PREVENTING DATA TRANSMISSION BY MISBEHAVING NODES IN DTN

B. Sakthisaravanan, R. Meenakshi and V. Priya
Department on Information Technology, Saveetha Engineering College, Chennai, India

ABSTRACT

Selfish and Malicious nodes (referred as misbehaving) present in the Delay Tolerant Network (DTN) results in insecure data transmission resulting in the packet loss .Currently the misbehaving nodes are identified only after data transmission. For this purpose Information Centric Network (ICN) is used along with DTN .ICN has a property of interactivity and it also supports mobility of nodes. Hence ICN identifies about misbehaving nodes in the path before the data transmission so that alternative path is chosen. Hence ICN avoids misbehaving nodes and the packet reaches the destination safely. This paper will be implemented in two parts. In the first part the misbehaving nodes are identified by DTN .A new load balancing concept is introduced in order to handle traffic. In the second part misbehaving nodes are intimated in advance by ICN and hence alternative path is chosen for the packets so that further transmission by misbehaving nodes is prevented.

Keywords: DTN, ICN, selfish nodes, malicious nodes, misbehaving nodes, DTN routing, network security, multihop.

1. INTRODUCTION

Delay Tolerant Network (DTN) has mobile nodes and there is no continuous path between source and destination. The packets from the source reach the destination by a number of intermediate nodes. Sometimes there is a delay in establishing connection between the nodes. So the nodes in the DTN have buffer limits to store the packets when the connection is lost and forwards the packets when connection is available. Some of the nodes present in the network are misbehaving that is either selfish or malicious. Selfish nodes as the name denotes is selfish in nature. They do not forward the packets during data transmission. Sometimes they participate in the routing packets by forwarding packets when it comes from its friends list. Malicious nodes results in the dropping of packets. Sometimes they also redirect packets [3]. If these nodes are present in the network the packets loss occurs. The nodes which are misbehaving are identified only after the data transmission. So some packets are lost. The energy of the node is also wasted.

In proposed system, ICN in DTN. ICN follows a publish/subscribe method and helps in efficient information retrieval. This can be accomplished by directly naming and operating on information objects. It is a receiver driven model. It provides large content storage and it supports mobility of nodes and interactivity ICN intimates about the misbehaving nodes in the path and hence further transmission by the misbehaving nodes are prevented. Alternative path is chosen for routing and packets reach destination safely. Hence data transmission is prevented by misbehaving nodes.

So the packet loss is prevented and security of the packets is assured .Nodes battery is also saved. Traffic is handled in the network by introducing load balancing concept.

2. LITERATURE REVIEW

In DTN misbehaving nodes causes serious threat and results in packet loss. We referred to “Delay-Tolerant Networking Architecture” to know in about Delay Tolerant Network characteristics, network topology, routing, mobility of nodes [4].

Dynamic Trust Management scheme is used to detect misbehaving nodes in the network. It finds misbehaving nodes based on the energy level after data transmission [5].

Selfish and Malicious nodes are identified in this paper .A security mechanism for DTN is developed in order to evaluate a node and how it interacts in the past. This is a graph based iterative algorithm which detects Byzantine adversaries, selfish, malicious node [1].

In sparse mobile ad-hoc networks the delivery of message is difficult. Hence, a social network analysis metrics has been used Three components are considered namely “between nesses”, “tie strength”, “similarity”. Messages are sent to the node with high SimBetTS utility [4].

We referred to the “A new design for Information Centric Networks” to know in detail about Information Centric Network. ICN is a receiver driven model and it supports in network catching. It supports mobility of nodes. Since the nodes in the DTN are mobile ICN can be effectively used with DTN [8].

We aim at detecting misbehaving nodes and choose alternative path so that the packet reaches the destination safely. Load balancing concept is introduced to handle with traffic. The proposed system ensures secure data transmission and packet delivery.

3. SYSTEM MODEL

We consider a Delay Tolerant Network where there is no end to end connectivity between source and destination. Packets from the source reaches destination by a number of intermediate nodes. In the intermediate nodes some are misbehaving (either selfish or malicious).

These are identified in the network as follows. Each node in the network has node id and energy level assigned by the user. The misbehaving nodes present in the network drop packets so as to save energy. DTN monitors the data transmission. After the process of routing the path history is updated in DTN. It identifies the misbehaving nodes based on the energy level. If traffic occurs it is difficult to monitor the routing process. Hence we increase DTN nodes in order to handle the traffic. For load balancing purpose some of the monitoring work switches over to other DTN automatically.

ICN monitors and stores all the information collected in DTN s. Once misbehaving nodes are identified by DTN, ICN intimates about the misbehaving nodes in the path and hence further transmission by the misbehaving nodes are prevented. Alternative path is chosen for routing and packets reach the destination safely

Advantages

- Easily identify the misbehaving nodes before data transmission
- Avoid packet loss
- Quick data transmission
- It provide high security

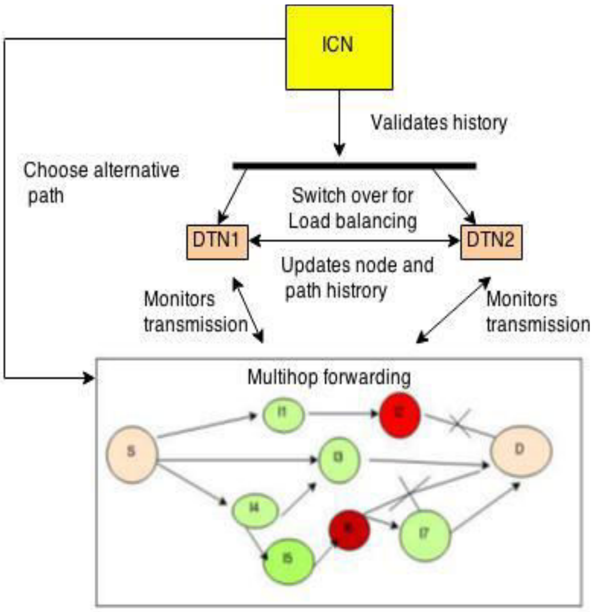

Figure-1. System Model of DTN.

4. IMPLEMENTATION

- **DTN identifies misbehaving nodes**

DTN has misbehaving nodes resulting in packet loss. Selfish node forwards the packets only from the friends list and it does not participate in routing process. Malicious nodes drop or redirect packets. The malicious nodes thus results in isolated networks and decrease in network performance. The misbehaving nodes are identified as follows.

For each node in the network node id, energy is assigned. Here the data is transmitted based on multihop forwarding algorithm. The multi hop forwarding algorithm forwards the packets to the nearest available hops. The DTN monitors the data transmission. Based on the node information available in the nodes list, source node select nodes to send packets to the destination .The data from the source node reaches destination by a number of intermediate nodes. When the packets reaches the destination node, the data transmission path will be available in the Source node's frame. Each node history and path history is updated into DTN. Based on node energy level and capacity selfish, malicious nodes are identified.

The efficiency of the system is increased by introducing a concept called load balancing. The traffic that needs to be forwarded by a node is split into at most two branches: one is sent to the requested DTN, the other is switch over directly to another DTN based on DTN feedback. For this purpose the number of DTN nodes used for monitoring purpose has been increased to manage the traffic. However the number depends on the number of nodes in the network.

- **Secure routing by ICN**

The nodes in DTN are mobile and hence ICN can be used with DTN since it supports mobility property. Information can be retrieved easily by means of publish-subscribe model. In our project ICN monitors all DTN s.

ICN provides large content storage. It validates all the path history and node history updated in DTN. If a path is chosen which contains misbehaving nodes ICN intimates about it. Hence alternative path is chose

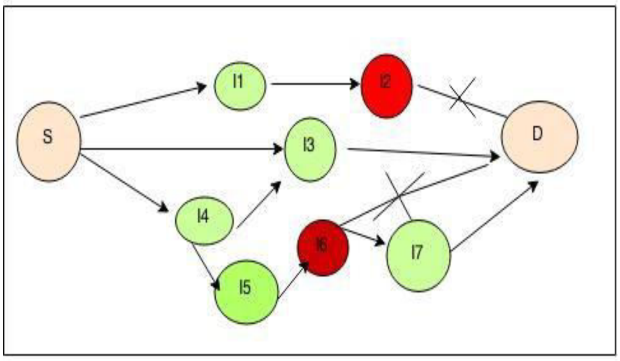

Figure-2. Secure routing.

Thus further packet loss is prevented**.** ICN monitors the DTN periodically. Hence ICN prevents routing by misbehaving nodes based on node history updated in DTN. Thus further packet loss is prevented. Thus secure transmission is ensured in DTN in the presence of misbehaving nodes.

5. ANALYSIS AND RESULTS

The simulation results are as follows. Figure-3 shows data transmission based on multi hop forwarding

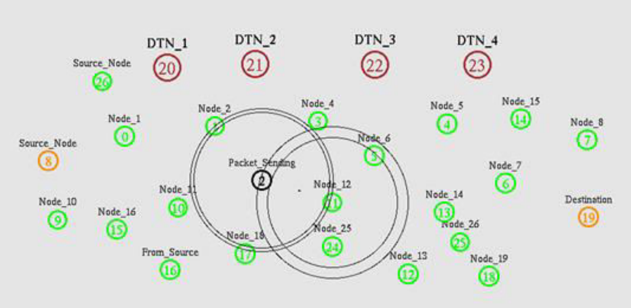

Figure-3. Data transmission.

The misbehaving nodes are present in the network and hence packet loss occurs. Figure-4 shows the packet dropping during data transmission.

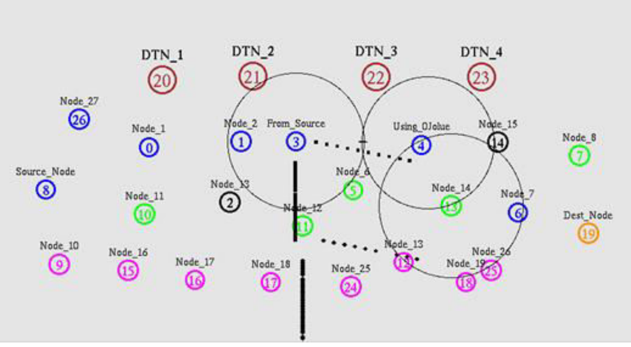

Figure-4. Packet dropping.

Figure-5 shows the packet loss during data transmission.

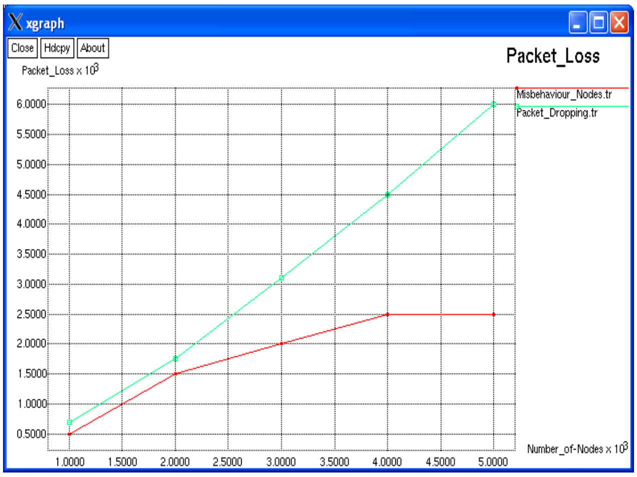

Figure-5. Packet Loss during transmission.

Figure-5 shows the delay in sending packets

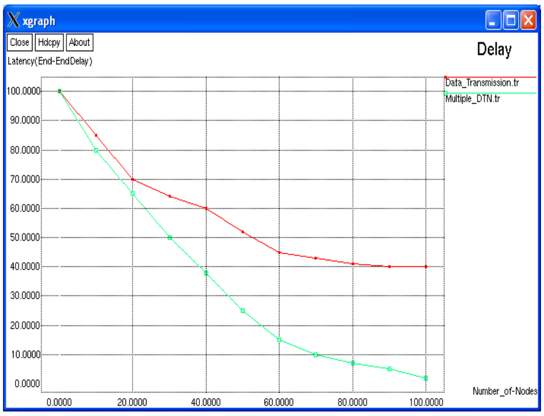

Figure-6. Delay in sending packets.

The systems efficiency is improved by using ICN along with DTN. ICN avoids misbehaving nodes during data transmission.

Figure-7 shows that packets has been delivered to destination within the specified time and thereby increasing throughput.

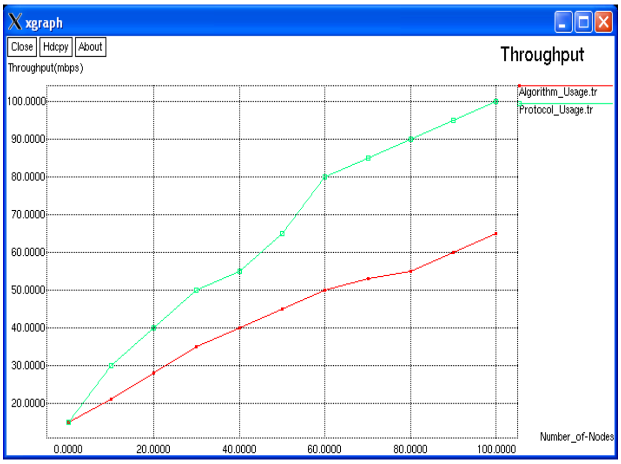

Figure-7. Increase in Throughput.

Figure-8 shows that packet has been delivered successfully to destination. ICN intimates about misbehaving nodes and so alternative path is chosen. Thus the rate of packet delivered is increased

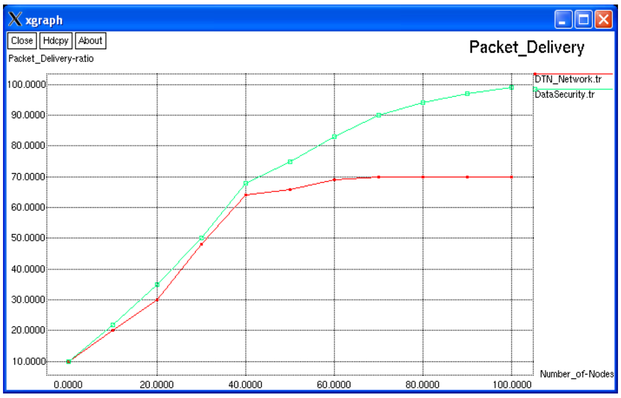

Figure-8. Packet delivery.

The following Figure-9 shows how secure transmission is ensured in DTN in the presence of misbehaving nodes.

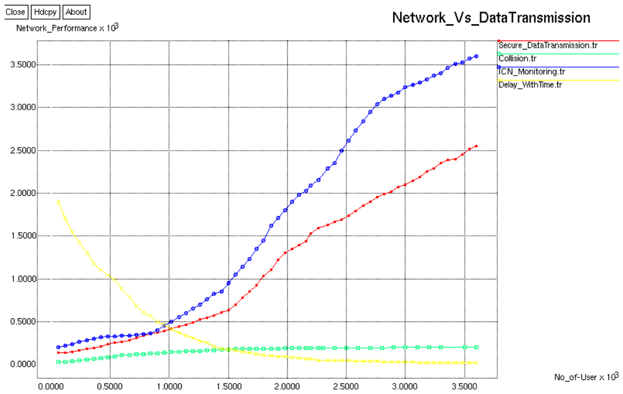

Figure-9. Secure routing.

6. CONCLUSIONS

Though misbehaving nodes are present, the multiple intermediate nodes are used for data transmission in a secure manner which avoids packet loss. Packets reach the destination safely in the presence of misbehaving nodes. Also load balancing concept is introduced to deal with the traffic in the networks. ICN is effectively utilized for information retrieval purpose and to deal with mobile nodes. The performance of the system has been increased and the energy of the node is saved. It provides high security for packets. Thus secure routing is ensured in the Delay Tolerant Networks even in the presence of misbehaving nodes.

REFERENCES

[1] Aydan. E, Lee .H, and Fekri. F. 2012. An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Networks', IEEE Trans.

[2] Burgess. J, Gallagher. B, Jensen. D and Levine. B.N. 2006. 'Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networking', Proc. IEEE INFOCOM, pp. 1-11

[3] Chen. I.R, Bao.F, Chang.M, and Cho. J.H. 2013. Supplemental Material for 'Dynamic Trust Management for Delay Tolerant Networks and Its Application to Secure Routing', IEEE Trans. Parallel and Distributed Systems.

[4] Cerf. V, Burleigh. S, Hooke. A, Torgerson. L, Durst. R, Scott. K, Fall. K and Weiss. H. 2007. Delay-Tolerant Networking Architecture', RFC 4838, IETF.

[5] Denko.M.K, Sun.T, and Woungang.I. 2011. 'Trust Management in Ubiquitous Computing: A Bayesian Approach,' Computer Comm. vol. 34, no. 3, pp. 398-406.

[6] Elizabeth M. Daly and Mads Haahr. 2009. Social Network Analysis for Information Flow in Disconnected Delay-Tolerant MANETs', IEEE Transactions.

[7] Ing-Ray Chen, Fenye Bao, MoonJeong Chang, Jin-Hee Cho. 2014. Dynamic Trust Management for Delay Tolerant Networks and Its Application to secure Routing', IEEE Transaction.

[8] Jøsang.A and Ismail. R, 'The Beta Reputation System. 2002. Proc. Bled Electronic Commerce Conf., pp. 1-14

[9] Mei.A,Stefa.J. 2012. Give2Get: Forwarding in Social Mobile Wireless Networks of Selfish Individuals', IEEE Transactions.

[10] Rao.A, Ratnasamy.S, Papadimitriou.C, Shenker.S, and Stoica.I. 2003. Geographic Routing without Location Information,' Proc. ACM MobiCom, PP. 96-108.

[11] Sadjadpour. H.R, Suns-tech Corporations, Santa Cruz.CA, 'A new design for Information Centric Networks', Information Sciences and systems.

[12] Stojmenovic.I. 2002. 'Position Based Routing in Ad Hoc Networks,' IEEE Comm. Magazine, Vol. 40, no. 7, PP. 128-134.

[13] Trifunovic. S, Legendre. F, and Anastasiades. C. 2010. 'Social Trust in Opportunistic Networks,' Proc. IEEE INFOCOM, pp. 1-6.

[14] Vahdat. A and Becker. D. 2000. Epidemic Routing for Partially Connected Ad Hoc Networks,' technical report, Duke University, USA.

[15] 'The ns-3 Network Simulator. 2011. http://www.nsnam.org/.