An Investigation on the Unwillingness of Nodes to Participate in Mobile Delay Tolerant Network Routing

Jingwei Miao[1], Omar Hasan[1], Sonia Ben Mokhtar[1], Lionel Brunie[1], Kangbin Yim[2]

[1]University of Lyon, CNRS, INSA-Lyon, LIRIS, UMR5205, F-69621, France

{jingwei.miao, omar.hasan, sonia.benmokhtar, lionel.brunie}@insa-lyon.fr

[2]Department of Information Security Engineering, Soonchunhyang University, Asan, Korea

yim@sch.ac.kr

Technical Report
University of Lyon, CNRS, INSA-Lyon, LIRIS, UMR5205, F-69621, France

November 2012

An Investigation on the Unwillingness of Nodes to Participate in Mobile Delay Tolerant Network Routing

Jingwei Miao[a], Omar Hasan[a], Sonia Ben Mokhtar[a], Lionel Brunie[a], Kangbin Yim[b]

[a] *University of Lyon, CNRS, INSA-Lyon, LIRIS, UMR5205, F-69621, France*
[b] *Department of Information Security Engineering, Soonchunhyang University, Asan, Korea*

Abstract

Message routing in mobile delay tolerant networks inherently relies on the cooperation between nodes. In most existing routing protocols, the participation of nodes in the routing process is taken as granted. However, in reality, nodes can be unwilling to participate. We first show in this paper the impact of the unwillingness of nodes to participate in existing routing protocols through a set of experiments. Results show that in the presence of even a small proportion of nodes that do not forward messages, performance is heavily degraded. We then analyze two major reasons of the unwillingness of nodes to participate, i.e., their rational behavior (also called selfishness) and their wariness of disclosing private mobility information.

Our main contribution in this paper is to survey the existing related research works that overcome these two issues. We provide a classification of the existing approaches for protocols that deal with selfish behavior. We then conduct experiments to compare the performance of these strategies for preventing different types of selfish behavior. For protocols that preserve the privacy of users, we classify the existing approaches and provide an analytical comparison of their security guarantees.

Keywords: mobile, delay tolerant, selfish, privacy, reputation, game theory, ecash

1. Introduction

The heavy utilization of mobile devices with short-range networking interfaces, such as smart phones and personal digital assistants, has led to the emergence of a new types of *opportunistic* networks called Mobile Delay Tolerant Networks (MDTNs). MDTNs are constructed by the (intermittent) con-

Email addresses: jingwei.miao@insa-lyon.fr (Jingwei Miao), omar.hasan@insa-lyon.fr (Omar Hasan), sonia.ben-mokhtar@liris.cnrs.fr (Sonia Ben Mokhtar), lionel.brunie@insa-lyon.fr (Lionel Brunie), yim@sch.ac.kr (Kangbin Yim)

nection of co-located mobile devices. Contrary to Mobile Ad-hoc NETworks (MANETs) [48], in MDTNs, a complete routing path between two nodes that wish to communicate cannot be guaranteed [12]. The applications developed for these networks are necessarily, geo-localized with no critical time constrains (e.g., advert dissemination, recommendation of points of interest, asynchronous communication). A number of networking scenarios have been categorized as MDTNs, such as Vehicular Ad-hoc NETworks (VANETs) [26], Pocket Switched Networks (PSNs) [15], etc.

Due to the frequent and long-term network partitions that characterize MDTNs, message delivery is considered as one of the major challenges in these networks. In order to deal with the lack of end-to-end connectivity between nodes (i.e., mobile devices), message routing is often performed in a "store-carry-and-forward" manner [12], in which a message is stored by intermediary nodes and forwarded to nodes closer and closer to the destination until it is eventually delivered or it expires. Therefore, message routing in MDTNs inherently relies on the cooperation between nodes.

In the literature, most of the existing routing protocols in MDTNs explicitly or implicitly assume that the nodes in a network are willing to relay messages for others. Unfortunately, reality is different. Indeed, first, as it has been previously demonstrated in the literature, collaborative systems are subject to rational behavior (also called selfish behavior). MDTNs are particularly suited for exacerbating such behavior due to the resource constrains of mobile devices (e.g., battery, memory and bandwidth) [46]. A second reason that leads to the unwillingness to participate in MDTN routing is the users' wariness of disclosing private information (e.g., identity, location, message content). The main contribution of this paper is to survey the existing related research works that overcome these two issues.

The remainder of this paper is organized as follows. We first analyze the impact of the unwillingness of nodes to participate through a set of experiments in Section 2. We then classify selfish behavior, and summarize the impact of selfish behavior on routing performance in Section 3. We then investigate different strategies for preventing selfish behavior in Section 4. This is followed by an experiment to compare the performance of different strategies in Section 5. In Section 6, we discuss and classify the privacy concerns that users face in MDTNs. We then investigate different privacy-preserving protocols in Section 7. The privacy-preserving protocols are then compared in Section 8. In discuss related works in Section 9. Finally, we conclude this paper in Section 10.

2. Impact of the Unwillingness to Participate in MDTN routing

In order to evaluate the impact on performance of the unwillingness of a proportion of nodes in the network to participate in the routing of messages, we performed the following experiment. We ran one of the most efficient routing protocols in DTNs, i.e., the Binary Spray and Wait [52] algorithm. In this algorithm, the source node holds a given number of copies of the message it wants to send. Each time it encounters another node, it hands over half of

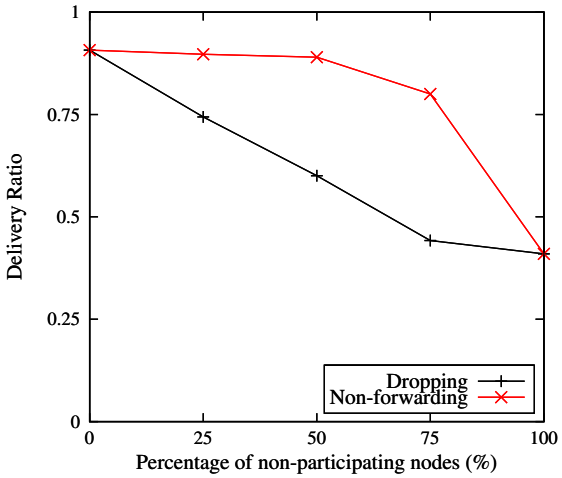


Figure 1: Impact of non participating nodes in MDTN routing

the remaining copies it holds, until it does not have enough copies to send. Similarly, if a node has more than one copy of a given message, it hands over half of the message copies to the encountered nodes, and so forth until the message reaches the destination. In this experiment we injected a proportion of nodes that are not willing to participate in the routing process and analyze their impact on the delivery ratio. We considered two types of behaviors for non-participating nodes, i.e., nodes that explicitly refuse to participate (referred to as "Non-forwarding" in the experiment results) and nodes that accept to receive messages but eventually drop them instead of forwarding them (referred to as "Dropping" in the experiment results). The experimental settings we used for this experiment are the same as those described in Section 5. Results, depicted in Figure 1 show that in presence of non-participating nodes, the delivery ratio is heavily impacted, especially if nodes do not explicitly declare themselves as non-participating (i.e., the Dropping curve in the graph). Note that in presence of 100% of non participating nodes, the delivery ratio drops to 40%, which represents the situations where the source node directly delivers the message to the destination node.

Our aim in this paper is to understand the reasons why a node may be unwilling to participate in an MDTN routing protocol and survey the related research contributions to deal with this issue. We identify two major reasons, i.e., nodes' selfishness (presented in sections 3, 4 and 5) and their wariness of disclosing private information (presented in sections 7 and 8).

3. Selfishness

In this section, we first develop a unified view of the classification of selfish behavior. We then discuss the methodologies utilized for investigating the in-

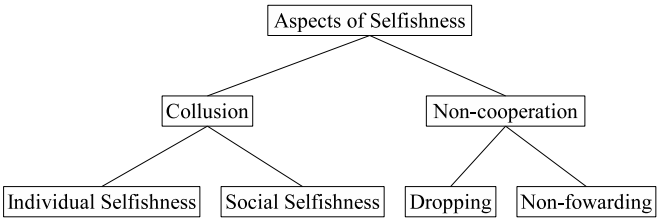


Figure 2: Classification of selfish behavior in DTNs

fluence of selfish behavior on the performance of routing protocols. Finally, we highlight the performance degradation caused by selfish behavior.

3.1. Classification of Selfish Behavior

Recent years have seen considerable research works addressing the issue of selfish behavior in DTNs [32, 63, 37]. Traditionally, most works consider selfish behavior as the unwillingness of a single node to relay the messages of all other nodes in order to conserve its limited resources. Nevertheless, people in real life (i.e., the carriers of mobile devices) generally do not act alone, but tend to belong to communities [17]. In an alternative type of selfishness, a node that belongs to a community is willing to relay messages for the nodes within the same community but refuses to relay messages for the nodes outside its community. For this reason, selfish behavior is classified into two categories: *individual selfishness* and *social selfishness* [29].

Moreover, in the literature investigating the impact of selfish behavior on routing performance [44, 21], the authors generally consider the following two types of selfish actions: *non-forwarding of messages* and *dropping of messages*. Non-forwarding of messages means that a node refuses to relay messages for the nodes towards which it is selfish. Dropping of messages means that a node agrees to relay messages for the nodes towards which it is selfish, but it drops the messages after receiving them.

From the above description, we can see that there are two classifications of selfish behavior from different aspects. In this paper, we develop a unified view of the classification of selfish behavior. We term the two aspects of the classification as *collusion* and *non-cooperation*. From the viewpoint of collusion, selfish behavior can be classified into two categories: individual selfishness and social selfishness. From the viewpoint of non-cooperation, selfish behavior can be classified into two categories as well: non-forwarding of messages and dropping of messages. The reader is requested to refer to Figure 2 for an illustration of the unified view of the classification. To the best of our knowledge, this is the first work to develop this unified view of the classification of selfish behavior.

3.2. The Methodologies of Investigating the Impact of Selfish Behavior

Since Panagakis et al. [44] first presented their study on the performance degradation caused by selfish behavior in DTNs, researchers have shown signif-

icant interest in this field. To evaluate the impact of selfish behavior on the performance of existing routing protocols, some works utilize theoretical analysis models, such as Continuous Time Markov Chains (CTMC), whereas others utilize simulations.

To the best of our knowledge, CTMC is first exploited by Karaliopoulos et al. [21] to demonstrate the impact of selfish behavior in DTNs. Later studies [30, 31, 33, 32] explored CTMC to show the influence of selfish nodes on routing performance in the contexts of social selfishness, constrained energy and multicast routing. CTMC provides a theoretical approach of analyzing selfish behavior in DTNs.

However, the routing process modeled by CTMC is built on the assumption that the inter-contact times between nodes follow exponential distribution, which rarely holds in real-life situations [15, 7]. Moreover, CTMC can only be utilized to model the routing process of simple routing protocols, such as Epidemic [55], Spray and Wait [52]. These routing protocols are generally considered to be inefficient in reality [39]. In addition, the studies based on CTMC do not evaluate the performance of routing protocols in terms of delivery ratio, which is traditionally considered to be the most important performance metric in DTNs. Therefore, authors in [24, 33, 9] utilize simulation methods to investigate the influence of selfish behavior on the routing performance.

3.3. The Impact of Selfish Behavior

Since Panagakis et al. [44] first presented their study on the performance degradation caused by selfish behavior in DTNs, researchers have shown significant interest in this field. The existing research works [32, 33, 24, 9] based on theoretical analysis and experimental simulations reveal the following two characteristics of the impact of selfish behavior on the routing performance. Firstly, the routing performance (i.e., delivery ratio, delivery cost and delivery latency) is seriously degraded, if a major portion of the nodes in the network is selfish. For instance, the delivery ratio in the presence of selfish nodes can be as low as 20% compared to what can be achieved under full cooperation [50]. Secondly, the impact on the routing performance is related to the non-cooperative action of selfish behavior (i.e., non-forwarding of messages and dropping of messages). Specifically, the behavior of non-forwarding of messages reduces the delivery cost, while the behavior of dropping of messages increases the delivery cost. However, both of them decrease the delivery ratio, and prolong the delivery latency, even if messages are eventually delivered.

4. Strategies for Preventing Selfish Behavior

In order to reduce the impact of selfish behavior on routing performance, a number of studies focus on stimulating selfish nodes to be cooperative. The existing incentive strategies are traditionally classified into three categories [4, 8]: barter-based [4, 3, 59], credit-based [8, 43, 63, 37, 62] and reputation-based [1, 56, 11, 57, 37, 28]. In the following subsections, we will introduce the representative strategies in each category and summarize their common problems.

4.1. Barter-based Strategies

The simplest strategies are barter-based or pair-wise Tit-For-Tat (TFT) strategies [4, 3, 59]. The mechanism is that two encountering nodes exchange the same amount of messages. In [4, 3], the authors divide the messages into two categories: primary messages and secondary messages. For a given node, the messages in which it is interested (e.g., the messages destined for it) are primary messages. Other messages are secondary messages. When two nodes encounter each other, they first exchange the description about the messages stored in their buffers. Based on the analysis of the description, each node determines an initial list of the desired messages from the other node, and sorts the messages in order of preference (i.e, the priority of primary messages is higher than that of secondary messages). For the sake of simplicity, let us assume that the size of messages is the same. Finally, each node refines the list by keeping the top K messages in its initial list, where K is the minimum size of two initial lists.

From the above depiction of message selection under this strategy, we can see that it is entirely up to the nodes to determine the desired messages. Thus, a node may adopt selfish behavior towards the secondary messages, in order to conserve its limited resources. However, exchanging the secondary messages is also beneficial, since they can be used to exchange the primary messages in the future. In other words, each message has a potential value, which is employed to prevent selfish behavior. Moreover, the authors in [4, 59] consider the message selection process as a two-person game, and utilize the Nash Equilibrium [41] to increase the message delivery ratio.

After the message selection process, two encountered nodes exchange the messages in the lists one by one (i.e., if a node has sent a message to the other node, it would not send another message, until it receives a message from the latter). In such a manner, even if the connection is disrupted during the exchange process, the maximum difference of the number of the exchanged messages between two nodes is one. Consequently, the fairness of message exchange can be ensured by exchanging approximately the same amount of messages between two encountering nodes.

However, the requirement of exchanging the same amount of messages is a two-edged sword. It degrades routing performance dramatically in the case that one of the two encountering nodes has fewer messages. For instance, let's consider that there are two encountering nodes, called node A and B. Node A contains a message whose destination is node B. However, there is no message in the buffer of node B at the moment. In such a case, the message cannot be delivered to node A. Furthermore, if node A is the source of the message, the performance in terms of delivery ratio is even worse than that achieved by utilizing Direct Delivery [54] which is generally considered to achieve the lower bound for delivery ratio in DTNs.

4.2. Credit-based Strategies

Credit-based strategies are proposed to avoid the disadvantages of barter-based strategies. This kind of strategy stimulates nodes to be cooperative by

utilizing the concept of virtual credit, which is utilized to pay for message forwarding. The mechanism is that if a node cooperates to forward a message for others, it receives a certain amount of credit as a reward that it can later utilize for its own benefit.

Based on which node is charged with the message forwarding, the credit-based strategies can be further sub-divided into two models [5]: 1) *Message Purse Model* and 2) *Message Trade Model*. In message purse model [63, 37, 8], the source node of a message pays credits to the intermediate nodes which participate in delivering the message to the destination. In the message trade model [43], messages are considered as valuable goods. The receiver pays credits to the sender of a message in each hop-by-hop transmission until the message reaches the destination, which finally pays for the message forwarding. Since the source nodes do not pay for the message forwarding, the message trade model is inherently vulnerable to the source nodes flooding the network. For this reason, most of the credit-based works utilize the message purse model.

In the strategies that belong to the message purse model, the common assumption is the existence of a Virtual Bank (VB), or Credit Clearance Service (CCS). The VB covers the space that the mobile nodes can reach, and can be connected by any nodes in the network. The responsibility of VB is to charge the source node of a message and reward the intermediate nodes which participate in delivering the message to the destination.

The strategies [37, 8, 63] belonging to the message purse model are suitable for different routing protocols. In [37], the proposed strategy is designed for the single-copy routing protocols (e.g., Direct Delivery and First Contact [18]) under which only one message copy exists in the routing process. Although single-copy routing protocols consume the least resources, the routing performances in terms of delivery ratio and delivery latency are generally too low to be applicable in reality [53]. Therefore, more routing protocols (e.g., Epidemic and Spray and Wait) are multi-copy based. In [8, 63], the proposed strategies are targeted to multi-copy based routing protocols in DTNs. In [63], Zhu et al. include the solution of cheating actions (i.e., credit forgery attack, nodular tontine attack and submission refusal attack) which are adopted by the selfish nodes to maximize their benefits. Detailed information about these cheating actions is given in [63].

From the above discussion, we can see that the process of charging and rewarding is invoked at the side of the VB, when (1) a message is successfully delivered to the destination and (2) there are intermediary nodes participating in the routing process. Let's consider a scenario where a major portion of the nodes is selfish and each node has enough credits to request the message forwarding service from an encountering node in a contact. In such a case, a message can only be delivered when the source node directly encounter the destination node. In addition, before the message reaches the destination node, the credits of the source node are reusable to request the message forwarding service. Therefore, a selfish node cannot be aware of the necessity of cooperation with other nodes. Due to the above two reasons, the credit-based strategies cannot efficiently stimulate the selfish nodes to be cooperative, when a major

portion of the nodes is selfish.

4.3. Reputation-based Strategies

We first explain the concept of reputation before discussing the reputation-based strategies: "Reputation of an agent is a perception regarding its behavior norms, which is held by other agents, based on experiences and observation of its past actions" [35]. In the scope of investigating selfish behavior, the reputation value of a node indicates other nodes' perception about the cooperation of the node. For instance, if the reputation value of a node is low, it means that the node is considered to be selfish by other nodes. If the reputation value of a node is high, it means that the node is considered to be cooperative by other nodes.

The mechanism of this kind of strategy is that a message generated by a given node is forwarded only if the node has forwarded messages originating from others. Therefore, the observation about the behavior of other nodes plays a significant role in this kind of strategy. Based on the feasibility of observation by other nodes, we further divide the existing strategies into two models: 1) *detection-based model* and 2) *non-detection model*.

In the detection-based model, each node monitors the behavior of the intermediary nodes. In [57, 28, 1], the authors utilize different methods to detect selfish behavior in DTNs. In [57], each intermediate node receives a receipt after forwarding a message to another node. The receipt is a proof about the cooperation of the intermediate node. The cooperation of an encountering node is assessed by Beta distribution, which is parameterized by the number of cooperative and selfish actions taken by the node. However, the strategy cannot prevent collusion cheating, which means that some nodes together cheat other nodes in order to increase their reputation. Detailed information about this cheating action is given in [63]. Similar to [57], the behavior of intermediary nodes is proved by the return of a receipt. The difference is that a receiver floods the receipt instead of sending the receipt to the sender. In [1], selfish behavior is detected in a different way. In [1], the sender of a message (including the source and intermediate nodes) keeps the records of the encountered nodes and the forwarding records which contain the identifier of the message, the destination of the message and the forwarding time. When two nodes encounter each other, they check the forwarding records and received messages since last encountered time, in order to detect the cooperative nodes and selfish nodes.

However, due to the unique features of DTNs (e.g., the lack of an end-to-end continuous path and high variation in network conditions), the detection of selfish behavior is considered to be difficult by some authors. The alternatives belonging to reputation-based strategies are not based on the detection of selfish nodes [11, 37]. In [11], Dini et al. decrease the reputation of all nodes periodically, and only increase the reputation of the intermediate nodes who participate in the successful message delivery. Similar to [11], the proposed strategy in [37] decreases the reputation of all nodes periodically. The differences between them are twofold. First, it involves the credit-based incentive strategy to reward the intermediate nodes which participate in the successful message delivery. Second, no matter whether the message delivery succeeds or

not, all cooperative nodes can get good reputation values by sending the proofs of collaboration to a Trusted Authority (TA), which is responsible for credit and reputation clearance.

From the above description, we can see that the reputation-based strategies can work well even if a major portion of the nodes takes the selfish behavior of dropping messages. However, this kind of strategy mistakenly considers the collaboration of intermediate nodes as selfish behavior, if the reason causing the failure of message delivery is the message expiration other than selfish behavior of intermediate nodes. It is unfair to the cooperative nodes. Furthermore, it results in the decrement of delivery probability of the message generated by this kind of cooperative node, since they are mistakenly considered as selfish nodes by other nodes. Moreover, since the reputation-based strategies only check whether an intermediate node forwards the message to other nodes or not, it cannot tackle the selfish behavior of non-forwarding messages.

5. Analysis of Strategies for Preventing Selfish Behavior

In this section, we first introduce representative strategies in the categories discussed above. We then present the experiment settings. The routing algorithm and performance metrics are subsequently depicted. Finally, we compare the performance of the different strategies for preventing selfish behavior.

5.1. Compared Strategies for Preventing Selfish Behavior

In the experiment, we compare the performance of preventing selfish behavior of the following strategies against a basic routing protocol (i.e., Binary Spray and Wait), called *Non-strategy*, which does not cope with the selfish behavior of nodes. The detailed settings of the selected strategies are depicted in Table 1.

Barter: In [3], when two nodes encounter each other, they exchange the same amount of messages.

MobiCent: Due to the selected routing algorithm, which will be presented later, is multi-copy based, we choose the MobiCent as the representative strategy in the category of credit-based. In [8], the charging and rewarding processes are performed at the side of Virtual Bank (VB), when a message is firstly delivered to the destination. A constant credit is charged from the account of the source node in VB. The charged credit is equally divided, and distributed to the intermediate nodes in the message delivery path as a reward.

IRONMAN: Compared to barter-based and credit-based strategies, IRONMAN [1] includes the detection of selfish behavior. Therefore, it is selected as the representative strategy in reputation-based strategy. As depicted in Section 4 Part C, when two nodes encounter each other, they firstly check the forwarding records and the received messages, in order to detect the selfish nodes. The two encountering nodes then update the opinion about others' behavior with each other.

5.2. Simulation Setup

In order to evaluate the performance of different strategies for preventing selfish behavior, we utilize a widely utilized mobility model in MDTNs called Random WayPoint (RWP) [20] in the Opportunistic Network Environment (ONE) simulator [23] to conduct the experiment. In RWP, each node is initially specified a random destination within a given area, and it then moves towards the destination with a given speed. When it reaches the destination, it stays there for a certain period of time (i.e., a pause time). When the pause time expires, it randomly chooses a new destination, and repeats the above process. In order to avoid the impact of the setting of pause time on the routing performance, there is no pause time in the simulations as [25]. In addition, we specify a warm-up period (0.5 hour) as in [6] to uniformly distribute the initial position of nodes.

In this experiment, there are 50 nodes in each simulation. To simulate the social relationships, we equally divide the nodes into two groups. Two nodes that belong to the same group are considered to have a social relationship; otherwise, the nodes are considered to not have a social relationship. During the simulation, a message with a random source and destination is generated at every 5 seconds. Since the message generation process lasts for 12 hours, there are 8640 messages generated in each simulation. The detailed settings of the simulation are listed in Table 2

Table 1: Simulation Parameters for Strategies

Strategy Name	**Parameter Name**	**Value**
MobiCent	Initial Credit for Each Node	1
	Payment for Each Message	1
IRONMAN	Initial Trust for Each Node	0.5
	Trust Increment	0.5
	Trust Decrement	0.5
	Threshold	0.49

Table 2: Simulation Parameters

Parameter Name	**Value**
Simulation Area	500 m x 500 m
Simulation Length	13.5 hours
Mobility Model	Random WayPoint (RWP)
Number of Mobile Nodes	50
Number of Groups	2
Number of Nodes in Each Group	25
Transmission Range	10 m
Node Speed	1 m/s
Warm-up Period	0.5 hour
Duration of Message Generation	12 hours
Message Generation Rate	1 message per 5 seconds
Time-To-Live (TTL)	1 hour

5.3. Routing Algorithm

Based on the above settings, we conducted our experiment with an efficient multi-copy routing algorithm in MDTNs, called Binary Spray and Wait [52]. The Binary Spray and Wait routing algorithm provides a platform for the selected strategies. The routing process is elaborated below.

Binary Spray and Wait: In [52], each message is associated with an attribute L, which indicates the maximum copies of the message that a message carrier can make. For each message, there are two phases: *spray* phase and *wait* phase. In the spray phase (i.e., $L > 1$), a message carrier hands over half of its message copies to an encountering node without the message. In the wait phase, the message can only be forwarded to the destination node. In the experiment, L is set to 5.

5.4. Performance Metrics

We observe the following metrics to assess the impact of selfish behavior in DTNs:

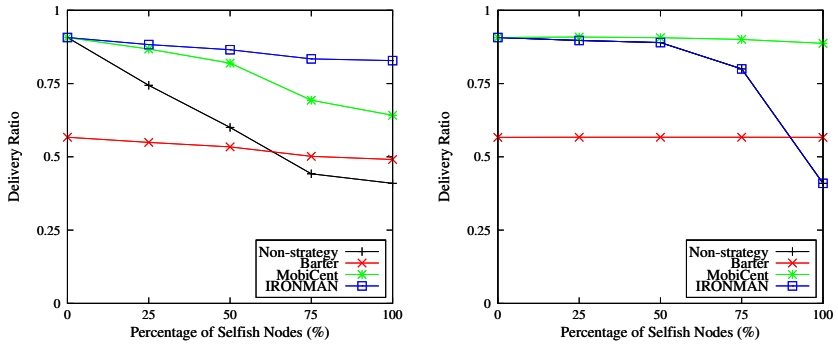
Delivery Ratio: The proportion of messages that have been delivered out of the total unique messages created.

Delivery Cost: The total number of messages (including duplicates) transmitted in the simulation. To normalize this, we divide it by the total number of unique messages created.

5.5. Simulation Results

In Figure 3(a), the performance of the strategies for preventing dropping messages is shown. When there is no selfish node, the performance of Non-strategy, MobiCent and IRONMAN is the same, since the cooperative nodes always cooperate with other nodes. However, the performance of barter is lower than those of other strategies, due to the requirement of exchanging the same amount of messages. As the percentage of selfish nodes increases, the performance of all strategies is degraded. The performance of IRONMAN and MobiCent is always better than that of Non-strategy. The performance of barter exceeds that of Non-strategy, when the percentage of selfish nodes is about 60%. The performance of IRONMAN is much better than those of other strategies even if all nodes are selfish, since it can detect the dropping of messages of a selfish node.

Figure 3(b) illustrates the performance of the strategies for preventing non-forwarding messages. The performance of all strategies decreases, as the percentage of selfish nodes increases. The performance of MobiCent is always better than other strategies. MobiCent can stimulate selfish nodes to be cooperative, as the number of the messages generated by selfish nodes increases. IRONMAN always achieves the same performance as Non-strategy, since it cannot detect the selfish behavior of non-forwarding of messages. The performance of Barter only exceeds than that of Non-strategy, when the percentage of selfish nodes is about 82%.



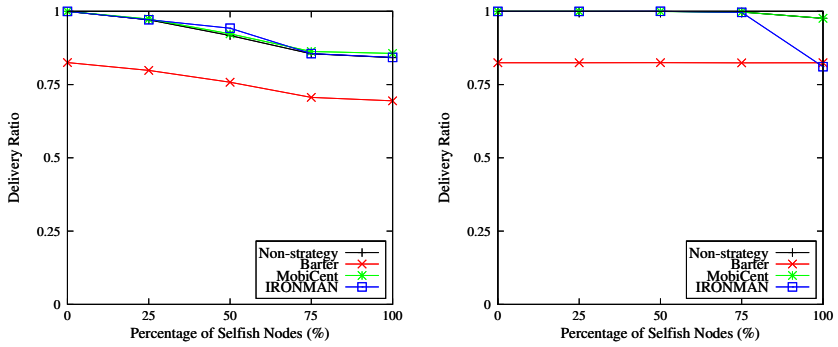
(a) Dropping (b) Non-forwarding

Figure 3: The routing performance in terms of delivery ratio under individual selfishness. The selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b) respectively.

In Figure 4, the performance of delivery ratio of the four strategies under the social selfishness is investigated. From the figures, we can see that all the strategies cannot work well under social selfishness. Specially, the performance of barter is even worse than that of Non-strategy, due to the requirement of exchanging the same amount of messages. For the selfish behavior of non-forwarding of messages, the performance of MobiCent is much better than those of other strategies, when the selfish nodes are 75% percentage.

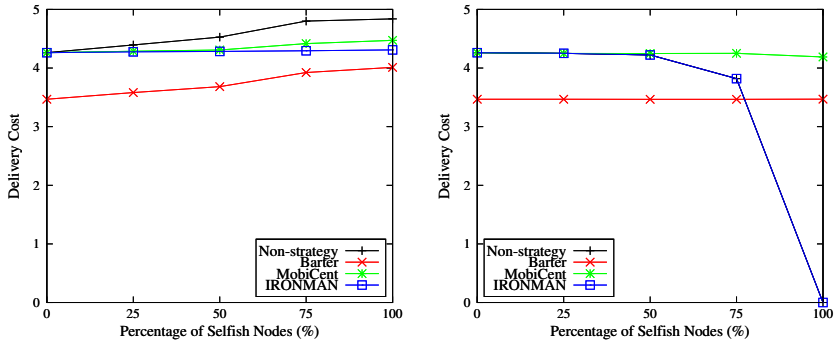
The performance of delivery cost is demonstrated in Figure 5 and 6. In Figure 5(a), due to the characteristics of dropping of messages, the delivery cost of all strategies increases, as the percentage of selfish nodes increases. Meanwhile, the delivery cost of all incentive strategies is lower than that of Non-strategy, since they stimulate selfish nodes to be cooperative. However, in Figure 6(b), the delivery cost of Non-strategy, IRONMAN, and MobiCent decreases, as the percentage of selfish nodes increases, since they cannot deal with social selfishness. In Figure 5(b) and Figure 6(b), due to the characteristics of non-forwarding of messages, the delivery cost of all strategies decreases, as the percentage of selfish nodes increases. The delivery cost of MobiCent is higher than that of Non-strategy when the percentage of selfish nodes is high, due to the stimulation of selfish nodes to be cooperative.

From the above analysis of the simulation results, we can see that, for individual selfishness, the reputation-based strategies cannot prevent the selfish behavior of non-forwarding of messages. For social selfishness, there is no strategy that can efficiently prevent the selfish behavior of dropping of messages, and credit-based strategies can prevent the selfish behavior of non-forwarding of messages. The performance of barter-based strategies is always worse than that of credit-based and reputation-based strategies.



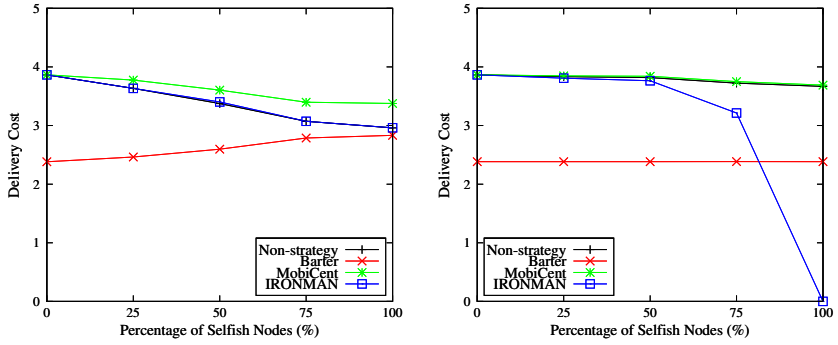
(a) Dropping (b) Non-forwarding

Figure 4: The routing performance in terms of delivery ratio under social selfishness. The selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b) respectively.



(a) Dropping (b) Non-forwarding

Figure 5: The routing performance in terms of delivery cost under individual selfishness. The selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b) respectively.



(a) Dropping (b) Non-forwarding

Figure 6: The routing performance of delivery cost under social selfishness. The selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b) respectively.

5.6. Comparison of Strategies

According to the above simulation results, we utilize three types of circles to indicate the performance of the selected strategies compared with that of Non-strategy: (1) ● indicates that the performance of a given strategy is always better than that of Non-strategy; (2) ◑ indicates that the performance of a given strategy is better than that of Non-strategy, only when the percentage of selfish nodes is high; and (3) ○ indicates that the performance of a given strategy always cannot exceed that of Non-strategy. The performance of the representative strategy in each category is listed in Table 3.

Table 3: Performance comparison of the selected strategies

Strategy	**Individual selfishness**		**Social selfishness**	
	Dropping	**Non-forwarding**	**Dropping**	**Non-forwarding**
Barter	◑	◑	○	○
MobiCent	●	●	○	◑
IRONMAN	●	○	○	○

6. Privacy

In this section, we will classify privacy preserving protocols for MDTN routing according to their specific privacy objectives.

6.1. Classification of Privacy Objectives

As mentioned in the introduction, messages in MDTNs are relayed by intermediary nodes. Apart from selfishness, mobile device carriers can be unwilling to participate in the routing process due to the concern of privacy. Recent

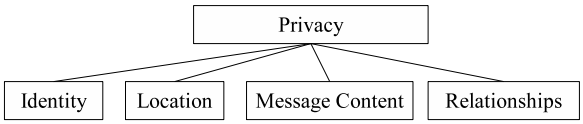


Figure 7: Classification of privacy from the aspect of privacy objective

years have seen considerable research works addressing the issues of privacy in MDTNs. The protocols in the literature are mainly concerned with preserving the privacy of one or more of the following sensitive user aspects: (1) identity, (2) location, (3) message content, and (4) relationships. We can thus classify the existing privacy preserving protocols according to their privacy objectives. Please refer to Figure 7 for an illustration of this classification. We discuss each of these privacy objectives in the following section along with some solutions proposed in the literature for achieving these objectives.

7. Strategies for Preserving Privacy

7.1. Identity Privacy

In the category of identity privacy, the identity of nodes participating in message delivery is considered as private information.

Kate et al. [22] presented an anonymous communication architecture for DTNs using Identity-Based Cryptography (IBC) [49]. This is one of the first anonymous communication solutions specifically for DTNs. Kate et al. use a construct called DTN gateways, which are entities assumed to be trusted and to be aware of user identities. In the routing process, a DTN gateway replaces the identity of a source node with a pseudonym unlinkable to the identity. The advantage of the protocol is that there is not much overhead for routing. However, the protocol relies on the assumption that trusted DTN gateways are present, which is a strong assumption for MDTNs.

Le et al. [27] proposed a privacy preserving infrastructure called Privacy-Enhanced Opportunistic Networks (PEON) based on onion routing [47]. In PEON, nodes are clustered into groups. Nodes in the same group share public keys. Before sending a message, a source node determines the routing path, which contains a certain number of node groups. The message is then encrypted by the public keys of the destination node and the determined groups in an inverse order. Thus, each relay node can only be aware of the next hop (i.e., a node group) in the routing path and remains unaware of the identity of the source node. Compared to classic onion routing, the routing performance of PEON in terms of delivery ratio and delivery latency is enhanced due to the utilization of multicasting inside a group. However, node groups are randomly clustered, which may result in the inefficient dissemination of messages inside a group. In addition, the assumption of a Public Key Infrastructure (PKI) rarely holds in MDTNs [22].

Lu et al. [36] presented a social-based privacy-preserving packet forwarding protocol (named SPRING) for Vehicular DTNs. In SPRING, Road Side Units (RSUs) are assumed to be trusted and uncompromisable. Similar to [61], RSUs are strategically deployed at some highly-social intersections to temporarily buffer the messages as relays. Due to the utilization of RSUs, an adversary cannot find out the identity of the source and the destination nodes. However, the private information of nodes is disclosed, if any RSU in the network is compromised. Additionally, all RSUs in SPRING are managed by a single management authority, which results in inflexibility.

7.2. Location Privacy

In the category of location privacy in MDTNs, the discovery of the user location by the adversary is considered as the main privacy threat. In an untrusted network, the mobile device owners do not want others to know their positions for personal security reasons [38].

In [38], Lu et al. proposed the Anti-Localization Anonymous Routing (ALAR) protocol for MDTNs. In ALAR, each message is divided into k segments and each segment is then encrypted and sent to n different neighbors. Therefore, an adversary may receive several copies of a segment at different times from different relay nodes. Even if the adversary collects these segments, they cannot localize the source node with high probability. The disadvantage is that the routing performance is influenced by the setting of the parameters k and n. Specifically, the routing performance in terms of delivery ratio and delivery latency is degraded as the two parameters increase.

Zakhary and Radenkovic [60] presented a location privacy protocol that is based on the utilization of social information of nodes. In this protocol, each node maintains a social profile, which includes n profile attributes. The social relationship between nodes are inferred by the matching of profile attributes. For each message, the forwarding is guided by the obfuscated attributes in the first k hops. After that, the message can be routed by any routing protocols. Therefore, an adversary cannot distinguish the location of the source node from the other k relay nodes. However, nodes that have strong social relationships are generally considered to be frequently co-located. Thus, the adversary can still detect the approximate location of the source node. Moreover, the routing performance is degraded, due to the extra k forwarding hops.

7.3. Message Content Privacy

Since messages are relayed by intermediary nodes in MDTNs, the content of messages can be unintentionally disclosed to these nodes in the routing process. Thus, in the category of message content privacy, the content of messages is considered as private information.

Jansen and Beverly [19] proposed a Threshold Pivot Scheme (TPS) based on the technique of secret sharing [42]. In TPS, a message, considered as the secret, is divided into multiple shares by the technique of secret sharing. The shares are delivered to the destination node via multiple independent paths.

The content of a message is thus protected from individual intermediary nodes. At the destination node, the message can be reconstructed by the knowledge of any τ shares. The disadvantage of this protocol is that if an adversary successes n monitoring a sybil attack, it can create multiple pseudonymous nodes and then intercept sufficient number of shares.

Shi and Luo [51] proposed an anonymous communication mechanism called ARDEN based on onion routing [47], multicast dissemination and Attribute-Based Encryption (ABE) [13]. In ARDEN, before sending a message, the source node determines a path of disjoint groups, one of which includes the destination node. The message is then encrypted by the keys of the destination node and the grouping keys. Compared with the traditional onion routing, the advantage of ARDEN is that it encrypts messages with the keys of groups rather than the keys of individual intermediate nodes. The performance in terms of delivery ratio and delivery latency can be improved, since all nodes in the same group can participate in message forwarding. On the other hand, the arbitrary group partitioning manner may result in performance degradation in terms of delivery ratio and delivery latency.

7.4. Relationships Privacy

As mentioned in the introduction, the mobility pattern of nodes plays an important role in the routing process. A number of proposed routing protocols exploit the encounter probability [10, 34] and social relationship of nodes [10, 16] to guide the message forwarding decision. However, such information is considered as personal and private [45] thus users may hesitate in participating in such protocols.

Hasan et al. [14] proposed a Privacy Preserving Prediction-based Routing (3PR) protocol for MDTNs. A prediction-based routing protocol for MDTNs works by forwarding a message from one intermediate node to another if the latter has higher probability of encountering the destination node. However, this process compromises the privacy of the nodes by revealing their mobility patterns. 3PR forwards messages by comparing information about communities of nodes instead of individual nodes. Specifically, it compares the maximum probability that a node in the community of a potential intermediate node will encounter the destination node. Simulations on a community-based mobility model demonstrate that the protocol has comparable performance to existing prediction-based protocols.

Parris and Henderson [45] presented the Privacy-enhanced Social-network Routing protocol. This protocol takes advantage of obfuscated social information rather than accurate social information to guide the message forwarding. The original social information of a node is obfuscated by the following two approaches: (1) modifying the friend list, i.e., adding or removing some items into or from the friend list, or (2) using a Bloom filter [2] to hash the friend list. The advantage of the protocol is that the presence of a public key infrastructure is not necessary. However, message routing may be guided erroneously due to the utilization of obfuscated social information. Moreover, in the case of modifying the friend list of a source node, an adversary can approximately determine the

source node's friends by collecting the messages from the source node. In the second approach, the probability of false positives increases as the Bloom filter becomes more full, due to the characteristics of Bloom filter.

8. Analysis of Strategies for Preserving Privacy

8.1. Criteria for Comparison

The criteria for comparison of the above privacy preserving protocols are described in the following sections.

8.1.1. Adversarial models

We identify two adversarial models, which characterize the behavior of dishonest users. The models are: Semi-Honest, and Malicious. A privacy preserving protocol is considered secure under one of these models if it can show correctness and meet its privacy requirements under the given model.

Semi-Honest. In the semi-honest model, the users do not deviate from the specified protocol. In other words, they always execute the protocol according to the specifications. The adversary abstains from wiretapping and tampering of the communication channels. However, within these constraints, the adversary passively attempts to learn the inputs of honest users by using intermediate information received during the protocol and any other information that it can gain through other legitimate means.

Malicious. Malicious users are not bound to conform to the protocol. Users under a malicious model may deviate from the protocol as and when they deem necessary. They actively attempt to achieve their objectives. They may participate in extra-protocol activities, devise sophisticated strategies, and exhibit arbitrary behavior. A malicious adversary has the following objectives: 1) learn the inputs of honest users, and 2) disrupt the protocol for honest users. The reasons for disrupting the protocol may range from gaining illegitimate advantage over honest users to completely denying the service of the protocol to honest users.

8.1.2. Collusion

A dishonest user may act alone or multiple dishonest users may act in agreement to achieve their ulterior motives. When multiple dishonest users work together, it is referred to as collusion. Privacy preserving protocols either consider that collusion can take place between users or consider that collusion does not take place.

8.1.3. Security Building Blocks

The privacy preserving protocols for MDTN routing are generally built using security building blocks such as Identity-Based Cryptography (IBC) [49], Public Key Infrastructure (PKI), Onion routing [47], Secret Sharing, Attribute-Based Encryption (ABE) [13], and Bloom filter [2].

8.2. Comparison of Strategies for Preserving Privacy

A comparison of the above privacy preserving strategies is given in Table 4 according to the established criteria.

Table 4: Comparison of Strategies for Preserving Privacy

Protocol	Privacy Objective	Collusion	Attack Model	Building Blocks
Kate et al. [22]	Identity	Group	Semi-Host	IBC
Le et al. [27]	Identity Content	Group	Semi-Host	Onion Routing PKI
Lu et al. [36]	Identity	Group	Semi-Host	
Lu et al. [38]	Location	Individual	Semi-Host	Secret Sharing
Zakhary and Radenkovic [60]	Location	Individual	Semi-Host	
Jansen and Beverly [19]	Content	Individual	Semi-Host	Secret Sharing
Shi and Luo [51]	Identity Content	Group	Semi-Host	Onion Routing ABE
Hasan et al. [14]	Relationships	Group	Semi-Host	Secret Sharing
Parris and Henderson [45]	Relationships	Individual	Semi-Host	Bloom Filter

9. Related Work

Recent years have seen considerable research works proposed to address the issues of selfish behavior and privacy in DTNs. However, only a few of them include the investigation or performance comparison of the proposed strategies for preventing selfish behavior [58, 40, 1, 64] and leakage of privacy.

Woungang et al. [58] survey the credit-based strategies. The authors compare the existing strategies in the evaluation part, according to the aspects of security issues, charging and rewarding models, and the suitable routing protocols.

Madarresi et al. [40] investigate the reputation-based strategies in terms of incentive patterns, security issues, and suitable routing algorithms. It should be emphasized that none of them focus on the performance comparison of the proposed strategies.

Bigwood et al. [1] compare the performance of some proposed strategies in the simulation part. However, the authors do not analyze the mechanism of the compared strategies, since the purpose in [1] is a proposal of reputation-based strategy. Moreover, the compared strategies are not selected from each category. Therefore, it cannot reflect the performance comparison between different strategy categories.

Zhu et al. [64] review some incentive strategies in each category (i.e., barter-based, credit-based, and reputation-based). The reviewed strategies are compared from the aspects of selfishness types (i.e., individual selfishness and social selfishness).

Our work on selfishness differs from the aforementioned works in two ways. First, we analyzed the proposed strategies, and classified them into three categories. Further, we pointed out the common problem of the existing strategies in each category. Second, we focus on the performance comparison between different categories by comparing the performance of the selected representative strategies from each category.

10. Conclusion

In this paper, we investigated the existing research works that address the unwillingness of nodes to participate in MDTN routing. We identified the factors of selfishness and privacy as the two primary reasons why nodes are unwilling to participate. For selfishness, we first developed a classification of the aspects of selfish behavior. We then classified the existing strategies for preventing selfish behavior into three categories: barter-based, credit-based and reputation-based. We subsequently analyzed the mechanisms of the proposed strategies and pointed out the problems in each category. We then conducted an experiment to investigate the performance of the representative strategies for preventing different types of selfish behavior. For privacy, we classified the existing privacy preserving protocols for MDTNs according to their specific privacy objectives: identity, location, message content, and relationships. We reviewed the various strategies proposed in the literature for preserving the privacy of nodes under each of these categories. We also presented an analytical comparison of the privacy preserving protocols.

References

[1] Bigwood, G., Henderson, T., 2011. Ironman: Using social networks to add incentives and reputation to opportunistic networks.

[2] Bloom, B. H., Jul. 1970. Space/time trade-offs in hash coding with allowable errors. Commun. ACM 13 (7), 422–426.

[3] Buttyan, L., Dora, L., Felegyhazi, M., Vajda, I., 2007. Barter-based cooperation in delay-tolerant personal wireless networks. In: World of Wireless, Mobile and Multimedia Networks, 2007. WoWMoM 2007. IEEE International Symposium on a. pp. 1–6.

[4] Buttyan, L., Dora, L., Felegyhazi, M., Vajda, I., 2010. Barter trade improves message delivery in opportunistic networks. Ad Hoc Networks 8 (1), 1–14.

[5] Buttyán, L., Hubaux, J.-P., 2000. Enforcing service availability in mobile ad-hoc wans. In: Proceedings of the 1st ACM international symposium on Mobile ad hoc networking & computing. MobiHoc '00. IEEE Press, Piscataway, NJ, USA, pp. 87–96.

[6] Camp, T., Boleng, J., Davies, V., 2002. A survey of mobility models for ad hoc network research. Wireless communications and mobile computing 2 (5), 483–502.

[7] Chaintreau, A., Hui, P., Crowcroft, J., Diot, C., Gass, R., Scott, J., 2007. Impact of human mobility on opportunistic forwarding algorithms. IEEE Trans. Mobile Comput. 6 (6), 606–620.

[8] Chen, B. B., Chan, M. C., 2010. Mobicent: a credit-based incentive system for disruption tolerant network. In: INFOCOM, 2010 Proceedings IEEE. pp. 1–9.

[9] Chuah, M., Yang, P., 2009. Impact of selective dropping attacks on network coding performance in dtns and a potential mitigation scheme. In: Computer Communications and Networks, 2009. ICCCN 2009. Proceedings of 18th Internatonal Conference on. pp. 1–6.

[10] Dang, H., Wu, H., 2010. Clustering and cluster-based routing protocol for delay-tolerant mobile networks. IEEE Trans. Wireless Commun. 9 (6), 1874–1881.

[11] Dini, G., Lo Duca, A., 2010. A reputation-based approach to tolerate misbehaving carriers in delay tolerant networks. In: Computers and Communications (ISCC), 2010 IEEE Symposium on. pp. 772–777.

[12] Fall, K., 2003. A delay-tolerant network architecture for challenged internets. In: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. SIGCOMM '03. ACM, New York, NY, USA, pp. 27–34.

[13] Goyal, V., Pandey, O., Sahai, A., Waters, B., 2006. Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM conference on Computer and communications security. CCS '06. ACM, New York, NY, USA, pp. 89–98.

[14] Hasan, O., Miao, J., Ben Mokhtar, S., Brunie, L., 2012. A Privacy Preserving Prediction-based Routing Protocol for Mobile Delay Tolerant Networks. Tech. Rep. RR-LIRIS-2012-011, LIRIS UMR 5205 CNRS/INSA de Lyon/Universit Claude Bernard Lyon 1/Universit Lumire Lyon 2/cole Centrale de Lyon.

[15] Hui, P., Chaintreau, A., Scott, J., Gass, R., Crowcroft, J., Diot, C., 2005. Pocket switched networks and human mobility in conference environments. In: Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking. WDTN '05. ACM, New York, NY, USA, pp. 244–251.

[16] Hui, P., Crowcroft, J., Yoneki, E., 2011. Bubble rap: Social-based forwarding in delay-tolerant networks. IEEE Trans. on Mobile Comput. 10 (11), 1576–1589.

[17] Hui, P., Yoneki, E., Chan, S. Y., Crowcroft, J., 2007. Distributed community detection in delay tolerant networks. In: Proceedings of 2nd ACM/IEEE international workshop on Mobility in the evolving internet architecture. MobiArch '07. ACM, New York, NY, USA, pp. 7:1–7:8.

[18] Jain, S., Fall, K., Patra, R., 2004. Routing in a delay tolerant network. SIGCOMM Comput. Commun. Rev. 34, 145–158.

[19] Jansen, R., Beverly, R., 2010. Toward anonymity in dtns: Threshold pivot scheme. In: Proc. of MILCOM. pp. 587–592.

[20] Johnson, D. B., Maltz, D. A., 1996. Dynamic source routing in ad hoc wireless networks. In: Imielinski, T., Korth, H. F. (Eds.), Mobile Computing. Vol. 353 of The Kluwer International Series in Engineering and Computer Science. Springer US, pp. 153–181.

[21] Karaliopoulos, M., 2009. Assessing the vulnerability of dtn data relaying schemes to node selfishness. IEEE Commun. Lett. 13 (12), 923–925.

[22] Kate, A., Zaverucha, G., Hengartner, U., 2007. Anonymity and security in delay tolerant networks. In: Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on. IEEE, pp. 504–513.

[23] Keränen, A., Ott, J., Kärkkäinen, T., 2009. The one simulator for dtn protocol evaluation. In: Proceedings of the 2nd International Conference on Simulation Tools and Techniques. Simutools '09. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), ICST, Brussels, Belgium, Belgium, pp. 55:1–55:10.

[24] Keranen, A., Pitkanen, M., Vuori, M., Ott, J., 2011. Effect of non-cooperative nodes in mobile dtns. In: World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a. pp. 1–7.

[25] Ko, Y.-B., Vaidya, N. H., Jul. 2000. Location-aided routing (lar) in mobile ad hoc networks. Wirel. Netw. 6 (4), 307–321.

[26] Kosch, T., Adler, C., Eichler, S., Schroth, C., Strassberger, M., 2006. The scalability problem of vehicular ad hoc networks and how to solve it. Wireless Communications, IEEE 13 (5), 22–28.

[27] Le, Z., Vakde, G., Wright, M., 2009. Peon: privacy-enhanced opportunistic networks with applications in assistive environments. In: Proceedings of the 2nd International Conference on PErvasive Technologies Related to Assistive Environments. PETRA '09. ACM, New York, NY, USA, pp. 76:1–76:8.

[28] Li, N., Das, S. K., 2010. Radon: reputation-assisted data forwarding in opportunistic networks. In: Proceedings of the Second International Workshop on Mobile Opportunistic Networking. MobiOpp '10. ACM, New York, NY, USA, pp. 8–14.

[29] Li, Q., Gao, W., Zhu, S., Cao, G., 2012. A routing protocol for socially selfish delay tolerant networks. Ad Hoc Networks 10 (8), 1619–1632.

[30] Li, Y., Hui, P., Jin, D., Su, L., Zeng, L., 2010. Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks. IEEE Commun. Lett. 14 (11), 1026–1028.

[31] Li, Y., Hui, P., Jin, D., Su, L., Zeng, L., 2011. Performance evaluation of routing schemes for energy-constrained delay tolerant networks. In: Communications (ICC), 2011 IEEE International Conference on. pp. 1–5.

[32] Li, Y., Su, G., Wang, Z., 2012. Evaluating the effects of node cooperation on dtn routing. AEU - International Journal of Electronics and Communications 66 (1), 62–67.

[33] Li, Y., Su, G., Wu, D., Jin, D., Su, L., Zeng, L., 2011. The impact of node selfishness on multicasting in delay tolerant networks. IEEE Trans. Veh. Technol. 60 (5), 2224–2238.

[34] Lindgren, A., Doria, A., Schelén, O., 2003. Probabilistic routing in intermittently connected networks. SIGMOBILE Mob. Comput. Commun. Rev. 7, 19–20.

[35] Liu, J., Issarny, V., 2004. Enhanced reputation mechanism for mobile ad hoc networks. In: Jensen, C., Poslad, S., Dimitrakos, T. (Eds.), Trust Management. Vol. 2995 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 48–62.

[36] Lu, R., Lin, X., Shen, X., 2010. Spring: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks. In: INFOCOM, 2010 Proceedings IEEE. pp. 1–9.

[37] Lu, R., Lin, X., Zhu, H., Shen, X., Preiss, B., 2010. Pi: A practical incentive protocol for delay tolerant networks. IEEE Trans. Wireless Commun. 9 (4), 1483–1493.

[38] Lu, X., Hui, P., Towsley, D., Pu, J., Xiong, Z., 2010. Anti-localization anonymous routing for delay tolerant network. Computer Networks 54 (11), 1899–1910.

[39] Miao, J., Hasan, O., Ben Mokhtar, S., Brunie, L., 2012. A self-regulating protocol for efficient routing in mobile delay tolerant networks. In: Digital Ecosystems Technologies (DEST), 2012 6th IEEE International Conference on. IEEE, pp. 1–6.

[40] Modarresi, A., Woungang, I., Reyhani, L., Razavi, H., 2011. Reputation-based enforcement schemes tailored to opportunistic networks design.

[41] Nash, J., 1953. Two-person cooperative games. Econometrica 21 (1), 128–140.

[42] Ogiela, M. R., Ogiela, U., 2012. Dna-like linguistic secret sharing for strategic information systems. International Journal of Information Management 32 (2), 175 – 181.

[43] Onen, M., Shikfa, A., Molva, R., 2007. Optimistic fair exchange for secure forwarding. In: Mobile and Ubiquitous Systems: Networking Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on. pp. 1–5.

[44] Panagakis, A., Vaios, A., Stavrakakis, I., 2007. On the effects of cooperation in dtns. In: Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on. pp. 1–6.

[45] Parris, I., Henderson, T., 2012. Privacy-enhanced social-network routing. Computer Communications 35 (1), 62–74.

[46] Pujol, J., Toledo, A., Rodriguez, P., 2009. Fair routing in delay tolerant networks. In: INFOCOM 2009, IEEE. IEEE, pp. 837–845.

[47] Reed, M., Syverson, P., Goldschlag, D., 1998. Anonymous connections and onion routing. IEEE J. Sel. Areas Commun. 16 (4), 482–494.

[48] Royer, E., Toh, C., 1999. A review of current routing protocols for ad hoc mobile wireless networks. Personal Communications, IEEE 6 (2), 46–55.

[49] Shamir, A., 1985. Identity-based cryptosystems and signature schemes. In: Blakley, G., Chaum, D. (Eds.), Advances in Cryptology. Vol. 196 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 47–53.

[50] Shevade, U., Song, H. H., Qiu, L., Zhang, Y., 2008. Incentive-aware routing in dtns. In: Network Protocols, 2008. ICNP 2008. IEEE International Conference on. pp. 238–247.

[51] Shi, C., Luo, X., Traynor, P., Ammar, M. H., Zegura, E. W., 2012. Arden: Anonymous networking in delay tolerant networks. Ad Hoc Networks 10 (6), 918–930.

[52] Spyropoulos, T., Psounis, K., Raghavendra, C. S., 2005. Spray and wait: an efficient routing scheme for intermittently connected mobile networks. In: Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking. WDTN '05. ACM, New York, NY, USA, pp. 252–259.

[53] Spyropoulos, T., Psounis, K., Raghavendra, C. S., 2008. Efficient routing in intermittently connected mobile networks: the multiple-copy case. IEEE/ACM Trans. Netw. 16, 77–90.

[54] Spyropoulos, T., Psounis, K., Raghavendra, C. S., 2008. Efficient routing in intermittently connected mobile networks: The single-copy case. IEEE/ACM Trans. Netw. 16 (1), 63–76.

[55] Vahdat, A., Becker, D., 2000. Epidemic routing for partially connected ad hoc networks. Tech. rep., Citeseer.

[56] Voss, M., Heinemann, A., Muhlhauser, M., 2005. A privacy preserving reputation system for mobile information dissemination networks. In: Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. First International Conference on. pp. 171–181.

[57] Wei, L., Zhu, H., Cao, Z., Shen, X., 2011. Mobiid: A user-centric and social-aware reputation based incentive scheme for delay/disruption tolerant networks. In: Frey, H., Li, X., Ruehrup, S. (Eds.), Ad-hoc, Mobile, and Wireless Networks. Vol. 6811 of Lecture Notes in Computer Science. Springer Berlin / Heidelberg, pp. 177–190.

[58] Woungang, I., Denko, M., 2011. Credit-based cooperation enforcement schemes tailored to opportunistic networks. Mobile Opportunistic Networks, 51.

[59] Xie, X., Chen, H., Wu, H., 2009. Bargain-based stimulation mechanism for selfish mobile nodes in participatory sensing network. In: Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON '09. 6th Annual IEEE Communications Society Conference on. pp. 1–9.

[60] Zakhary, S., Radenkovic, M., 2012. Utilizing social links for location privacy in opportunistic delay-tolerant networks. the Proc IEEE ICC.

[61] Zhiwei Yan, H. Z., You, I., 2010. N-nemo: A comprehensive network mobility solution in proxy mobile ipv6 network. Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications Vol.1 (2/3), 52–70.

[62] Zhong, S., Chen, J., Yang, Y., 2003. Sprite: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In: INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies. Vol. 3. pp. 1987–1997.

[63] Zhu, H., Lin, X., Lu, R., Fan, Y., Shen, X., 2009. Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks. IEEE Trans. Veh. Technol. 58 (8), 4628–4639.

[64] Zhu, Y., Xu, B., Shi, X., Wang, Y., 2012. A survey of social-based routing in delay tolerant networks: Positive and negative social effects. IEEE Communications Surveys & Tutorials PP (99), 1–15.