Pi: A Practical Incentive Protocol for Delay Tolerant Networks

Rongxing Lu, *Student Member, IEEE,* Xiaodong Lin, *Member, IEEE,* Haojin Zhu, *Member, IEEE,* Xuemin (Sherman) Shen, *Fellow, IEEE,* and Bruno Preiss

***Abstract*—Delay Tolerant Networks (DTNs) are a class of networks characterized by lack of guaranteed connectivity, typically low frequency of encounters between DTN nodes and long propagation delays within the network. As a result, the message propagation process in DTNs follows a store-carry-and-forward manner, and the in-transit bundle messages can be opportunistically routed towards the destinations through intermittent connections under the hypothesis that each individual DTN node is willing to help with forwarding. Unfortunately, there may exist some selfish nodes, especially in a cooperative network like DTN, and the presence of selfish DTN nodes could cause catastrophic damage to any well designed opportunistic routing scheme and jeopardize the whole network. In this paper, to address the selfishness problem in DTNs, we propose a practical incentive protocol, called Pi, such that when a source node sends a bundle message, it also attaches some incentive on the bundle, which is not only attractive but also fair to all participating DTN nodes. With the fair incentive, the selfish DTN nodes could be stimulated to help with forwarding bundles to achieve better packet delivery performance. In addition, the proposed Pi protocol can also thwart various attacks, which could be launched by selfish DTN nodes, such as free ride attack, layer removing and adding attacks. Extensive simulation results demonstrate the effectiveness of the proposed Pi protocol in terms of high delivery ratio and lower average delay.**

***Index Terms*—Delay tolerant networks, selfish node, fairness, practical incentive.**

I. Introduction

DELAY Tolerant Networks (DTNs), such as space communication and networking in sparsely populated areas [1], vehicular ad hoc networks [2]–[5], and underwater networks [6], have been subject to extensive research efforts in recent years. Different from the traditional networks, the newly emerging DTNs are characterized by the lack of guaranteed connectivity, the typically low frequency of encounters by DTN nodes and long propagation delays within the network [1,7]. For example, the in-transit messages in DTNs, also called bundles, as shown in Fig. 1, could only be forwarded when two DTN nodes $(\mathrm{N}_A, \mathrm{N}_B)$ move within each other's transmission range and contact with each other during a period of time. If no other DTN node is within the transmission range of DTN node N_A, N_A will buffer the current bundles and carry them until other DTN node appears within its transmission range. Therefore, the bundle propagation process in DTNs follows a "store-carry-and-forward" manner [8] and the bundles are *opportunistically* routed toward the destinations by intermittent connections.

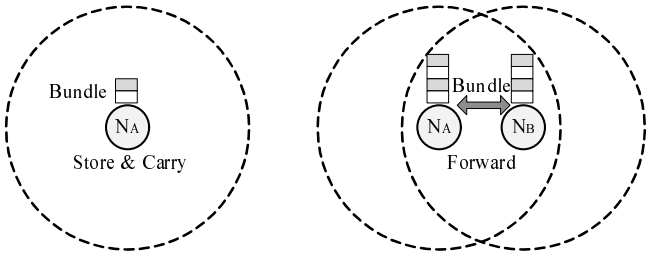


Fig. 1. Bundle store-carry-and-forward in DTNs.

The opportunistic data propagation in DTNs has been well studied so far, and several efficient opportunistic routing protocols have been proposed under the hypothesis that each individual DTN node is willing to forward bundles for others [6,9,10]. However, when DTN nodes are controlled by rational entities, such as human or organization [11,12], some DTN nodes will behave selfishly and may not be willing to help others to forward bundles, so the hypothesis will be violated [13,14]. For example, in order to conserve power, buffer and computing resources, a selfish DTN node may be reluctant in the cooperation that is not directly beneficial to it, which could make a well designed opportunistic routing useless. Therefore, how to efficiently and effectively resolve the selfishness problem in DTNs has become a very challenging issue to achieve better packet delivery performance of DTNs.

To stimulate the possible selfish nodes to forward packets, many reputation-based and credit-based incentive protocols for wireless ad hoc network have been proposed [15]–[22]. However, due to the unique features of DTNs, such as the lack of contemporaneous path and high variation in network conditions, it is hard to detect DTN nodes' selfish behaviors or predetermine a routing path. Therefore, these challenges in DTNs make the existing incentive protocols, which usually rely on a contemporaneous routing, not applicable to DTNs.

In this paper, in order to improve the performance of the

Manuscript received April 21, 2009; revised November 24, 2009; accepted January 27, 2010. The associate editor coordinating the review of this paper and approving it for publication was I. Habib.

R. Lu and X. Shen are with the Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, Canada N2L 3G1 (e-mail: {rxlu, xshen}@bbcr.uwaterloo.ca).

X. Lin is with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada L1H 7K4 (e-mail: xiaodong.lin@uoit.ca).

H. Zhu is with the Department of Computer Science & Engineering, Shanghai Jiao Tong University, Shanghai 200240, China (e-mail: zhuhj@cs.sjtu.edu.cn).

B. Preiss is with the Research In Motion, 295 Phillip Street Waterloo, ON, Canada N2L 3W8 (e-mail: brpreiss@brpreiss.com).

Digital Object Identifier 10.1109/TWC.2010.04.090557

DTNs in terms of high delivery ratio and low average delay, we propose a Practical incentive (Pi) protocol to address the selfishness problem in DTNs. In the proposed protocol, when the source DTN node sends a bundle, it doesn't set a routing path in advance, but only need to attach some incentive on the bundle. Then, the selfish DTN nodes on the road could be stimulated to help with forwarding the bundle to improve the delivery ratio and reduce the average delay of the whole DTNs. Specifically, the contributions of this paper are threefold.

- First, we provide a fair incentive model in which selfish DTN nodes are stimulated to help forward bundles with credit-based incentive as well as reputation-based incentive. In the reward model, to achieve fairness, if and only if the bundles arrive at the destination node, the intermediate forwarding nodes can get credits from the source node. Furthermore, for the failure of bundle forwarding, those intermediate forwarding nodes still can get good reputation values from a trusted authority (TA). Therefore, with this stimulation, the packet delivery performance of DTNs can be improved. To the best of our knowledge, no previously reported stimulation schemes provide the fairness in DTNs.
- Second, in order to guarantee the feasibility of the fair incentive model, we use the layered coin model [14,23] and verifiably encrypted signature techniques [24,25] to provide authentication and integrity protection in the proposed Pi protocol.
- Third, to confirm the effectiveness of the proposed Pi protocol, we also develop a custom simulator built in Java to substantially show that the proposed Pi protocol can achieve the high delivery ratio and low average delay of DTNs when the high incentive is provided.

The remainder of this paper is organized as follows. In Section II, we formalize the network model, the node model, and identify the design goal. Then, we present the Pi protocol in Section III, followed by the security analysis and performance evaluation in Section IV and Section V, respectively. We also review related work in Section VI. Finally, we draw our conclusions in Section VII.

II. Models and Design Goal

In this section, we formalize the network model, the node model, and identify the design goal.

A. Network Model

Delay Tolerant Networks (DTNs) are typically characterized by the unguaranteed connectivity and the low frequency of encounters between a given pair of nodes within the network [1]. In our model, we consider a DTN as a directed graph $G = (V, E)$, where V and E represent the set of DTN nodes and opportunistic contact edges, respectively. In the DTN, a source S can deliver packets to a destination D via the movement of DTN nodes with proper data forwarding algorithm. Currently, contingent upon whether they allow multiple copies of a message relaying within the network, the existing data forwarding algorithms may be categorized into single-copy and multi-copy algorithms. In the single-copy algorithm [10], only one copy is relayed in the network until it arrives at the destination. While in the multi-copy algorithms, such as flooding or spray routing [6], more than one copy are relayed in the networks. Due to large number of message copies in the networks, this kind of approach consumes a high amount of resources which are scarce in DTNs. In this work, in order to clearly illustrate the practical incentive, we just consider a single-copy data forwarding algorithm, i.e., for each bundle B, only one copy is initially spread by the source S, then the only copy is opportunistically relayed from one forwarding node to another until its reaching the destination D.

B. Node Model

In DTNs, the selfish behaviors of DTN nodes are naturally caused by human entities who control them [11,12]. In our model, in order to study the selfish DTN nodes in a non-abstract fashion, we take vehicular ad hoc network as a concrete delay tolerant network — vehicular DTN, where each DTN node is instantiated by vehicle driven by people running in a city environment with some velocity. In the rest of this paper, we will use the terms "node" and "vehicle" interchangeably to refer to the same DTN entity.

In vehicular DTNs, each vehicle is equipped with On Board Unit (OBU) communication device, which allows different vehicles to communicate with each other based on the 802.11p protocol [2]. Note that the 802.11p physical layer offers different bitrates, ranging from 3 to 27 Mbps, from which OBU devices can choose [26]. Therefore, when two vehicles are within the transmission range, e.g., 300 meters, they can exchange bundles [2]. In general, a vehicle is almost resource-unlimited, while the equipped OBU communication device is considered resource-constrained, i.e., buffer and computation power constraints [27]. Therefore, there may exist many selfish DTN nodes in the networks. In order to conserve buffer space, these selfish DTN nodes may be very reluctant in the cooperation that is not directly beneficial to them. As a result, the selfishness would be against the goal of the vehicular DTN to cooperatively deliver a bundle from its source S to the destination D. Therefore, the cooperation probability of a selfish DTN node can be modeled as follows

$$P_c = \alpha P_s + (1-\alpha)P_u = \alpha P_s + 1 - \alpha \qquad (1)$$

where $0 \leq \alpha \leq 1$ is the *selfish factor*, $P_s < 1$ is the cooperation probability under selfish condition, i.e., $P_s = 0.01$, while $P_u = 1$ denotes the unselfish cooperation probability. Clearly, if $\alpha = 0$, a DTN node is unselfish, i.e., it is always willing to help with forwarding with probability $P_c = 1$. On the contrary, if $\alpha = 1$, the DTN node is selfish, the cooperation probability is just $P_c = P_s = 0.01$. Therefore, the smaller the *selfish factor* α, the better the cooperation in DTNs.

C. Design Goal

Our design goal is to develop a practical incentive protocol to stimulate the selfish DTN nodes to improve the cooperation probability P_c in the networks. Specifically, the following two desirable objectives will be achieved.

- *Improving DTN's performance with stimulation:* In order to prevent the overall performance degradation, i.e., low

delivery ratio and high average delay, due to the selfish DTN nodes in DTNs, the credit-based incentive strategy is adopted. Similar to [14], the basic strategy is to provide incentives for intermediate forwarding DTN nodes to faithfully forward bundles. Generally, the intermediate nodes will get paid for bundle forwarding from the other nodes, and will take the same payment mechanism to pay for their bundle forwarding requests, by which the overall performance (i.e., high delivery ratio and low average delay) of the DTNs can be assured.

- *Fairness:* In the practical incentive protocol, the fairness is also considered. Concretely, the intermediate forwarding DTN nodes can receive credits if and only if the destination node receives the bundles, which is fair to the source node. At the same time, even though the bundles don't arrive at the destination, those intermediate DTN nodes who participated in relaying still can get good reputation values for their cooperations. Because a good reputation can build other DTN nodes' confidence in helping forward the bundles (when the reputation value is higher than a reputation threshold R_{th}), the fairness can further stimulate DTN nodes to improve the DTN's packet delivery performance.

1) Incentive Strategy: To achieve the above objectives, the following hybrid incentive strategy is adopted.

- There exists a trusted authority (TA) in the system similar to [20]. Although it does not participate in bundle forwarding in DTNs, TA performs trusted fair credit and reputation clearance for DTN nodes. Therefore, before joining the DTNs, each DTN node should register itself to the TA and obtain its personal credit account (PCA) and personal reputation account (PRA) in the initialization phase. Later, when a DTN node has an available fast connection to the TA, it can report to the TA for credit and/or reputation clearance [20]. For example, in the vehicular DTN, a vehicle can communicate with TA for clearance when it makes contact with some RoadSide Units (RSUs). For each DTN node, PCA stores its credits, while PRA records its dynamic reputation value as follows: Let $\mathrm{R}_{IP(n-1)}$ be the DTN node's reputation value at time T_{n-1}. Then, the new reputation value $\mathrm{R}_{IP(n)}$ at time T_n is formulated as $\mathrm{R}_{IP(n)} = e^{-\lambda T_i} \cdot \mathrm{R}_{IP(n-1)} + C_{T_i}$, where $T_i = T_n - T_{n-1}$, λ is the rate at which the reputation value would decrease, and C_{T_i} denotes the reputation cumulative function, which is the summation of new gained reputation values in the time period T_i.
- It is not mandatory for the intermediate DTN node to forward bundles. All intermediate nodes in the DTN network can self-determine whether or not to participate in bundle forwarding.
- However, once an intermediate DTN node participates in forwarding bundle, it can get the credits from the source node as well as reputation values from the TA.
- If the bundle doesn't arrive at the destination node, the source node won't need to pay credits. However, those intermediate nodes who helped forward can still get good reputation values from the TA. Based on the above reputation calculation, if no new reputation value is gained in T_i, i.e., $C_{T_i} = 0$, then $\mathrm{R}_{IP(n)} = e^{-\lambda T_i} \cdot \mathrm{R}_{IP(n-1)}$ will decrease with the time. The larger the parameter λ, the quicker the reputation value $\mathrm{R}_{IP(n)}$ decreases. Therefore, in order to keep/increase good reputation values, this fair incentive strategy is attractive to each DTN node.

The design of reward calculation is the pivot of a practical incentive protocol, which should guide the selfish DTN nodes to follow the protocol to help with forwarding bundles. In the incentive model, the following reward calculation is exercised: once an intermediate DTN node N_i helped forward a bundle for Dis_i distance, it can get a reward either $Dis_i \cdot \mathrm{C}_{IP} + Dis_i \cdot \mathrm{R}_{IP}$ if the bundle B arrives at the destination D finally or $Dis_i \cdot \mathrm{R}_{IP}$ otherwise, i.e.,

$$\mathrm{Reward}_i = \begin{cases} Dis_i \cdot \mathrm{C}_{IP} + Dis_i \cdot \mathrm{R}_{IP}, & \text{if B arrives at } D; \\ Dis_i \cdot \mathrm{R}_{IP}, & \text{otherwise.} \end{cases} \tag{2}$$

where C_{IP} is a unit incentive credit provided by the source S, R_{IP} is a fixed unit reputation value defined by the TA for optimizing the network. Assume that C_F is the unit resource cost used for forwarding. We define the *gaining factor* of DTN node N_i as

$$\zeta_i = \frac{Dis_i \cdot \mathrm{C}_{IP} - Dis_i \cdot \mathrm{C}_F}{Dis_i \cdot \mathrm{C}_F} = \frac{\mathrm{C}_{IP} - \mathrm{C}_F}{\mathrm{C}_F} \tag{3}$$

and redefine the cooperation probability of N_i with reputation value R_{IP} as

$$P_c = \begin{cases} 1, & \textbf{if } R_{IP} < R_{th}; \\ & \textbf{else if } R_{IP} \geq R_{th} \\ 1, & \alpha_i - \zeta_i \leq 0; \\ (\alpha_i - \zeta_i)P_s + 1 - (\alpha_i - \zeta_i), & \alpha_i - \zeta_i > 0. \\ & \textbf{end if} \end{cases} \tag{4}$$

Then, with the cooperation probability P_c, the DTN node N_i is interested in helping forward the bundle. Note that, when $R_{IP} \geq R_{th}$, different intermediate DTN node may have different initial selfish factor α_i. Therefore, to guarantee the success of stimulation on all intermediate DTN nodes, the source S can choose a large C_{IP} (i.e., large gaining factor ζ_i) in its incentive policy such that each $\alpha_i - \zeta_i$ can be minimal. In addition, since Reward_i is a linear increase function of Dis_i in Eq. (2), the longer the Dis_i, the more the Reward_i. Therefore, the intermediate node is willing to forward the bundle as long as possible.

2) Layered Coin Model: To guarantee the incentive strategy working well, the incentive must be secure. Therefore, in the implementation, we use the layered coin to stimulate the bundle delivery [14,23]. A typical layered coin usually consists of a *base layer* formed by the source node and multiple *endorsed layers* formed by the intermediate nodes. Fig. 2 shows an example of layered coin architecture, where (S, L_s), (D, L_d), (N_i, L_i) are the source node and its location, the destination node and its location, and the i-th intermediate node and the location that it contacts with the $i+1$-th node, respectively. IP is the incentive policy provided by the source node S, TTL, TS, and Sig_i refer to the time-to-live information, the timestamp, and the signature, respectively. IP

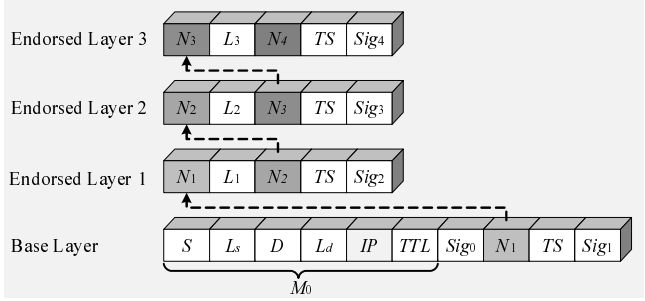


Fig. 2. An example of layered coin architecture.

includes the source's reputation value R_{IP} signed by TA and the incentive policy in this bundle packet forwarding, i.e., the incentive in Eq. (2), and the signatures $Sig_0, Sig_1, \cdots$ can witness the cooperation among DTN nodes while preventing possible malicious nodes from disrupting the system.

Overhead of layered coin. Except the signature fields, we assume the IP field is 64-byte length, and all other fields are 8-byte length, then the overhead of a n-layered coin is around $120 + 32 \cdot n + |Sig| \cdot (n+2)$ bytes, where $|Sig|$ denotes the length of adopted signature.

III. Practical Incentive Protocol

In this section, we propose Pi protocol, which consists of four parts: system initialization, bundle generation, bundle forwarding, and charging and rewarding. Before describing them, we first review the bilinear pairing technique [28], which is a mature cryptographic technique and serves as the basis of the proposed Pi protocol.

A. Bilinear Pairing

Let $\mathbb{G}$, $\mathbb{G}_T$ be two multiplicative cyclic groups of the same prime order q. Suppose $\mathbb{G}$ and $\mathbb{G}_T$ are equipped with a pairing, i.e., a non-degenerated and efficiently computable bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ such that $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab} \in \mathbb{G}_T$ for all $a, b \in \mathbb{Z}_q^*$ and any $g_1, g_2 \in \mathbb{G}$ [28]. In group $\mathbb{G}$, the Computational Diffie-Hellman (CDH) problem is considered to be hard, i.e., given $\langle g, g^a, g^b \rangle$ for $g \in \mathbb{G}$ and unknown $a, b \in \mathbb{Z}_q^*$, there is no algorithm running in expected polynomial time, which can compute g^{ab} with non-negligible probability, while the Decisional Diffie-Hellman (DDH) problem is easy, i.e., given $\langle g, g^a, g^b, g^c \rangle$ for $g \in \mathbb{G}$ and unknown $a, b, c \in \mathbb{Z}_q^*$, it is easy to judge whether $c = ab \bmod q$ by checking $e(g^a, g^b) \stackrel{?}{=} e(g^c, P)$. We refer to [24,25,28] for a more comprehensive description of pairing technique, and complexity assumptions.

Definition 1: A bilinear parameter generator $\mathcal{G}en$ is a probabilistic algorithm that takes a security parameter k as input, and outputs a 5-tuple $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ where q is a k-bit prime number, $\mathbb{G}, \mathbb{G}_T$ are two groups with order q, $g \in \mathbb{G}$ is a generator, and $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is a non-degenerated and efficiently computable bilinear map.

B. The Pi Protocol

1) System Initialization: We assume that all DTN nodes $\mathcal{N} = \{N_1, N_2, \cdots\}$ and TA are using the same suite of system parameters. Given the security parameter k, the bilinear parameters $(q, g, \mathbb{G}, \mathbb{G}_T, e)$ are first generated by running $\mathcal{G}en(k)$. Then, a cryptographic hash function $H : \{0,1\}^* \to \mathbb{Z}_q^*$ and a secure symmetric encryption algorithm $\mathcal{E}()$ are chosen [28]. In the end, the system parameter $\mathsf{params} = (q, g, \mathbb{G}, \mathbb{G}_T, e, H, \mathcal{E})$ are published.

Each DTN node with a unique identity $N_i \in \mathcal{N}$ chooses a random number $x_i \in \mathbb{Z}_q^*$ as its private key and computes the corresponding public key as $y_i = g^{x_i}$. At the same time, each DTN node $N_i \in \mathcal{N}$ also registers its personal credit account (PCA) and personal reputation account (PRA) to the TA. Note that, all public keys in the system should be certified by public key certificates issued by certificate authority (CA). In addition, each DTN node's reputation value R_{IP} during a period is signed by TA and anyone can check it.

2) Bundle Generation: When a source node S with the private-public key pair $(x_s, y_s = g^{x_s})$ at location L_s wants to send a bundle m to the destination node D with the key pair $(x_d, y_d = g^{x_d})$ at location L_d, S will run the following steps.

Step 1. Compute the static shared key $k_{sd} = y_d^{x_s} = g^{x_s x_d}$ between S and D, and encrypt the bundle m into $\mathrm{B} = \mathcal{E}_{k_{sd}}(m)$ to achieve confidentiality.

Step 2. Determine a proper incentive policy (IP) as in Eq. (2), and make a verifiably encrypted signature σ_0 on $M_0 = S||L_s||D||L_d||IP||TTL$ and B as $\sigma_0 = y_d^{(H(M_0||B)+x_s)^{-1}}$.

When an intermediate node N_1 is interested in the IP and willing to forward the bundle to a possible location L_1, it first checks the source's reputation value R_{IP} and verifies the validity of σ_0 with the equation $e(\sigma_0, g^{H(M_0||B)} \cdot y_s) \stackrel{?}{=} e(y_d, g)$. If the source's reputation is acceptable, i.e., $R_{IP} \geq R_{th}$, and the equation holds, N_1 signs $\sigma_1^* = g^{(H(M_0||N_1||L_s||TS)+x_1)^{-1}}$ as an *Interest Acknowledgement* (ACK), and sends σ_1^* and L_1 to the source node S. After receiving σ_1^* and L_1, the source node S runs the next steps.

Step 3. Verify the validity of ACK by checking the equation $e(\sigma_1^*, g^{H(M_0||N_1||L_s||TS)} \cdot y_1) \stackrel{?}{=} e(g, g)$. If it holds, S makes the signature σ_1 on $M_0||N_1||L_s||TS$ as $\sigma_1 = g^{(H(M_0||N_1||L_s||TS)+x_s)^{-1}}$. Otherwise, S neglects the ACK.

Step 4. Set the *base layer* as $\mathrm{BL} = (\mathrm{M}_0||\sigma_0||N_1||TS\ ||\sigma_1)$ and forward the bundle B together with the base layer BL to the intermediate node N_1 as follows

$$S \to N_1 : \mathrm{B}, \mathrm{BL} \tag{5}$$

After verifying $\sigma_1 = g^{(H(M_0||N_1||L_s||TS)+x_s)^{-1}}$ by checking $e(\sigma_1, g^{H(M_0||N_1||L_s||TS)} \cdot y_s) \stackrel{?}{=} e(g, g)$, N_1 begins to forward the bundle.

3) Bundle Forwarding: When approaching to the location L_1, the intermediate node N_1 considers it can't carry the bundle B close to the destination node D any more and forwards the bundle to the next-hop DTN node by running the Algorithm 1. Likewise, each subsequent forwarding node also uses the Algorithm 1 to forward the bundles. Without loss of generality, the bundle B finally arrives at the destination node D by opportunistic bundle forwarding with the routing $S \to N_1 \to N_2 \to \cdots \to N_l \to D$, as shown in Fig. 3. In the following, the detailed bundle forwarding protocol is described.

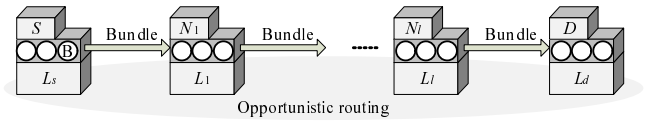


Fig. 3. An opportunistic routing in DTN.

Algorithm 1: Bundle forwarding

Data: When approaching to the location L_1, the node N_1 sets a *holding time to wait next-hop node* (T_h), and tries to forward the bundle B to the next-hop DTN node within T_h

begin
  if *a DTN node N_2 is interested in forwarding within T_h* **then**
    N_1 checks the possible location L_2 that N_2 can carry the bundle B to
    if *location L_2 is closer to the destination D than L_1* **then**
      N_1 forwards the bundle B to N_2
    else
      N_1 continues to wait other DTN node which is interested in forwarding
    end
  else
    when there is no DTN node which is interested in forwarding the bundle at location L_1, N_1 has to drop the bundle packet, since the next-hop route is not immediately available
  end
end

At the location L_i, the intermediate node N_i, $1 \le i \le l-1$, is ready to forward the bundle to the next-hop node N_{i+1}, the following steps are executed.

Step 1. When the intermediate node N_{i+1} is interested in forwarding the bundle B, it first checks the source S's reputation value embedded in IP and the validity of $(\sigma_0, \cdots, \sigma_i)$. If the source's reputation value is acceptable and $(\sigma_0, \cdots, \sigma_i)$ are valid, N_{i+1} signs

$$\sigma_{i+1}^{*} = \sigma_0^{x_{i+1}} \cdot \sigma_1^{x_{i+1} H(N_i||L_i||N_{i+1}||TS)} \tag{6}$$

as an ACK to the N_i.

Step 2. After receiving the ACK σ_{i+1}^{*}, the intermediate node N_i checks

$$e(\sigma_{i+1}^{*}, g) \stackrel{?}{=} e(\sigma_0, y_{i+1}) \cdot e\left(\sigma_1, y_{i+1}^{H(N_i||L_i||N_{i+1}||TS)}\right) \tag{7}$$

If it holds, N_i computes

$$\sigma_{i+1} = \sigma_0^{x_i} \cdot \sigma_1^{x_i H(N_i||L_i||N_{i+1}||TS)} \tag{8}$$

and sets the i-th endorsed layer as $\mathrm{EL}_i = (N_i||L_i\ ||N_{i+1}||TS\ ||\sigma_{i+1})$ and forwards the bundle packet B to the next node N_{i+1} as follows

$$N_i \rightarrow N_{i+1} : \mathrm{B}, \mathrm{BL}, \mathrm{EL}_1, \cdots, \mathrm{EL}_i \tag{9}$$

Step 3. After verifying the validity of σ_{i+1} by checking

$$e(\sigma_{i+1}, g) \stackrel{?}{=} e(\sigma_0, y_i) \cdot e\left(\sigma_1, y_i^{H(N_i||L_i||N_{i+1}||TS)}\right) \tag{10}$$

the intermediate node N_{i+1} forwards the bundle packet B.

At the location L_d, the last intermediate node N_l forwards the bundle $(\mathrm{B}, \mathrm{BL}, \mathrm{EL}_1, \cdots, \mathrm{EL}_{l-1})$ to the destination node D. After the destination node D checks the signatures $(\sigma_0, \cdots, \sigma_l)$ and correctly recovers m from $\mathrm{B} = \mathcal{E}_{k_{sd}}(m)$, it signs a special signature $\sigma_{l+1} = \sigma_0^{x_d^{-1}}$ such that

$$\sigma_{l+1} = y_d^{(x_d \cdot (H(M_0||B)+x_s))^{-1}} = g^{(H(M_0||B)+x_s)^{-1}} \tag{11}$$

and sends σ_{l+1} back to the last intermediate node N_l. After verifying the validity of σ_{l+1} by checking $e(\sigma_{l+1}, g^{H(M_0||B)} \cdot y_s) \stackrel{?}{=} e(g, g)$, N_l can submit $(\sigma_0, \cdots, \sigma_{l+1})$ to the TA for clearance in the future.

4) Charging and Rewarding: When the last intermediate node N_l has an available fast connection to the TA, N_l reports $(\sigma_1, \cdots, \sigma_l)$ to the TA, then the TA performs the fair credit and reputation clearance as the following steps.

Step 1. TA checks the freshness and the validity of $(\sigma_0, \cdots, \sigma_{l+1})$. If they are fresh and valid, TA continues; otherwise terminates the operation.

Step 2. Based on the locations $(L_s, L_1, \cdots, L_l, L_d)$ in the signatures, TA measures the actual relay distance of each intermediate node. Then, according to the incentive policy in IP, TA stores the merited credits and reputation values in each intermediate node's PCA and PRA, and withdraws the corresponding credit values from the source node's PCA, as shown in Algorithm 2.

Algorithm 2: Credit and reputation clearance

Data: The TA obtains valid signatures $(\sigma_1, \cdots, \sigma_l)$ from the last intermediate node N_l.

begin
  get the location information $(L_s, L_1, \cdots, L_l, L_d)$ from these signatures
  measure each intermediate node N_i's actual relay distance Dis_i, where $Dis_1 = |L_1 - L_s|$, $Dis_l = |L_d - L_l|$ and $Dis_i = |L_i - L_{i-1}|$, where $2 \le i \le l$
  for $i = 1$ *to* l **do**
    according to the incentive policy in IP, withdraw $C_i = L_i \times C_{\mathrm{IP}}$ from the source node S's PCA, and store the merited credits C_i in N_i's PCA
    store $R_i = Dis_i \times R_{IP}$ reputation values in N_i's PRA based on the reputation calculation
  end
end

If the bundle packet doesn't arrive at the destination node D, each intermediate node $N_i \in \mathcal{N}$, which helped forwarding, still can get the good reputation value by submitting σ_i and σ_{i+1}^{*}. As shown in Algorithm 3, from the locations L_{i-1} in $\sigma_i = \sigma_0^{x_{i-1}} \cdot \sigma_1^{x_{i-1} H(N_{i-1}||L_{i-1}||N_i||TS)}$ and L_i in $\sigma_{i+1}^{*} = \sigma_0^{x_{i+1}} \cdot \sigma_1^{x_{i+1} \cdot H(N_i||L_i||N_{i+1}||TS)}$, TA can compute the relay distance, and store the merited reputation values to N_i's PRA.

Correctness. The correctness of σ_0, σ_1 and σ_{i+1} are given as follows:

$$\begin{aligned} & e(\sigma_0, g^{H(M_0||B)} \cdot y_s) \\ =& e\left(y_d^{\frac{1}{H(M_0||B)+x_s}}, g^{H(M_0||B)} \cdot y_s\right) = e(y_d, g) \end{aligned} \tag{12}$$

Algorithm 3: Reputation clearance

Data: The TA obtains valid signatures $(\sigma_i, \sigma_{i+1}^*)$ from the intermediate node N_i.

begin
- get the location information LN_{i-1} in σ_i and LN_i in σ_{i+1}^*
- measure the intermediate node N_i's actual relay distance $Dis_i = |L_i - L_{i-1}|$
- store $R_i = Dis_i \times R_{IP}$ reputation values in N_i's PRA based on the reputation calculation

end

$$\begin{aligned} & e(\sigma_1, g^{H(M_0||N_1||L_s||TS)} \cdot y_s) \\ =& e\left(g^{(H(M_0||N_1||L_s||TS)+x_s)^{-1}}, g^{H(M_0||N_1||L_s||TS)} \cdot y_s\right) \\ =& e(g,g) \end{aligned} \tag{13}$$

$$\begin{aligned} e(\sigma_{i+1}, g) &= e\left(\sigma_0^{x_i} \cdot \sigma_1^{x_i H(N_i||L_i||N_{i+1}||TS)}, g\right) \\ &= e\left(\sigma_0^{x_i}, g\right) \cdot e\left(\sigma_1^{x_i H(N_i||L_i||N_{i+1}||TS)}, g\right) \\ &= e(\sigma_0, y_i) \cdot e\left(\sigma_1, y_i^{H(N_i||L_i||N_{i+1}||TS)}\right) \end{aligned} \tag{14}$$

Similarly, the correctness of σ_i^* can also be checked. Then, due to the hybrid incentives, the DTN nodes will be stimulated to faithfully forward the bundles to the destination nodes in a cooperative fashion.

Communication Overhead. Similar to the BLS signature [29], each signature $\sigma_i, i = 0, 1, \cdots$, can be implemented as short as 160 bits (= 20 bytes). Then, the overhead of l-layered coin is $160 + 52 \cdot l$ bytes. When $l = 20$ is assumed, the overhead of layered coin is only $1,200$ bytes (≈ 1.17 Kb). Assume each bundle is 2 Mb or more, then the overhead of layered coin is much smaller than 2 Mb and acceptable for providing security in vehicular DTNs.

Aggregation and Batch Verification. In the proposed Pi protocol, each signature's signing cost is very low, only exponentiation operation is required. However, since the verification requires pairing operation, the computation cost becomes a little higher, but still less than 20 ms [2]. In order to further reduce the communication and computation overheads, the signatures $\sigma_2, \sigma_3, \cdots, \sigma_l$ in the proposed Pi protocol can be aggregated as

$$\sigma = \sigma_2 \cdot \sigma_3 \cdot \cdots \cdot \sigma_l = \sum_{i=2}^{l} \sigma_i \tag{15}$$

Then, the aggregated signature σ can be batch-verified as

$$e(\sigma, P) = e\left(\sigma_0, \prod_{i=1}^{l-1} y_{i+1}\right) \cdot e\left(\sigma_1, \prod_{i=1}^{l-1} y_{i+1}^{H(N_i||L_i||N_{i+1}||TS)}\right) \tag{16}$$

Clearly, the correctness of Eq. (16) directly follows from Eq. (14). Because the signatures σ_0, σ_1 are provably secure in the random oracle model [24,25] and the CDH problem is also assumed hard in $\mathbb{G}$, the signature in Eq. (14) is secure. Then, the security of $\sigma = \sum_{i=1}^{l-1} \sigma_{i+1}$ also follows. More details on security proof of σ can be found in [24,25].

IV. Security Analysis

In this section, we discuss security issues of the proposed Pi protocol, i.e., the fairness issue in stimulation, the free ride attack [21], the layer removing attack [14], and the layer adding attack. Note that, since the proposed Pi protocol only deals with the selfish DTN nodes in DTNs, other attacks launched by malicious DTN nodes are out of the scope of this paper.

• *The proposed Pi protocol provides fair incentive.* In the charging and rewarding phase, if *i*) a bundle is really relayed to the destination node, the source node S will pay credits to those intermediate nodes for forwarding. However, if *ii*) the bundle fails to reach the destination node, the source node S won't pay any credits. Therefore, it is fair to the source node. For the intermediate nodes, although they can't get credits for their forwarding in case *ii*), they still can increase their good reputation values from the TA. When the gaining factor ζ_i is large, those intermediate nodes still feel fair for bundle forwarding. In addition, since the provably secure short signature schemes are employed [24,25], the authentications from the signatures can provide strong witnesses. If an intermediate node didn't participate in forwarding, it can't get any reward. Therefore, from the above analysis, the proposed Pi protocol can provide fair incentive in the DTN network.

• *The proposed Pi protocol is resistent to the free riding attack.* The free riding attack is a notorious selfish attack in DTN, which is conducted by two selfish DTN nodes that attempt to exchange messages without paying their credits [21]. If these two DTN selfish nodes are neighbor, this attack makes no sense, since they can directly exchange messages without the aid of others. When there is at least one normal node residing between them, launching such an attack is possible. Assume that the intermediate node N_i wants to send message m' to N_{i+2} by piggybacking it with the forwarded bundle packet $(\mathrm{B}, \mathrm{BL}, \mathrm{EL}_1, \cdots, \mathrm{EL}_i)$. Since the signature $\sigma_0 = y_d^{(H(M_0||B)+x_s)^{-1}}$ can provide the integrity protection on $(\mathrm{M}_0, \mathrm{B})$, the free riding message m' will not pass the verification equation. Thus, the intermediate node N_{i+1} can detect the free riding message m' and delete it before passing the bundle message to the node N_{i+2}. As a result, the proposed Pi protocol is resistant to the free riding attack in the DTN network.

• *The proposed Pi protocol is resistent to the layer removing attack.* The layer removing attack [14] refers to *i*) a selfish intermediate node removes previous layers on the forwarding path or *ii*) two selfish intermediate nodes remove the layers between them to maximize their credits. However, this attack can be thwarted by the proposed Pi protocol. In the bundle forwarding phase in Section III-B3, each intermediate node N_i holds two valid witnesses σ_i and σ_{i+1}^*, where $\sigma_i = \sigma_0^{x_{i-1}} \cdot \sigma_1^{x_{i-1} H(N_{i-1}||L_{i-1}||N_i||TS)}$ is signed by N_{i-1}, and $\sigma_{i+1}^* = \sigma_0^{x_{i+1}} \cdot \sigma_1^{x_{i+1} H(N_i||L_i||N_{i+1}||TS)}$ is signed by N_{i+1}. Note that, the first intermediate node N_1 gets the witness $\sigma_1 = g^{(H(M_0||N_1||L_s||TS)+x_s)^{-1}}$ from the source node, and the last intermediate node N_l gets the witness σ_{l+1} from the destination node. If a selfish intermediate node N_i launches the first kind of removing layer attack, after removing the previous layers, it can't get $\sigma_i = g^{(H(M_0||N_i||L_s||TS)+x_s)^{-1}}$

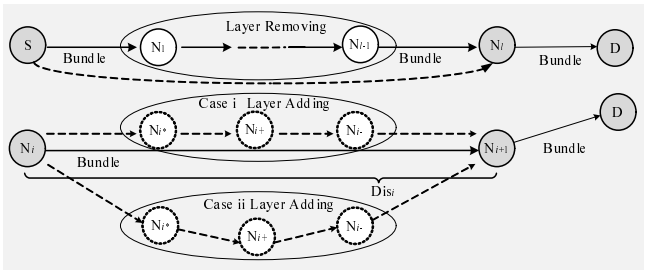


Fig. 4. Layer removing / adding attacks in DTN.

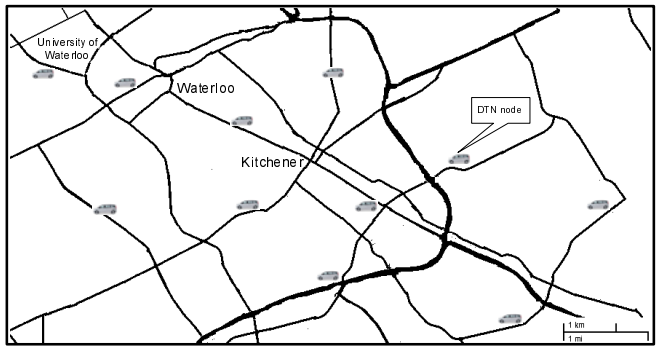


Fig. 5. Vehicular DTN considered for simulation.

from the source node. Therefore, it can be detected. If two selfish intermediate nodes launch the second kind of removing layer attack, those removed intermediated nodes can provide their witnesses to prove their participation. Thus, the selfish nodes will also be detected, and their reputation values will decrease.

A special removing layer attack, as shown in Fig. 4, is the last intermediate node N_l colludes with the source node S to remove all previous layers for enabling the source node to pay less rewarding credits. However, this special attack is still hard to launch. This is because the source node S doesn't know the last intermediate node N_l in advance in the DTN network. Even though S knows N_l and provides $\sigma_l = g^{(H(M_0||N_l||L_s||TS)+x_s)^{-1}}$ to N_l, it can't deny its signing on $\sigma_1 = g^{(H(M_0||N_1||L_s||TS)+x_s)^{-1}}$. Therefore, the selfish behaviors of S and N_l in this special case can also be detected.

• *The proposed Pi protocol is resistent to the layer adding attack.* If a system allows a DTN node with multiple identities, then the layer adding attack could be launched. The layer adding attack refers to a selfish intermediate node with multiple identities adds some additional layers with its different identities on *i*) the same forwarding path or *ii*) detour the forwarding path to maximize its credits, as shown in Fig. 4. However, in the proposed Pi protocol, the $\text{Reward}_i = Dis_i \cdot \text{C}_{IP} + Dis_i \cdot \text{R}_{IP}$ increases linearly with Dis_i. If these additional layers don't enlarge the actual distance Dis_i as in case *i*), the selfish node still can't get more credits. In case *ii*), although Dis_i increases, TA can detect these forwarding nodes N_{i^*}, N_{i+}, N_{i-} are the same node N_i at charging and rewarding phase, since the trusted authority TA knows all DTN node's PCA and PRA. In our system, since one DTN node holds only one unique identifer, and multiple identities are not allowed, this attack is prevented. Note that in DTN network, more than one DTN nodes collude with each other to launch layer adding attack is a malicious attack, how to resist it is still a challenging issue.

V. Performance Evaluation

In this section, we study the performance of the proposed Pi protocol using a custom simulator built in Java. The performance metrics used in the evaluation are i) the *delivery ratio*, which is the fraction of generated messages that are correctly delivered to the final destination within a given time period; 2) the *average delay*, which is defined as the average time between when a message is generated at some source and when it is successfully delivered to its destination. Both *delivery ratio* and *average delay* can be used to examine the ability of the proposed Pi protocol with some incentive strategy to deliver the bundle to the destination within a specified period.

A. Simulation Settings

In the simulations, total n DTN nodes with a transmission radius of 300 meters are first uniformly deployed in an area of 6,000 m $\times$ 15,000 m, as shown in Fig. 5, to simulate a sparse vehicular DTN.

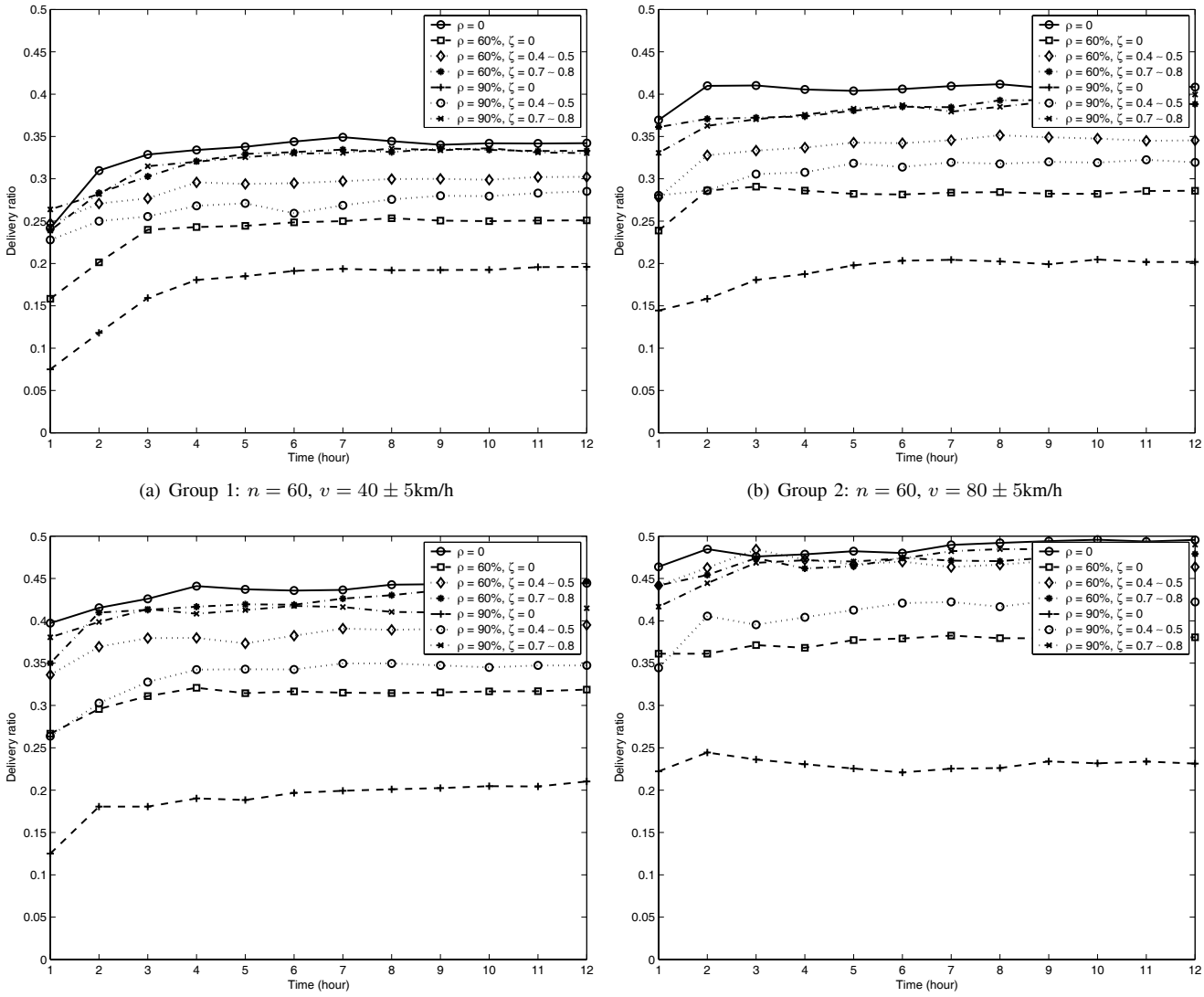
Mobility model. In vehicular DTNs, the performance of bundle forwarding is highly contingent upon the mobility of vehicles. Since vehicles are usually driven along the roads in a city, we assume each DTN node follows the *shortest path map based movement* routing. Specifically, each vehicle first randomly chooses a destination in the area, and gets there using the shortest route with the average velocity v. After reaching the destination, with 2-minute pause time, the vehicle randomly chooses a new destination and repeats the above.

Selfish ratio. Let $\rho = \frac{\text{the number of selfish DTN nodes}}{\text{the total number of DTN nodes}}$ be the selfish ratio (SR) among these DTN nodes, which usually is a variable based on how many DTN nodes that behave selfishly in the network [30]. Once a DTN node is selfish, then according to Eq. (4), it may refuse to forward the bundle packets if the gaining factor ζ is less than its selfish factor α when $R_{IP} \geq R_{th}$. However, with some incentives, i.e., the gaining factor ζ in Eq. (4) is increased, the selfish node may faithfully forward. Note that, in our simulation, we do not consider the case that $R_{IP} < R_{th}$. The reason is that, when $R_{IP} < R_{th}$, the selfish nodes will faithfully forward the bundles, which is equivalent to lowering the selfish ratio ρ in the simulation.

The detailed parameter settings in the simulations are summarized in Table I. We perform the experiments for the specified period varying from 1 hour to 12 hours with increment of 1 hour. For each case, we run the simulation 10 times, and the average *delivery ratio* and *average delay* are reported.

B. Simulation Results

In Fig. 6, we compare the *delivery ratio* of the sampled DTN networks in different incentive policies, i.e., *without incentive* $\zeta = 0$, *with low incentive* $\zeta \in [0.4, 0.5]$ and *with high incentive* $\zeta \in [0.7, 0.8]$, under different selfish ratio $\rho = 0, 60\%, 90\%$. From the figure, we can see the



(a) Group 1: $n = 60$, $v = 40 \pm 5$km/h

(b) Group 2: $n = 60$, $v = 80 \pm 5$km/h

(c) Group 3: $n = 120$, $v = 40 \pm 5$km/h

(d) Group 4: $n = 120$, $v = 80 \pm 5$km/h

Fig. 6. Delivery ratio varies with the specified period from 1 hour to 12 hours.

TABLE I
SIMULATION SETTINGS

Parameter	Setting
Simulation area, duration	$6,000$ m $\times$ $15,000$ m, 12 hours
DTN nodes	
Number	$n = 60, 120$
Velocity	$v = 40 \pm 5$km/h, 80 ± 5km/h
Transmission range, buffer size	300 m, 20 Mb
Mobility model	shortest path map based movement
Holding time to wait next node	$T_h = 3$ minutes
Selfish factor of each DTN node	$\alpha \in [0.2, 0.8]$
Selfish ratio (SR)	$\rho = [0, , 60\%, 90\%]$
Bundle messages	
Generation interval, size, TTL	120 ± 20 s, 2 ± 0.5 Mb, 12 hours
Gaining factor of each bundle	$\zeta = 0, 0.4 \sim 0.5, 0.7 \sim 0.8$

delivery ratio without incentive is very low, especially when the selfish ratio $\rho = 90\%$. The reason is that many selfish DTN nodes move around the network, then there exist many dropping events in which *when a forwarding node seeks a next forwarding node at some location but only meets selfish nodes who are not willing to forward, the bundle message has to be dropped, since the next hop is not immediately available due to the selfishness*. Therefore, Fig. 6 shows that the larger the selfish ratio ρ, the more the dropping events take place and the lower the delivery ratio. On the other hand, when the network is stimulated with some incentive, the delivery ratio will increase. Because different selfish node has different selfish factor, the same incentive can't satisfy all selfish nodes' stimulation conditions in Eq. (4). Therefore, there still exists a small fraction of selfish nodes. Intuitively, when the incentive is higher, the fraction of selfish nodes becomes smaller. By observing the figure, this intuition is corroborated, where the delivery ratio with high incentive is much higher than that with low incentive, and almost approaches to that with no selfish nodes, i.e., $\rho = 0$, in the DTN network. Therefore, we can be sure that, when choosing a proper incentive, the proposed Pi protocol can effectively stimulate the selfish nodes and improve the performance the DTN network in terms of high delivery ratio.

We further compare the delivery ratios in Group 1 and

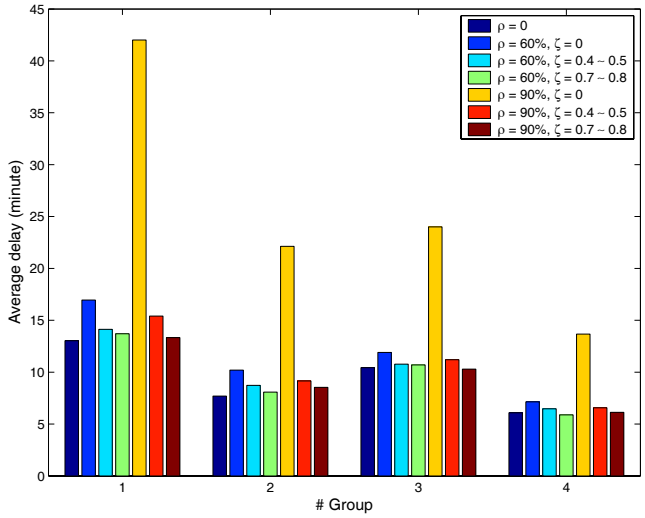


Fig. 7. Average delay within 12 hours with different parameter settings.

Group 2 in terms of different velocity. From the comparisons, we can see the delivery ratios in Group 2 are higher than those in Group 1. The reason is that the faster the velocity v, the more chances a DTN node can contact with other unselfish DTN nodes in time period T_h. As a result, the number of dropping events becomes small, and the delivery ratio increases. We also compare the delivery ratios in Group 1 and Group 3 in terms of different number of DTN nodes, and the comparisons show that the increase of DTN node's number will bring a positive affect on the delivery ratios. When the total number of DTN nodes increases, the density of unselfish DTN nodes subsequently increases. Then, a DTN node has more chances to contact with other unselfish DTN nodes, and the delivery ratio increases. The high delivery ratios in Group 4 with $n = 120$, $v = 80 \pm 5$ km/h further confirm our observations.

Fig. 7 depicts the average delay with 12 hours with different parameter settings. From the figure, we can see when there exist selfish nodes in DTN network, the average delay will decrease. The higher the selfish ratio ρ, the longer the average delay. However, when the network is stimulated with some incentive, the average delay will decrease quickly. Especially, when the *high incentive* is exercised, i.e., the gaining factor ζ is around $0.7 \sim 0.8$, the average delays can approach to that with no selfish nodes, i.e., $\rho = 0$, in the DTN network. In addition, comparing the average delays in Groups 1, 2, 3 and 4, when the number of DTN nodes n and/or the velocity v increase, the average delay can be further reduced.

VI. Related Work

In DTNs, the lack of contemporaneous routing and high variation in network conditions make the selfishness problem very different from the one in traditional wireless ad hoc network, and many existing incentive solutions can not be directly applied to DTNs. Recently, two research works on incentive-aware routing in DTNs have been appeared [13,14], which are closely related to the proposed Pi protocol.

In [13], Shevade et al. first study the impact of selfish behaviors in DTNs. Based on the simulation results, they show that the presence of selfish DTN nodes can greatly degrade total delivered traffic. To mitigate the damage caused by selfish DTN nodes, they use the pair-wise tit-for-tat (TFT) as a simple, robust and practical incentive mechanism for DTNs, and develop an incentive-aware routing protocol that allows selfish DTN nodes to maximize their individual utilities while conforming to TFT constraints. Extensive simulation results are given to show that the TFT mechanism can increase total delivered traffic in the whole DTN network. Although Shevade et al.'s scheme is the first practical incentive-aware routing scheme for DTNs, the security issues lying in the incentive-based DTNs are not addressed in the work. In [14], Zhu et al. propose a secure multilayer credit-based incentive (SMART) scheme for DTNs affiliated with selfish nodes. In SMART, layered coins are used to provide incentives to selfish DTN nodes for bundle forwarding. In addition, compared with Shevade et al.'s scheme, several security issues lying in DTNs, i.e., credit forgery attack, nodular tontine attack, and submission refusal attack, are addressed in the SMART protocol, and the corresponding countermeasures are also briefly discussed.

Different from the SMART protocol, the proposed Pi protocol focuses on the fairness issue in DTNs. Specifically, we propose a hybrid (credit plus reputation) incentive model with verifiably encrypted signature technique to stimulate the selfish DTN nodes to help forward bundles. To achieve fairness, if and only if the bundles arrive at the destination node, the intermediate forwarding nodes can get credits from the source node. Furthermore, for the failure of bundle forwarding, those intermediate DTN nodes still can get good reputation values from the trusted authority. Therefore, DTN nodes will be more confident in participating in bundle forwarding.

VII. Conclusions

In this paper, we have developed a practical incentive (Pi) protocol to stimulate selfish nodes in order to cooperate in forwarding bundle packets in DTNs. By adopting the proper incentive policy, the proposed Pi protocol can not only improve the whole DTN network's performance in terms of *high delivery ratio* and *low average delay* but also achieve the fairness among DTN nodes. Detailed security analyses have shown that the proposed Pi protocol can resist most attacks launched by selfish DTN nodes. In addition, extensive simulations have been conducted to demonstrate the effectiveness of the proposed Pi protocol. For our future work, we will design the fair incentive protocol for multi-copy algorithms. In addition, we will integrate Pi with anonymity to provide each DTN node's privacy protection.

Acknowledgment

This research work is financially supported by grants from the Natural Science and Engineering Research Council (NSERC) of Canada and Research In Motion.

References

[1] K. Fall, "A delay tolerant networking architecture for challenged Internet," in *Proc. 2003 Conf. Applications, Technol., Architectures, Protocols Computer Commun., SIGCOMM '03*, Karlsruhe, Germany, 2003, pp. 27-34.

[2] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. 27th Conf. Computer Commun. (INFOCOM 2008)*, Phoenix, AZ, USA, Apr. 2008, pp. 1229-1237.

[3] J. Chen, X. Cao, Y. Zhang, W. Xu, and Y. Sun, "Measuring the performance of movement-assisted certificate revocation list distribution in VANET," *Wireless Commun. Mobile Comput.*, DOI: 10.1002/wcm.858, to appear.

[4] X. Lin, X. Sun, P.-H. Ho, and X. Shen, "GSIS: a secure and privacy-preserving protocol for vehicular communications," *IEEE Trans. Veh. Technol.*, vol. 56, no. 6, pp. 3442-3456, 2007.

[5] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: a new VANET-based smart parking scheme for large parking lots," in *28th Conf. Comput. Commun. (INFOCOM 2009)*, Rio de Janeiro, Brazil, Apr. 2009.

[6] T. Spyropoulos, K. Psounis, and C. Raghavendra, "Efficient routing in intermittently connected mobile networks: the multiple-copy case," *IEEE/ACM Trans. Networking*, vol. 16, no. 1, pp. 77-90, 2008.

[7] A. Panagakis, A. Vaios, and I. Stavrakakis, "On the effects of cooperation in DTNs," in *Proc. 2nd International Conf. Commun. Syst. Software aMiddleware, COMSWARE 2007*, 2007, pp. 1-6.

[8] M. Grossglause and D. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. Networking*, vol. 10, no. 4, pp. 477-486, 2002.

[9] Delay tolerant networking research group. [Online]. Available: http://www.dtnrg.org, Nov. 2008.

[10] T. Spyropoulos, K. Psounis, and C. Raghavendra, "Efficient routing in intermittently connected mobile networks: the single-copy case," *IEEE/ACM Trans. Networking*, vol. 16, no. 1, pp. 63-76, 2008.

[11] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "MaxProp: routing for vehicle-based disruption-tolerant networks," in *25th Conf. Comput. Commun. (INFOCOM 2006)*, Barcelona, Spain, Apr. 2006.

[12] A. Chaintreau, P. Hui, J. Crowcroft, C. Diot, R. Gass, and J. Scott, "Impact of human mobility on the design of opportunistic forwarding algorithms," in *25th Conf. Comput. Commun. (INFOCOM 2006)*, Barcelona, Spain, Apr. 2006.

[13] S. Upendra, H. H. Song, L. Qiu, and Y. Zhang, "Incentive-aware routing in DTNs," in *Proc. IEEE ICNP 2008*, Orlando, FL, USA, 2008, pp. 238-247.

[14] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: a secure multilayer credit based incentive scheme for delay-tolerant networks," *IEEE Trans. Veh. Technol*, vol. 58, no. 8, pp. 4628-4639, 2009.

[15] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proc. Sixth International Conf. Mobile Comput. Netw. (MobiCom 2000)*, Boston, MA, Aug. 2000, pp. 255-265.

[16] S. Buchegger and J.-Y. L. Boudec, "Performance analysis of the confidant protocol: cooperation of nodes - fairness in dynamic ad-hoc networks," in *Proc. IEEE/ACM Workshop Mobile Ad Hoc Netw. Comput. (MobiHoc 2002)*, Lausanne, Switzerland, June 2002, pp. 226-236.

[17] Y. Liu and Y. R. Yang, "Reputation propagation and agreement in mobile ad-hoc networks," in *Proc. IEEE WCNC 2003*, vol. 3, New Orleans, LA, Mar. 2003, pp. 1510-1515.

[18] L. Buttyan and J.-P. Hubaux, "Enforcing service availability in mobile ad-hoc WANs," in *Proc. IEEE/ACM Workshop Mobile Ad Hoc Netw. Computing (MobiHoc 2000)*, Boston, MA, Aug. 2000, pp. 87-96.

[19] J.-P. Hubaux, T. Gross, J.-Y. L. Boudec, and M. Vetterli, "Toward self-organized mobile ad hoc networks: the terminodes project," *IEEE Commun. Mag.*, vol. 31, no. 1, pp. 118-124, Jan. 2001.

[20] S. Zhong, J. Chen, and Y. Yang, "Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks," in *Proc. 22nd Conf. Computer Commun. (INFOCOM 2003)*, vol. 3, Barcelona, Spain, Mar.-Apr. 2003, pp. 1987-1997.

[21] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A secure incentive protocol for mobile ad hoc networks," *Wireless Netw. (WINET)*, vol. 13, no. 5, pp. 118-124, Oct. 2007.

[22] M. Mahmoud and X. Shen, "Stimulating cooperation in multi-hop wireless networks using cheating detection system," in *29th Conf. Computer Commun. (INFOCOM 2010)*, San Diego, CA, USA, Mar. 2010.

[23] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: secure localized authentication and billing scheme for wireless mesh networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 10, pp. 3858-3868, 2008.

[24] F. Zhang, R. Safavi-Nani, and W. Susilo, "An efficient signature scheme from bilinear pairings and its applications," in *Lecture Notes Computer Science, Proc. PKC 2004*, vol. 2947. Springer-Verlag, 2004, pp. 277-290.

[25] ——, "Efficient verifiably encrypted signature and partially blind signature from bilinear pairings," in *Lecture Notes Computer Science, Proc. INDOCRYPT 2003*, vol. 2904. Springer-Verlag, 2003, pp. 191-204.

[26] P. Shankar, T. Nadeem, J. Rosca, and L. Iftode, "Cars: context-aware rate selection for vehicular networks," in *Proc. ICNP 2008*, 2008, pp. 1-12.

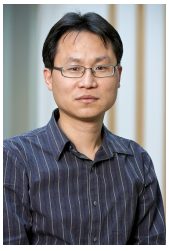
[27] A. Studer, F. Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication," in *Proc. 6^{th} Embedded Security Cars Conf. (ESCAR 08)*, 2008.

[28] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," in *Lecture Notes Computer Sci., Advances Cryptology - CRYPTO 2001*, vol. 2139. Springer-Verlag, 2001, pp. 213-229.

[29] D. Boneh, H. Shacham, and B. Lynn, "Short signatures from the Weil pairing," *J. Cryptology*, vol. 17, no. 4, pp. 297-319, 2004.

[30] P. Kar, S. Sen, and P. Dutta, "Effect of individual opinions on group interactions," *Connection Sci.*, vol. 14, no. 4, pp. 335-344, 2002.

Rongxing Lu (S'09) is currently working toward a Ph.D. degree with the Department of Electrical and Computer Engineering, University of Waterloo, Canada. He is currently a research assistant with the Broadband Communications Research (BBCR) Group, University of Waterloo. His research interests include wireless network security, applied cryptography, and trusted computing.



Xiaodong Lin (S'07-M'09) received the Ph.D. degree in information engineering from Beijing University of Posts and Telecommunications, Beijing, China, in 1998 and the Ph.D. degree (with Outstanding Achievement in Graduate Studies Award) in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2008. He is currently an assistant professor of information security with the Faculty of Business and Information Technology, University of Ontario Institute of Technology, Oshawa, ON, Canada. His research interests include wireless network security, applied cryptography, computer forensics, and software security. Dr. Lin was the recipient of a Natural Sciences and Engineering Research Council of Canada (NSERC) Canada Graduate Scholarships (CGS) Doctoral and the Best Paper Awards of the IEEE International Conference on Computer Communications and Networks (ICCCN 2009) and the IEEE International Conference on Communications (ICC 2007) - Computer and Communications Security Symposium.

Haojin Zhu (M'09) received the B.Sc. degree in computer science from Wuhan University, Wuhan, China, in 2002, the M.Sc. degree in computer science from Shanghai Jiao Tong University, Shanghai, China, in 2005, and the Ph.D. degree in electrical and computer engineering from the University of Waterloo, Waterloo, ON, Canada, in 2009. He is currently an Assistant Professor with Department of Computer Science and Engineering, Shanghai Jiao Tong University. His current research interests include wireless network security, wireless communication and mobile computing. Dr. Zhu was a recipient of the Best Paper Award at the 2007 IEEE International Communications Conference: Computer and Communications Security Symposium and at the 2008 Third International Conference on Communications and Networking in China: Wireless Communication Symposium.

Xuemin (Sherman) Shen (M'97-SM'02-F'09) received the B.Sc.(1982) degree from Dalian Maritime University (China) and the M.Sc. (1987) and Ph.D. degrees (1990) from Rutgers University, New Jersey (USA), all in electrical engineering. He is a Professor and University Research Chair, Department of Electrical and Computer Engineering, University of Waterloo, Canada. Dr. Shen's research focuses on resource management in interconnected wireless/wired networks, UWB wireless communications networks, wireless network security, wireless body area networks and vehicular ad hoc and sensor networks. He is a co-author of three books, and has published more than 400 papers and book chapters in wireless communications and networks, control and filtering. Dr. Shen has served as the Technical Program Committee Chair for IEEE VTC'10, the Tutorial Chair for IEEE ICC'08, the Technical Program Committee Chair for IEEE Globecom'07, the General Co-Chair for Chinacom'07 and QShine'06, the Founding Chair for IEEE Communications Society Technical Committee on P2P Communications and Networking. He has also served as a Founding Area Editor for IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS; Editor-in-Chief for PEER-TO-PEER NETWORKING AND APPLICATION; Associate Editor for IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY; COMPUTER NETWORKS; and ACM/WIRELESS NETWORKS, Guest Editor for IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATION, IEEE WIRELESS COMMUNICATIONS, IEEE COMMUNICATIONS MAGAZINE, and ACM MOBILE NETWORKS AND APPLICATIONS, etc. Dr. Shen received the Excellent Graduate Supervision Award in 2006, and the Outstanding Performance Award in 2004 and 2008 from the University of Waterloo, the Premier's Research Excellence Award (PREA) in 2003 from the Province of Ontario, Canada, and the Distinguished Performance Award in 2002 and 2007 from the Faculty of Engineering, University of Waterloo. Dr. Shen is a registered Professional Engineer of Ontario, Canada, and a Distinguished Lecturer of IEEE Communications Society.

Bruno R. Preiss is Technical Director, BlackBerry Systems Architecture at Research In Motion, Limited in Waterloo, Canada. He received the B.A.Sc degree in Engineering Science in 1982, the M.A.Sc degree in Electrical Engineering in 1984, and the Ph.D. degree in Electrical Engineering in 1987 from the University of Toronto, Canada. Dr. Preiss is a Licensed Professional Engineer in the Province of Ontario, Canada.