SUCCESS: A Secure User-centric and Social-aware Reputation based Incentive Scheme for DTNs

LIFEI WEI[1], HAOJIN ZHU[1], ZHENFU CAO[1]*, XUEMIN (SHERMAN) SHEN[2]

[1] *Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai, China*

[2] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, Ontario, Canada*

Received 15 October 2011; In final form 12 March 2012.

Delay/Disruption tolerant networks (DTNs) are self-organized wireless ad-hoc networks, where end-to-end connectivity can not be guaranteed and communications rely on the assumption that the nodes are willing to *store-carry-and-forward* bundles in an opportunistic way. However, this assumption would be easily violated due to the *selfish nodes* which are unwilling to consume precious wireless resources by serving as bundle relays. To apply conventional reputation based incentive schemes in DTNs is extraordinarily challenging due to the unique network characteristics. To tackle this issue, in this paper, we propose **SUCCESS**, a secure *user-centric* and *social-aware* reputation based incentive scheme for DTNs. Different from conventional reputation schemes which rely on neighboring nodes to monitor the traffic and keep tracks of each other's reputation, **SUCCESS** allows a node to manage its reputation evidence and demonstrate its reputation whenever necessary. Two concepts, *self-check* and *community-check*, are defined for reputation evaluation according to the candidate's forwarding competency and the sufficiency of the evidence shown by the node itself, and for speeding up reputation establishment and forming consensus views towards targets in the same community, respectively. Extensive performance analysis and simulations are given to demonstrate the se-

*The corresponding author, email: zfcao@cs.sjtu.edu.cn.

curity, effectiveness and efficiency of the proposed scheme.

Key words: Selfish; Reputation based incentive; Cooperating stimulation; Security; Delay/Disruption tolerant networks; Social-aware.

1 INTRODUCTION

Most of popular Internet applications rely on the existence of a contemporaneous end-to-end link between source and destination, with moderate round trip time and small packet loss probability. This fundamental assumption does not hold in some challenged networks, which are often referred to as Delay/Disruption Tolerant Networks (DTNs) [1]. Typical applications of DTNs include vehicular DTNs for dissemination of location-dependent information, pocket switched networks, underwater networks, etc. Different from traditional wireless ad hoc networks, data in DTNs are *opportunistically* routed toward the destination by exploiting the temporary connection and store-carry-and-forward transmission fashion.

Most of the DTN routing schemes require the hypothesis that the individual node is ready to forward bundles for others. However, in certain DTN applications such as vehicular DTNs or pocket-switched networks, which are decentralized and distributed over a multitude of devices that are controlled and operated by rational entities, DTN nodes can thus behave selfishly and try to maximize their own utility without considering the system-level welfare. Existing researches have shown that a non-cooperative DTN may suffer from serious performance degradation [2–4]. Therefore, to deploy applicable DTNs in real-world scenarios, a proper incentive scheme should be in place to stimulate selfish nodes to contribute to the DTNs.

In general, the conventional incentive schemes can be classified into the following two categories: credit-based [2–10] and reputation-based [11–22]. Credit-based incentive schemes introduce some virtual currency to regulate the packet-forwarding relationships among different nodes. Reputation-based incentive schemes rely on individual nodes to monitor neighboring nodes' traffic and keep track of each others' reputation so that uncooperative nodes are eventually detected and then excluded from the networks. In practice, reputation-based incentive systems have already been widely used in most of the successful commercial online applications such as eBay and Amazon [14]. Even though incentive schemes have been well studied for the conventional mobile ad hoc networks, the unique network characteristics in DTNs including lack of contemporaneous path, high variation in network

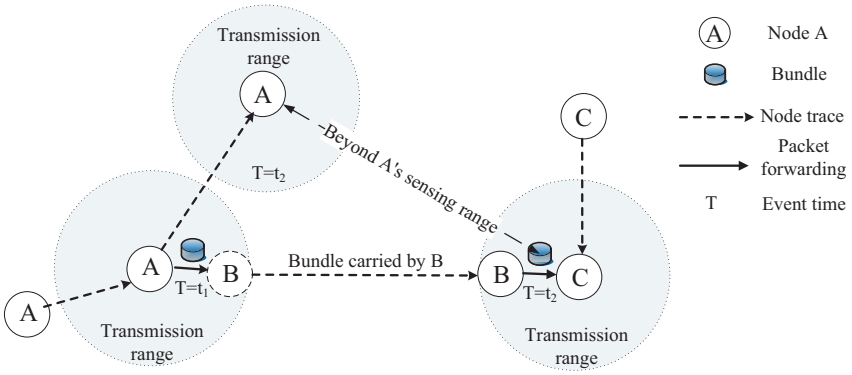


FIGURE 1
A typical store-carry-and-forward transmission fashion.

conditions, difficulty to predict mobility patterns, and long feedback delay, have made the incentive issue quite different. Therefore, there is an increasing significance in designing the reputation-based incentive schemes for the emerging DTNs.

The reported incentive schemes in DTNs are mainly focusing on the credit-based solutions, whereas the reputation based schemes still receive less attention due to the following three reasons. Firstly, existing reputation based incentive schemes designed for conventional wireless networks assume that the sender can monitor the next hop's transmission and detect if the next hop appropriately forwards the traffic [11, 12]. This assumption may not hold in DTNs due to the store-carry-and-forward transmission. For example, as shown in Figure 1, a node A forwards bundles to a node B at t_1, which carries the bundles until it meets the next hop node C at t_2. Meanwhile, the data transmission from B to C is beyond the sensing range of A. This unique characteristic makes existing reputation schemes which are based on the neighboring detection unsuitable in DTNs. Secondly, due to the long propagation delay and frequent disconnectivity, how to efficiently and effectively propagate the reputation is another challenging issue. Different from credit-based incentive scheme [4], it needs a credit clearance process by virtual bank or globe manager. Without a globe reputation manager [12, 15] or other efficient reputation-aided management [16, 18], the distributed reputation is hard to accumulate to form a consensus view towards the target node in DTNs. In this paper, we propose a secure *user-centric* and *social-aware* reputation based incentive scheme for DTNs, named as ***SUCCESS***, to stimu-

late cooperation among selfish nodes in DTNs. **SUCCESS** is a dynamic reputation system where reputation can be maintained, updated, and shown for verification by each node whenever needed. Specifically, in the store-carry-and-forward transmission, each successful transmission can be demonstrated by either the previous/next hop nodes or their community, which can be divided into two categories: *self-check* and *community-check*.

The *self-check* is defined as that a node keeps its forwarding evidence for the purpose of directly checking by the bundle sender in the future. Different from existing reputation based incentive schemes which rely on neighbors' monitoring and scoring targets, all the reputation related information for a specific node is stored in its own local buffer in our scheme, which enables efficient reputation retrieval for other nodes. Thus, our **SUCCESS** can be named a *user-centric* scheme.

The *community-check* means that the forwarding evidence is collected and then checked through the social network to improve reputation propagating efficiency in DTNs. Furthermore, **SUCCESS** provides a suitable way to measure the metrics of social relationships for reputation community check efficiently. Recently, there is an increasing interest to study the social relationship by mapping the contact history to directed graph [23]. However, we argue that this social relationship built on the physical locality and contact history can not reflect their real willingness in the bundle forwarding. This could be demonstrated by the scenarios that two people are just a nodding acquaintance relationship although they almost meet every day in the daily life. Instead, **SUCCESS** abstracts the true willingness between the nodes by honestly recording each data forwarding. Thus, **SUCCESS** is a *social-aware* scheme.

However, the main challenge in designing **SUCCESS** is to ensure that the security properties of the scheme are not compromised. Since the security related to self-maintained reputation, especially during the store-carry-and-forward process, is managed by the node itself, it also leaves the owner possibilities to intentionally or even maliciously to modify its maintained reputation records. This is the *security perspective* of **SUCCESS**. Further, any security functionality will incur extra computation and transmission overhead. A secure reputation based incentive scheme should be efficient enough to not significantly compromise the system performance. This is the *performance perspective* of our system.

The contributions of this paper can be summarized as follows:

- Firstly, we propose **SUCCESS** to stimulate cooperation among selfish

nodes in DTNs, which allows a node to maintain, update, and submit its reputation tickets whenever needed. Based on the Dempster-Shafer theory, we make a comprehensive reputation evaluation considering both the node's forwarding competency and the sufficiency of the evidence shown by the node itself.

- Secondly, we define a new social metric of DTN nodes, which considers the forwarding willingness from forwarding history, and identifies the social community based on this new metric. we make use of social property to speed up **SUCCESS**'s reputation establishment and allow nodes in the same community to share reputation information and form consensus views towards the targets.

- Lastly, **SUCCESS**, as a high level scheme, can be compatible with diverse data-forwarding algorithms. We also use the security techniques such as identity based signatures to prevent reputation tickets from compromising by the malicious nodes and batch verification to reduce the computational overhead. Extensive performance analysis and simulations demonstrate the efficiency and efficacy of the proposed schemes.

The remainder of this paper is organized as follows. In Section 2, we review the related work. In Section 3, we present the system models and design goals. Necessary preliminaries are introduced in Section 4. Section 5 proposes **SUCCESS**, which builds a reputation based incentive mechanism to stimulate cooperation in bundles forwarding through reputation self-check and community-check. In Section 6 and Section 7, extensive performance analysis and simulation are given, respectively. Finally, we draw the conclusion in Section 8.

2 RELATED WORK

The issues on studying selfish behavior and designing incentive schemes have received extensive attentions in all kinds of networks. Most of previously reported studies have focused on how to stimulate selfish nodes through different approaches in the ad-hoc, sensor, and P2P networks. Credits-based incentive schemes [2–9], are usually employed to provide incentive such as virtual credits to encourage selfish nodes forwarding. An interesting work [10] proposes pair-wise Tit-for-Tat as an incentive scheme in DTNs.

Reputation-based incentive schemes [11–22] often rely on the individual nodes to monitor neighboring nodes' traffic and keep track of each others' reputation so that uncooperative nodes can be eventually detected and excluded from the networks. Meanwhile, reputation based incentive mechanisms always accompany the trust systems [14] to reward or punish selfish node. [19] proposes two techniques: watchdog and pathrater. CORE, in [21], uses the watchdog mechanism to observe neighbors and then detect and isolate selfish nodes. [11] proposes OCEAN, in which each node maintains the ratings for neighbors through directly interacting, but these ratings are not propagated to other node. SORI [12] proposes the concepts of first-hand reputation and second-hand reputation and shows how to compute the weighted sum from these values. [15] proposes a reputation management system (RMS) in mobile ad hoc networks. [20] presents two forwarding protocols for mobile wireless networks and formally shows that both protocols are Nash equilibria. However, in DTNs, existing reputation-based incentive schemes may face the challenges. Using willingness to measure the strength of the social tie, [17] proposes a social selfishness aware routing algorithm to provides better routing performance in an efficient way. [16] designs a reputation-assistant framework to accurately evaluate encounter's competency of delivering data in opportunistic networks. [18] presents a hierarchical Account-aided Reputation Management system, named as ARM, to efficiently and effectively provide cooperation incentives.

3 SYSTEM MODELS AND DESIGN GOALS

In this section, we define our DTN models, attack models and design goals.

3.1 General DTN Model

We first consider a general DTN system model, which is characterized as end-to-end connections are not always guaranteed and routings are made in an *opportunistic* way as shown in Figure 1.

Specifically, in a general DTN model, a source node Src wants to send bundles to a destination node Dst depending on relays of the intermediate nodes $\{N_1, N_2, \cdots, N_n\}$. Similar to credit-based incentive schemes in [4], we assume that there exists an *Offline System Manager* (**OSM**), which is responsible for key distribution. At the beginning of the system initialization, each node in the DTNs should register to the **OSM** and get the secret keys and public parameters in a secure channel. However, different from [4], our

system model does not need the credit or reputation clearance process by virtual bank or **OSM** and our reputation is evaluated in a self-organizing manner which caters to the DTN environment.

3.2 Social Based DTN Model

We also define the social relationship model from the forwarding history. Our social based DTNs could be modeled as a weighted directed graph $(\mathbb{V}, \mathbb{E})$, where the vertex set $\mathbb{V}$ consists of all the DTN nodes and the edge set $\mathbb{E}$ consists of the social links between these nodes. In this work, we use the *forwarding history* instead of contact history in [23] to evaluate the weight of social links between nodes since the fact that the contact of two nodes does not mean that they are willing to forward bundles for others in a rational assumption. Maybe they are just running into each other. To extract the social relationship, we introduce the measurement of *Average forwarding time* (AFT), which is used to reflect both the contact frequency and forwarding capability for one bundle. AFT from node i to node j is defined as

$$AFT_{ij} = \frac{T}{\sum_k N_{t_k,t_{k+1}}}, \tag{1}$$

where T is a training time window and $N_{t_k,t_{k+1}}$ represents the number of forwarding bundles between two meeting time t_k and t_{k+1}. The smaller AFT_{ij} is, the more willingness i has to forward for j. It is obvious that $AFT_{ij} \neq AFT_{ji}$. Several examples of willingness extractions are shown in Figure 2. In the Figure 2(a), the node i meets the node j at time t_0, t_1, t_2, and t_4 and finishes forwarding $2N_0$ bundles for j in the separating time period $[t_0, t_1]$, N_0 bundles in the period $[t_1, t_2]$, and $3N_0$ bundles in the period $[t_2, t_4]$. Thus, we can calculate the Average forwarding time as follows

$$AFT_{ij}(a) = \frac{T}{2N_0 + N_0 + 3N_0} = \frac{T}{6N_0}.$$

Similarly, $AFT_{ij}(b) = AFT_{ij}(a) = T/6N_0$. Though it does not forward any bundles in the period $[t_3, t_4]$, it has the same contribution as that in the Figure 2(a). $AFT_{ij}(c) = T/9N_0$. It forwards another $3N_0$ bundles in the period $[t_3, t_4]$, which shows that the node j in the Figure 2(c) has a better forwarding capability and contact frequency than that in the Figure 2(a) and Figure 2(b).

Finally, we deduce nodes' knowledge into a single *willingness* metric $w_{ij} \in [0, 1]$ for node i to node j. We use Gaussian similarity function [23, 24] to

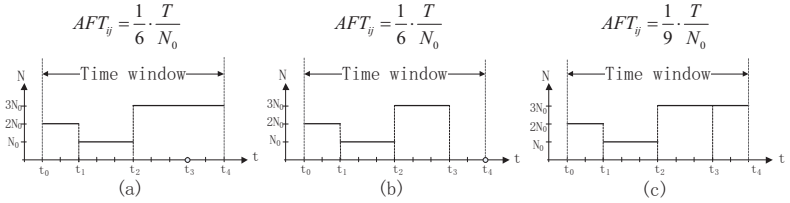


FIGURE 2
Average forwarding times extraction from forwarding histories.

normalize AFT_{ij} in equation (1) and denote the resulting metric as the willingness

$$w_{ij} = \exp\left(-\frac{AFT_{ij}^2}{2\sigma^2}\right). \tag{2}$$

Here, σ is a scaling parameter [23, 24]. We set the threshold T_w and employ the technique of social group identification where the non-overlapped community structure can be constructed in a distributed manner using a simplified clique formation algorithm from [23].

According to the definitions above, we have enough reasons to slightly modify the good property in [20] as the *first good property*: assuming that if two nodes meet and forward bundles once, it is very likely that they will meet again in the near future. Besides, in our settings, we assume a *second good property* that if two nodes belong to the same community, the chance that they meet is higher than that of belonging to different communities.

3.3 Attack Models

In this paper, we consider two kinds of DTN nodes: *selfish-but-rational* nodes and *malicious* nodes among these intermediate nodes.

Due to the selfish nature and energy consuming, selfish nodes are not willing to forward bundles for others without stimulation or rewards. Such a selfish behavior could significantly degrade network performance. In addition, we assume that every node is rational in two sides. on the one hand, the nodes with a high reputation have the chance to be chosen than the low ones since their past successful forwarding history may lead to a better delivery rate. On the other hand, the nodes can improve their reputation through actively involving the bundle forwarding to avoid being put into *blacklist*, which is often used in the reputation based incentive scheme [25].

Moreover, the malicious nodes may launch the attacks such as modifying the forwarding history to overclaim a high reputation and then attract bundles

and drop them to isolate the target user, which destroys network performance. This kinds of attacks may not be easy to be discovered in the distributed networks without the monitors, especially in the DTNs.

3.4 Design Goals

Our goals are to develop a user-centric and social-aware reputation-based incentive scheme for DTNs. Specifically, the following three desirable objectives will be achieved:

Goal-I: Effectiveness. Our proposed scheme is effective in stimulating cooperation among the selfish nodes in DTNs.

Goal-II: Security. Our scheme resists various regular attacks launched by malicious nodes.

Goal-III: Efficiency. It is an efficient scheme without introducing too much extra communication and transmission overhead.

4 PRELIMINARY

In this section, we would like to introduce some prliminaries of our work.

4.1 Beta Distribution And Bayesian Systems

Bayesian systems often take binary inputs such as positive or negative ratings to compute scores by statistical updating of *Beta probability density functions* $Beta(\alpha, \beta)$ [13, 14]. The updated score is combined the previous score with a new rating. It updates as follows. Initially, the prior is function $Beta(\alpha, \beta) = Beta(1, 1)$, which is the uniform distribution on $[0, 1]$. When a new observation, including f negative ratings and s positive ratings, is collected, the prior function is updated by $\alpha \leftarrow \alpha + s$ and $\beta \leftarrow \beta + f$. The advantage of Bayesian system is that it provides a theoretically sound basis for computing scores and it only needs two parameters α and β that are continuously updated along with reported observations [12]. According to the definition, the mathematical expectation of evidence distribution is defined as following:

$$EXP(Beta(\alpha, \beta)) = \frac{\alpha}{\alpha + \beta}. \tag{3}$$

In addition, $EXP(Beta(\alpha, \beta))$ is only a ratio that can *not* reflect the uncertainty of distribution. Thus, we need to find out the variance of evidence distribution to describe the uncertainty.

$$VAR(Beta(\alpha, \beta)) = \frac{\alpha \cdot \beta}{(\alpha + \beta)^2 \cdot (\alpha + \beta + 1)} \tag{4}$$

We will show how to use these values in the reputation generation in the next section.

4.2 Cryptographic Technology

In **SUCCESS**, signatures, signed by the next hop node, are introduced to authenticate the forwarding evidence. Each node has an unique ID never changed in the scheme, which is used as its public key to verify the signatures. To reduce the computational cost of **SUCCESS**, we adopt a cryptographic technology based on a signature scheme [26] and its well-known batch verification version [27], which consists of five algorithms:

Setup. OSM runs setup algorithm to generate the system parameters and master secret keys. Specifically, OSM selects bilinear pairing on elliptic curve*. In addition, it chooses two cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$ and $H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$. After that, OSM picks a random number s, where $s \in \mathbb{Z}_q^*$ is its secret key, and sets its public key as $P_{pub} = sP$. The system parameters are $params = (\mathbb{G}_1, \mathbb{G}_2, q, \hat{e}, P, P_{pub}, H_1, H_2)$. The system's secret is s, which is known only by OSM itself. When a DTN node wants to join into this network, it needs to register to OSM. The node is assigned its identity ID, $params$ and a secret key sk_{ID} from OSM in a secure way. Specifically, OSM does as follows: $sk_{ID} = s \cdot H_1(ID)$. Note that this **Setup** step could be accomplished in the off-line phase.

Sign. To generate a signature on a message m, it first encodes m to a non-zero element in $\mathbb{Z}_q^*$. Then it selects a random number r in $\mathbb{Z}_q^*$ and computes signature $\textbf{Sign}_{ID}(m) = (U, V)$ where $U = r \cdot H_1(ID)$ and $V = (r + H_2(U\|m)) \cdot sk_{ID}$.

IndVer. To verify a message-signature $\textbf{Sign}_{ID}(m)$, it verifies individually by $\hat{e}(V, P) \stackrel{?}{=} \hat{e}(U + (H_2(U\|m)) \cdot H_1(ID), P_{pub})$.

Aggr. To improve efficiency, it first combines signatures $\{\textbf{Sign}_{ID_i}(m_i) = (U_i, V_i) | 1 \leq i \leq n\}$ by $V_{Bat} = \sum_{i=1}^{n} V_i$ and $U_{Bat} = \sum_{i=1}^{n} U_i + (H_2(U_i\|m_i)) \cdot H_1(ID)$.

BatVer. It verifies the combined signature in a batch model $\hat{e}(V_{Bat}, P) \stackrel{?}{=} \hat{e}(U_{Bat}, P_{pub})$.

*An efficient admissible bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are two cyclic multiplicative groups of the same prime order q, (i.e., $|\mathbb{G}_1| = |\mathbb{G}_2| = q$), has the following properties (Let P be a generator of $\mathbb{G}_1$): (1) Bilinear: for all $P \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$, $\hat{e}(aP, bP) = \hat{e}(P, P)^{ab}$; (2) Non-degenerate: there exists $P \in \mathbb{G}_1$ such that $\hat{e}(P, P) \neq 1$; (3) Computable: there is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}_1$.

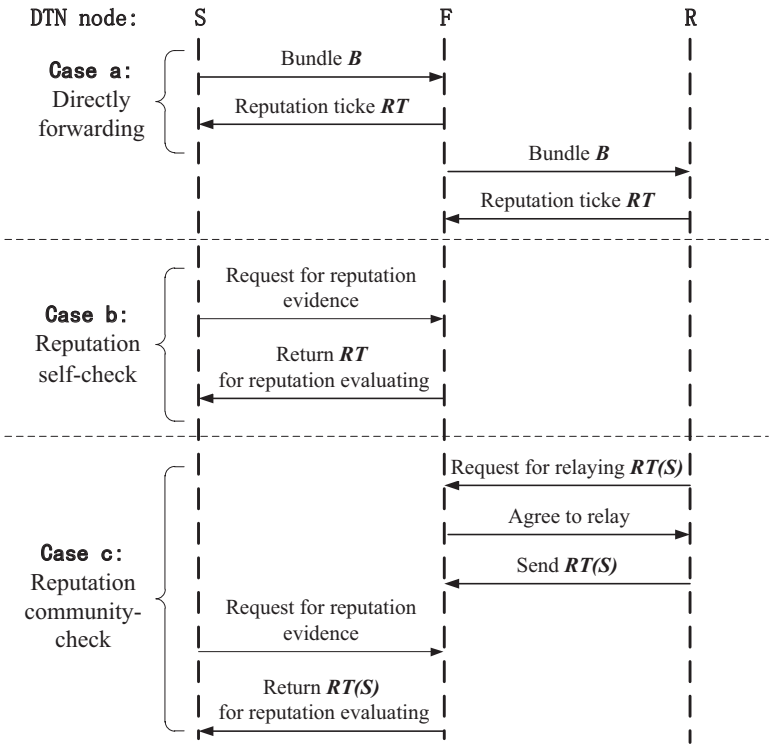


FIGURE 3
The proposed **SUCCESS** scheme.

5 THE PROPOSED SUCCESS SCHEME

In this section, we first give an overview of the SUCCESS scheme and introduce the concept of *reputation ticket*. Then we illustrate how **SUCCESS** works in the bundle forwarding by making full use of these reputation tickets to stimulate nodes' cooperation. By detecting and punishing selfish nodes, we show that behaving selfish will not gain benefits. Instead, behaving cooperative has a better chance to increase their benefit, which achieves **Goal-I** effectiveness. We also use the security techniques such as identity based signatures to prevent reputation tickets from compromising by malicious nodes, which achieves **Goal-II** security. Community-based checking reputation and Batch verification of signature techniques are used to reduce the computational overhead, which achieves **Goal-III** efficiency.

5.1 Overview Of SUCCESS

Figure 3 shows the bundle forwarding process. When a node F reaches the transmission range of a sender S, they first check whether they are in the blacklist. If either of them in the blacklist, the forwarding stops. Otherwise, according to whether they have met before, three cases emerge.

Case a: directly forwarding. If they meet at the first time, S directly forwards bundles to F and sets the initiate reputation value of F. After that, F replies to S a reputation ticket as an evidence of successful forwarding of S. Similarly, F receives another reputation ticket from the next hop node R and keeps it for future checking in the next encounter with S. The format of

id	S	SI_S	F	R	TS	TTL	$H(B)$	$\textbf{Sign}_R$

FIGURE 4
The format of reputation ticket.

reputation ticket is shown in Figure 4. Specifically, it is comprised of ticket sequence number id, sender node S, forwarding node F, receiving node R, time stamp TS, expiration time TTL and bundle hash value $H(B)$. SI_S is the social group identifier of S used in the reputation social agreement we explain in Section 5.4. As shown in the Section 4.2, R computes its signature as $\textbf{Sign}_R(id\|S\|SI_S\|F\|R\|TS\|TTL\|H(B))$. After that, this reputation tickets has been constructed. This reputation ticket provides an evidence that F forwarded S's bundle to R at time TS. Different from any existing reputation schemes, **SUCCESS** allows each node to maintain its own reputation tickets in the local buffer, which is able to show its own reputation on its demand.

Case b: reputation self-check. If these two nodes met before, S starts the reputation self-checking algorithm. Since we assume the *first good property*, it is very likely that S and F meet again. The node F is requested to show the reputation evidence for reputation self-checking algorithm that is introduce in Section 5.2 and Section 5.3.

Case c: reputation community-check. Due to DTN's long propagation delay and frequent disconnectivity, if the *first good property* in the reputation self-checking process somehow (or sometime) does not preform so well when two nodes belong to different communities and just encountered occasionally before. It will start reputation community-check algorithm instead. Since two nodes in the same community have a higher probability not only in meeting each other but also in the willingness to forward bundles periodically than that of in the different community, we can use the *second good property* to achieve reputation check we explain in Section 5.4.

5.2 Reputation Self-Check

When S starts the reputation self-checking algorithm, S first finds out the forwarding records in the last encounter to verify the expiration time of reputation tickets and then asks F for forwarding evidence to evaluate reputation. F needs to actively return the related reputation tickets to S, or F is evaluated a low reputation leading to be put into blacklist.

After that, S makes an observation. $NtF(S, F)$ denotes the number of copies that S required F *to forward* in the last encounter. $NaF(S, F)$ denotes the number of copies that F has *actually forwarded* for S.

Definition 1 (Observation) *The observation starts at time t_s and ends at time $min(t_d, t_s + TTL)$. S verifies reputation tickets for one bundle in a individual model or a batch model:*

Individual-Verification model: *S individually takes **IndVer**(U_i, V_i). If it returns 1, $NaF(S, F) \leftarrow NaF(S, F) + 1$.*

Batch-Verification model: *S first takes **Aggr**(U_i, V_i) for n signatures and then **BatVer**(U, V). If it return 1, $NaF(S, F) \leftarrow NaF(S, F) + n$, else S processes divide-and-conquer to identify the invalid signatures.*

If for one bundle $NtF(S, F) \leq NaF(S, F)$, that is, F completes a bundle forwarding mission, the observation result is regarded as a success, Otherwise, a failure.

To justify observation results and further to generate the reputation metric, we denote α and β to represent the total number of observed success and failure, respectively. s and f are the success and failure in the current observation. Thus, we update α and β by

$$\alpha \leftarrow \alpha + s \ \ and \ \ \beta \leftarrow \beta + f. \tag{5}$$

However, just as described in the Section 4.1, only the history observation results can not be directly used in the reputation evaluation. For example, assuming S encounters the relay node F_1 with $\alpha = \beta = 5$ and the other relay node F_2 with $\alpha = 2$ and $\beta = 1$. S can not easily distinguish which one has a better reputation without the further history evidence evaluation. From our abstract version [22], we made a simple conclusion that, according to the definition of Bayesian inference, the basic reputation value can be quantified by the expectation equation (3) of evidence distribution

$$v_{_{S-F}} = EXP((Beta(\alpha, \beta))) = \frac{\alpha}{\alpha + \beta}. \tag{6}$$

For the certainty part, we should assign advanced reputation value according to the proportion of supporting evidence in the observed results. We assign *advanced reputation value* (ARV):

$$ARV_{_{S-F}} = v_{_{S-F}} \cdot (1 - u_{_{S-F}}) = \frac{\alpha}{\alpha + \beta} \cdot (1 - u_{_{S-F}}) \tag{7}$$

where $u_{_{S-F}} = VAR(Beta(\alpha, \beta))$.

Aging in evaluation. Additionally, to take it into account that the reputation value fades along the time for the following reasons. First, it can resist regular sleeper attack where a node created a good reputation before and then became selfish later. Second, according to limitation of the DTNs node's buffer, reputation tickets become useless along the time and are discarded for saving the buffer, which stimulates nodes to realize reputation tickets checking as soon as possible in Section 5.4. To achieve this goal, we give some discount weight ω to indicate the freshness of reputation as an aging factor for a time slot ΔT, such that,

$$\alpha = \omega^{\frac{t_d - t_s}{\Delta T}} \alpha + s \ \ and \ \ \beta = \omega^{\frac{t_d - t_s}{\Delta T}} \beta + f \tag{8}$$

5.3 Further Reputation Evaluation

For further making a comprehensive reputation evaluation[†], we follow the Dempster-Shafer theory [28] to develop a belief reasoning process to measure our reputation by both forwarding competency and evidence sufficiency in a unified framework.

This theory is a framework related to probability theory, but where the sum of probabilities over all possible outcomes not necessarily add up to 1, and the remaining probability is interpreted as uncertainty. Thus, the Dempster-Shafer theory is often used as a mathematical theoretical tool about the evidence on belief and plausible explanation, which could combine the separate evidence to calculate the probability of the event.

5.3.1 Measuring forwarding competency and evidence sufficiency

We formalized the reputation evaluation problem under the Dempster-Shafer theory as follows. Let $\mathbb{X}$ be the set of all states under S's consideration. Here, $\mathbb{X}$ = $\{F$ is competent$\}$, $\{F$ is incompetent$\}$. Its power set, $\mathbb{P}(\mathbb{X})$, is the set of all possible sub-sets of $\mathbb{X}$. We denote three value b,d,u to represent the

[†]For the limit of the space, we omit the detailed explanation in our paper [22]. In the paper, we extend our results by using the Dempster-Shafer theory [28] for further reputation evaluation based on the forwarding competency and evidence sufficiency.

probability on F's forwarding competency of belief, disbelief, and uncertainty, respectively where $b, d, u \in [0, 1]$ and $b + d + u = 1$. According to the Dempster-Shafer theory, the next step is to find a proper mass assignment for $\mathbb{P}(\mathbb{X})$, that is, b, d, u. Here, we use Bayesian inference as the bridge to connect observation results with the mass assignment.

Evidence sufficiency measurement. We consider how to assign a proper mass for the scenario that the candidate F is either forwarding competent or forwarding incompetent, which is the uncertainty (probability) of the evidence towards F, denoted u. From the Dempster-Shafer's theory, the *normalized variance* of the Beta distribution actually is satisfied. Since

$$\begin{aligned} 0 &\leq VAR(Beta(\alpha, \beta)) = \frac{\alpha \cdot \beta}{(\alpha + \beta)^2 \cdot (\alpha + \beta + 1)} \\ &\leq \frac{\alpha \cdot \beta}{4 \cdot \alpha \cdot \beta \cdot (\alpha + \beta + 1)} = \frac{1}{4 \cdot (\alpha + \beta + 1)} \leq \frac{1}{12}, \end{aligned} \tag{9}$$

we multiply a constant 12 to the variance $VAR(Beta(\alpha, \beta))$ as follows:

$$u = 12 \cdot VAR(Beta(\alpha, \beta)) = \frac{12 \cdot \alpha \cdot \beta}{(\alpha + \beta)^2 \cdot (\alpha + \beta + 1)}. \tag{10}$$

This uncertainty can reflect the adequacy of the observations. Thus, u in the Dempster-Shafer's unified framework can be used in the reputation evaluation representing the sufficience of the evidence.

Forwarding competency measurement. For the certainty part, we should assign mass to the proportion of supporting evidence in the observed results which means the probability of the belief. According to Bayesian Inference, we assign

$$b = EXP(Beta(\alpha, \beta)) \cdot (1 - u) = \frac{\alpha}{\alpha + \beta} \cdot (1 - u). \tag{11}$$

Similarly, d for the set $\{F \text{ is incompetent}\}$ can be defined

$$d = \frac{\beta}{\alpha + \beta} \cdot (1 - u). \tag{12}$$

Here, the belief and the disbelief values in the statement $\{F \text{ is competent}\}$ have been defined, which reflect the F's forwarding competent in certainty.

5.3.2 Reputation evaluation

For further reputation evaluation, we introduce the probability of the plausibility. Since in the Dempster-Shafer's framework, it allows for the probability of the belief to be represented as two bounded values: $belief$ and

$plausibility$ where $belief \leq plausibility$. ***Belief*** in a hypothesis is constituted by the sum of the masses of all sets enclosed by it. It is the amount of belief that directly supports a given hypothesis at least in part, forming a lower bound. *Plausibility* is 1 minus the sum of the masses of all sets whose intersection with the hypothesis is empty. It is an upper bound on the possibility that the hypothesis could possibly happen, i.e. it *could possibly happen* up to that value, because there is only so much evidence that contradicts that hypothesis. From the discussion above, we have the probability of the plausibility, denoted p, as

$$p = 1 - d = 1 - \frac{\beta}{\alpha + \beta} \cdot (1 - u) = \frac{\alpha + \beta \cdot u}{\alpha + \beta} = b + u, \tag{13}$$

According to the selfish-but-rational nature, nodes always select and forward the bundles to the most competent forwarders with sufficient evidence. We utilize the Dempster-Shafer theory in making comprehensive decisions on the reputation evaluation. With the lower bound belief and upper bound plausibility, nodes can make more comprehensive decisions on reputation evaluation according to their own characteristics. We can define this characteristic factor c ($c \in [0, 1]$) to describe a node's aggressiveness. S can use the following metric REP as the *reputation value* to evaluate the candidates F.

$$REP_{_{S-F}} = (1 - c) \cdot b + c \cdot p = b + c \cdot u. \tag{14}$$

An extremely aggressive node ($c = 1$) would choose the candidate with the highest plausibility as the best candidate. A conservative node ($c = 0$) would choose a candidate based on their belief.

5.3.3 Decision making

After the reputation value generation, S needs to make a decision on whether to reward or punish F. In our setting, **OSM** sets two thresholds: T_{High} and T_{Low} for the candidate forwarder. If REP is higher than T_{High}, it indicates that this candidate node is willing to forward bundles for S and S sends it the new bundles as in the section 5.1. Besides, as a reward, S agrees to forward reputation tickets for F and starts reputation social establishment procedure in section 5.4. In the case, the reputation value is lower than T_{Low}, which means the candidate node behaves selfish in forwarding bundles for S and S puts it into *blacklist* and later informs its community members when they are meeting later in section 5.4. In the case that the reputation value is between T_{High} and T_{Low}, S still sends bundles to F but warns to F by not propagating

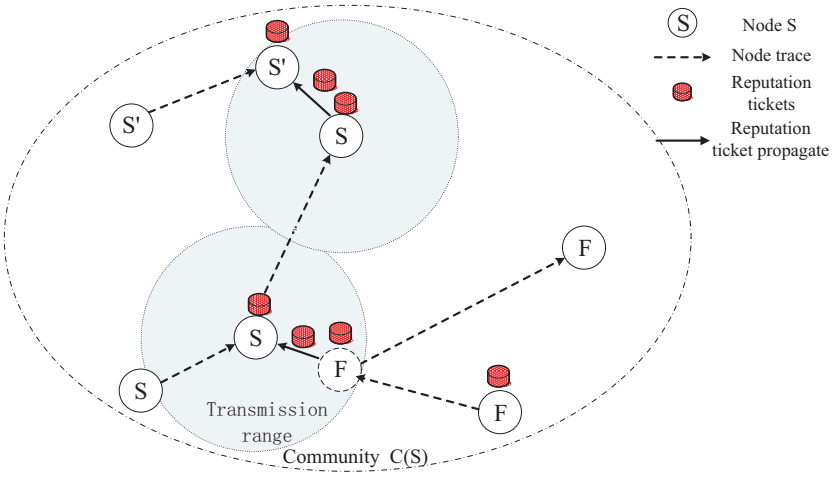


FIGURE 5
Reputation Social Establishment By Community Checking

reputation tickets. Note that the thresholds T_{High} and T_{Low} must be carefully defined. Otherwise, false positive and false negative could be high.

The nodes in the *blacklist* can not be asked for forwarding because their low reputation leads to unreliable bundle forwarding. At the same time, as a punishment, their forwarding evidence can not be community checked by other nodes. This leads to a reputation drop of the selfish nodes. Therefore, they need to find new nodes or just wait for the senders.

5.4 Reputation Community-Check

In this section, we demonstrate how to efficiently and effectively propagate reputation tickets by the community-checking algorithm when the first good property in the reputation self-checking sometimes would not preform so well. According to our definition of social community, two nodes in the same community have a higher probability not only in meeting each other but also in the willingness to forward bundles periodically than that of in the different community. Thus, our reputation community checking mechanism can be built on the community level, which allows nodes in the same community to share reputation information to accelerate reputation collections. After that, all nodes in the same community can form consensus views towards the targets.

Let us take an example as shown in Figure 5, if S agrees to help F to

Algorithm 1: Reputation Community Checking Algorithm

1: **procedure** RepCommCheck

2: When S meets its community member, S', they exchange their reputation tickets and blacklists.

3: After verifying the validity of these tickets, they can make a consensus on F's reputation by updating:

$$u_{_{SS'-F}} = u_{_{S-F}} + u_{_{S'-F}} - 1$$

and

$$v_{_{SS'-F}} = \frac{(1-u_{_{S-F}}) \cdot v_{_{S-F}} + (1-u_{_{S'-F}}) \cdot v_{_{S'-F}}}{(1-u_{_{S-F}}) + (1-u_{_{S'-F}})}$$

4: **end procedure**

community check reputation tickets, F sends the related reputation tickets whose $SGI \in SI_S$. This means that those senders and S belong to the same community, who have more chance to meet in the near future than that of F. S holds these reputation tickets in its buffer until it meets S' in the same community and then it starts reputation community checking Algorithm 1 between S and S'. Here, we just consider the condition that the node's aggressiveness $c = 0$ for simplicity.

As this reputation community checking algorithm continues, nodes in the same community can form consensus views towards the target F by

$$v_{_F} = \frac{\sum_{i \in C(i)} (1-u_{_{i-F}}) \cdot v_{_{i-F}}}{\sum_{i \in C(i)} (1-u_{_{i-F}})}, \tag{15}$$

where $C(i)$ represents the social group node i belongs to. $(v_{_{i-F}}, u_{_{i-F}})$ represents node i's view towards node F. The consensus view $v_{_F}$ is weighted sum of views from the nodes in the same community. The weight is decided by node i's certainty towards the reputation value $v_{_{i-F}}$. Thus, nodes in one community can form consensus views towards the target F by

$$ARV_{_{S-F}} = v_{_F} \cdot (1-u_{_F}). \tag{16}$$

When a selfish node has been put into the blacklist, other nodes in the same community will refuse community check as a punishment.

6 PERFORMANCE ANALYSIS

We model our reputation community check as an epidemic problem [29] for investigating the factors which influence the reputation social establishment. If the establishment speed is higher than the mobility of the selfish node, selfish nodes will be isolated.

We define the variables in Table 6. We also denote a constant λ to show

Notations	Definitions
t	time slot
N	The total number of nodes in this community
$i(t)$	a ratio, which of N have shared the blacklist until t
$s(t)$	a ratio, which of N have not shared the blacklist until t
T	the threshold to identify the social group

TABLE 1
Parameters used for performance analysis.

the relationship of the willingness and infected number. Thus, λT is the low bound of nodes which each node can inform. Suppose that every node, holding a blacklist, can contact at least $\lambda T s(t)$ nodes at the end of time slot t. Thus, at least $\lambda T s(t) N i(t)$ nodes could share this blacklist when $N i(t)$ nodes have shared this list at the beginning of time slot t. We have

$$N\dot{i(t)} = \lambda T N s(t) i(t). \tag{17}$$

We assume that the total number of nodes is fixed in one community, so we have (18)

$$i(t) + s(t) = 1, \tag{18}$$

at any time slot t. Given the initial value condition, this model can be simplified to (19)

$$\dot{i(t)} = \lambda T i(1-i) \quad and \quad i(0) = \frac{1}{N} \tag{19}$$

where only one node in the community has detected a selfish node and put into the blacklist. Solving the partial differential equation, we have the analytical solution

$$i(t) = \frac{1}{1 + (N-1)^{-\lambda T t}}. \tag{20}$$

From equation (19), we can also find that establishment speed $\dot{i(t)}$ achieves its maximum when $i = 1/2$. From equation (20), we can get this time slot

$$t_m = \frac{\ln(N-1)}{\lambda T}. \tag{21}$$

In order to shorten the time to the maximum reputation establishment speed, we need to choose small N and large T in practice. However, from the network point of view, t_m could be large in the extreme situation $(N \to 1)$ when all of the nodes are in the same community.

7 SIMULATION

We evaluate the performance of **SUCCESS** in two aspects: the cryptographic operation cost in **SUCCESS** and the effectiveness and efficiency of **SUCCESS** in stimulating selfish nodes with extensive simulations.

7.1 Cryptographic Overhead Evaluation

Our simulation consists of Intel Core 2 Duo P7450 (2.13GHz) with 1 GB RAM based on the Pairing Based Cryptography Library (PBC) [30] in the Ubuntu 9.10 to evaluate the delays of cryptographic operations, which are summarized in Table 7.1. Since signature-aggregation algorithm could be performed incrementally by nodes, this computational cost can be reduced. Given n unauthenticated tickets, the computational cost is bounded by 2 pairings plus several multiplications in the batch-verification, which is a significant improvement over $2n$ pairings by individual verification.

Operations	**Execution Time**
Ticket generation	12.578 ms
Individual verification for *one* ticket	20.167 ms
Individual verification for 10 tickets	201.674 ms
Aggregation for 10 tickets	62.891 ms
Batch verification for 10 tickets	13.878 ms

TABLE 2
Cryptographic overhead.

7.2 Performance Simulation

Simulation Step. We implement our **SUCCESS** in a public DTN simulator, namely, the Opportunistic Networking Environment (ONE) simulator [31],

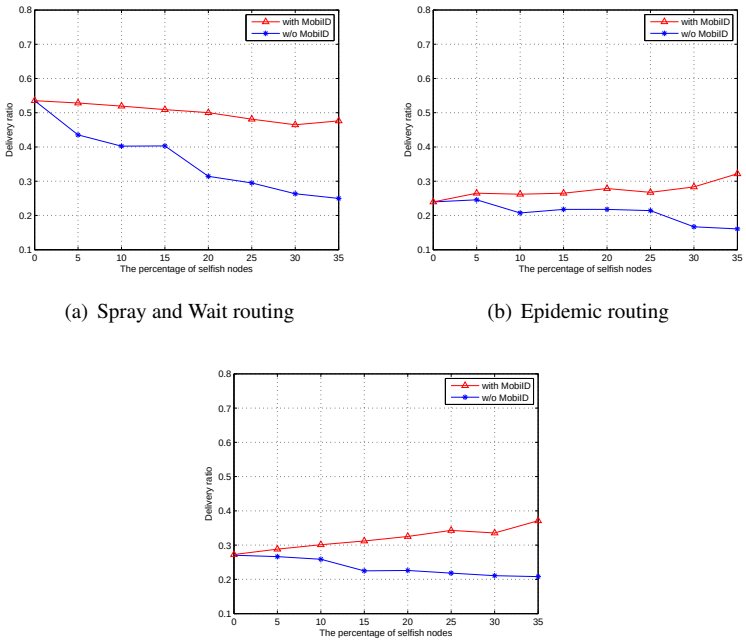
and evaluate its performance under a practical application scenario, i.e., vehicular DTNs. Each vehicle first randomly appears at one position and moves towards another randomly selected position along the roads in a map. The detail parameters are given in Table 7.2.

Parameter	**Value range**
Duration	12 hours
Number of nodes	126
Speed of nodes	0.5 m/s $\sim$ 13.92 m/s
Transmission range	10 m
Transmission speed	2 Mbps
Buffer size	5 MB $\sim$ 50 MB
Bundle generation interval	15 s $\sim$ 35 s

TABLE 3
Parameters used for simulations.

Incentive Effectiveness. We begin our simulation by observing the incentive effectiveness of **SUCCESS**, which can be measured by the bundles' average successful delivery probability under different percentages of selfish nodes or selfish behaviors, as shown in Figure 6, from 0% to 35%. Additional, our scheme can be compatible with diverse data-forwarding algorithms such as Spray and Wait (Figure 6(a)), Epidemic (Figure 6(b)), Prophet (Figure 6(c)). These results indicate that the network delivery could significantly degrade if the selfish nodes or selfish behaviors exist. Moreover, the average successful delivery ratio becomes worse as the percentage of selfish nodes or selfish behaviors increases. However, with **SUCCESS**, nodes are naturally motivated to participate in bundle forwarding to avoid being in the blacklist. The delivery ratio changes little as selfish increases. This demonstrates the incentive effectiveness of **SUCCESS**.

Impact of Traffic Load To evaluate the practicality of **SUCCESS**, we observe the system performance under various sending frequencies by adjusting the message generation interval initialized at 15s and gradually increased to 35s. Figure 7 shows the system performance comparison between the original Spray-and-Wait protocol and the protocol with **SUCCESS**. The network performance is measured in terms of the three metrics: (1) Successful delivery ratio, (2) Overhead ratio, and (3) Average buffer time. Figure 7(a) shows that the successful delivery ratio varies by different the message generation intervals. It is observed that a longer message generation interval would lead to a



(a) Spray and Wait routing

(b) Epidemic routing

(c) Prophet routing

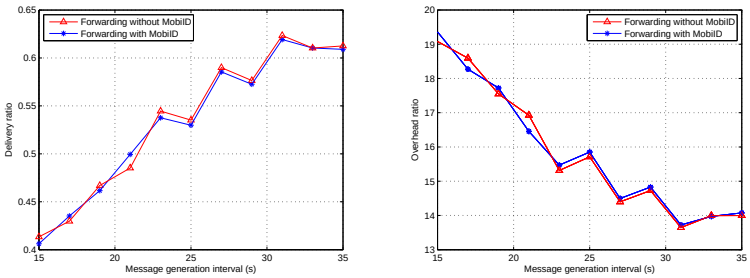
FIGURE 6
Incentive effectiveness of **SUCCESS** with diverse data-forwarding algorithms.

higher delivery ratio since when the number of forwarding bundles decreases, nodes' buffer would not be easily filled up and the bundles have more chance to be carried and forwarded. Figure 7(b) and Figure 7(c) show the overhead ratio and average buffer time of different scenarios, respectively. From above figures, we can conclude that the increased traffic load is not significant to the overall performance of **SUCCESS**.

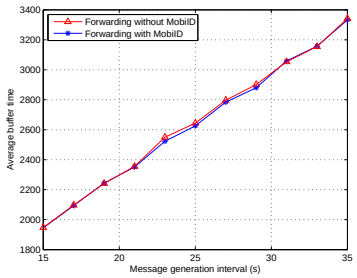
In summary, the simulation results demonstrate that **SUCCESS** is a practical and effective solution that stimulates cooperation in bundle forwarding in DTNs.

8 CONCLUSIONS

In this paper, we have proposed **SUCCESS**, a secure user-centric and social-aware reputation based incentive scheme for DTNs to stimulate cooperation in bundle forwarding. Different from the conventional reputation based in-



(a) Successful Delivery ratio (b) Overhead



(c) Average buffer time

FIGURE 7
Performance comparison under impact of traffic load.

centive schemes, **SUCCESS** allows each node to maintain and update its reputation tickets in the local buffer and thus provide its reputation on demand. We have provided a comprehensive reputation evaluation by measuring the candidate's forwarding competency and the sufficiency of the evidence in the reputation self-checking. In addition, we have introduced a new measurement on the willingness between two nodes to model our social DTNs, which further leads to a community-based solution to accelerate the reputation checking and establishing. Extensive performance analysis and simulations have demonstrated the security, effectiveness and efficiency of the proposed scheme.

ACKNOWLEDGMENTS

This paper is partially supported by the Key Program of National Natural Science Foundation of China (Grant No. 61033014), National Natural Science

Foundation of China (Grant No. 60972034, 60970110, and 61003218) and the Asia 3 Foresight Program under National Natural Science Foundation of China (Grant NO. 61161140320).

REFERENCES

[1] K. Fall and S. Farrell. (2008). DTN: an architectural retrospective. *IEEE Journal on Selected Areas in Communications*, 26(5):828–836.

[2] B.B. Chen and M.C. Chan. (March 2010). MobiCent: a Credit-Based Incentive System for Disruption Tolerant Network. In *the 29th IEEE Conference on Computer Communications (INFOCOM'10)*, San Diego, California, USA.

[3] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss. (2010). Pi: a practical incentive protocol for delay tolerant networks. *IEEE Transactions on Wireless Communications*, 9(4):1483–1493.

[4] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen. (2009). SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks. *IEEE Transactions on Vehicular Technology*, 58(8):4628–4639.

[5] T. Ning, Z. Yang, X. Xie, and H. Wu. (June 2011). Incentive-aware data dissemination in delay-tolerant mobile networks. In *the 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'11)*, Salt Lake City, UT, USA.

[6] C. Zhang, X. Zhu, Y. Song, and Y. Fang. (April 2011). C4: A new paradigm for providing incentives in multi-hop wireless networks. In *the 30th IEEE Conference on Computer Communications (INFOCOM'11)*, Shanghai, China.

[7] Y. Cui, H. Wang, and X. Cheng. (April 2011). Multi-hop access pricing in public area wlans. In *the 30th IEEE Conference on Computer Communications (INFOCOM'11)*, pages 2678–2686, Shanghai, China.

[8] M. E. Mahmoud and X. Shen. (2011). ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-hop Wireless Networks. *IEEE Trans. on Mobile Computing*, 10(7):997–1010.

[9] M. E. Mahmoud and X. Shen. (to appear). FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multi-hop Cellular Networks. *IEEE Trans. on Mobile Computing*.

[10] U. Shevade, H.H. Song, L. Qiu, and Y. Zhang. (October 2008). Incentive-Aware Routing in DTNs. In *the 6th IEEE International Conference on Network Protocols (ICNP'08)*, Orlando, Florida, USA.

[11] S. Bansal and M. Baker. (2003). Observation-based cooperation enforcement in ad hoc networks. *Arxiv preprint cs/0307012*.

[12] Q. He, D. Wu, and P. Khosla. (March 2004). SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad hoc Networks. In *the IEEE Wireless Communications and Networking Conference (WCNC'04)*, Atlanta, GA, USA.

[13] A. Jøsang and R. Ismail. (June 2002). The beta reputation system. In *the 15th Bled Electronic Commerce Conference*, Bled, Slovenia.

[14] A. Jøsang, R. Ismail, and C. Boyd. (2007). A survey of trust and reputation systems for online service provision. *Decision Support Systems*, 43(2):618–644.

[15] T. Anantvalee and J. Wu. (June 2007). Reputation-based system for encouraging the cooperation of nodes in mobile ad hoc networks. In *IEEE International Conference on Communications (ICC'07)*, SECC, Glasgow, Scotland.

[16] N. Li and S.K. Das. (February 2010). RADON: reputation-assisted data forwarding in opportunistic networks. In *Proceedings of the Second International Workshop on Mobile Opportunistic Networking (MobiOpp'10)*, Pisa, Italy.

[17] Q. Li, S. Zhu, and G. Cao. (March 2010). Routing in socially selfish delay tolerant networks. In *the 29th IEEE Conference on Computer Communications (INFOCOM'10)*, San Diego, California, USA.

[18] Z. Li and H. Shen. (April 2011). A hierarchical account-aided reputation management system for large-scale manets. In *the 30th IEEE Conference on Computer Communications (INFOCOM'11)*, Shanghai, China.

[19] S. Marti, T.J. Giuli, K. Lai, and M. Baker. (August 2000). Mitigating routing misbehavior in mobile ad hoc networks. In *the 6th annual international conference on Mobile computing and networking (MOBICOM'00)*, Boston, MA, USA.

[20] A. Mei and J. Stefa. (June 2010). Give2get: Forwarding in social mobile wireless networks of selfish individuals. In *the 30th International Conference on Distributed Computing Systems (ICDCS'10)*, Genova, Italy.

[21] P. Michiardi and R. Molva. (September 2002). Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Sixth Joint Working Conference on Communications and Multimedia Security*, Portorož, Slovenia.

[22] L. Wei, H. Zhu, Z. Cao, and X. Shen. (July 2011). MobiID: A user-centric and social-aware reputation based incentive scheme for delay/disruption tolerant networks. In *The 10th International Conference on Ad Hoc Networks and Wireless (ADHOC-NOW'11)*, Paderborn, Germany.

[23] F. Li, Y. Yang, and J. Wu. (March 2010). CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-based Mobile Networks. In *the 29th IEEE Conference on Computer Communications (INFOCOM'10)*, San Diego, California, USA.

[24] U. Von Luxburg. (2007). A tutorial on spectral clustering. *Statistics and Computing*, 17(4):395–416.

[25] M. E. Mahmoud, and X. Shen. (2011). An Integrated Stimulation and Punishment Mechanism for Thwarting Packet Drop in Multihop Wireless Networks. *IEEE Transactions on Vehicular Technology*, 60(8):3947–3962.

[26] J.C. Cha and J.H. Cheon. (January 2003). An Identity-Based Signature From Gap Diffie-Hellman Groups. In *the 6th International Workshop on Theory and Practice in Public Key Cryptography (PKC'03)*, Miami, Florida, USA.

[27] A. Ferrara, M. Green, S. Hohenberger, and M. Pedersen. (April 2009). Practical short signature batch verification. In *CT-RSA'09*, San Francisco, USA.

[28] G. Shafer. (1976). *A mathematical theory of evidence*. Princeton university press Princeton, NJ.

[29] V. Capasso. (1993). *Mathematical structures of epidemic systems*. Springer Verlag.

[30] Ben Lynn. The Pairing-Based Cryptography Library (PBC). *http://crypto.stanford.edu/pbc/*.

[31] A. Keränen, J. Ott, and T. Kärkkäinen. (2009). The ONE Simulator for DTN Protocol Evaluation. In *the 2nd International Conference on Simulation Tools and Techniques (SIMUTools'09)*.