International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.4, No.1, January 2015 DOI:10.15693/ijaist/2015.v4i2.231-236

A Possibility Misdeed Node Catching Scheme in Delay Tolerant Networks

R. Shalini
ME(CSE) (student) Sri Muthukumaran Institute of technology Chennai, India

D. Shanmugavel, M.E,
Assistant Professor/CSE
Sri Muthukumaran Institute of technology Chennai, India

ABSTRACT: Malicious and misdeed manners make up a major source of danger opposed to routing in delay tolerant networks (DTNs). So, designing a misdeed catching scheme in DTN is regarded as great challenge. This paper propose itrust, the basic idea of itrust is introducing a Trusted Authority (TA) to judge the nodes manner based on the collected routing evidences and probabilistically checking. Routing evidences includes the delegation history, forwarding history and contact history. Trusted Authority verify the routing evidence by an appropriate investigation probability, TA could ensure the security of DTN routing at a reduced cost. TA decides to check some target node; it will broadcast a message to ask other node to submit all the evidence about target node. The nodes which previous to the target node submit the delegation history, the target node submit the forwarding history, and the next node submits the contact history. Then, the TA could punish (or) compensate the node based on its manner. A user's reputation (or trust level) is correlated to the catching probability, which further reduces the catching probability. 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.

Keywords: - Delay tolerant networks, security, misdeed catching

I.INTRODUCTION

Delay Tolerant Networks (DTNs) is a network designed to operate effectively over extreme distances such as those encountered in space communications. A node which want to transfer the data have to wait and carry data till next node enter into their the transmission range (e. g a node buffered data till next node appears in the transmission range).This data transfer process is normally named to as the "store-carry-and-forward" strategy. In an opportunistic fashion routing is decided [2], [3], [4], [5].In DTNs, a node has a capability (e. g., sufficient buffers and meeting opportunities) to transfer the data but intentionally dropping packets is named as misdeed node [4], [6]. Misdeed nodes caused the routing misbehaviour that do not pass or relay others" packets but it makes use of neighbour or cooperative nodes to relay its packets, or in order to launch attacks packets are modify or drop by malicious nodes. Therefore, d e s i g n i n g a misdeed catching scheme and mitigation protocol is highly worthy 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. To detect packet dropping these works use neighborhood monitoring or destination acknowledgement [7], and to stimulate rational nodes use exploit credit-based and reputation-based incentive schemes or to revoke malicious nodes use revocation schemes [4], [8]. Even though the traditional wireless networks work well in the existing misbehavior detection schemes, 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].

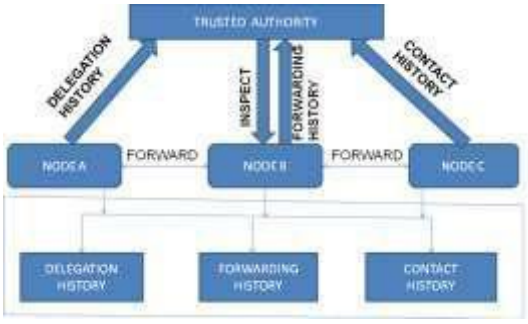
To propose itrust, a probabilistic misdeed catching scheme to achieve effective trust establishment in DTNs. This paper considered the misdeed catching and incentive scheme in the same framework, which is the major different from existing works that consider either of misdeed catching or incentive scheme. The proposed itrust scheme is inspired from the inspection game, a game theory model in which an inspector verifies if another party, called inspected, adheres to certain legal rules. In this model, the inspected 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 misdeed of inspected. Furthermore, the inspector could check the inspected with a higher probability than the Nash Equilibrium points to prevent the offences, as the inspected must choose to comply the rules due to its rationality.

Inspired by inspection game, to achieve the tradeoff between the security and catching cost, iTrust introduces a periodically available TA, which could launch the probabilistic catching for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. TA decides to check some target node; it will broadcast a message to ask other node to submit all the evidence about target node. The nodes which previous to the target node submit the delegation history, the target node submit the forwarding history, and the next node submits the contact history. Then, TA could punish or compensate the node based on its behaviors.

To further improve the performance of the proposed probabilistic inspection scheme, to 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. The propose 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 proposed evidence framework could not only detect various misdeed but also be compatible to various routing protocols.

Overall design



A. First Contact Routing Protocol

First contact routing protocol will send the message to the node that first meet, this protocol also has a liminal buffer and liminal range. But compare with the epidemic routing protocol which also chose the node with no prior knowledge, its liminal buffer is much more less. Large contact range will help the node meet more nodes. The communication range of data sender which is out of destination nodes can only transmit packetized data via a sequence of intermediate nodes. So, node transmit data to the intermediate node which it meet first.

B. DTN Network Formation:

A Delay Tolerant network is established. In DTN node have been created with the starting range and ending range (that is transmission range of node). The nodes communicate with each other directly or through the neighboring nodes. If one of the node sends the message „Hello‟, this message is received by the neighboring node. Then it will check whether the destination is the neighbor or not. If destination is found, the message is sent or forwarded to the next intermediate node.

C. Nearest Node Identification:

Here adopt the single-copy routing mechanism such as First Contact routing protocol, and 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. For the simplicity of presentation, 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. This process will define three kinds of data forwarding evidences. They are Delegation Task Evidence, Forwarding History Evidence and Contact History Evidence.

D. Trust Authority I-Scheme:

The tradeoff between the security and detection cost, iTrust introduces a periodically available Trust Authority (TA), which could launch the probabilistic catching 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, to 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. Now 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.

E. Network and Routing Model:

Similar to other network and routing model, assume that there are two separate buffers for each node. One buffer is used to store its own packets and it space unlimited; the another one is used to store packets received from other nodes and it space is limited. Assume that the network is loosely synchronized; i.e., at any time in the same time slot any two nodes should be present. Since the intercontact time is usually at the scale of minutes or hours, the time slot can be at the scale of one minute. Thus, such loose time synchronization is not hard to achieve.

F. Security Model:

The nodes may be two form: named as *misdeed nodes* and *normal nodes*. The nodes which intentionally drop packet even though have a sufficient buffer to forward the packets, but it does not drop its own packets and it makes use of neighbour or cooperative nodes to relay its packet. That type of node is referred as misdeed node. It may also drop the control messages of our catching scheme. Assume a small number of misdeed nodes may collude to avoid being catch, and they may synchronize their actions via out- band communication channels. When the buffer overflows only a normal node may drop packets, but it follows our protocol.

In some DTN applications, each packet has a certain life time, whether or not there is buffer space expired packets should be dropped. Source is signed the expiration time of the packet from that such dropping packets can be identified. Such dropping is not a misdeed, and will not be considered in the following presentations.

Assume a public-key authentication service is available. For example, hierarchical identity-based cryptography has been shown to be practical in DTNs. A public/private key pair is generate only by offline trusted private key generator in identity-based authentication, so a misdeed node it-self cannot forge node identifiers. However, colluding nodes may know each other‟s private key but a node‟s private key is only known by it-self.

G. Trusted Authority for Misdeed Catching in DTN

This paper proposed a novel basic itrust scheme for misdeed catching scheme in DTN. They are two phases in the itrust, named as routing evidence generation phase and routing evidence auditing phase. For each contact or data forwarding , the nodes will generate contact and data forwarding evidence this process is normally performed in the evidence generation phase. TA will differentiate the nodes which is normal from the misdeed nodes is performed in the auditing phase.

H. Evidence generation phase:

Consider the node A, B, C. The node A which want to send the packet to node C. Node B enter the transmission range of node A which will help to forward the packet to node C, node B receives the packet from node A and carry data till node C enter into their transmission range. Then it will forward the packet to node C. To find whether the node is a malicious one or not here define three kinds of data forwarding evidences.

- **Delegation task evidence**:
  The nodes which may be a source want to send a message to some destination node via a help of intermediate node. The intermediate node stores a message, which will follow a specific routing protocol to forward message to the next node and the node send the message to the suitable next node when it enter into their transmission range. After sent a message by each node, delegation task evidence needs to be generated to demonstrate that a new task has been delegated from one node to another node.

- **Forwarding history evidence**:
  When the node meets the next intermediate node, it will check if is the desirable next intermediate node in terms of a specific routing protocol. If it is then forward the packets, intermediate node has successfully finished the forwarding task which will be demonstrate by who will generate a forwarding history evidence. During the audit phase, forwarding history evidence will be submitted to TA by the investigation target node in order to demonstrate that he has tried his best to fulfill the routing tasks, which are defined by delegation task evidences.

- **Contact history evidenc**e:
  Whenever two nodes meet, a new contact history evidence will be generated as the evidence of the presence of two node. The contact history contains the detail of each nodes to which are all it

have contact. During the audit phase, for an investigation target node, for verification both of target nodes and other nodes will submit their contact history evidence. The black hole or gray hole attack is prevent by the contact history because the nodes with sufficient contact with other users fail to forward the data will be regarded as a malicious one.

Auditing phase:

During auditing phase, TA will launch an investigation request toward node target node in the global network during a certain period. Then, each node in the network will submit its collected task evidence, forward history evidence and contact history evidence to TA. By collecting all of the evidences related to target node, TA obtains the set of messages forwarding requests, the set of messages forwarded, and the set of contacted users, all of which could be verified by checking the corresponding evidences. To check if a suspected target node is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by target node.

I. The Advanced itrust: A Probabilistic Misdeed Catching Scheme In DTN

Introduce a probabilistic misdeed catching scheme, which allows at a certain probability the TA to launch the misdeed catching in order to reduce the high verification cost incurred by routing evidence auditing. From the inspection game the advanced iTrust is motivated, 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 noncompliance. The details of the proposed probabilistic misdeed catching scheme which shown in Algorithm 1. 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 1. The Proposed Probabilistic Misbehavior Detection algorithm.

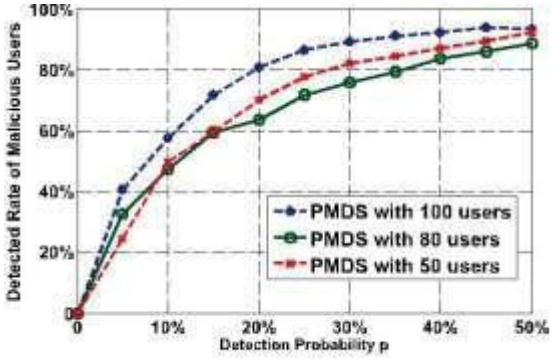
1: initialize the number of nodes n
2: for i 1 to n do
3: generate a random number m_i from 0 to 10^n _ 1
4: if $m_i=10^n < p_b$ then
5: ask all the nodes (including node i) to provide evidence about node i
6: if BasicDetection(i; SS_{task}; $SS_{forward}$; ½t1; t2&; R; D)
then
7: give a punishment C to node i
8: else
9: pay node i the compensation w
10: end if
11: else
12: pay node i the compensation w
13: end if
14: end for

II. EXPERIMENT RESULTS:

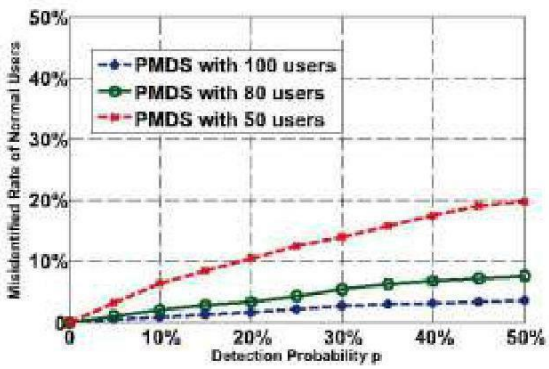
To set up the experiment environment with the opportunistic networking environment (The ONE) simulator, which is designed for evaluating DTN routing and application protocols. In my experiment, here adopt the First Contact routing protocol.

A. The Evaluation of the Scalability of iTrust

First, evaluate the scalability of iTrust, which is shown in Fig. As here predict in, the number of nodes will affect the number of generated contact histories in a particular time interval. So here just measure the detected rate (or successful rate) and misidentified rate (or false positive rate) in Fig. Fig.a shows that when detection probability p is larger than 40 percent, 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 the experiment. Furthermore, the misidentified rate of normal users is lower than 10 percent when user number is large enough, as shown in fig.b, which means that itrust has little impact on the performance of DTN users. Therefore, itrust achieves a good scalability.



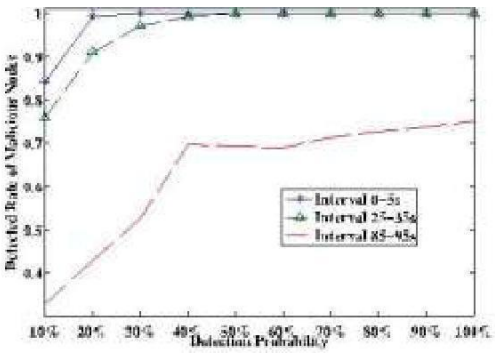
(a) Detected rate of malicious nodes



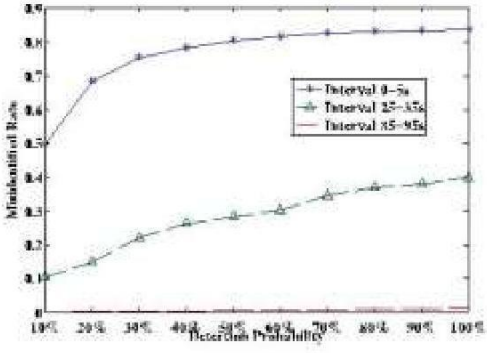
(b) false rate of misidentified nodes

B. The Impact of Message Generation Interval on iTrust

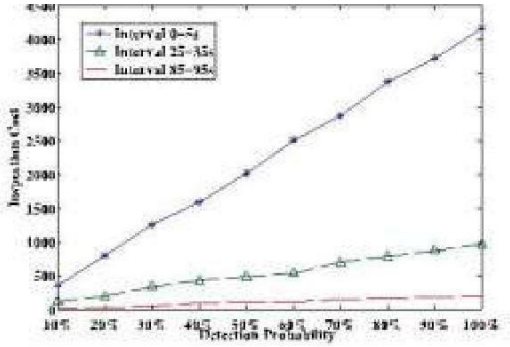
To also measure the effect of the message generating rate on iTrust. The message generation interval is the time between two message generating events, which describes the demand of the users in the network. In a high-density network, the message generation interval is short because of the large demand of users.



(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

The experiment result is shown in Fig.. Fig. a shows that the performance of iTrust at long message generation interval (85-95 s) is not as good as that at a short message generation interval. This is because the messages propagation in the network does not 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 percent at a small detection probability (e.g., 10 percent). So, if the network is not busy, TA could extend the inspection interval, for example, from 3 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. 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. c. So there is a tradeoff between the detected rate and misidentified rate when the message generation interval varies.

III.CONCLUSION:

This paper proposed a probability misdeed catching scheme (iTrust), which detect the misdeed node in DTN. This scheme which could reduce the catching overhead effectively and assure the security of the DTN at a reduced catching overhead. A probabilistic misdeed catching scheme (iTrust), which could reduce the detection overhead effectively. Trusted Authority could ensure the security of DTN routing at a reduced cost via choosing an appropriate investigation probability. The cost of misbehavior detection could significantly reduced without compromising the detection performance.

IV. ACKNOWLEDGEMENT

The author wishes to thank Sri Muthukumaran Insitute of technology for providing all necessary resource for this research to be

successful. On top of it all Dr. R.M.Suresh Principal, Mrs S. Dhanalakshmi, H. O. D, Mr. A. Mathan Gopi Associate Professor and Mr.D. Shanmugavel Assistant Professor for the guidance. The databases used for testing purpose were Sri Muthukumaran Insitute of technology is highly appreciated.

REFERENCES

[1] Lu, X. Lin, H. Zhu, and X. Shen, "SPARK: A New VANET- Based Smart Parking Scheme for Large Parking Lots," Proc. IEEE INFOCOM ‟09, Apr. 2009.

[2] T. Hossmann, T. Spyropoulos, and F. Legendre, "Know the Neighbor: Towards Optimal Mapping of Contacts to Social Graphs for DTN Routing," Proc. IEEE INFOCOM ‟10, 2010.

[3] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM ‟10, 2010.

[4] H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, "SMART: A Secure Multilayer Credit-Based IncentiveSchemeforDelay-Tolerant Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 8, pp. 828-836, 2009.

[5] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858-3868, Oct. 2008.

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

[7] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom ‟00, 2000.

[8] R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr. 2010.

[9] F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM ‟09, 2009.

[10] E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay-Tolerant Networks," Proc. Military Comm. Conf. (Milcom ‟10), 2010.

[11] D. Fudenberg and J. Tirole, Game Theory. MIT Press, 1991.

[12] M. Rayay, M.H. Manshaeiy, M. Flegyhziz, and J. Hubauxy, "Revocation Games in Ephemeral Networks," Proc. 15th ACM Conf. Computer and Comm. Security (CCS ‟08), 2008.

[13] S. Reidt, M. Srivatsa, and S. Balfe, "The Fable of the Bees: Incentivizing Robust Revocation Decision Making in Ad Hoc Networks," Proc. 16th ACM Conf. Computer and Comm. Security (CCS ‟09), 2009.

[14] B.B. Chen and M.C. Chan, "Mobicent: A Credit-Based Incentive System for Disruption-Tolerant Network," Proc. IEEE INFOCOM ‟10, 2010.

[15] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple Cheat-Proof, Credit- Based System for Mobile Ad-Hoc Networks," Proc. IEEE INFOCOM ‟03, 2003.

[16] J. Douceur, "The Sybil Attack," Proc. Revised Papers from the First Int‟l Workshop Peer-to-Peer Systems (IPTPS ‟01), 2001.

[17] R. Pradiptyo, "Does Punishment Matter? A Refinement of the Inspection Game," Rev. Law and Economics, vol. 3, no. 2, pp. 197-219, 2007.

[18] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM ‟06, 2006

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

[20] Haojin Zhu, Suguo Du, Mianxiong Dong, Zhenfu Cao, "A Probabilistic Misbehavior Detection Scheme towards Efficient Trust Establishment in Delay Tolerant Networks," IEEE Transaction on Parallel and Distributed System, VOL. 25, 2014.