A scheme for stimulating message relaying cooperation

Haifeng Lin and Fuquan Zhang

Abstract
It is expected that all the nodes try their best to store and forward the messages in the intermittent connection network. However, due to the limited resources, such as memory, power, and transient communication chance, selfish nodes may relay the messages without responsibility. Stimulating selfish to behave normally could improve network performance. However, usually, it is difficult to distinguish the selfish behavior from the inability to relaying the message. By monitoring the behavior of relay nodes that messages are forwarding through, this article proposes a scheme that relays messages according to the reputation of intermediate nodes. The proposed reputation estimation scheme combines selfish behavior and inability behavior, and reveals very little private information for the protocol practice. There is a trade-off between the threshold and the performance. Too low value may not distinguish the selfish nodes. On the contrary, some normal nodes may excluded and cannot join the relaying and processing. Simulation effectively demonstrates that the reputation affects the node’s performance, and an appropriate reputation threshold value is useful for improving the network performance.

Keywords
Selfish, behavior, relaying, cooperation

Date received: 16 October 2019; accepted: 22 January 2020

Handling Editor: Andino Maseleno

Introduction
The nodes store, carry, and forward a message in an intermediate tolerant network, by assuming that every node would like to cooperate, wait for opportunities, and try their best to deliver each message. However, selfish nodes existing in the networks or nodes that are constrained with memory, bandwidth, and calculation ability are likely to easily violate this hypothesis.

The selfish behavior of node, such as keeping itself the message when the memory becomes full1 or first relaying itself the message when a connection “opportunity” arises,2 will result in a lower delivery probability,3 a higher overhead, and the overall performance decrease.4,5 This would be more serious when the majority of nodes are selfish.

The barter-based schemes5 aim at stimulating nodes to cooperate by exchanging messages.6 Virtual currency is introduced in the credit-based system7,8 and pricing game.9 Cooperating nodes will be paid according to their service10 of processing and relaying the messages of other nodes.11 Selfish nodes that easily deny relaying messages would gradually cooperate.12,13

Blackhole will decrease the network performance, which can be viewed as a kind of network attack and may be caused by the nodes that drop the message with the intention.14 The node load was considered in selecting the communication mode of nodes; however, the residual energy of the node was not considered. Thus,
it may not reflect the real load that the node can be processed.\(^\text{15}\)

Interactions among nodes communication\(^\text{14,16}\) are used to evaluate and select the one that passes the threshold. Moreover, the more the personal information obtained, such as the mobile model, encounter frequency, and connection time, the more accurate the evaluations would be.\(^\text{17,18}\) Furthermore, machine learning has been widely used in parameter decision;\(^\text{19–21}\) in such methods, generally, a few key factors are chosen to design the message relaying and processing.\(^\text{22}\) By analyzing the relation between the throughput and the packet dropping probability of the wireless channel, a joint adaptive modulation was designed to improve the throughput with guaranteed low and tolerable packet dropped probability.\(^\text{23}\)

By observing and evaluating the interaction pattern of nodes in network, reputation-based strategies identify which node is the selfish one. A node can adopt a different strategy by checking others reputation values when they meet each other.

Moreover, usually it is difficult to distinguish the behavior of node. For example, some nodes are honest but not competent to the task of relaying message due to lack of memory, unable to move, due to short communication range, and so on. Some nodes are selfish that pay no heed to carry on relaying nodes.

Furthermore, the relay node should reveal private information as little as possible, such as the history and location information, and require low computation ability and a small amount of memory space in order to be widely used. Therefore, how to make correct calculation of node reputation has become a challenging issue in delay tolerant networks (DTN).

Conceptually, the selfish and uncompetitive behavior should be considered in node reputation for candidate selection. However, there are a lot of issues involved in reputation calculation, often the calculation of most appropriate value has to reveal various types of personal information, such as data delivery rates, memory, delay, and bandwidth consumption, and they influence each other and require high computation ability.

In order to evaluate the reputation without revealing the node’s private information as little as possible, this article proposed a novel scheme. It treated the evaluation of selfish behaviors same as the uncompetitive activities. Dropping messages will eventually result in performance deterioration, even if the behavior that dropping messages are caused by insufficient.

In other words, selfish or uncompetitive behavior will result in failure of relaying message. That is, such nodes are low in reputation to task the forwarding message. Thus, fixed criteria can be used, and thus the calculation is simplified. For the protocol practice, we calculate the reputation using the successful relayed message information, which indicates all the factors affecting successful relaying message. Thus, by monitoring the results of relaying message, we can reflect their behavior in a simple way.

### The reputation estimation

In the network routing, some nodes will refuse to take the duty of relaying messages due to its inadequate resources—such nodes are called selfish nodes. Usually, a reputation value is used to evaluate and mark the selfishness of the nodes. Node’s reputation represents how selfish a node is. The routing algorithm should not select the node with a low reputation as a relay node. That is, the selfishness should reflect the node with a low reputation and should be avoided to be selected as relay node or may have little impact on the routing performance.

However, for practice, it is difficult to identify the primary reason that the node did not relay the node. For example, a node that did not relay a message may not only due to selfishness but also due to low power, insufficient power, short communication range, and so on. Therefore, the reputation calculation should reflect these factors to some extent.

In this way, a reputation value is used to represent the ability and the reliability that a message would be successfully processed in an intermediate node. Thus, by selecting the node with a higher reputation value, the relaying behavior and processing ability of a node are reflected and integrated into the proposed scheme.

First, a candidate node is selected as a relay node when its reputation is beyond the threshold. Second, to achieve fairness, the reputation value of a candidate node is evaluated not only by the sending node but also by the other nodes with their records of the candidate’s historic behavior.

The above steps include both the quantity that a node cooperates and the ratio of successful forwarding on reputation values. In order to obtain a good reputation value, nodes need to continuously relay the reliable forward message.

Furthermore, every node would like to require service from node with higher reputation, and to process messages for nodes with high reputation, consequently, reputation values of selfish node will gradually decrease. Eventually, a selfish node will be isolated when its reputation is below a predefined threshold. This stimulates all individuals to cooperate in forwarding in order to earn a higher reputation.

In order to deal with a selfish node, an effective node cooperation mechanism that promotes the cooperation of nodes is necessary. The classical protocols, such as epidemic algorithm, are kind of flooding-based protocols in DTN. It is assumed that nodes are fully cooperative. But, in fact, due to the restrictions of various
network conditions, there are always some nodes that become selfish or unable to serve continuously. The performance of network will be seriously affected due to such selfish nodes.

On the purpose of effectively estimating the selfishness degree and possibility of cooperation of nodes in DTN, each candidate node is evaluated by recording its transmission and forwarding behavior.

As we mentioned in the previous section, a node \( j \) calculates reputation of a node \( i \), \( R_{ij} \), in equation (1). It consists of two parts: One part is directly calculated based on node \( j \)'s record data, another is indirectly from other node’s remark value. We use \( R_{ij}^d \) and \( R_{ij}^m \) to present the direct and indirect values, respectively. The parameter \( \alpha \) is the weight:\textsuperscript{24}

\[
R_{ij} = \alpha \times R_{ij}^d + (1 - \alpha) \times R_{ij}^m, \quad 0 \leq \alpha \leq 1 \quad (1)
\]

The directed reputation value is calculated in equation (2). \( N_j \) is the number of messages that node \( j \) sends to node \( i \), and requires node \( i \) to relay. \( N_j \) is the number of messages that node \( i \) relayed for node \( j \)

\[
R_{ij}^d = \frac{N_j}{N_j}, \quad 0 \leq R_{ij}^d \leq 1 \quad (2)
\]

Equation (3) calculates the indirect reputation. It is the average value of the direct values scored by all the other nodes

\[
R_{ij}^m = \frac{1}{n - 2} \sum_{k=1}^{n} R_{ij}^d, \quad k \neq i, k \neq j \quad (3)
\]

The reputation-based forwarding scheme

All non-duplicated messages are forwarded to each other when they are in the communication range in epidemic-based protocol. This processing will not stop until the message eventually delivered to the destination nodes. Ideal, if the message has a long time-to-live value, and the memory of the node is sufficient, a flood-based protocol could obtain a shorter delay and a higher delivery ratio. However, usually, the memory and the time slot of encountering are very limited, and the flooding process wasted the bandwidth and deteriorated the performance of protocol.\textsuperscript{25}

Nowadays, everyone pays attention to secure their private information, revealing very little private information (such as the history and location information), and requires low computation ability, and a small amount of memory space is one of the most important factors for a protocol to be widely deployed.\textsuperscript{26}

In this article, we propose a reputation-based epidemic algorithm. Conceptually, the reputation should be considered to reflect the behavior of nodes and to effectively satisfy requirement on performance metric. However, there are a lot of issues involved in reputation calculation; often the calculation of most appropriate value has to reveal various types of personal information, such as data delivery rates, memory, delay, and bandwidth consumption, and they influence each other and require high computation ability. For the protocol practice, we calculate the reputation using the successful relayed message, which indicates all the factors that affect successful relaying message. The factors, such as low memory and short communication range, result in failure of relaying message to some extent. That is, candidate node is assessed by monitoring the relaying behavior and developing a reputation-based message forwarding mechanism.

When a node \( j \) meets node \( i \) without the message, node \( j \) calculates the reputation value \( R_{ij} \) of node \( i \). If \( R_{ij} \) is beyond the threshold, the message will be sent to node \( i \) for relay. The nodes with good reputation are selected as candidate nodes for relay and priority service. In order to obtain routing service, the selfish nodes will have to be honest and good to relay messages so that they get a good reputation. This mechanism stimulates all individuals to cooperate in relay message.

At the beginning, since the contact between nodes is not frequent, the direct reputation may not effectively represent the overall reputation. When more and more nodes encounter others, the reputation value may indicate reality to some extent.

Simulation results

Performance metrics

Following metrics, the Opportunistic Network Environment (ONE) simulator\textsuperscript{27} was widely used in the delay tolerate network simulation to evaluate the performance of protocols:

1. Delivery probability is defined as the ratio between the number of received messages at the destination and the total number of generated messages from the source nodes.
2. Latency is used to evaluate the average time of message from generation to reception.
3. Overhead ratio is the number of delivered messages divided by the number of messages to be delivered.
4. Created represents the number of messages created excluding the duplicated message.
5. Dropped represents the number of messages dropped from nodes' buffers.
6. Hopcount is the hops through source to destination node.
Parameters used in simulation

The proposed scheme used some default parameters in ONE simulator for simulation, as shown in Table 1. The event interval and increment in the number of nodes will increase the number of messages that needed to be delivered. A node with an appropriate buffer size would be helpful to buffer the messages and kept them in the process of the relay. If the buffer size is too small, it may result in the message dropping, especially when large size messages and more messages are generated in the dynamic networks. Hence, the value of the parameters considers and meets all the above-mentioned requirements.

**Table 1. Parameters.**

| Parameters            | Values          |
|-----------------------|-----------------|
| Time of simulation    | 10,800 s        |
| Buffer size           | 5 M             |
| Message size          | 500 K           |
| Number of nodes       | Maximal 360     |
| Event interval        | 5–25 m/s        |
| Wait time             | 0–120 s         |
| Maximum speed         | 2.5 m/s         |

**Speed factor**

As shown in Figure 1, mobility is one of the critical factors for increasing the network capacity and improving the coverage and connectivity. When all the nodes move slowly at the beginning, the overall performance is almost the same. Because the nodes’ mobility is low, consequently the searched areas are small and the probability of meeting the destination is low. Moreover, a
high threshold means that more nodes will be excluded from relaying messages.

When all the nodes move at a higher speed, the performance degradation caused by the inadequate number of nodes could make up to some extent. This is because denser nodes provide more redundancy for the message flooding. In a sparse node, the loss of a few partial qualified nodes can result in loss of coverage to significant portions of the network. At the same number of created, a higher reputation value results in a short hopcount to forward the message. This is because the candidate nodes selected with a higher reputation will try to forward the message. Numerical results indicated that when the reputation is low, the decrease in delay due to the increased number of nodes for relaying a message is modest. This is because the delay is dominated by the validity of potential paths formed by the nodes.

**Traffic load factor**

Figure 2 shows the performance with various message generation intervals from 25 to 5 s. The performance degraded as the message generation interval decreased.
for all reputation values. However, a high reputation value has a relatively good performance when a short interval is used to inject messages into the network. This showed that a higher reputation threshold is appropriate for handling the message forwarding if there is not a very high stress of message delivery.

When more and more messages are generated in the network, the intermediate nodes will drop some messages when their buffer is full. The result is that such invalid copies dropped at higher traffic load, which results in a decrease in overhead. However, the vibration of overhead is not obvious for different thresholds.

A higher reputation threshold is good for the performance of overhead, as shown in Figure 2. A higher reputation threshold results in short hops between the source and the destination since there is not an irresponsible attitude toward the message forwarding.

**Node density factor**

Figure 3 shows the performance with varying number of nodes from 24 to 72. For the given network setting with reference to 72 nodes, performance fluctuations are high. In a network with sufficient nodes, it is quite

---

**Figure 3.** The performance of different density of nodes: (a) overhead ratio, (b) latency, (c) delivery ratio, (d) created, (e) dropped, and (f) hopcount.
likely that one of the relay nodes to which the message has been relayed will find a node that has a valid short hop to the eventual destination, thereby increasing the possibility that the message will be successfully delivered and decreasing the latency, as shown in Figure 3.

Conclusion
Due to the limited resources, such as memory, power, and transient communication chance, selfish nodes may relay the messages without responsibility. This article proposed a reputation-based scheme, which evaluates the node’s reputation in its behavior of relaying message and node’s ability to deliver message. By combining selfish behavior and inability behavior, the proposed reputation estimation method reveals very little private information. It is useful for the protocol to be widely accepted and applied in practice. Results showed that the proposed scheme is effective. The higher moving speed of nodes improves the encountering frequency so that the possibility of encountering the destination nodes is also improved. An appropriate reputation threshold value is useful to improve the network performance in different node load, speed, and density of nodes.

Conceptually, the reputation should be considered to entirely reflect the behavior of nodes. If all the information on the network can be collected, the information would be useful to exactly judge the behavior of the nodes. For example, if messages are dropped by a relay node and when the available space of the buffer of the node is enough, the dropping behavior may be unreasonable. If a node always delivers its message with high priority, then the nodes may be selfish. In other words, the more the delivery-related information obtained, the more the flexible strategy could be designed. In this article, we aim to design a protocol that collects little private information. Thus, in the future, the evaluation accurate of the results can be further improved by collecting more information.

In the future, a strategy may be applied that tries to utilize more public information, such as the mobile model, the average connection time, and the average speed, as well as to select the appropriate rule to punish and stimulate the nodes to satisfy the requirement on the performance metric. Collecting and calculating all the factors, such as data delivery rates, memory, delay, and bandwidth consumption, require high computation ability of the nodes. For the protocol practice, such protocols would be available with the developing of the hardware technique.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This study was supported by the Jiangsu Basic Research Program (Natural Science Foundation) Project (grant no. BK20191393), Nanjing Forestry University Science and Technology Innovation Fund (grant no. CX2016024), and the Priority Academic Program Development (PAPD) of Jiangsu Higher Education Institutions.

ORCID iD
Haifeng Lin https://orcid.org/0000-0002-3835-6075

References
1. Miao J, Hasan O, Mokhtar SB, et al. An analysis of strategies for preventing selfish behavior in mobile delay tolerant networks. In: Proceedings of the sixth international conference on innovative mobile and Internet services in ubiquitous computing (IMIS-2012), Palermo, 4–6 July 2012. New York: IEEE.
2. Roy S. An observer-based distributed scheme for selfish-node detection in a post-disaster communication environment using delay tolerant network. In: Proceedings of the applications and innovations in mobile computing, Kolkata, India, 27 February–1 March 2014. New York: IEEE.
3. Buttyán L, Dora L, Felegyhazi M, et al. Barter trade improves message delivery in opportunistic networks. Ad Hoc Netw 2010; 8(1): 1–14.
4. Chen BB and Chan MC. MobiCent: a credit-based incentive system for disruption tolerant network. In: Proceedings of the 2010 IEEE INFOCOM, San Diego, CA, 14–19 March 2010, pp.1–9. New York: IEEE.
5. Buttyán L, Dora L, Felegyhazi M, et al. Barter-based cooperation in delay-tolerant personal wireless networks. In: Proceedings of the 2007 IEEE international symposium on a world of wireless, mobile and multimedia networks (WoWMoM 2007), Espoo, 18–21 June 2007, pp.1–6. New York: IEEE.
6. Xie X, Chen H and Wu H. Bargain-based stimulation mechanism for selfish mobile nodes in participatory sensing network. In: Proceedings of the 2009 6th annual IEEE communications society conference on sensor, mesh and ad hoc communications and networks (SECON ‘09), Rome, 22–26 June 2009, pp.1–9. New York: IEEE.
7. Lu R, Lin X, Zhu H, et al. Pi: a practical incentive protocol for delay tolerant networks. IEEE T Wirel Commun 2010; 9(4): 1483–1493.
8. Rolla VG and Curado M. Enabling wireless cooperation in delay tolerant networks. Inform Sciences 2015; 290: 120–133.
9. Haq A and Faheem Y. A peer-to-peer communication based content distribution protocol for incentive-aware delay tolerant networks. Wirel Netw 2019; 26: 583–601.
10. Wei L, Cao Z and Zhu H. MobiGame: a user-centric reputation based incentive protocol for delay/disruption tolerant networks. In: Proceedings of the 2011 IEEE global telecommunications conference IEEE GLOBECOM, Houston, TX, 5–9 December 2011. New York: IEEE.
11. Bigwood G and Henderson T. Ironman: using social networks to add incentives and reputation to opportunistic networks. In: Proceedings of the 2011 IEEE international conference on privacy, security, risk, and trust, and IEEE international conference on social computing, Boston, MA, 9–11 October 2011. New York: IEEE.

12. Wei L, Zhu H, Cao Z, et al. MobiID: a user-centric and social-aware reputation based incentive scheme for delay/disruption tolerant networks. In: Frey H, Li X and Ruehrup S (eds) Ad-hoc, mobile, and wireless networks (Lecture notes in computer science), vol. 6811. Berlin; Heidelberg: Springer, 2011, pp.177–190.

13. Zhang X, Wang X, Liu A, et al. PRI: a practical reputation-based incentive scheme for delay tolerant networks. KSII T Internet Inf 2012; 6(4): 973–988.

14. Xu Q, Wang L, Hei XH, et al. GI/Geom/1 queue based on communication model for mesh networks. Int J Commun Syst 2014; 27(11): 3013–3029.

15. Xu Y-H, Liu M-L, Xie J-W, et al. An IEEE 802.21 MIS-based mobility management for D2D communications over heterogeneous networks (HetNets). Concurr Comp: Pract E. Epub ahead of print 7 November 2019. DOI: 10.1002/cpe.5552.

16. Zhou T and Zhang J. Analysis of commercial truck drivers’ potentially dangerous driving behaviors based on 11-month digital tachograph data and multilevel modeling approach. Accident Anal Prev 2019; 132: 105256.

17. Wei W and Qi Y. Information potential fields navigation in wireless ad-hoc sensor networks. Sensors 2011; 11(5): 4794–4807.

18. Roy A, Acharya T and DasBit S. Quality of service in delay tolerant networks: a survey. Comput Netw 2018; 130: 121–133.

19. Wang J, Chen X, Cao L, et al. Individual rubber tree segmentation based on ground-based LiDAR data and faster R-CNN of deep learning. Forests 2019; 10: 793.

20. Huang Z, Xu X, Ni J, et al. Multimodal representation learning for recommendation in Internet of Things. IEEE Internet Things 2019; 6(6): 10675–10685.

21. Rolla VG and Curado M. A reinforcement learning-based routing for delay tolerant networks. Eng Appl Artif Intell 2013; 26(10): 2243–2250.

22. Chao Q, Yao H, Yu F, et al. Deep Q-learning aided networking, caching, and computing resources allocation in software-defined satellite-terrestrial networks. IEEE T Veh Technol 2019; 68: 5871–5883.

23. Jiao W, Ding H, Wu H, et al. Spectrum efficiency of jointing adaptive modulation coding and truncated ARQ with QoS constraints. IEEE Access 2018; 6: 46915–46925.

24. Zhang F, Shi M, Yang X, et al. A reputation based intermediate message forwarding scheme. In: Proceedings of the 5th international conference on electrics, electronics, and computer science, 24–26 November 2016. Jeju Island, Korea: Jeju National University.

25. Zhang F, Joe I, Gao D, et al. Evaluating the impact of network conditions on routing performance in delay tolerant networks. Int J Control Autom 2016; 9: 231–242.

26. Wang Q, Wang X and Lin X. Mobility increases the connectivity of K-hop clustered wireless networks. In: Proceedings of the 15th annual international conference on mobile computing and networking (ACM MobiCom), Beijing, China, 20–25 September 2009. New York: ACM.

27. The Opportunistic Network Environment simulator, version 1.4.0, 2010, http://www.netlab.tkk.fi/tutkimus/dtn/theone/