The Journal of Systems and Software 86 (2013) 211–221

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

Chaos-based detection of LDoS attacks☆

Wu Zhi-jun[a,*], Lei Jin[a], Yao Di[a], Wang Ming-hua[b], Sarhan M. Musa[c]

[a] Tianjin Key Laboratory for Advanced Signal Processing, Civil Aviation University of China, No. 2898, Jinbei Rd., Dongli District, Tianjin 300300, China[1]
[b] China Computer Emergency Response Team (CNCERT), Beijing 100029, China[2]
[c] Engineering Technology Department, Prairie View A&M University, TX 77446, USA[3]

ARTICLE INFO

Article history:
Received 16 February 2012
Received in revised form 18 June 2012
Accepted 25 July 2012
Available online 18 August 2012

Keywords:
Chaos
LDoS
Duffing oscillator
Detection

ABSTRACT

A low-rate denial of service (LDoS) attack behaves as a small signal in periodic pulses with low average rate, which hides in normal TCP traffic stealthily. LDoS attacks reduce link throughput and degrade QoS of a target. An approach of detecting LDoS attacks is proposed based on Duffing oscillator in chaos systems. The approach detects LDoS attacks by adopting the technology of digital signal processing (DSP), which takes an LDoS attack as a small signal and normal TCP traffic as background noise. Duffing oscillator is used to detect LDoS attacks in normal TCP traffic. Simulations show that the LDoS attacks can be detected through diagram of the chaotic state, and the period and pulse width of LDoS attacks can be estimated.

1. Introduction

Low-rate denial of service (LDoS) attacks exploit TCP's retransmission time-out (RTO) and additive increase and multiplicative decrease (AIMD) mechanism to send periodic burst pulses of attack packets. An LDoS attacker makes a target system consecutively switching between states of overload and underload and degrades the quality of service (QoS) seriously. An LDoS attack with single source is modeled by a square waveform with an attack period of $RTOmin + 2RTT$, burst length of L, and the burst rate of R, as shown in Fig. 1 (Macia-Fernandez et al., 2009).

The period of $RTOmin + 2RTT$ is the time interval between two consecutive attack pulses. The burst length of L indicates the pulse width, during which attackers send packets with high rate in one period. The peak rate of R exhibits the height of attack burst, i.e., the strength of attack flow. The period of $RTOmin + 2RTT$ is calculated by estimating the value of TCP RTO timer at the end of trust sources. The attack pulses create a busty and severe congestion on the links to the victim during the burst with a peak rate of R. The legitimate TCP flows make the sending rate decrease due to the control of rate-limiting mechanism.

Fig. 1 shows that an LDoS attack is a sequence of pulses with certain period and pulse width. The average volume of attack traffic is determined by RL/T, which is much lower than normal TCP traffic (Macia-Fernandez et al., 2009). Furthermore, it is well known that more than 90% of traffic on Internet today is using TCP protocol (Proano and Lazos, 2012). Research indicates that the number of packets in a TCP flow is quite bigger than that of an LDoS attack flow. Hence, from the viewpoint of signal processing, an LDoS attack can be defined as a small periodical signal, and TCP flow is background noise. Statistics on three days network traffic that sampled from university campus is classified by protocols as shown in Table 1.

Consequently, the detection theory for a small signal can be used for detecting LDoS attacks from normal TCP traffic. This paper proposes a detection approach of LDoS attack based on a chaotic system, which is very sensitive to small deterministic signal and immune to background noise. It is practical to detect LDoS attacks in network traffic by using the theory of chaos system. The chaos-based detection of LDoS attacks to extract the signatures of LDoS attacks from the instability and unbalances of chaos system with a lower detection threshold (Nie and Wang, 2011).

2. Related works

At present, there are many researches on detection of LDoS attacks. Zhang et al. (2010) proposed a random early detect (RED) algorithm to counter LDoS attacks. Xiang et al. (2011) presented

☆ Part of this paper was first appear in "The detection of LDoS attack based on Duffing chaos system", which is published on the proceedings of 2011 international conference on information theory and information security. This work was supported in part by National Natural Science Foundation of China under grant 61170328, and Natural Science Foundation of Tianjin under grant 12JCZDJC20900.

* Corresponding author.
E-mail addresses: zjwu@cauc.edu.cn (Z.-j. Wu), jlei@cauc.edu.cn (J. Lei), yaodi_cauc@163.com (D. Yao), wmh@cert.org.cn (M.-h. Wang), smmusa@pvamu.edu (S.M. Musa).

[1] http://www.cauc.edu.cn.
[2] http://www.cert.org.cn.
[3] http://www.pvamu.edu.

0164-1212/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2012.07.065

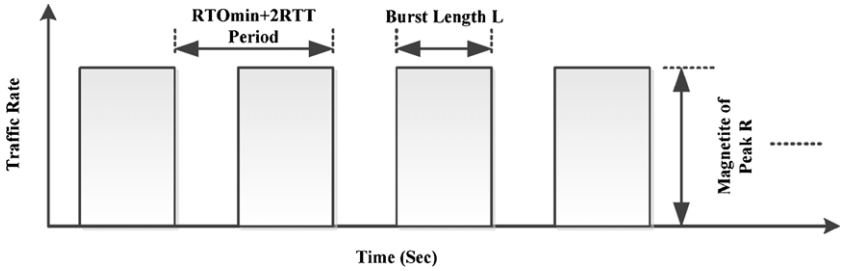

Fig. 1. Model of LDoS attack traffic.

Table 1
Classification of traffic on Internet.

Date	Size (Mb)	TCP (%)	ICMP (%)	UDP (%)
08/11	30.5	91.6%	0.91%	7.61%
08/12	48.4	91.2%	0.91%	7.54%
08/13	41.6	93.1%	0.65%	6.02%

an approach of LDoS attacks detection and traceback by using new information metrics. Tang and Cheng (2011) researched quick detection of stealthy SIP flooding attacks in VoIP networks. Kwong et al. (2005) proposed an new stateful adaptive queue management technique called HAWK (Halting Anomaly with Weighted choKing) which identifies malicious shrew packet flows using a small flow table and dropping such packets decisively to halt the attack, so that well-behaved TCP sessions can re-gain their bandwidth shares.

DSP technology has been widely applied in the field of communications, navigation and surveillance. In recent years, DSP technology has been extended to the Internet network traffic analysis, especially for network security (Carl et al., 2006). The available methods are using the technologies of signal processing or wavelet analysis to extract the characteristics of attack flows for the purpose of detecting LDoS attacks. Abnormal flow in the network can be observed through the signal processing or wavelet analysis. At present, there are two kinds of methods to detect LDoS attacks by adopting DSP technology. One is wavelet-based detection of DoS attacks (Dainotti et al., 2006), and the other is using spectral analysis in detection and defense against DoS attacks (Cheng et al., 2002). The methods of wavelet and spectral analysis are discussed as follows individually.

In the wavelet-based detection of DoS attacks, Dainotti et al. (2006) proposed an automated system to detect volume-based anomalies in network traffic caused by DoS attacks. The system has a two-stage architecture combining more traditional approaches (Adaptive Threshold and Cumulative Sum) with a novel one based on the Continuous Wavelet Transform (CWT). This system obtained good results in terms of tradeoff between correct detections and false alarms, estimation of anomaly duration, and an ability to distinguish between subsequent anomalies. Huang et al. (2006) developed and implemented a Waveman framework for real time wavelet-based analysis of network traffic anomalies. They used two metrics, percentage deviation and entropy to evaluate the performance of various wavelet functions on detecting different types of anomalies like DoS attacks and portscans. Shinde and Guntupalli (2007) proposed a method that considers the network traffic as a time-series and smoothens it by using exponential moving average and analyzes the smoothened wave by using energy distribution based on wavelet analysis. By analyzing the energy distribution in the wavelet form of a smoothened time-series, and the growth in the traffic indicates that is a DoS attack. Suen et al. (2010) applied diffusion wavelets to project the high dimensional data onto a low-dimensional space according to the correlations between various attributes. And they proposed a leverage system which can differentiate DoS attacks from legitimate web-access requests. He and Cao (2009) proposed a Detection System Based on Wavelet Analysis (DSBWA) to detect LDoS attacks. This system is designed and implemented based on feature extraction using wavelet transform. The proposed system focuses on the number of arriving packets at the monitoring node, and extracts five feature indices of LDoS flows through wavelet multi-scale analysis of network traffic. Then a synthesis diagnosis is made by a trained BP neural network. Once the LDoS attack is determined, the information related to attacks can be got by locating malicious pulses. Salagean and Firoiu (2010) proposed a detection mechanism of abnormal network traffic based on Analytical Discrete Wavelet Transform (ADWT) and high-order statistical analysis. A set of features based on different metrics is used in this mechanism.

In spectral analysis, all the operations used for detection and defense against DoS attacks are completed in frequency domain. As early as Petropulu and Nowak (2002) focused on an exciting new area of signal processing and devoted to the study, modeling, and analyzing networks and network traffic. Barford et al. (2002) reported signal analysis results of four classes of network traffic anomalies: outages, flash crowds, attacks and measurement fail. Cheng et al. (2002) proposed an approach by using spectral analysis to identify normal TCP traffic in order to defense against DoS attacks. This approach adopts the number of arriving packets within fixed-length time intervals in a flow as the signal, and estimates the power spectral density (PSD) of this signal. In the signal, the information of periodicity or lack thereof, reveals itself. Wu and Yue (2008) proposed an approach of detecting LDDoS attacks based on Kalman filter. The error between one step prediction and the optimal estimation is used as the detection criterion in the proposed approach. Chen and Hwang (2006) proposed a character-based method of detecting LDoS attacks in frequency domain. This method obtains the PSD of sampled sequence by using Discreet Fourier Transform (DFT) of autocorrelation function. Then discrimination feature could be set by selecting a normalized PSD accumulation value at a fixed frequency point (like 20 Hz). At last, a normalized judgment value (e.g. 0.6) may be found by using the likelihood function. However, this method is featured with large computation and low detection rate (around 88.0%). Furthermore, there is a certain degree of missed alarm probability and false alarm probability.

In this paper, a chaos-based approach is proposed to detect LDoS attack by using the technology of weak signal detection. In the previous literatures, many attentions were paid on detecting weak sinusoidal signals by analysis of chaotic data series. In this paper, the target signals to be detected are small periodic square pulses.

3. Analysis of LDoS attack traffic

As shown in Fig. 1, the LDoS attacker sends bursts with the duration of L and the rate of R in a deterministic on-off pattern with a period of T. Hence, the model of LDoS attacks is a set of three elements $\{R, L, T\}$, in which R is the rate, large enough to induce loss