Int. j. inf. tecnol. (March 2022) 14(2):915–929
https://doi.org/10.1007/s41870-019-00392-w

ORIGINAL RESEARCH

T-SEA: trust based secure and energy aware routing protocol for mobile ad hoc networks

Deepika Kukreja[1] · Deepak Kumar Sharma[1]

Received: 19 January 2019 / Accepted: 7 November 2019 / Published online: 18 November 2019

Abstract A trust based secure and energy aware (T-SEA) routing protocol for detection and isolation of black/gray hole nodes in mobile ad hoc networks (MANETs) is proposed in this paper. Energy aware characteristic is a vital requirement for prolonging MANET lifespan. Intrusion detection systems (IDSs) are used to monitor and catch black/gray hole nodes. Nodes having sufficient energy, high value of trust and maximum connections are selected as IDS capable nodes. T-SEA first detects suspicious nodes during data transfer phase without requiring any node to activate in sniff mode. Only few nodes (IDS nodes) out of IDS capable nodes function in sniff manner for monitoring during data transmission phase. During monitoring, IDS nodes detect a node as malicious based on nodes' current behavior, current trust and behavior recorded during previous transmissions. The detection technique is energy aware since IDS executes only on few nodes at a time subsequent to the discovery of attack. This paper employs NS-2 to validate the proposed protocol.

Keywords Mobile ad hoc networks · Intrusion detection system · Energy aware · Black hole attack · Gray hole attack · Security · Trust · Dynamic source routing protocol

✉ Deepak Kumar Sharma
dk.sharma1982@yahoo.com

Deepika Kukreja
deepikakukreja18@gmail.com

[1] Division of Information Technology, Netaji Subhas University of Technology (Formerly Netaji Subhas Institute of Technology), New Delhi, India

1 Introduction

MANETs deal with a range of confronts due to resource constraints, non-centralized management, dynamic network topology, wireless associations between the nodes, lack of security infrastructure and battery operated nodes. Due to inherent vulnerabilities of MANET, security is the paramount requirement for protected communication among network nodes. Unlike wired networks, MANETs are infrastructure less networks where nodes themselves carry out fundamental network operations as a router as well as packet forwarders. This sets new confronts for the required security architecture they apply.

Nodes in a mobile ad hoc environment are mostly operated using battery. Energy aware routing is inevitable in these kinds of networks because battery power associated with mobile nodes may trench out while doing various network operations. For a mobile node to do well in performing other routing tasks, it should have sufficient energy. Nodes that are deficient in energy may cause recurrent path failures. Which usually happens because of broken links that occur in network. Routing protocols which are energy conscious prevent the reoccurring of link breakages. Therefore, they reduce the usage of nodes' energy and henceforth increase the network lifetime and consequently, the performance.

Therefore, security and energy are two key problems that need to address while designing a routing protocol. T-SEA routing protocol is intended as energy aware and secure that maintains the connectivity in the network besides secures the communication among the different network nodes.

The proposed T-SEA protocol aims to give solution to two types of attacks, namely: black hole and its variant gray hole attack. Black hole attack is the one where if a path route between source and destination pair has been created, a malevolent node that lie in that path drops the messages carrying data that are directed for this node and which it is required for forwarding in data transfer phase.

Black hole attack has a variant named as gray hole attack. A gray hole node tends to drop captured messages with some likelihood. Gray hole attack is not easy to identify as a malicious node may show its malevolent conduct in dissimilar ways. It may not forward packets coming from some particular nodes during routing though forward the messages coming from some other nodes. It may show malevolent conduct for some time period but may change to show benevolent conduct after some time. A malevolent node may show a mixed behavior; as a consequence, finding becomes even harder. In some cases, nodes may not have sufficient energy or they may be overloaded; instead, nodes may have become self-centred, for example to save energy, they may not forward packets on behalf of others.

In MANETs, wireless link transmission errors, mobility, and congestion are main reasons for packet dropping. Packet dropping caused by transmission errors is because of the physical condition of the wireless channel, the environment where networks are set up, etc. They cannot be eradicated by improving the routing protocols. A network becomes congested whenever the usage go beyond the utmost capacity of a communication link. Congestion in a network increases with the growth of communication requests. That is, more the number of pairs for data communication, more will be the network congestion. Packet dropping due to mobility can occur in many ways. A packet may be dropped whenever a path to a specific destination does not exist or the buffer used for storing awaiting packets becomes full. Packet dropping may also happen when the link between any node lying in the route with the its following hop breaks [33]. For the above mentioned causes of packet dropping, T-SEA uses an accepted level of data dropping percentage, $\delta_{threshold}$. It represents the percentage amount of data losses that occur because of unavoidable network problems.

T-SEA protocol is proposed to secure the data transfer phase of Dynamic Source Routing (DSR) protocol [14] in an energy efficient way. The proposed T-SEA protocol identifies and isolates the nodes that induce black hole and gray hole attacks in the network. The network nodes having sufficient amount of energy, high value of trust and that cover up the entire network (nodes connected to high number of nodes) are chosen as IDS capable nodes. The protocol first detects the suspicious nodes which may be responsible for significant data loss during the transmission without requiring any node to operate in sniff mode. In sniff mode, nodes listen to all transmissions within their communication range; they hence consume substantial nodes' energy. A small number of nodes termed as active IDS nodes are selected from the IDS capable nodes based on the vicinity of the IDS nodes to the suspicious nodes. The selected active IDS nodes operate in sniff mode to monitor the behavior of suspicious nodes during data transmission phase. During monitoring, the active IDS nodes detect a node as malicious (gray hole or black hole) based on nodes' current forwarding behavior, current trust value and behavior recorded during previous data transmission cycle. The gray/black hole nodes' detection technique is energy aware since IDS executes only on few nodes at a time and that too after the identification of the attack. The proposed T-SEA protocol identifies and isolates the malicious nodes, without false positives, if suitable threshold values are set.

In T-SEA, source node and destination node maintain tables named as *source_path* table and *destination_path* table respectively. After sending every packet, source node makes an entry of path through which data packet is sent in the *source_path* table. Similarly, on receiving a packet, destination node makes an entry of path through which data packet is received in *destination_path* table. After every fixed period of time called *detect_suspect* interval, source node transmits *source_path* table to destination node. Destination node compares *destination_path* table with the received *source_path* table and identifies non trustworthy paths. Non trustworthy paths are the paths through which percentage of data dropping during transmission is above an acceptable data dropping threshold percentage, $\delta_{threshold}$. Destination node then spot out suspicious nodes lying in these non trustworthy paths. The identified suspicious nodes are placed into a list known as suspicious list (discuss later in section 3) for second phase of detection by the IDS nodes. Destination node sends the list to source node. Source node then sends message to IDS nodes to monitor the suspicious nodes. Active IDS nodes operate in sniff mode and start monitoring the suspicious nodes only if any suspicious node belongs in the route during data transmission. In T-SEA protocol, only active IDS nodes that are in vicinity of suspicious nodes are required to operate in sniff mode, resulting in the reduction of network operating cost. Active IDS nodes update trust values of the suspicious nodes in accordance with their behavior.

The outline of the paper is organized as follows. In Sect. 2, the related work and the limitations of existing secure and energy aware routing protocols in MANETs is given. Section 3 covers the methodology and implementation of the proposed method. In Sect. 4, we present the extensive experimental results and their analysis. Finally, the conclusions are drawn in Sect. 5.

2 Related Work

The related work is divided into three sections. In the first section, works related to secure routing protocols in MANETs is presented. In Sect. 2.2, works related to energy aware routing protocols is given, Sect. 2.3 presents energy aware secure routing protocols. Trust based secure routing protocols are presented in Sect. 2.4. Section 2.5 discusses the routing protocols that are trust based, energy aware and secure as well.

2.1 Secure Routing Protocols

Gonzalez et al. [11] employed the principle of flow conservations for detection of nodes which show packet forwarding misconduct. Yang et al. [31] used cryptography methods that raise complexity due to computations. In Marti et al. [17], authors were unsuccessful in detecting malicious conduct in occurrence of partial dropping, receiver collisions, false misbehaviour, ambiguous collisions and limited transmission power. Banergee [4] also introduced a scheme to discover and eliminate black hole and gray hole attacks. In this method, data packets are transmitted as data blocks that increase the routing delay in the case when gray hole node is there in the route. Su [26] used IDS to detect the nodes that onward Route Reply (RREP) packets but they do not forward Route Request (RREQ) packets. This method proves appropriate for the detection of black hole attack but not suitable for detecting gray holes as the gray holes take part properly in route finding stage.

2.2 Energy aware routing protocols

EN-AODV protocol was proposed in Sridhar et al. [25]. Energy levels of network nodes are calculated in the proposed work and then energy of network nodes is compared with a predefined threshold of energy. If the node's energy is greater than the threshold energy than the node is allowed to take part in routing process. This protocol hence determines the nodes which have sufficient energy for transmitting the data. Henceforth, the protocol does not choose nodes that could trench out energy in data transfer. It shows remarkable results in the terms of various parameters, for example, end to end delay and packet delivery ratio (PDR). This protocol does not takes care about the security in transmission of data and that is the most basic demand for MANETs.

Few energy-aware routing protocols are also proposed in literature surveys [29, 32]. A relative study of some energy-aware routing protocols is made in Cano and Kim [6]. Li et al. [15] gave a survey of power-aware protocols. Sheu et al. [24] used global synchronization coordinates beacon intervals among the devices to save energy. None of the aforesaid energy-aware routing protocols consider security feature of MANETs.

2.3 Energy aware secure routing protocols

The work in Mohanapriya and Krishnamurthi [18] also used IDS system for the identification of gray hole attack. Data packets are send out in the arrangement of blocks. Sending of more than one data blocks is required to identify and take apart the gray hole nodes, this delays the identification and elimination procedure. The method also fails to discover all malevolent nodes in a dynamic network. The method is not fully secure as the route used for sending the information about the count of data packets per block may also contain gray nodes. The protocol also fails when neighbor nodes collude.

A routing protocol presented in Jain and Sharma [13] (so-called as EESM-AODV). This protocol made changes in AODV routing protocol and is projected for multi-path routing. For energy competent, the protocol practices adaptive methods. Jain and Sharma related the outcomes of the anticipated protocol with the outcomes of AODV in attack situations.

Work in Asadi et al. [3] proposes a protocol for securing the network in an energy resourceful way. If any node receives message from some other network node, in order to preserve the energy, the node employs the proposed protocol to decide whether to forward the received packet or not.This convention exploits game theory method for governing most finest likely prearrangement that extend nodes' energy life. By means of game theory technique, each node onwards the suitable count of the messages. This protocol forces every network node to cooperate with each other and penalize the nodes if they do not cooperate.

Ahila and Chitra [1] proposed a protocol so-called as PPSEER protocol. This protocol assures to increase the confidentiality of messages though sustaining power efficiency of the nodes. This protocol initially categorizes network nodes into two types: one type is super node and the other is normal node. Messages are transmitted grounded on energy control. This method makes the routing secure thru applying encryption methods. Dhurandher et al. [7] introduced a new method that has power consciousness form of the SCAN [31] for detection of attacks that are made at the network layer. Work presented a reviewed credit strategy for reintroducing the tokens. The method has been applied by multiplicative increase in the life of the token whenever node renews. Route that is most high in quality factor is selected as routing path.

The work in Biswas et al. [5] proposes a protocol which gives solution for the discovery as well as the avoidance of black hole attack. This explanation makes sure that data is sent securely between the two nodes while sustaining the resource consumption. This protocol discovers a reliable and secure path for routing which functions properly in the network that has black holes and has changing network topology. In this method, each node contains information like: rank, node stability and residual battery energy. A node is discovered to be black hole, if the rank of this node is 0. In Heena and Kumar [12], authors introduced a protocol for an ad hoc network that made changes in RREP packet. RREP packet modified by the authors contained the information such as: packet type, destination address, source address, nodes remaining battery life, node count and token of node. By means of this form of Route Reply packet, the protocol finds shortest route having only trustworthy nodes in the route that is formed between the given source and destination pair.

Authors of Ghander and Shaaban [9] proposed one another energy conscious routing protocol namely Power Aware Cooperation Enforcement (PACE) distributed mechanism. This protocol identifies and prevents the nodes that induce routing misbehaviour. The protocol put in force the corporation among malicious nodes and other network nodes. Thus prolongs the network lifetime. This method discovers the malevolent nodes that take part during the route discovery procedure but later they do not want to forward data packets. In data transmission stage, PACE mechanism identifies the malevolent nodes by means of saving a message copy in the cache afterwards sending the packet and there after it monitors neighbours of that node for some time period. Observing nodes evaluate the grades of the neighbouring nodes. When any neighbour node has grading which is less than a pre-specified defective threshold value, at that time this node is put into a list named as faulty nodes list. The list is then advertised and applies to each Route Request message. Hence, malevolent nodes are thus prevented in the route. This scheme compensates the power loss in observing and sniffing by the selection of only consistent nodes that have high remaining power in the ultimate route. Authors have applied the PACE method by participating it with standard DSR routing protocol and AODV then named them as PACE-DSR & PACE-AODV.

2.4 Trust based secure routing protocols

Tan et al. [28] also introduced a trust grounded secure routing convention for MANETs. In this, a routing scheme based on trust is utilized to avert attacks that compromise security of MANETs. The scheme uses Optimized Link State Routing (OSLR) as basic protocol. Work implements fuzzy Petri net for the trust model. Fuzzy Petri net method has been applied to compute trust of different nodes. Trust levels of various routes between source and destination are then calculated. This way, the method prevents the malevolent nodes to come in the ultimate route selected to transmit data. This is implemented by opting a route having maximum route trust amongst all the other likely routes. Trusts' levels of the nodes are calculated grounded upon the presentation parameters in the data plane and the routing plane both.

2.5 Trust based and energy aware secure routing protocols

Ahmed et al. [2] proposed a trust as well as energy aware routing protocol (TERP). It uses a distributed trust scheme for the discovery as well as segregation of malicious nodes. This proposed model detects the network nodes as malicious which do not forward messages in an ad hoc network. The work applies non cryptographic technique and the protocol operates in four stages named as: trust database, trust approximation, route arrangement and route maintenance. Work proposed in Subramaniam and Ramachandran [27] introduces one another version of AODV routing protocol based on trust. Trust levels and energy levels of nodes that are the part of route are computed first. The network nodes having residual power as well as trust levels above a pre-specified threshold value have been then permitted to partake in the routing procedure. This way, the scheme segregates the mischievous nodes which prompt packet dropping induced by coming in the route.

Estahbanati et al. [8] proposed one another routing protocol based on trust as well as energy. The scheme implements Hidden Markov Model (HMM) for computing nodes' trusts. This routing protocol uses metric to select the best path for data transmission as well as Markov chain trust that is grounded on the leftover energy and the calculated value of trust of nodes. Gong et al. [10] proposed

ETARP. This work's objective is to lessen nodes' energy usage while transmitting messages. Protocol uses utility theory approach for reducing the consumption of nodes' energy. The work considers trustworthiness as well as power of different network nodes. It also uses Bayesian network to estimate nodes' trustworthiness.

Woungang et al. [30] proposed an E-TBM routing procedure for introducing security in an ad hoc network. Protocol is modified version of DSR protocol. Proposed methods give solutions to secure data transmission. The solutions are built on the trust as well as the multi-path routing technique. Proposed method implements 3 chief steps: assignment of trust, encryption using soft-encryption technique and DSR based multipath routing procedure.

Sarkar and Datta [21] proposed PEER procedure for routing. This protocol also has been built on trust as well as exploits ratio of energy usage for determining power factor of different nodes. Power factor is defined as nodes' remaining energy divided by node's initial energy. A node participates in data transmission process grounded on determined energy factor value. This protocol is further extended as SEES [22] protocol. This new method is used for transmission of data packets by means of multiple routes. Authors modelled routing method in MANETs using stochastic routing that is based upon Markov chain. Quantity of nodes' energy used during message transmission is applied as an operation in Markov chain model that further uses Bellman's Principle of Optimality equation. This work is more expanded in Sarkar and Datta [23]. Sarkar and Datta [23] proposes a secure as well as power efficient stochastic multiple routes routing procedure. This procedure is also dependent upon Markov chain model. The protocol discovers the various manifold paths between source and destination. The method thereafter chooses best energy efficient route stochastically amongst all the other routes to forward data packets. This protocol makes the data transmission phase secure because messages are being transferred that uses arbitrary routes from source node to destination node. Hence, it becomes difficult to capture, jam or hijack information as the attacking node now is not able to snoop all routes from source node to destination node. The scheme uses power used in packet forwarding as the cost which is considered as the value function for Markov chain model for the determination of optimal route selection strategy.

Work proposed in Su [26], Gonzalez et al. [11], Yang et al. [31], Marti et al. [17], Banergee [4] and Ghander and Shaaban [9] involve every network node to persistently watch their adjoining nodes which necessitates all nodes to work in sniff mode at all times. This diminishes life span of nodes and consequently that of the network. Su [26] and Mohanapriya and Krishnamurthi [18] do not talk about the selection and position of IDS.

The majority of ad hoc routing procedures that practices Intrusion Detection Systems, an IDS is installed on each node of the network and runs for the whole life. They listen to all the communications within their vicinity; hence draining significant nodes' battery. The watchdog technique installed on different IDS nodes is an effective as well as fruitful method in MANETs. Massive volume of energy is used in these protocols which makes these protocols to fight against energy effective design requirement of MANETs. Most of the protocols presented in the related work do not show the setting up of IDS. To our best information there do not exist security solutions for MANETs that are suitable to preserve energy even though keeping data transmission phase secure together. Therefore, a smart as well as an energy aware secure routing protocol is extremely in demand. T-SEA aims to lessen the energy requirement acquired by IDS to the best possible though upholding an adequately needed security limit. For achieving this desired objective, T-SEA improves IDS method in following two phases. The first phase selects the IDS on the nodes where there locations are optimized and the second phase optimizes the quantity of IDS nodes required. Optimizing the quantity of IDS nodes reduce redundancy of nodes that run IDS.

3 Proposed model

3.1 Model assumptions

The proposed protocol T-SEA has following assumptions:

1. Bidirectional communication links exist between the nodes.
2. All network nodes have wireless interfaces to support sniff mode.
3. The initial set of IDS nodes are not malicious.

3.2 Working model

The proposed protocol uses the Route discovery procedure as in dynamic source routing protocol. DSR protocol is one of the reactive routing procedures that consists of two stages. These two stages of the protocol function hand in hand for finding the route between the given source-destination pair and maintaining these source routes discovered. During the first stage known as route discovery stage, route is created by flooding the Route Request packets in the entire network. When the destination node receives a Route Request packet, it sends a respond using Route Reply packet to node which has generated RREQ packet. Route Reply packet contains the route used by Route Reply packet to reach the destination. Any intermediate node may also contain route to that particular destination in its cache. If such nodes receive a RREQ message, then that node sends respond to the sender node through Route Reply packet containing the complete source route [19]. During route maintenance stage, if any node that belongs to the discovered route breaks the link, in order to inform the source node, the node adjacent to that node generates and sends Route Error (RERR) packet. On receiving RERR packet, the source node checks its cache, if no other route exists then it again initiates the route finding process.

DSR is used to establish route between source node and destination node. Source node stores discovered routes in the cache and carries out procedure to select IDS capable nodes which is explained in the following section. Section 3.2.2 enlightens on the data transfer stage of T-SEA protocol. Section 3.2.3 enlightens on the calculation of trust values of suspicious nodes. Algorithm that shows the working of T-SEA protocol is given in Sect. 3.2.4.

3.2.1 Selection of IDS capable nodes

IDS capable nodes are chosen in a manner that they have adequate energy to execute IDS, they should not belong in list of malicious nodes, have high trust value, provide full coverage to the network and are completely connected with each other. T-SEA extends the approach given in Li et al. [16] to select the IDS capable nodes with two added criteria of selection: the selected node should have plentiful energy and it should not be there in the list that contains malicious nodes. It makes sures the full coverage of the network as all IDS capable nodes are in connection with each other and network node that is not IDS capable node connect to minimum one IDS capable node. To reduce energy consumption, only some nodes from IDS capable nodes are needed to function in sniff mode, run IDS to monitor the suspicious nodes, compute their trust value and catch gray hole and black hole nodes.

3.2.2 Data transmission phase

When source node transmits messages containing data to the destination node, source node is required to select a path from its cache as done using DSR protocol. During data transmission, different data packets may have different routes between source node to destination node due to changing network topology. Source node upholds the following information: (1) prime suspicious list having nodes suspected by destination node, (2) malicious list and (3) *source_path* table. Malicious list have the nodes that are detected malevolent by IDS nodes. The *source_path* table consists of two fields: (1) paths traversed by data packets & (2) number of the messages in the form of packets transmitted using the mentioned routes. One another table called *destination_path* table is upheld by the destination node having two fields: (1) paths through which destination node has received data packets and (2) number of the data packets received through these paths. A sample format of *source_path* table and *destination_path* table after *detect_suspect* interval are shown in Tables 1 and 2 respectively. Here source node is A and F is the destination.

Table 1 *source_path* table upheld by source node

Path no.	Path	Packets
1	A->B->C->D->F	40
2	A->C->H->I->E->F	20
3	A->C->D->E->K->F	30
4	A->C->I->D->E->F	60
5	A->D->I->K->J->F	30
6	A->B->C->K->L->F	20
Total count of packets sent out		200

Table 2 *destination_path* table upheld by destination node

Path no.	Path	Packets
1	A->B->C->D->F	36
2	A->C->H->I->E->F	18
3	A->C->D->E->K->F	27
4	A->C->I->D->E->F	12
5	A->D->I->K->J->F	19
6	A->B->C->K->L->F	18
Total count of packets received in		130

After every *detect_suspect* interval, source sends *source_path* table to destination using the path formed of connecting IDS capable nodes. This path created using IDS capable nodes is utmost consistent path. Destination node utilizes received *source_path* table to determine percentage of data drop out of total data packets transmitted between source and destination nodes using Eq. (1).

$$drop\_total = \frac{PTotal_{src} - PTotal_{dest}}{PTotal_{src}} * 100 \quad (1)$$

Where *drop_total* is the percentage of total data packets drop, $PTotal_{src}$ is the total packets that source node has sent and $PTotal_{dest}$ is the total packets received at the destination node. Destination node gets the values of $PTotal_{src}$ and $PTotal_{dest}$ from the received *source_path* table and *destination_path* table respectively.

If the percentage of total data packets drop, *drop_total* is below the acceptable data dropping threshold percentage, $\delta_{threshold}$, then malicious node detection process is not needed to execute as packet dropping is within the acceptable range and hence, no IDS capable node is then required to function in sniff mode. If *drop_total* is above the $\delta_{threshold}$, destination node matches the records in *destination_path* table to corresponding records in the *source_path* table. Destination node evaluates the percentage of data packets drop in each path mentioned in the *source_path* table using Eq. (2).

$$drop\_path(i) = \frac{P(i)_{src} - P(i)_{dest}}{P(i)_{src}} * 100 \quad (2)$$

where $drop\_path(i)$ is the percentage of the data packets drop using path i, $P(i)_{src}$ is the count of packets sent through source node using path i and $P(i)_{dest}$ is the count of packets that are received at the destination node using path i.

If the percentage of data drop in path *i*, $drop\_path(i)$ is below the acceptable data dropping threshold percentage, $\delta_{threshold}$, then path *i* is marked as trustworthy path. Otherwise, path *i* is discovered as a non-trustworthy path. Destination node evaluates trustworthy index of all the nodes that come in non-trustworthy paths using Eq. (3). Trustworthy index represents dependability of a node. Trustworthy index of any node A is evaluated as:

$$T(A) = \sum_{i=1}^{i=t} \frac{N_i/I_i}{N} - \gamma \sum_{j=1}^{j=nt} \frac{D_j/I_j}{N} \quad (3)$$

Here *t* represents count of trustworthy paths that have node A, *nt* is count of non-trustworthy paths containing node A, N_i is the count of data packets that follow trustworthy path *i* within *detect_suspect* interval, D_j denotes count of data messages dropped in transit through non-trustworthy path *j* within *detect_suspect* interval, I_j and I_i represent the count of in-between nodes in non-trustworthy path *j* and trustworthy path *i* respectively, here *N* is the sum of data packets sent in *detect_suspect* interval and γ is an invariable. Less is the value of γ, it is more probable that T-SEA discovers any malevolent activity and for high value of γ, additional IDS nodes will be needed to operate in sniff mode as more nodes will be detected as suspicious. This incurs high energy disbursement. Appropriate value of γ is needed to increase the possibility of discovering true malicious nodes while keeping the energy consumption low.

In Eq. 3, trustworthy index of any node A, T(A) falls in the range $-\gamma$ to 1. Node that has T(A) = 1 is most trustworthy. A trustworthy index threshold, $\alpha_{threshold}$, is chosen whose value lies in between $-\gamma$ to 1. Nodes having trustworthy index less than $\alpha_{threshold}$ are suspected to be non trustworthy nodes. Destination node creates a suspicious list and adds the nodes (having trustworthy index less than $\alpha_{threshold}$) along with their corresponding trustworthy indexes to this list. The destination node then transmits this suspicious list to source through the highly trustworthy path (having drop_path(i) $<\delta_{threshold}$) in its path table whenever it exists. If it does not exist, then it utilizes the path created by connecting IDS capable nodes. Source node when receives the suspicious list, it adds the nodes included in this list to the prime suspicious list. For our simulation we chose the values of γ as 2 and $\alpha_{threshold}$ as 0, which signifies that a trustworthy node sends more than twice the messages not forwarded by it.

For example, using Tables 1 and 2, if $\delta_{threshold}$ is chosen as 20%, *drop_total* comes out to be 35% which is above the $\delta_{threshold}$. Destination node computes $drop\_path(1)$, $drop\_path(2)$, $drop\_path(3)$, $drop\_path(4)$, $drop\_path(5)$ and $drop\_path(6)$ as 10%, 10%, 10%, 80%, 36.66% and 10% respectively. Therefore, path numbers 1, 2, 3 and 6 are discovered as trustworthy paths. Path numbers 4 and 5 are identified as non-trustworthy paths. Destination node computes trustworthy indexes of nodes belonging to path numbers 4 and 5. For this example, the value of trustworthy index threshold is chosen as 0. Trustworthy indexes of nodes C, I, D, E, K and J (nodes of non-trustworthy paths) are $0.01875, -0.125, -0.05375, -0.06375, 0.02875$ and -0.0275 respectively. Destination node F puts the nodes I, D, E and J (having T(A) < 0) along with their trustworthy index values into the suspicious list and transmits the list to the source node.

When source node chooses a path for transmitting data packets, it matches all nodes of the selected path with the prime suspicious list and the malicious list. It takes step as per the following situations:

1. When selected path have one or more nodes that belong to the prime suspicious list then active IDS nodes lying in the vicinity of the suspected nodes are

switched to operate in sniff mode. Data packets are transmitted between the source and the destination nodes. Active IDS nodes compute the trust (explained in the next section) of the suspected nodes. If trust of any suspected node results in a value which is less than minimum required trust threshold, *trust_threshold*, the IDS node shares the node id and its trust with the source node. Source node deletes the record of this node from prime suspicious list & adds the record in malicious list. It also floods information about this malicious node in the network so that other network nodes avoid this node.

2. Source node removes a path from its cache, if any node in the selected path occurs in the malicious list. Source node selects a new path again.
3. If path does not have any suspicious or malicious node, data packets are transmitted from the source to the destination nodes. In this case, no IDS node is required to operate in sniff mode.

3.2.3 Trust calculation

Each network node is initialized with a trust value. When the path selected by source node for data transmission contains suspicious nodes, source node triggers the monitoring procedure on active IDS nodes. During monitoring, an active IDS node increments or decrements the trust of its nearby suspicious node according to its conduct. If a node drops a packet, the trust value of that node is decremented and if a node forwards a packet; the trust value of that node is incremented. Since a node may have more than one active IDS node in its vicinity, only one trust update must be done on one node's activity.

Active IDS node updates the trust value of suspicious node in accordance with the current forwarding behavior, the trustworthy index of the node and its current trust value. If suspicious node shows dropping misconduct during traffic monitoring, on every packet drop the trust value of the node is decremented by an amount evaluated as:

$$dec\_amt(A) = \frac{|T(A)|}{C_{trust(A)} * 10^{-1}} \tag{4}$$

where $dec\_amt(A)$ is the factor by which trust value of the node A under monitoring is reduced, $C_{trust(A)}$ is the current trust value of node A and $T(A)$ is the trustworthy index of node A evaluated using Eq. (3). The new current trust value of the node A is then determined as:

$$C_{trust(A)} = C_{trust(A)} - dec\_amt(A) \tag{5}$$

If suspicious node shows benevolent conduct during traffic monitoring, on every packet forwarding the trust value of the node is incremented by an amount evaluated as:

$$inc\_amt(A) = \frac{C_{trust(A)}}{|T(A)| * 10^{2}} \tag{6}$$

where $inc\_amt(A)$ is the amount by which trust value of the node A under monitoring is increased. The new current trust value of the node A is then evaluated as:

$$C_{trust(A)} = C_{trust(A)} + inc\_amt(A) \tag{7}$$

In T-SEA, active IDS nodes identify gray hole and black hole nodes and ensure that only one active IDS node updates the trust of a specific suspicious node. As multiple active IDS nodes may overhear the packets forwarded by any node during monitoring, the T-SEA protocol uses sequence number of packets as the parameter to differentiate between the packets and preceding node of the packet to know the forwarding nodes. Using these parameters, if trust level of a node is lessened for a sequence number by an active IDS node, no other active IDS nodes can decrement the trust level for the packet having same sequence number. Similarly, these parameters are also checked when the trust levels of the nodes are increased.

3.2.4 T-SEA protocol algorithm

Algorithm 1 shows the working of the proposed protocol.

```
 1: if (the node is source node) then
 2:   if (If it wants to transmit packets) then
 3:     Set c = source node's clock time
 4:     Run route discovery process
 5:     Choose IDS nodes
 6:     Source node chooses a path to destination node from the cache
 7:     if (no path exists in the cache) then
 8:       Go to step 4
 9:     end if
10:     if (path has nodes that belong to list of malicious nodes) then
11:       eliminate path from the cache
12:       Go to step 6
13:     end if
14:     if (path has nodes that belong to prime suspicious list) then
15:       IDS nodes in vicinity of suspicious nodes are turn to work in sniff mode
16:     end if
17:     if ((present source node's clock time - c) mod detect_suspect interval == 0) then
18:       Send source_path table
19:     end if
20:     Send data
21:     Enter this path in the source_path table
22:     go to step 6
23:   end if
24:   if (node has received suspicious list OR malicious list) then
25:     if (received suspicious list) then
26:       Update prime suspicious list
27:     end if
28:     if (received malicious information) then
29:       Update malicious, prime suspicious lists and floods this information in the network
30:     end if
31:     if (node has no more data to send) then
32:       do nothing
33:     else
34:       go to step 6
35:     end if
36:   end if
37:   if  (received RERR) then
38:     go to step 6
39:   end if
40: end if
41: if (it is an intermediate node) then
42:   relay all packets to next neighbour
43:   if (link break is detected) then
44:     Generate RERR and send it to source node
45:   end if
46: end if
47: if (IDS capable node) then
48:   if (sniff mode == ON) then
49:     Observe forwarding behavior of its neighbor nodes
50:     if (node shows malevolent forwarding behavior) then
51:       Update trust value of the neighbor node using equations (4) and (5)
52:     else
53:       if (node shows benevolent forwarding behavior) then
54:         Update trust value of the neighbor node using equations (6) and (7)
55:       else
56:         Do nothing
57:       end if
58:     end if
59:     if (trust < trust_threshold) then
```

```
60:          Generate a packet that contains malicious information and send this to source node
61:          Set own sniff mode == OFF
62:       end if
63:    end if
64: end if
65: if (Destination node) then
66:    if (received data packet) then
67:       Enter the path in the destination_path table
68:    end if
69:    if (received source_path table) then
70:       Determine drop_total using equation (1)
71:       if (drop_total > $\delta_{threshold}$) then
72:          i = 1
73:          for i < number of paths in source_path table do
74:             Compute drop_path(i) using equation (2)
75:             if (drop_path(i) > $\delta_{threshold}$)) then
76:                Mark path i as non-trustworthy path
77:             else
78:                Mark path i as trustworthy path
79:             end if
80:             i++
81:          end for
82:          Select a node A s.t. A $\in$ non trustworthy path and A $\notin$ suspicious list
83:          Determine trustworthy index T(A) of node A using equation (3)
84:          if (T(A) < $\alpha_{threshold}$) then
85:             Add node A and T(A) to suspicious list
86:             if (T(A) of all nodes belonging to non trustworthy paths has been computed) then
87:                Send suspicious list to source node
88:             else
89:                Go to step 82
90:             end if
91:          end if
92:       end if
93:    end if
94: end if
```

4 Experimental results and analysis

4.1 Setup

Network Simulator NS-2.34 [20] is used to assess the competence of T-SEA protocol. The simulated results of the proposed scheme T-SEA has been matched against standard DSR routing protocol, PACE-DSR [9] and MDSR (Mohanapriya and Krishnamurthi [18]). The parameters that are evaluated to show the efficacy of T-SEA are: Packet Delivery Ratio, packet drop ratio, average end-to-end latency, control packet overhead and average energy of network nodes. The different parameters used during simulation are listed in Table 3. In simulations, the minimum required trust threshold, *trust_threshold* is chosen to be 4.0 for a fixed initial trust value of 6.0. This trust parameter depends on the initial trust value and the deduction factor (evaluated using Eq. (4)).

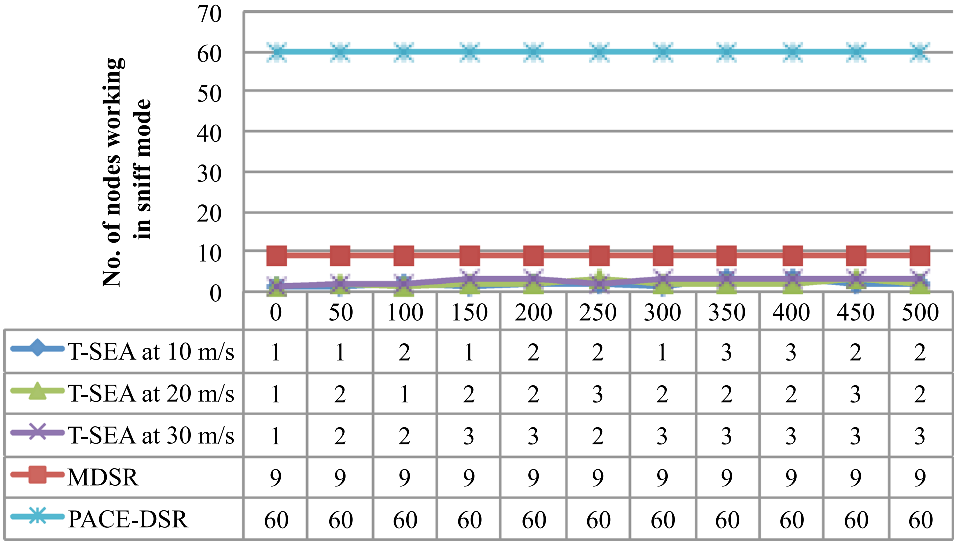
Table 3 Simulation parameters

Parameter	Simulation value
Simulator	NS-2.34
Simulation time	520 s
Simulation area	1000 m × 1000 m
Number of nodes	60
No. of connections	20
Transmission range	250 m
Movement model	Random waypoint
Maximum speed	20 m/s
Pause time	0, 5, 15, 20 s
Traffic type	CBR (UDP)
CBR rate	0.2 Mbps
Packet size	512 bytes
Maximum number of malicious nodes	5
Dropping threshold $\delta_{threshold}$	15% and 20%
Constant γ	2
detect_suspect interval	8 s
Trustworthy index threshold	0
Initial energy	350 J
rxPower	1 W
txPower	1 W
idlePower	1 W

4.2 Results and analysis

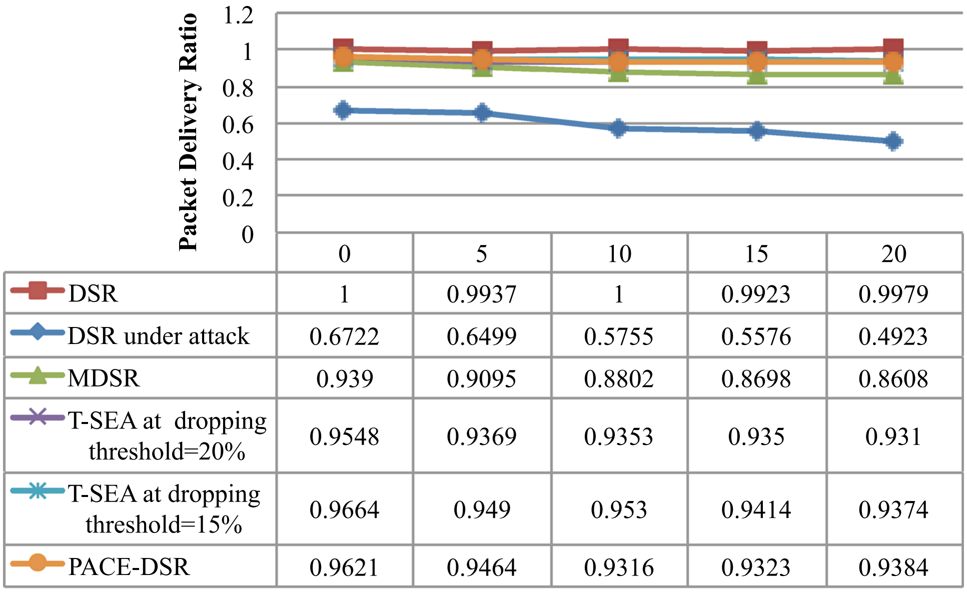
The section presents and compares the performance outcomes of the proposed security scheme with standard DSR protocol, DSR under attack, PACE-DSR and MDSR at varying nodes' speeds. Figure 1 shows the number of network nodes that operate in sniff mode at different time and for varying nodes' speeds. As portrayed in the figure, T-SEA requires only one to three active IDS nodes (that work in sniff mode) for different nodes' speed to catch the

Fig. 1 Number of nodes working in sniff mode v/s simulation time



	0	50	100	150	200	250	300	350	400	450	500
T-SEA at 10 m/s	1	1	2	1	2	2	1	3	3	2	2
T-SEA at 20 m/s	1	2	1	2	2	3	2	2	2	3	2
T-SEA at 30 m/s	1	2	2	3	3	2	3	3	3	3	3
MDSR	9	9	9	9	9	9	9	9	9	9	9
PACE-DSR	60	60	60	60	60	60	60	60	60	60	60

Fig. 2 Packet delivery ratio v/s nodes' speed (m/s)



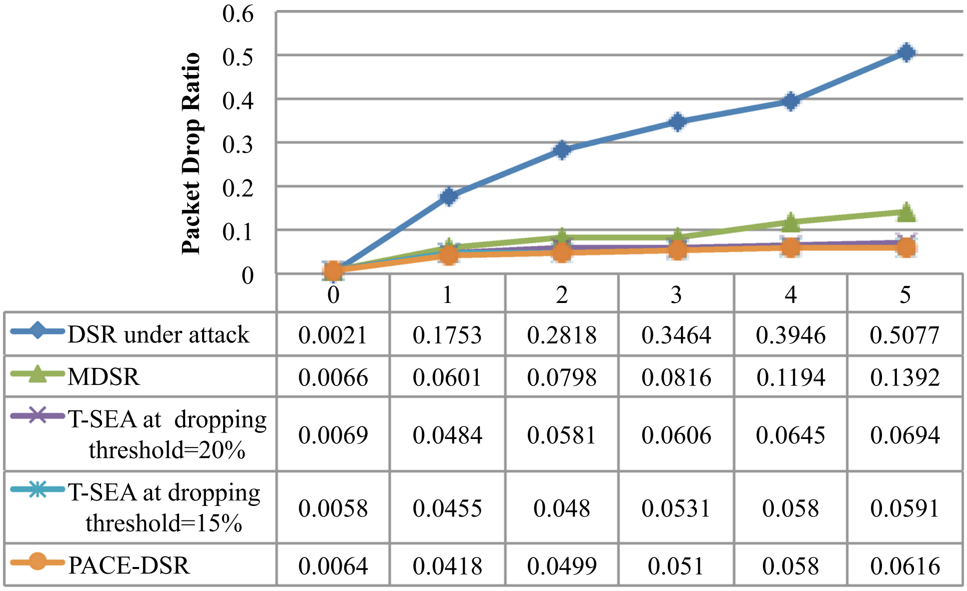
	0	5	10	15	20
DSR	1	0.9937	1	0.9923	0.9979
DSR under attack	0.6722	0.6499	0.5755	0.5576	0.4923
MDSR	0.939	0.9095	0.8802	0.8698	0.8608
T-SEA at dropping threshold=20%	0.9548	0.9369	0.9353	0.935	0.931
T-SEA at dropping threshold=15%	0.9664	0.949	0.953	0.9414	0.9374
PACE-DSR	0.9621	0.9464	0.9316	0.9323	0.9384

misbehaving nodes in comparison to MDSR which needs nine fixed IDS nodes and PACE-DSR which requires all the sixty nodes that work in sniff mode for the detection of black/gray hole nodes. The lessening of number of active IDS nodes, results in lesser energy consumption, hence increasing the network life.

Figure 2 shows the Packet Delivery Ratio at different nodes' speeds. The PDR utilizing the proposed TSEA protocol is higher than MDSR approach, PACE-DSR approach and DSR in attack scenario. T-SEA is simulated at γ =2 and at two distinct estimations of packet dropping threshold percentage, $\delta_{threshold}$. It is seen from the figure that the PDR improves slightly when $\delta_{threshold}$ is reduced from 20 to 15%. The mean value of PDR for T-SEA at $\delta_{threshold}$ = 15% is 0.94944 and at $\delta_{threshold}$ = 20% is 0.9386. and these values are comparatively higher than that of DSR under attack (= 0.5895), PACE-DSR (= 0.93756) and MDSR (= 0.89186). The increase in PDR of the proposed protocol is because of the fact that T-SEA protocol selects a fresh path instantly after detecting misconducting node in the path. Further, the standard deviation of PDR of the T-SEA protocol at $\delta_{threshold}$ = 15% is 0.0101, T-SEA protocol at $\delta_{threshold}$ = 20% is 0.00833, DSR is 0.00321, DSR in attack scenario is 0.06504, PACE-DSR is 0.01028 and MDSR is 0.02871.

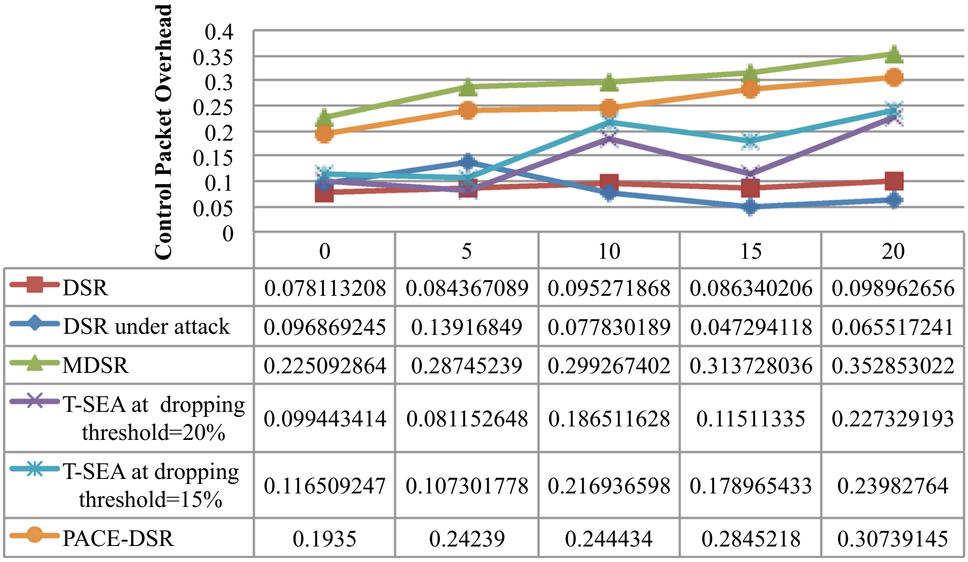
Figure 3 demonstrates the packet drop proportion at different number of malevolent nodes at nodes' speed of 20 m/s. The figure shows that the packet drop ratio of DSR in attack scenario most astounding (mean value = 0.28465) as no mechanism for identification and seclusion of getting

Fig. 3 Packet drop ratio v/s number of malicious nodes



	0	1	2	3	4	5
◆ DSR under attack	0.0021	0.1753	0.2818	0.3464	0.3946	0.5077
▲ MDSR	0.0066	0.0601	0.0798	0.0816	0.1194	0.1392
× T-SEA at dropping threshold=20%	0.0069	0.0484	0.0581	0.0606	0.0645	0.0694
✱ T-SEA at dropping threshold=15%	0.0058	0.0455	0.048	0.0531	0.058	0.0591
● PACE-DSR	0.0064	0.0418	0.0499	0.051	0.058	0.0616

Fig. 4 Control packet overhead v/s nodes' speed (m/s)

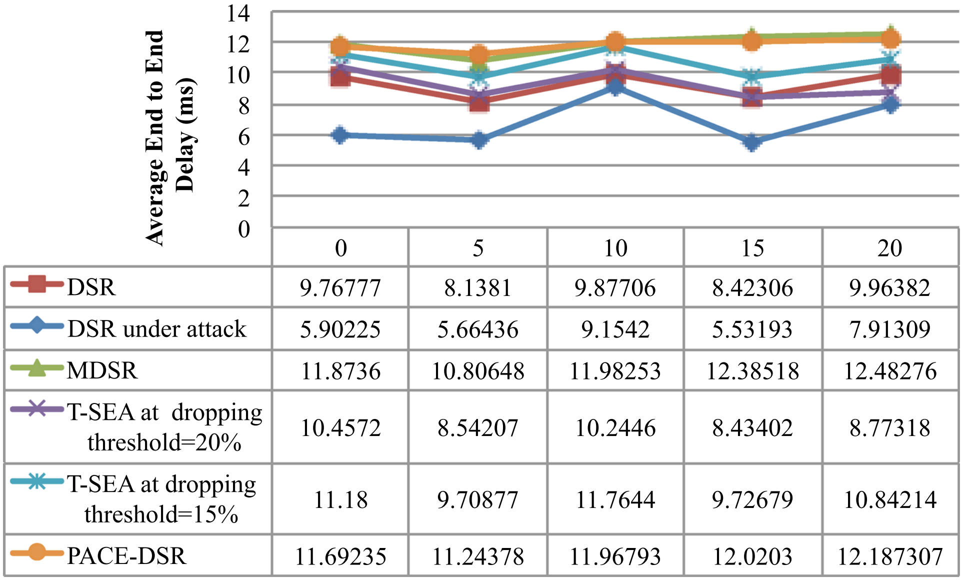


	0	5	10	15	20
■ DSR	0.078113208	0.084367089	0.095271868	0.086340206	0.098962656
◆ DSR under attack	0.096869245	0.13916849	0.077830189	0.047294118	0.065517241
▲ MDSR	0.225092864	0.28745239	0.299267402	0.313728036	0.352853022
× T-SEA at dropping threshold=20%	0.099443414	0.081152648	0.186511628	0.11511335	0.227329193
✱ T-SEA at dropping threshold=15%	0.116509247	0.107301778	0.216936598	0.178965433	0.23982764
● PACE-DSR	0.1935	0.24239	0.244434	0.2845218	0.30739145

misbehaving nodes is utilized. The message drop ratio of MDSR is more than the proposed convention when compare at two distinct values of $\delta_{threshold}$. The mean estimation of packet drop proportion of MDSR approach (= 0.08112) is more than that of T-SEA (=0.04492 at $\delta_{threshold}$ = 15% and is 0.05132 at $\delta_{threshold}$ = 20%). The mean estimation of packet drop proportion of PACE-DSR is 2.078% more than that of T-SEA.

Figure 4 represents control packet overhead at different values of nodes' mobility. Simulation shows that the number of control packets needed to deploy MDSR model is most elevated when contrasted with PACE-DSR, DSR and T-SEA as MDSR utilizes additional control packets such as QREQ, QREP, MNREQ and ALARM messages. Control packet overhead of T-SEA at $\delta_{threshold}$ = 15% is higher than the same overhead of T-SEA at $\delta_{threshold}$ = 20%. The rise in overhead is because of reason that at less estimation of $\delta_{threshold}$, T-SEA turns out to be more stringent for malicious nodes, more are active IDS required for observing, which increment the quantity of control messages which are being transmitted between IDS nodes and the source node. T-SEA protocol involves 46.93% less control messages overhead when contrasted with MDSR approach as in T-SEA no additional control packets or no message is communicated in the network to segregate malicious node. Packet overhead of T-SEA is 38.33% less than that of PACE-DSR. Message overhead of PACE-DSR is more when contrasted with DSR and T-SEA, as in PACE-DSR monitoring scheme is deployed on every node. All network nodes make a list known as faulty list and then

Fig. 5 End to end delay v/s nodes' speed (m/s)



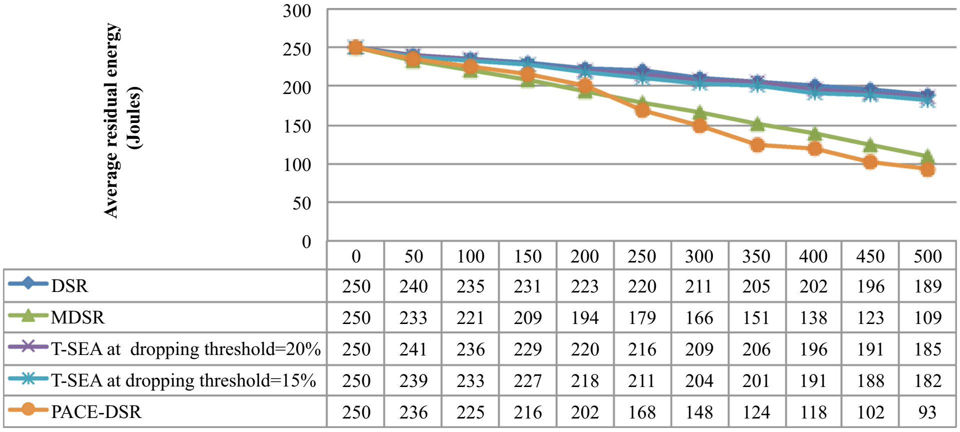
	0	5	10	15	20
DSR	9.76777	8.1381	9.87706	8.42306	9.96382
DSR under attack	5.90225	5.66436	9.1542	5.53193	7.91309
MDSR	11.8736	10.80648	11.98253	12.38518	12.48276
T-SEA at dropping threshold=20%	10.4572	8.54207	10.2446	8.43402	8.77318
T-SEA at dropping threshold=15%	11.18	9.70877	11.7644	9.72679	10.84214
PACE-DSR	11.69235	11.24378	11.96793	12.0203	12.187307

share the list in entire network which generates unnecessary route packets and thus, the message overhead increases. In T-SEA, the source node does not choose the route that have misbehaving node for transfer of messages. Along these lines, misbehaving nodes are confined from the network without the need of additional control packets.

Average end to end delay of the proposed scheme (at $\delta_{threshold}$ of 15% & 20%), MDSR, PACE-DSR and DSR protocols is represented in Fig. 5. In MDSR protocol, transmission of minimally two blocks of data is needed for detection and isolation of a gray hole node, this introduces delay for removing the gray hole node. PACE-DSR requires rediscovery of the routes to isolate misbehaving nodes which leads to increase in average latency. Average end to end delay of T-SEA is 15.95% less than that of MDSR and 15.35% less than that of PACE-DSR. T-SEA chooses trustworthy, reliable and secure path with no misbehaving nodes in the path. This uniqueness from the paths chose by DSR lifts the average end to end delay in transmission when contrasted with standard DSR protocol shown in the figure.

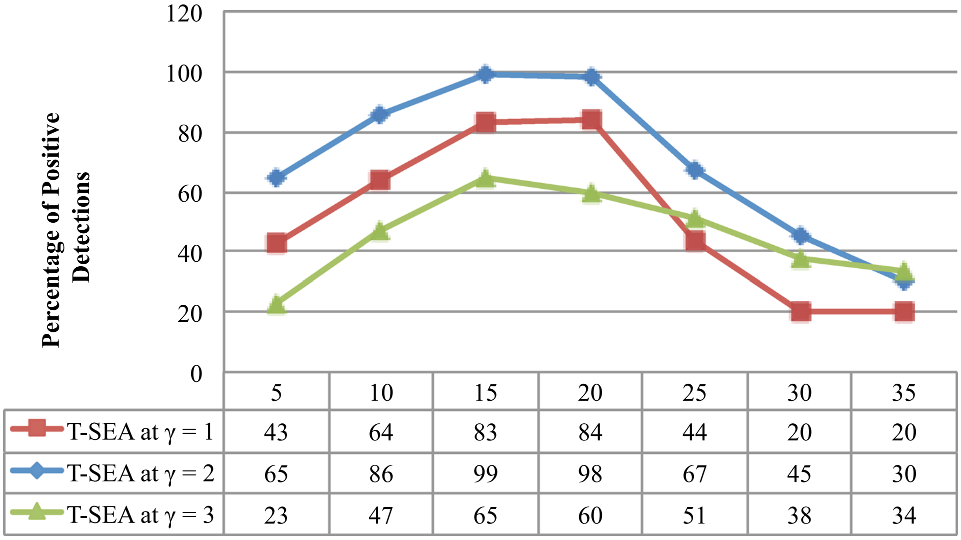
Figure 6 shows average leftover battery life of the nodes at various times with nodes' mobility of 15 m/s. In MDSR, the similar IDS nodes are working amid the network lifetime. Thus, selected IDS nodes' battery is expended quickly and after some time IDS nodes move toward becoming battery deficient and dead. In PACE-DSR, every node in the network operate in sniff mode and listen to routing packets within their range. PACE-DSR employs broadcasting mechanism to inform about malicious nodes. Broadcasting and sniff mode increases the nodes' battery consumption. Average residual energy of MDSR and PACE-DSR are 16.45% and 20.3% respectively less that that of T-SEA. T-SEA guarantees distributed loss of battery power. Subsequently, keeps any node from getting to be power lacking. MDSR fails to identify any malevolent node after 250 s as a portion of the IDS nodes have got power deficient that is their leftover battery power turn out

Fig. 6 Average residual energy of nodes at different times



	0	50	100	150	200	250	300	350	400	450	500
DSR	250	240	235	231	223	220	211	205	202	196	189
MDSR	250	233	221	209	194	179	166	151	138	123	109
T-SEA at dropping threshold=20%	250	241	236	229	220	216	209	206	196	191	185
T-SEA at dropping threshold=15%	250	239	233	227	218	211	204	201	191	188	182
PACE-DSR	250	236	225	216	202	168	148	124	118	102	93

Fig. 7 Percentage of positive detections v/s packet dropping threshold percentage



	5	10	15	20	25	30	35
■ T-SEA at γ = 1	43	64	83	84	44	20	20
◆ T-SEA at γ = 2	65	86	99	98	67	45	30
▲ T-SEA at γ = 3	23	47	65	60	51	38	34

to be under 21 J and hence not able to work or execute detection mechanism.

Figure 7 shows the percentage of positive detections as a function of dropping threshold for different values of γ. It can be inferred from the figure that the satisfactory dropping threshold, $\delta_{threshold}$ values are 15% & 20% and ideal value of γ is 2. Generally, dropping limit relies upon the confidence level needed in the network and on the network uniqueness, for example, network size and node density. Higher the estimation of $\delta_{threshold}$, more probable that T-SEA convention does not detect any misbehaving node that drops packets intentionally. However, the inherent nature of MANETs causes some packets to be lost, so at lower threshold well-behaving nodes can be falsely detected as malicious. Therefore, appropriate selection of $\delta_{threshold}$ is needed to diminish the likelihood of false recognitions and raise the likelihood of detecting truly misbehaving nodes.

PACE-DSR convention indicates great performance with regard to Packet Delivery Ratio and packet loss proportion yet its performance degrades in regard to control packet overhead proportion, end to end delay and average residual energy.

5 Conclusion and future scope

A routing protocol which is trust based, secure as well as energy conscious is introduced for the discovery and elimination of misbehaving nodes that encourage black hole/gray hole attacks in MANETs. T-SEA protocol gives emphases to security and power management of the battery operational portable devices and subsequently beneficial in an ad hoc circumstances where in security is the fundamental essential and power is a significant network asset. IDS nodes operate in sniff mode simply after the discovery of attack. This spares the energy of battery controlled devices and henceforth draws out the network life span. Simulations demonstrate that the T-SEA convention disconnects the malevolent nodes and subsequently enhances the Packet Delivery Ratio without any increase in computational complexity and the network overhead as it is non-cryptographic.

In future, this work can be reached out to identify and go around other MANET security attacks. The work can likewise be altered to add security to other existing reactive ad hoc routing protocols.

References

1. Ahila E, Chitra K (2014) Security based energy efficient routing protocol for adhoc network. In: Proc. of IEEE international conference on control, instrumentation, communication and computational technologies (ICCICCT), pp 1522–1526. ISBN: 978-1-4799-4191-9
2. Ahmed A, Bakar KA, Channa MI, Haseeb K, Khan AW (2016) A trust aware routing protocol for energy constrained wireless sensor network. Telecommun Syst 61:123–140. https://doi.org/10.1007/s11235-015-0068-8
3. Asadi M, Zimmerman C, Agah A (2013) A game theoretic approach to security and power conservation in wireless sensor networks. Int J Netw Secur 15:50–58
4. Banergee S (2008) Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. In: Proc. of the world congress on engineering and computer science (WCECS 2008), San Francisco, USA, pp 337–342. ISBN: 978-988-98671-0-2 WCECS 2008
5. Biswas S, Nag T, Neogy S (2014) Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. In: Proc. of IEEE applications and innovations in mobile computing (AIMoC), pp 157–164. https://doi.org/10.1109/AIMOC.2014.6785535. ISBN: 978-1-4799-3881-0

6. Cano J C, Kim D (2002) Investigating performance of power-aware routing protocols for mobile ad-hoc networks. In: Proc. of the international workshop on mobility and wireless access (MobiWac 2002). IEEE Computer Society, Washington, DC, USA, pp 80–86. https://doi.org/10.1109/MOBWAC.2002.1166956. ISBN: 0-7695-1843-5
7. Dhurandher S K, Woungang I, Traore I (2014) C-scan: an energy-efficient network layer security protocol for mobile ad hoc networks. In: Proc. of 28th IEEE international conference on advanced information networking and applications workshops (WAINA), pp 530–535. https://doi.org/10.1109/WAINA.2014.85. ISBN: 978-1-4799-2654-1
8. Estahbanati M M, Rasti M, Hamami S M S (2014) A mobile ad hoc network routing based on energy and markov chain trust. In: Proc. of IEEE 7th international symposium on telecommunications (IST), pp 596–601 https://doi.org/10.1109/ISTEL.2014.7000775
9. Ghander A, Shaaban E (2015) Power aware cooperation enforcement MANET routing protocols. Procedia Comput Sci 73:162–171. https://doi.org/10.1016/j.procs.2015.12.062
10. Gong P, Chen TM, Xu Q (2015) ETARP: an energy efficient trust-aware routing protocol for wireless sensor networks. J Sens. https://doi.org/10.1155/2015/469793
11. Gonzalez OF, Howarth M, Pavlou G (2008) Detection and accusation of packet forwarding misbehavior in mobile ad hoc networks. J Internet Eng 2:181–192
12. Heena, Kumar N (2014) Battery power and trust based routing strategy for MANET. In: Proc. of IEEE international conference on advanced communication control and computing technologies (ICACCCT), pp 1559–1562. https://doi.org/10.1109/ICACCCT.2014.7019368. ISBN: 978-1-4799-3915-2
13. Jain H R, Sharma S K (2014) Improved energy efficient secure multipath AODV routing protocol for MANET. In: Proc. of IEEE international conference on advances in engineering and technology research (ICAETR), pp 1–9. https://doi.org/10.1109/ICAETR.2014.7012847
14. Johnson DB, Maltz DA (1996) Dynamic source routing in ad hoc wireless networks. In: Mobile computing, the kluwer international series in engineering and computer science, vol 353. Springer, pp 153–18. https://doi.org/10.1007/978-0-585-29603-6_5. ISBN: 978-0-7923-9697-0
15. Li J, Cordes D, Zhang J (2005) Power-aware routing protocols in ad hoc wireless networks. IEEE Wirel Commun 12:69–81. https://doi.org/10.1109/MWC.2005.1561947
16. Li Y, Peng S, Chu W (2006) An efficient algorithm for finding an almost connected dominating set of small size on wireless ad hoc networks. In: Proc. of 2006 IEEE international conference on mobile adhoc and sensor systems (MASS), pp 199–205. https://doi.org/10.1109/MOBHOC.2006.278557. ISBN: 1-4244-0506-8
17. Marti S, Giuli T J, Lai K, Baker M (2000) Mitigating routing misbehavior in mobile ad hoc networks. In: Proc. of sixth annual international conference on mobile computing and networking (MobiCom ’00), Boston, USA, pp 255–265. https://doi.org/10.1145/345910.345955. ISBN:1-58113-197-6
18. Mohanapriya M, Krishnamurthi I (2014) Modified DSR protocol for detection and removal of selective black hole attack in MANET. Comput Electr Eng 40:530–538. https://doi.org/10.1016/j.compeleceng.2013.06.001
19. Murthy Siva Ram C, Manoj BS (2004) Ad hoc wireless networks: architectures and protocols. Prentice Hall, Upper Saddle River
20. Network Simulator 2 (NS–2). http://www.isi.edu/nsnam/ns/. Accessed 13 Nov 2016
21. Sarkar S, Datta R (2012) A trust based protocol for energy-efficient routing in self-organized MANETs. In: Proc. of annual IEEE India conference (INDICON), pp 1084–1089. https://doi.org/10.1109/INDCON.2012.6420778. ISBN: 978-1-4673-2270-6
22. Sarkar S, Datta R (2014) A secure and energy-efficient stochastic routing protocol for wireless mobile ad-hoc networks. In: Proc. of IEEE twentieth national conference on communications (NCC), pp 1–6. https://doi.org/10.1109/NCC.2014.6811358. ISBN: 978-1-4799-2363-2
23. Sarkar S, Datta R (2016) A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks. Ad Hoc Netw 37:209–227. https://doi.org/10.1016/j.adhoc.2015.08.020
24. Sheu JP, Chao CM, Hu WK, Sun CW (2007) A clock synchronization algorithm for multihop wireless ad hoc networks. Wirel Pers Commun 43:185–200. https://doi.org/10.1007/s11277-006-9217-4
25. Sridhar S, Baskaran R, Chandrasekar P (2013) Energy supported AODV (EN-AODV) for QoS routing in MANET, In: Proc. of the 2nd international conference on integrated information (IC-ININFO 2012), Budapest, Hungary, vol 73 of procedia-social and behavioral sciences, pp 294–301. https://doi.org/10.1016/j.sbspro.2013.02.055
26. Su MY (2011) Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comput Commun 34:107–117. https://doi.org/10.1016/j.comcom.2010.08.007
27. Subramaniam S, Ramachandran R (2014) Energy-and trust-based AODV for quality-of-service affirmation in MANETs. In: artificial intelligence and evolutionary algorithms in engineering systems, vol 324 of the series advances in intelligent systems and computing. Springer, Berlin, pp 601–607. https://doi.org/10.1007/978-81-322-2126-5_65. ISBN: 978-81-322-2125-8
28. Tan S, Li X, Dong Q (2015) Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Netw 30:84–98. https://doi.org/10.1016/j.adhoc.2015.03.004
29. Wang Y (2010) Study on energy conservation in MANET. J Netw 5:708–715
30. Woungang I, Dhurandher S K, Sahai M (2013) An energy-aware secured routing protocol for mobile ad hoc networks using trust-based multipath. In: grid and pervasive computing, vol 7861 of the series lecture notes in computer science. Springer, Berlin, pp 517–525. https://doi.org/10.1007/978-3-642-38027-3_55. ISBN: 978-3-642-38026-6
31. Yang H, Shu J, Meng X, Lu S (2006) SCAN: self-organized network-layer security in mobile ad hoc networks. IEEE J Sel Areas Commun 24:261–273. https://doi.org/10.1109/JSAC.2005.861384
32. Yang T, Wei L (2007) Modified energy-aware DSR routing for ad hoc network. In: Proceedings of the international conference on wireless communications, networking and mobile computing (WiCom 2007), pp 1601–1603. https://doi.org/10.1109/WICOM.2007.403
33. Zhang Y, Lee W (2005) Security in mobile ad-hoc networks. In: Ad hoc networks, pp 249–268. https://doi.org/10.1007/0-387-22690-7_9. ISBN: 978-0-387-22689-7