Computers & Security (2006) **25**, 213–220

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

Change trend of averaged Hurst parameter of traffic under DDOS flood attacks

Ming Li*

School of Information Science and Technology, East China Normal University,
No. 3663, Zhongshan Bei Road, Shanghai 200026, PR China

Received 22 November 2004; revised 15 November 2005; accepted 15 November 2005

KEYWORDS
Hurst parameter;
Traffic;
Time series;
Distributed denial-of-service flood attacks;
Anomaly detection

Abstract Distributed denial-of-service (DDOS) flood attacks remain great threats to the Internet though various approaches and systems have been proposed. Because arrival traffic pattern under DDOS flood attacks varies significantly away from the pattern of normal traffic (i.e., attack free traffic) at the protected site, anomaly detection plays a role in the detection of DDOS flood attacks. Hence, quantitatively studying statistics of traffic under DDOS flood attacks (abnormal traffic for short) are essential to anomaly detections of DDOS flood attacks.

References regarding qualitative descriptions of abnormal traffic are quite rich, but quantitative descriptions of its statistics are seldom seen. Though statistics of normal traffic are affluent, where the Hurst parameter *H* of traffic plays a key role, how *H* of traffic varies under DDOS flood attacks is rarely reported. As a supplementary to our early work, this paper shows that averaged *H* of abnormal traffic usually tends to be significantly smaller than that of normal one at the protected site. This abnormality of abnormal traffic is demonstrated with test data provided by MIT Lincoln Laboratory and explained from a view of Fourier analysis.

Introduction

The Internet is the infrastructure that supports computer communications. It has actually become the ''electricity'' of the modern society because its use in modern society is so pervasive and many people rely on it so heavily. For instance, employees in the modern society would rather give up access to their telephone than give up their access to their email. Nevertheless, it is subject to electronic attacks (Coulouris et al., 2001), e.g., distributed denial-of-service (DDOS) flood attacks (Sorensen, 2004). The threats of DDOS attacks to the individuals are severe. For instance, any denial-of-service of a bank server implies a loss of money, disgruntling or losing customers. Hence, intrusion

* Tel.: +86 21 62233389; fax: +86 21 62232517.
E-mail addresses: mli@ee.ecnu.edu.cn, ming_lihk@yahoo.com.
URL: http://www.ee.ecnu.edu.cn/teachers/mli/js_lm(Eng).htm.

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.11.007

detection system (IDS) and intrusion prevention system (IPS) are desired (Kemmerer and Vigna, 2002; Householder et al., 2002; Schultz, 2004; Sorensen, 2004; Gong, 2003; Li, 2004; Streilein et al., 2003; Bencsath and Vajda, 2004; Feinstein et al., 2003; Oh and Lee, 2003; Liston, 2004).

There are several categories of denial-of-service (DOS) attacks (Gong, 2003). The CERT Coordination Center (CERT/CC) divides DOS attacks into three categories: (1) flood (i.e., bandwidth) attacks, (2) protocol attacks, and (3) logical attacks. This paper considers flood attacks.

A DDOS flood attack sends attack packets upon a site (victim) with a huge amount of traffic, the sources of which are distributed over the world so as to effectively jam its entrance and block access by legitimate users or significantly degrade its performance. It never tries to break into the victim's system, making security defenses at the protected site irrelevant (DDoS; Dittrich-a; Dittrich-b; Dittrich-c; Dittrich-d; Dietrich et al.; Geng et al., 2002).

Usually, IDSs are classified into two categories. One is misuse detection and the other anomaly detection. Solutions given by misuse detection are primarily based on a library of known signatures to match against network traffic. Hence, unknown signatures from new variants of an attack mean 100% miss. Therefore, anomaly detectors play a role in detection of DDOS flood attacks. As far as anomaly detection is concerned, quantitatively characterizing abnormalities of statistics of abnormal traffic is fundamental.

A traffic stream is a packet flow. A packet consists of a number of fields, such as protocol type, source IP, destination IP, ports, flag setting (in the case of TCP or UDP), message type (in the case of ICPM), timestamp, and data length (packet size). Each may serve as a feature of a packet. The literature discussing traffic features is rich (see e.g. Li, 2004; Streilein et al., 2003; Bencsath and Vajda, 2004; Feinstein et al., 2003; Oh and Lee, 2003; Cho and Park, 2003; Cho and Cha, 2004; Lan et al., 2003; Paxson and Floyd, 1995; Li et al., 2003; Beran, 1994; Willinger and Paxson, 1998; Willinger et al., 1995; Csabai, 1994; Tsybakov and Georganas, 1998; MIT; Garber, 2000; Kim et al., 2004; Mahajan et al., 2002; Kim et al., 2004; Bettati et al., 1999). For instance, Mahajan et al. (2002) consider flow rate, Kim et al. (2004) use head message, Oh and Lee (2003) alone consider 86 features of traffic (not from a statistics view though), and so on. To the best of our knowledge, however, taking into account the Hurst parameter H in characterizing abnormality of traffic series in packet size under DDOS flood attacks is rarely seen except for Li (2004), where autocorrelation function (ACF) of traffic series in packet size (traffic for short) with long-range dependence (LRD) is taken as its statistical feature. As a supplementary to Li (2004), this paper specifically studies how H of traffic varies under DDOS flood attacks. In this regard, the following two questions are fundamental.

(1) Whether H of traffic when a site is under DDOS flood attacks (abnormal traffic for short) is significantly different from that of normal one (i.e., attack free traffic)?
(2) What is the change trend of H of traffic when a site suffers from DDOS flood attacks?

We will give the answers to the above questions from the point of views of processing data traffic and theoretic inference and analysis.

In the rest of paper, section ''Test data sets'' is about test data. We brief data traffic and use a series of normal traffic in ACM to explain how its H normally varies in section ''Brief of data traffic''. The answer to the question (1) is given in section ''Using H to describe abnormality of traffic under DDOS flood attacks''. Then, in section ''Change trend of traffic under DDOS flood attacks'', we use a pair of series (one is normal traffic and the other abnormal one) that is provided by MIT Lincoln Laboratory to demonstrate that averaged H of abnormal traffic tends to be significantly smaller than that of normal one and briefly discusses this abnormality of abnormal traffic from a view of Fourier analysis. The answer to the question (2) is given in this section. Section ''Conclusions'' concludes the paper.

Test data sets

Three series of test data are utilized in this paper. The first one is an attack free series measured at the Lawrence Berkeley Laboratory from 14:00 to 15:00 on Friday, 29 January 1994. It is named LBL-PKT-4, which has been widely used in the research of general (normal traffic) traffic pattern (see e.g. Paxson and Floyd, 1995; Li et al., 2004). We use it to show a case how H of normal traffic varies. The second is Outside-MIT-week1-1-1999-attack-free (OM-W1-1-1999AF for short) (MIT). It was recorded from 08:00:02, 1 March (Monday) to 06:00:02, 2 March (Tuesday), 1999. The third is Outside-MIT-week2-1-1999-attack-contained (OM-W2-1-1999AC for short) (MIT), which was collected from 08:00:01, 8 March (Monday) to 06:00:49, 9 March (Tuesday), 1999. Two MIT series are used to