ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A Survey on Detection of Malicious Nodes in Delay Tolerant Network

Prachi Jain

Assistant Professor, Department of Computer Science, SIRTE Bhopal, India

ABSTRACT: In Delay Tolerant Networks (DTNs), the information is transferred from its source to destination without end-to-end connectivity of the network. Delay Tolerant Networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Delay-Tolerant Networks (DTNs) consists of nodes that cooperate to forward messages despite connectivity issues. It also has a limitation in network resources. The DTN permits communication only if it is in the communication range. Because of this constraint there is a chance of dropping or dipping the received packets by the selfish or malicious nodes. Finally this leads to attacks. Malicious nodes within a Delay Tolerant Network (DTN) may attempt to delay or drop data in transit to its destination. Such attacks include dropping data, saturating the network with extra messages, humiliating routing tables, and imitating network acknowledgments. Malicious nodes consume network resources, plummeting its concert and accessibility; therefore they constitute an important issue that should be considered. Many approaches are proposed to solve the problems which are occurred in DTN. In this paper, we are providing a survey on Delay Tolerant Network to detect malicious node.

KEYWORDS: DTN, malicious node, detection, security

I. INTRODUCTION

Delay Tolerant Network-Delay tolerant networking is a networking structure that is designed to provide communications in the most unevenand stressed environment, where the network would generally be topic to regular and long lasting disturbance and high bit error rates that could severely degrade normal communications. Delay tolerant networks areoften used in disaster relief assignments, peace-keeping assignments, and in vehicular networks.
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 therouting is done in opportunistic fashion [1][2].

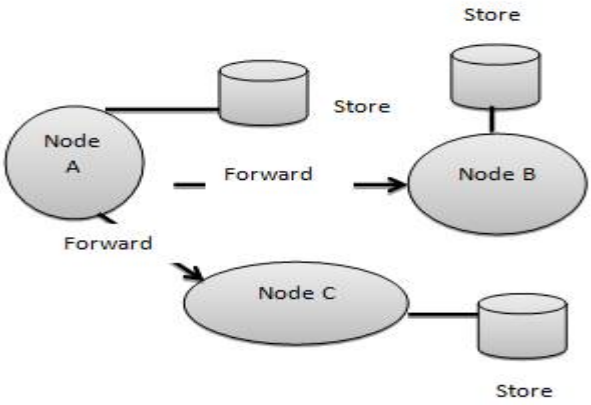

Fig 1.1 Store-Carry-Forward Strategies [8]

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

DTNs overcome the problems associated with intermittent connectivity, elongated or variable delay, distorted data rates, and great error rates through store-and-forward message switching. As shown in Figure whole messages (entire blocks of application program user data) or fragments of such messages are forwarded from a storage place on one node to a storage place on another node, beside a path that in timegrasps the destination. DTN routers requires persistent storage for their queues because

- A communication connection may not be easy to get for a long time.
- One node may send or receive data much quicker or more reliably than the other node.

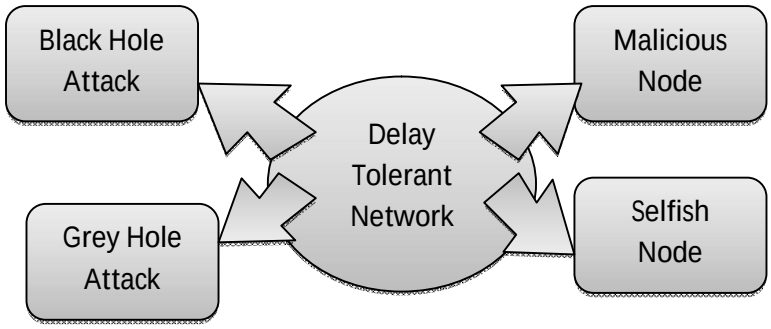

Fig 1.2 Threats of Delay Tolerant Network(DTN) [8]

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.
A delay tolerant network (DTN) is a network designed so that temporary or irregular communications evils, restrictions and incompatibilities have the smallestpossible adverse impact. There are several features to the effective design of a DTN, holding:

- The usage of fault-tolerant techniques and technologies.
- The superiority of agile dilapidation under aggressive situations or great traffic loads.
- The capacity to prevent or rapidly recuperate from electronic attacks.
- Capability to function with negligible latency even when routes are unclear or unpredictable.

Nodes in DTN-Mainly nodes in DTNs are of two types which are more different from other networks:
Selfish nodes minimize their assistances to the network communal and maximize their own gains by placing conniving nodes into the network communal (to grab information). Malicious nodes attack prope network operations and do not consider their own gains. DTNs security protocols have to be more invincible and powerful to handle these types of nodes.

a) SELFISH NODE: In the real world most people are selfish and selfish user usually trying to help other with whom he has social ties. Because he has got help from them in the past or will possibly get help from them in future. Aninterpersonal tie means asocialtie that is fall into strong or weak category. Social ties, a selfish user may give difference preference. He is willing to provide improved service to those with strong ties than those with weaker ties. Social selfish will effect on node behavior. Selfish node do not forward other data or packets, thus enlarge their gain at the overhead of all other. They are presumed to always behave rationally, so they cheat only if it gives them on advantage.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

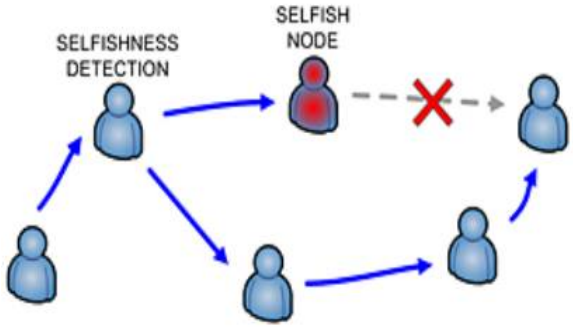

Fig 1.3 Selfish Nodes

In ad hoc network it does not depend on a pre-existing infrastructure, such as routers in wired networks or access points in managed wireless networks. Ad hoc network is a peer to peer network of wireless nodes where nodes are needed to execute routing activity to give end to end related among nodes. As mobile nodes are strained by battery power and bandwidth, some nodes may act selfishly and refuse forwarding packets for other nodes,even though they await other nodes to forward packets to keep network connected. Selfish nodes do not ahead data or control packets for other nodes and the second, selfish nodes put off their network combine card when they have nothing to broadcast. An ad-hoc network is a local area network that is built impulsively as devices connect. Instead of relying on a base station to equalize the flow of messages toeach node in the network, the specific network nodes forward packets to and from each other.

b) MALICIOUS NODE: Malicious nodes are exist in a delay tolerant network, they may attack to diminish network connectivity by pretending to be matched but in effect dropping any data they are meant to allow. These actions may result in defragmented networks, separate nodes, and drastically reduced network completion. We aim to evaluate the added effect of the presence of malicious nodes on Delay Tolerant Network (DTN) performance. Packet delivery cannot be assured even when malicious nodes are not present, and sending data packets again does not provide a good solution.

The simulation experiments examined various network conditions, including node density, portability speed, transportation power, and geographical circulation of devices. The simulation outcome determines that the existence of only one malicious node in a MANET can cause an added packet loss of more than 25%. With multiple packets droppers, nearly 60% of data packets could be vanished. In such cases, the existence of malicious nodes hasserious security indication.

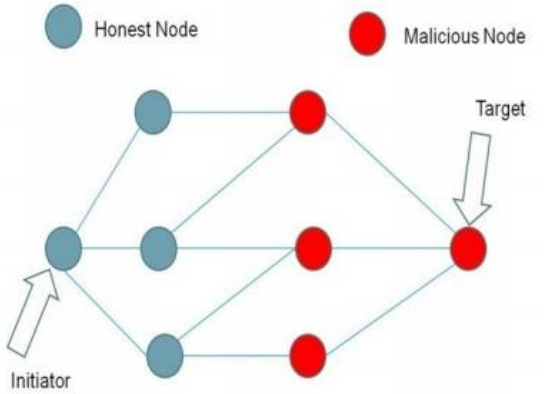

Fig 1.4 Malicious Nodes

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A DTN relies on the fact that nodes cooperate with each other to forward messages. A node can misbehave, i.e., to fail maliciously, generically in two ways: (1) by doing content failures, i.e., delivering modified messages; and (2) by doing timing failures, i.e., delivering messages out of time (or not at all, which corresponds to infinite delay, or repeatedly).
We do not consider the first class of misbehavior because it is simple to convert into omissions, which are timing failures. The mechanism to make this conversion consists simply in the sender concatenating a digital signature (obtained, e.g., with RSA or DSA) [18] to every message sent; the receiver verifying the signature and discarding or drop the message if the verification fails. This mechanism promises that if a node corrupts a message, this is equivalent to discarding or dropping it, except for the resources disbursed. Alternatively, using digital signatures it is also possible to have any non-malicious node doing the verification (using the public-key) and discarding/droppingcorrupted messages. We considered two types of misbehavior:

- **Type I**. By receiving the message, the node drops it. It is the quintessential selfish behavior.
- **Type II**. By receiving the message, the node drops it. Upon message creation, the node creates ten additional new messages and sends them. In spite of these forms of misbehaviors, we assume that all nodes receive the messages destined for them.

II. RELATED WORK

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 procedureas 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 neighboring nodes [2].
Y. Ren, M.C. Chuah, J. Yang, and Y. Chen, explains that the packet delivery record can be used to overcome the misbehaviornodes. 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 won't 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 &

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

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].

The Previous works [9][10][11] in DTNs have focused on building reputation management mechanisms. In reputation mechanisms there are two types of systems:

1. Global reputation systems: The reputation of a service provider is based on the ratings from general users [12] [13].
2. Personalized reputation systems: The reputation of a service provider is determined based on the ratings of a cluster of particular users, which may depend on different users worked on different systems [12] [14].

III. CONCLUSION

This survey paper gives an overview of Delay Tolerant Network (DTN) for detecting malicious node. We can conclude that 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 andNegative Social Effects”, IEEE Communications Surveys &Tutorials, Vol. 15, NO. 1, pp.387 – 401, First Quarter 2013.
8. M.Rajalakshmi, P.Rajeshwari, Dr.S.Anbu “Survey on Delay Tolerant Networking”, IJERD, Vol. 3, Issue 1, 2014.
9. E. Ayday,H. Lee,and F. Fekri,"An iterative algorithm for trust and reputation management," ISIT '09: Proceedings of IEEE International Symposium on Information Theory,2009.
10. E. Ayday, H. Lee, and F. Fekri, "Trust Management and Adversary Detection for Delay Tolerant Networks " Proc. IEEE Military Comm. Conf. (MILCOM '10),2010
11. E. Ayday and F. Fekri "An Iterative Algorithm for Trust Management and Adversary Detection for Delay Tolerant Networks., IEEE Transaction on Mobile Computing, Vol.ll, No.9,sept 2012.
12. G. Zacharia,A. Moukas,and P. Maes, "Collaborative reputation mechanisms in electronic marketplaces," HICSS '99: Proceedings of the Thirty-second Annual Hawaii International Conference on System Sciences-Volume 8,1999.
13. S. Buchegger and J. Boudec, "Coping with false accusations in misbehavior reputation systems for mobile ad-hoc networks," EPFL-DI-ICA Technical Report IC/2003/3I,2003.
14. C.Dellarocas, "Immunizing online reputation reporting systems against unfair ratings and discriminatory behavior," EC '00: Proceedings of the 2ndACM coriference on Electronic commerce,pp. 150--157,2000.
15. E. Ayday and F. Fekri, "A Protocol for Data Availability in Mobile Ad-Hoc Networks in the Presence of Insider Attacks,"Elsevier Ad HocNetworks, vol. 8, no. 2, pp. 181-192, Mar. 2010.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

BIOGRAPHY

Prachi Jain is a Assistant Professor in Computer Science Department at Sagar Institute of Research & Technology. She received Master of Technology degree in Software Engineering with a specialization of computer network from SVITS, Indore. Her research interests are Computer Network, Software Engineering and Cloud Computing etc.