DDoS Attacks Traffic and Flash Crowds Traffic Simulation with a Hardware Test Center Platform

Jie Wang, Raphael C.-W. Phan, John N. Whitley and David J. Parish
High Speed Networks Research Group
Department of Electronic and Electrical Engineering
Loughborough University, UK
{J.Wang3, R.Phan, J.N.Whitley, D.J.Parish}@lboro.ac.uk

Abstract

DDoS attacks are one of the top security problems affecting networks and disrupting services to legitimate users. The first vital step in dealing with this problem is the network's ability to detect such attacks. To that end, it is important that an intrusion detection mechanism be able to differentiate between real DDoS traffic and Flash Crowds traffic, the latter of which constitutes sudden bursts of legitimate network activity. To train and analyze detection mechanisms, researchers typically simulate the DDoS traffic in the testbed; while for Flash Crowds, most researchers replay the web server captures obtained from third parties. This paper proposes the design of a special testbed-based simulation method with Spirent Test Center hardware platform, to simulate both DDoS traffic and Flash Crowds traffic. We give empirical results, including the simulation of four kinds of DDoS traffic including UDP Flooding attack, ICMP Flooding attack, TCP SYN Flooding attack and App-DDoS attack.

1. Introduction

DDoS attacks are devastating to computer networks as they threaten legitimate network usage and cause substantial damage. From the technical view, such attacks consume the network bandwidth and the host resources denying legitimate users' requests and usages. In 2009, the DDoS attack handicapped China's Internet surfing and caused a five-province traffic jam. Additionally, these attacks compromise thousands of victims, irrespective of whether it is the primary victim or the secondary victim. Recent research estimates that the number of the compromised secondary victims, which are popularly known as "bots", can be as large as 60,000 machines for a DDoS attack [15]. From the business view, DDoS attacks cause tremendous economic and business loss, both directly and indirectly.

The DDoS attack is not only harmful, but also hard to detect in an instantaneous manner compared with other network attacks, i.e. SQL injection attacks, XSS, CSRF, etc. Generally, the detection model is difficult to be build up due to increasingly sophisticated attack methods and increasingly complicated attack behaviors [18]. In addition, it is a challenge to distinguish the DDoS attack traffic from *Flash Crowd* (FC) traffic [4, 7, 14] in a short time, since the DDoS attack traffic tends to appear "legitimate". *The FC traffic is a large surge of traffic to a particular Web site causing a dramatic increase in server load and putting severe strain on the network links leading to the server, which results in considerable increase in packet loss and congestion* [4]. Thus two scenarios must be considered in the DDoS attacks detection procedure: DDoS attack traffic versus stable background traffic; and DDoS attack traffic versus FCs traffic [20].

The significant negative impact gives the network security researcher a huge motivation to examine DDoS attacks traffic and FCs traffic. One of the most important steps is to implement traffic simulation on either virtual simulation software or testbed. The main reason for traffic simulation is because quantitative traffic data is seldom obtainable from real network environment, especially the DDoS attack traffic [8]. Firstly, it is hard to predict when and where DDoS and FCs happen in the computer network. Secondly, it is illegal to implement DDoS attacks on the public network. Furthermore, it is difficult to simulate FCs by organising very large number of legitimate clients visiting one particular Web server simultaneously. Therefore, we introduce a design for the DDoS attacks and FCs simulation by using a special hardware testbed platform, which is the industry-level traffic packet generation equipment, namely, *Spirent Test Center platform*. To the best of our knowledge, this is the first work describing DDoS attacks and FCs simulation by using the Spirent Test Center platform.

The remainder of this paper is organized as follows. Section 2 describes other traffic simulation methods as the related work. Section 3 describes the simulation traffic design including network topology

978-0-9564263-7/6/$25.00©2011 IEEE

and traffic classification. Section 4 and Section 5 present the simulation system and corresponding traffic generation process. Section 6 discusses the related strengths and limitations of this simulation method and the traffic capture usage. Finally, we draw some conclusions in Section 7.

2. Related Work

There are two main simulation methodologies: software based simulation and testbed based simulation.

NS-2 is a very popular network simulator software. It had been utilized to achieve many DDoS attacks research targets, including simulating the reflector based DDoS attacks [6], examining the simulation impact from five queueing mechanisms [10], analysing the web server performance under the DDoS attacks [6], detecting the DDoS attacks within the proposed simulation environment [21], among others. Additionally, it had been applied to simulate FCs [19]. However, the significant problem in using NS-2 is that it does not generate real traffic packet without the assistance of third-party simulation applications. Instead, it focuses on dealing with network congestion control and determination of network parameters to suit a certain traffic.

Testbed-based simulation is the most common simulation method. Intel IXP2400 network processor and Intel Workbench SDK 3.5 [9] builds a specialized DDoS attacks traffic simulation testbed. DDoS attacks simulation and FCs simulation had been applied in a 32 traffic sources testbed with same topology to examine the aggregate-based congestion control [12]. Also, FCs had been simulated in different network topologies of LAN, MAN and WAN levels with 30 hosts in testbed [1]. In DDoS attacks simulation, the popular way is to implement the real DDoS attacks tools in testbed in recent years. If both the tool and the network traffic are configured appropriately, the simulation would have many similarities with the real attack traffic. Paper [5] describes eight attack tools and makes the comparisons between each other. However, the tremendous drawback of those real attack tool simulations is that most of the attack tools, e.g., TFN2K [2], had been developed almost ten years ago. The original coding techniques are out of date. In addition, most of current advanced Operation Systems and network devices can identify the generated attack traffic and drop them automatically.

3. Simulation Traffic Design

3.1. Network Topology

Network topology deals with finding the topological structure of the network. DDoS attacks and FCs share similar network topology. The only difference is that all the attack hosts in DDoS attacks are manipulated by the attack master, whereas the hosts in FCs are totally independent. The abstracted network topology for both DDoS attacks and FCs is shown as Figure 1. For DDoS attacks, all of the hosts from Host 1 to Host n represent the bots which are controlled by the bot master and all of the generated attack traffic destined to the primary victim. In contrast for FCs, all of the hosts represent the legitimate hosts in Internet and the generated traffic destined to the targeted Web server. It is clear that there are two boxes in Figure 1, one is the dashed box which represents the topology of DDoS attacks, and another is the solid box which represents the topology of FCs. Both boxes overlap except the part where the attacker as attack master server in the DDoS attacks dashed box.

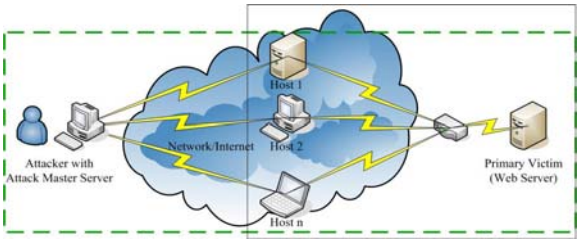


Figure 1. Abstracted Network Topology

3.2. Traffic Classification

The network traffic can be classified into *Background Traffic* and *Attack Traffic*

The background traffic is the normal data stream transmitted between hosts in network. It is an important component in the traffic simulation, especially for the intrusion detection system (IDS)/intrusion prevention system (IPS) research. The detection mechanism can determine the accuracy of detection with the background traffic. In addition, it reflects what is seen in the real network where the detection mechanism is deployed. The legal client traffic [9] is a special group of the background traffic. It is the completed traffic which carries useful application layer information relating to the Web application.

The attack traffic is the generated attack traffic flowing from the attack traffic source to the victim.

3.3. Simulated Traffic

Both DDoS attack traffic and FC traffic share two common features. The first feature is that they only have one target and all of the packets are destined to it. The second one is that a huge amount of traffic is sent to the destination persistently enough to congest the link and host.

3.3.1. DDoS Attacks Traffic. We consider four classes of DDoS attacks: UDP flooding attack, TCP SYN flooding attack, ICMP flooding attack and the application-layer DDoS attack (App-DDoS) [20]. App-DDoS attack is also known as the Flash Crowd attack [13], which is a kind of DDoS attack that mimics the FC traffic. The significant feature of App-DDoS is that the number of hosts dynamically fluctuates to simulate any legal clients in and out, in contrast to the other DDoS attacks where the host number basically remains fixed.

3.3.2. Flash Crowds Traffic. The FC traffic is an extreme case of legal client traffic. Although the FC flows are definitely from legitimate users and they are absolutely normal requests, the generated results may be similar to what DDoS attacks cause. Hence, it is important to be able to distinguish DDoS attack flows from FC flows in the background traffic. The significant feature of FC traffic is that the generated traffic volume may fluctuate and looks like random wave zig-zag [3], due to the number of clients dynamically changing, while DDoS traffic volume is continuously stable.

Table 1 describes the comparisons between the DDoS traffic and the FC traffic. The main differences are the traffic and the traffic control response. For the FC traffic, it is genuine traffic and responsive. For the DDoS attack traffic, it is malicious and unresponsive.

Table 1. Comparison Between Flash Crowd and DDoS Attack [14]

Category	Flash Crowds	DDoS
Network Impact	Congested	Congested
Server Impact	Overloaded	Overloaded
Traffic	Genuine	Malicious
Response to Traffic Control	Responsive	Unresponsive
Traffic Type	Mostly Web	Any
Number of Flows	Large Number of Flows	Any
Predictability	Mostly Predictable	Unpredictable

4. Simulation System

Our designed simulation uses the Spirent Test Center (STC) platform [11], which offers an object-oriented model for defining traffic utilizing the advantages of encapsulation and inheritance. It provides cutting edge hardware components to enable complexity and real-time control to simulate large and "real-world" traffic, while concentrating on the scalability and the test automation. This section introduces the components in our applied simulation system and the corresponding physical connections of those hardware components.

4.1. System Components

4.1.1. Hardware. There are two main hardware components in our applied STC system, namely the SPT-2000A chassis and EDM-2001B Small Form Factor. SPT-2000A chassis is populated with EDM-2001B test module. EDM-2001B module can be used to measure performance of Layer 4 to 7 devices, e.g., firewall, IDS/IPS, SSL accelerator, etc. When combined with high-scale STC software components, it offers the complete high performance testing solution.

The main purpose of STC platform is to test the performance of Device Under Test (DUT) under the simulated "real-world" network traffic. Since STC simulates the network traffic under a Client/Server structure, a DUT is needed to transmit the generated traffic between the simulated clients and the simulated host. We apply a CISCO DUT connecting with the Spirent test module.

4.1.2. Software. STC packet generator and analyzer base package (BPK-1001A) is the software component in the Spirent system to control the packet generation. In our system, this BPK-1001A runs on the Windows XP operating system.

4.2. System Architecture

Figure 2 illustrates the architecture of our simulation system that contains a management computer running STC package (BPK-1001A), an STC chassis (SPT-2000A) containing a single STC module (EDM-2001B) with four ports, and the DUT. The laptop we use runs Windows XP and STC BPK-1001A software, and acts as a base to control the hardware components.

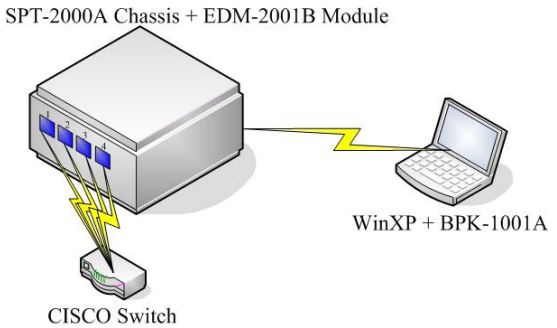


Figure 2. Architecture of our Simulation System

All four test ports of EDM-2001B module connect with the switch. A test port simulates a number of hosts, each of which can either be a single host or a block of hosts. According to the two common characteristics of DDoS attacks and FCs,

we define that Port 1, Port 2 and Port 3 represent client host blocks as the traffic sources, whereas Port 4 represents single host as the traffic destination. The ingress traffic into the CISCO switch consists of the aggregate traffic generated by all the configured hosts within Port 1, Port 2 and Port 3. All of these generated DDoS attacks and FCs packet streams transmit to Port 4.

5. Traffic Generation

In order to simulate either DDoS attacks or FCs in a testbed, there are two conditions that must be satisfied. First is that the number of traffic source hosts should be large enough. Second, the generated traffic should have typical characteristics according to the network protocol. The STC platform meets those two requirements by making it possible to configure the host block object and the stream block object through the software interface. This section describes our comprehensive configuration for DDoS attacks and FCs simulation.

5.1. Host/Port Configuration

A host block within one port simulates a large number of source and destination hosts. Since the host number determines the traffic volume, we examine this factor by setting two simulation scenarios with different numbers. Scenario 1 simulates the traffic generation with a large number of hosts. The number of hosts for Port 1, Port 2, Port 3 and Port 4 are set as 211, 198, 347 and 1, respectively. Scenario 2 simulates the traffic generation with a small number of hosts. The number of hosts for Port 1, Port 2, Port 3 and Port 4 are set as 10, 20, 20 and 1, respectively. Thus there are 756 source hosts in Scenario 1 and 50 source hosts in Scenario 2. For the IP address setting in each host block, there is a manually set initial IP address with a user defined octet incremental step to unique each IP address. Figure 3(a) shows the snapshot of the host configuration process with the host number setting and the corresponding IP address setting.

5.2. Stream Configuration

A stream block defines the characteristics for a stream of network traffic.

5.2.1. Source and Destination Configuration. This configuration step describes the detailed communication source and destination setting. As mentioned in Section 4.2, the simulation traffic transmits from Port 1, Port 2 and Port 3 into Port 4. For the host distribution for network topology, we select *Pair* to provide point-to-point traffic transmission from bots to victim, or legitimate clients to Web server. In addition, we choose *Unidirectional* to allow the simulated host traffic which only travels in one direction from source to destination. Figure 3(b) illustrates the snapshot of source and destination configuration.

5.2.2. Frame Size Configuration. Frame size configuration allows the setting of frame size. In order to simulate a dynamical network traffic, we define the frame size as *Random* which ranges from 128 Bytes to 256 Bytes. Additionally, we define the appropriate traffic protocol by selecting *Vary Protocols & QOS*. Hence, the appropriate traffic protocol can be selected for DDoS attack traffic, e.g., select UDP protocol for UDP flooding simulation. Figure 3(c) illustrates the snapshot of this operation.

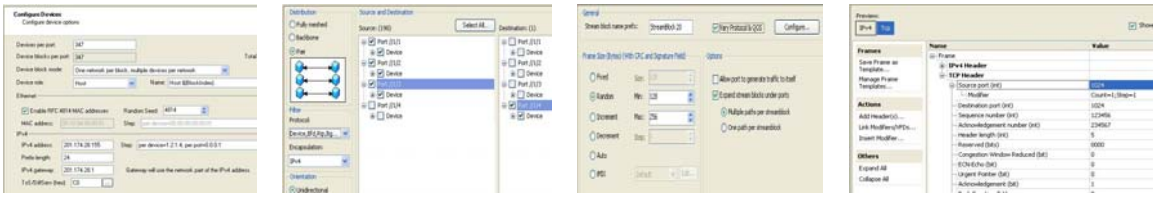
5.2.3. Packet Header Configuration. This configuration process customizes the packet header information for the corresponding protocols. Take TCP SYN flooding attack for example, the TCP packet header can be added with the targeted source and destination port numbers. Additionally, the sequence number, the ACK number, reserved, checksum, etc, all of these mandatory header fields can be configured. Figure 3(d) illustrates the snapshot of packet header configuration.

5.3. Traffic Capture

We use the traffic capture service within the STC platform to record the generated traffic. The capture process can also be configured according to the simulation requests. We obtain the .pcap capture file through this service.

5.4. Statistics of Captured Traffic

Both Scenario 1 and Scenario 2 examine UDP flooding attack, ICMP flooding attack, TCP SYN flooding and App-DDoS. In Scenario 1, the simulation parameters are set as follows, the host number n=768, the simulation duration t=600sec and the port load pl=512Mbps. In Scenario 2, the parameters are n=50, t=600sec and pl=512Mbps. Note that each port load can be set with 1000Mbps as maximum. If we set all three port loads as maximum, that means the receiving port will drop approximate 2/3 generated traffic. Although the high loss rate is one of the DDoS attack traffic characteristics, we consider that it is not practical for the bots to generate the whole bandwidth-occupied traffic in real DDoS. Thus we define each port load with 50% capability and so the traffic loss rate is around 33%.
Table 2 summarizes the statistics of both DDoS scenarios. It is very clear that Scenario 1 and Scenario 2 have approximately equal numbers for each attack category. Therefore, we conclude that the hosts number cannot determine the traffic volume by using STC platform. That is because the traffic



(a)Host Configuration (b) Source and Destination Configuration (c) Frame Size Configuration (d) Packet Header Configuration

Figure 3. Configuration Snapshots

generation capability had been defined for each port instead of each simulated host. Since Scenario 1 has much more host number than Scenario 2, each simulated host in Scenario 1 generates less traffic than the simulated hosts in Scenario 2 does.

Scenario 3 simulates the FCs traffic. The parameters are set as n=768, t=600sec and $pl \in$ [100, 1000]Mbps. We apply *the Command Sequencer* to define a command sequence which is used to control the host on/off. Through this way, we can simulate the legitimate web application client behavior as begin request applications or end request application. The number of captured frames is 356,123,487.

In terms of differentiation, the simulated DDoS attacks traffic and FCs traffic can be distinguished according to the traffic protocol characteristics. However, it is quite unable to identify the simulated App-DDoS traffic against simulated FCs traffic because they share very similar traffic characteristics and also App-DDoS imitates the features of FCs as the matter of fact.

Table 2. Captured DDoS Traffic Packets Number

Category	Scenario 1	Scenario 2
UDP Flooding	353,450,836	353,469,581
ICMP Flooding	353,895,905	353,396,282
TCP SYN Flooding	353,169,345	353,227,520
App-DDoS	354,020,266	353,932,521

6. Discussion

This section discusses the advantages and limitations by using STC platform to simulate the DDoS attacks traffic and the FCs traffic. In addition, this section describes how to utilize the captured traffic for the next stage of intrusion detection research.

6.1. Strengths

By configuring the STC platform appropriately, we recognize two main advantages compared with the conventional DDoS attack simulation method, i.e. applying real attack tool. One is the *flexibility*, another is *automation*. For the flexibility issue, the characteristics of simulated DDoS attack traffic, e.g., the number of attack agents, the frame size of attack packets, the number of attack packets, etc, can be flexibly customized through the software interface. For the automation issue, the configuration changes are propagated automatically through the objects in simulation system and result in time saving during simulation.

6.2. Limitations

During the simulation, we found out several limitations caused by the STC simulation software (BPK-1001A). There are two major problems, one is the *limited capture buffer size* and another is *the customer pre-defined sequencer*. With the limited capture buffer size, we cannot obtain the whole generated traffic, especially App-DDoS and FC, which contain run-time changed information. The customer pre-defined sequence provides the capability to control the host on/off for App-DDoS and FCs. However, the simulation only follows the customer pre-defined sequence, which can not be dynamically changed as practical ones.

Two minor limitations are the *IP address configuration problem* and the *packet generation sequence problem*. For the first problem, all of the host IP addresses in the host block follow a particular pre-defined sequence, which generated by a numerical increment factor for each IP address octet. For the second problem, the packet generation sequence always obeys the same host sequence from top to bottom without any randomness.

6.3. Implementation of Traffic Capture

The main purpose of traffic simulation is to provide the simulated DDoS attack traffic and the FCs traffic for the DDoS related detection and prevention research, notably to be used to test the detection capability of IDS/IPS and examine the corresponding detection algorithm [17].

Because the simulation traffic had been generated iteratively and continuously, our proposed implementation method is to replay the captured .pcap file by utilizing *Tcpreplay* in the testbed. In order to provide a practical network testing environment, the ideal implementation scenario is to replay the DDoS attack traffic capture together with the background traffic and the FCs traffic, and the detection server implements the

detection algorithm or protection mechanism to identify the malicious traffic.

7. Conclusion and Future Work

We had generated four kinds of DDoS attacks traffic and the Flash Crowds traffic with Spirent Test Center platform, which is an industry-level network packet generation testbed. Two case studies had been given and we conclude that the number of source hosts cannot determine the traffic volume in this platform due to the port based traffic generation mechanism. We will apply those simulated traffic to test our DDoS attacks detection mechanism [17] as our next stage of intrusion detection research.

8. Acknowledgment

The authors would like to thank George Oikonomou for help with restricted perimeter access. This work is supported in part by the UK HEFCE/RCIS funding.

9. References

[1] I. Ari, B. Hong, E. Miller, S. Brandt, and D. Long. Managing Flash Crowds on the Internet. In *Proc. MASCOTS2003*, pages 246–249, Oct 2003.

[2] E. Cole. *Hackers Beware*. Indianapolis, In: New Riders,, 2002.

[3] Y. Huang, H. Sun, H. Chao, and X. Chao. Non-negative Increment Feature Detection of the Traffic Throughput for Early DDoS Attack. In *Proc. SITIS'07*, pages 121–126, 2007.

[4] J. Jung, B. Krishnamurthy, and M. Rabinovich. Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites. In *Proc. WWW'02*, pages 293–304, 2002.

[5] A.R. Kumar, P. Selvakumar, and S. Selvakumar. Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms. In *Proc. IACC 2009*, volume 1, pages 1275–1280, Mar 2009.

[6] H.W. Lee, T. Kwon, and H.J. Kim. NS-2 Based IP Traceback Simulation Against Reflector Based DDoS Attack. *Artificial Intelligence and Simulation*, pages 90–99, 2005.

[7] K. Li, W.L. Zhou, P. Li, J. Hai, and J.W. Liu. Distinguishing DDoS Attacks from Flash Crowds Using Probability Metrics. In *Proc. NSS'09*, pages 9–17, Oct 2009.

[8] M. Li, J. Li, and W. Zhao. Simulation Study of Flood Attacking of DDOS. In *Proc. ICICSE'08*, pages 286–293, Jan 2008.

[9] X.L. Li, K.F. Zheng, and Y.X. Yang. A Simulation Platform of DDoS Attack Based on Network Processor. In *Proc. CIS'08*, vol.1, pages 421–426, Dec 2008.

[10] C. H. Liu and C. L. Lo. The Simulation for the VoIP DDoS Attack. In *Proc. MMIT'08*, pages 280–283, Dec 2008.

[11] A. Ma. Using Spirent TestCenter to Generate Real-World Traffic. White paper, Spirent Communications Ltd. Jan 2008.

[12] R. Mahajan, S. Bellovin, S. Floyd, J. Ioannidis, V. Paxson, and S. Shenker. Aggregate-Based Congestion Control. *Computer Communication Review*, vol.32(3), 2002.

[13] G. Oikonomou and J. Mirkovic. Modeling Human Behavior for Defense against Flash-Crowd Attacks. In *Proc. ICC'09*, pages 1–6, Jun 2009.

[14] T. Peng, C. Leckie, and K. Ramamohanarao. Survey of Network-Based Defense Mechanisms Countering the DoS and DDoS Problems. *ACM Computing Surveys*, vol.39(1):3, 2007.

[15] S. Ranjan, R. Swaminathan, M. Uysal, A. Nucci, and E. Knightly. DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks. In *Proc. IEEE/ACM Transactions on Networking*, vol.17, Feb 2009.

[16] M. Sachdeva, K. Kumar, G. Singh, and K. Singh. Performance Analysis of Web Service under DDoS Attacks. In *Proc. IACC 2009*, pages 1002–1007, Mar 2009.

[17] J. Wang, R.C.W. Phan, J.N. Whitley, and D.J. Parish. Augmented Attack Tree Modeling of Distributed Denial of Services and Tree Based Attack Detection Method. In *Proc. CIT2010*, pages 1009–1014, Jun 2010.

[18] W.Wang and S. Gombault. Efficient Detection of DDoS Attacks with Important Attributes. In *Proc. CRiSIS'08*, pages 61–67, Oct 2008.

[19] L. Xie, P. Smith, M. Banfield, H. Leopold, J. Sterbenz, and D. Hutchison. Towards Resilient Networks Using Programmable Networking Technologies. *Active and Programmable Networks*, pages 83–95, 2009.

[20] Y. Xie and S. Yu. Monitoring the Application-Layer DDoS Attacks for Popular Websites. *IEEE/ACM Transactions on Networking*, vol.17(1), pages 15–25, 2009.

[21] Y.H. You, M. Zulkernine, and A. Haque. A Distributed Defense Framework for Flooding-Based DDoS Attacks. In *Proc. ARES'08*, pages 245–252, Mar 2008.