Available online at www.sciencedirect.com
ScienceDirect
Computer Networks 51 (2007) 3564–3573
Computer Networks
www.elsevier.com/locate/comnet

A queueing analysis for the denial of service (DoS) attacks in computer networks

Yang Wang [a], Chuang Lin [a], Quan-Lin Li [b], Yuguang Fang [c,*]

[a] Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China
[b] Department of Industrial Engineering, Tsinghua University, Beijing 100084, China
[c] Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, United States

Received 10 May 2006; received in revised form 25 December 2006; accepted 19 February 2007
Available online 18 March 2007

Responsible Editor: Christos Douligeris

Abstract

In most network security analysis, researchers mainly focus on qualitative studies on security schemes and possible attacks, and there are few papers on quantitative analysis in the current literature. In this paper, we propose one queueing model for the evaluation of the denial of service (DoS) attacks in computer networks. The network under DoS attacks is characterized by a two-dimensional embedded Markov chain model. With this model, we can develop a memory-efficient algorithm for finding the stationary probability distribution which can be used to find other interesting performance metrics such as the connection loss probability and buffer occupancy percentages of half-open connections for regular traffic and attack traffic. Different from previous works in the literature, this paper gives a more general analytical approach to the study of security measures of a computer network under DoS attacks. We hope that our approach opens a new avenue to the quantitative evaluation of more complicated security schemes in computer networks.

Keywords: DoS attack; Network security; Queueing; Connection loss probability

1. Introduction

Due to the widely deployed wide-area computer and communications networks, the Internet has undergone rapid development all over the world and has become indispensable in our daily lives. However, the Internet has caused many security problems and financial loss due to the unauthorized access. Network security has thus attracted considerable attention in the last few decades. The first international well-publicized security incident of the ARPANET was identified by Cliff Stoll in 1986 [1]. Later in 1988, the ARPANET had experienced the first automated network security attack, referred to as the Morris worm [1]. As network capability grows faster and larger, network security has become a rather important issue from both theoretical point of view and engineering applications.

* Corresponding author. Tel.: +1 352 846 3043.
E-mail addresses: ywang@csnet1.cs.tsinghua.edu.cn (Y. Wang), clin@csnet1.cs.tsinghua.edu.cn (C. Lin), liquanlin@tsinghua.edu.cn (Q.-L. Li), fang@ece.ufl.edu (Y. Fang).

1389-1286/$ - see front matter
doi:10.1016/j.comnet.2007.02.011

Network attacks are common nowadays. There are several types of crucial attacks, such as the denial of service (DoS), worm, trojan horse and virus, each of which causes serious problems to normal business operations. The DoS attacks usually cause significant disruptions to computer networks. A DoS attack can be regarded as an explicit attempt of attackers to prevent legitimate users from gaining a normal network service (see Sandstrom [2]). Due to the serious consequence of DoS attacks, there are intensive research in this area. In general, DoS attacks can be classified into several different types, however, the prevalent type is referred to as the packet flooding attack. Attackers may flood a network with a large volume of data in order to deliberately consume the basic and limited resources of a victim, such as the process control blocks and the maximum allowed connections. In particular, DoS attacks may disrupt the normal operation of physical components in the network, and may also manipulate data in transit such as encrypted data [3]. Moreover, multiple hosts may be employed to coordinate an attack by flooding a victim with a barrage of attack packets, which is usually referred to as the distributed denial of service (DDoS) attacks. A reflection attack, which is a special case of DDoS attacks, uses the compromised hosts as reflectors to hide the identity of the attackers or to amplify an attack. Therefore, the reflection attacks can cause more severe damages to the networks.

Many defense mechanisms have been proposed in the literature to defend against DoS attacks [4–8]. For these mechanisms, most researchers primarily focused on attack detections and responses. Commonly, the anomaly-detection or signature-scan technique can be used to identify an ongoing attack; while the responses can take the reactive or proactive measures to mitigate the networking damages. These mechanisms include blocking attack packets to reduce the intensity of attacks, tracing the packets to locate the attacking source(s), and using the proactive measures to filter the attack packets ([4] and reference therein). Based on the effective detection and filtering techniques, we may be able to characterize the behavior of the DoS attacks and estimate the impact of the DoS attacks quantitatively. Moore et al. [9] provided some insights on the prevalence of DoS activities over the Internet and used a traffic monitoring technique, called *backscatter analysis*, to estimate the worldwide prevalence of the DoS attacks. Hussain et al. [6] proposed a framework for classifying the DoS attacks based on the header contents, the transient ramp-up behaviors and the spectral analysis, and presented a statistical analysis for the DoS attacks and came up with some defense mechanisms, a useful study of quantifying the dynamics of DoS attacks.

However, only a few available works have employed rigorous mathematical models to analytically study the DoS attacks. This motivates us in this paper to develop some more general mathematical models (such as queueing models) to analyze the DoS attacks. Along this line, Chang [4] mentioned a simple queueing model for the SYN flooding attack, which is one of the most common DoS attacks. Long et al. [7] proposed two queueing models for the DoS attacks in order to obtain the packet delay jitter and the loss probability. Khan and Traore [8] analyzed the impact of DoS attacks on three parameters: the arrival rate, the queue-growth-rate, and the response time, which were used for the attack detection. Huang et al. [10] used a generalized multi-class Erlang and Engset mixed loss model to analyze the DDoS attacks, which was later extended for 3G wireless cellular networks [11]. Different from these works in the literature, our paper studies the DoS attacks analytically by using a more general queue model, a two-dimensional embedded Markov chain, which can more accurately capture the dynamics of the actual DoS attacks.

The main contributions of this paper are twofold. The first one is the theoretical model for the study of the DoS attacks, which is motivated by a few available results on quantitative analysis of the DoS attacks. We propose a two-dimensional queueing model to evaluate the system performance of a computer network under DoS attacks. The queueing model of this paper is novel because we model the system with two requesting queues for regular requests and the attack requests with different service time distributions. In this model, all connection requests share the same backlog queue, and each request immediately receives a buffer space of the backlog queue once it arrives at the system upon finding an idle buffer space and is blocked otherwise. The difficulty in the analysis lies in the fact that the regular requests and the attack requests behave differently, e.g., their buffer occupancy times will have different probability distributions. Therefore, we can only use the two-dimensional embedded Markov chain to characterize the DoS attacks. The second contribution of the paper is to compute the stationary probability distribution of the embedded Markov chain, from which we can com-