Advance Access publication on January 13, 2011
doi:10.1093/comjnl/bxq101

A Game-based Sybil-resistant Strategy for Reputation Systems in Self-organizing MANETs

MEHRAN S. FALLAH* AND MARYAM MOUZARANI

Department of Computer Engineering and Information Technology, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran
**Corresponding author: msfallah@aut.ac.ir*

A promising method to stimulate cooperation among the nodes of a self-organizing mobile ad hoc network is the application of reputation systems. In these systems, usually, a node uses the recommendations made by the others when evaluating the reputation of the node under consideration. This renders such systems vulnerable to the Sybil attack in which an attacker forges several identities and uses them to recommend itself as a well-behaved node. In this paper, we propose a multistage-game strategy for reputation systems that discourages Sybil attacks. The underlying notion in devising such a strategy is that a Sybil identity, to remain trustworthy, should be active and sincere in recommending the others. Thus, for an effective attack, the attacker should incur the cost of maintaining the trustworthiness of its Sybil identities. This feature can be exploited to design a reputation system in such a way that the attack becomes more costly than cooperation. It is shown that the proposed strategy makes a subgame-perfect equilibrium, which justifies its deployment in real-life networks.

Keywords: cooperation stimulation; game theory; reputation systems; sybil attacks

Received 20 July 2010; revised 10 December 2010
Handling editor: Yu-Chee Tseng

1. INTRODUCTION

Cooperation among the nodes is critical to the successful operation of a self-organizing mobile ad hoc network (MANET). In order to cooperate, a node should allocate its own resources to provide services, e.g. routing and packet forwarding, to the others. As there is no centralized control on the nodes in such networks, however, a node may behave selfishly as a result of its limited resources. There are evidences that, without an appropriate incentive mechanism, cooperation cannot be achieved in these networks [1].

In recent years, a number of incentive mechanisms have been proposed to encourage cooperation in self-organizing MANETs. The underlying notion in these mechanisms is that an uncooperative node should be deprived of network services. To bring functionality to this idea, one method is to pay nodes with some kind of money only for their cooperative behavior [2–4]. As nodes are required to pay for the services they take, a badly behaved one cannot afford to buy services.

An alternative approach is the use of *reputation systems* [5–10]. By reputation we mean an estimate of the quality of a node's behavior in the network. In a typical reputation system, nodes keep track of the others' behavior and exchange this information with each other. In this way, they are able to identify—and to deny the requests from—notorious ones. It is worth noting that the use of second-hand information in addition to own observations can expedite the accurate estimation of a node's behavior. Another reason is the dynamic nature of MANETs and the high probability of meeting a stranger in an interaction.

The mechanisms based on reputation have received more attention than the ones based upon remuneration owing to their simpler structure. The possibility of having free or cheap pseudonyms, however, facilitates some attacks on the functionality of a reputation system. A well-known example is the *Sybil attack* in which an attacker masquerades as simultaneously different identities so that it is able to hide its past bad behavior by recommending itself as a good node. Throughout this paper, by an attacker we mean a selfish node that acts as above to be able to get free rides from the others in taking network services.

A number of defense mechanisms have already been devised to frustrate Sybil attacks. Most of these studies have been on peer-to-peer systems that have many features in common with self-organizing MANETs. In [11], it is first shown that local resource testing cannot prevent Sybil attacks. Then, it is claimed that the only way to prevent such attacks is the use of a central trusted authority which issues an identity after verifying the credentials unique to the requester. Nonetheless, there are a number of decentralized mechanisms based on resource testing that aim at detecting Sybil identities [12–14]. By asking the nodes to respond to our queries and assuming that an attacker does not have enough resources to reply with more than one of its identities, we may detect a Sybil identity. The location of responding nodes can act as a means for detecting such identities as well [15, 16]. Although interesting, the above mechanisms can barely be used in self-organizing MANETs. Indeed, these networks have no central authority. Moreover, local resource testing imposes a high workload on a node, which hampers its deployment in such networks.

Another line of research, which seems promising in self-organizing MANETs, has been on the use of reputation systems themselves. Cheng and Friedman [17, 18] classify reputation functions into symmetric and asymmetric ones. Such a function maps every vertex of the trust graph to a reputation value. The trust graph is a directed graph in which vertices represent the nodes of the network and a directed edge between two nodes shows that they have had interaction with each other. Edge values denote how much trust the nodes have in each other. When this function is symmetric, the reputation of a node depends only on the topology of the graph and not on the relative positions of the querier and the node whose reputation is queried. The authors then show that this kind of reputation functions are vulnerable to the Sybil attack.

Asymmetric reputation functions, on the contrary, compute the reputation of a node based on the reputation chains starting from some fixed vertices on the graph. Under some conditions, these functions can be robust against Sybil attacks. The trust graph considered in [17], however, is static and does not reflect changes in trust values according to interactions among the nodes. This is resolved in [19], where trust values are updated in such a way that the reputation system can defeat the Sybil attack. Nevertheless, the suggested scheme decreases the reputation of a truthful node reporting a successful transaction. This causes reputation assignments grow slowly, which is detrimental to normal operation of a reputation system.

This paper resolves the above shortcomings. In particular, our solution, as opposed to decentralized resource testing, imposes a negligible burden on a node. Moreover, unlike [19], any truthful report of a successful transaction leads to a reward. In fact, we exploit the cost an attacker incurs in the Sybil attack to modify reputation systems. The effect of such costs on attackers' behavior has been studied through a cost–benefit analysis [20]. When applied to reputation systems, it is deduced that the Sybil attack can be thwarted if the attacker's profit from deceiving a single node is less than the product of Sybil valuation and the cost of maintaining a single Sybil identity. Here, Sybil valuation is the minimum number of identities required for an effective attack. Therefore, to achieve a Sybil-proof reputation system, one may decide on an appropriate cost of maintaining an identity or may compel an attacker to deploy a large number of identities for an effective attack. Our proposal leverages on the latter.

To do so, we adopt a game-theoretic approach and model the interactions among the nodes as a multistage game. Then, a subgame-perfect strategy profile is proposed under which an attack is unsuccessful unless a large number of Sybil identities are employed. When solving the model, we do not attempt to find or characterize all possible equilibria. Instead, we assume that ordinary nodes follow simple pure strategies that do not require high computational or memory resources. In fact, we decide on an appropriate threshold of trustworthiness. To attain such a threshold, an attacker should accept the cost of having a number of recommendations that are enough to compensate for its reputation deficit. The higher the threshold is, the more number of Sybil identities are required for attack. On the other hand, injudicious high thresholds may interfere with the normal operation of the reputation system. It is worth noting that there are a large number of studies on cooperation enforcement in MANETs using game theory, e.g. [21, 22]. To the best of our knowledge, however, this is the first paper trying to incorporate game theory into devising a solution to Sybil attacks.

The proposed strategy profile is presented in an abstract manner so that it can be easily employed in different reputation systems. It is also shown how this strategy profile may be deployed in real-life MANETs and to what extent it is helpful in mitigating the Sybil attack.

This paper goes on as follows. Section 2 provides the assumptions underlying our study. Then, it presents the game model of interactions among the nodes in the presence of a reputation system. A symmetric subgame-perfect equilibrium is suggested in Section 3. Section 4 is about the deployment of the proposed strategy in MANETs and its usefulness in discouraging the Sybil attack. Section 5 concludes the paper.

2. GAME MODEL

The nodes of a self-organizing MANET can be viewed as autonomous entities acting on behalf of rational users. Indeed, they can be modeled as the players of a game that take their actions strategically.

2.1. Assumptions

Our modeling relies on a number of assumptions. It is assumed that every two nodes may interact with each other. In an interaction, one node requests a service from the other, which may be accepted or refused. Each node has one or more pseudonyms, or IDs, and can get new ones whenever it wants.

Nodes are not demanded to pay for their new identities. It is also assumed that the IDs of two different nodes are disjoint.

A reputation system with the following features is assumed to be present in the network. Every node records in a table the reputations of those identities it is aware of. There are two entries for an ID in such a table: its reputation in *delivering services* and its reputation in *making honest recommendations*. The former is an estimate of the node's behavior in serving the others while the latter is about the quality of recommendations it makes. The recommendation queries from an identity that does not truthfully participate in recommending the others are disregarded. It is assumed that this provides a sufficient incentive for a node—possibly except for a Sybil identity which never makes such queries—to be active and sincere in making recommendations. Furthermore, recommendations from an ID being notorious for its dishonest testimonials are not used in computing a node's reputation. This necessitates a Sybil identity to be active and honest enough so that its untruthful recommendations about the attacker can take effect. Moreover, to make a recommendation, a node should consume some resources. Hence, maintaining the trustworthiness of a large number of Sybil identities is very costly for an attacker.

The nodes are assumed selfish in the sense that they try to receive more network services while providing less services to the others. We classify them into two classes based on the extent to which they are willing to utilize complex strategies in their selfish behavior. A node that may pursue a complicated strategy is called a *potential Sybil attacker*. The others are considered as *ordinary* nodes.

In order to launch a Sybil attack, the attacker must create as many identities as required and manage them in such a way that they acquire a good reputation in recommending the others. The sufficient number of Sybil identities for an effective attack depends on the overall number of identities asked to recommend the requester. When asked about the reputation of the attacker, all the nodes except for the attacker's Sybil identities respond honestly. Therefore, the number of Sybil identities must be large enough so that their reports can compensate for the ones being witness to the attacker's bad behavior.

2.2. Model

The decisions made by the nodes of a MANET can be represented as the actions taken in a multistage game. In fact, the nodes constitute the set of players. A player's type is either *good* or *bad* that includes the node's private information about the extent to which it may deploy complicated strategies. A good player is an ordinary node, whereas a bad player is a potential Sybil attacker. A node can have one or more IDs and may be unsure about the owners of the IDs it is dealing with.

The game representing the interactions among the nodes is comprised of a number of stages. Each stage itself can be viewed as a game in which there are two players, one making a request and the other responds to it. To make a request, a player has the opportunity to deploy his Sybil identities provided he has created—and incurred the cost of maintaining—these identities in earlier stages. The stage game models this opportunity by considering the action 'To Sybil' for the player who makes the request. In fact, taking this action is an abstraction of all the things this player has done from the time he actually decided to launch an attack for his next request. Similarly, the action 'Not To Sybil' means that he has not decided to launch an attack since the last stage he made a request.

It is worth noting that although the nature determines which players are matched in a stage, the details are not applicable to our analysis. The reason is that the nature is assumed to be completely indifferent between the nodes. Indeed, in the eyes of a player, when deciding on a strategy, there is a uniform distribution over the players he may meet. Moreover, a player uses only one of his IDs to make a request in a stage. It is also assumed that a player does not strategically decide whether or not to request a service.

When a player chooses the action 'To Sybil', the cost he has incurred for preparing the attack since his last request is considered in his stage utility. As the two players who are matched in a stage are obtained from a uniform probability distribution, we can easily determine the expected number of stages lasts for a player to make a new request. In this way, we are able to approximate the expected cost a player should incur to maintain the trustworthiness of a Sybil ID. This cost is denoted by α. Thus, a player with I Sybil IDs has to pay αI between his two consecutive requests to keep these IDs trustworthy. Moreover, the cost of turning a new ID to the one whose recommendations are accepted by the others is denoted by α' with $\alpha < \alpha'$.

Figure 1 is an example showing the actions taken by a player in stages he makes a request. As shown, the cost of attack is reflected by stage utilities. This cost is computed on the basis of the required number of Sybil identities as well as the number of Sybil IDs deployed by the player in his last request. It is assumed that reviving an ID, which has not been maintained between two requests, is more costly than creating a new one. This is because a new ID has a default reputation value that requires less effort by the node to make it trustworthy.

Figure 2 shows the stage game where player i requests a service from player j. As seen, the stage utility for player i depends on his type. Note that the stage utility for a player not moving in the stage is zero. In this figure, S and DS denote the actions 'Serve the request' and 'Do not Serve the request' while TS and NTS stand for 'To Sybil' and 'Not To Sybil.' The profit from receiving a service is denoted by P. Moreover, X and E represent the cost of attack and the cost of providing a service, respectively. The reluctance of good players to do the Sybil attack is reflected by making 'To Sybil' a dominated action. To do so, a good player is assumed to receive a negative payoff when choosing this action. Furthermore, the cost a player incurs to recommend the others by his non-Sybil ID is not

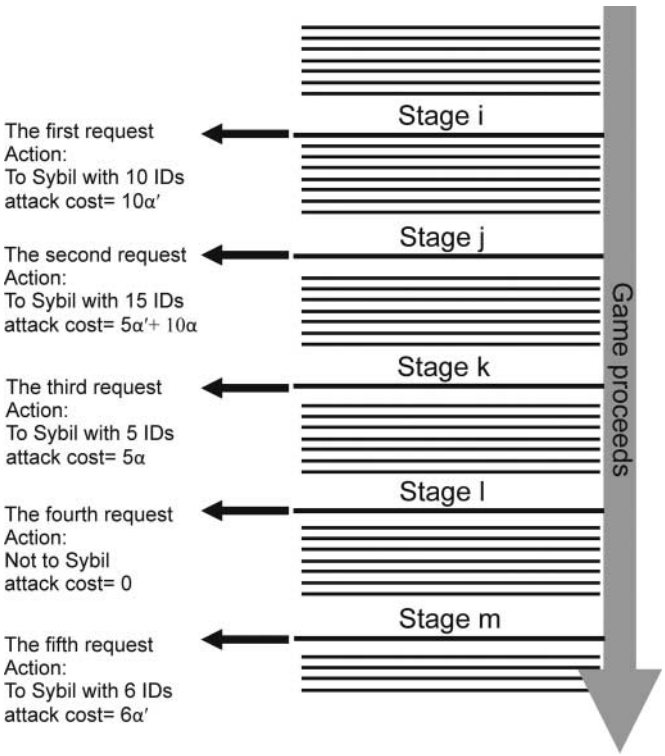

FIGURE 1. The cost of Sybil attack when a player makes a request. This cost is a function of the number of required Sybil IDs as well as the number of the ones involved in his last request.

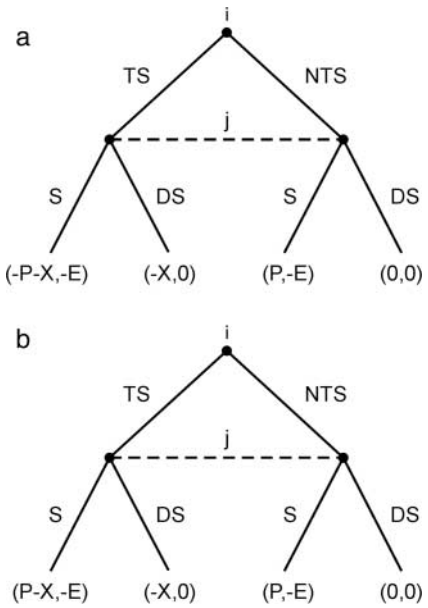

FIGURE 2. Players i and j matched in a stage. (a) Player i's type is good. (b) Player i's type is bad.

considered in Fig. 2. In fact, as all players have to pay such a cost regardless of their types and actions, it can be safely omitted from payoff values.

The overall payoff of a player is defined as what he gains under the time-average criterion. That is, for player i, it would be

$$u_i = \lim_{T\to\infty} \frac{1}{T} \sum_{t=1}^{T} u_i^t, \tag{1}$$

where u_i^t is the utility for player i in stage t. Note that player i's opponent in a stage is drawn from the set $\{1, 2, \ldots, i-1, i+1, \ldots, N\}$, where N is the maximum number of nodes in the network.

The history of the game revealed to player i at stage t when he takes an action is in the form of

$$h_i^t = \{(R^{n_{ir}}_{\mathrm{ID}_j,\mathrm{ID}_k}, \mathrm{ID}_i, a_i^{n_{ir}})\} \cup \{(\mathrm{ID}_i, a_i^{n_r}, a^{n_r}_{\mathrm{ID}_k})\}, \tag{2}$$

in which $n_{ir} < t$ ranges over the stages where the player i is requested to provide a service and $n_r < t$ over the ones he makes a request. Moreover, $R^{n_{ir}}_{\mathrm{ID}_j,\mathrm{ID}_k}$ is the ID_k's reputation as recommended by ID_j in stage n_{ir}, where ID_j ranges over the set of IDs consulted in stage n_{ir}. Furthermore, $a_i^{n_{ir}} \in \{S, DS\}$ and $a_i^{n_r} \in \{TS, NTS\}$ are player i's actions. ID_i is player i's identity requested for service in stage n_{ir} or the one he uses to make his request in stage n_r. Finally, $a^{n_r}_{\mathrm{ID}_k}$ is the action taken by the owner of ID_k when player i requests a service from him. As seen, the actions taken by the player who makes a request—TS and NTS—are indistinguishable to the player serving the request.

The set of all possible histories at stage t, for player i, is represented by H_i^t. A strategy for player i would then be a sequence of maps $s_i = \{s_i^t : H_i^t \to A^t\}_{t=0}^{\infty}$, where $A^t = \{S, DS\}$ if the player is requested for service in stage t and $A^t = \{TS, NTS\}$ when he makes a request.

3. SEARCHING FOR A NASH EQUILIBRIUM

A desired equilibrium is the one in which a player takes 'Not To Sybil' when making a request. Moreover, compliance with this equilibrium should result in cooperation, i.e. to serve when requested for a service. In this section, we first propose a symmetric strategy profile realizing these requirements. In fact, we concentrate on *simple pure strategies* that do not place excessive demands on nodes' computational power. Then, we show that it is subgame-perfect. This strategy profile prescribes the following to player i.

s_i^*: *At stage* t, *when playing with a player whose identity is* ID_k, *do the following:* (a) *take NTS if you make a request, and* (b) *if your identity* ID_i *is requested for a service, play S subject to* $R^t_{\mathrm{ID}_k} \geq \theta$ *or* $\hat{R}^t_{\mathrm{ID}_i} < \theta$ *and play DS otherwise.*

In this strategy profile, $R^t_{\mathrm{ID}_k}$ and $\hat{R}^t_{\mathrm{ID}_i}$ are obtained from

$$R^t_{\mathrm{ID}_k} = \frac{1}{|\mathcal{M}^t|} \sum_{\mathrm{ID}_j \in \mathcal{M}^t} R^t_{\mathrm{ID}_j,\mathrm{ID}_k} \tag{3}$$

and

$$\hat{R}^t_{\mathrm{ID}_i} = \frac{|\{1 \le c \le t | a^c_i = S\}|}{|\{1 \le c \le t | a^c_i = S \vee (a^c_i = DS \wedge R^c_{\mathrm{ID}_r} > \theta)\}|}, \quad (4)$$

where $\mathcal{M}^t$ is the set of identities that ID_i consults with, $R^t_{\mathrm{ID}_j,\mathrm{ID}_k}$ is ID_k's reputation as reported by ID_j, and $R^c_{\mathrm{ID}_r}$ is the reputation of the identity that has made a request from ID_i in stage c. Moreover,

$$R^t_{\mathrm{ID}_j,\mathrm{ID}_k} = \begin{cases} \dfrac{|\{1 \le c_j \le t | a^{c_j}_{\mathrm{ID}_k} = S\}|}{|\{1 \le c_j \le t | a^{c_j}_{\mathrm{ID}_k} = S \vee (a^{c_j}_{\mathrm{ID}_k} = DS \wedge \hat{R}^{c_j}_{\mathrm{ID}_j} > \theta)\}|}, & \mathrm{ID}_j \notin S_k \\ 1, & \mathrm{ID}_j \in S_k \end{cases} \quad (5)$$

in which S_k comprises the Sybil identities recommending in favor of ID_k. Note that we have added subscript j to c to emphasize that the calculation is restricted to the stages where ID_k has had interaction with ID_j.

Indeed, (3)–(5) characterize part of the reputation system. Player i calculates the reputation of the identity requesting a service based on the recommendations made by other identities according to (3). Every player updates his estimation of ID_i's social reputation—one of his own IDs—using (4) whenever ID_i is requested for a service. The last equation shows how a player—the owner of ID_j—answers the enquiry he receives about the reputation of ID_k. As seen in (5), the more an identity exhibits cooperative behavior, it gains more reputation. Moreover, playing DS while the requester's reputation is greater than θ will have negative effect on its reputation.

It is reasonable to assume that the reputation of a requesting identity, as computed using (3), remains the same for different sets $\mathcal{M}^t$ if there is no Sybil attack and the sets $\mathcal{M}^t$ are sufficiently large. We will study the strategy profile s^* under a similar assumption that we call it *homogeneity in recommendations*.

DEFINITION 3.1. *A reputation system is said to preserve homogeneity in recommendations if $\mathcal{M}^t$ is selected in such a way that*

$$R^t_{\mathrm{ID}_i} = \frac{1}{|\mathcal{M}^t|} \sum_{\mathrm{ID}_j \in \mathcal{M}^t} R^t_{\mathrm{ID}_j,\mathrm{ID}_i} = \frac{1}{|\mathcal{N}^t|} \sum_{\mathrm{ID}_j \in \mathcal{N}^t} R^t_{\mathrm{ID}_j,\mathrm{ID}_i} \quad (6)$$

holds in every stage t when all the nodes are truthful in their recommendations and $\mathcal{N}^t$ is the set of all identities up to and including stage t.

THEOREM 3.1. *The strategy profile s^* is a Nash equilibrium if the reputation system preserves homogeneity in recommendations, $\alpha M_{\min} \ge \alpha'$, and*

$$\max\left\{\frac{E}{E+P}, \frac{E}{E+\alpha'}, \frac{E-\alpha}{E}\right\} \le \theta < 1, \quad (7)$$

where $M_{\min}$ is the minimum number of nodes, other than the requester, that are asked to answer the recommendation query.

Proof. In order to prove that s^* is a Nash equilibrium, it should be shown that no unilateral deviation is profitable for a player. To do so, we consider all possible deviations by a player and show that he cannot gain when the conditions stated in Theorem 3.2 hold. In fact, the set of possible strategies for player i comprises two classes, the strategies which prescribe TS in some situations and the ones with no TS altogether. The former is called an *attack-included* strategy. Through Lemmas 3.1 and 3.2, we first prove that s^*_i outperforms the other strategies in the second class against s^*_{-i}.

LEMMA 3.1. *Playing S in any stage that player i is requested for a service is his best strategy against s^*_{-i} regardless of his type if the conditions stated in Theorem* 3.1 *hold and he follows a strategy with no TS.*

Proof. As stated earlier, the only difference between good and bad players is their payoff for playing TS. Since a player does not follow an attack-included strategy, his type is irrelevant here. We first identify the best strategies against s^*_{-i} among the ones with no TS. When player i plays at stage t, he is in one of the following states according to the value of $R^t_{\mathrm{ID}_i}$ as judged by *truthful* recommenders.

$$A : R^t_{\mathrm{ID}_i} < \theta,$$
$$B : R^t_{\mathrm{ID}_i} \ge \theta.$$

As the other players comply with s^*, their reputations become higher than θ after a finite number of stages. Thus, their decisions on whether to serve player i's request or not depend only on the reputation of the identity used by player i. Moreover, according to the hypotheses of Lemma 3.1, player i does not choose TS and the reputation system preserves homogeneity in recommendations. Thus, player i can estimate his ID_i's reputation as computed by the identity he is requesting from. This is because the player can obtain (5) from the history of his own interactions with the others and then compute $R^t_{\mathrm{ID}_i}$ using the right side of (6). In this way, he would be able to estimate possible responses to his requests. Furthermore, as player i does not take TS when requesting a service, there is no difference between his ID's reputation as may be judged by different players in a stage t. Consequently, he receives the same response in stage t regardless of the ID he is requesting from.

Evidently, only one of S or DS is the best action a player may decide on while he is in the same state. Therefore, we can represent his potential best strategies by the automata shown in Fig. 3. As seen in this figure, there are three possibilities. For example, Fig. 3b represents the strategy in which the player serves all the requests he receives. In fact, he is initially in state A and will be in state B—in the future—as a result of his good behavior. Note that, as player i does not take TS, the actions TS and NTS are not present in these automata.

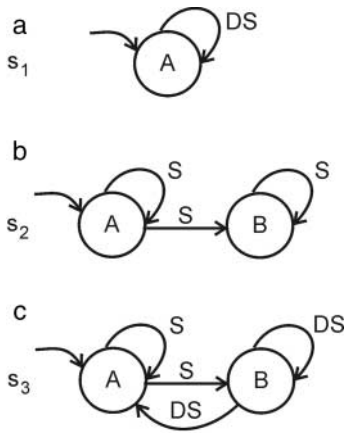

FIGURE 3. Three possible best strategies for player i.

According to (1), the time-average payoff to player i when he follows the strategy s_i is

$$u_i(s_i, s^*_{-i}) = \lim_{T\to\infty} \frac{1}{T}\Bigg[(P)\Big|\Big\{1 \le n_r \le T | a^{n_r}_{\mathrm{ID}_k} = S\Big\}\Big| + (-E)\Big|\Big\{1 \le n_{ir} \le T \mid a_i^{n_{ir}} = S\Big\}\Big|\Bigg], \quad (8)$$

where n_{ir} and n_r are the same as in (2), $a^{n_r}_{\mathrm{ID}_k}$ is the action taken by the owner of ID_k when player i requests a service from him and $a_i^{n_{ir}}$ is the action taken by player i when asked for a service. By a technique similar to [23], it can be proven that, for the strategies s_1, s_2 and s_3 illustrated in Fig. 3, (8) is reduced to (see Appendix 1)

$$u_i(s_i, s^*_{-i}) = \begin{cases} 0, & s_i = s_1 \\ P - E, & s_i = s_2 \\ \theta(-E) + (1-\theta)(P), & s_i = s_3. \end{cases} \quad (9)$$

From (7), we have

$$\theta(-E) + (1-\theta)(P) \le P - E.$$

Therefore, following s_2 would result in the maximum achievable payoff among the strategies not being attack-included. In other words, playing S in any stage when player i is requested for a service is his best strategy against s^*_{-i} if he never takes TS and the conditions of Theorem 3.1 hold. □

LEMMA 3.2. *Under the conditions stated in Lemma* 3.1, *playing s_i^* results in the same overall payoff as s_2 (shown in Fig.* 3*) for player i against s^*_{-i}.*

Proof. When other players comply with s^*, their reputations become higher than θ after a finite number of stages. If player i plays s_i^*, he has to serve all other players' requests. Therefore, he receives the same overall time-average payoff as s_2. □

Now, we should prove that s_i^* is better than any attack-included strategy against s^*_{-i}. In doing so, we show that player i's maximum payoff to the most profitable attack-included strategy, in different situations, is lower than what he achieves by playing s_i^*. Since a good player's payoff to TS is negative, he does not achieve higher payoffs by attack-included strategies. As a result, we can restrict our attention to bad players.

LEMMA 3.3. *Under the conditions stated in Theorem* 3.1, *the most achievable payoff to a bad player by following an attack-included strategy against s^*_{-i} is less than or equal to the payoff of s_i^*.*

Proof. Using the same technique as in the proof of Lemma 3.1, we first identify the potential best attack-included strategies. These strategies are shown in Fig. 4. Note that, as in Fig. 3, the states A and B reflect the status of the player's reputation as judged by truthful recommenders. In other words, recommendations by the player's Sybil identities are not considered in computing his state. Moreover, the strategies in which the player takes NTS in state A are not considered here. In fact, some of such strategies have been studied in Fig. 3. The others prescribe NTS when the player is in state A and TS when he is in state B. This is not profitable for an attacker, because he incurs the cost of maintaining his Sybil identities when they are not required, i.e. in state B, and does not deploy such identities when he is in state A.

We now identify the best strategy among the ones shown in Fig. 4. First, notice that $u_i(s_5, s^*_{-i}) < u_i(s_4, s^*_{-i})$. It is because player i receives services when he plays any of the

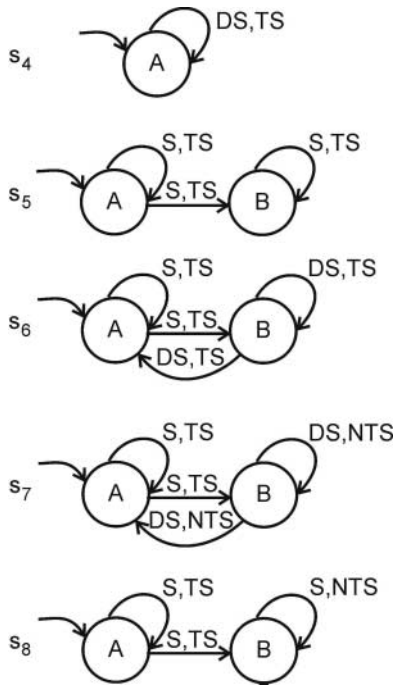

FIGURE 4. Five possible best attack-included strategies for player i.

two strategies. By following s_5, however, he has to pay the cost of serving others as well as the cost of his attack. Moreover, it holds that $u_i(s_8, s^*_{-i}) = u_i(s^*_i, s^*_{-i})$. The reason is that under s_8 player i takes S and TS for a finite number of stages in state A. His state then changes to B where he remains in forever. The action he takes in state B is the same as the ones prescribed by s^*_i. Therefore, he achieves the same payoff as s^*_i.

Consequently, we focus only on s_4, s_6 and s_7 to show that none of them is better than s^*_i against s^*_{-i}. To do so, we assume that player i takes TS in the best possible condition. That is, the resulting time-average payoff of these strategies with the least attack cost. This cost corresponds to the case when only $M_{\min}$ truthful identities answer the request for ID_i's reputation. Therefore, the average minimum number of required Sybil IDs for the above strategies can be obtained from

$$I(s_4) = \left\lceil \min\left\{ I \,\middle|\, \frac{I}{I + M_{\min}} \geq \theta \right\} \right\rceil = \left\lceil \frac{\theta M_{\min}}{1-\theta} \right\rceil \tag{10}$$

and

$$I(s_6) = I(s_7) = \lim_{\gamma \to 1^-} \left\lceil \min\left\{ I \,\middle|\, \frac{I + \gamma\theta M_{\min}}{I + M_{\min}} \geq \theta \right\} \right\rceil = \lim_{\gamma \to 1^-} \left\lceil \frac{(1-\gamma)\theta M_{\min}}{1-\theta} \right\rceil = 1. \tag{11}$$

In fact, when a player asks about player i's reputation, he receives a number of recommendations. When player i follows s_4, his reputation would be zero as judged by truthful recommenders. Therefore, if there are I Sybil identities and $M_{\min}$ truthful recommenders, he needs $I(s_4)$ Sybil IDs as defined in (10). On the other hand, playing s_6 or s_7 does not bring him a reputation value of zero in state A. Here, as seen in (11), its average is taken to be $\gamma\theta$, where $0 < \gamma < 1$. As proven in Appendix 1, γ approaches to 1 for sufficiently large t's.

Using the same method as in Lemma 3.1, it can be shown that

$$u_i(s_i, s^*_{-i}) = \begin{cases} P - \alpha \left\lceil \dfrac{\theta M_{\min}}{1-\theta} \right\rceil, & s_i = s_4 \\ \theta(P - E - \alpha) + (1-\theta)(P - \alpha), & s_i = s_6 \\ \theta(P - E - \alpha') + (1-\theta)(P), & s_i = s_7. \end{cases} \tag{12}$$

(See Appendix 2.)

From (7),

$$\theta \geq \frac{E}{E + \alpha'} \geq \frac{E}{E + \alpha M_{\min}}.$$

This is reduced to

$$E \leq \frac{\alpha\theta M_{\min}}{1-\theta},$$

and therefore,

$$u_i(s_4, s^*_{-i}) = P - \alpha \left\lceil \frac{\theta M_{\min}}{1-\theta} \right\rceil \leq P - \frac{\alpha\theta M_{\min}}{1-\theta} \leq P - E = u_i(s^*_i, s^*_{-i}).$$

Similarly, from (7), we have

$$u_i(s_6, s^*_{-i}) = P - \alpha - \theta E \leq P - E = u_i(s^*_i, s^*_{-i})$$

and

$$u_i(s_7, s^*_{-i}) = P - \theta E - \theta\alpha' \leq P - E = u_i(s^*_i, s^*_{-i}).$$

This completes the proof of Lemma 3.3. □

In this way, we have proven that unilateral deviation from s^* is not profitable for player i. Therefore, s^* is a Nash equilibrium. This completes the proof of Theorem 3.1. □

THEOREM 3.2. *Under the conditions stated in Theorem* 3.1, s^* *is subgame-perfect.*

Proof. A strategy profile is subgame-perfect if its restriction to any subgame, starting from a given history, is a Nash equilibrium. Clearly, at any subgame, a player is in one of the states A or B. Moreover, as all other players follow s^* in the subgame, they will achieve a good reputation after a finite number of stages. Consequently, we have a stationary game in the sense that the player is in the same situation in the game and its subgames. Thus, according to Theorem 3.1, s^* is subgame-perfect. □

4. DEPLOYMENT IN MANETS

Section 3 suggests a subgame-perfect equilibrium. If all players follow this strategy profile, every player takes NTS when he makes a request and plays S when he is requested for a service. Therefore, it can stimulate cooperation while discouraging the Sybil attack. To deploy it in MANETS, s^* can be regarded as a protocol that should be followed by the nodes. Thus, a node i can be equipped with the required software implementing s^*_i. If a node decides to follow this protocol, it will adjust the parameters θ and $M_{\min}$—using an appropriate mechanism—according to Theorem 3.1.

Now, we have a modified reputation system in which every node records a list of identities and their reputations. The reputations are computed through (5). Whenever requested by an identity to deliver a service, a node follows the protocol and asks the others to recommend the requester. In doing so, it uses an appropriate broadcasting technique [24] to send its query so that it can receive recommendations from at least $M_{\min}$ nodes other than the requester. Then, this node computes the reputation

of the requester from (3). By comparing the result with the threshold value, it can decide whether to serve the requester or not.

As θ satisfies (7), it must be higher than

$$C_1 = \frac{E}{E + \alpha'},$$
$$C_2 = \frac{E - \alpha}{E}$$

and

$$C_3 = \frac{E}{E + P}.$$

As alluded to in Lemmas 3.1–3.3, the conditions $\theta \geq C_1$ and $\theta \geq C_2$ allows the reputation system to discourage the Sybil attack, whereas $\theta \geq C_3$ is to stimulate cooperation. Figure 5 shows that if α is sufficiently large, cooperation enforcement leads to resistance against the Sybil attack. In fact, a greater α reflects a more crowded network where the attacker has to pay more cost to maintain the trustworthiness of his Sybil IDs. In this figure, it is assumed that $E = 3$, $P = 5$ and $\alpha' = 2\alpha$.

The proposed equilibrium, however, needs to be justified. Indeed, by considering the selfishness of nodes, being loyal to a protocol that results in serving all requests may seem unpromising. There are many justifications in the game theory itself. Nevertheless, we have conducted a number of analyses showing that the game-theoretic solution proposed in this paper is helpful in designing Sybil-proof reputation systems.

As stated earlier, the nodes of a network are at different levels of egoism. Some are called ordinary being only interested in receiving more services and not in doing the Sybil attack. It can be reasonable to assume that most of them follow the protocol exactly. However, some of them may deviate slightly by adopting a threshold value other than the one recommended by the protocol. In our analysis, we assume that they may adopt lower values of θ. Potential Sybil attackers, on the contrary, may disobey the protocol completely by launching an attack.

The results show that the more ordinary nodes follow the protocol, the less an attacker achieves from the Sybil attack. In other words, to be resistant against the Sybil attack, a sufficient number of nodes must follow what prescribed by s^*. Our analysis is conducted as follows. As stated earlier, an ordinary node may deviate from the protocol by choosing θ lower than what is suggested by (7). It is denoted by θ' and is set to the half of the least θ satisfying (7). By assuming that $\beta \in [0, 1]$ is the fraction of ordinary nodes complying exactly with the protocol, the maximum achievable payoff through an attack-included strategy would be

$$\beta\Big(\theta(P - E - \alpha) + (1 - \theta)(P - \alpha)\Big) + (1 - \beta)\Big(\theta'(P - E - \alpha) + (1 - \theta')(P - \alpha)\Big).$$

Figure 6 illustrates how the most achievable profit from an attack decreases with β. In this analysis, the parameters P, E and α are set to 5, 3 and 1, respectively. Moreover, it is assumed that $\alpha' = 2\alpha$. As seen, the profit from attack decreases more quickly for higher values of θ. The payoff when θ is set to the least value satisfying (7) is u_1. Furthermore, the payoff for a cooperative node is the constant shown by u^*. It is seen that

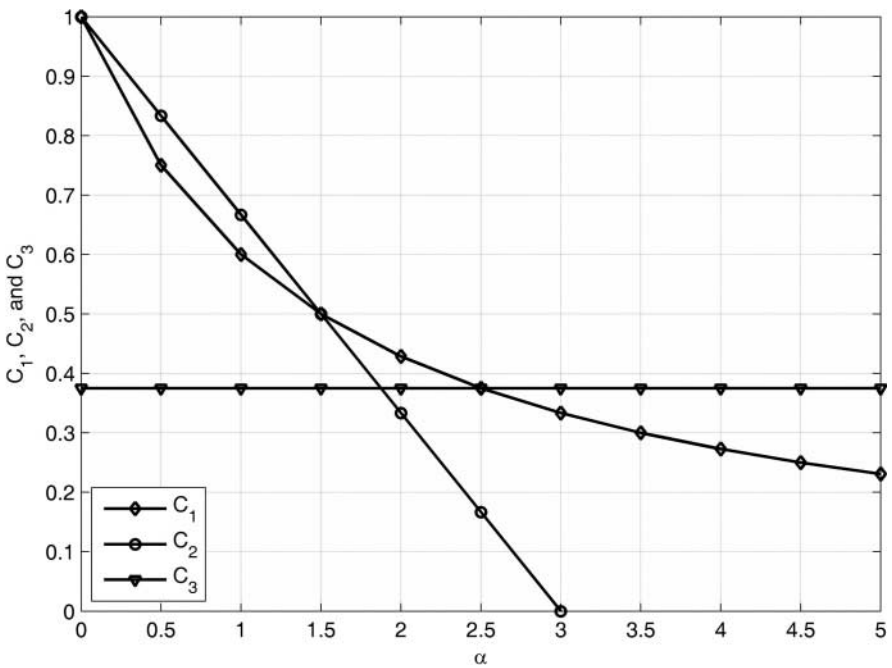

FIGURE 5. The relation between cooperation enforcement and discouraging the Sybil attack.

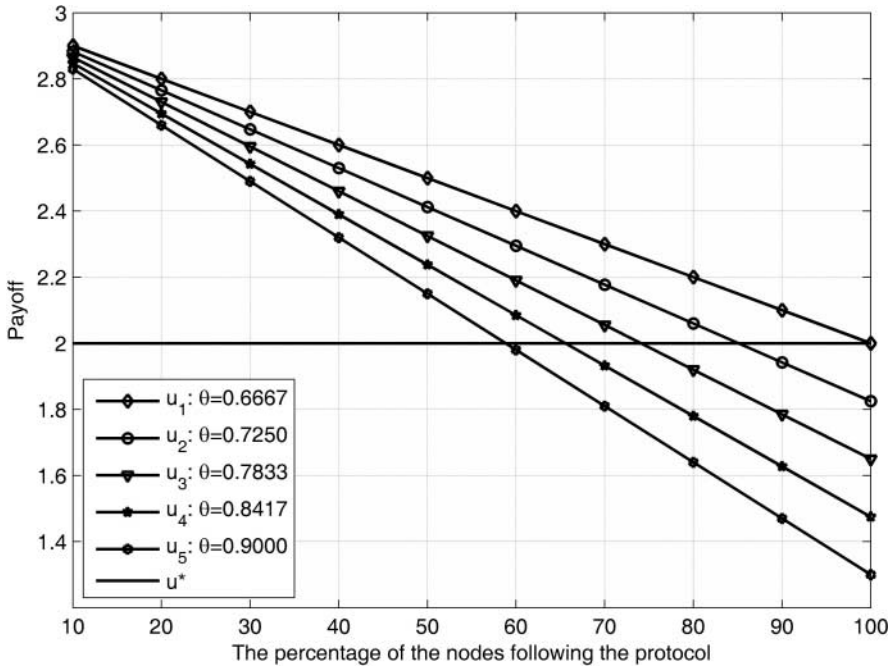

FIGURE 6. The utility of a player as a function of the percentage of the nodes complying with the equilibrium. The payoff for a Sybil attacker is u_1–u_5. The utility of a cooperative node is u^*.

the attack is not profitable when a sufficient number of nodes comply with the protocol.

It is worth noting that the attackers may interfere with each other. The reason is that the number of Sybil identities required for an attack increases with the number of attackers. As stated earlier, when a node receives a request, it consults with at least $M_{\min}$ nodes other than the requester. If there are a number of Sybil attackers among these nodes, they reply to the recommendation query with all of their Sybil IDs. Thus, for a given γ in (11), the cost of attack can be estimated at αI_n, where

$$I_1 = \left\lceil \frac{\theta(1-\gamma)M_{\min}}{1-\theta} \right\rceil,$$

$$I_n = \left\lceil \frac{\theta(1-\gamma)\Big(M_{\min} + (n-1)(I_{n-1}-1)\Big)}{1-\theta} \right\rceil,$$

and n is the number of attackers among the nodes asked for recommendation. Figure 7 shows how the cost of attack increases with n. Here, the parameters P, E and α are set to 5, 3 and 1, respectively. Moreover, $M_{\min} = 20$, $\alpha' = 2\alpha$, and θ is set to the least value satisfying (7).

It is worth noting that the mechanism proposed in this paper relies on, and is restricted by, a number of assumptions. We assume that the recommendation system is only vulnerable to Sybil attacks. In fact, it is assumed that there exist appropriate measures that prevent other attacks on the recommendation system. Without such measures, our solution is menaced by manipulation, deception and disruption that may be realized in the form of man-in-the-middle, spoofing and denial-of-service attacks. Although there are acceptable mitigation mechanisms for such attacks in traditional networks, they are among the research topics in self-organizing MANETs. Note that the use of judicious broadcasting techniques may alleviate some of the problems, though their combination with multihop transmissions seems inevitable in MANETs. The scarcity of resources in such networks is another source of difficulty in devising appropriate solutions. Nonetheless, the literature witnesses to the existence of diverse defense proposals against different kinds of attacks on MANETs, e.g. [25, 26].

Another assumption is that the recommendation queries, recommendations and requested services are delivered safely by the network. By relaxing such an assumption, we should analyze the effect of connection failures and transmission errors on the decisions made by the nodes. This requires accurate models of node mobility, network coverage and noise. For example, the effect of noise may be modeled by multiplying current payoffs by the probability of a successful end-to-end transmission [27]. Formulating the effect of mobility on the decisions made by the nodes, however, is more demanding than transmission errors. In this paper, it is assumed that the nodes matched in a stage are drawn uniformly from the set of all the nodes existing in the network. An accurate probability distribution function, however, may be obtained on the basis of the underlying model of node mobility.

As a final remark, we note that our solution is to safeguard reputation systems against Sybil attacks, where ordinary authentication and data integrity mechanisms can barely be

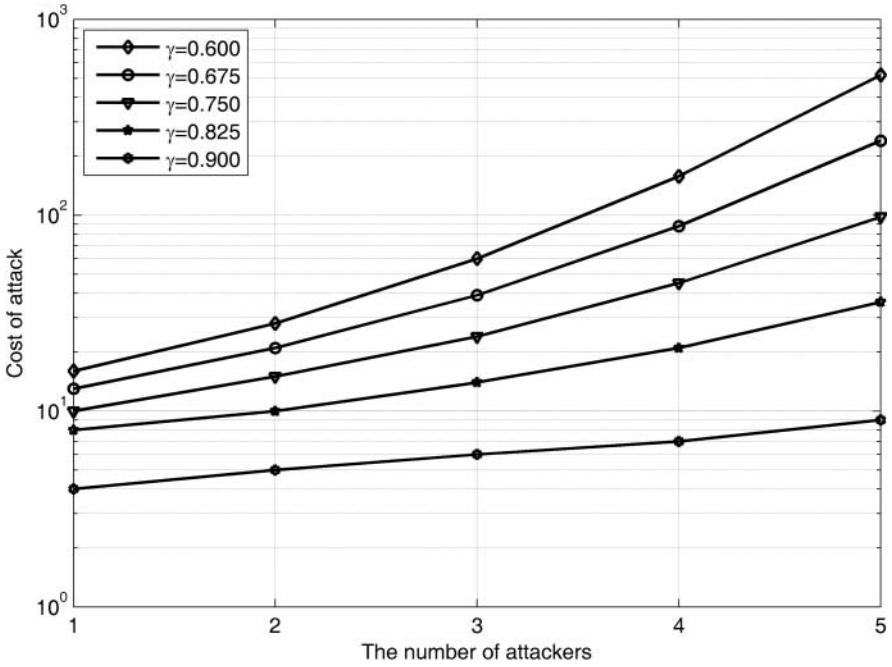

FIGURE 7. The cost of attack as a function of the number of attackers.

applied. It should be indicated that the proposed mechanism is intended to operate on top of many protocols and solutions responsible for preserving those security aspects that cannot be provided by reputation systems. For example, many attacks on integrity, e.g. man-in-the-middle, can be mitigated by the use of appropriate authentication mechanisms adapted to MANETs. A good idea has been the use of a modified public-key infrastructure in which the functions of a central certification authority (CA) is done by the nodes themselves, e.g. [28–30]. In such an infrastructure, the CA provides a public-key certificate to each identity. The authenticity of the signed messages created by a node can then be verified according to the certificate it offers. Another example is the mechanisms to prevent certain network-layer behaviors such as the ones appearing in wormhole and flood rushing attacks [31, 32]. Evidently, a complete security solution for MANETs is comprised of diverse security measures of different levels.

5. CONCLUSIONS

This paper provides a game-theoretic model of the interactions among the nodes of a self-organizing MANET in the presence of a reputation system. The reputation systems considered here are the ones based on second-hand information that are vulnerable to the Sybil attack. Then, a simple pure-strategy profile is presented that discourages such attacks. It is shown that this strategy profile is subgame-perfect which is a justification of its deployability in real-life networks. To give more justification, it is studied through a number of analyses. The results show that it can be effective in defeating Sybil attacks. In fact, it is shown that the more ordinary nodes comply with the equilibrium, the less an attacker achieves from the Sybil attack.

There is still much to be done. This study is based on a number of assumptions that can be relaxed or scrutinized in a future work. The effect of mobility on the actions taken by the nodes can be studied more accurately. Devising a mechanism being able to resist collusion among the nodes is another problem. Moreover, deployment issues such as the limitations of implementing the proposed strategy in real-life MANETs deserve careful consideration.

FUNDING

This research was supported in part by Amirkabir University of Technology.

REFERENCES

[1] Al-Karaki, J.N. and Kamal, A.E. (2008) Stimulating node cooperation in mobile ad hoc networks. *Wirel. Pers. Commun.*, **44**, 219–239.

[2] Buttyan, L. and Hubaux, J.P. (2001) Nuglets: A Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks. *Technical Report*, DSC/2001/001, EPFL, Lausanne.

[3] Zhong, S., Chen, J. and Yang, Y.R. (2003) Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks. *22nd IEEE Int. Conf. Computer Communications*

(IEEE INFOCOM'03), San Francisco, CA, USA, March–April, pp. 1987–1997. IEEE.

[4] Buttyan, L. and Hubaux, J.P. (2003) Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Netw. Appl.*, **8**, 579–592.

[5] Marti, S., Giuli, T.J., Lai, K. and Baker, M. (2000) Mitigating Routing Misbehavior in Mobile Ad Hoc Networks. *6th Annual Int. Conf. Mobile Computing and Networking*, Boston, MA, USA, August, pp. 255–265. ACM.

[6] Michiardi, P. and Molva, R. (2002) Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks. *6th IFIP Communications and Multimedia Security Conf.*, Portorosz, Slovenia, September, pp. 107–121. Kluwer Academic Publishers.

[7] Buchegger, S. and Le Boudec, J.Y. (2002) Performance Analysis of the CONFIDANT Protocol. *3rd ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, Lausanne, Switzerland, June, pp. 226–236. ACM.

[8] Buchegger, S. and Le Boudec, J.Y. (2004) A Robust Reputation System for P2P and Mobile Ad-Hoc Networks. *2nd ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems*, Cambridge, MA, USA, June, pp. 119–123. ACM.

[9] Liu, J. and Issarny, V. (2004) Enhanced Reputation Mechanism for Mobile Ad Hoc Networks. *2nd Int. Conf. on Trust Management*, Oxford, UK, March–April, pp. 48–62. Springer.

[10] Mundinger, J. and Le Boudec, J.Y. (2008) Analysis of a reputation system for mobile ad hoc networks. *Perform. Eval.*, **65**, 212–226.

[11] Douceur, J. (2002) The Sybil Attack. *1st Int. Workshop on Peer-to-Peer Systems*, Cambridge, MA, USA, March, pp. 251–260. Springer.

[12] Monica, D., Leitao, J., Rodrigues, L. and Ribeiro, C. (2009) On the Use of Radio Resource Tests in Wireless Ad Hoc Networks. *3rd Workshop on Recent Advances on Intrusion-Tolerant Systems*, Estoril, Lisbon, Portugal, June, pp. 21–26. IEEE.

[13] Newsome, J., Shi, E., Song, D. and Perrig, A. (2004) The Sybil Attack in Sensor Networks: Analysis & Defenses. *3rd Int. Symp. Information Processing in Sensor Networks*, Berkeley, CA, USA, April, pp. 259–268. ACM.

[14] Vishnumurthy, V., Chandrakumar, S. and Sirer, E.G. (2003) KARMA: A Secure Economic Framework for Peer-to-Peer Resource Sharing. *1st ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems*, Berkeley, CA, USA, June, pp. 1–6. ACM.

[15] Bazzi, R.A. and Konjevod, G. (2007) On the establishment of distinct identities in overlay networks. *Distrib. Comput.*, **19**, 267–287.

[16] Zage, D.J. and Nita-Rotaru, C. (2007) On the Accuracy of Decentralized Virtual Coordinate Systems in Adversarial Networks. *14th ACM Conf. Computer and Communications Security*, Alexandria, VA, USA, October–November, pp. 214–224. ACM.

[17] Cheng, A. and Friedman, E. (2005) Sybilproof Reputation Mechanisms. *3rd ACM SIGCOMM Workshop on Economics of Peer-to-Peer Systems*, Philadelphia, PA, USA, August, pp. 128–132. ACM.

[18] Cheng, A. and Friedman, E. (2006) Manipulability of PageRank Under Sybil Strategies. *1st Workshop on the Economics of Networked Systems*, Ann Arbor, MI, USA, June, pp. 75–82. ACM.

[19] Resnick, P. and Sami, R. (2009) Sybilproof Transitive Trust Protocols. *10th ACM Conf. Electronic Commerce*, Stanford, CA, USA, July, pp. 345–354. ACM.

[20] Margolin, N.B. and Levine, B.N. (2008) Quantifying Resistance to the Sybil Attack. *12th Int. Conf. Financial Cryptography and Data Security*, Cozumel, Mexico, January, pp. 1–15. Springer.

[21] Michiardi, P. and Molva, R. (2003) A Game Theoretical Approach to Evaluate Cooperation Enforcement Mechanisms in Mobile Ad Hoc Networks. *IEEE/ACM Int. Symp. Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt)*, Sophia Antipolis, France, March, pp. 55–58. INRIA Press.

[22] Ji, Z., Yu, W. and Liu, K.J.R. (2008) A game theoretical framework for dynamic pricing-based routing in self-organized MANETs. *IEEE J. Sel. Areas Commun.*, **26**, 1204–1217.

[23] Theodorakopoulos, G. and Baras, J.S. (2008) Game theoretic modeling of malicious users in collaborative networks. *IEEE J. Sel. Areas Commun.*, **26**, 1317–1327.

[24] Williams, B. and Camp, T. (2002) Comparison of Broadcasting Techniques for Mobile Ad Hoc Networks. *3rd ACM Int. Symp. Mobile Ad Hoc Networking and Computing*, Lausanne, Switzerland, June, pp. 194–205. ACM.

[25] Yang, H., Luo, H., Ye, F., Lu, S. and Zhang, L. (2004) Security in Mobile Ad Hoc Networks: challenges and solutions. *IEEE Wirel. Commun.*, **11**, 38–47.

[26] Van Der Merwe, J., Dawoud, D. and McDonald, S. (2007) A survey on peer-to-peer key management for mobile ad hoc networks. *ACM Comput. Surv.*, **39**, 1–45.

[27] Yu, W. and Liu, K.J.R. (2008) Secure cooperation in autonomous mobile ad-hoc networks under noise and imperfect monitoring: a game-theoretic approach. *IEEE Trans. Inf. Forensics Sec.*, **3**, 1204–1217.

[28] Arboit, G., Crepeau, C., Davis, C.R. and Maheswaran, M. (2008) A localized certificate revocation scheme for mobile ad hoc networks. *Ad Hoc Netw.*, **6**, 17–31.

[29] Chinni, S., Thomas, J., Ghinea, G. and Shen, Z. (2008) Trust model for certificate revocation in ad hoc networks. *Ad Hoc Netw.*, **6**, 441–457.

[30] Papapanagiotou, K., Marias, G.F. and Georgiadis, P. (2010) Revising centralized certificate validation standards for mobile and wireless communications. *Comput Stand. Interfaces*, **32**, 281–287.

[31] Nait-Abdesselam, F. (2008) Detecting and avoiding wormhole attacks in wireless ad hoc networks. *IEEE Commun.*, **46**, 127–133.

[32] Hu, Y. C., Perrig, A. and Johnson, D.B. (2003) Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols. *ACM Workshop on Wireless Security*, San Diego, CA, USA, September, pp. 30–40. ACM.

APPENDIX 1: PROOF OF (9)

Under the strategy s_1, a player i never serves the others and stays in state A forever. Therefore, he never receives service profits and his overall payoff would be zero. By s_2, player i gains a good reputation after a finite number of stages and goes to B where he remains forever. It is worth noting that the payoffs

obtained from a finite number of stages has no effect on the overall time-average payoff to a player. Thus, according to (8), we have $u_i(s_2, s^*_{-i}) = P - E$.

For s_3, we should first determine the empirical frequency of the times player i is in state A, which is denoted by f_A. As stated earlier, it is assumed that there are a finite number of potential nodes and identities in the network. Suppose that the number of potential identities in the network is Q and a player has had interaction with all of them for sufficiently large t's. Therefore, according to the property of homogeneity in recommendations, we have

$$R^t_{\mathrm{ID}_i} = \frac{1}{Q}\sum_{j=1}^{Q} R^t_{\mathrm{ID}_j,\mathrm{ID}_i},$$

for sufficiently large t's. Moreover, as the players who are matched in a period are obtained from a uniform distribution, it is as well reasonable to assume that $R^t_{\mathrm{ID}_j,\mathrm{ID}_i} = R^t_{\mathrm{ID}_k,\mathrm{ID}_i}$ for such t's. Thus,

$$f_A = \lim_{t\to\infty} R^t_{\mathrm{ID}_i} = \lim_{t\to\infty} R^t_{\mathrm{ID}_j,\mathrm{ID}_i}. \tag{A.1}$$

Now, we concentrate on stages m, where ID_j has made a request from ID_i and m is large enough such that $R^m_{\mathrm{ID}_i} = R^m_{\mathrm{ID}_j,\mathrm{ID}_i}$. Such an m is in one of the sets

$$\mathcal{J}_1 = \left\{m | R^{m+1}_{\mathrm{ID}_j,\mathrm{ID}_i} < \theta \le R^m_{\mathrm{ID}_j,\mathrm{ID}_i},\ a_i^{m_{ir}} = DS\right\},$$
$$\mathcal{J}_2 = \left\{m | R^m_{\mathrm{ID}_j,\mathrm{ID}_i} < \theta \le R^{m+1}_{\mathrm{ID}_j,\mathrm{ID}_i},\ a_i^{m_{ir}} = S\right\},$$
$$\mathcal{J}_3 = \left\{m \mid R^m_{\mathrm{ID}_j,\mathrm{ID}_i},\ R^{m+1}_{\mathrm{ID}_j,\mathrm{ID}_i} < \theta,\ a_i^{m_{ir}} = S\right\},$$
$$\mathcal{J}_4 = \left\{m \mid R^m_{\mathrm{ID}_j,\mathrm{ID}_i},\ R^{m+1}_{\mathrm{ID}_j,\mathrm{ID}_i} \ge \theta,\ a_i^{m_{ir}} = DS\right\}.$$

It is evident that there are infinitely many instants in $\mathcal{J}_1 \cup \mathcal{J}_2$. Furthermore,

$$R^{m+1}_{\mathrm{ID}_j,\mathrm{ID}_i} - R^m_{\mathrm{ID}_j,\mathrm{ID}_i} = \begin{cases} \dfrac{1 - R^m_{\mathrm{ID}_j,\mathrm{ID}_i}}{m+1}, & R^m_{\mathrm{ID}_j,\mathrm{ID}_i} < \theta \\ \dfrac{-1 - R^{m+1}_{\mathrm{ID}_j,\mathrm{ID}_i}}{m+1}, & R^m_{\mathrm{ID}_j,\mathrm{ID}_i} \ge \theta \end{cases}.$$

Therefore,

$$\mid R^{m+1}_{\mathrm{ID}_j,\mathrm{ID}_i} - R^m_{\mathrm{ID}_j,\mathrm{ID}_i} \mid \le \frac{2}{m+1}.$$

Given $\epsilon > 0$, if we pick

$$M(\epsilon) = \min\left\{m | m \in \mathcal{J}_1 \cup \mathcal{J}_2,\ \frac{2}{m+1} < \epsilon\right\},$$

then

$$\forall \epsilon > 0 \exists M(\epsilon) \forall m > M(\epsilon) :\mid R^m_{\mathrm{ID}_j,\mathrm{ID}_i} - \theta \mid < \epsilon. \tag{A.2}$$

From (A.1) and (A.2), we have

$$f_A = \lim_{m\to\infty} R^m_{\mathrm{ID}_j,\mathrm{ID}_i} = \theta.$$

Hence,

$$u_i(s_3, s^*_{-i}) = \theta(-E) + (1-\theta)(P).$$

APPENDIX 2: PROOF OF (12)

For s_4, the player is in state A forever where he serves no request and takes TS when he makes a request. Under such a strategy, the empirical frequency of state A is 1. Therefore, the player receives the service profit P while incurring the cost of maintaining $I(s_4)$ Sybil identities. This implies that $u_i(s_4, s^*_{-i}) = P - \alpha I(s_4)$, where $I(s_4)$ is obtained from (10).

Using the same technique as in Appendix 1, it can be proven that the empirical frequency of state A is θ when the player follows s_6 or s_7. Under s_6, the player takes TS for all the requests he makes. Thus, he pays for maintaining his Sybil identities in both states A and B. Hence, his overall payoff would be $\theta(P - E - \alpha I(s_6)) + (1-\theta)(P - \alpha I(s_6))$, where $I(s_6)$ is obtained from (11). Under s_7, on the contrary, the player does not maintain his Sybil identities when he is in state B. Thus, in state A, he should pay for the required new trustworthy Sybil identities. The cost of acquiring such an identity is greater than maintaining an existing one and is taken to be α'. This implies that $u_i(s_7, s^*_{-i}) = \theta(P - E - \alpha' I(s_7)) + (1-\theta)(P)$.