www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 3 March, 2014 Page No. 4053-4056

Robustness of Disruption Tolerant Network against Flood Attacks

Priyanka H V[1], Akhila Thejaswi R[2]

[1]Department of Computer Science and Engineering, Sahyadri College of Engineering and Management Mangalore-575007

[2]Department of Information Science and Engineering, Sahyadri College of Engineering and Management Mangalore-575007

[1] IV Semester M.Tech (Computer Science and Engineering)

[2] Assistant Professor, ISE, Sahyadri College of Engineering and Management

Emails: [1]priyanka_hv@yahoo.com, [2]akhila.is@sahyadri.edu.in

***Abstract*— Disruption Tolerant Networks (DTNs) utilize the quality of nodes and also the opportunist contacts among node for information communications. Because of the limitation in network resources such as contact opportunity and buffer space, DTNs are at risk to flood attacks within which attackers send as several packets or packet replicas as possible to the network,so as to exhaust or overuse the restricted network resources. In this paper, there is a rate limiting to defend against flood attacks in DTNs, such that every node has a limit over the amount of packets that it will generate in every time interval and a limit over the amount of replicas that it will generate for every packet. There is a distributed scheme to discover if a node has violated its rate limits. To handle the challenge that it is troublesome to count all the packets or replicas sent by a node due to lack of communication infrastructure,the detection scheme adopts claim-carry-and check: every node itself counts the amount of packets or replicas that it has sent and claims the count to alternative nodes; the receiving nodes carry the claims once they move, and ensure if their carried claims are inconsistent once they contact; The claim structure uses the pigeonhole principle to ensure that an attacker will build inconsistent claims which can cause detection. There is a rigorous analysis on the possibility of detection, and valuate the effectiveness and efficiency of our scheme with in depth trace driven simulations.**

***Keywords*—** *DTN, flood attacks, security, detection, rate limit.*

I.INTRODUCTION

Disruption-tolerant networks (DTNs) give communication in situations that challenge ancient mobile network solutions. DTNs [1] consist of mobile nodes carried by human beings [2], [3], vehicles [4], [5], etc. DTNs use the inherent quality of the network to deliver messages in the face of sparse deployments, extremely mobile systems, and intermittent power [5]. DTNs enable information transfer when mobile nodes are only intermittently connected, making them applicable for applications wherever no communication infrastructure is available such as military situation and rural areas. Due to lack of consistent property, two nodes can only exchange information once they move into the transmission range of every alternative (which is named a contact between them). DTNs use such contact opportunity for information forwarding with "store-carry-and-forward"; i.e., once a good node receives some data, it stores these data in its buffer space,and carries them around until it contacts another different node, then it forwards them. Since the contacts between nodes are opportunistic and the time of a contact may be short, the usable bandwidth which is only available during the opportunistic contacts is a limited resource. Also, mobile nodes would have limited buffer space.

Due to the limitation in bandwidth and buffer space, DTNs are at risk of flood attacks. In flood attacks, maliciously or egotistically intended attackers inject as several packets as possible into the network, or instead of injecting completely different packets the attackers forward replicas of the identical packet to as many nodes as possible. For convenience, there are two kinds of attack they are packet flood and replica flood attack. Flooded packets and replicas packets will waste the precious bandwidth and buffer resources, which prevent good packets from being forwarded and therefore degrade the network service provided to good smart nodes. Moreover, mobile nodes pay a lot of energy on transmitting/receiving flooded packets and replicas which can shorten their battery

life. Therefore, it is imperative to secure DTNs against flood attacks. Although many schemes are projected to defend against flood attacks on the web [6] and in wireless sensor networks [7], they assume persistent connectivity and cannot be directly applied to DTNs that have intermittent connectivity. Thus, it is an open problem to address flood attacks in DTNs. In this paper, there is a rate limiting [8] to defend against flood attacks in DTNs. In this approach, every node has a limit over the amount of packets that it, as a source node, will send to the network in every time interval. Every node also has a limit over the number of replicas that it can generate for each packet (i.e., the number of nodes that it can forward every packet to). The rate limit scheme is used to mitigate packet flood and replica flood attacks. If a node violates its rate limits, it will be observed and its information traffic will be filtered. In this way, the quantity of flooded traffic is controlled.

II. EXISTING SYSTEM:

In Existing System the gateway of DTN is used. Gateway is a special node for counting amount of packet and storing the packets. It is also used to monitors the activities of nodes and detects an attack if there is any deviation from expected behaviour. [11]

III. PROPOSED SYSTEM

In our proposed system, the flood attack is a major problem. To defend against this flood attacks, node itself counts the amount of packets it as sent out. Every node includes a rate limit L on the number of unique packets that it as a source can generate and send into the network within every time interval T.The packets generated within the rate limit are deemed legitimate; however the packets generated beyond the limit are deemed flooded by this node. The rate limit is generated by the trustworthy authority for the source node depending on the packet count.

IV. BASIC IDEA

To observe the attackers who violate the rate limit L, we must count the amount of unique packets that every node as a source has generated and sent to the network among the present interval. However, since the node might send its packets to any node it contacts at any time and place, no alternative node can monitor all of its sending activities. To deal with this challenge, our plan is to let the node itself count the amount of unique packets that it has sent out, as a source node and claim the up-to-date packet count in every packet which is sent out. The node's rate limit certificate is additionally hooked up to the packet, such that other alternative nodes receiving the packet will learn its approved rate limit L. If an attacker is flooding a lot of packets than its rate limit, therefore it is a clear indicator of attack. If the claimed counts have been used before by the attacker in another claim, which is secured by the pigeonhole principle, and these two claims cause inconsistent. When the node received packets from the attacker, it carry those claims enclosed in those packets after they move around. Once two of the nodes contact, they check if there is any inconsistency between their collected claims. The attacker is detected once associate inconsistency is found.

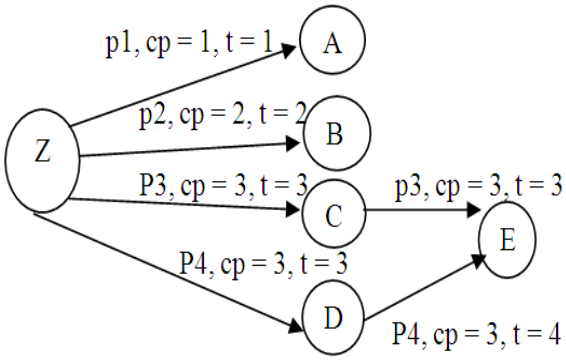

Fig 1. Packet Flood Detection

In the Fig. 1, Let's consider Z is as an attacker who injects 4 packets to nodes A, B, C, D. Where L is a Rate limit i.e. L = 3, cp is a packet count, t is a transmission count, If Z claims that the count value is 4 in p4, then that packet will be discarded, since rate limit included in the packet is 3,So Z dishonestly claims count to be 3, which is same as p3 . P3 packet is forwarded to E. When D and E contact, it acknowledges that two packets have the same count value. Therefore it detects that Z is an attacker and discards the packets and notify other nodes about the attacker.

V. MODELS

- Network Model
- Adversary Model
- Trust Model

Network Model: In DTNs, since contact durations will be short, a large data item is always split into smaller packets (or fragments) to facilitate data transfer. For simplicity, we have a tendency to assume that all packets have the similar predefined size. Though in DTNs the allowed delay of packet

delivery is typically long, it is still impractical to permit unlimited delays. Thus, we assume that every packet has a lifetime. The packet becomes unimportant when its lifetime ends and will be discarded. We assume that every packet generated by nodes is unique. This can be implemented by supplying the source node ID and a domestically distinctive sequence range that is assigned by the source for this packet, in the packet header. We also assume that time is loosely synchronic, specified any two nodes are within the same time slot at any time.Since the intercontact time in DTNs is often at the dimensions of minutes or hours, the time slot can be at the dimensions of one minute. Such loose time synchronization is not difficult to achieve.

Adversary Model: There are a variety of attackers within the network. An attacker can flood packets or replicas. On flooding packets, the attacker behave as a source node. It creates and injects a lot of packets into the network than its rate limit L. When flooding replicas, the attacker sends its buffered packets (which can be generated by itself or received from other nodes) more than its limit l for another nodes. The attackers can also be insiders with valid cryptographic keys. Some attackers may also collude and communicate via out-band channels.

Trust Model: We assume that a public-key cryptography system is accessible. For example, Identity-Based Cryptography (IBC) [9] has been shown to be practical for DTNs [11]. In IBC, only an offline Key Generation Center (KGC) is needed. KGC generates a non-public key for every node. Except the KGC, no party will generate the non-public key for a node id. With this type of system, an attacker can't forge a node identification and non-public key pair. Also, attackers do not know the non-public of a honest node (not attacker). Every node has a rate limit certificate obtained from a trustworthy authority. The certificate includes the node's ID, its secure rate limit L, the life time of this certificate and the trustworthy authority's signature. The rate limit certificate can be united into the general public key certificate or stand alone.

VI. CLAIM CONSTRUCTION

Two pieces of metadata units are added to every packet

1. Packet Count Claim (P-claim) and
2. Transmission Count Claim (T-claim)

P-claim is added by the source node and transmitted to later hops together with the packet. T-claim is generated by every node and processed hop-by-hop. Specifically, the source itself generates a T-claim and appends it to the packet. Once the first hop receives this packet, it peels off the received T-claim; once it forwards the packet out, it appends a brand new T-claim to the packet. This technique continues in later hops. Every hop keeps the P-claim of the source and also the T-claim of its previous hop to notice attacks.

P-Claim: When a source node S sends a brand new packet m (which is generated by S and not sent out before) to a contacted node, it generates a P-claim. The P-claim is hooked up to packet m as a header field, and will be forwarded together with the packet to later hops. Once the contacted node receives this packet, it verifies the signature within the P-claim, and checks the worth of cp(packet count). If cp is larger than L, it discards this packet; otherwise, it stores this packet and also the P-claim.

T-Claim: When node A transmits a packet m to node B, it attaches a T-claim to m. The T-claim consists of A's current transmission count ct for m (i.e., the number of times it has transmitted m out t to n number of nodes) and also the current time t.

VII. INCONSISTENCY CAUSED BY ATTACK

In a dishonest P-claim, an attacker uses a smaller packet count than the real value. (We don't take into account the case wherever the attacker uses a much bigger packet count than the real value, since it doesn't make any sense for the attacker.) However, this packet count has been used in another P-claim generated earlier. This causes an inconsistency referred to as count reuse, which implies the utilization of the identical count in two completely different P-claims generated by the identical node.

VIII.ALGORITHM

Algorithm 1: The protocol must be run by every node during a contact

1: Metadata P-claim and T-claim is exchange and attack is detected with rate limit;
2: if Have packets to send then
3: For every new packet, P-claim and T-claim is generated;
4: Attach and send every packet with the P-claim and T-claim; end if
5: if Receive a packet then
6: if the count value in its P-claim or T-claim is invalid then discard this packet; end if
7: Check the P-claim and T-claim against those collected locally and generated among the same time interval to

observe inconsistency;
8: if Inconsistency is determined then
9: Tag the signer of the P-claim (T-claim, respectively) as an attacker and
10: Disseminate an alarm against the those attacker to the network;
11: else
12: Store the new P-claim and T-claim; end if end if

IX. PERFORMANCE EVALUATIONS

The following are the performance evaluation metrics:

- Detection rate: The ration of attackers that are observed out of all the attackers.
- Detection delay: From the time the primary invalid packet is sent to the time the attacker is observed.
- Computation cost: The typical range of signature generations and analysis per contact.
- Communication cost: The amount of P-claim/T-claim pairs transmitted into the air, normalized by the amount of packets transmitted.
- Storage cost. The time-averaged kilobytes stored for P-claims and T-claims per every node.

X. EXPECTED RESULT

The followings are the results which will be analysed in this system.

Communication cost: The communication cost mainly has two elements. One element is that the P-claim and T-claim transmitted with every packet, and the alternative element is that the partial claims transmitted during metadata exchange. As to the latter, at the most P-claims and T-claims are exchanged in every contact, with one half for sampled and the other half for redirected claims.

Storage cost: Most P-claims and T-claims are compacted when the packets are forwarded. The sampled P-claims and T-claims are stored in full until the packets are forwarded or are exchanged to K nodes, whichever is later, then compacted. For every received packet, less than 20 bytes of compact claims are stored for restricted time duration.

Collusion Analysis: One attacker might send a packet with a dishonest packet count to its colluder, which is able to forward the packet to the network. Certainly, the colluder won't exchange the dishonest P-claim with its contacted nodes. However, so as long as the colluder forwards this packet to a honest node, this honest node has a chance to observe the dishonest claim as well as the attacker.

XI. CONCLUSION

In this paper, we tend to use rate limiting to mitigate flood attacks in DTNs, and planed a scheme that exploits claim-carry-and-check to probabilistically discover the violation of rate limit in DTN environments. This scheme uses efficient constructions to keep the computation, communication and storage price low. Also, we analyzed the lower bound and upper bound of detection probability. This scheme works in a very distributed manner, not counting on any on-line central authority or infrastructure, which well fits the atmosphere of DTNs.

REFERENCES

[1] K. Fall *"A Delay-Tolerant Network Architecture for Challenged Internets," proc.ACM SIGCOMM*, 2003.

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

[3] M. Motani, V. Srinivasan, and P. Nuggehalli, *"People Net: Engineering a Wireless Virtual Social Network," Proc. MobiCom*, 2005.

[4] G.D. Bissias, M. Corner, J. Burgess, and B.N. Levine *"Maxprop :Routing for Vehicle-based Disruption Tolerant Network,"Proc. IEEE INFOCON*, pp 1-11, 2006.

[5] Zhi-Jun Li, Shou-Xu Jiang *"Planning the Mobility of Routing Ferries for Intermittently Connected Mobile Networks," in ICST International Conference*, 2011.

[6] A.Afanasyev, P. Mahadevan, I.Moiseenko,E.Uzun,and L.Zhang, *"Internet flooding attack and countermeasures in Named Data Networking," in IFIP Network Conference*, 2013.

[7] R. Bhatnagar and U. Shankar,*"The proposal of hybrid intrusion detection for defence of sync flood attack in wireless sensor network,*" *International Journal of Computer Science & Engineering Survey*, vol. 3, pp. 31-38, 2012.

[8] Barath Raghavan, Kashi Vishwanath, Sriram Ramabhadran, Kenneth Yocum, and Alex C. Snoeren, *"Cloud Control with Distributed Rate Limiting," SIGCOMM*, 2007.

[9] C. Gentry and A. Silverberg, *"Hierarchical Id-Based Cryptography," Proc. Int'l Conf. Theory and Application of Cryptography and Information Security EUROCRYPT*, 2002.

[10] A. Seth, D. Kroeker, M. Zaharia, S. Guo, and S. Keshav, *"Low cost Communication for Rural Internet Kiosks Using Mechanical Backhaul," Proc. ACM Mobicom*, 2006.

[11] V. Natarajan, Y. Yang, and S. Zhu, *"Resource-Misuse Attack Detection in Delay-Tolerant Networks,"Proc. Int'l Performance Computing and Comm. Conf. (IPCCC)*, 2011.