Journal of Computer Science 10 (7): 1216-1221, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.1216.1221 Published Online 10 (7) 2014 (http://www.thescipub.com/jcs.toc)

DETECTION OF FLOOD ATTACKS IN DTN USING RATE LIMITER TECHNIQUE

Balamurugan, C., M. Viswanathan, T. Abhishek Kumar and G.S. Raj

Department of CSE, VEL Tech University, Chennai, India

Received 2013-12-04; Revised 2013-12-30; Accepted 2014-02-19

ABSTRACT

Flood attacks means a network becomes so weighed down with packets, caused by the attackers. It prevents packets being sent/received between the nodes in the network. There are many methods adopted to prevent flood attacks in other networks, but none has been installed successfully for DTN’s. Disruption tolerant network is a network, developed in such a manner that intermittent communication problems have very low effect on the outcome of the result. However, due to the limited network resources in this network such as buffer space and bandwidth, it is liable to flood attacks. In order to protect resources and defend against flood attacks, the rate limiting technique should be adopted. In which each node must be set up with a restriction over the number of packets it can send to the network and number of duplicates that can be created for each packets, such as rate limit L and rate limit R respectively. However flood attacks are caused even in application level resulting in losses of resources such as CPU and sockets. So, technique for detection of application level floods attacks is implemented by verifying DNS query with a specific tool and validating it with mysql database.

Keywords: Flood Attacks, DTN, Disruption Tolerant Networks

1. INTRODUCTION

Disruption tolerant network is a valuable network includes mobile nodes which enable to transfer data among nodes. The connection among nodes may be held inconsistently or intermittently connected. Due to this inconsistency, two nodes can transfer data when they enter into an communication range of each other. Data is transferred via keep-carry-forward method. When the node receives the packet it locates in its buffer and holds until a contact is established with neighbour node and then moves the packet forward.

However DTN’s has limitations such as low bandwidth and buffer space. Due to this they are liable to flood attacks. A flood attack is one in which the attackers send as many packet into the network and overuse the limited resources. Two types of flood attacks are packet flood attack and replica flood attack. There are many methods to prevent flood attacks, but none has been inducted for DTN’s. A flood attack caused by outsider (unauthorized) can be prevented by authentication techniques. However it is not possible to prevent for attack caused by insiders (authorized).

In order to defend flood attacks, rate limiter technique is employed,where assigned each node a restriction for the total packets it can send to the network and number of duplicates it can reverberate for each packet. If the node crosses its rate limits, it will be detected as flood attack.

An method is adopted, where each node counts the total packets it has sent out and acknowledges the count value to the other nodes. The node which receives the packet holds the value around and check inbetween to see if the values are changed. If it is found to be inconsistent, then flood attack has been detected. The application level flood attack is detected by verifying DNS query with a specific tool and validating it with database.

A Flood attack is one in which the attackers submit a large number of requests to servers through multiple Proxy agents which minimizes server resources within short interval and causes denial of services. Such attacks are developed by completely ignoring the normal firewall protection; attacks can be done easily

Corresponding Author: Balamurugan, C., Department of CSE, VEL Tech University, Chennai, India

using the proxy agents such as botnet computers which is shown in the **Fig 1**. The limitations for the attacker are that, when met with static web pages proxies will expose attackers' IP addresses.

Attackers cause flood attacks for selfish purposes. Malicious nodes are the nodes that are willfully deployed by the adversary or attackers to exhibit attacks and reduce the network resources of other nodes. In DTN, the delivery ratio of an packet to the destination is of a probability <1, due to the intermittent connectivity. If a node generates many duplicates of its own packet,there is an increase in packet delivery ratio, because the delivery of any duplicate packet proves delivery of the original packet. For example, Assume S sends a packet to T. S can develop 200 packets similar to the original packet it distinguishes in two or three bytes and sends the 200 similar packets to T separately without any dependency. When T receives atleast one of the 200 packets, it leaves away the additional byte and generate the original packet.

The severity of flood attacks in DTN can be found considering the routing strategies. 1. Single routing: A node should delete its copy of a packet after forwarding a packet out. Theredore, each packet holds only one duplicate in the network. 2. Multicopy routing: The source node of a packet sends some amount of duplicates of the packet to other nodes using the single routing method. The highest number of duplicates that each packet can generate is determined initially and cannot be altered.In the simulations it explains that 3 duplicate packets are permitted to be generated.A duplicate flood attacker duplicates the packets and sends to every node that does not have a copy. Each good node generates 30 packets on the 121st day of the Reality trace and the same method is used for duplicate flood attacks. Each packet validity gets over in 50 days. The size of the buffer of every node is 10 MB, bandwidth is 300 kbps and size of the packet is 20KB.

Flood attacks are caused due to the following aspects which motivates the attacker to cause a flooded attack.

1. Financial gain: In this, the attackers do for the nature of their incentive; they are generally the most technical experienced attackers. These attacks are the most dangerous and unstoppable attacks. 2. Revenge: Attackers belonging to this category are usually frustrated or painful individuals, who seek to take revenge on the organization, the reason for revenge may or may not be justified. However they have low technical skills, 3.Ideological trust: Attackers of this category are inspired by their ideological beliefs to attack their targets or enemies. This category is the most happening and common attackers and this ideology is the main reason for the attackers to launch flood attacks.4. Intellectual confrontation: Attackers in this category attack the target network in order to experiment, analyze and learn how to launch the various attacks.

1.1. Motivated Work

The implementation of rate limiting technique was introduced in order to reduce network traffic caused by the attackers. TCP based design was effective and can be employed in large networks (Raghavan *et al*., 2007).

A network architecture was proposed which has limited network resources and connectivity, which will be useful for inconsistent communication networks (Fall, 2003).

The routing concept in disruption tolerant networks wre inducted using an protocol.Maxprop protocol was used to improve the features of DTN (Burgess *et al*., 2006).

Detection of black hole attacks in DTN is done using encounter ticket technique. Encounter ticket technique provides security and detects malicious nodes (Li *et al*., 2009).

Later, the technique of generating relation record was implemented to prevent malicious nodes from dropping packets. The relation record holds the information from the souce to the current node (Li and Cao, 2012).

A technique to detect replication attacks in sensor networks was injected, where the detection is achieved using multicast algorithm. Some kind of inconsistency leads to node detection (Parno *et al*., 2005)

1.2. Existing Framework

Due to the low bandwidth and inadequate buffer space, Disruption tlerant network are liable to flood attacks. In flood attacks, attackers insert maximum number of packets into the network. Sometimes the attackers forward duplicates of the packet to the other nodes. Flooded packets degrade the bandwidth and buffer resources. Mobile nodes use more resource on sending and receiving those packets which reduces their battery life. Flood attack prevents packets of normal users to be moved and thus degrades the performance of network and its service for the other nodes. There are many methods to prevent flood attacks for other networks such as wireless sensor networks, but none has been inducted for DTN. Eventually the method adopted was to prevent attacks caused by unauthorized persons. But mostly attackers are with authorized credentials. So no method has been developed to prevent attacks caused by insiders. Therefore it is necessity to prevent and secure disruption tolerant networks from flood attacks.

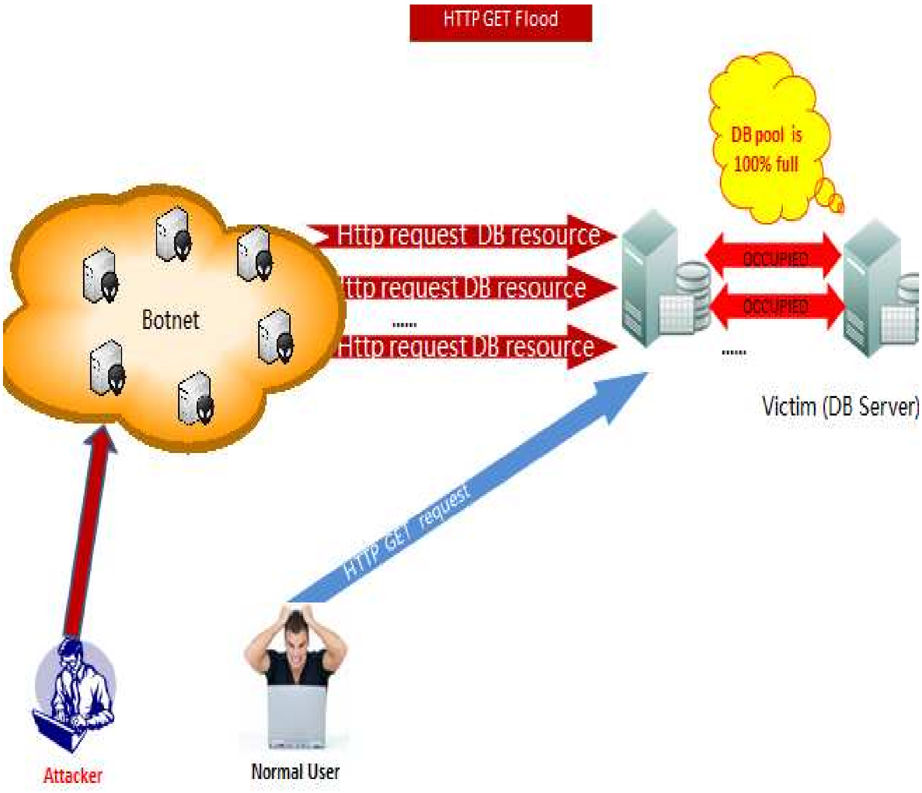

Fig. 1. Overview of Flood Attack

1.3. Proposed Framework

1.3.1. Improvised Detection Using RL Technique

In this each node has a rate limit L on the number of unique packets that it can generate and send within time interval T. the time interval are 0, T, 2T. To defend against packet flood attacks, our goal is to detect if rate limit is exceeded. Time interval must not be either too long or too short. It should be appropriate.

In this, the goal is to set a limit R on the number of times that the node can forward this packet to other nodes. A node's limit R is determined by the routing protocol. In multicopy routing, R = L' if node is a source node and R = 1 if node is intermediate node. In single copy routing, R = 1 irrespective of source or intermediate node. However L and R are not dependent upon each other.

When the user joins the network, the user should requests for a rate limit from a network operator. The network operator issues a rate limit certificate to this user. Rate limit can be increased or decreased according to the demand.

Identity Based Cryptography (IBC) is suitable for DTN's. In this, only an offline key generation is required.OKG generates a private key for every node based on node's ID and assigns security for the node. So except OKG, no other party can generate the private key for a node ID. In this type of system an attacker cannot forge a node ID and private key pair. Each node can be enhanced with security by providing a rate limit certificate to it by a trusted authority. The certificate includes node ID, its rate limit L, the validation time of the certificate and trusted authority signature. Assume that each and every packet generated by nodes is unique. This can be done by including the source node ID and a unique sequence number, which is assigned in the packet header. In DTNs, since the duration of contact is short, a large data is usually split into smaller packets for swift data transfer. Packet delivery ratio should be maintained. The packet not delivered on time will be discarded.

1.4. Flooding Attacks (Application Level)

Flooding attacks are caused at 2 levels, Network and application layer. In this, defensive mechanism for application level is adopted. Transport layer attacks deals with network resources such as bandwidth. Application layer deals with server resources such as CPU, sockets, memory and database. Generally attacks are generated through specialized computers; attackers send lots of service request to the target network and cause traffic. Eventually it slows down\and crashes. Flood attacks have incurred huge losses for organizations. Two hour of network traffic, can indulge in losses for the advertising revenue. Though several defensive mechanisms have been adopted, the attackers have found complex methods to attack. Application level: The attackers disrupt legitimate users by attacking server resources such as CPU, memory they generate DNS query with fake IP address, which leads to network traffic as DNS response are larger than DNS queries. This traffic is directed to target system and flood it. In order to defense, actually most of the application level deals with the client server model. Server offers service to the client and the client requests for innumerable services. Defense technique should be employed at server, where the attack has occurred. DNS detection technique includes a scheme where DNS requests are made through a specific tool. The tool verifies query and validates with Mysql database, if it does not seem to be legitimate, it instructs that attack has been caused.

1.5. Methodology

It is difficult to count the no of packets the source node has generated. So we implement a method, such that the node itself should count the number of packets it generates. It claims up to date count in each packet sent out to other node along with rate limit certificate.

If attacker is flooding more packets, then it has to dishonestly claim a count smaller than real value. This indicates attack. This method is similar to mechanism where attacks are detected due to the inconsistency in values In the **Fig. 2**, Consider Z is an attacker that sends 4 packets to nodes A, B, C, D. Rate limit L = 3, cp = packet count, t = transmission count, If Z claims that count value is 4 in p4, then that packet will be discarded (because rate limit = 3) So Z dishonestly claims count to be 3, which is same as p3. P3 is forwarded to E. When D and E contact, it acknowledges that same count value in 2 packets. Therefore it detects that Z is an attacker and discards it.

Transmission count is induced for each packet to notify the number of times each packet has been transferred. It has limit R, based on false claims the attacker is detected, similar to packet flood attack. In this rate limit R = 2. ct refers to transmission count.

In the **Fig. 3**, the node Z claims the transmission count ct = 2 again for node C. then, the node C directs the packet p1 to B, where it cross checks and finds inconsistency as two nodes having same transmission count values. This shows that Z is an attacker and discards it.

1.6. Routing Misconduct

Routing misconduct deals with the concept where malicious nodes tend to drops packets which are received. It is caused by attackers to minimize packet delivery ratio and wastage of resources. So this has to be prevented to maintain the network. The general idea is, when two nodes are contacted they should generate a relation record, which consists of when contact has been made, which packets are available in their buffer before exchange of data and what packets need to be sent, unique ID. Then the record must include a sign for assuring verified. So the node has to carry its relation record and report it to the next contacted node. So by this scheme the dropped packets are detected.

In the **Fig. 4** node N1 contacts with Node N2, the relation record M is generated. Node N1 sends packet m2 to node N2. Then if suppose N2 drops packet m2 from its node and contacts N3. Node N3 analyses relation record and finds that packet m2 is dropped. This shows that the node N2 is malicious and attackers have caused to drop the packets. However, the attackers might induce false record that the packet has not been dropped by induction N1 report to the node N3. So that its disables the technique to detect the malicious node. But since the record includes information such as unique ID, it easily distinguishes between true and false records. Therefore the record claims the same ID twice, which detects the latter as the malicious node.

Algorithm

P-claim includes the contents S, CP, T, H (M), L where S → source node, CP → packet count, T → current time, M → packet; L → rate limit S increases CP by 1, after sending m out. P claim is attached to packet ‘M’ as header field. If P claim is larger than “L”, then it discards the packet.

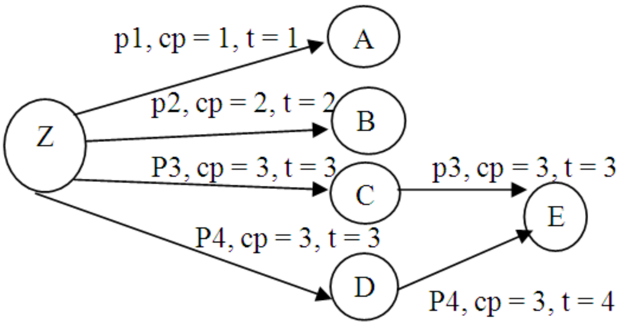

Fig. 2. Packet flood detection

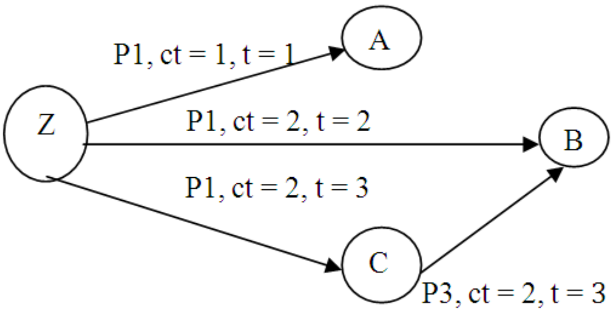

Fig. 3. Replica flood detection

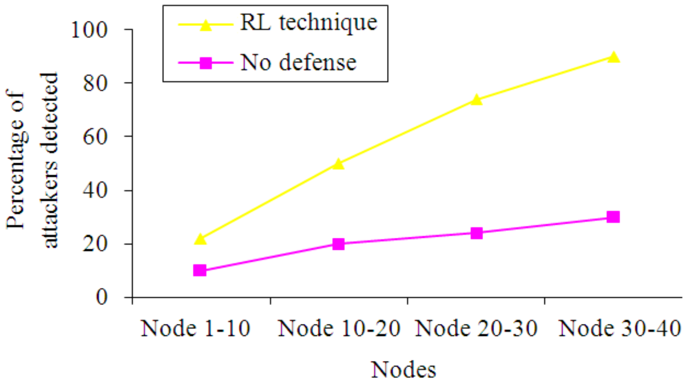

Fig. 4. Detection analysis

T-claim includes header contents such as A, B, H (M), CT, T where A→ node A, B→ node B, M→ packet, CT→ transmission count and R→ rate limit T claim is attached to packet ‘M’. Node B checks if CT is in its limit ‘R’, by assuming A as source node. If it is valid store this new T claim.

1. Metadata (T-claim and P-claim) for attack detection
2. If packets to send then,
For each new packet, generate P claim for all packets, generate T claim.
3. Every packet with P claim and T claim attached.
4. If receive a packet then If verification of count value results in failure then Discard the packet
5. Check P claim and T claim for inconsistency, if detected inconsistent. Then term the signer of claim as attacker
6. Update an alarm to the network.

```
Else
End if
```

1.7. Analysis

Consider an attacker Z floods inconsistent packets to node A and B. In order to confuse the detector, the attacker floods consistent packets to both the nodes. But the inconsistent packet will make a dishonest claim, which will make to detect the attacker as well as the packet. It is also liable to quota based routing protocols. Quota based protocol specifies the number of duplicates a packet can be generated by allotting a quota. Whenever the duplicates or replicas are created, the quota of a packet is reduced by 1. Therefore if an attacker sends out more duplicates than the quota then it is detected as an attacker. Communication cost involves P-claim and T-claim transmitted with each packet and also redirected claims. Computation cost involves signature generation. Each node generates signature for each packet and also the signature is verified. Storage cost is low, as mostly the P claim and T claim are compacted when the packets are forwarded.

In the analysis, it is shown there is a difference in the percentage of detection when compared with RL technique. Select ten packets to be sent to each node junction, one junction consists of 10 nodes, when it is analyzed based on RL technique, it is proven that the percentage of attackers are detected as more and more flooded packets are injected. There is a significant increase in detection as the packets are increased.

2. CONCLUSION

In this study, we enable techniques to defend and detect against flood attacks in disruption tolerant networks. Rate limiter technique allows defending against attacks by blocking attacker from injecting flooded packets. Claim construction method used to detect both flood and duplicate attacks by inconsistency claims made by the attacker. Also the application layer attacks are detected and nodes which drop packets are detected. This scheme is cost effective and provides security for precious network such as disruption tolerant network.

3. REFERENCES

Raghavan, B., K. Vishwanath, S. Ramabhadran, K. Yocum and A. Snoeren, 2007. Cloud control with distributed rate limiting. Proceedings of the 2007 Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, ACM, New York, pp: 337-348. DOI: 10.1145/1282380.1282419

Burgess, J., B. Gallagher, D. Jensen and B. Levine, 2006. Maxprop: Routing for vehicle-based disruption-tolerant networks. Proceedings of the 25th IEEE International Conference on Computer Communications, Apr. 23-29, IEEE Xplore Press, Barcelona, Spain, pp: 1-11. DOI: 10.1109/INFOCOM.2006.228

Fall, K., 2003. A delay-tolerant network architecture for challenged internets. Proceedings of the Conference on Applications Technologies, Architectures and Protocols for Computer Communications, Aug. 25-29, ACM, New York, pp: 27-34. DOI: 10.1145/863955.863960

Li, F., A. Srinivasan and J. Wu, 2009. Thwarting blackhole attacks in distruption-tolerant networks using encounter tickets. Proceedings of the IEEE INFOCOM, Apr.19-25, IEEE Xplore Press, Rio de Janeiro, pp: 2428-2436. DOI: 10.1109/INFCOM.2009.5062170

Li, Q. and G. Cao, 2012. Mitigating Routing misbehavior in disruption tolerant networks. IEEE Trans. Inf. Forens. Security, 7: 664-675. DOI: 10.1109/TIFS.2011.2173195

Parno, B., A. Perrig and V. Gligor, 2005. Distributed detection of node replication attacks in sensor networks. Proceedings of the IEEE Symposium on Security and Privacy, May, 8-11, IEEE Xplore Press, pp: 49-63. DOI: 10.1109/SP.2005.8.1353