ISSN 2278-7763

Categorizing Packet Loss in Disruption Tolerant Network

Gangadevi M, Vijayaraj A

Gangadevi M (PG Scholar)Department of Information Technology, Saveetha Engineering College, Chennai - 602105, India; Vijayaraj A (Assosiate Proffessor) Department of Information Technology, Saveetha Engineering College, Chennai - 602105, India.
Email: ganga.mathi@gmail.com

ABSTRACT

Disruption tolerant networks (DTNs) are a special type of wireless network which has the lack of continuous connectivity. Due to the unique characteristic of frequent partitioning in DTNs, multicasting is a considerably different and challenging problem. To overcome this issue Distributed scheme is used to detect packet dropping in DTNs. A node may misbehave by dropping packets. Routing misbehaviour can be caused by selfish nodes that are unwilling to spend resources such as power and bandwidth on forwarding packets. It reduces the packet delivery ratio and wastes system resources. Distributed scheme is used to detect packet dropping in DTNs. And genuine packet loss is differentiated with malicious packet loss by comparing the buffer level of every node and assigning bandwidth as per the category. For security, data packets are encrypted. Routing misbehaviour is reduced by limiting the number of packets forwarded to the misbehaving nodes.

Keywords : Disruption Tolerant Networks, malicious packet loss, routing misbehavior, genuine packet loss, misbehavior mitigation.

1 INTRODUCTION

Disruption Tolerant Networks (DTNs) are wireless mobile networks which results in the non-availability of an end-to-end contemporaneous path at each instant of time. Nodes are sparsely connected in tactical fields, and search and rescue missions. Due to high node mobility, low node density, and short radio ranges, thus leading to poor performance by the conventional Internet.

In DTNs, two nodes exchange data only when they move into the transmission range of each other. DTN routing usually follows "store-carry-forward." i.e., when a node receives some packets, it stores these packets in its buffer, carries them around until it contact another node, and then forwards the packet. These networks have a variety of applications in situations that include crisis environments, such as emergency response. And military battlefields, vehicular communication, deep-space communication, and non-interactive Internet access in rural areas. It has ability to prevent or quickly recover from electronic attacks and to function with minimal latency even when routes are ill-defined or unreliable.

In this paper we propose a Delegation routing algorithm to increase the performance. And after detecting packets drop misbehavior is categorized into genuine packet loss and malicious packet loss. To demonstrate this, we have an idea to simulate the effects of routing misbehavior in DTN routing algorithm. Delegation is a replication based routing algorithm where a packet may have multiple replicas. The message holder for each destination will replicate the copy (for that destination) and forward it to an encountered node that has a higher quality than all previous nodes seen so far, with respect to that particular destination.

This paper is structured as follows. Section 2 reviews related work. Section 3 introduces overview of our approach. Section 4 introduces our contribution. Section 5 concludes the paper.

2 RELATED WORK

Kejun et al. [2] proposed the 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 neighbor to confirm that the neighbor has forwarded the data packet. In order to reduce additional routing overhead, only a fraction of the received data packets are acknowledged in the 2ACK scheme. 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. The 2ACK scheme detects misbehavior through the use of a new type of acknowledgment packet, termed 2ACK.

The main disadvantages are it is more difficult to decide the behavior of a single node. This is mainly due to the fact that communication takes place between two nodes, and is not the sole effort of a single node. When a link misbehaves, either of the two nodes associated with the link may be misbehaving. In order to decide the behavior of a node and punish it, we may need to check the behavior of links around that node. Chances of collision is more in 2ACK.ie) this technique is vulnerable to collusions; the neighbor 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

ISSN 2278-7763

DTNs. Moreover, in routing protocols where each packet has multiple replicas, it is difficult for the source to verify which replica is acknowledged since there is no persistent routing path between the source and destination in DTNs.

Hao et al. [3] describes 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. SCAN also adopts a novel credit strategy to decrease its overhead as time evolves. Without appropriate protection, the malicious nodes can readily function as routers and prevent the network from correctly delivering the packets.

In SCAN, each node monitors the routing and packet forwarding behavior of its neighbors, and independently detects any malicious nodes in its own neighborhood. SCAN exploits two ideas to protect the mobile ad hoc network such as local collaboration and information cross validation. In cases, 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., and the malicious nodes may intentionally accuse legitimate nodes.

The main disadvantage is more powerful collusion among the attackers will break SCAN. The communication overhead due to token renewal, collaborative monitoring, and token revocation. It has impact on node mobility. Mobile ad hoc networks reduce the traffic flowing to the misbehaving nodes by avoiding them in path selection. However, they cannot be directly applied to DTNs due to the lack of persistent path.

To achieve interoperability Kevin Fall [4] proposes 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. These networks tend to be comparatively simple and local in scope.DTN gateways are responsible for storing messages in non-volatile storage when reliable delivery is required and mapping between differing transports by resolving globally-significant name tuples to locally resolvable names for traffic destined internally to an adjacent region. 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. Network fails to provide even the baseline abstractions that are well-matched for supporting layered protocol families. Email falls short due to its lack of dynamic routing, weakly defined delivery semantics, and lack of consistent application interface. With respect to routing, existing approaches rely on a set of mail relays which provide very little tolerance to network outages. 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

Sergio et al. [5] proposes a watchdog and path rater techniques 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. Ad hoc network are ideal in situations where installing an infrastructure is not possible. Ad hoc networks maximize total network throughput by using all available nodes for routing and forwarding. A node may misbehave by agreeing to forward packets and then failing to do so because of overloaded, selfish, malicious or broken. 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;" i.e., when a node receives some packets, it stores these packets in its buffer, carries them around until it contacts another node, and then forwards the packet. The path rater, run by each node in the network, combines knowledge of misbehaving nodes with link reliability data to pick the route most likely to be reliable. 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.

The major limitation is Currently the path rater only decrements a node's rating when another node tries unsuccessfully to send to it or if the watchdog mechanism is active and determines that a node is misbehaving. Without the watchdog active, the path rater cannot detect misbehaving nodes. 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. As neighborhood monitoring relies on a connected link between the sender and its neighbor, which most likely will not exist in DTNs. In DTNs, a node may move away right after forwarding the packet to its neighbor, and thus cannot overhear if the neighbor forwards the packet.

Wei et al. [6] proposes a novel approach for user-centric data dissemination in DTNs, which considers satisfying user interests and maximizes the cost-effectiveness of data dissemination. Our 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. The relay selection depends on the scope of network information maintained at individual nodes. A relay is selected by its neighbor relay. The effectiveness of relay selection depends on the scope of network information maintained at individual nodes. The new relay always has better capability of disseminating data to interested relays than the existing relays. A node estimate the interest of another node in a data item as probability, based on which we propose user-centric data dissemination from the social network perspective.

The main disadvantages of the paper are Relay selection is based on the local network knowledge may not be optimal. The data items to be selected mainly depend on the buffer size. Due to the lack of end-to-end network connectivity in

ISSN 2278-7763

DTNs, such difference essentially makes it difficult to guarantee the global optimality for relay selection, which means that every relay selection increases the global value. a relay selection which increases the local cost-effectiveness ratio may not necessarily increase the global ratio. Where nodes dynamically join and leave the network and network data is randomly being updated. The maintenance of network information in DTNs is expensive. The major difficulty of user-centric data dissemination in DTNs is that the interested relays 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.

Seungjoon et al. [7] suggests a wireless ad hoc network, a collection of mobile nodes with no fixed infrastructure. When a source searches for a route to a destination, an intermediate node can reply with its cached entry. To strengthen correctness of such routing discovery process, we propose a method in which 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. As a result, this strategy discourages malicious nodes from intercepting packets. 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. Since each node is free to move around, network topology frequently changes. Moreover, it uses open transmission medium, and every node within the range can access it .Before two nodes communicate with each other, they need to know the identity of the other party at first. Since all nodes act as routers and routing information can come from any node in most routing protocols, they should be able to tell if originators of routing information are valid and trustworthy. The percentage of data packets delivered to destination with respect to the number of packets sent. This metric shows the reliability of data packet delivery. The ratio of the number of packets sent or forwarded to the number of received packets at the destination. This metric reflects the efficiency of data packet delivery.

The main disadvantages of the paper are consequently, data packets sent through the path will not be delivered to destination. Data transmission overhead occurs. The route maintenance should be performed very often. The mobility of the packets becomes lower with increase in delivery ratio. It introduces additional route confirmation request and response messages, and is interoperable with most existing on demand routing protocols. Since bandwidth is a scarce resource in wireless environment, routing efficiency is more critical in ad hoc networks. The absence of central authorization facility in dynamic and distributed environment requires collaboration among nodes as there is no administrative node in wireless ad hoc networks, most network algorithms are based on the collaboration between nodes. In short wireless ad hoc network is inherently vulnerable.

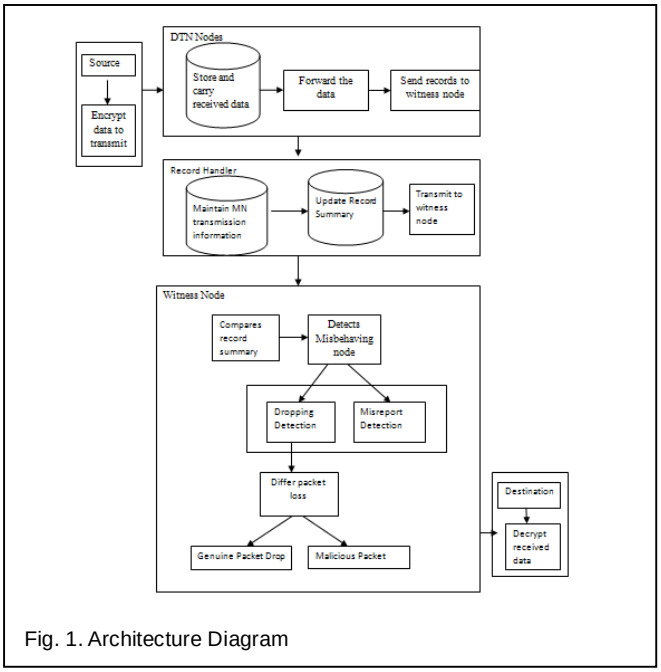

Fig. 1. Architecture Diagram

3 Overview Of The Approach

3.1 Packets Dropping Detection

A node is required to generate a *contact* during each contact and report its previous contact records to the contacted node which will detect if it has dropped packets since the previous contact. A misbehaving node may drop a packet but keep the packet ID, pretending that it still buffers the packet. Thus the next contacted node can easily detect this misbehaviour and will not forward packets to this misbehaving node. The record includes unique sequence number, what packets are in their buffers before data exchange, and what packets they send or receive during data exchange. In this way one node knows the two sets of packets the other node buffers at the beginning of the previous contact and the beginning of the current contact. Also knows the two sets of packets the other node sends and receives in the previous contact.

3.2 Misreporting Detection

A misbehaving node may report a false record to hide dropping from being detected. It results in inconsistency contact records. Misreporting is to replay an old record which is generated by previous record. Consistency rules such as using unique sequence number in each contact. To detect misreporting for each contact, normal node selects *w* witness nodes and transmits the record summary to them. The summary includes the part of the record necessary for detecting misreporting.

3.3 Record Handler

The Records handler is used to maintain the records of the each and every node. The records are all about the data transmission information like size of the packet, time from a particular node to the other nodes. From the Records handler we may able to find data transmission information each node.

ISSN 2278-7763

3.4 Witness Node

Witness node is a node which has some authority to compel testimony to have, knowledge relevant to an event or other matter of interest. The witness node will verify the original data packets the will be sent via each and every node. So that we can find the Attacker node or the node would give the wrong information

4 OUR CONTRIBUTION

4.1 Packets Dropping Detection

In DTN routing misbehavior is reduced by identifying malicious node using packets dropping detection. The packets drop naturally happen in the network. Packets drop are categorized into two: 1) Genuine packet loss and 2) Malicious packet loss.

By comparing the buffer level of every node and assigning bandwidth as per the category in DTN Genuine traffic packet loss is differentiated with malicious packet loss. To find the capacity of the node buffer a technique called Buffer Capacity Technique is used. Even though the node has a required buffer capacity, sometimes packets drop occurs in the network. It is called malicious packet loss. A packet loss is said to be genuine packet loss if the node does not have require buffer capacity to transfer the data or due to buffer overflow.

4.2 Delegation Routing Algorithm

Delegation is the routing algorithm used for DTN routing. It is a replication-based routing algorithm, where the receiving node replicates the packet to a neighbour if the neighbour has the highest utility it has seen. We use the contact frequency with the destination as the utility metric. In this scheme we do not rely on global information. (i.e.) forwarding decisions are made using local information only when nodes encounter. It only forwards the message to a node with a higher quality value than its own level value and 'asks' this node to help forward the message to destination. This approach does not need global knowledge. Each node decides whether it should or should not forward the message by itself. This is suitable for a distributed environment, such as DTNs.

4.3 Metrics

- **Detection rate:** The percentage of misbehaving nodes detected by normal nodes.
- **Detection delay:** The time taken to detect the misreporting.
- **Packet delivery ratio:** The percentage of packets delivered to the destinations.
- **Number of wasted transmission:** The percentage of packets dropped by misbehaving nodes.
- **Bytes transmitted per contact:** The number of bytes transmitted per contact.
- **Bytes stored per node:** The no bytes stored per node.

4 CONCLUSION

In this paper an algorithm used is for high performance. It works in a distributed way. And packets drop, misreporting are detected using the detection scheme. After that packet loss is categorized. This paper presented a scheme to detect packet dropping in DTNs. The detection scheme works in a disseminated way. Each node detects packet dropping based on nearby collected information and misbehavior is mitigated in DTNs.

REFERENCES

[1] Qinghua Li, Guohong Cao "Mitigating Routing Misbehavior in Disruption Tolerant Networks", IEEE transactions on information forensics and security, vol. 7, no. 2, april 2012.

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

[3] Hao Yang, James Shu, XiaoqiaoMeng, SongwuLu,"An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs" ,in Proc.IEEE INFOCOM Aug 2005.

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

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

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

[7] E. Daly and M. Haahr, "Social network analysis for routing in disconnected delay tolerant manets," in Proc. ACM MobiHoc, 2007.

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

[9] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for vehicle-based disruption-tolerant networks," in Proc.IEEE INFOCOM, 2006.

[10] Yunsheng Wang, Xiaoguang Li, and Jie Wu "Delegation Forwarding in Delay Tolerant Networks" Multicasting Department of Computer and Information Sciences Temple University Philadelphia, PA 19122, USA.

[11] V. Erramilli, A. Chaintreau, M. Crovella, and C. Diot, "Delegation forwarding," in *Proc. ACM MobiHoc*, 2008..