International Journal of Digital Crime and Forensics
Volume 11 • Issue 2 • April-June 2019

Exploiting Routing Strategy of DTN for Message Forwarding in Information Hiding Applications

Shuangkui Xia, Wuhan University, Wuhan, China

Meihua Liu, Wuhan University, Wuhan, China

Xinchen Zhang, Huazhong Normal University Wuhan, China

Hong Sun, Wuhan University, Wuhan, China

Mao Tian, Wuhan University, Wuhan, China

ABSTRACT

Delay tolerant networks (DTNs) represent a class of intermittently connected networks. In such networks, messages are hard to track since they are transmitted by opportunistic encounters between mobile nodes. This feature makes DTN an appropriate masking channel for information hiding systems. However, the DTN often has poor communication quality, given that it suffers from frequent disruptions. In order to improve the communication quality of DTN and meet the needs of information hiding system, an efficient routing strategy is proposed in this article. On the other hand, in information hiding systems, a relatively long Time-To-Live (TTL) of messages will increase the risk of the message being exposed. To achieve a balance between delivery ratio and concealment, the sensitivity of message TTL is analyzed and a suitable value of lifetime is given. Finally, the simulation results show that the proposed algorithm can improve the effectiveness of message transmission, and the DTN can be used as masking channel to realize information hiding system.

KEYWORDS

Communication Quality, DTN, Information Hiding Applications, Masking Channel, Network Layer, Routing Strategy

INTRODUCTION

Characterized by dynamically changing topology as well as frequent connectivity disruptions, delay tolerant networks (DTNs) represent a common type of self-organizing networks, such as pocket switched network, mobile social network and mobile sensor network (Hrabčák, Matis, Doboš, & Papaj, 2017). In these networks, numerous mobile intelligent devices exchange data through short-range communication interface (Pentland, Fletcher, & Hasson, 2004). Since end-to-end paths cannot be guaranteed, messages are transmitted through opportunistic encounters between nodes (Fall, K). That is, a message could be sent over an existing link, get buffered at the current node until the next link in the path comes up, until it reaches its destination (Spyropoulos, Psounis, & Raghavendra, 2005). As a result, the path that a message passed through is more difficult to be tracked than infrastructure-based communication and traditional wireless communication. This feature makes DTN an appropriate masking channel for information hiding systems. Generally, information hiding system includes content

DOI: 10.4018/IJDCF.2019040103

hiding and transmission hiding (Johnson, & Katzenbeisser, 2000; Chen, et al., 2017). The content hiding mainly focuses on technologies such as cryptography, steganography and digital watermarking (Lin, Yang, & Wang, 2016; Soderi, Mucchi & Hämäläinen, 2017; Hust, & Wuhan, 2005). Besides, the transmission hiding is concerned with the design of masking channel, which exploits some of the inherent characteristics to achieve communication hiding in physical layer (Yang, Kim, & Lo, 2016; Yang, Kim, & Lo, 2015, Huang, Liu, & Lv, 2015; Liu, 2015). In this paper, the DTN is used for the hidden transmission of messages in information hiding systems. After encryption or steganography of the content, the encrypted information such as images or videos are delivered by multi-hop under the intermittently connected environment. In this way, the transmission path becomes unpredictable, and the source senders can be protected from being tracked by the unknown third party. Therefore, both the transmission process and the sender can be "hided" in network layer.

Although DTN is an excellent masking channel, its intermittently connected property makes the delivery of message a challenge (Hui, Chaintreau, Scott, Gass, Crowcroft, & Diot, 2005). As a result, the communication quality can be affected seriously. Thus, to make sure that the DTN is capable to be used as masking channel, the delivery efficiency of message forwarding must be improved. In this paper, an efficient routing strategy which includes two critical schemes is proposed to solve this issue. Firstly, considering that message may stuck and expire in an inactive node, a multi-copy scheme is used to increase the probability of the delivery of message. To enhance the safety of message, a dynamic control of the number of message copies is designed. Secondly, in order to choose a more appropriate next hop for message, available encountering information of nodes in DTN should be exploited, and a utility-based relay node selection mechanism that can assess the delivery capability of the encountered node is developed.

On the other hand, a relatively long TTL (Time-To-Live) will be helpful to improving delivery probability of the message in DTN. However, in information hiding systems, long TTL of message will increase the risk of the message being exposed. To make a balance between delivery ratio and concealment, the lifetime of message should be designed very strictly. In this paper, the sensitivity of message TTL is analyzed, and then a suitable value of lifetime is given.

Several simulations are conducted to investigate the effectiveness of the proposed routing strategy. The performance is evaluated by three indexes: delivery ratio, average delivery delay and network overhead. The results show that the proposed algorithm can improve the effectiveness of message transmission, and the DTN can be used as masking channel to realize information hiding system.

The rest of this paper is organized as follows. In Section 2, a brief overview of related work about spread spectrum technology for information hiding and typical routing protocols in DTN is introduced. In Section 3, the network model is proposed and the problems that need special consideration in information hiding applications will be analyzed. In Section 4, the routing strategy of the RS-IHA for the applications is shown. In Section 5, several simulations and evaluations on the RS-IHA are given. Finally, our work is concluded briefly in Section 6.

RELATED WORKS

The traditional masking channel hiding methods mainly take advantage of some of the inherent characteristics of the channel. One of the most widely-used approaches is the spread spectrum technology which transmits secret information in physical layer to achieve the purpose of communication hiding (Cox, Kilian, Leighton, & Shamoon, 1997; Gkizeli, Pados, & Medley, 2007; Yousaf, Loan, Babiceanu, Maglaras, & Yousaf, 2017; Yang, Kim, & Lo, 2016). Li Ming and Ti Guangyu (2016) propose a spread spectrum information hiding method with pseudo-noise mask. Wenjun et al. (2010) propose an audio information hiding algorithm without destroying the orthogonality of pseudo random sequence. Ming Li et al. (2012) develop an iterative generalized least-squares core procedure to seek unknown data hidden in hosts via multi-signature direct-sequence spread-spectrum embedding. These works are all based on the physical layer technology. In this paper, the purpose by exploiting the network layer of DTN will be achieved.

In order to improve the transmission quality of DTN, scholars proposed the store-carry-forward strategy to deliver messages [14-18]. The early classic routing protocols can be divided broadly into two categories: 1) Strategy based on replication, such as Epidemic (Yang, Kim, & Lo, 2000), Spray and Wait (Spyropoulos, Psounis, & Raghavendra, 2005). 2) Strategy based on forwarding, such as Prophet (Lindgren, Doria, & Schelen, 2004), Bubble Rap (Hui, Crowcroft, & Yonek, 2010). The typical replication-based Epidemic routing lies in the large number of message copies to obtain a satisfying delivery rate, and will result in network overhead and message delay. The typical forwarding-based Prophet routing can significantly improve the message delivery rate and reduce the delivery delay (Lindgren, Doria, & Schelen, 2004). However, it does not make full use of the network information, such as the contact time between nodes, which can improve the prediction accuracy of Prophet, and contribute to the performance of the routing. These common routing do not work well with the needs of concealment of the information hiding applications. In contrast, this paper considers the conditions and constraints of the information hiding applications, and make full use of the encounter information of DTN, to design an efficient routing strategy that can improve the message transmission quality.

NETWORK MODEL AND PROBLEM STATEMENT

Network Model

In information hiding system, in order to avoid the information content being attacked, at the same time, the processing and sender of message can't be tracked, this paper pay attention to a category of information hiding applications which are applied in delay-tolerant networks exhibiting certain social features like PSN (pocket switched network) or MSN (mobile social network). In these networks, the number of nodes is large, and these mobile nodes are carried by humans, communication happens when they come into the short communication range of each other. The structure of the information hiding system is presented as figure 1, the original message is first processed by encryption or steganography, then the encrypted information is delivered hop by hop under the intermittently connected environment. By designing an appropriate routing strategy, the sender can be protected from being tracked to the unknown third party, and the entire transmission process can be hidden. When the receiver gets the message, it decrypts the data. Even through the messages pass through multiple nodes, it won't be exposed because of the efficient steganography technology. So, both the message and the sender can be "hidden."

This paper assume that all nodes are willing to conduct store-carry-forward mechanism, every node can successfully send and receive message, and record the encounter information such as encounter times and contact duration with other nodes. Unicast is considered. Every message has lifetime and is delay-tolerable. Multi-copy of message is allowed to increase the ratio of successful delivery. Once a message copy is received by the destination, a corresponding control message will be generated and spread through the network by epidemic manner, to inform those nodes that store a copy of this message to clean up their buffer.

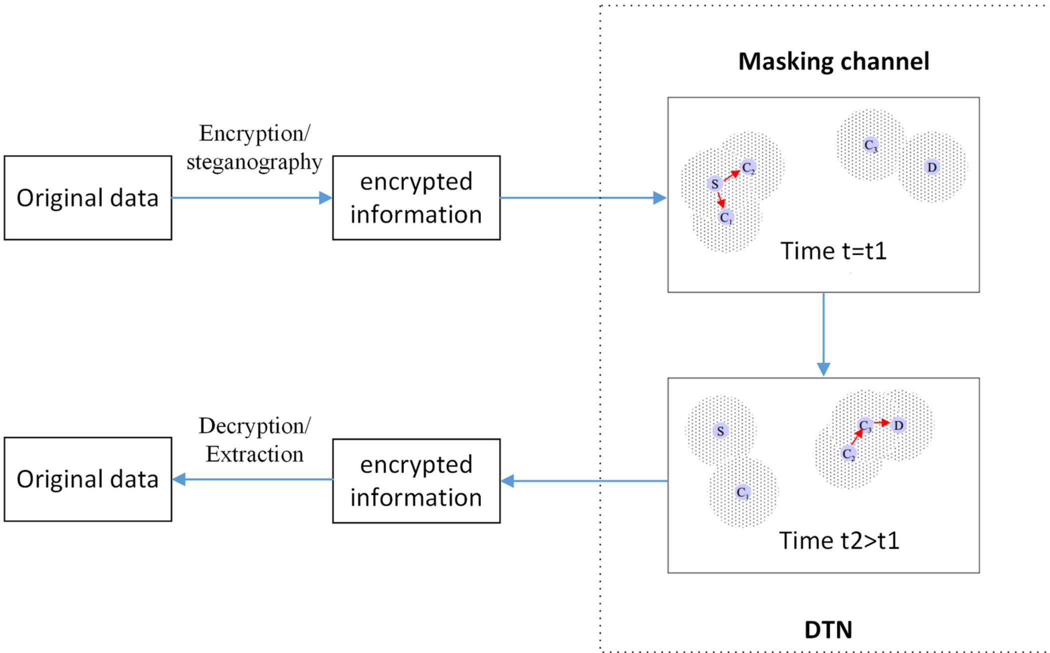
Problem Statement

Some issues that need to be considered specifically in information hiding applications are stated as follows.

Multi-Copy Scheme

As described in the network model, in order to apply DTN in actual information hiding, the number of nodes in DTN should be large. Since the message's carrier node do not know the activity of other nodes in advance, it is possible that message is forwarded to some inactive nodes. For those messages

Figure 1. Structure of the proposed information hiding system



with single copy, they may stick and expire. As a result, the delivery of message can be affected seriously. To cope with this problem, a multi-copy scheme should be applied in the development of routing strategy. However, since blind replication will result in high risk of exposing of message and high delivery cost, the number of message copies must be controlled in a reasonable range.

Relay Node Selection Mechanism

Since the delivery capabilities of relay nodes largely determine whether messages can be successfully delivered, the selection of relay nodes is critical for message transmission. Thus, it is essential to assess the delivery capabilities of nodes. However, it is very costly for nodes to assess the capability of other nodes in a global perspective, due to the intermittently connected feature of DTN. For this issue, distributed computing is an appropriate solution. To estimate the delivery capability of nodes accurately in a distributed manner, how to make use of the available local information becomes an important problem. Hence, a suitable relay node selection mechanism is needed in the design of routing strategy.

Message's TTL

Considering the intermittently connected properties of DTNs, the delivery of the message will endure uncertain and unpredictable delay. To cope with this challenge, message's TTL is set to a relatively large value in many related routing protocols for DTNs, so that the message has enough time to be delivered to its destination. Nevertheless, long TTL of message will increase the risk of exposing of the hiding transmission. Therefore, we need to set a shorter lifetime for messages than common situation while keeping a satisfying delivery rate of the messages. More details will be discussed in the simulation and evaluation section.

THE PROPOSED ALGORITHM

In this section, taking the hidden requirements into account, an efficient and practical routing strategy is developed for information hiding applications (RS-IHA). RS-IHA takes full use of the locally stored information, such as the number of encounters and the duration of contact, to make distributed assessments about link status and the delivery capabilities of nodes. This routing strategy consists of two main components: 1) Dynamical control of the number of message copies; 2) message forwarding decision with the foundation of utility function.

Dynamical Control of the Number of Copies of Message

For message forwarding, a multi-copy strategy is adopted, at the same time, the number of copies of message should be controlled to effectively reduce the network overhead. When the source node generates a message, it sets the maximum number of copies L for the message according to the estimated link state, L is calculated as follows:

$$L = \frac{T_{trans\_delay}}{T_{meet}} \tag{1}$$

where T_{trans_delay} represents the average transmission delay of messages. Since it is difficult for nodes to get the actual average transmission delay of messages in global perspective under real environment, each node only calculates the average delay of messages when it is the recipient. In this way, the T_{trans_delay} of each node is different, which is unreasonable. In order to make the T_{trans_delay} of each node close to the average delivery delay of messages in the whole network, the T_{trans_delay} of node is updated under the following 2 cases.

Case 1: If a message is successfully received by this node, the node will use the average value of this message's transmission delay $T_{trans\_delay}^{current}$ and the node's original $T_{trans\_delay}^{old}$ as the new T_{trans_delay}:

$$T_{trans\_delay}^{new} = \frac{T_{trans\text{-}delay}^{current} + T_{trans\_delay}^{old}}{2} \tag{2}$$

Case 2: When two nodes *i* and *j* meet, they both use the average value of the current $T_{trans\_delay}^{i}$ and $T_{trans\_delay}^{j}$ of the two nodes as their new T_{trans_delay}:

$$T_{trans\_delay}^{new} = \frac{T_{trans\text{-}delay}^{i} + T_{trans\_delay}^{j}}{2} \tag{3}$$

T_{meet} represents the average encounter time between two nodes, and it is easy to calculate:

$$T_{meet} = \frac{T_{pass}}{N} \tag{4}$$

where *N* represents the number of nodes encountered by the node so far, and T_{pass} represents the elapsed time.

As can be seen from the above description, the T_{trans_delay} and T_{meet} of nodes are constantly changing, this will cause the optimal number of copies *L* of the message change dynamically. Through this dynamic control of the maximum number of copies of message, this paper can reduce network overhead while obtaining satisfying delivery rate of messages.

Message Forwarding Decision

When the message is generated, it needs to be forwarded to the destination node by multi-hop. Therefore, how to choose the relay node has become the key issue in the message delivery process. This paper proposes a utility-based forwarding strategy which adopts a utility function to calculate the delivery capability of nodes. The function consists of two elements which are stated as follows.

Contact Probability Between Nodes

Obviously, the more the number of encounters between two nodes, the greater the likelihood of the next encounter. Therefore, we measure the probability of contact by exploiting the number of historical encounters between nodes. And node *i* calculates its contact probability with destination node *d* as follows:

$$p_{id} = \frac{N_{id}}{N_{i*}} \tag{5}$$

where N_{id} represents the number of encounters between *i* and *d*, and N_{i*} represents the number of encounters between *i* and all the other nodes, and obviously, $0 \le p_{id} \le 1$.

The Transmission Efficiency Between Nodes

The contact duration between two nodes can reflect the transmission efficiency which measure how many messages can be transmitted when they meet. And the transmission efficiency between node *i* and message's destination node *d* is calculated in node *i* as follows:

$$\eta_{id} = \frac{\sum_{N=1}^{\infty} T[i(N), d(N)]}{\sum_{k=1}^{*} \sum_{N=1}^{\infty} T[i(N), k(N)]} \tag{6}$$

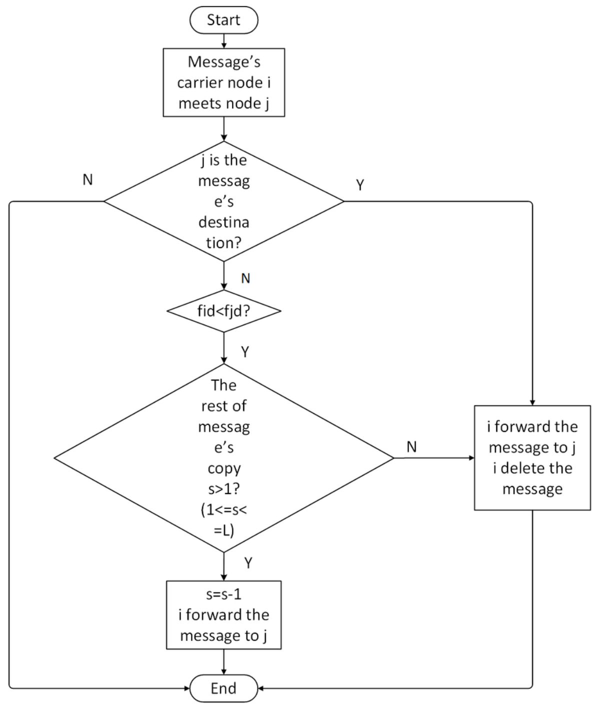
where the molecule represents the sum of contact time between the node *i* and node *d*, and the denominator represents the sum of contact time between node *i* and all other nodes. *N* represents the number of encounters between *i* and all the other nodes. Obviously, $0 \le \eta_{id} \le 1$.

The utility function is defined as the product of contact probability and transmission efficiency between node *i* and message's destination node *d*, it is stated as follows:

$$f_{id} = p_{id} \times \eta_{id} \tag{7}$$

When message's carrier node *i* encounters node *j*, it compares its utility value f_{id} (delivery capability) and the utility value f_{jd} of node *j*, if $f_{id} > f_{jd}$, *i* will forward the message to *j*, otherwise, do

Figure 2. Flowchart of the proposed routing



not forward. In this way, message's carrier selects the most capable node as relay so that the message can be delivered to its destination successfully.

Process of the Proposed Routing

The routing involves the dissemination of message's copies and the selection of message's next hop. The common point of the two components is: message's carrier selects the most capable node as next hop, and forward the message to its destination. The flowchart of the proposed routing is shown in Figure 2.

As shown in the flowchart, for a given message *m*, when its carrier node *i* meets node *j*, they exchange archives of each other, if node *j* happens to be the destination node, then *i* forwards message m to *j*, after that, *i* deletes *m*. Otherwise, node *i* compares the utility value of i with that of node *j*, if *j* has bigger utility, then *i* forwards message *m* to *j*, and if the number of message copies in node *i* is bigger than 1, then the copies will be reduced by one; otherwise, *i* deletes *m* after forwarding. And if the utility value of node *j* is less than that of node *i*, then *i* does not forward message *m*.

In spite of the intermittently connected feature of Delay Tolerant Networks, we can improve the efficiency of message transmission through the dynamic control of message copies and utility-based forwarding mechanism. Messages will be transmitted to more capable carriers and delivered to their destinations with high probability. And limited message copies can optimize the utilization of network resources. The efficiency of the proposed routing will be presented in the simulation section.

SIMULATION AND EVALUATION

In this section, the performance of the proposed routing strategy RS-IHA is evaluated using the Opportunistic Network Environment simulator (ONE). At the same time, we compare our RS-IHA with two classic routing strategies: the Epidemic and Prophet. Epidemic is an infectious and redundancy-

Table 1. Simulation parameters

	Parameters		
Simulation scenario	Simulation time		86400s (24h)
	Area		4500m*3400m
	Map		Helsinki
Information of nodes	Transmit speed	car	2.7~15.9 m/s
		pedestrian	0.5~1.5 m/s
		tram	10~20 m/s
	Transmit range	car	50m
		pedestrian	10m
		tram	100m
	Number of Hosts		126
	Buffer size	car	50M
		pedestrian	10M
		tram	50M
packet	Message size		100~500k
	TTL		360min (6h)
	Generation interval		30~60s

based routing which reproduce message copies unboundedly; and Prophet is a utility-based routing which considers the number and frequency of encounters between nodes. Simulation parameters are set in Table 1. What's more, to find a suitable message TTL, the sensitivity of message TTL is analyzed in the following analysis.

Simulation and Comparison of the Proposed Routing and Two Classic Routing in DTN

Performance in terms of message delivery ratio of the proposed algorithm and the two classic algorithms are shown in Figure 3. The results show that, when the communication time is short, the regular mobility pattern of nodes is not obvious, and the performance of our routing algorithm does not show much advantage: RS-IHA algorithm has a low delivery ratio in short communication time. Nevertheless, with the increase of communication time, the growth rate of the delivery ratio of RS-IHA is significant, and it outperforms the other protocols. And the reasons are stated as follows:

1. It is common that the control of message copies can reduce unnecessary message copies. Moreover, our dynamic scheme can detect and exploit the real-time link status to adjust the degree of redundancy of the message. Consequently, the efficiency of message forwarding is improved. In addition, the longer the communication time is, the more accurately it estimates the number of copies of the message, and the delivery ratio of RS-IHA can benefit more from this scheme. In contrast, Epidemic and Prophet may suffer from network congestion, and cannot achieve high performance in the long run, given that node's cache is limited;
2. For the contact probability and the transmission efficiency included in RS-IHA, it performs better than two traditional routing strategies in the delivery rate under the long-time communication. Although both Prophet and RS-IHA are utility-based routing, Prophet fails to make use of the contact duration between nodes. Therefore, the delivery ratio of Prophet is lower than that of RS-IHA.

Figure 3. Simulation results in terms of delivery ratio

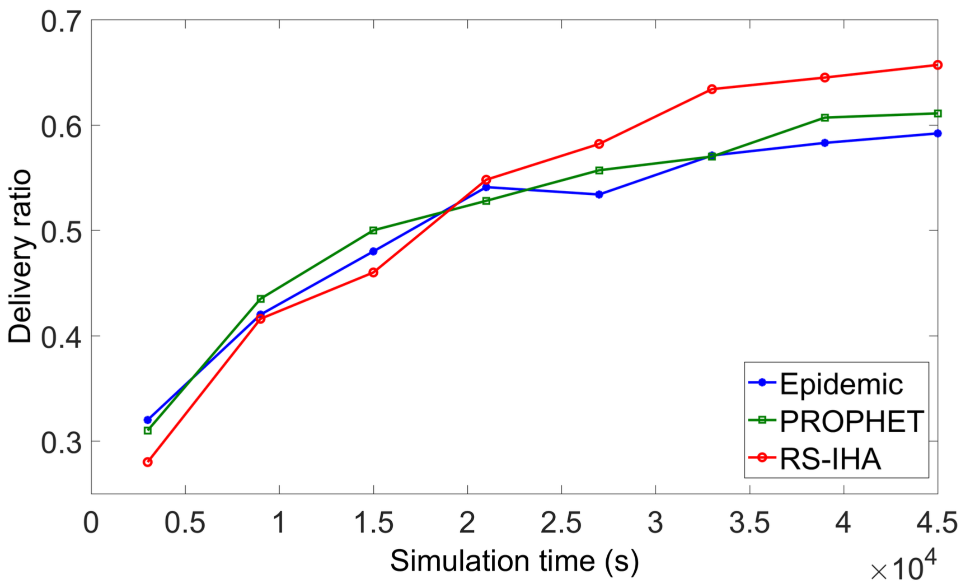


Figure 4 shows the average delay of RS-IHA and the two classic routing. Similar to the case of delivery ratio, the average delay of RS-IHA shows better performance than the two classic protocol in a long time communication. Figure 5 shows the network overhead of RS-IHA and the two classic routing. It can be seen that the overhead of RS-IHA is the lowest in the three routing strategies. And the reasons are stated as follows:

1. Recall that the dynamic control of message copies can optimize the utilization of resources to a large extent, relieve network congestion, and improve the efficiency of message forwarding. Therefore, in terms of network overhead, the proposed routing has significant advantage over the routing strategies which has no message copy control strategy;
2. The utility function in the proposed message forwarding strategy considers both the transmission efficiency and the probability of contact. Thus, the forwarding capability of encountered node can be evaluated more comprehensively, and the performance of routing can be further optimized. Therefore, we have the lowest average delivery delay and network overhead.

In summary, in spite of the harsh communication environment of delay tolerant networks, the proposed routing can achieve satisfying performance which can be better especially in the long-time communication. Therefore, the DTN can be used as masking channel to realize information hiding system.

Sensitivity Analysis of Message TTL

As described in previous, long TTL of message will increase the risk of exposing of the hiding transmission. However, a short TTL will affect the performance of routing seriously, since message may expire before it was successfully delivered. To achieve a better balance, we analyze the sensitivity of message TTL and select an appropriate value. Therefore, we make message TTL varies, and investigate the performance of our RS-IHA (for the other parameters, we refer to the table 1). Since the delivery ratio is a metric that we concern about most, we represent the delivery ratio results when message TTL varies.

Figure 4. Simulation results in terms of the average delay

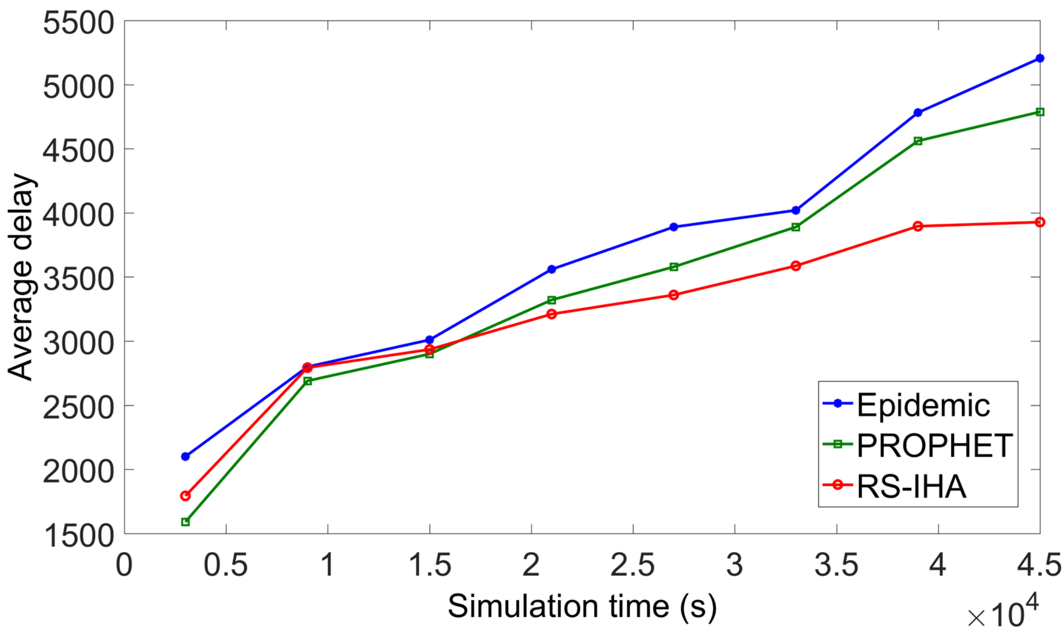
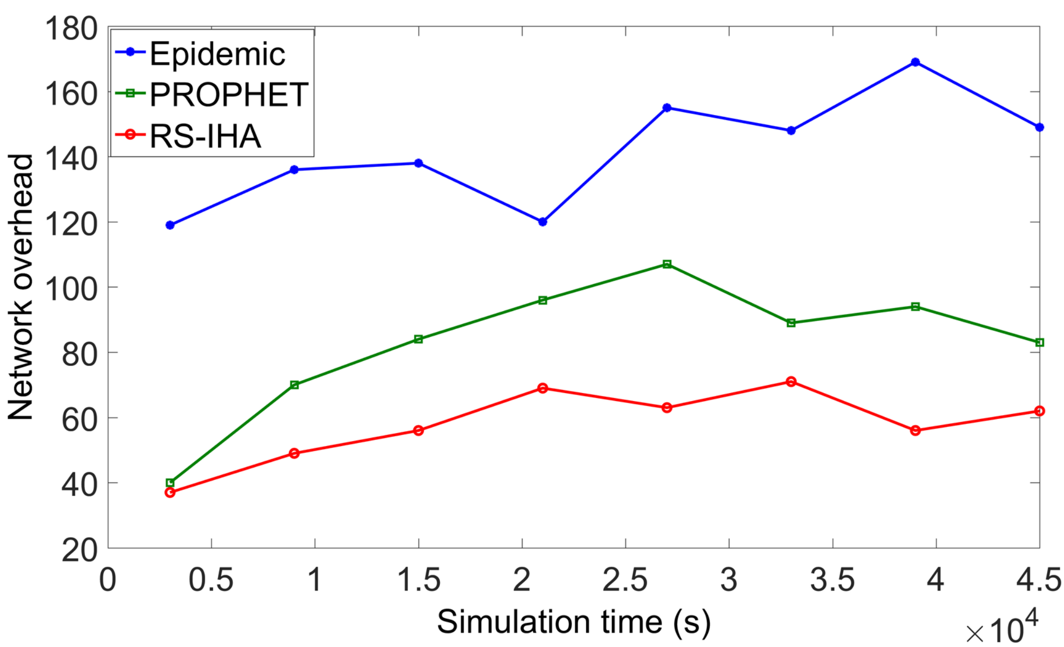
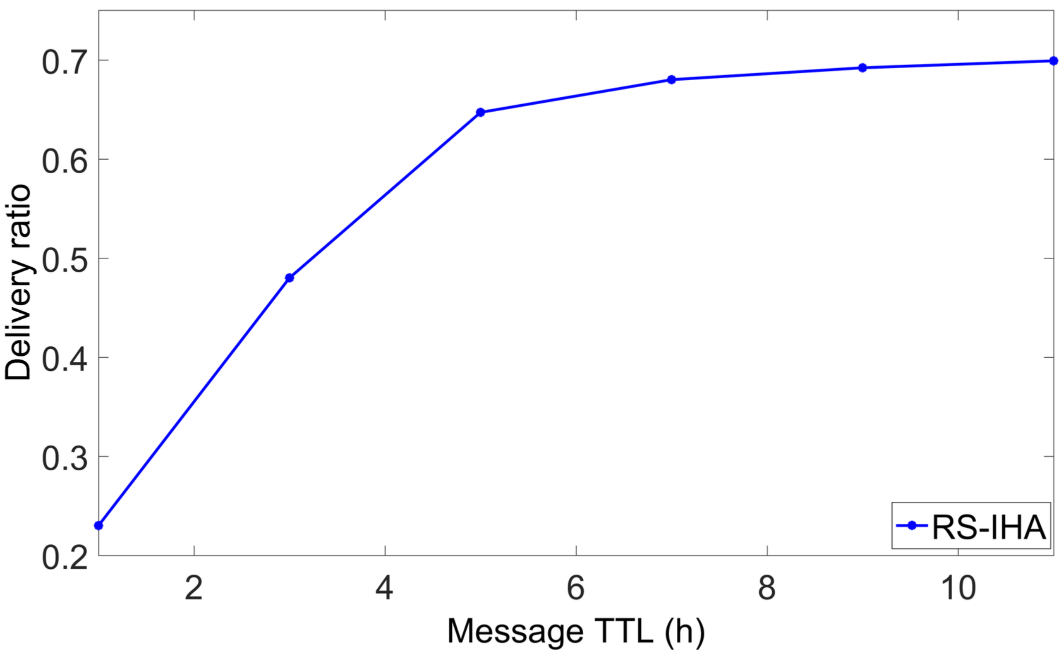


Figure 5. Simulation results in terms of network overhead



It can be seen in Figure 6, with message TTL increases, delivery ratio of the proposed RS-IHA grows fast at first, then tends to be gentle, and is close to stagnant in the end. Obviously, under our simulation parameters, 5 hours is the fulfilling message TTL, since it is not a long lifetime and it almost has no effect on the performance of routing. It is noteworthy that this fulfilling TTL is not generic, it will change with different communication parameters and conditions.

Figure 6. Delivery ratio of the RS-IHA when message TTL varies



CONCLUSION

In this paper, the DTN is used as masking channel for message forwarding in information hiding applications. To cope with the unfavorable feature of the intermittent connection of DTN, we improve the communication quality of the DTN by proposing an efficient routing strategy. Multi-copy scheme is exploited in the routing, and further control on the number of message copies is considered. And historical encounter information of nodes that collected in DTN is used in routing design. On the other hand, we make a sensitivity analysis on message TTL to find a lifetime that is suitable for information hiding. Then we conduct some simulations and comparisons to verify the proposed strategy. The simulation results show that, with the control of the number of message copies and the forwarding mechanism based on utility function, our routing algorithm can acquire satisfying performance in DTN, the message delivery ratio can be improved significantly, the average delay and the overhead ratio can be reduced. And the proposed algorithm can be instructive for applying DTN theory to actual information hiding system.

ACKNOWLEDGMENT

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This study was financially supported by the National Natural Science Foundation of China (grant number: U1736121).

REFERENCES

Chen, Z., Lu, J., Yang, P., Luo, X., Chen, Z., & Lu, J. et al.. (2017). Recognizing substitution steganography of spatial domain based on the characteristics of pixels correlation. *International Journal of Digital Crime and Forensics*, *9*(4), 48–61. doi:10.4018/IJDCF.2017100105

Cox, I. J., Kilian, J., Leighton, F. T., & Shamoon, T. (1997). Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing A Publication of the IEEE Signal Processing Society, 6*(12), 1673.

Fall, K. (2003). Delay-tolerant network architecture for challenged internets. *Sigcomm03 Aug, 33*(4), 27-34.

Gkizeli, M., Pados, D. A., & Medley, M. J. (2007). Optimal signature design for spread-spectrum steganography. *IEEE Transactions on Image Processing*, *16*(2), 391–405. doi:10.1109/TIP.2006.888345 PMID:17269633

Hrabčák, D., Matis, M., Doboš, L., & Papaj, J. (2017). Students Social Based Mobility Model for MANET-DTN Networks. *Mobile Information Systems*, *2017*, 1–13. doi:10.1155/2017/2714595

Huang, Z., Liu, J., & Lv, Q. (2015). Digital Watermarking Algorithm Based on Spread Spectrum and Fourier Transform. *International Conference on Management, Education, Information and Control*. doi:10.2991/meici-15.2015.237

Hui, P., Chaintreau, A., Scott, J., Gass, R., Crowcroft, J., & Diot, C. (2005). Pocket switched networks and human mobility in conference environments. *ACM SIGCOMM Workshop on Delay-Tolerant NETWORKING* (pp.244-251). ACM.

Hui,P, J. Crowcroft, & E. Yonek. (2010). Bubble Rap: social based forwarding in delay tolerant networks. *Mobile Computing, IEEE Transactions on, November 10(11)*, 1576-1589.

HUST. (2005). *Research on information hiding techniques*. Wuhan: Computer & Digital Engineering.

Johnson, N. F., & Katzenbeisser, S. C. (2000). A survey of steganographic techniques.

Li, M., Kulhandjian, M., Pados, D. A., Batalama, S. N., Medley, M. J., & Matyjas, J. D. (2012). On the extraction of spread-spectrum hidden data in digital media. *IEEE International Conference on Communications* (Vol.11, pp.1031-1035). IEEE. doi:10.1109/ICC.2012.6364055

Li, M., Li, L., Guo, Y., Wang, B., & Kong, X. (2015). Security analysis of optimal multi-carrier spread-spectrum embedding. *IEEE China Summit and International Conference on Signal and Information Processing* (pp.851-855). IEEE. doi:10.1109/ChinaSIP.2015.7230525

Lindgren, A., Doria, A., & Schelen, O. (2004). Probabilistic Routing in Intermittently Connected Networks. *Sigmobile Mobile Computing and Comm. Rev.*, *7*(3), 19–20. doi:10.1145/961268.961272

Liu, Z. (2015). *Summary of the research based on information hiding technique*. Industrial Instrumentation & Automation.

Ming, L., & Ti, G. (2016). Spread-Spectrum Information Hiding with PN_Sequence Mask. *The Twelfth National Conference on Information Hiding and Multimedia Information Security*.

Pentland, A., Fletcher, R., & Hasson, A. (2004). DakNet. Rethinking connectivity in developing nations. *IEEE Computer*, *37*(1), 78–83. doi:10.1109/MC.2004.1260729

Soderi, S., Mucchi, L., & Hämäläinen, M. (2017). Physical layer security based on spread-spectrum watermarking and jamming receiver. *Transactions on Emerging Telecommunications Technologies*, *27*(12).

Spyropoulos, T., Psounis, K., & Raghavendra, C. S. (2005). Spray and wait: an efficient routing scheme for intermittently connected mobile networks. *ACM SIGCOMM Workshop on Delay-Tolerant NETWORKING* (pp.252-259). ACM. doi:10.1145/1080139.1080143

Chun-Lin, Song Yang, & Wang. 2016. Secure and Robust Digital Watermarking:Survey, A. *Journal of Electronics (China)*, (4): 343–354.

Vahdat, A., & Becker, D. (2000). Epidemic routing for partially-connected ad hoc networks. *Master Thesis*.

Wen-jun, M. A., Yan-pu, C. H. E. N., Yue, G. A. O., & Gang, M. I. N. (2010). Performance analysis for audio information hiding algorithm based on spread spectrum. *Jisuanji Yingyong*, *30*(8), 2272–2274. doi:10.3724/SP.J.1087.2010.02272

Yang, C. N., Kim, C., & Lo, Y. H. (2016). Adaptive real-time reversible data hiding for jpeg images. *Journal of Real-Time Image Processing*, (3): 1–11.

Yousaf, A., Loan, A., Babiceanu, R. F., Maglaras, L., & Yousaf, O. (2017). Architectural and information theoretic perspectives of physical layer intruders for direct sequence spread spectrum systems. *Computers & Security*, *70*, 124–143. doi:10.1016/j.cose.2017.05.011

Shuangkui Xia is currently a PhD Student at theSchool of Electronic and information engineering, Wuhan University, majoring in digital watermarking. His current research interests are in the areas of wireless mobile networks, Steganography, information hiding system.

Meihua Liu received the MS degree from the Power and mechanical School, Wuhan University, China in 2015 and is currently a PhD Student at theSchool of Electronic and information engineering, Wuhan University, majoring in mobile communication. Her current research interests are in the areas of wireless mobile networks, delay/disruption tolerant networks, mobile social network and algorithm design.

Xinchen Zhang received the MS and PhD degrees from Wuhan University, China, and is currently an associate professor at the School of Physical science and technology, Huazhong Normal University. His current research interests are in the areas of wireless mobile networks, delay/disruption tolerant networks, mobile social network and algorithm design.

Hong Sun is currently a professor at the School of Electronic and information engineering, Wuhan University. His current research interests are in the areas of wireless mobile networks, electronic circuit and system and algorithm design.

Mao Tian is currently a professor at the School of Electronic and information engineering, Wuhan University. His current research interests are in the areas of Ground penetrating radar, electronic circuit and system and algorithm design.