ISSN:0975-9646

Mitigating Flood Attack Using AODV in Disruption Tolerant Network

Jananii.M, Vasanthi.S

PG scholar,Department of Information Technology,
Sona College of Technology, Salem,TN,India

Assistant Professor, Department of Information Technology,
Sona College of Technology,Salem,TN,India

Abstract :Disruption Tolerant Network is a networking architecture that is designed to provide communications in the most unstable and stressed environments. The network would normally be subject to frequent, long lasting disruptions that could severely degrade normal communications. Disruption tolerant network abbreviated as DTN make use of mobility of nodes for data communication. Two mobile nodes can exchange data when they move into the transmission range as they are connected intermittently. DTN is a network designed to limit the temporary or intermittent communication problems and anomalies have the least possible adverse impact. DTN network is used in environment where no communication infrastructure is available such as rural area and military scenario. DTN network lacks end-to-end connectivity. Thus, this network is vulnerable to flood attack which in turn causes the disconnection of the network. So the packet delivery ratio is affected and reduced. Thusa new trust approach based on the extent of friendship between the nodes is proposed which makes the nodes to co-operate and prevent flooding attacks in a Disruption tolerant network environment. The performance of the trust algorithm is tested in andisruption network implementing the secure Ad hoc On-demand Distance Vector protocol.

Index Terms-DTN, flood attack, detection

I INTRODUCTION

Disruption tolerance network [1] is a network that is designed to provide communication in an environment which is frequently subjected to disruption that could strip down normal communication in such environment. In Disruption tolerant network communication is made possible even there is no end-to-end connectivity. Disruption tolerant network is abbreviated as DTN, provide data communication by using the mobility of nodes in unstable environment where persistence infrastructure is not available like space communication, rural areas and military. Two mobile nodes can exchange data when they move into the transmission range as they are connected intermittently. Due to opportunistic contacts and lack of periodical contact DTN "store-carry-and-forward" for data forwarding. i.e., When a node receives a packet it stores that packet in buffer, carry them until it contacts other node and forward the packet.

Due to short duration of contact of nodes because of mobility, limitation in buffer space and other resources, DTN are liable to flood attack. In flood attack, the selfishly or maliciously motivated attackers add different packets or forward the replica of same packet to as many nodes as possible. Flood attack is of two types: Replica flood attack and packet flood attack. These attacks by injecting and forwarding more packets, they jam the network, waste the limited buffer space and bandwidth resources and thus degrade the network services. In addition the nodes spend more energy for receiving and transmitting flooded packet which may reduce their battery life. Thus DTN is need to be secured from flood attack. Although many schemes have been proposed to defend against flood attack in internet[6] they assume persistence connection.

In this paper, they employed secure Ad hocOn-demand Distance Vector protocol[3],[6] to mitigate flood attack. This paper is organized as follows section2 provides the techniques used, in section3 the methodology is given, section4 provides existing system, section 5 provide the result and conclude the paper.

II BACKGROUND WORK

Disruption tolerant network is an approach to building architecture that models network tolerant to long delays. The properties of DTN are High Latency, Low Data Rate, Disconnection, LongQueuing Delay, Short Range Contact, Dynamic Network Topology. The application of Telemedicine for Developing Regions, DTN-based Social Network Service , Communication in the Presence of Oppressive Governments , File Sharing and Bulk Data Transfer , Share Air Minutes. As DTN is an opportunistic kind of network which is characterized by absence of end-to-end path that leads to various attack. So to defend against flood attack rate limit factor is introduced.

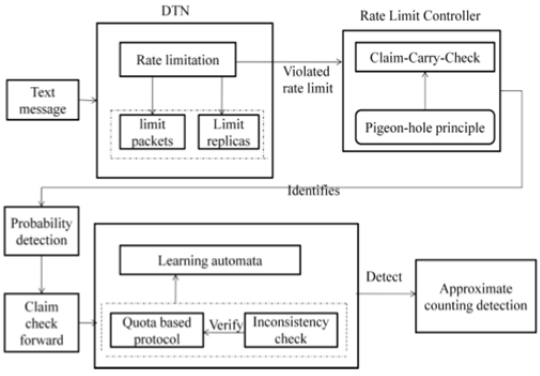

Fig 2.1 System architecture for self-adaptive approach

As per this approach, as a source node every node has limit over the number of packets it can generate. Every node has limit over the number of replicas it can forward. Thus any node violates the rate limit factor will be detected and alarmed to other nodes. In this manner, amount of flooded packets are controlled.

The main contribution is the detection technique for violation of rate limit. In challenging network like DTN due to mobility of nodes and intermittent connection it is difficult to count the number of replicas and packets transmitted. Thus they make use of "claim-carry-and-check: Instead of maintaining a separate node to determine the violation, each node must itself count the number of packets or replica it has sent and claims the count to other nodes. The received nodes carry the claim and exchange it with next node and cross check when inconsistence occurs.

21. *FLOOD ATTACK*

For selfish or malignant purpose many node launch flood attack. Selfish node launch flood attack in order to increase their throughput and delivery ratio. In DTN, as nodes are mobile and due to opportunistic contact the probability of delivering single packet to destination is less than one. Thus, to increase their delivery ratio the selfish nodes replicate their packets. For example John needs to send packet to David. John creates 100 different packets of original which only vary in unimportant padding bytes and sent it to David. While David receives anyone of those 100 variant packets, he ignores the padding byte and gets the original. Thus the throughput of the selfish node increases. Malignant node exploits flood attack to waste precious resources.

2.2 METHODOLOGY

2.2.1 *SETTING THE RATE LIMIT*

Request-approve style method is used to set the rate limit factor F. On joining the network the user request for rate limit based on their traffic demand from network operator. To prove to other nodes the user uses the rate limit factor issued by network operator. The certificate comprises of node's ID, approved rate limit, authority's signature, validation of this certificate. To avoid unwanted request of large rate limit, the user pays virtual currency or amount of money for her rate limit.

2.3 NETWORK MODEL

In DTN, all packets are assumed to be in same predefined size [4],[5],[7]. Every packets have lifetime, after that time ends the packet became meaningless and so it will be discarded. The packets generated by each node are unique.

III PROPOSED IDEA

Ad hoc On-demand Distance Vector protocol is proposed to mitigate flood attack in DTN. Using neighborhood suppression, a single threshold is set up for all neighboring nodes In Data flooding attack the attack node first sets up the path to all the nodes and send useless packets. The given solution is that the data packets are identified in application layer and later path cutoff is initiated.

3.1 **Topology Formation and Hello packet sending**

In this phase, project design in NS-2 is constructed and hello packets are sent. Based on the sensing capability each node identify its topology that is neighboring nodes. Each node will send hello packets to neighbors those are all in within the communication range.

3.2 **Malicious node activities**

In this phase, the activities of malicious nodes in the network are shown. A malicious node may actively involve in the flooding attack by repeatedly sending RREQ or garbage DATA packets to different destinations some of which never exists. And also which will drop data packets from sender to receiver, and also in some cases it will inject false data between sources to destination.

3.3 **Flooding attack prevention**

A trust estimator is used in each node to evaluate the trust level of its neighboring nodes. Accordingly, the neighbors are categorized into friends (most trusted), acquaintances (trusted) and strangers (not trusted). To prevent RREQ flooding, the threshold level is set for the maximum number of RREQ packets a node can receive from its neighbors. To prevent DATA flooding, the intermediate node assigns a threshold value for the maximum number of data packets it can receive from its neighbors. Attack detection strategy that it relies on the ability of honest nodes to detect the discrepancy between the expected PDR (ePDR) and the perceived PDR (pPDR).Based on that values we will detect and Eliminates malicious nodes in the network. To isolate attackers, our protocol uses a controlled-accusation mechanism which is used to inform about the presence of malicious nodes in the network.

IV SYSTEM OVERVIEW

4.1 CLAIM-CARRY-AND-CHECK

To discover the violation of rate limit factor F, we need to count the number of packets generated and transmitted by a source node. Since it is opportunistic contact between nodes i.e., node can meet any node and transfer packets at any time it is difficult to set a node for monitoring the packet count. So, they introduce the basic idea of each node itself count the number of packets and claim the updates to the targeted node. Every node is provided with rate limit certificate for authentication purpose. If any malicious or selfish node adds packets more than its rate limit factor then it must claim a value smaller than its rate limit which is already been used. It cannot claim larger value than rate limit factor F. Two pieces of metadata are added to each packet to find the violation.

A. *FLOOD PACKET DETECTION*

Packet Count Claim (P-claim) is added by the source and transmitted to later hops along with the packet.Each hop keeps the P-claim of the source to detect attacks.

When a source node S sends a new packet m (which has been generated by S and not sent out before) to a contacted node, it generates a P-claim as follows:

P-claim: $S, c_p, t, H(m), SIG_S(H(H(m)|S|c_p|t))$

Let S is an attacker that successively sends out four packets to A, B, C, and D, respectively. Since L = 3, if S claims the true count 4 in the fourth packet m4, this packet will be discarded by D. Thus, S dishonestly claims the count to be 3, which has already been claimed in the third packet m3. m3 (including the claim) is further forwarded to node E. When D and E contact, they exchange the count claims included in m3 and m4, and check that S has used the same count value in two different packets. Thus, they detect that S as an attacker.

B. REPLICA FLOOD DETECTION

Transmission Count Claim (T-claim) is used to detect replica flood attacks. 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 T-claim of its previous hop to detect attacks.

When node A transmits a packet m to node B, it appends a T-claim to m. The T-claim includes A's current transmission count ct for m (i.e., the number of times it has transmitted m out) and the current time t. The T-claim is

T-claim: $A,B,H(m),c_t,t,SIG_A(H(A|B|H(m)|c_t|t))$.

B checks if ct is in the correct range based on if A is the source of m. If ct has a valid value, B stores this T-claim.

C. PROTOCOL

Suppose two nodes contact and they have a number of packets to forward to each other. Then our protocol is sketched in Algorithm 1.

Algorithm 1. The protocol run by each node in a contact

1: Metadata (P-claim and T-claim) exchange and attack detection
2: if Have packets to send then
3: For each new packet, generate a P-claim;
4: For all packets, generate their T-claims and sign them with a hash tree;
5: Send every packet with the P-claim and T-claim attached;
6: end if
7: if Receive a packet then
8: if Signature verification fails or the count value in its P-claim or T-claim is invalid then
9: Discard this packet;
10: end if
11: Check the P-claim against those locally collected and generated in the same time interval to detect inconsistency;
12: Check the T-claim against those locally collected for inconsistency;
13: if Inconsistency is detected then
14: Tag the signer of the P-claim (T-claim, respectively) as an attacker and add it into a blacklist;
15: Disseminate an alarm against the attacker to the network;
16: else
17: Store the new P-claim (T-claim, respectively);
18: end if
19: end if

4.2 INCONSISTENCY CHECK

Suppose node W wants to check a pair of P-claim and T-claim against its local collections to detect if there is any inconsistency. The inconsistency check against full claims is trivial: W simply compares thepair of claims with those collected. In the following, we describe the inconsistency check against compactly stored claims.

A. INCONSISTENCY CHECK WITH P-CLAIM

From the P-claim node W gets: the source node ID S, packet count cp, timestamp t, and packet hash H. To check inconsistency, W first uses S and t to map the P-claim to the structure C^i_s. Then it reconstructs the hash remainder of H using the locators in C^i_s. If the bit indexed by the packet count cp is set in the bit-vector but the hash remainder is not included in C^i_s, count reuse is detected and S is an attacker.

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. However, since the attacker does not know which bits constitute the hash remainder, the probability of false negative is only 2^{-8}. Thus, it has minimal effect on the overall detection probability.

B. INCONSISTENCY CHECK WITH T-CLAIM

From the T-claim node W gets: the sender ID R, receiver ID Q and transmission count ct. IfQ is W itself (which is possible if the T-claim has been sent out by W but returned by an attacker), W takes no action. Otherwise, it uses R to map the T-claim to the structure C_R. If there is a 2-tuple IN C_R is same then the issuer of the T-claim is an attacker.

4.3 ALARM

Suppose in a contact a node receives a claim C_r from a forwarded data packet or from the metadata exchange process. and it detects inconsistency between C_r and a local claim C_l that the node has collected.

If C_l is a full claim, the node can broadcast a global alarm[8] to all the other nodes to speed up the attacker detection process. The alarm includes the two full claims C_l and C_r. When a node receives an alarm, it verifies the inconsistency between the two included claims and their signatures. If the verification succeeds, it adds the attacker into its blacklist andbroad- casts the alarm further; otherwise, it discards the alarm. The node also discards the alarm if it has broadcast another alarm against the same attacker.

5 SYSTEM ANANLYSIS

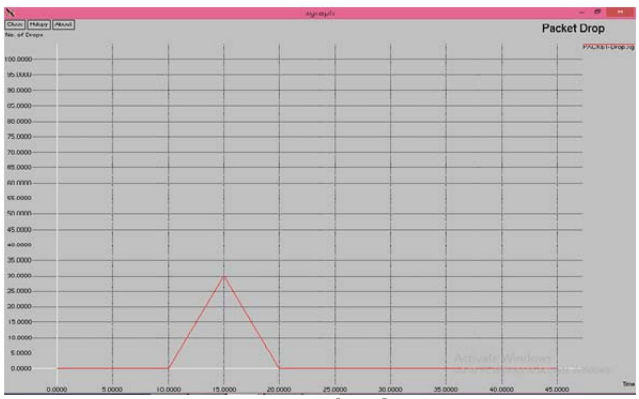

Fig 5.1 Packet drop

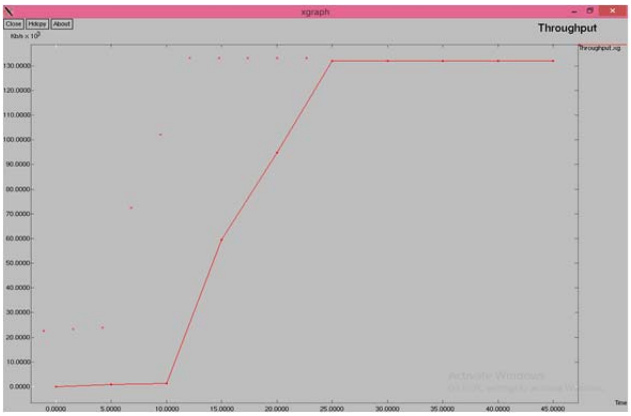

Fig 5.2 Throuh put

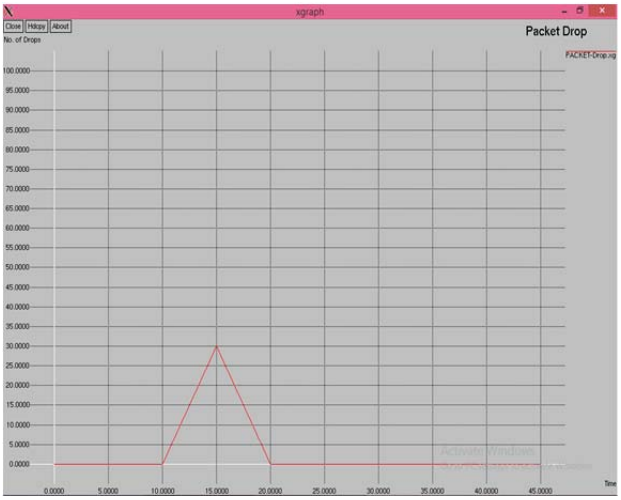

Fig 5.3 Packet delivery ratio

6. CONCLUSION

In this paper, to mitigate flood attacks in DTNs, they employed adhoc on-demand distance vector routing protocol. This scheme is effective to detect flood attacks and it achieves such effectiveness in an efficient way. This 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. It increases the packet delivery ratio in turn increases the network services by mitigating the flood attack in such environment.

REFERENCE

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

[2]. J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms. Prentice Hall, 2005.

[3]. B. Raghavan, K. Vishwanath, S. Ramabhadran, K. Yocum, and A. Snoeren, "Cloud Control with Distributed Rate Limiting," Proc. ACM SIGCOMM, 2007.

[4]. T. Spyropoulos, K. Psounis, and C.S. Raghavendra, "Efficient Routing in IntermittentlyConnected Mobile Networks: The Multiple-Copy Case," IEEE/ACM Trans. Networking, vol. 16, no. 1, pp. 77-90, Feb. 2008.

[5]. W. Gao and G. Cao, "On Exploiting Transient Contact Patterns for Data Forwarding in DelayTolerant Networks,"Proc. IEEE 18th Int'l Conf. Networks Protocols (ICNP), 2010.

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

[7]. R. Groenevelt, "Stochastic Models in Mobile Ad Hoc Networks," technical report, Univ. of Nice, Sophia Antipolis, INRIA, 2006.

[8]. S.C. Nelson, M. Bakht, and R. Kravets, "Encounter-Based Routing in Dtns," Proc. IEEE INFOCOM, pp. 846-854, 2009.