Detection of DDoS traffic by using the technical analysis used in the the stock market

Junghoon Yun
Division of Electrical Engineering
School of EECS KAIST 373-1
Guseong-dong Yeseong-gu Daejeon
305-701, Republic of Korea
Email: jhyun@netsys.kaist.ac.kr

Song Chong
Division of Electrical Engineering
School of EECS KAIST 373-1
Guseong-dong Yeseong-gu Daejeon
305-701, Republic of Korea
Email: song@ee.kaist.ac.kr

***Abstract*—We propose a method for detecting Distributed Denial of Service (DDoS) traffic in real-time inside the network. For this purpose, we borrow the concepts of Moving Average Convergence Divergence, Rate of Change, and Relative Strength Index, 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 detection algorithm and simulation results, we show how the detection level is determined and demonstrate the degree to which the accuracy of detection is enhanced.**

***Index Terms*—DDoS traffic detection, flash event traffic, divergence, momentum, rate of change.**

I. Introduction

It is critical that network operators are able to detect Distributed Denial of Service (DDoS) traffic, such traffic is intended to break down the network [1]. However, it is not a trivial problem to distinguish accurately between DDoS traffic and normal traffic, because even normal traffic contains a lot of unusual traffic patterns and they occur in a totally unpredictable way. Throughout the paper, we will use the terms "DDoS traffic" and "abnormal traffic" interchangeably.

In [2] and [3], 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 the confidence band. This has the consequence that if the assigned confidence band is too narrow, a lot of traffic patterns may be detected as abnormal, with the result that there may be positive false alarms. On the contrary, if the assigned confidence band is too wide, abnormal traffic patterns may not be detected, with the result that there may also be negative false alarms.

In [4] and [5], 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 increases 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. We focus particulary on reducing the false alarm ratio by discriminating between DDoS traffic and normal traffic. We use the term "false alarm" to include both negative and positive false alarms and assume that normal traffic consists of ordinary and flash event traffic. Ordinary and flash event traffic results from the actions of legitimate users and does not have any malicious intention to break down the network. However, while the ordinary traffic has a periodic pattern day after day and does not have any sudden increase of traffic volume, the flash event traffic has unusual peak of traffic volume which looks like DDoS traffic pattern. However, this lasts for only a very short time, at most one or two minutes, and hence this feature makes flash event traffic different from DDoS traffic.

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, the Moving Average Convergence Divergence (MACD) [6], the Rate of Change (RoC) [7], and the Relative Strength Index (RSI) [8] are the most important measures. For the detailed usage of each measure, please refer to [6], [7], and [8].

We use these three 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, the measures used in the proposed method show a concrete, assessable directional difference when DDoS traffic occurs, thus the method enables us to determine the threshold for alarm quantitatively. We will demonstrate that the method has

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

all these properties through the simulation results.

The remainder of the paper is organized as follows. In section II, we explain in detail the characteristics and formulation of each measure. In section III, we present the proposed detection algorithm. In section IV, in order to show the features of the proposed method, we provide simulation results for the false alarm ratio with respect to various traffic types and detection methods. In section V, we present a summary.

II. Formulation of Measures

A. Divergence & Momentum

We define divergence 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:

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

where $\gamma > \beta$, $x(t)$ is the volume of current traffic, measured in packets per second. From Eq. (1), by substituting the first and the second equations into the last one, we obtain the momentum, $m(t)$, as follows:

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

where $e'(t) = x(t) - y(t-1)$ and $e''(t) = x(t) - z(t-1)$. According to the property of the time-series expansion, if parameter $\gamma > \beta$ and $x(t)$ changes severely, then $y(t)$ always follows $x(t)$ better than $z(t)$. Here is the key concept regarding the momentum. If $x(t)$ changes in an abnormal way, then the difference between $|e'(t)|$ and $|e''(t)|$ is large, i.e., $|e'(t)| << |e''(t)|$. Hence, the quantity of change in momentum is also large. However, if $x(t)$ does not change abnormally, then the difference between $|e'(t)|$ and $|e''(t)|$ is relatively small, i.e., $|e'(t)| \approx |e''(t)|$. Thus, the momentum can be kept low. This can be summarized as follows:

$$m(t) \Rightarrow \begin{cases} |m(t)| \gg 0, & \text{if } |x(t) - x(t-1)| \gg 1, \\ |m(t)| \approx 0, & \text{if } |x(t) - x(t-1)| \approx 0. \end{cases} \tag{3}$$

Because of this feature, 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.

If we define $e_{pred}(t-1) = e'(t) - e''(t)$ as the prediction error between two time series $y(t)$ and $z(t)$ with respect to $x(t)$, we derive the following proposition with the abuse of notation.

Proposition 2.1: Let $y(t)$ and $z(t)$ be the two time series of the current traffic volume $x(t)$, and γ and β be the parameters for $y(t)$ and $z(t)$, respectively. Further, assume that γ is greater then β and the momentum $m(t)$ is normalized by $z(t)$, i.e., $m(t)' = m(t)/z(t)$. Then, if $|m'(t)|$ is larger than δ, the absolute value of the difference of the prediction errors at t and $t-1$, $|e_{pred}(t) - e_{pred}(t-1)|$, is greater than $\delta\%$ with respect to $z(t)$.

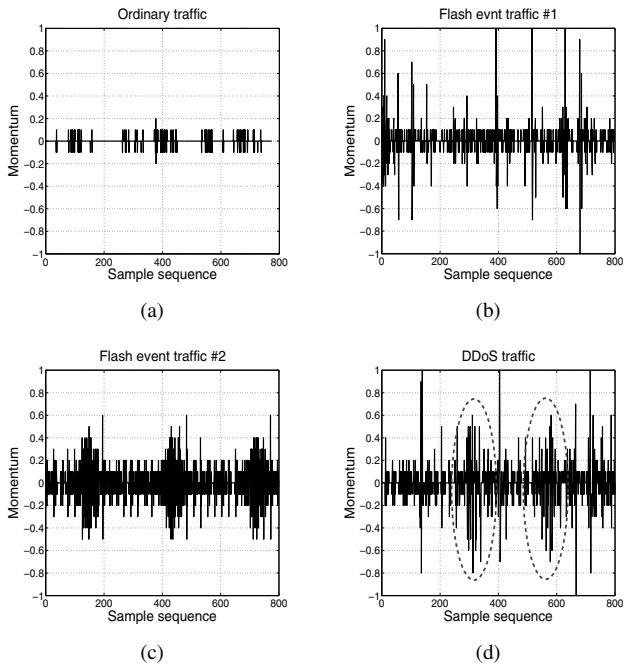


Fig. 1. Momentum of various traffic patterns that is normalized by $z(t)$ (parameters for momentum are set to $\gamma = 0.7$ and $\beta = 0.3$, respectively): (a) ordinary traffic, (b) flash event traffic #1, (c) flash event traffic #2, (d) DDos traffic.

Proof of Proposition 2.1: Since the momentum is normalized by $z(t)$, the equation of momentum is converted as follows,

$$m'(t) = \frac{d(t)}{z(t)} - \frac{d(t-1)}{z(t)}, \tag{4}$$

where $m'(t)$ denotes the momentum that is normalized by $z(t)$. After substituting $d(t) = y(t) - z(t)$ and $d(t-1) = y(t-1) - z(t-1)$ into Eq. (4) and applying $e''(t-1) - e'(t-1) = z(t-1) - y(t-1)$ to the equation, we can obtain a following equation:

$$m'(t) = \frac{e_{pred}(t)}{z(t)} - \frac{e_{pred}(t-1)}{z(t)}. \tag{5}$$

From Eq. (5), we can recognize that each prediction error, $e_{pred}(t)$ and $e_{pred}(t-1)$, is normalized by $z(t)$. This property eventually shows that the absolute value of the difference between the prediction errors at t and $t-1$, $|e_{pred}(t) - e_{pred}(t-1)|$, is greater than $\delta\%$ with respect to $z(t)$, if $|m'(t)|$ is greater than δ. ■

In Fig. 1, we show the momentum of various traffic patterns, normalized by $z(t)$. Note from the figures and proposition 2.1 that if the momentum is greater than 0.4, the difference of the prediction errors between two time series is greater than 40% with respect to $z(t)$. This result enables us to set the threshold value quantitatively. By determining a percentage of the difference of prediction errors of two time series that is tolerable as normal traffic, the momentum can be set quantitatively with respect to the percentage. By using the threshold value, we use the momentum to determine ordinary traffic. We will explain

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

in detail why the momentum is restricted to that traffic in a later section.

B. Rate of Change (RoC)

Momentum is a good measure for showing whether or not unusual traffic pattern occurs. However, it is not sufficient for distinguishing between DDoS and flash event traffic. The momentum only shows changes in traffic volume; hence, while it tells us that an unusual phenomenon is occurring, it does 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 a flash event traffic pattern occurs, the momentum may indicate that such traffic is DDoS. However, it must be regarded as normal. In order to compensate for this drawback of using the momentum alone, we employ another important measure, which is called RoC.

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

$$RoC(t) = \frac{x(t)}{x(t-\tau)}, \tag{6}$$

where τ denotes past time. In general, ordinary traffic shows almost the same pattern over the course of a day. Hence, the RoC of ordinary traffic does not change severely as shown in Fig. 2(a). However, if DDoS traffic is injected into the network, the amount of traffic increases drastically and lasts for a relatively long time. Thus, the RoC of DDoS traffic shows unusually high value and this last for more than fifteen consecutive sample sequences as shown in Fig. 2(d). In the case of flash event traffic, even though it has a similar pattern as DDoS traffic, the increase in the volume of traffic is not maintained for more than three consecutive sample sequences and is not as severe as in the case of DDoS traffic, as shown in Fig. 2(b) and Fig. 2(c).

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 patterns of 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.

C. Relative Strength Index (RSI)

So far, we have explained the characteristics and advantages of using the momentum and the RoC for detecting DDoS traffic. These measures are effective ones showing the change in and quantity of traffic volume when DDoS traffic occurs in the network. However, if the overall volume of traffic is very low, the RoC becomes too sensitive to the change of traffic volume, to the extent that it might create a lot of false alarms when especially flash event traffic that has relatively low traffic volume is injected into the network. For example, we can observe from Eq. (6) that if the volume of past traffic, $x(t-\tau)$, remains relatively low and the volume of current traffic, $x(t)$, is injected at a level of general flash event traffic,

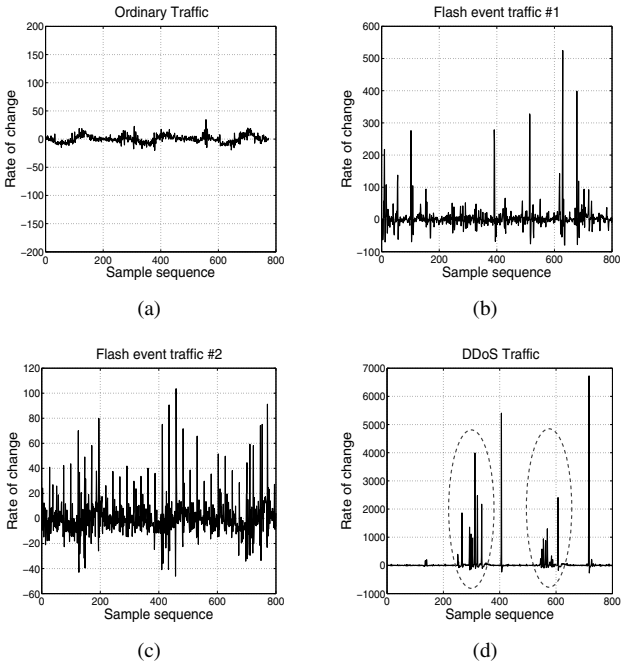


Fig. 2. RoC of various traffic patterns (with $\tau = 1$): (a) ordinary traffic, (b) flash event traffic #1, (c) flash event traffic #2, (d) DDoS traffic.

the RoC increases more than that of general flash event case and may exceed the threshold. Eventually, we may observe lots of positive false alarms. This phenomenon is well described in Fig. 3. Given that it is possible for this phenomenon to cause positive false alarms, we need a complementary measure to support the RoC, thus increasing the accuracy of detection when low-volume flash event traffic occurs in the network.

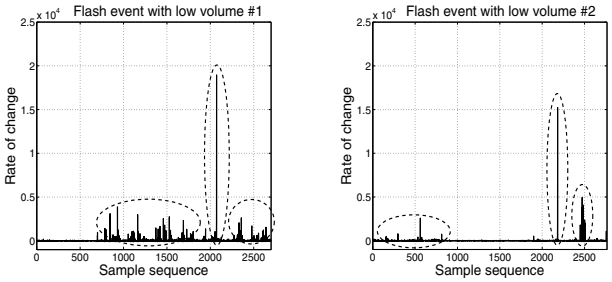


Fig. 3. RoC of flash event traffic patterns that have low traffic volume (with $\tau = 1$): (a) RoC of flash event traffic #1 that has low traffic volume, (b) RoC of flash event traffic #2 that has low traffic volume.

Note that this phenomenon is not a unique problem of the proposed method, but a common problem of methods of detecting DDoS that are based on the traffic volume. Indeed, many DDoS detection methods that are deployed in commercial networks impose a minimum limit on the volume of traffic to circumvent this obstacle. Thus, even if a DDoS traffic pattern is detected and the alarm is set as a result,

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

existing methods ignore this alarm if the volume of traffic is below the specified minimum. Of course, this method is simple and easy to implement. However, an important question remains to be answered: what is the appropriate minimum limit, such that it can be commonly applicable to all traffic patterns? According to the particular minimum limit that is set, there may occurs a lot of positive or negative false alarms. We think that this question cannot be answered satisfactorily.

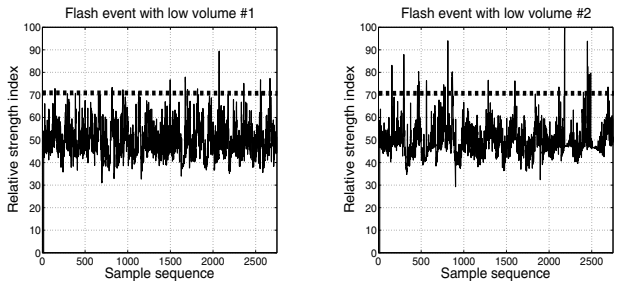
Instead of using a minimum limit for traffic volume, we employ the concept of a relative traffic strength(intensity) index, which is called RSI. The RSI measures the intensity of traffic during an observation period. When the RSI is taken into consideration, even though the alarm is set according to the RoC level, the alarm is ignored if the RSI remains below the required threshold. The RSI is computed as follows:

$$RSI(t) = 100 - \frac{100}{(1 + RS(t))}, \tag{7}$$

where

$$\begin{aligned} &RS(t) = G_{avg}(t)/L_{avg}(t), \\ &G_{avg}(t) = [G_{avg}(t-1) \times (D-1) + G(t)]/D, \\ &L_{avg}(t) = [L_{avg}(t-1)) \times (D-1) + L(t)]/D. \end{aligned} \tag{8}$$

To simplify the explanation of the RSI formula, we break down Eq. (7) into its basic components: $RS(t)$, $G_{avg}(t)$, $L_{avg}(t)$, $G(t)$, and $L(t)$. $RS(t)$ denotes the relative strength of traffic volume. $G_{avg}(t)$ is average gain that is calculated as the total of all positive gains during observation period D and $L_{avg}(t)$ is average loss that is calculated as the total of all negative gains during observation period D. $G(t)$ is the current positive gain and is computed as follows: if the volume of current traffic $x(t)$ is greater than that of past traffic $x(t-1)$, then $G(t) = x(t) - x(t-1)$. $L(t)$ is the current negative gain and is computed as follows: if the volume of current traffic $x(t)$ is smaller than that of past traffic $x(t-1)$, then $L(t) = x(t-1) - x(t)$. For a more detailed explanation about computing $RSI(t)$, please refer to [8].



(a) (b)

Fig. 4. RSI of flash event traffic patterns that have low traffic volume (observation period D is set to 1 hour): (a) RSI of flash event traffic #1 that has low traffic volume, (b) RSI of flash event traffic #2 that has low traffic volume.

Fig. 4 shows the RSI of traffic that is described in Fig. 3. As we claimed before, if the RSI is applied to the flash event traffic that has low volume, the rate that the value of the RSI exceeds the threshold line decreases drastically. We can see this fact by comparing Fig. 3(a) and Fig. 3(b) with Fig. 4(a) and Fig. 4(b). By using this feature, we use the RSI as a complementary measure of RoC as follows: when an alarm is detected according to the RoC level, we make a concrete decision as to whether or not the alarm is false by checking the level of intensity of traffic volume given by the RSI. The value for the threshold line used in this paper is derived directly from that of the RSI used in stock chart analysis and we will explain in detail the physical meaning of the threshold value in a following section.

III. DDoS DETECTION ALGORITHM

By using the measures of momentum, RoC, and RSI, we can create a detection algorithm for DDoS traffic as follows. First, we use the momentum $m(t)$ to determine whether or not incoming traffic is ordinary traffic. For this purpose, we set the threshold for the momentum to 0.4. This threshold is a reasonable value, because it is almost impossible for the difference in the prediction errors between two time series to be greater than 40% when the traffic is normal without a flash event pattern.

After picking out the ordinary traffic, we apply RoC to the rest of the traffic in order to identify flash event traffic. In this case, we use a heuristic device to determine the threshold for RoC. In general, if the RoC that is computed by using the traffic volume at two consecutive times t and $t-1$, $x(t)/x(t-1)$, is greater than 800, it is reasonable to regard this phenomenon as abnormal. Thus, we set τ to 1. In addition, as we mentioned before, flash event traffic is such that the sudden increase in traffic volume usually does not recur at two or three consecutive times. We can use these two features to determine whether or not incoming traffic is a flash event. That is, we compare two RoC values of $RoC(t)$ and $RoC(t-1)$ and determine whether or not both RoC values exceed the threshold level. If they do, we regard this phenomenon as abnormal, and normal otherwise.

Lastly, we use the RSI as an optional method to increase the accuracy with which we can distinguish between flash event traffic and DDoS traffic especially, in the last-mile network, where the volume of customer traffic is usually low and changes in a totally unpredictable way. However, note that in addition to being effective for discriminating flash event traffic from DDoS traffic in the last-mile network, the RSI can also help the proposed method to detect DDoS traffic more accurately in the core networks. Thus, the number of false alarms of DDoS traffic in the core network can be decreased as well. We will confirm these claims through the simulation results. For this purpose, we set the threshold for the RSI to 70, because the RSI is derived directly from that of the stock market without modification. The physical meaning of the level of 70 can be interpreted as follows, using the perspective of the network provider: if the RSI of any incoming traffic exceeds that value, the volume of the incoming traffic suddenly increases to the extent that it deviates more than 40% from the level of the average volume of traffic that obtains in the

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

Algorithm 1 Detection algorithm

```
procedure1 : Momentum investigation
m'(t) ← (d(t) − d(t − 1))/z(t)
if m'(t) ≥ 0.4 then
    goto 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
    if RSI(t) is not applied then
        alarm(t) is set
    else
        goto procedure3
    end if
else
    alarm(t) is off
end if
End of procedure2
procedure3 (optional process) : RSI evaluation
RSI(t) ← 100 − 100/(1 + RS(t))
if RSI(t) ≥ 70 then
    alarm(t) is set
else
    alarm(t) is off
end if
End of procedure3
```

normal state. Because the level of RSI at the normal or neutral state is 50.

IV. Simulation results

We now evaluate the performance of the proposed method for detecting DDoS traffic. We mainly focus on the reduction in the number of false alarms between DDoS and normal (ordinary/flash event) traffic. For this purpose, γ and β are set to 0.7 and 0.3, respectively, for computing the momentum, D is set to thirty minutes for RSI, and the unit of time t is set to five minutes throughout the simulation.

A. Momentum & RoC

We first estimate the effect of momentum and RoC on the reduction in the number of false alarms in each case of traffic pattern that we tested. For this purpose, we applied the proposed method without the RSI option and tested four 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 ordinary traffic, which has neither flash event nor DDoS attack patterns. Two 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. In brief, the operation of the two methods is as follows. For the time-series method, we used single exponential smoothing with the parameter α, which is set to the value that allows observations in the last 60 minutes to account for 95% of the weight, as in [2]. To investigate the detection 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 the arbor network devices uses three threshold lines (BASE, MIDDLE and SEVERE) and the traffic average. Hence, if the traffic exceeds the BASE (MIDDLE, SEVERE) line and the traffic average, then a MINOR (MAJOR, CRITICAL) ALARM is triggered, according to the threshold level. We focus particulary on MAJOR and CRITICAL ALARMS to investigate whether or not the detected alarm is false. We also apply wider threshold lines in arbor case #2 to investigate the effect of the width between threshold lines on the detection performance. For example, the BASE, MIDDLE, and SEVERE lines of case #2 are 1.5, 1.25, and 1.25 times higher than those of case #1, respectively.

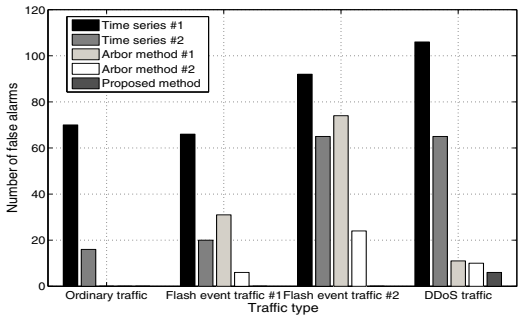


Fig. 5. The number of false alarm that is detected according to the applied methods and traffic type.

We describe the result in Fig. 5. 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 patterns and normal (ordinary/flash event) traffic patterns, irrespective of the width of confidence band; hence, a lot of false alarms are generated. The algorithm used in arbor network devices detects ordinary traffic successfully, but has a relatively high false alarm rate for flash event traffic. Note from the results that as the distance between the threshold lines increases, the number of false alarm for flash event traffic decreases. However, the number of false alarm for DDoS traffic remains almost unchanged. The reason is that due to the fact that the gap between the threshold lines is wide, the method fails to detect DDoS traffic patterns that lies below the lines, which results in negative false alarms being generated. By contrast, the proposed method distinguishes between DDoS and normal (ordinary/flash event)

978-1-4244-4148-8/09/$25.00 ©2009
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.

traffic successfully; hence, the only false alarms that occur are for DDoS traffic and the number of false alarms is lowest among the methods.

B. RSI performance evaluation

We now evaluate the effect of using the RSI in the proposed method on the reduction in the number of false alarms of flash event traffic and DDoS traffic. For this purpose, we mainly focus on how amount of false alarms the proposed method can eliminate regarding flash event traffic that occurs in the last-mile network with the condition of low traffic volume. We also investigate how much the accuracy with which the proposed method detects DDoS traffic can be enhanced in the core network. For this simulation, we used two types of flash event traffic that is observed in the last-mile network, which has low traffic volume and is normal, and the DDoS traffic that was used in the above section. The name of traffic is called *low volume traffic #1*, *low volume traffic #2*, and *DDoS traffic* in Fig. 6, respectively. In this case, we applied the proposed method, which uses all detection measures.

To compare the detection performance of the proposed method with that of the other methods, we employ the arbor method that was used in the above subsection. The arbor method in the previous section has been used with two different threshold settings, one with narrower threshold lines and the other with wider threshold lines. Thus, we can eventually explore the effect of the level of minimum limit of the traffic volume on the false alarm ratio by using the arbor method. The results of the simulation might therefore be a good example of comparing the performance of methods that are based on the minimum traffic limit and the RSI, respectively.

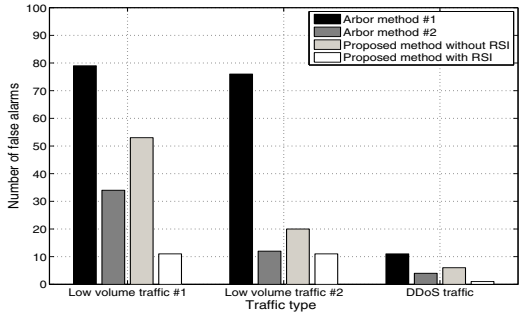


Fig. 6. The number of false alarms that are detected, according to the applied methods and traffic type.

We show the results in Fig. 6. From the figure, we can see that in order to reduce the number of false alarms irrespective of the applied methods, we need a mechanism that ignores any alarm that is generated if the traffic volume is below the specified minimum. Both the arbor method in which the lower minimum limit is set and the proposed method in which the RSI is not used generate a relatively large number of positive false alarms, irrespective of the traffic patterns. However, if we adopt the mechanism that ignores alarms if the traffic volume is below the specified minimum, the accuracy of detection is surprisingly enhanced. Especially, when the proposed method that uses the RSI is applied, the detection performance that reduces the number of false alarms can be enhanced by about 75% at the most if it is compared with the arbor method that is set to the higher minimum limit. Even when the proposed method that uses the RSI is applied to detect DDoS traffic in the core network, the accuracy of detecting DDoS traffic is enhanced by more than 80% at the maximum than when the proposed method is used without the RSI.

In summary, the RSI is a good complementary measure to the proposed method. It can recognize the level of traffic intensity of incoming traffic and thus enhance the detection accuracy of not only DDoS traffic in the core network, but also flash event traffic in the last-mile network.

V. Conclusion

We have proposed a method for detecting DDoS traffic that is based on the technical analysis used in the stock market. The advantages of the proposed method are as follows. It makes it possible to decide the threshold level quantitatively. In addition, the method exploits raw traffic data itself to determine whether or not the traffic in the network is abnormal and has a simple structure, so that DDoS traffic can be detected in real time while maintaining an increased level of accuracy.

In the future, we will address the following issues: (i) We will calibrate the parameters and the threshold value of each measure more finely to find out the optimal value. (ii) We will present evidence that the parameters and the threshold value that we will find are optimal through the mathematical proof and simulation results of various traffic types.

Acknowledgment

This research was supported by the Ministry of Knowledge Economy, Korea, under the Information Technology Research Center support program supervised by the Institute of Information Technology Advancement. (grant number IITA-2009-C1090-0902-0006)

References

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

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

[3] A. Ziviani, A. T. A. Gomes, M. L. Monsores, and P. S. S. Rodrigues, "Network anomaly detection using nonextensive entropy," *IEEE Communications Letter*, vol. 11, no. 12, pp. 1034–1036, Dec. 2007.

[4] K. Xu, Z.-L. Zhang, and S. Bhattacharyya, "Profiling internet backbone traffic: Behavior models and applications," in *Proc. ACM Sigcomm2005*, Aug. 2005, pp. 169–180.

[5] P. S. Kalekar, "Time series forecasting using holzt-winters exponential smooting," *www.it.iitb.ac.in/∼praj/acads/seminar/04329008_ExponentialSmoothing.pdf*, Dec. 2004.

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

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

[8] *Relative Strength Index*, http://stockcharts.com/school/doku.php?id=chart_school:technical_indicators:relative_strength_index_rsi.

978-1-4244-4148-8/09/$25.00 ©2009

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE "GLOBECOM" 2009 proceedings.