Wireless Pers Commun (2018) 101:2029–2052
https://doi.org/10.1007/s11277-018-5804-4

Trust Based Intrusion Detection Technique to Detect Selfish Nodes in Mobile Ad Hoc Networks

Sunil Kumar[1] · **Kamlesh Dutta**[1]

Published online: 18 May 2018

Abstract The applications and protocols conceived for mobile ad hoc networks rely on the assumption of cooperation amongst the mobile nodes because of lacking infrastructure. All nodes have to spend their precious resources (e.g. battery power, memory, computational power, and network bandwidth) for routing and packet forwarding operations for other nodes, in a cooperative way in the network. However, there are some nodes that may intentionally turn themselves to behave selfishly in order to conserve their valuable resources. The selfish behaviour of such nodes drastically reduces the desired degree of cooperation amongst the mobile nodes. Over the course of time, the non-cooperative activities of, such selfish nodes would paralyze the normal functioning of the whole network. Therefore, these types of nodes should be detected and isolated from the network, as soon as they begin to exhibit their selfish behaviour. In this paper, a dynamic trust based intrusion detection technique is presented to detect and isolate the selfish nodes from the network, where the direct trust degree based on direct communication interactions and indirect (recommended) trust degree based on the neighbours' recommendations are taking into account to accurately judge the selfishness nature of the nodes. The results obtained throughout the simulation experiments clearly show the feasibility and effectiveness of the proposed intrusion detection technique.

Keywords MANETs · AODV · Selfish nodes · Direct trust · Indirect trust · Energy consumption

✉ Sunil Kumar
sunilkaushik27@gmail.com

Kamlesh Dutta
kd@nith.ac.in

[1] Department of Computer Science and Engineering, National Institute of Technology, Hamirpur, Himachal Pradesh, India

1 Introduction

A mobile ad hoc network (MANET) is a group of heterogeneous mobile nodes that communicate over wireless links without any assistance of fixed infrastructure or centralized facility such as base stations or routers [1]. In MANETs, the mobile nodes are resource constrained in terms of the radio transmission range, memory size, battery and computational power. The communication among the mobile nodes can be done either using the single hop transmission or multi-hop transmissions with the assistance of intermediate nodes acting as routers to relay and forward the messages.

Due to non-requirement of backbone infrastructure facility and instantaneous deployment nature of mobile ad hoc networks, make them more appealing for wide applications in diverse domains such as military communication and operations, police and fire services, emergency search and rescue operations, disaster recovery, inter-vehicle networks (VANET), personal area networks (PANs), set up virtual classrooms or conference rooms, supporting doctors and nurses in hospitals etc. [2]. However, the multi-hop communication in MANETs causes a serious problem that a node may turn itself to behave selfishly by refraining from forwarding the packets for other nodes in order to conserve its valuable resources.

Since, the mobile nodes have to spend their valuable resources in routing and packet forwarding operations for other nodes without any benefit. In terms of power consumption, data transmission is the most expensive service in MANETs. Al-Karaki and Kamal [3] proved that the energy consumed by a mobile node to send a bit over 10 or 100 m distance is same to execute thousands to millions of arithmetic operations. Buttyan and Hubaux [4] showed on the basis of simulation that almost 80% of the transmission energy is consumed in packets forwarding when the average hops distance from a sender to a receiver is about to five. Therefore, some nodes turn themselves to behave selfishly while considering their limited resources, and reluctant to spend their resources for others. Basically, the selfish nodes attempt to utilize the network resources for their own benefits, but reluctant to spend their own resources in routing and packet forwarding operations for others.

If intermediate nodes in the network behave selfish and do not cooperate in forwarding the packets for other nodes, the communication beyond radio range would not possible. Over the course of time, the non-cooperative activities of, such selfish nodes would paralyze the normal functioning of the whole network. Therefore, these types of nodes should be detected and isolated from the network as soon as they begin to exhibit their selfish behaviour.

Significant efforts have been invested by the researchers towards the development of detection and mitigation techniques against selfish nodes (see details in Sect. 3). More recent work in [5] is a reputation based system for detecting and isolating the selfish nodes from mobile ad hoc networks. This approach evaluates the reputation of a node based on direct monitoring technique. However, direct monitoring based detection technique may overestimate the selfish behaviour of nodes due to the effects of radio transmission errors, congestion or packet collisions [6]. As a result, the availability of normal nodes may be reduced, and the overall performance of the network may be deteriorated.

In order to provide the reliable and secure communication over the mobile ad hoc networks against the selfish nodes, one natural idea is to develop a trust based intrusion detection technique that not only based on direct communication interactions but also based on neighbours' recommendations in order to accurately judge the selfishness nature of the nodes. According to Sun et al. [7], the detection rate of misbehaving nodes would be

greater when indirect and recommendation trust information is integrated with direct trust information. According to Jiang et al. [8], the trustworthiness of sensor nodes can be evaluated more effectively if direct trust value is integrated with indirect trust value. The mobile nodes would trust and support each other in the normal operation of the network on the basis of trusted relationships maintained among them.

The motivation behind the proposed detection technique in this paper is to detect and isolate the selfish nodes from the network, and minimize the possibility of overestimating the selfish behaviour of innocent nodes due to radio transmission errors, network congestion or packet collisions. Here each node determines the direct trust degree values of its one hop neighbours through analysing their direct communication transactions over a short period of time. The final trust degree value is computed dynamically by taking into account both direct and indirect (based on neighbours' recommendations) trust degree in order to acquire more accuracy in detecting the selfish nodes. The trust degree values are also used in the route discovery process as a constraint to elect the route free from the selfish nodes for data transmission. The primary contributions of this paper are summarized:

- An efficient intrusion detection technique based on direct trust and indirect trust degree values that detects the selfish nodes within a very short time as they begin to exhibit their anomalous behaviour, thereby isolating them from the normal functioning of the network.
- An effective mechanism to measure the trust degree value of nodes by employing multiple parameters rather than a single parameter.
- This detection technique confines the impact of the selfish node over the network by its one hop neighbours such that no route packet is forwarded through or from it during the route discovery procedure. The selfish nodes are also denied to access the network resources.
- In addition to assessment of trust degree value, the residual energy of a node is also estimated in order to detect those nodes which turn their behaviour selfishly by dropping the packets according to their residual energy.
- The proposed detection scheme is adapted to frequent changes in the network topology and produces little overhead over the network.

In this paper, ad hoc on demand distance vector (AODV) [9] is considered to apply our proposed intrusion detection technique, because it is one of the best and commonly used reactive routing protocols. However, the proposed scheme can be applied to other routing protocols in similar fashion.

The results obtained throughout the simulation experiments clearly show that the proposed intrusion detection technique is practical to improve the packet delivery ratio and reduce average end-to-end delay, and capable to alleviate the impact of selfish nodes from the network. The rest of the paper is structured as follows. Section 2 briefly describes the functioning of selfish nodes. Section 3 summarizes the related work. In Sect. 4, the relevant elements of the proposed detection technique and methodology are described. In Sect. 5, the experimental design and simulation results are presented. Finally, Sect. 6 concludes the proposed detection technique and provides the directions to future work.

2 Selfish Nodes

On the basis of simulation experiments, Michiardi and Molva [10] stated that the security of MANETs can be exposed by two types of misbehaving nodes: selfish node and malicious node. A selfish node attempts to utilize the network resources for its own benefits, but

reluctant to spend its resources for others. The probability of a node to act as selfish would be lower when it has more energy and higher when it has low energy and sufficient number of one hop neighbours. A selfish node can exhibit its selfish behaviour in the following ways:

(a) Type 1—these types of selfish nodes participate in route discovery process but don't forward the data messages (i.e. drop the packets)intentionally for other nodes.
(b) Type 2—these selfish nodes neither participate in route discovery process (i.e. drop the routing packets) nor forward the data packets.
(c) Type 3—these selfish nodes forward the routing messages with a delay near to upper limit of timeout in order to avoid being the active member of the route for others [11].
(d) Type 4—these selfish nodes may turn their behaviour selfish by dropping the packets according to their residual energy [12].

Kargl et al. [13] investigated the effect of selfish nodes in MANETs with 50 mobile nodes in the networks, and experienced that the packet delivery ratio is decreased by 50% when all the 50 nodes behave as selfish. Yoo et al. [14] showed that the packet delivery ratio is decreased from 80 to 30% with increasing the selfish nodes from 0 to 50%. Yoo and Agrawal [15] analyzed the packet delivery rate against the ratio of selfish nodes, and experienced that delivery rate is no more than 27.19% with 50% selfish nodes. Toh et al. [16] showed that the number of packet losses in mobile ad hoc networks is increased by 50% with increasing the proportion of selfish nodes from 0 to 40%. Gupta et al. [17] examined the effects of selfish nodes on the performance of mobile ad hoc networks with increasing the proportion of selfish nodes from 10 to 100%. They noticed on the basis experiment analysis that the network has 60% percentage of packet dropped, a decrease in throughput by 30% and an increase in average hop count by 2.5 times in the presence of 90 percentages of selfish nodes. Hence, the presence of selfish nodes in a network results in network partitioning, data unavailability, and hampers the performance metrics such as throughput, packet delivery ratio etc. The degree of impact of the selfish nodes differs significantly according to the number of selfish nodes and other parameters used.

3 Related Work

Significant efforts have been invested by the research community towards the development of detection and counteracting techniques against the selfish nodes in MANETs.

Hern´andez-Orallo et al. [19] used the cooperative watchdog mechanism [18] to motivate the different watchdogs to operate in cooperative fashion to reduce the detection time for selfish nodes. The detection accuracy of this scheme is affected due to presence of ambiguous collisions, receiver collisions, noisy channel, and limited transmission power. Ferraz et al. [20] proposed Trust-based Exclusion Access control Mechanism (TEAM), where trust values collected by one hop neighbours at local context are passed to the global context, consisting of jury nodes to further evaluate the behaviour of a suspected node. The trustworthiness of jury nodes must be assured and reliability of the relative information provided by them should be validated.

Rodriguez-Mayolet and Gozalvez [6] implemented three techniques [reset activity mode (RAM), warning mode (WM) and reset failure mode (RFM)] together with Marti's

protocol [18] and TEAM protocol [20] in order to minimize the incorrect accusations created due to radio transmission errors and packet collisions in network.

The routing protocols with requisite modification have been presented by the researchers to encourage the cooperation amongst the participating mobile nodes, and isolate or discourage the selfish behaviours of participating nodes [21–23]. Shakashuki et al. [21] proposed an IDS named Enhanced Adaptive ACKnowledgment (EAACK) to handle the weaknesses of Watchdog EAACK which relies on end to end ACK, as well as on Secure ACK (S-ACK) to detect the misbehaving nodes in the network. But, this approach increases the computational overhead due to employment of Digital signature and traditional cryptography. Djenouri et al. [22] presented an optimization technique based on the two-hop ACK to alleviate the impact of selfish nodes where each node requests its two hop neighbour to send back an ACK, randomly. This technique is unable to distinguish who is the malicious/selfish node (next hop or the requested node) when the requested node fails to send back an ACK. Miranda and Rodrigues [23] proposed a scheme with an aim to ensure the balanced consumption of the resources as well as discourage the selfish behaviours where every node advertises three sets of node IDs: Friends nodes (to which advertiser node is willing to provide service), Foes nodes (to which advertiser node not provide any service) and Selfish nodes (regarded as foes nodes). This scheme requires a large memory space in order to keep the details of friends, foes and selfish lists of other mobile nodes.

Kargl et al. [13] proposed a mechanism named Mobile Intrusion Detection System (MobIDS), where a node monitors the activities of others nodes, and assign positive values to cooperative nodes and negative value to non-cooperating nodes in order to detect selfish Nodes. However, this scheme fails to distinguish between the real non-cooperative nodes (selfish nodes) and non-cooperative nodes due to low battery power.

Some approaches have been proposed by the researchers by deploying a traditional credit system to encourage the cooperative behaviour among the nodes [24–28]. Das [24] proposed a credit-based system where incentives are delivered to nodes on cooperative behaviour. Demir and Comaniciu [25] incorporated the mechanism of traditional auctions and credit in the AODV routing protocol to mitigate the effects of selfish nodes. Wang et al. [26] developed an efficient incentive scheme to persuade the cooperative behaviours. Soltanali et al. [27] also presented a combined approach of reputation and incentives to encourage the cooperation among the participating nodes in MANETs. A similar technique named Token Based Umpiring Technique (TBUT) is presented in [28] where a token is required for every node in order to participate in the basic functioning of routing and communication in the network. These credit-based schemes require the virtual currency as a form of reward to nodes that co-operate in packet forwarding activities in the network. These schemes suffer from additional computational overheads due to maintaining the virtual currency transactions.

In [12, 29, 30], the defensive approaches based on statistical analysis have been proposed to study the cooperative behaviour and selfish behaviours of the participating mobile nodes. An exponential reliability coefficient based reputation mechanism (ERCRM) [12] is presented for isolating the selfish nodes in MANETs. Sengathir and Manoharan [29] implemented a semi-Markov process based cooperation enforcement model (SMPCEM) by investigating the network survivability parameters such as residual energy and packet delivery rate. They also presented a futuristic trust based coefficient based semi Markov prediction model (FTCPM) for mitigating the effects of selfish nodes in the networks [30]. These techniques require accurate statistical distributions; otherwise can lead to high false

alarms due to their inability to quickly adapt to legitimate changes in the system's operation and user's activities over the time.

Some secure schemes based on game theory have been proposed to encourage the cooperative behaviour and discourage selfish behaviours of the participating mobile nodes [31–36], Kaliappan and Paramasivan [31] proposed a secure routing protocol using Dynamic Bayesian Signaling Game model (SRPDBG) to study the strategy profile for normal and malicious nodes. Mao and Zhu [32] used the game theory to develop an energy-aware routing protocol to mitigate the effects of selfish nodes. Das et al. [33] proposed a selfish node detection method based on game theory where Total Cost Factor (TCF) of each route is calculated, and a route with Least Total Cost Factor (LTCF) is selected for data transmission. Zhao [34] and Yan and Hailes [35] proposed similar approaches using the basic game theory mechanism to encourage the cooperative behaviour of the participating nodes. Komali et al. [36] utilized the Nash equilibrium properties to confirm the selfish behaviour of nodes. The game theory based defensive approaches generally suffers from computational overhead in recalculating the system parameters for the dynamically changed environment.

A number of defensive schemes have been proposed by the research community based on the concept of reputation or trust in order to detect and isolate the selfish nodes [5, 11, 27, 37–42] from the normal functioning of the network. Chiejina et al. [5] proposed a reputation based scheme to detect and mitigate the effects of selfish nodes and deceitful nodes (selective packets dropping) in the network. Subramaniyan et al. [11] presented a Record- and Trust-Based Detection (RTBD) technique where every node maintains a global trust state for all nodes in the network. Refaei et al. [37] presented a reputation based mechanism by using various types of reputation functions to isolate the selfish nodes with reduced false alarms. The functioning of the mechanism relies on TCP acknowledgments, where each node increases the reputation index of their successor nodes along the route on receiving a successful ACK from the destination node. He et al. [38] designed a reputation-based management system named SORI (Secure and Objective Reputation-based Incentive). The basic functioning of SORI is based on traditional incentive mechanism. Cho and Chen [39] proposed a trust based mechanism based on demand and pricing (DP) mechanism with employing multiple types of trust functions in order to model the altruism and selfishness behaviour of network nodes. Thorat and Kulkarni [40] proposed an opportunistic routing protocol by taking into account the trustworthiness degree of nodes during the route discovery. Chakrabarti et al. [41] proposed a reputation based scheme to detect selfish nodes where the reputation value of nodes is computed by a Trusted Authority (TA). Velloso et al. [42] presented a human behaviour inspired model by employing the maturity relationship concept among the mobile nodes in the network. Most of these schemes don't succeed to differentiate between the real non-cooperative nodes (selfish nodes) and non-cooperative nodes due to low battery power, and also suffer from lack of effective mechanisms to evaluate the reputation and trust degree values of nodes in the network.

4 Proposed Intrusion Detection Technique

In this proposed intrusion detection technique, the selfish nodes are detected by their one hop neighbour through evaluating their trust degree value as well as estimating their residual energy over a period of time. The selfish nodes of type 1, type 2 and type 3 are detected by their one hop neighbour through evaluating their trust degree value over a

period of time, whereas type 4 selfish nodes are detected by their one hop neighbour through estimating their residual energy in addition to an assessment of their trust values over a period of time.

4.1 Definition and Properties of Trust

The trust is defined as the level of faith that puts one node to another to perform a particular action in accordance with a set of earlier successful communication interactions among them i.e. node N_i has a certain level of faith (trust) in node N_j to cooperate in the route discovery process and packets forwarding process. Similar to [8, 43], the trust degree is computed and updated through following two parameters:

Trust updates based on experience: In the initial setup of the network, there may be no trust relationship between node N_i and node N_j which is built up later on according to successful communication interactions among them over a period of time. The trust relationship derived from direct interactions, experiences or observations over a period of time is termed as direct trust.

Trust updates based on recommendations: Node N_i and node N_j do not have any past experience or observations, and node N_i's level of trust in node N_j is influenced by the opinion and recommendations communicated by node N_k to node N_i about the node N_k's level of trust in node N_j. This type of second-hand information obtained from other nodes on the request in order to evaluate the trust degree value of the monitored node is termed as indirect trust based on recommendations.

4.2 Architecture of Proposed Detection Technique

In this technique, each node periodically sends very short 'HELLO' messages to discover its one hop neighbouring nodes, and also share the details of their one hop neighbours with each other. All the nodes are placed in promiscuous mode to monitor the communication activities of their one hop neighbours, that is, if a node N_i forwards a packet to successor node N_j on the established route or during the route discovery process, it checks the correct packet forwarding behaviour of the successor node N_j through promiscuous mode. Similar to [44], each node maintains a trust table $\mathcal{T}$ for its one hop neighbours, according to data structure described in Fig. 1.

Similar to [8], the detection mechanism also utilizes the evaluation of both direct and indirect trust (based on neighbours' recommendations) values of nodes in order to improve the detection accuracy of selfish nodes in the network. The architecture of proposed technique is described in Fig. 2.

The proposed detection technique includes of two main components: Trust Evaluator and Trust Recommendation Group as shown in Fig. 2, which further consists the following nine modules: Recommendation request, Recommendation response, Deviation checker,

NODE_ID	NODE_TRUST	DIRECT TRUST VALUE	INDIRECT (RECOMMENDED) TRUST VALUE	CURRENT TIME	LAST UPDATING TIME

Fig. 1 Data structure of trust record table

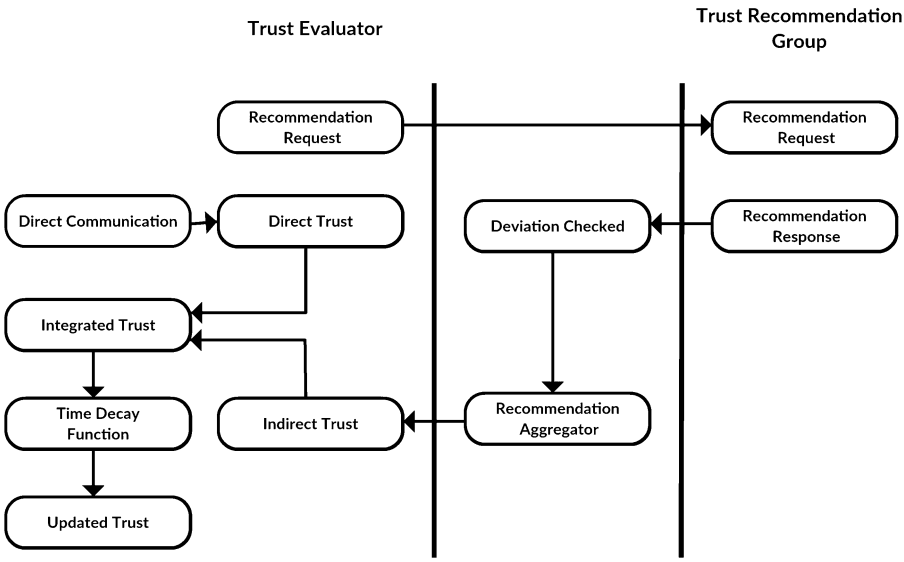

Fig. 2 Architecture of proposed intrusion detection technique

Recommendation aggregator, Indirect trust, Direct trust, Integrated trust, Time Decay function, and Updated Trust.

4.3 Trust Calculation in Proposed Technique

In the proposed intrusion detection technique, the detection mechanism utilizes the evaluation of both direct and indirect (based on neighbours' recommendations) trust values of nodes. Let $T_{ij}(t)$ denote the trust degree value of node N_j perceived by its direct neighbour N_i at time t, which is the weighted average of two parts as shown in Eq. 1.

$$T_{ij}(t) = \alpha T^d_{i,j}(t) + \beta T^r_{i,j}(t) \tag{1}$$

where $T^d_{i,j}(t)$ *is* direct trust degree value and $T^r_{i,j}(t)$ is indirect trust degree value (aggregate recommended trust value provided to N_i about node N_j by one hop neighbours of node N_j) of node N_j evaluated by node N_i at time t. The weight factors α and β ($\alpha+\beta=1$, $0 \leq \alpha \leq 1$ and $0 \leq \beta \leq 1$) are assigned to $T^d_{i,j}(t)$ and $T^r_{i,j}(t)$ respectively.

The trust degree value of a node is defined as a continuous value in the range from 0 to 1 ($i.e. 0 \leq T_{ij}(t) \leq 1$). Table 1 represents the different meaning of trust degree level used in this chapter, and trust degree value of a node equal to one indicates complete trust ("fully

Table 1 Different meanings of trust degree value

Level	Trust degree value	Meaning
1	(0.85, 1]	Complete trustworthy Node
2	(0.7, 0.85]	Trustworthy node
3	(T^{Thld}, 0.7]	Low trustworthy Node
4	[0, T^{Thld}]	Selfish node

trustworthy"), whereas a value close to zero indicates complete untrustworthy and confirmation of the attacker. The initial trust degree value of a node is set to 0.5 in order to avoid the cold start problem.

4.3.1 Direct Trust Calculation

The direct trust module is triggered by an evaluator node N_i in order to obtain the trust value of its recorded list of one hop neighbours where the direct trust value of a neighbour node (i.e. monitored node) N_j is computed on the basis of direct observation of communication transactions by node N_j over a period of time. At time t, the direct trust value of node N_j evaluated by node N_i (i.e., represented as $T_{ij}^{d}(t)$) is calculated as weighted sum of two terms as shown in following Eq. 2.

$$T_{ij}^{d}(t) = \gamma CCFR_{ij}(t) + \delta CDFR_{ij}(t) \tag{2}$$

where $T_{ij}^{d}(t)$ is direct trust value of node N_j evaluated by node N_i at time t, $CCFR_{ij}(t)$ is N_j's correct control packets forwarding ratio observed by node N_i at time t over the time interval $[t - \Delta t, t]$ and $CDFR_{ij}(t)$ is N_j's correct data packets forwarding ratio observed by node N_i at time t over the time interval $[t - \Delta t, t]$. The weight factors γ and δ ($\gamma + \delta = 1$, $0 \leq \gamma \leq 1$ and $0 \leq \delta \leq 1$) are assigned to $CCFR_{ij}(t)$ and $CDFR_{ij}(t)$ respectively.

The summary and notations of monitoring details maintained by monitoring node (N_i) in its table about the monitored/target node (N_j) are described in the Table 2. $CCFR_{ij}(t)$ and $CDFR_{ij}(t)$ are computed as per Eqs. 3 and 4 respectively with the assistance of algorithms 1 and 2:

$$\mathrm{CCFR_{ij}(t)} = \frac{\left(C_{ij}^{pt\_trans} - C_{ij}^{pt\_gener} - C_{ij}^{pt\_delay}\right)}{\left(C_{ij}^{pt\_recv} - C_{ij}^{pt\_recv\_dest}\right)} \tag{3}$$

Table 2 Notations used to keep the monitoring details about the monitored / target node (N_j) by monitoring node (N_i) in its table

Symbol	Description
$C_{ij}^{pt\_recv}$	Number of control packets received by target node
$C_{ij}^{pt\_trans}$	Number of control packets transmitted by target node
$C_{ij}^{pt\_gener}$	Number of control packets generated by target node
$C_{ij}^{pt\_delay}$	Number of control packets delayed by target node
$C_{ij}^{pt\_recv\_dest}$	Number of control packets received having destination target node
$D_{ij}^{pt\_recv}$	Number of data packets received by target node
$D_{ij}^{pt\_trans}$	Number of data packets transmitted by target node
$D_{ij}^{pt\_gener}$	Number of data packets generated by target node
$D_{ij}^{pt\_delay}$	Number of data packets delayed by target node
$D_{ij}^{pt\_recv\_dest}$	Number of data packets received having destination target node

$$\mathrm{CDFR_{ij}(t)} = \frac{\left(D_{ij}^{pt\_trans} - D_{ij}^{pt\_gener} - D_{ij}^{pt\_delay}\right)}{\left(D_{ij}^{pt\_recv} - D_{ij}^{pt\_recv\_dest}\right)} \tag{4}$$

Algorithm 1: ***Auditing at Node N_i during monitoring target node N_j for control packet p.***

// *Control Packets Receiving Phase* //

// Let Node N_i monitoring node N_j for control packet p //

if the received control packet *p* is destined for Node N_j **then**
$C_{ij}^{pt\_recv}++$; *// No. of control packets Received//*
$C_{ij}^{pt\_recv\_dest}++$; *// No. control packets having Destination Node j//*
else
$C_{ij}^{pt\_recv}++$; *// No. of control packets Received//*
Set timer $\pounds_j^p$ *at* $Node\ N_i$; *// Set Packet Timeout ($\pounds_j^p$) at Node **i** for monitoring target node **j** //*
end if;

// *Control Packets Transmission Phase* //

// for each control packet p transmitted by target node N_j //

if *control packet p is to be transmitted by target node N_j is generated by itself (N_i) or other nodes* **then**
for *each packet p* **do**
if *packet p has been transmitted by Node j before expire the time* $\pounds_j^p$ **then**
$C_{ij}^{pt\_trans}++$; *// No. of control packets transmitted//*
else
Set timer again $\pounds_j^p = \frac{\pounds_j^p}{2}$.
If *packet p has been transmitted by node N_j before expire the time* $\pounds_j^p$ **then**
$C_{ij}^{pt\_trans}++$; *// No. of control packets transmitted //*
$C_{ij}^{pt\_delay}++$; *// No. of control packets delayed//*
else
Packet p has been dropped by Node N_j.
end if;
end if;
end for;
else
$C_{ij}^{pt\_trans}++$; *// No. of control packets transmitted //*
$C_{ij}^{pt\_gener}++$ *// No. of transmitted control packets generated by target node N_j //*
end if;

Algorithm 2: ***Auditing at Node N_i during monitoring target node N_j for data packet p.***

// Data Packets Receiving Phase //

// Let Node N_i monitoring node N_j for data packet p //

if the received data packet *p* is destined for Node N_j **then**

$D_{ij}^{pt\_recv}++;$ *// No. of data Packets Received//*

$D_{ij}^{pt\_recv\_dest}++;$ *// No. data packets having Destination Node j//*

else

$D_{ij}^{pt\_recv}++;$ *// No. of data Packets Received//*

Set timer $\pounds_j^p$ *at Node* i ; *// Set Packet Timeout* ($\pounds_j^p$) *at Node* N_i *for monitoring target node* N_j *//*

end if;

// Data Packets Transmission Phase //

// for each data packet p transmitted by target node N_j //

if *data packet p is to be transmitted by target node N_j is generated by itself (N_i) or other nodes* **then**

for *each packet p* **do**

if *packet p has been transmitted by Node N_j before expire the time* $\pounds_j^p$ **then**

$D_{ij}^{pt\_trans}++;$ *// No. of data packets transmitted//*

else

Set timer again $\pounds_j^p = \frac{\pounds_j^p}{2}$;

if *packet p has been transmitted by node j before expire the time* $\pounds_j^p$ **then**

$D_{ij}^{pt\_trans}++;$ *// No. of data packets transmitted //*

$D_{ij}^{pt\_delay}++;$ *// No. of data packets delayed//*

else

Packet p has been dropped by Node N_j.

end if;

end if;

end for;

else

$D_{ij}^{pt\_trans}++;$ *// No. of data packets transmitted //*

$D_{ij}^{pt\_gener}++$ *// No. of transmitted data packets generated by target node N_j //*

end if;

4.3.2 Indirect Trust Calculation

Due to limited communication interactions, radio transmission errors, and congestion or packet collisions on the way, evaluating the behaviour of a node on the basis of direct observed communication transactions is not justified. Therefore, the indirect trust values (based on neighbours' recommendations) from one hop neighbours of target node is essential to take into account in order to boost the trust evaluation process as well as improve the detection accuracy of selfish nodes in the network. In addition to the direct trust module, the recommendation request module is also activated by an evaluator node N_i by sending the special recommendation trust request packet (RTREQST) to one hop neighbours of the target node. In response to RTREQST packet, the one hop neighbours of target node send the recommendation trust response packets (RTRESPs) to the evaluator node N_i as shown in Fig. 3.

The Recommendation Trust Request Packet (RTREQST) contains three fields as shown in Fig. 4.

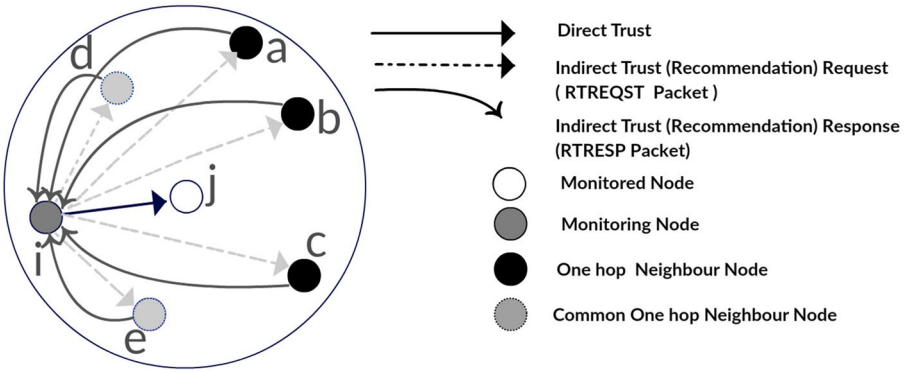

Fig. 3 Request and response for the indirect (recommendation) trust value

SREQ_ID	TARGET_ID	Timestamp

Fig. 4 Recommendation request packet (RTREQST) format

RECOM_ID	SREQ_ID	TARGET_ID	$T^r_{m,j}$	Timestamp

Fig. 5 Recommendation response packet (RTRESP) format

SREQ_ID Node ID of Recommendation Trust Request Packet originator (N_i)
TARGET_ID Node ID of Target Node (N_j) for which indirect trust value is desired
Timestamp Exact time at which the RTREQST packet was released by N_i

Upon receiving the RTREQST packets at one hop neighbour nodes of evaluating/target node (N_j) from the evaluator node (N_i), they responds back against the SHNRQ packet by generating the recommendation trust response packet (RTRESP) with the recommendation trust value about the target node (N_j). Recommendation Trust Response Packet (RTRESP) is containing five fields as shown in Fig. 5.

RECOM_ID Node ID of Recommendation Trust Response Packet originator
SREQ_ID Node ID of Recommendation Trust Request Packet originator (N_i)
TARGET_ID Node ID of Target Node (N_j)
$T^r_{m,j}$ Recommendation trust value provided by Recommender N_m about N_j
Timestamp Exact time at which the RTRESP packet was released by N_m

Upon receiving the recommendation trust value, N_i applies the deviation check on them as per Eq. 5 in order to defend against the slander attack [45], and excludes those recommendation trust values which are deviating above the deviation threshold. The deviation check is executed with the help of a deviation checked module. The recommendation trust values are considered for the recommendation aggregator if they are not deviating above the deviation threshold as shown in Eq. 5.

$$\left|T_{ij}^{d}(t) - T_{mj}^{r}(t)\right| \leq D^{Thld} \tag{5}$$

where D^{Thld} is deviation threshold. If the above test is positive, then the recommended trust value provided by say node N_m is considered compatible and used to update the trust value of node N_j. The recommendation aggregator module aggregates the recommendation trust values provided by the one hop neighbours of node N_j after passing through the deviation checker module. The recommendation aggregator module aggregates the recommendation trust values using the simple average formula as shown in Eq. 6.

$$T_{ij}^{r}(t) = \frac{\sum T_{mj}^{r}(t)}{\mathrm{n} - \mathrm{d}} \tag{6}$$

where n is the number of one hop neighbours of node N_j who reply with recommendation trust values against the RTREQST packets received from N_i about N_j, and d is number of those one hop neighbours of node N_j whose recommendation trust values failed to pass the deviation check.

Now, $T_{ij}(t)$ (i.e. trust degree value of node N_j) perceived by its direct neighbour N_i at time t is calculated by implying above mention Eq. 1 (i.e. $T_{ij}(t)=\alpha\ T_{i,j}^{d}\ (t)+\beta\ T_{i,j}^{r}\ (t)$).

4.3.3 Time Decay Function ($e^{-(n-k)}$)

The influence of past interactions or experience changes over time in a highly dynamic environment such as MANETs. Therefore, in order to assess an accurate node's direct trust value, it is required to account the influence of past direct trust values assessed by node N_i towards node N_j. The proposed intrusion detection technique incorporates an exponential decay function (i.e. $e^{-(n-k)}$ made for the k^{th} interaction interval) to gradually degrade the direct trust value of monitored nodes' overtime, where n is the number of intervals of small duration Δt from time 0 to current time t and the value of k lies as $0 \leq k \leq n$. This function contributes more weight to communication transactions that took place recently as compared to communication transactions that took place in the past.$T_{ij}^{f}(t)$ denotes the updated trust value of node N_j perceived by its direct neighbour N_i at time t after incorporating an exponential decay function as shown in Eq. 7.

$$T_{ij}^{f}(t) = \sum_{k=1}^{n}\left(T_{ij}(t) * e^{-(n-k)}\right) / \sum_{k=1}^{n}\left(e^{-(n-k)}\right) \tag{7}$$

4.4 Residual Energy

Energy is an important metric in assessing the selfish behavior of mobile nodes since the transmission and reception of packets in MANETs are particularly relies on the amount of energy that the mobile nodes have. Using an energy prediction model, the residual energy of mobile nodes in the different periods can be estimated.

The residual energy of node N_j is estimated through monitoring node N_j's packet transmission and receiving activities over the time period [t-Δt, t]. The first order energy consumption radio model as discussed in [46] is considered here with identical parameter values in estimating the energy consumption for transmission as well as for receiving the packets. The energy consumption per bit in transmission of single bit from node N_j to node N_k is given in Eq. 8.

$$E_{jk}^{Tsmit} = E_{txelec} + E_{tx,amp} * (d_{j,k})^{\mu} \tag{8}$$

where E_{txelec} is the energy dissipated in the transmitter electronics circuitry (per bit) and $E_{tx,amp} * (d_{j,k})^{\mu}$ is the energy dissipated for transmission of a single bit over a distance $d_{j,k}$, $E_{tx,amp}$ is constant value that reflects the energy depleted in amplifier in the transmitter for transmitting data, and μ is path loss exponent (usually $2.0 \leq \mu \leq 6.0$) and dependent on the propagation channel. Similarly, the energy consumption per bit in receiving of single bit at node N_j is given in Eq. 9.

$$E_{j}^{Recv} = E_{rxelec} \tag{9}$$

where E_{rxelec} is a function of the receiver electronics circuitry (per bit) at receiver. The energy dissipated for transmission of a K-bit packet over a distance $d_{j,k}$ is given in Eq. 10.

$$E_{jk}^{Tsmit}(K) = (E_{txelec} + E_{tx,amp} * \left(d_{j,k}\right)^{\mu}) * K \tag{10}$$

The total energy consumption in receiving a K-bit packet at node N_j is given in Eq. 11.

$$E_{j}^{Recv}(K) = E_{rxelec} * K \tag{11}$$

As per structure of the proposed technique, all the nodes are placed in promiscuous mode and overhear the surrounding packets of their one hop neighbours. It means the energy consumption of the nodes increases would be more due to overhearing the transmissions in its close vicinity. According to Basu and Redi [47], the total energy consumption at node N_j in overhearing the packets of its one hop neighbour in its close vicinity is same the energy consumption in receiving the packets. Therefore, total energy consumption at node N_j in overhearing a bit (see Eq. 12) is equal to energy consumption in receiving a bit.

$$E_{j}^{Over} = E_{rxelec} \tag{12}$$

The total energy consumption in overhearing a K-bit packet at node N_j is given in Eq. 13.

$$E_{j}^{Over}(K) = E_{rxelec} * K \tag{13}$$

If $Nb(j)$ is the number of one hop neighbours of node N_j, then the energy consumption of the node N_j in overhearing the transmissions of its direct neighbours is proportional to $Nb(j) * E_{rxelec}$. Finally, a node N_j suffers from total energy consumption (E_j^{Total}) with three components as shown in Eq. 14.

$$E_{j}^{Total} = \mathrm{C}_1 * E_{jk}^{Tsmit} + \mathrm{C}_2 * E_{j}^{Recv} + \mathrm{C}_3 * E_{j}^{Over} \tag{14}$$

Where C_1, C_2, and C_3 are constants, dependent on the size and number of packets in communication (transmission and receiving of packets) through node N_j as well as on its one hop neighbours. The Eq. 14 can be rewrite as in Eq. 15.

$$E_{j}^{Total} = \mathrm{C}_1 * [E_{txelec} + E_{tx,amp} * (d_{j,k})^{\mu}] + \mathrm{C}_2 * E_{rxelec} + \mathrm{C}_3 * E_{rxelec} \tag{15}$$

In this model, the notations E_j^{init} is used to denote the initial energy of node N_j and E_j^{res} is used to denote the estimated residual energy of node N_j over the time period $[t - \Delta t, t]$. The energy consumption at node N_j in overhearing the packets of its one hop neighbour is estimated on the average basis. This model also computes the energy drain rate, denoted by DR_j^E for every Δt second. The actual value of energy drain rate (DR_j^E) is computed by employing the well-known exponential weighted moving average method (see Eq. 16)

similar to [12] on previous drain rate value (DR^E_{old}) and newly calculated drain rate value (DR^E_{new}).

$$DR^E_j = \mathrm{q} * DR^E_{old} + (1 - \mathrm{q}) * DR^E_{new} \tag{16}$$

where q is weighted average factor, and higher priority is given to the newly calculated drain rate value (DR^E_{new}) by setting q =0.3. Using this energy prediction model, the residual energy (E^{res}_j) of mobile node N_j is estimated over the regular interval of time.

4.5 Detection and Isolation of Selfish Nodes

In the proposed detection technique, type 1, type 2 and type 3 selfish nodes are detected by their one hop neighbour through evaluating their trust degree value over a period of time, whereas type 4 selfish node is detected by estimating the residual energy of a monitored/target node in addition to an assessment of its trust value over a period of time. The algorithm 3 illustrates the procedure of detecting the selfish nodes as well as isolating them from normal functioning of the network.

Algorithm 3: ***Detection and isolation the selfish node ( );***

Requires:

N_i	:	Evaluator node
N_j	:	Evaluating node
$E^{res}_j(t)$	:	Residual energy of N_j at time t .
$T^f_{ij}(t)$	:	Updated Trust Value of N_j in its neighbour node N_i trust table at time t
E^{Thld}	:	Residual energy Threshold .
T^{Thld}	:	Trust Value Threshold.

Begin

if $(T^f_{ij}(t) \leq T^{Thld})$ then
  if $(E^{res}_j(t) \leq E^{Thld})$ then
    N_j is selfish node of type 4.
    Isolate the node N_j from normal functioning of the network by its one hop neighbours.
    Inform the source node to setup a new route for data transmission.
  else
    N_j is selfish node of either type 1, or type 2 or type 3.
    Isolate the node N_j from normal functioning of the network by its one hop neighbours.
    Inform the source node to setup a new route for data transmission.
  end if;
else
N_j is not a selfish node.
Continue the normal functioning of the network with node N_j.
end if;

After evaluating the total trust value of monitored nodes as discussed in Sect. 4.3, the values are stored in the trust table Ţ according to data structure depicted in Fig. 1 and trust values are updated at regular intervals. The estimated residual energy as well as computed total trust degree values of all monitored nodes is compared with their respective threshold values to decide the actual status of a node as shown in algorithm 3. According to algorithm 3, a node that is identified as selfish node will be isolated from the normal functioning of the network by its one hop neighbours such that no routing packet is forwarded through or from it, and selfish node would not be able to access the network resources because the requests originated from it will not be processed by its direct neighbours. If the subsequent node is acting as an intermediate node of existing route, then the source node is immediately informed to source node to setup an alternative route by

avoiding the selfish node. In this way, a fresh route is established between the source and destination node in the network by limiting the functionality of selfish nodes.

5 Network Simulation and Performance Evaluation

In this section, the simulation experiments have been performed using a NS-2 network simulator (version NS-2.34) [48] to examine the effectiveness of the proposed intrusion detection technique. The requisite amendments were also carried out in the existing NS-2.34 modules to integrate the selfish and normal behaviours of mobile nodes, and the operative procedure of the proposed intrusion detection technique.

The mobile nodes are randomly distributed over the simulated area of 1500 X 1500 m^2 flat space area. The set of experiments is carried out with node density of 50 nodes. Table 3 shows the other related parameters used in the simulation. CSMA/CA (Carrier Sense Multiple Access protocol with Collision Avoidance) is used to transmit the routing packets as well as data packets during the simulation experiments. Random way point (RWP) mobility model is used in the simulation with maximum movement speed of 10, 15 and 20 m/s. Here, each node moves independently from one location to another location (destination) in accordance to Random Waypoint Model with a speed chosen arbitrarily from the range [0, max]. In these sets of experiments, three types of pause time for the network nodes, 20 s (high mobility), 30 s, and 40 s (low mobility), are distinctly considered where the pause time means the frequency of network topology changes. When a movable node reaches its destination location it remains stationary for a certain period of time equal to pause time there and starts moving to another destination location. DCF (Distributed Coordination Function) of IEEE 802.11 is considered as a MAC layer protocol during the simulation experiments.

The value of Packet Timeout (i.e. $£_j^p$) is taken 50 ms as mentioned in [6]. The weighting values of α, β, γ and δ are set equal to 0.67, 0.33, 0.6 and 0.4 respectively. The value of Δt is set equal to five second. Hua and Yum [49] suggested that the value of μ should be taken equal to two for effective results. According to Chen et al. [50], the values of parameters E_{txelec}, E_{rxelec} and $E_{tx,amp}$ are generally taken as: $E_{txelec} = E_{rxelec} = 100$ pJ/bit/m^2 and $E_{tx,amp}$

Table 3 Simulation parameters

Simulator	Ns-2 (ver. 2.34)
Simulation time	500 (s)
Number of mobile nodes (node density)	50
Mobility model	Random waypoint model
MAC specification	IEEE 802.11
Radio bandwidth	10 Mbps
Number of selfish nodes	5, 10, 15, 20, 25
Simulated area	1500 m × 1500 m
Transmission range	100 m
Routing protocols	AODV
Traffic	Constant Bit Rate (CBR)
Pause time	20, 30, and 40 (s)
Packet size	512 bytes
Data rate	10 Kbits/sec

=50 nJ/bit. In NS-2, the default energy consumption values in transmission a packet, in receiving a packet, and in idle condition are 0.660 Joules (1.6 W drained power), 0.395 Joules (1.2 W drained power) and 0.035 Joules (1.15 W drained power) respectively. The nodes are assigned the initial energy of 95-300 Joules randomly. The value of E^{Thld} is taken 25 J as mentioned in [12]. The values of D^{Thld} and T^{Thld} are taken 0.3 and 0.4 respectively. Maximum 50% nodes are arbitrarily chosen to show their selfish behaviour in the network. Further, the source and destination nodes are also selected in arbitrary fashion in the rest of the network.

In order to examine the effectiveness of the intrusion detection technique, the simulation experiments are carried out with 3 different maximum movement speed scenarios (i.e. 10, 15 and 20 m/s), 3 different pause time scenarios (i.e. 20, 30, and 40 s) and mean value is reported here. In addition, the performance of the proposed intrusion detection technique is evaluated and compared with Chiejina et al. [5] and classical AODV routing protocol under the 10% to 50% of the selfish nodes with respect to packet delivery ratio, throughput, average end-to-end delay, true positive rate and false positive rate metrics.

5.1 Packet Delivery Ratio (PDR)

PDR is defined as the ratio of total number of data packets successfully delivered to the destination node to the number of data packets originated by the source node throughout the simulation run.

$$PDR = (Packets\,Delivered / Packets\,Originated) \tag{17}$$

A decrease in the PDR is an outcome of the selfish nodes in the network. PDR shows the correctness and completeness of the proposed intrusion detection technique, and also measure the efficiency of the proposed intrusion detection technique. Figure 6 shows the packet delivery ratio for classical AODV, Chiejina et al. [5] and proposed detection technique with varying the number of selfish nodes from 5 to 25. As can be seen from Fig. 6, the PDR for AODV is gradually decreasing with increasing the number of selfish nodes in the network, this is because the selfish nodes either do not participate in the route discovery process or if participate they do not forwards the data packets to successor nodes on being selected as an active member on the route. These nodes discard the packets instead of forwarding them to the successor nodes, and this type of situation leads to gradually decrease in the PDR with increasing the number of selfish nodes in the network.

However, the PDR also decreases for both Chiejina et al. [5] and proposed intrusion detection technique because both the schemes identify the selfish nodes and isolate them from the normal functioning of the network, which results high demand of trusted nodes in carry out the normal functioning of the network. The packet delivery ratio in the presence of 50% selfish nodes for classical AODV is approximately 27%, while the packet delivery ratio for proposed intrusion detection technique is approximately 55%. Similarly, the packet delivery ratio in Chiejina et al. [5] is approximately 52%, which is less by 3% when compared to our proposed intrusion detection technique.

This improved PDR recorded by the proposed intrusion detection technique and Chiejina et al. [5] as compared to the classical AODV protocol is due to the isolation of selfish nodes from normal functioning of the network in both the schemes. Further, the minor improvement in PDR for proposed intrusion detection technique as compared to

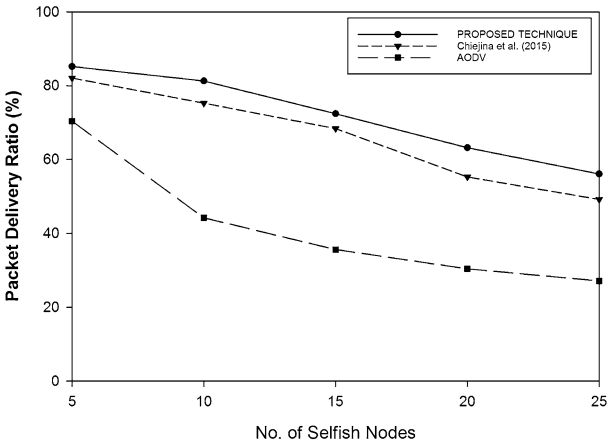

Fig. 6 Packet delivery ratio versus no. of selfish nodes

Chiejina et al. [5] is due to improved detection accuracy of selfish nodes by employing the indirect trust (based on neighbours' recommendations) about the target nodes from their one hop neighbour nodes.

5.2 Average End-to-End Delay (AEED)

AEED is referred as an average transmission delay experienced by data packets in transmission from source node to the destination node.

$$Average\ End\ to\ End\ Delay = \frac{\sum(time\ packet\ received - time\ packet\ transmitted)}{number\ of\ packets\ received} \quad (18)$$

According to Wang et al. [44], the delay in the transmission is contributed by several other factors such as delay in servicing retransmission requests at the MAC layer, packets queuing delays at interface transmission queues and packets buffering delays during route discovery. Figure 7 shows the average end-to-end delay for AODV, Chiejina et al. [5] and proposed intrusion detection technique with varying the number of selfish nodes from 5 to 25. The average end-to-end delay for AODV increased sharply with varying the number of selfish nodes from 5 to 25 because the presence of selfish nodes in the network breakup the network into smaller independent segments. The average end-to-end delay also increases in both Chiejina et al. [5] and proposed intrusion detection technique, because both techniques identify the selfish nodes and isolate them from the normal functioning of the network. As a result, the route with more number of hops may be selected for data transmission.

The proposed intrusion detection technique has less average end-to-end delay as compared to Chiejina et al. [5] because the evaluator node in Chiejina et al. [5] may be overestimate the selfish behaviour of normal nodes due to the effects of radio transmission errors, congestion or packet collisions in the network. As a result, the availability of normal nodes is reduced, and the average end-to-end delay increase in Chiejina et al. [5], whereas the proposed intrusion detection technique helps a node to accurately judge the selfish

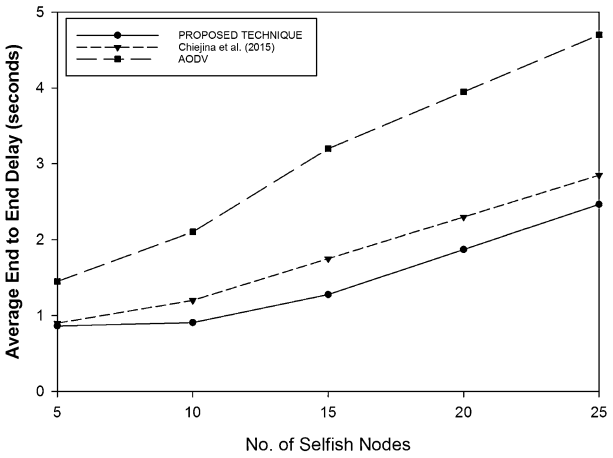

Fig. 7 Average end to end delay versus number of selfish nodes

nature of its one hop neighbours by employing effective mechanism to measure the trust degree value of nodes.

5.3 Throughput (T)

It is defined as the amount of data transferred from source to destination per unit of time.

$$T = \frac{bits}{transmission\_time_{end} - transmission\_time_{start}} bps \tag{19}$$

A shrink in throughput is an effect of the presence of selfish nodes in the network. Figure 8 shows the throughput for AODV, Chiejina et al. [5] and proposed intrusion detection technique with varying the number of selfish nodes from 5 to 25.

As can be seen from Fig. 8, the network throughput for classical AODV, Chiejina et al. [5] and proposed intrusion detection technique are slightly decreasing with increasing the selfish nodes from 5 to 25 because small numbers of packets are being delivered to the destination node. The proposed intrusion detection technique and Chiejina et al. [5] show better performance as compared to classical AODV because both techniques identify the selfish nodes and isolate them from the normal functioning of the network, which results high availability of the network resources to the remaining benign nodes to perform the normal functioning of the network. The proposed intrusion detection technique performs better as compared to Chiejina et al. [5] in presence of selfish nodes due to due to improved detection accuracy of selfish nodes by employing the indirect trust (based on neighbours' recommendations) about the target nodes from their one hop neighbour nodes.

5.4 True Positive Rate (TPR)

It is defined as the ratio of the number of selfish nodes detected to the total number of selfish nodes present in the network. Figure 9 shows the true positive rate for the proposed intrusion detection technique and Chiejina et al. [5] with increasing the number of selfish nodes from 5 to 25 in the network. The detection mechanism in both techniques becomes harder to judge the selfish nature of the nodes with increasing the selfish nodes because of

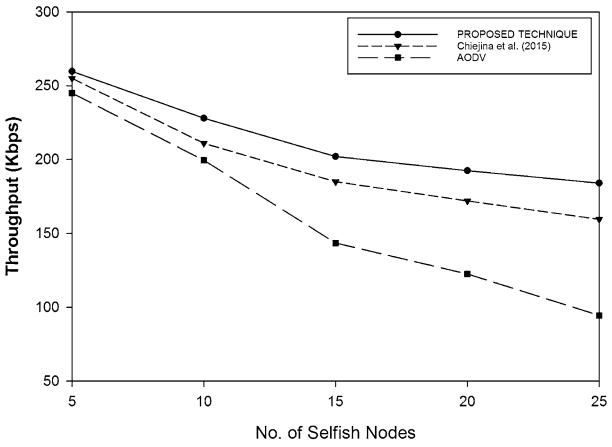

Fig. 8 Throughput versus number of selfish nodes

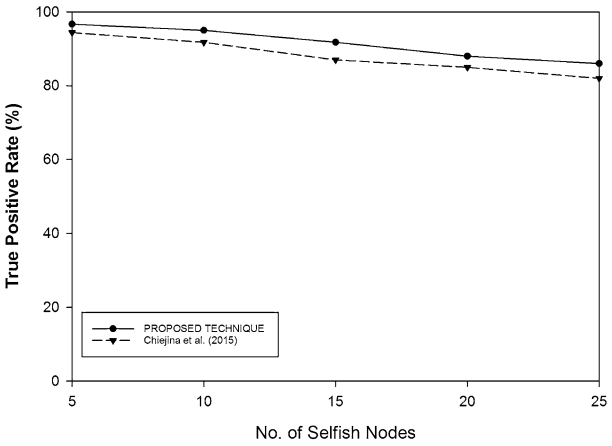

Fig. 9 True positive rate versus number of selfish nodes

nodes mobility. The true positive rate in both the techniques decreases with increasing the selfish nodes in the network. It has been observed that the true positive rate for the proposed intrusion detection technique is 96.7% in the best case and 85.63% in the worst case and for Chiejina et al. [5] is 94.41% in the best case and 81.92% in the worst case.

The slightly decrease in TPR in Chiejina et al. [5] as compared to the proposed intrusion detection technique is due to not considering the effects of delayed control packets by the nodes while evaluating their reputation values.

5.5 False Positive Rate (FPR)

It is defined as the ratio of the number of normal nodes being detected as selfish ones to the total number of normal nodes in the network.

It is clear from the Fig. 10 that the maximum value of false positive rate in the presence of 50% of selfish nodes for the proposed technique is less than 10%, which is also

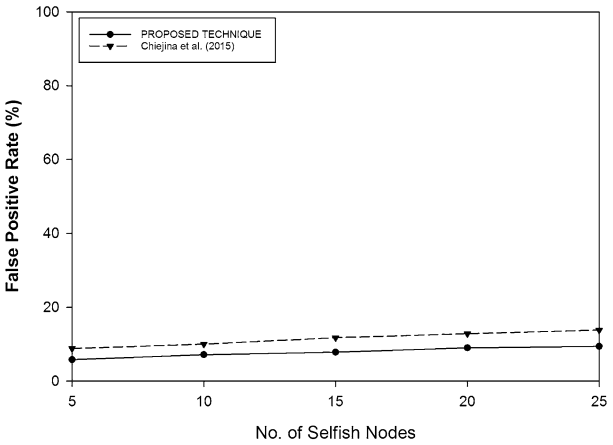

Fig. 10 False positive rate versus number of selfish nodes

relatively less as compared to Chiejina et al. [5], because the evaluator node in Chiejina et al. [5] may be overestimate the selfish behaviour of normal nodes due to the effects of radio transmission errors, congestion or packet collisions in the network. The false positive rate in the proposed intrusion detection technique is mainly due to mobility of nodes and trust update interval.

6 Conclusion

In this paper, an effective dynamic trust based intrusion detection technique is presented to detect and isolate the selfish nodes from the mobile ad hoc networks. Taking the node's trust degree value as the input, the proposed detection technique is smoothly extended for detecting and isolating the selfish nodes from the normal functioning of the network, such that no routing packet is forwarded through or from the selfish nodes. This technique minimizes the possibility of overestimating the selfish behaviour of innocent nodes due to radio transmission errors, network congestion or packet collisions by employing the indirect trust (based on neighbours' recommendations) about the target nodes. Furthermore, this technique restricts the ability of the selfish nodes to take the benefits of network resources for their own purpose. After detection the selfish nodes by their direct neighbours, selfish nodes would not be able to access the network resources because the requests originated from them will be disregarded by their direct neighbours. The effectiveness of the proposed detection technique is evaluated and compared with Chiejina et al. [5] and classical AODV routing protocol with varying the number of selfish nodes from 10% to 50%. The simulation results clearly indicate the efficiency of the proposed detection technique in terms of the packet delivery ratio, the average end-to-end delay, throughput, true positive rate and false positive rate. In this paper, the proposed intrusion detection technique demonstrates the solution for detecting and mitigating the effect of selfish nodes in the network. However, the same technique after requisite modification can be used to cope with other types of misbehaving nature of nodes.

References

1. Chlamtac, I., Conti, M., & Liu, J. J. N. (2003). Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks, 1*(1), 13–64.
2. Hoebeke, J., Moerman, I., Dhoedt, B., & Demeester, P. (2004). An overview of mobile ad hoc networks: applications and challenges. *Journal-Communications Network, 3*(3), 60–66.
3. Al-Karaki, J. N., & Kamal, A. E. (2004). Routing techniques in wireless sensor networks: A survey. *IEEE Wireless Communications, 11*(6), 6–28.
4. Buttyán, L., & Hubaux, J. P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications, 8*(5), 579–592.
5. Chiejina, E., Xiao, H., & Christianson, B. (2015). A dynamic reputation management system for mobile ad hoc networks. *Computers, 4*(2), 87–112.
6. Rodriguez-Mayol, A., & Gozalvez, J. (2014). Reputation based selfishness prevention techniques for mobile ad-hoc networks. *Telecommunication Systems, 57*(2), 181–195.
7. Sun, Y. L., Han, Z., Yu, W., & Liu, K. R. (2006). A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. In *Proceedings of 25TH IEEE international conference on computer communications (IEEE INFOCOM 2006)* (pp. 1–13). IEEE.
8. Jiang, J., Han, G., Wang, F., Shu, L., & Guizani, M. (2015). An efficient distributed trust model for wireless sensor networks. *IEEE transactions on parallel and distributed systems*, *26*(5), 1228–1237.
9. Perkins, C. E, & Royer, E. M. (1999). Ad hoc on-demand distance vector routing. In *Proceedings of 2nd IEEE workshop on mobile computing systems and applications (WMCSA'99)* (pp. 90–100). IEEE.
10. Michiardi, P., & Molva, R. (2002). Simulation-based analysis of security exposures in mobile ad hoc networks. In *Proceedings of European wireless conference 2002: Next generation wireless networks: Technologies, protocols, services applications* (pp. 15–17).
11. Subramaniyan, S., Johnson, W., & Subramaniyan, K. (2014). A distributed framework for detecting selfish nodes in MANET using Record-and Trust-Based Detection (RTBD) technique. *EURASIP Journal on Wireless Communications and Networking, 2014*(1), 205.
12. Sengathir, J., & Manoharan, R. (2015). Exponential reliability coefficient based reputation mechanism for isolating selfish nodes in MANETs. *Egyptian Informatics Journal, 16*(2), 231–241.
13. Kargl, F., Klenk, A., Schlott, S., & Weber, M. (2004). Advanced detection of selfish or malicious nodes in ad hoc networks. In *European Workshop on Security in Ad hoc and Sensor Networks* (pp. 152–165). Springer Berlin Heidelberg.
14. Yoo, Y., Ahn, S., & Agrawal, D. P. (2005). A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks. In *Proceedings of IEEE International Conference on Communications (ICC 2005)* (Vol. 5, pp. 3005–3009). IEEE.
15. Yoo, Y., & Agrawal, D. P. (2006). Why does it pay to be selfish in a MANET? *IEEE Wireless Communications, 13*(6), 87–97.
16. Toh, C. K., Kim, D., Oh, S., & Yoo, H. (2010). The controversy of selfish nodes in ad hoc networks. In *Proceedings of 12th IEEE International Conference on Advanced Communication Technology (ICACT)* (Vol. 2, pp. 1087–1092). IEEE.
17. Gupta, S., Nagpal, C. K., & Singla, C. (2011). Impact of selfish node concentration in manets. *International Journal of Wireless & Mobile Networks (IJWMN), 3*(2), 29–37.
18. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000). Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the 6th ACM annual international conference on Mobile computing and networking* (pp. 255–265). ACM.
19. Hernández-Orallo, E., Olmos, M. D. S., Cano, J. C., Calafate, C. T., & Manzoni, P. (2014). A fast model for evaluating the detection of selfish nodes using a collaborative approach in MANETs. *Wireless Personal Communications, 74*(3), 1099–1116.
20. Ferraz, L. H. G., Velloso, P. B., & Duarte, O. C. M. (2014). An accurate and precise malicious node exclusion mechanism for ad hoc networks. *Ad Hoc Networks, 19,* 142–155.
21. Shakshuki, E. M., Kang, N., & Sheltami, T. R. (2013). EAACK—A secure intrusion-detection system for MANETs. *IEEE Transactions on Industrial Electronics, 60*(3), 1089–1098.
22. Djenouri, D., Ouali, N., Mahmoudi, A., & Badache, N. (2005). Random feedbacks for selfish nodes detection in mobile ad hoc networks. In T. Magedanz, E. R. M. Madeira, & P. Dini (Eds.), *Operations and Management in IP-Based Networks. IPOM 2005. Lecture Notes in Computer Science* (Vol. 3751, pp. 68–75). Springer, Berlin.
23. Miranda, H., & Rodrigues, L. (2003). Friends and foes: Preventing selfishness in open mobile ad hoc networks. In *Proceedings of 23rd IEEE international conference on distributed computing systems workshops* (pp. 440–445). IEEE.

24. Das, V. V. (2007). IP-based credit mobile ad-hoc networks. In *Proceedings of IEEE international conference on computational intelligence and multimedia applications (ICCIMA 2007)* (Vol. 4, pp. 453–457). IEEE.
25. Demir, C., & Comaniciu, C. (2007). An auction based AODV protocol for mobile ad hoc networks with selfish nodes. In *Proceedings of IEEE International Conference on Communications (ICC'07)* (pp. 3351–3356). IEEE.
26. Wang, Y., Giruka, V. C., & Singhal, M. (2008). Truthful multipath routing for ad hoc networks with selfish nodes. *Journal of Parallel and Distributed Computing, 68*(6), 778–789.
27. Soltanali, S., Pirahesh, S., Niksefat, S., & Sabaei, M. (2007). An efficient scheme to motivate cooperation in mobile ad hoc networks. In *Proceedings of IEEE Third International Conference on Networking and Services (ICNS '07)* (pp. 98–103). IEEE.
28. Kumar, J. M. S. P. J., Kathirvel, A., Kirubakaran, N., Sivaraman, P., & Subramaniam, M. (2015). A unified approach for detecting and eliminating selfish nodes in MANETs using TBUT. *EURASIP Journal on Wireless Communications and Networking, 2015*(1), 143.
29. Sengathir, J., & Manoharan, R. (2015). Semi-markov Process Based Cooperation Enforcement Mechanism for MANETs. In L. Jain, H. Behera, J. Mandal & D. Mohapatra (Eds.), *Computational Intelligence in Data Mining — Volume 2. Smart Innovation, Systems and Technologies* (Vol 32, pp. 683–693). Springer: New Delhi.
30. Sengathir, J., & Manoharan, R. (2015). A futuristic trust coefficient-based semi-Markov prediction model for mitigating selfish nodes in MANETs. *EURASIP Journal on Wireless Communications and Networking,* 2015(1), 158.
31. Kaliappan, M., & Paramasivan, B. (2015). Enhancing secure routing in Mobile Ad Hoc Networks using a Dynamic Bayesian Signalling Game model. *Computers & Electrical Engineering, 41,* 301–313.
32. Mao, Y., & Zhu, P. (2015). A game theoretical model for energy-aware DTN routing in Manets with nodes' selfishness. *Mobile Networks and Applications, 20*(5), 593–603.
33. Das, D., Majumder, K., & Dasgupta, A. (2015). Selfish node detection and low cost data transmission in MANET using game theory. *Procedia Computer Science, 54,* 92–101.
34. Zhao, D. (2006). Access control in ad hoc networks with selfish nodes. *Wireless Communications and Mobile Computing, 6*(6), 761–772.
35. Yan, L., & Hailes, S. (2008). Designing incentive packet relaying strategies for wireless ad hoc networks with game theory. In A. Miri (Ed.), *Wireless Sensor and Actor Networks II. IFIP — The International Federation for Information Processing II* (Vol 264, pp. 137–148). Springer: Boston.
36. Komali, R. S., MacKenzie, A. B., & Gilles, R. P. (2008). Effect of selfish node behavior on efficient topology design. *IEEE Transactions on Mobile Computing, 7*(9), 1057–1070.
37. Refaei, M. T., Srivastava, V., DaSilva, L., & Eltoweissy, M. (2005). A reputation-based mechanism for isolating selfish nodes in ad hoc networks. In *Proceedings of 2nd IEEE annual international conference on mobile and ubiquitous systems: Networking and services (MobiQuitous 2005)* (pp. 3–11). IEEE.
38. He, Q., Wu, D., & Khosla, P. (2004). SORI: a secure and objective reputation-based incentive scheme for ad-hoc networks. In *Proceedings of IEEE wireless communications and networking conference (WCNC. 2004)*, (IEEE Cat. No.04TH8733) (Vol. 2, pp. 825–830). IEEE.
39. Cho, J. H., & Chen, R. (2013). On the tradeoff between altruism and selfishness in MANET trust management. *Ad Hoc Networks, 11*(8), 2217–2234.
40. Thorat, S. A., & Kulkarni, P. J. (2015). Opportunistic routing in presence of selfish nodes for MANET. *Wireless Personal Communications, 82*(2), 689–708.
41. Chakrabarti, C., Banerjee, A., Chakrabarti, S., & Chakraborty, A. (2015). A novel approach for non-cooperative node detection and avoidance using reputation-based scheme in mobile ad hoc network. In K. Maharatna, G. Dalapati, P. Banerjee, A. Mallick, M. Mukherjee (Eds.), *Computational Advancement in Communication Circuits and Systems. Lecture Notes in Electrical Engineering* (Vol 335, pp. 279–289). New Delhi: Springer.
42. Velloso, P. B., Laufer, R. P., Cunha, D. D. O., Duarte, O. C. M., & Pujolle, G. (2010). Trust management in mobile ad hoc networks using a scalable maturity-based model. *IEEE Transactions on Network and Service Management, 7*(3), 172–185.
43. McGibney, J., & Botvich, D. (2007). Establishing trust between mail servers to improve spam filtering. In B. Xiao, L. T. Yang, J. Ma, C. Muller-Schloer, Y. Hua (Eds.), *Autonomic and Trusted Computing. ATC 2007. Lecture Notes in Computer Science,* (Vol 4610, pp. 146–155). Springer.
44. Wang, B., Chen, X., & Chang, W. (2014). A light-weight trust-based QoS routing algorithm for ad hoc networks. *Pervasive and Mobile Computing, 13,* 164–180.
45. Velloso, P. B. B., Laufer, R. P. P., Duarte, O. C. M., & Pujolle, G. (2008). A trust model robust to slander attacks in ad hoc networks. In *Proceedings of 17th IEEE International Conference on Computer Communications and Networks (ICCCN'08)* (pp. 1-6). IEEE.

46. Kansal, A., Ramamoorthy, A., Srivastava, M. B., & Pottie, G. J. (2005). On sensor network lifetime and data distortion. In *Proceedings of IEEE International Symposium on Information Theory (ISIT 2005)* (pp. 6–10). IEEE.
47. Basu, P., & Redi, J. (2004). Effect of overhearing transmissions on energy efficiency in dense sensor networks. In *Proceedings of ACM 3rd international symposium on Information processing in sensor networks—IPSN'04* (pp. 196–204). ACM.
48. NETWORK SIMULATOR-2.34. http://www.isi.edu/nsnam/ns/.
49. Hua, C., & Yum, T. S. P. (2008). Optimal routing and data aggregation for maximizing lifetime of wireless sensor networks. *IEEE/ACM Transactions on Networking (TON), 16*(4), 892–903.
50. Chen, C. L., Lee, J. W., Lin, C. Z., Chen, Y. T., Ker, J. S., & Kuo, Y. H. (2007). Generic energy-efficient geographic routing for ad-hoc wireless networks. In M. K. Denko et al. (Eds.), *Emerging Directions in Embedded and Ubiquitous Computing. EUC 2007. Lecture Notes in Computer Science* (Vol 4809, pp. 321–332). Springer.

Sunil Kumar is at present working as Associate Professor at Maharaja Agrasen University, Baddi (Solan)-174103 (H.P.) India. He received his bachelor's degree in Computer Engineering from the Kurukshetra Univesrsity, Kurukshetra (India) in 2002 and master's degree in Computer Science and Engineering from Guru Jambheshwar University of Science and Technology, Hisar (India) in 2007. He has been awarded Gold Medal for standing first in 2005–2007 batch of Master of Technology in Computer Science and Engineering, Guru Jambheshwar University of Science and Technology, Hisar (India). He earned his Ph.D degree in Computer Science and Engineering from National Institute of Technology, Hamirpur (H.P.), India. His research interests include Wireless Networks and Information Security.

Kamlesh Dutta is at present working as Associate Professor and Head of Computer Science and Engineering Department at National Institute of Technology, Hamirpur (H.P.), India. She earned her Ph.D. degree from Guru Gobind Singh Indraprastha University, Delhi (INDIA) and M.Tech. degree from Indian Institute of Technology, Delhi (India), and M.S. from Vladimir State University, Russia. Her major research interests include Artificial Intelligence, Network Security and Software Engineering. Seven students have completed their Doctorate under her guidance and other three are pursuing their Ph.D. under her. She has published more than 95 research papers in national and International Journals and Conferences. Quite a few of her technical papers have been awarded "Best paper award". She has chaired many national and international conferences and workshops. She reviews manuscripts on behalf of a large number of international journals.