VOLUME-8, ISSUE-6, JUNE-2019 • PRINT ISSN No. 2277 - 8160

Original Research Paper

Engineering

A TRUST BASED SCHEME TO DETECT SELFISH NODES USING DELAY TOLERANT NETWORK

Chandrima Chakrabarti

Assistant Professor, CSE Department, Narula Institute of Technology, Kolkata, West Bengal, India

ABSTRACT

Physical and communication infrastructure will be totally damaged after a major disaster. Delay Tolerant Network (DTN) can be implemented with smart phone carried by volunteers to handle the devastating situation under control. In this situation, some malicious nodes may drop or corrupt data to make the situation difficult to handle. DTN is a network where the communication infrastructure and network connectivity are not guaranteed. Messages are transmitted from source to destination through multi-hop approaches. Checker detects selfish nodes and if they do not get any mismatch in transmission of node's messages within maximum time limit then the node is good in performance else not. In our scheme, forwarder nodes are chosen based on good reputation of nodes and nodes with bad reputation are repelled from the network. Hence we propose a reputation based scheme for improving the performance of the network and simulations are done using ONE simulator.

KEYWORDS : reputation, incentive, cooperation, malicious node

INTRODUCTION

Delay or Disaster Tolerant Network (DTN) can be used in post disaster situation with the help of smart phone. The main motive of this work is for detecting selfish nodes, by cooperativeness and cooperativeness can be quantify by packet dropping threshold, Time Threshold. This kind of thinking was due to the presence of selfish or malicious nodes in the network. These types of nodes always accept the messages from the sender node and modify it, so when the receiver node accepts the messages then the mismatch will occur and the proper messages or data will not reach to the proper destination. This will also degrade the system's performance.

The motivation for delay tolerant network was simulated by several other factors which a given below.

1) Make sure that the delivery of the messages has been done within the maximum Time limit and which improves the system's performance.
2) Make sure that no data inconsistency will occur among the system's nodes.

We, in this paper, aim to develop Reliable Communication scheme in post-disaster situation using Delay Tolerant Network by detecting and minimizing the misbehavior of nodes and to increase packet delivery with low overhead.

Nalini et. al proposed an approach for identifying,detecting and eliminating of selish and malicious nodes with Buffer Level monitoring for secured Data communication in DTN [1]. Rajaram proposed an approach to solve the problem of Black Whole attacks [2]. In [3-5] Chakrabarti et. al proposed reputation based scheme to detect selfish nodes. Chen et. al [6] introduced a mechanism for detecting the selfish node in the network in those situation when the problem of disconnection will arise as a result it becomes very tough to identify the selfish one and it also become very difficult to identify the appropriate routing path. To recover this problem, scientists proposed "Mobicent". It is basically an incentive based protocol, that helps to detect the most efficient paths and also helps for not to transfer the data to the non- existing nodes [6]. Lu et. al proposed an practical incentive protocol i.e, Pi to detect the selfish nodes in the network. When a source node want to send clump(Bundle) of messages to the receiving node,it also adds some incentives with the clump and this become more attractive to the selfish one which helps to deliver the message to the proper receiving nodes without making any complications and that helps to increase the system's performance [7].

In an opportunistic environment, special attention must be given to the data delivery. Energy consumption, storage capacity of the system. While doing this work it was observed that all nodes are not interested to deliver the messages to their proper destination. These fictitious needs to be identified and resolved. This is because, this will occur a serious problem in the system.

The second most important issue is that, in this paper, the Reputation has been given according to the co-operativeness and co-operativeness can be quantify by the packet dropping. So, in the network every node is consuming their battery continuously. So we need to observe that the transaction is completed within the Maximum time limit or not, if it is not then this will occur a serious problem in the system.

So it is very essential to design an effective fast network that can easily detect the selfish nodes and can deliver the messages within maximum time limit.

Motivated by the works proposed in literature, it is very essential to design an effective system that can easily detect the selfish nodes and can deliver the messages within maximum time limit.

SYSTEM MODEL

In the post disaster scenario different volunteer nodes will exchange packets that are transmitted using multihop pattern. So each node will maintain packet history Table as in table 1.

TABLE – 1: PACKET HISTORY TABLE

Receive Packet ID	Sent packet ID	Receiver Node	ID NO. of Sender Node	No. of Receiving Packet	No. of Sending Packet	Time of Packet Sending	Time of Packet receiving
M1	M1	S2	S1	N2	N1	T_{M1}	T_{M2}
M3	M2	S3	S2	N3	N2	T_{M3}	T_{M4}
M4	M3	S4	S3	N4	N3	T_{M5}	T_{M6}

We are calculating total number of sending and receiving packet.

Here, M2,M3,M4 is Id no. of Receiving packet,M1,M2,M3 is Id no. of sending packet.S2,S3,S4 is Id no. of Receiver node,S1,S2,S3 is Id no. sender node,N2,N3,N4 is No. of receiving packet, N1,N2,N3 is No. of sending packet,T_M1,T_M3,T_M5 is Time of packet sending, T_M2,T_M4,T_M6 is Time of packet receiving. Then will further calculate total number of sending and receiving packet.

For an example, In the first row, M2 is Id no. of Receiving packet, M1 is Id no. of sending packet,S2 is Id no. of Receiver node, which receives the packets from S1.If the ratio among N1 and N2 is greater than 0.8, i.e,N1/N2 >0.8the node is reliable and good.

If the ratio value among N1 and N2 lies between 0.5 to 0.8, i.e,N1/N2=0.5-0.8.The node is medium in performance.

If the ratio among M1 and M2 is less than 0.5, i.e,N1/N2<0.5.Then the node is not reliable and bad.

No.of packet dropping = (no of sending packet- no of receiving packet).

Spending time in buffer of a packet = T_M1 – T_M2 Performance of a node= 1/(Spending time in buffer of a packet) In table 1 packet dropping are calculated.

No of packet dropping= No of receiving packet – No of sending packet

If the value of packet dropping lies between 1 to 10 then grade of the node is A. If the value of packet dropping lies between 11 to 50 then grade of the node is B. If the value of packet dropping lies between 51to 70 then grade of the node is C. If the value of packet dropping lies between 71to 100 then grade of the node is D. In this way selfish nodes are identified. Here, C and D group of nodes are selfish.

We also discuss grade of a node based on sending and receiving time. If the sending and receiving time belongs to the first range i.e, 0 to5 sec then the Grade of the node is "A". If the sending and receiving time belongs to the first range i.e, 6 to20 sec then the Grade of the node is "B". If the sending and receiving time belongs to the first range i.e, 21 to60 sec then the Grade of the node is "C". If the sending and receiving time belongs to the first range i.e, greater than 61 sec then the Grade of the node is "D".

In an opportunistic environment, special attention must be given to the data delivery. Energy consumption, storage capacity of the system. While doing this project it was observed that all nodes are not interested to deliver the messages to their proper destination. These fictitious needs to be identified and resolved. This is because, this will occur a serious problem in the system.

The second most important issue is that, in this paper, the Reputation has been given according to the cooperativeness and cooperativeness can be quantify by the packet dropping. So, in the network every node is consuming their battery continuously. So we need to observe that the transaction is completed within the Maximum time limit or not, if it is not then this will occur a serious problem in the system.

So it is very essential to design an effective fast network that can easily detect the selfish nodes and can deliver the messages within maximum time limit.

Here, reputation is calculated based on ratio of sending and receiving packets. If the ratio is greater than threshold the node is good and will get grade A. Else the node will be of grade B and they are selfish nodes. Selfish nodes will get special incentive as encouragement so that they can forward and receive more packets.

A node will choose a forwarder node based on its reputation value. If buffer space is available then the message will be sent to receiver node. Sender node keeps a copy of sent message. Transaction will be successful if the packet is received by receiver within time limit and with minimum power consumption. We also check energy level of nodes.

SIMULATION

In this paper ONE simulator is used for the simulation [8]. The proposed technique may be much better as expected from the previous result which are obtained from the other papers. We take total volunteer nodes as 50,100.150,200, No. of shelter nodes (stationary) as 3, no. of control station node (stationary) as 1, speed of nodes' as 1.5 – 10 m/s, routing protocol as Spray and Wait.

The graph in fig. 1 depicts delivery probability is high without the presence of selfish node as our scheme detects and avoid selfish nodes.

Figure 1: Graph of delivery probability

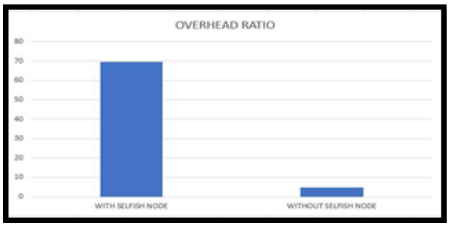

Figure 2: Graph of overhead ratio

The graph in fig. 2 depicts that overhead ratio is high in presence of selfish node.

CONCLUSIONS

Various scientists applied various ideas to send messages from source to destination in the network. But messages are proceeding from source to destination are facing so many problems in which selfish nodes are one of the main cause. In this paper we tried to introduce such a mechanism by which we can easily identify the selfish and malicious nodes in the network. The simulation results show that the proposed system detects the malicious and selfish nodes efficiently. In future we shall use the multi hop approach which will help to improve the system's security. We can also associate cryptography with scrambling plaintext into cipher text, then back again.

REFERENCES:

[1] Nalini C., Aakansha, Abhilasa. (2015), "Identification, Detection, Elimination of Selfish & Malicious Nodes with Buffer Level Monitoring For Secured Data Communication In DTN", International Journal of Advanced Research in Computer Science and Software Engineering.
[2] Rajaram A, Palaniswami S. (2010), "Malicious node detection for mobile AD-hoc Networks", IJCSIT.
[3] Chakrabarti C., Banerjee A. and Roy S. (2014), "An Observer-based Distributed Scheme for Selfish-Node Detection in a Post-disaster

Communication Environment using Delay Tolerant Network", AIMoC 2014, IEEE proc. pp. 151-156.
[4] Chakrabarti C. and Roy S. (2015), "Adapting Mobility of Observers for Quick Reputation Assignment in a Sparse Post-Disaster Communication Network", AIMoC 2015, IEEE proc. pp. 29-35.
[5] Chakrabarti C, Roy S, Basu S. (2018), "Intention aware misbehavior detection for post-disaster opportunistic communication over peer-to-peer DTN", Springer-Verlag, Peer-to-Peer Networking and Applications, pp 1-19.
[6] Chen Bin Bin, Chan Mun Choon. (2010), "MobiCent: a Credit Based Incentive System for Disruption Tolerant Network", IEEE Infocom proc.
[7] Lu R, Lin X, Zhu H, Shen X, Preiss B. (2010), "Pi : A Practical Incentive Protocol for Delay Tolerant Networks", IEEE Transactions on Wireless Communications.
[8] Keranen, A., Ott, J., Karkkainen, T. (2009), "The ONE Simulator for DTN Protocol Evaluation", in SIMUTools, Rome, Italy