts threats that stops and ensure them before causing severe effects. The major objective of developing intrusion detection is to automate them and attempt to interrupt the integrity. For observing the behaviour and traffic of networks, predicting the unwanted happenings in the network and at the last stage setting up isolation for this unwanted activity. Intrusion Detection System (IDS) undergoes four phases, namely.

1. Collection of data	2. Trust verification of data
2. Recognition of intrusion, and	4. Reporting and blocking them

One of WSN's dynamic challenges is detecting malicious nodes. If a cluster member is malevolent, the data delivered to the Cluster Head is corrupted, and the cluster as a whole fails. As a result, identifying malicious nodes is critical. To efficiently identify malicious nodes, the proposed CHMND uses Cluster Head (Self-test) to detect dangerous nodes. The Cluster Head examines its cluster's routing table to see whether any nodes have sent data to other nodes without their knowledge, and if so, flags that node as a malicious node. The primary node is responsible for storing information about nodes and identifying malicious nodes that send data from one cluster to another. Another method is to send a message to Cluster Head with the node id to check the node if any other node receives data from another member node. The Cluster Head examines the node to see whether it is malicious. The proposed system assumes a node to be malicious if it transmits data to any other node without knowledge of Cluster Head. These malicious activities are monitored by the system in the network with the help of the knowledge base and its interference engine. By storing the Base Station values in the knowledge base, the data is then collected from the CHs network that is then permitted by CH with the help of an inference engine. The inference engine takes responsibility for creating rules at the knowledge base for performing the operation, and every member node creates events that consist of behavioural data value—monitoring the node activity and sharing its collection of data that is taken under the control of CH that verifies the BS data. By verifying them, if it is found that it is a malicious node selected that gets out by computing the fitness function. By sending a threatening message along with data according to malicious node and CH, as they are computing a complicated sensor node that minimizes the result in speedy performance.

3.3.1 Collection of data

Data collection is an essential function as the management entities gather node and network details from the Ad hoc network. Details such as status of battery power, link quality, direction and speed are collected from each node. Message overhead may occur while performing the data collection process in ad hoc networks due to its limited bandwidth. In the application layer, network management executes as it is the simplest way for data collection.

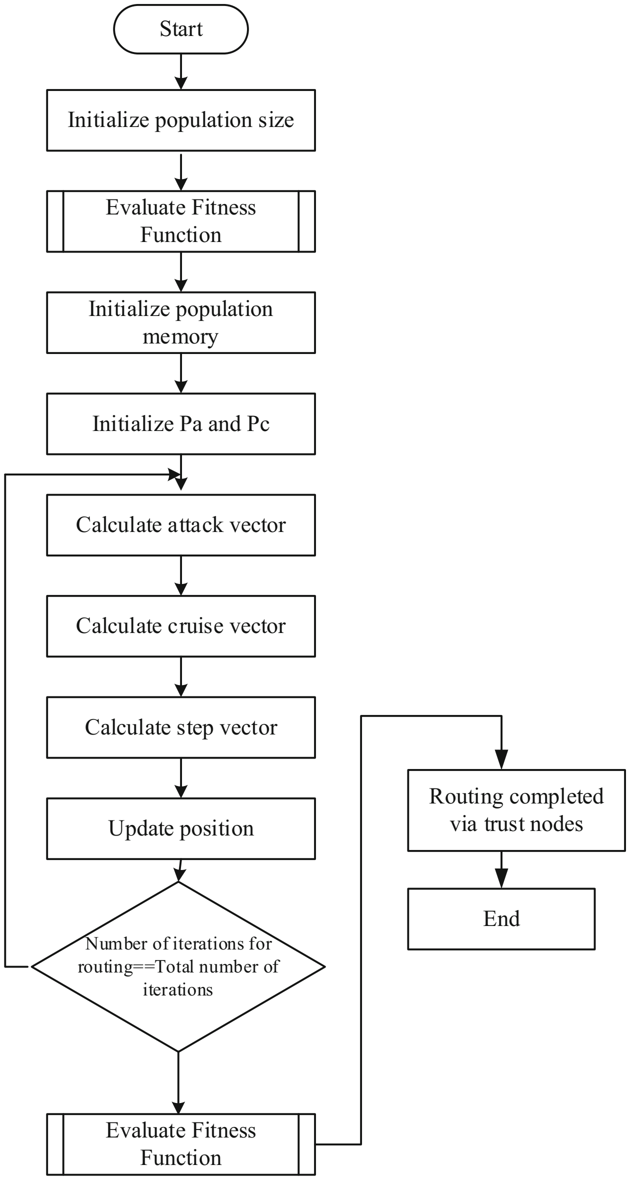

Start
Initialize population size
Evaluate Fitness Function
Initialize population memory
Initialize Pa and Pc
Calculate attack vector
Calculate cruise vector
Calculate step vector
Update position
Number of iterations for routing==Total number of iterations
Evaluate Fitness Function
Routing completed via trust nodes
End

Fig. 2 Flow diagram of selecting route using GEO

3.3.2 Trust verification of data

Based on the behaviour and traffic of sensor networks the trust is verified, the believability degree between nodes begins to transfer the data even securely as network nodes do not show the delivery extraction of data. Rather it can also update more details in the acknowledged data packets and also transfers them to the approaching node. Thus, it is necessary to make sure that the transferring of data between nodes are secure. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attacks. The attack against privacy is passive in nature. Some of the more common attacks against sensor privacy are monitoring and eavesdropping, traffic analysis and camouflage adversaries. If the unauthorized attackers monitor, listen and modify the data stream in the communication channel, then the attack is active attack. Routing attacks such as spoofing, replay, selective forwarding, sinkhole, Sybil, wormhole are active attacks. Denial of service attacks such as neglect and greed, misdirection, black hole are also active in nature. Trustless detail occurs when there is an attack by a passive or active attack. General attacks occur at the stage of transmission, and it's related to carousal attack or stretch attack. This happens when the malicious node makes the data packet circle continuously in loops. The packets to reach the destination node is not permitted, and this abnormal behaviour caused duplicate node energy to decrease severely in a small amount of time. There are two types of Trust, indirect and direct trust, that depends on the contact of two single nodes that get computed. By calculating indirect trust for informative and other related nodes that are trusted. Whether packets of the data request is not established by BS, a time interval is given inside, and BS takes CH to compute the trust value for the entire node of members. The equation for Direct trust is given as shown in (4)

$$Z^k(t) = \frac{S_{n1}(t)}{S_{n2}(t)} \tag{2}$$

In this Eq. (2), $Z^k(t)$ is termed as direct trust is calculated among the nodes n1 and n2. $S_{n1}(t)$ and $S_{n2}(t)$ are received packets and total packets sent. Equation (3) shows the indirect trust calculated with respect to neighbouring nodes as shown.

$$Z^J(t) = \frac{1}{m}\sum_{k=1}^{m} Z^k(t) \tag{3}$$

In this equation, m represents the number of neighbouring nodes, and direct trust degree is computed and denoted as $Z^k(t)$. Drop trust is computed and established on the history of prior packet drop along with its neighbours

$$Z_{DT} = \frac{1}{k}\sum_{k=1}^{m} \frac{Z_{Dk}}{Z_{Sk}} \tag{4}$$

In this Eq. (4), Z_{DT} represents packet drop trust value, Z_{Sk} represents previously sent the total number of packets by i to the neighbouring node $\ominus$, the number of packets is represented by Z_{Dk} that leaves the neighbouring node k received previously. Whether the packet drop trust gets closer to 1 and it shows the untrustworthy mode. The attributed value of trust is calculated before the sensor deployment, and some attributes are assigned to each node like country, source ID, language and destination ID and also the position of the destination. While initializing communication between each node, the process checks for the next neighbour hop node and thus a common interest with every node using Eq. (5)

$$Z_{at} = \frac{N_{commatt}}{N_{numberatt}} \tag{5}$$

In this Eq. (5), the total number of attributes are denoted as $N_{numberatt}$ and common number of attributes are denoted as $N_{commatt}$. With the help of this equation, common attributes are reduced and emphasized the degree of trust. When the ratio of attributes value is 1, then it denotes that the node has a maximum degree of trust value. Hence, the total trust degree is given as shown in Eq. (6)

$$Z = \propto Z^k(t) + \beta Z^j(t) + \gamma Z_{DT} + \delta Z_{at} \tag{6}$$

Previously the value for α, β, γ *and* δ starts from 0 and 1, that is given as $\alpha + \beta + \gamma + \delta = 1$, after that threshold value for trust is given as $0.99 - 1$ and thus it is calculated with the value that drops beyond this value. The sensor is considered a malicious node because it has more packet loss at the time of transmission. Successful consideration of trust factors is done for transmitting the data to be reached at the delivery side at a particular path value.

3.4 Malicious node detection

By performing the verification process, depending on its trust degree equation, the BS selects a malicious node, transmits an alert message to CH within the location, and it's the ID for choosing a malicious node at the sensor space. At this stage, CHs now separate and blacklist the fault node and then it represents ID for the entire member nodes in the cluster.

i. *Problem formulation for secure routing*

The BS collects the data periodically according to the entire neighbouring nodes of source node i collected from the set of data, the evaluation of fitness is done by BS $f(x)$ for the n number of neighbouring nodes with the help of the proposed algorithm. After the process of evaluation, the ID of the best-identified neighbour is sent by BS to the source node i. The execution of the objective function is done for each position of nodes using the formula as given in Eq. (7)

$$f(x) = \frac{1}{4}[Z + N + E + d(i,j)] \tag{7}$$

In this Eq. (5), Z is the trust, E is the delay in packet delivery, N is the consumed total energy by the node and $d(i,j)$ is the distance between nodes $iandj$. Here, the trust is calculated from Eq. (7)

ii.
Distance

The objective function utilizes distance between sensors and distance from BS to SNs. In order to select optimal CHs, $f1$ is to be minimized, and it is given by Eq. (8),

$$d_{dist} = \left(\sum_{i=1}^{M} \theta(n_{SN}, p_{CH}) + \theta(p_{CH}, p_{BS}) \right) \tag{8}$$

In this equation, $\theta(n_{SN}, p_{CH})$ represent the distance between SNs to CH and $\theta(p_{CH}, p_{BS})$ denotes the distance between CH to BS and M denoted number of sensor nodes.

iii. *Energy*

Communication, when occurs through CH, it needs to update the value for every transmission. Therefore residual energy of CHs gets drained, which further reduces the lifetime of the network. Next, the objective for CH selection is given as a function that inverse the total current energy of all CHs selected.

$$N_{res} = E_{Tot} - \left(E_c + E_{tran} + E_{rec} + E_{agg}\right) \tag{9}$$

Equation (7) represents, residual energy of the node.E_{Tot} represents the total energy of SN, E_c denotes energy consumed during data collection and E_{tran} denotes energy consumed during data transmission and E_{rec} and E_{agg} energy consumed for reception and aggregation is denoted as and respectively. Hence, the selection of a node with high energy and less energy consumption as CH might be helpful for an appropriate CH based routing.

iv.
End-to-end delay

The excess time is taken to reach the sink from the data packet. Vampire attacks like the carousel and stretch attack, which cause a high delay in packet transmission.

$$D = \frac{AT - ST}{K} \tag{10}$$

ST is the sent time, AT is the arrival time, and K is the number of connections.

v. *Fitness Function*

Fitness function evaluation for the proposed design is given as shown in Eq. (11)

$$Minimizef(x), wherex = \left(x^1, x^2, \ldots, x^D\right) \tag{11}$$

D is the matrix dimension, and i is the number of nodes Considering four dimensions based on delay, trust, energy and distance.

3.5 GEOSR routing model

Golden Eagle Optimization (GEO) is originated for the change of intelligence on the attack and cuisine propensity, in which the golden eagle performs the search for hunting and prey. Golden eagles had a close relationship with humans. They held sacred and lofty locations in the principles; meanwhile, tribal humans and ancient were considered as a sign of positive events. Attack, cruise and the intelligent balance that makes the golden eagle lay between these two are the natural appearances of exploitation, transition and exploration from the prior to the final. This covers the method for devising a metaheuristic algorithm.

i. *Spiral motion of golden eagles*

GEO is established depending on helix based motion of Golden Eagles, as the eagle kept the best location in memory, and it is either way denoted as the best solution. Memory is now filled with the best solution obtained from them so far visited place. Eagle gets attracted to prey and moves towards a cruise in search of better food; during every iteration, golden eagle i selected a random prey of another f termed golden eagle. By designing circle around best location visited by f eagle. As it selects to circle its own memory, it can be given as $f \in \{1, 2, ...popsize\}$.

In every iteration, the golden eagle selects prey to analyze cruise and attack progressions. This optimization algorithm is modelled in such a way that the best solution is identified so far is kept in memory. After iteration, the search agent gets an updated position, and hence memory gets updated. Each and every golden eagle chooses its prey and by using a random one to one mapping technique.

ii.
Exploitation phase

By initializing the vector, the attack can be generated from the present location of the golden eagle that stops when matched with a location in the memory eagle. Golden eagle attack vector can be derived from Eq. (12)

$$\vec{A_i} = \overrightarrow{X_f^*} - \vec{X_i} \tag{12}$$

Here $\vec{A_i}$ is denoted for eagle's attack vector i and $\overrightarrow{X_f^*}$ is the best position of eagle and $\vec{X_i}$ is the current location of the eagle. As attack vector tends to the population of golden eagle towards best-visited locations and it focuses exploitation phase in this algorithm.

iii. *Exploration phase*

The linear speed of the golden eagle is calculated as a cruise vector. Basically, it is an attack vector. It remains tangent to perpendicular and tangent to the circle of the attack vector. With n-dimensions, a tangent hyperplane is located inside the circle. Therefore by calculating hyperplane, the attack vector can be calculated. The scalar form of the hyperplane equation is given in Eq. (13).

$$h_1x_1 + h_2x_2 + \ldots + h_nx_n = d \rightarrow \sum_{j=1}^{n} h_jx_j = d \tag{13}$$

In Eq. (4), $h_1, h_2, h_3, \ldots, h_n$ is normal vector and $x_1, x_2, x_3, \ldots, x_n$ is variables vector. To find circle, arbitrary point of hyperplane $P_1, P_2, P_3, \ldots, P_n$ and distance vector $d = \vec{H}.\vec{P} = \sum_{k=1}^{n} a_kx_k = \sum_{k=1}^{n} a_k^t x_k^*$. By assigning random values to all variables except $k - th$ variable as it has fixed value. The fixed value is calculated using Eq. (14)

$$D_m = \frac{d - \sum_{j,j\neq m} a_k}{a_m} \tag{14}$$

3.5.1 Update position

Dislocation of f termed golden eagles comprises both cruise vector and attack vector. Step vector for golden eagle f in i equation t as given in Eq. (15).

$$\Delta_{yi} = \vec{r_1} P_a \frac{\vec{A_i}}{\vec{A_i}} + \vec{r_2} P_c \frac{\vec{C_i}}{\vec{C_i}} \tag{15}$$

In Eq. (7), the attack coefficient is represented as P_a^t at t iteration and cruise, the coefficient is represented as P_c^t at the same iteration. By adjusting the values of the attack vector and cruise vector, two random vectors are selected, such as $\vec{r_1}$ and $\vec{r_2}$ with an interval [-1, 1]. Euclidean norm variables are represented as $\vec{A_i}$ and $\vec{C_i}$ and derived using Eqs. (16) and (17)

$$\vec{A_i} = \sqrt{\sum_{j=1}^{n} a_j^2} \tag{16}$$

$$\vec{C_i} = \sqrt{\sum_{j=1}^{n} C_j^2} \tag{17}$$

By adding a step vector, the space of the golden eagle in iteration t + 1 is computed in each t iteration to its position. Hence position update can be derived using Eq. (18)

$$x^{t+1} = x^t + \Delta x_i^t \tag{18}$$

After calculating the fitness function, if the new position is a better solution than the position already placed in the memory, the memory of the eagle gets updated to a new position, or it remains without change.

3.5.2 *Update $p_a andp_c$*

GEO optimization use $p_a andp_c$ values to shift from exploration to exploitation. It gets executed from low p_a value to high p_c Value. By defining initial and final values, intermediate values are calculated using linear transition by using Eq. (19)

$$\begin{cases} p_a = p_a^0 + \frac{t}{T}\left|p_a^T - p_a^0\right| \\ p_c = p_c^0 - \frac{t}{T}\left|p_c^T - p_c^0\right| \end{cases} \tag{19}$$

In Eq. (11), the current iteration is indicated by t, and the maximum iteration is indicated by T. The final and initial values for the attack vector are p_a^0 and p_a^T respectively. Final and initial values for the propensity to cruise vector are p_c^T and p_c^0 respectively. Golden Eagle Optimization is able to predict the best position of the Trust node to perform routing using various operators.

```
Initiali1ze the population of golden eagles
Evaluate Fitness Function
Initialize population memory
Initialize pa and pc
For each iteration t
Update pa and pc
compute crowding distance for previous archive values
for each golden eagle i
Randomly select prey from archive using roulette wheel
weighted by crowding distances
Compute attack vector
if attack vectors length is not equal to zero
Compute cruise vector
Compute Step vector
Update Position
Evaluate fitness function in new position
if new position is non-dominated to present archive values
if external values is not  full
add new solution result to the archive
else
Compute sparsity distance
Select outgoing archive members
By weighting roulette wheel for sparsity distances
replace outgoing solution with new one
end
end
end
end
```

Wireless ad hoc sensor network with trust-based secure routing initially performs clustering the different numbers of the network. Each CH is assigned with each cluster, and its member nodes for every cluster is represented as $M, SandN$. Collection of data is done based on details collected like node energy, distance, delay, trust values, source address node, as well as destination node. This is then sent to BS that finds out the malicious activity. If any nodes are identified as malicious nodes, then the nodes are not considered to establish routing. While transmitting data routing, a path is recognized that forwards the data packets and at the stage of a secured path chosen with the help of GEO algorithm for transmitting data in an effective way with low energy consumption and ought to eliminate other malicious packets. As stated, path selection for a secure process contains finding a safe route for transmitting data. It denotes that the path is not affected by the stretch attack and false data injection. The nodes check the presence of antinode at the time of data transmission with the attained details for evaluating trustworthiness. By disconnecting the connection with antinodes, a route has been selected using GEO optimization.

3.5.3 Malicious node isolation

If the behaviour ID of the antinode is transmitted by BS to the entire sensors inside the network as a broadcast message, safe nodes that receive this message disconnects their connection with that antinode completely, and that antinode gets isolated.

```
Input : Data from each next hop neighbouring nodes
Output: Genuine next hop neighbour
for each next hop neighbouring node do
    compare the residual energy of the senor nodes with the threshold value
    calculate the distance between the neighbouring node and the destination
    calculate the delay in communication with the neighbouring nodes
    For the node with min $f(x)$
        Do GEO
        Select next hop forwarding node
    Else
        Choose alternate path for forwarding node
    Else
        Choose alternate path and report node with minimum trust
    End for
End for
```

Indirect trust, direct trust, attribute test, packet drop test and total trust value are all part of the trust computation process for isolating the malicious node. The nodes that are trustworthy are routed for routing, while the ones that are malevolent are labelled as such. This rogue node's information is transmitted throughout the network, and these nodes are then detached from it. Routing was also done by analyzing energy, distance, and latency and then choosing a route using the GEO algorithm, which then processes and transmits the packets across the existing networks. Attacks can have a number of impacts on Ad-hoc network communication, such as duplicating and altering detected data packets, leading BS to make incorrect routing decisions. The impacts of stretch and carousal assaults have an impact on the functioning of a sensor network. The suggested Golden Eagle Optimized Secure Routing (GEOSR) architecture positions nodes in sensor space and started clustering depending on a threshold. The Cluster Head (CH) is assigned to the node with the most energy, while the member nodes are assigned to the node with the least energy. Each node collects behavioural data from its neighbours and sends it to BS through CH. BS is currently evaluating the trust computation process. Figure 3 illustrates the process flow of the proposed architecture.

4 Experimental results

There are various methods in which attacks disrupt Ad-hoc network communication, including the ability to duplicate and alter data packets that might lead BS to make an incorrect routing choice. The effect of carousal attack and stretch attack also disturbs the performance of the sensor network. At data packets and stretch attacks are controlled by multiple nodes that in return cause drainage of energy, the data packet is transferred as in the form of a loop that shows an outcome of state at which the identical node appears in the route n times. The proposed design of Golden Eagle Optimized Secure Routing (GEOSR) was implemented in the NS-2 simulation tool, then evaluated for its performance using parameters delay, False Positive Rate (FPR), Precision, Residual Energy (RE), Recall and throughput. Evaluated parameters are then compared with previous techniques such as SDARP (Security based Data-Aware Routing Protocol) for Ad-hoc sensor networks, Reliable Minimum energy cost routing (RMECR), Trust-based Secure Routing (TBSR) and Secure Trust aware energy-efficient adaptive routing in wireless sensor networks (STEAR).

A deterministic deployment and a random deployment are the two main forms of deployment. This deployment method is ideal when the application environment is understood, the network operation status is reasonably stable, and the sensor nodes are clearly positioned in space. As shown in Fig. 4, nodes are deployed randomly as per the coverage rate. As soon as the sensors are deployed, the coverage rate is utilized to determine the effectiveness of the deployment process. Given that is the sensor's coverage area and that is the monitoring area's size, the coverage rate can be calculated as 13. In this proposed deployment,

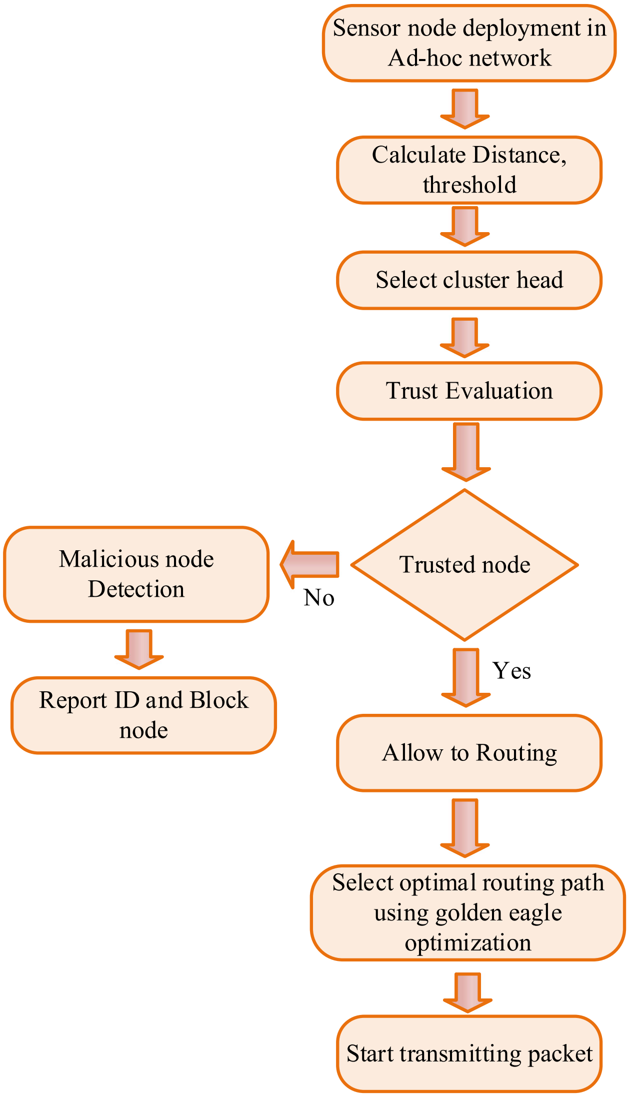

Sensor node deployment in Ad-hoc network
Calculate Distance, threshold
Select cluster head
Trust Evaluation
Trusted node
No
Yes
Malicious node Detection
Report ID and Block node
Allow to Routing
Select optimal routing path using golden eagle optimization
Start transmitting packet

Fig. 3 Process flow of the proposed architecture

there are 50 sensors deployed in the environment, and then it was clustered based on Euclidean distance. Depending on the distance, the sensors are then clustered, as shown in

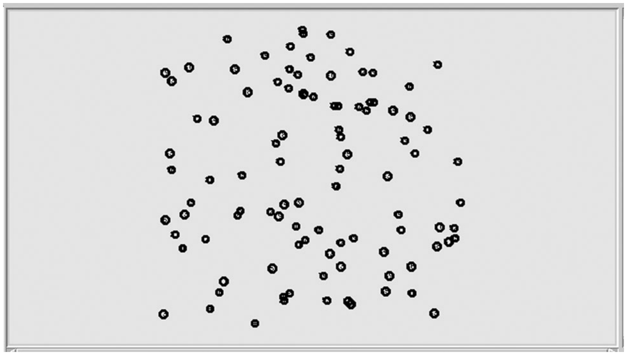


Fig. 4 Deployment of nodes

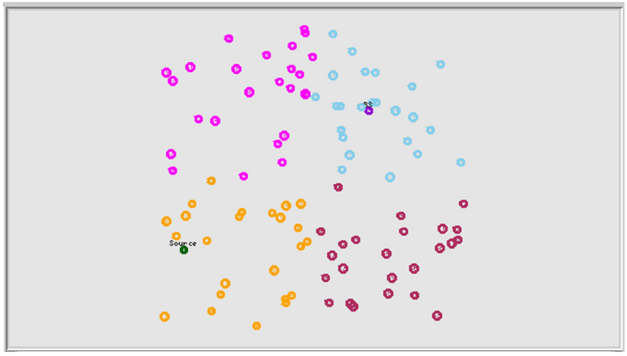


Fig. 5 Clustering of nodes

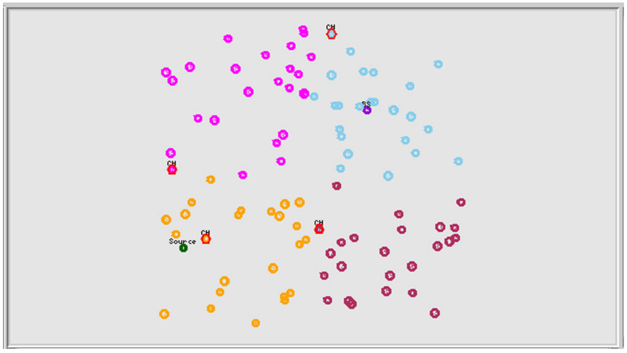


Fig. 6 Cluster head selection

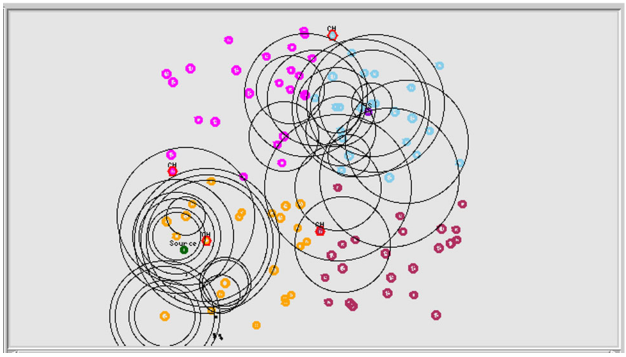


Fig. 7 Data transmission signals

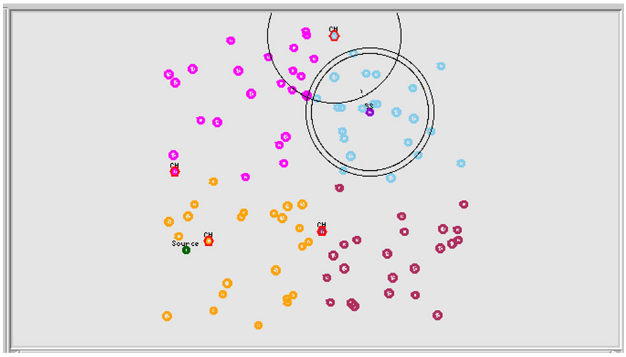


Fig. 8 GEOSR protocol-based routing

Table 1 Parameters of network

Parameters	Value
Area of the network	1000m^2
Number of sensors in the network	100
Position of base station	(100,10)
Initial energy of sensor node	2.0 J
Communication range of CH	50 m
Transmission energy	0.01 J
Receiving energy	0.01 J
Data packet size (bytes)	500
Data transmission rate	1 Mbps
Threshold value of CH	0.05
Number of malicious nodes	10–50

Fig. 3. Figure 5 shows 4 clusters as they are eventually clustered for routing.

The formation of clusters deploys the sensor network, and every cluster has its member nodes and Cluster Head (CH) that has CH in the count for collecting data from member nodes that share Base Station (BS) with us. Cluster Head is selected such that its neighbouring nodes are minimum and distance to BS, and this method is used to transmit the data packet faster with a minimal amount of time delay. As part of the cluster, there is a master node and at least two workers. In order to execute operations, all of these nodes interact with one another over a common network. This master node is the CH node, selection of CH was made in the proposed design using the initial energy level of the node, the node that postulates higher energy was selected as CH, as shown in Fig. 6.

Selection of CH was made, and then it tends to make optimal routing using the GEO optimization technique. For that, there was a necessity to perform a certain process to evaluate the parameters, and this was done using the transmission of signals that was shown in Fig. 7.

Figure 8 shows the path taken by GEOSR protocol, nodes that are secure ones were used for routing. Node 51 is blocked due to its maliciousness that was determined by the mechanism of trust evaluation. After blocking compromised node selection of CH was made that to make a route via the established ones. Analysis was done with respect to previous methods that are then shown in the next stage. Chosen by CH to build a route via the existing nodes after blocking compromised nodes, previously used

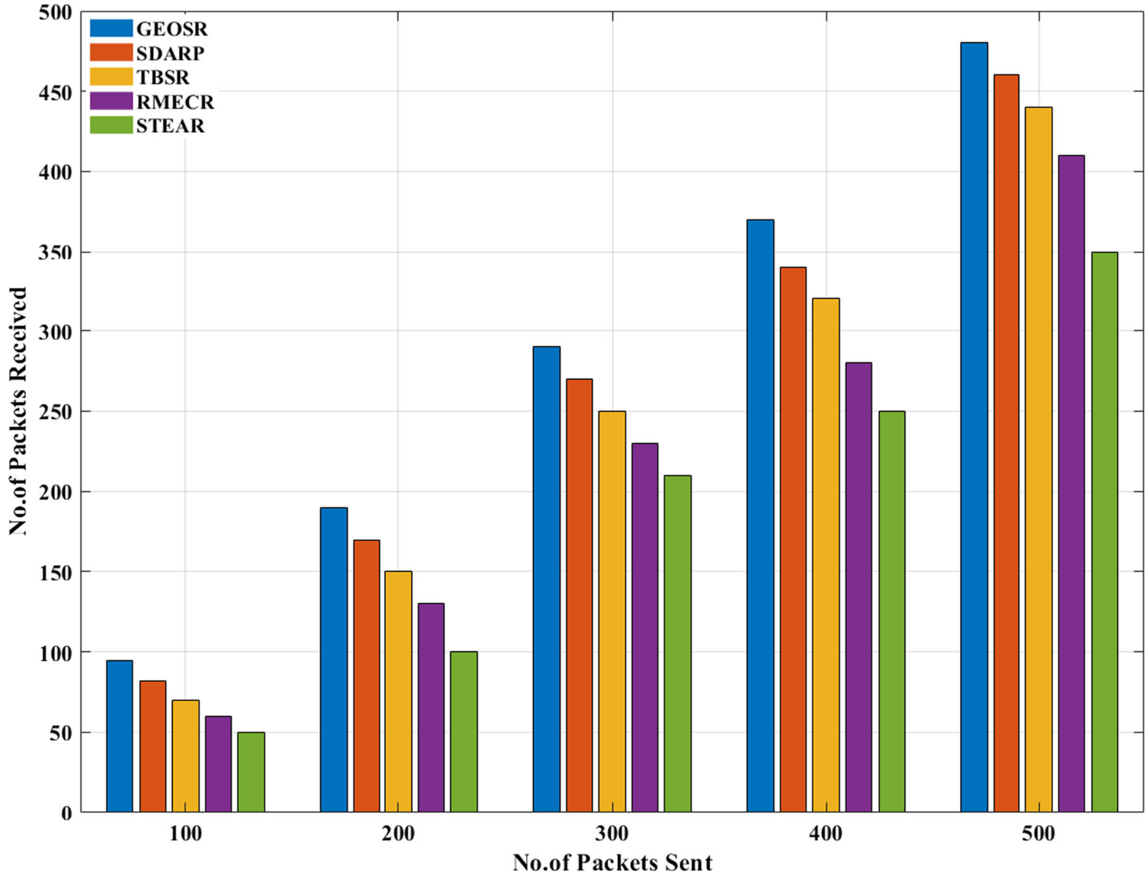


Fig. 9 Comparison graphs for previous methods of packets sent vs packets received

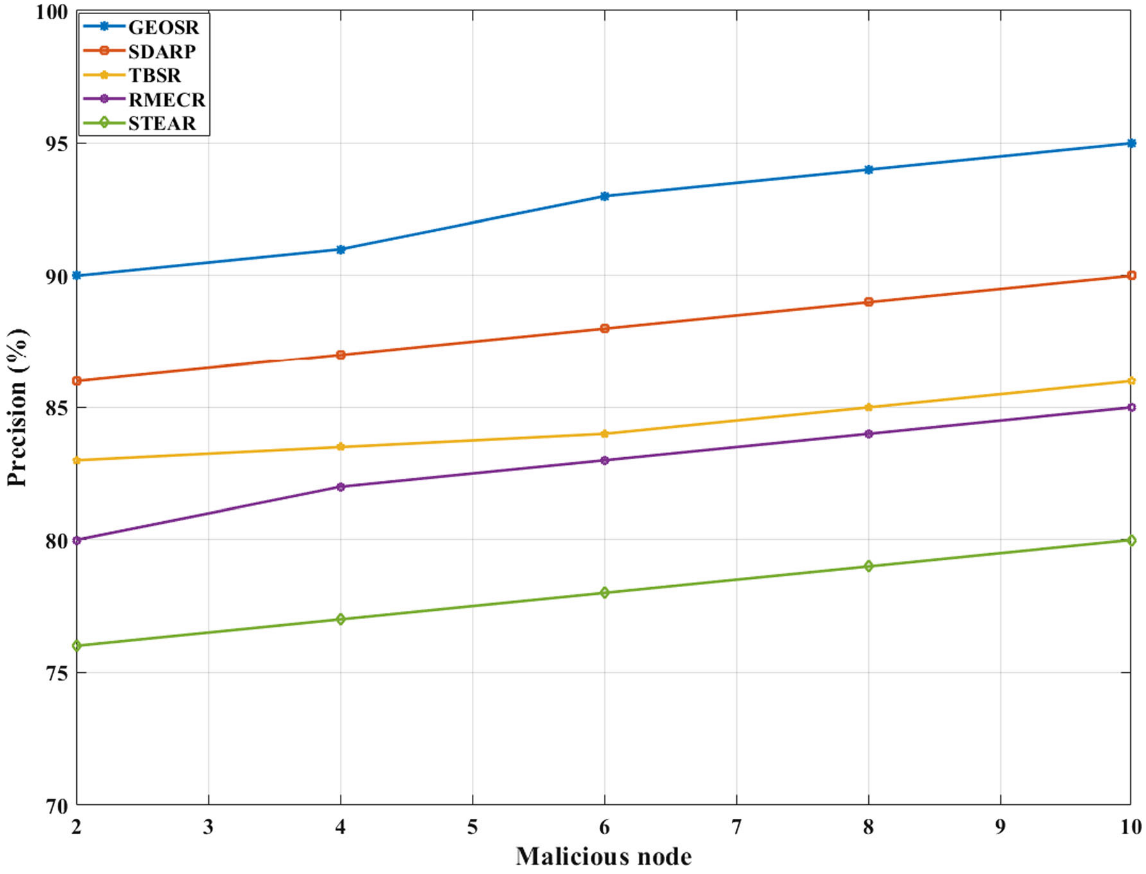


Fig. 10 Comparison graphs for previous methods of malicious node vs precision

approaches were examined and compared in the following stage. An energy consumption analysis was performed so as to find that the proposed model was performing better than previous ones. Parameters of the network are tabulated in Table 1.

From Fig. 9, it was clearly visible that when the number of packets transmission rate increases, then receiving rate also should be increased for an efficient routing protocol. From the graph, when 100 packets are transmitted, GEOSR receives 99 packets that show the proposed routing protocol has been secured, and on the other hand, other techniques such as SDARP, TBSR, RMECR and STEAR shows a quite higher level of packet dropping rate. Similarly, while transmitting 200 packets, STEAR showed an increased packet drop rate of 100 that was not suitable for long-distance applications as this might cause loss of packets completely. RMECR gives 130 packets, TBSR shows reception of 150 packets, and finally proposed GEOSR protocol gives reception of 190 packets. At a transmission of 300 packets, the GEOSR model gives a maximum of 290 packets, SDARP gives data packets in a range of 275, and STEAR shows data packet reception in the range of 250. While transmitting 500 packets, the proposed GEOSR gives maximum retrieval at the receiver side. On the receiver side, 475 packets have been obtained at the reception side. The reception rate has been increased to a certain extent as it was due to the elimination of malicious nodes. Routing has been done only via secure nodes. Thus, the GEOSR model performed better while transmitting packets at the node environment.

In this paper, use both P and R to evaluate the accuracy of the proposed scheme for identifying dishonest nodes in Ad-hoc. F-score (F) is the weighted average of, and R values are used to reflect the overall accuracy of the trust management model. The parameters are defined as follows

$$P = \frac{No.oftrulymaliciousnodecaught}{Totalnumberofdishonestnodescaught}$$

$$R = \frac{No.oftrulymaliciousnodecaught}{Totalnumberoftrulynodescaught}$$

$$F = \frac{2 * P * R}{P + R}$$

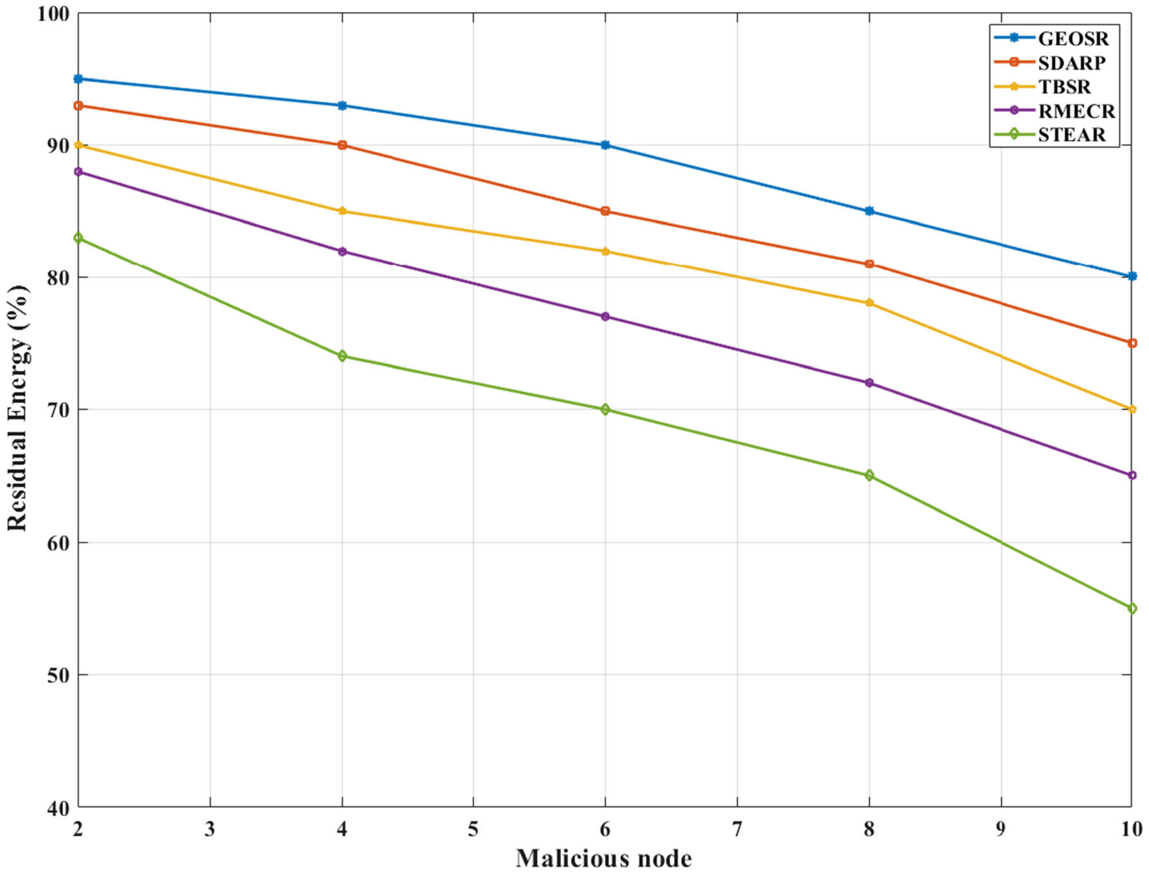


Fig. 11 Residual energy vs malicious node

From this Fig. 10, it was clearly seen that the number of malicious nodes caught for the GEOSR model has been higher than other previous methods. For other methods such as SDARP, the precision value ranges from 86% and ranges up to 90% for predicting 10 malicious nodes. The other previous methods, such as TBSR, shows a lesser precision value of 83%, and it has been reached a range of 86%. Thus, finally, the GEOSR protocol reached a higher range of 90% to 95% precision values. GEOSR has been vitally proved to be used during real-time applications.

Figure 11 shows the measurement graph for the number of malicious nodes with respect to residual energy. As residual energy has been considered as the best parameter to evaluate node level that gets wasted while transmitting via malicious node. Thus measurement of residual energy while detecting malicious nodes is necessary. At the deployment of 50 nodes, the malicious node was found in the range of 2–10. For proposed GEOSR, residual energy has been measured to be high, which was more than 95%, which has been then minimized but remains in a standard range of 80%. SDARP, TBSR, RMECR, STEAR methods undergo a loss of residual energy for an increase in the malicious node that as of 92%, 90%, 89% and 82%, respectively. The minimum level of previous methods are 55%, 65%,70% and 79%, thus proposed GEOSR reached 80% of residual energy even malicious node detection got increased. Figure 12 shows the graph for recall values vs malicious nodes. From the analysis of observation, the proposed GEOSR is higher than the other remaining methods. The score of the proposed GEOSR is higher than the remaining STEAR, RMECR, TBSR and SDARP. GEOSR shows a higher range of 94% and further increased linearly up to the range of 96% that shows that the proposed model was efficient than other methods.

Figure 13 illustrates comparison analysis of average delay vs malicious node. The proposed technique is compared with several existing techniques such as, SDARP, TBSR, RMECR and STEAR. The proposed techniques attained average delay (ms) 0.1 at malicious node 2, 0.5 at malicious node 4, 2 at malicious node 6, 3 at malicious

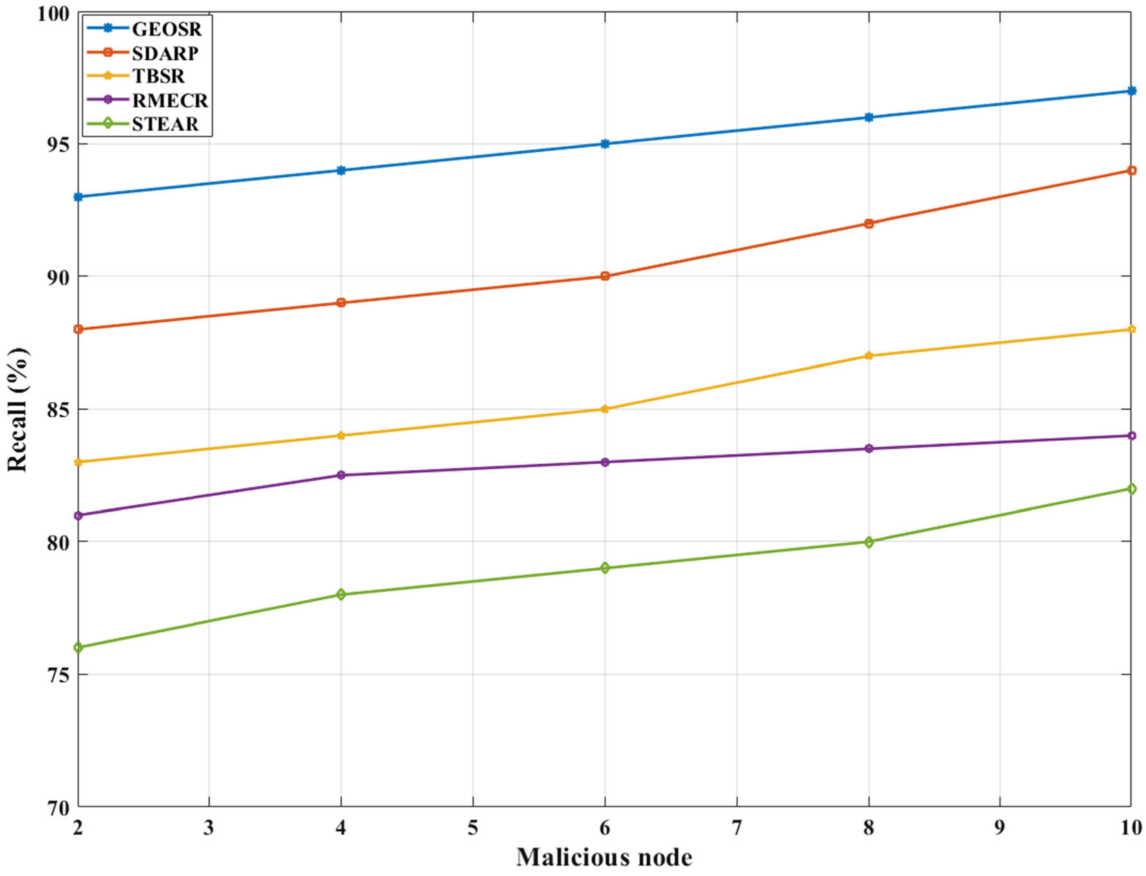


Fig. 12 Recall vs malicious node

node 8. The SDARP techniques attained average delay (ms) 1 at malicious node 2, 1.5 at malicious node 4, 2 at malicious node 6, 6 at malicious node 8. The TBSR techniques attained average delay (ms) 1.5 at malicious node 2, 1.7 at malicious node 4, 4 at malicious node 6, 10 at malicious node 8. The RMECR techniques attained average delay (ms) 3 at malicious node 2, 5 at malicious node 4, 7 at malicious node 6, 12 at malicious node 8. The STEAR techniques attained average delay (ms) 5 at malicious node 2, 7.5 at malicious node 4, 10 at malicious node 6, 17 at malicious node 8. As the result, the proposed technique attained less delay compared to other techniques.

Figure 14 shows the malicious detection rate for the proposed GEOSR protocol by comparing it with the existing protocols such as STEAR, RMECR, TBSR and SDARP for trust update intervals of 0.02, 0.04, 0.06, 0.08, and 0.1. When trust is updated at the time interval of 0.02 s, the detection rate is at the maximum of 50%. With a time period of 0.02 s, the detection rate reaches a maximum of 50%. Increasing the time interval causes a steady drop in the detection rate. The suggested approach, according to the study, has the highest detection rate compared to the existing methods. According to the GEOSR algorithm, trust, latency, energy, and distance between nodes are all taken into account while determining which way is the For each node with the five best surrounding nodes. First, the fitness function is computed, and then location and velocity are updated. It is decided to choose the most optimum approach for packet delivery among these five best neighbour nodes. This improves the detection of malicious activity in the network.

Figure 15 shows the analysis conducted for FPR (False Positive Rate) methods SDARP STEAR, RMECR and TBSR. True Negative (TN) is the number of antinodes that are mistakenly identified as real nodes (TN). Precision is analyzed by changing the number of Malicious Nodes from 10 to 50% is used to analyze the FPR. The FPR is determined using FPR = FP/FP + TN. According to the understanding of FPR, the TBSR and STEAR are 0 below 10% malicious nodes. While the FPR for the remaining method SDARP is higher than the TBSR method of about 10%.This enhancement in SDARP because of the

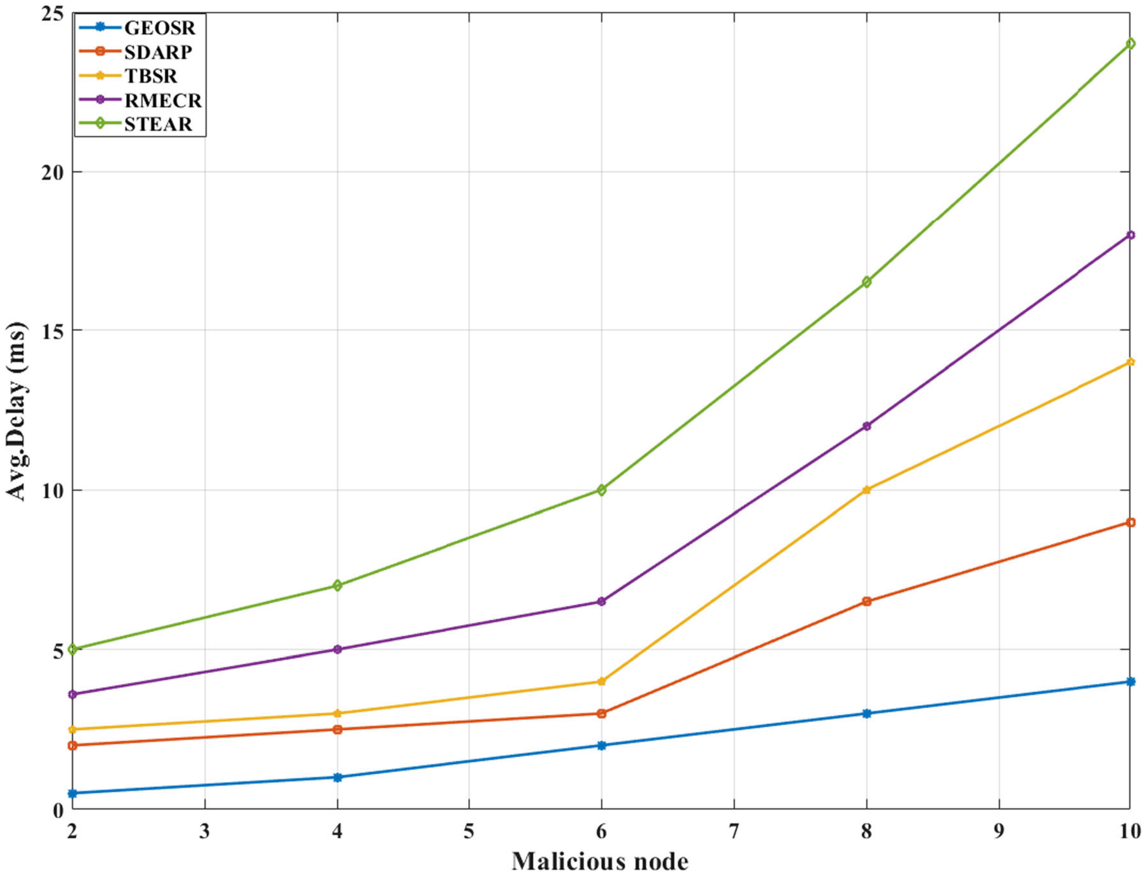


Fig. 13 Average delay vs malicious node

introduction of an effective trust mechanism that considers the quantity of the packet delivered successfully for GEOSR, the previous history of packets dropped by the nodes and the similarities in attributes.

Figure 16, while the present algorithms are unable to identify malicious activity in the network produced by stretch and carousal attacks, GEOSR offers the longest lifespan possible. Using transmission of closed-loop to reach longer route for their target, these assaults use more energy from the sensors. So the network's life expectancy decreases faster.

Table 2 illustrates the comparison analysis of proposed TEAR-GEOSR technique with some existing techniques such as, ERP, ESMR. The proposed method obtained throughput of 200(kbps) which is greater compared to other two techniques. ESMR have throughput of 135 (kbps) and TERP have throughput of 150 (Kbps). The proposed method obtained average delay is 0.1(ms) which is less compared to TERP techniques and having same average delay of ESMR technique. ESMR have throughput of 0.1 (ms) and TERP have throughput of o.4 (ms).

Table 3 illustrates the comparison of packet transmission among proposed and existing technique. The proposed technique is compared with several existing techniques such as, EATSRA [28], ECATS [30], ETGSA [29] and TCSSA [27]. The proposed technique attained Packet Transmission Rate (%) is 99.6, 99.1, 98.7, 98.6 and 98.4 at different mobility speed (M/s). EATSRA technique attained Packet Transmission Rate (%) is 96.7, 94.3, 94.5, 92.8 and 90.1 at different mobility speed (M/s). ETGSA technique attained Packet Transmission Rate (%) is 98.5, 96.5, 94.1, 89.5 and 88.3 at different mobility speed (M/s).

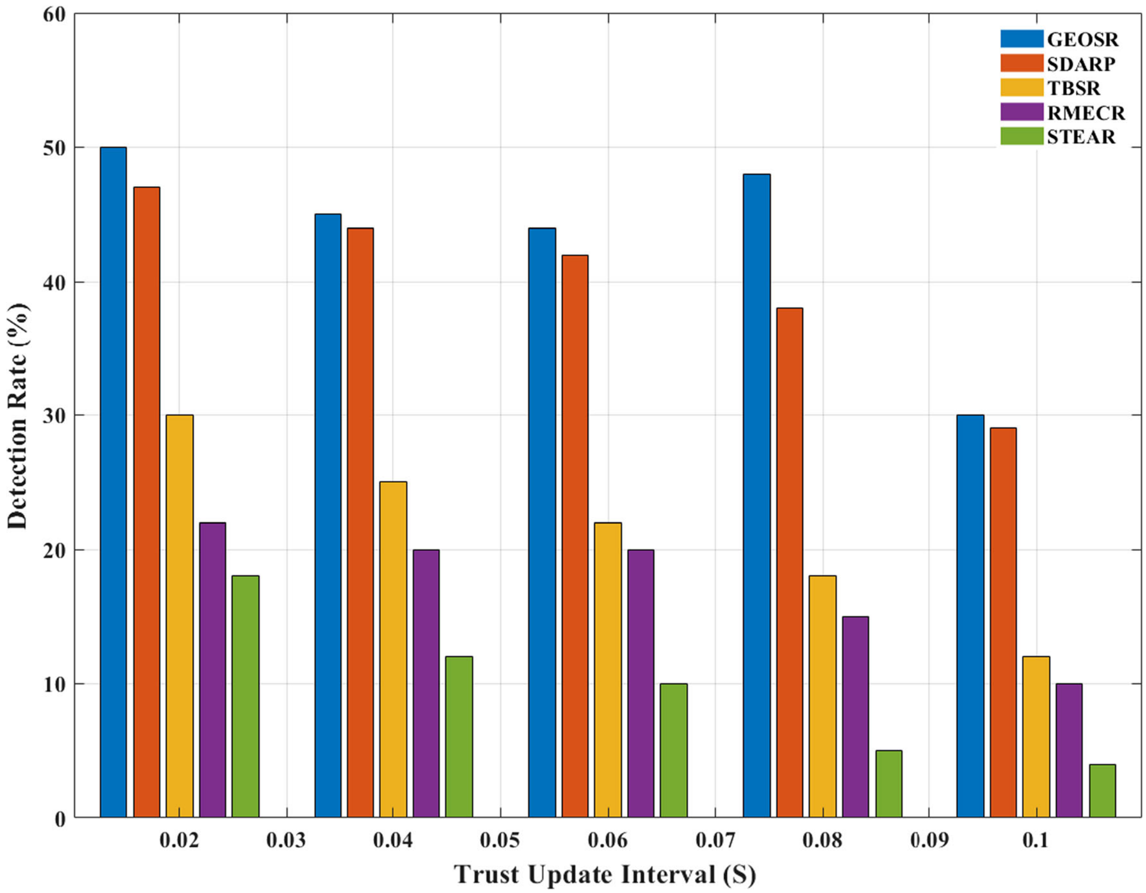


Fig. 14 Malicious detection rate

ECATS technique attained Packet Transmission Rate (%) is 98.3, 98.1, 97.3, 97.4 and 94.3 at different mobility speed (M/s). TCSSA technique attained Packet Transmission Rate (%) is 98.5, 94.1, 90.2, 88.4 and 87.8 at different mobility speed (M/s). Compared to the exiting technique the proposed technique attained better outcome.

Table 4 illustrates the comparison of network life time among proposed and existing technique. The proposed technique is compared with several existing techniques such as, EATSRA [28], ECATS [30], ETGSA [29] and TCSSA [27]. The network life time (%) of the proposed technique attained 49, 65, 79, 94 and 96 at different number of nodes. EATSRA technique attained network life time (%) is 45, 62, 80, 85 and 91 at different number of nodes. ETGSA technique attained network life time (%) is 42, 52, 66, 75 and 80 at different number of nodes. ECATS technique attained network life time (%) is 41, 51, 69, 74 and 78 at different number of nodes. TCSSA technique attained network life time (%) is 43, 57, 71, 77 and 81 at different number of nodes. Compared to the exiting technique the proposed technique attained better outcome.

Table 5 illustrates the comparison of attacks based on the packet delivery ratio. The attack are analysed based on the packet delivery ratio and number of malicious nodes. At two malicious nodes present in the network then the packet drop ratio is 4, 4.5, 5 and 6. At four malicious nodes present in the network, the packet drop ratio is 4.5, 4.5, 5 and 6.3. At six malicious nodes present in the network then the packet drop ratio is 4.5, 4.5, 5.5 and 7. At eight malicious nodes present in the network, the packet drop ratio is 4.5, 5, 5.5 and 7.5. At ten malicious nodes present in the network then the packet drop ratio is 4.5, 4.5, 6.2 and 8.

The average delay is given by graphical representation in Fig. 17. The proposed GEOSR protocol is related to the

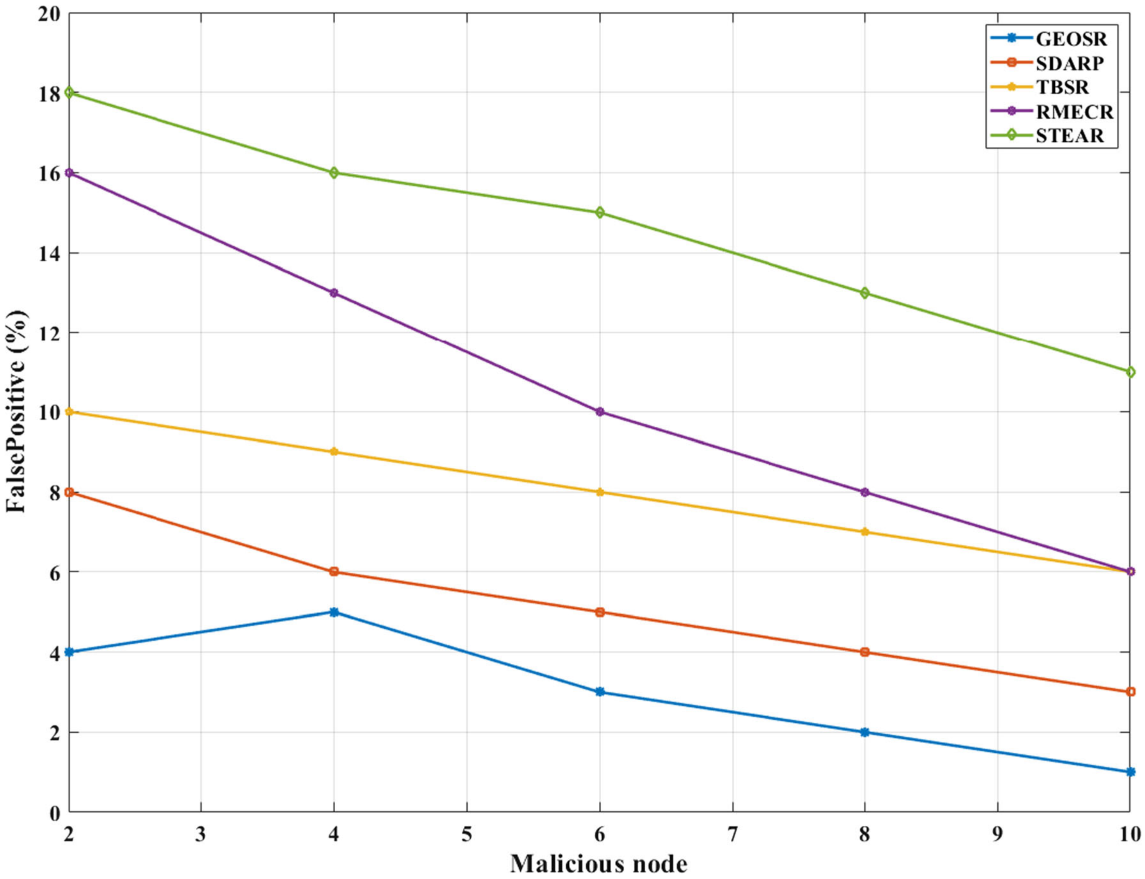


Fig. 15 False positive rate detection

protocols of existing STEAR, RMECR, TBSR and SDARP under 2 to 10 malicious nodes. The maximum delay of STEAR has 24 ms for 10 malicious nodes, whereas the suggested GEOSR algorithm has the minimum delay of 2 ms for 10 malicious nodes, based on the For example while assessing the fitness function, STEAR considers delays. Fitness is determined by the neighbouring node with the least or minimal latency. Nodes with a large delay are deemed unfit for packet transmission and vice versa. STEAR can now transmit packets with less delay.

Figure 18 shows the developed average amount for the GEOSR below the changing number of malicious nodes. From that, the entire method decreases as the number of antinodes increases. Nevertheless, the proposed GEOSR protocol has the maximum throughput than STEAR, RMECR, TBSR and SDARP. Throughput value started from 200kbps and reached 180kbps value, SDARP started from 180kbps and reached 159kbps value. Similarly, on the other hand, TSBR starts from 159kbps and reaches 100kbps value, again started from RMECR starts from 150kbps then reached 90kbps value. Most recursive throughput starts from 120kbps and ends at 70kbps. Thus, the proposed GEOSR reached a maximum value of throughput that shows that there was an efficient data transmission at the receiver side.

5 Conclusion

In this paper, trust and energy-based routing protocols have been presented. This mechanism can successfully detect malicious nodes then made actions on them. Golden Eagle Optimization (GEO) for route selection in the network protects against plain text attacks utilizing a trust evaluation method and Golden Eagle Optimization (GEO). Clustering based on distance was done after initializing the nodes in the field. The cluster head (CH) was selected based on a threshold value. To pick the next hop, parameters such as the distance delay and the energy objective function were used in GEO. A series of simulations were

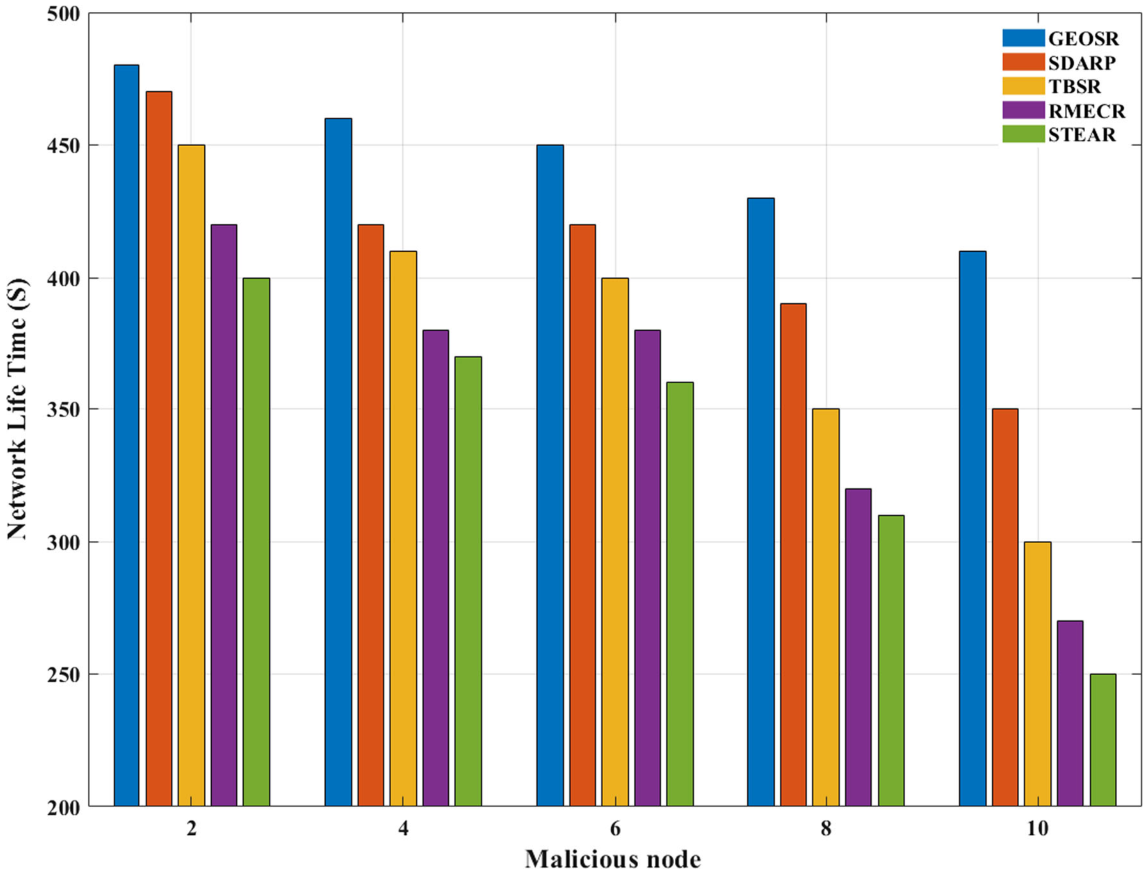


Fig. 16 Network Lifetime

Table 2 Comparison of proposed techniques with exiting techniques

Authors	Method	Throughput (kbps)	Average Delay (ms)
Ahmed et al. [25]	TERP	150	0.4
Haseeb et al. [26]	ESMR	135	0.1
Proposed	TEAR-GEOSR	200	0.1

Table 3 Comparison of packet transmission ratio among proposed and existing techniques

Mobility speed (M/s)	Packet transmission rate (%)				
	EATSRA [27]	ETGSA [28]	ECATS [29]	TCSSA [30]	Proposed
1	96.7	98.5	98.3	98.5	99.6
5	94.3	96.5	98.1	94.1	99.1
10	94.5	94.1	97.3	90.2	98.7
15	92.8	89.5	97.4	88.4	98.6
20	90.1	88.3	94.3	87.8	98.4

done to test the performance of the GEOSR model. Simulation results showed that the presence of malicious node in ad hoc sensor network that is combined with trust mechanism of proposed mode, which has been better than other previous techniques as that of GEOSR shows high packet delivery ratio. Thus, the GEOSR protocol can be used in real-time applications. Upcoming work contains adjusting the GEOSR model to respond to more attacks from malicious in an Ad-hoc environment. The future work will be based on modifying the proposed model to communicate more malicious attacks on the MANET like, resource consumption attack, Byzantine attacks, wormhole attacks and attacks targeting the confidence model, for example, making confidence model and plotting to

Table 4 Comparison of network lifetime among proposed and existing techniques

Number of nodes	Network life time (%)				
	EATSRA [27]	ETGSA [28]	ECATS [29]	TCSSA [30]	Proposed
15	45	42	41	43	49
25	62	52	51	57	65
55	80	66	69	71	79
105	85	75	74	77	94
205	91	80	78	81	96

Table 5 Comparison of attacks

Number of malicious nodes	Packet delivery ratio (10^{-3})			
	Rushing attack-MAET EW-R	Black hole Attack -MANET EW-BH	Rushing attack-WSN OW-R	Black hole attack-WSN OW-BH
2	4	4.5	5	6
4	4.5	4.5	5	6.3
6	4.5	4.5	5.5	7
8	4.5	5	5.5	7.5
10	4.5	4.5	6.2	8

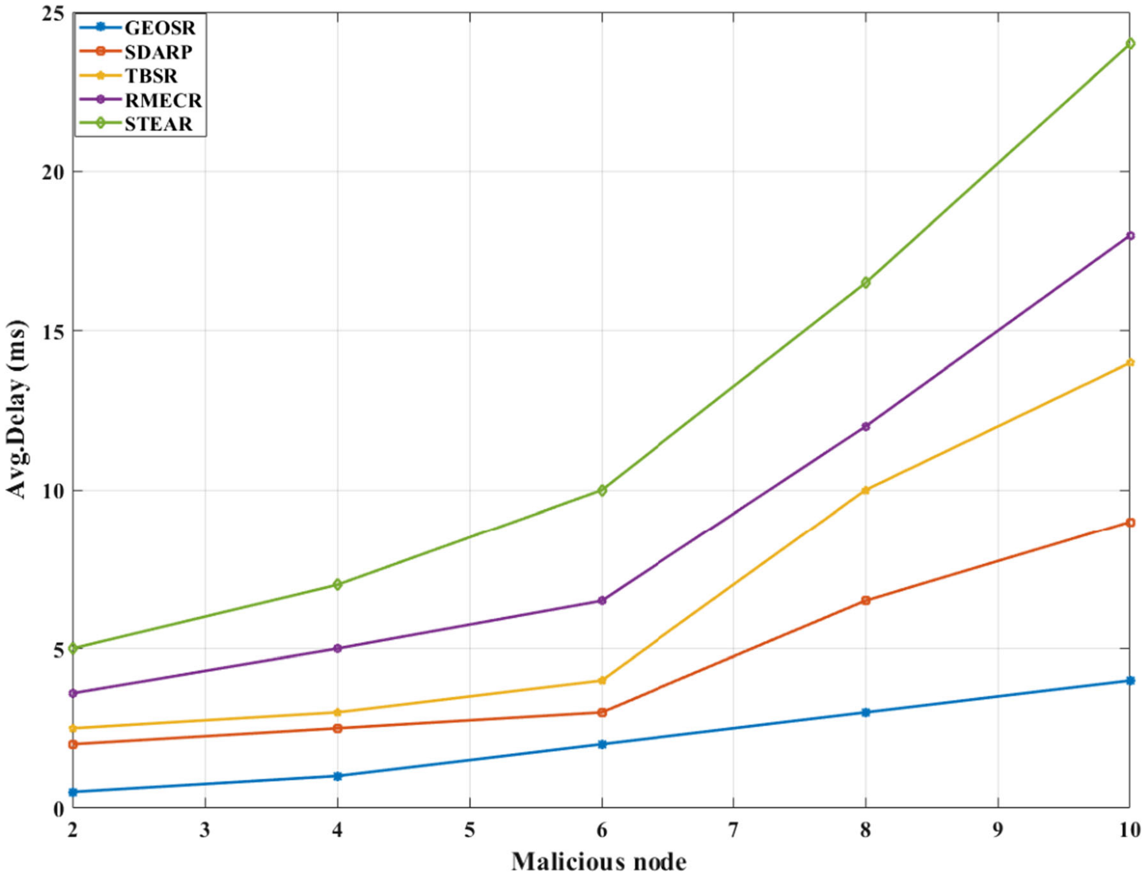


Fig. 17 Average delay detection rate

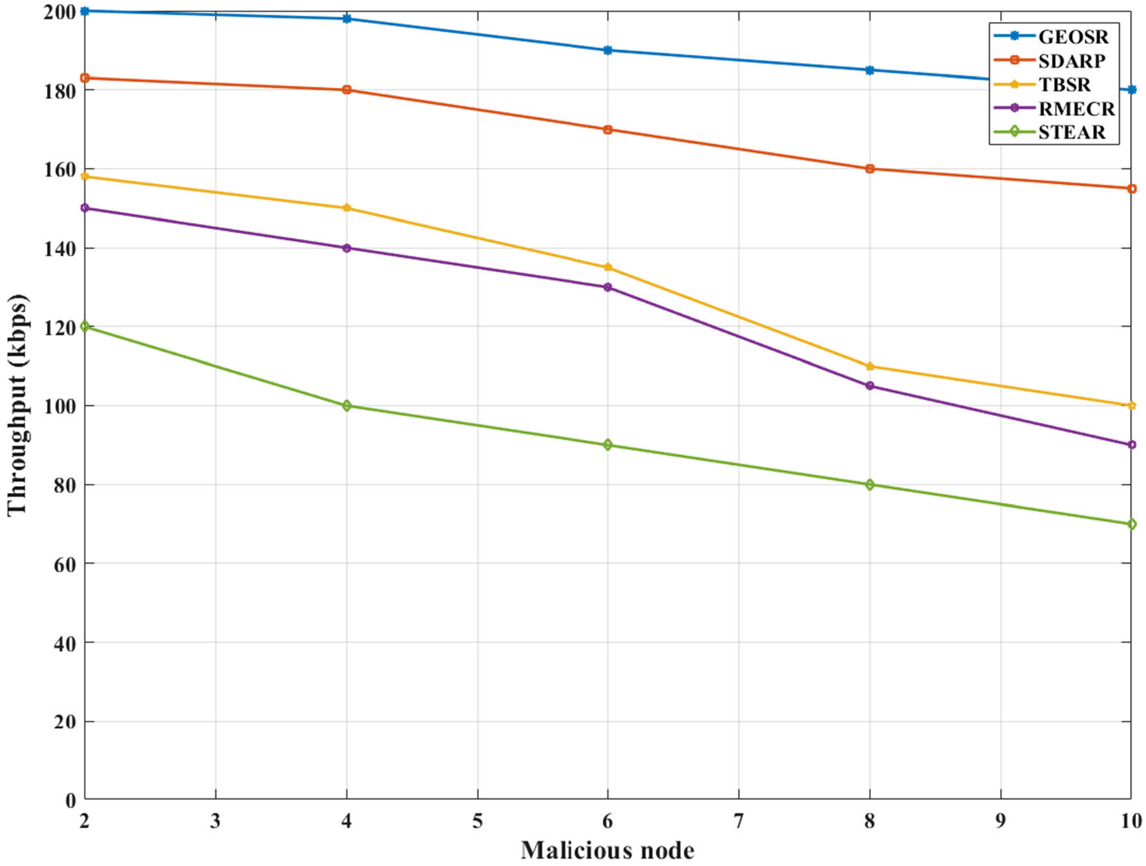


Fig. 18 Throughput analysis

overestimate each other and scores on malicious nodes were also considered.

Funding There is no funding provided to prepare the manuscript.

Data availability There is no availability of data or materials available or report for the manuscript.

Code availability No code is available for this manuscript.

Declarations

Conflict of interest There is no conflict of Interest between the authors regarding the manuscript preparation and submission.

References

1. Thiagarajan, R., Babu, M. R., & Moorthi, M. (2021). Quality of service based Ad hoc on-demand multipath distance vector routing protocol in mobile ad hoc network. *Journal of Ambient Intelligence and Humanized Computing, 12*(5), 4957–4965.
2. Hassan, M. H., Mostafa, S. A., Mahdin, H., Mustapha, A., & Ramli, A. A. (2021). Hassan MH and Jubair MA Mobile ad-hoc network routing protocols of time-critical events for search and rescue missions. *Bulletin of Electrical Engineering and Informatics, 10*(1), 192–199.
3. Tahboush, M., & Agoyi, M. (2021). A hybrid wormhole attack detection in mobile Ad-Hoc network (MANET). *IEEE Access, 9*, 11872–11883.
4. Akhter, A. F. M., Ahmed, M., Shah, A. F. M., Anwar, A., Kayes, A. S. M., & Zengin, A. (2021). A blockchain-based authentication protocol for cooperative vehicular ad hoc network. *Sensors, 21*(4), 1273.
5. Rana, K. K., Tripathi, S., & Raw, R. S. (2021). Fuzzy logic-based directional location routing in vehicular ad hoc network. *Proceedings of the National Academy of Sciences, India Section A: Physical Sciences, 91*(1), 135–146.
6. Sridevi, N., & Nagarajan, V. (2021). Efficient traffic control and lifetime maximization in mobile ad hoc network by using PSO–BAT optimization. *Wireless Networks, 27*(2), 861–870.
7. Zhang, X., Li, R., Hou, W., & Shi, J. (2021). Research on Manhattan distance based trust management in vehicular Ad hoc network. *Security and Communication Networks, 2021*.
8. Anand, M., Balaji, N., Bharathiraja, N., & Antonidoss, A. (2021). A controlled framework for reliable multicast routing protocol in mobile ad hoc network. *Materials Today: Proceedings*
9. Hanin, M. H., Amani, M., & Fakhri, Y. (2021). Improved TCP prediction congestion in mobile Ad hoc network based on cross-layer and fuzzy logic. *International Journal of Interactive Mobile Technologies, 15*(14), 125.
10. Mohammed, A., Abdullah, N. F., Alani, S., Alheety, O. S., Shaker, M. M., Saad, M. A., & Mahmood, S. N. (2021). Weighted round robin scheduling algorithms in mobile AD HOC network. In: 2021 3rd International Congress on Human-

Computer Interaction, Optimization and Robotic Applications (HORA), IEEE, 1–5.

11. Maakar, S. K., Khurana, M., Chakraborty, C., Sinwar. D., & Srivastava, D. (2021). Performance evaluation of AODV and DSR routing protocols for flying Ad hoc network using highway mobility model. *Journal of Circuits, Systems and Computers,* 2250008.
12. Reddy, M. V. K. & PremKumar, S. (2021) Predicting the malfunctioning node in mobile Ad Hoc network. *Design Engineering* 8337–8346.
13. Papadimitratos, P., & Haas, Z. J. (2006). Secure data communication in mobile ad hoc networks. *IEEE Journal on Selected Areas in Communications, 24*(2), 343–356.
14. Gong, W., You, Z., Chen, D., Zhao, X., Gu, M., & Lam, K. Y. (2010). Trust based routing for misbehavior detection in ad hoc networks. *Journal of Networks, 5*(5), 551.
15. Bertino, E. (2014). Data trustworthiness—approaches and research challenges. In: Data privacy management, autonomous spontaneous security, and security assurance, Springer, Cham, 17–25.
16. Malar, A., 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. *Journal of Ambient Intelligence and Humanized Computing, 12*(3), 4007–4017.
17. Poongodi, M., Hamdi, M., Sharma, A., Ma, M., & Singh, P. K. (2019). DDoS detection mechanism using trust-based evaluation system in VANET. *IEEE Access, 7*, 183532–183544.
18. Gunasekaran, M., & Periakaruppan, S. (2017). A hybrid protection approaches for denial of service (DoS) attacks in wireless sensor networks. *International Journal of Electronics, 104*(6), 993–1007.
19. Kim, B., & Song, J. (2019). Energy-efficient and secure mobile node reauthentication scheme for mobile wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking, 2019*(1), 1–16.
20. Jhaveri, R. H., & Patel, N. M. (2017). Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. *International Journal of Communication Systems, 30*(7), e3148.
21. Jhaveri, R. H. & Patel, N. M. (2016). Evaluating energy efficiency of secure routing schemes for mobile Ad-Hoc networks. *International Journal of Next-Generation Computing*, *7*(2).
22. Salam, A., Javaid, Q., & Ahmad, M. (2020). Bioinspired mobility-aware clustering optimization in flying ad hoc sensor network for internet of things: BIMAC-FASNET. *Complexity*.
23. Kumar, K. V., Jayasankar, T., Eswaramoorthy, V., & Nivedhitha, V. (2020). SDARP: Security based data aware routing protocol for ad hoc sensor networks. *International Journal of Intelligent Networks, 1*, 36–42.
24. Sajan, R. I., & Jasper, J. (2020). Trust-based secure routing and the prevention of vampire attack in wireless ad hoc sensor network. *International Journal of Communication Systems, 33*(8), e4341.
25. Ahmed, A., Kamalrulnizam, A. B., Muhammad, I. C., Khalid, H., & Abdul, W. K. (2015). TERP: a trust and energy aware routing protocol for wireless sensor network. *IEEE Sensors Journal, 15*(12), 6962–6972.
26. Haseeb, K., Naveed, I., Ahmad, A., Ikram, U. D., Almajed, H. N., & Nadra, G. (2019). Secret sharing-based energy-aware and multi-hop routing protocol for IoT based WSNs. *IEEE Access, 7*, 79980–79988.
27. Selvi, M., Thangaramya, K., Sannasi, G., Kanagasabai, K., Khannah Nehemiah, H., & Arputharaj, K. (2019). An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks.". *Wireless Personal Communications, 105*(4), 1475–1490.
28. Zahedi, A., & Parma, F. (2019). An energy-aware trust-based routing algorithm using gravitational search approach in wireless sensor networks. *Peer-to-Peer Networking and Applications, 12*(1), 167–176.
29. Kavidha, V., & Ananthakumaran, S. (2019). Novel energy-efficient secure routing protocol for wireless sensor networks with Mobile sink. *Peer-to-Peer Networking and Applications, 12*(4), 881–892.
30. Vinitha, A. & Rukmini, M. S. S. (2019). Secure and energy aware multi-hop routing protocol in WSN using Taylor-based hybrid optimization algorithm. *Journal of King Saud University-Computer and Information Sciences.*

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Ranjit Kumar Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, Jharkhand, Pin-826004, India.

Sachin Tripathi Department of Computer Science and Engineering, Indian Institute of Technology (Indian School of Mines), Dhanbad, Jharkhand, Pin-826004, India. Research Interests: Group Security, Ad-Hoc And Sensor Network, Artificial Intelligence

Rajeev Agrawal G.L. Bajaj Institute of Technology and Management, Greater Noida, Pin-201306, India. Research Interests: wireless communication, ultrasound medical Imaging, remote patient monitoring.