주식시장 기술 분석 기법을 활용한 DDoS 탐지 방법

DDoS detection method based on the technical analysis used in the stock market

윤 정 훈*, 정 송**
Junghoon Yun, Song Chong

Abstract

We propose a method for detecting DDoS (Distributed Denial of Service) traffic in real-time inside the backbone network. For this purpose, we borrow the concepts of MACD (Moving Average Convergence Divergence) and RoC (Rate of Change), which are used for technical analysis in the stock market. Due to the fact that the method is based on a quantitative, rather than a heuristic, detection level, DDoS traffic can be detected with greater accuracy (by reducing the false alarm ratio). Through simulation results, we show how the detection level is determined and demonstrate how much the accuracy of detection is enhanced.

Keywords : DDoS traffic detection, flash event traffic, divergence, momentum, rate of change.

I. Introduction

Detecting DDoS traffic is a challenging issue for network operators, since DDoS traffic has malicious intention to break down the network [1].

This issue has been addressed in a number of papers by detecting abnormal traffic or patterns in the network. Throughout the letter, we will use both terms of abnormal traffic and DDoS traffic interchangeably. In [2], the authors try to detect abnormal traffic by using time-series analysis. The method uses both an expectation value that is calculated using an exponential smoothing and confidence band. If incoming traffic lies within the confidence band, it is regarded as normal, while if it lies outside the confidence band, it is regarded as abnormal. This method has a very simple detection mechanism. However, it has the drawback that it depends to a great extent on the width of confidence band. This has the consequence that if the assigned confidence band is too narrow, there may be positive false alarms, while if the assigned confidence band is too wide, abnormal traffic patterns may not be detected so that there may also exist negative false alarms.

In [3], the authors suggest an entropy-based detection method. The method uses the idea that when DDoS traffic passes through the network, a lot of unusual source IP addresses, destination IP addresses, source ports, and destination ports are suddenly observed, with the result that the entropy or the uncertainty of each argument eventually increases. The authors say that by detecting such increase in entropy, their method can detect DDoS traffic. This method performs better than the time-series method, but it has a critical drawback: it is unsuitable for use in real time, because it is almost impossible to distinguish and compute the entropy of each source IP, destination IP, source port, and destination port at the speed of packet interarrival. Thus, the method is best suited for forensic examination after problems have occurred.

In this paper, we propose a new method for detecting DDoS traffic. Especially, we mainly focus on the decrease of false alarm ratio by discriminating between DDoS traffic and normal traffic. We assume that the false alarm includes both negative and positive ones and the normal traffic consists of usual and flash event traffic. Flash event traffic is a kind of normal traffic that is caused by legitimate users and does not have any malicious intention to break down the network, even though it has unusually peak traffic volume during very short time period for at most 1 or 2 minutes.

The proposed method is based on the kind of technical analysis used in the stock market, which usually employs two or three critical measures to predict the direction in which the value of stock is moving. Among them, Moving Average Convergence Divergence (MACD) [4] and Rate of Change (RoC) [5]

접수일자 : 2009년 8월 04일
최종완료 : 2009년 8월 14일
*LG-Dacom 기술연구원 (jhyun5235@lgdacom.net)
** EECS, KAIST, Network Systems 연구실

are the most important measures. Details of the usage of the two measures are provided in [4] and [5].

We use these two measures to detect DDoS traffic after modifying them so that they can be applied directly to the packet network environment. The method has a simple structure; hence, it is fast enough for real-time detection. In addition, due to the fact that the proposed method does not use a confidence band, but raw traffic data itself, to detect DDoS traffic, the accuracy of detection is increased. Lastly, since the measures used in the proposed method show a concrete, assessable directional difference when DDoS traffic occurs, the method enables us to determine the threshold for alarm quantitatively. We will demonstrate that the method has all these properties through the simulation results.

II. Problem formulation

1. Divergence & momentum

Divergence in our case is defined as the difference of two time-series. We first show how the divergence is calculated. If we assume y(t) and z(t) to be the two time series and they have different parameters γ and β, respectively, then the divergence, d(t), is defined as follows:

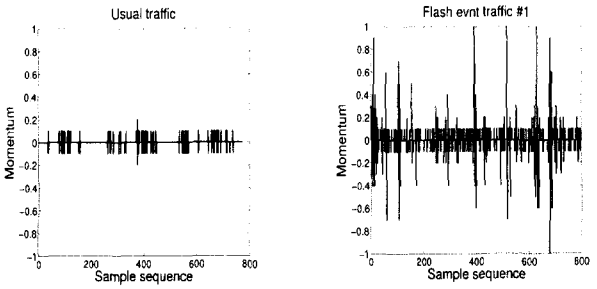
$$\begin{aligned} y(t) &= (1-\gamma)y(t-1)+\gamma x(t), \\ z(t) &= (1-\beta)z(t-1)+\beta x(t), \\ d(t) &= y(t)-z(t). \end{aligned} \quad (1)$$

where $\gamma > \beta$, x(t) is the volume of current traffic, and unit of time, t, is set to 5 minutes throughout the paper. From Eq. (1), by substituting the first and the second equations into the last one, we obtain the momentum, m(t), as follows:

$$\begin{aligned} d(t) &= d(t-1)+\gamma x(t)-\gamma y(t-1)- \\ &\quad \beta x(t)+\beta z(t-1), \\ m(t) &= d(t)-d(t-1)=\gamma e'(t)-\beta e''(t). \end{aligned} \quad (2)$$

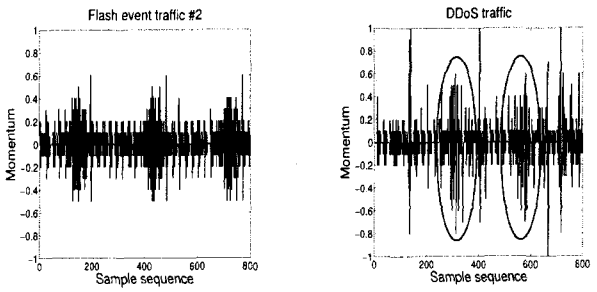
where e'(t)=x(t)-y(t-1) and e''(t)=x(t)-z(t-1).

the momentum can be given an operational definition as follows: the measure that shows both the direction and quantity of the change in the volume of traffic. The traffic volume is measured as packet per second.



In Fig. 1, we show the momentum of various traffic patterns normalized by e''(t). Note from the figures that if the momentum is greater than 0.4, the difference between two time series is greater than 40 %. This result enables us to set the threshold value quantitatively. By determining a percentage of the difference of two time series that is tolerable as normal traffic, the momentum can be set quantitatively with respect to the percentage. We set the threshold for the momentum at 0.4 throughout the paper, since we observed from the results that the momentum of traffic that may be viewed as usual traffic without flash event pattern is not greater than that value.

Fig. 1. Momentum of various traffic patterns (parameters for momentum are set to γ=0.7 and β=0.3, respectively): (a) usual traffic, (b) flash event traffic #1, (c) flash event traffic #2, (d) DDos traffic.



2. Rate of change

Momentum is a good measure for showing whether or not an unusual traffic occurs. However, it is not sufficient for distinguishing between DDoS and flash evnet traffic. The momentum only shows changes in traffic volume; hence, while it tells us that an unusual phenomenon is occurring, it dose not tell us exactly what that phenomenon is, i.e., whether or not it constitutes DDoS traffic. For example, as shown in Fig. 1(b) and Fig. 1(c), when flash event traffic pattern occurs, the momentum may indicate that such traffic is DDoS. But, it must be regarded as normal. In order to compensate this drawback, we employ another important measure, which is called RoC.

The definition of RoC is very simple. RoC calculates the ratio between the current traffic volume and the historical one and is defined mathematically as follows:

$$RoC(t) = \frac{x(t)}{x(t-\tau)} . \quad (3)$$

where τ denotes past time. In general, usual traffic has almost the same pattern over the course of a day. Hence, if DDoS traffic is injected into the network, the duration and the degree of change in traffic volume are relatively long and critical, as shown in Fig. 2(d). However, in the case of flash event traffic, even though it has the similar pattern as DDoS traffic, the deviation in the volume of traffic is not maintained for a long time and the degree of the deviation is not as severe as in the case of DDoS traffic, as shown in Fig. 2(b) and Fig. 2(c).

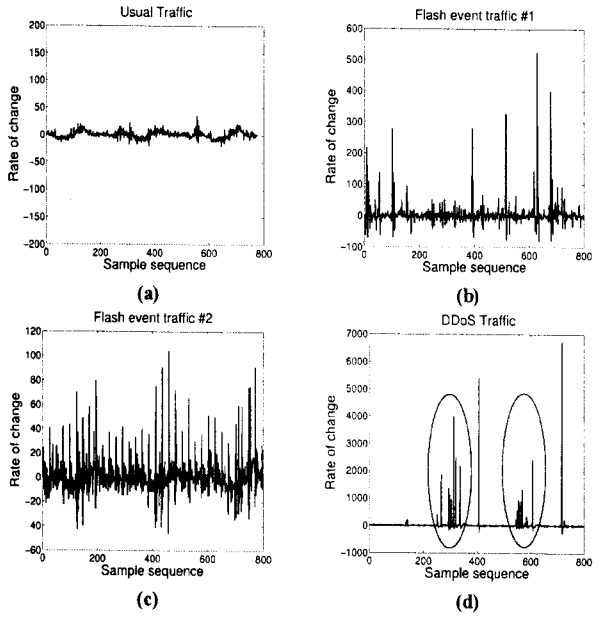


Fig. 2. RoC of various traffic patterns: (a) usual traffic, (b) flash event traffic #1, (c) flash event traffic #2, (d) DDoS traffic.

By using this fact, we distinguish between DDoS traffic and flash event traffic as follows: First, we determine whether or not the RoC value lies beyond the threshold. Secondly, we investigate the duration of unusual pattern of the suspect traffic, by comparing two RoC values of *RoC(t)* and *RoC(t-1)*. If both values are above the threshold, the traffic is deemed to be DDoS. Using the data presented in Fig. 2 as a guide, we set the threshold and τ to 800 and 1, respectively.

III. Simulation result

We now evaluate the performance of the proposed method for detecting DDoS traffic. We mainly focus on the decrease of false alarms between DDoS and normal (usual/flash event) traffic. For this purpose, we first set up the detection algorithm like Algorithm. 1, which has γ=0.7 and β=0.3 for computing the momentum.

Algorithm 1 Detection algorithm

```
procedure1 : Momentum investigation
m(t) ← d(t) − d(t − 1)
if m(t) ≥ 0.4 then
    procedure2
else
    alarm(t) is off
end if
End of procedure1
procedure2 : RoC assessment
roc(t − 1) ← x(t − 1)/x(t − 2)
roc(t) ← x(t)/x(t − 1)
if roc(t) ≥ 800 and roc(t − 1) ≥ 800 then
    alarm(t) is set
else
    alarm(t) is off
end if
End of procedure2
```

Using this algorithm, we tested five sample traffic patterns that are commonly observed at the core network of LG-dacom, which is the second largest commercial ISP in South Korea. One of them is usual traffic, which has neither flash event nor DDoS attack patterns. Three of them are flash events that do not have a DDoS attack pattern but have an unusual traffic surge. The last one is DDoS traffic. For the purpose of performance comparison, we use two more method: one is based on the time-series method and the other is based on an algorithm that is used in Arbor network devices. We briefly explain the operation of the two methods. For the time-series method, we used single exponential smoothing with the parameter α that is set to the value that let observations in the last 60 minutes account for 95% of the weight, as in [2]. To investigate the detecting performance with respect to the width of the confidence band, the parameter for the confidence band was set to 2 for case #1 and 3 for case #2, respectively. The algorithm used in Arbor devices uses three threshold lines (BASE, MIDDLE and SEVERE) and traffic average. Hence, if the traffic exceeds the BASE (MIDDLE, SEVERE) line and also the traffic average, then a MINOR (MAJOR, CRITICAL) ALARM is triggered, according to the threshold level. We mainly focus on MAJOR and CRITICAL ALARMS to investigate whether or not the detection is false. We also apply wider threshold lines at Arbor case #2 to investigate the impact of the width among threshold lines on performance of detection. We omit detail specification of threshold due to space limitation.

We describe the result in Fig. 3. It is evident that the time-series method performs the worst among the detection methods. Especially, in DDoS traffic case, it almost fails to distinguish between DDoS traffic and normal (usual/flash event) traffic irrespective of the width of confidence band, so that a lot of false alarms

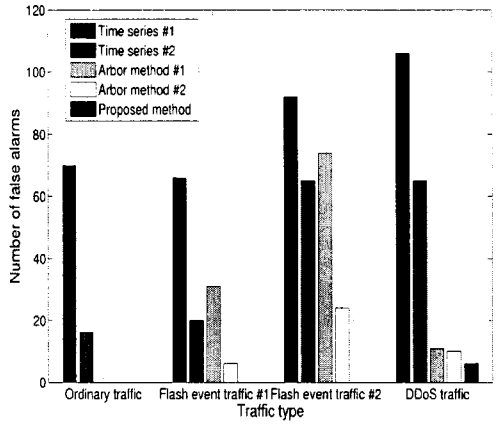


Fig. 3. The number of false alarm that is detected according to the applied methods and traffic type.

are observed. The algorithm used in Arbor network devices successfully detects usual traffic, but has a relatively high false alarm rate for flash event traffic. Note from the results that as the width among the threshold lines are wider, the false alarm rate of flash event traffic is getting lower. However, that of DDoS traffic is nearly unchanged. The reason is that since the width among threshold lines is wide, the method fails to detect DDoS traffic pattern that lies beyond the lines, i.e., negative false alarms occur. By contrast, the proposed method distinguishes between DDoS and normal (usual/flash event) traffic; hence, the only false alarms that occur are for DDoS traffic.

IV. Conclusion

In this letter, we have proposed a method for detecting DDoS traffic that is based on the technical analysis used in the stock market. The advantage of the proposed method is that the method makes it possible to determine the threshold quantitatively and apply the threshold consistently irrespective of the traffic pattern, with the result that DDoS traffic can be detected with greater accuracy. To extend and improve upon the research reported herein, we intend to apply another measure that deals with traffic volume intensity. This concept is based on the observation that DDoS traffic is induced to severe degree over a relatively long time period.

[참 고 문 헌]

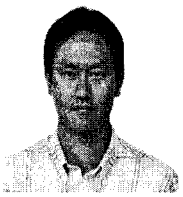
[1] P. Chhabra, C. Scott, E. Kolaczyk, and M. Crovella, "Distributed spatial anomaly detection," in *IEEE INFOCOM '08*, Apr. 2008.

[2] J. D. Brutlag, "Aberrant behavior detection in time series for network monitoring," in *Proc. the 14th Conference on System Administration (LISA 2000)*, pp. 139-146, Dec. 2000.

[3] K. Xu, X.-L. Zhang, and S. Bhattacharyya, "Profiling internet backbone traffic: Behavior models and applications," in *Proc. ACM Sigcom2005*, pp. 169-180, Aug. 2005.

[4] Moving Average Convergence and Divergence, *http://stockcharts.com/school/doku.php?id=chart_school:technical_indicators:moving_average_conve.*

[5] Rate of Change and Momentum, *http://stockcharts.com/school/doku.php?id=chart_school:technical_indicators:rate_of_change_roc_a.*



윤 정 훈

1998년 충남대학교 전자공학과 졸업
2000년 KAIST 전기및전자공학과(공학석사)
2005년 KAIST 전기및전자공학과(박사수료)
2008년~현재 LG-Dacom 기술연구소
<관심분야> Traffic Engineering, Wireless Mesh Network, Abnormal traffic detection.
<e-mail> jhyun5235@lgdacom.net

정 송

1988년 서울대학교 제어계측공학과 졸업
1990년 서울대학교 제어계측공학과(공학석사)
1995년 University of Texas Austin Electrical and Computer Engineering(공학박사)
2000년~현재 KAIST 정교수
<관심분야> 광대역 네트워크, 무선 메쉬 네트워크, 네트워크 성능분석
<e-mail> song@ee.kaist.ac.kr