Safeguard Information Infrastructure Against DDoS Attacks: Experiments and Modeling

Yang Xiang and Wanlei Zhou

School of Information Technology, Deakin University,
221 Burwood Highway, Vic 3125, Australia
yxi@deakin.edu.au, wanlei@deakin.edu.au

Abstract. Nowadays Distributed Denial of Service (DDoS) attacks have made one of the most serious threats to the information infrastructure. In this paper we firstly present a new filtering approach, Mark-Aided Distributed Filtering (MADF), which is to find the network anomalies by using a back-propagation neural network, deploy the defense system at distributed routers, identify and filtering the attack packets before they can reach the victim; and secondly propose an analytical model for the interactions between DDoS attack party and defense party, which allows us to have a deep insight of the interactions between the attack and defense parties. According to the experimental results, we find that MADF can detect and filter DDoS attack packets with high sensitivity and accuracy, thus provide high legitimate traffic throughput and low attack traffic throughput. Through the comparison between experiments and numerical results, we also demonstrate the validity of the analytical model that can precisely estimate the effectiveness of a DDoS defense system before it encounters different attacks.

1 Introduction

Distributed denial-of-service attacks (DDoS) currently bring a tremendous threat to the information infrastructure. In a DDoS attack, multiple malicious hosts (zombies) that are recruited by the attacker launch a coordinate attack against one host or network victim, which cause denial of service to legitimate users. To defend against DDoS attacks, much of the current research focus on filtering [1], traceback [2], and congestion control [3]. Many demonstrate the effectiveness of the countermeasures under some preset conditions and assumptions. Among the traceback schemes, packet marking overwrites some fields in the IP header, which are called marks, to record the information needed to reconstruct the sources. It includes two main streams: Probabilistic Packet Marking (PPM) [4] and Deterministic Packet Marking (DPM) [5]. In particular, an improved DPM scheme, Flexible Deterministic Packet Marking (FDPM) [6], requires a small number of IP packets to find out more sources than other schemes, and has a built-in overload prevention mechanism to intelligently mark packets when system is overloaded in high-speed networks. The work in this paper is based on FDPM. Firstly, we present Mark-Aided Distributed Filtering (MADF) and

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 320–333, 2005.

its experiments. This system is to find the network anomalies by using a back-propagation neural network, deploy the defense system at distributed routers, identify and filtering the attack packets before they can reach the victim. Then secondly we propose an analytical model for the interactions between DDoS attack party and defense party, which allows us to have a deep insight of the interactions between the attack and defense parties.

2 Experiments on DDoS Defense by MADF

2.1 Background

Flexible Deterministic Packet Marking (FDPM) [6] deploys its encoding modules are deployed at the edge routers that are close to the attack source end. When packets enter the network, they are marked by the encoding modules. The real source IP addresses of the entry points and hash of the address (we call these bits digest bits) are stored in the marking fields. The mark will not be changed when the packet traverses through the network. The address digest bits make sure the group of packets comes from the same entry point, they also provide a picture of the aggregation feature of packets; and segment number is used to reconstruct the real source in it original order. When the packets reach the victim end, the source IP addresses of entry points can be reconstructed. More details of the marks can be found in related references.

If the attacker sends attack packets through the same entry point, there will be a special pattern of marked packets with the same destination IP address and address digest bits. Therefore, in a global view, there will be a pattern with several groups of packets with corresponding address digest bits, and the same destination IP address. The pattern reflexes clearly the character of DDoS traffic that come from multiple sources and aggregate at one destination. This information is especially beneficial to find out attack traffic and remove them from legitimate traffic. In our work, the pattern is recognized by neural network.

2.2 System Design

As it is shown in figure 1, Mark-Aided Distributed Filtering (MADF) can be deployed at any point between the source end (one hop behind FDPM encoding module) and the victim end. The system includes two parts, the Offline Training System (OTS) and Online Filtering Systems (OFSs). The reason for this design is that most of the computation time is spent on the training of neural network. Once the network is trained, the filtering system can perform filtering at almost real time because the test phase of a neural network is very fast. The OTS is a lightweight neural network [7] with back-propagation algorithm [8]. This offline system collects traffic features and trains the neural network without influencing the normal operation of the network. In order to save the computation time of training, we propose a serialized neural network approach, which is that the trained neural networks can be serialized and be shared for different OFSs. In