ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Handling Flood Attacks in Disruption Tolerant Networks Based On Claim Verification

G. Pushpa Rega[1]

Department of Computer Science and Engineering, Syed Ammal Engineering College, Ramanathapuram, Tamilnadu, India[1]

ABSTRACT— Disruption Tolerant Networks (DTNs) utilize the mobility of nodes and the opportunistic contacts among nodes for data communications. Due to the limitation in network resources such as contact opportunity and buffer space, DTNs are vulnerable to flood attacks. Rate limiting was proposed to defend against flood attacks in DTNs, such that each node has a limit over the number of packets that it can generate in each time interval and a limit over the number of replicas that it can generate for each packet. Here detection adopted claim-carry-and check: each node itself counts the number of packets or replicas that it has sent and claims the count to other nodes; the receiving nodes carry the claims when they move and cross-check if their carried claims are inconsistent when they contact. Using Rate limit certificate only the flood attacker who exceeds the rate limit was identified. To overcome this proposed approach uses key. Key will be generated for the node who wishes to send packets less than the rate limit. The key Generation based on AES algorithm. Based on keys, attackers who sends packet within the rate limit can also be easily identified.

KEYWORDS— DTN, security, flood attack, detection, Key

I. INTRODUCTION

Disruption Tolerant Networks (DTNs) consist of mobile nodes carried by human beings, vehicles, etc. DTNs enable data transfer when mobile nodes are only intermittently connected, making them appropriate for applications where no communication infrastructure is available such as military scenarios and rural areas. Due to lack of consistent connectivity, two nodes can only exchange data when they move into the transmission range of each other (which is called a contact between them).DTNs employ such contact opportunity for data forwarding with "store-carry-and-forward"; i.e., when a node receives some packets, it stores these packets in its buffer, carries them around until it contacts another node, and then forwards them. Since the contacts between nodes are opportunistic and the duration of a contact may be short because of mobility, the usable bandwidth which is only available during the opportunistic contacts is a limited resource. Also, mobile nodes may have limited buffer space. Due to the limitation in bandwidth and buffer space, DTNs is vulnerable to flood attacks. In flood attacks, maliciously or selfishly motivated attackers inject as many packets as possible into the network, or instead of injecting different packets the attacker's forward replicas of the same packet to as many nodes as possible. For convenience, we call the two types of attack packet flood attack and replica flood attack, respectively. Flooded packets and replicas can waste the precious bandwidth and buffer resources, prevent benign packets from being forwarded and thus degrade the network service provided to good nodes. Moreover, mobile nodes spend much energy on transmitting/receiving flooded packets and replicas which may shorten their battery life. Therefore, it is urgent to secure DTNs against flood attacks.

Although many schemes have been proposed to defend against flood attacks on the Internet and in wireless sensor networks, they assume persistent connectivity and cannot be directly applied to DTNs that have intermittent connectivity. In DTN Rate limiting was employed to defend against flood attacks in DTNs. In this approach, each node has a limit over the number of packets that it, as a source node, can send to the network in each time interval. Each node also has a limit over the number of replicas that it can generate for each packet (i.e., the number of nodes that it can forward each packet to). The two limits are used to mitigate packet flood and replica flood attacks, respectively. If a node violates its rate limits, it will be detected and its data traffic will be filtered. In this way, the amount of flooded traffic can be controlled.

Here main objective is to detect if a node has violated its rate limits. Although it is easy to detect the violation of rate limit on the Internet and in telecommunication networks where the egress router and base station can account each user's traffic, it is challenging in DTNs due to lack of communication infrastructure and consistent connectivity. Since a node moves around and may send data to any contacted node, it is very difficult to count the number of packets or replicas sent out by this node. Basic idea of detection is claim carry-and-check. Each node itself counts the number of packets or replicas that it has sent out, and claims the count to other nodes; the receiving nodes carry the claims around when they move, exchange some claims when they contact, and cross-check if these claims are inconsistent. If an attacker floods more packets or replicas than its limit, it has to use the same count in more than one claim according to the pigeonhole principle and this inconsistency may lead to detection. Using this techniques, only Attackers who exceeds the rate limit can be identified. Key based approaches will be used to detect all kind of attackers.

Based on this idea, we use different cryptographic constructions to detect packet flood and replica flood attacks. Because the contacts in DTNs are opportunistic in nature, our approach provides probabilistic detection. The more traffic an attacker floods, the more likely it will be detected. The detection probability can be flexibly adjusted by system parameters that control the amount of claims exchanged in a contact. We provide a lower and upper bound of detection probability and investigate the problem of parameter selection to maximize detection probability under a certain amount of exchanged claims. The effectiveness and efficiency of our scheme are evaluated with extensive trace-driven simulations.

II. LITERATURE REVIEW

1)A Delay-Tolerant Network Architecture for Challenged Internets

The existing TCP/IP based Internet operates on a principle of providing end-to-end inter-process communication using a concatenation of potentially dissimilar link-layer technologies. The standardization of the IP protocol and its mapping into network-specific link-layer data frames at each router as required supports interoperability using a packet-switched model of service. Although often not explicitly stated, a number of key assumptions are made regarding the overall performance characteristics of the underlying links in order to achieve smooth operation: an end-to-end path exists between a data source and its peer(s), the maximum round-trip time between any node pairs in the network is not excessive, and the end-to-end packet drop probability is small. Unfortunately, a class of so-called challenged networks, which may violate one or more of the assumptions, are becoming important and may not be well served by the current end-to-end TCP/IP model. Challenged networks arise primarily as a result of various forms of host and router mobility, but may also come into being as a result of disconnection due to power management or interference.

The highly successful architecture and supporting protocols of today's Internet operate poorly when faced with operating environments characterized by very long delay paths and frequent network partitions. These problems are exacerbated by end nodes that have severe power or memory constraints. Often deployed in mobile and extreme environments lacking "always-on" infrastructure, many such networks have their own specialized protocols, and do not utilize IP.

To achieve interoperability between them, we propose a network architecture and application interface structured around optionally-reliable asynchronous message forwarding, with limited expectations of end-to-end connectivity and node resources. The architecture operates as an overlay above the transport layers of the networks it interconnects, and provides key services such as in-network data storage and retransmission, interoperable naming, authenticated forwarding and a coarse-grained class of service.

2) Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs

A Mobile Ad hoc Network (MANET) is a dynamic wireless network with or without fixed infrastructure. Nodes may move freely and organise themselves arbitrarily. Sparse Mobile Ad hoc Networks are a class of Ad hoc networks where node density is low, and contacts between the nodes in the network do not occur very frequently. As a result, the network graph is rarely, if ever, connected and message delivery must be delay-tolerant. Traditional MANET routing protocols make the assumption that the network graph is fully connected and fail to route messages if there is not a complete route from source to destination at the time of sending. For this reason traditional MANET routing protocols cannot be used in sparse MANETs. To overcome this issue, node mobility is exploited to physically carry messages between disconnected parts of the network. These schemes are sometimes referred to as mobility assisted routing that employ the store-carry-and-forward model. Mobility-assisted routing consists of each node independently making forwarding decisions that take place when two nodes meet. A message gets forwarded to encountered nodes until it reaches its destination. Here the use of social network analysis techniques proposed in order to forward data in a disconnected delay-tolerant MANET.

Social networks exhibit the small world phenomenon which comes from the observation that individuals are often linked by a short chain of acquaintances.Message delivery in sparse Mobile Ad hoc Networks (MANETs) is difficult due to the fact that the network graph is rarely (if ever) connected. A key challenge is to find a route that can provide good delivery performance and low end-to-end delay in a disconnected network graph where nodes may move freely. This paper presents a multidisciplinary solution based on the consideration of the so called small world dynamics which have been proposed for economy and social studies and have recently revealed to be a successful approach to be exploited for characterizing information propagation in wireless networks. To this purpose, some bridge nodes are identified based on their centrality characteristics, i.e., on their capability to broker information exchange among otherwise disconnected nodes.

Due to the complexity of the centrality metrics in populated networks the concept of ego networks is exploited where nodes are not required to exchange information about the entire network topology, but only locally available information is considered. Then SimBet Routing is proposed which exploits the exchange of preestimated 'betweenness' centrality metrics and locally determined social 'similarity' to the destination node. We present simulations using real trace data to demonstrate that SimBet Routing results in delivery performance close to Epidemic Routing but with significantly reduced overhead. Additionally, we show that SimBet Routing outperforms PRoPHET Routing, particularly when the sending and receiving nodes have low connectivity.

3) Mitigating Routing Misbehavior in Disruption Tolerant Networks

In DTNs, a node may misbehave by dropping packets even when it has sufficient buffers. Routing misbehaviour can be caused by selfish nodes that are unwilling to spend resources such as power and buffer on forwarding packets of others, or caused by malicious nodes that drop packets to launch attacks. Routing misbehaviour will significantly reduce the packet delivery ratio and waste the resources of the mobile nodes that have carried and forwarded the dropped packets. In this paper, we address routing misbehaviour in DTNs by answering two questions: how to detect packet dropping and how to limit the traffic flowing to the misbehaving nodes. We first propose a scheme which detects packet dropping in a distributed manner. In this scheme, a node is required to keep previous signed contact records such as the buffered packets and the packets sent or received, and report them to the next contact node which can detect if the node has dropped packets based on the reported records. Misbehaving nodes may falsify some records to avoid being detected, but this will violate some consistency rules. To detect such inconsistency, a small part of each contact record is disseminated to some selected nodes which can collect appropriate contact records and detect the misbehaving nodes with certain probability. A mitigating scheme is proposed for routing misbehaviour by limiting the number of packets forwarded to the misbehaving nodes.

In disruption tolerant networks(DTNs),selfish or malicious nodes may drop received packets. Such routing misbehavior reduces the packet delivery ratio and wastes system resources such as power and bandwidth. Although techniques have been proposed to mitigate routing misbehavior in mobile ad hoc networks, they cannot be directly applied to DTNs because of the intermittent connectivity between nodes. To address the problem, we propose a distributed scheme to detect packet dropping in DTNs.Here a node is required to keep a few signed contact records of its previous contacts, based on which the next contacted node can detect if the node has dropped any packet. Since misbehaving nodes may misreport their contact records to avoid being detected, a small part of each contact record is disseminated to a certain number of witness nodes, which can collect appropriate contact records and detect the misbehaving nodes. We also propose a scheme to mitigate routing misbehavior by limiting the number of packets forwarded to the misbehaving nodes. Trace-driven simulations show that our solutions are efficient and can effectively mitigate routing misbehavior.

4) Multicasting in Delay Tolerant Networks: A Social Network Perspective

Node mobility and end-to-end disconnections in Delay Tolerant Networks (DTNs) greatly impair the effectiveness of data dissemination. Although social-based approaches can be used to address the problem, most existing solutions only focus on forwarding data to a single destination. In this paper, we are the first to study multicast in DTNs from the social network perspective. We study multicast in DTNs with single and multiple data items, investigate the essential difference between multicast and unicast in DTNs, and formulate relay selections for multicast as a unified knapsack problem by exploiting node centrality and social community structures. Extensive trace-driven simulations show that our approach has similar delivery ratio and delay to the Epidemic routing, but can significantly reduce the data forwarding cost measured by the number of relays used. In this paper, we focus on improving the cost-effectiveness of multicast in DTNs by exploiting the two key concepts in Social Network Analysis, i.e., centrality and communities. We aim at minimizing the multicast cost, in terms of the number of relays used, given the required delivery ratio and time constraint. We first consider multicasting a single data item to the network, and then generalize the problem to multiple data items with node buffer constraints.
Our detailed contributions are as follows:
• We develop analytical models for multicast relay selection using social network concepts.
• We formulate the relay selections for single-data and multiple data multicast in DTNs as a unified knapsack problem.

III. EXISTING SYSTEM

Disruption Tolerant Networks (DTNs) consist of mobile nodes carried by human beings, vehicles, etc. DTNs enable data transfer when mobile nodes are only intermittently connected, making them appropriate for applications where no communication infrastructure is available..Due to the limitation in network resources such as contact opportunity and buffer space, DTNs are vulnerable to flood attacks. Rate limiting was proposed to defend against flood attacks in DTNs, such that each node has a limit over the number of packets that it can generate in each time interval and a limit over the number of replicas that it can generate for each packet. Here detection adopted claim-carry-and check

Packet Flood Detection

To detect the attackers that violate their rate limit L, we must count the number of unique packets that each node as a source has generated and sent to the network in the current interval. The node itself count the number of unique packets that it, as a source, has sent out, and claim the up-to-date packet count (together with a little auxiliary information such as its ID and a timestamp) in each packet sent out. The node's rate limit certificate is also attached to the packet, such that other nodes receiving the packet can learn its authorized rate limit L. If an attacker is flooding more packets than its rate limit, it has to dishonestly claim a count smaller than the real value in the flooded packet, since the real value is larger than its rate limit and thus a clear indicator of attack. The claimed count must have been used before by the attacker in another claim, which is guaranteed by the pigeonhole principle, and these two claims are inconsistent. The nodes which have received packets from the attacker carry the claims included in those packets when they move around. When two of them contact, they check if there is any inconsistency between their collected claims. The attacker is detected when an inconsistency is found.

Replica Flood Detection

Claim-carry-and-check can also be used to detect the attacker that forwards a buffered packet more times than its limit l. Specifically, when the source node of a packet or an intermediate hop transmits the packet to its next hop, it claims a transmission count which means the number of times it has transmitted this packet (including the current transmission). Based on if the node is the source or an intermediate node and which routing protocol is used, the next hop can know the node's limit l for the packet, and ensure that the claimed count is within the correct range.

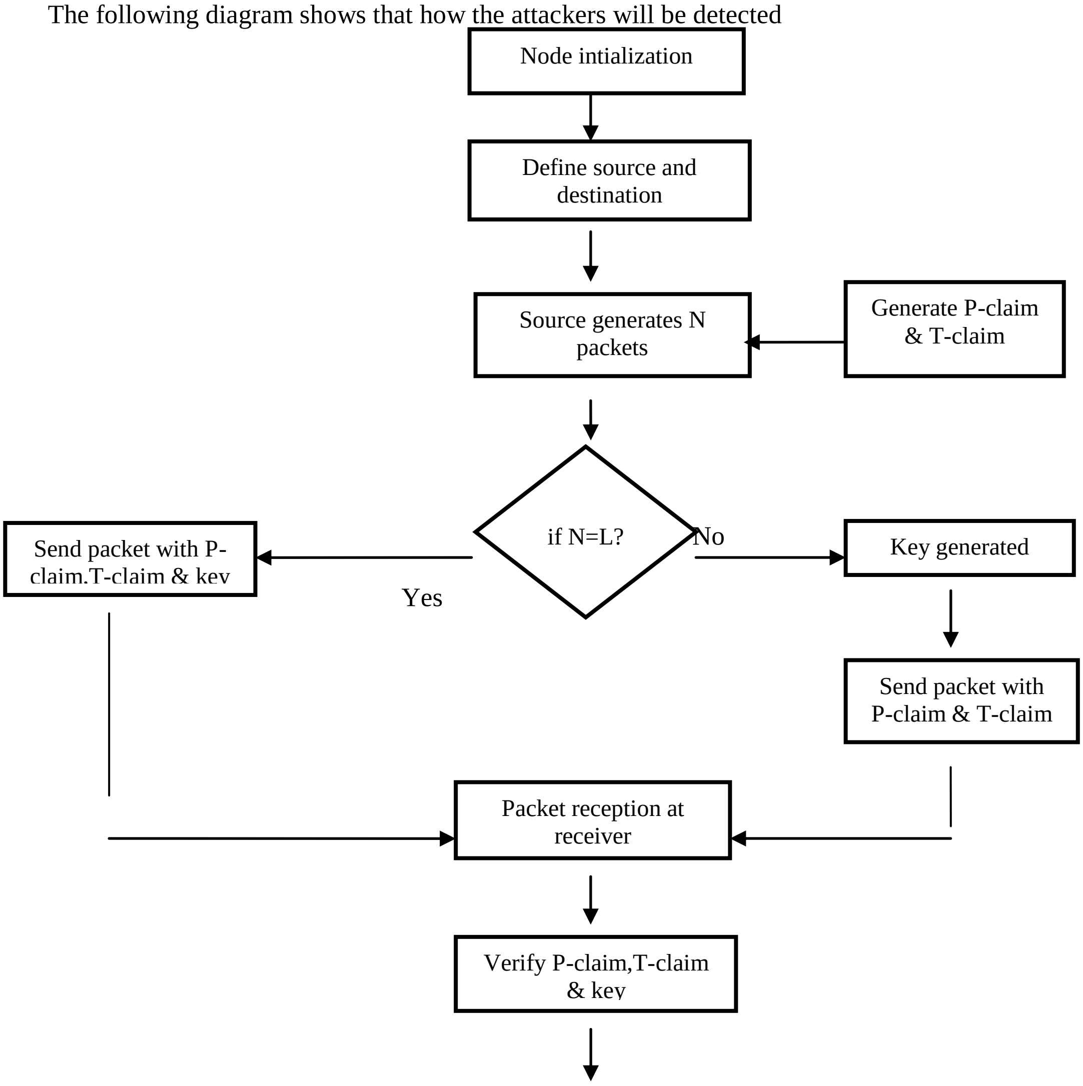
IV. PROPOSED SYSTEM

In the existing system, we can identify only the attackers who exceed the rate limit with the help of rate limit certificate. But if they sends packet within the rate limit, they won't be identified in the Disruption Tolerant Networks .So as to identify that kind of attacks we are going to use key. If the original user sends packet less than rate limit value, then they have to generate key with that packet count. So that key is transferred to each and every node along with the packets. At the receiver side Rate limit certificate and key will be checked. Based on the key, we can easily identify the attackers who sending unwanted packets within the rate limit. The key will be generated based on AES algorithm.

Advantages of Proposed System

By using keys, Attackers who send packets within the rate limit can be easily identified
In this system, Network efficiency and its performance can be improved by identifying attackers using keys.
Network bandwidth and buffers can be efficiently used.
Most of the packets will be prevented from loss.

The following diagram shows that how the attackers will be detected


Node intialization
Define source and destination
Source generates N packets
Generate P-claim & T-claim
if N=L?
No
Yes
Send packet with P-claim.T-claim & key
Key generated
Send packet with P-claim & T-claim
Packet reception at receiver
Verify P-claim,T-claim & key

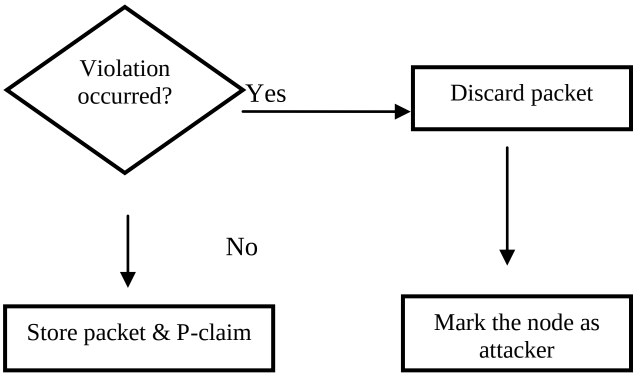


Fig. 1.Flow diagram

To improve the efficiency in network utilization and to detect the attackers, the following components are required
Node création & packet Generation

In this process, the sample network formation is created. The dynamic network formation is based on node creation & node connection in MANET. The node creation is based on set of node deployment. After the node deployment, the connections are provided. We study the problem of transmitting a large file over paths of potentially many hops, and seek optimal ways of splitting the file into a large number of packets over multiple paths, each with different operating parameters over its hops, to minimize the end-to-end delay. The form of delay we consider consists primarily of random queueing delay and transmission delay at each intermediate hops. The file which is to be transfer is to be selected & it is splitted into number of packets for data transmission. The splitting process is based on file length , according to that the files are splitted.

Trusted Authority

When a user joins the network, the user requests for a rate limit from a trusted authority which acts as the network operator. In the request, this user specifies an appropriate value of L based on prediction of user file size. If the trusted authority approves this request, it issues a rate limit certificate to this user, which can be used by the user to prove to other nodes the legitimacy of her rate limit. When a user predicts an increase (decrease) of her demand, she can request for a higher (lower) rate limit. The request and approval of rate limit may be done offline. The flexibility of rate limit leaves legitimate users' usage of the network unhindered. So that the certificate is verified, & send to user.

Claim Détection

Claim-carry-and-check can also be used to detect the attacker that forwards a buffered packet more times than its limit. Specifically, when the source node of a packet or an intermediate hop transmits the packet to its next hop, it claims a transmission count which means the number of times it has transmitted this packet (including the current transmission). Based on if the node is the source or an intermediate node and which routing protocol is used, the next hop can know the node's limit for the packet, and ensure that the claimed count is within the correct range. Thus, if an attacker wants to transmit the packet more than its limit, it must claim a false count which has been used before. Similarly in packet flood attacks, the attacker can be detected.

Flood Detection

To detect the attackers that violate their rate limit L, we must count the number of unique packets that each node as a source has generated and sent to the network in the current interval. Main idea is to let the node itself count the number of unique packets that it, as a source, has sent out, and claim the up-to-date packet count (together with a little auxiliary information such as its ID and a timestamp) in each packet sent out. The node's rate limit certificate is also attached to the packet, such that other nodes receiving the packet can learn its authorized rate limit L. If an attacker is flooding more packets than its rate limit, it has to dishonestly claim a count smaller than the real value in the flooded packet, since the real value is larger than its rate limit and thus a clear indicator of attack. The claimed count must have been used before by the attacker in another claim, which is guaranteed by the pigeonhole principle, and these two claims are inconsistent. The nodes which have received packets from the attacker carry the claims included in those packets when they move around. When two of them contact, they check if there is any inconsistency between their collected claims. The attacker is detected when an inconsistency is found.In the same way replica attackers also identified. Based on AES, key will be generated for the node who wish to send packet within their rate limit,Then attackers will be identified based on rate limit certificate and key.

Performance Evaluation

In this module, the performance of the algorithm is evaluated by using Graph representation. This shows that the proposed framework is able to adapt to changes in time & cost parameter values while the other approaches cannot. Since in the real world, it is uncommon that the same entity instances are recorded in a large number of data sources, and the costs are typically different. The performance gap between the proposed framework and other approaches is at the high level compare to other approaches. It provides better flexibility in the query processing process.

V. CONCLUSION AND FUTURE WORKS

Rate Limiting technique is used to mitigate flood attacks in DTNs using Rate limit Certificates from the Trusted Authority, and proposed a scheme which exploits claim-carry-and-check to probabilistically detect the violation of rate limit in DTN environments. Our scheme uses efficient constructions to keep the computation, communication and storage cost low. It works in a distributed manner, not relying on any online central authority or infrastructure, which well fits the environment of DTNs. Besides, it can tolerate a small number of attackers to collude.

In future work, in order to identify attacker who sends packet within the rate limit and to improve resource utilization, Key based security will be used along with Rate Limiting technique to increase efficiency in resource utilization.AES algorithm going to be used for key generation.

REFERENCES

[1] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. ACM SIGCOMM, pp. 27-34, 2003.

[2] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot, "Pocket Switched Networks and Human Mobility in Conference Environments," Proc. ACM SIGCOMM, 2005.

[3] M. Motani, V. Srinivasan, and P. Nuggehalli, "PeopleNet:
Engineering a Wireless Virtual Social Network," Proc. MobiCom, pp. 243-257, 2005.

[4] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.

[5] S.J.T.U.Grid Computing Center, "Shanghai Taxi Trace Data," http://wirelesslab.sjtu.edu.cn/, 2012.

[6] J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.

[7] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE First Int'l Workshop Sensor Network Protocols and Applications, 2003.

[8] E. Daly and M. Haahr, "Social Network Analysis for Routing in Disconnected Delay-Tolerant MANETs," Proc. MobiHoc, pp. 32-40, 2007.

[9] W. Gao, Q. Li, B. Zhao, and G. Cao, "Multicasting in Delay Tolerant Networks: A Social Network Perspective," Proc. ACM MobiHoc, 2009.

[10] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Distruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM, 2009.

[11] Y. Ren, M.C. Chuah, J. Yang, and Y. Chen, "Detecting Wormhole Attacks in Delay Tolerant Networks," IEEE Wireless Comm. Magazine, vol. 17, no. 5, pp. 36-42, Oct. 2010.

[12] U. Shevade, H. Song, L. Qiu, and Y. Zhang, "Incentive-Aware Routing in DTNS," Proc. IEEE Int'l Conf. Network Protocols (ICNP '08), 2008.

[13] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.

[14] H. Zhu, X. Lin, R. Lu, X.S. Shen, D. Xing, and Z. Cao, "An Opportunistic Batch Bundle Authentication Scheme for Energy Constrained DTNS," Proc. IEEE INFOCOM, 2010.

[15] B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, and A. Snoeren, "Cloud Control with Distributed Rate Limiting," Proc. ACM SIGCOMM, 2007.

[16] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," Proc. IEEE INFOCOM, 2010.