Asian Journal of Computer Science and Technology
ISSN: 2249 - 0701 Vol. 3 No. 1, 2014, pp. 36-40

Malicious Packet Loss Identification in Disruption Tolerant Network

J. Shaldit Sheni[1], K.Jayashree[2] and B.Fowzia Sihana[3]

[1]PG Student, [2&3]Assistant Professor (SS), Rajalakshmi Engineering College, Chennai - 602 105, Tamil Nadu, India

E-mail: shenisj.88@gmail.com, jayashree.k@rajalakshmi.edu.in

(Received on 25 December 2013 and accepted on 05 March 2014)

Abstract – **In recent days network is suffering serious problems with the packet loss. Dropping of received packets, even it has adequate buffers is very common in Disruption Tolerant Network. The DTN node facilitates communication between mobile nodes. Sometimes the mobile node selects the DTN with lowest reputation that affects packet delivery ratio. If there is a malicious node in the route, the data packet does not reach its destination. Repeatedly the misbehaving nodes may forge some records to avoid being spotted. To solve these issues we propose a scheme to limit the packet rolling in the direction of misbehaving node. The contact record preserves the previous performance of DTN and the mobile nodes select the best rated DTN for its communication. The record handler is maintained to keep track of incoming and outgoing packets. The witness nodes identify the real misbehaving node. The malicious node needs to be identified and is barred. The genuine packet loss, malicious packet loss are differentiated.**

Keywords: **DTN, MN, Packet Loss, Misbehaving Node, Malicious Packet Loss, Packet life time**

I. Introduction

Delay and disruption-tolerant networks (DTNs), are characterized by their lack of connectivity, resulting in a lack of instantaneous end-to-end paths. Disruption-tolerant networks (DTNs) provide communication in circumstances that challenge outdated mobile network solutions. In these challenging environments, popular ad hoc routing protocols such as AODV and DSR fail to establish routes. This is due to these protocols trying to first establish a complete route and then, after the route has been established, forward the actual data. The malicious nodes within a DTN may attempt to delay or destroy data in transit to its destination. Such attacks include dropping data, flooding the network with extra messages, corrupting routing tables and counterfeiting network acknowledgments.

Mobile Nodes

A mobile node is an internet-connected device whose location and point of attachment to the Internet may frequently be changed.

There are 2 types of nodes.

1 Misbehaving nodes

2 Normal nodes

1. Misbehaving nodes

A misbehaving node drops the received packets even if it has available buffers, but it does not drop its own packets. We assume a small number of misbehaving nodes may collude to avoid being detected. Whether there exists a path between nodes or not, a malicious node can send fake routes to the legitimate nodes in order to get the packets or to disturb the operations.

2. Normal Nodes

Each packet has certain life time. The expired packets should be dropped whether or not there is buffer space. Such dropping can be identified if the expiration time of the packet is signed by the source. A normal node drop packets when its buffer overflows. Such dropping is not misbehavior.

Packet Loss

Packet loss occurs when one or more packets of data travelling across a computer network fail to reach their destination. Packet loss can be caused by a number of

factors including signal degradation over the network medium due to multi-path fading, packet drop because of channel congestion, corrupted packets rejected in-transit, faulty networking hardware, faulty network drivers or normal routing routines. Some network transport protocols such as TCP provide for reliable delivery of packets. In the event of packet loss, the receiver asks for retransmission or the sender automatically resends any segments that have not been acknowledged.

Routing Misbehavior in mobile ad-hoc networks

Routing is the transfer of data packets from one location to another, and it's one of the fundamental network functions. Network throughput, which is the ratio of data packets sent and received, is directly related to the routing function of any network. In other words, if the routing function is good enough, then we can expect a better output from the network. Routing in mobile ad-hoc networks is achieved through mobile nodes acting as intermediate nodes. These nodes are responsible for receiving and forwarding data packets from one host to another in the network. The absence of a fixed infrastructure makes routing a challenge in a mobile ad-hoc environment.

II. Packet Dropping and Mitigation

The technique watchdog and pathrater that increases the throughput in an ad-hoc network in the presence of nodes that agreed to forward the packet but fails to do so. We implement the watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. DTN routing usually follows "store-carry-forward". Each node maintains a rating for every other node it knows about in the network. If there are multiple paths to the same destination, we choose the path with the highest metric. There is the chance of denial of services. The packet needs to be in the buffer for a longer period of time. Watchdog suffers with low overhead, ambiguous collisions, receiver collisions, and limited transmission power [2].

An approach known as 2ACK scheme that serves as an add-on technique for routing schemes to detect routing misbehavior and to mitigate their adverse effect. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. The sending node waits for an ACK from the next hop of its neighbour to confirm that the neighbour has forwarded the data packets. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. If there are multiple paths to the same destination, we choose the path with the highest metric. The 2ACK scheme tries to detect those misbehaving nodes which have agreed to forward data packets for the source node but refuse to do so when data packets arrive. Chances of collision is more in 2ACK. ie) this technique is vulnerable to collusions; the neighbour can forward the packet to a colluder which drops the packet. Although end-to-end ACK schemes are resistant to such colluding attacks, the ACK packets may be lost due to the opportunistic data delivery in DTNs [3].

SCAN a unified network layer security solution for protecting the network layer from malicious attacks. This also protects both routing and data forwarding operations through the same reactive approach. In SCAN, local neighboring nodes collaboratively monitor each other and sustain each other, while no single node is superior to the others. It can crosscheck these packets to discover whether this neighbor behaves normally in advertising routing updates and forwarding data packets .The motivation is that a single node may have inaccurate monitoring results due to node mobility, interference, channel error, etc. The main disadvantages are more powerful collusion among the attackers will break SCAN. The communication overhead is due to token renewal, collaborative monitoring, and token revocation. It has impact on node mobility [4].

A network architecture and application interface structured around optionally-reliable asynchronous message forwarding, with limited expectations of end-to-end connectivity and node resources. The standardization of the IP protocol and its mapping into network-specific link-layer data frames at each router supports interoperability using a packet-switched model of service. Message aggregates are known as bundles and the routers that handle them are called bundle forwarders. They also may perform authentication and access control checks on arriving traffic to ensure forwarding is to be allowed. The disadvantage is it rejecting incoming connections for new messages when buffer space is full. The proactive methods are insufficient or unavailable. Synchronization problem is more common. However, they do not consider the intermittent connectivity in DTNs and cannot be directly applied to DTNs. Messages can fail to be delivered due to mis-addressing, persistent lack of intermediate or end-node storage, failure of

underlying transport protocols, or enforcement of policies on content[5].

A novel approach for user-centric data dissemination in DTNs, which considers satisfying user interests and maximizes the cost-effectiveness of data dissemination. The relay selection depends on the scope of network information maintained at individual nodes. This approach is based on a social centrality metric, which considers the social contact patterns and interests of mobile users simultaneously, and thus ensures effective relay selection. A relay is selected by its neighbor relay the maintenance of network information in DTNs is expensive. The major difficulty of user-centric data dissemination in DTNs is that the interesters of a data item are generally unknown a priori at the data source, because it is difficult for the data source to have knowledge about the interests of other nodes in the network [6].

In wireless ad hoc network, a collection of mobile nodes with no fixed infrastructure is common. When a source searches for a route to a destination, an intermediate node can reply with its cached entry. The intermediate node requests its next hop to send a confirmation message to the source. After receiving both route reply and confirmation message, the source determines the validity of path according to its policy. There is no administrative node to control the network, and every node participating in the network is responsible for the reliable operation of overall network. Data transmission overhead occurs. The route maintenance should be performed very often. The mobility of the packets becomes lower with increase in delivery ratio. The absence of central authorization facility in dynamic and distributed environment requires collaboration among nodes [7].

III. Problem Formulation

To remove the node this is misbehaving in Disruption Tolerant Network. Identifying the type of packet loss and finding out the suitable solution to fix it .The mobile node will select only the best DTN node from the contact records. By the above activity the packet delivery ration can be increased. This approach also detects the incorrect record of misbehaving node from being detected. The packet is encrypted to avoid unauthorized access. The number of packets travelling towards the misbehaving node can be minimized.

IV. Misbehavior Mitigation

The node that misbehaves are blacklisted and will not receive any packet from other nodes .It will be excluded from communication. The mobile nodes will not select the particular node as an intermediate for communication. A malicious node can enter in the network without authentication. All the malicious node purposely delay the packet forward to it. A malicious node can fiddle the content of the packets while forwarding. Whether there exists a path between nodes or not, a malicious node can send fake routes to the legitimate nodes in order to get the packets or to disturb the operations.

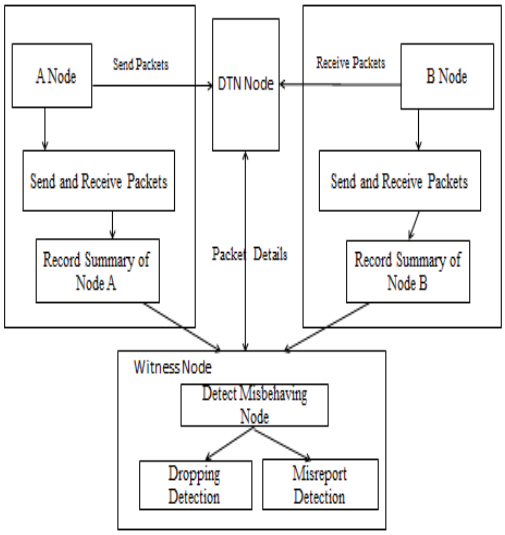

Fig. 1 DTN as an intermediate for communication

The Figure 1 demonstrates the communication between sender and receiver with DTN as an intermediate. The main duty of DTN node is to act as an intermediate bridge between mobile nodes. There will be multiple DTN nodes available for each mobile node. Each node signs a contact record with these DTN nodes. The contact record contains the previous performance of DTN. The DTN with best performance is used for packet transmission. The DTN receive the packet from the source. Based on the destination address in the packet DTN forwards the packet to the destination. The DTN is “store-Carry-Forward” basis. The DTN carry the packet till it finds the exact destination address. The DTN detect the packet to find whether it contains any SPAM messages .If it finds such messages in the packets, it drops the packets without forwarding. Such dropping is useful for the safety of rest of the nodes. This avoids SPAM messages

to be spreading to other mobile nodes. The DTN can detect the type of packet loss. It will report only if the packet loss is caused by attacker. If any node misbehaves it just trace the node and excluded it from the communication link. Here each nodes shares the data/packets with the another nodes. If the amount of packet received is beyond the buffer size we can simply drop the packets. Such dropping don't account any problem in the network. Also we detect whether the packet loss is due to genuine packet loss or malicious packet loss. If the packet loss is Genuine, then we can ignore and if the packet loss is caused by intruders we need to find solution.

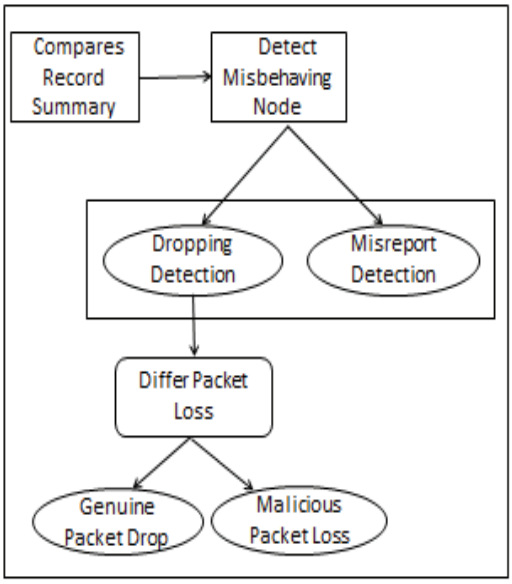

Fig. 2 Witness node role recognizing packet loss type

The Fig 2 illustrates witness node compares the record summary and detect whether there is any misbehaving node. Using the misbehaving node the witness node differentiates the packet loss type.

The modules narrative is as follows

Node to Node Communication

Here each nodes shares the data/packets with the another nodes. There is no network controller available for each node. So any nodes can be easily misbehave through another node. Also each node can send the data through the witness node only. Using the record of witness node we can validate the correct node and misbehaving node.

Witness Node

It maintains the data status of each node. It collects the data from a node and the information is stored. This information will be updated during each packet transmission. The past record of Witness node is used to verify whether the node is malicious node. It also acts as a barrier to SPAM messages entering into the network.

Record Handler

All nodes have its particular record handler. The main job of record handler is to collect the data from specific node for specific Record Handler. The witness node uses this record handler to compare with its record. The misbehaving node will be tracked and is excluded. It contains the history of all packets send and received. Even the node with SPAM messages has its own record handler.

Buffer Capacity Technique

The Buffer Capacity Technique (BCT) is used to find the original buffer capacity of the DTN Nodes. If the capacity of the DTN nodes is mentioned as 20 Mb and the node is sending the 10 Mb, but it originally handles only 5 Mb. By using this we may able to find the capacity of the buffer space easily by using the BCT. Similarly we differentiate genuine traffic packet loss with malicious packet loss, by comparing the Buffer level of every node. This makes us to find the type of attack easily.

Malicious Node

This node contains SPAM messages. It will send the SPAM message to any one of the node. Now this node is infected. As usual that node sends the SAPM messages to the Witness node. But Witness node verifies and drop packets. So every time malicious node can spread their data to any other node easily. It will take less performance and degrade to all nodes. So process will having more time available for complete.

Encryption And Decryption

For security purpose we're encrypting the data packet at the sender end and decrypt it in the receiver end. This will provide more security, when the data packets were hacked by the hacker at the time of data transmission. For Encryption we're using RC4 Algorithm.

V. Results

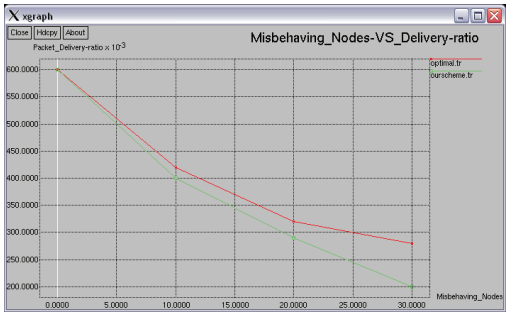

Fig. 3 Misbehaving Vs Packet Delivery Rate

The X-axis signifies the Misbehaving Nodes and Y-axis represents the Packet delivery ratio. When the misbehavior is more the packet delivering rate is very low. The packet delivered is high if the misbehavior is low.

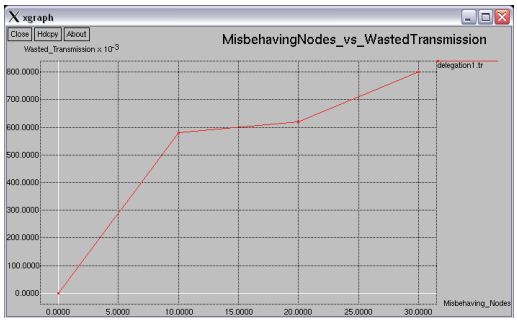

Fig. 4 Misbehaving Vs Wasted Transmission

The X-axis shows the Misbehaving node and Y-axis the wasted transmission.When the node starts to misbehave the number of packets wasted during transmision will be more. So the acknowledged packets will be less.

VI. Conclusion and Future Work

In this paper we have discussed the root cause for packet loss and identified the type of packet loss. Genuine packet loss is more common if the buffer size is less than the packet size. Misbehaving node is traced out and is not used for further communications. The proposed scheme is very generic and it does not rely on any specific routing algorithm.

In future the misbehaving node categorization and denial of service needs to be handled .The Quality of Service and maximum packet delivery ratio needs to be considered.

Acknowledgement

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions to improve the presentation of this paper. The authors extend the sincere thanks to Rajalakshmi Engineering College for the constant support and encouragement.

References

[1] Qinghua Li and Guohong Cao ,"Mitigating Routing Misbehavior in Disruption Tolerant Networks", *IEEE Transactions On Information Forensics And Security,* Vol. 7, No. 2, April 2012.

[2] Sergio Marti, T.J. Giuli, Kevin Lai, and Mary Baker ,"Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", in Proc. ACM MobiCom,2010.

[3] Kejun Liu, Jing Deng, Pramod K. Varshney, and KashyapBalakrishnan ,"An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs", in Proc. ACM MobiHoc, Sep 2006.

[4] Hao Yang, James Shu, XiaoqiaoMeng, Songwu Lu," SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks" ,in Proc.IEEE INFOCOM Aug 2005.

[5] Kevin Fall,"A Delay-Tolerant Network Architecture for Challenged Internets", in ACM, SIGCOMM'03, August 25-29, 2003,

[6] Wei Gao and GuohongCao,"User-Centric Data Dissemination in Disruption Tolerant Networks", IEEE 2009.

[7] Seungjoon Lee, Bohyung Han, Minho Shin,"Robust Routing in Wireless Ad Hoc Networks", in Proc. ACM MobiCom, 2009.

[8] Radhika Saini, Manju Khari,"Defining Malicious Behavior of a Node and its Defensive Methods in Ad Hoc Network", in IJCA, April 2011.

[9] John Burgess, George Dean Bissias, Mark Corner, Brian Neil Levine," Surviving Attacks on Disruption-Tolerant Networks without Authentication", in MobiHoc'07.

[10] Qiyan Wang, Long Vu, Klara Nahrstedt, Himanshu Khurana,"Identifying Malicious Nodes in Network-Coding-Based Peer-to-Peer Streaming Networks", IEEE INFOCOM, 2007.

[11] Alper T. Mzrak, Stefan Savage, Keith Marzullo," Detecting Malicious Packet Losses" IEEE transactions on parallel and distributed systems, Feb 2009.