International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-3 Issue-5, October 2013

Correlated Low Rate DDoS Attack on Router Queues

Pavithra .J, Arnika Tripathi

Abstract: ***Network security is the booming issue inspite of tremendous advancements in the security aspects. Among the available network issues, attacks performed to breach the security against a particular host is also a major concern. In regard to this we preferred to study and perform DDoS attack in a coordinated manner that utilizes Botnet technology which attempts to show that it becomes difficult to identify the attacker by using this method. As a result by this it becomes a challenge to the existing attacker to invent an even more devasticated attack type to perform attack. In this method we propose to perform UDP-type attack. The introduced correlated DDoS attacks are more powerful than simple DDoS attacks which involves the combined effort of several machines in attacking a target system, in which an attacker generates highly correlated attack bursts from different sources towards a target router. The main idea behind it is to exploit the correlation among multiple groups of zombies scattered across different locations and have them aggregated to generate attack burst traffic at the target router. For this we use packet level simulations that demonstrate the UDP attack in a simulator test bed.***

Key words: DoS, DDoS, correlated DDoS, UDP

I. INTRODUCTION

DoS (Denial-of-Service): denial-of-service attack means making the legitimate users not being made available with the computer resources that are provided by particular host by either injecting a computer virus or congesting the network with attack intended traffic.

A Denial of Service (DoS) attack aims to stop the service provided by a target. It can be launched in two forms. The first form is to exploit software vulnerabilities of a target by sending malformed packets and crash the system. The second form is to flood massive volumes of useless traffic towards target. All DDoS attacks start by breaking into hundreds or thousands of machines (handlers) over the Internet. Then, the attacker installs DDoS software on the machines, allowing them to control all the attacked machines (zombies or agents) to launch coordinated attacks. The practicality of the correlation attack is further justified with the emergence of Botnets [1]. In a Botnet, an attacker (called Botmaster) controls a group of compromised hosts called bots. The Botmaster can send a command to the bots and schedule them to send attack bursts to a target router in a correlated manner. Correlation attack [2] means attacker intentionally introducing traffic burstiness at the target router which is exhibited in a highly correlated manner and is low rate in nature.

Manuscript published on 30 October 2013.
*Correspondence Author(s)
Pavithra .J, Computer science, Dayananda Sagar College, Bangalore-560037, India.
Arnika Tripathi, Systems Analysis and Computer Applications, NITK Suratkal, Mangalore-575025, India.

The main idea is to correlate the attacks emerged from different locations, from all the attack flows in different locations produces a small traffic burst wherein finally all these bursts are aggregated to produce a large burst of traffic that increases the router queue length and also end-to-end transfer delays. Unlike the flooding-based denial-of-service attacks that generate an overwhelming amount of attack traffic, the correlation attack is low-rate by nature due to which identifying an attacker becomes difficult.

The proposed method contain a detailed analysis of a variant of low-rate attack called correlation attack, wherein instead of single attack, the attacker generates the attack traffic, multiple attackers collectively generates the flood to create the same situation as in the case of normal DDoS attacks. Two types of protocols considered to perform attacks are:

TCP (Transmission control protocol)

The TCP provides full transport-layer services to applications.TCP is a reliable stream transport protocol. The term stream, in this context, means connection-oriented: A connection must be established between both ends of a transmission before either can transmit data.

At the sending end of each transmission, TCP divides a stream of data into smaller units called segments. Each segment includes a sequence number for reordering after receipt, together with an acknowledgement number for the segments receiving end, TCP collects each datagram as it comes in and reorders the transmission based on sequence numbers.

UDP (user datagram protocol)

UDP is another transport protocol in the TCP/IP protocol suite. UDP provides an unreliable datagram service. It is process-to-process protocol that adds only port addresses, checksum error control, and length information to the data from the upper layer.

A. Problem Formulation

The system architecture of discussed method consists of three important components: Sender node, Router, Receiver node. The connection between the components of the system architecture is shown in fig 1

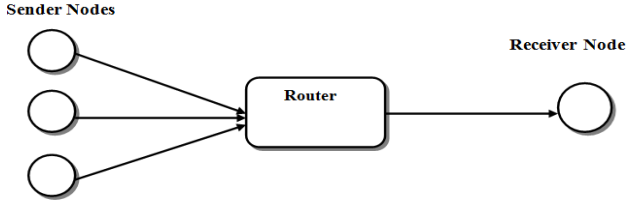

Fig 1: System architechture

They are the source of information and are sending packets to the destination node through intermediate nodes.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

In Fig:1 Node module takes input from the user. Router is a module which performs the buffering of the packets once the router queue is filled it starts dropping them, queueing system used is first in first out (FIFO) at the router.The sink node acts as a receiver or destination. The function of wired network is to provide connection among these different modules. Receiver node is the destination node to which the sender wishes to send packets to.

Algorithm to perform low rate correlated UDP attack:

Step 1: consider $S_1...S_i$ are senders, $R_1.R_j$ are receivers and $Rt_1 \ldots Rt_k$ are routers.

Step 2: If senders are Attackers represented as $A_1 \ldots A_n$ Distribute Time (T) among $A_1 \ldots A_n$ as t_1, $t_2 \ldots t_m$ then flood packets (P_k) in correlated manner to router R_t.

// Here, A_n represents the number of attackers. According to the delay, each attacker can be controlled to launch attack flow at appointed time.

Step 3: Let A_1 send datagrams at time $t_1$and stop.
Let A_2 send datagrams at time t_2 and stop.
Continue the same for all A_n.

Step 4: The distributed time is estimated by Eqn (1)
$T = t_1+t_2+t_3 \ldots +t_m$ ……..(1)

Step 5: set Router (R_{t1}) queue size to be "Q".
Estimate 'Q' using:

$Q=P_{arrivals}-P_{departures}-P_{drops}$ …….....(2)

Where, $P_{arrivals}$ = No of packes arrived at router.
$P_{departures}$ = No. of packets left the router.
P_{drops} = No. of packets dropped due to overflow.

Step 6: If (queue size > Q)
Reject the further incoming packets.
Else
Forward the dagrams to receiver or destination.

UDP attack is performed based on above algorithm. Here $S_1 \ldots S_i$ represents normal senders among which few are attackers indicated by A1….A_n in this method, $R_1 \ldots R_j$ represents receivers or destination and R_t denotes Router.When a particular sender is an attacker, he floods the ack packets in a stipulated time t_1 and stops, next few seconds is kept idle i.e., no packet flow takes place by any of the attacker, next turn is taken up by A_2 at time t_2, and so on. In this method the duration of each flood is limited to 2ms and 4ms is an idle period. In this way the entire attack sequence is been distributed among each attacker and flooding is performed in a correlated manner.

Now the total time taken for DDoS attack in a correlated manner is given by summing all time taken by each attacker i.e., according to eqn (1). Further the router capacity is fixed here and the buffer filling is estimated by eqn (2). When a router buffer size exceeds its threshold value, overflow occurs.

Simulation Topology for UDP flood attack:

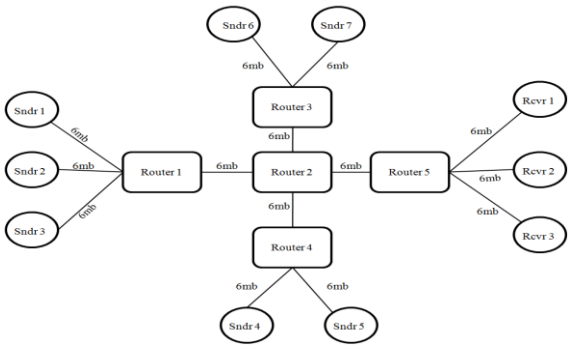

Fig 2: Simulation Topology

The simulation topology used is shown in Fig. 2; in this topology wired network with 15 nodes are considered. All nodes are connected to each other by duplex link with bandwidth 6mb and delay 1ms.We use FCFS (drop tail) queue mechanism with queue size 40 between all nodes. The target node is Router 1 for performing UDP attack. Sndr1, sndr2 and sndr3 are sender nodes and rcvr1, rcvr2 and rcvr3 forms the receiver nodes. The details of other simulation parameters are listed in the following table.

Table: 1 Simulation parameters

channel	channel/Wired
Network Interface	Wired
NS Version	ns-2.35
CBR and FTP Packet Size	12bytes
interface Queue	drop Tail
Queue Length	40
No. of Nodes	15
simulation Area Size	800*600
simulation Duration	10.25
Packet Rate	2mbps

B. Simulation Results

In the above topology node 0, 1, 2 are senders considered for performing attack and node 3 is the router which forms the victim of UDP attack, nodes 12, 13 & 14 are the receivers. The packet drops against communication between node 0 and 12, 1 to 13, 2 to 14 are identified with different colors during simulation and their respective graphs are shown in the following figures, Fig. 3, Fig. 4, Fig. 5. When all the three packet flow are combined they form the correlated attack on the router node, shown in Fig. 6.

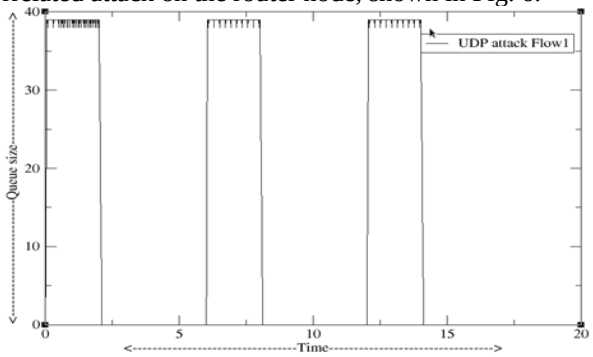

Fig 3: UDP attach flow 1

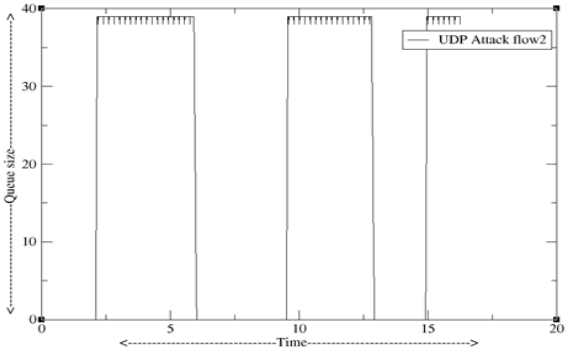

Fig 4: UDP attach flow 2

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

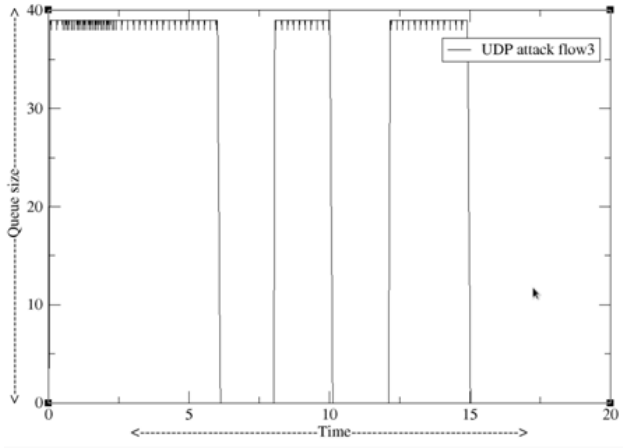

Fig 5: UDP attach flow 3

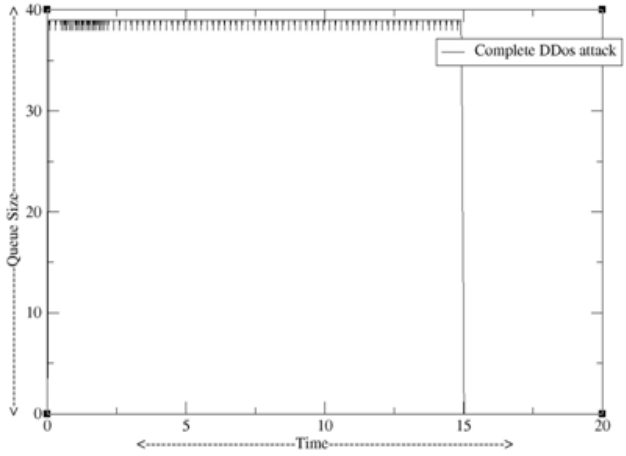

Fig 6: correlated attach flow

II. CONCLUSION

This project work discusses the effect of correlated DDOS attack on router by using UDP-type attack. By using UDP based attack method it becomes difficult to identify the actual attacker since the attack time is distributed and correlated. Therefore this method can be applied in order to overcome the attack if attack performed in real time.

III. ACKNOWLEDGEMENTS

This work was supported by CSIR-Fourth Paradigm Institute (4PI). Any opinions, findings, conclusions and/ recommendations in this paper either expressed or implied, are those of the authors.

REFERENCES

1. "Amit Kumar Tyagi, G.Aghila "A Wide Scale Survey on Botnet", International Journal of Computer Applications (0975 – 8887) Vol 34– No.9, November 2011.
2. Yan Cai , Patrick P.C. Lee b,, Weibo Gong , Don Towsley "Analysis of traffic correlation attacks on router queues", journal at Science Direct Computer Networks 55 (2011).
3. Aleksandar Kuzmanovic and Edward W. Knightly, Senior Member, IEEE "Low-Rate TCP-Targeted Denial of Service Attacks and Counter Strategies", IEEE/ACM transactions on networking, vol. 14, no. 4, august 2006.
4. "On Remote Exploitation of TCP Sender for Low-Rate Flooding Denial-of-Service Attack" V. Anil Kumar, P. S. Jayalekshmy, G. K. Patra, and R. P. Thangavelu , IEEE Communication Letters, Vol. 13,No.1, January 2009
5. Avi Kak "TCP/IP Vulnerabilities: IP Spoofing and Denial-of-Service Attacks", Lecture Notes on "Computer and Network Security" April 30, 2013.

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)