MobiID: A User-Centric and Social-Aware Reputation Based Incentive Scheme for Delay/Disruption Tolerant Networks

Lifei Wei[1], Haojin Zhu[1], Zhenfu Cao[1,*], and Xuemin (Sherman) Shen[2]

[1] Shanghai Jiao Tong University, Shanghai, China
[2] University of Waterloo, Waterloo, Ontario, Canada

Abstract. Delay/Disruption tolerant networks (DTNs) are 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. Incentive issue in DTNs is extraordinarily challenging due to the unique network characteristics. To tackle this issue, in this paper, we propose *MobiID*, a novel *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 track of each other's reputation, **MobiID** allows a node to manage its reputation evidence and show to demonstrate its reputation whenever necessary. We also define the concepts of *self-check* and *community-check* to speed up reputation establishment and allow nodes to form consensus views towards targets in the same community, which is based on our social metric by forwarding willingness. Performance simulation are given to demonstrate the security, effectiveness and efficiency of the proposed scheme.

Keywords: Selfish; Reputation based incentive, Cooperating stimulation, Security, Delay/Disruption tolerant networks.

1 Introduction

Most 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 individual node is ready to forward bundles for others. However, in certain DTN applications such as

[*] Corresponding author. `zfcao@cs.sjtu.edu.cn`

H. Frey, X. Li, and S. Ruehrup (Eds.): ADHOC-NOW 2011, LNCS 6811, pp. 177–190, 2011.

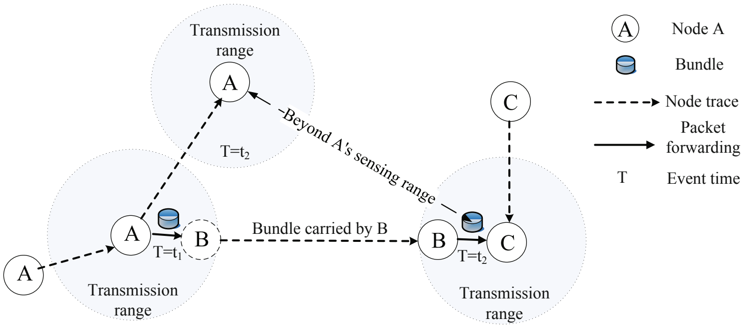


Fig. 1. A typical store-carry-and-forward transmission fashion

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 research has shown that a non-cooperative DTN may suffer from serious performance degradation [2–4]. Therefore, to deploy applicable DTNs in real-world scenarios, the proper incentive schemes considering such characteristics should be the most promising ways.

In general, incentive schemes can be classified into the following three categories: credit-based [2–9], tit-for-tat based [10], and reputation-based [11–20]. Even though incentive schemes have been well studied for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficulty to predict mobility patterns, and long feedback delay, have made the incentive issue in DTNs quite different. Therefore, there is an increasing interest in designing the incentive schemes in DTNs.

The reported incentive schemes in DTNs are mainly focusing on the credit-based and tit-for-tat based solutions. However, the reputation based schemes still receive less attention due to the special challenges brought by unique characteristics of DTNs. 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. This assumption may not hold in DTNs due to the store-carry-and-forward transmission. For example, as shown in Fig. 1, a node A forwards bundles to a node B, which carries the bundles until it meets the next hop node C. 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 neighboring detection unsuitable in DTNs. In addition, due to the long propagation delay and frequent disconnectivity, how to efficiently and effectively propagate the reputation is another challenging issue.

In this paper, we introduce a user-centric and social-aware reputation based incentive scheme, named ***MobiID***, to stimulate cooperation among selfish nodes in DTNs. **MobiID** is a dynamic reputation system where reputation can be maintained, updated, and shown for verification by each node whenever needed. Specifically, in a 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 former is defined as that a node keeps its forwarding evidence for the purpose of future directly checking by the bundle sender. The latter means that the forwarding evidence is collected and then checked through the social network to improve reputation propagating efficiency in DTNs. 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 **MobiID** can be named a "user-centric reputation" scheme.

Furthermore, **MobiID** 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 [21]. 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, **MobiID** abstracts the true willingness between the nodes by honestly recording each data forwarding. Thus, **MobiID** is also a "social-aware" scheme.

To the best of our knowledge, this paper is a novel one to propose the reputation based scheme for DTNs. Our contributions can be summarized as follows:

- Firstly, 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.
- Secondly, we propose **MobiID** to stimulate cooperation among selfish nodes in DTNs, which allows a node to maintain, update, and show its reputation tickets as an identity card whenever needed.
- Thirdly, we make use of social property to speed up **MobiID**'s reputation establishment and allow nodes in the same community to share reputation information and form consensus views towards targets.
- Lastly, **MobiID**, as a high level scheme, can be compatible with diverse data-forwarding algorithms. We also use the security techniques such as identity based signatures and batch verification to reduce the computational overhead. Extensive simulation demonstrates the efficiency and efficacy of the proposed schemes.

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

2 Models and Assumptions

In this section, we define our system model, attack model and design goals.

2.1 Social Based DTN Model

We consider a social based DTN system model, which is characterized as not only end-to-end connections are not always guaranteed and routings are made in an *opportunistic* way, but also nodes in this networks have social relationships based on their willingness.

Specifically, 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 schemes in [2], 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. Different from credit-based schemes [2], our system model do 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.

Moreover, to introduce the concept "community-check", we first define the social relationship model from the forwarding history. Our social based DTNs could be modeled as a weighted directed graph (V, E), where the vertex set V consists of all the DTN nodes and the edge set E consists of the social links between these nodes. In this work, we use the *forwarding history* instead of contact history in [21] to evaluate the weight of social links between nodes since the fact that two nodes contact 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 concept 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_i and t_{i+1}. The smaller AFT_{ij} is, the more willingness i have to forward for j. It is obviously that $AFT_{ij} \neq AFT_{ji}$. 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 [21, 22] to normalize AFT_{ij} in equation (1) and denote the resulting metric as the willingness $w_{ij} = \exp\left(-\frac{AFT_{ij}^2}{2\sigma^2}\right)$. Here, σ is a scaling parameter [21, 22]. 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 [21]. In our settings, we assume that if two nodes belong to the same community, the chance that they meet is higher than that of belonging to different communities.

2.2 Attack Models

In this paper, we assume that every node is rational. The nodes with a high reputation have chance to be chosen than the low ones for their past successful forwarding history in DTNs while 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.

In addition, we consider two kinds of DTN nodes: selfish nodes and malicious nodes, except the innocent ones 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 selfish behavior could significantly degrade network performance.

Moreover, 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.

2.3 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:

- Effectiveness. Our proposed scheme is effective in stimulating cooperation among the selfish nodes in DTNs.
- Security. Our scheme resists various regular attacks launched by malicious nodes.
- Efficiency. It is an efficient scheme without introducing too much extra communication and transmission overhead.

3 Preliminary

3.1 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* $Beta(\alpha, \beta)$ [12, 17]. 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 [15]. According to the definition, the mathematical expectation of evidence distribution is defined as following:

$$EXP(Beta(\alpha, \beta)) = \frac{\alpha}{\alpha + \beta}. \tag{2}$$

In addition, $EXP(Beta(\alpha, \beta))$ is only a ratio that can *not* reflect the uncertainty of distribution since the mathematical expectation are equal in the case of $(\alpha, \beta) = (1, 1)$ and $(\alpha, \beta) = (10, 10)$. Thus, we need to find the normalized variance of evidence distribution to describe the uncertainty.

$$VAR(Beta(\alpha, \beta)) = \frac{12 \cdot \alpha \cdot \beta}{(\alpha + \beta)^2 \cdot (\alpha + \beta + 1)} \tag{3}$$

3.2 Cryptographic Technology

In **MobiID**, signatures, signed by the next hop node, are introduced to authenticate forwarding evidence. Each node has an unique ID never changed in the scheme, which is used as its public key to verify signatures. To reduce the computational cost of **MobiID**, we adopt a cryptographic technology based on a signature scheme [23] and its well-known batch verification version [24], which consist 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. An efficient admissible bilinear pairing $\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ be two cyclic multiplicative groups of the same prime order q, (i.e., $|\mathbb{G}_1| = |\mathbb{G}_2| = q$), has 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 exist $P \in \mathbb{G}_1$ such that $\hat{e}(P, P) \neq 1$; (3) Computable: there is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in \mathbb{G}_1$. In addition, it chooses two cryptographic hash functions $H_1 : \{0,1\}^* \to \mathbb{G}_1$ and $H_2 : \{0,1\}^* \to \mathbb{Z}_q^*$. After that, OSM picks a random number s, where $s \in \mathbb{Z}_q^*$ as 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, system parameters $params$ 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 system initialization and registration 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 $Sig_{ID}(m)$ $= (U, V)$ where $U = r \cdot H_1(ID)$ and $V = (r + H_2(U\|m)) \cdot sk_{ID}$.

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

Aggr. To improve efficiency, it first combines signatures $\{Sig_{ID_i}(m_i)=(U_i, V_i)|1 \leq i \leq n\}$ 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: $\hat{e}(V_{Bat}, P) \overset{?}{=} \hat{e}(U_{Bat}, P_{pub})$

4 The Proposed MobiID Scheme

In this section, we first introduce the primitive concept of "reputation ticket". Then we illustrate how **MobiID** works in the bundle forwarding by making full use of reputation tickets to stimulate nodes' cooperation. The goal of our scheme is to detect and punish selfish nodes in order to encourage nodes' forwarding. By punishing these nodes, we show that behaving selfish will not benefit them. Instead, behaving cooperative has a better chance to increase their benefit.

4.1 Bundle Forwarding

Fig. 2 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, two cases emerge.

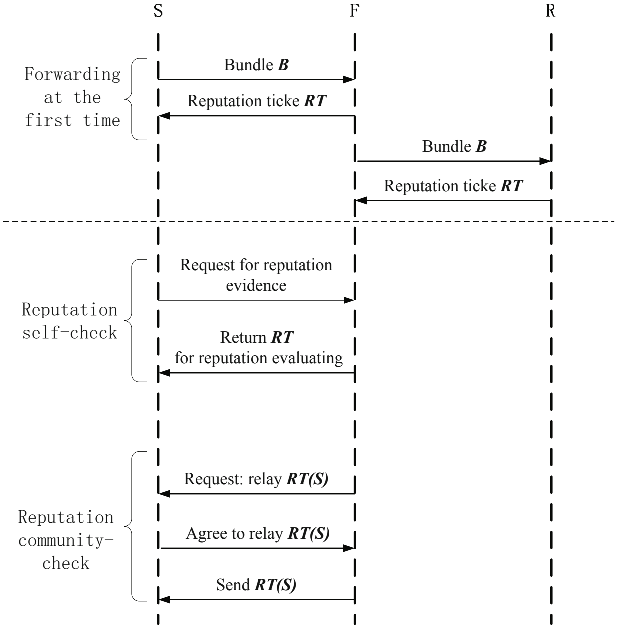


Fig. 2. The Proposed **MobiID** Scheme

Case a: If they meet at first time, F directly forwards bundles to S and sets the initiate reputation value of F. After S sends the bundle to F, F replies to S a reputation ticket as an evidence of successful forwarding of S. Similarly, F receives a reputation ticket from the next hop node R and keeps it for future checking in the next encounter with S. The format of reputation ticket is shown in Fig. 3. Specifically, it is comprised of ticket sequence number id, sender node S, forwarding node F, receiving node R, time stamp TS and bundle hash value. SI_S is the social group identifier of S which will be used in the reputation social agreement later. R's signature $Sig_R(id\|S\|SI_S\|F\|R\|TS\|H(B))$ is constructed. This reputation ticket provides an evidence that F forwarded S's bundle to R at time TS.

id	S	SI_S	F	R	TS	$H(B)$	Sig_R

Fig. 3. A reputation ticket after forwarding a packet

Different from any existing reputation schemes, **MobiID** allows each node to maintain its own reputation tickets in the local buffer and thus is able to provide its own reputation on its demand. The node could also actively update its reputation by self checking. Therefore, **MobiID** is a *user-centric* scheme, where reputation computing does not depend on others. This feature makes it highly appealing in DTNs which suffer from frequent disconnectivity and high propagation delay.

Case b: If these two nodes met before, S starts the reputation self-check algorithm. In our settings, we assume the "good property": If S and F meet once, it is likely that they will meet again in the near future.

4.2 Reputation Self-Check

S starts the reputation self-check algorithm to evaluate F's forwarding quality. S first finds out the forwarding records in the last encounter to verify the expiration time of reputation tickets and then requires 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 where $NtF(S, F)$ denotes the number of bundles that S required F to forward in the last encounter. $NaF(S, F)$ denotes the number of bundles 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 in a individual model or a batch model:*

Individual-Verification model: *S individually takes $IndVer(U_i, V_i)$.*

Batch-Verification model: *S takes $Aggr(U_i, V_i)$ and $BatVer(U, V)$.*

If the node F completes the bundle forwarding, that is, $NtF(S, F) \leq NaF(S, F)$. The observed forwarding result is considered to be a success, Otherwise, a failure.

To reason from observation results and further to generate the reputation metric, we denote α and β to represent the total number of observed successful forwarding and failure forwarding, respectively. s and f are the successful forwarding and failure forwarding in this observation. Thus, we have

$$\alpha \leftarrow \alpha + s \ \ and \ \ \beta \leftarrow \beta + f; \tag{4}$$

According to the definition of Bayesian inference, the basic reputation value can be quantified by the expectation (2) of evidence distribution $v_{S-F} = EXP((Beta(\alpha, \beta)))$ and $u_{S-F} = VAR(Beta(\alpha, \beta))$. 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):

$$ARV_{S-F} = v_{S-F} \cdot (1 - u_{S-F}) = \frac{\alpha}{\alpha + \beta} \cdot (1 - u_{S-F}). \tag{5}$$

Additionally, to take it into account that the reputation value fades along the time, we give some discount weight ω to indicate the freshness of reputation as an aging factor for a time slot ΔT, such that,

$$\alpha = \omega^{\frac{t_d - t_s}{\Delta T}} \alpha + s \ \ and \ \ \beta = \omega^{\frac{t_d - t_s}{\Delta T}} \beta + f \tag{6}$$

4.3 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. The case that ARV is higher than T_{High} indicates that this candidate node is willing to forward bundles for S and S prepares to send it new bundles as in the section 4.1. Besides, as a reward, S agrees to forward reputation tickets for F and starts reputation social establishment procedure in the section 4.4. 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

Algorithm 1. Reputation Self-Check Algorithm

```
procedure ReputationSelfCheck
if node $F$ is in the blacklist then
    procedure stops;
end if
$S$ asks $F$ to show its reputation ticket;
for each reputation tickets $F$ returns do
    $S$ verifies in a individual model or in a batch model
end for
$S$ makes observations to obtain $s$ and $f$ and $S$ updates $F$'s $ARV_{S-F}$ by (5);
$S$ starts to make a decision based on new $ARV_{S-F}$.
if $ARV_{S-F} < T_{Low}$ then
    $F$ is considered as a selfish node and put into the blacklist and procedure stops;
else
    if $ARV_{S-F} \geq T_{High}$ then
        $F$ is considered as a good forwarder and $S$ starts community check procedure:$F$
        submits the reputation tickets in its buffer belonging to the same community of $S$.
    else
        $F$ is considered an inactive node. $S$ warns $F$ by not doing community check.
    end if
end if
end procedure
```

when they are meeting later in the section 4.4. In the case that the reputation value is between T_{High} and T_{Low}, S still sends bundles to F but gives a warning to F and does not propagate reputation tickets this time to encourage F forwarding more actively. 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 in time. This leads to a reputation drop of the selfish nodes. Therefore, they need to find some new nodes which do not put them in the blacklist or they just wait for the sender to meet again.

4.4 Reputation Community-Check

We demonstrate how to efficiently and effectively propagate reputation by reputation community-check. Due to DTN's long propagation delay and frequent disconnectivity, the "good property" in the reputation self-check would not preform so well when two nodes, belonging to different communities, encountered occasionally before. According to the definition of social community, two nodes in the same community have a higher probability to meet and forward bundles to each other periodically than that of in the different community since our community is constructed to reflect locality and forwarding willingness. Therefore, our reputation community-check mechanism is built on the community level, which allows nodes in the same community to share reputation information to accelerate reputation collection. After that, all nodes in the same community can form consensus views towards the targets.

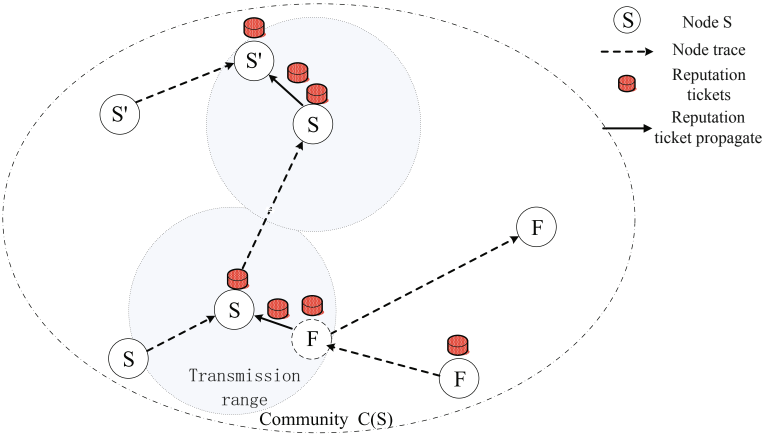


Fig. 4. Reputation social establishment

As shown in Fig. 4, if S agrees to help F to community check reputation tickets, F sends the related reputation tickets whose $SGI \in SI_S$. This means 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 check algorithm 2.

Algorithm 2. Reputation Community Check Algorithm

```
procedure ReputationCommunityCheck
    When $S$ meets its community member, $S'$, they exchange their reputation tickets and blacklists.
    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
        $v_{SS'-F} = \frac{(1-u_{S-F}) \cdot v_{S-F} + (1-u_{S'-F}) \cdot v_{S'-F}}{(1-u_{S-F}) + (1-u_{S'-F})}$
end procedure
```

When this reputation community check continues, nodes in the same community can form consensus views towards the target F by

$$v_F = \frac{\sum_{i \in C(i)} (1-u_{i-F}) \cdot v_{i-F}}{\sum_{i \in C(i)} (1-u_{i-F})}, \tag{7}$$

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

$$ARV_{S-F} = v_F \cdot (1 - u_F). \tag{8}$$

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

5 Performance Analysis

We model our reputation community check as an epidemic problem [25] 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. For the limit of space, we omit the proof.

6 Simulation

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

6.1 Cryptographic Overhead Evaluation

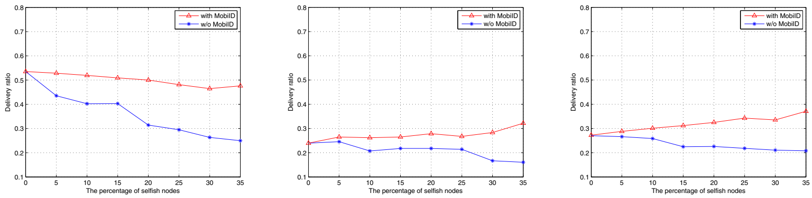
Our simulation consists of Intel Core 2 Duo P7450 (2.13GHz) with 1 GB RAM based on the Pairing Based Cryptography Library (PBC) [26] in the Ubuntu 9.10 to evaluate the delays of cryptographic operations, which are summarized in Table 1. Since signature-aggregation algorithm could be performed incrementally 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.

Table 1. Cryptographic Overhead

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

6.2 Performance Simulation

Simulation Step. We implement our **MobiID** in a public DTN simulator, namely, the Opportunistic Networking Environment (ONE) simulator [27], 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 details parameters are given as follows: Duration: 12 hours; Number of nodes: 126; Speed of nodes: 0.5 m/s $\sim$ 13.92 m/s; Transmission



(a) Spray and Wait routing (b) Epidemic routing (c) Prophet routing

Fig. 5. Incentive effectiveness comparison of **MobiID** with diverse data-forwarding algorithms

range: 10 m; Transmission speed: 2 Mbps; Buffer size: 5 MB $\sim$ 50 MB; Bundle generation interval: 15 s $\sim$ 35 s.

Incentive Effectiveness. We begin our simulation by observing the incentive effectiveness of **MobiID**, which can be measured by the bundles' average successful delivery probability under different percentages of selfish nodes or selfish behaviors, as shown in Fig. 5, from 0% to 35%. Additional, our scheme can be compatible with diverse data-forwarding algorithms such as Spray and Wait (Fig. 5(a)), Epidemic (Fig. 5(b)), Prophet (Fig. 5(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 **MobiID**, 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 **MobiID**.

7 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, 28], are usually employed to provide incentive such as virtual credits to encourage selfish nodes forwarding. A recent work [10] proposes pair-wise Tit-for-Tat as an incentive scheme in DTNs.

Reputation-based incentive schemes 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 [17] to reward or punish selfish node. [11] proposes two techniques: watchdog and pathrater. CORE, in [13], uses the watchdog mechanism to observe neighbors and then detect and isolate selfish nodes. [14] proposes OCEAN, in which each node maintains the ratings for neighbors through directly interacting, but these ratings are not propagated to other node. SORI [15] proposes the concepts of first-hand reputation and second-hand reputation and shows to weighted sum these values. [16] proposes a reputation management system (RMS) in mobile ad hoc networks. [19] 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, [20] proposes a social selfishness aware routing algorithm to provides better routing performance in an efficient way. [18] designs a reputation-assistant framework to accurately evaluate encounter's competency of delivering data in opportunistic networks.

8 Conclusions

In this paper, we propose **MobiID**, a novel "user-centric" and "social-aware" reputation based incentive scheme for DTNs to stimulate cooperation in bundle forwarding. Different from the conventional reputation based incentive schemes, **MobiID** allows each node to maintain and update its reputation tickets in the local buffer and thus provide its reputation on demand. Besides, we measure a new willingness between two nodes, which is extracted from a social wireless network. We further provide a social based solution "community check" to accelerate the reputation checking and establishing. Our future work includes investigating the privacy issue of reputation systems in DTNs.

Acknowledgments

This paper is partially supported by the Key Program of the National Natural Science Foundation of China (Grant No. 61033014), the National Natural Science Foundation of China (Grant No. 60972034, 60970110, and 61003218) and the National Fundamental Research Development Program of China (973) (Grant No. 2007CB311201). This paper is also supported by the Science and Technology Fundamental Infrastructure Construction Project of Jiangsu Province–Engineering Research Center (Grant No. BM20101014). Prof. Zhenfu Cao is the corresponding author, whose email address is zfcao@cs.sjtu.edu.cn.

References

1. Fall, K., Farrell, S.: DTN: an architectural retrospective. IEEE Journal on Selected Areas in Communications 26(5), 828–836 (2008)
2. Zhu, H., Lin, X., Lu, R., Fan, Y., Shen, X.: SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks. IEEE Transactions on Vehicular Technology 58(8), 4628–4639 (2009)
3. Chen, B., Chan, M.: MobiCent: a Credit-Based Incentive System for Disruption Tolerant Network. In: INFOCOM 2010, San Diego, California, USA, March 14-19 (2010)
4. Lu, R., Lin, X., Zhu, H., Shen, X., Preiss, B.: Pi: a practical incentive protocol for delay tolerant networks. IEEE Trans. on Wireless Communications 9(4), 1483–1493 (2010)
5. Buttyan, L., Hubaux, J.P.: Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications 8(5), 579–592 (2003)
6. Zhong, S., Chen, J., Yang, Y.: Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: INFOCOM 2003, San Franciso, USA, March 30-April 3 (2003)
7. Anderegg, L., Eidenbenz, S.: Ad hoc-VCG: a truthful and cost-efficient routing protocol for mobile ad hoc networks with selfish agents. In: MOBICOM 2003, San Diego, CA, USA, September 14-19 (2003)

8. Zhang, Y., Lou, W., Liu, W., Fang, Y.: A secure incentive protocol for mobile ad hoc networks. Wireless Networks 13(5), 569–582 (2007)
9. Mahmoud, M.E., Shen, X.: FESCIM: Fair, Efficient, and Secure Cooperation Incentive Mechanism for Multi-hop Cellular Networks. IEEE Trans. on Mobile Computing (to appear)
10. Shevade, U., Song, H., Qiu, L., Zhang, Y.: Incentive-Aware Routing in DTNs. In: ICNP 2008, Orlando, Florida, USA, October 19-22 (2008)
11. Marti, S., Giuli, T., Lai, K., Baker, M.: Mitigating routing misbehavior in mobile ad hoc networks. In: MOBICOM 2000, Boston, MA, USA, August 6-11 (2000)
12. Jøsang, A., Ismail, R.: The beta reputation system. In: The 15th Bled Electronic Commerce Conference, Bled, Slovenia, June 17-19 (2002)
13. Michiardi, P., Molva, R.: 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, September 26-27 (2002)
14. Bansal, S., Baker, M.: Observation-based cooperation enforcement in ad hoc networks. Arxiv preprint cs/0307012 (2003)
15. He, Q., Wu, D., Khosla, P.: SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad hoc Networks. In: WCNC 2004, Atlanta, GA, USA, March 21-25 (2004)
16. Anantvalee, T., Wu, J.: Reputation-based system for encouraging the cooperation of nodes in mobile ad hoc networks. In: ICC 2007, SECC, Glasgow, Scotland, June 24-28 (2007)
17. Jøsang, A., Ismail, R., Boyd, C.: A survey of trust and reputation systems for online service provision. Decision Support Systems 43(2), 618–644 (2007)
18. Li, N., Das, S.: RADON: reputation-assisted data forwarding in opportunistic networks. In: MobiOpp 2010, Pisa, Italy, February 22-23 (2010)
19. Mei, A., Stefa, J.: Give2get: Forwarding in social mobile wireless networks of selfish individuals. In: ICDCS 2010, Genova, Italy, June 21-25 (2010)
20. Li, Q., Zhu, S., Cao, G.: Routing in socially selfish delay tolerant networks. In: INFOCOM 2010, San Diego, California, USA, March 14-19 (2010)
21. Li, F., Yang, Y., Wu, J.: CPMC: An Efficient Proximity Malware Coping Scheme in Smartphone-based Mobile Networks. In: INFOCOM 2010, San Diego, California, USA, March 14-19 (2010)
22. Von Luxburg, U.: A tutorial on spectral clustering. Statistics and Computing 17(4), 395–416 (2007)
23. Cha, J., Cheon, J.: An Identity-Based Signature From Gap Diffie-Hellman Groups. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 18–30. Springer, Heidelberg (2002)
24. Ferrara, A.L., Green, M., Hohenberger, S., Pedersen, M.Ø.: Practical short signature batch verification. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 309–324. Springer, Heidelberg (2009)
25. Capasso, V.: Mathematical structures of epidemic systems. Springer, Heidelberg (1993)
26. Lynn, B.: The Pairing-Based Cryptography Library (PBC), `http://crypto.stanford.edu/pbc//`
27. The Opportunistic Network Environment simulator (The ONE) Version 1.4.0 (March 18, 2010), `http://www.netlab.tkk.fi/tutkimus/dtn/theone/`
28. Mahmoud, M.E., Shen, X.: ESIP: Secure Incentive Protocol with Limited Use of Public-Key Cryptography for Multi-hop Wireless Networks. IEEE Trans. on Mobile Computing (to appear)