An Analysis of Strategies for Preventing Selfish Behavior in Mobile Delay Tolerant Networks

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
[1]E-mail: {jingwei.miao, omar.hasan, sonia.benmokhtar, lionel.brunie}@insa-lyon.fr
[2]Department of Information Security Engineering, Soonchunhyang University, Asan, Korea
[2]E-mail: yim@sch.ac.kr

***Abstract*—In mobile Delay Tolerant Networks (DTNs), messages are routed in a mobility-assisted manner. Therefore, the willingness of nodes to relay messages for other nodes plays a significant role in the routing process. Moreover, since the resources in mobile devices are generally limited, carriers of mobile devices may be unwilling to relay messages for other nodes in order to conserve their scarce resources. Furthermore, recent studies on the impact of selfish behavior in DTNs show that the performance metrics (i.e., delivery ratio, delivery overhead, and delivery latency) are severely influenced if a major portion of the nodes is selfish. A number of strategies have been proposed to prevent the impact of selfish behavior. It is therefore necessary to give an overview of the representative strategies.**

In this paper, we first classify the different types of selfish behavior. The existing strategies for preventing selfish behavior are traditionally classified into three categories: barter-based, credit-based and reputation-based. We then survey some representative strategies in the literature belonging to each category. Finally, we conduct experiments to compare the performance of these strategies for preventing different types of selfish behavior.

***Keywords*-mobile, delay tolerant, selfish, reputation, game theory, ecash.**

I. Introduction

Mobile Delay Tolerant Networks (DTNs) are composed of a finite set of mobile devices[1], such as cell phones and Personal Digital Assistants (PDAs). In mobile DTNs, an end-to-end routing path cannot be assumed to exist between the source and the destination of a message [1]. The characteristics of DTNs include frequent and long-term partitions which make message delivery one of the major challenges in these networks. In order to deal with the lack of end-to-end connectivity between nodes[2], message dissemination is often performed in a "store-carry-and-forward" (or mobility-assisted) manner [1], where a message is stored by intermediary nodes and forwarded to nodes closer and closer to the destination until the latter is eventually reached. Therefore, the willingness of nodes to relay messages for other nodes plays an important role in the message dissemination process.

In the literature, a variety of routing protocols for DTNs have been proposed, such as PRoPHET [2], Habit [3], 3R [4], SimBet [5], IFR [6] and BUBBLE [7]. The existing routing protocols rely on studies on the characteristics of node mobility (i.e., the probability of encountering a given node in the near future, or the potential social graph constructed by mobile nodes). Furthermore, most of the existing protocols potentially assume that the nodes in the network are unselfish. However, the resources (e.g., battery, memory and bandwidth) in mobile devices are traditionally limited. Moreover, the resources in the heavily utilized mobile devices can be quickly depleted [8]. Therefore, the carriers of mobile devices may be unwilling to relay messages for others, if their resources get exhausted.

Moreover, recent studies [9][10][11][12] on the impact of selfish behavior on the routing performance (i.e., delivery ratio, delivery latency, and delivery overhead) of routing protocols in DTNs show that the routing performance is severely degraded, if a major portion of the nodes is selfish (or the nodes have a high probability of being selfish).

In order to stimulate selfish nodes to be cooperative, a number of incentive strategies have been proposed. The existing incentive strategies can be classified into three categories [13][14]: barter-based, credit-based, and reputation-based. In this paper, we investigate the existing strategies in each category, and make a comparison among them in terms of routing performance.

The contributions of this paper are as follows:

- We classify selfish behavior from different aspects (i.e., from the viewpoints of collusion and non-cooperation). To the best of our knowledge, this is the first work to develop this unified view of the classification of selfish behavior.
- We summarize the various methodologies used to evaluate the impact of selfish behavior on routing performance (i.e. theoretical models and simulation methods).
- We review the different strategies for preventing selfish behavior in DTNs.
- We conduct an experiment to compare the performance of these strategies for preventing different types of selfish behavior.

The remainder of this paper is organized as follows. In Section II, we classify selfish behavior, and summarize the impact of selfish behavior on routing performance. We then investigate different strategies for preventing selfish behavior

[1]We assume that mobile devices are equipped with a radio interface for a short-range communication (e.g., Bluetooth). When two mobile devices are in the transmission range of each other, they are considered to encounter each other and can exchange messages.

[2]In this paper, nodes denote mobile devices or the carriers of mobile devices.

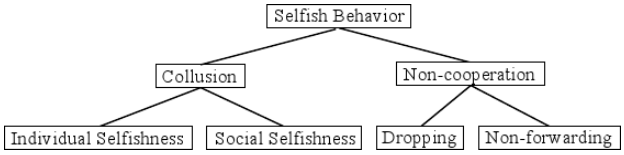


Fig. 1: Classification of selfish behavior in DTNs

in Section III. This is followed by an experiment to compare the performance of different strategies in Section IV. Finally, we conclude this paper in Section VI.

II. Selfish Behavior

In this section, we first develop a unified view of the classification of selfish behavior. We then discuss the methodologies utilized for investigating the influence of selfish behavior on the performance of routing protocols. Finally, we summarize the performance degradation caused by selfish behavior.

A. The Classification of Selfish Behavior

Recent years have seen considerable research works addressing the issue of selfish behavior in DTNs [11][15][16]. 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, Li et al. [18] classify selfish behavior into two categories: *individual selfishness* and *social selfishness*.

Moreover, in the literature investigating the impact of selfish behavior on the routing performance [9][10], the authors generally consider the following two types of selfish action: *non-forwarding of messages* and *dropping of messages*. Non-forwarding of messages means that a node refuses to relay messages for the nodes to which it is selfish. Dropping of messages means that a node agrees to relay messages for the nodes to which it is selfish, but it drops the messages after receiving them.

From the above description, we can see that there are two classifications 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 Fig.1 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.

B. The Methodologies of Investigating the Impact of Selfish Behavior

Researchers have shown significant interest in this field since Panagakis et al. [9] first presented their study on the performance degradation caused by selfish behavior in DTNs. 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.

Karaliopoulos et al. [10] first explored CTMC to demonstrate the impact of selfish behavior in DTNs. Later studies [19][20][12][11] explored CTMC to show the influence of selfish nodes on routing performance in the contexts of social selfishness, constrained energy and multicast routing. The studies based on theoretical analysis models assume that the occurrence of contacts between nodes follows Poisson distribution. Consequently, the inter-contact time between two nodes follows exponential distribution, which is proved by numerical simulations based on random-based mobility models (i.e., Random WayPoint and Random Direction) [21][22]. The works based on CTMC can only assess the performance of delivery latency and delivery cost, but cannot evaluate the performance of delivery ratio, which is the most important performance metric in DTNs [23]. Moreover, these works based on the CTMC can only model the routing process of simple routing protocols, such as Epidemic [24], Spray and Wait [25]. Recent studies on the characteristics of inter-contact time [26][27], which are based on human mobility from real world, demonstrate that the tail distribution of inter-contact time between nodes can be approximated by a power law distribution rather than an exponential distribution.

In order to evaluate the performance of routing protocols in terms of delivery ratio and to investigate the impact of selfish behavior on more non-trivial routing protocols (e.g., PRoPHET [2]), authors in [28][12][29] have utilized simulation methods.

C. The Impact of Selfish Behavior

The exiting research works [9][10][11][12][19][20][28][29] based on theoretical analysis models and simulations reveal the following two characteristics of the performance degradation caused by selfish behavior. 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. Secondly, the impact on the routing performance is related to the uncooperative action of selfish behavior (i.e., non-forwarding of messages and dropping of messages). 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.

III. Strategies for Preventing Selfish Behavior

Since the carriers of mobile devices tend to be selfish in nature, and the performance of routing protocols is degraded

by selfish behavior of nodes, a number of studies focus on stimulating selfish nodes to be cooperative. The existing incentive strategies can be classified into three categories [13][14]: barter-based [13][30][31], credit-based [14][32][15][16][33] and reputation-based [34][35][36][37][16][38]. In the following subsections, we will introduce the representative strategies in each category and summarize their common problems.

A. Barter-based Strategies

The simplest strategies are barter-based or pair-wise Tit-For-Tat (TFT) strategies [13][30][31]. The mechanism is that two encountering nodes exchange the same amount of messages. In [13][30], 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 to 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 [13][31] consider the message selection process as a two-person game, and utilize Nash theorem 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 two encountered nodes has fewer messages. For instance, there are two encountered 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 [39] which is generally considered to achieve the lower bound for delivery ratio in DTNs.

B. 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 the 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 explore for its own benefit.

Based on which node is charged for the message forwarding, the credit-based strategies can be further sub-divided into two models [40]: 1) *Message Purse Model* and 2) *Message Trade Model*. In message purse model [15][16][14], 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 [32], 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 [16][14][15] belonging to the message purse model are suitable to different routing protocols. In [16], the proposed strategy is designed for the single-copy routing protocols (e.g., Direct Delivery and First Contact [41]) 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 [42]. Therefore, more routing protocols (e.g., Epidemic and Spray and Wait) are multi-copy based. In [14][15], the proposed strategies are targeted to multi-copy based routing protocols in DTNs. In [15], 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 [15].

From the above discussion, we can see that the process of charging and rewarding is invoked at the side of the VB, when a message is successfully delivered to the destination. However, the probability of message delivery is low in the network where the nodes have a high probability of being selfish (or a major portion of the nodes is selfish). Although the message delivery can still be achieved when the source

node directly encounters the destination node, there is no intermediary nodes participating in message forwarding. In such a case, nodes cannot be stimulated to cooperate with other nodes, since the process of charging and rewarding cannot be performed at the side of the VB. Moreover, the credit-based strategies do not freeze the credits which have been utilized to request intermediary nodes to relay messages, before the messages are delivered to the destination. Therefore, nodes which have some credits cannot be stimulated to be cooperative to other nodes. Due to the above two reasons, the credit-based strategies cannot achieve a good performance, when nodes have a high probability of being selfish.

C. 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" [43]. 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 with 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 an significant role in this kind of strategy. Based on the feasibility of observation of other nodes, we further divide the existing strategies into two models: 1) *detection-based model* and 2) *without detection model*.

In the detection-based model, each node monitors the behavior of the receivers which receive a message from it, in order to detect the selfish nodes and stimulate them to be cooperative with others. In [37][38][34], the authors utilize different methods to detect selfish behavior in DTNs. In [37], 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. To assess the cooperation of an encountered node, Wei et al. utilize Beta distribution $Beta(\alpha, \beta)$. 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 [15]. In [38], the strategy proposed by Li et al. is similar to the strategy in [37]. The difference is that a receiver floods the receipt instead of sending the receipt to the sender. In [34], Bigwood et al. detect the selfish nodes in a different way. In [34], 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 [36][16]. In [36], 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. Like [36], the proposed strategy in [16] decreases the reputation of all nodes periodically. The differences between them are in two ways. 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 successes or not, all cooperative nodes can get good reputation values by sending the proofs of collaboration to the Trusted Authority (TA), which is responsible for credit and reputation clearance.

From the above description, we can see that the reputation-based strategies can works 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.

IV. Simulation

In this section, we first introduce representative strategies in the above categories. 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.

A. 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., Spray and Wait), called *Non-strategy*, which does not cope with the selfish behavior of nodes.

Barter: When two nodes encounter each other, they exchange the same amount of messages. In barter, the incentive attribute is the number of the messages in a node.

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 [14], 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. In MobiCent, the incentive attribute is the credit in a node.

IRONMAN: As depicted in Section III 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 encountered nodes then update the opinion about others' behavior with each other. In IRONMAN, the incentive attribute is the reputation of a node. Compared to credit-based strategy, IRONMAN includes the detection of selfish behavior. Therefore, it is selected as the representative strategy in reputation-based strategy.

For each selected strategy, if the value of the incentive attribute in a node, which is explored to stimulate nodes to be cooperative to other nodes, is lower than a given threshold, the node turns into cooperation with other nodes; otherwise, the node may be selfish to other nodes with a given probability. The detailed settings are depicted in TABLE I.

B. Simulation Setup

In order to evaluate the performance of different strategies for preventing selfish behavior, we utilize the Opportunistic Network Environment (ONE) simulator [44] and the Random WayPoint (RWP) mobility model to conduct the experiment. In the RWP model, 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 randomly chooses a new destination, and repeats the above process. Since the initial position of nodes which is generated by the RWP model is not uniform distribution [45], we specify a warm-up period (1000 seconds) to let the position of nodes meet the uniform distribution.

In this experiment, each simulation is repeated 5 times with different random seeds for statistical confidence. 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 72 seconds. Since the message generation process lasts for 12 hours, there are 600 messages generated in total. The detailed settings are listed in TABLE II

TABLE I: Simulation Parameters for Strategies

Strategy Name	Parameter Name	Value(s)
Barter	Threshold	2
MobiCent	Initial Credit for Each Node	2
	Payment for Each Message	1
	Threshold	1
IRONMAN	Initial Trust for Each Node	0.5
	Trust Increment	0.25
	Trust Decrement	0.5
	Threshold	0.49

TABLE II: Simulation Parameters

Parameter Name	Value(s)
Simulation Area	1km x 1km
Simulation Length	55000 seconds
Mobility Model	Random WayPoint (RWP)
Number of Mobile Nodes	50
Number of Group	2
Number of Nodes in Each Group	25
Transmission Range	10 m
Node Speed	1 m/s
Warm-up Period	1000 seconds
Duration of Message Generation	12 hours
Message Generation Rate	1 message per 72 seconds
Time-To-Live (TTL)	3 hours

C. Routing Algorithm

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

Spray and Wait: Messages are associated with an attribute L, which indicates the maximum copies of the message that can be made by the message carrier. There are two phases: the Spray phase and the Wait phase. In the spray phase, the source node "sprays" $L-1$ copies of a message to the first distinct $L-1$ encountered nodes. The message carriers, whose attribute L is 1, switch to the wait phase. In the wait phase, the message carriers can only forward the message to the destination.

D. Performance Metrics

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

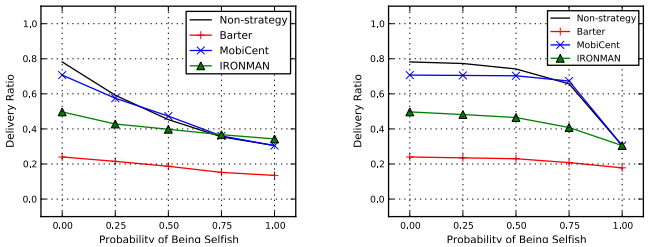
Delivery Ratio: The proportion of messages that have been delivered out of the total unique messages created.

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.

Average Delivery Latency: The average time needed to finish transmitting messages to their destinations.

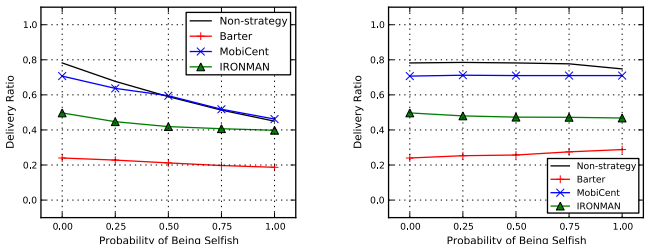
E. Simulation Results

In Fig.2(a), the performance of the strategies for preventing dropping messages is shown. When all nodes are cooperative, the performance of MobiCent and IRONMAN is worse than non-strategy. The reason for MobiCent is that the performance is constrained by the available credit that a node holds. For IRONMAN, since the strategy considers the nodes, who participate in forwarding messages which expire before reaching the destinations, as selfish nodes, the others nodes refuse to provide message forwarding for this kind of nodes until they increase their reputation values by successfully relaying sufficient messages for other nodes. For all nodes, when the probability of being selfish is about 0.5, the performance of MobiCent is better than non-strategy by about 2-3%. However, as the increment of the probability, the performance decreases, due to the weakness of MobiCent (See Section III Part B).



(a) Dropping (b) Non-forwarding

Fig. 2: The routing performance of delivery ratio under individual selfishness with the selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b), respectively.



(a) Dropping (b) Non-forwarding

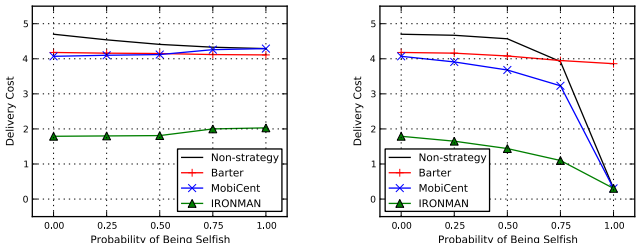
Fig. 3: The routing performance of delivery ratio under social selfishness with the selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b), respectively.

When the probability of being selfish is high, the performance of IRONMAN is much better than those of other strategies, since it can detect the selfish nodes, and encourage the selfish nodes to be cooperative. Moreover, the performance of barter-based strategy is always worse than the other strategies, due to the few messages in nodes (See Section III Part A).

Fig.2(b) illustrates the performance of the strategies for preventing non-forwarding messages. The performance of IRONMAN is always worse than those of MobiCent and non-strategy, since it cannot explicitly prevent the selfish behavior of non-forwarding messages. However, MobiCent can implicitly stimulate nodes to be cooperative, as the number of the messages, which are generated and stored in their buffers, increases. Moreover, the performance of barter-based strategy is always worse than the other strategies.

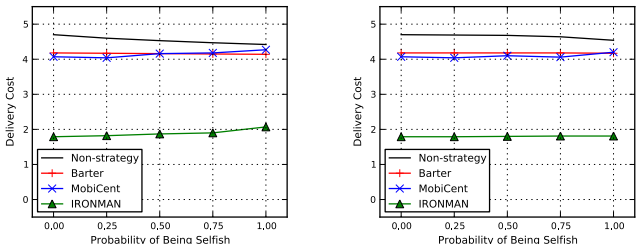
In Fig.3, the performance of delivery ratio of the four strategies under the social selfishness is investigated. From the figures, we can see that all the strategies cannot work well under social selfishness. When nodes participate in message forwarding under the social selfishness, the nodes' the credit or reputation becomes the constrained condition which degrades the routing performance.

The performance of delivery cost is demonstrated in Fig.4 and 5. From the figures, we can see that all the strategies can achieve a good performance in terms of delivery cost. When the nodes adopt the selfish behavior of dropping messages, the



(a) Dropping (b) Non-forwarding

Fig. 4: The routing performance of delivery cost under individual selfishness with the selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b), respectively.

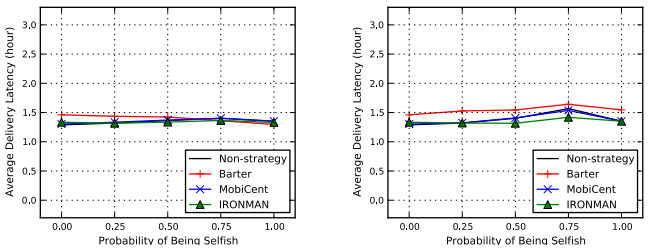


(a) Dropping (b) Non-forwarding

Fig. 5: The routing performance of delivery cost under social selfishness with the selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b), respectively.

reason of the decrement of delivery cost is that the strategies deter nodes from performing selfish behavior. When the nodes run under the selfish behavior of non-forwarding messages, the decrement of delivery cost is caused by the selfish behavior. It also proves that the strategies cannot deal with the selfish behavior of non-forwarding messages.

The performance of delivery latency is demonstrated in Fig.6 and 7. From the figures, it is shown that the barter-based strategy achieves the worst performance in terms of delivery latency, due to the weakness of barter-based strategies.

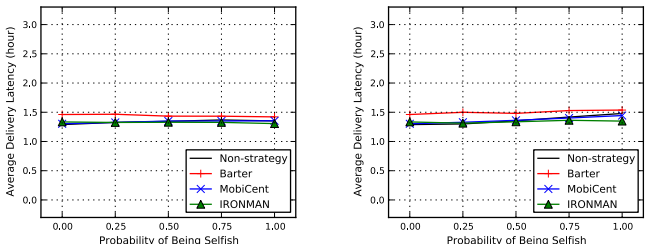


(a) Dropping (b) Non-forwarding

Fig. 6: The performance of delivery latency under individual selfishness with the selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b), respectively.

TABLE III: Performance comparison of the selected strategies

Strategy	performance when nodes' probability of being selfish exceeds 0.5	individual selfishness		social selfishness		the detection of selfish nodes	time and space complexity
		dropping	non-forwarding	dropping	non-forwarding		
Barter	Low	Low	Low	Low	Low	N/A	Low
MobiCent	Low	High	Low	Low	Low	N/A	Low
IRONMAN	High	High	Low	Low	Low	Yes	High



(a) Dropping (b) Non-forwarding

Fig. 7: The performance of delivery latency under social selfishness with the selfish actions of dropping and non-forwarding messages are illustrated in (a) and (b), respectively.

From the above analysis of the simulation results, we can see that the credit-based and reputation-based strategies can prevent the selfish behavior of dropping messages. The performance of barter-based strategies is always worse than the the above two kinds of strategy. All of the strategies cannot deal with the selfish behavior of non-forwarding messages.

F. Comparison of Strategies

According to the above simulation results, the performance of the representative strategy in each category is listed in TABLE III.

V. Related Work

Recent years have seen considerable research works proposed to address the issues of selfish behavior in DTNs. However, only a few of them include the investigation or performance comparison of the proposed strategies for preventing selfish behavior [46][47][34]. In [46], Woungang et al. 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. In [47], Madarresi et al. 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 the performance comparison of the proposed strategies.

In [34], Bigwood et al. 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 [34] is a proposal of reputation-based strategy. Moreover, the compared strategies is not selected from each category. Therefore, it cannot reflect the performance comparison between different strategy categories.

Our work differs with 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.

VI. Conclusion

In this paper, we first classified the selfish behavior in DTNs. The existing strategies for preventing selfish behavior are traditionally classified into three categories: barter-based, credit-based and reputation-based. We subsequently analyzed the mechanisms and explored techniques of the proposed strategies. Further, we pointed out the problems in each category. At last, we conducted an experiment to investigate the performance of the representative strategies in each category. The results of our experiment illustrate that 1) the performance of barter-based strategies is impaired by the requirement of exchanging the same amount of messages; 2) credit-based strategies cannot work in an environment in which the nodes have a high probability of being selfish to other nodes; 3) the performance of reputation-based strategies is seriously impaired with the message lost; and 4) all the strategies cannot deal with the selfish behavior of non-forwarding messages.

Acknowledgments

This work is supported in part by the China Scholarship Council (CSC) UT-INSA PhD program, the MDPS German-French Doctoral College and the French National Research Agency (SocEDA, Grant ANR-10-SEGI-013).

References

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

[2] A. Lindgren, A. Doria, and O. Schelén, "Probabilistic routing in intermittently connected networks," *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 7, pp. 19–20, Jul. 2003.

[3] A. J. Mashhadi, S. Ben Mokhtar, and L. Capra, "Habit: Leveraging human mobility and social network for efficient content dissemination in delay tolerant networks," in *Proc. IEEE Int. Symp. a World of Wireless, Mobile and Multimedia Networks & Workshops WoWMoM 2009*, pp. 1–6, 2009.

[4] L. Vu, Q. Do, and K. Nahrstedt, "3r: Fine-grained encounter-based routing in delay tolerant networks," in *Proc. IEEE Int World of Wireless, Mobile and Multimedia Networks (WoWMoM) Symp. a*, pp. 1–6, 2011.

[5] E. M. Daly and M. Haahr, "Social network analysis for routing in disconnected delay-tolerant manets," in *Proceedings of the 8th ACM international symposium on Mobile ad hoc networking and computing*, ser. MobiHoc '07. New York, NY, USA: ACM, pp. 32–40, 2007.

[6] Y. Li, Y. Cao, S. Li, D. Jin, and L. Zeng, "Integrating forwarding and replication in dtn routing: A social network perspective," in *Proc. IEEE 73rd Vehicular Technology Conf. (VTC Spring)*, pp. 1–5, 2011.

[7] P. Hui, J. Crowcroft, and E. Yoneki, "Bubble rap: Social-based forwarding in delay-tolerant networks," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 11, pp. 1576–1589, Nov. 2011.

[8] J. Pujol, A. Toledo, and P. Rodriguez, "Fair routing in delay tolerant networks," in *INFOCOM 2009, IEEE*. IEEE, pp. 837–845, 2009.

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

[10] M. Karaliopoulos, "Assessing the vulnerability of dtn data relaying schemes to node selfishness," *Communications Letters, IEEE*, vol. 13, no. 12, pp. 923–925, Dec. 2009.

[11] Y. Li, G. Su, and Z. Wang, "Evaluating the effects of node cooperation on dtn routing," *AEU - International Journal of Electronics and Communications*, vol. 66, no. 1, pp. 62–67, 2012.

[12] Y. Li, G. Su, D. Wu, D. Jin, L. Su, and L. Zeng, "The impact of node selfishness on multicasting in delay tolerant networks," *Vehicular Technology, IEEE Transactions on*, vol. 60, no. 5, pp. 2224–2238, Jun. 2011.

[13] L. Buttyan, L. Dora, M. Felegyhazi, and I. Vajda, "Barter trade improves message delivery in opportunistic networks," *Ad Hoc Networks*, vol. 8, no. 1, pp. 1–14, 2010.

[14] B. B. Chen and M. C. Chan, "Mobicent: a credit-based incentive system for disruption tolerant network," in *INFOCOM, 2010 Proceedings IEEE*, pp. 1–9, Mar. 2010.

[15] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "Smart: A secure multilayer credit-based incentive scheme for delay-tolerant networks," *Vehicular Technology, IEEE Transactions on*, vol. 58, no. 8, pp. 4628–4639, Oct. 2009.

[16] R. Lu, X. Lin, H. Zhu, X. Shen, and B. Preiss, "Pi: A practical incentive protocol for delay tolerant networks," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 4, pp. 1483–1493, Apr. 2010.

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

[18] Q. Li, W. Gao, S. Zhu, and G. Cao, "A routing protocol for socially selfish delay tolerant networks," *Ad Hoc Networks*, no. 0, pp. –, 2011.

[19] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Evaluating the impact of social selfishness on the epidemic routing in delay tolerant networks," *Communications Letters, IEEE*, vol. 14, no. 11, pp. 1026–1028, Nov. 2010.

[20] ——, "Performance evaluation of routing schemes for energy-constrained delay tolerant networks," in *Communications (ICC), 2011 IEEE International Conference on*, pp. 1–5, Jun. 2011.

[21] R. Groenevelt, P. Nain, and G. Koole, "The message delay in mobile ad hoc networks," *Perform. Eval.*, vol. 62, pp. 210–228, Oct. 2005.

[22] R. Groenevelt, "Stochastic models for ad hoc networks," *PhD thesis*, vol. INRIA, Apr. 2005.

[23] J. Shen, S. Moh, and I. Chung, "Routing protocols in delay tolerant networks: A comparative survey," in *The 23rd International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC 2008)*, pp. 6–9, 2008.

[24] A. Vahdat and D. Becker, "Epidemic routing for partially connected ad hoc networks," Citeseer, Tech. Rep., 2000.

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

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

[27] 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 *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*, pp. 1–13, Apr. 2006.

[28] A. Keranen, M. Pitkanen, M. Vuori, and J. Ott, "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, Jun. 2011.

[29] M. Chuah and P. Yang, "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, Aug. 2009.

[30] L. Buttyan, L. Dora, M. Felegyhazi, and I. Vajda, "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, Jun. 2007.

[31] X. Xie, H. Chen, and H. Wu, "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, Jun. 2009.

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

[33] S. Zhong, J. Chen, and Y. Yang, "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 vol.3, Apr. 2003.

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

[35] M. Voss, A. Heinemann, and M. Muhlhauser, "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, Sept. 2005.

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

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

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

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

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

[41] S. Jain, K. Fall, and R. Patra, "Routing in a delay tolerant network," *SIGCOMM Comput. Commun. Rev.*, vol. 34, pp. 145–158, Aug. 2004.

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

[43] J. Liu and V. Issarny, "Enhanced reputation mechanism for mobile ad hoc networks," in *Trust Management*, ser. Lecture Notes in Computer Science, C. Jensen, S. Poslad, and T. Dimitrakos, Eds. Springer Berlin / Heidelberg, vol. 2995, pp. 48–62, 2004.

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

[45] C. Bettstetter, G. Resta, and P. Santi, "The node distribution of the random waypoint mobility model for wireless ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 2, pp. 257–269, Jul. 2003.

[46] I. Woungang and M. Denko, "Credit-based cooperation enforcement schemes tailored to opportunistic networks," *Mobile Opportunistic Networks*, pp. 51–82, 2011.

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