Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 7 – 15

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Trends in Validation of DDoS Research

Sunny Behal[a*], Krishan Kumar[b]

[a]Deptt of Computer Sci. & Engg, Shaheed Bhagat Singh State Technical Campus, Ferozepur-152004, India [b]Deptt of Computer Sci. & Engg, Shaheed Bhagat Singh State Technical Campus, Ferozepur-152004, India

Abstract

Over the last decade, attackers are compromising victim systems to launch large-scale coordinated Distributed Denial of Service (DDoS) attacks against corporate websites, banking services, e-commerce businesses etc. These attacks results in cripple down their services to legitimate users and cause huge financial losses. Numerous solutions have been purported to combat against these DDoS attacks but there is no impeccable solution to this challenging problem till date. Most of the existing solutions have been validated using experiments based on simulation but recently, the researchers have started using publically available real datasets for the validation of DDoS research. In this paper, the validation techniques used for DDoS research are investigated comprehensively and it is proposed to extend them with the inclusion of new validation technique of analyzing real datasets. A brief review of existing real datasets is presented to elucidate the trends in the validation of DDoS research.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: DDoS; Intrusion; Flash Events; Datasets; Network Security

1. Introduction

DDoS attacks have become a serious cause of problem and security threat for the enterprises, banks etc. doing businesses over the Internet. These attacks have brought enormous financial losses to them over the years. According to CERT[1,2], "A DDoS attack is a malicious attempt from multiple systems to make computer or network resources unavailable to its intended users, usually by interrupting or suspending services connected to the Internet". There are number of evidences reported[1,3,4,5,6] which points out the severity of the DDoS problem. According to the survey conducted by Kaspersky lab in 2015[4], the average financial loss to the companies' suffering from DDoS attacks is in between $52000 to $440000. According to Q1 DDoS attack report 2015 by Arbor networks [5], the attackers are using three main types of DDoS attacks TCP SYN flood, DNS flood and Smurf attacks, out of which 76% are TCP SYN flood attacks, the 90% of the attacks are application layer attacks whereas 42% are of TCP State-Exhaustion attacks. The volume of traffic of such attacks have been amplified to around 400 Gbps in the year 2014 as compared to 100 Gbps in the year 2010. Even the number of DDoS attacks has also increased exponentially over the years[5]. According to Security watchdog report[6], the number of DDoS attacks have been increased by 240% in 2014.

* Corresponding author. Sunny Behal, Tel.: +1-91-82880-12007 Email address: sunnybehal@rediffmail.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.170

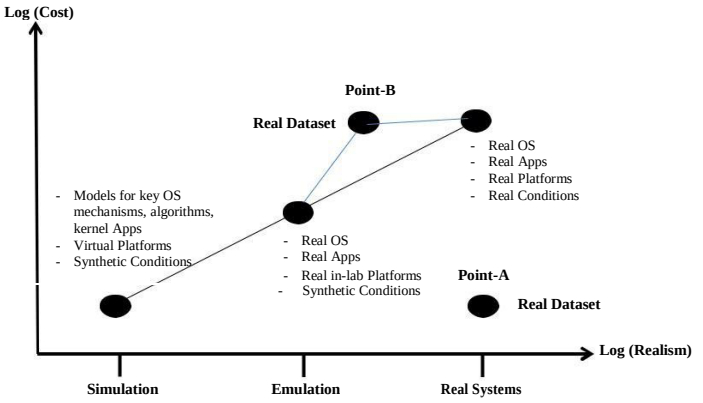

Fig. 1. Validation techniques used for DDoS related research

This is evident from this exponential increase in attack traffic that the attackers are continuously updating their skills, using advanced attack techniques to launch such huge amount of traffic and at the same time defeating the existing defense solutions. It has been observed that all of these DDoS attacks are launched now-a-days by using botnets [7]. These botnets are composed of millions of compromised machines which are controlled through some command and control server to flood enormous amount of data towards the victim[8]. The major contributions of this paper are :

- A review of validation techniques used for DDoS research.
- Addition of a new dimension of real datasets in the existing validation paradigms used for DDoS research.
- A review of publically available real datasets used for the validation of DDoS research on various identified attributes.
- Identification of the properties of a real datasets that would be more appropriate for the accurate validation of DDoS research.

The remainder of the paper is organized as follows. Section-II focuses on various validation techniques used for DDoS experimentation and their comparison. In section-III, a brief review of publically available real datasets on identified attributes is given and the last section concludes the work by highlighting the properties of an ideal realistic dataset that would be more appropriate for DDoS research.

2. Validation Techniques used for DDoS Research

Whenever a researcher proposes any novel detection or defense method in the field of network security, the proposed method has to be implemented in the form of a network based experiment for its evaluation and then it needs to be validated through available set of validation techniques. There are basically four approaches used for validation in network based experiments [9].

- **Mathematical models** are theoretical in nature. In such models, the given system, applications, platforms and conditions are modeled symbolically and then validated mathematically.
- **Simulation** provides a repeatable and controllable framework for network based experiments on a single com-puter system. A simulation based experiment is very easy to configure and manage. It gives flexibility to the programmers to do experiments in a rapid prototype and evaluation based environment so that many bad al-ternatives could be discarded timely before attempting a full implementation. Simulation use models of key operating system functions, kernel mechanisms, virtual platforms and synthetic conditions for experiments. Examples include NS2 [10], NS3[11], OMNET++[12], Qualnet3 [13], OPNET [14], CORE [15] etc.