Minimax Theory Based Scheme to Detect Selfish Node and Reduce Latency in Delay Tolerant Network

Dhiraj kr. Mishra*
M.Tech, Maulana Azad National Institute of Technology, Bhopal
Bhopal(Madhya Pradesh), 462051, India

Dr. Meenu Chawla
Associate Professor (Department of Computer Sc. & Engg), Maulana Azad National Institute of Technology, Bhopal
Bhopal(Madhya Pradesh), 462051, India
E-mail: chawlam@manit.ac.in
www.manit.ac.in

Abstract

Delay Tolerant Networks are resource constraint network. Selfish behavior of a node causes it to drop legitimate packets of other nodes, leading to low message delivery and wastage of valuable network resources. Here a Minimax Theory Based Scheme is proposed to distribute credits among non selfish nodes .It reduces the message dropping rate, detects selfish node and enhance network performance in terms of latency, aborted message rate and delivery ratio.

Keywords: message dropping rate, credit, Delay Tolerant Network, security, selfish behavior, minimax theory.

1. Introduction

Delay or Disruption tolerant Network[1] (DTN) has gained popularity among researchers for past few years. In wired/wireless network, source to destination path is fixed or computable & continuous connectivity is assumed. On the other hand delay tolerant network works on the principle of intermittent connectivity and opportunistic contacts. It means, there is probability that other node may come in it's transmission range and they will share message as no fixed path exist between source and destination. To enhance the probability of successful delivery of message, store and forward mechanism is used. In this mechanism a DTN node which may or may not be the source node, if holds the message keeps it in it's buffer until it meets the next node or it's buffer get flooded. As soon as this node meets the next node it tries to forward the message to next node. Message in DTN are also called bundle[2].A bundle consist of three types of data: i).source application user data ii).control information provided by source for the destination iii). A bundle header inserted by bundle layer. Bundle layer is new protocol layer which ties together the region specific lower layers[3], so that application programs can communicate across multiple regions.

DTN are resource constrained network, so it may possible that the next node may have selfish behavior[4].It may try to maximize it's own benefit by dropping the packet from other nodes and will forward only it's own

*Dhiraj Kumar Mishra,M.Tech Scholar ,Maulana Azad National Institute of Technology,Bhopal(Madhya Pradesh).
email:dhirajmishra.nitb@gmail.com

message. Such node in the network will degrade the network performance as this behavior will increase the message dropping rate and reduce the probability of message delivery. Mechanisms are needed to reduce message dropping rate and detect selfish node. An algorithm based on minimax game theory has been proposed here which will encourage the node to forward packet and get rewarded. The proposed algorithm is expected to reduce message dropping rate, network latency and aborted message rate. This algorithm can also be extended to identify the misbehaving node.

2. Previous Work

There are few schemes developed to detect selfish node in which they either need a Trust Authority (TA) [5]or an evidence to check the trustworthiness of the node. Besides, nodes involved in communication get incentive only if message gets delivered successfully.In[6] Authors have proposed a scheme in which transaction occurs between service providers and consumers. Service providers and consumers are represented as a bipartite graph. After each transaction consumers provides feedback about the service provider in the form of rating. Based on feedback given by consumer ,rating of a service provider changes. If a consumer 'c' has a rating about the s^{th} service provider, an edge with value Ecs, from the c^{th} vertex to the s^{th} vertex is created. If a new rating arrives from the c^{th} consumer about the s^{th} service provider, this scheme updates the new value of the edge cs. If rating of an edge crosses a threshold then the node is black listed. To evaluate the scenario in DTN, the judge node waits for 'k' feedback and based upon that a node status is evaluated. Disadvantage of this schemes are

- In DTN nodes are sparsely connected so to get feedback from 'k' number of nodes, judge has to wait unpredictable amount of time, which often increases network latency.
- The node which is providing feedback (evidence) is not being rewarded, so because of constraints in resources a node may avoid giving feedback. No Policy is discussed to encourage the node to give feedback.
- If a honest node is mistakenly blacklisted then no policy is mentioned to recover it.

A Probabilistic misbehavior detection scheme (PMDS) is used in[5]. It's based on inspection game[7] verification method. PMDS needs a periodically available Trust Authority (TA), which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from it's upstream and downstream nodes. Disadvantages of these schemes are:

- Connectivity in DTN is intermittent in nature. Upstream and downstream node may not be available at same time to collect evidence. However upstream and downstream node may be available opportunistically at same time but in that case communication cost is quite high.
- Installing a TA is quite costly so number of TA is fixed and small. So availability of TA cannot be guaranteed if size of network is large.

In[8]a secure incentive based protocol (SIP) is proposed which provides incentives to node to encourage packet forwarding .Here source and destination is charged only if message is successfully delivered. Nodes effort (resource) goes in vain if packet is not delivered whatsoever good effort they put to forward the packet.

3. Preliminary

3.1. *System Model*

A normal DTN consisted of mobile devices owned by individual users has been considered. Each node 'i' is assumed to have a unique ID 'Ni' and a corresponding public/private key pair. Each node's credit[9-10] is checked by a TA or a judge node. To detect selfish node three loop scheme similar to[5] has been used.

- When a node 'X' meets the node 'Y' it forwards packet from it's buffer to 'Y' at time t_0.
- At time t1 node 'Y' meets node 'Z' if node 'Y' is not selfish node it will forward the packet received from 'X' to node 'Z' along with the timestamp signed by it.
- At time t2 when node 'Z' meets node 'X' it can prove that it indeed met node 'Y'. Additionally node 'Y' also transfer the receipt it received to witness 'Z'.

3.2. *Minimax Theory*

Minimax [11]is a decision rule used in decision theory, statistics, philosophy and game theory for *mini*mizing the possible loss for a worst case scenario. Alternatively, it can be thought of as maximizing the minimum gain (**maximin**). Originally formulated for two-player zero-sum game[12], covering both the cases where players take alternate moves and those where they make simultaneous moves.

The minimax theorem states:-

For every two-person, zero-sum game with finitely many strategies, there exists a value K and a mixed strategy for each player, such that

(i) Given player 2's strategy, the best payoff possible for player 1 is K, and
(ii) Given player 1's strategy, the best payoff possible for player 2 is –K

Equivalently, Player 1's strategy guarantees him a payoff of K regardless of Player 2's strategy, and similarly Player 2 can guarantee himself a payoff of −K.

3.3. *Adversary Model:*

For an adversary model it is assumed that the adversary node drops the legitimate packet it has received. Otherwise nodes are assumed to be rational i.e they cheat only if it provides them more incentives as compared to acting honestly.

4. Proposed Scheme

The basic idea for detecting the selfish node is derived from the concept that in DTN when a node meets another node it should forward the packet to enhance the probability of message delivery. Selfish node will not forward the other node's packet.
To reduce the latency it's proposed that instead of waiting for 'k' witness, a small credit say 'e' will be deposited for each node 'i' ,if it passes the honesty test. Once the credit crosses the threshold it will be given an honest status. Apart from that Each and every node involved in communication will be charged and get incentive for it's effort. For the distribution of credit, to be given to a node to encourage them to participate in communication the proposed work uses the MINIMAX model.
To reduce the message dropping rate, proposed algorithm checks each node's credit regularly. If the node's credit is less than double of average hop count, the node is being forced to forward the message until it's credit becomes greater than or equal to double of average hop count**.** For this model the network is assumed to have a special node which is called as judge node. Judge node could be a TA or an ordinary DTN node but with very high credit. The judge node has two strategy either it inspect a node with probability p_f or it does not inspect the node with probability (1- p_f).On the other hand the suspicious node(i.e the node under consideration) also has two strategy ,either forwards the packet or does not forward the packet.

4.1. *Penalty and reward Scheme*

4.1.1 Explanation of term used

i) c -It is the credit rewarded/punished by a judge node to the node under consideration.
ii) w -It is the credit given to a node, if judge node chooses not inspecting strategy &w<<c.
iii) h -It is the transmission cost of communication, and is fixed for all node**.**

4.1.2 Working methodology

If a judge node is investigating a node and node passes the test then a credit say c is given by judge node to the node under consideration however if node fails in test a credit of (c+h) will be deducted from node . When the judge node is not investigating the node, the node under consideration will be credited with (w+h) if it is forwarding the packet else it will only get a credit w.

Table 1:Different Strategy of (suspicious, judge) node

	Inspecting	Not Inspecting
Forwarding	c,-c	w+h,-w-h
Not Forwarding	-c-h,c+h	w,-w

Cases in the table can be explained as follows:
Case 1: If a node chooses forwarding packet strategy and judge node chooses the inspect strategy then it will

receive a huge incentive 'c', however if node chooses not forwarding strategy then it loses a credit of c+h.
Case 2: If judge node chooses the not inspection policy then suspicious node can have two choice either forward or not forward packet, if it is not forwarding packet then it's gaining only 'w' credit however if it's forwarding then it's getting 'w+h' credit.
From the above explanation it's clear that if a node strategy is forwarding then it's getting maximum gain(incentive plus it's communication cost).so the best strategy for a node is to forward the packet, because if it's not forwarding the packet and get caught credit 'c' will be penalized which is much- much greater than the incentive 'w'.

4.2 Proposed Algorithm

1. initialize each node with initial credit k.
2. set each node status="ok".
3. Generate a random number i<1000 for node x.
4. If i>0.5
5. Call inspect_node(x)
6. End if
7. Else set x. credit=x.credit+w for node x.
8. If x.credit> threshold
9. Set status=reputed
10. End if
11. Else if credit< 2*avg_hop_count
12. Set status=black_list
13. End else if
14. End algo

4.2.1 *Inspect_node Algorithm*

1. inspect(node x)
2. check_message=x. last_message_transferred
3.last_node_visited=check_message.getTo();
4.your_message=last_node_visited.last_message_accepted.
5.if(check_message.getId()==your_message.getId())
6.set x.credit=x.credit+c
7.end if
8.else
9. set x.credit=x.credit-c-h
10.end Algo

5. Simulation and Set-up

The experiment environment has been set up with the Opportunistic Networking Environment (The ONE) simulator[13]which is designed for evaluating DTN routing and application protocols. Comparison has been made between routing algorithm modified with this scheme against the existing routing protocols such as epidemic[14], spray and wait[15]and Max prop[16]. We have designed a new queue model which sorts messages, based on their credit. Some initial Comparison result has been shown in figure1 and figure 2. Extensive work is going on to reduce message dropping rate and selfish node detection. Different parameters that we used are

Table 2: Simulation parameters

No of Groups	6
Movement Model	Shortest path map based
Buffer size	5 M
Interface	Bluetooth
Message TTL	300 minutes
Message creation interval	0-5 sec
Message size	500K,1M
Number of nodes	80
Map size	4500m x 3400m

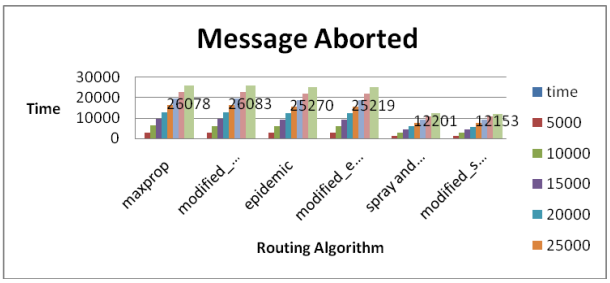

Fig1:comparison between different routing algorithm and modified routing algorithm on basis of no. of message aborted

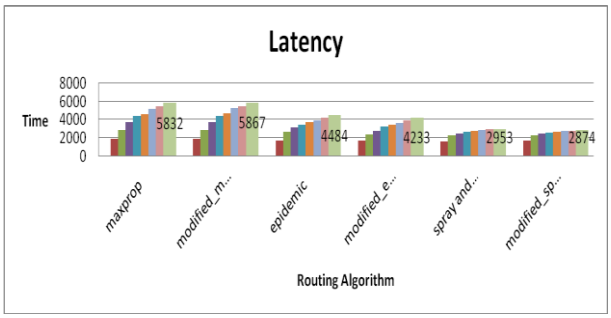

Fig2 :comparison between different routing algorithm and modified routing algorithm on basis of latency

6. Conclusion and Future Work

We are implementing the credit based scheme. Initially it helps us to reduce latency and aborted message. In future we will try to identify the selfish node and reduce message dropping rate.

References

1. K. Fall,S. Farrell, *DTN*: *An Architectural Retrospective*, IEEE Journal on Selected Areas in Communications, Vol. 26, No. 5, June2008

2. M. Loubser, *Delay Tolerant Networking for Sensor Networks*," SICS Technical Report, ISSN 1100-3154, January 2006

3. S. Burleigh, A. Hooke, L. Torgerson, K. Fall, V. Cerf, B. Durst,K. Scott, and H. Weiss, "*Delay-tolerant networking: An approach to interplanetary Internet*" IEEE Comm. Mag., vol. 41, no. 6, pp. 128–136, Jun. 2003.

4. Q. Li, S. Zhu, and G. Cao, Routing in socially selfish delay tolerant networks, *in Proc. IEEE INFOCOM, 2010*, pp. 1–9.

5. Zhaoyu Gao; Haojin Zhu; Suguo Du; Chengxin Xiao; Rongxing Lu, PMDS :A Probabilistic misbehavior detection scheme in DTN, *IEEE International Conference on Communications (ICC), 2012*,pp. 4970 - 4974

6. E. Ayday, H. Lee, and F. Fekri, An iterative algorithm for trust and reputation management, *Proc of IEEE International Symposium on Information Theory*, 2009

7. D. Fudenburg and J. Tirole, "*Game Theory*", p17-18, The MIT Press,Cambridge, Massachusetts, London, England

8.Y. Zhang, W. Lou, W. Liu, and Y. Fang, *A secure incentive protocol for mobile ad hoc networks*, Wireless Net. (WINET), vol. 13, no. 5, pp. 118-124, Oct. 2007.

9. 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. Veh. Technol.*, vol. 58, no. 8, pp.4628 -4639, 2009

10. U. Shevade, H. Song, L. Qiu, and Y. Zhang, Incentive-aware routing in DTNs,in *Proc. IEEE ICNP, 2008*, pp. 238–247

11. Wikipedia [online], http://en.wikipedia.org/wiki/Minimax

12. Wikipedia [online],http://en.wikipedia.org/wiki/Zero-sum

13. A. Keranen, J. Ott and T. Karkkainen, The ONE Simulator for DTN Protocol Evaluation, in *Proc. of SIMUTools'09*, 2009.

14. A. Vahdat and D. Becker, *Epidemic routing for partially connected ad-hoc networks*, Tech. Rep. Duke CS-2000-06, Duke University, April 2000

15. Spyropoulos T, Psounis K, Raghavendra C S, Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks in *Proc. of ACM SIGCOMM 2005*,pp252-259

16. J. Burgess, B. Gallagher, D. Jensen and B. Levine, Maxprop: Routing for Vehicle-based Disruption Tolerant Networks, in *Proc. of IEEE INFOCOM'06*, 2006