MISBEHAVIOR DETECTION SCHEME IN DELAY TOLERANT NETWORKS (DTNS) USING ITRUST

[1]Annie Jerusha Y, [2]Kukatlapalli Pradeep Kumar
[1]MTech Student, Dept. of CSE, Christ University,Bangalore
[2]Assistant Professor, Dept. CSE, Christ University,Bangalore
Email:[1]y.jerusha@mtech.christuniversity.in,[2]kukatlapalli.kumar@christuniversity.in

***Abstract*— The delay/disruption tolerant networks are affected by the malicious and selfish behavior of the nodes. This misbehavior detection in the networks with specific characteristics is a challengeable issue. We propose, iTrust, a misbehavior detection scheme to provide efficient trust establishment in the networks. The iTrust scheme works similar to the inspection game, with a trusted authority in it. The TA (trusted authority) finds all the information from the nodes periodically to alert them. This scheme runs on the game theory model. The proposed work is the basic iTrust mechanism which is secured and trust worthy.**

Keywords— Misbavior detection, Security, Inspection Game, Incentive scheme, Delay Tolerant Networks.

I. INTRODUCTION

The transmission in the delay tolerant networks get troubled with continuous network disconnectivity and many other routing problems. The message propagation process in the delay tolerant networks happens as “Store-Carry-and-Forward” method. In this method, each node enters all these levels during its message transmission. The node stores the message at first in its buffer for a time period till it finds the next right hop to send, it carries the message to the next hop and forwards it.

In DTNs, a node could misbehave probably in two ways, a malicious and selfish behaviors. A malicious node is one which drops the packets intentionally into the wrong router. They would launch the attacks, by not forwarding the messages though it has enough buffer and the capacity. A selfish (rational) node is one which does not want to forward the messages to other nodes wontedly. It wants to maximize its own benefits. However, these misbehavior nodes cause threats to the network performance. The packet delivery rate and other routing, message transmission problems cause the DTNs to low performance. Henceforth, a misbehavior detection scheme is highly desirable to overcome the problems in the DTNs.

In the traditional misbehavior schemes, works followed are neighborhood monitoring or destination acknowledgement to defect packet dropping, and exploit credit-based and reputation-based incentive schemes.

A neighborhood monitoring or destination acknowledgement

In this scheme, each node will be monitoring its respective neighbor in forwarding the messages. The node acts as the monitor in the transmission of the messages. The destination acknowledgement is, each node provides a message with an acknowledgement saying it has received the message. But this method of acknowledgment becomes an issue in storage capacity of the buffer. The node may take a very long time to acknowledge about the message which makes the sender to retransmit the message. So, the long delay in receiving acknowledgement does not support the DTNs.

Credit based model

The credit based model works on gaining the credits on each transmission of the message. A node will be credited each time it completes its transmission of the message successfully. The node with least credentials will be discarded from the network. Though the traditional misbehavior detection techniques works will with a limited number of nodes in a network, they cannot work in the wide range of networks. The continuous change in the number of nodes and network topology in these days makes these traditional misbehavior schemes unsuitable.

II. PROPOSED WORK

Recently there are quite a few proposals for misbehavior detection in DTNs [5], [6], [7], [8], most of which are based on forwarding history verification (e.g., multilayered credit [5], [6], three-hop feedback mechanism [8], or encounter ticket [9], [10], which are costly in terms of transmission overhead and verification cost. The proposed scheme is iTrust, a misbehavior detection scheme in delay tolerant networks (DTNs). The presence of trusted authority (TA) makes the scheme unique.

Trusted authority

TA works just similar to the inspection game, a game theory model. In the inspection game theory, a inspector with number of inspectee will be present and the inspector verifies the inspectee if he is following the legal rules or not. The inspectee may try to violate the rules by not following them. The inspector checks on the inspectee and punishes him to discourage the misbehaviors in the game.

The similar process is followed in the DTNs, the trusted authority (TA) as the inspector and the nodes as the inspectee. The TA will check on the nodes periodically using the history from the nodes. The type of history it collects and their process is mentioned in 3.1. iTrust introduces a periodically available TA, which could launch the misbehavior detection for the target node and judge it by collecting the history evidence [1].

The working model of iTrust scheme with TA can be summarized as follows:

- First, a general misbehavior detection framework is introduced with collecting the evidences of history from the nodes.
- Second, the misbehavior detection scheme by adopting the inspection game model is followed.

TA after receiving the history evidences from the nodes for the target node, will compensate it for the misbehavior done in the network.

Requirements for the design of the proposed work

The design requirements are as follows:

- The trusted authority (TA) must be capable of monitoring the network periodically without fail and it should be trust worthy.
- The scheme should be independent of the size and density of the network.
- The misbehavior detection scheme should be able to tolerate the external failures such as network environments, as including nodes or deleting nodes from the network at any point of time.

III. THE PROPOSED BASIC ITRUST SCHEME

The iTrust scheme works with the Trust Authority (TA) which follows the inspection game theory for misbehavior detection in delay tolerant networks. The basic iTrust scheme has two phases, routing evidence generation phase and routing evidence auditing phase. The method works as shown in Fig. 1,

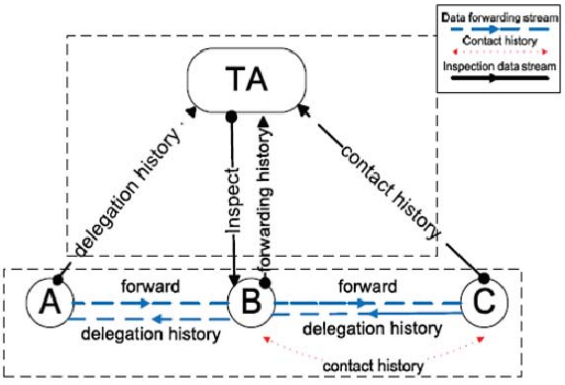

Fig. 1. The basic architecture of the iTrust misbehavior detection scheme

1. Routing Evidence Generation Phase

In this phase, the Trusted Authority (TA) generates evidences from all the

nodes in the network. This phase contains three-steps, using this we could find the malicious node easily. This three-step process in this phase is to make the procedure as simple.

- *Delegation Task Evidence*

  Now, if a source node S has to send a message M to the destination D. We assume that the forwarded message has to be stored in some intermediate node N. Here, source S generates a delegation task evidence to say that a new task has been delegated from S to N.

  The delegation task evidence is used to record the number of tasks assigned from the upstream nodes to the lower stream nodes. During the audit phase, the trusted authority collects this delegation task evidences from the upstream nodes.

- *Forwarding History Evidence*

  Suppose, J is another intermediate node after node N. Node N has to forward the message M to node J after checking its availability. Node J generates the forwarding history evidence on node N, indicating that node N has successfully completed its task.

  The forwarding history evidence, the tasks generated by the delegation task evidences are attained.

- *Contact History Evidence*

  A new contact history will be generated when the two nodes meet to forward a message. Say, node N and node J meet to forward message M. Node N generates a contact history evidence.

  In the audit phase, node N submits the contact history evidence showing all the contacts it has during the process of forwarding the message M. In this step, the malicious and selfish nodes can be easily detected, as the nodes which are in contact history and does not participate in forwarding message are considered as malicious and selfish nodes.

2. Routing Evidence Auditing Phase

   In the auditing phase, trusted authority (TA) will request all the nodes to send their history. To check if a node has misbehaved in the network or not, TA request for the history of all the nodes on the suspected node. This misbehavior detection procedure is as follows:

- *An honest data forwarding with sufficient contacts*

  A node forwards the data honestly without dropping it in wrong node. This phase shows that, an honest data forwarding with sufficient contacts will forward data to next hop successfully without misbehaving.

- *An honest data forwarding with insufficient contacts*

  A node would misbehave here due to lack of contacts. The node may not find the next hop to forward the data, as the node has dead or discarded from the network. Network connections, network environment are also the problems in failure of finding the contacts to forward the data.

- *A misbehaving data forwarding with/without sufficient contacts*

  Nodes which are malicious and selfish fall under this category. These type of nodes does not forward the data though they have sufficient contacts. Malicious nodes drops the data into wrong contact wontedly.

IV. OPERATIONS IN THE ITRUST SCHEME

iTrust, a misbehavior detection mechanism in delay tolerant networks with trusted authority (TA) in it is inspired by the inspection game, a game theory model. The workflow in the TA is mentioned in the Fig. 2.

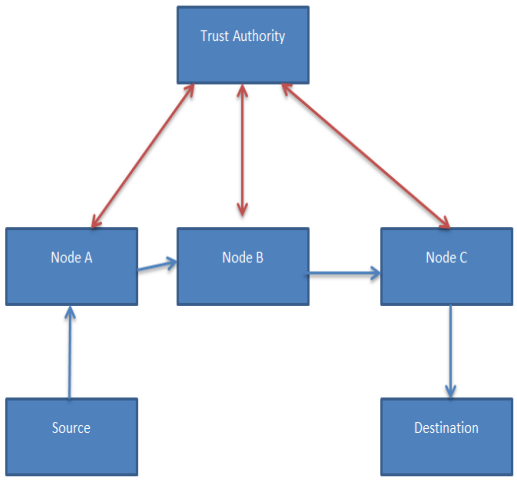

Fig. 2. Operations in the basic iTrust scheme

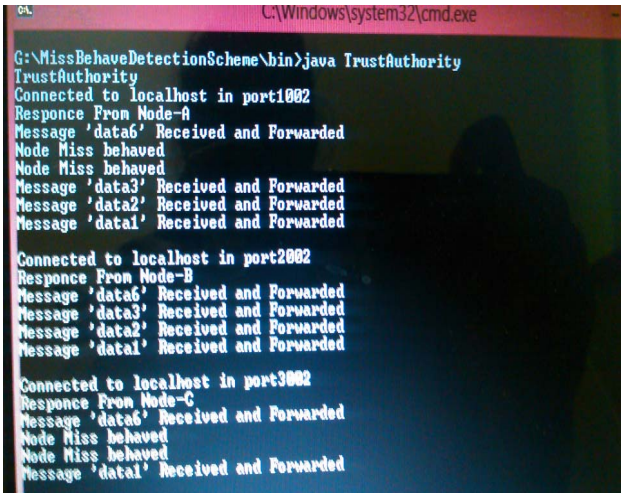

Fig. 3. Output of the messages transmitted in the iTrust mechanism

Nodes

From the figure we see that, nodes are the intermediate nodes which are forwarding the message from source to destination. Any node could misbehave at any time.

Source

Source is the node that generates a message that to be transmitted to the destination. In this framework, the destination is fixed. The message generated by the source should reach destination from passing through all the nodes.

Destination

The message reaches the final node is destination.

Trusted authority (TA)

The misbehavior detection scheme completely depends on the TA. TA verifies all the nodes with the inspection game model.

V. EXPERIMENT RESULTS

The nodes in the network transmits the messages to the destination from the source. To demonstrate the procedure we can see the Fig. 3, which is the result to the input of sequence of messages into the source.

Considering Fig. 2, Fig. 3, three nodes are experimented in this section with a source and destination under TA. The result is shown in the TA, in which each time one of the nodes fails to forward the message.

CONCLUSION

In this paper, we propose a misbehavior detection scheme (iTrust), inspired with the inspection game. We have focused in detecting the misbehaving node in the network mostly. Our future work will focus on the process of reducing the transmission overhead incurred by misbehavior detection.

ACKNOWLEDGMENTS

Sincere gratitude to project guide Prof. Kukatlapalli Pradeep Kumar on his useful review and continues monitory in this paper work Also thanks to management, Faculty of Engineering, Christ University for providing the appropriate laboratory facilities.

REFERENCES

[1] Haojin Zhu, Suguo Du, Zhaoyu, Mianxiong Dong, Zhenfu Cao, "A Probablistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Dealy-Tolerant Netwoks," vol.25, No.1, January 2014.

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

[3] B.B. Chen and M.C. Chan, "Mobincent" A Credit-Based Incentive System for Mobile

Ad-Hoc Network," *Proc. IEEE INFOCOM* '10, 2010.

[4] W. Gao and G. Cao, "User-Centric Data Dissemination in Disruption-Tolerant networks," *Proc. IEEE INFOCOM* '11, 2011.

[5] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," *IEEE Trans. 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," *IEEE Trans. Wireless Comm.*, vol. 9, no. 4, pp. 1483-1493, Apr. 2010..

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

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

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