Copyright ⓒ 2012 KSII

PRI: A Practical Reputation-based Incentive Scheme for Delay Tolerant Networks

Xi Zhang, Xiaofei Wang, Anna Liu, Quan Zhang and Chaojing Tang[1]

[1] School of Electronic Science and Engineering, National University of Defense Technology
Changsha, 410073 – China
[e-mail: zisline.nudt@gmail.com]
*Corresponding author: Xi Zhang

Received December 13, 2011; revised February 19, 2012; accepted April 6, 2012; published April 25, 2012

Abstract

Delay tolerant networks (DTNs) characterized by the lack of guaranteed end-to-end paths exploit opportunistic data forwarding mechanism, which depends on the hypothesis that nodes are willing to store, carry, and forward the in-transit messages in an opportunistic way. However, this hypothesis might easily be violated by the presence of selfish nodes constrained with energy, bandwidth, and processing power. To address this problem, we propose a practical reputation-based incentive scheme, named PRI, to stimulate honest forwarding and discipline selfish behavior. A novel concept of successful forwarding credential and an observation protocol are presented to cope with the detection of nodes' behavior, and a reputation model is proposed to determine egoistic individuals. The simulation results demonstrate the effectiveness and practicality of our proposal.

Keywords: DTNs, reputation, incentive, cooperation, security.

This research was supported by the National Natural Science Foundation of China under Grant 61101073. We express our thanks to the Editors and the anonymous reviewers for their detailed comments and valuable contribution to improve our manuscript.

http://dx.doi.org/10.3837/tiis.2012.04.001

1. Introduction

Delay tolerant networks (DTNs) provide a promising approach to support various applications in challenging environments where an end-to-end path between the communication sources and destinations is unavailable occasionally [1][2]. The application of DTN concept benefits diverse applications that often suffer from frequent network partitioning, e.g. supporting rural schools in developing countries, low-cost Internet service provision, zebra tracking in Africa, and social networking [3][4][5]. In DTNs, due to sparse node density and unpredictable node mobility, bundles, the in-transit messages, are opportunistically routed to the destinations, which follows a store-carry-and-forward paradigm.

Most of the literatures on opportunistic data propagation in DTNs [6][7][8] so far have assumed that each node is willing to cooperate in the dissemination process and forward bundles for others honestly. However, since each DTN node operates under energy and storage resource constraints, some nodes may exhibit various degrees of selfishness and be unwilling to serve as bundle relays or custodians on behalf of others to conserve limited buffer and power. Thus, the hypothesis that each individual node behaves rationally to share its own resources for global connectivity might easily be violated [9][10][11]. In order to conserve energy, bandwidth, and processing power, egoistic nodes may refuse to cooperate and serve as a bundle relay, which dramatically degrades network performance, even leads to a nonfunctional network in certain circumstances when opportunistic routes are needed. Therefore, how to restrain selfishness in DTNs has become a challenging issue.

To address the selfishness issue, some credit-based and reputation-based incentive schemes [12][13][14][15][16], providing efficient and promising solutions, are proposed. Credit-based schemes, e.g. payment schemes, aim at stimulating selfish nodes to cooperate through introducing some form of virtual currency. Nodes are paid for forwarding, and pay for the forwarding of their own bundles transmitted by others. These schemes make selfish nodes unwilling to deny forwarding, however, selfish nodes target other types of misbehavior, e.g. silent route changes. Reputation-based schemes monitor and rate the behavior of neighboring nodes so that nodes can respond according to the opinion on others. These schemes enable nodes to distinguish and exclude egoistic nodes. Reputation schemes are eligible for coping with any kind of misbehavior as long as it is observable [15].

However, the unique characteristics of DTNs make the existing schemes, which are proposed for conventional ad hoc networks or P2P networks, not applicable for DTNs. First, due to the intermittent connectivity and network partitioning, the hypothesis, adopted in existing schemes, that there is a contemporaneous end-to-end path between the source and destination does not hold. Second, opportunistic forwarding makes the main approaches to detect neighboring nodes' behavior, e.g. promiscuous listening mode, inefficient. Third, multiple-copy routing adopted in DTNs to improve network performance and communication reliability is not compatible with existing schemes designed for single-copy routing.

In this paper, to cope with the selfishness in DTNs, we propose a practical reputation-based incentive scheme, named PRI, which enables DTNs to keep functioning and improves network performance despite the presence of misbehaving nodes. With the proposed scheme, selfish nodes have to behave honestly in the bundle propagation process in order to avoid being isolated from networks. Specifically, the contributions of this paper are twofold.

- First, in order to address the monitoring of nodes' behavior, we provide a novel concept of successful forwarding credential (SFC) which serves as a behavior record of

successful forwarding. The generation and transmission of this credential is integrated into an observation protocol presented in our proposal. A verifiable signature technique [17] is adopted to guarantee the feasibility and provides authentication and integrity protection in the PRI scheme.

- Second, to achieve fairness, a novel reputation model is presented. In this model, both the quantity that a node cooperates and the ratio of successful forwarding to total have an impact on reputation values. In order to obtain a good reputation value, nodes need to provide reliable service of forwarding continuously. Furthermore, each DTN node provides service of forwarding for honest nodes in advance, and excludes selfish nodes whose values are below a deterministic reputation threshold, which energetically stimulates all individuals to cooperate in forwarding in order to earn a great reputation.

The remainder of this paper is organized as follows: In Section 2, we give an overview of related work. Section 3 provides the system models and the design goal. In Section 4, we present our PRI scheme in detail. The performance evaluation is given in Section 5, followed by a conclusion in Section 6.

2. Related Work

In DTNs, the lack of contemporaneous end-to-end routes and high variation in network conditions make most of the existing incentive schemes designed for traditional ad hoc networks and P2P networks [12][15][16][18][19] not eligible. Recently, more and more researchers start to focus on the selfishness problem in DTNs.

Karaliopoulos analytically assesses the performance of the unrestricted and two-hop relay schemes when nodes behave selfishly in the process of bundle propagation. Their numerical results demonstrate the negative impact of selfish behavior only on the message transmission delay [20]. Shevade et al. [10] study the impact of selfish behavior on DTNs, and present an incentive mechanism to stimulate cooperation. However, the security issues of this incentive scheme are not taken into consideration. Li et al. [21] study the social selfishness and propose an incentive-aware routing to improve network performance. Li et al. [22] evaluate the impact of social selfishness on DTN unicast routing in terms of delay and cost. Furthermore, Li et al. [11] investigate how the selfish behavior affect the performance of DTN multicast, and give a conclusion that the performance of multicast with selfish nodes depends on the multicast group size.

Most of the aforementioned literatures focus on the impact of misbehaving nodes rather than the solutions of egoism in DTNs. The SMART [9] and Pi [10], as credit-based schemes, are firstly propoesd to resolve the selfishness problem in DTNs. In [9], Zhu et al. propose a secure multilayer credit-based incentive scheme, called SMART, to stimulate cooperation among DTN nodes. In SMART, a layered coins model is presented and serves as virtual currency to pay for the relays who participate in forwarding bundles. Furthermore, the proposed scheme can be implemented to thwart various attacks, e.g. credit forgery attack, nodular tontine attack, and submission refusal attack. In [10], a pactical incentive protocol, named Pi, is presented to provide the fairness in DTNs. In the Pi protocol, if and only if bundles are successfully delivered to the destination, intermediate nodes can get credits from the source node, or else, for the failure of bundle forwarding, intermediate nodes can earn good reputation values from a trusted authority. In both of the aforementioned schemes, there exists a trusted authority to take charge of credit clearance. The authority serves as a virtual bank and performs fair virtual currency clearance. In the Pi protocol, it introduces reputation values to

compensate intermediate nodes who take part in a failed forwarding process, however, it still relays on the virtual bank for reputation clearance.

Different from the aforementioned schemes, we propose a reputation-based incentive scheme for DTN and provide an efficient solution, the introduction of SFC and the observation protocol, to monitor neighboring nodes , detect misbehavior, and rate on others' behavior, which distinguishes the PRI scheme from all the aforementioned works. To the best of our knowledge, no previous incentive schemes for DTNs falls into the category of reputation. We are the first to investigate the solution based on reputation to resolve the selfishness in DTNs. Furthermore, our proposal is compatible with multiple-copy routing adopted to enhance the reliability of communication, which makes PRI pactical for DTNs.

3. System Model and Design Goals

In this section, we describe our system model and design goal in detail.

3.1 Network Model

In our model, a general DTN, e.g. a vehicular DTN, is formed by a set of mobile vehicles with limited transmission capabilities. Due to the lack of a contemporaneous end-to-end link, the data forwarding process follows a "store-carry-and-forward" paradigm, and bundles are opportunistically routed. When two mobile nodes move into each other's transmission range and contact for a period of time, bundles could only be forwarded. For two nodes outside the transmission range of each other, the transmissions of bundles rely on the forwarding of intermediate nodes in a multiple-hop manner.

We assume that there is an offline security manager, abbreviated as OSM, which is in charge of key distribution. Before joining the network, each DTN node should be registered in the OSM and obtain its secret key.

3.2 Node Model

In DTNs, each node i is assumed to have a unique identifier ID_i. We will use node i and N_i interchangeably to refer to the same DTN entity hereafter. In general, each node is considered resource-restrained, e.g. computational power, storage and energy. In order to conserve energy, some selfish nodes are unwilling to serve as relays and may provide unreliable service to others. They are assumed to misbehave in the message propagation process and drop bundles on purpose.

In our model, when a node i has a bundle B for forwarding, it does not set a routing path in advance, but only needs to attach some affiliation information AI. The AI consists of the followings: BI, which contains the basic information of the bundle, e.g. the identities of the source node and the destination node, the session number, and time-to-life information; HI, which contains the identities of the node from whom the bundle is forwarded and to whom the bundle is sent besides itself; TS, which denotes the creation timestamp; and Sig, which refers to the signature signed by node i to protect the authenticity and integrity of this affiliation information.

3.3 Design Goal

Our design goal is to develop a practical reputation-based scheme to cope with the selfishness in DTNs. In general, two following objectives will be achieved.

- Improving the network performance in the presence of selfish nodes: The egoism in DTNs leads to a dramatically performance degradation. To address the egoistic misbehavior, a reputation-based scheme is proposed. With the PRI scheme, nodes will exclude selfish nodes from the network, by both avoiding them in routing and denying their cooperation, so that selfishness will result in isolation and thus can be restrained. The DTNs' performance, in terms of high successful delivery rate and low average delay, can be assured.
- Fairness in bundle forwarding: As a reputation-based scheme, we take the fairness into consideration. In order to get a good reputation, nodes must be able to have a higher successful probability of transmission, and provide more forwarding services for others. The fairness in DTNs makes nodes willing to provide their own resources for global connectivity.

4. Proposed PRI Scheme

In this section, we propose the PRI scheme, which is composed of the followings: monitoring, in which an observation protocol is presented to cope with monitoring the behavior of others; reputation, which is in charge of the computation of reputation values; and response, which describes the strategy on misbehaving nodes. Before the detailed description of our proposal, we give some preliminary background of bilinear pairing technique and an overview of the PRI scheme first.

4.1 Bilinear Pairing

The bilinear pairing, a mature cryptographic technique, serves as the basis of our scheme. Let G_1 and G_2 denote an additive cyclic group and a multiplicative cyclic group, respectively. Both of the groups are with the same order *q*. Let *P* be an arbitrary generator of G_1. The cryptographic pairing is defined as $\hat{e}: G_1 \times G_1 \to G_2$, which has the following properties:

- Bilinear. $\forall R, S \in G_1$ and $a, b \in Z_q^*$, $\hat{e}(aP, bP) = \hat{e}(P, P)^{ab}$.
- Nondegenerate. $\hat{e}(P, P) \neq 1_{G_2}$.
- Computable. There is an efficient algorithm to compute $\hat{e}(R, S)$, $\forall R, S \in G_1$.

4.2 Overview of PRI scheme

In the PRI scheme, we assume a general multiple-copy forwarding manner, as shown in **Fig.1**. For each bundle *B* generated by the source node *S*, multiple copies of *B* spread into the network and opportunistically route to the destination node *D*, which follows a hop-by-hop strategy.

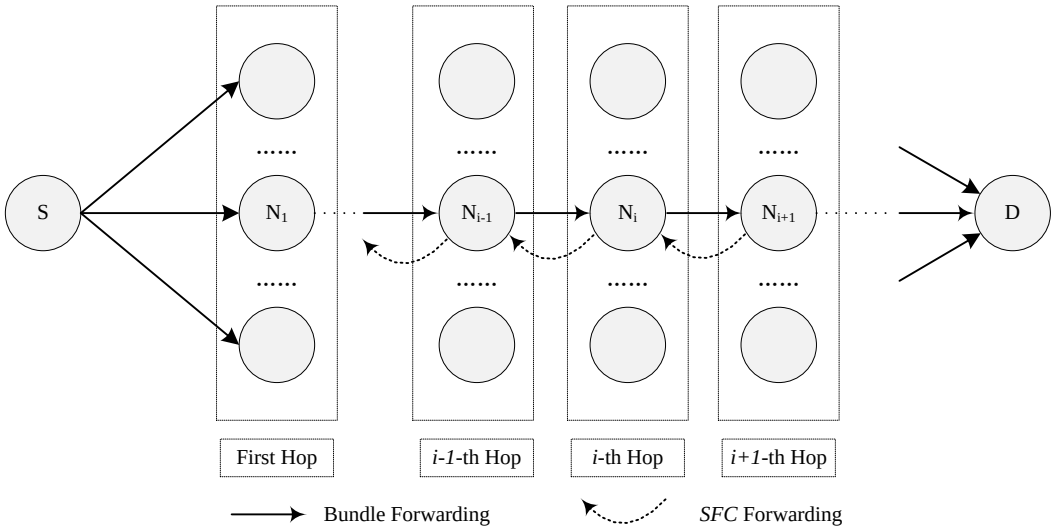


Fig. 1. Generalized data forwarding strategy in the PRI scheme

In DTNs, intermittent connectivity, network partitioning, and sparse node density makes promiscuous listening mode, the main approach to detect neighboring nodes' misbehavior, inefficient. In order to detect misbehavior of selfish nodes, the concept of SFC is introduced, and the transmission of SFC is integrated into the bundle propagation process. Notice that, SFC can be forwarded back to previous hop nodes through opportunistic links. Furthermore, with the observation protocol presented in our scheme, each DTN node is capable of keeping track on first-hand information about the bundle-forwarding behavior of neighboring nodes. In PRI, the introduction of SFC and the design of the observation protocol take the place of conventional observation modes, and provide a novel solution for the detection of misbehaving in challenged networks. A node i always maintains and updates a list of n nodes, denoted by NL_i, which contains all the forwarding nodes that node i contacts directly or receives related information from others. Node i keeps track of two factors for node j in the NL_i, as below.

- TF_{ij}: The total number of bundles that node i has transmitted to node j for forwarding.
- CF_{ij}: The number of bundles that node i has received the SFC and confirmed the successful forwarding of node j.

According to the first-hand information of transactions with others, the two factors are updated after a deterministic time period τ by the following rules. After a bundle is successfully delivered, receiving node N_{i+1} needs to send a SFC_{i+1} back to the forwarding node N_i as a respond. The factor $TF_{i(i+1)}$, which records the total times of forwarding about node N_{i+1}, increases by one automatically. After the bundle is successfully forwarded, node N_{i+1} will receive SFC_{i+2} from the next-hop intermediate node, and then, send SFC_{i+2} to node N_i as the credential for honest forwarding through an opportunistic link. After the verification of SFC_{i+2} is passed, node N_i confirms the forwarding of node N_{i+1}, meanwhile, the factor $CF_{i(i+1)}$, which records the times of confirmed forwarding about node N_{i+1}, increases by one automatically.

Additionally, in order to detect misbehaving nodes before having a bad experience, node i is allowed to use second-hand information through reputation propagation from others. It is worth pointing out that the reputation-related information exchanged between two nodes is piggybacked only once in each time period to minimize transmission cost.

As shown in **Fig. 2**, a framework of the PRI scheme is presented. The calculating of reputation value is composed of three parts: historical reputation values in former time period, the first-hand information obtained through direct monitoring, and the second-hand information through reputation propagation. When a node wants to send a bundle, it checks the list of nodes within its transmission coverage. And then, through the query of reputation value maintained in database, the node determines the list of honest nodes in terms of reputation decision rules. Finally, all the selfish nodes are excluded in routing, and the next-hop intermediate nodes are selected from the list of honest nodes according to routing algorithms. Thus, the PRI scheme is integrated into DTN routing, and enables nodes to distinguish egoistic individuals in routing decision. The performance of DTNs can be improved despite of the presence of selfishness.

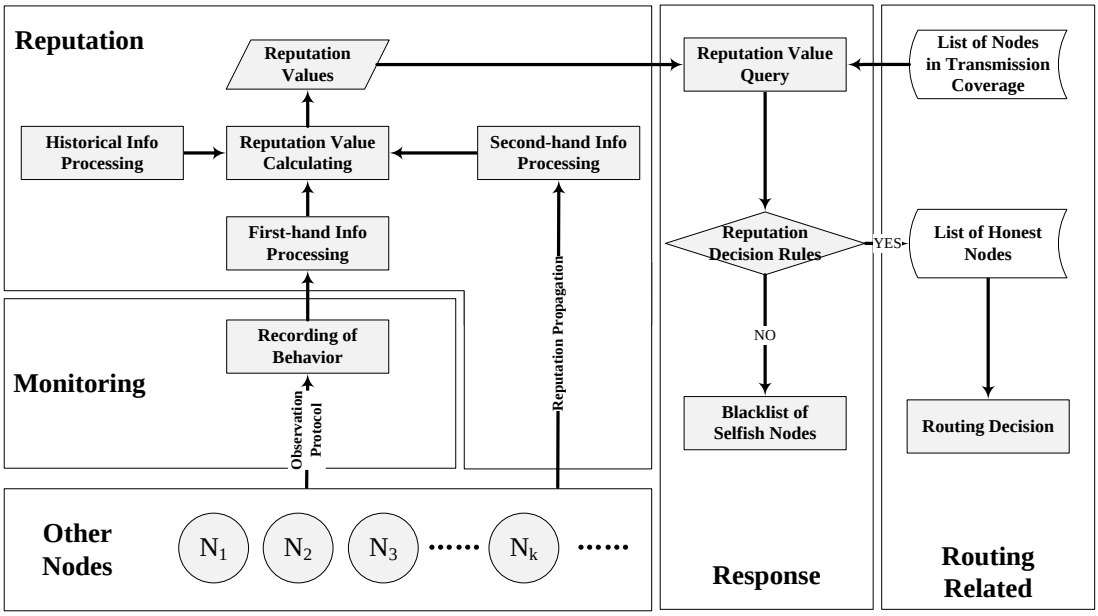


Fig. 2. The Framework of the PRI Scheme

4.3 Monitoring

We propose an observation protocol to monitor others and gather the first-hand information on their behavior. The proposed observation protocol consists of three parts: system initialization, bundle generation, and bundle forwarding.

1) System Initialization: The OSM is in charge of key distribution in registration procedure. The OSM chooses $s \in Z_q^*$ as its secret key, and computes the global public key $P_{pub} = sP$. A hash function $H : \{0,1\}^* \rightarrow G_1$ is chosen. And then, the system parameter $\{G_1, G_2, \hat{e}, P, P_{pub}, H\}$ is published, which will be configured in each DTN node. After the verification of identity information is passed in the registration procedure, the OSM computes the secret key for the identity as $sk = sH(ID)$, in which $pk = H(ID)$ serves as the public key.

2) Bundle generation: When a source node *S* wants to send a bundle *B* to the destination node *D*, it will run the following steps.

Step. 1: Generate *B*, which follows the format defined in bundle protocol specification [23].

Step. 2: Determine the list of next-hop forwarding nodes within its transmission range. Notice that, the reputation values of all the selected nodes need to exceed a deterministic reputation threshold.

Step. 3: Choose a $r \in Z_q^*$, and compute $\sigma_1 = sk_s + rH(B \| BI \| HI \| TS)$ and $\sigma_2 = rP$ to get the final signature $Sig = (\sigma_1 \| \sigma_2)$. Here, Sakai-Ohgishi-Kasahara's ID-based signature is selected to generate signature [17].

Step. 4: Forwards *B* attached with the affiliation information *AI* to the list of next-hop intermediate nodes as follows:

$$S \to List : B, AI_s \tag{1}$$

Notice that, the proposed observation protocol is compatible with multiple-copy routing. The generation and delivery of SFC is the key issue for the observation protocol. For a multiple-copy forwarding scheme, bundle copies may be forwarded along with multiple paths, and the same as SFC. In each forwarding path, SFC can be sent back to the previous hop node through opportunistic links. A multiple routing is compatible with the observation protocol. We assume that the bundle is delivered by the forwarding path $S \to N_1 \to ... \to N_{i-1} \to N_i \to N_{i+1} \to ... \to D$, as shown in **Fig.1**. We cite it as an example to show the details of our protocol.

3) Bundle Forwarding: When an intermediate node N_i receives the message, it performs the following steps to verify *B* and *AI*.

Step. 1: Check the timestamp and *TTL* if the bundle is in its lifetime.

Step. 2: Check the timestamp in the *AI* if the affiliation information is in its lifetime.

Step. 3: Check the signature by verifying if the following equation holds good.

$$\hat{e}(pk_{N_{i-1}}, P_{pub})\hat{e}(H(B \| BI \| HI \| TS), \sigma_2) = \hat{e}(\sigma_1, P) \tag{2}$$

After the aforementioned verification is passed, intermediate node N_i performs the following steps:

Step. 1: Generate the SFC, where *SET* includes the identities of three parts, the node that provides this evidence, the node who forwards the bundle, and the node to whom the SFC is destined.

Step. 2: Send it back to the forward-hop node N_i as a response for successful delivery as follows:

$$N_i \to N_{i-1} : SFC_{N_i}, \text{ where } SFC_{N_i} = (BI \| SET_{N_i} \| TS \| Sig_{N_i}) \tag{3}$$

Step. 3: Determine the next-hop node N_{i+1}, and generate new affiliation information just as what the source node does.

Step. 4: Forward *B* and new *AI* to nodes N_{i+1}, as follows:

$$N_i \to N_{i+1} : B, AI_{N_i} \tag{4}$$

After the similar steps are taken, node N_{i+1} gives the SFC, where *SET* contains the identities of N_{i-1}, N_i and N_{i+1}, as a response:

$$N_{i+1} \rightarrow N_i : SFC_{N_{i+1}}, \text{ where } SFC_{N_{i+1}} = (BI \,||\, SET_{N_{i+1}} \,||\, TS \,||\, Sig_{N_{i+1}}) \quad (5)$$

And then, node N_i sends the SFC to node N_{i-1} through an opportunistic link as follows:

$$N_i \rightarrow N_{i-1} : SFC_{N_{i+1}}, \text{ where } SFC_{N_{i+1}} = (BI \,||\, SET_{N_{i+1}} \,||\, TS \,||\, Sig_{N_{i+1}}) \quad (6)$$

After the verification of SFC passing, node N_{i-1} confirms the forwarding behavior of node N_i. Notice that, similar steps are also taken by each node before the bundle arrives at the destination node.

4.4 Reputation

The goal of reputation is to make sense of gathered information about the behavior of others. The reputation determines how monitored events are translated into reputation ratings of participants in forwarding. It serves as an incentive for honest forwarding behavior; in addition, it provides a basis for the choice of prospective forwarding partners. Reputation is defined here to evaluate the performance of a node in cooperation. The use of second-hand information obtained from others enables nodes to detect misbehaving individuals before having a failed transaction.

In the PRI scheme, DTN nodes update reputation values about others after a deterministic time period τ. In order to obtain an objective and overall rating on nodes' behavior, nodes need to take historical behavior of others, direct transaction experience and indirect transaction experience into consideration. For example, node *i* records the reputation value about node *j* at time τ_n, described as $RV_{ij}(\tau_n)$, which is determined by the followings: the historical reputation value at the former time period, the computational value in terms of the first-hand and second-hand information about recent behavior. Thus, we define the reputation value as

$$RV_{ij}(\tau_n) = e^{-\sigma(\tau_n - \tau_{n-1})} \cdot RV_{ij}(\tau_{n-1}) + FHV_{ij}(\tau_n) + SHV_{ij}(\tau_n) \quad (7)$$

where $FHV_{ij}(\tau_n)$ denotes the computational value based on the first-hand experiences from direct transactions. Let $SHV_{ij}(\tau_n)$ be the value associated with the second-hand information about node *j* obtained from the process of reputation integration. In addition, σ is a discount factor for the rate at which the historical value would decrease. The larger the factor σ is, the quicker the reputation value decreases.

Assume that γ is the factor of punishment, which denotes the degree that nodes treat misbehavior. We define the value of first-hand information as

$$FHV_{ij}(\tau_n) = e^{-\theta(\tau_n - \tau_{n-1})} \cdot \frac{n}{\sum_{k \in NL_i} TF_{ik}(\tau_n)} \cdot \left[(1+\gamma) \cdot CF_{ij}(\tau_n) - \gamma \cdot TF_{ij}(\tau_n) \right] \quad (8)$$

where θ is a discount factor for the rate at which the value of first-hand information would decrease. To achieve the fairness, we introduce the average value of TF_{ij} to emphasize the times that nodes participate in forwarding, so that, nodes who serve as relays more times with high delivery ratio, gain a better reputation value than others. The main idea of the PRI scheme is that nodes that give more contribution to DTNs gain more rewards than their "lazy" counterparts. Notice that, it is guaranteed that the reputation value of an honest node increases

and the value of a selfish node decreases after a transaction. Thus, γ is determined to satisfy the following conditions as

$$\begin{cases}(1+\gamma)\cdot CF_{ih}-\gamma\cdot TF_{ih}>0\\(1+\gamma)\cdot CF_{is}-\gamma\cdot TF_{is}<0\end{cases} \tag{9}$$

where the pair of CF_{ih} and TF_{ih} denote the statistics about an honest node recorded by node i, and the pair of CF_{is} and TF_{is} denote the statistics about a selfish node. Let P_D and P_M denote the delivery probability of SFC and the probability under selfish condition, respectively. The rules are given by the following equations

$$\frac{P_D\cdot(1-P_M)}{1-P_D\cdot(1-P_M)}<\gamma<\frac{P_D}{1-P_D} \tag{10}$$

Furthermore, the computational value of second-hand information is defined as

$$SHV_{ij}(\tau_n)=\frac{1}{N}e^{-\omega(\tau_n-\tau_{n-1})}\frac{\sum_{k\in NL_i,k\neq j}RV_{ik}(\tau_{n-1})CF_{kj}(\tau_n)}{\sum_{k\in NL_i,k\neq j}RV_{ik}(\tau_{n-1})TF_{kj}(\tau_n)} \tag{11}$$

where ω is a discount factor for the rate at which the value of second-hand information would decrease, and N denotes the number of nodes participating in reputation propagation.

4.5 Response

The application of reputation aims at isolating selfish nodes by not using them for routing; at the meantime, and making misbehaving nodes excluded by denying all the requests and not providing service. There are three purposes for isolation in DTNs. First, not to use the misbehaving nodes in routing makes the performance of DTNs improved. Second, depriving egoistic nodes of the opportunity to join the network is an incentive for all the nodes to behave honestly in order to avoid the exclusion. Third, it minimizes the negative impact and impairment of selfishness on the network.

In the PRI scheme, due to the performance of DTNs and the velocity of vehicles, the decision rules are given as

$$\begin{cases}RV_{ij}(\tau_n)\geq\eta_H & \Rightarrow Honest\\ \eta_S<RV_{ij}(\tau_n)<\eta_H & \Rightarrow Normal\\ RV_{ij}(\tau_n)<\eta_S & \Rightarrow Selfish\end{cases} \tag{12}$$

where η_H and η_S are the threshold of honesty and selfishness, respectively. Both of the thresholds are selected according to the condition of DTNs, e.g. the transmission coverage of wireless devices, the velocity of vehicles, and environmental disturbances. The selection of threshold makes the ratio of honest nodes and selfish nodes to total in NL_i set at a predefined level. The threshold value needs to be adjusted according to the performance condition and the secure strategy of the networks. Notice that, the threshold of selfishness cannot be selected at an over high level in order to avoid excluding too much nodes out of networks. If the condition of the network goes worse, e.g. the decrease of network delivery ratio or the increase of environmental disturbance, the thresholds need to adjust to a lower level. There are three

responses according to decision results. First, when nodes are considered honest, the forwarding requests from these nodes are given priority over any others to stimulate nodes to serve for DTNs. Second, when nodes are determined as normal, they are not given any priority. Third, if nodes are considered selfish, they will be added to a blacklist, and finally be excluded from the network. Furthermore, all the requests from misbehaving nodes are denied as the punishment for egoism.

5. Performance Evaluation

In this section, we evaluate the performance of the PRI scheme from several aspects. The performance metrics used in the evaluation are the followings: the delivery ratio, which is the fraction of generated bundles that are successfully delivered to the destination node within TTL; the average delay, which is defined as the average time between when a bundle is generated from the source node and when it is delivered to its destination; and the overhead, which is the ratio of bundles that are relayed in intermediate nodes to bundles that arrive at its destination.

1) System Initialization: Our scheme is implemented in the Opportunistic Networking Environment simulator, which is known as the ONE simulator [24]. In our simulation scenario, there are 250 vehicles adopted with 300 m transmission coverage and uniformly distributed in an area of 4500 m × 3500 m. The speed of vehicles varies from 10 km/h to 50 km/h. The scenario is extracted from a city map, and all the vehicles follow the shortest path map-based movement model, which makes our simulation realistic. Furthermore, the evaluation runs on top of the binary spray and wait routing (BSW) protocol which is a prevalent multiple-copy routing scheme in DTNs [8]. The details of simulation parameters are summarized in **Table 1**.

Table 1. Simulation Parameters

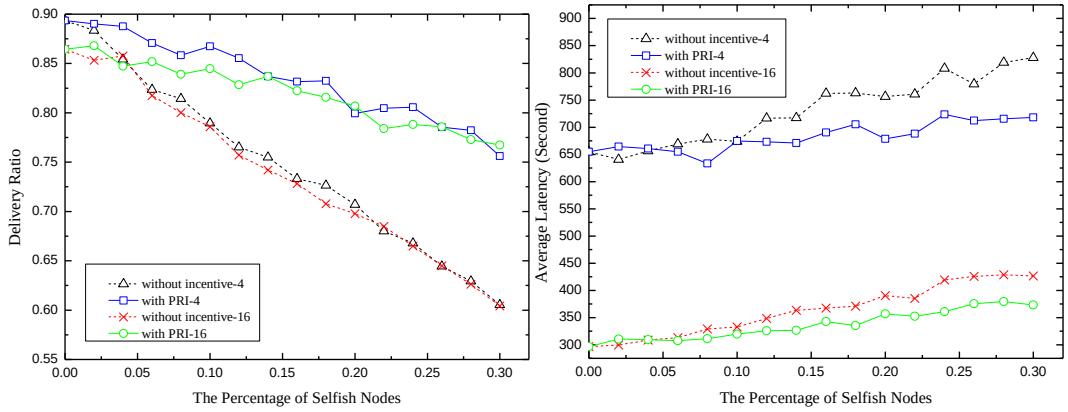
Parameter	Value
Scenario	
Simulation area	4500 m × 3500 m
Duration	12 hours
DTN nodes	
Number	250
Velocity	10 km/h to 50 km/h
Routing Protocol	Spray and wait routing
Transmission Coverage	100 m
Mobility Model	Shortest path map-based model
Buffer size	5 Mb
Bundles	
Generation interval	5 s to15 s, 5 s to 25 s, 5 s to 45 s
TTL	5 hours
Number of forwarding copies	1 to 32

2) *Scenario I – Effectiveness of the PRI scheme:* To evaluate the effectiveness and practicality of the proposed PRI scheme, we examine the system performance at different percentage of selfish nodes, and compare the performance difference between with and

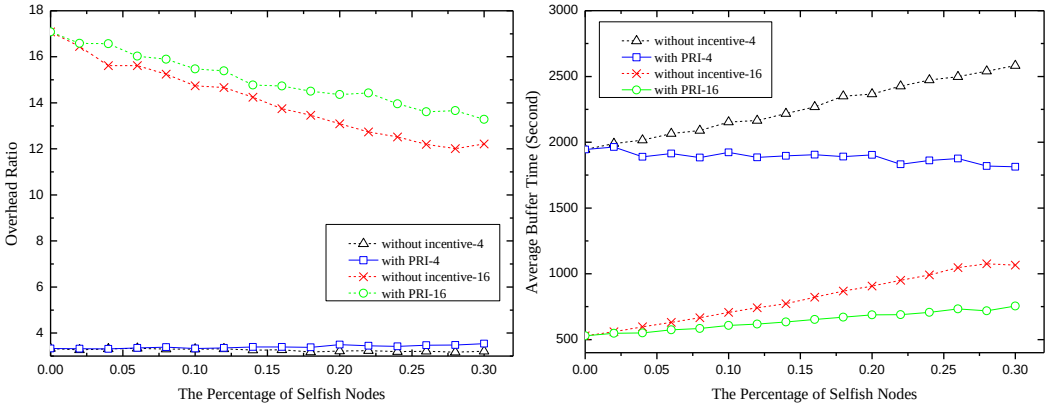
without PRI on the top of BSW routing scheme. We also investigate the impact of forwarding copy number in this scenario. The number of forwarding copies is set to 4 and 16, just as denoted in legends to following figures. In **Fig. 3**, we compare the system performance of the original BSW scheme without incentive to BSW with the PRI scheme.

As shown in **Fig. 3-(a),** when the percentage of selfish nodes increases from 0% to 30%, the delivery rate of original BSW scheme configured with 4 copies will drop from 0.89 to 0.61, which dramatically descends nearly 27 percent. The result suggests that the selfishness impairs the system performance severely. Due to the high consuming of network resources, the delivery rate of original BSW scheme with 16 copies is inferior to that with 4 copies, which are both depicted in dash line. When more nodes start to drop bundles, the overmuch consuming of network resources is mitigated. Thus, after a deterministic threshold of selfish nodes, the difference between the two dash lines becomes smaller. With the PRI scheme in place, the delivery rate descends mildly, and the gap between the no-incentive scheme and PRI scheme is enlarging with the increased percentage of selfishness. Notice that, the overmuch forwarding copies, e.g. the PRI scheme configured with 16 copies, becomes a burden for DTNs, and leads to a lower delivery rate all the time. As a result, the PRI scheme may determine honest partners, and avoid egoistic individuals in routing, so that, our scheme gains an advantage over the no-incentive scheme.

In **Fig. 3-(b)**, it is clear that the more bundle copies are configured, the more quickly nodes spread copies to the network. The average latency for the schemes with 16 copies is significantly lower than that with 4 copies. The selfish nodes drop bundles in routing, which results in the decrease of existing copies in the network. With the PRI scheme, nodes may determine a rational relay, which enables more practical copies to be forwarded rather than discarded. Thus, the latency of the PRI scheme is slightly lower to original BSW scheme without incentive. As shown in **Fig. 3-(c)**, the determination of egoistic nodes makes the dropping of bundles constrained, so that, there are more copies for spread. The overhead of the PRI scheme is slightly larger than that without incentive. In **Fig. 3(d)**, the schemes configured 16 copies makes more copies for spreading, which makes nodes spread copies to the network quickly. Thus, the average buffer time for the schemes with 16 copies decreases significantly. Notice that, the application of PRI makes more practical copies for forwarding rather than discarding; so that, the average buffer time with PRI is slight lower than that without incentive.



(a)Delivery Ratio (b)Average Latency

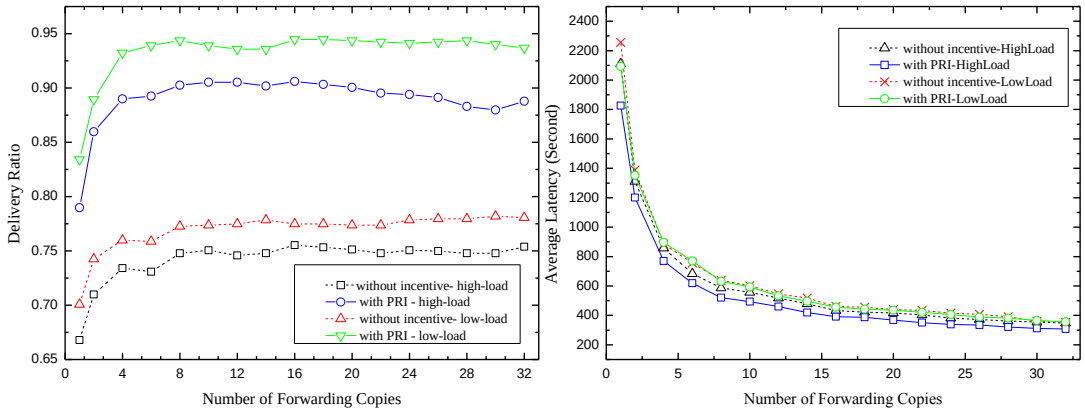


(c)Overhead Ratio (d)Average Buffer Time

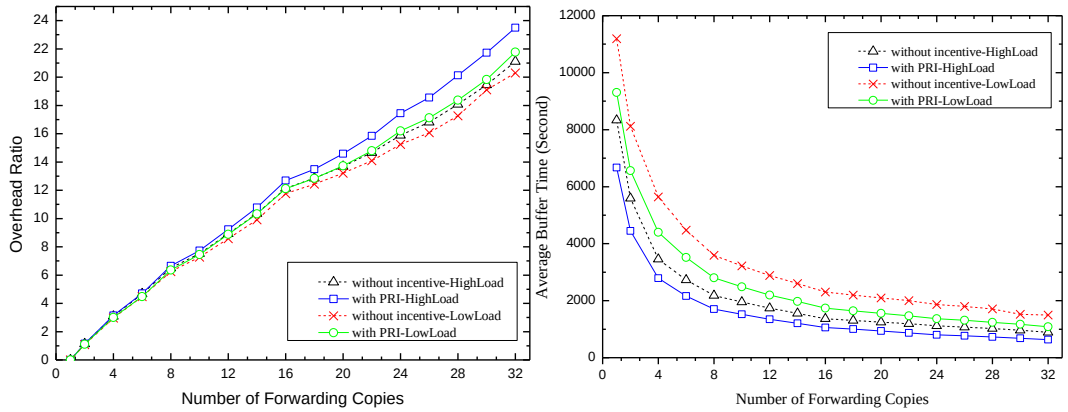
Fig. 3. Effectiveness of the Proposed PRI scheme

3) *Scenario II – Impact of forwarding copy number:* Forwarding copy number is a significant parameter for multiple-copy routing in DTNs. The impact of forwarding copy number on system performance is evaluated in this scenario in the presence of selfish nodes, and an optimal forwarding copy number is also investigated in this section. Two event creation intervals, e.g. 5 s to 25 s and 5 s to 45 s, are adopted and denoted as high-load and low-load in legends to **Fig. 4**, respectively.

Fig. 4-(a) shows the evolution of delivery rate when the forwarding copy number is increased from 1 to 32. The delivery rate increases rapidly at the beginning. After the number of forwarding copies arrives at a deterministic threshold, e.g. 8 in our simulation, the delivery rate nearly keeps stable. Although the number of forwarding copies increases, it does not result in the decrease of system performance due to the low traffic load. It is important to point out that a lower traffic load results in a higher delivery rate. As shown in **Fig. 4-(b) Fig. 4- (d) and (c)**, average latency and average buffer time decrease with the increased copies, on the contrary, overhead ratio increases along the forwarding copies.



(a)Delivery Ratio (b)Average Latency



(c)Overhead Ratio (d)Average Buffer Time

Fig. 4. Impact of forwarding copy number on system performance

In conclusion, the simulation results demonstrate the PRI scheme is effective in stimulating bundle forwarding and minimizing the impairment of selfishness in DTNs.

6. Conclusion

In this paper, we propose a PRI scheme to stimulate bundle forwarding in DTNs. An observation protocol is presented to cope with the detection of misbehavior, and a novel reputation model is proposed to determine selfish individuals. The PRI scheme, which is compatible with multiple-copy routing, is practical to minimize the impairment of selfishness and improve the network performance despite of selfish nodes.

Reputation-related applications are on our schedule of future research. The reputation in DTNs is still an open issue and in need of more attention.

7. References

[1] S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst, K. Scott, and H. Weiss, "Delay-tolerant networking: An approach to interplanetary Internet," *IEEE Communications Magazine*, vol.41, no.6, pp.128-136, Jun.2003. Article (CrossRef Link).

[2] K. Fall, "A delay-tolerant network architecture for challenged Internets," *Computer Communication Review*, vol.33, no.4, pp.27-34, Oct.2003. Article (CrossRef Link).

[3] K. Fall and S. Farrell, "DTN: An architectural retrospective," *IEEE Journal on Selected Areas in Communications*, vol.26, no.5, pp.828-836, Jun.2008. Article (CrossRef Link).

[4] A. McMahon and S. Farrell, "Delay- and Disruption-Tolerant Networking," *IEEE Internet Computing*, vol.13, no.6, pp.82-87, Nov.2009. Article (CrossRef Link).

[5] S. Farrell, V. Cahill, D. Geraghty, I. Humphreys and P. McDonald, "When TCP breaks - Delay- and disruption-tolerant networking," *IEEE Internet Computing*, vol.10, no.4, pp.72-78, Jul.2006. Article (CrossRef Link).

[6] S. Jain, K. Fall and R. Patra, "Routing in a delay tolerant network," *Computer Communication Review*, vol.34, no.4, pp.145-157, Oct.2004. Article (CrossRef Link).

[7] T. Spyropoulos, K. Psounis and C. S. Raghavendra, "Efficient routing in intermittently connected mobile networks: The single-copy case," *IEEE-ACM Transactions on Networking*, vol.16, no.1, pp.63-76, Feb.2008. Article (CrossRef Link).

[8] T. Spyropoulos, K. Psounis and C. S. Raghavendra, "Efficient routing in intermittently connected mobile networks: The multiple-copy case," *IEEE-ACM Transactions on Networking*, vol.16, no.1, pp.77-90, Feb.2008. Article (CrossRef Link).

[9] H. J. Zhu, X. D. Lin, R. X. Lu, Y. F. Fan and X. M. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," *IEEE Transactions on Vehicular Technology*, vol.58, no.8, pp.4628-4639, Oct.2009. Article (CrossRef Link).
[10] R. Lu, X. Lin, H. Zhu and X. Shen, "Pi:A Practical Incentive Protocol for Delay Tolerant Networks," *IEEE Transactions on Wireless Communications*, vol.9, no.4, pp.1483-1493, Apr. 2010. Article (CrossRef Link).
[11] Y. Li, G. L. Su, D. O. Wu, D. P. Jin, L. Su and L. G. Zeng, "The Impact of Node Selfishness on Multicasting in Delay Tolerant Networks," *IEEE Transactions on Vehicular Technology*, vol.60, no.5, pp.2224-2238, Jun.2011. Article (CrossRef Link).
[12] Q. He, D. P. Wu and P. Khosla, "A secure incentive architecture for ad hoc networks," *Wireless Communications & Mobile Computing*, vol.6, no.3, pp.333-346, May.2006. Article (CrossRef Link).
[13] G. F. Marias, P. Georgiadis, D. Flitzanis and K. Mandalas, "Cooperation enforcement schemes for MANETs: a survey," *Wireless Communications & Mobile Computing*, vol.6, no.3, pp.319-332, May.2006. Article (CrossRef Link).
[14] Y. Yoo and D. P. Agrawal, "Why does it pay,to be selfish in a MANET?," *IEEE Wireless Communications*, vol.13, no.6, pp.87-97, Dec.2006. Article (CrossRef Link).
[15] S. Buchegger and J. Y. Le Boudec, "Self-policing mobile ad hoc networks by reputation systems," *IEEE Communications Magazine*, vol.43, no.7, pp.101-107, Jul.2005. Article (CrossRef Link).
[16] H. C. Tsai, N. W. Lo and T. C. Wu, "A Threshold-Adaptive Reputation System on Mobile Ad Hoc Networks," *IEICE Transactions on Information and Systems*, vol.E92D, no.5, pp.777-786, May.2009. Article (CrossRef Link).
[17] R. Sakai, K. Ohgishi and M. Kasahara, "Cryptosystems based on pairing," in *Proc. of Symposium on Cryptography and Information Security*, pp. 26-28, Jan.2000.
[18] X. Y. Li and X. L. Gui, "A Comprehensive and Adaptive Trust Model for Large-Scale P2P Networks," *Journal of Computer Science and Technology*, vol.24, no.5, pp.868-882, Sep.2009. Article (CrossRef Link).
[19] A. Boukerch, L. Xu and K. El-Khatib, "Trust-based security for wireless ad hoc and sensor networks," *Computer Communications*, vol.30, no.18, pp.2413-2427, Sep.2007. Article (CrossRef Link).
[20] M. Karaliopoulos, "Assessing the Vulnerability of DTN data relaying schemes to node selfishness," *IEEE Communications Letters*, vol.13, no.12, pp.923-925, Dec.2009. Article (CrossRef Link).
[21] Q. H. Li, S. C. Zhu, G. H. Cao and *IEEE*, "Routing in socially selfish delay tolerant networks," in *Proc. of 2010 IEEE Infocom*, pp.1-9, Mar.2010. Article (CrossRef Link).
[22] Y. Li, P. Hui, D. P. Jin, L. Su and L. G. Zeng, "Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks," *IEEE Communications Letters*, vol.14, vol.11, pp.1026-1028, Nov.2010. Article (CrossRef Link).
[23] K. Scott and S. Burleigh, "Bundle protocol specification," *IETF RFC 5050*, Nov.2007. Article (CrossRef Link).
[24] *The One Simulator*. Available: http://www.netlab.tkk.fi/tutkimus/dtn/theone/

Xi Zhang was born in Shandong, China, in 1983. He received the B.Sc. degree in Information Engineering from School of Electronic Science and Engineering at National University of Defense Technology (NUDT), China, in 2006. From 2006, Xi Zhang pursued his Master degree in NUDT. He was awarded to pursue Ph.D. degree ahead of schedule in February 2008. His research interests are in the areas of wireless network security, interplanetary networks and trusted computing. He is mainly interested in reputation, routing, and mobility models in DTN.

Xiaofei Wang was born in Hebei, China, in 1981. He received the B.Sc. degree in Communication Command in 2004 and the M.S. in Military Communication in 2006, both from NUDT. He is now a Ph.D. candidate in NUDT. His research interests include spectrum management, protocol design and security, especially in spectrum assignment algorithm.

Anna Liu was born in Hunan, China, in 1983. She received the B.Sc. degree in Communication Engineering from NUDT, in 2005. She was awarded to pursue Ph.D. degree ahead of schedule in February 2008. Her research interests are in the areas of signal processing.

Quan Zhang received the Ph.D. degree in information and communication engineering from NUDT, in 2001. He is an associate professor in the School of Electronic Science and Engineering at NUDT. His research interests include information security, wireless network security, and quantum communications.

Chaojing Tang was born in Jiangsu, China in 1962. He received his M.S. in Electronic Systems in 1986, and the Ph.D. in Information and Communication engineering in 2003, respectively, both from NUDT. He is a professor of Communication Engineering, and he is in the board of directors of the China Communication Institute. His research interests span the fields of information security, space communications networks and quantum communications.