Computers and Mathematics with Applications 63 (2012) 501–510

Contents lists available at SciVerse ScienceDirect

Computers and Mathematics with Applications

journal homepage: www.elsevier.com/locate/camwa

Detection of DDoS attacks using optimized traffic matrix

Sang Min Lee [a], Dong Seong Kim [b,c,*], Je Hak Lee [a], Jong Sou Park [a]

[a] Department of Computer Eng., Korea Aerospace University, Seoul, Republic of Korea

[b] Department of Electrical and Computer Eng., Duke University, Durham, NC, USA

[c] Department of Computer Science and Software Eng., University of Canterbury, New Zealand

ARTICLE INFO

Keywords:
DDoS attacks
Genetic algorithm
Intrusion detection
Traffic matrix

ABSTRACT

Distributed Denial of Service (DDoS) attacks have been increasing with the growth of computer and network infrastructures in Ubiquitous computing. DDoS attacks generating mass traffic deplete network bandwidth and/or system resources. It is therefore significant to detect DDoS attacks in their early stage. Our previous approach used a traffic matrix to detect DDoS attacks quickly and accurately. However, it could not find out to tune up parameters of the traffic matrix including (i) size of traffic matrix, (ii) time based window size, and (iii) a threshold value of variance from packets information with respect to various monitored environments and DDoS attacks. Moreover, the time based window size led to computational overheads when DDoS attacks did not occur. To cope with it, we propose an enhanced DDoS attacks detection approach by optimizing the parameters of the traffic matrix using a Genetic Algorithm (GA) to maximize the detection rates. Furthermore, we improve the traffic matrix building operation by (i) reforming the hash function to decrease hash collisions and (ii) replacing the time based window size with a packet based window size to reduce the computational overheads. We perform experiments with DARPA 2000 LLDOS 1.0, LBL-PKT-4 of Lawrence Berkeley Laboratory and generated attack datasets. The experimental results show the feasibility of our approach in terms of detection accuracy and speed.

1. Introduction

In recent years, communication between mobile computing devices has become more common because of a rapid development of mobile computing devices, the performance improvement of communication devices, and a drop in their prices. In addition, microelectronic devices, such as a Radio Frequency IDentification (RFID) system, and Wireless Sensor Networks (WSNs) have been interconnected through the network. This Ubiquitous and Pervasive computing, which is considered as an Information Technology (IT) to fuse real physical space and cyber space, has improved human life. However, the mobile computing devices which are important components in Ubiquitous and Pervasive computing environments have been exposed in many kinds of security threats. Especially, Distributed Denial of Service (DDoS) attacks have emerged as one of the most serious threats among others [1,2]. The intensity of DDoS attacks has become stronger through the development of network infrastructure. Basically, DDoS attacks are launched by generating an extremely large volume of traffic and they rapidly exhaust resources of target systems, such as network bandwidth and computing power. Defense mechanisms against DDoS attacks to cope with them can be classified into four categories: prevention, detection, mitigation and response [3].

* Corresponding author at: Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, New Zealand. Tel.: +64 3 364 2362x7757; fax: +64 3 364 2569.
E-mail address: dongseong.kim@canterbury.ac.nz (D.S. Kim).

0898-1221/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2011.08.020

When DDoS attacks occur, the first step to thwart DDoS attacks is detection and it should be done as quickly as possible. However, it is difficult to distinguish between a DDoS attacks and normal traffic, since DDoS attacks often do not contain malicious contents in the packets. Moreover, attackers forge their source addresses to conceal their locations to make DDoS attacks more sophisticated [4]. DDoS attack detection schemes should guarantee both short detection delay and high detection rates with low false positives. Computational overheads should be also considered because a detection engine (or module) has to deal with a large volume of real-time network traffics.

Detection mechanisms can mainly be divided into two categories; the first type is to use misuse detection relying on predefined DDoS attack patterns (or signatures). There are several well-known solutions, such as NetRanger [5], NID [6], SecureNet PRO [7], RealSecure [8], NFR-NID [9] and Snort [10–12]. However, pattern based detection mechanisms are hard to detect new intrusions. The second type is to use anomaly detection which focuses on comparing the normal behavior of the system with abnormal behaviors. Thus, anomaly detection schemes may be more effective to detect unknown intrusions. Some previous approaches on anomaly detection rely on monitoring IP (internet protocol) attributes of incoming packets. Peng et al. [13] proposed a simple detection scheme using arrival rates of new source IP addresses but it takes at least 10 seconds, which is not an appropriate detection delay. Feinstein et al. [14] presented an entropy based statistical detection model that is computed on selected IP attributes of some consecutive packets. However, they did not perform any parameters optimization for their detection model so that they could not provide the optimal window size. In addition, Kim et al. [15] collected a baseline profile on various attribute combinations but the combined attributes increased computational overheads. Our previous work [16] proposed a traffic matrix to detect DDoS attacks quickly and accurately. However, it could not find out to tune up parameters of the traffic matrix and time based window size, leading to computational overheads when DDoS attacks did not occur. Moreover, the proposed hash function creates many hash collisions.

In this paper, we propose an enhanced DDoS detection model using a revised traffic matrix from our previous work [16]. The traffic matrix is built up with packet based window size to reduce the computational overheads and a reformed hash function to reduce hash collisions. It makes our proposed model effective in terms of processing overheads and detection delay. Therefore, our proposed approach can be used to detect DDoS attacks at the early stage in real-time. Furthermore, we use a Genetic Algorithm (GA) for optimization of parameters used in the traffic matrix. The GA is a well-known heuristic approach to figure out an optimal value in large search space. To maximize detection rates, we optimize three parameters in our detection model; (i) size of traffic matrix, (ii) packet based window size, and (iii) threshold value of variance from packet information. Then, we carry out experiments on not only a LBL-PKT-4 [17] dataset but also a DARPA 2000 LLDOS 1.0 [18] dataset and an attack traffic dataset that we created. The experimental results show the feasibility of our proposed approach. A preliminary version of this paper appeared in [19].

The rest of this paper is organized as follows. In Section 2, related work is presented briefly. Our proposed detection model is presented in Section 3. In Section 4, the experiments and analysis are described. Finally, we conclude this paper in Section 5.

2. Related work

Anomaly detection schemes can mainly be divided into the following technical categories; rate limiting, data mining, and statistical analysis techniques. At first, rate limiting techniques detect anomalous connection behavior based on the premise that an infected host will try to connect to many different machines in a short period of time. It detects portscans by putting new connections exceeding a certain threshold in a queue. An alarm is raised when the queue length exceeds a threshold. The rate limiting techniques are easy to understand and implement as well. However, they are too simple to detect sophisticated intrusions and it is hard to set up proper threshold values. Next, data mining techniques are used to build a detection model (classifier) that can discover profile of network features. Lee and Stolfo [20] built a classification model to detect anomalies. They achieved a reasonable success in terms of classifying normal and intrusion data and reduced misclassification rates by using additional statistical features. A meta-detection model [21] was proposed to improve their previous approach. It used combined multiple detection models to increase detection accuracy but multiple models definitely made computation more complex. Finally, many detection techniques have been proposed in a statistical analysis field. Several statistical analysis based detection models, in particular those relying on monitoring IP attributes of arrival packets were proposed. Talpade et al. [22] proposed NOMAD which is a scalable and passive network monitoring system. It can detect attacks by analyzing IP packet header information such as a time to live (TTL) field, packet delay variation and traffic flow. It does not support creating the classifier for high-bandwidth traffic that is aggregated from distributed sources [3]. Peng et al. [13] proposed a simple detection scheme called Source IP address Monitoring (SIM) to detect high bandwidth attacks. The model monitors arrival rates of new source IP addresses and detects changes of them using a non-parametric Cumulative Sum (CUSUM) algorithm [23,24] which is more suitable for analyzing a complex network environment than a parametric algorithm. Their approach showed high detection accuracy with low computational overheads. Attacks including subnet spoofed IP addresses [3,25] can be also detected by this model. But their experimental results showed that the detection delay was between 10 and 127.3 seconds which is not satisfactory in terms of the detection delay for a real-time detection system. Feinstein et al. [14] proposed a statistical detection model to identify DDoS attacks by computing entropy and frequency-sorted distributions of specific IP attributes. The entropy could be calculated through a number of consecutive packets called a sliding window of a fixed width. They implemented an entropy model as a plug-in for Snort [11,12] and performed experiments to