Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 130-134, 2015
ISSN 1990-9233
© IDOSI Publications, 2015
DOI: 10.5829/idosi.mejsr.2015.23.ssps.33

Misbehavior Detection of Nodes in Delay Tolerant Networks

Kubra Amanullah and V. Pushpalatha

Department of Electronics and Communication Engineering,
Saveetha Engineering College, Chennai, India

Abstract: Malicious and egocentric behaviors represent a heavy threat by opposing routing in delay/disruption tolerant webs (DTNs). Due to the exceptional web characteristics, arranging a misbehavior detection scheme in DTN is considered as a outstanding challenge. We propose iTrust, a probabilistic misbehavior discovery scheme, for secure DTN steering to productive trust foundation. The basic plan of iTrust is to introduce a periodically obtainable Trustworthy Authority (TA) to judge the node's behavior supported by the collected routing evidences and probabilistically checking. We show iTrust as the inspection game and use game theory analysis by setting a suitable investigation probability, to demonstrate that TA could guarantee the security of DTN steering at a lessened expense. To more enhance the efficiency of the proposed scheme we tend to associate detected probability with a node's name, that permits a dynamic detection probability dictated by the trust of the users. The investigation and recreation results exhibit the effectiveness and productivity of the proposed scheme.

Key words: Misbehavior detection · Delay tolerant networks · Inspection game · Trustworthy authority

INTRODUCTION

Delay tolerant networks [1] (DTNs, for example, sensor systems with planned discontinuous integration, vehicular DTNs that disperse location dependent data (e.g., neighborhood advertisements, parking information, traffic reports) [9] and pocket-exchanged systems that permit people to impart without system framework, are profoundly apportioned systems that may experience the ill effects of regular disconnectivity. In DTNs, the in-transit messages, additionally named bundles, may be sent over existing link and buffered at next hop until the following connection in the way shows up (e.g., another hub moves into the range or an existing one awakens). This message propagation method is usually stated "store-carry-and-forward" strategy and also the routing is set in an "opportunistic style".

In DTNs, a node may act by dropping packets intentionally even once it has the capability to forward the data (e.g., sufficient buffers and meeting opportunities) [1], shown in Fig 1. Routing misbehavior can be caused by egocentric [5] (or rational) nodes that attempt to maximize their own benefits by enjoying the services provided by DTN whereas refusing to forward the in-transit messages for others, or malicious nodes that drop parcels or altering the parcels to launch attacks [17].

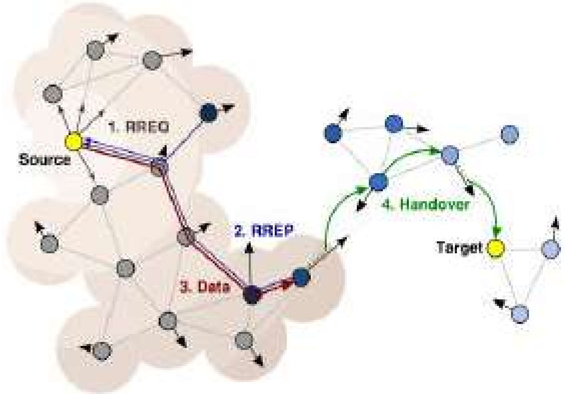

Fig. 1: An example of Delay Tolerant Networks.

The current researches show that routing misbehavior will significantly reduce the packet delivery rate and, thus, pose a significant threat against the network performance of DTN [4], [6]. Therefore, a misbehavior detection and mitigation protocol is highly

Corresponding Author: Kubra Amanullah, Department of Electronics and Communication Engineering,
Saveetha Engineering College, Chennai, India

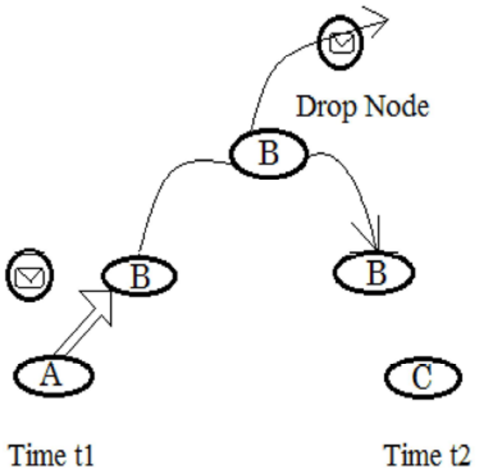

Fig. 2: An example of black hole attack in DTNs.

fasinating to assure the secure DTN routing furthermore the establishment of the trust among DTN nodes in DTNs.

Mitigating routing misbehavior has been well studied in traditional mobile [11] ad hoc networks. These works neighborhood detection or destination acknowledgement to observe packet dropping [3] and exploit credit-based and reputation-based incentive schemes to stimulate rational nodes or revocation schemes to revoke malicious nodes [1],[4]. Even if the prevailing misbehavior detection schemes work well for the traditional wireless networks, the exceptional network characteristics together with lack of contemporaneous path, high variation in network conditions, issues to predict mobility patterns and long feedback delay have created the neighborhood monitoring based misbehavior detection scheme unsuitable for DTNs. This could be illustrated by Fig. 2, in which an egocentric node [15] B receives the packets from node A however launches the black hole attack by refusing to forward the packets to the next hop receiver C. Since there is also no neighboring nodes at the moment that B meets C, the misbehavior (e.g., dropping messages) cannot be detected as a result of lack of witness, which provides the monitoring-based misbehavior detection less practical in a scattered DTN.

Proposed Methodology: In some hybrid DTN networks [2], the transmission between TA and each node could be also performed in a direct manner Since the misbehavior detection is performed periodically, the message transmission is performed in a batch model, which could further reduce the transmission overhead.

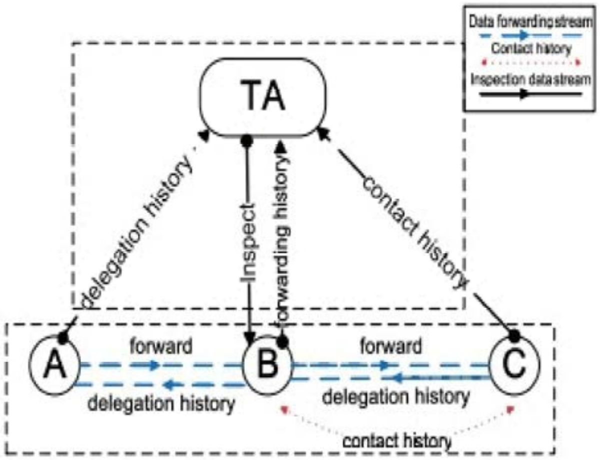

Fig. 3: Node A forwards packets to node B and gets the delegation history back. Then node B holds the packet and when it encounters node C, it gets the contact history about node B. When TA decides to check node B, TA broadcasts a message to ask all the other nodes to submit the evidences about B, hence node A submits the delegation history from node B, node B submits the forwarding history from C, node C submits the contact history about B.

Basic iTRUST Method for Misbehavior Detection in DTNs: As shown in Fig. 3, the basic iTrust [7] has 2 phases, together with routing evidence generation section and routing proof auditing section. Within the evidence generation section, the nodes can generate contact and forward proof for every contact or proof forwarding. Within the consequent auditing phase, TA can distinguish the traditional nodes from the misbehaving nodes.

Evidence Generation Section: We take a three-step information [8] forwarding method as associate example. Suppose that node A has packets, which can be forwarded to node C. Now, if node A meets another node B that might facilitate to forward the packets to C, A can replicate and forward the packets to B. Thereafter, B can forward the packets to C once C arrives at the transmission span of B. During this method, we define three forms of information forwarding evidences that might be used to judge if a node may be a malicious one or no.

Delegation Assignment Evidences: Used to record the amount of routing tasks assigned from the upstream nodes to the target node. In the audit section, the upstream nodes can submit the delegation assignment evidences to TA for verification.

Forwarding History Evidences: When a task has been successfully forwarded from one node to another node forwarding history evidences is generated. In the audit section, the investigation target node can submit his forwarding history evidences to TA to demonstrate that he has tried his best to meet the routing tasks, that are described by delegation assignment evidences.

Contact History Evidences: Whenever two nodes N m and N n meet, a new contact history evidence will be generated as the evidence of the presence of nodes N m and N n. In the audit phase, for an investigation target N m, both of N m and other nodes will submit their contact history evidence to TA for verification.

Auditing Section: In the auditing phase, TA can launch associate degree of investigation request toward node N m in the global network throughout a certain amount (t1, t2). Then, given N because of the set of total nodes in the network, every node within the network can submit its collected evidences to TA. By collecting all of the evidences associated with N m, TA obtains the set of messages forwarding requests task, the set of messages forwarded and also the set of contacted users, all of that may be verified by checking the corresponding evidences.

To check if a suspected node N m is malicious or not, TA should check if any message forwarding request has been honestly fulfilled by N m.

The contributions of this paper are often summarized as follows:

- First, we consider a general misbehavior detection framework which supports a series of newly introduced data progressing evidences. The recommended evidence framework could not only detect various misbehaviors however also be compatible to varied routing protocols [10].
- Second, we introduce a probabilistic misbehavior detection technique [12], [13], [14] by adopting the inspection game. A detailed game theoretical analysis can demonstrate that the cost of misbehavior detection could be significantly reduced while not compromising the detection performance. They also discuss how to correlate a user's reputation (or trust level) to the detection probability, which is expected to further bring down the detection probability.

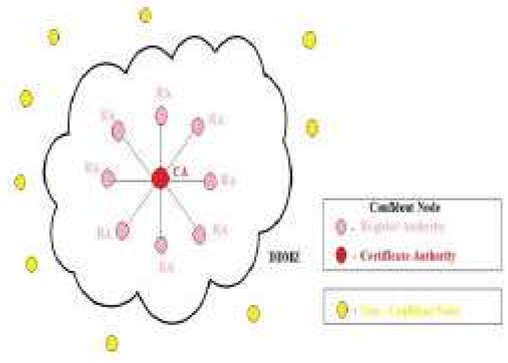

Fig. 4: Dynamic Demilitarized Zone (DDMZ)

- Third, we use intensive simulations similarly as detailed analysis to demonstrate the effectiveness and the productivity of the iTrust.

Secure Mechanism for MANETs: In wired/wireless infrastructure networks, a trusty third party, called Certification Authority (CA), is required to certify users' digital certificate. It is expected to produce a secure communication among users and guarantee some security needs like confidentiality, integrity and authentication of transited knowledge. To avoid the one purpose of failure for the certificate authority (CA) in MANET, a localized answer is planned where nodes are classified into completely different clusters. Each and every cluster should contain a minimum of 2 assured nodes. One is called as CA and therefore the another as register authority RA.

For protecting the CA node against the potential attacks a Dynamic Demilitarized Zone (DDMZ) is proposed, shown in Fig 4. It is formed from one or more RA node. The problems of this model are: (1) Clusters with one confident node, CA, cannot be created which negatively affect clusters' services and stability. (2) Clusters with high density of RA can cause channel collision at the CA. (3) Clusters' lifetime are reduced since RA monitors are always launched. So we propose a model supported mechanism that may allow clusters with single trustworthy node (CA) to be created. Our mechanism can inspire nodes that don't fit in to the assured community to participate by providing them incentives within the type of trust, which might be used for cluster's services.

A distributed clustering algorithm [16] is planned to cluster nodes based on a collection of trustworthy nodes that belong to a assured community. A cluster head is chosen among trustworthy nodes to play the role of CA.

To beat the single point of failure attack against CA, a collection of one-hop nodes called RA, are selected from the set of trustworthy nodes to create a Dynamic Demilitarized Zone (DDMZ).

Design Requirements: The design requirements include:

- Motivate nodes from a non-confident community to serve as RA and build a DDMZ.
- Increase the clusters' life based on a particular selection-criteria operate by choosing the RA nodes.
- Increase the quantity of clusters and reduce the cluster's size.

MANET Clustering Algorithm: A clustering algorithm that clusters MANET and elects a CA in every cluster. To confirm the security, it's assumed that the set of nodes belong to a confident community. For clusters with one trusty node, the CA is chosen among these nodes which rely on node's stability that will increase cluster's period. And also ensures the authentication and integrity of the transited knowledge throughout the election method.

Each trusty node sends 2 successive *how do you do* message in order to calculate the Relative Mobility (RM), after that, it announces itself as CA with an explicit cluster's size (k-hop). When a trusty node receives a beacon, from one in every of its neighbors, it execute clustering rule to vary its status from cluster-head (CA) to cluster-member. the choice to change the standing from CA to cluster-member depends on two main parameters: Security and stability. A CA is regarded as more stable than others even if it has a low relative mobility. Any trusty node with relative mobility greater than a selected threshold is taken into account as unstable and so won't be considered during the CA election method. The nodes settled between two adjacent clusters will become gateway (GW).

Once the CA node is elective per cluster, it starts to transmit cluster's beacon so as to tell the cluster's member nodes about its convenience. The cluster's nodes that aren't receiving any beacon from a CA for a predefined amount of time is considered as unavailable.

The selection criteria function has the subsequent parameters:

Trust Level/Metric: This determines the confident level of nodes that is evaluated by the observation mechanism. every node features a name generated by the monitoring mechanisms consistent with its contribution within the network like forwarding quantitative relation or others network' services.

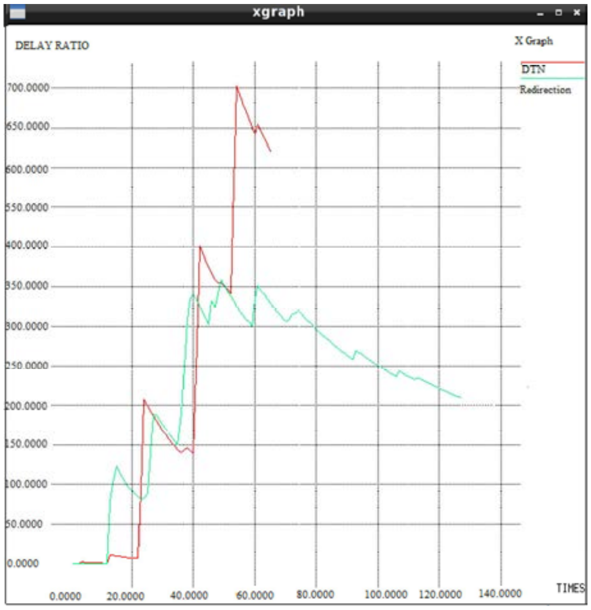

Fig. 5: Detected rate of malicious node

Stability Metric: RA node's stability is predicated on the relative mobility according to the CA node. The mobility metric is predicated on the power level detected at receiving node, it's indicative of the space between the transmission and receiving node pairs. The quantitative relation between the two successive packets transmissions offers an honest information about the relative mobility between the two neighboring nodes.

Residual Energy Metric: This determines the residual energy state of the nodes. this can be conjointly a non-public information of a node.

Connectivity Degree: It's the amount of links a node is connected with. A node having greater connectivity degree implies that it can cover more nodes for monitoring within the cluster.

RESULTS AND DISCUSSION

In our experiment, we adopt the First Contact routing protocol, which is a single-copy routing mechanism. We set the time interval T to be about 400 s as the default value and we deploy 26 nodes on the map, respectively. With each parameter setting, we conduct the experiment. We use the packet loss rate (PLR) to indicate the misbehavior level of a malicious node.

CONCLUSION

The Dynamic Demilitarized Zone (DDMZ) is made from one or additional RA nodes, where the CA and RA nodes belong to the confident community. Clusters with one confident node, CA, cannot be created and so clusters sizes are increased that negatively affect clusters stability and services. Thus, we proposed a model based on mechanism design that allow clusters with single trusted node (CA) to be created. Once the chance of attacks is high, more RA nodes need to be selected to form a robust DDMZ. Simulation results indicate that our model result in additional range of clusters and quality DDMZ can be created based on selection criteria function (F).

REFERENCES

1. Zhu, H., X. Lin, R. Lu, Y. Fan and X. Shen, 2009. "SMART: A Secure Multilayer Credit-Based Incentive Scheme for Delay-Tolerant Networks," IEEE Trans. Vehicular Technology, 58(8): 828-836.
2. Burgess, J., B. Gallagher, D. Jensen and B. Levine, 2006. "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM '06.
3. Marti, S., T.J. Giuli, K. Lai and M. Baker, 2000. "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom '00.
4. Lu, R., X. Lin, H. Zhu and X. Shen, 2010. "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., 9(4): 1483-1493, Apr. 2010.
5. Anderegg, L. and S. Eidenbenz, 2003. Ad hoc-VCG: A truthful and cost efficient routing protocol for mobile ad hoc networks with selfish agents. Proceedings of the ACM MobiCom'03, San Diego, California.
6. Leshem, A. and E. Zehavi, 2009. "Game theory and the frequency selective interference channel-A tutorial," IEEE Signal Process. Mag., 26(5): 28-40, Sep. 2009.
7. Osborne, M. and A. Rubinstein, 1994. A Course in Game Theory. Cambridge, MA: MIT Press.
8. Zhang, L., Y.C. Liang, Y. Xin and H.V. Poor, 2009. "Robust cognitive beamforming with partial channel state information," IEEE Trans.Wireless Commun., 8(8): 4143-4153, Aug. 2009.
9. Gao, W. and G. Cao, 2011. "User-Centric Data Dissemination in Disruption-Tolerant Networks," Proc. IEEE INFOCOM '11.
10. Keranen, A., J. Ott and T. Karkkainen, 2009. "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int'l Conf. Simulation Tools and Techniques (SIMUTools '09).
11. Spyropoulos, T., K. Psounis and C.S. Raghavendra, 2008. "Efficient routing in intermittently connected mobile networks: The single-copy cast," IEEE/ACM Trans. Netw., 16(1): 63-76, Feb. 2008.
12. Lindgren, A., A. Doria and O. Schelen, 2004. "Probabilistic routing in intermittently connected networks," in Proc. SAPIR, pp: 239-254.
13. Fall, K., 2003. "A delay-tolerant network architecture for challenged internets," ACM SIGCOMM, pp: 27-34.
14. Gao, W., Q. Li, B. Zhao and G. Cao, 2009. "Multicasting in delay tolerant networks: A social network perspective," Proc. ACM MobiHoc.
15. Li, F., A. Srinivasan and J. Wu, 2009. "Thwarting blackhole attacks in distruption-tolerant networks using encounter tickets," Proc. IEEE INFOCOM.
16. Hui, P., E. Yoneki, S. Chan and J. Crowcroft, 2007. Distributed community detection in delay tolerant networks. Proc. MobiArch.
17. Li, Q., S. Zhu and G. Cao, 2010. Routing in Socially Selfish Delay Tolerant Networks. Proc. INFOCOM.