A Novel Visualization Method for Detecting DDoS Network Attacks

Jiwan Zhang, Guoqiang Yang, Liangfu Lu*, MaoLin Huang, Ming Che
1. School of Computer Science and Technology, Tianjin University, Tianjin, P.R.China;
2. Mathematics Department, Tianjin University, Tianjin, P.R.China, 300072;
3. Faculty of information Technology, University of Technology, Sydney, Australia
*Corresponding Author E-mail: liangfulv@gmail.com

Abstract. With the rapid growth of networks in size and complexity, network administrators today are facing more and more challenges for protecting their networked computers and other devices from all kinds of attacks. Unlike the traditional methods of analyzing textual log data, a visual interactive system called DDoSViewer is proposed in this paper for detecting DDoS kind of network attacks. DDoSViewer is specifically designed for detecting DDoS attacks through the analysis of visual patterns. We will discuss the data sources, visual structures and interactive functions that are used in the proposed visualization system. We will also discuss the advantages and disadvantages of the existing visual solutions for DDoS detection. The extraction and analysis of network data, the calculation and display of graphic elements’ attributes and the pre-characteristics of DDoS attacks are all included in the new visualization technique. The experiments showed that the new system can detect DDoS attacks effectively.

Keywords: network security; DDoS attacks; information visualization; port scan

1 Introduction

Networks and data communication systems are becoming more and more complex [1]. However, there is no absolute solution to secure a networked system perfectly. Most existing network security techniques and tools still rely heavily on human detection of intrusions. These techniques require users to analyze and detect the anomalies and intrusions manually. To enhance the human perception and understanding of all kinds of network intrusion and attacks, network visualization has become a hot research field in recent years that attempts to speed up the intrusion detection process through the visual analytics. Unlike the traditional methods of analyzing textual log data, visualization can increase the efficiency and effectiveness of network intrusion detection significantly. It can not only help analysts to deal with the large-volume of analytical network data effectively, but also help network administrators to detect anomalies through the pattern recognition in visual graphs. It can even be used for discovering new types of attacks and forecasting the trend of unexpected events.
Some visualization techniques and tools have been proposed recently for detecting hostile attacks [2,3,4]. However, these techniques are more focusing on how to produce novel visual structures for general real-time monitoring of large volume of network traffic data, and they are not specifically designed for detecting DDoS (Distributed Denial of Service) attacks. Up to now there are no specific tools available for DDoS attack detection.

This paper proposes a novel visualization system called DDoSViewer that uses a new visual representation to display the main features and characteristics of DDoS attack. The proposed technique utilizes a variety of visual elements to map a collection of datagram to the graph for emphasizing DDoS patterns. The focus+context viewing and interaction techniques used in our system will also be discussed. The experiments have shown that the new system is able to detect port scans and many other kinds of DDoS attacks quickly and effectively.

The rest of the paper is organized as follows. Section 2 presents some of the related work. We describe our approach in section 3, including the details of data collection and processing, nodes coordinates calculation and their visualization. Case studies are shown in section 4. Finally, we give the conclusions and future work in section 5.

2 Related work

The study of DDoS attack detection has been popular for the last decade. Some works have been done in finding ways to detect DDoS attacks in large-volume alerts produced detection tools which employed visualization methods. Pearlman [5] proposed a new visualization in 2007 for network security by approaching the problem from a service-oriented perspective. This research provides a real time system for network administrators to monitor service activities, enabling for the early stage detection of attacks, including Denial of Service (DoS) attacks. Chris Lee etc [6] proposed a VisualFirewall in 2005 that seeks to aid in the configuration of firewalls and monitoring of networks by providing four simultaneous views that display varying levels of detail and time-scales as well as correctly visualizing firewall reactions to individual packets. Christos etc [7] introduced 3D interactive auto-stereoscopic (AS) displays for visual representations of attacks.

Although the above visualization techniques can assist network analysts in analyzing abnormal (or unusual) patterns of network data in the early stage of network intrusion detection, they can only produce alarms and in most cases the accuracy rate of alarming for real attacks is very low. Therefore, the actual identifications and classifications of a variety of attacks are still rely on human brain. Furthermore, so far there is no specific tools developed for detecting DDoS attacks, and the above approaches are only focusing on the visualization of suspicious network activities and they do not help in the analysis of network event characteristics.

In this work, we focused on both the analysis of DDoS features and the investigation of novel visual representations. This enables the new system work effectively in some complex situations for DDoS attack detections, such as Smurf attacks detection, port scans detection etc.