Thwarting Sybil Attackers in Reputation-based Scheme in Mobile Ad hoc Networks[1]

Sohail Abbas[1], Madjid Merabti[1], Kashif Kifayat[2], and Thar Baker[3]
[1]Department of Computer Science, University of Sharjah, College of Sciences, Sharjah, UAE
[e-mail: sabbas@sharjah.ac.ae, mmerabti@sharjah.ac.ae]
[2]Department of Computer Science and Engineering, Air University, Islamabad, Pakistan
[e-mail: Kashif.Kifayat@mail.au.edu.pk]
[3]Department of Computer Science, Liverpool John Moores University, Liverpool, UK
[e-mail: t.baker@ljmu.ac.uk]

Received 3 June, 2018; revised June 20, 2019; accepted July 17, 2019; published December 31, 2019

Abstract

Routing in mobile ad hoc networks is performed in a distributed fashion where each node acts as host and router, such that it forwards incoming packets for others without relying on a dedicated router. Nodes are mostly resource constraint and the users are usually inclined to conserve their resources and exhibit selfish behaviour by not contributing in the routing process. The trust and reputation models have been proposed to motivate selfish nodes for cooperation in the packet forwarding process. Nodes having bad trust or reputation are detected and secluded from the network, eventually. However, due to the lack of proper identity management and use of non-persistent identities in ad hoc networks, malicious nodes can pose various threats to these methods. For example, a malicious node can discard the bad reputed identity and enter into the system with another identity afresh, called whitewashing. Similarly, a malicious node may create more than one identity, called Sybil attack, for self-promotion, defame other nodes, and broadcast fake recommendations in the network. These identity-based attacks disrupt the overall detection of the reputation systems. In this paper, we propose a reputation-based scheme that detects selfish nodes and deters identity attacks. We address the issue in such a way that, for normal selfish nodes, it will become no longer advantageous to carry out a whitewash. Sybil attackers are also discouraged (i.e., on a single battery, they may create fewer identities). We design and analyse our rationale via game theory and evaluate our proposed reputation system using NS-2 simulator. The results obtained from the simulation demonstrate that our proposed

[1] The initial version of this work has been presented in [1] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Deterring Whitewashing Attacks in Reputation based Schemes for Mobile Ad hoc Networks," in *Wireless Days (WD), IEEE/IFIP*, 2010, pp. 1-6.
https://doi.org/10.1109/WD.2010.5657719

technique considerably diminishes the throughput and utility of selfish nodes with a single identity and selfish nodes with multiple identities when compared to the benchmark scheme.

Keywords: selfish node, reputation and trust systems, Sybil attacks, whitewashing, game theory.

1. Introduction

Mobile Ad hoc Networks (MANETs) are constructed in a fully self-organized manner which are composed of battery powered mobile nodes that can roam across freely, following random topologies. MANETs are fully distributed and are considered as robust. These networks are not dependent on centralized infrastructure or administration. Hence, these networks are mostly used in situations where there is no fixed network infrastructure available or there is difficult to deploy one [2], for instance emergency situations, battle fields, robot networks, vehicular ad hoc networks [3], sensor networks, Internet of Things (IoTs) [4], under water networks, network of drones [5], etc.

Routing in MANETs is performed in multihop fashion (i.e., communication from a source to a destination is established through intermediate nodes falling in between the two). Since there are no dedicated routers used for routing the data traffic, routing process is purely cooperative (i.e., nodes act as hosts and also as routers in order to forward each other packets). Due to the resource constraint devices, users are always preferred to save their resources and exhibit selfish behaviour, thereby showing unwillingness to forward packets for others. In the literature, selfishness is also called misbehaviour. Various models based on trust and reputations have been proposed in the literature to enforce cooperation and counteract selfish nodes [6, 7]. Under these schemes, each node monitors its 1-hop neighbours for packet forwarding activity. If a node forwards a packet, its trust or reputation is increased and decreased otherwise. Eventually, nodes having high trust or reputation are offered with packet forwarding services and bad reputed nodes are secluded from the network. This is how nodes are encouraged to cooperate. However, the lack of efficient identity management system and the open nature of MANETs (where nodes can freely join and leave using non-persistent identifiers) enable malicious nodes to create as many identities as they like. So, a malicious node may discard its bad reputed identity and create new identity to start afresh. This is how a malicious node may whitewash its past bad history. This is called whitewashing attack which is one form of the Sybil attack [8]. Hoffman *et al*. [6] analyse this issue as follows, "*whitewashing attacks occur when attackers abuse the system for short-term gains by letting their reputation degrade and then escape the consequences of abusing the system by using some system vulnerability to repair their reputation*". In other words, non-persistent identifiers are difficult to hold malevolent nodes accountable for their malign acts.

In order to mitigate the effect of whitewashing and make it a less attractive choice for the attackers, some authors proposed to assigning the smallest possible trust or reputation for the new entrants to start with or imposing entry fee for every newcomer [9, 10]. These solutions are scalable and effective due to the fact that they do not rely on any centralized trusted third party for managing identities. However, in the former approach, the smallest starting trust or reputation may still be exploited due to the zero cost identities. The latter approach, i.e.

monetary based entry fee for each identity may not be suitable for MANETs due to a number of reasons. First, it suffers from fee management complications. Second, it requires a tamper proof hardware to secure the fee payments' mechanism. Third, fee structure and payments in the form of money or charged text message [9] would cause extra burdens for the users and the system. Owing to these limitations, we incorporate a non-monetary fee concept in our proposed reputation-based scheme for each newcomer. We use fee as a kind of work done, i.e. cooperation in the form of packet forwarding, imposed on each new identity in the system. Each new identity must expend a portion of its battery power (consuming it to provide packet forwarding service to its neighbours) in order to pay the fee. Our proposed fee payment system is scalable and distributed without relying on any centralized fee management system or tamper proof hardware. Since the fee applies on each new identity, our proposed scheme thwarts Sybil attackers and whitewashers alike. Attackers can execute fewer whitewashing attacks depending upon its existing battery. In this paper, we focus more on whitewashing attacks than the Sybil attacks but the proposed scheme will work for both. This will not prevent malicious nodes from identity creation but will definitely deter normal selfish nodes. We use game theory to model the cooperation among nodes and to analyse the whitewashing deterrence. The fee represents a social cost incurred by each new node; yet, it is still useful and advantageous for improving the performance. Finally, we evaluate our scheme using the NS-2 simulator and the result obtained illustrate that our proposed technique considerably decreases the utility and throughput consumed by malicious nodes that exploit multiple identities, as compared to our benchmark, i.e. CONFIDANT [11, 12].

The rest of the paper is organized as follows. In Section 2, we discuss the proposed schemes from the literature. In Section 3, we analyse the adverse effects of selfishness during routing. Section 4 highlights the building blocks of our reputation system. In Section 5, we elaborate the fee mechanism and its inclusion in our reputation system for whitewashing attack deterrence. Section 6 is about deterrence analysis of the fee-based mechanism using game theory. In Section 7, we describe an important issue related to our scheme, (i.e., how to secure the fee and reputation information from fabrication). In Section 8, we discuss simulation-based performance evaluation of our proposed scheme. The paper is concluded in Section 9.

2. Related Work

The solutions proposed in the literature for selfish node detection or prevention are generally called cooperation enforcement schemes [7] which include credit based, reputation and trust based solutions. The main aim of these solutions is to encourage cooperation in the network and discourage selfishness.

In credit based solutions [13], nodes buy and sell the packet forwarding services and act as buyers and sellers of the service. A virtual currency, called nuggets is used for this business. When a source node tries to communicate with a distant destination node, it puts the due amount in the packet based on the number of hops involved in the path. Each node forwarding the packet collects its nuggets from the received packets until the packet reaches the destination. In order to protect the nuggets from being stolen or from a deceitful transaction, a tamper proof hardware is used. For currency management and ensuring secure transactions, a centralized entity called virtual bank is used. Due to the tamper proof

hardware and the centralized virtual bank these schemes are costly and not scalable and thus are not suitable for MANETs.

The reputation and trust-based solutions on the other hand are considered more promising due to their distributed nature. They are scalable and more robust because they do not require any extra hardware or rely on any centralized entity. Both of these schemes use Watchdog mechanism [14] to monitor the 1-hop neighbours for packet forwarding activities. In this mechanism, before transmitting any packets, each node caches the packet for time *t*. During this time nodes monitor their next hop nodes for packet forwarding behaviour. If they overhear a packet that matches with the already cached packet, reputation for the forwarder nodes is increased. If no packet is overheard that matches the cached packet within time *t*, reputation of those nodes is decreased. Schemes like [15-19], exploit the Watchdog mechanism for local reputation builds up. Watchdog mechanism is based on passive acknowledgments which suffers from ambiguous collision and receiver collision problems [20], some authors devised their schemes that use monitoring based on explicit acknowledgments [21, 22] at the cost of augmented communication overhead and some authors, such as [23-25], use other techniques for direct observation collection. For better detection accuracy, these schemes collaboratively detect selfish nodes thereby enabling nodes to disseminate their direct experience in the form of first-hand reputation ratings in the network. A problem ensued due to rating dissemination is called rumours spreading or bad mouthing [26]. Owing to this problem, some authors proposed locally aware reputation based schemes, such as [27], that do not share the ratings with the neighbours.

The above-mentioned schemes focus mainly on cooperation enforcement and other related problems such as rumour spreading and others. However, these schemes have been proposed to secure MANETs but they are not secured themselves. With non-persistent identifiers, there is no use for good nodes to increase their reputation or trust; similarly, selfish nodes may not be stopped from using the system resources and services after being secluded from the network. Because these malicious nodes will discard the bad reputed identity and create a new one. Malicious nodes can easily evade the detection and escape the accountability. Various authors, such as [6, 10, 28], also pointed out the severity of these attacks for the trust and reputation-based schemes. We believe that without counteracting these attacks trust and reputation-based schemes may not be beneficial and effectual in improving the network performance.

Various Sybil attack detection techniques have been proposed in the literature for MANETs. These schemes can broadly be categorized into cryptographic, resource testing, and localization based approaches [29, 30]. Cryptographic based countermeasures for Sybil attacks suffers from heavy computation, costly setup, and secure cryptographic key distribution and management in the MANET environments. Whereas, the resource testing-based solutions are usually based on an assumption related to restrictive hardware, such as network interface card, memory, and computation power; but hardware resources are cheap to buy now-a-days and attackers can exploit extra hardware to counteract the detection system. Finally, the localization-based solutions are more promising than the other two [31]. They use location-based information, such as signal strength, and sometimes use extra hardware, such as GPS and directional antennae to detect Sybil attacks.

Our work is different than the schemes mentioned above because they work standalone on a specific network layer and we believe it will be costly to combine these schemes into a reputation or trust based mechanism for Sybil attack detection. Moreover, more network layers interaction will be involved for the successful detection operation.

3. Adverse Effect of Selfish Nodes

In this section, we analytically show the adverse effect of selfish nodes in the network. In the lower level, the selfish nodes are involved in the routing paths and start different kinds of misbehaviour. Irrespective of their behaviour, we want to show the probability of misbehaving routes that are contaminated by the selfish nodes. We define a misbehaving route as the one having at least one selfish node along the routing path.

3.1 System model

Let us suppose a network is composed of N number of nodes that are randomly distributed over an area of size $X \times Y$. The location of each node is independent of the locations of all the other nodes. The source and the destination nodes are randomly selected in order to establish traffic flows that construct routing paths in the network. The intermediate nodes along the route/path are chosen as selfish nodes independently with a probability that is denoted by p_s. In our analysis, we examine an arbitrary route having average number of hops, h. In any route, intuitively, there will be $h-1$ packet forwarding nodes (routers) along the path from the source to the destination. Each of these intermediate nodes can act selfishly with probability p_s. Now the probability of the path having at least one selfish node is given as

$$p_{sp} = 1 - (1 - p_s)^{h-1}. \quad (1)$$

In order to evaluate Eq. (1) and to determine p_{sp}, the average number of hops h of a routing path must be known. We follow a simple approach to estimate the h, i.e. first, we estimate the average progress along each hop in the network, k. Second, we then approximate the average distance between the source and the destination, d. finally, we then can calculate h as follows.

$$h = d/k \quad (2)$$

We can further estimate the average 1-hop progress, k, as the average maximum distance between the transmitter and each of the neighbours (preferably the farthest one) within its transmission circle. For the sake of simplicity, we assume that the farthest node will be in the direction towards the destination node. The average number of nodes falling in the radio range may be given as

$$\rho = \frac{N}{X*Y} . (\pi R^2) \quad (3)$$

Where R is the transmission range of each node and assuming that to be homogenous across all the network nodes.

The probability of all ρ nodes falling within distance r_0 from the center of the radio range (assuming location independence and randomness of nodes) may be given as

$$F(r_0) = P(All\ \rho\ nodes\ falling\ within\ a\ circle\ of\ radius\ r_0) = [P(a\ node\ resides\ with\ r_0)]^{\rho}$$

$$= \left[\frac{\pi {r_0}^2}{\pi R^2}\right]^{\rho}$$

$$= \frac{{r_0}^{2\rho}}{R^{2\rho}}$$

By definition, the probability density function $f(r_0)$ of progress r_0 from the source is given by the derivative of $F(r_0)$:

$$f(r_0) = \frac{d}{dr}F(r_0) = \frac{2\rho\,.\,{r_0}^{2\rho-1}}{R^{2\rho}}$$

The average progress k can then be calculated as the expected value of r w.r.t the $f(r_0)$,

$$k = \int_0^R r_0 f(r_0) dr_0 = \frac{2\rho\,.R}{2\rho+1} \quad (4)$$

In Eq. (4), when $\rho = 0$, there can be no progress made, hence, $k = 0$. And, when $\rho = 1$, the progress will become the expected value of the distance on which the only node is located from the center, i.e. $k = \frac{2}{3}R$. Furthermore, when ρ is large the progress ultimately approaches R, i.e. $k \to R$.

For uniformly distributed nodes in a network of size $X \times Y$ (assuming the squared area: $X = Y$), the expected distance between two random nodes (i.e. source and destination) is given as

$$d = 0.5214054L \quad (5)$$

The d in Eq. (5) is the Euclidean distance between a random source and a random destination deployed in a squared area of side L [32].

The expected number of hops using Eq. (4) and (5) can be estimated as follows.

$$h \approx \frac{d}{k} \approx \frac{(2\rho+1).(0.5214054L)}{2\rho\,.R} \quad (6)$$

putting the value of h in Eq. (1), we get

$$p_{sp} = 1 - (1 - p_s)^{\frac{(2\rho+1).(0.5214054L)}{2\rho\,.R}-1} \quad (7)$$

We use Eq. (7) in order to compare the probability of selfish routes when the network area of size 1000x1000 and 250m radio range for different number of nodes, the numerical results are depicted in **Table 1**. It is evident from the results that the probability of selfish routes/paths increases with the increase in selfish nodes ratios. The number of nodes also affects the value of P_{ps}, which may be due to more routes created and hence polluted by selfish nodes in the network. Furthermore, the adverse effect of selfish nodes in the network can also be observed from the table. For instance, when the selfish nodes ratio is 30% in the network, around 50% of the routes contain at least one selfish node in the path. This high probability would definitely lead the network into severe throughput performance degradation.

Table 1. P_s vs. node density

P_s = 0.1			
Nodes	50	100	200
P_{ps}	0.06	0.07	0.08

P_s = 0.2			
Nodes	50	100	200
P_{ps}	0.23	0.25	0.26

P_s = 0.3			
Nodes	50	100	200
P_{ps}	0.43	0.45	0.46

P_s = 0.4			
Nodes	50	100	200
P_{ps}	0.65	0.67	0.67

4. Reputation System

4.1 System Overview

In this section, we discuss the basic working and building blocks of our proposed reputation-based scheme. We modify the Dynamic Source Routing (DSR) [33] protocol and incorporate our reputation based scheme in it. We use the watchdog mechanism [14] in order for each node to monitor its 1-hop neighbours for packet forwarding/dropping activities. In this mechanism, each node after sending packets to its next node for forwarding, promiscuously listens to the channel for the same packet being forwarded by that node. As shown in **Fig. 1**, a source node *S* sends a packet on an already established route towards node *A*. Node *S* caches the same packet for further confirmation and also assigns a timer to it. When *A* forwards the packet to *B*, due to the broadcast nature of wireless medium, *S* also receives a copy of the same packet, also known as passive acknowledgement. If the sequence number of the packet being forwarded and the cached packet at node *S* matches (before a timer expires), *S* will increase reputation value for node *A*; otherwise, *S* will decrease *A*'s reputation if it does not hear anything from *A* with the stipulated time. Using this technique, reputations are locally evolved at each node in the system. Each node maintains a table for storing these reputation ratings for every neighbour. Reputation tables are used by each and every node when forwarding packets for neighbours, for instance, if the transmitter is a well reputed node (as per the table), its packet will be forwarded otherwise ignored. The reputation ratings evolved locally via direct interactions among nodes is called first-hand reputation ratings. This provides a limited view of the system for each node; which is also more subjective. To improve the evaluation of nodes' behaviour and the detection of selfish

nodes, each node must share his first-hand reputations with its 1-hop neighbours. As a result, each node will have first-hand and second-hand (shared by neighbours) reputation information.

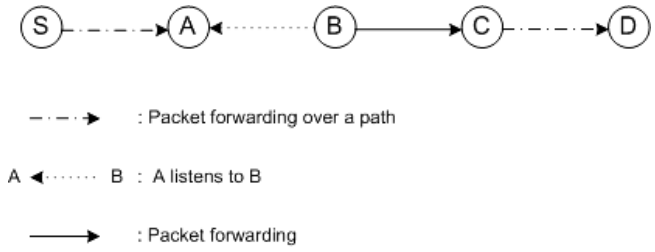


Fig. 1. Passive Acknowledgment

We adopt the reputation model followed by [26, 34] which is as follows.

Handling first-hand ratings: We define two variables α and β, the former symbolizes packet dropping or selfish behaviour whereas the latter denotes benign or packet forwarding behaviour. It is worth mentioning to note that these variables denote first-hand information and their values decrease or increase based on the nodes' behaviour monitored by the watchdog mechanism discussed above. Eq. (8) provides a reputation system that comprises first-hand information, second-hand information, and fading updates.

$$\alpha = \zeta\alpha + \omega a$$
$$\beta = \zeta\beta + \omega b \tag{8}$$

Here, a and b are second-hand reputation information received from neighbours, where a denotes selfish behaviour committed by a selfish node, b is good behaviour, ζ is the fading factor that fades reputation ratings over time, i.e. for assigning higher weights to the current actions. The value of fading factor falls in the range [0, 1]. ω is the weighting factor assigned to the second-hand ratings, its value falls in the range of [0, 1]. The initial reputation rating for a node will be $\alpha = \beta = 1$. Reputations, as in α and β in Eq. (8), are updated by three events which are depicted in **Table 2**. Each event provides different values for a, b, ω and ζ, as elaborated below.

1. First-hand update: the events α and β denote a single direct observation. If its value is 1, this indicates the confirmation of the observed behaviour (i.e., drop or forward of a packet). For example, $\alpha = 1$ implies a drop event whereas $\beta = 1$ means a forward event. These values are added to the final reputation rating, see Eq. (8).

2. Second-hand update: in this event, every node shares its direct experiences, denoted to as α and β, with its 1-hop neighbours. For instance, after recording direct interaction experiences with node j, node i shares α and β regarding node j with its 1-hop neighbours. After receiving this information shared by i regarding j, the 1-hop neighbours will treat α and β as a and b in Eq. (8) and will also apply the second-hand weight, as given in **Table 2**.

Table 2. Reputation update processes

S. No.	Process Description	*a*	*b*	ζ	ω
1	First-hand Update	0/1	0/1	1	1
2	Second-hand Update	α	β	1	Second-hand Weight
3	Fading Update	0	0	Fading Weight	1

3. Fading update: in order to motivate nodes to cooperate more, reputations are continually faded when the fading timeout expires. This will also reduce the chance for a malicious node to use its high reputation for malicious activities. During fading events, ratings are faded; however, second-hand information are just ignored, as shown in **Table 2**.

Handling second-hand information: every node shares its first-hand ratings at regular intervals – after a timeout to notify its 1-hop neighbours regarding its direct experiences. On the other side, a node after receiving first-hand ratings will conduct a deviation test on each individual rating. In other words, ratings shared by third party are compared with the directly observed reputation ratings. If the shared ratings happen to deviate too much from the own experiences (i.e., exceeding the deviation threshold), the second-hand rating in that case would not be accepted; otherwise the rating will be updated accordingly.

Detection: in order to setup a criterion that distinguishes good nodes from selfish ones, we setup a detection threshold using the formula given in Eq. (9).

$$M_T = \frac{\alpha}{\alpha+\beta} \tag{9}$$

After calculating the reputation, it is checked against the detection threshold; if it happens to be less than the threshold this would indicate a good behaviour; and selfish behaviour otherwise. Whereas reputation values above the threshold are deemed to be selfish and they will be secluded from the network (i.e., their data and route request packets would be just ignored).

5. Deterring Whitewashing

5.1 Design Rationale

In almost all of the existing reputation-based schemes, the new nodes are assigned some reputation to begin with, known as a *neutral reputation*, represented by *X* as depicted in **Fig. 2**. In this context, the smallest possible reputation a node can have, represented by *Z*, will be the reputation a little bit greater than the detection threshold. If a node has reputation *Z* (or higher), it may be allowed to use the network services. The tendency to whitewash may increase whenever the current reputation *n* of a node falls in the region α[2]. In the absence of restrictions, the neutral reputation, i.e. $\alpha = X - Z$, may always be exploited by a whitewasher. For instance, in the absence of any constraints the initial reputation opens the door for whitewashers to exploit the network services. Furthermore, after the detection, this

[2] This alpha is different than the one used in Section 4.

will also stimulate selfish nodes to whitewash by creating new identities. Some authors, for instance [10], suggested assigning the smallest possible initial reputation to new nodes; however, because of zero restrictions and zero-cost identities this reputation will always be exploited, no matter how small this reputation is made. In our reputation-based scheme, discussed above, we propose the smallest permissible reputation Y to be greater than that of the node's neutral reputation X by an amount β, called fee.

After employing the above modifications, we portray our scheme as follows. Each new node must pay an entry fee of amount β in the form of cooperation in packet forwarding thereby spending its battery power for the overall network good. As a result, this will enhance its reputation up to the level Y in its neighbours' reputation tables. It is worth mentioning that after the fee payment if a node maliciously drops packets and falls below the threshold, it would still be detected and secluded from the network by the reputation-based detection system.

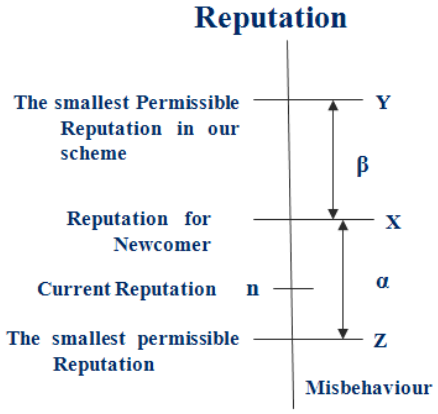


Fig. 2. Reputation levels

The benefit of fee will be that the malicious nodes may not be able to exploit the neutral reputation assigned to them because services will only be provided to them if they have reputation greater than Y. It will not be advantageous for a normal selfish node to change its identity after attaining Y reputation. By a normal selfish node, we mean a malicious node that just wants to save its battery with no other malign objectives. Such normal whitewashers will always bear a loss when changing their identities after attaining to the level Y, i.e. $X - Y = \beta < 0$; which means that after an identity change, there will always be a loss of an amount β to the reputation or to the fee that has been paid.

5.2 Fee Inclusion

We incorporate the above-mentioned fee mechanism into our reputation-based scheme as follows. Each node must pay the fee while joining the network, before consuming any network services. A node can start building its reputation once the fee has been paid, as shown in **Fig. 3**. Nodes create fee counts for nodes to which they have either interacted directly or have known about them from neighbours through fee-related (second-hand) information sharing. The fee count for a node is updated either via direct interaction experience or indirect experience when a forwarding event is experienced through overhearing (using passive acknowledgments). Forwarding events would not be considered as reputation count unless the fee has been paid completely, i.e. when the reputation becomes

greater than the *fee payment* threshold. In other words, if a node has not completed its fee payment phase and in the meantime, it forwards a packet then it will be considered as a fee update event (not a reputation update event). After the fee is paid, forwarding events would be deemed as reputation count event. Nodes will share the fee counts in addition to the reputation ratings with their 1-hop neighbours. Data and route requests packets would be ignored for nodes failing to pay the fee.

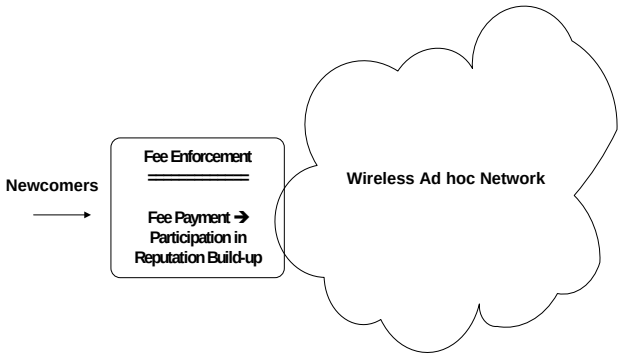


Fig. 3. The process of a new node entering into the network

5.3 Node Interactions

Mobility is an essential characteristic of MANETs. MANETs enable nodes to freely move in the network from one neighbourhood to another interacting with different nodes. Due to the random mobility patterns, nodes interact with old and new nodes. Reputation tables may help nodes distinguish between new and already known nodes, i.e. the existence of an entry for a node in the reputation table would indicate a known node, and the absence of an entry will indicate a new node. Some of the nodes will be indirectly known through the neighbouring nodes when they share their interactive experience with those nodes in the form of second-hand reputation information, as discussed above. According to the reputation table, nodes can categorize other nodes into different classes, for instance, nodes that have paid the fee, we will call them as *mature* nodes, and nodes that have not paid the fee; we call them *new* nodes. As depicted in **Table 3**, there are 4 possibilities of nodes' interactions. Columns indicate data traffic sources and rows indicate the next hop nodes along the routing path. Suppose $N_i \longrightarrow N_j$ is the communication pattern between source node N_i and destination node N_j, the arrow designates the direction of data traffic flow. The number of interaction cases can be formulated based on mature and new nodes as follows.

Table 3. Node Interaction Policy Matrix

	Receiver		
Sender	**Nodes**	**Mature**	**New**
	Mature	1. Cooperate	2. Cooperate
	New	3. Ignore	4. Ignore

1. Both nodes N_i and N_j are mature: they would offer services to each other.
2. Node N_i is mature and N_j is new: in this case if node N_j is not selfish then it should forward N_i's packets to pay the fee.
3. Node N_i is new and node N_j is mature: node N_j would ignore the data traffic generated from node N_i only if node N_j did not get any second-hand information from its neighbours about node N_i (that the fee has been paid).
4. Both N_i and $N_j$are new: they simply ignore the service requests from each other. It is worth mentioning here that when new nodes ignore one another, this might create a deadlock at the bootstrapping in the network because all the nodes are new and ignore each other. That is why, in our scheme, the fee enforcement would commence from the first detection, not at the time of bootstrapping. This assumption is valid because an attacker usually whitewashes after exploiting its first identity for malign actions.

6. Analysis of the Deterrence

6.1 Battery Consumption Perspective

In this section, we analyse the deterrence produced by our proposed scheme. Assuming a generic and theoretic communication model that is in place for wireless ad hoc networks, in order to send a message to a destination, a source node first creates a message and stores it in memory for further transmission. Assuming that the path from the source to the destination has already been established via a routing protocol, the source node would send out the message to the nearest 1-hop neighbour along the route to the destination. Let E_{T} be the amount of energy (*i.e.*, battery power) consumed in all this processing and transmission of a packet. Let E_{R} and E_{F} be the amount of energy consumed in receiving and forwarding a packet, respectively. In order to maximize the life time, a selfish node would try to employ itself in actions that bear it low battery power consumption. Let ΔE be the minimum amount of energy a selfish node may consume by choosing among the actions, like transmission, reception or forwarding. Assuming $E_{\max}(n)$ be the maximum battery available to a node n. The maximum life span of node n's communication capability $C(n)$ can be defined as follows:

$$C(n) = \frac{E_{\max}(n)}{\Delta E} \tag{10}$$

Eq. (10) implies that the communication capability of node n depends on (and directly proportional to) the maximum available energy and (inversely proportional to) the energy required for each packet to be forwarded, transmitted, or received; the selection from these three activities solely depends on the attacker's choice for increased lifetime.

Let β be the number of packets forwarded by node n for others as a fee payment. Further, let node n may utilize I identities simultaneously (acting as a Sybil attacker) or use them one after the other (acting as whitewasher). By incorporating β and I into Eq. (10), according to our proposed scheme, we get the following.

$$C(n) = \frac{E_{\max}(n)}{\Delta E} - (\beta \times I) \tag{11}$$

Eq. (11) demonstrates that the communication capability of a node depends on β and I as well. Firstly, when the amount of fee imposed is augmented, i.e. β, then $C(n)$ is decreased. This is because of the greater the number of packets forwarded as a fee; the lower the amount of $C(n)$ would become for node n's own communications. Secondly, the greater the number of identifiers node n employs for whitewashing or Sybil attacks, the greater number of times the fee will be paid. Hence, node n would have a lower amount of $C(n)$ for its own communication. This sort of fee inclusion, we believe, would demoralize and discourage selfish nodes from exploiting multiple identities.

This proposed scheme thwarts the Sybil attackers and whitewashers alike, because the product $\beta \times I$ in Eq. (11) is performed on both of the attackers alike. Further, the product $\beta \times I$ would also improve the overall system performance in terms of utility and throughput because fee payment increases contribution in the network.

6.2 Game Theoretic Analysis

In order to analyse the decision making of individual nodes participating in the proposed fee-based mechanism, we use non-cooperative game theory. We first analyse the strategy (or strategies) available to a self-centric node (we call it a rational node in the game theory context) in taking decision whether to cooperate or not during interactions with neighbours. Subsequently, we use this model to capture the cooperation in the network and to analyse whitewashing and its deterrence.

6.2.1 System Model

In this section, we give an overview of the necessary notations and elements of the non-cooperative games. Detail discussion and rigorous treatment of the subject can be found in [35, 36].

One of the main objectives of game theoretic models is the study of games, which are basically considered as formal models of interactive decision-making circumstances. A strategic-form non-cooperative game may be denoted by $\Gamma = \langle N, A, u \rangle$ having the following elements:

1. A finite set of players $N = \{1, 2, 3, \dots, n\}$.
2. A finite set of actions available to each player, denoted by $A: a \in A = \prod_{i=1}^{n} A_i$ which is the space of all action tuple. Each element $a_i$of the space a belongs to actions profile of player i, i.e. A_i. The action profile $a = (a_i, a_{-i})$ would mean the player i's action $a_i$during an arbitrary play and the other $n - 1$ players' actions a_{-i}. In the same way, other players' action profiles excluding i can be represented by $A_{-i} = \prod_{j \neq i} A_i$.
3. The preferences or benefits gained by each player $i \in N$ over action profiles can be represented by a utility function $u_i: A \to \mathbb{R}$ and $u = (u_1, u_2, \dots, u_n): A \to \mathbb{R}^{\boldsymbol{n}}$is the utility vector for the whole game. Utility of a node i is usually calculated as $u_i = benefit - cost$.

Throughout this article, we assume that all players are rational, i.e. they are inclined to maximize their payoffs (utilities) during the game using their actions.

As discussed above, in MANET, since there are no dedicated routers, nodes act as routers to forward packets for each others, voluntarily. Since, nodes are usually self-centric they may not consume their batteries to forward packets for others. In order to portray this self-centric behaviour of nodes, like other existing models [37-39], we model the interaction between two neighbours as the two-player strategic form game, the payoff matrix of which can be seen in **Table 4**. Each player may opt an action from its strategy set either to cooperate (i.e., to forward packet for the neighbour) or to drop packet for the neighbour. This is denoted as the action or strategy set as (*C*, *D*). If player 1 cooperates and player 2 does not, player 1 will get –*c* payoff (it means player 1 will incur cost *c*) where $c > 0$ and player 2 will get benefit *b* as a payoff where $b > c$. The cost *c* indicates the energy consumption accrued from computation and communication costs in forwarding a packet. Similarly, the payoffs will be swapped if the players reverse their strategies. If both of them cooperate, each will get the payoff of $b - c$. Finally, if both of them do not cooperate (drop each others' packets), each of them will get zero.

In order to analyse the payoff of each node, it is evident from the table that $b > b - c > 0 > -c$. This is the typical form of the popular game, called Prisoner's Dilemma [40] where $b - c > \frac{b-c}{2}$. Since, $b > b - c \; and \; -c < 0$ irrespective of what node *j* chooses to play, drop is the best strategy for node *i*. Similarly, drop is the best strategy for node *j* against node *i*'s strategies. In other words, strategy *D* strictly dominates *C*: no matter what the opponent does, each player would better off playing *D*. In this scenario, no player can lucratively deviate from the action profile (*D*, *D*) which means the game reached a stable state, called Nash equilibrium.

DEFINITION: A Nash Equilibrium (NE) is an action tuple constituted by the mutual best response that would result a mutually advantageous outcome, such that no player can attain any benefit by unilaterally deviating from this strategy. More formally, the action profile $\bar{a} = (\bar{a_1}, \bar{a_2}, \ldots, \bar{a_n})$is a Nash equilibrium if $u_i(\bar{a_i}; \bar{a_{-i}}) \geq u_i(a_i; \bar{a_{-i}}), \forall a_i \in A_i \; and \; \forall i \in N.$

Table 4. Payoff matrix for two-player packet forwarding game

		Node j	
		C	D
Node i	C	(*b*-*c*, *b*-*c*)	(-*c*, *b*)
	D	(*b*, -*c*)	(0,0)*

The above-mentioned game is called one-shot game (once played game). Such games are not very useful because the NE ensued from one-shot games are non-cooperative. For instance, players prefer to drop than to forward packets, this does not produce a socially beneficial solution, i.e. to promote cooperation in the network. Moreover, in a real-world scenario, in MANETs, nodes play the one-shot game more than once, in a series. In game theory context, such one-shot games if played in a sequence will become a bigger game, called the repeated game, where the strategies adopted by players for the current round or stage of a game may affect their strategies choices in the upcoming rounds of the game being played. It can be shown that an *infinitely repeated* game can promote cooperative behaviour, if played by rational players. By an "infinitely repeated" game we mean a game which will eventually

end with probability one; however, the players will be uncertain about the final round. In a repeated game, the set of actions available to a player will be same throughout the game; however, the payoff for each player will be different depending upon the strategies being chosen for a particular round. It is assumed that the outcome of each round will be revealed to the players before the start of the next round. This is due to the fact that the subsequent choices (of actions or strategies) will be based on the past actions of other players. Before discussing the equilibrium strategies in repeated games, it is important to build some terminology and notation for the repeated game; we may also extend our previous notation of a single shot game, where applicable.

We assume, the first round of the game to be denoted by $t = 0$ and the last round is T (this will not violate the case when $T = \infty$ as we will see later in this section); such that the total number of rounds will become $T + 1$. The action profile played at round t can be denoted as $a^t = (a_1^t, \dots, a_n^t)$. In order to condition players' strategies selection on the past actions taken, the notion of history is used which represents all previous rounds. For instance, the history builds up at time t can be denoted as $h^t = (a^0, a^1, \dots, a^{t-1})$. The history h^tincludes all histories $h^0, h^1, \dots, h^{t-1}$. It is the concatenation of h^{t-1} and a^{t-1}, i.e. $h^t = (h^{t-1}; a^{t-1})$. Similarly, history of the entire game is $h^{T+1} = (a^0, a^1, \dots, a^T)$ and the set of all possible histories at round t can be shown as: $A^t = \prod_{j=0}^{t-1} A$.

In order to represent the players' strategies conditioned on past histories, we denote player i's action for round t as a function of his/her strategy s_i^t played during that round, that is $a_i^t = s_i^t(h^t)$. The player i's history contingent strategy set for the whole repeated game is $s_i = (s_i^0, s_i^1, \dots, s_i^T)$ and the strategy profile for the whole game can be written as $s = (s^0, s^1, \dots, s^T)$.

Let in this repeated game, each player i accumulates his/her payoffs in each round and each player tries to maximize a weighted sum of his/her payoffs (received in each round). Players would weight earlier rounds more than that of the later rounds. The player i's discounted and normalized average payoffs for T+1 round repeated game can be written as

$$(1-\delta)\sum_{t=0}^{\infty}\delta^t u_i^t$$

Where δ is called the discount factor and $\delta \in (0,1)$ and its value for any finite sequence can be calculated as

$$\sum_{t=T_1}^{T_2}\delta^t = \frac{\delta^{T_1} - \delta^{T_2+1}}{1-\delta}.$$

This is also valid for $T_2 = \infty$ because the stage game payoffs are bound; which implies that the weighted payoffs of infinitely repeated game will be finite. We can also compute the mean discounted payoffs of an infinite game for player i as follows:

$$(1-\delta)\sum_{T=0}^{\infty}\delta^T v_i^T = (1-\delta)\left[\sum_{T=0}^{t-1}\delta^T v_i^T + \sum_{T=t}^{\infty}\delta^T v_i^T\right]$$

$$= (1-\delta)\left[\frac{v_i'(1-\delta^t)}{1-\delta} + \frac{v_i''\delta^t}{1-\delta}\right]$$

$$= v_i'(1-\delta^t) + v_i''\delta^t$$

Where v_i' is the payoff of player *i* for the first *t* rounds and $v_i''$is the payoff for the subsequent rounds till infinity. Similarly, using the above procedure, we can divide the discounted payoffs for player *i* into three sub-payoffs as follows:

$$(1-\delta^t)v_i' + \delta^t[(1-\delta)v_i'' + \delta v_i'''] \qquad (12)$$

As we discussed above, in the one-shot game of PD, players will not deviate from their dominant strategies, i.e. D; hence, ensuring an uncooperative NE, i.e. (D, D) strategy profile. However, if the game is played infinitely many times or the players do not know when the game will end, cooperative NE can be achieved, as shown by authors [41, 42]. To demonstrate this, let us devise a strategy based on our proposed reputation-based scheme (but with buffer size = 1), in which a player will cooperate in the first round and then will continue to cooperate if the opponent cooperates and stop cooperation otherwise. Suppose a player plays C in the first *t*-1 rounds and suddenly changes his/her mind and plays D in order to get increased payoff. As a result, the opponent will respond also by playing D in the rest of the rounds. The discounted payoffs of the player can be computed using Eq. (12) and **Table 4** as:

$$(1-\delta^t)(b-c) + \delta^t[(1-\delta)b + \delta.0] = (b-c) - \delta^t[\delta(b-c)] \qquad (13)$$

Eq. (13) shows that by deviating from C to D even once, the overall payoff of the player is reduced, even less than what he/she would achieve through C, i.e. $b-c$, for $\delta \geq 1/2$. It indicates that the player shall be better off by playing C rather than D in the above infinitely repeated PD game. Since, no player may increase his/her payoff by deviating from C; hence, by one-shot deviation principle these strategies form a subgame-perfect equilibrium [42, 43].

Many strategies have been proposed in the literature to analyse cooperation, such as Tit-For-Tat (TFT), Generous TFT, Anti TFT, Grim Trigger [44]. These strategies have been analysed without considering whitewashing. Some authors, such as [45-47], consider whitewashers as uncooperative entities in their models; however, more practically, whitewashers may cooperate for some rounds to consume the neutral reputation and then perform a whitewash. In the above-mentioned strategies, the first move of players is C (i.e., at $t = 0$); no matter if there is a D from the opponent(s). In real world situation this one-time C may be exploited by the whitewashers while playing *n* times, each time playing with a different identity. For instance, suppose a whitewasher plans to intentionally play the first two rounds (or maybe more rounds) against his/her opponent using his fabricated identity, the game strategy profile will be $s = \{(D, C), (D, D)\}$. The payoff of the whitewasher using Eq. (12) can be computed as:

$$u_w = b(1-\delta^t) + 0 = b \qquad (14)$$

Where u_w denotes the payoff or utility of whitewasher and $\delta^t \approx 0$ because the whitewasher plays only two rounds. Eq. (14) indicates that the attacker can gain *b* amount of payoff per identity exploiting the C move of the opponent. And when the opponent reciprocates by playing D, the attacker quits and changes identity and starts new interactions in the network. The scenario repeats until the attacker achieves his objective.

As per our proposed reputation-based scheme, whitewashing is deterred if each node before entering into the game/network pays a fee at least of an amount of payoff he/she gets in the whitewashing.

Proposition 1: In a repeated game $\Gamma = \langle N, A, u \rangle$, if nodes are made to pay the fee of an amount equal to at least a payoff of a whitewash, then whitewash will become not a best strategy for a rational player.

Proof: From the payoff matrix shown in **Table 4**, in a T rounds repeated game (ignoring the discounting factor) the maximum payoff player i can gain in the k[th] round is

$$(k-1)(b-c) + b + (T-k).0 \qquad (15)$$

And minimum payoff in the same round using worst strategy is

$$(k-1)(b-c) - c + (T-k).0 \qquad (16)$$

From Eq. (15) and Eq. (16), it is evident that the payoff that instigates a player into whitewashing or deviating from cooperation is the amount $b + c$. In order to motivate a user to cooperate or to deter him/her from launching a whitewash, we propose the amount of $b + c$ to be paid as a fee, as we discussed above. What it means in our model is that if we make each user pay the amount $b + c$ as a fee before the game, whitewashing during the game will not become a best strategy anymore. Incorporating the fee in Eq. (12), we get

$$u_w = b + c - b(1 - \delta^t) = c \qquad (17)$$

Using the fee imposition, whitewashing is not as attractive as it was the case before in Eq. (14).

Proposition 2: In a repeated game $\Gamma = \langle N, A, u \rangle$, the whitewashing strategy does not lead to Nash Equilibrium.

Proof: we will prove this by contradiction. Suppose that the whitewashing strategy, denoted by s_i' is the best strategy for player i that gives higher payoff to i which according to NE implies that the following inequality holds for all players.

$$u_i(s_i', s_{-i}) > u_i(s_i, s_{-i}) \Rightarrow c > b - c$$

Which is not true according to Eq. (17) because we have another strategy that has greater payoff than s_i'.

7. Fee Information Fabrication

One of the main issues in our proposed reputation-based system is the protection of reputation and fee-related information, we refer to them as reputation table (RT). Malicious nodes may generate their own fabricated reputation ratings and fee, or tamper with the existing ones.

In order to protect the RT from being fabricated or tampered with, we use a symmetric cryptographic based technique, called one-way hash chains [48, 49]. Various authors used one-way hash chains to guard against malicious attacks, such as DoS and resource consumption attacks, etc. [49]. A one-way hash chain is usually constructed based on a hash function, H, that maps a variable length input to a fixed length bit string, i.e. $H: \{0,1\}^* \rightarrow \{0,1\}^\rho$, where ρ is the hash function output length (in bits). Examples of hash functions include MD5[50] and SHA-1 [51]. Some of the properties of an ideal hash function H include:

- *H* can take an input of any length but must generate a fixed length output.
- For any given input *x*, *H*(*x*) will be easy to compute.
- It will be computationally infeasible to computer *x* from the function *H*(*x*) (one-way property).
- *H*(*x*) will not produce identical outputs for two or more same inputs (collision-free property).

For establishing a one-way has chain, each node must select a random number $x \in \{0,1\}^{\rho}$. This random number is used further to calculate a list of values $h_i = H(h_{i-1})$ for $0 < i \leq n$ where $h_0 = x$. These hash chains are created from $h_0 \rightarrow h_n$ and are used in during the communication from $h_n \rightarrow h_0$ for data security. For instance, for an authenticated element h_n, a node can validate any value in the chain less than h_n, such as h_{n-1} and then computing $H(h_{n-1})$. Similarly, even h_{n-4} can be validated by calculating $H(H(H(H(h_{n-4}))))$ and then comparing the results with the h_n.

These chains can be created all at once and each element can be stored before usage. Alternatively, these chained elements can also be computed on-demand. Hybrid approach has also been proposed. The authors in [48, 52] proposed a storage efficient solution, i.e. one-way hash chain with *N* elements would only need *log*(*N*) computation and *log*(*N*) storage.

To use the one-way hash chains and to authenticate the reputation and fee information, each node must first distribute the h_n value to its 1-hop neighbours. Usually a trusted certification authority is used to distribute $h_n$elements in the network; however, due to the distributed architecture and mobile nature of ad hoc networks this is rarely a possibility. Assuming that each pair of nodes has pre-shared symmetric keys, each node will distribute with its immediate (1-hop) neighbours the encrypted value h_n directly without using any trusted third party, such as certification authority. Assume node *B* distributes h_n with its neighbours before sharing its RT, as shown in **Fig. 4**. Before sharing the h_i, node *B* would sequentially use it to sign the RT, for $0 \leq i < n$. Assuming that a hash value h_{i+1} has been exposed to a neighbor node (e.g., node *E*), node *B* will then create a packet and attach RT with the next element of the hash chain (i.e., h_i) as given below.

$$Pkt(RT < ID, R_{ID}, f_{ID}, timestamp >, h_i, M_{h_{i-1}})$$

The *M* is called Message Authentication Code (MAC) and it is a hash of RT, such that

$$MAC[RT < ID, R_{ID}, f_{ID}, timestamp >]_{h_{i-1}}$$

Node *E* already knows h_{i+1}, it will simply calculate $H(h_i)$ and compare with h_{i+1}. If the result is a match, the element h_i will be accepted (implying the authentic information) and will be rejected otherwise.

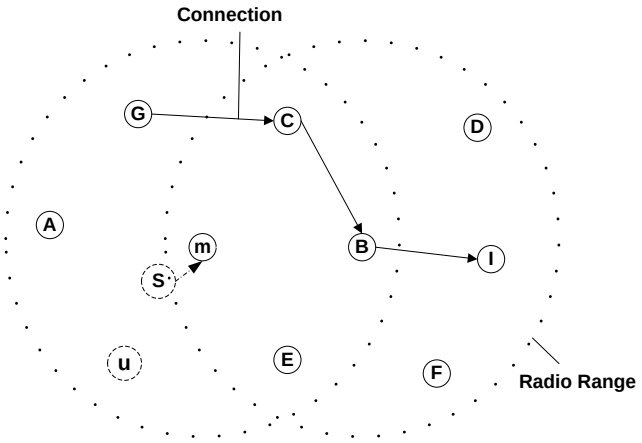


Fig. 4. Information Fabrication Scenario

Using the hash chains will protect the RT; however, there is still a chance of fabrication; especially for fee-related information. For instance, a malicious node can share falsified information regarding another malicious node in a group or in collusion. A mature malevolent node *m*, as depicted in **Fig. 4**, may collude with either another newcomer *u* (that did not pay the fee yet) or with its own created Sybil node *s*. The malevolent node *m* can clandestinely offer services either to another malevolent node *u* or to its own generated Sybil identity *s*. For instance, *m* may disseminate the identity of *u* or *s* to present an impression to its neighbours that these nodes are mature. In either case, neighbours (such as *E*, *C*, *B*) receiving this disseminated information will update their tables with fabricated information without knowing the reality.

To cope with this issue and to mitigate the effect of fabricated shared fee information, a voting-based scheme is proposed here. Assuming that the number of benign nodes is greater than that of the malicious fabricators in the network and fee information will be accepted only from those nodes that have already paid the fee. Since, in the network, the benign nodes are more than the malicious nodes, it is reasonable to presume that this will be reflected in most of the neighbourhoods. For example, if *N* neighbours of a node disseminate fee-related information about it and *m* malicious nodes (out of *N*) lie regarding the fee. Each node, receiving the fee information would decide regarding its credibility based on the number of votes. That is, a greater number of votes would imply the truthfulness of the information while assuming that most of the network nodes is benign.

For instance, as depicted in **Fig. 4**, the behaviour of node *B* in the transmission from *G* to *I* is overheard by its neighbours, *i.e. C*, *E*, *F*, *D*, and *m*. If a new node's identity is attested by the neighbours to be mature or paid identity, they would update their reputation tables accordingly and would further disseminate the updated tables to their 1-hop neighbours. The result of this dissemination would be that every node at 2-hop distance from the newly matured node would save it in their tables.

The simple solution for the above fabrication attack is that nodes should accept any shared information if the same information is validated by at least one other mature neighbour within a time window *t*. For instance, when a node, say *B*, got a first update message from a malevolent neighbour node *m*, it would not accept this update unless being validated. So, node *B* must wait for time *t* in order to get the same update message from other mature neighbour(s). And, after the timeout the message will be just ignored and discarded.

8. Simulation Based Evaluation

8.1 Selfishness with Single Identity

In this subsection, we will evaluate the effectiveness of our reputation-based scheme in the presence of selfish nodes with single identities. It is important to see how the detection of selfish node will affect the overall performance of the network in terms of the throughput available to good as well selfish nodes. In each experiment, we compare our scheme with a defenceless routing protocol; we choose a widely used routing protocol, called DSR [33] for this purpose.

8.1.1 Simulation Setup

To evaluate the performance of our proposed reputation-based system, we use NS-2.30 simulator with parameters given in **Table 5**. We created selfish nodes such that each selfish node will participate and cooperate in the routing process, i.e. forwarding control packets but drop data packets originated from other nodes. This sort of selfishness is more detrimental to the normal network functioning because selfish nodes present themselves for cooperation during the route construction process and then do not cooperate in data forwarding. The ultimately increase the chance of more routes being contaminated in the network.

The random waypoint mobility model [53, 54] is used for random movement pattern for all the simulation scenarios in which initially each node stays static for the duration of pause time. After the completion of the pause time, the node selects a random location and moves towards that location with a random velocity. This process continues until the end of the simulation.

Table 5. Simulation Parameters

Parameter	Level
Area	1K × 1K
Speed	10 m/s
Pause Time	60s
Number of Nodes	30
Number of Connections	20
Application	CBR
Simulation Time	900s
Movement	Random Waypoint Model
Node Deployment	Random
Selfish nodes	0% to 100%

8.1.2 Simulation Results

The main contribution of the reputation system is to discourage selfish nodes and to reduce their benefits acquired from selfish behaviour. In DSR with no preventive measures, the

throughput availed by selfish nodes is comparatively greater than that of the reputation enabled DSR, as shown by **Fig. 5(a)**. When the number of selfish nodes increases so is the overall drop rate in the network and also the difference between the evil throughputs decreases. In other words, nodes rarely make their packets reach their corresponding destinations. It is clear from the Fig. that when all the nodes are selfish, there is still some throughput availed by selfish nodes. The reason for this is direct interactions, where selfish source directly interacts with selfish destination with no intermediate node between them.

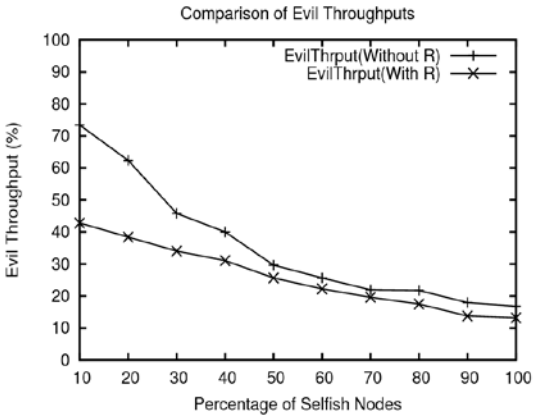


Fig. 5(a). Comparison of Evil Throughput

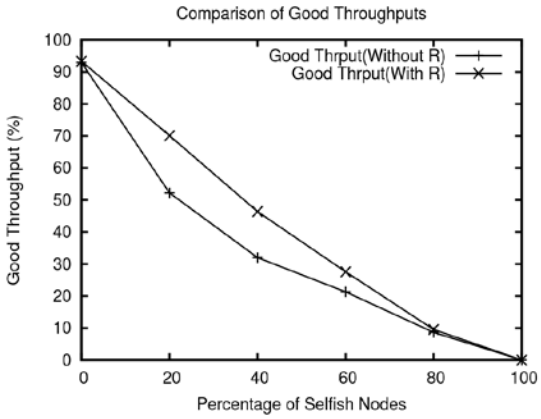


Fig. 5(b). Comparison of Good Throughput

As shown in **Fig. 5(b)**, the throughput availed by good nodes in both, the defenceless DSR and reputation enable DSR, is relatively steady. Intuitively, the good throughput drops and ceases to exist when the number of selfish nodes increases; however, the reputation enabled DSR is relatively stable. Since the reputation enabled DSR detects and isolates selfish nodes, the number of packets dropped due to selfish activity also significantly reduces, as depicted in **Fig. 6**.

8.2 Selfishness with Multiple Identities

In order to evaluate our fee incorporated reputation-based system in the presence of selfish nodes having multiple identities, we set our experiments using NS-2.30 with simulation parameters given in **Table 3**. Our aim of this simulation is to determine how our proposed fee imposition affects the network performance, i.e. throughput and utility of both evil and good nodes in different environments; and also, to determine whether it is useful. In both of the cases, we compare our proposed fee-incorporated reputation based system with our benchmark reputation based scheme, called CONFIDANT [11, 12]. Throughout the simulations, we selected the selfish nodes' percentage as 10% of the whole network population. Each selfish node exploits five identities in total for whitewashing. All results obtained and depicted are collected as mean values of 20 random seeds or simulation scenarios.

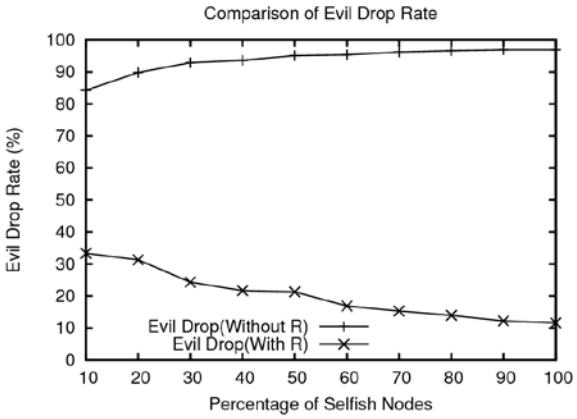


Fig. 6. Comparison of Evil Drop Rate

We use utility as a metric for our scheme evaluation. Utility is the benefit a node can attain from the network services or resources. Utility of a node *i* can be calculated as

$$u_i = b_r \sum P_{\text{received}} + b_s \sum P_{\text{sent}} - c_f \sum P_{\text{forwarded}}$$

where b_r, b_s and c_f are benefit achieved from received and sent packets and cost incurred by forwarding packets, respectively. The value of these variables is taken to be 1 in order to measure the utility in packets only. A negative utility would indicate the loss incurred by a node. Evil utility is the utility attained by malicious nodes whereas Good utility is the utility attained by benign nodes.

8.2.1 Attack Models

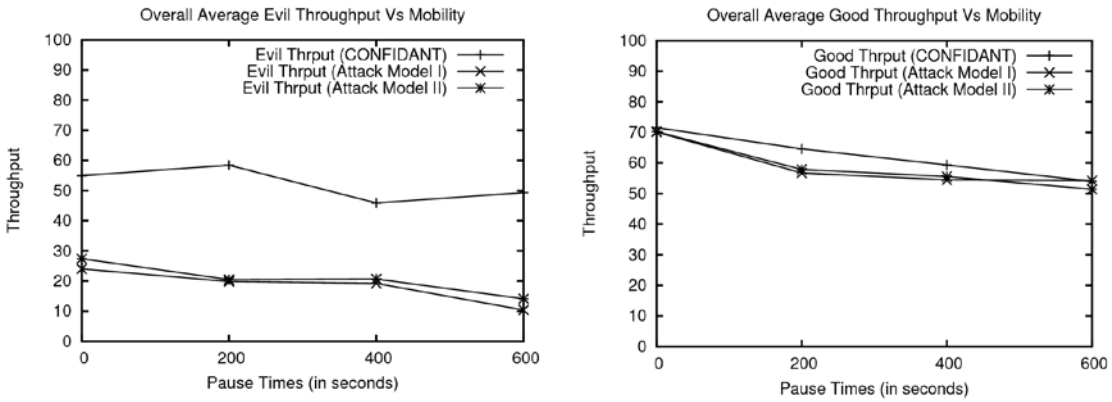
Throughout the simulation, the number of identities an attacker can exploit in order to carry out whitewashing attacks is fixed. We categorize attackers into two classes. One class of malicious nodes, called class-I attackers, will misbehave and drop packets *without* paying the fee. In a real-world scenario, these kinds of malicious nodes may be ordinary users having no expert knowledge of the field; however, who use a misbehaving software or application for extending the battery life. They usually don't know the fee threshold and how to bypass it. The other class comprises those malicious nodes that drop packets but they *do* pay the fee, we referred to them as class-II attackers. In this case, our interest would be to evaluate their impact on network throughput and utility. For instance, if some malicious nodes pay the fee and then start dropping packets.

8.2.2 Results Analysis

In case of zero restrictions enforced on identity creation in a network, i.e. users may obtain an unlimited number of new identifiers at zero cost. In such a scenario, whitewashers can achieve huge benefits from the network. The results depicted in **Fig. 7(a)** demonstrate that the throughput consumed by malicious nodes in the CONFIDANT is significantly higher than that of our scheme. It is due to the fact that there are no restrictions in place on new nodes; hence, malicious nodes may gain multi-fold benefits in terms of utility and throughput. The more the number of identifiers exploited, the more the network resources and services will be consumed and the augmented benefits a malicious node can get. By imposing the fee, the throughput consumed by malicious nodes is reduced by about half in

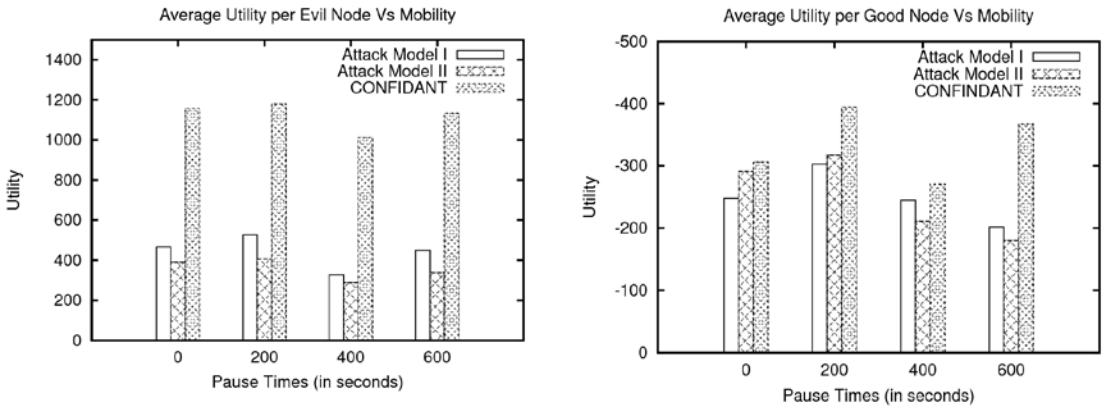
the network. The throughput consumed by class-I attackers is lower than that of the class-II attackers; because, class-II attackers pay the fee, which means they forward packets for other malicious nodes as well. That is why the malicious nodes gain a little higher throughput on average. Whereas, in CONFIDANT, the throughput consumed by benign nodes is slightly higher than that of our scheme for moderate mobility, as shown by **Fig. 7(b)**. The reason for this reduced good throughput in our scheme is due to the situation when two new nodes ignore each other data traffic.

In CONFIDANT, the average utility gained by a malicious node is significantly higher as compared to our scheme, as depicted in **Fig. 8(a)**. One of the reasons behind this is that in CONFIDANT malicious nodes drop 100% packets, i.e. no forwarding at all; however, these malicious nodes may still consistently benefit from the neutral or initial reputation. The utility of class-II attackers is less than that of the class-I attackers because of class-II attackers pay their fee; hence, their overall packet forwarding count is greater as compared to class-I attackers.



(a) (b)

Fig. 7. Overall average (a) evil and (b) good throughput *vs.* mobility



(a) (b)

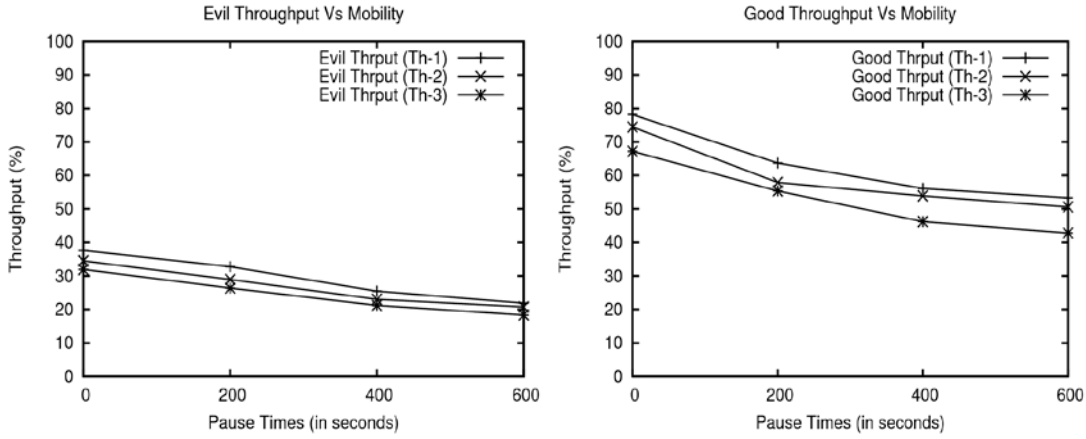
Fig. 8. Average utility per (a) evil and (b) good nodes *vs.* mobility

In CONFIDANT, benign nodes suffer comparatively more than they do in our scheme. The more benefit the malicious nodes gain, the more the benign nodes suffer. It is due to the fact that good nodes forward malicious nodes' packets before being detected; hence, good nodes have low utility. As depicted in **Fig. 8(b)**, in CONFIDANT benign nodes enjoy comparatively less utility than in our scheme (note that the y-axis shows negative values in **Fig. 8(b)**) as their packets hardly ever reach their destinations due to the malicious nodes in the network. Since class-II attackers pay the fee by forwarding packets for others; hence, in their presence, the good nodes suffer less than in the scenarios where class-I attackers exist.

It important to check the effect of the fee threshold β on the evil and good throughputs as well as on the packet drops due to the new-new node interactions. For this purpose, we set up three thresholds such that $Th\text{-}3 > Th\text{-}2 > Th\text{-}1$, where *Th* stands for threshold.

Higher threshold produces low evil throughput as compared to smaller thresholds, as shown in **Fig. 9(a)**. However, it also produces low good throughput because of the packet drops in fee payment phase, **Fig. 9(b)**. So a moderate threshold will be preferable that thwarts whitewashers by producing low evil throughput and should not reduce good throughput. In highly mobile environments, the higher threshold (*Th*-3) causes more data packet drops than the lower thresholds, as shown in **Fig. 10**. It is because the high mobility increases new-new node interactions. In a static scenario, the same situation occurs but with low packet drops than the mobile one.

From the above discussion, it is evident that *Th*-2 is the better option among the three.



(a) (b)

Fig. 9. Average (a) evil and (b) good nodes throughputs with fee thresholds *vs.* mobility

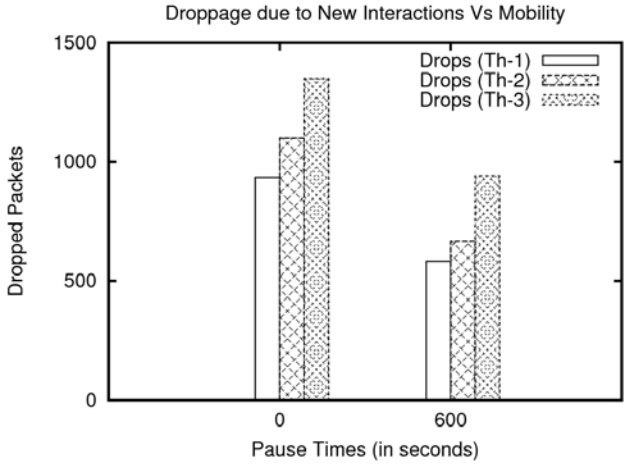


Fig. 10. Dropped packets due to the new-new node interactions vs. mobility

9. Conclusion

In this research article, we discussed selfish node and their adverse effects on the routing in mobile ad hoc networks. To detect and counteract them, we proposed a reputation-based scheme. However, like the existing reputation-based schemes, our scheme was also vulnerable to whitewashing attack. By exploiting the short-lived identities of MANETs, a smart selfish node can evade the detection mechanism by discarding the bad reputed identity and create new ones, entering the system with a fresh identity: whitewashing all their bad history. Attackers can also create over one identity simultaneously, called Sybil attacks, in order to self-promote their selves, bad mouth about other innocent nodes, disrupt the detection system, etc. To discourage and thwart such attackers, we incorporate an entry fee-based mechanism into our proposed reputation-based scheme in which each new entrant node must pay a fee in the form of a contribution to the network. Each new node would first contribute to the network and forward packets for others before consuming the network services. We analysed the effectiveness and the deterrence of the rationale using game theoretic model. This technique thwarted not only the whitewashers; but also, the Sybil attackers. Finally, we evaluated our scheme performance using NS-2 simulator and compared with a popular benchmark scheme. The results obtained confirmed that our scheme achieved better performance in reducing throughput consumed by malicious nodes and increasing good node throughput in the network.

In future, we will extend our game theoretic model to work on incomplete information.

References

[1] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Deterring Whitewashing Attacks in Reputation based Schemes for Mobile Ad hoc Networks," *Wireless Days (WD), IEEE/IFIP*, pp. 1-6, 2010. Article (CrossRef Link)

[2] E. Biagioni and S. Giordano, "Ad Hoc and Sensor Networks [Series Editorial]," *IEEE Communications Magazine*, vol. 52, no, 7, pp. 140-140, 2014. Article (CrossRef Link)

[3] S. Fatih and S. Sevil, "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV," *Ad Hoc Networks*, vol. 61, pp. 33-50, 2017. Article (CrossRef Link)
[4] A. Osseiran, O. Elloumi, J. Song, and J. F. Monserrat, "Internet of Things," *IEEE Communications Standards Magazine*, vol. 1, no. 2, pp. 84-84, 2017. Article (CrossRef Link)
[5] G. Lav, J. Raj, and V. Gabor, "Survey of important issues in UAV communication networks," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1123-1152, 2016. Article (CrossRef Link)
[6] K. Hoffman, D. Zage, and C. Nita-Rotaru, "A Survey of Attack and Defense Techniques for Reputation Systems," *ACM Computing Surveys*, vol. 42, no. 1, pp. 1-31, 2009. Article (CrossRef Link)
[7] S. Abbas, M. Merabti, and D.Llewellyn-Jones, "A Survey of Reputation Based Schemes for MANET," in *Proc. of The 11th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2010), Liverpool, UK*, 2010.
[8] J. R. Douceur, "The Sybil Attack," in *Proc. of First International Workshop on Peer-to-Peer Systems*, pp. 251-260, 2002. Article (CrossRef Link)
[9] N. B. Margolin and B. N. Levine, "Quantifying Resistance to the Sybil Attack," *presented at the Financial Cryptography and Data Security*, pp. 1-15, 2008. Article (CrossRef Link)
[10] E. Carrara and G. Hogben, "Reputation-based Systems: A Security Analysis," *ENISA Position Paper No. 2*, October 2007.
[11] S. Buchegger and J.-Y. L. Boudec, "Performance Analysis of the CONFIDANT Protocol," in *Proc. of the 3rd ACM International Symposium on Mobile Ad hoc Networking & Computing, Lausanne, Switzerland*, pp. 226-236, 2002. Article (CrossRef Link)
[12] S. Buchegger and J.-Y. L. Boudec, "A robust reputation system for P2P and mobile ad-hoc networks," in *Proc. of P2PEcon, Harvard University, USA*, 2004.
[13] Y. Yoo, S. Ahn, and D. P. Agrawal, "A credit-payment scheme for packet forwarding fairness in mobile ad hoc networks," in *Proc. of the IEEE International Conference on Communications (ICC)*, 2005. Article (CrossRef Link)
[14] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehaviour in Mobile Ad hoc Networks," in *Proc. of the 6th Annual International Conference on Mobile Computing and Networking, Boston, Massachusetts, United States*, pp. 255-265, 2000. Article (CrossRef Link)
[15] S. R. Zakhary and M. Radenkovic, "Reputation-based security protocol for MANETs in highly mobile disconnection-prone environments," in *Proc. of Seventh International Conference on Wireless On-demand Network Systems and Services (WONS)*, pp. 161-167, 2010. Article (CrossRef Link)
[16] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4647-4658, 2014. Article (CrossRef Link)
[17] N. Marchang and R. Datta, "Light-weight trust-based routing protocol for mobile ad hoc networks," *IET Information Security*, vol. 6, no. 2, pp. 77-83, 2012. Article (CrossRef Link)
[18] K. Graffi, P. S. Mogre, M. Hollick, and R. Steinmetz, "Detection of Colluding Misbehaving Nodes in Mobile Ad Hoc and Wireless Mesh Networks," in *Proc. of the IEEE Global Telecommunications Conference (GLOBECOM)*, 2007. Article (CrossRef Link)
[19] L. Zhao and J. G. Delgado-Frias, "MARS: Misbehavior Detection in Ad Hoc Networks," in *Proc. of the IEEE Global Telecommunications Conference (GLOBECOM)*, 2007. Article (CrossRef Link)
[20] N. Kang, E. M. Shakshuki, and T. R. Sheltami, "Detecting Misbehaving Nodes in MANETs," in *Proc. of the ACM 12th International Conference on Information Integration and Web-based Applications & Services*, pp. 216-222, 2010. Article (CrossRef Link)
[21] L. Kejun, D. Jing, K. V. Pramod, and B. Kashyap, "An Acknowledgment-Based Approach for the Detection of Routing Misbehavior in MANETs," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536-550, 2007. Article (CrossRef Link)

[22] K. Balakrishnan, J. Deng, and V. K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," in *Proc. of IEEE Wireless Communications and Networking Conference*, vol. 4, pp. 2137-2142 , 2005. Article (CrossRef Link)
[23] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-Based Misbehavior Detection in Wireless Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 15, no. 8, pp. 1893-1907, 2016. Article (CrossRef Link)
[24] T. Shu and M. Krunz, "Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 14, no. 4, pp. 813-828, 2015. Article (CrossRef Link)
[25] N. Battat, A. Makhoul, H. Kheddouci, S. Medjahed, and N. Aitouazzoug, "Trust Based Monitoring Approach for Mobile Ad Hoc Networks," *Lecture Notes in Computer Science: Ad-hoc, Mobile, and Wireless Networks*, pp. 55-62, 2017. Article (CrossRef Link)
[26] S. Buchegger and J.-Y. L. Boudec, "The Effect of Rumor Spreading in Reputation Systems for Mobile Ad-hoc Networks," in *Proc. of WiOpt `03: Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks, France*, 2003. Article (CrossRef Link)
[27] J. Hu and M. Burmester, "LARS: A Locally Aware Reputation System for Mobile Ad hoc Networks," in *Proc. of the 44th annual Southeast regional conference, Melbourne, Florida*, pp. 119-123, 2006. Article (CrossRef Link)
[28] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Identity-based Attacks against Reputation-based Systems in MANETs," in *Proc. of 12th Annual Conference on the Convergence of Telecommunications, Networking & Broadcasting (PGNet 2011)*, Liverpool, UK, 2011.
[29] B. N. Levine, C. Shields, and N. B. Margolin, "A Survey of Solutions to the Sybil Attack," *Technical Report 2006-052, University of Massachusetts Amherst, Amherst, MA*, 2006.
[30] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Signal Strength Based Sybil Attack Detection in Wireless Ad Hoc Networks," in *Proc. of Second International Conference on Developments in eSystems Engineering (DESE)*, pp. 190-195, 2009. Article (CrossRef Link)
[31] M. Faisal, S. Abbas, and H. U. Rahman, "Identity attack detection system for 802.11-based ad hoc networks," *EURASIP Journal on Wireless Communications and Networking*, journal article vol. 2018, no. 1, p. 128, 2018. Article (CrossRef Link)
[32] O. Younes and N. Thomas, "Analysis of the expected number of hops in mobile ad hoc networks with random waypoint mobility," *Electronic Notes in Theoretical Computer Science*, vol. 275, pp. 143-158, 2011. Article (CrossRef Link)
[33] D. B. Johnson, D. A. Maltz, and J. Broch, "DSR: the dynamic source routing protocol for multihop wireless ad hoc networks," in *Proc. of Ad hoc networking (Ch 5): Addison-Wesley Longman Publishing Co.*, pp. 139-172, 2001.
[34] J. Liu and V. Issarny, "An incentive compatible reputation mechanism for ubiquitous computing environments," *International Journal of Information Security*, vol. 6, no. 5, pp. 297-311, 2007. Article (CrossRef Link)
[35] K. Sydsaeter, A. Strom, and P. Berck, "Non-cooperative game theory," *Economists™ Mathematical Manual,Springer*, pp. 187-190, 2010.
[36] Fujiwara-Greve and Takako, *Non-cooperative game theory*, Springer, 2015.
[37] J. J. Jaramillo and R. Srikant, "DARWIN: Distributed and Adaptive Reputation Mechanism for Wireless Ad-hoc Networks," in *Proc. of The 13th Annual ACM International Conference on Mobile Computing and Networking (MobiCom'07)*, pp. 87-98, 2007. Article (CrossRef Link)
[38] F. Milan, J. J. Jaramillo, and R. Srikant, "Achieving cooperation in multihop wireless networks of selfish nodes," in *Proc. of Workshop on Game theory for communications and networks*, p. 3, 2006. Article (CrossRef Link)
[39] Z. Li and H. Shen, "Analysis the cooperation strategies in mobile ad hoc networks," in *Proc. of 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 880-885, 2008. Article (CrossRef Link)
[40] R. Axelrod, "The evolution of strategies in the iterated prisoner's dilemma," *The dynamics of norms*, pp. 1-16, 1987.

[41] M. Felegyhazi, J. P. Hubaux, and L. Buttyan, "Nash equilibria of packet forwarding strategies in wireless ad hoc networks," *Mobile Computing, IEEE Transactions on*, vol. 5, no. 5, pp. 463-476, 2006. Article (CrossRef Link)
[42] *J Ratliff Game Theory Lectures Notes*.
[43] P. Michiardi, *Cooperation enforcement and network security mechanisms for mobile ad hoc networks*, PhD Thesis, 2004.
[44] L. Buttyan and J.-P. Hubaux, *Security and cooperation in wireless networks: thwarting malicious and selfish behavior in the age of ubiquitous computing*, Cambridge University Press, 2007.
[45] S. Seradji and M. S. Fallah, "A Bayesian Game of Whitewashing in Reputation Systems," *The Computer Journal*, vol. 60, no. 8, pp. 1223-1237, 2017. Article (CrossRef Link)
[46] N. Oualha and Y. Roudier, "A game theoretical approach in securing p2p storage against whitewashers," in *Proc. of 18th IEEE International Workshops on Enabling Technologies: Infrastructures for Collaborative Enterprises WETICE'09*, pp. 128-133, 2009. Article (CrossRef Link)
[47] M. Feldman and J. Chuang, "The evolution of cooperation under cheap pseudonyms," in *Proc. of Seventh IEEE International Conference on E-Commerce Technology*, pp. 284-291, 2005. Article (CrossRef Link)
[48] D. Coppersmith and M. Jakobsson, "Almost optimal hash sequence traversal," in *Proc. of International Conference on Financial Cryptography*, pp. 102-119, 2002. Article (CrossRef Link)
[49] Y. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Networks*, vol. 1, no. 1, pp. 175-192, 2003. Article (CrossRef Link)
[50] R. L. Rivest, "RFC 1321—The MD5 Message-Digest Algorithm," *Technical report, MIT Laboratory for Computer Science and RSa Data Security, Inc.*, 1992.
[51] D. Eastlake and P. Jones, "US secure hash algorithm 1 (SHA1)," *Technical Report, Motorola and Cisco Systems*, 2070-1721, 2001.
[52] M. Jakobsson, "Fractal hash sequence representation and traversal," in *Proc. of Information Theory, 2002. Proceedings. 2002 IEEE International Symposium on*, p. 437, 2002.
[53] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, no. 3, pp. 257-269, 2003. Article (CrossRef Link)
[54] G. Resta and P. Santi, "An analysis of the node spatial distribution of the random waypoint mobility model for ad hoc networks," in *Proc. of The second ACM international workshop on Principles of mobile computing, Toulouse, Franc*e, pp. 44-50, 2002. Article (CrossRef Link)

Sohail Abbas received PhD degree in wireless network security from Liverpool John Moores University, UK in 2011. Currently, he is working as an Assistant Professor in the Department of Computer Science, College of Sciences, University of Sharjah, UAE. He has been involved in academia for more than 14 years and in research for more than 10 years. His research interests include security issues, such as intrusion detection, identity-based attacks, and trust in wireless networks, such as mobile ad hoc networks, wireless sensor networks, and the Internet of Things. Dr. Sohail is a member of various technical program committees, including IEEE CCNC, IEEE VTC, IEEE ISCI, IEEE ISWTA, etc. He is also serving various prestigious journals as a reviewer, such as Security and Communication Networks, IET Wireless Sensor Systems, Mobile Networks and Applications, International Journal of Electronics and Communications, International Journal of Distributed Sensor Networks.

Madjid Merabti is Professor of Networked and Security Systems and Dean of the College of Sciences, University of Sharjah, UAE. He was previously Dean of the School of Computing and Mathematical Sciences, Liverpool John Moores University, UK and Director of a Research Centre for the Protection of Critical Infrastructure. He is a graduate of Lancaster University in the UK. He has over 30 years' experience in conducting research and teaching in the areas of Computer Networks (fixed and wireless), Computer Network Security, Digital Forensics, Multimedia, Games Technology, and their applications. Professor Merabti is widely published with over 300 publications in these areas and leads a number of EU, UK, and industry-supported research projects. He is a frequent Keynote Speaker at major International Conferences in his research areas and an editor for the IEEE Communications Magazine Home Networking Series. Madjid is Co-Editor in Chief for the International Journal of Pervasive Computing and Communications. He is also Associate Editor for Elsevier Computer Communications Journal, Wiley Journal of Security and Communication Networks, Springer Peer-to-Peer Networking and Applications Journal, Advances in Multimedia Journal, and the Journal of Computer Systems, Networks and Communication (Hindawi Publishing). He is a member and the Chair of a number of conference TPCs and the Chair of the Post Graduate Networking Symposium series (PGNet) for UK PhD students.

Kashif Kifayat is chair of the Department of Computer Science and Engineering, Air University, Pakistan. Formerly, he worked as Reader in Computing for the School of Computing and Mathematical Science at Liverpool John Moores University and a member of the PROTECT Research Centre for Critical Infrastructure Computer Technology and Protection. He is head of Cybersecurity Research Group at Computer Science Department and also Head of Cybercrime Research at Liverpool Centre of Advance Policing Studies. Prior to this, Kashif worked as a Research Fellow in Network Security for two years at the University, where he also received a PhD for his work on the security of Wireless Sensor Networks in 2008. His research interests include network security, security of complex and scalable systems, and security in wireless sensor networks. Kashif is a member of a number of technical program committees, including IEEE SOSE and IEEE ICCCT. He is a member of the European Network and information Security Agency (ENISA) and the Cloud Computing Interoperability Forum (CCIF). Kashif is also an editor for the Journal of Convergence Information Technologies (JCIT).

Thar Baker is Senior Lecturer in Distributed Systems Engineering and Head of Applied Computing Research Group (ACRG) in the Faculty of Engineering and Technology at Liverpool John Moores University (LJMU, UK). He received his PhD in Autonomic Cloud Applications from LJMU in 2010, and became a Senior Fellow of Higher Education Academy (SFHEA) in 2018. Dr Baker has published numerous refereed research papers in multidisciplinary research areas including: Big Data, Algorithm Design, Green and Sustainable Computing, and Energy Routing Protocols. Dr Baker has been actively involved as member of editorial board and review committee for a number peer reviewed international journals, and is on programme committee for a number of international conferences. For example, he is Associate Editor of Future Generation Computer System. Dr. Baker is Expert Evaluator of EU H2020, ICTFund, and British Council.