IJCSMA

T. Anusha *et al*, International Journal of Computer Science and Mobile Applications,
Vol.1 Issue. 5, November- 2013, pg. 44-50 ISSN: 2321-8363

Improving The Trust and Adversary Detection Process For Delay-Tolerant Networks

T. Anusha[1], N. Srihari Rao[2]
[1]M.Tech. Student, CSE Dept, CMR Institute of Technology, Hyderabad, A.P
Email-id: anushareddy.ram@gmail.com
[2]Associate Prof., CSE Dept., CMR Institute of Technology, Hyderabad, A.P
MIAENG, MCSI, MISTE
Email-id: raon2006@gmail.com

Abstract

Trust and reputation play critical roles in most environments wherein entities participate in various transactions and protocols among each other. A potential low-cost solution to the problem of connecting devices in areas, where end-to-end connectivity cannot be assumed is required, and such low-cost networks are known as Delay Tolerant Networks (DTNs). Delay/Disruption Tolerant Networks have been identified as one of the key areas in the field of wireless communication, wherein sparseness and delay are particularly high. DTNs are characterized by large end to- end communication latency and the lack of end-to-end path from a source to its destination. These characteristics pose several challenges to the security of DTNs. Iterative Trust and Reputation Management (ITRM) mechanism is an iterative malicious node detection mechanism for DTNs. This scheme is a graph-based iterative algorithm motivated by the prior success of message passing techniques for decoding low-density parity-check codes over bipartite graphs. ITRM mechanism is used for completing our research project work. ITRM scheme is far more effective than well-known reputation management techniques such as the Bayesian framework and EigenTrust.

Index Terms

Trust, Reputation; DTN; Attack; Mobile Ad-Hoc Network (MANET)

I. Introduction

Trust depends on the trusted entity or party, and the reliability of the trusted entity or party. Trust and reputation systems [4] represent a significant trend in decision support for Internet mediated service provisions. DTN is a computer network architecture which tries to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Trust and reputation play critical roles in most environments wherein entities participate in various transactions and protocols among each other. The recipient of the service has no choice but to rely on the reputation of the service provider based on the latter's prior performance. Trust and reputation systems have found widespread adoption in online communities, web services, ad-hoc networks, P2P computing, and in e-commerce communities. In most environments, the consumer of the service (e.g., the buyer) has no choice but to rely on the reputation of the service provider (e.g., the seller) based on the latter's prior performance. Hence, the service recipient should take a prior risk before receiving the actual service. This risk puts the recipient into an unprotected position since he has no opportunity to try the service before he receives it.

Delay and disruption-tolerant networks [3] are characterized by their lack of connectivity, resulting in a lack of instantaneous end-to-end paths. DTNs are characterized by intermittent contacts between nodes, leading to space time evolution of multi hop paths (routes) for transmitting packets to the destination, and hence intermediate nodes may need to store, carry, and wait for opportunities to transfer data packets toward their destinations. Hence, DTNs are much more general than MANETs in the mobile network space, whereas MANETs are special types of DTNs. In developing regions, especially rural areas, DTNs can be used to provide network access for education, health care or government services. They also enhance low bandwidth Internet connections to transfer large files at low cost, while using the Internet connection for control messages.

The rest of this paper is organized as follows. In Section II, the related work is summarized. Section III explains the method used for our project. Section IV presents the results of our project work. Section V gives conclusions and future work.

II. Related Work

Reputation systems for P2P networks [5] and online systems received a lot of attention However, reputation systems for P2P networks are either not applicable for DTNs or they require excessive time to build the reputation values of the peers. Most proposed P2P reputation management mechanisms utilize the idea that a peer can monitor others and obtain direct observations or a peer can enquire about the reputation value of another peer and hence, obtain indirect observations before using the service provided by that peer. However, neither of these techniques is practical for DTNs. In DTNs, direct observations are not possible. However, considering the opportunistic and intermittent connectivity in DTNs, this method requires excessive time to build the reputation values of all peers in the network. The EigenTrust algorithm [6] is not practical for applications in which the trustworthiness and reputation are two separate concepts. In schemes utilizing the Bayesian framework [7], each reputation value is computed independent of the other nodes' reputation values.

Dellarocas [8] proposed to use the Cluster Filtering method for reputation management. However, Cluster Filtering introduces quadratic complexity while the computational complexity of ITRM [2] is linear with the number of users in the network. As a result, this scheme is more scalable and suitable for large-scale reputation systems. Different from the existing schemes, ITRM algorithm is a graph-based iterative algorithm motivated by the previous success on message passing techniques and belief propagation algorithms. The challenges of providing secure communication in DTNs, is discussed and the use of Identity-Based Cryptography (IBC) is suggested in [9]. In this scheme, source authentication and anonymous communication as well as message confidentiality are provided using IBC. In [10], the use of packet replication is proposed to improve message delivery rate instead of using cryptographic techniques. The ITRM mechanism provides malicious node detection and high data availability with low packet latency in the presence of Byzantine attacks.

III. Method

The challenging problem of countering Byzantine (insider) attacks is that it gives serious damage to the network in terms of data availability, latency, and throughput. They are not explicitly considered for our research work instead we considered two broader types of attacks: 1) attack on the network communication protocol, 2) attack on the security mechanism.

i. Packet drop and packet injection (attack on the network communication protocol)

An insider adversary drops legitimate packets it has received. This behavior of the malicious nodes has a serious impact on the data availability and the total latency of the network.

ii. Bad mouthing and ballot stuffing on the trust management (attack on the security mechanism)

A legitimate node needs feedback from a subset of nodes to determine its trust on a specific node. When a malicious node is an element of this subset, it gives incorrect feedback in order to undermine the trust management system. Bad-mouthing and ballot-stuffing attacks attempt to reduce the trust on a victim node and boost the trust value of a malicious ally, respectively.

iii. Random attack on trust management (attack on the security mechanism)

A Byzantine node may adjust its packet drop rate on the scale of zero-to-one to stay under cover, making it harder to detect.

iv. Bad mouthing and ballot stuffing on the detection scheme (attack on the security mechanism)

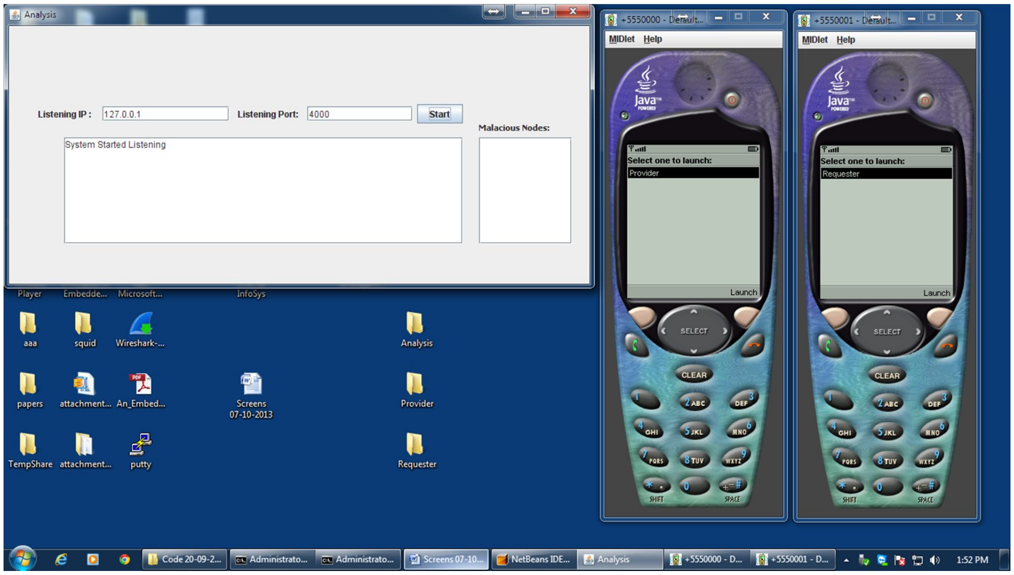
Every legitimate node, in order to detect the nature of every network node, creates its own trust entries in a table referred to as the node’s rating table for a subset of network nodes for which the node has collected sufficient feedbacks.

Iterative Detection for DTNs

ITRM is adapted in DTNs [1] as an iterative malicious node detection mechanism. In this mechanism, a judge node creates its own rating about another network node by collecting feedbacks about the node and aggregating them. Each judge node has a table referred to as a rating table whose entries which are obtained using the feedback mechanism are used for storing the ratings of the network nodes. In DTNs, due to intermittent contacts, a judge node has to wait for a very long time to issue its own ratings for all the nodes in the network. However, it is desirable for a judge node to have a fresh estimate of the reputation of all the nodes in the network in a timely manner, mitigating the effects of malicious nodes immediately. To achieve this goal, this iterative detection mechanism operates by using the rating tables formed by other nodes acting as judges themselves. The rating table of a judge node can be represented by a bipartite graph consisting one check vertex and some bit vertices i.e., a subset of all the nodes in the network for which the judge node has received sufficient number of feedbacks to form a rating with high confidence.

IV. Results

For our project work, ITRM mechanism is implemented and different results are shown below. The mechanism is implemented in Java technology on a Pentium-IV PC with minimum 20 GB hard-disk and 1GB RAM. We have achieved good results after testing on different datasets. The implemented scheme detects and isolates the malicious nodes from the network to minimize their impact.



Listening IP : 127.0.0.1

Listening Port: 4000

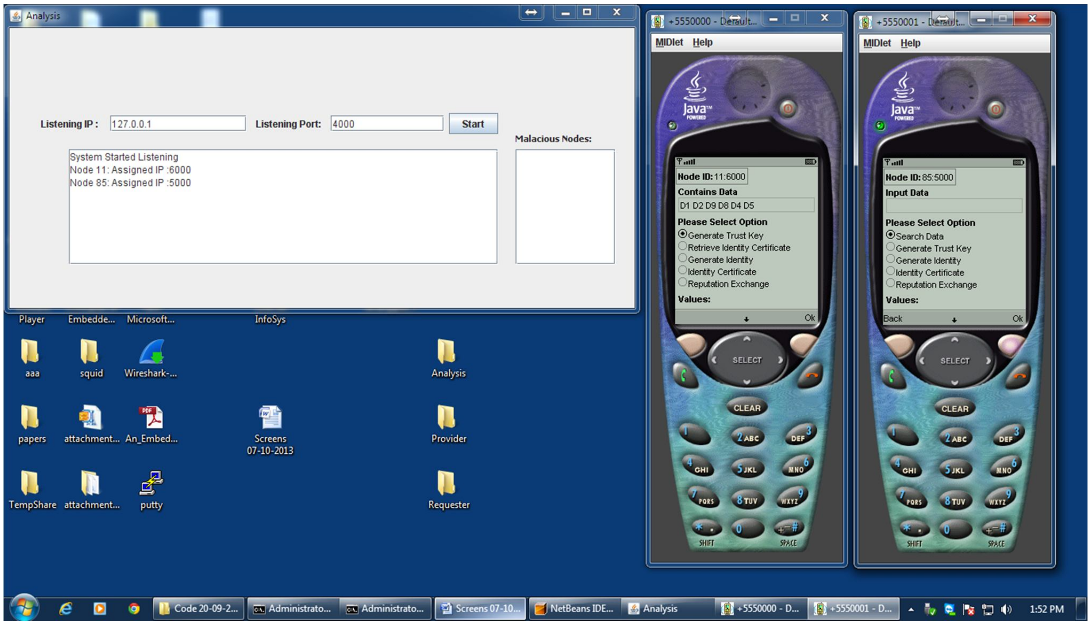
System Started Listening

Malacious Nodes:

Select one to launch:
Provider

Select one to launch:
Requester

Fig. 1: Showing the Provider and Requester adjacently



Listening IP : 127.0.0.1 **Listening Port:** 4000

Malacious Nodes:

```
System Started Listening
Node 11: Assigned IP :6000
Node 85: Assigned IP :5000
```

Node ID: 11:6000

Contains Data

D1 D2 D9 D8 D4 D5

Please Select Option

● Generate Trust Key
○ Retrieve Identity Certificate
○ Generate Identity
○ Identity Certificate
○ Reputation Exchange

Values:

Ok

Node ID: 85:5000

Input Data

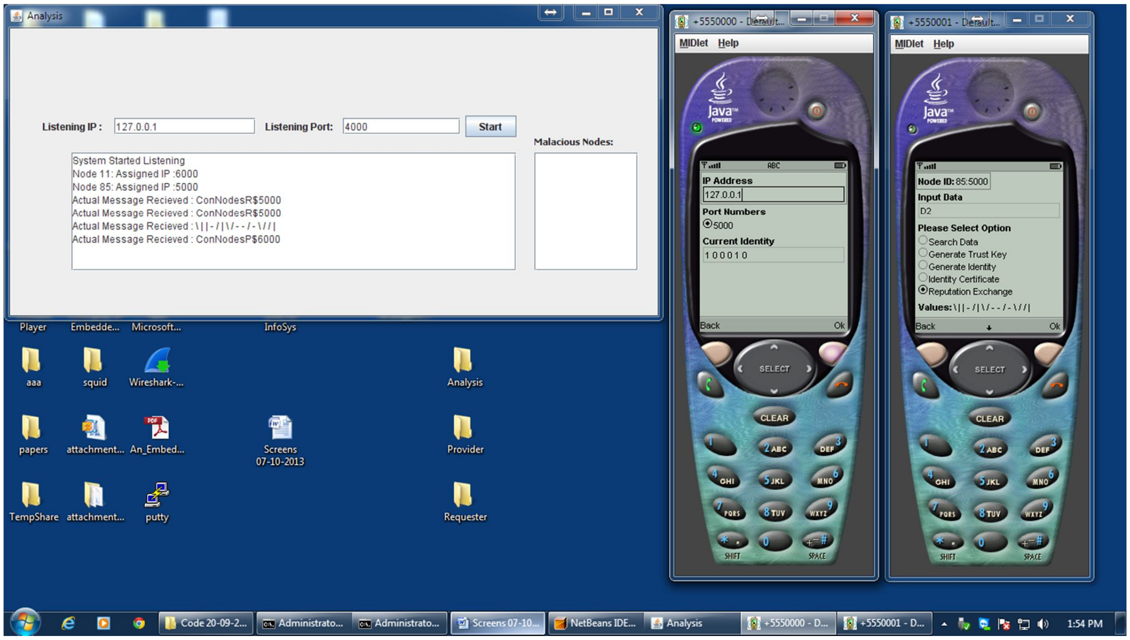
Please Select Option

● Search Data
○ Generate Trust Key
○ Generate Identity
○ Identity Certificate
○ Reputation Exchange

Values:

Back Ok

Fig. 2: Input data is entered in Requester side



Listening IP : 127.0.0.1 **Listening Port:** 4000

Malacious Nodes:

```
System Started Listening
Node 11: Assigned IP :6000
Node 85: Assigned IP :5000
Actual Message Recieved : ConNodesR$5000
Actual Message Recieved : ConNodesR$5000
Actual Message Recieved : \||-/|\/--/-\//|
Actual Message Recieved : ConNodesP$6000
```

IP Address

127.0.0.1

Port Numbers

● 5000

Current Identity

1 0 0 0 1 0

Back Ok

Node ID: 85:5000

Input Data

D2

Please Select Option

○ Search Data
○ Generate Trust Key
○ Generate Identity
○ Identity Certificate
● Reputation Exchange

Values: \||-/|\/--/-\//|

Back Ok

Fig3: After simultaneously transferring the data in Provider and Requester, we get the trust value

V. Conclusions & Future work

In this paper, we introduced a robust and efficient security mechanism for delay-tolerant networks. The proposed security mechanism consists of a trust management mechanism and an iterative reputation management scheme. The trust management mechanism enables each network node to determine the trustworthiness of the nodes with which it had direct transactions. On the other hand, ITRM takes advantage of an iterative mechanism to detect and isolate the malicious nodes from the network in a short time. The performance of the ITRM scheme is observed to be effective in detecting the malicious nodes even in the presence of the attacks on the trust and detection mechanisms. Moreover, this mechanism provides high data availability with low information latency by detecting and isolating the malicious nodes in a short time.

The proposed system can be enhanced by including the global reputation data which can be better protected against any malicious modification by the third party peer and are immune to any malicious modifications by their owner. The enhanced system will be able to reduce the number of malicious transactions and consumes less bandwidth per transaction than the other reputation systems proposed. It will also handle the problem of highly erratic availability pattern of the peers in P2P networks. Currently, the reputation of the provider is considered and the reputation of the requester is ignored. This system can be extended to encapsulate the reputations of both the provider and the requester. In addition, instead of generic number values, the reputation values can be modified in accordance with the context of the reputation.

References

[1] Erman Ayday, and Faramarz Fekri, “An Iterative Algorithm for Trust Management and Adversary Detection for Delay-Tolerant Networks,” IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 11, NO. 9, SEPTEMBER 2012.

[2] E. Ayday, H. Lee, and F. Fekri, “An Iterative Algorithm for Trust and Reputation Management,” Proc. IEEE Int’l Symp. Information Theory (ISIT ’09), 2009.

[3] T.Anusha Reddy and N.Srihari Rao “A Comprehensive Survey on Security Issues of Delay Tolerant Networks.” IJCSRT Journal Volume-1,Issue-5, Oct-2013,Pg No:70-75.

[4] A. Josang, R. Ismail, and C. Boyd, “A Survey of Trust and Reputation Systems for Online Service Provision,” Decision Support Systems, vol. 43, no. 2, pp. 618-644, 2007.

[5] E. Damiani, D.C. di Vimercati, S. Paraboschi, P. Samarati, and F. Violante, “A Reputation-Based Approach for Choosing Reliable Resources in Peer-to-Peer Networks,” Proc. Ninth ACM Conf. Computer and Comm. Security (CCS ’02), pp. 207-216, 2002.

[6] S.D. Kamvar, M.T. Schlosser, and H. Garcia-Molina, “The Eigentrust Algorithm for Reputation Management in P2P Networks,” Proc. 12th Int’l Conf. World Wide Web (WWW ’03), pp. 640-651, 2003.

[7] S. Buchegger and J. Boudec, “Performance Analysis of CONFIDANT Protocol (Coorperation of Nodes: Fairness in Dynamic Ad-Hoc Networks),” Proc. ACM MobiHoc, June 2002.

[8] Dellarocas, “Immunizing Online Reputation Reporting Systems against Unfair Ratings and Discriminatory Behavior,” Proc. Second ACM Conf. Electronic Commerce (EC ’00), pp. 150-157, 2000.

[9] S. Cui, P. Duan, and C. Chan, “An Efficient Identity-Based Signature Scheme with Batch Verifications,” Proc. First Int’l Conf. Scalable Information Systems (InfoScale ’06), p. 22, 2006.

[10] J. Burgess, G. Bissias, M. Corner, and B. Levine, “Surviving Attacks on Disruption-Tolerant Networks without Authentication,” Proc. Eighth ACM Int’l Symp. Mobile Ad Hoc Networking and Computing, pp. 61-70, 2007.

Authors’ Profile

T.Anusha Reddy had B.Tech from Christu Jyothi Institute of Technology & Science, Yeshwanthapur, Jangon. She is an M.Tech. student in CSE Department of CMR Institute of Technology, Hyderabad. She is currently working for her M.Tech. research project work under the guidance of Mr.N.Srihari Rao. Her areas of interest include Network Security, Computer Networks, and Programming languages.

N.Srihari Rao had his B.E. from C.B.I.T., Hyderabad, and he had M.E. from Karunya Deemed University, Coimbatore. He is currently working as Associate Professor in CSE Department of CMR Institute of Technology, Hyderabad. He is working for Ph.D. in CSE Discipline at JNTUA Univeristy, Anantapur. His areas of interest are Network Security, Data Mining, Image Processing, and ICT for various fields.