International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 06, June-2015

Enhanced Technique for Identification of Misbehaviour of Nodes and Trust Establishment in DTN

Seema K V
Department of Computer Science and Engineering,
H K B K C E Bangalore, India

Dr. Mala V Patil
HOD,Department of Computer Science and Engineering,
H K B K C E Bangalore, India

***Abstract*— Delay Tolerant Networks (DTNs) are a group of networks characterized by lack of guaranteed connectivity, in this kind of network message propagation is in store ,carry and forward manner which has typically low frequency of encounters between DTN nodes and long propagation delays within the network. In DTN network there may exist some selfish nodes or malicious nodes, a node could misbehave by dropping the packet intentionally even though it has the capability of transferring the packet to the destination is called selfish node. Malicious nodes that drop packets or modifying the packets to launch attacks. Malicious and selfish behaviours represent a serious threat against routing in Delay/Disruption Tolerant Networks (DTNs).Enhanced misbehaviour technique for detection of misbehaviour of nodes in DTN and trust connectivity establishment Misbehaviour of nodes causes reduction in packet delivery rate and network performance, to overcome this problem an enhanced misbehaviour detection technique is used, to increase the probability of a data being transmitted**

Keywords: Delay Tolerant Network, Reputation system, Inspection Game, Trust adversary system

I. INTRODUCTION

Delay-Tolerant Network(DTN) is a communication network which encompass all types of long-delay, disconnected, disrupted or intermittently-connected networks, these communication networks designed to withstand long delays. Disruption-tolerant networks (DTNs) attempt to route network messages via intermittently connected nodes. In all distributed systems, end-to-end connection may not exist in DTNs. In such case the messages which is named as bundles, can be transmitted through an existing link and buffered at the next hop until the next link in the path appears This kind of message propagation process is usually known as the "store-carry-and-forward" strategy, and the routing is decided in an "opportunistic" Fashion. DTNs have the advantage of relaying data with temporary connections. DTNs accommodate long delays between and within regional networks, to achieve interoperability between the regional networks. It accommodates mobility and limited power of evolving wireless communication devices. Some nodes in the delay tolerant network could misbehave by dropping the packets even it has sufficient buffers and meeting opportunities to forward the data. Routing misbehaviour can be caused by selfish nodes or malicious node .Selfish nodes are the nodes which do not forward the data packet to the next hop (node).Malicious nodes are the nodes that drop the packet of other nodes and cause an attack, these kinds of attack which decreases the network performance and packet delivery rate.

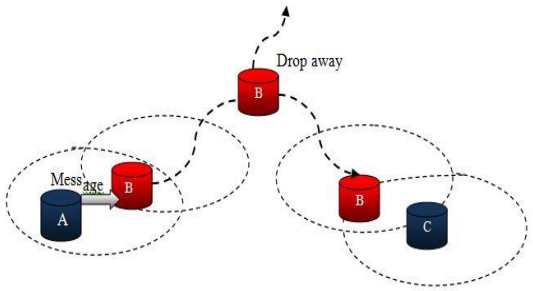

Figure 1: Node B acts as selfish node which drops the data packet Node A which sends the data packet to node B ,node B which holds the packet and does not forward the data packet to node C. Misbehaviour of nodes causes reduction in packet delivery rate and network performance, to overcome this problem an enhanced misbehaviour detection technique is used, to increase the probability of a data being successfully transferred to its destination. Detection technique consists of incentive scheme and reputation system which analyses the bad node with high priority and good node with comparatively less priority. By considering inspection game in this technique, game theory analysis which results in reduction of misbehaviour without affecting detection performance.

II. RELATED WORK

In delay tolerant network message propagation is in store, carry and forward manner. Each and every node contains internal buffer when the data traffic increases by addition of duplicate data from the selfish node which causes overflow of buffer. Node will drops the incoming packet due to internal buffer overflow this leads to the misbehaviour of node which reduces the packet delivery rate and increases the time delay in order to overcome this problem misbehaviour detection technology is used[1][2].
Mitigating routing misbehaviour detection technology which is used to detect the routing misbehaviour in network. This Detection Technology mainly works on neighbourhood monitoring or destination acknowledgement to detect dropping of packet, due to long feedback delay the neighbourhood monitoring based misbehaviour detection technology is unsuitable for DTNs[3][4].
Secure Multilayer Credit Based Incentive scheme which is also called as SMART scheme, in which virtual currency is used to monitor the packet that link exists among nodes and is determined before the data-forwarding process. But this kind of suspicion does not hold good in DTN[3][4].

Reputation-based incentive scheme rely on individual nodes to control neighbouring nodes traffic and keep trace of all nodes reputation so that misbehaviour nodes are detected and omitted

from the networks[5]. In reputation system, the inspection presumption could vary with the target node's reputation. A node with a bad reputation will be checked with a higher probability while a good reputation node could be checked with relatively lower probability. Even though the existing misbehaviour detection schemes works good for the traditional wireless networks, the distinct network features including lack of end to end path, high variation in network conditions, difficulty to analyse mobility patterns, and extensive feedback delay have made the neighbourhood monitoring based misbehaviour detection scheme unsuitable for DTNs. There are some proposals for misbehaviours detection in DTNs [4], [8], [9], [10], many of these schemes are based on forwarding history verification which are costly in terms of transmission overhead and verification cost.
The paper describes as follows. Existing detection schemes and its drawbacks are explained in Section 2,The misbehaviour of nodes discovery algorithms are explained in Section 3, implementation of enhanced misbehaviour detection scheme and experiments ,graphical analysis are discussed in Section 4. Section 5 concludes our work and discusses future research directions.

III ENHANCED MISBEHAVIOUR DETECTION TECHNIQUE

In this detection technique which detects the misbehaviour of nodes in DTN, we utilise basic misbehaviour detection algorithm, in this algorithm T A monitor the cluster of nodes in network which controls the intermediate node during data forwarding task. TA will distinguish the normal nodes from the misbehaving nodes. In basic detection scheme mainly rely on judge node there are three cases.

Case A: Reliable data forwarding with adequate nodes.
Generally a user will honestly follows the routing protocol by forwarding the messages as long as there are sufficient nodes. Source node forwards the data among the intermediate nodes by hop by hop strategy ,finds the number of honest nodes which follows routing protocol, and the misbehaviour nodes in the network. Misbehaviour node which holds data forwarded by the source node in order to increase their reputation.

Case B: Reliable data forwarding with inadequate nodes users perform the routing protocol but fails to obtain the expected results due to lack of sufficient nodes. Therefore, reliable data forwarding in the presence of sufficient nodes can be determined. In case B only a small number of nodes are available and the number of nodes is less than the number of data copies needed by the routing protocols. although the DTN nodes performs the routing protocol, it cannot fulfil the routing due to lack of nodes.
Case C: A misbehaving data forwarding with or without Adequate number of nodes. A misbehaving node will refuse to forward the data or drops the packets of data even though when there are adequate nodes, in the first case that the forwarder refuses to forward the data even when the forwarding facility is available. The second case is, the forwarder has succeeded in forwarding but it fails to perform the routing protocol. In The last case the forwarder allows to forward the data but unsucceeds to propagate sufficient number of copies

Basic Misbehaviour Detection Algorithm

1 PROCEDURE BASICDETECTION ((J,M_{ft},S_{mf} ,[t1,t2],R,D))
2 for Each m$\not\epsilon$ M_{ft}, do
3 if m ϵ S_{mf} and R!=0 then
4 return 1
5 else if m ϵ S_{mf} and $N_t(m)\not\epsilon$ R then
6 return 1
7 else if m ϵ S_{mf} and $N_t(m)$ ϵ R and $N_{t(m)}$< D then
8 return 1
9 end if
10 end for
11 return 0
12 end procedure

where j –T A judge,M_{ft}- message forwarding task S_{mf}- set of forwarded message N_t- target node, R- routing protocol, D-input.
In Basic Detection technology, which intakes j; mft; Smf;[t1, t2];R;D as well as the routing requirements of a distinct routing protocol R and D as the input, and output the detection result "1" to indicate that the target node is a misbehaviour or "0" to indicate that it is an honest node. Basic detection algorithm itself incurs a low detection overhead. However, to get rid of malicious users from providing duplicate data evidences judge node should check the honest of each evidence by confirming the corresponding endorsement, which introduce a high transmission and signature verification overhead. In the following section, inspired by the inspection game, we propose an enhanced probabilistic misbehaviour detection technique to detect misbehave node which reduce the detection overhead without compromising the detection performance.

Enhanced Misbehaviour detection scheme design requirements

The design requirements are Distributed, robust, scalability. In Distributed, Mainly network authority is periodically available which is responsible for the administration of the network and therefore unable to monitor the operational details of the network .In Robust, we require an enhanced misbehaviour detection scheme that could withstand different forwarding failures caused by various network environments. In Scalability, we require an EMD scheme that is purely independent of the communication range and strength of the network.

Enhanced Misbehaviour Detection Algorithm

1 : initialize the number of nodes in Network to n
2: for i =1 to n do
3: Nodes are aware of their direct neighbours. The one-hop neighbours of all the mobile nodes are identified .
4: Consider source node as adversary node
5: Generate a random number packet[i] from 0 to $10^n - 1$
6: if packet[i]/10^n < pb then
7: Adversary node ask all the nodes (including node i) to provide Evidence about node i
8: if Basic Detection(j; mft ;Smf; [t1, t2];R;D) Then
9: forward the pure packet [i] and blocks misbehaviour packet
10: else
11: forward pure packets[i] to the target node
12: end if
13: else
14: pay node i the remuneration w
15: end if
16: end for

Which briefly describes the proposed enhanced misbehaviour detection scheme For a distinct node i, Judge node TA will initiates the investigation at the probability of pb. If i could pass the inquisition, node i will receive a compensation W from the judge node TA; or else, judge node will blocks the duplicate data packets. In the further step, a model of algorithm is made as an inspection game. And we substantiate that, by implementing a suitable detection probability threshold, we use reputation system in order to describe the reputation of

each and every node in the network .we could accomplish a lower detection overhead and regulate the nodes to forward the data packets for next nodes.

Investigation Probability With Reputation System Technique

Before the presentation of inspection game, we assume the transmission costs of each node g to make a data forwarding. Node i will receive a compensation W from the judge node TA or else judge node will blocks the duplicate data packets. The compensation may be the virtual credits provided by TA; judge node also benefits from every successful data forwarding by gaining v, which can be attained from source node. In the time of inspecting, judge node TA checks the node Ni with the probability pb. The process of checking will incur a cost value h, judge node TA has two strategies, enquiring (I) or not enquiring (N). Every node will have two strategies, forwarding (F) and not forwarding (O). Therefore, The inspection game inspects every node and checks the reputation of the node in the network ,good node is verified with low probability and bad node is verified with high probability .hence reduces misbehaviour detection overhead and increases packet delivery rate.

IV. IMPLEMENTATION AND EXPERIMENT

We used JDK 6.0 with Eclipse IDE 6.9.1 and Jfreechart for graphical representation. We developed and tested our system on Windows XP operating system with 2.80-GHz, Intel Pentium 4 CPU with 1GB RAM.

We tested our approach in the subnet of a DTN. In subnet we found number of misbehaviour nodes, their details and also the good nodes rate of packet delivery. These are tested multiple times and physically verified. The problem we came across is to find the connectivity of our system to the device port .Other than this everything is working properly. In figure 2(a) which depicts the misbehaviour nodes detection rate and reputation of the 100 ,80,50 nodes were malicious nodes are detected with higher probability, good reputed nodes are detected with lower probability in DTN network with usage of Enhanced Misbehaviour Detection Scheme (EMDS).

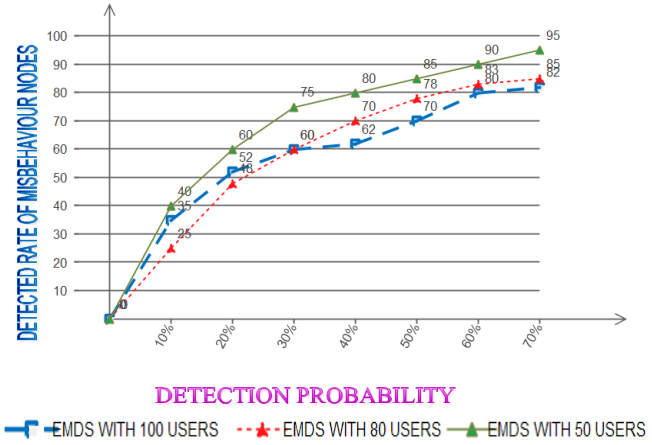

Fig 2(a) Detection of misbehaviour node using EMDS.

Enhanced misbehaviour detection scheme which reduces misbehaviour detection overhead and transmission overhead Fig 2(b) which depicts the reduction in transmission overhead using EMDS compare to other detection scheme

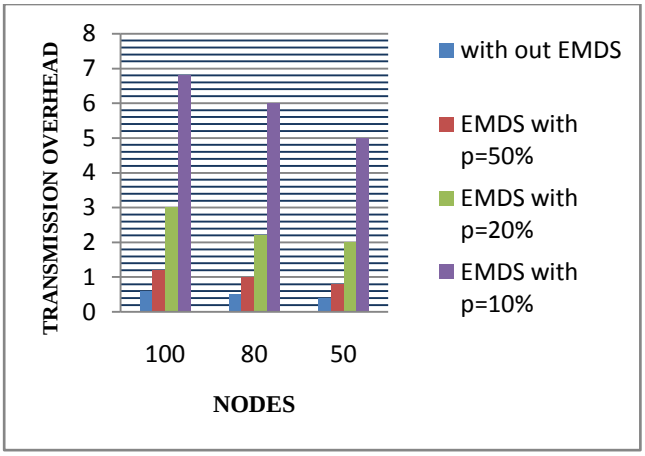

Fig 2(b) Transmission overhead using different probabilities

V CONCLUSION

In this paper, we not only focused on identification of misbehaviour nodes in DTN. We extended the work of others by introducing an algorithm to identify impure packets generated from malicious node and to discover the reputation of each nodes using reputation system along with the probability concept which can reduce the detection overhead efficiently and effectively. Our Simulations results assures that the EMDS scheme will reduce transmission overhead occurred by misbehaviour detection and detects defective nodes efficiently. This system does well in stability, reliability and safety. Our extensive tests are significant in terms of efficiency and the number of misbehaviour nodes and good nodes are discovered.

Various analyses of changes to EMDS scheme will also be done in future and applying to other types of networks.

ACKNOWLEDGMENT

The Acknowledgement word is very suitable in this work for the organization (BHEL COMPANY Bangalore) where they gave me an opportunity to implement my technique and to utilize my knowledge. I whole heartedly thank the organization and my guide who helped to complete this work.

REFERENCES

(1) Suguo Du, H. Zhu, and Zhaoyu Gao, "A Probabilistic Misbehaviour Detection Scheme Towards Efficient Trust Establishment in Delay Tolerant Netwaorks" Proc. IEEE' , Jan 2014

(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 Incentive Scheme for Delay-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 Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp. 664-675, Apr. 2012.

(7) 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.

(8) F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Disruption-Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM '09, 2009.
(9) E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay-Tolerant Networks," Proc. Military Comm. Conf. (Milcom '10), 2010.
(10) D. Fudenberg and J. Tirole, Game Theory. MIT Press, 1991.
(11) 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.
(12) 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.
(13) B.B. Chen and M.C. Chan, "Mobicent: A Credit-Based Incentive System for Disruption-Tolerant Network," Proc. IEEE INFOCOM '10, 2010.
(14) 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.
(15) J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM '06, 2006.