PMDS: A Probabilistic Misbehavior Detection Scheme in DTN

Zhaoyu Gao[†], Haojin Zhu[†], Suguo Du[†], Chengxin Xiao[†] and Rongxing Lu[‡]
[†]Shanghai Jiao Tong University, Shanghai 200240, P. R. China
{gaozy1987, xcxjack}@gmail.com, {zhu-hj, sgdu}@sjtu.edu.cn
[‡]University of Waterloo, Waterloo, Ontario, Canada
rxlu@bbcr.uwaterloo.ca

Abstract—**Malicious and selfish behaviors represent a serious threat against routing in Delay or Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN represents a great challenge. In this paper, we propose PMDS, a probabilistic misbehavior detection scheme, for secure DTN routing. The basic idea of PMDS is introducing a periodically available Trusted Authority (TA), which judges the node's behavior based on the collected routing evidences. We model PMDS as the Inspection Game and use game theoretical analysis to demonstrate that, by setting an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. To further improve the efficiency of the proposed scheme, we correlate detection probability with a node's reputation, which allows a dynamic detection probability determined by a node's reputation. The extensive analysis and simulation results show that the proposed scheme substantiates the effectiveness and efficiency of the proposed scheme.**

Keywords – **DTN, Security, Punishment and Compensation, Inspection Probability**

I. Introduction

Most current networking protocols have been designed with the assumption that an end-to-end path between the packet source and the destination is almost always available. If connectivity is interrupted, then routing protocols would provide an alternative path after at most a transient outage. This is also assumed for emerging wireless Mobile Ad-hoc NETworks (MANETs). However, there is an entire class of wireless networks for which this assumption does not hold. For wireless networks with intermittent connectivity, also called Delay or Disruption Tolerant Networks (DTNs), lack of continuous connectivity, network partitioning and very long delays are actually the norm, not the exception. Such networks have recently received an increasing interest due to their great potential for supporting applications deployed in challenged environments, such as vehicular networks [1], wireless social networks [2], pocket switched networks [3] and *etc*.

The recent studies show that the Byzantine (insider) adversary may pose a serious threat against DTN to compromise the network performance [4]. A Byzantine adversary (i.e., a physically captured and controlled legitimate node) can do serious damage to the network in terms of data availability, latency, and throughput. The typical examples of Byzantine attack include dropping, modifying the legitimate packets and injecting fake packets. Further, even for the non-malicious nodes, the rational (selfish) nodes may also try to maximize their own benefits by enjoying the services provided by the DTN network and, at the same time, refusing to relay the bundles for others [5].

Recently, there are quite a few proposals for reputation based or credit based incentive schemes in DTN [4]–[7]. However, it is observed that most of existing literatures are based on forwarding history verification, (e.g. multi-layered credit [5], [6], three-hop feedback mechanism [4], or encounter ticket [7]), which are costly in terms of transmission overhead and verification cost. The security overhead incurred by forwarding history checking is critical for a DTN since expensive security operations will be translated into more energy consumptions, which represents a fundamental challenge in resource-constrained DTN. Further, even from the Trusted Authority (TA) point of view, misbehavior detection in DTNs will inevitably incur a high security overhead, which may include the cost of collecting the forwarding history evidence via deployed *judgenodes* [4] and transmission cost to TA. Therefore, an efficient and adaptive misbehavior detection and reputation management scheme is highly desirable in DTN.

In this paper, we propose PMDS, a Probabilistic Misbehavior Detection Scheme for DTN, to adaptively detect misbehaviors in DTN and achieve the tradeoff between the detection cost and the detection performance. PMDS is motivated from the *Inspection Game* [8], which is a game theory model in which an inspector verifies if an another party, called inspectee, adheres to certain legal rules. In this model, the inspectee has a potential interest in violating the rules while the inspector may have to perform the partial verification due to the limited verification resources. Therefore, the inspector could take advantage of partial verification and corresponding punishment to discourage the misbehaviors of inspectees. Furthermore, the inspector could check the inspectee with a higher probability than the Nash Equilibrium points to prevent the offences, as the inspectee must choose to comply the rules due to its rationality.

Inspired by *Inspection Game*, to achieve tradeoff between the security and detection cost, PMDS introduces a periodically available Trust Authority (TA), which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then thus TA could punish or compensate the node based on its behaviors. To further improve the performance of the proposed probabilistic inspection scheme, we introduced a reputation system, in which the inspection probability could vary along with the target node's reputation. Under the reputation system, a node with a good reputation will be checked with a lower probability while a bad reputation node could be checked with a higher probability. We model PMDS as the Inspection Game and use game theoretical analysis to demonstrate that TA could ensure the security of DTN routing at a reduced cost via choosing an appropriate investigation probability.

The remainder of this paper is organized as follows. In Section II, we present the system model, adversary model considered throughout the paper. In Section III we proposed the basic PMDS and the analyze from the perspective of game theory. The simulation of PMDS is given in Section IV, followed by the conclusion in Section V.

II. PRELIMINARY

A. System Model

In this paper, we adopt the system model similar to [5]. We consider a normal DTN consisted of mobile devices owned by individual users. Each node i is assumed to have a unique ID N_i and a corresponding public/private key pair. We assume that each node must pay a deposit C before it joins the network, and the deposit will be paid back after the node leaves if there is no offend activity of the node. Similar to [10], we assume that a periodically available TA exists so that it could take the responsibility of misbehavior detection in DTN. For a specific detection target N_i, TA will request N_i's forwarding history in the global network. Therefore, each node will submit its collected N_i's forwarding history to TA via two possible approaches. In a pure peer-to-peer DTN, the forwarding history could be sent to some special network components (e.g., roadside unit (RSU) in vehicular DTNs or judgenodes in [4]) via DTN transmission. In some hybrid DTN network environment, the transmission between TA and each node could be also performed in a direct transmission manner (e.g., WIMAX or cellular networks [11]). We argue that since the misbehavior detection is performed periodically, the message transmission could be performed in a batch model, which could further reduce the transmission overhead.

B. Routing Model

We adopt the single-copy routing mechanism such as First Contact routing protocol, and we assume the communication range of a mobile node is finite. Thus a data sender out of destination node's communication range can only transmit packetized data via a sequence of intermediate nodes in a multihop manner. Our misbehaving detection scheme can be directly used but not limited in metric-based routing algorithms, such as MaxProp [12] and ProPHET [13].

C. Threat Model

First of all, we assume that each node in the networks is rational and a rational node's goal is to maximize its own profit. In this work, we mainly consider two kinds of DTN nodes: selfish nodes and malicious nodes. Due to the selfish nature and energy consuming, selfish nodes are not willing to forward bundles for others without sufficient rewarding. As an adversary, the malicious nodes arbitrarily drop others bundles (blackhole or greyhole attack), which often take place beyond others observation, leading to serious performance degradation. Note that any of the selfish actions above can be further complicated by the collusion of two or more nodes.

D. Design Requirements

The design requirements include

- *Distributed*:We require that a network authority responsible for the administration of the network is only periodically available and consequently incapable of monitoring the operational minutiae of the network.
- *Robust*: We require a misbehavior detection scheme that could tolerate various forwarding failures caused by various network environments.
- *Scalability*: We require a scheme that works irrespective of the size and density of the network.

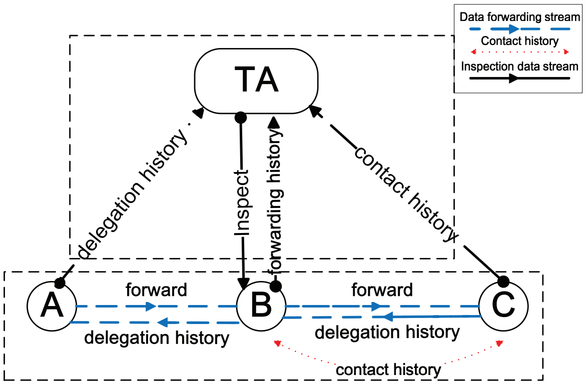


Fig. 1. In the Routing Evidence Generation Phase, A forwards packets to B ,then gets the delegation history back. B holds the packet and then encounters C. C gets the contact history about B. In the Auditing Phase, when TA decides to check B, TA will broadcast a message to ask other nodes to submit all the evidence about B, then A submits the delegation history from B, B submits the forwarding history (delegation history from C), C submits the contact history about B.

III. A Proposed Basic PMDS for DTN

In this section,we initially analyze the PMDS as a basic scheme, then we will explore the PMDS with a global reputation system.

A. Generation and Auditing of the Routing Misbehavior Detection Metrics

In the proposed misbehavior detection scheme, we further separate the whole misbehavior detection process into the Routing Evidence Generation Phase and Auditing phase.

1) Routing Evidence Generation Phase: For the simplicity of presentation, we take a three step data forwarding process as an example. Suppose that node A has packets to be delivered to node C. Now, if node A meets an another node B that could help to forward the packets to C, A will replicate and forward the packets to B. Thereafter, B will forward the packets to C when C arrives at the transmission range of B. In this process, we define three kinds of data forwarding evidences which could be used to judge if a node is a misbehavior or not:

- *Delegation Evidence $\mathcal{D}$*: After node A delegates the packet transmission task to B, B will generate a delegation evidence back to A, the evidence includes $\mathcal{D} = \{M, A, B, Dst, TS, Exp, Sig_B\}$, where M is the message, TS and Exp refer to the time stamp and the packets expiration date of the packets, respectively, Dst is the packets destination, Sig_B refers to the signature generated by B. So $\mathcal{D}_B$ is the set of routing tasks of B, which will be stored at node A.
- *Forwarding History Evidence $\mathcal{F}$*: If node B successfully forward the packets to node C, C will generate a forwarding history evidence to demonstrate that B has successfully finished a forwarding task. $\mathcal{F} = \{M, B, C, Dst, TS, Exp, Sig_C\}$, where Sig_C refers to the signature generated by node C to demonstrate the authenticity of this evidence. $\mathcal{F}$ is stored at node B.
- *Contact History Evidence $\mathcal{E}$*: Whenever B meets a new node E, a new contact history [14] evidence will be generated to demonstrate the contact of B and E as $\{B, E, TS, Sig_B, Sig_E\}$, where Sig_B refers to the signature generated by both of node B and E to demonstrate the authenticity of this evidence. Note that $\mathcal{E}$ will be stored at both of node B and E.

As shown in Fig.1, whenever node A forwards the packets to B, Delegation Evidence $\mathcal{D}$ is generated by B and sent to A. When B meets C, they will jointly generate the Contact History Evidence $\mathcal{E}$ and then a Forwarding History Evidence $\mathcal{F}$ will be generated by C towards B during the data transmission phase.

2) Auditing Phase: In the Auditing phase, TA will launch an investigation request towards node B in the global network. Then, each node will submit its collected Delegation Evidences and contact history evidences to TA. Node B will also submit its forwarding history evidences to TA. Note that Delegation Evidence represents the forwarding tasks, Contact History Evidence records the network environment constraints, and Forwarding History Evidence demonstrates the real data forwarding performed by node B. If B is an honest node, he will try his best to finish the forwarding tasks. So if we don't consider network constraints, $\mathcal{F}$ should fully match Delegation Task $\mathcal{D}$. However, in reality, node B may fail to finish all of the tasks due to the network constraints (e.g., lack of enough contacts). Therefore, to judge if a node is a misbehavior or not, we should take all of the three factors above into consideration.

Therefore, in the proposed scheme, TA judges if node B is a misbehavior or not by triggering the Algorithm 1. In this algorithm, we introduce **Find**, which takes $\mathcal{D}$, $\mathcal{E}$ as well as a specific routing protocol $\mathcal{R}$ as the input, and output the ideal forwarding candidates $\mathcal{W}$. Algorithm 1 will compare $\mathcal{W}$ and $\mathcal{F}$. If they match, B is a good node. Otherwise, it is malicious.

Algorithm 1: Judge(node i)

```
demand all the nodes (including node $i$) to provide
  evidence $\mathcal{D}, \mathcal{E}, \mathcal{F}$ about node $i$
$\mathcal{W}$=**Find**(*Delegation Evidence* $\mathcal{D}$, *Contact History
  Evidence* $\mathcal{E}$, *Routing Protocol* $\mathcal{R}$)
**if** $\mathcal{F} == \mathcal{W}$ **then**
    return 1
**else**
    return 0
**end if**
```

However, we notice that it may introduce a heavy load on TA to collect and audit various routing evidences. In the following, inspired by the inspection game, we will propose a basic probabilistic misbehavior detection scheme to reduce the detection overhead without compromising the system security.

B. The Basic Probabilistic Misbehavior Detection Scheme

Different from periodical detection, the proposed PMDS allows the TA to launch the misbehavior detection at a certain probability. Algorithm 2 shows the details of the proposed probabilistic misbehavior detection scheme. For a particular node i, TA will launch an investigation at the probability of p_b. If i could pass the investigation by providing the corresponding evidences, TA will pay node i a compensation w; otherwise, i will receive a punishment C (lose its deposit).

Algorithm 2: Basic PMDS

```
initialize the number of nodes $n$
**for** $i \leftarrow 1$ to $n$ **do**
    generate a random number $m_i$ from 1 to $10^n - 1$
    **if** $m_i/10^n < p_b$ **then**
        ask all the nodes (including node $i$) to provide
          evidence about node $i$
        **if** Judge(node $i$)==1 **then**
            pay node $i$ the compensation $w$
        **else**
            give a punishment $C$ to node $i$
        **end if**
    **else**
        pay node $i$ the compensation $w$
    **end if**
**end for**
```

In the follows, we will model the above described algorithm as an Inspection Game. And we will demonstrate that, by setting an appropriate detection probability threshold, we could achieve a lower detection overhead and still stimulate the nodes to forward the packets for other nodes.

TABLE I
THE PAYOFF MATRIX OF TA AND AN INDIVIDUAL NODE

		TA	
		I (p_b)	N ($1 - p_b$)
an individual node	O (p_f)	*-C, C-h*	*w, -w*
	F ($1 - p_f$)	*w-g, v-w-h*	*w-g, v-w*

C. Game Theory Analysis

Before presenting the detailed Inspection Game, we assume that the forwarding transmission costs each node g to forward a packet and, thus, each node will receive a compensation w from TA, if successfully passing TA's investigation; otherwise, it will receive a punishment C from TA. The compensation could be the virtual currency or credits issued by TA; on the other hand, the punishment could be the deposit previously given by users to TA. TA will also benefit from each successful data forwarding by gaining v, which could be charged from source node similar to [5]. In the auditing phase, TA checks each node with the same probability p_b. Since checking will incur a transmission cost h, TA has two strategies, inspecting (I) or not inspecting (N). Each node also has two strategies, forwarding (F) and offending (O). Therefore, we could have the Probabilistic Inspection Game as follows:

Definition *According to PMDS, the Probabilistic Inspection Game is*

$$G =< N, \{s_i\}, \{\pi_i\}, \{p_i\} >$$

- $N = \{a_0, a_1, ..., a_n\}$ *is the set of the players,* a_0 *donates TA and* a_i *donates node i.*
- $s_i = \{s_{i0}, s_{i1}, s_{i2}, ..., s_{iK}\}$ *is the strategy set of the player i,* $s_0 = \{I, N\}$*,* $s_i = \{F, O\}$*.*
- π_i *is the payoff of the ith player* a_i*, and it is measured by credit earnings.*
- p_i *is a mixed strategy for player i, and the probability distribution* $p_i = \{p_{i0}, p_{i1}, ..., p_{iK}\}$ *corresponds to the strategy set* s_i *of the player i, where* $0 \leq p_{ik} \leq 1$ *for* $k = 0, ..., K$ *and* $p_{i0} + \cdots + p_{iK} = 1$*. Specifically,* $p_0 = \{p_b, 1 - p_b\}$*,* $p_i = \{p_f, 1 - p_f\}$*,* p_b *donates inspection probability and* p_f *donates forwarding probability.*

Then we could get the payoff matrix shown in Table I, and we could use Theorem 1 to demonstrate that TA could maintain the network security with a low inspection cost by PMDS.

Theorem *1: If TA inspects at the probability of* $p_b = \frac{g+\varepsilon}{w+C}$ *in our Basic PMDS, a rational node must choose forwarding strategy, and the TA will get a higher profit than it checks all the nodes in the same round.*

Proof: This is a static game of complete information, though no dominating strategy exists in this game, there is a mixed Nash Equilibrium point according to the Table I as

$$(p_b, p_w) = (\frac{g}{w + C}, \frac{h}{w + C})$$

If the node chooses offending strategy, its payoff is

$$\pi_w(S) = -C \cdot \left(\frac{g + \varepsilon}{w + C}\right) + w \cdot \frac{g + \varepsilon}{w + C} = w - g - \varepsilon$$

If the node chooses forwarding strategy, its payoff is

$$\pi_w(W) = p_b \cdot (w - g) + (1 - p_b) \cdot (w - g) = w - g$$

The latter one is obviously larger than the previous one. Therefore, if TA chooses the checking probability $\frac{g+\varepsilon}{w+C}$, a rational node must choose the forwarding strategy.

Furthermore, if TA announces it will inspect at the probability $p_b = \frac{g+\varepsilon}{w+C}$ to every node, then its profit will be higher than it checks all the nodes, for

$$v - w - (\frac{g + \varepsilon}{w + C}) \cdot h > v - w - h \tag{1}$$

the latter part in the inequality means TA checks all the nodes.

■

Since the probability that a malicious node cannot be detected after k rounds is $(1 - \frac{g+\varepsilon}{w+C})^k \rightarrow 0, k \rightarrow \infty$. Thus it is almost impossible that a malicious node cannot be detected after a certain number of rounds. In the simulation section, we will show that the detected rate of malicious users is close to 100% with a proper detection rate, at the same time, the transmission cost is much lower than inspection without PMDS.

D. Inspection Based on Reputation

The previous analysis has shown that the basic PMDS is enough to assure the security. However, the basic scheme assumes the same detection probability for each node, which may not be desirable in practice. It is observed that a good node could be detected less frequently while a bad node should be inspected at a higher probability. Therefore, we could combine PMDS with a reputation system which correlates the detection probability with nodes' reputation.

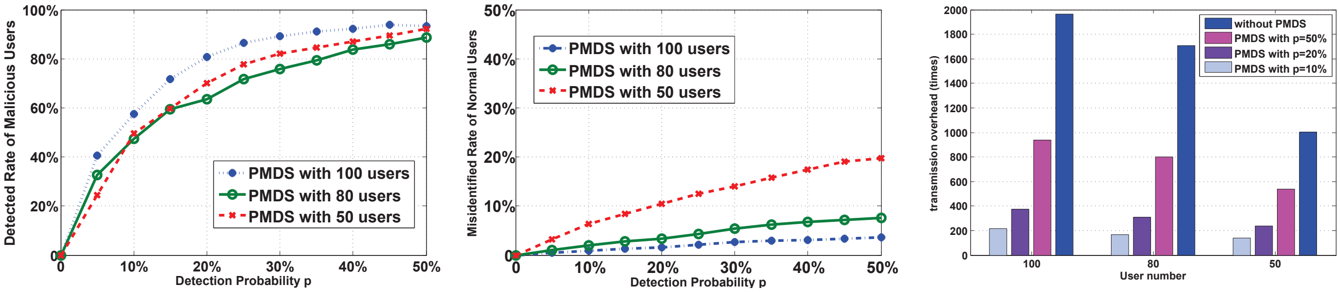
The reputation system of PMDS could update node's reputation r based on the last detection result, then the reputation could be used to determine the inspection probability p of the node. The inspection probability p should be the inverse function of reputation r. Note that, p must not be higher than the bound $\frac{g}{w+C}$ to assure the network security, which we have analyzed above. And based on the property of probability, it is obvious that p can not be larger than 1, which is the upper bound of detection probability. If the detection probability p for a particular node is 1, it means the node should always be detected, then it must be a malicious node.

With the help of the reputation system, PMDS will be enhanced and the detection efficiency will be improved. Furthermore, the reputation system could tolerate the transmission errors of a node with a reputation $r = 1$. What's important, a node with a lower reputation will lead to a higher inspection probability as well as a decrease of its expected payoff π_w. Due to the limitation of pages, the details of reputation system are discussed in our full paper.

IV. SIMULATION OF PMDS

We set up the experiment environment with the Opportunistic Networking Environment (The ONE) simulator [15], which is designed for evaluating DTN routing and application

Fig. 2. Experiment results with user number of 100, 80, 50



(a) Detected rate of malicious nodes

(b) false rate of misidentified nodes

(c) Transmission overhead incurred by PMDS

protocols. In our experiment, we adopt the First Contact routing protocol, which is a single-copy routing mechanism, and we use our campus (Shanghai Jiao Tong University Minhang Campus) map as the experiment environment.

We use the Packet Loss Rate (PLR) to describe the misbehavior level of a malicious node. In DTN, when a node's buffer is depleted, a new received bundle will be dropped by the node, and PLR denotes the rate between dropped bundles and received bundles. But a malicious node will pretend no more buffer for others and drop all the bundles it received. Thus PLR actually denotes a node's misbehavior level, e.g. if a node's PLR is 1, it is totally a malicious node; if a node's PLR is 0, we take it as a normal node. In our experiment, we set PLR=1. On the other hand, since a normal node may also be identified as malicious due to the depletion of its buffer, so we need to measure the false rate of such misidentified nodes to prove that PMDS has little impact on the normal users who adhere to the security and routing protocols. Finally, as we claimed, PMDS will incur a much lower transmission overhead than the system without PMDS, so we will evaluate and compare the transmission times of the system with and without PMDS.

We use Malicious Node Rate (MNR) to denote the proportion of the malicious nodes among all the nodes, and MNR is 10% in our experiment. We set the time interval t to be about 3 hours ($10800s$), and we run experiments with different numbers of nodes, such as 50, 80, 100, where the number of malicious nodes is 5, 8, 10 respectively. The detection probability p varies from 0 to 50%, and we run each case for 10 times. Then we compare the average results with and without PMDS, the experiment results are showed in Fig. 2.

Fig. 2(a) shows that when detection probability p is larger than 40%, PMDS could almost detect all the malicious nodes, where the detected rate of malicious nodes is close to 100%. It implies that PMDS could assure the security of the DTN in our simulation. Furthermore the misidentified rate of normal users is lower than 10% when user number is large enough, as showed in Fig. 2(b), which means that PMDS will not impact the activities of DTN users a lot. In fact, Fig. 2(c) indicates that PMDS will reduce much transmission overhead compared to the DTN without PMDS, that means PMDS will improve the detection performance of TA and save the transmission cost of the whole system.

V. Conclusion

In this paper, we propose a Probabilistic Misbehavior Detection Scheme (PMDS), which could reduce the detection overhead effectively. We model it as the Inspection Game and show that an appropriate probability setting could assure the security of the DTNs at a reduced detection overhead. Our simulation results confirm that PMDS will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively. Our future work will focus on the extension of PMDS to other kinds of networks.

References

[1] R. Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET-based Smart Parking Scheme for Large Parking Lots," in Proc. of *IEEE INFOCOM'09*, Rio de Janeiro, Brazil, April 19-25, 2009.

[2] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know The Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," in Proc. of *IEEE INFOCOM'10*, 2010.

[3] Q. Li, S. Zhu and G. Cao, "Routing in Socially Selfish Delay Tolerant Networks," in Proc. of *IEEE Infocom'10*, 2010.

[4] E. Ayday, H. Lee and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks," in *Milcom'10, 2010.*

[5] H. Zhu, X. Lin, R. Lu, Y. Fan and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," in *IEEE Transactions on Vehicular Technology,vol.58,no.8,pp.828-836,2009.*

[6] R. Lu, X. Lin, H. Zhu and X. Shen, "Pi: a practical incentive protocol for delay tolerant networks," in *IEEE Transactions on Wireless Communications,vol.9,no.4,pp.1483-1493,2010.*

[7] F. Li, A. Srinivasan and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks using Encounter Tickets," in Proc. of *IEEE INFOCOM'09*, 2009.

[8] D. Fudenburg and J. Tirole, "Game Theory," p17-18, *The MIT Press, Cambridge*, Massachusetts, London, England.

[9] M. Rayay, M. H. Manshaeiy, M. Flegyhziz and J. Hubauxy, "Revocation Games in Ephemeral Networks," in *CCS'08,2008*

[10] S. Reidt, M. Srivatsa and S. Balfe, "The Fable of the Bees:Incentivizing Robust Revocation Decision Making in Ad Hoc Networks," in *CCS'09, 2009*

[11] B. B. Chen and M. C. Chan, "Mobicent:a Credit-Based Incentive System for Disruption Tolerant Network," in *IEEE INFOCOM'2010.*

[12] J. Burgess, B. Gallagher, D. Jensen and B. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," In *Proc. of IEEE INFOCOM'06, 2006.*

[13] A. Lindgren and A. Doria, " Probabilistic Routing Protocol for Intermittently Connected Networks," draft-lindgren-dtnrg-prophet-03, 2007.

[14] P. Wang, Z. Gao, X. Xu, Y. Zhou, H. Zhu and K.Q. Zhu, "Automatic Inference of Movements from Contact Histories," in *Proc. of SIGCOMM'11, Poster*, 2011.

[15] A. Keranen, J. Ott and T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," in *SIMUTools 2009*, Rome, Italy.