# Routing Algorithm Based on Nash Equilibrium against Malicious Attacks for DTN Congestion Control

Chengjun Wang, Baokang Zhao, Wanrong Yu, Chunqing Wu, Zhenghu Gong



# Routing Algorithm based on Nash Equilibrium against Malicious Attacks for DTN Congestion Control

Chengjun Wang, Baokang Zhao, Wanrong Yu,
Chunqing Wu, and Zhenghu Gong

School of Computer Science, National University of Defense Technology,
Changsha, Hunan, China
{cjwmhd@gmail.com,
bkzhao@nudt.edu.cn,wlyu@nudt.edu.cn,
wuchunqing@nudt.edu.cn,gzh@nudt.edu.cn}

**Abstract.** *In Delay-Tolerant Network(DTN), certain malicious node might generate congestion in attack to reduce the overall performance of the whole network, especially the target of message successful delivery ratio. In this paper, a novel Nash equilibrium based congestion control routing algorithm with the function of security defense (NESD) is proposed. In the process of message delivery, node can use Nash equilibrium to compute the largest proportion of transfer messages occupancy to node memory capacity. This mechanism constrains the attack from malicious node and guarantees the message transfer of regular node. This congestion control routing algorithm for security defense is evaluated by experiment. It is important application in the field of homeland defense. The results show that related key parameters are significantly improved in DTN scenario.*

**Keywords:** Delay-Tolerant Network Routing, Congestion Control, Gaming theory, Nash equilibrium

## 1 Introduction

DTN [1] is widely applied in the obscure or tragedy district [2], vehicle network [3], satellite communication [4] and other wireless network environment.These fields mostly have close relationship with homeland defense.It resolves the problem of intermittent connection, high latency, low data transfer speed, high packet loss rate in DTN by adding a bundle layer [5] between the traditional transmission and application layer and designing storage transfer protocol [6].

As a special wireless network environment, the chief goal of DTN is to guarantee the message successful delivery ratio. The previous algorithms mostly adopt the mechanism of increasing message replicas [7] or leverage the historical information of node's encounter probability [8] as the criterion of transfer node selection in the message delivery.

Meanwhile, limit of DTN resource causes the congestion which also affects the message successful delivery ratio in some extent. Previous congestion control algorithms mostly adopt the passive message delete [9] or migration [10] when congestion happens, or adjust message generation ratio and sending speed by feedback control system [11]. This kind of method usually is passive and lagging. In some extent, it results in the frequent jitter of traffic and unstable network environment.

These methods mostly assume that network nodes are regular and it doesn't consider the presence of malicious nodes. Malicious node tends to forge the probability of its encounter with the target node. High encounter probability is forged by malicious node (Blackhole Attack) [12]. Message transfer request is accepted and then received message is discarded. Or malicious node forges the low probability of its encounter with the target node (Resource-Misuse Attack) [13] which occupies the memory of transfer node and causes network congestion. Two attack methods both block the communication between the other nodes and target nodes and this reduces message successful delivery ratio. The impact of attack is visible in the field of homeland defense.

The presence of malicious nodes causes the failure of the past mechanism which passively controls congestion in order to guarantee the message successful delivery ratio. The active congestion control mechanism to deal with the attack of malicious nodes should be adopted. This paper leverages the Nash equilibrium in game theory [14] to allocate node memory appropriately that makes the fair sharing of local node memory between existing messages in this node and messages which are about to be transferred to this node. This mechanism not only satisfies the essential message transfer operation for message successful delivery and but also avoids the arbitrary message delivery from malicious node to regular nodes. This attack behavior of malicious node makes regular node's whole memory is occupied by malicious node's transfer message which causes the congestion and packet loss in the regular node. It reduces the overall message successful delivery in the network.

## 2 Related Work

To increase message successful delivery ratio, the simplest way to leverage message replica is the flooding routing [7]. This unrestricted duplication of message is a great waste of bandwidth resource. In [15], the authors improve this mechanism by transferring message replicas to all the neighbor nodes in the first communication. Then, these nodes deliver message directly which decreases the amount of replicas, but the successful delivery ratio is obviously affected. In[16], the authors comprehensively consider the tradeoff of resource utilization and successful delivery ratio. It provides message replicas to the successive transfer nodes with the decreasing probability until the message is delivered to destination node at last.

The most popular message delivery strategy is routing algorithm based on the historical information of node encounter probability [8]. This algorithm adopts

storage transfer protocol and node carries message until it encounters the node which has larger probability to meet destination node. This is just the common measure which malicious node uses to attack in DTN. It forges its encounter probability with destination node to destroy usual transfer of message in DTN. Thus, the successful delivery ratio of message is reduced.

To assign different functions for nodes, they are classified as regular node and ferry node. In [17], regular node use random movement and ferry node is transferred in a constant path to assist message delivery of the regular node. This resolves many issues in the traditional DTN network. But the path selection of ferry node is still a hard problem to researchers. This motivates the idea of social network [18] applications in DTN. DTN network is divided into multiple regions. The routing in a region and between regions is different.

For the congestion control, the most common method in message process is to delete new arrival message or previous old message stored in the node [10]. In [19], the authors add the probability management for the operation of message deleting that adopts the predefined constant threshold to control the new arrival message's deleting ratio. In [20], the authors introduce the migration algorithm that means when congestion happens, and then the message is transferred to the nearby nodes. Migration will result in the increase of message transfer overhead, the decrease of message successful delivery ratio and increase of message delivery latency.

In the aspect of message sending speed adjustment,the authors define threshold to implement Additive Increase Multiplicative Decrease (AIMD) [21] dynamically to adjust message sending rate [22]. The constant threshold sometimes can't reflect the network status which might cause the inaccuracy of control. The authors in [23] use ACK as the sign to adjust the message sending speed. When node derives the feedback of message loss, it directly rollbacks the sending speed to that the message was successful delivered recently.

The above two aspects both can't control congestion from the overall situation which needs to build the global feedback control system [24]. Due to the latency as the specific attribute in DTN, control effect of ACK always has the lag phenomenon and congestion identification mistake. Meanwhile, it might cause the severe jitter of message sending speed which leads to the instability of DTN data transfer speed. If the Nyquist Criterion [25] is used in the feedback control system , the instability of message transfer speed in system is mostly resolved.

In conclusion, the above congestion control mechanisms assume all the nodes are regular. In the process of message delivery, the forge of node's attribute is not considered. Meanwhile, when congestion happens, passive method is adopted to control congestion. If there is active attack from malicious node in the network, limited storage resource would be consumed. This passive control method always can't reach the expected effect. This demands the algorithm which can actively control congestion and guarantee the message's successful delivery ratio has the capacity to do active defense. Moreover, some other issues can be considered, including the localization[26, 27], human mobilities[28].

# 3 NESD congestion control routing algorithm

## 3.1 Problem Description

Node in DTN network is distributed discretely and adopts random routing. Random routing results in randomness of node's encounter to a large extent which makes the successful ratio of message delivery unpredictable. The previous solutions usually select transfer node based on historical encounter record to improve the message delivery successful ratio. But the network security is not considered which has no active defense capacity to the active attack. Once history record based on encounter probability is leveraged by malicious node, the consumption attack is implemented to the memory resource of network node which causes network congestion, and the network message successful delivery ratio is lessened as well.

## 3.2 Algorithm Idea

In most cases, the resource is limit which inevitably leads to competition of individuals for public resources in the same system. How to balance the interests of all parties and reach a win-win situation in some extent facilitates the emergence of game theory. This theory adopts formal language derivation to compute the optimal combination of the interests of all parties. Under this combination, each individual would not deviate from this balance for the interest temptation. Thus, it avoids the loss of one individual's interest or the non-optimal situation of overall individuals' interest caused by the individual's competition for public resources.

Memory resource is very rare in DTN node. If presence of malicious nodes is considered, active defense measures must be taken to constrain its active consumption attack for the resource of the node in DTN. Meanwhile, regular occupation demand for memory resource should be guaranteed for the message delivery of regular node. If malicious node attack and regular node demand can't be distinguished, we can adopt the game theory for trade-off. Memory resource of each node should be allocated appropriately. The memory occupation during the regular delivery of regular node message is guaranteed. Meanwhile, malicious occupation of malicious node is avoided.

## 3.3 Algorithm Implementation

The memory of each node in DTN is mostly occupied by two types of messages: existing messages in this node and messages which are about to be transferred to this node. Malicious node always unlimitedly demands other nodes to transfer its brought messages. The memory of attacked nodes is wholly occupied. The memory of attacked party is used out which results in congestion. The method to deal with congestion always deletes the oldest messages. It makes attacked node drop all existing messages in memory.

We adopt Nash equilibrium [14] in gaming theory to tradeoff the share of node memory between existing messages in this node and messages which are about to be transferred to this node. In conditions that malicious node and regular node are not differentiated, active defense is adopted to guarantee the message delivery of regular node. Meanwhile, the attack from malicious node is weakened in some extent and congestion is avoided.

The key of NESD is to leverage Nash equilibrium. The optimal combination of node memory occupancy for existing messages in this node and messages which are about to be transferred to this node is computed. The memory of node is fully shared by two kinds of messages, but not excessively occupied by one party.

The message transfer scenario under malicious node attack is applied to gaming theory. To make use of Nash equilibrium, we assume:

Attendee: existing messages in this node and messages which are about to be transferred to this node.

Action: node memory occupancy of existing messages in this node and messages which are about to be transferred to this node.

Preference:existing messages in this node and messages which are about to be transferred to this node all hope to obtain more opportunities to be transferred unitl reaching the destination node.

**Table 1.** Symbols Used in Theorems

| **Symbol** | **Description** |
|---|---|
| $L_x$ | Preference of $X$ type message |
| $p_x$ | Memory size occupied by type $X$ message |
| 1 | messages which are about to be transferred to this node |
| 2 | existing messages in this node |
| $b$ | Size of node memory |
| $c$ | Node congestion degree |
| $S_x$ | Spare memory size allocated in proportion to type $X$ message |
| $T_x$ | Node memory ratio already occupied by type $X$ message |
| $R$ | Spare memory size of node |
| $D_x$ | Drop-off message amount of type X caused by congestion |

**Theorem 1** When $L_1$ and $L_2$ both reach maximum, based on the characteristic of Nash equilibrium, $p_1$ and $p_2$ can reach the same reasonable value.

*Proof.*

$$L_x = S_x + p_x - D_x \tag{1}$$

$$S_x = T_x \times R \tag{2}$$

$$T_x = \begin{cases} \frac{p_x}{b} & , \quad p_x \leq b \\ 1 & , \quad p_x > b \end{cases} \tag{3}$$

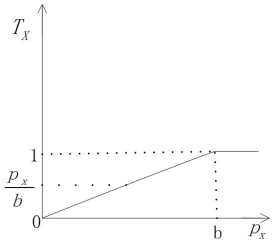


**Fig. 1.** $T_x$

Figure 1 is derived from formal (3)

$$R = \begin{cases} b - p_1 - p_2 & , \quad p_1 + p_2 \leq b \\ 0 & , \quad p_1 + p_2 > b \end{cases} \tag{4}$$

Figure 2 is derived from formal (4)

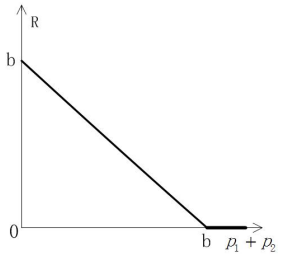


**Fig. 2.** $R$

$$D_x = cp_x (0 \leq c \leq 1) \tag{5}$$

The setting of $D_x$ represents the idea that more occupancy means more responsibility. More memory consumption by certain kind of message results in larger packet drop-off probability for the messages when congestion happens.

According to formal (1) to (5):

$$L_1 = \begin{cases} \frac{p_1}{b} \times (b - p_1 - p_2) + p_1 - cp_1 & , \quad p_1 + p_2 \leq b \\ p_1 - cp_1 & , \quad p_1 + p_2 > b \end{cases} \tag{6}$$

$$L_2 = \begin{cases} \frac{p_2}{b} \times (b - p_1 - p_2) + p_2 - cp_2 & , \quad p_1 + p_2 \leq b \\ p_2 - cp_2 & , \quad p_1 + p_2 > b \end{cases} \tag{7}$$

Figure 3 is derived from formal (6)

When $p_1 + p_2 \leq b$ and $p_2 = 0$, $L_1$ achieves maximum under formula (8)

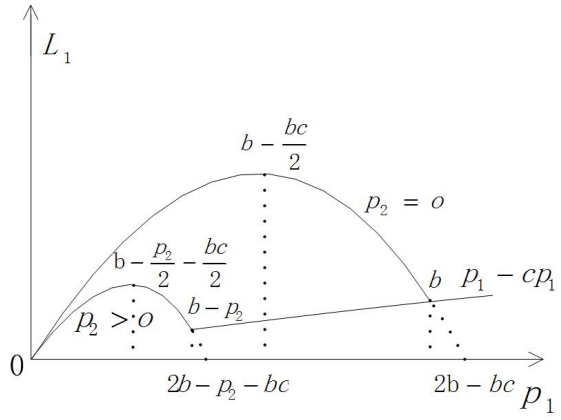


**Fig. 3.** Preference of $L_1$

$$p_1 = b - \frac{bc}{2} \tag{8}$$

When $p_1 + p_2 \leq b$ and $p_2 > 0$,$L_1$ achieves maximum under formula (9)

$$p_1 = b - \frac{p_2}{2} - \frac{bc}{2} \tag{9}$$

When $p_1 + p_2 \leq b$ and $p_1 = 0$,$L_2$ achieves maximum under formula (10)

$$p_2 = b - \frac{bc}{2} \tag{10}$$

When $p_1 + p_2 \leq b$ and $p_1 > 0$,$L_2$ achieves maximum under formula (11)

$$p_2 = b - \frac{p_1}{2} - \frac{bc}{2} \tag{11}$$

According to (9), we argue that when y-axis $L_1$ adopts the maximum value, x- axis depends on $p_2$

$$f_1(p_2) = \begin{cases} b - \frac{p_2}{2} - \frac{bc}{2} & , \quad p_2 \leq b \\ 0 & , \quad p_2 > b \end{cases} \tag{12}$$

According to (11), we argue that when y-axis $L_2$ adopts the maximum value, x- axis depends on $p_1$

$$f_2(p_1) = \begin{cases} b - \frac{p_1}{2} - \frac{bc}{2} & , \quad p_1 \leq b \\ 0 & , \quad p_1 > b \end{cases} \tag{13}$$

Based on Nash equilibrium, Figure 4 is derived from formal (12) and formal (13).When $L_1$ and $L_2$ adopt maximum at the same time, we have.

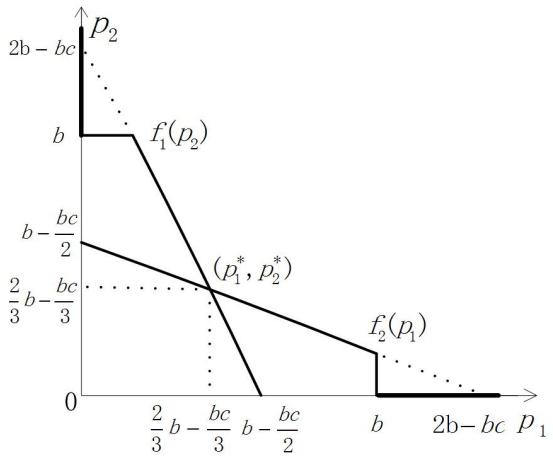


**Fig. 4.** Nash Equilibrium

$$p_1^* = p_2^* = \frac{2}{3}b - \frac{bc}{3} \tag{14}$$

According to the Theorem 1 and verification, We configure the concrete threshold for the node memory occupancy by two kinds of messages as $p_1^* = p_2^*$. This mechanism realizes the full share of node memory resource between existing messages in this node and messages which are about to be transferred to this node. It also makes the resource not overused by one party. This effectively defenses the attack of memory occupancy from malicious node. The active control to congestion caused by malicious node memory occupancy increases the system global message successful delivery ratio.

## 4 Evaluation

We leverage DTN-dedicated simulator THE ONE to do the simulation. NESD congestion control routing algorithm and encounter history based regular routing algorithm is compared in this paper. Meanwhile, network congestion ratio, message successful delivery ratio and message successful delivery cost are analyzed under the situation that memory is attacked through active consumption by a small quantity of malicious nodes.

The parameters in routing algorithm are set as table 2.

In order to prove the advantages of this algorithm in a limited testing time, we set more nodes, smaller nodes memory, faster node speed, more frequent message generation rate and larger message transfer speed. Thus, congestion control performance can be exhibited in short experiment time. And whether message is successfully delivered also can be exhibit promptly. It's beneficial to our evaluation to the algorithm performance.

**Table 2.** Simulation parameters

| **Parameter** | **Value** |
|---|---|
| Scenario length and width | 10000m |
| Hotspot area length and width | 4000m |
| Node number | 20 |
| Node memory | 3 MB |
| Node speed | 10 m/s |
| Communication radius | 50m |
| Message generation rate | 20 seconds per message |
| Message size | 500KB |
| Message transfer speed | 5000KB/s |

By the comparison of congestion ratio shown in Figure 5, we found that NESD congestion control routing algorithm significantly improves DTN network congestion compared to regular routing algorithm based on historical encounter information. It sets the concrete threshold for node memory occupancy to limit the node memory consumption from malicious node. The exhaustion of the whole encounter node memory in the attack of malicious node compels the attacked node to accept all the messages for transfer from malicious node. Since we set the same memory size for each node, this inevitably causes attacked node lose its' message for accepting all the messages from malicious node which results in congestion. The algorithm we design avoids the emergence of this problem and reduces the network congestion ratio.

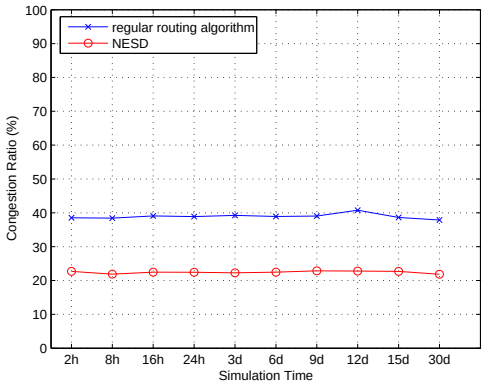


**Fig. 5.** Congestion ratio

By the comparison of successful delivery ratio shown in Figure 6, we found that NESD congestion control routing algorithm significantly increases message

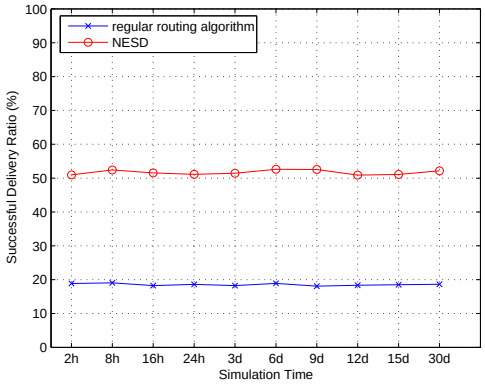


**Fig. 6.** Successful delivery ratio

successful delivery ratio. Node's message delivery in DTN mainly depends on the assistance of message transfer operation. More than one hop is needed to complete the successful delivery. But in the network with memory consumption attack from malicious node, messages are always forcefully deleted before the arrival at the destination node due to the memory exhaustion by malicious node's attack. This inevitably lessens the message successful delivery ratio. The algorithm we design limits the attack from malicious node and guarantees the necessary transfer operation of regular node for successful message delivery and the success ratio is also insured.

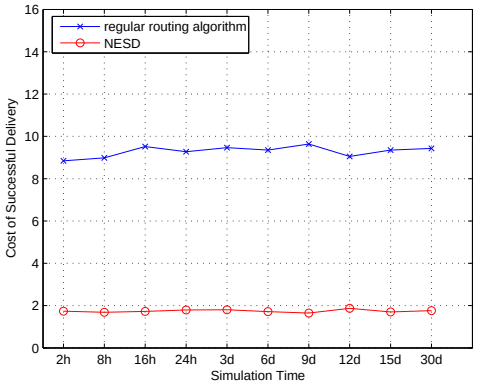


**Fig. 7.** Cast of successful delivery

By the comparison of the cost for message successful delivery in Figure 7, NESD congestion control routing algorithm significantly lessens cost of message successful delivery. In this experiment, we define the cost of message successful delivery as the delivery number to destination node divided by the number to un-destination node. Obviously, congestion and packet loss caused by malicious node attack increases the overall delivery number to un-destination node and lessens overall delivery number to destination node which increases the cost of message successful delivery. The constraint operation to the malicious node attack inevitably reduces the cost of message successful delivery.

## 5 Conclusion

Based on the conclusion of the main research work for DTN congestion control routing, this paper proposes NESD congestion control routing algorithm under the premise that there is memory consumption attack from malicious node. These also have significant application values in the field of homeland defense.This algorithm leverages Nash equilibrium in game theory by setting concrete threshold to tradeoff the node memory occupancy between existing messages in this node and messages which are about to be transferred to this node. The transfer operation for successful message delivery of regular node is guaranteed. Meanwhile, illegal occupancy of node memory from malicious node is constrained effectively. This algorithm improves the congestion degree and enhances message successful delivery ratio. This paper in detail proves existing messages in this node and messages which are about to be transferred to this node both can be transferred continually with high probability until coming into contact with the destination node. At the same time, the concrete threshold for the share of node memory by two-class messages is computed for achieving this target. And the high performance of this algorithm is proved by experiment.

We will continue the research on active defense mechanism to all kinds of attacks from malicious node. Message successful delivery ratio should be guaranteed. The mechanism also should perfect congestion control, optimize the defense result and effectively decrease the delivery latency of messages. In next step, we will discuss the effect of other attack behavior to DTN from malicious node and propose the corresponding defense measurement. The message successful delivery ratio should be guaranteed and congestion should be controlled effectively.

## Acknowledgement

The work described in this paper is partially supported by the grants of the National Basic Research Program of China (973 project) under Grant No.2009CB320503, 2012CB315906; the National 863 Development Plan of China under Grant No. 2009AA01A334, 2009AA01A346, 2009AA01Z423; and the project of National Science Foundation of China under grant No. 61070199, 61003301, 60903223, 60903224, 61103189, 61103194, 61103182; and supported by Program for Changjiang

Scholars and Innovative Research Team in University of the Ministry of Education("Network Technology",NUDT), the Innovative Research Team in University of Hunan Province("Network Technology",NUDT), and the Innovative Research Team of Hunan Provincial natural science Foundation(11JJ7003).

## References

1. DTNRG:Delay-tolerant networking research group. http://www.dtnrg.org
2. Pentland A. S., Fletcher R., Hasson A.:DakNet:Rethinking Connectivity in Developing Nations. In: Computer 37, 78-83 (2004)
3. Burgess J., Gallagher B., Jensen D., Levine B. N.:Maxprop: Routing for Vehicle-Based Disruption-tolerant Networks. In: Proceedings of INFOCOM, pp.1-11.Barcelona, Spain (2006)
4. Burleigh S., Hooke A., Torgerson L., Fall K., Cerf V., Durst B., Scott K.:Delay-tolerant Networking: an Approach to Interplanetary Internet'. In: IEEE Communications Magazine, 41(6):128.136 (2003)
5. Scott K., Burleigh S.:Bundle Protocol Specification. Internet RFC 5050 (2007)
6. Fall K., Hong W., Madden S.:Custody Transfer for Reliable Delivery in Delay Tolerant Networks. Technical Report, IRB-TR-03-030, Intel Research at Berkeley (2003)
7. Vahdat A., Becker D.:Epidemic routing for partially connected ad hoc networks. Technical Report, CS-2000-06, Duke University (2000)
8. Lindgren A., Doria A., Scheln O.:Probabilistic routing in intermittently connected networks. In: SIGMOBILE Mobile Computing Communications Review, 7(3):19-20 (2003)
9. Jain R., Ramakrishnan K. K.:Congestion Avoidance in Computer Networks with a Connectionless Network Layer:Concepts,Goals,and Methodology,Proc. In: IEEE Comp. Networking Symp., Washington, D.C., pp.134-143 (1988)
10. Seligman M., Fall K., Mundur P.:Storage routing for DTN congestion control. In: Wireless communications and mobile computing, 1183-1196 (2007)
11. Hollot C. V., Misra V., Towsley D., Gong W. B.:A Control Theoretic Analysis of RED. In: IEEE INFOCOM (2001)
12. Feng L., Jie W., Avinash S.:Thwarting Blackhole Attacks in Distruption-Tolerant Networks using Encounter Tickets. In: IEEE INFOCOM (2009)
13. Vivek N., Yi Y., Sencun Z.:Resource-Misuse Attack Detection in Delay-Tolerant Networks. In: Performance Computing and Communications Conference (IPCCC), 2011 IEEE 30th International (2011)
14. Martin J.:An Introduction to Game Theory. Oxford University Press (2004)
15. Spyropoulos T., Psounis K., Raghavendra CS.:Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks. In: Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant Networking(WDTN '05), New York, NY, USA, ACM, 252-259 (2005)
16. Spyropoulos T., Psounis K., Raghavendra CS.:Efficient routing in intermittently connected mobile networks:the multiple-copy case. In: IEEE/ACM Trans, on Network, 16(1), 77-90 (2008)
17. Zhao W., Ammar M., Zegura E.:A message ferrying approach for data delivery in sparse mobile ad hoc networks. In: Proc.of the ACM Mobihoc, 187-198 (2004)
18. Costa P., Mascolo C., Musolesi M., Picco GP.:Socially-Aware routing for publish-subscribe in delay-tolerant mobile ad hoc networks. In: IEEE Journal of Selected Areas in Communication, 26(5):748-760 (2008)

19. Floyd S., Jacobson V.:Random Early Detection Gateways for Congestion Avoidance. In: IEEE/ACM Transactions on Networking (1993)
20. Seligman M., Fall K., Mundur P.:Alternative Custodians for Congestion Control in Delay Tolerant Networks. In: SIGCOMM Workshops, Pisa, Italy (2006)
21. Chiu D. M., Jain R.:Analysis of the Increase and Decrease Algorithms for Congestion Avoidance in Computer Networks. In: Comput.Networks ISDN Sys., vol.17, pp.1-14 (1989)
22. Nishiyama H., Ansari N., Kato N.:Wireless Loss-tolerant Congestion Control Protocol Based on Dynamic Aimd Theory. In: IEEE Wireless Communications, 1536-1284 (2010)
23. Godfrey P. B., Schapira M., Zohar A., Shenker S.:Incentive Compatibility and Dynamics of Congestion Control. In: SIGMETRICS, New York, USA (2010)
24. Firoiu V., Borden M.:A Study of Active Queue Management for Congestion Control. In: IEEE INFOCOM (2000)
25. Paganini F., Wang Z. k., Doyle J. C., Low S. H.:Congestion Control for High Performance,Stability,and Fairness in General Networks. In: IEEE/ACM Transactions on Networking, 13, 43-56 (2005)
26. Karl Andersson: Interworking Techniques and Architectures for Heterogeneous Wireless Networks. In: Journal of Internet Services and Information Security, vol.2, pp. 22-48 (2012)
27. Charles J. Z, Turgay K.: A Comparative Review of Connectivity-Based Wireless Sensor Localization Techniques. In: Journal of Internet Services and Information Security, vol.2, pp. 59-72 (2012)
28. Jingbo Sun, Yue Wang, Hongbo Si, et.al: Aggregate Human Mobility Modeling Using Principal Component Analysis. In: Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, vol.1, pp. 83-95 (2010)