

Characteristics of Denial of Service attacks on Internet using AGURI

Ryo Kaizaki¹, Osamu Nakamura², and Jun Murai³

¹ Graduate School of Media and Governance, Keio University,
5322 Endo, Fujisawa, Kanagawa, 252-5322, Japan
kaizaki@sfc.wide.ad.jp
<http://www.sfc.wide.ad.jp/~kaizaki/>

² Faculty of Environmental Information, Keio University,
5322 Endo, Fujisawa, Kanagawa, 252-5322, Japan
osamu@wide.ad.jp

³ Faculty of Environmental Information, Keio University,
5322 Endo, Fujisawa, Kanagawa, 252-5322, Japan
jun@wide.ad.jp

Abstract. Denial of Service attacks are divided into two types, one is logic attack and the another one is flooding attack. Logic attack exploits security hole of the software such as operating system and web server bugs, then causes system crash or degrade in the performance. Logic attack can be defended by upgrading software and/or filtering particular packet sequences.

In this paper, characteristics of the flooding attacks is described. For the monitoring tools, AGURI, that we have developed, is used. Using the traffic pattern aggregation method, AGURI can monitor the flooding attacks in real network traffic for a long term.

1 Introduction

Internet is the packet switching network, sharing the every resources such as the bandwidth of the links and router's processing unit. Resource management should be done by every end node. For example, congestion controls can be done only by end nodes. End nodes can also send data without congestion controls. Thus ,usage of network resources depends on behavior of end nodes. However current Internet does not have any mechanisms to control ill behavior. During the network operations, it is very important to detect the flooding attacks as soon as possible. After detecting the flooding attacks, operators can take several actions : dropping the packets from attackers ,limiting number of packets from attackers, and discovering the attackers .

Denial of Service attacks is divided into two types[1], one is logic attack and the another one is flooding attack. Logic attack exploits security holl of the software such as operating system and web server bugs, then causes system crash or degrade in the performance. Logic attack can be defended by upgrading software and/or filtering particular packet sequences.

Comparing each packets of the flooding attack and the other normal communication traffics, the only difference is the number of the packets. Flooding attack creates enormous amount of packets. Therefore, to protect systems from flooding attacks, the same method for logick attacks can not be used. While operationing networks, operators can detect flooding attacks using traffic monitoring tools such as MRTG[2]. However those tools will not show detail information of flooding attack packets.

2 Traffic monitoring for flooding attacks

There are several types of flooding attacks.

1. the large number of the bytes
2. the large number of the packets
3. packets with ill behavior protocols such as sync attack

The traffic with the large number of the bytes for the single destination degrades the performance of the end system and the routers that switching this traffic. And recent routers incur more damages by recieving the large number of packets rather than bytes.

That traffic can be monitored by using SNMP[3]. MRTG is good graphic interface for the detecting the unusual traffic. But it is not sufficient for detecting the flooding attacks. There is limitation of gathering the information using SNMP. The number of the bytes and the packets for the each interface on the routers can be collected. However the number of the byte and the packets to the single hosts can not be collected. If the bandwidth of the link was occupied in general condition, particular attacks could not be detected by using SNMP/MRTG monitoring, because total bandwidth of the link is not changed.

For detecting the flooding attacks, we should know the normal conditions of the networks. It needs for large number of the traffic data. SNMP is simple mechanisms for collecting the data from the routers and switches. It is needed for aggregation mechanisms for storing the data. NeTraMet and FlowScan which are flow based monitoring tools can monitor specific type of the traffic, such as number of bytes and packets in a long term on HTTP, FTP, IPv6 etc. However these tools require the fixed rule sets. So those tools can not detect unexpected traffic pattern.

2.1 AGURI

AGURI is an aggregation based traffic profiler targeted for long term measuring. AGURI adapts itself to spatial traffic distribution by aggregating small volume flows into its root. AGURI does not need a pre-defined rule set and is capable of detecting an unexpected increase of unknown packet patterns or flooding attacks.[4]

Figure 1 shows the concept of aggregation: small entries are aggregated into its root. There are two phases in the basic aggregation algorithm of AGURI First

AGURI monitors every packets. Second , at the end, aggregates entries whose counter value is less than an aggregation threshold.

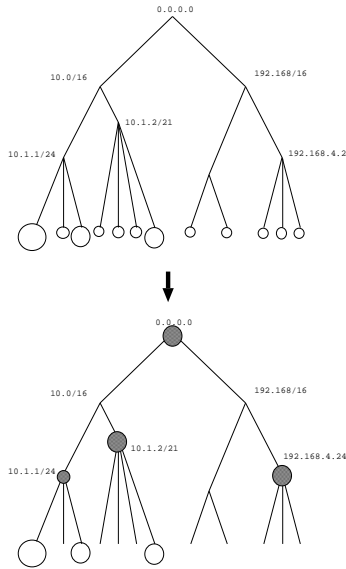


Fig. 1. aggregation concept:small entries are aggregated into aggregates.

In figure 1, each circle shows entries and its counter value is indicated by its size. Each filled dot shows sets of aggregated entries whose counter value is less than an aggregation threshold. For example, the filled dot “10.1.2/21” shows set of aggregated entries whose counter value is less than an aggregation threshold and whose IP address is included in address block “10.1.2/21”.

Figure 2 shows an example of aguri’s summary output. A summary consists of header part and body part.

The header part describes version, start-time of profiling, end-time of profiling and average-rate of all traffic. The header part starts with %.

The body part contains 4 profile types:

1. source ip address
2. destination ip address
3. source protocol
4. destination protocol

In the address profile, each row shows an address entry and the prefix length. The first column shows the address and the prefix length of the entries. The second column shows the cumulative byte counts. The third column shows the percentages of the entry and its subtrees.

The input for this example is a month-long packet trace taken from a transparent link of the WIDE[5] backbone. The parameters of aguri is configured with

```

%%!AGURI-1.0
%%StartTime: Thu Mar 01 00:00:00 2001 (2001/03/01 00:00:00)
%%EndTime: Sun Apr 01 00:00:00 2001 (2001/04/01 00:00:00)
%AvgRate: 14.91Mbps

[src address] 4992392109177 (100.00%)
0.0.0.0/0      87902964189 (1.76%/100.00%)
0.0.0.0/1      206637364377 (4.14%/14.78%)
0.0.0.0/2      205796877844 (4.12%/7.12%)
60.0.0.0/6     97928228974 (1.96%/3.00%)
  62.52.0.0/16  51875058871 (1.04%/1.04%)
  64.0.0.0/8   100831910967 (2.02%/3.51%)
  64.0.0.0/9   74610984109 (1.49%/1.49%)
128.0.0.0/2    142349668983 (2.85%/13.33%)
128.0.0.0/3    197067746696 (3.95%/10.48%)
128.0.0.0/5    202911635757 (4.06%/5.45%)
133.0.0.0/8    69142535628 (1.38%/1.38%)
  150.65.136.91 54123094932 (1.08%)
192.0.0.0/4    212653628837 (4.26%/38.41%)
192.0.0.0/6    88855538654 (1.78%/1.78%)
202.0.0.0/7    235853368912 (4.72%/14.70%)
  202.0.0.0/9    117196493427 (2.35%/6.77%)
    202.12.27.33 160473669718 (3.21%)
    202.30.143.128/25 60239291958 (1.21%/1.21%)
    203.178.143.127 94031811680 (1.88%)
204.0.0.0/6    228960094456 (4.59%/17.68%)
204.0.0.0/8    125458765333 (2.51%/7.58%)
  204.123.7.2   87103414877 (1.74%)
  204.152.184.75 165733431144 (3.32%)
206.0.0.0/7    164036959478 (3.29%/5.51%)
  206.128.0.0/9  53526598302 (1.07%/1.07%)
207.0.0.0/8    57628266965 (1.15%/1.15%)
208.0.0.0/4    282590640975 (5.66%/31.72%)
208.0.0.0/6    116047154301 (2.32%/22.20%)
209.0.0.0/8    140888988219 (2.82%/11.78%)
  209.1.225.217 238192306019 (4.77%)
  209.1.225.218 209160635530 (4.19%)
210.0.0.0/7    154008321340 (3.08%/3.08%)
  216.0.0.0/9    192899750315 (3.86%/3.86%)
%LRU hits: 86.82% (1021/1176)

```

Fig. 2. Example of AGURI summary output

256 nodes and 1% aggregation threshold. Among many src addresses ,only 8 addresses are indentified as individual address.

Using AGURI’s script, we can archive summaries with minimum disk space. This enables long term measurements.

Thus, AGURI achieves long term traffic monitoring and detecting characteristic flows without a pre defined rule set.

We use AGURI to archive characteristic of traffic in a long term.

AGURI uses a traffic profiling technique in which records are maintained in a prefix based tree a compact summary which is produced by erentries.

Figure3 shows tree structure of archiving summaries. In figure3, AGURI generate hourly summary “A” by aggregating minutes summaries “1”-“12”.

We can see various summaries of time scale granularity .

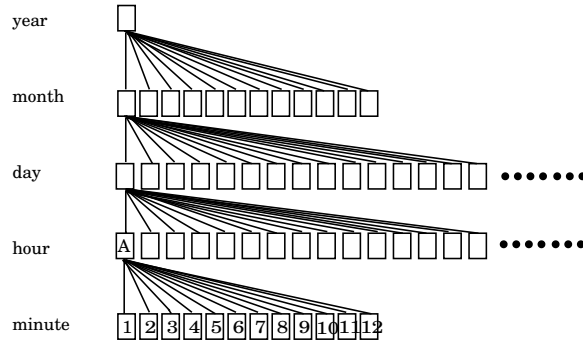


Fig. 3. archiving structure of AGURI

3 Basic methodolgy

To characterise actual flooding attacks , we have to collect traffic information from internet backbone. Thus, we set AGURI on WIDE backbone to monitor flooding attacks for a long term. AGURI should detect an unexpected increase of unknown packet patterns or flooding attacks.

3.1 Information of Experimental platform

We can collect three types of trace data to set three AGURI programs on WIDE backbone. WIDE backbone is formed with giga bit ethernet and fast ethernet.

WIDE Internet has two trans-pacific links. One its own link,the other is directly connected to an ISP which has a trans-pacific link. Figure4 shows information of traffic monitoring points.

Comparing to WIDE internal link and ISP internal links, trans-pacific links are narrow. Thus ,international flooding attacks quickly fullfils those links.

3.2 Information of collected data

Table 1 shows basical information of three data. Data A is made of 4 month long data from July to October. Data B is made of 5 month long data from June to October. Data B is made of 18 month long data from May(2001) June to October.

Table 1. Information of sampling data

| | term | data size (MB) |
|--------|----------|----------------|
| Data A | 4 month | 1340 |
| Data B | 5 month | 720 |
| Data C | 18 month | 5012 |

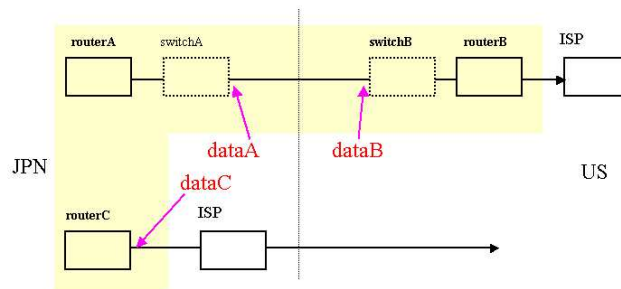


Fig. 4. Traffic monitoring points: three points on WIDE backbone. all of sampling points connected to trans-pacific link between Japan and USA.

Each data size shows size of archiving AGURI data.
 Each data consists of 2-minutes-long data .

4 Result

Using the previously described three types of data (section 3), we observed many flooding attacks.

In this section, we first define flooding attacks, and then characterize the attacks according to both type of attacks and the type of victims.

4.1 Definition of flooding attacks

We can not detect all flooding packet because of AGURI's aggregation concept, however we can detect flooding attacks with the large number of bytes for a long term.[6]

In this paper, we define flooding attacks as following requirements.

- Total number of all traffic increase over 20% compare with average of monthly traffic Bandwidth of trans-pacific links of WIDE backbone has margin in average, thus when remarkable flooding attacks come, there is an increase in total traffic.
 - Attacks continue for over 10minutes
- In this experiment, we set 2-minutes-long as a time-series threshold. So we can not monitor flooding attack for a short term.

- A single characteristic of flow occupy over 70% in all traffic
 AGURI can profile 4types; 1)source IP address 2)destination IP address
 3)source port and protocol and 4)destination port and protocol.
 We define single characteristic of flow in any profile which occupy over 70%
 in all traffic profile as flooding attack.

4.2 Summary of flooding attacks

Table 2 shows flooding attacks we detected based on data July 2002.

Table 2. Summary of flooding attacks on July 2002

| | Data A | Data B | Data C |
|--|--------|--------|--------|
| Number of days in case of flooding attacks | 12 | 12 | 9 |
| Number of flooding attacks | 28 | 28 | 43 |
| Maximum usage of bandwidth | 97Mbps | 97Mbps | 14Mbps |

Maximam usage of bandwidth are nearly equal to Maxmam width of link ,
 Thus flooding attacks occupied almost all bandwidth of links.

All flooding attacks which we can detect spoofed their source IP address, we
 have trouble to trace attacker.

4.3 Destination IP addresses

We can find outstanding characteristics of flooding attacks from profiles of destination IP addresses. We can divide victims of flooding attacks into two types, one is IRC(Internet Relay Chat) servers and the other is Router’s interface. Table 3 shows breakdown of vistims.

Table 3. Breakdown of victims

| | IRC servers | Router's interface | other |
|------------------------------------|-------------|--------------------|-------|
| Destionation IP addresses(victims) | 87% | 12% | 1% |

IRC server and Router’s interface have each characteristic.

- IRC servers
 Almost destination IP address of flooding attack packets are IRC servers. WIDE Internet contains three IRC servers ,all of IRC servers were attacked. IRC servers keep communication sessions each other and share same name space of comunity and user name, thus user can not use same user name

,same community name and right of control community. However once servers can not connect each other ,name space and community is independent. So anyone can gain any user name and community name.

An attacker attacks IRC servers to gain user name and community name which they want. Thus flooding attacks toward IRC servers continue to disconnect IRC servers each other.

– Router’s interface

The other of victims are Router’s interface which user can see their IP address using traceroute et. Thus once network operator sets filter against packet whose destination IP address is Router’s interface, an attacker changes destination IP address to next hop of Router’s interface.

4.4 Destination ports and protocols

We can outstanding characteristic of flooding attacks in poing of destination ports and protocols. We can divide victims of flooding attacks into two types , one is ICMP and on the other hand is TCP.

Almost flooding packets are ICMP echo-reply or TCP SYN floodig, however we found outstanding characteristics of flooding attack in figure5.

```

%!AGURI-1.0
%%StartTime: Sun Oct 14 14:00:00 2001 (2001/10/14 14:00:00)
%%EndTime: Sun Oct 14 15:00:00 2001 (2001/10/14 15:00:00)
%AvgRate: 24.30Mbps[ip:proto:dstport] 10933438650 (100.00%)
4:6:2 220337940 (2.02%)
4:6:5 220259760 (2.01%)
4:6:8 224630700 (2.05%)
4:6:11 220901820 (2.02%)
4:6:14 220496040 (2.02%)
4:6:17 219956580 (2.01%)
4:6:20 221177488 (2.02%)
4:6:23 221431646 (2.03%)
4:6:26 219968880 (2.01%)
4:6:29 219885240 (2.01%)
4:6:32 226155786 (2.07%)
4:6:35 220104840 (2.01%)
4:6:38 220877880 (2.02%)
4:6:41 220083780 (2.01%)
:
:
:
4:6:101 220132020 (2.01%)
4:6:104 229349040 (2.10%)
4:6:107 220964460 (2.02%)
4:6:110 221768098 (2.03%)
4:6:119 213498789 (1.95%)

```

Fig. 5. Example of TCP flooding attacks

In figure 5, "4:6:2" shows IPversion 4 : protocol number 6(TCP) : port number 2. Figure 5 shows that flooding attack packets uses port number which increase per three times.

4.5 Distributed attack

We can see distributed attacks in figure 6 and figure 7.

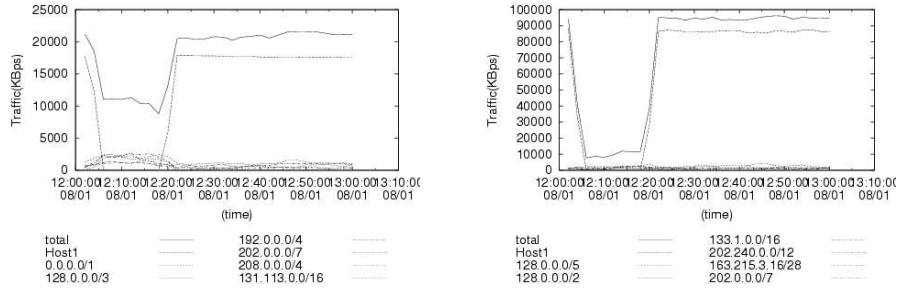


Fig. 6. Data C : flooding attack to Host1 **Fig. 7.** Data A : flooding attack to Host1

Figure 6 shows data C and figure 7 shows data A. Both point C and A are connected to different networks. However, both figures show same flooding attack. They show flooding attacks toward Host 1 in a same time period, and attacks stopped at the same time.

Thus, we can see distributed flooding attacks in these figures.

5 Conclusion

In this paper, characteristics of the flooding attacks are described. Attackers can exhaust network resources using any source ip address, any port number and any protocols.

Thus, to operate networks against flooding attacks, we need to monitor characteristics of flooding attacks: source ip address, destination ip address, port number and protocols.

For the monitoring tools, AGURI, that we have developed, is used. Using the traffic pattern aggregation method, AGURI can monitor the flooding attacks in real network traffic for a long term.

We classify flooding attacks that we define into 4 profiles; 1) source IP address 2) destination IP address 3) source port and protocol 4) destination port and protocol.

We can find characteristic of flooding attacks on destination ip address and destination port and protocol.

AGURI can monitor distributed flooding attacks, port scan attacks. Also, AGURI successfully detected flooding attacks which are remarkably one-sided to specific hosts.

References

1. R.Needham,"Denial of Service: An Example",Communications of the ACM volume 37,November 1994
2. MRTG:www,http://www.mrtg.org
3. SNMP:www,http://www.ietf.org/rfc/rfc1157
4. Kenjiro Cho, Ryo Kaizaki, Akira Kato,"AGURI: An Aggregation-Based Traffic Profiler",QofIS2001,September 2001
5. WIDEproject:www,http://www.wide.ad.jp
6. Ryo Kaizaki, Kenjiro Cho,Osamu Nakamura,"Detection of Denial of Service attacks using AGURI",ICT2002,June 2002