The International Journal Of Engineering And Science (IJES)
|| Volume || 4 || Issue || 5 || Pages || PP.06- 11|| 2015 ||
ISSN (e): 2319 – 1813 ISSN (p): 2319 – 1805

Trust Providence in Delay Tolerant Networks

Shruti V Deshapande, Prof. Kavita D Hanabaratti
[1, 2,] *Department of Computer Science, GIT Belgaum*

----------**ABSTRACT**----------
The network consists of several nodes, some nodes represents malicious and selfish behavior. This gives the heavy threat for the routing in Delay Tolerant networks(DTNs). The DTNs have unique characteristic so designing a misbehavior detection scheme is very difficult. The probabilistic misbehavior detection scheme that is iTrust, is established for secure routing in DTN. The iTrust introduces a Trusted Authority (TA) for detecting the node's behavior. By collecting the routing evidences from the nodes the TA checks the node about its behavior then performs the appropriate actions for the behavior of nodes. TA gives the security of DTN routing at lower cost. The detection probability is correlated with a node's reputation, this gives the dynamic detection probability based on the trust of users. The simulation results show that the proposed scheme is efficient for establishing trust with the DTNs.

KEYWORDS- Compensation *(w), Delay tolerant networks (DTN),misbehavior detection scheme, punishment (C), trusted authority(TA) .*

Date of Submission: 11-May-2015 Date of Accepted: 30-May-2015

I. INTRODUCTION

Delay tolerant networks (DTNs) acts as overlay on top of regional networks. It supports interoperability of regional networks by accommodating long delays between and within regional networks including the internet. DTNs have unique characteristic such as the end-to-end connectivity is intermittent, long delays, asymmetric data rates, high error rates[1]. The DTNs uses the "store-carry-and-forward" strategy. The in-transit messages are named as bundles, and can be sent over the existing link until the next link in the path appears the bundles are stored in next hop node. The routing is carried in an opportunistic fashion[2][3].

Routing misbehavior can be caused by selfish nodes or malicious nodes. The main intention of selfish nodes is to save its own power, capacity, memory cycles by enjoying the services provided by DTN and refuses to forward the bundles further. The malicious nodes intention is to attack or damage the network by droping the packets intentionally or creating the false route to the destination. This will reduce the packet delivery rate and produces a heavy threat against the network performance of DTNs[4][5]. Therefore, a misbehavior detection and controlling scheme is very much required to provide a secure and trustable DTN routing.[6]

For controlling the misbehavior of nodes the traditional mobile adhoc network uses the techniques such as neighborhood monitoring or destination acknowledgement. These techniques exploits the credit-based and reputation-based incentive schemes for selfish nodes and revocation schemes for malicious nodes[7] but these techniques are not suitable for DTNs because of the unique characteristic such as intermittent connectivity, large or long delays, asymmetric data rates, high error rates etc.[8-11]

In the example Fig1 shown below A acts as sender wants to send packets to receiver C. B acts as intermediate neighboring node. A sends packets to B, B will not forward the packets to the receiver C and launches the black hole attack. In the black hole attack the malicious nodes either drops packets or creates the false route to damage the network. At the moment B meets C there will be no neighboring nodes that is no witness, so the misbehavior cannot be easily detected.

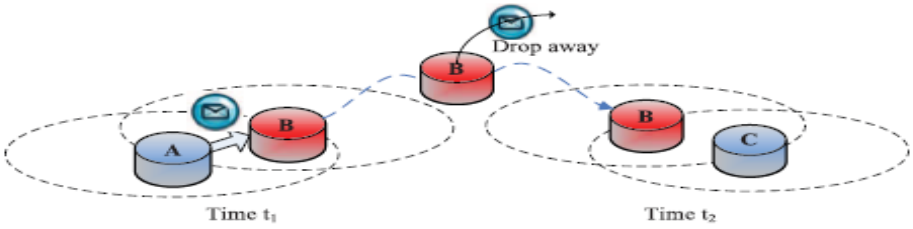

Fig 1.1.example of black hole attack in DTN.

For this purpose the traditional neighborhood monitoring techniques are less practical in a sparse DTN. Recently the misbehavior detection technique such as forwarding history verification is proposed but it is costly in terms of transmission overhead, security overhead and verification cost.

The iTrust a probabilistic misbehavior detection scheme for establishing trust in DTNs. Different from older works which only consider the misbehavior detection or incentive scheme, it jointly consider both misbehavior detection and incentive scheme in the same framework. [12][13]

The iTrust scheme is inspired from the inspection game in which an inspector verifies inspectee, adheres to certain legal rules. The inspectee wants to violate the rules while the inspector performs the partial verification and corresponding punishment is given to discourage the misbehaviors of inspectees. Furthermore, the inspector checks the inspectee with a higher probability than Nash Equilibrium points to remove the offences, as the inspectee has to select legal rules for its rational behavior.

iTrust introduces a periodically available TA(Trusted Authority) to perform the probabilistic detection of selfish node by collecting the evidence history from all the nodes which are involved in packet transmission. Then, TA decides to punish or compensate the node based on its behavior. This achieves the tradeoff between the security and detection cost. [14][15]

To further improve the performance of the proposed probabilistic inspection scheme, the reputation system is also introduced. In which the inspection probability can be varied 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 will be checked with a higher probability. Thus the proposed misbehavior detection scheme is very efficient for secure routing as well as providing trust with the user.[16]

The rest of the paper is organized as follows. Section 2 includes the related work. Section 3 gives the problem formulation. Section 4 explains system design. Section 5 gives the working process of the proposed scheme. Section 6 gives the interpretation of results. Finally, Section 7 provides the conclusion.

II. RELATED WORK

H.Zhu, S.Du, Z.Gao, M.Dong, Z.Cao says that DTNs are networks of self-organizing wireless nodes, where end-to-end connectivity is intermittent. To detect the misbehavior in DTN probabilistic misbehaviour detection scheme iTrust provides Trusted Authority (TA) for detecting the node's behavior. By collecting the routing evidences from the nodes the TA checks the node about its behavior then performs the appropriate actions for the behavior of nodes. iTrust is designed as inspection game and performs game theoretical analysis using an appropriate investigation probability. TA gives the security of DTN routing at lower cost.[1]

Q. Li, S. Zhu, and G. Cao says that routing misbehavior can be caused by selfish (or rational) nodes, intention is to maximize their own benefits and enjoys the services of DTN while refuses to forward the bundles to others, or malicious nodes intention is to drop the packets even when it has the capability to forward the data. This will reduce the packet delivery rate and gives the severe threat against the network performance of DTN. The Social Selfishness Aware Routing (SSAR) algorithm is used to allow the user selfishness and gives the good routing performance. For selecting the next hop node, SSAR algorithm checks both users wish and the contact opportunity in the neighbouring nodes. This results to better forwarding strategy than other approaches.[2]

H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen says that DTNs exists end-to-end network connectivity is not fully available. The intermediate nodes present in the communication path are require to do store-carry-forward mechanism. The messages are called as bundles and it is performed in opportunistic way so it is called as opportunistic data forwarding. The selfish or malicious nodes, main intention is to waste the resources by not forwarding packets or by droping packets. To solve this problem the secure multilayer credit-based incentive scheme is generated. This credit based scheme is used to resolve the problem of detection overhead and provides the efficient optimization techniques..[3]

H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen says that the wireless mesh networks (WMNs) are usually contain a high frequency inter-domain roaming events with the mesh access points (MAPs). The secure localized authentication and billing (SLAB) scheme is one of the good solution for roaming and billing events in WMNs. The SLAB is proposed to provide fully protected network transmission. The SLAB provides the secure roaming facility and billing facility in metropolitan area WMNs. [4]

R. Lu, X. Lin, H. Zhu, and X. Shen says that (DTNs) are a class of networks which has characteristics as lack of guaranteed connectivity, low frequency between nodes, long propagation delays, asymmetric data rates within the network. The message transmission in DTN takes place in store-carry-forward manner. The selfish nodes in DTN gives catastrophic damage to opportunistic routing scheme. For solving the selfishness problem the incentive protocol, Pi is proposed. The source node sends a message, and attaches some incentive on the bundle, which is very attractive and good to all nodes. With the fair incentive scheme, the selfish DTN nodes can be resolved and gives good packet delivery performance..[5]

III. PROBLEM FORMULATION

The network consists of several nodes, some nodes represents malicious and selfish behavior. This gives rise to heavy threat against routing in Delay/Disruption Tolerant networks(DTNs). Since DTNs have unique characteristic such as as intermittent connectivity, large or long delays, asymmetric data rates, high error rates etc, so designing a misbehavior detection scheme in DTNs is very difficult.

IV. SYSTEM DESIGN

The system Design is defined as the process of, applying various techniques and principles for the purpose of defining the elements of a system such as the architecture, modules and components to satisfy specific needs. System architecture includes the system components or building blocks that will work together and creates the overall system.

4.1 Basic System Architecture:

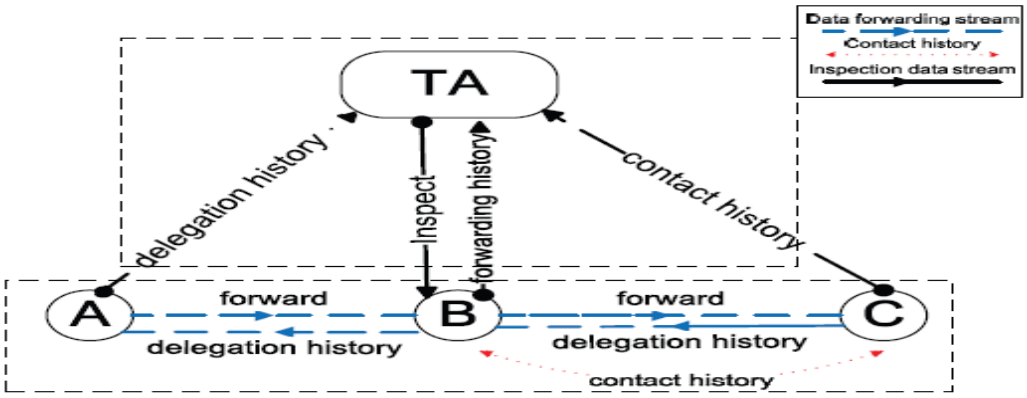

Fig 4.1.1 System Architecture

The basic system architecture involves mainly two phases. One is routing evidence generation phase and second is the auditing phase.

In the routing evidence generation phase, A forwards packets to B, then gets the delegation history back. B holds the packet and then forwards to C and gets the delegation history back. 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 evidences about B, then A submits the delegation history to TA, B submits the forwarding history (delegation history from C) to TA, C submits the contact history about B to TA. By checking these evidences TA will going to decide whether the node is malicious or not.

4.2Block diagram:

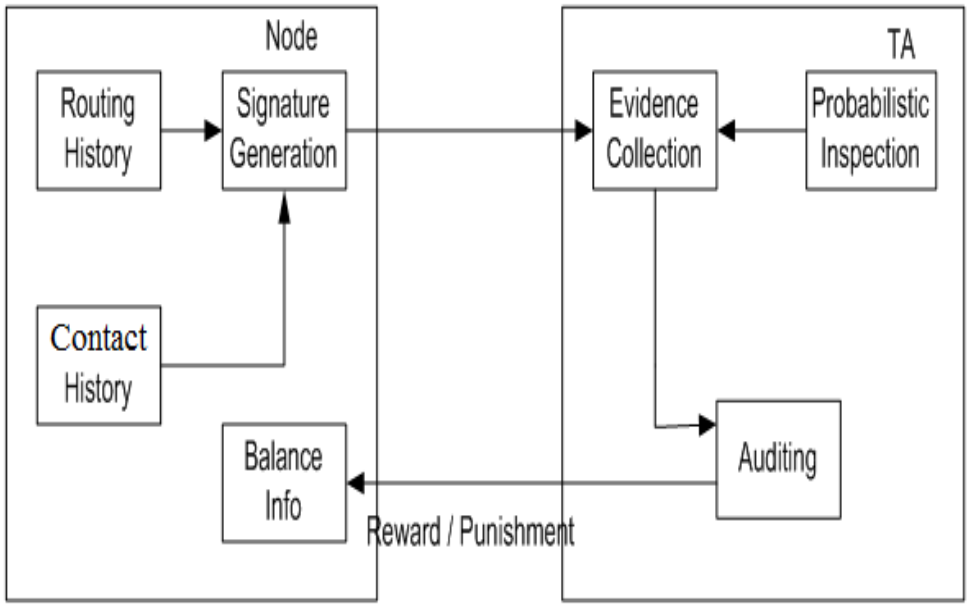

Fig 4.2.1Block diagram

There are mainly two modules in the block diagram. One is Node and other is TA(trusted authority). Node module consists of sub modules. Routing history is going to maintain a history of all nodes from source to destination including intermediate nodes that is the entire path. Contact history is going to maintain the history of only contacted nodes that is from one node to its next hop node. Signature generation produces the signature by using the routing and contact history. This is provided to TA module. TA performs the evidence collection from all the nodes. This performs the probabilistic inspection of nodes for checking the nodes behavior. In auditing it verifies if the node is detected as selfish, that node should be punished otherwise that node is compensated or rewarded. In balance info sub module the information about the node (selfish or normal node) is maintained.

V. WORKING PROCESS

Working process involves the implementation of the project where the theoretical design is converted into the working system.

5.1 Language and platform used for implementation

For implementation purpose TCL/C++ is chosen as the programming language. Few reasons for which TCL is selected as a programming language can be outlined as follows:-

- Tcl is simpler. Those without a C/Unix background generally find Tcl syntax far easier to learn and retain.
- Tcl is smaller and easier to extend, embed, and customize.
- Tcl source code traditionally is a model of lucidity. Perl source code traditionally is dense in magic.

The NS2 Simulator is used as platform for implementation. NS is a discrete event simulator targeted at networking research. NS provides substantial support for simulation of TCP, routing, and multicast protocols over wired and wireless (local and satellite) networks.

5.2 Working process involves the following steps.

Step1. The number of nodes(n) are initialized and random numbers are generated for deploying the nodes.

Step2. Compare the calculated probability(pbr) and investigation probability(pb) which is launched by Trusted authority. If the former is less than the later then Trusted authority asks all the nodes to send some evidences about the required node.

Step3. Basic detection is performed to find the targeted node is selfish or not. In basic detection packet sent(ps) are not equal to the packet received(pr) then that node is considered as selfish one. [1]

Step4. If the node is found as selfish the punishment(c) is given for the selfish node by reducing its trust value otherwise the compensation(w) is given for that node by increasing its trust value.

VI. INTERPRETATION OF RESULTS

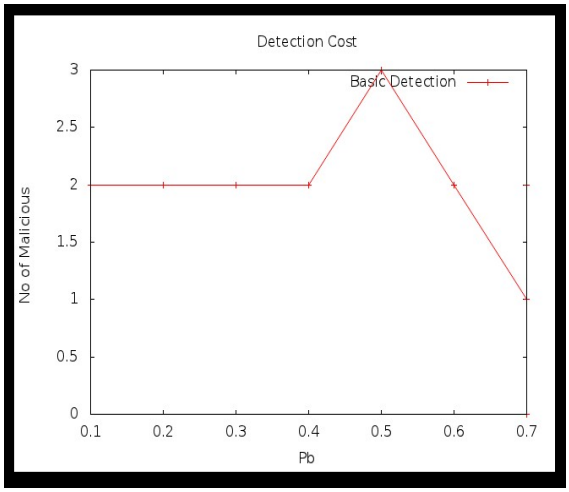

Fig.6.1.The graph shows the Detection cost, on X-axis the probability value which is given as threshold by TA (Pb) is taken and on Y-axis the number of malicious nodes with the probability set value are taken.

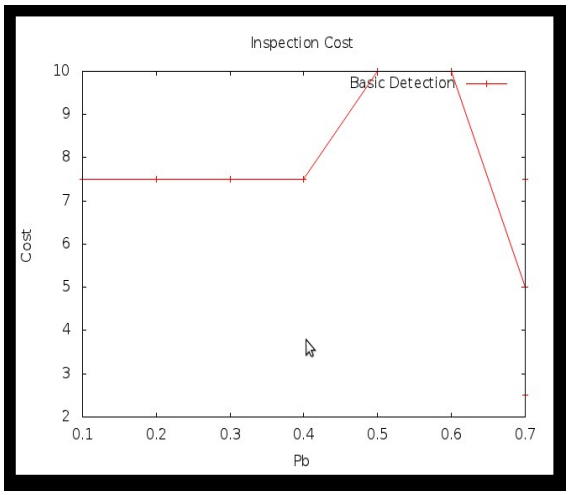

Fig.6.2. The graph shows the Inspection cost, on X-axis probability value which is given as threshold by TA(pb) is taken and on Y-axis the total time involved in detecting malicious nodes that is cost is taken.

Detection cost:

For example with x axis pb value = 0.2, no of malicious nodes were 2 and with x axis pb value = 0.5, no of malicious nodes were 3.

The performance of iTrust will be same when the detection probability given as threshold by TA is up to 0.4 that is 40 percent, but the performance of iTrust increases when the detection probability given by TA is in between 0.4 to 0.5 (40 to 50 percent). Thus, the malicious node rate has less effect on the detection cost of malicious nodes so iTrust will be effective scheme for any number of malicious nodes.

Inspection Cost :
for example with x axis pb value = 0.2 , the cost is 7.5 with x axis pb value = 0.5 , the cost is 10.

The performance of iTrust saves lot of resources on the inspection by choosing appropriate detection probability.

CONCLUSION & FUTURE WORK

The proposed probabilistic misbehavior detection scheme(iTrust), which reduces the misbehavior detection overhead effectively. The scheme is modeled as the inspection game and shows the appropriate probability setting and gives the security of DTNs at lower overhead and provides the trust in the path of DTNs. The simulation results can gives the reduced transmission overhead provided by misbehavior detection and detects the malicious nodes effectively. The future work will focus on the extension of iTrust to other kinds of networks.

REFERENCES

[1] H.Zhu, S.Du, Z.Gao, M.Dong, Z.Cao, "Probabilistic misbehaviour detection scheme toward efficient trust establishment in delay tolerant networks." *Proc. IEEE INFOCOM '14*, Jan. 2014.

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

[3] H. Zhu, X. Lin, R. Lu, Y. Fan, 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] B.B. Chen and M.C. Chan, "Mobicent: A Credit-Based Incentive System for Disruption-Tolerant Network," *Proc. IEEE INFOCOM '10*, 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] A. Lindgren and A. Doria, "Probabilistic Routing Protocol for Intermittently Connected Networks," *draft-lindgren-dtnrg-prophet- 03*, 2007.

[11] 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.

[12] R. 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

[13] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," *Proc. ACM MobiCom'00*, 2000.

[14] Ing-Ray Chen, Fenye Bao,MoonJeong Chang and Jin-Hee Cho, "Dynamic Trust Management for DTNs and its application to secure routing" *IEEE Transaction on parallel and distributed systems, vol 25*,no 5, may 2014.

[15] J.Ameen Basha , D.S Arul Mozhi, "Detection of Misbehaviour Activities in Delay Tolerant Network Using Trust Authority" *IJEDR, Volume 2*, Issue 2, ISSN: 2321-9939,2014.

[16] Sarawagya Singh, Elayaraja.K, "A survey of misbehaviors of node and routing attack in Delay tolerant networks" *IJSETR, Volume 4*, Issue 2, February 2015.