Survey on Delay Tolerant Networking

[1]M.Rajalakshmi, [2]P.Rajeshwari, [3]Dr.S.Anbu
[1]M.E. Student, [2]M.E. Student, [3]Professor
[1]Department of Computer Science and Engineering,
[1]St. Peter's College of Engineering and Technology, Chennai, India.

***Abstract* - The malicious and selfish nodes are the serious threat of the delay tolerant network (DTN). The delay tolerant network is an intermittent connected network. It can tolerate larger delay comparing to the other networks. The misbehaving nodes must be identified and data must be transferred accordingly. Most of the delay tolerant networks use incentive schemes to make the selfish or misbehaving nodes effectively participate in the packet transmission and to reduce the rate of packet loss. Currently the Probabilistic Misbehavior Detection Scheme is being used for the effective transmission of packets in the delay tolerant network. This paper is a survey based on the delay tolerant network. It deals with the different techniques involved in the delay tolerant network.**

***Keywords* - Delay tolerant network, incentive schemes, and misbehavior nodes.**

I. INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires. The delay tolerant network is an intermittent network that comes under the adhoc network. The research is going how to implement the delay tolerant network for interplanetary communication.

Most of the techniques used in the other networks for finding the misbehaving nodes is not suitable for the delay tolerant network. It doesn't have end-to-end connectivity. The delay factor is tolerable to some extent. The black hole attack occurs often. The malicious nodes and selfish nodes are the serious threat of the DTN. So these factors have to be considered while handling the misbehaving nodes of the delay tolerant network.

II. DELAY-TOLERANT NETWORKING

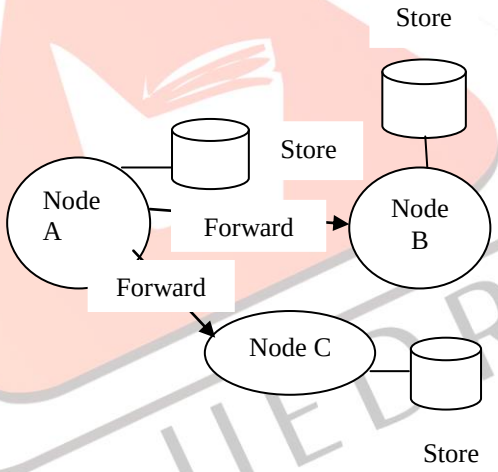

Fig 1 Store-Carry-Forward Strategy

Delay-Tolerant Networking is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity due to the limitation of the mobile nodes energy resources, attack and noise. In DTNs, the in-transit messages, also named bundles, can be sent over an existing link and buffered at the next hop until the next link in the path appears. So end- to-end routing path is not applicable for the DTN packet transmission. The message propagation process is usually referred to as the store-carry-and-forward strategy and the routing is done in opportunistic fashion [1][2].

DTN is a heterogeneous network that suffers from the frequent disconnectivity. The DTN characteristics are lack of contemporaneous path or instantaneous end-to-end path, high variation in network conditions, difficult to predict mobility patterns and long feedback delay. The Black Hole Attack is the major threat to the DTN. It is the attack done by the misbehavior nodes which drops the packets intentionally. The misbehavior node reduces the packet delivery rate which is the serious threat of DTN. The misbehavior can be caused by the selfish nodes or malicious nodes. The selfish nodes maximize their own benefits by enjoying the services of DTN but they refuse to forward the packets. The malicious nodes drop or modify the packet to launch attack to disrupt the network. The secure routing is needed to establish the trust among DTN nodes.

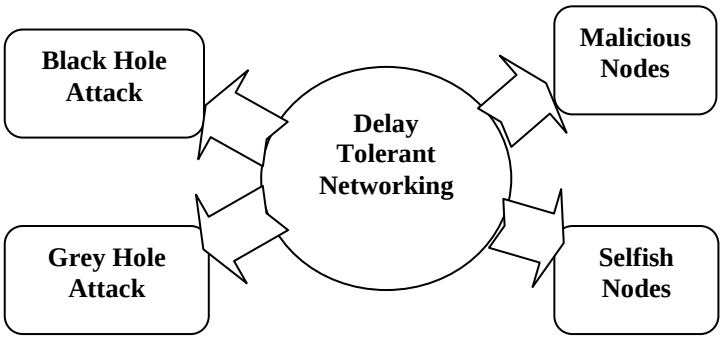

Fig 2 Threats of Delay Tolerant Network

III. RELATED WORKS

H. Zhu, X. Lin, R. Lu, Y. Fan, and X. Shen, say about the credit-based incentive scheme for the selfish nodes in delay tolerant network. The selfish nodes are the serious threat for the delay tolerant network. The selfish nodes try to save their wireless resources and refuse to serve as a bundle relay. The incentive is provided in the form of multi layered coin. The base layer is generated by the source node and it contains the payment rate, remuneration condition, class of service requirement and other rewards. The endorsed layer is generated by the intermediate node which is non-forgeable digital signature. The limitation is the attack on the payment rate [1].

Q. Li, S. Zhu, and G. Cao, convey that the selfish nodes are willing to forward the packets with which they have social ties. In this paper they have proposed Social Selfishness Aware Routing (SSAR). The forward node is selected with the user's willingness and the contact opportunity. The SSAR forms the data forwarding process as a Multiple Knapsack Problem with Assignment restrictions (MKPAR). MKPAR forwards the most effective packets for social selfishness and routing performance. The SSAR allocate resources i.e. buffer bandwidth based on the packet priority. It quantifies the relays willingness to evaluate the forwarding capability and thus reduces the packet dropping rate. The limitation is it is difficult to find always the social tie nodes as the neighbouring nodes [2].

Y. Ren, M.C. Chuah, J. Yang, and Y. Chen, explains that the packet delivery record can be used to overcome the misbehaviour nodes. A compromised node will attract more packets by faking packet delivery probability to other nodes. When two nodes encounter each other they will exchange packet and perform recording of the packet information. Each node will maintain two record tables. In the receiving record table, a node keeps packet exchange record generated by the encountering node. In the self record table a node maintains the record it generates for each node encountered. To identify the forge nodes these two records will be cross checked. The limitation of this paper is modification or attack on the self record [3].

R. Lu, X. Lin, H. Zhu, and X. Shen, says that the incentive scheme is used for overcoming the problem of the malicious and selfish nodes. The Pi (Practical incentive) protocol is used to provide the incentive scheme. The incentive will be fair and attractive. The incentive attracts or stimulates even the selfish nodes for forwarding to achieve better packet delivery performance. The electronic credit layered coin is used as the incentive. The intermediate selfish nodes which forwarded the packet will be credited if and only if the packet reaches the destination. This method gives high delivery ratio and low average delay. If the packet is dropped inbetween even the forwarded intermediate selfish nodes wont be provided with the incentive [4].

B.B. Chen and M.C. Chan convey that the incentive mechanism will encourage cooperation among the selfish mobile nodes. This paper uses the credit based incentive mechanism to encourage the selfish nodes to participate efficiently in the packet forwarding. The rational nodes will not purposefully waste transfer opportunity or cheat by creating non existing contacts to increase its reward. There are different payment mechanisms to cater to client that wants to minimize other payment or data delivery delay [5].

Sukhbirl, and Dr. Rishipal Singh proposed that the SRT drop policy is better than the DROP FRONT policy for different routing protocol. The different routing protocols tested are First Contact, ProPHET, Direct Delivery, Spray & Wait and Epidemic Routing protocols. The Drop Front will tend to drop the front message of the buffer. The SRT drop policy will tend to drop the larger sized message. The different metrics that are taken into account are delivery probability, overhead ratio, packet drop rate, buffer time and hop count. Considering all the metrics the SRT drop policy is good for the delay tolerant networking. This paper helps to find the effective routing protocol for delay tolerant networking [6].

Y. Zhu, B. Xu, X. Shi, and Y. Wang, done a survey on social based routing in delay tolerant networking. They discussed about the positive and the negative social characteristics of the social nodes. The knowledge of social characteristics are used for better forwarding of packet. The social relations and behaviors among the mobile users are usually long term characteristics and less volatile than node mobility. The positive social characteristics are the community and friendship to assist the packet forwarding. The negative social characteristics are the selfishness of the nodes [7].

Guoyou He says that the Destination Sequenced Distance Vector (DSDV) is the protocol that is appropriate for the dtn whereas the link state routing protocol and distance vector routing protocol does not fit for the dtn characteristics. The looping problem of these protocols can be overcome by the dsdv protocol. The DSDV routing protocol is a proactive protocol. The routing table will contain the metrics such as destination, metric (hop count), next hop and sequence number. The sequence number parameter makes this protocol efficient than the other. The route preference is given the newer sequence number or if equal sequence number then to the metrics [8].

H. Zhu, S. Du, M. Dong and Z. Cao says that the probabilistic misbehavior detection scheme is used for finding the misbehaving nodes in the delay tolerant network. The trusted authority uses this scheme to find the forward node is trusted one or

not. The trusted authority uses the forward history evidence contact history evidence and delegation history evidence to find the misbehaving nodes and the trusted nodes. It uses the inspection scheme. To further improve the system the reputation scheme is used. The nodes exchange the history evidences between them and the trusted authority collects and checks the evidences to find the misbehaving nodes. This scheme provides efficient trust establishment in delay tolerant network [9].

IV. PROPOSED SYSTEM

The probabilistic misbehavior detection scheme is used to find the misbehavior nodes in the network. The probabilistic misbehavior detection scheme uses the history evidences such as forward history, contact history and delegation history. Using this trusted authority finds the misbehavior nodes in the route. The Trusted Authority finds the higher probability packet delivery route. The route will be discovered without any misbehaving nodes. The data is forwarded through that route. The route has to be discovered such that the nodes will be moving dynamically. The route discovery is a tedious job for the dynamic nodes.

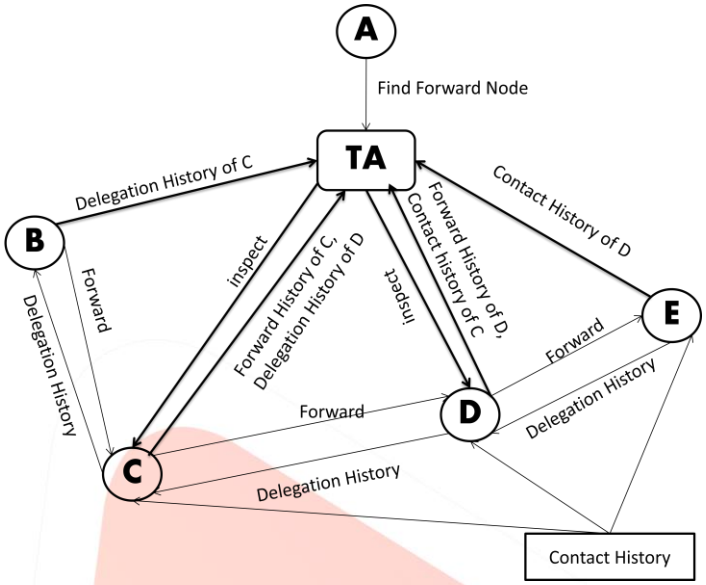

Fig 3 Architecture Diagram

The adversary nodes find the misbehaving nodes. Those node details are not maintained only by the specialized nodes, it is known to all the nodes. So there is no need for a single node to be a forward node. So randomly the forward nodes are selected according to the route discovery. The link nodes are used to connect the different path if required.

V. CONCLUSION AND FUTURE WORK

The probabilistic misbehavior detection scheme is the efficient method for finding the misbehaving nodes in the delay tolerant network. The trusted authority is responsible for the route discovery and data forwarding among the mobile nodes in the network. This scheme can be applied to the other kind of networks in future. The reputation scheme can also be used to further improve the efficiency of this scheme.

REFERENCES

[1] 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, Oct. 2009.

[2] Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay-Tolerant Networks," Proc. IEEE INFOCOM '10, pp. 1-9, 2010.

[3] Y. Ren, M.C. Chuah, J. Yang, and Y. Chen, "Detecting Blackhole Attacks in Disruption- Tolerant Networks through Packet Exchange Recording," IEEE, pp. 1-6, 2010.

[4] 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

[5] B.B. Chen and M.C. Chan, "Mobicent: A Credit-Based Incentive System for Disruption-Tolerant Network," Proc. IEEE INFOCOM '10, pp. 1 – 24, 2010.

[6] Sukhbirl, and Dr. Rishipal Singh "Effective routing protocols for delay tolerant network", IJMER, Vol. 2, Issue.4, July-Aug. 2012 pp. 1732-1735.

[7] Y. Zhu, B. Xu, X. Shi, and Y. Wang, "A Survey of Social-Based Routing in Delay Tolerant Networks: Positive and Negative Social Effects", IEEE Communications Surveys & Tutorials, Vol. 15, NO. 1, pp. 387 – 401, First Quarter 2013.

[8] Guoyou He, "Destination-Sequenced Distance Vector (DSDV) Protocol" Networking Laboratory, Helsinki University of Technology, pp. 1-9.

[9] H. Zhu, S. Du, M. Dong and Z. Cao, "A Probabilistic Misbehavior Detection Scheme toward efficient trust establishment in Delay-Tolerant Networks" IEEE Trans. On Parallel and Distributed systems, Vol 25, No 1, Jan. 2014, pp. 22-32.