J Ambient Intell Human Comput (2018) 9:941–956
DOI 10.1007/s12652-017-0496-2

ORIGINAL RESEARCH

Power aware malicious nodes detection for securing MANETs against packet forwarding misbehavior attack

Deepika Kukreja[1] · S. K. Dhurandher[1] · B. V. R. Reddy[2]

Received: 17 January 2017 / Accepted: 22 April 2017 / Published online: 27 April 2017

Abstract A power aware detection procedure for securing mobile ad hoc networks (MANETs) against packet forwarding misbehavior attack is introduced. Packet forwarding misbehavior attack is one of the security attacks in which malicious nodes make MANETs weak by showing packet dropping misconduct. The proposed protocol is named as power aware malicious detection for security (PAMDS) protocol. The feature of power aware is desirable to prolong MANET lifetime as under certain conditions, it is impracticable to replace or recharge the nodes' batteries. The protocol employs intrusion detection system (IDS) for the detection and exclusion of the nodes inducing packet forwarding misbehavior attack in the network. The detection procedure reacts quickly in detecting and isolating malicious nodes. The detection procedure is power aware as only a small set of nodes that have enough energy and that cover the entire network are selected for running IDS. Also, IDS nodes are not required to work in promiscuous listening mode 100% of the time, this further saves power. PAMDS protocol emphasizes on security of the mobile ad hoc environment and power saving of the battery powered hand held devices. The protocol has been extensively simulated using network simulator NS-2. The findings indicate that PAMDS protocol is effective in terms of power saving, quick malicious node isolation and packet delivery ratio percentage.

Keywords Mobile ad hoc networks · Intrusion detection system · Packet forwarding misbehavior · Power aware · Dynamic source routing protocol · Security

1 Introduction

Secure communication is an essential characteristic required in all types of networks. MANETs are prone to different security threats as mobile nodes depend on each other for data transmission, limited battery power of the mobile devices, changing network topology and lack of central authority. Therefore, the intrinsic nature of MANETs makes them susceptible to a wide range of attacks. Shielding MANETs from malicious attacks is an essential and challenging issue. There are mainly two types of attacks in ad hoc networks: internal attacks and external attacks (Zhang and Lee 2005). External attacks can be disallowed by means of regular security methods. Internal attacks are usually more brutal attacks, since misbehaving nodes are the part of the network. So, they become hard to find by security methods.

Misbehavior can either be a routing misbehavior or a packet forwarding misbehavior. In routing misbehavior, malicious nodes do not behave according to a routing protocol and malicious nodes show packet forwarding misbehavior when they do not relay data packets according to a data transfer protocol (Nadeem and Howarth 2013). In packet forwarding misbehavior attack, once the route between a source node and a destination node is established, a malicious node lying in a route drops the data packets directed

✉ Deepika Kukreja
deepikakukreja18@gmail.com

S. K. Dhurandher
dhurandher@gmail.com

B. V. R. Reddy
profbvrreddy@gmail.com

[1] Division of Information Technology, N.S.I.T., University of Delhi, Delhi, India

[2] U.S.I.C.T., Guru Gobind Singh Indraprastha University, Delhi, India

to it and which it is supposed to forward during data transfer phase.

Ad hoc environments are secured primarily by two approaches. The first approach for securing an ad hoc network is by implementing a secure routing protocol which ensures the secure transmission by taking care of the mandatory security requirements. The other approach is to design and implement an intrusion detection system that detects and circumvents the nodes inducing malevolent behavior in the network. This paper presents a solution to packet forwarding misbehavior attack. It uses a non-cryptographic method to secure MANETs against packet forwarding misbehavior attack by jointly employing both the security approaches.

Limited battery power of the mobile devices is one another main restraint of MANETs. In many situations, replacing or recharging nodes' battery is not easy. In such a scenario, the only solution for providing increased network life and improved communication is to judiciously use node's battery power. Power consumption of nodes also depends upon some network factors such as high mobility of nodes, more number of retransmissions and too much routing messages.

Power aware routing is desirable in such networks as the battery power of some nodes may drain out during operation. A mobile node can perform well, forward packets and participate in other routing operations only when it has enough power. A power aware routing protocol must be such that it should distribute the power consumption rate evenly among network nodes and at the same time, it should enhance the network performance by incorporating reliable and secure data transfer. Nodes which do not have enough energy cause the problem of frequent route failures due to broken links in the network. Power aware routing protocols avoid frequent link breaks and hence increase the network performance by reducing the energy consumption of mobile nodes. Power efficient routing protocols provide solution to frequent link failures and there by maintains performance level for a longer time. Therefore, power aware routing provides an efficient solution to extend the lifetime of energy constrained mobile nodes in MANETs (Misra et al. 2010; Vazifehdan et al. 2011).

In order to achieve enhanced lifetime of the network with secure communication, efficient utilization of battery power of different network nodes is required. Therefore, limited energy and secure communication are the two main demanding issues in MANETs. Power aware secure routing has become imperative because of the fact that if one network node fails due to power shortage in an ad hoc environment, it can create problems like network partitioning and loose links connectivity.

The proposed protocol checks the energy levels of mobile nodes before its participation in routing. The main aim of the proposed work is to design a power aware secure routing protocol that maintains the network connectivity and secures the communication between the nodes as long as possible. The paper proposes a routing protocol which utilizes the energy of the mobile nodes wisely and efficiently. The protocol thus enhances the life of MANET and makes the communication between the nodes secure. The proposed protocol further maximizes the network existance by balancing the power consumption of nodes globally.

The data transmission phase of the dynamic source routing (DSR) protocol (Johnson and Maltz 1996) is modified in this work. Unlike standard DSR protocol, source and destination nodes keep record of routes through which data packets are sent and received respectively in certain time duration called *check_time*. Doing this, the protocol first detects routes through which the data packets are dropped with a certain ratio. That is the protocol first detects the routes which are accountable for considerable data loss during the transmission. Then the nodes which may be liable for significant data loss are put into an accusation list (discussed later in Sect. 3) for further detection by IDS system. IDSs are deployed on some of the network nodes and this set of nodes is termed as IDS set. These nodes are capable to work in promiscuous listening mode when require. In promiscuous listening mode, nodes overhear all the transmissions within its range; hence consuming substantial nodes' energy. In the proposed PAMDS protocol, only few nodes out of the IDS set are required to work in promiscuous listening mode, this results in lesser network overhead and saves nodes' energy as compared to the existing secure routing protocols which require all the network nodes to work in promiscuous listening mode for identifying misbehaving nodes.

The rest of the paper begins with the related work and their limitations discussed in Sect. 2. Key features of the proposed PAMDS protocol and detailed discussion of its methodology with an illustration are presented in Sect. 3. This is followed by simulation and experimental results shown in Sect. 4. In Sect. 5, we end with few concluding remarks and the work that can be done in future.

2 Related work

Many secure routing protocols have been proposed to protect the network against malicious nodes and packet forwarding misbehaviors. Some of these protocols as proposed in (Hu et al. 2003, 2005; Zapata 2002; Perrig et al. 2000; Buchegger and Boudec 2002; Su 2011) only secure the route discovery phase of routing protocols. PAMDS protocol secures the data forwarding phase and hence, can be used along with the aforesaid protocols. Research has also been conducted to protect data forwarding against malicious attacks as proposed by Marti et al. (2000), Banergee (2008) and Mohanapriya and Krishnamurthi (2014) and proposed in Gonzalez et al. (2008) and Yang et al. (2006).

In Su (2011), selective black hole attack is detected and isolated by deploying IDS nodes. In order to monitor its neighboring nodes, all the IDS nodes work in promiscuous listening mode during the entire lifetime of the network. On detection of an abnormal difference between the number of route request (RREQ) packets and the number of route reply (RREP) packets transmitted by a node, the nearby IDS node broadcast a block message to other network nodes so as to isolate the malicious node. The mechanism increases the network overhead due to two main reasons. First, an IDS node informs the other nodes about the malicious node through broadcasting of block message. Second, all the IDS nodes are required to persistently work in promiscuous listening mode in order to sniff all routing packets within its transmission range. Broadcasting can produce unnecessary routing overhead in the MANET. It also increases node's battery power consumption spent on hearing these messages. Broadcasting may also create network congestion. The paper does not give any method for how the IDS nodes among all network nodes are chosen for monitoring its neighbor nodes. Moreover, dynamic network topology is an inherit characteristic of MANETs. No method for changing the IDS nodes when network topology change is discussed in the paper. The authors assume fixed IDS nodes which is unrealistic in MANET environment. Moreover, it employs a mechanism using IDS nodes to calculate approximate suspicious value for the nodes that forward RREP but do not forward RREQ. This approach is more suitable for detecting black hole attack rather than gray hole attack as gray hole nodes participate properly during route discovery phase.

Work proposed in Gonzalez et al. (2008) used the principle of flow conservation for detecting and accusing nodes that exhibit packet forwarding misbehavior. Method detects black hole and gray hole nodes by calculating the approximate percentage of dropped packets by that nodes. Cryptography techniques are used in Yang et al. (2006) that increase computational complexity. Marti et al. (2000) fails to detect malicious behavior in presence of ambiguous collisions, false misbehavior, receiver collisions, partial dropping and limited transmission power. Banergee (2008) proposed an approach to detect and remove cooperative black and gray hole attack. Source node sends the data in the form of data blocks. This increases the delay in routing if any gray hole node is present in the source route.

Some research efforts have also been focused to make routing protocols power-aware (Wang 2010; Yang and Wei 2007). A comparative study of few power-aware protocols is done by Cano and Kim (2002). Also, a survey of energy-aware protocols is illustrated in Li J et al. (2005). Sheu et al. (2007) developed another protocol to save battery by using global synchronization coordinate beacon intervals between devices. Mohanapriya and Krishnamurthi (2014) modified DSR protocol (named as MDSR) using an IDS for detection of selective black hole attack. Data traffic is divided and transmitted in the form of small fixed size blocks. IDS nodes work in promiscuous mode only after the detection of gray hole nodes. It takes transmission of at least two data blocks to detect and then isolate a gray hole node, delaying the detection and isolation process. In this work, as IDS nodes are static it is not practicable to catch all malicious nodes in a network having dynamic topology. Further, the path used for the intimation of number of data packets in a block may have gray hole node/s. This protocol fails if two or more neighboring nodes collude together.

Sridhar et al. (2013) proposed an energy based ad hoc on-demand distance vector (EN-AODV) protocol. The proposed scheme calculates the energy levels of the nodes and if the calculated energy of a node is greater than a predefined energy threshold than only that node is considered to participate in the routing process. The protocol discovers the nodes that have enough energy level for transmission of data. Hence the protocol does not select the nodes that may drain out their energy during data transmission. The protocol shows good results in terms of different QoS parameters like packet delivery ratio and end to end delay but the protocol does not consider secure data transmission which is an unavoidable MANET requirement.

Ahmed et al. (2016) proposed a trust and energy aware routing protocol (TERP). The protocol utilizes a distributed trust model approach that detects and isolates malicious nodes. The work considers the nodes that induce packet dropping attack in the network as malicious nodes. The Protocol uses a non cryptographic method and works in four phases namely, trust estimation, trust database, route setup and route maintenance. Subramaniam and Ramachandran (2014) proposed a trust based AODV routing protocol. In the proposed protocol, trust and energy of the nodes that want to participate in routing process are first determined. The nodes that have energy level and trust higher than predefined threshold values are allowed to take part in routing process. The method isolates the misbehaving nodes that induce packet dropping attack from being a part of the route.

Gong et al. (2015) proposed an energy efficient trust aware routing protocol (ETARP). The proposed protocol intends to reduce the energy consumption of nodes during data transmission phase. The method implements utility theory for achieving the aforementioned aim. Authors consider the trustworthiness and energy of the mobile nodes and use Bayesian network for estimating the trustworthiness of the network nodes. Asadi et al. (2013) designed a protocol to secure the network in an energy efficient way. In order to conserve its energy, a node uses the protocol for deciding whether to forward a packet or not, that it has received from another node. The protocol utilizes game theory approach to determine the best possible arrangement to prolong node's battery power. Using game theory, every node forwards a satisfactory number of data packets in the network. The protocol put in force the cooperation in between the network nodes and gives penalty for non cooperative act. Dhurandher et al. (2014) proposed a novel protocol which is energy aware version of SCAN for the attacks induced at network layer. The paper introduces a revised credit policy for renewing of tokens. This is implemented by multiplicatively increasing the life of a token each time a node renews it. In this work, the routing path which has the highest quality factor is chosen for routing.

Biswas et al. (2014) has given a solution for detection and prevention of black hole attacks. The solution assures that the data is transmitted securely while maintaining the resource consumption. The work determines a reliable and secure routing path that can function correctly in a network having black hole nodes and having changing topology too. In the proposed protocol, every network node is assigned three values which are: rank, remaining battery power and node stability. A node is considered as a black hole node, if its rank becomes 0. Heena and Kumar (2014) designed a new protocol for ad hoc networks. The proposed protocol modifies the formation of the RREP packet. RREP packet proposed contains the information namely: packet type, source address, destination address, nodes remaining battery power, token of node and node count. Using this type of RREP packet, the protocol discovers the shortest route containing only trustworthy nodes between source and destination. An energy-aware trust based multipath (E-TBM) secure routing protocol has been proposed by Woungang et al. (2013). The protocol is based on DSR protocol. The work gives methods that secure the data packets based on trust and multipath routing techniques. The work uses three main mechanisms: trust assignment, soft-encryption method and multipath DSR based routing method.

Sarkar and Datta (2012) designed a protocol named as protocol for energy-efficient routing (PEER). The protocol is trust based and uses energy consumption ratio to determine the energy-factor of nodes. Energy-factor is the ratio of the residual energy to the initial energy of a node. Based on the computed value of the energy-factor, a node is decided whether to participate in transmission of data packets or not. Authors further proposed secure and energy efficient stochastic (SEES) (Sarkar and Datta 2014) protocol for transmitting the data using multiple paths. Authors modeled the routing problem in MANETs as stochastic routing based on Markov chain model. The amount of energy consumed in packet forwarding is implemented as a function for Markov chain model using Bellman's principle of optimality equation. The authors further extended their work in Sarkar and Datta (2016). In this work, they proposed a secure and energy-efficient stochastic multipath routing protocol for MANETs. The protocol is based on Markov chain. It first finds out different multiple paths between the given source and destination pairs. It then selects the most energy efficient path stochastically among all these paths for forwarding the data packets. The protocol secures the data during transmission as the packets are transmitted using random paths between source and destination nodes. So it is not easy to intercept, jam, and hijack the data packets as attacker cannot listen to all paths between source node and the destination node. In this, the packet forwarding energy consumption cost is considered as a value function in a Markov chain to determine optimal routing policy.

Tan et al. (2015) proposed a trust based secure routing protocol for MANETs. A trust based routing mechanism is used to resist the security attacks in an optimized link state routing (OSLR) based MANET. The proposed scheme implements a trust model based on fuzzy Petri net. Fuzzy Petri net is used to calculate the trust levels of network nodes and then the trust level of the different paths from source to destination. The proposed solution avoids the malicious nodes to become a part of the final path chosen for data transmission by selecting a path that has highest path trust among all the other probable paths. The trust value of a node is computed based on its performance parameters in both data plane and routing plane.

Jain and Sharma (2014) introduced a routing protocol named as energy efficient secure multipath AODV (EESM-AODV). The protocol modifies AODV and is proposed for multipath routing. In order to be energy efficient, the protocol uses adaptive methods. Authors compared the results of the proposed protocol with AODV routing protocol under attacking scenarios. Estahbanati et al. (2014) proposed a trust and energy based routing protocol. The method uses hidden Markov model (HMM) to compute the trust of the nodes. Based on the computed trust and available energy of the nodes, authors proposed a new routing protocol using metric for selecting the good route for transmission and Markov chain trust.

Ahila and Chitra (2014) introduced a protocol named as privacy protecting secure and energy efficient routing (PPSEER) protocol. The proposed protocol claims to raise the privacy of the message while maintaining the energy effectiveness of nodes. The PPSEER protocol first classifies the nodes of the network into two types of nodes, super node or normal node. The transmission of the messages takes place based on the power control. The protocol secures the routing by implementing encryption techniques.

An energy aware routing protocol named as power aware cooperation enforcement (PACE) distributed mechanism has been proposed in (Ghander and Shaaban 2015). The protocol detects and avoids the nodes inducing routing misbehavior, forces malicious nodes to corporate with other network nodes and prolongs lifetime of the network. The protocol detects the malicious nodes that participate in the route discovery process but do not forward data packets. During data transmission phase, PACE method detects the malicious nodes by first saving a copy of data packet in cache after sending and then monitoring the neighbors of the node for certain duration of time. Monitoring node determines rating of its neighboring nodes. If a neighbor node has a rating lesser than a predefined faulty threshold value, then it is added to the faulty list. This faulty list is then broadcasted and used with every RREQ packet. This way, malicious nodes are avoided in the routing path. The proposed method claims to compensate the energy lost in monitoring and overhearing by selecting only reliable nodes that have highest leftover energy in the final routing path. The authors implemented the PACE mechanism by integrating it with DSR (named as PACE-DSR) and AODV (named as PACE-AODV) routing protocols.

Further, protocols proposed by Marti et al. (2000) and Banergee (2008) and as given in Su (2011), Gonzalez et al. (2008), Yang et al. (2006) and Ghander and Shaaban (2015) require all network nodes to continually monitor their neighboring nodes. This requires nodes to operate in promiscuous listening mode all the time, minimizing the lifetime of nodes and thus the network itself. The watchdog method deployed on IDS nodes for the identification of malicious nodes has been proved as an efficient and successful approach in MANETs. But a massive amount of energy consumption is introduced in the protocols that employ watchdog technique and hence these protocols conflict with the energy efficient design requirements of routing protocols. More precisely, mobile devices in a MANET environment are generally battery operated. In order to prolong their battery life, mobile nodes are required to be energy conserving. Therefore, there is an imperative need to devise power conserving routing protocol so as to extend the battery life of each mobile node. Most of the proposals that employ IDS do not present about the scheduling of watchdogs in their work as proposed by Mohanapriya and Krishnamurthi (2014) and in Su (2011). Protocols proposed by Marti et al. (2000) and Banergee (2008) and as given in Su (2011), Gonzalez et al. (2008), Yang et al. (2006) and Ghander and Shaaban (2015) do not even talk about when an IDS node should work in sniff mode and what are the different selected IDS nodes. They assume that the IDS nodes should work all time in promiscuous listening mode. The approach used by the aforementioned schemes make running IDS redundant and dissipate a lot of valuable energy resource without providing network security assistance. To our best knowledge, no existing routing security solutions in MANETs are appropriate that conserve energy while keeping the data transmission secure and reliable at the same time. As a result, an intelligent power aware secure routing protocol is highly required.

It can be concluded from the related work that the routing protocols discussed before do not perform well in all types of network environments. The existing power aware secure routing protocols in MANETs can be further improved to provide more consistent security solutions. In order to enhance the performance of MANET, the proposed protocol is devised to balance and efficiently utilize energy of the network nodes and to include security feature in the communication. We propose a protocol which is designed in a way to cope with the characteristics, requirements and constraints of an ad hoc environment by incorporating the security while keeping the power expenses low.

The eventual aim of the proposed work is to reduce the power cost incurred by IDS as much as practicable, while maintaining a sufficiently required security level in the network. In order to accomplish the aim, the proposed work optimizes the IDS technique in two stages. In first stage, the IDS locations are optimized. The network nodes that are located near to each other require less energy consumption for monitoring each other but in order to protect themselves, these nodes are more prone to compromise with each other and launch collaborative attacks. Therefore, in order to minimize the energy consumption and maximize the security requirement, the IDS nodes whose locations are optimized are selected using algorithm (Li et al. 2006). In the second stage, in order to reduce redundancy, nodes capable of running watchdog are optimized in number. In particular, the proposed work does not require all IDS nodes to work for entire lifetime.

3 Proposed protocol

3.1 Key features of PAMDS protocol

1. Although deployment of IDS in MANET enhances network performance and security, the energy overhead induced by such systems cannot be ignored. Unlike the previous works that use IDS, the proposed work moves a step ahead to conserve power by reducing unnecessary IDS monitoring. The proposed protocol optimizes the IDS technique and hence prolongs network lifetime.
2. In MANETs, nodes change their positions time to time and thus the scheme requires to change the positions of IDS nodes (or change the IDS nodes) as per cur-

rent network topology. This dynamic network topology problem causes many of the IDS schemes to fail at run time. The proposed method, reselects the IDS nodes in such a mobile scenario.
3. PAMDS protocol acts quickly for the detection and the prevention of misbehaving nodes.
4. PAMDS protocol employs non-cryptographic technique for enforcing secure communication. Hence does not increase computational complexity that occurs due to cryptography methods.
5. The protocol avoids collaborative attacks caused by colluding malicious nodes.
6. The protocol implements an algorithm for the selection of IDS nodes.
7. The protocol ensures QoS in terms of average energy consumption, packet delivery ratio, end to end delay and control packet overhead.

3.2 Model assumptions

The PAMDS protocol assumes that each direct connection between a pair of nodes has bidirectional communication symmetry. It also assumes that all network nodes are adapted with wireless interfaces that support promiscuous listening mode.

3.3 Working model

Source node first establishes a route to a destination node using route discovery procedure of DSR. After storing routes in the cache, the source node executes an algorithm to select IDS set as explained in the next section. Section 3.3.2 explains the data transmission phase of PAMDS protocol. Algorithm to show execution flow of the PAMDS protocol is presented in Sect. 3.3.3. Section 3.3.4 illustrates PAMDS protocol with the help of an example.

3.3.1 Selection of the IDS set

A set of nodes called IDS set is selected in such a way that the nodes belonging to IDS set have sufficient energy to run IDS, they do not belong to the malicious list, cover the entire network, all IDS nodes are connected to each other and the IDS set is small in size. In Li t al. (2006), authors proposed an algorithm to find Connected Dominating Set. PAMDS uses and extends the algorithm given in Li t al. (2006) to select the IDS set with two additional features. In PAMDS, nodes' energy and their nonexistence in the malicious list are also checked before putting the nodes into IDS set. It ensures full coverage as the set of IDS nodes are connected and the network nodes that are not in the IDS set connect to at least one node in the IDS set. At a time, all nodes belonging to IDS set do not run intrusion detection system. To save power, a required subset of IDS set is chosen to work in promiscuous listening mode and run IDS. The IDS nodes selection procedure ensures that all IDS nodes themselves are also monitored by the neighboring IDS node/s.

While selecting a new IDS set, a node may be barred from running the IDS if it has been running IDS for a long time or it is finishing its battery or it belongs to malicious list. Let A be any node and let:

- $E\_total(A)$ be A's total battery power when fully charged.
- $E\_IDS(A)$ be A's battery level at the beginning of running IDS.
- $E\_current(A)$ be A's current battery level.
- α be the maximum percentage of $E\_IDS(A)$ that can be spent in running IDS.
- β be the minimum percentage of $E\_total(A)$ that must be preserved.

Therefore, we can state more precisely that a node A shall not be selected as an IDS if

$$\left(1 - \frac{E\_current(A)}{E\_IDS(A)}\right) \times 100 > \alpha \tag{1}$$

or if

$$\frac{E\_current(A)}{E\_total(A)} \times 100 < \beta \tag{2}$$

The percentage values of α and β are selected based on the average energy of the network nodes. A stage where none of the IDS nodes meet formula (1) and (2) may come when residual energy of all the nodes becomes very less as compared to their initial energy. At this stage there are two choices. The first option is to increase the value of α and reduce the value of β. Doing this, the IDS nodes will still get selected in low energy network but this is not a wise choice. As IDS nodes consume more energy as compared to other regular nodes, the energy of the selected IDS nodes (which are already energy deficient) will get drained fast and will eventually die. In order to increase the network lifetime, the proposed protocol opts the second option where it does not select any IDS node in a power deficient network keeping the values of α and β same throughout the network lifetime.

3.3.2 Data transmission

Source node sends data packets to a destination node through a route selected as in standard DSR protocol. As the network has dynamic topology, different data packets may follow different routes between source and destination nodes. In PAMDS protocol, source node maintains three records: (1) primary accusation list containing nodes accused by destination node, (2) malicious list having misbehaving nodes and (3) a path table which contains the routes along with number of data packets transmitted via these routes in *check_time* duration. Destination node also maintains a path table containing the routes through which it has received data packets along with the number of data packets received through different routes within *check_time* duration. After every *check_time*, source node sends its path table to the destination node through the connected IDS nodes. The route formed by IDS nodes is the most reliable route. Destination node uses the path table sent by source node to check for any data loss during the transmission.

Packet loss in MANETs is mainly due to network congestion, mobility, broken links and transmission errors. The acceptable packet loss depends on the type of data being sent. The percentage of congestion-related packet loss increases with communication requests (Lu et al. 2003). PAMDS protocol makes use of an acceptable data dropping threshold percentage, $\lambda_{threshold}$, which is the percentage of data dropping that occur due to above mentioned unavoidable network problems. The satisfactory dropping threshold, $\lambda_{threshold}$ depends on the confidence level required in the network and on the network distinctiveness such as network size and node density.

Destination node matches the two tables and if the difference in the total number of data packets sent by the source node and the total number of data packets received at the destination node within *check_time* duration is above the dropping threshold $\lambda_{threshold}$, then destination node compares the entries of its path table with the corresponding entries in the received path table. This way, it identifies the reliable routes through which data has been delivered without significant drop that is number of packets dropped are below dropping threshold, $\lambda_{threshold}$ and non-reliable route/routes through which the data loss has occurred more than $\lambda_{threshold}$. It is apparent that these identified non-reliable route/routes have one or more malicious nodes. Before adding all the nodes that belong to non-reliable routes to the accusation list, destination node first computes the reliability index of these nodes as given by Eq. (3). Reliability index computation results in a value that is used to determine how much reliable a node is and thus eliminating the need of activating IDS for monitoring of reliable nodes that come in non-reliable routes.

Reliability index of a node A is computed as:

$$R(A) = \sum_{i=1}^{i=r} \frac{N_i/I_i}{N} - \mu \sum_{j=1}^{j=nr} \frac{D_j/I_j}{N}, \qquad (3)$$

where r is the number of reliable routes containing node A as one of the intermediate node, nr is the number of non-reliable routes having node A, N_i is the number of data packets sent through reliable route i within *check_time* duration, D_j is the number of data packets dropped during transmission using non-reliable route j within *check_time* duration, I_i and I_j are the number of intermediate nodes in reliable route i and non-reliable route j respectively, N is total data packets sent in *check_time* duration and μ is a constant. Lesser the value of μ, more likely that PAMDS protocol detects any malicious behavior and higher the value of μ, more is the number of IDS nodes required to work in promiscuous mode resulting in more energy disbursement. Therefore, suitable value of μ is required to raise the probability of detecting truly misbehaving nodes by spending minimum amount of energy. For our simulation we chose the value of μ as 2, $\mu = 2$ in Eq. (3) signifies that for a node to be reliable, it should transmit more than double the number of packets dropped by it.

As from Eq. (3), reliability index of a node A, $R(A)$ lies in the range $-\mu$ to 1. A node having reliability index of 1 is highly reliable, that is, it only belongs to reliable routes. A node having reliability index of $-\mu$ is highly unreliable as it only belongs to non reliable routes. A suitable threshold value of reliability index (*reliability_threshold*) is chosen such that if a node has reliability index that lies between *reliability_threshold* and 1, then destination node does not add that node to the accusation list. Otherwise, it is added to the accusation list.

After building the accusation list, destination node sends this accusation list containing accused nodes to the source node using the most reliable route in its route table if it still exists otherwise uses the route formed by connected IDS nodes. On receiving accusation list, source node adds the nodes enclosed in the list to its primary accusation list.

When source node selects a route for the transmission of data packets, route is parsed for the presence of accused and malicious nodes before transmitting data. Source node proceeds according to the following conditions:

1. If route contains accused node/nodes then the IDS nodes near the accussed nodes are switched to work in promiscuous listening mode for monitoring and analyzing the forwarding behavior of accused nodes. Packets are transmitted between the intended source destination pair and if any of the accused nodes is found to be dropping packets in excess of the pre-established dropping threshold, $\lambda_{threshold}$, the monitoring IDS node sends this information to the source node. IDS node

then switches OFF its promiscuous listening mode. Source node removes malicious node from the primary accusation list and moves it to the malicious list.

2. If any of the nodes in the route belongs to the malicious list then that route is dumped and removed from the source cache. Source node selects a new route from its cache.
3. If route is free from accused and malicious nodes, packets are transmitted between the intended source destination pair and in this case, promiscuous listening mode of IDS nodes remains OFF.

If the nodes in the accusation list belong to the current active route then the malicious node/nodes can be detected without significant delay as it is most likely that the source node selects the same route for transmitting data. The requisite IDS nodes work in the promiscuous listening mode only after the detection of the attack. This saves energy of the battery powered mobile devices.

In a network where nodes' speed is slow, route selected for data transmission during *check_time* interval may not change. PAMDS protocol forces the source node to change the route if destination node detects misbehavior in data forwarding during *check_time* interval. In this way, PAMDS protocol responds quickly in detecting and segregating malicious nodes thus strengthening the network security.

Initially, when the network is set up, the nodes of the selected IDS set has enough energy to run the IDS, cover the entire network, the set is small in size and nodes are connected to each other. At this time, the malicious list is empty but after first data transmission phase, destination classifies the suspected nodes and suspected nodes will be added to malicious nodes if found to be misbehaving during data transfer. The malicious list grows with time. If reliability index of an IDS node (node as a part of the route) as computed by the destination node is below the *reliability_threshold*, then it is further monitored by their neighboring IDS. The mechanism does not check the reliability index of the nodes directly before IDS selection procedure. However, a node is not selected as IDS if it belongs to malicious list during IDS selection procedure as mentioned in Sect. 3.3.1. In the initial stage, a malevolent node may be selected as an IDS but will be detected soon by its neighboring IDS as soon as it starts misbehaving.

PAMDS protocol detects and avoids collaborative attacks. As collaborative attacks are induced by set of malicious nodes, they occur when in order to disturb the network, more than one colluding nodes collaborate with each other. In the proposed protocol, destination node first identifies the nodes which are suspected as malicious nodes. IDS nodes which are active during data transmission phase have optimized locations such that they are placed in the vicinity of each accused node (suspected node). Each IDS node is able to examine the local data to identify intrusion and hence detect attacks induced by multiple nodes.

Cryptographic methods used for making MANETs secure are: symmetric key and asymmetric key methods. The same key is used for encryption and decryption in symmetric key cryptography method. Asymmetric key cryptography method uses different keys for encryption and decryption. Cryptographic methods result in more processing and computational overhead and hence are computationally complex and expensive. The security mechanism used in the PAMDS protocol is much more effective in terms of computational complexity as in MANETs, the security mechanism needs to detect the misbehaving nodes during data transmission. It is not as expensive and complex as cryptographic methods. Secure routing protocols become less scalable and less energy efficient while considering the overhead and latency brought in by the cryptographic methods. The cost of implementation of cryptographic techniques is another major drawback.

3.3.3 PAMDS protocol algorithm

Algorithm 1 shows the execution flow of the PAMDS protocol.

Algorithm 1 Algorithm to show the execution flow of the PAMDS protocol

```
1:  if (source node) then
2:    if (has data to send) then
3:      Set t = source node clock time
4:      Execute route discovery procedure
5:      Select IDS nodes
6:      Source selects a route to destination from its cache
7:      if (no route to destination exists in its cache) then
8:        Go to step 4
9:      end if
10:     if (route contains nodes belonging to malicious list) then
11:       Remove route from its cache
12:       Go to step 6
13:     end if
14:     if (route contains nodes belonging to primary accusation list) then
15:       IDS nodes near to accused nodes are switched ON to work in the promiscuous listening mode
16:     end if
17:     if ((current source node clock time - t) mod $check\_time$ == 0) then
18:       Send path table
19:     end if
20:     Transmit the data packet
21:     Make entry in the path table
22:     go to step 6
23:   end if
24:   if (receives accusation list OR malicious list) then
25:     if (receives accusation list) then
26:       Update primary accusation list
27:     end if
28:     if (receives malicious information) then
29:       Update malicious list and primary accusation list
30:     end if
31:     if (end of data) then
32:       do nothing
33:     else
34:       go to step 6
35:     end if
36:   end if
37:   if  (receives RERR) then
38:     go to step 6
39:   end if
40: end if
41: if (Intermediate node) then
42:   Forward all the packets to the next neighbor
43:   if (detects link break) then
44:     Generate and send RERR to source
45:   end if
46: end if
47: if (IDS node) then
48:   if (promiscuous listening mode == ON) then
49:     Monitor forwarding behavior of its neighbors
50:     if (detected forwarding misbehavior) then
51:       Create packet to contain malicious information and send it to the source
52:       Set its own promiscuous listening mode == OFF
53:     end if
54:   end if
55: end if
56: if (Destination node) then
57:   if (receives data packet) then
58:     Make entry in the path table
59:   end if
60:   if (receives path table) then
61:     Compute Diff = Total no. of packets sent by source-Total no. of packets received
62:     if (Diff > $\lambda_{threshold}$) then
63:       Compare the two path tables to identify reliable and non reliable routes
64:       Select a node A that belongs to non reliable route but does not belong to accusation list
65:       Compute reliability index $R(A)$ for node A belonging to non reliable route
66:       if ($R(A)$ <= 0) then
67:         Add node A to accusation list
68:         if ($R(A)$ of all nodes belonging to non reliable routes is computed) then
69:           Create and send accusation list to source
70:         else
71:           Go to step 64
72:         end if
73:       end if
74:     end if
75:   end if
76: end if
```

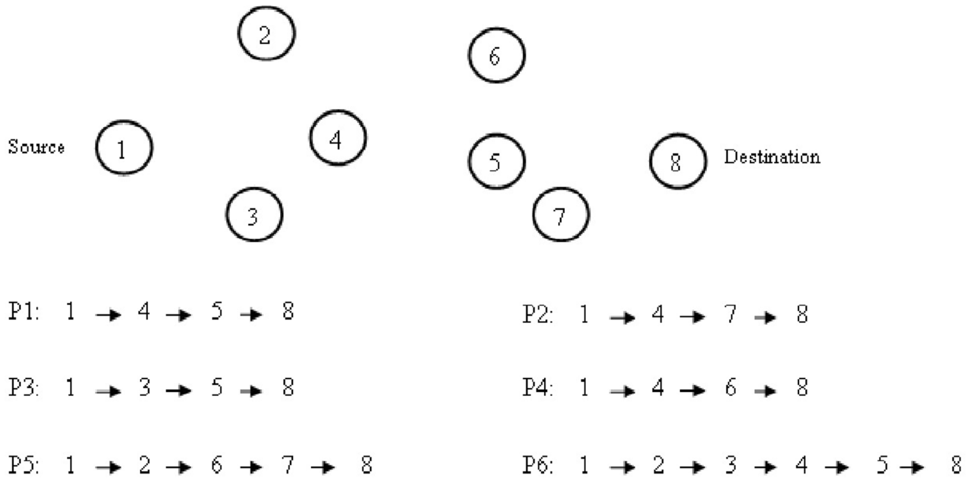

Fig. 1 Routes selected for data transmission from source node 1 to destination node 8

Table 1 Path table maintained by source node 1

Route	Packets
P1	30
P2	30
P3	40
P4	50
P5	20
P6	30
Total packets sent	200

Table 2 Path table maintained by destination node 8

Route	Packets
P1	27
P2	27
P3	30
P4	09
P5	10
P6	27
Total packets received	130

3.3.4 Illustration

Figure 1 depicts a network scenario wherein source node 1 intends to send data packets to destination node 8. After the route discovery phase, source node 1 sends data packets to node 8 through a selected route. Let the *check_time* duration be 15 s. As the network has dynamic topology, data packets follow routes P1, P2, P3, P4, P5 and P6 for transmission within 15 s. At a time, one of the routes amongst P1, P2, P3, P4, P5 or P6 is used. Source node 1 maintains a path table shown in Table 1 which contains the routes selected during the transmission along with the number of data packets transmitted via them. Destination node 8 also maintains a corresponding path table shown in Table 2 containing the routes beside the number of data packets received through them. After every 15 s, source node 1 sends its path table to the destination node. Let the dropping threshold $\lambda_{threshold}$ for this illustration be 20%. As shown in Table 1, source node 1 sends 200 data packets to destination node in 15 s. Therefore, $\lambda_{threshold}$ is 40 data packets.

As shown in the two path tables, the difference in the number of data packets sent by the source node and data packets received at the destination node is not within the acceptable range in *check_time* duration (difference of 70 data packets). Destination node 8 compares the entries of its path table with the corresponding entries in the received path table. It identifies that routes P1, P2 and P6 are reliable routes and routes P3, P4 and P5 are not reliable as the difference in the data packets sent by the source node and received by the destination node through routes P3, P4 and P5 exceeds the dropping threshold (drop more than 20% data packets sent to them for forwarding). So, routes P3, P4 and P5 may have malicious nodes.

Destination node computes the reliability index of all the nodes that belong to non-reliable routes P3, P4 and P5 using Eq. (3). Reliability indexes of nodes 2, 3, 4, 5, 6 and 7 come out to be 0.00041667, −0.01625, −0.03625, 0.05125, −0.27166667, 0.03416667, respectively. *reliability_threshold* for this example is considered to be 0. The reliability indexes of nodes 2, 5 and 7 are above the *reliability_threshold* ($R(A) > 0$) and hence, they are not put into the accusation list and nodes 3, 4 and 6 are put into the accusation list. This method reduces the length of the accusation list and there by saves the energy of the IDS nodes as less number of IDS nodes are now required to work in promiscuous mode. Destination node then sends this accusation list to the source node through routes P1, P2 or P6 if any one of them still exists otherwise sends the accusation list through connected IDS nodes. Source node on receiving the accusation list from the destination node, adds nodes contained in the received list to the primary accusation list.

When source node selects a route for the transmission of data packets, if the selected route contains nodes 3, 4 or 6, then the IDS nodes near the accused node/s in the route are operated in promiscuous listening mode for monitoring and analyzing the forwarding behavior of the accused node/s. Monitoring IDS sends information about any misbehaving node to the source node and source node 1 then removes these nodes from the primary accusation list and put them into the malicious list.

4 Simulation results and analysis

The simulation tool Network Simulator-2 (2016) is used to perform simulations in various scenarios to evaluate the performance of PAMDS protocol. NS-2 contains an energy model that notifies a node regarding its instantaneous energy level. The simulation parameters are listed in Table 3. In order to utilize energy model in PAMDS, the four energy parameters namely, initial energy, transmission power (txPower), reception power (rxPower) and idlePower along with their simulation values are mentioned in Table 3.

Table 3 Simulation parameters

Parameter	Simulation value
Simulator	NS-2.34
Simulation time	520 s
Simulation area	1500 m × 1500 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	5 Kbps
Packet size	512 bytes
Maximum malicious nodes	5
Dropping threshold $\lambda_{threshold}$	15 and 20%
reliability_threshold	0
Constant μ	2
α	Ranges from 20 to 30%
β	15%
check_time duration	8 s
Initial energy	250 J
rxPower	1.0 W
txPower	1.5 W
IdlePower	0.1 W

Each node is allocated with an initial energy of 250 J. The energy of a node gets reduce as the node transmits or receives packets. The nodes working in promiscuous listening mode consume more energy due to overhearing of packets. To measure the amount of energy consumed in transmission of a packet, the transmission power (txPower) is multiplied by the time require to transmit a packet (packet size/bandwidth), and to measure the amount of energy consumed in reception of a packet, the reception power (rxPower) is multiplied by the time require in receiving a packet (packet size/bandwidth). To evaluate the performance of PAMDS routing protocol, two scenarios are created in NS-2: performance of the protocols under different nodes' speed and performance of the protocols by inducing varying number of malicious nodes in the network.

In simulations, we compare the performance of PAMDS with the standard DSR protocol, MDSR protocol proposed by Mohanapriya and Krishnamurthi (2014) and PACE-DSR (Ghander and Shaaban 2015). The reasons for selecting MDSR and PACE-DSR for comparison are: firstly, PAMDS, MDSR and PACE-DSR use DSR protocol as their underlying routing protocol. Secondly, all these aforementioned protocols are designed for the detection and removal of nodes inducing packet forwarding misbehavior attack. Thirdly, the approaches used in these protocols claim for selection of most reliable path while maintaining the network energy usage. Fourth reason is that these all protocols use monitoring mechanism for the detection of routing misbehavior and all use non-cryptographic methods to enforce security in the network.

To implement PACE method with DSR protocol (PACE-DSR), one additional parameter *residualEnergy* is added to original *Path* class in NS-2 simulator. This class contains node IDs that form the routes in the source node, and *residualEnergy* parameter that contains the remaining energy of every node in the list of nodes creating the route in the source node.

Figure 2 offers the number of IDS nodes that operate in promiscuous listening mode at different times and

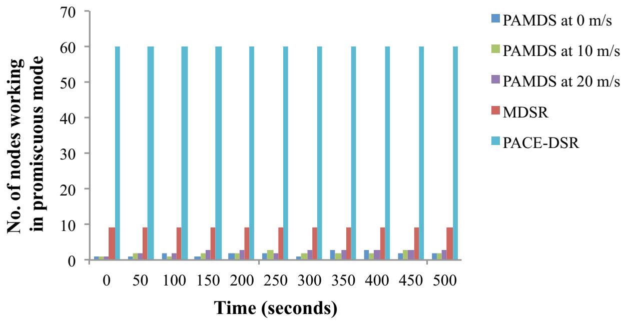

Fig. 2 Number of nodes operating in promiscuous listening mode at different times

at different nodes' mobility. As depicted from the figure, PACE-DSR requires all 60 nodes of the network to work in promiscuous listening mode and MDSR requires nine IDS nodes all the time in a network size of 60 nodes to constantly work in promiscuous listening mode. In contrast to this, the average number of nodes that are required to work in promiscuous listening mode to catch the nodes inducing packet dropping misconduct in the network of the same size in PAMDS operating at $\lambda_{threshold} = 15\%$ and $\mu = 2$ are 2, 2 and 3 at node mobility of 0, 10 and 20 m/s, respectively. This reduction in the number of IDS nodes lessens the consumption of nodes energy as compared to methods used in PACE-DSR and MDSR and consequently increases the existence of the network as shown in Fig. 9.

Figure 3 shows the packet delivery ratio (PDR) percentage at different nodes' speed for a network size of 60 nodes and out of 60 nodes, five nodes are malicious. PDR using the proposed scheme, PAMDS is higher than the MDSR, PACE-DSR and DSR under attack. PAMDS is simulated at μ =2 and at two different values of packet dropping threshold percentage, $\lambda_{threshold}$. Reducing the $\lambda_{threshold}$ from 20 to 15% further improves the PDR. The mean value of PDR %age for PAMDS at $\lambda_{threshold}$ = 15% is 94.784 and at $\lambda_{threshold}$ = 20% is 93.774. Hence the mean value of the PDR %age at both of the dropping threshold values is higher than the mean value of PDR %age for DSR under attack (=58.95) and MDSR (=89.186). The proposed protocol selects a new route immediately after the detection of misbehaving node; this is why PDR of PAMDS protocol is higher when compared to that of MDSR and DSR under attack. PDR %age of PACE-DSR (=94.216) is only 0.067 % less than that of PAMDS as in PACE-DSR, all the nodes persistently work in promiscuous listening mode all the time to catch the misbehaving nodes. Further, the standard deviation in PDR %age for PAMDS protocol at $\lambda_{threshold}$ = 15% is 0.99809, for PAMDS protocol at $\lambda_{threshold}$ = 20% is 0.82347, for DSR is 0.3210856, for DSR under attack is 6.503675884, for PACE-DSR it is 1.13 and MDSR has 2.870774.

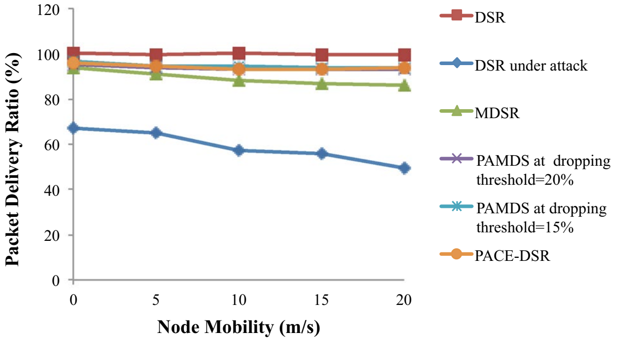

Fig. 3 Packet delivery ratio (PDR) percentage at different nodes' speed

Figure 4 represents PDR percentage for varying number of malicious nodes. Protocols are simulated at nodes' mobility of 20 m/s and PAMDS has been observed for two different values of $\lambda_{threshold}$. Figure shows that the PDR %age of DSR falls drastically from 99.79 to 49.23% and PDR %age of MDSR reduces from 99.34 to 86.08%, while 5 malicious are introduced into the network. In contrast to these, for same number of malicious nodes, the PDR for our protocol reduces from 99.38 to 93.69% and PDR %age of PACE-DSR reduces from 99.36 to 93.84%.

Figure 5 depicts the total packet loss percentage v/s varying nodes' speed.The total packet loss percentage of DSR under attack is highest (mean value 41.05) as no scheme for the detection and isolation of misbehaving nodes is employed. The total packet loss percentage of MDSR is higher than the proposed protocol when compared at two different values of $\lambda_{threshold}$. The mean value of total packet loss percentage of MDSR is 10.814 and that of PAMDS is 5.216 at $\lambda_{threshold}$ = 15% and is 6.226 at $\lambda_{threshold}$ = 20%. The mean value of total packet loss percentage using PACE-DSR (=5.784) is higher than PAMDS at $\lambda_{threshold}$ = 15%.

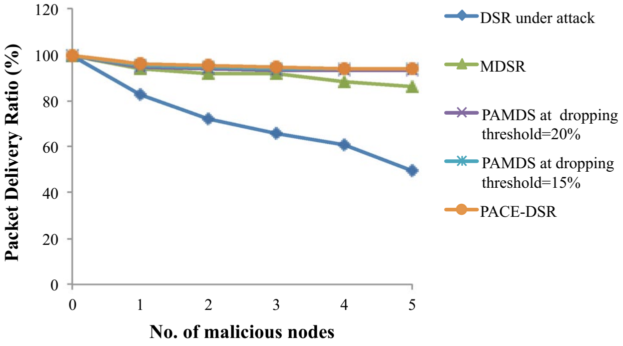

Fig. 4 Packet delivery ratio (PDR) percentage for varying number of malicious nodes

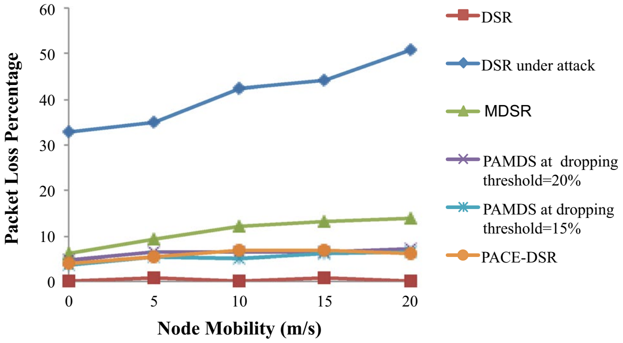

Fig. 5 Packet loss percentage at different nodes' speeds

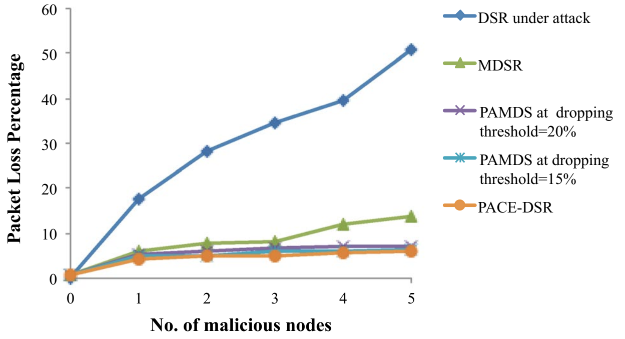

Fig. 6 Packet loss percentage for varying number of malicious nodes

The total packet loss percentage for a network having varying number of malicious nodes at nodes' mobility of 20 m/s is shown in Fig. 6. In the absence of malicious nodes, the mean packet loss percentage using standard DSR protocol is about 0.21%; it rises sharply to 50.77%, when five malicious nodes are introduced in the network. With the deployment of IDS in MDSR, PAMDS and PACE-DSR protocol, the packet loss percentage reduces to 13.92, 6.675 and 6.16%, respectively.

Figure 7 shows control packet overhead at varying nodes' speed. The number of control packets required to implement MDSR is highest as compared to DSR, PACE-DSR and PAMDS as MDSR uses extra control packets (QREQ, QREP, MNREQ and ALARM packets) for the detection and isolation of malicious nodes. Control packet overhead using PACE-DSR is higher when compared to DSR and PAMDS, this is because of the fact that PACE-DSR deploys monitoring mechanism at all the network nodes. All nodes create faulty list and broadcast this list in the network. Broadcasting produces unwanted routing messages and hence increases the packet overhead. Control packets required to implement PAMDS is higher than that of DSR because of the fact that DSR is not secure and hence, does not require any control packets for executing security measures. Control packet overhead of PAMDS at $\lambda_{threshold}$ = 15% is more than that of PAMDS at $\lambda_{threshold}$ = 20%. This is due to the fact that at lesser value of $\lambda_{threshold}$, the protocol becomes more stringent and requires more number of IDS for monitoring, which increases the number of control packets that are sent from IDS nodes to the source node. PAMDS protocol has 46.6% less control packet overhead (mean value of 0.173908139 at $\lambda_{threshold}$ = 15% and is 0.141910046 at $\lambda_{threshold}$ = 20%) when compared to MDSR (mean value of 0.295678743) and has 37.9% less control packet overhead as compared to PACE-DSR. In PAMDS, source node does not select the path for transmission having malicious node. In this way, malicious nodes are isolated from the network without requiring extra control packets.

Figure 8 shows average end to end delay of PAMDS at $\lambda_{threshold}$ of 15 and 20%, MDSR, PACE-DSR and DSR protocol. MDSR requires transmission of at least two data blocks to detect and then isolate a gray hole node, delaying the detection and isolation process. In PACE-DSR rediscovery of the routes is required for the isolation of misbehaving nodes which increases the average latency. Average end to end delay of PAMDS is 16.13 and 15.53% less than that of MDSR and PACE-DSR respectively. PAMDS chooses secure route without malicious nodes for data transmission. This divergence from the routes selected by DSR leads to a lift in the average end to end delay when compared with the standard DSR protocol as revealed in the figure.

Average residual energy of the network nodes at different times at fixed nodes' speed of 15 m/s for PAMDS, PACE-DSR, DSR and MDSR is shown in Fig. 9. MDSR employs the same IDS nodes that are operational during the network lifetime. Hence, the energy of the selected IDS nodes is consumed fast and after some time IDS nodes become energy deficient and dead. In PACE-DSR, all the nodes are required to persistently work in promiscuous listening mode in order to listen all routing packets within its transmission range. As discussed before, In PACE-DSR, monitoring nodes inform the other network

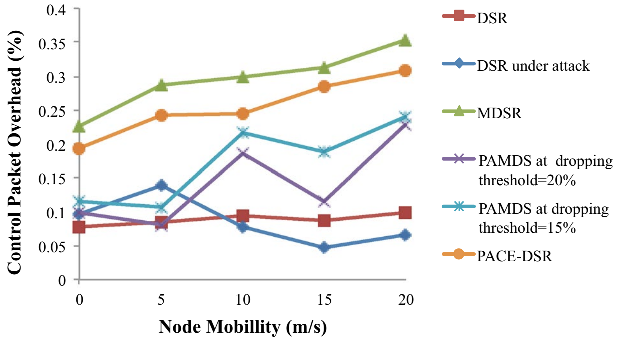

Fig. 7 Control packet overhead at varying nodes' speed

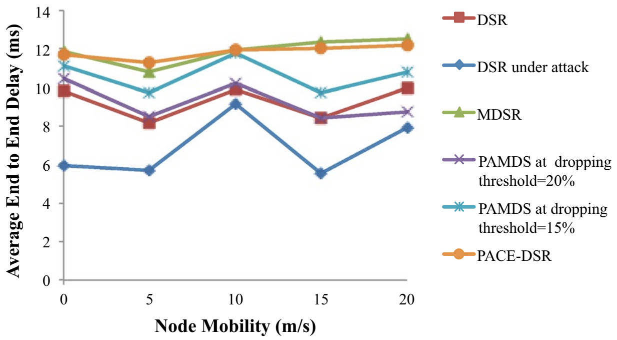

Fig. 8 Average end to end delay at varying nodes' speed

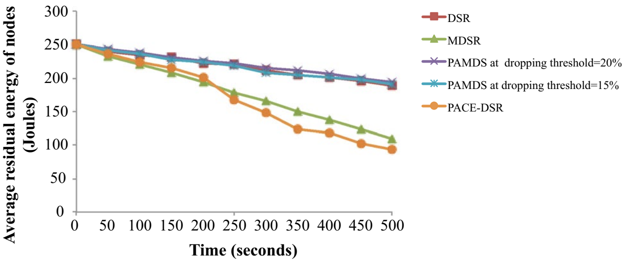

Fig. 9 Average residual energy of the network nodes at different times

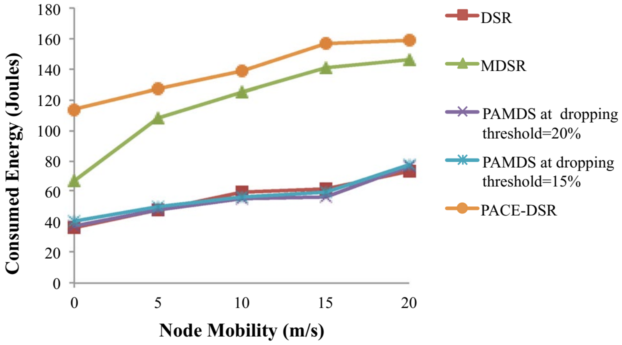

Fig. 10 Average energy consumption of network nodes at different nodes' speed

nodes about the misbehaving nodes through broadcasting. Broadcasting and promiscuous listening mode cause more nodes' battery power consumption spent on hearing these messages. MDSR (mean value of average residual energy at different times = 179.36 J) has 18.49% less average residual energy as compared to PAMDS protocol (mean value of average residual energy at different times = 220.045 J). PAMDS protocol (mean value of energy consumption at different times = 29.95 J) on an average consumes 57.6 and 62.04% less energy when compared with MDSR (average energy consumption = 70.64 J) and PACE-DSR (average energy consumption = 78.9 J), respectively. Thus PAMDS protocol proves to be more power conscious.

The average network energy consumption at varying nodes' speed is represented in Fig. 10. As seen from the Figure that PAMDS protocol begins to consume more power as compared to standard DSR protocol when nodes' speed is increased from 15 m/s to 20 m/s. On taking an average of network energy consumption at different nodes' speed, the standard DSR protocol consumes 0.042% less energy as compared to PAMDS protocol. PAMDS protocol consumes 52.74 and 60.09% less power than MDSR and PACE-DSR respectively.

Figure 11 shows the total energy consumption of different network nodes. As depicted from the figure, MDSR fixes nine out of sixty network nodes to work in promiscuous listening mode. The energy of these nodes consumes faster than the other network nodes. The proposed protocol, PAMDS ensures distributed loss of energy. Hence, prevents any node from becoming energy deficient. The standard deviation of consumed energy using DSR protocol, MDSR, PAMDS at $\lambda_{threshold}$ of 15%, PAMDS at $\lambda_{threshold}$ of 20% and PACE-DSR is 4.836, 35.423, 6.357252674, 7.247737599 and 25.94055733, respectively. MDSR fails to detect any malicious node after 400 s as some of the IDS nodes become energy deficient (i.e. remaining energy become less than 21 J) and are not able to function and execute detection procedure.

It can be observed from Figs. 3, 4, 5 and 6 that PACE-DSR protocol shows good performance in terms of PDR percentage and packet loss percentage but as shown in Figs. 7, 8, 9, 10 and 11, the performance of PACE-DSR degrades in terms packet overhead, average end to end delay and power consumption.

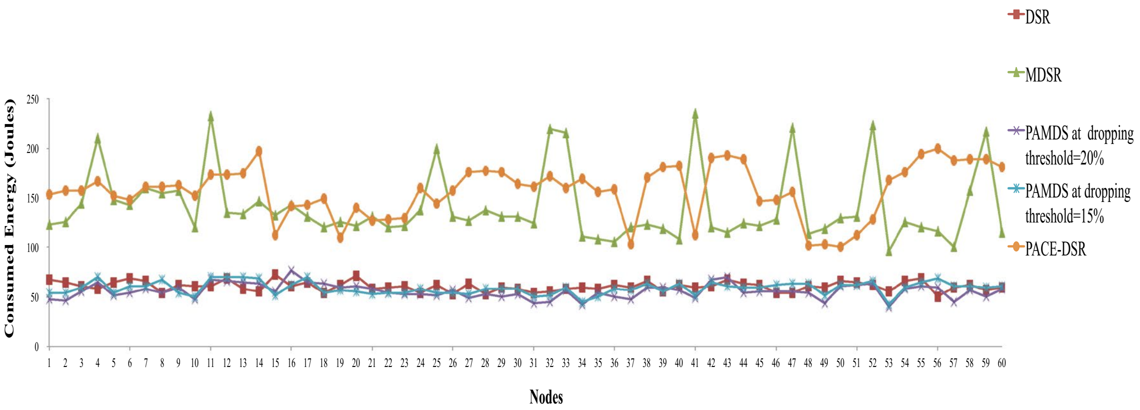

Fig. 11 Total energy consumption of network nodes

5 Conclusion and future scope

A secure routing protocol is proposed for the detection and isolation of nodes exhibiting packet forwarding misbehavior attack by deploying IDS. The new protocol gives prominence on security and power saving of the battery operated mobile devices and consequently useful in an ad hoc environment wherein security is an essential requisite and energy is a vital resource. Simulations show that the proposed protocol isolates the malicious nodes and hence degrades the packet loss ratio without increasing the computational complexity and the network overhead as it is non cryptographic. In future, we can extend our work to detect and circumvent other MANET security attacks. The work can also be modified to make other existing reactive routing protocols secure.

References

Ahila E, Chitra K (2014) Security based energy efficient routing protocol for adhoc network. In: Proceedings of IEEE international conference on control, instrumentation, communication and computational technologies (ICCICCT), pp 1522–1526. ISBN: 978-1-4799-4191-9

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. doi:10.1007/s11235-015-0068-8

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

Banergee S (2008) Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. In: Proceedings of the world congress on engineering and computer science (WCECS 2008), WCECS, San Francisco, USA, pp 337–342. ISBN: 978-988-98671-0-2

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: Proceedings of IEEE applications and innovations in mobile computing (AIMoC), pp 157–164. doi:10.1109/AIMOC.2014.6785535. ISBN: 978-1-4799-3881-0

Buchegger S, Boudec J Y L (2002) Performance analysis of the CONFIDANT protocol. In: Proceedings of 3rd ACM international symposium on mobile ad hoc networking and computing (MobiHoc ’02), Lausanne, Switzerland, pp 226–236. doi:10.1145/513800.513828. ISBN: 1-58113-501-7

Cano J C, Kim D (2002) Investigating performance of power-aware routing protocols for mobile ad-hoc networks. In: Proceedings of the international workshop on mobility and wireless access (MobiWac 2002), IEEE Computer Society, Washington, DC, USA, pp 80–86. doi:10.1109/MOBWAC.2002.1166956. ISBN: 0-7695-1843-5

Dhurandher S K, Woungang I, Traore I (2014) C-SCAN: an energy-efficient network layer security protocol for mobile ad hoc networks. In: Proceedings of 28th IEEE international conference on advanced information networking and applications workshops (WAINA), pp 530–535. doi:10.1109/WAINA.2014.85. ISBN: 978-1-4799-2654-1

Estahbanati M M, Rasti M, Hamami S M S (2014) A mobile ad hoc network routing based on energy and Markov chain trust. In: Proceedings of IEEE 7th international symposium on telecommunications (IST), pp 596–601. doi:10.1109/ISTEL.2014.7000775

Ghander A, Shaaban E (2015) Power aware cooperation enforcement MANET routing protocols. Procedia Comput Sci 73:162–171. doi:10.1016/j.procs.2015.12.062

Gong P, Chen TM, Xu Q (2015) ETARP: An energy efficient trust-aware routing protocol for wireless sensor networks. J Sens. doi:10.1155/2015/469793

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

Heena, Kumar N (2014) Battery power and trust based routing strategy for MANET. In: Proceedings of IEEE international conference on advanced communication control and computing technologies (ICACCCT), pp 1559–1562. doi:10.1109/ICACCCT.2014.7019368. ISBN: 978-1-4799-3915-2

Hu YC, Johnson DB, Perrig A (2003) SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Netw 1:175–192. doi:10.1016/S1570-8705(03)00019-2

Hu YC, Perrig A, Johnson DB (2005) Ariadne: a secure on-demand routing protocol for ad hoc networks. Wirel Netw 11:38. doi:10.1007/s11276-004-4744-y

Jain H R, Sharma S K (2014) Improved energy efficient secure multipath AODV routing protocol for MANET. In: Proceedings of IEEE international conference on advances in engineering and technology research (ICAETR), pp 1–9. doi:10.1109/ICAETR.2014.7012847

Johnson D B, Maltz D A (1996) Dynamic source routing in ad hoc wireless networks. In: Mobile computing, the Kluwer International series in engineering and computer science, vol 353, Springer, US, pp 153–218. doi:10.1007/978-0-585-29603-6_5. ISBN: 978-0-7923-9697-0

Li J, Cordes D, Zhang J (2005) Power-aware routing protocols in ad hoc wireless networks. IEEE Wirel Commun 12:69–81. doi:10.1109/MWC.2005.1561947

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: Proceedings of 2006 IEEE international conference on mobile adhoc and sensor systems (MASS), pp 199–205. doi:10.1109/MOBHOC.2006.278557. ISBN: 1-4244-0506-8

Lu Y, Zhong Y, Bhargava B (2003) Packet loss in mobile ad hoc networks. Computer Science Technical Reports, Paper 1558, Department of Computer Science, Purdue University. Report Number: 03-009. http://docs.lib.purdue.edu/cstech/1558

Marti S, Giuli T J, Lai K, Baker M (2000) Mitigating routing misbehavior in mobile ad hoc networks. In: Proceedings of sixth annual international conference on mobile computing and networking (MobiCom ’00), Boston, USA, pp 255–265. doi:10.1145/345910.345955. ISBN:1-58113-197-6

Misra S, Dhurandher SK, Obaidat MS, Gupta P, Verma K, Narula P (2010) An ant swarm-inspired energy-aware routing protocol for wireless ad-hoc networks. J Syst Softw 83:2188–2199. doi:10.1016/j.jss.2010.06.025

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. doi:10.1016/j.compeleceng.2013.06.001

Nadeem A, Howarth MP (2013) A survey of MANET intrusion detection and prevention approaches for network layer attacks. IEEE Commun Surv Tutor 15:2027–2045. doi:10.1109/SURV.2013.030713.00201

Network simulator 2 (NS–2). http://www.isi.edu/nsnam/ns/. Accessed 13 Nov 2016

Perrig A, Canetti R, Tygar J D, Song D (2000) Efficient authentication and signing of multicast streams over lossy channels. In:

Proceedings of IEEE symposium on security and privacy, Berleley, USA. doi:10.1109/SECPRI.2000.848446. ISBN: 1081-6011

Sarkar S, Datta R (2012) A trust based protocol for energy-efficient routing in self-organized MANETs. In: Proceedings of annual IEEE India Conference (INDICON), pp 1084–1089. doi:10.1109/INDCON.2012.6420778. ISBN: 978-1-4673-2270-6

Sarkar S, Datta R (2014) A secure and energy-efficient stochastic routing protocol for wireless mobile ad-hoc networks. In: Proceedings of IEEE twentieth national conference on communications (NCC), pp 1–6. doi:10.1109/NCC.2014.6811358. ISBN: 978-1-4799-2363-2

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. doi:10.1016/j.adhoc.2015.08.020

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. doi:10.1007/s11277-006-9217-4

Sridhar S, Baskaran R, Chandrasekar P (2013) Energy supported AODV (EN-AODV) for QoS routing in MANET, In: Proceedings of the 2nd international conference on integrated information (IC-ININFO 2012), Budapest, Hungary, vol 73 of Procedia—Social and Behavioral Sciences, pp 294–301. doi:10.1016/j.sbspro.2013.02.055

Su MY (2011) Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comput Commun 34:107–117. doi:10.1016/j.comcom.2010.08.007

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 India, pp 601–607. doi:10.1007/978-81-322-2126-5_65. ISBN: 978-81-322-2125-8

Tan S, Li X, Dong Q (2015) Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Netw 30:84–98. doi:10.1016/j.adhoc.2015.03.004

Vazifehdan J, Prasad RV, Onur E, Niemegeers I (2011) Energy-aware routing algorithms for wireless ad hoc networks with heterogeneous power supplies. Comput Netw 55:3256–3274. doi:10.1016/j.comnet.2011.06.015

Wang Y (2010) Study on energy conservation in MANET. J Netw 5:708–715

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. doi:10.1007/978-3-642-38027-3_55. ISBN: 978-3-642-38026-6

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. doi:10.1109/JSAC.2005.861384

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. doi:10.1109/WICOM.2007.403

Zapata MG (2002) Secure ad hoc on-demand distance vector routing. ACM SIGMOBILE Mobile Comput Commun 6:106–107. doi:10.1145/581291.581312

Zhang Y, Lee W (2005) Security in mobile ad-hoc networks. In: Ad hoc networks, pp 249–268. doi:10.1007/0-387-22690-7_9. ISBN: 978-0-387-22689-7