Advanced DDoS Attacks Traffic Simulation with a 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
Loughborough, UK, LE11 3TU
{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 vital step in dealing with this problem is the network’s ability to detect such attacks. To train and analyze countermeasures, researchers typically simulate the DDoS attacks traffic by either the specialized simulator (i.e. software, hardware) or the comprehensive testbed. This paper proposes the advanced implementations of a special simulator-based simulation with Spirent Test Center platform, to simulate DDoS attacks traffic with/without simulated practical network traffic routing mechanisms.

1 Introduction

DDoS attacks are one of the most threatening computer network security problems as they handicap legitimate network usage and cause substantial damage. The devastating negative impact inspires the network security researcher costing great effort to understand and learn them, together with developing and deploying feasible and effective countermeasures against them. Since quantitative DDoS attacks are seldom obtainable from the real network environment [7], the critical research step is to set up and run the simulated DDoS attacks. Typically, this step requires substantial configuration effort.

As the fundamental but popular way, the practical attack tools, which are obtained from the hacker’s side, are still being utilized by the security researchers for their researches. If both attack tools and network traffic been configured appropriately, the simulation would have many similarities with the real DDoS attacks. Kumar et al. [5] describe eight attack tools and make comparisons between them. Nevertheless, the most significant drawback of the real attack tools implementations is that most of the applied attack tools (i.e. TFN2K [4]) have been developed more than ten years ago. Consequently, most of the used up-to-date network devices and software have embedded corresponding countermeasure mechanisms to identify and against such tool generated attack traffic and cause the experiments failure. In addition, the simulated traffic by the old attack tools lacks of capability to model the current sophisticated attack traffic within the large heterogeneous networks.

Therefore, there is a need to apply advanced approaches to simulate DDoS attacks. One main direction is to apply the specialized simulator for simulation or the comprehensive testbed for emulation. The way to implement the simulation or the emulation depends on the traffic type generation requirement (i.e. practical traffic packets, virtual traffic flow) and the experiment implementation purpose (i.e. QoS investigation, countermeasure verification). In security researches, the typical main streams of traffic generation are physically applying either simulator or testbed. Though some of the researchers utilize virtual simulators (i.e. NS-2 [6, 9]) to generate the virtual DDoS traffic for their researches (i.e. the victim server performance analysis with DDoS attack traffic [13]). By applying the physical simulator or testbed, the simulated traffic may practical and close to real DDoS attack traffic, but the problems are not only the expensive cost to purchase simulator and testbed, but also the extra professional knowledge/experience required to create, deploy and operate the development kit or the controlling system.

In this paper, we introduce several DDoS attacks simulation approaches to perform large-scale repeatable experiments by using a commercial industry-level traffic generation platform, namely, Spirent Test Center platform (STC), with step-by-step configuration guide. Our introduced approaches contain two main categories: the fundamental approach without network routing mechanism and the advanced approach with network routing mechanism. The main business function of STC platform is to test the performance of Device Under Test (DUT) under the simulated
“real-world” network traffic [10].

The rest of this paper is organized as follows. Section 2 introduces the related work about the DDoS attacks generation with the simulator simulation and the testbed emulation. Section 3 describes the abstracted DDoS attacks network topology and the features of DDoS attacks. Section 4 presents the simulation platform. The fundamental simulation approach and the advanced simulation approaches are depicted in Section 5. Section 6 discusses the related strengths and limitations of this simulation method and the traffic capture usage. Finally, we outline the conclusions in Section 7.

2 Related Work

Recent work [2] has pointed out three basic requirements for computer network security experiments: (1) hypotheses must be falsifiable; (2) experiments must be controllable; and (3) experiments must be repeatable and reproducible. Refer to the DDoS attacks experiment implementation, another three requirements [14] have been outlined: (1) specify, save and replay an experiment (specified and reproducible); (2) deploy, run and stop an experiment (controllable); and (3) monitor the simulated DDoS attack in progress and to save the results to disk for later replay or analysis (surveillable and saveable). As controllable and reproducible are overlapped in both requirement sets, they have priority to be guaranteed in our experiment. Although it may desirable to meet all of these requirements, each simulator and testbed may have its own strengths and limitations.

We classify DDoS attacks generation approaches into two main strategies: Simulator Simulation and Testbed Emulation. Both simulator simulation and testbed emulation mimic the expected DDoS attacks traffic behavior. We assume that the key differences between these two strategies are the size and the implementation methodology. From the view of size, the simulator is the system typically contain a single hardware with the configuration application, whereas the testbed includes multiple hardware to build a network with an administration server. From the view of implementation methodology, the simulator is typically been applied with the comprehensive virtual configuration through the provided GUI, whereas the testbed need to configure the physical devices manually.

2.1 Simulator Simulation

Since GUI provides the configuration options to virtually set up the nature of simulated DDoS attacks (e.g. topology of network, number of bots, characteristics of traffic, etc.), the key advantage of simulator simulation is that the simulation can be virtually created quickly and inexpensively, whereas the main shortage is that simulated networks may behave very differently from real or emulated network when under attack [3].

Spirent Test Center [17] and Intel IXP2400 network processor [8] are professional traffic simulators. In our previous work [17], we have applied Spirent Test Center platform and Spirent TestCenter Application 3.00 to configure the build-up option and generate four kinds of DDoS attacks traffic (TCP SYN flooding attack, UDP flooding attack, ICMP flooding attack and App-Doc attack) and Flash Crowds traffic with the basic C/S connections. According to the above mentioned DDoS attacks experiment requirements, the main drawback is that Spirent Test Center platform has poor saveable capability to store the whole generated traffic. Intel IXP2400 network processor works together with Intel Workbench SDK 3.5 and combines a high performance Intel XScale core with eight 32-bit independent multi-threaded micro-engines (ME), which are programmable processors to provide rapid development. The simulated DDoS attacks flow [8] has the characteristics of self-similarity by introducing fractal Brownian motion model.

The Experimenter’s Workbench [11] and its extension, SEER [15] provide GUI to interact with DETER [1], which is the simulator foundation, by setting the already combined third-party components (e.g., the attack traffic generators, the legitimate traffic generators and the network topology generator, etc) within the simulator to implement simulation. There are three required configuration steps: (1) topology generation; (2) legitimate traffic generation; and (3) attack traffic generation.

2.2 Testbed Emulation

The testbed is normally the specialized LAN. Thus, it has following features: (1) it is difficult to extend a local Ethernet network to model the performance of the entire ISP network, which cause the problem of scalability [14]; (2) the testbed have usually been isolated with the public network to guarantee the control of the generated malicious behavior; and (3) most of the testbeds (i.e. DETER [1], Netbed [18]) are developed for the multiple computer network security researches instead of the single DDoS attacks purpose.

DETER testbed [1] is the well-known security research testbed. It provides the medium-scale network with security experimental capability for security researchers to replicate threats of interest in a secure environment and to develop, deploy, validate and evaluate potential theories and solutions. There are two clusters of experimental PC nodes and each of clusters contain approximately 100 nodes. These nodes are interconnected by high speed Ethernet switches. The original testbed can model DDoS attacks, worm behav-
ior experiments and early routing security experiments.

dosTF testbed [14] is a specialized DDoS attacks experimental testbed and it provides the functionalities to examine the effectiveness of different DDoS mitigation mechanisms and to allow for the testing of defense appliances. This testbed is the combination of the physical PC and the virtual technique including 8 physical PCs (expandable) and 3 VMWare servers provide around 200 virtual hosts in the simulated DDoS attacks. The significant problem is that the structure of the network topology need to be reconfigured manually.

3 Background of DDoS Attacks

3.1 Abstracted Network Topology of DDoS Attacks

Network topology deals with finding the topological structure of the network. The abstracted network topology for DDoS attacks 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 adversary (the bot master) and all of the generated attack traffic destined to the primary victim.

![Figure 1. Abstracted DDoS Attack Network Topology](image)

3.2 Features of DDoS Attacks

There are two main features of DDoS attacks traffic transmission: (1) typically, only one target is the primary victim, which is the destination of all the DDoS traffic packets; (2) numerous packets are sent to the destination persistently enough to congest the link and overload the victim.

Additionally, there are some characteristics [12] about the nature of DDoS attacks traffic: (1) the traffic is unresponsive due to the source IP of traffic packets may be faked; (2) the type of attack traffic can be any (though, some of the classical DDoS attacks has the single traffic type, i.e. UDP flooding attack only with UDP packets); (3) the number of flows can be any; and (4) DDoS attacks traffic normally is unpredictable.

4 Simulation Platform

4.1 Platform Components

4.1.1 Hardware

Our applied STC platform has two main hardware components: (1) SPT-2000A chassis; and (2) EDM-2001B Small Form Factor. SPT-2000A chassis is populated with EDM-2001B test module. Since STC simulates the network traffic with simulated clients and servers, a DUT is needed to transmit the generated traffic between the simulated clients and the simulated server. We apply a CISCO switch as the DUT connecting with EDM-2001B test module.

4.1.2 Software

STC packet generator and analyzer base package (BPK-1001A) controls the packet generation of Spirent platform. This BPK-1001A installs on a separated Windows XP laptop in our applied simulation platform.

4.2 Platform Architecture

Figure 2 illustrates the architecture of our simulation system including: a management laptop running STC package (BPK-1001A), a STC chassis (SPT-2000A) containing a single STC module (EDM-2001B) with four ports (Port$_1$, Port$_2$, Port$_3$ and Port$_4$), and DUT (CISCO switch). The laptop acts as a base to control the hardware components. All four test ports of the EDM-2001B module connect with the DUT. Each test port simulates either a single host or a number of hosts. According to the two common characteristics of DDoS attack traffic transmission, we define that Port$_1$, Port$_2$ and Port$_3$ simulate the client hosts as the traffic sources (bots)\(^1\), whereas Port$_4$ represents the server host as the traffic destination (primary victim). The ingress traffic into switch consists of the generated aggregate traffic from all the configured bots within Port$_1$, Port$_2$ and Port$_3$. All of these simulated DDoS attacks transmit to Port$_4$.

\(^1\)We assume that “bot” is the simulated “source host” of DDoS attacks traffic. Hence, we use bot and source host interchangeably in rest of this paper for simplicity.
5 Traffic Generation

We propose two kinds of DDoS attacks traffic generation methodologies with Spirent Test Center platform. One is to model DDoS attacks by applying C/S structure to simulate numerous bots simply connecting to the single victim server without the sophisticated network topology and routing information. While, another is to model DDoS attacks with a more practical environment including comprehensive network topology and routing information.

5.1 Fundamental Configuration Approach

This subsection briefly describes our configuration based on the simulator platform offered host block object and stream block object to simulate DDoS attacks. More information can be found in our previous work [17].

5.1.1 Host Block Configuration

A host block within one port simulates a reasonable number of hosts as either source or destination. The host block objects in Port1, Port2 and Port3 simulate large amount of bots. The host block object in Port4 simulates the single victim server. To set the IP address of each bot in each host block, we manually configure an initial IP address with a customized octet incremental step to unique each IP ad-
network traffic. Figure 3(a) shows a snapshot of the host configuration process with the bot number setting and the corresponding IP address setting.

5.1.2 Stream Block Configuration

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

- **Source and Destination Configuration.** This configuration step describes the detailed communication setting between bots and victim server. For the host distribution of network topology, we select Pair to provide point-to-point traffic transmission from bots to victim server. In addition, we choose Unidirectional to allow the simulated traffic which only travel in one direction from bots to victim server. Figure 3(b) illustrates the snapshot of source and destination configuration.

- **Frame Size Configuration.** Frame size configuration allows the setting of frame size. In order to provide the similarity with the practical traffic, we define the frame size as Random which is range 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 attacks traffic, i.e. select TCP protocol for TCP SYN flooding simulation. Figure 3(c) illustrates the snapshot of frame size configuration.

- **Packet Header Configuration.** This configuration process customizes the packet header information for the corresponding protocols. Figure 3(d) illustrates the snapshot of packet header configuration.

5.2 Advanced Configuration Approaches

We apply the provided routing configuration templates in the platform configuration wizard to generate the comprehensive DDoS attacks with routing mechanism. This subsection introduce PWE configuration and RSVP-TE configuration, which are two kinds of protocols to manage Multiprotocol Label Switching (MPLS) path. Practically, there are the customer side and the provider side in MPLS. In order to model DDoS attacks, we assume that the customer side plays as the bot, whereas the provider side plays as the victim.

5.2.1 PWE Configuration

The first applied network topology template is the Pseudo-Wire Emulation Edge-to-Edge (PWE3) configuration wizard. By creating the simulated routers and selecting and enabling routing and labeling protocols (i.e. Label Distribution Protocol (LDP), Resource Reservation Protocol - Traffic Engineering (RSVP-TE)), we configure customer side (bots) and provider side (victim server) pseudowires and generate the traffic across pseudowires. Both the bot side and the victim server side include the route and the routing between the simulated routing devices.

- **Configure Provider Ports.** We take Port4 as the provider port to model the victim server. In addition, we configure the detailed information about the simulated server (i.e. IP address, prefix length). Figure 4(a) illustrates the snapshot of this configuration step.

- **Configure Provider Routers.** We enable and configure Provider (P) and Provider Edge (PE) routers and associated IP addresses according to the provided configuration option. Then, we select LDP protocols and associated options to model the routers on the provider side. Figure 4(b) displays the snapshot of provider router configuration step.

- **Configure Customer Ports.** We apply Port1, Port2 and Port3 as the customer side to model the numerous bots as the attack traffic source. The configuration process snapshot is shown as Figure 4(c).

- **Configure Pseudowires.** This configuration step requires the modelled information including number of pseudowires, Ethernet encapsulation, etc. Figure 4(d) shows the snapshot to configure pseudowires.

- **Configure Hosts.** This configuration mainly specifies the MAC address formatting patterns and assigns number of host and host MAC addresses to Customer Edge (CE) routers. In order to meet against the features of DDoS attacks, a reasonably large number of hosts per CE router may desirable. Figure 4(e) depicts the host configuration snapshot.

- **Configure Label Switched Path (LSP) traffic.** The simulated traffic stream is setup in this configuration step. As most of the malicious DDoS attack traffic transit from the bot to the victim server as unidirectional, we select the traffic transmission only directing from the customer side to the provider side. In addition, we define the traffic generation capability of each port. The traffic configuration is illustrated as Figure 4(f).

5.2.2 RSVP-TE Configuration

As Resource Reservation Protocol-Traffic Engineering (RSVP-TE) is more widely applied in many QoS-oriented networks nowadays, we apply RSVP-TE configuration wizard in simulator platform as our second advanced DDoS attacks generation approach to model DDoS attacks within
more practical network environment. This template provides two types of RSVP-TE IPv4 network topologies: Point-to-point (P2P) RSVP-TE and Point-to-multipoint (P2MP-TE).

This wizard emulates basic RSVP-TE signaled networks from two points-of-view: ingress-customer side and egress-provider side. The customer side represents the network of bots including the CE routers and attack traffic sent from those bots. The provider side represents the network of victim server including P and PE devices. The labeled traffic transmits from the customer side to the provider side of the network.

- **Configuration Topology.** Figure 5(a) shows the snapshot of the configuration process. We select Point-To-MultiPoint with Leaf topology.

- **Configure Ingress Ports.** Figure 5(b) illustrates the ingress port configuration. Once again, we select Port1, Port2 and Port3 as the traffic source to simulate DDoS attack bots and configure the IP address of each port.

- **Configure Egress Ports.** Similar as the fundamental configuration in Section 5.1, we choose Port4 to represent the traffic destination as the DDoS attack victim server. Figure 5(c) displays the related egress ports configuration.

- **Configure Routers, Tunnel and Routes.** The configuration snapshots of routers configuration, tunnel configuration and routes configuration are shown as Figure 5(d), Figure 5(e) and Figure 5(f).

- **Configure Traffic.** This configuration step creates the stream block to simulate the DDoS attacks traffic. We select Aggregate as the type of stream block. Then, we define the port traffic load is 40% for each ingress port. Thus, there would be 20% generated traffic loss, which is one of the characteristics of DDoS attacks.

6 Discussion

6.1 Approaches Analysis

Besides we applied simulation approaches based on PWE and RSVP-TE routing mechanisms and configured options, there are more other routing mechanisms (e.g. BGP, IS-IS, RIP, etc) and more detailed comprehensive configuration options provided by Spirent Test Center platform. Hence, we believe that there could be more advanced and better DDoS attacks traffic simulation ways than our proposed approaches.

Refer to our applied approaches, the key difference between the fundamental approach and the advanced approaches is whether contain the routing mechanism in the traffic generation mechanism or not. Since the goal of both approaches is to generate DDoS attacks, it is clear that the former way is easy to be implemented due to no deep computer network knowledge required from the experimenter, whereas the latter way requests the well understanding about specified routing protocols. But both of the approaches are easily to be implemented with virtual configuration. Thus, the experimenter selects the appropriate way to simulate DDoS attacks by Spirent Test Center platform mainly depending on the simulation purpose and the requirement of network traffic behavior.

6.2 Strengths

Two main advantages have been identified. (1) Flexibility, the characteristics of simulated DDoS attack traffic (i.e. the number of bots, the frame size of attack packets) can be flexibly customized through the software interface. (2) Automation, the configuration changes are propagated automatically through the objects in simulation system and result in time saving during simulation.

Refer to the experimental requirement in Related Work, the Spirent Test Center simulation satisfies the requirements of controllable and reproducible. The platform provides the specialized GUI to configure the traffic characteristics (i.e. the number of bots) and to control the behavior of traffic generation (i.e. start and stop the generation). Additionally, all of the configured options can be saved in the script file and can be reused to implement traffic generation with same characteristics repeatedly.

6.3 Limitations

There are three founded weaknesses of our traffic simulation approach. The major weakness is Limited capture buffer size, which has handicapped the capture of whole simulated traffic. Hence, the saveable capability cannot be well satisfied. The two minor problems are IP address configuration problem and packet generation sequence problem. In the former one, all of the bot IP addresses in the host block following the particular pre-defined sequence, which is lack of the randomness of bot IP address distribution. In the latter one, the packet generation sequence obeys exactly the same bot IP address sequence from the first simulated bot to the last simulated bot. Thus, we argue that Spirent Test Center platform lacks of randomness to simulate hosts and assign the corresponding IP addresses.
6.4 Implementation of Simulated DDoS Attacks

The main target of DDoS attacks traffic simulation is to facilitate DDoS related detection and prevention researches, notably to be replayed to test the detection capability of IDS/IPS and examine the relevant detection algorithm (i.e. AAT-based intrusion detection algorithm [16]). Ideally, the traffic replay should mix with the background traffic as noise to examine detection accuracy performance.

7 Conclusion

We have introduced DDoS attacks traffic simulation approaches by applying the Spirent Test Center platform, which is a commercial industry-level network traffic generator. Two main kinds of traffic simulations have been given: one is the basic approach with the provided host object and block stream object configuration based on the fundamental C/S structure, another is the advanced approach with the network topology and routing configuration.

Acknowledgment

This work is supported in part by the UK HEFCE/RCIS funding.

References


Figure 4. Configuration Snapshots of PWE Approach
Figure 5. Configuration Snapshots of RSVP Approach