A Probabilistic Misbehavior Detection Scheme towards Efficient Trust Establishment in Delay-tolerant Networks

Haojin Zhu, *Member, IEEE,* Suguo Du, Zhaoyu Gao, *Student Member, IEEE*, Mianxiong Dong, *Member, IEEE*, and Zhenfu Cao, *Senior Member, IEEE*

Abstract—Malicious and selfish behaviors represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs). Due to the unique network characteristics, designing a misbehavior detection scheme in DTN is regarded as a great challenge. In this paper, we propose iTrust, a probabilistic misbehavior detection scheme, for secure DTN routing towards efficient trust establishment. The basic idea of iTrust is introducing a periodically available Trusted Authority (TA) to judge the node's behavior based on the collected routing evidences and probabilistically checking. We model iTrust 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 the trust of the users. The extensive analysis and simulation results show that the proposed scheme substantiates the effectiveness and efficiency of the proposed scheme.

1 Introduction

Delay tolerant networks (DTNs), such as sensor networks with scheduled intermittent connectivity, vehicular DTNs that disseminate location-dependent information (e.g., local ads, traffic reports, parking information) [1], and pocket-switched networks that allow humans to communicate without network infrastructure, are highly partitioned networks that may suffer from frequent disconnectivity. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears (e.g., a new node moves into the range or an existing one wakes up). This message propagation process is usually referred to as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" fashion [2] [3].

In DTNs, a node could misbehave by dropping packets intentionally even when it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities) [4]. Routing misbehavior can be caused by selfish (or rational) nodes that try to maximize their own benefits by enjoying the services provided by DTN while refusing to forward the bundles for others, or malicious nodes that drop packets or modifying the packets to launch attacks. The recent researches show that routing misbehavior will significantly reduce the packet delivery rate and thus pose a serious threat against the network performance of DTN [4], [19]. Therefore, a misbehavior detection and mitigation protocol is highly desirable to assure the secure DTN routing as well as the establishment of the trust among DTN nodes in DTNs.

Mitigating routing misbehavior has been well studied in traditional mobile ad hoc networks. These works use neighborhood monitoring or destination acknowledgement to detect packet dropping [20], and exploit credit-based and reputation-based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes [4], [6]. Even though the existing misbehavior detection schemes work well for the traditional wireless networks, the unique network characteristics including lack of contemporaneous path, high variation in network conditions, difficulty to predict mobility patterns, and long feedback delay, have made the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs [4]. This can be illustrated by Fig. 1, in which a selfish node B receives the packets from node A but launches *the black hole attack* by refusing to forward the packets to the next hop receiver C [7]. Since there may be no neighboring nodes at the moment that B meets C, the misbehavior (e.g., dropping messages) cannot be detected due to lack of witness, which renders the monitoring based misbehavior detection less practical in a sparse DTN.

Recently, there are quite a few proposals for misbehaviors detection in DTNs [4]–[7], most of which are based on forwarding history verification (e.g., multi-layered credit [4], [6], three-hop feedback mechanism [5], or encounter ticket [7], [19]), 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

This research is supported by National Natural Science Foundation of China (Grant No.61003218, 70971086, 61272444, 61161140320, 61033014), Doctoral Fund of Ministry of Education of China (Grant No.20100073120065).
H. Zhu, Z. Gao, and Z. Cao are with Computer Science Department of Shanghai Jiao Tong University (e-mail: {zhu-hj, zhaoyu, zfcao}@sjtu.edu.cn).
S. Du is with Antai College of Economics & Management of Shanghai Jiao Tong University (e-mail: sgdu@sjtu.edu.cn).
M. Dong is with The University of Aizu. (e-mail: mx.dong@ieee.org).

Digital Object Indentifier 10.1109/TPDS.2013.36

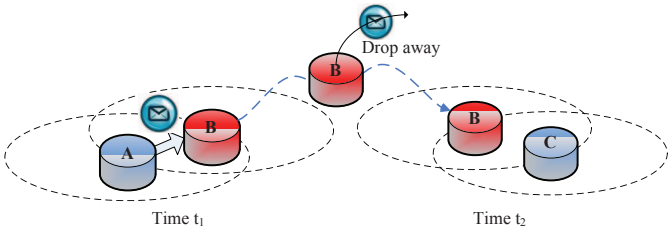


Fig. 1. An Example of Black Hole Attack in DTNs

(TA) point of view, misbehavior detection in DTNs inevitably incurs a high inspection overhead, which includes the cost of collecting the forwarding history evidence via deployed *judgenodes* [5] 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 iTrust, a Probabilistic Misbehavior Detection Scheme to achieve efficient trust establishment in DTNs. Different from existing works which only consider either of misbehavior detection or incentive scheme, we jointly consider the misbehavior detection and incentive scheme in the same framework. The proposed iTrust scheme is inspired from the *Inspection Game* [8], a game theory model in which an inspector verifies if 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 the tradeoff between the security and detection cost, iTrust 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 TA could punish or compensate the node based on its behaviors. To further improve the performance of the proposed probabilistic inspection scheme, we introduce 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 iTrust 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 contributions of this paper can be summarized as follows.

- Firstly, we propose a general misbehavior detection framework based on a series of newly introduced data forwarding evidences. The proposed evidence framework could not only detect various misbehaviors but also be compatible to various routing protocols.
- Secondly, we introduce a probabilistic misbehavior detection scheme by adopting the Inspection Game. A detailed game theoretical analysis will demonstrate that the cost of misbehavior detection could be significantly reduced without compromising the detection performance. We also discuss how to correlate a user's reputation (or trust level) to the detection probability, which is expected to further reduce the detection probability.
- Thirdly, we use extensive simulations as well as detailed analysis to demonstrate the effectiveness and the efficiency of the iTrust.

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 iTrust and the analysis from the perspective of game theory. The simulation results of iTrust are given in Section IV, followed by the conclusion in Section V.

2 PRELIMINARY

This section describes our system model and design goals.

2.1 System Model

In this paper, we adopt the system model similar to [4]. 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 misbehavior 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 [5]) 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.

2.2 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 multi-hop manner. Our misbehaving detection scheme can be applied to delegation based routing protocols or multi-copy based routing ones, such as MaxProp [15] and ProPHET [16]. We assume that the network is loosely synchronized (i.e., any two nodes should be in the same time slot at any time).

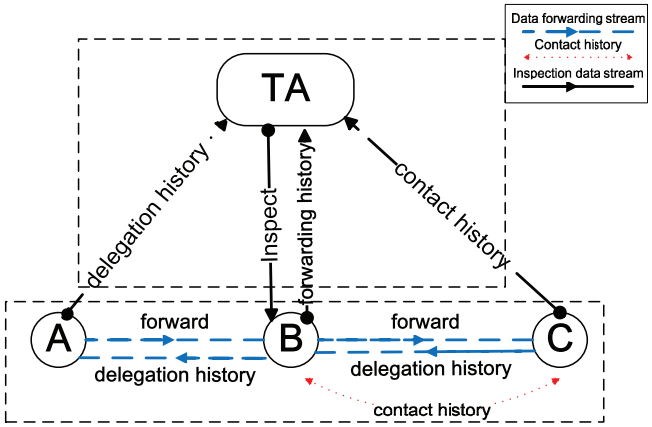


Fig. 2. In the Routing Evidence Generation Phase, A forwards packets to B ,then gets the delegation history back. B holds the packet and then encounters C. C gets the contact history about B. In the Auditing Phase, when TA decides to check B, TA will broadcast a message to ask other nodes to submit all 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.

2.3 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 reward. As an adversary, the malicious nodes arbitrarily drop others' bundles (blackhole or greyhole attack), which often take place beyond others' observation in a sparse DTN, 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.

2.4 Design Requirements

The design requirements include

- *Distributed*: We require that a network authority responsible for the administration of the network is only required to be 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 independent of the size and density of the network.

3 The Proposed Basic iTrust Scheme for Misbehavior Detection in DTNs

In this section, we will present a novel basic iTrust scheme for misbehavior detection scheme in DTNs. The basic iTrust has two phases, including Routing Evidence Generation Phase and Routing Evidence Auditing Phase. In the evidence generation phase, the nodes will generate contact and data forwarding evidence for each contact or data forwarding. In the subsequent auditing phase, TA will distinguish the normal nodes from the misbehaving nodes.

3.1 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, which will be delivered to node C. Now, if node A meets 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 malicious one or not:

- *Delegation Task Evidence* $\mathbb{E}_{task}^{i\to j}$: Suppose that source node $\mathcal{N}_{src}$ is going to send a message M to the destination $\mathcal{N}_{dst}$. Without loss of generality, we assume the message is stored at an intermediate node $\mathcal{N}_i$, which will follow a specific routing protocol to forward M to the next hop. When $\mathcal{N}_j$ arrives at the transmission range of $\mathcal{N}_i$, $\mathcal{N}_i$ will determine if $\mathcal{N}_j$ is the suitable next hop, which is indicated by flag bit $flag$. If $\mathcal{N}_j$ is the chosen next hop (or $flag = 1$), a Delegation Task Evidence $\mathbb{E}_{task}^{i\to j}$ needs to be generated to demonstrate that a new task has been delegated from $\mathcal{N}_i$ to $\mathcal{N}_j$. Given that T_{ts} and T_{Exp} refer to the time stamp and the packets expiration time of the packets, we set $\mathbb{M}_M^{i\to j} = \{M, \mathcal{N}_{src}, flag, \mathcal{N}_i, \mathcal{N}_j, \mathcal{N}_{dst}, T_{ts}, T_{Exp}, Sig_{src}\}$, where $Sig_{src} = Sig_{src}(H(M, \mathcal{N}_{src}, \mathcal{N}_{dst}, T_{Exp}))$ refers to the signature generated by the source nodes on message M. Node $\mathcal{N}_i$ generates the signature $Sig_i = SIG_i\{\mathbb{M}_M^{i\to j}\}$ to indicate that this forwarding task has been delegated to node $\mathcal{N}_j$ while node $\mathcal{N}_j$ generates the signature $Sig_j = SIG_j\{\mathbb{M}_M^{i\to j}\}$ to show that $\mathcal{N}_j$ has accepted this task. Therefore, we obtain the Delegation Task Evidence as follows:

$$\mathbb{E}_{task}^{i\to j} = \{\mathbb{M}_M^{i\to j}, Sig_i, Sig_j\} \tag{1}$$

  Note that, delegation task evidences are used to record the number of routing tasks assigned from the upstream nodes to the target node $\mathcal{N}_j$. In the audit phase, the upstream nodes will submit the delegation task evidences to TA for verification.
- *Forwarding History Evidence* $\mathbb{E}_{forward}^{j\to k}$: When $\mathcal{N}_j$ meets the next intermediate node $\mathcal{N}_k$, $\mathcal{N}_j$ will check if $\mathcal{N}_k$ is the desirable next intermediate node in terms of a specific routing protocol. If yes (or $flag = 1$), $\mathcal{N}_j$ will forward the packets to $\mathcal{N}_k$, who will generate a forwarding history evidence to demonstrate that $\mathcal{N}_j$ has successfully finished the forwarding task. Suppose that $\mathbb{M}_M^{j\to k} = \{\mathbb{M}_M^{i\to j}, flag, \mathcal{N}_k, T'_{ts}\}$. $\mathcal{N}_k$ will generate a signature $Sig_k = SIG_k\{H(\mathbb{M}_M^{j\to k})\}$ to demonstrate the authenticity of forwarding history evidence. Therefore, the complete forwarding history evidence is generated by

$\mathcal{N}_k$ as follows

$$\mathbb{E}_{forward}^{j\to k} = \{\mathbb{M}_M^{j\to k}, Sig_k\}, \tag{2}$$

which will be sent to $\mathcal{N}_j$ for future auditing. In the audit phase, the investigation target node will submit his forwarding history evidence to TA to demonstrate that he has tried his best to fulfill the routing tasks, which are defined by delegation task evidences.

- *Contact History Evidence* $\mathbb{E}_{contact}^{j\leftrightarrow k}$: Whenever two nodes $\mathcal{N}_j$ and $\mathcal{N}_k$ meet, a new contact history evidence $\mathbb{E}_{contact}^{j\leftrightarrow k}$ will be generated as the evidence of the presence of $\mathcal{N}_j$ and $\mathcal{N}_k$. Suppose that $\mathbb{M}^{j\leftrightarrow k} = \{\mathcal{N}_j, \mathcal{N}_k, T_{ts}\}$, where T_{ts} is the time stamp. $\mathcal{N}_j$ and $\mathcal{N}_k$ will generate their corresponding signatures $Sig_j = SIG_j\{H(\mathbb{M}^{j\leftrightarrow k})\}$ and $Sig_k = SIG_k\{H(\mathbb{M}^{j\leftrightarrow k})\}$. Therefore, the contact history evidence could be obtained as follows

$$\mathbb{E}_{contact}^{j\leftrightarrow k} = \{\mathbb{M}^{j\leftrightarrow k}, Sig_j, Sig_k\} \tag{3}$$

Note that $\mathbb{E}_{contact}^{j\leftrightarrow k}$ will be stored at both of meeting nodes. In the audit phase, for an investigation target $\mathcal{N}_j$, both of $\mathcal{N}_j$ and other nodes will submit their contact history evidence to TA for verification. Note that, contact history could prevent the blackhole or greyhole attack since the nodes with sufficient contact with other users fail to forward the data will be regarded as a malicious or selfish one. In the next section, we will show how to exploit three kinds of evidences to launch the misbehavior detection.

3.2 Auditing Phase

In the Auditing phase, TA will launch an investigation request towards node $\mathcal{N}_j$ in the global network during a certain period $[t_1, t_2]$. Then, given $\mathcal{N}$ as the set of total nodes in the network, each node in the network will submit its collected $\{\mathbb{E}_{task}^{i\to j}, \mathbb{E}_{forward}^{j\to k}, \mathbb{E}_{contact}^{j\leftrightarrow k} | \forall i, k \in \mathcal{N}\}$ to TA. By collecting all of the evidences related to $\mathcal{N}_j$, TA obtains the set of messages forwarding requests $\mathbb{S}_{task}$, the set of messages forwarded $\mathbb{S}_{forward}$ and the set of contacted users $\mathbb{S}_{contact}$, all of which could be verified by checking the corresponding evidences.

To check if a suspected node $\mathcal{N}_j$ is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by $\mathcal{N}_j$. We assume that $m \in \mathbb{S}_{task}$ is a message sent to $\mathcal{N}_j$ for future forwarding and $T_{ts}(m)$ is its expiration time. We further define $\mathcal{N}_k(m)$ as the set of next-hop nodes chosen for message forwarding, $\mathcal{R}$ as the set of contacted nodes satisfying the requirements of DTN routing protocols during $[T_{ts}(m), t_2]$ and $\mathcal{D}$ as the number of copies required by DTN routing. The misbehavior detection procedure has the following three cases.

- **Class I (An Honest Data Forwarding with Sufficient Contacts)**: A normal user will honestly follow the routing protocol by forwarding the messages as long as there are enough contacts. Therefore, given the message $m \in \mathbb{S}_{task}$, an honest data forwarding in the presence of sufficient contacts could be determined if

$$m \in \mathbb{S}_{forward} \text{ and } \mathcal{N}_k(m) \subseteq \mathcal{R} \text{ and } |\mathcal{N}_k(m)| == \mathcal{D}, \tag{4}$$

which shows that the requested message has been forwarded to the next hop, the chosen next hop nodes are desirable nodes according to a specific DTN routing protocol, and the number of forwarding copies satisfy the requirement defined by a multi-copy forwarding routing protocol.

- **Class II (An Honest Data Forwarding with Insufficient Contacts)**: In this class, users will also honestly perform the routing protocol but fail to achieve the desirable results due to lack of sufficient contacts. Therefore, given the message $m \in \mathbb{S}_{task}$, an honest data forwarding in the presence of sufficient contacts could be determined if

$$m \notin \mathbb{S}_{forward} \quad \text{and} \quad |\mathcal{R}| == 0 \tag{5}$$

or

$$m \in \mathbb{S}_{forward} \text{ and } \mathcal{N}_k(m) == \mathcal{R} \quad \text{and} \quad |\mathcal{N}_k(m)| == |\mathcal{R}| < \mathcal{D} \tag{6}$$

Equation 5 refers to the extreme case that there is no contact during period $[T_{ts}(m), t_2]$ while Equation 6 shows the general case that only a limited number of contacts are available in this period and the number of contacts is less than the number of copies required by the routing protocols. In both cases, even though the DTN node honestly performs the routing protocol, it cannot fulfill the routing task due to lack of sufficient contact chances. We still regard this kind of users as honest users.

- **Class III (A Misbehaving Data Forwarding with/without Sufficient Contacts)**: A Misbehaving node will drop the packets or refuse to forward the data even when there are sufficient contacts, which could be determined by examining the following rules

$$\exists m \in \mathbb{S}_{task}, m \notin \mathbb{S}_{forward} \quad \text{and} \quad \mathcal{R}! = 0 \tag{7}$$

or

$$\exists m \in \mathbb{S}_{task}, m \in \mathbb{S}_{forward} \quad \text{and} \quad \mathcal{N}_k(m) \nsubseteq \mathcal{R} \tag{8}$$

or

$$\exists m \in \mathbb{S}_{task}, m \in \mathbb{S}_{forward} \quad \text{and} \quad \mathcal{N}_k(m) \subset \mathcal{R} \quad \text{and} \quad |\mathcal{N}_k(m)| < \mathcal{D} \tag{9}$$

Note that Equation 7 refers to the case that the forwarder refuses to forward the data even when the forwarding opportunity is available. The second case is that the forwarder has forwarded the data but failed to follow the routing protocol, which is referred to Equation 8. The last case is that the forwarder agrees to forward the data but fails to propagate the enough number of copies predefined by a multi-copy routing protocol, which is shown in Equation 9.

Next, we give the details of the proposed scheme as follows. In particular, TA judges if node $\mathcal{N}_j$ is a misbehavior or not by triggering the Algorithm 1. In this algorithm, we introduce $\mathbf{BasicDetection}$, which takes $j, \mathbb{S}_{task}, \mathbb{S}_{forward}, [t_1, t_2], \mathcal{R}, \mathcal{D}$ as well as the routing requirements of a specific routing protocol $\mathcal{R}, \mathcal{D}$ as the input, and output the detection

Algorithm 1 The Basic Misbehavior Detection algorithm

procedure BASICDETECTION($(j, \mathbb{S}_{task}, \mathbb{S}_{forward}, [t_1, t_2], \mathcal{R}, \mathcal{D})$)
  for Each $m \in \mathbb{S}_{task}$ **do**
    if $m \notin \mathbb{S}_{forward}$ and $\mathcal{R}! = 0$ **then**
      return 1
    else if $m \in \mathbb{S}_{forward}$ and $\mathcal{N}_k(m) \nsubseteq \mathcal{R}$ **then**
      return 1
    else if $m \in \mathbb{S}_{forward}$ and $\mathcal{N}_k(m) \subset \mathcal{R}$ and $|\mathcal{N}_k(m)| < \mathcal{D}$ **then**
      return 1
    end if
  end for
  return 0
end procedure

result "1" to indicate that the target node is a misbehavior or "0" to indicate that it is an honest node.

The proposed algorithm itself incurs a low checking overhead. However, to prevent malicious users from providing fake delegation/forwarding/contact evidences, TA should check the authenticity of each evidence by verifying the corresponding signatures, which introduce a high transmission and signature verification overhead. We will give a detailed cost analysis in Section 4.2. In the following section, inspired by the inspection game, we will propose a probabilistic misbehavior detection scheme to reduce the detection overhead without compromising the detection performance.

4 The Advanced iTrust: A Probabilistic Misbehavior Detection Scheme in DTNs

To reduce the high verification cost incurred by routing evidence auditing, in this section, we introduce a probabilistic misbehavior detection scheme, which allows the TA to launch the misbehavior detection at a certain probability. The advanced iTrust is motivated by the Inspection Game, a game theoretical model, in which an authority chooses to inspect or not, and an individual chooses to comply or not, and the unique Nash equilibrium is a mixed strategy, with positive probabilities of inspection and non-compliance.

We start from Algorithm 2, which 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).

In the next subsection, 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.

4.1 Game Theory Analysis

Before presenting the detailed Inspection Game, we assume that the forwarding transmission costs of each node g to make

Algorithm 2 The Proposed Probabilistic Misbehavior Detection algorithm

initialize the number of nodes n
for $i \leftarrow 1$ to n **do**
  generate a random number m_i from 0 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 BasicDetection($i, \mathbb{S}_{task}, \mathbb{S}_{forward}, [t_1, t_2], \mathcal{R}, \mathcal{D}$) **then**
      give a punishment C to node i
    else
      pay node i the compensation w
    end if
  else
    pay node i the compensation w
  end if
end for

a packet forwarding. It is also assumed that 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 [4]. In the auditing phase, TA checks the node N_i with the probability p_b^i. Since checking will incur a 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 iTrust, the Probabilistic Inspection Game is*

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

- $N = \{N_0, N_1, ..., N_n\}$ *is the set of the players,* N_0 *donates TA.*
- $s_i = \{s_{i0}, s_{i1}, s_{i2}, ..., s_{in}\}$ *is the strategy set of the player* N_i*,* $s_0 = \{I, N\}$*,* $s_i = \{F, O\}$*.*
- π_i *is the payoff of the* i*th player* N_i*, and it is measured by credit earnings.*
- p_i *is a mixed strategy for player* i*, specially,* $p_0 = \{(p_b^1, 1 - p_b^1), \ldots, (p_b^n, 1 - p_b^n)\}$*,* $p_i = \{p_f^i, 1 - p_f^i\}$*,* p_b *denotes inspection probability,* p_f *denotes offending probability.*

Then we could get the payoff matrix between TA and an individual node as shown in Table 1, and we could use Theorem 1 to demonstrate that TA could ensure the security level with a low inspection cost by the proposed probabilistic checking approach.

Theorem *1: If TA inspects at the probability of* $p_b = \frac{g+\varepsilon}{w+C}$ *in iTrust, 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

TABLE 1
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*

a mixed Nash Equilibrium point according to the Table 1 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

$$v - w - (\frac{g+\varepsilon}{w+C}) \cdot h > v - w - h \tag{10}$$

the latter part in the inequality is the profit of TA when it checks all the nodes. □

Note that the probability that a malicious node cannot be detected after k rounds is $(1-\frac{g+\varepsilon}{w+C})^k \to 0$, if $k \to \infty$. 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 iTrust.

4.2 The Reduction of Misbehavior Detection Cost by Probabilistic Verification

In this section, we give a formal analysis on the misbehavior detection cost incurred by evidence transmission and verification. We model the movements and contacts as a stochastic process in DTNs, and the time interval t between two successive contacts of node N_i and N_j follows the exponential distribution [17]:

$$P\{t \le x\} = 1 - e^{-\lambda_{ij} x}, x \in [0, \infty)$$

where λ_{ij} is the contact rate between N_i and N_j, the expected contact interval between N_i and N_j is $E[t] = \frac{1}{\lambda_{ij}}$. We further denote $Cost_{transmission}$ as the evidences transmission cost and $Cost_{verification}$ as the evidence signature verification cost for any contact. The below Theorem 2 gives a detailed analysis on the cost incurred by iTrust.

Theorem 2: Given that p_b is the detection probability, $\bar{\lambda}$ is the mean value of all the λ_{ij}, T is the inspection period, N is the number of nodes, $Cost_{transmission}$ and $Cost_{verification}$ are the evidence transmission cost and evidence signature verification cost for a contact, the misbehavior detection cost in the whole network could be estimated as

$$\frac{1}{2} p_b \bar{\lambda} T |N|^2 * (Cost_{transmission} + Cost_{verification}). \tag{11}$$

Proof: Given the above mentioned parameters, we could obtain the number of contacts $|H|$ as

$$|H| = \frac{1}{2} \sum_i \sum_{j \ne i} T / \frac{1}{\lambda_{ij}} \approx \frac{1}{2} \bar{\lambda} T |N|^2 \tag{12}$$

If the detection probability is p_b, the expectation of the transmission and verification cost for these contact evidences will be

$$E = p_b |H| = \frac{1}{2} p_b \bar{\lambda} T |N|^2 * (Cost_{transmission} + Cost_{verification}) \tag{13}$$

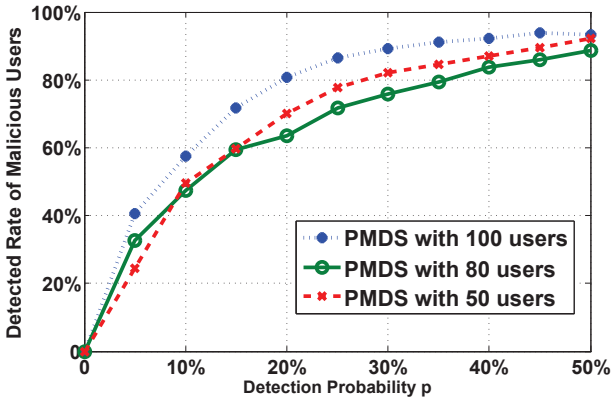
□

Equation 12 shows that between two time slots, the number of the contacts among $|N|$ nodes is in line with the time T and the square of the number of the nodes. Then the cost of misbehavior detection (including evidence transmission and verification cost) is linear to the detection probability p_b. From Theorem 2, it is observed that the misbehavior detection cost could be significantly reduced if choosing an appropriate detection probability without compromising the security level. In the experiment section, we will show that a detection probability of 10% is efficient enough for misbehavior detection, which means the cost of misbehavior detection will be reduced to 10%, which will save a lot of resource of the TA and the network.

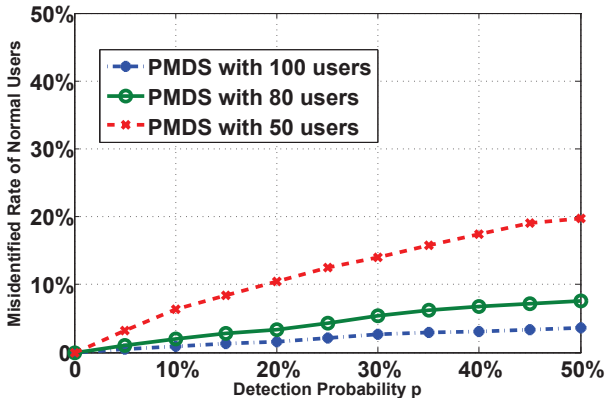
4.3 Exploiting Reputation System to Further Improve the Performance of iTrust

In the previous section, we have shown that the basic iTrust could assure the security of DTN routings at the reduced detection cost. However, the basic scheme assumes the same detection probability for each node, which may not be desirable in practice. Intuitively, an honest node could be detected with a low detection probability to further reduce the cost while a misbehaving node should be detected with a higher detection probability to prevent its future misbehavior. Therefore, in this section, we could combine iTrust with a reputation system which correlates the detection probability with nodes' reputation.

The reputation system of iTrust could update node's reputation r based on the previous round of detection result, and, thereafter, the reputation of this node could be used to determine its inspection probability p. We define the inspection probability p to 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 level, which has been discussed before. Further, it is obvious that p can not be larger than 1, which is the upper bound of detection probability. If a node's p is 1, it means this node has been labeled as a malicious one and thus should be detected for all the time. What's more 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.



(a) Detected rate of malicious nodes



(b) false rate of misidentified nodes

Fig. 3. Experiment results with user number of 100, 80, 50

5 Experiment Results

We set up the experiment environment with the Opportunistic Networking Environment (The ONE) simulator [18], which is designed for evaluating DTN routing and application 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. The size of this area is 2.88 km^2. We set the time interval T to be about 3 hours ($10800s$) as the default value, and we deploy $50, 80, 100$ nodes on the map respectively. With each parameter setting, we conduct the experiment for 100 rounds randomly.

We use the Packet Loss Rate (PLR) to indicate the misbehavior level of a malicious node. In DTNs, when a node's buffer is full, a new received bundle will be dropped by the node, and PLR denotes the rate between the dropped bundles out of the received bundles. But, a malicious node could pretend no available buffer and thus drop the bundles received. Thus PLR actually represents the misbehavior level of a node. For example, if a node's PLR is 1, it is totally a malicious node who launches a black hole attack. If a node's PLR is 0, we take it as a normal node. Further, if $0 < PLR < 1$, the node could launch a grey hole attack by selectively dropping the packets. In our experiment, we use the detected rate of the malicious nodes to measure the effectiveness of iTrust, and we take all the nodes whose PLR larger than 0 as the malicious ones. On the other hand, since a normal node may also be identified as the malicious one due to the depletion of its buffer, we need to measure the false alert of iTrust and show that iTrust has little impact on the normal users who adhere to the security protocols. Thus we use the misidentified rate to measure the false negative rate. Moreover, we evaluate the transmission overhead $Cost_{transmission}$ and verification overhead $Cost_{verification}$ in terms of the number of evidence transmission and verification for misbehavior detection. In the next section, we will evaluate the effectiveness of iTrust under different parameter settings.

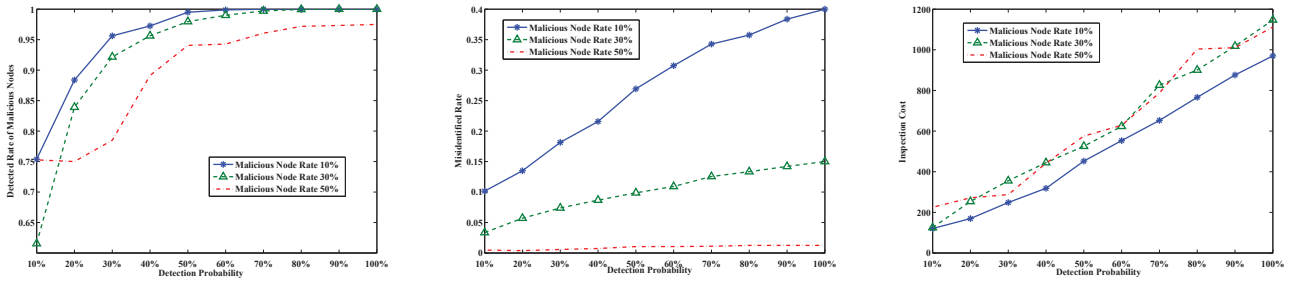
5.1 The Evaluation of The Scalability of iTrust

Firstly, we evaluate the scalability of iTrust, which is shown in Fig. 3. As we predict in Equation.12, the number of nodes will affect the number of generated contact histories in a particular time interval. So we just measure the detected rate (or successful rate) and misidentified rate (or false positive rate) in Fig. 3. Fig. 3(a) shows that when detection probability p is larger than 40%, iTrust could detect all the malicious nodes, where the successful detection rate of malicious nodes is pretty high. It implies that iTrust could assure the security of the DTN in our experiment. Furthermore, the misidentified rate of normal users is lower than 10% when user number is large enough, as showed in Fig. 3(b), which means that iTrust has little impact on the performance of DTN users. Therefore, iTrust achieves a good scalability.

5.2 The Impact of Percentage of Malicious Nodes on iTrust

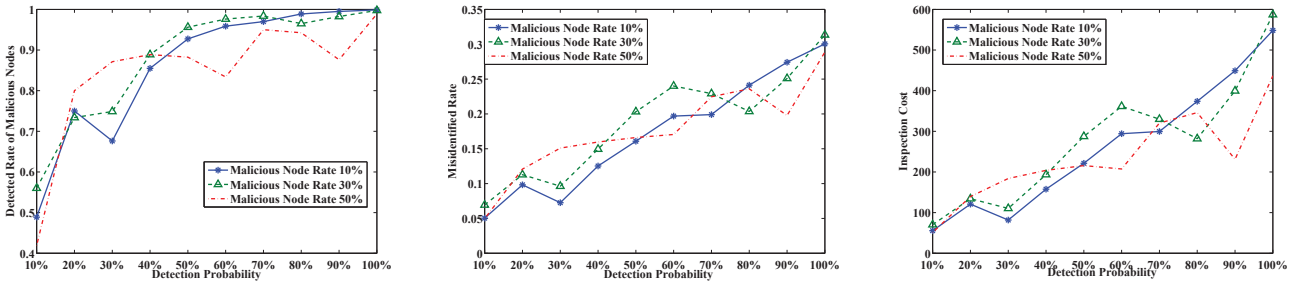
We use Malicious Node Rate (MNR) to denote the percentage of the malicious nodes of all the nodes. In this experiment, we consider the scenarios of varying MNR from 10% to 50%. In this experiment, PLR is set to be 1, and the velocity of 80 nodes varies from $10.5m/s$ to $11.5m/s$. The message generation time interval varies from $25s$ to $35s$, and the TTL of each message is $300s$.

The experiment result is shown in Fig. 4. Fig. 4(a) shows that three curves have the similar trends, which indicate that iTrust could achieve a stable performance with different MNRs. Even though the performance of iTrust under high MNR is lower than that with low MNR, the detected rate is still higher than 70%. Furthermore, the performance of iTrust will not increase a lot when the detection probability exceeds 20 percents, but it is good enough when the detection probability is more than 10%. Thus the malicious node rate has little effect on the detected rate of malicious nodes. That means iTrust will be effective, no matter how many malicious nodes there are. Further, a high malicious node rate will help reduce the misidentified rate as shown in Fig. 4(b), because the increase of the malicious nodes will reduce the proportion of the normal nodes who will be misidentified. However, all the misidentified rates in Fig. 4(b) will be no more than 20%, which means iTrust has little effect on the normal nodes. Since the cost is linear to the detection probability, iTrust will save



(a) Detected rate of malicious nodes with different MNRs (b) Misidentified rate with different MNRs (c) The cost of inspection under different MNRs

Fig. 4. Experiment results with different MNRs



(a) Detected rate of malicious nodes with different PLRs (b) Misidentified rate with different PLRs (c) The cost of inspection under different PLRs

Fig. 5. Experiment results with different PLRs

a lot of resource on the inspection if choosing a small but appropriate detection probability.

5.3 The Impact of Various Packet Loss Rate on iTrust

In the previous section, we have shown that iTrust could also thwart the grey hole attack. In this section, we evaluate the performance of iTrust with different PLRs. In this experiment, we measure the scenarios of varying PLR from 100% to 80%. We set MNR as 10%, and the speed of 80 nodes varying from $10.5m/s$ to $11.5m/s$. The message generation interval varies from $25s$ to $35s$, and the TTL of each message is $300s$. The experiment result is shown in Fig. 5. Also, PLRs have little effect on the performance of iTrust, as shown in Fig. 5(a).

This implies iTrust will be effective for both black hole attack and grey hole attack. The misidentified rate is not affected by PLRs either. It is under 8% when the detection probability is under 10%. Thus the variation of PLR will not affect the performance of iTrust.

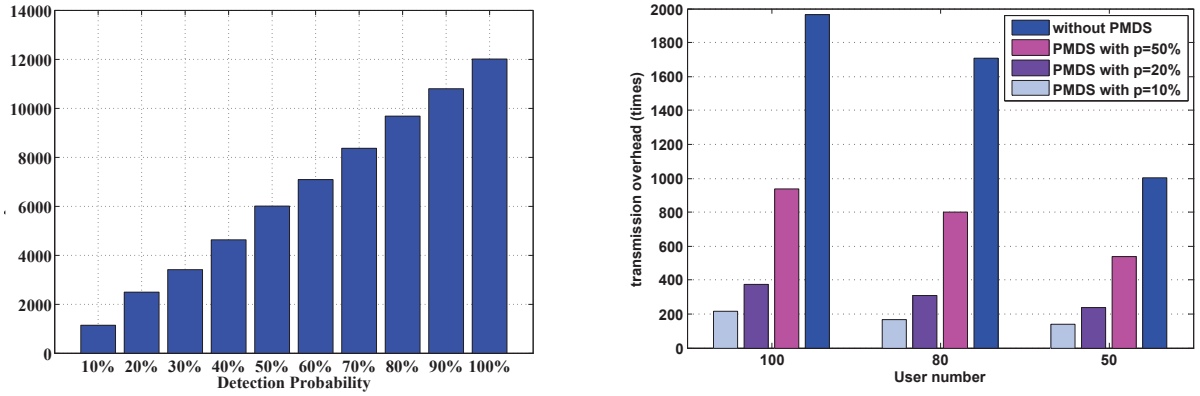
5.4 The Impact of Choosing Different Detection Probabilities

In this section, we discuss the impact of choosing different detection probabilities on the performance of iTrust. In Fig. 6(a), it is shown that iTrust will reduce the authentication cost of the thousands of contact histories, which is in line with the detection probability. And Fig. 6(b) implies that iTrust will significantly reduce transmission overhead compared with the DTN without iTrust. This means iTrust will improve the detection performance of TA and save the transmission cost. Fig. 6(c) and (d) show the cost of the inspection under different MNRs and PLRs. It is obvious that iTrust will significantly reduce the misbehavior detection cost.

The above experiment results demonstrate that iTrust could achieve a good performance gain due to the following two reasons. Firstly, the detection performance of iTrust will not increase significantly as the increase of detection probability. Secondly, the inspection cost will increase along with the increase of the detection probability. Thus we suggest a lower detection probability such as 10% or 20%. And given the analysis of the inspection game, TA could set a proper punishment to ensure the detection probability. In this way, TA could thwart the misbehavior of the malicious nodes and stimulate the rational nodes.

5.5 The Impact of Nodes' Mobility

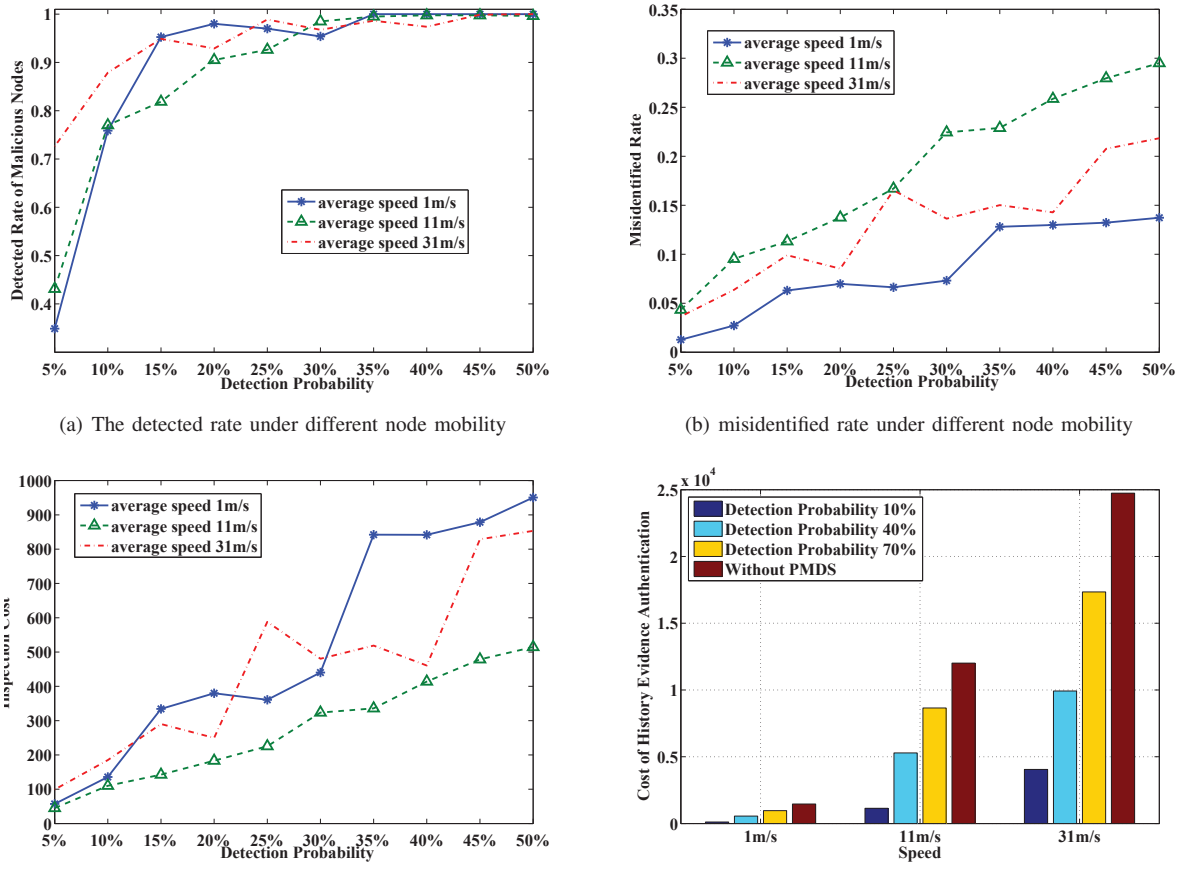
Besides the number of nodes and the length of inspection period, there are some other potential factors that will contribute to the cost of contact history authentication, one of which is the node's speed. In the previous experiment, we set the node's speed in the range of $10.5m/s$ to $11.5m/s$. In this experiment, we will change the velocity of the node, and the experiment result is shown in Fig. 7. The variation of the speed will not affect the effectiveness of iTrust on both of the detected rate and misidentified rate, which has been shown in Fig. 7(a) and (b). Fig. 7(a) implies in a high speed network, iTrust will be more efficient in misbehavior detection when the detection



(a) The cost of contact history authentication

(b) Transmission overhead under different detection probabilities

Fig. 6. Experiment Results with Different Detection Probabilities



(a) The detected rate under different node mobility

(b) misidentified rate under different node mobility

(c) The cost of inspection under different node mobility

(d) The cost of contact evidence authentication under different node mobility

Fig. 7. Experiment Results with Different Velocities of the Nodes

probability is small. Fig. 7(b) indicates that the misidentified rate is irrelevant with the speed. It is because that a lower speed will lead to a smaller chance of packet forwarding, but a higher speed will lead to a quicker depletion of the nodes' buffer. So they will drop some packets before they forward the data at the speed $11m/s$. But a higher speed will make the packet more easily reach the destination node, which will reduce the misidentified rate again. The cost of inspection is almost the same as shown in Fig. 7(c). But the higher speed will inevitably help to generate more contact chances, which will increase the cost of contact history authentication. Fig. 7(d) shows that iTrust will reduce the authentication cost much more when the speed of nodes is very high. Because, at the high speed, a large detection probability is not necessary any more, and the cost thus will be reduced. This result further demonstrates the efficiency of iTrust again.

5.6 The Impact of Message Generation Interval on iTrust

We also measure the effect of the message generating rate on iTrust. The message generation interval is the time between two message generating events, which describes the demand of the users in the network. If the network is a busy one, the message generation interval is short because of the large demand of users. The experiment result is shown in Fig. 8. Fig. 8(a) shows that the performance of iTrust at long message generation interval $(85-95s)$ is not as good as that at a short message generation interval. This is because the messages propagation in the network don't involve all the malicious nodes in the network due to the shortage of the messages. But if the messages are enough, the detected rate of malicious nodes will be more than 90% at a small detection probability (e.g. 10%). So, if the network is not busy, TA could extend the inspection interval, e.g., from 3 hours to 6 hours, the low inspection frequency will reduce more inspection cost because the malicious ones are all involved. But the low message generation frequency also has some advantages for TA. As shown in Fig. 8(b). The misidentified rate will decrease when the message generation interval is long. Another advantage of low message generation interval is cost saving as shown in Fig. 8(c). So there is a tradeoff between the detected rate and misidentified rate when the message generation interval varies.

6 Conclusion

In this paper, we propose a Probabilistic Misbehavior Detection Scheme (iTrust), 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 iTrust will reduce transmission overhead incurred by misbehavior detection and detect the malicious nodes effectively. Our future work will focus on the extension of iTrust 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, G. Cao, "Routing in Socially Selfish Delay Tolerant Networks" in Proc. of *IEEE Infocom'10*, 2010.

[4] 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.*

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

[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] Fudenburg,"Game Theory",p17-18,example1.7:inspection game.

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

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

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

[12] S. Zhong, J. Chen, Y. R. Yang"Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks",in *INFOCOM'03,2003.*

[13] J. Douceur,"The sybil attack" *in IPTPS,2002.*

[14] R. Pradiptyo"Does Punishment Matter? A Refinement of the Inspection Game",in *German Working Papers in Law and Economics,Volume 2006,Paper 9.*

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

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

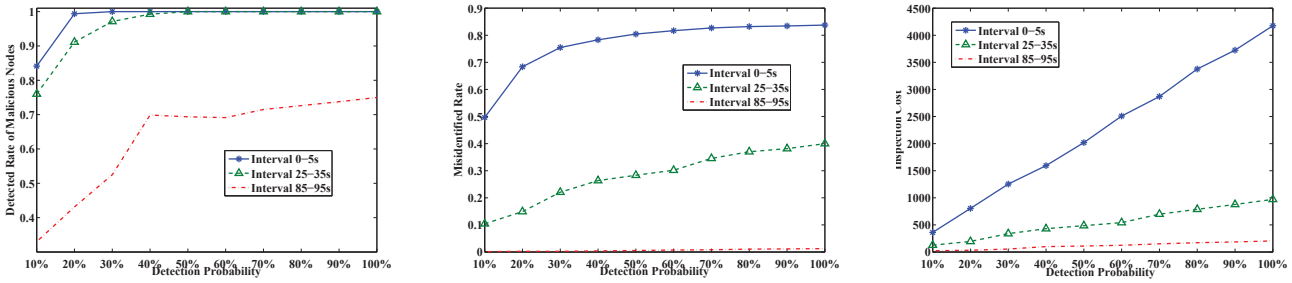
[17] W. Gao and G. Cao "User-centric data dissemination in disruption tolerant networks", in Proc. of *IEEE INFOCOM*, 2011.

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

[19] Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, April 2012.

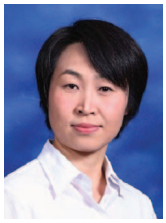
[20] S. Marti, T. J. Giuli, K. Lai, and M. Baker, Mitigating routing misbehavior in mobile ad hoc networks, in Proc. *ACM MobiCom'06*, 2000.

Haojin Zhu received his B.Sc. degree (2002) from Wuhan University (China), his M.Sc.(2005) degree from Shanghai Jiao Tong University (China), both in computer science and the Ph.D. in Electrical and Computer Engineering from the University of Waterloo (Canada), in 2009. He is currently an Associate Professor with Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His current research interests include wireless network security and distributed system security. He is a co-recipient of best paper awards of IEEE ICC 2007 - Computer and Communications Security Symposium and Chinacom 2008- Wireless Communication Symposium. He served as Guest Editor for IEEE Networks and Associate Editor for KSII Transactions on Internet and Information Systems. He currently serves as the Technical Program Committee for international conferences such as INFOCOM, GLOBECOM, ICC, WCNC and etc. He is a member of IEEE.

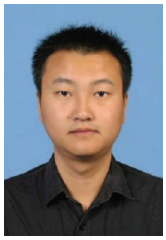


(a) Detected rate with different message generation interval (b) Misidentified Rate with different message generation interval (c) The cost of inspection with different message generation interval

Fig. 8. Experiment Results with different message generation interval



Suguo Du received the BSc degree in Applied Mathematics from Ocean University of Qingdao, China, in 1993, the MSc degree in Mathematics from Nanyang Technological University, Singapore, in 1998, and the PhD degree in Control Theory and Applications Centre from Coventry University, U.K., in 2002. She is currently an Associate Professor of Management Science Department in Antai College of Economics & Management, Shanghai Jiao Tong University, China. Her current research interests include Risk and Reliability Assessment, Fault Tree Analysis using Binary Decision Diagrams, Fault Detection for nonlinear system and Wireless Network Security Management.



Zhaoyu Gao received his B.Sc. degree in Applied Mathematics(2009) from Wuhan University (China) and now he is a M.Sc candidate in Department of Computer Science and Engineering, Shanghai Jiao Tong University, China. His research interests include Cognitive Radio Network, security and privacy of wireless network.

Mianxiong Dong received his B.Sc. degree in Computer Science (2009) from the University of Aizu (Japan) and now he is a PhD candidate in Department of Computer Science, the University of Aizu. His research interests include networking and wireless security.

Zhenfu Cao (SM10) received the B.Sc. degree in computer science and technology and the Ph.D. degree in mathematics from Harbin Institute of Technology, Harbin, China, in 1983 and 1999, respectively.

He was exceptionally promoted to Associate Professor in 1987 and became a Professor in 1991. He is currently a Distinguished Professor and the Director of the Trusted Digital Technology Laboratory, Shanghai Jiao Tong University, Shanghai, China. He also serves as a member of the expert panel of the National Nature Science Fund of China.

Prof. Cao is actively involved in the academic community, serving as Committee/Session Chair and program committee member for several international conference committees, as follows: the IEEE Global Communications Conference (since 2008), the IEEE International Conference on Communications (since 2008), the International Conference on Communications and Networking in China (since 2007), etc. He is the Associate Editor of Computers and Security (Elsevier), an Editorial Board member of Fundamenta Informaticae (IOS) and Peer-to-Peer Networking and Applications (Springer- Verlag), and Guest Editor of the Special Issue on Wireless Network Security, Wireless Communications and Mobile Computing (Wiley), etc. He has received a number of awards, including the Youth Research Fund Award of the Chinese Academy of Science in 1986, the Ying-Tung Fok Young Teacher Award in 1989, the National Outstanding Youth Fund of China in 2002, the Special Allowance by the State Council in 2005, and a corecipient of the 2007 IEEE International Conference on CommunicationsłComputer and Communications Security Symposium Best Paper Award in 2007. He also received seven awards granted by the National Ministry and governments of provinces such as the first prize of the Natural Science Award from the Ministry of Education.