ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

Preserving Flood Attack on Delay Tolerant Network

[I]R.Saranya, [II]W.Lydia Shinny
[I,II]Dept. of CSE, Sethu Institute of Technology, Kariapatti, Tamilnadu, India

Abstract
Disruption Tolerant Networks utilize the mobility of nodes and the opportunistic contacts among nodes for data communications. Due to the limitation in network resources such as contact opportunity and buffer space, DTNs are vulnerable to flood attacks in which attackers send as many packets or packet replicas as possible to the network, in order to deplete or overuse the limited network resources. In this paper, we employ rate limiting to defend against flood attacks in DTNs, such that each node has a limit over the number of packets that it can generate in each time interval and a limit over the number of replicas that it can generate for each packet. We propose a distributed scheme to detect if a node has violated its rate limits. To address the challenge that it is difficult to count all the packets or replicas sent by a node due to lack of communication infrastructure, our detection adopts claim-carry-and check: each node itself counts the number of packets or replicas that it has sent and claims the count to other nodes; the receiving nodes carry the claims when they move, and cross-check if their carried claims are inconsistent when they contact. The claim structure uses the pigeonhole principle to guarantee that an attacker will make inconsistent claims which may lead to detection. We provide rigorous analysis on the probability of detection, and evaluate the effectiveness and efficiency of our scheme with extensive trace driven simulations.

Keywords
Delay Tolerant Network, claim-carry-and-check, flood attacks, telecommunication security, Detection.

I. Introduction

Disruption Tolerant Networks consist of mobile nodes carried by human beings vehicles etc. DTNs enable data transfer when mobile nodes are only intermittently connected, making them appropriate for applications where no communication infrastructure is available such as military scenarios and rural areas. Due to lack of consistent connectivity, two nodes can only exchange data when they move into the transmission range of each other which is called a contact between them. DTNs employ such contact opportunity for data forwarding with "store-carry-and-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 them. Since the contacts between nodes are opportunistic and the duration of a contact may be short because of mobility, the usable bandwidth which is only available during the opportunistic contacts is a limited resource. Also, mobile nodes may have limited buffer space. Due to the limitation in bandwidth and buffer space, DTNs are vulnerable to flood attacks. In flood attacks, maliciously or selfishly motivated attackers inject as many packets as possible into the network, or instead of injecting different packets the attackers' forward replicas of the same packet to as many nodes as possible. For convenience, we call the two types of attack packet flood attack and replica flood attack, respectively.

Flooded packets and replicas can waste the precious bandwidth and buffer resources, prevent benign packets from being forwarded and thus degrade the network service provided to good nodes. Moreover, mobile nodes spend much energy on transmitting/ receiving flooded packets and replicas which may shorten their battery life. Therefore, it is urgent to secure DTNs against flood attacks. Although many schemes have been proposed to defend against flood attacks on the Internet and in wireless sensor networks, they assume persistent connectivity and cannot be directly applied to DTNs that have intermittent connectivity. In DTNs, little work has been done on flood attacks, despite the many works on routing data dissemination, black hole attack wormhole attack, and selfish dropping behavior. We noted that the packets flooded by outsider attackers (i.e., the attackers without valid cryptographic credentials) can be easily filtered with authentication techniques. However, authentication alone does not work when insider attackers the attackers with valid cryptographic credentials flood packets and replicas with valid signatures. Thus, it is still an open problem is to address flood attacks in DTNs.

We employ rate limiting to defend against flood attacks in DTNs. In our approach, each node has a limit over the number of packets that it, as a source node, can send to the network in each time interval. Each node also has a limit over the number of replicas that it can generate for each packet the number of nodes that it can forward each packet to. The two limits are used to mitigate packet flood and replica flood attacks, respectively. If a node violates its rate limits, it will be detected and its data traffic will be filtered. In this way, the amount of flooded traffic can be controlled.

Our main contribution is a technique to detect if a node has violated its rate limits. Although it is easy to detect the violation of rate limit on the Internet and in telecommunication networks where the egress router and base station can account each user's traffic, it is challenging in DTNs due to lack of communication infrastructure and consistent connectivity. Since a node moves around and may send data to any contacted node, it is very difficult to count the number of packets or replicas sent out by this node. Our basic idea of detection is claim-carry-and-check. Each node itself counts the number of packets or replicas that it has sent out, and claims the count to other nodes; the receiving nodes carry the claims around when they move, exchange some claims when they contact, and cross-check if these claims are inconsistent. If an attacker floods more packets or replicas than its limit, it has to use the same count in more than one claim according to the pigeonhole principle,1 and this inconsistency may lead to detection. Based on this idea, we use different cryptographic constructions to detect packet flood and replica flood attacks. Because the contacts in DTNs are opportunistic in nature, our approach provides probabilistic detection. The more traffic an attacker floods, the more likely it will be detected. The detection probability can be flexibly adjusted by system parameters that control the amount of claims exchanged in a contact. We provide a lower and upper bound of detection probability and investigate the problem of parameter selection to maximize detection probability under a certain amount of exchanged claims.

II. Problem Definition

A. Existing System

Store-and-forward approach nodes store packets if they cannot find a next-hop node to deliver them to destinations. The each node first stores packets in its memory and then selectively transmits packets when it encounters other nodes based on various metrics including the last encounter time, the numbers of previous encounters, and the estimated packet delivery probability values to other nodes. Such metrics are derived from information provided by forwarding nodes themselves and it is hard to verify due to the network sparseness as well as the intermittent connectivity between nodes.

Disadvantages

- It is easy for an adversary to compromise nodes within the network and launch insider attacks using the compromised nodes.
- They cannot address insider attacks launched by compromised nodes.
- Insider attacks can cause significant problems in networks.

The main contribution is a technique to detect if a node has violated its rate limits. Each node itself counts the number of packets or replicas that it has sent out, and claims the count to other nodes; the receiving nodes carry the claims around when they move, exchange some claims when they contact, and cross-check if these claims are inconsistent.

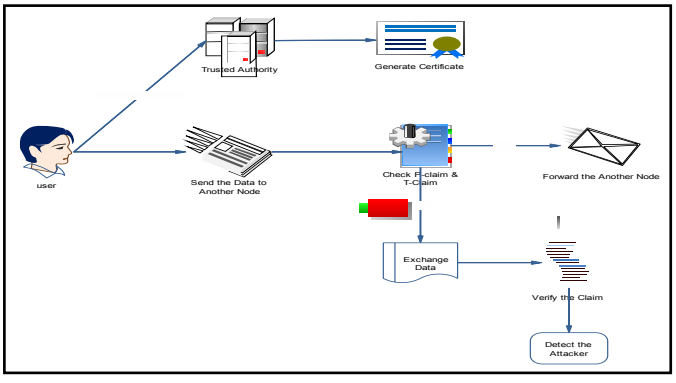
III. System Design

A. Proposed System

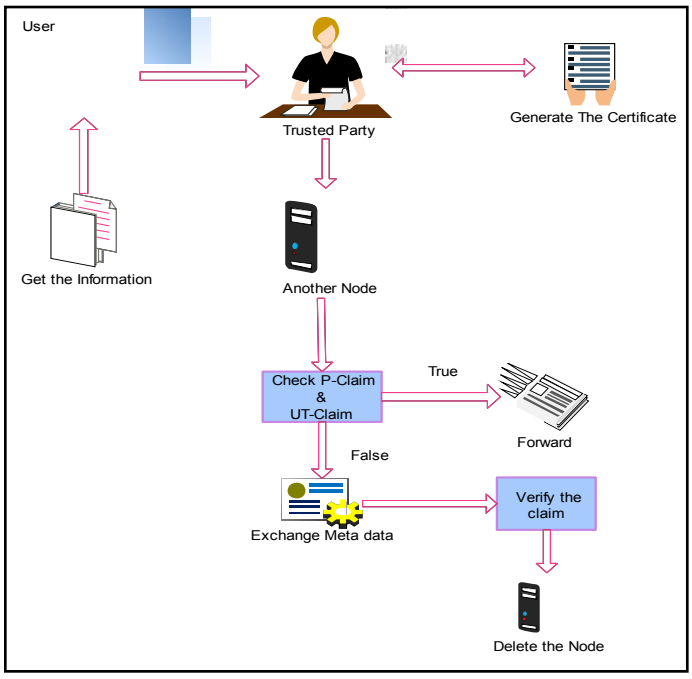
In Our Proposed System to employ the rate limiting to defend against flood attacks in DTNs. In our approach, each node has a limit over the number of packets that it, as a source node, can send to the network in each time interval. Each node also has a limit over the number of replicas that it can generate for each packet (the number of nodes that it can forward each packet to). If a node violates its rate limits, it will be detected and its data traffic will be filtered. In this way, the amount of flooded traffic can be controlled.

Advantages

- Our basic idea of detection is claim-carry-and-check.
- Each node itself counts the number of packets or replicas that it has sent out, and claims the count to other nodes.
- The receiving nodes carry the claims around when they move, exchange some claims when they contact, and cross-check if these claims are inconsistent.



Architectural Design



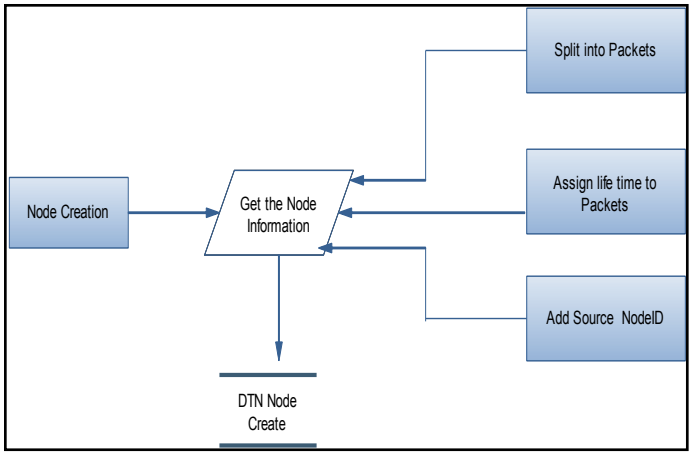
Data Flow Diagram

IV. Modules Description

Our Proposed work has the following modules. There is Listed Below

- DTN Network Creation
- Rate Limit Certification Creation.
- Claim Construction.
- Inconsistency Analysis.
- Metadata Exchanging Process.
- Verification Process

A. DTN Network Creation



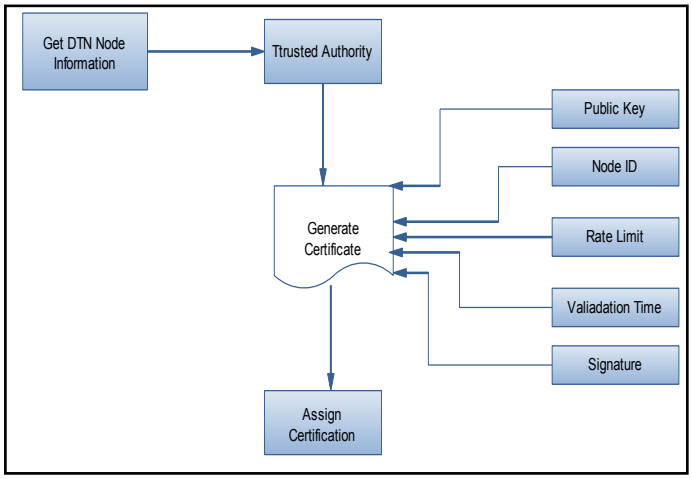
That every packet generated by nodes is unique. This can be implemented by including the source node ID and a locally unique sequence number, which is assigned by the source for this packet; we assume that each packet has a lifetime. The packet becomes meaningless after its lifetime ends and will be discarded.

B. Ratelimit Certification Reation

When a user joins the network, she requests for a rate limit from a trusted authority which acts as the network operator. In the request, this user specifies an appropriate value of L based on prediction of her traffic demand. If the trusted authority approves this request, it

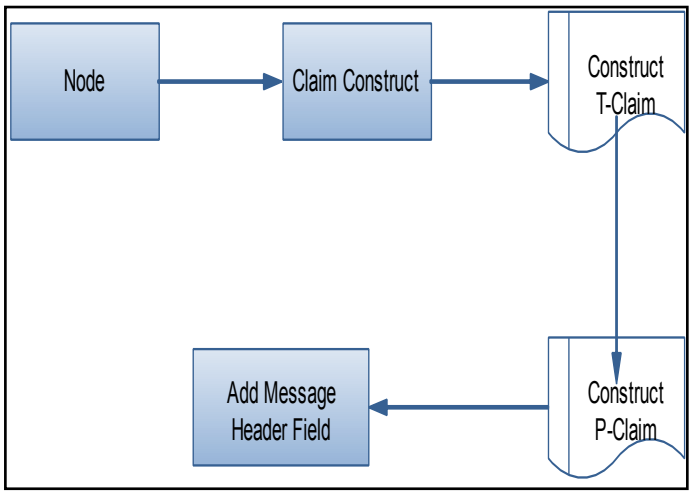
ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

issues a rate limit certificate to this user, which can be used by the user to prove to other nodes the legitimacy of her rate limit.Each node has a rate limit certificate obtained from a trusted authority. The certificate includes the node's ID, its approved rate limit L, the validation time of this certificate and the trusted authority's signature. The rate limit certificate can be merged into the public key certificate or stand alone.



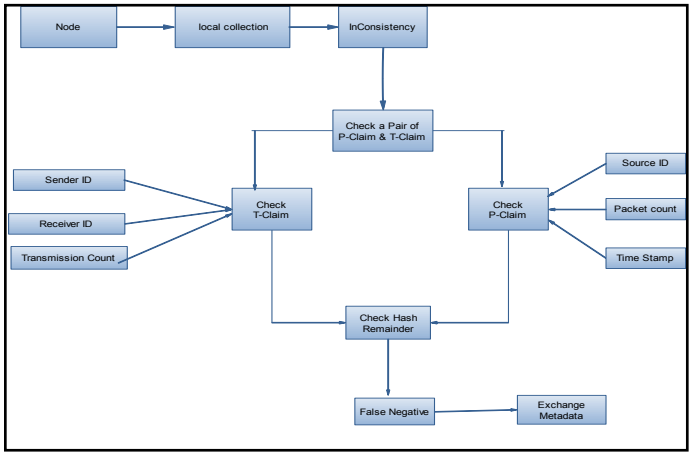
C. Claim Construction

P-claim is added by the source and transmitted to later hops along with the packet. T-claim is generated and processed hop-by-hop. Specifically, the source generates a T-claim and appends it to the packet. When the first hop receives this packet, it peels off the T-claim; when it forwards the packet out, it appends a new T-claim to the packet. This process continues in later hops. Each hop keeps the P-claim of the source and the T-claim of its previous hop to detect attacks.



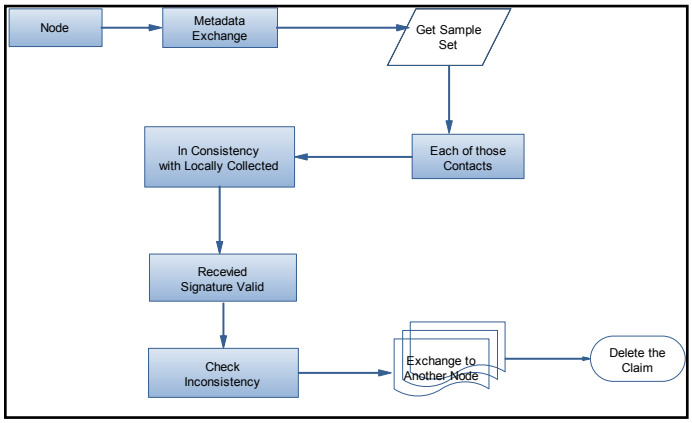
D. Inconsistency Analysis

The inconsistency check based on compact P-claims does not cause false positive, since a good node never reuses any count value in different packets generated in the same interval. The inconsistency check may cause false negative if the two inconsistent P-claims have the same hash remainder.



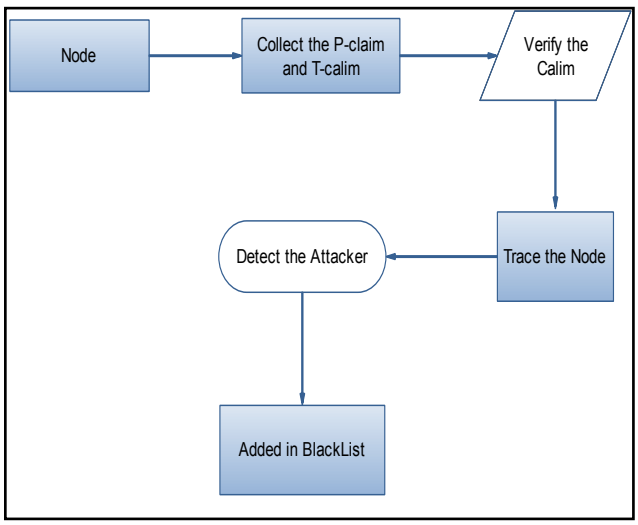
E. Metadata Exchanging Process

When two nodes contact they exchange their collected P-claims and T-claims to detect flood attacks. Each node maintains two separate sets of P-claims ,T-claims, for metadata exchange, a sampled set which includes the P-claims sampled from the most recent contacts with K different nodes and a redirected set which includes the P-claims redirected from those contacts. Both sets include Z P-claims obtained in each of those contacts.



F. Verfication Process

To better detect flood attacks, the two nodes also exchange a small number of the recently collected P-claims and T-claims and check them for inconsistency. When a node detects an attacker, it adds the attacker into a blacklist and will not accept packets originated from or forwarded by the attacker.



V. Conclusion & Future Enchancement

To employed rate limiting to mitigate flood attacks in DTNs, and proposed a scheme which exploits claim-carry-and-check to probabilistically detect the violation of rate limit in DTN environments. Our scheme uses efficient constructions to keep the computation, communication and storage cost low. Also, we analyzed the lower bound and upper bound of detection probability. Extensive trace-driven simulations showed that our scheme is effective to detect flood attacks and it achieves such effectiveness in an efficient way. Our scheme works in a distributed manner, not relying on any online central authority or infrastructure, which well fits the environment of DTNs. Besides, it can tolerate a small number of attackers to collude. Our scheme uses efficient constructions to keep the computation, communication and storage cost low. Also, we analyzed the lower bound and upper bound of detection probability. Extensive trace-driven simulations showed that our scheme is effective to detect flood attacks and it achieves such effectiveness in an efficient way. Our scheme works in a distributed manner, not relying on any online central authority or infrastructure, which well fits the environment of DTNs. Besides, it can tolerate a small number of attackers to collude.

References

[1] K. Fall, "A Delay-Tolerant Network Architecture for Challenged Internets," Proc. ACM SIGCOMM, pp. 27-34, 2003.

[2] P. Hui, A. Chaintreau, J. Scott, R. Gass, J. Crowcroft, and C. Diot,"Pocket Switched Networks and Human Mobility in Conference Environments," Proc. ACM SIGCOMM, 2005.

[3] M. Motani, V. Srinivasan, and P. Nuggehalli, "PeopleNet: Engineering a Wireless Virtual Social Network," Proc. MobiCom,pp. 243-257, 2005.

[4] J. Burgess, B. Gallagher, D. Jensen, and B. Levine, "Maxprop: Routing for Vehicle-Based Disruption-Tolerant Networks," Proc. IEEE INFOCOM, 2006.

[5] S.J.T.U.Grid Computing Center, "Shanghai Taxi Trace Data," http://wirelesslab.sjtu.edu.cn/, 2012.