Traffic Characterization of the Web Server Attacks of Worm Viruses

Kihun Chong, Ha Yoon Song, and Sam H. Noh

School of Information and Computer Engineering, Hongik University
{khchong, song, noh}@cs.hongik.ac.kr

Abstract. With the explosive popularity of the Internet, the number of accessible web servers has proliferated as well. Subsequently, malicious attacks on these servers via viruses have become more prevalent. Due to the self-propagation and self-duplication nature of these viruses, such attacks can congest the network quickly, aggravating the already limited bandwidth available and curtail service provided by the server, eventually leading to denial of all services. The IIS, in particular, has been gravely affected by such Denial of Service (DoS) attacks. Hence, various methods to prevent such attacks from affecting the network and server have been researched and proposed. In this paper, we analyze the characteristics of worm virus attack traffics, by extracting and analyzing virus attack logs. With the use of various statistical methods, we show that worm attack patterns show self-similarity with Hurst parameter H . Our purpose is to use this characteristic in annulling the negative effects of worm attacks.

1 Introduction

The number of the web servers has proliferated with the explosive popularity of Internet, especially with the advent of the World Wide Web (WWW) and its various services. Simultaneously, computer virus attacks on web servers over the Internet have also increased. Due to viruses' characteristic to self-propagate, the number of attacking packets of viruses tend to increase exponentially, eventually leading to network congestion. Web servers, the IIS in particular, are usual victims of such Denial of Service (DoS) attacks. It is imperative to recognize the pattern of such virus attacks in order to take measure to defend from such attacks.

It has been well known that network traffic shows self-similarity. It is also well known that the WWW traffic shows self-similar characteristics[1]. However, there have been little research on self-similar characteristics of traffic generated by viruses that attack web servers. So, we analyzed the viruses' requests that attack web servers and measured whether the distribution of those requests seems to be self-similar. The requests of viruses are a subset of the total requests to web servers and the distribution of the total requests for web servers are self-similar. Hence, checking to see whether the distribution of the requests of viruses that attack web servers are self-similar is an interesting endeavor, as if it is so, this characteristic could be used to defend against such attacks. We analyzed

and measured the requests of the worms which attack the IIS using the logs made by the Apache web server. We were able to verify that the distribution of worms' requests are self-similar with self-similarity parameter H , that is, the Hurst parameter,.

The rest of this paper is organized as follows. The next section reviews related works. Section 3 introduces self-similarity and summarizes statistical tests for self-similarity. Section 4 describes worm viruses' properties and attacking pattern. We analyze the real data of logs of attacking web server in Section 5 and conclude with directions for future research in Section 6.

2 Related Works

There are a considerable number of statistical studies about traffics of network and WWW [1][2]. Early studies are about the self-similarity of network traffics, e.g. LAN, WAN, etc. [2][3], and later studies are about the self-similarity of WWW traffics [1], video stream traffics [4], wavelets [5], etc. For viruses, vaccines are made in general by analyzing occurrence day, properties, and factors of danger, and a real state of worms, recently run actively, is researched about the ways of attacks and recovery [6][7]. Therefore, the work presented here is different from existing studies that serves as a means to cure the viruses in that the study of traffic patterns of worm's attacking web servers is presented as a starting point to safeguard servers from worm attacks. There are two basic related topics that relate to our research: fractal and self-similarity.

2.1 Fractal

Fractal is something that has characteristics of *self-similarity* and *recursiveness* [8]. Fractal's characteristic can be derived from a Fractal diagram. A Fractal diagram is similar to its sub-diagram and its area is finite but its circumference is infinite.

2.2 Self-Similarity

Self-similarity follows the self-similarity and recursiveness properties of a Fractal. A self-similar object is also similar to its subset from a statistical view. It manages a time process or a time series with time parameter t as shown in figure 1. Figure 1 shows a sort of network traffic and it is similar to a Fractal diagram with the change of the scale of time unit. This characteristic is called Self-similarity.

3 The Mathematics of Self-Similarity

We will summarize the mathematical and statistical techniques regarding self-similarity that will be used to analyze the traffic patterns of worm attacks.

3.1 Mathematical Foundation of Self-Similarity

Stationarity and second-order self-similarity are theoretical basis underlining self-similarity. This subsection describes the mathematical and statistical foundations of *stationarity* and the *derivation of self-similarity* [9].

Stationarity and Second-order Stationarity. We denote the time series as follows.

$X(t)$ is time series, where $t \in N$ and N is a natural number.

We denote the time series with a cumulative parameter of time t as $Y(t)$. We will then reserve $X(t)$ to be the increment process corresponding to $Y(t)$, that is,

$$X(t) = Y(t) - Y(t - 1) . \quad (1)$$

For traffic modeling purposes, $X(t)$ has to be *stationary*, which means that the behavior and structure of $X(t)$ are the same as one that is shifted in some time. $X(t)$ is strictly stationary if $(X(t_1), X(t_2), \dots, X(t_n))$ and $(X(t_{1+1}), X(t_{2+1}), \dots, X(t_{n+1}))$ has the same joint distribution for all $n, t_n, k \in Z$. Hence, when we denote X_k as the k -shifted time process or time series, X and X_k are said to be equivalent in the sense of finite-dimensional distributions, and we denote it as follows.

$$X =_d X_i . \quad (2)$$

Stationarity is too strict to implement in real processes, henceforth a weaker form of stationarity is used in general and is called *second-order stationarity*. Second-order stationarity is weaker than stationarity, and it requires the *autocovariance function* as follows.

$$\gamma(r, s) = E [(X(r) - \mu) (X(s) - \mu)] . \quad (3)$$

When $\gamma(r, s)$ has to satisfy the *translation invariance* as follows.

$$\gamma(r, s) = \gamma(r + k, s + k) \quad (\text{for all } r, s, k \in Z) . \quad (4)$$

Suppose that there are r, s which are finite, and we set $\mu = E[X(t)]$, $\rho^2 = E[(X(t) - \mu)^2]$ for all $t \in Z$. And also assume $\mu = 0$, then $\gamma(r, s) = \gamma(r - s, 0)$ by stationarity, and it is denoted the autocovariance by $\gamma(k)$.

We define $X^{(m)}$, the aggregated process of X at aggregation level m , to formulate scale invariance as follows.

$$X^{(m)}(i) = \frac{1}{m} \sum_{t=m(i-1)+1}^{m \times i} X(t) . \quad (5)$$

That is, $X(t)$ is partitioned into nonoverlapping blocks of size m , their values are averaged and i is used to index these blocks. We denote $\gamma^{(m)}(k)$ to be the autocovariance function of $X^{(m)}$. Under the supposition of this second-order stationarity, we can define the second-order self-similarity.

Second-order Self-similarity. $X(t)$ is *second-order self-similar* with Hurst parameter H if

$$\gamma(k) = \frac{\rho^2}{2}((k+1)^{2H} - 2k^{2H} + (k-1)^{2H}) . \quad (6)$$

where $\gamma(k)$ is the autocovariance function of $X(t)$, ρ^2 is the variance of $X(t)$ and H is *Hurst parameter*. And $X(t)$ is *asymptotically second-order self-similar* when $X(t)$ satisfies the following.

$$\lim_{m \rightarrow \infty} \gamma^{(m)}(k) = \frac{\rho^2}{2}((k+1)^{2H} - 2k^{2H} + (k-1)^{2H}) . \quad (7)$$

Distributional Self-similarity. Consider the cumulative process $Y(t)$ mentioned in section 3.1. $Y(t)$ is *self-similar with self-similarity parameter H* ($0 < H < 1$), that is, the Hurst parameter, denoted H -ss, if

$$Y(t) =_d a^{-H} Y(at) \quad (\forall a, t, \quad a > 0, t \geq 0) . \quad (8)$$

That is $Y(t)$, and its time scaled and normalized version have the same distribution. Suppose $Y(t)$ has these finite variances as follows.

$$\begin{aligned} E[Y(t)] &= 0, \\ E[Y^2(t)] &= \rho^2 |t|^{2H}, \\ \gamma(k) &= \frac{\rho^2}{2} (|t|^{2H} - |t-s|^{2H} + |s|^{2H}) \end{aligned}$$

Thus, $Y(t)$ can be defined as follows.

$$Y(t) =_d t^H Y(1) \quad (Y(t) =_d a^{-H} Y(at), \quad t = 1, a = t) . \quad (9)$$

And also suppose $X(t)$, we can show $X^{(m)}$ as follows.

$$\begin{aligned} X^{(m)} &= \frac{1}{m} \sum_{i=1}^m X(t) \\ &= m^{-1} (Y(m) - Y(0)) \\ &=_d m^{-1} m^H (Y(1) - Y(0)) \\ &= m^{H-1} X . \end{aligned}$$

Therefore, if $Y(t)$ shows H -self-similarity and has *stationarity increments*, denoted H -sssi, then its increment process $X^{(m)}$ satisfies the following.

$$X^{(m)} =_d m^{H-1} X \quad (10)$$

And $X(t)$ is *exactly self-similar* or *asymptotically self-similar* if

$$\lim_{m \rightarrow \infty} =_d m^{H-1} X \quad (11)$$

for all $m, m \geq 0$. In this paper, we say that X is self-similar with parameter H when X satisfies the following.

$$X_t =_d m^{-H} \sum_{i=(t-1)m+1}^m X_i \quad (\text{for all } m \in \mathbb{N}) \quad (12)$$

And also, a time series X is self-similar with parameter H if it and $X^{(m)}$ have the same *autocorrelation function*, $\gamma(k) = \frac{E[(X_i - \mu)(X_{i+k} - \mu)]}{\rho^2}$. Thus, parameter H has to satisfy the following.

$$\frac{1}{2} < H < 1 \quad (13)$$

3.2 Statistical Tests for Self-Similarity

This section presents statistical methodologies for self-similarity. These statistical methodologies are variance-time plot, R/S plot, periodogram, etc. [1].

Variance-time plot. $\text{var}(X^{(m)})$, the variance of $X^{(m)}$ for large number m , is plotted against m on a log-log plot. Suppose β is an approximate slope of the plotted distribution, and H satisfies $H = 1 - \beta/2$. Then $X^{(m)}$ is self-similar with parameter H if $\frac{1}{2} < H < 1$.

R/S plot. The rescaled version $X^{(m)}$ by R/S is plotted against n on a log-log plot. R and S are denoted as follows.

$$\begin{aligned} S(n) &= \sqrt{\text{var}(X^{(m)})}, \\ R(n) &= [\max(0, W_1, W_2, \dots, W_n) - \min(0, W_1, W_2, \dots, W_n)] \\ &\quad (W_k = (X_1 + X_2 + \dots + X_k) - k\bar{X}(n), \quad k = 1, 2, \dots, n) \end{aligned}$$

Thus, H is the estimated slope of the graph on a log-log plot, and $X^{(m)}$ is self-similar with parameter H if $\frac{1}{2} < H < 1$.

Periodogram. The periodogram is plotted on a log-log plot. A periodogram can be formulated as follows.

$$I(\lambda) = \frac{1}{2\pi N} \left| \sum_{j=1}^N X_j e^{ij\lambda} \right|^2 \quad (14)$$

where λ is a period and N is the number of series. Suppose β is an approximate slope of the plotted distribution, and H satisfies $H = 1 - \beta/2$. Then, $X^{(m)}$ is self-similar with parameter H if $\frac{1}{2} < H < 1$.

4 Worm Attacks against the Web Server over the Internet

Worm attacks against general servers as well as web servers have increased tremendously. In particular, the Internet Information Server (IIS) [10] is the most popular target of these web server attacks. IIS is a product of Microsoft and runs on the Windows operating system. Hackers frequently choose the IIS as their target due to its weak security. Though IIS provides security measures as fast as possible, new attacks continue to appear as rapidly as these new measures are provided.

A typical attack method of a virus is to infect the system and attack the file system. However, in recent years, the attacks are inflicted so that the infected system also becomes an attacker inflicting harm to neighboring systems or thereby congesting the network itself. Virus attacks on web servers also take this form, infecting all of clients connected to the infected web server or attacking the web server by a Denial of Service (DoS) attack. For example, Code Red and Nimda Worm(W32/Nimda worm) are a couple of the more well known notorious ones. Particularly, the Nimda worm, which appeared later than Code Red, acts intelligently by searching the back door, which was made by the Code Red virus. The attack patterns of the Nimda worm are described as follows.

```
(1) GET /scripts/root.exe?/c+dir
(2) GET /MSADC/root.exe?/c+dir
(3) GET /c/winnt/system32/cmd.exe?/c+dir
(4) GET /d/winnt/system32/cmd.exe?/c+dir
(5) GET /scripts/..%5c../winnt/system32/cmd.exe?/c+dir
...
(6) GET /scripts/..%2f../winnt/system32/cmd.exe?/c+dir
```

The attack logs between line (1) and line (4) are attempts to search the back door made by the Code Red virus and the other logs are to attack the weakness of the directory traversal.

5 Characterization of Worm Attack Traffics

We used log data that was made by the Apache web server of the Department of Computer Engineering, Hongik Univ. This section describes information of log data and the web server system, and explains the results of the data analysis.

5.1 Collection of Worm Attack Traffic Logs

The almost attacks against web servers are concentrated onto the MS Windows and IIS, and cannot attack UNIX systems and the Apache web server [11]. The failed worm virus attacks are written on the log files of the Apache web server, thus we could collect a large amount of logs. The size of raw log data is 343MB

and the size of attack data is 13MB. The web server system runs on the Apache version 1.3.9 on the SUN SPARC station-10 using UNIX System V release 4.0 (SunOS 5.5). The duration for gathering the log data is from 10/1/2001 00:00 to 2/28/2002 24:00.

5.2 Self-Similarity of Worm Attack Traffics

Figure 1 shows the distribution of the log data at time unit 1, 10, 100, and 1000 of worm attack traffic patterns. The x -axis is for time and y -axis is for the number of attacks at time x . We can see that the distributions of each time unit are all similar in Figure 1. It seems to show that the distribution pattern of web server attacks is self-similar.

Fig. 1. The measured frequency of worm attacks over time domain.

Figure 2 shows a variance-time plot. The dotted line is the value of the variance and the solid line is the approximate line calculated by the method of least squares. We found the value of β on a log-log plot to be 0.65 and the value of parameter H to be 0.67.

Figure 3 shows a R/S plot. In Figure 3, concentrated plotting of dots express the value of r/s , and the value of n on the x -axis is the same as the value of m

Fig. 2. Variance-time plot of worm attack traffic.

at $X^{(m)}$. The slopes of the two lines above and under the dots are 0.5 and 1, respectively, showing that H is between 0.5 and 1. The real value of parameter H is 0.57.

Finally, Figure 4 shows a periodogram. The dots represent the values of the periodogram, and the line among dots is the approximate line identified by the least squares method. The value of the slope of β is 0.11, and so the value of parameter H is 0.94.

All three methods shown that parameter H satisfies the condition $\frac{1}{2} < H < 1$. Therefore we may safely conclude that the attack pattern of worm viruses is self-similar with parameter H .

6 Conclusions and Future Works

In this paper, we have analyzed the request distribution of attacking web servers by worm viruses. From the fact that most of the worm attacks are concentrated on the IIS of Windows platforms, we could collect logs of worm attacks on the Apache web servers on UNIX systems. These logs were analyzed to obtain the characteristics of the attacks. We used statistical methods, e.g. variance-time plot, R/S plot and periodogram to test for self-similarity. We found the request distribution of worm attacks is self-similar with parameter H . Therefore we can determine worm attacks and defend against such attacks by using the value of parameter H .

For the future works, we plan to consider the possibility of detecting worm attacks in real time by using parameter H , thereby blocking or taking appropriate action to such attacks as it happens.

Fig. 3. R/S plot of worm attack traffic.

Fig. 4. Periodogram of worm attack traffic.

References

1. Mark E. Crovella and Azer Bestavros. Self-similarity in World Wide Web traffic: evidence and possible causes. *IEEE/ACM Transactions on Networking*, 5(6):835–846, December 1997.

2. Walter Willinger, Murad S. Taqqu, Robert Sherman, and Daniel V. Wilson. Self-similarity through high-variability: statistical analysis of Ethernet LAN traffic at the source level. *IEEE/ACM Transactions on Networking*, 5(1):71–86, February 1997.
3. Boris Tsybakov and Nicoals D. Georganas. On self-similar traffic in ATM queues: definitions, overflow probability bound, and cell delay distribution. *IEEE/ACM Transactions on Networking*, 5(3):397–409, June 1997.
4. Mark W. Garrett and Walter Willinger. Analysis, modeling and generation of self-similar vbr video traffic. In *Proceedings of ACM SIGCOMM 94*, pages 269–280, 1994.
5. Patrice Abry and Darryl Veitch. Wavelet analysis of long-range-dependent traffic. *IEEE Trans. Information Theory*, 44(1):2–15, January 1998.
6. Korea Information Security Agency. <http://www.kisa.or.kr>.
7. Ahnlab, Inc. <http://www.ahnlab.com>.
8. Benoit B. Mandelbrot. *The Fractal Geometry of Nature*. W.H. Freeman & Company, New York, 1977.
9. Peter J. Brockwell and R. A. Davis. *Time Series: Theory and Methods (Springer Series in Statistics)*. Springer Verlag, New York, February 1991.
10. Microsoft Corporation. Internet Information Services Features. <http://www.microsoft.com/windows2000/server/evaluation/features/web.asp>.
11. Apache Software Foundation. The Apache Web Server. <http://www.apache.org>.