ISSN:0975-9646
A.Chitkala et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4) , 2011, 1720-1724

Flow Control Packet Marking Scheme: to identify the sources of Distributed Denial of Service Attacks

A.Chitkala , K.S. Vijaya Lakshmi
VRSE College,India.

***ABSTRACT*-Flow Control Packet Marking Scheme is a tracing technique, to identify the sources of Distributed Denial of Service (DDOS) attacks. DDOS attacks reduce the quality of the system. While a number of other tracing techniques exist, Flow Control Packet Marking Scheme can obtain better tracing capability than the others. FCPM marks the packets based on the flow at the router. FCPM also adaptively adjusts its marking rate based on the load of a router. Based on the marking, it identifies the source address. The motivation of Flow Control Packet Marking Scheme is to identify the source address of the DDOS attack traffic. It can also show the difference between normal and abnormal state of the network.**

INTRODUCTION

Nowadays internet crime has become a common phenomenon with wide usage of automated attack tools. Distributed Denial of Service is an attempt to make resources unavailable to its users. It is very difficult to find the sources of attacks, since the attacker can forge the source address field. Although many counter measures have been proposed against internet crime, they cannot identify where the DDOS attacking packets come from, where malicious email is originated and where suspect intruder is located.

DDOS attacks reduce the quality of the system. DDOS attacks use multiple attack sources to attack the single system. At any point, within the network, if there is a sudden surge in the number of packets, it was the sign of DDOS attack. Although many tracing techniques have been existed, they cannot prevent the router from overload problems.

CURRENT TRACING TECHNIQUES AND THIER DRAWBACKS

Current tracing techniques can be classified into three categories. They are:

1. Link Testing
2. Logging Schemes
3. Probabilistic Packet Marking Scheme

Link Testing

The main idea of link testing is to start from victim to upstream links to identify the source of the attack. It is easy to implement. The disadvantage of link testing is it does not consider the overload problem of the router.

Logging Scheme

Logging Schemes maintains a database at each router to store the packet's information. It identifies the source address by querying the database. The disadvantage of logging scheme is, the router is heavily loaded by maintaining log information of each packet.

Packet Marking Schemes

Packet Marking Schemes marks the packet, based on the marking fields, they identify the source address. Probabilistic packet marking scheme marks the packet based on the path information in a probabilistic manner. Based on the marking, it identifies the real sources of attacks. It assumes that the attack graph is same as constructed graph.

The disadvantages of Probabilistic Packet Marking Scheme are:

- It cannot find out the packet travel path.
- Duplication of packets arrives at the receiver.
- It is not useful when the number of sources needed to be traced increases.
- It cannot prevent the router from overload problems.

The possibility of the overload problem always exists because the resources of a router are always limited. If the router is overloaded, the marking scheme can be totally ineffective. Al l packet marking schemes consume the computing power and storage capacity of routers. Therefore, overload prevention is important to all packet marking schemes.

Proposed System

The newly proposed system, Flow Control Packet Marking Scheme marks the packet based on the flow at the router. FCPM marks the packet based on the Flow Control marking algorithm. FCPM marks the packet in a deterministic manner. It can identify the source of DDOS attack based on the marking and with the help of trace file. It also considers the QOS parameters such as bandwidth and delay.

Ns2 was used to implement FCPM scheme.

NS2 OVERVIEW

NS2 is an open source network simulation tool. It is discrete event driven simulator. The primary use of NS2 is in network researches to simulate various types of wired/wireless local and wide area networks; to implement network protocols such as TCP and UDP, traffic source behavior such as FTP, Telnet, Web, CBR and VBR, router queue management mechanism such as Drop Tail, RED and CBQ, routing algorithms such as Dijkstra, and many more.

TCL script describes the network topology that consists of nodes, links, protocols and applications. Before the topology can be setup, a simulation object is created with the command:

set ns [new Simulator]

This simulator object has a member function that enable creating nodes, links connecting agents etc.

ELEMENTS OF NETWORK SIMULATION

1. NODE

Node is a collection of agents and classifiers. Nodes have unique address. Nodes in the network may be either

intermediate or an end system. If the node is not a router but end system, the traffic sources and applications such as CBR, FTP, etc. must be added to the traffic agents such as TCP, UDP etc. These traffic agents must be added to nodes for packet transmission.

2. AGENTS

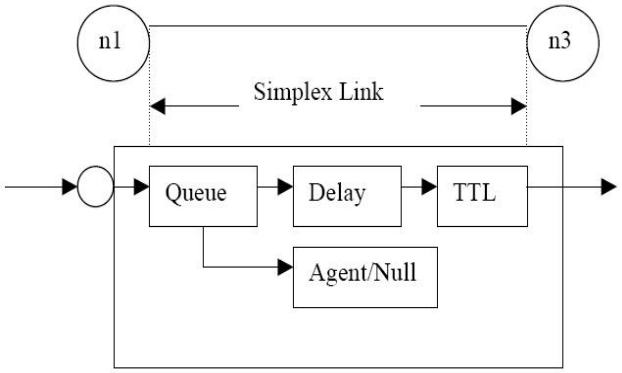
Agents are end points of logical connection .They are used create and receive packets. The most common agents used in NS2 are TCP and UDP.The most common agent types provided by NS2 are:

1. Agent/TCP – a Tahoe TCP sender
2. Agent/TCP/Reno – a Reno TCP sender
3. Agent/TCP/Sack1 – TCP with selective acknowledgement

The most common applications and traffic sources provided by ns2 are FTP and CBR.

3. LINKS

Links are used to connect two nodes. Links keeps track of "from" to "to" of a node object. Links may be either simplex or duplex links. Simplex links are used for unidirectional link between nodes. Duplex links are used to make bidirectional link between two nodes. If a duplex link is used two simplex are created one for each direction.



4. QUEUE

Queues are parts of links. These are used to store and to drop the packets if necessary. In the link, packet is first enqueued at the queue. After this packet is either dropped, or passed to the null agent and freed there or dequeued and passed to the delay object to simulate the link delay.

Links can be created with the following command:

$ns duplex/simplex-link endpoint1 endpoint2 bandwidth delay queue-type

Queue type may either Drop tail (FIFO), Random Early Detection (RED) or CBQ. If the FIFO queue is full then the packet which comes first should leave the queue at first. Random Early Detection marks the packet based on the weight of the queue.

The values for bandwidth can be given as a pure number or by using qualifiers k (kilo), M (mega), b (bit) and B (byte). The delay can also be expressed in the same manner, by using m (milli) and u (micro) as qualifiers.

There are several queue management algorithms implemented in ns2, but in this exercise only Drop Tail and RED will be needed.

TRACE SUPPORT

There are two types of outputs.

1. Namtrace **2**. Trace

1**. Namtrace:**

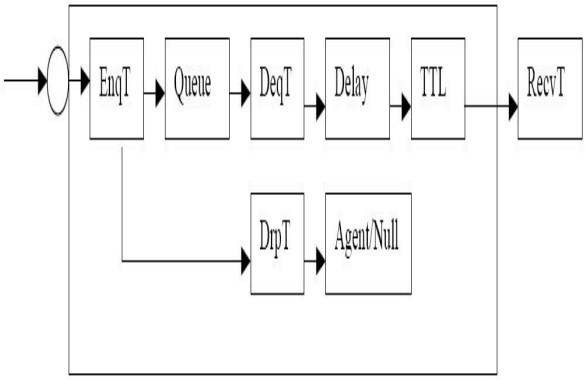
Nam is a graphical user interface for replaying simulation. Namtrace is only useful for nam. Editor generates simulation scripts.

2. Traces

All events from the simulation can be recorded to a file with the following commands:

set trace_all [open out.nam w]
$ns file name $trace_all
$ns flush-trace
close $file name

First, the output file is opened and a handle is attached to it. Then the events are recorded to the file specified by the handle. Finally, at the end of the simulation the trace buffer has to be flushed and the file has to be closed. This is usually done with a separate finish procedure.



Trace file describes the type of event whether packet is enqueued, dequeued, received or dropped and time of the simulation, packet type, packet ID, Flow Id, source and destination address of a packet.

Services provided by the Internet Transport protocols (TCP, UDP)

TCP Services

The TCP service includes a connection-oriented service and reliable data transfer service. When an application invokes TCP for its transport protocol, the application receives both of these services from TCP.

Connection-oriented service:

TCP has the client and server exchange transport layer control information with each other before the applicatioin level messages begin to flow. After this, a TCP connection is said to exist between the sockets of two processes. The connection is full duplex connection in that two processes can send messages to each other over the connection at same time. When the applications finished sending messages, it must tear down the connection.

Reliable transport service:

The communicating processes can rely on TCP to deliver all data sent without errors and in the proper delivery. When one side of the application passes a stream of bytes into a socket, it

can count on TCP to deliver the same stream of bytes to the receiving socket with no missing and duplicate bytes.
TCP also includes a congestion control mechanisms. TCP congestion control mechanism throttles a sending process when the network is congested between sender and receiver.

UDP Services

UDP is a light weight transport protocol. UDP is connection less, so there is no handshaking before two processes start to communicate. UDP provides unreliable data transfer service-that is, when a process sends a message into UDP socket, UDP provides no guarantee that the message will ever reach the receiving process.
UDP does not include congestion control mechanisms, so sending process can pump data into a UDP socket at any rate it pleases.
The throttling of the transmission rate can have a very harmful effect on realtime aplications. Moreover, real-time applications are loss tolerant and don't need a fully reliable transport service. For these reasons, developers usually run their applications over UDP rather than TCP.

DESIGN AND IMPLEMENTATION OF FLOW CONTROL PACKET MARKING SCHEME

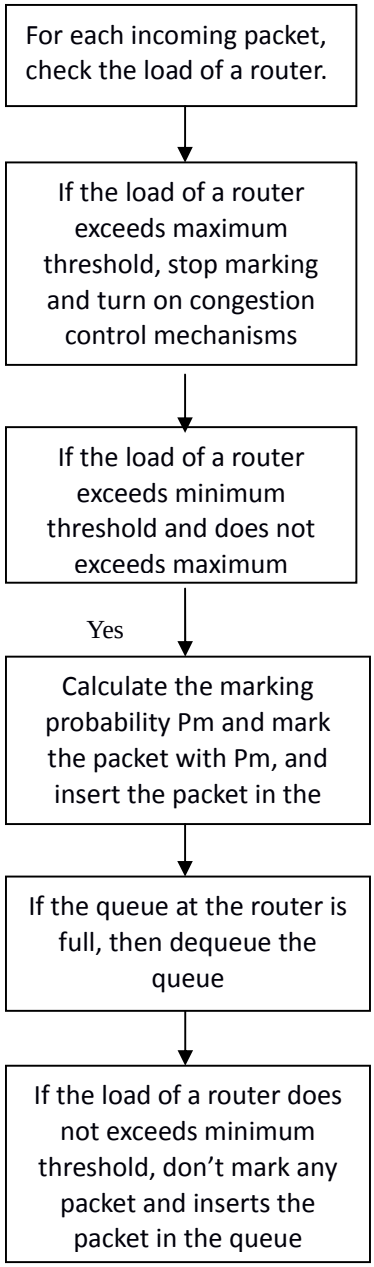
Flow control packet marking scheme marks the packet based on the load of a router. Each router maintains a RED queue. For marking, it uses Flow Control Packet marking algorithm .When a packet enters the network, it is marked by the closest router. FCPM also maintains trace file to trace the packet information such as source address, destination address, packet id, flow id, time, packet type and packetsize in bytes, the packet status and acknowledgement from the TCP sink if any. It uses three colors to mark the packet. Based on the marking field and with the help of trace file it identifies the source address of the packet.

FCPM algorithm

For each incoming packet, FCPM checks the load of a router. If the load of a router is less than minimum threshold do not mark any packet. If the load of a router exceeds the minimum threshold and does not exceeds the maximum threshold, then insert packet in the queue and marks the packet with the marking probability **Pm.** If the load of a router exceeds maximum threshold, it stops marking and turn on congestion control mechanisms (RED) and decide whether packet is dropped/marked.

Pa= Maxp (Q-Minth)/(Maxth – Minth)
Pm= Pa/(1-count) pa

Where Maxp is the maximum probability to drop the packet, which is given as queue parameter.
Minth is the minimum threshold of a router.
Maxth is the maximum threshold of a router.
Q is the average queue size.
The values of Minth and Maxth are given as queue parameters.



System Overview

Flow Control Packet Marking Scheme consists of four modules.

1. **Create Network Topology**

Create network topology with 12 nodes. In this, four nodes are acts as routers (r0,r1,r2,r3),one node acts as server(s0) and the remaining seven nodes acts as clients including attackers(c0,c1,a0,a1,a2,a3,a4). Simulatior object must be created to setup network topology and to trace the flow. Open the trace file for tracing, and define the node varibles, assign labels and colors to nodes.

Establish links between nodes

Duplex-link is used to make connection between two nodes. Duplex link creates two simplex-links for each direction. Establish link between nodes(c0,c1,a0,a1,a2,a3,a4,s0) and routers (r0,r1,r2,r3).Each link consists of fixed bandwidth. Define bandwidth, delay and link type. Drop-tail queue is maintained between nodes and routers to store the packets. Random Early Detection (RED) queue is maintained between the routers to store the packets. Set the RED queue parameters such as minimum threshold, maximum threshold and marking rate and maximum probability to mark the packet.

2. **Establish TCP and UDP Connections between client and server**

Agents are used to create and to transmit packets between nodes. TCP agents are attached to the source nodes (c0,a0,a3,a4)and a connection is established to a tcp "sink" agent attached to the destination node(s0).A TCP agent generates and sends acknowledgement to the sender and frees the received packet. As default, the maximum size of a packet that "tcp" agent can generate is 1KB.UDP agents are attached to source nodes (c1, a1, a2) is connected to a null agent attached to destination (s0).A null agent just frees the packets.

3. Attach Traffic Sources (FTP, CBR) to agents: The Internet protocol used by FTP is TCP/IP and the Internet protocol used by CBR is UDP. Assign FTP to TCP agent and assign CBR agent to UDP to create and receive packets. FTP agents produce bulk data for a TCP object to send. CBR objects generate packets at constant rate. Set the packet size and set the maximum number of packets to transmit between source and destination.

4**. Schedule events**

The simulator object has many scheduling member functions. However, the function $ns at time "string" is mostly used. This function of simulator object makes the scheduler to schedule the execution of specified string at given simulation time.

After all configuration, scheduling and post simulation procedure specifications are done, run the simulation. This is done by $ns run.

EXPLANATION

In general an NS2 script starts with making a Simulator object instance.

Set ns [new Simulator] creates simulation object instance and assign it to variable ns. This simulator object has member functions that are used to create nodes, to establish links between nodes, to set the orientation, to label, to color the nodes and to specify nam display options. Open the trace file and NAM file for write to capture the packet information and to display the nam.

To create node use the member function:

Set node-name [$ns node]

- To assign colors use the member function **$node-name color "color"**

To establish duplex -link between the nodes and routers use the member function.

$ns duplex-link $node1 $node2 bandwidth delay queue-type

To create duplex-link between c0 and r0 with bandwidth 10MB and delay 10ms and with queue-type RED, the member function is as follows

$ns duplex-link $c0 $r0 10MB 10ms RED

- Set the RED queue parameters such as maximum threshold and minimum threshold as 16 and 5 respectively.

To assign labels to nodes use the member function:

$ns at time "node-name label label-name"

To set orientation to links use the member function:

$ns at time duplexlink-op $node1 $node2 orient orientation

orientation is either right, left, down, up, right-down, right-up, right-down, left-up, or left right.

To establish TCP connection and to attach agents to nodes use the member function:

Set tcp [$ns create-connection TCP $source-node TCPSink $destnation-node]

To establish UDP connection use the following member functions.

Set udp [new Agent/UDP]
Set null [new Agent/Null]
$ns attach-agent $source $udp
$ns attach-agent $destination $null
$ns connect $udp $null

- To assign FTP traffic to TCP agent use
  Set ftp [new Application/FTP]
  $ns attach-agent $tcp $ftp
- Set $ftp packetsize- Size of the packet, defines the packet size.
- Schedule the events and run the simulation to start simulation.

CONCLUSION

FCPM trace the packet information, which contains source address of the packet .It prevents the router from overload problem. It also show the result of attacking and difference between normal and abnormal state of the network through network animations.

The network is in normal state before the source starts attack. At normal state, TCP and UDP are fine .At normal state, the number of dropped packets is very low. When the source starts attack, the number of dropped packet increases and after some time the TCP and UDP links fails.

REFERENCES

1.H. Farhat, "Protecting TCP Services From Denial of Service Attacks," in Proceedings of the 2006 ACM SIGCOMM workshop on Large-scale Attack Defense, Pisa, Italy, 2006, pp. 155-160.

2. H. Wang, C. Jin, and K. G. Shin, "Defense Against Spoofed IP Traffic Using Hop-Count Filtering," IEEE/ACM Transactions on Networking, vol. 15, no. 1, pp. 40-53, 2007.

3. M. T. Goodrich, "Efficient Packet Marking for Large-Scale Traceback," in Proceedings of the 9th ACM conference on Computer and Communications Security, 2002, pp. 117-126.

4. A. Belenky, and N. Ansari, "On IP traceback," IEEE Communications, vol. 41, no. 7, pp. 142-153, 2003

5. Z.Gao, and N. Ansari, "Tracing Cyber Attacks from the Practical Perspective," IEEE Communications, vol. 43, no. 5, pp. 123-131, 2005.

6. S. Floyd, and V. Jacobson, "Random Early Detection Gateways for Congestion Avoidance," IEEE/ACM Transactions on Networking, vol. 1, no. 4, pp. 397-413, 1993.
7. P. Gevros, J. Crowcroft, P. Kirstein et al, "Congestion Control Mechanisms and the Best Effort Service Model," IEEE Network, vol. 15, no. 3, pp. 16-26, 2001.8. J. Jung, B. 8. 8. 8.Krishnamurthy, and M.Rabinovich, "Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites," in Proceedings of the International World Wide Web Conference, 2002, pp. 252-262.
9. H. Wang, D. Zhang, and K. G. Shin, "Change-Point Monitoring for the Detection of DOS Attacks," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 4, pp. 193-208, 2004.
10. W.Feller, an Introduction to Probability Theory and Its Applications, New York John Wiley & Sons, 1968.
11. Network simulation http:// www.ns2