Detecting DDoS Attacks Using Dispersible Traffic Matrix and Weighted Moving Average

Tae Hwan Kim[1], Dong Seong Kim[2], Sang Min Lee[1], and Jong Sou Park[1]

[1] Dept. of Computer Engineering, Korea Aerospace University, Seoul, South Korea
{thkim,minuri33,jspark}@kau.ac.kr
[2] Dept. of Electrical and Computer Engineering, Duke University, Durham, USA
dongseong@gmail.com

Abstract. Distributed Denial of Service (DDoS) attacks have become significant threats on Internet according to the development of network infrastructure and recent communication technology. There are various types of DDoS attacks with different characteristics. These differences have made very difficult to detect such attacks. Furthermore, the sophisticated the evolution of DDoS attacks techniques and the enhanced scale of Botnet encourage attackers to launch DDoS attacks. The IP spoofing technique also makes difficult detect and traceback of DDoS attacks. In this paper, we propose a new detection model for spoofed DDoS attacks using dispersible traffic matrix and weighted moving average. This proposed detection model can not only visualize network traffic streams but also describe the dispersibility characteristics of DDoS attacks such as intensity, duration and rate of DDoS traffic. We carry out experiments on both DARPA 2000 dataset and real data in our network testbed environments so as to validate the feasibility of our approach. Our approach demonstrates that it effectively detects the DDoS attacks in the early stage and in very short time, even though DDoS attacks' streams are low. Also, the proposed detection model shows a good performance in terms of detection accuracy, speed, and false alarms.

Keywords: Distributed Denial of Service attacks, IP spoofing, Intrusion detection, Traffic matrix, Traffic visualization, Weighted moving average.

1 Introduction

For several years now, society has been dependent on information and telecommunication technology such as Internet and e-commerce. As the network speed becomes faster, the amount of information which is interconnecting within networks has been increased tremendously. However, it has also resulted in frequent opportunities for intrusions and attacks so security analysis techniques are needed to prevent and protect networks and systems. Among the intrusions and attacks, in particular, Distributed Denial of Service (DDoS) attacks are very critical these days. DDoS attacks are a large-scale, coordinated attack targeting on the availability of services at a victim system or network resources. DDoS attack is launched by sending an extremely large volume of legitimate packets

J.H. Park et al. (Eds.): ISA 2009, LNCS 5576, pp. 290–300, 2009.

or malformed packets. DDoS attacks exploit the vulnerability of protocols to a target through the simultaneous cooperation of a large number of compromised hosts that are distributed throughout the Internet. DDoS attacks traffic consumes the bandwidth resources of the network or the computing resources at the target host, so that legitimate requests will be discarded. Moreover, DDoS attacks use IP spoofing to conceal their location and identity. In other words, attackers forge or spoof the source IP address of each packet they send to avoid the traceback of DDoS attacks [5, 10]. The ingress filtering technique [2] has been proposed to prevent spoofing but the attackers have devised more sophisticated techniques, such as subnet spoofing [6] that can avoid current defense approaches. The impact of these attacks can vary from minor inconvenience to the users of a web site, to serious financial losses to companies that rely on their on-line availability to do business [7, 8, 11]. To counteract them, a great number of approaches for recognizing DDoS attacks have already been proposed. Typical detection approaches [1, 3] relied on filtering based on packet type and rate. Essentially, the detection software attempts to correlate the type of packet used for the attack. While these techniques have reasonable success, they have several limitations. Firstly, they are not very flexible because they are typically customized for known attack patterns. Therefore, these techniques are likely to fail if a new type of packet is used or if the attack consists of a traffic pattern that is a combination of different types of packets. In such cases, packet profiling is defeated. Secondly, a large number of detection techniques use traffic logs to identify attacks. However, traffic logs generate a large amount of data even during normal operation so it is difficult and time-consuming to scan traffic logs looking for patterns when the network is under attack. Finally, when the streams of packets on a network suddenly increase, it cannot still be sure that it is because of a DDoS attack in progress or FE(Flash Event; too many accesses of legitimated users). In this paper, we propose a novel approach to detect DDoS attacks using dispersible traffic matrix and weighted moving average. Our proposed approach can analyze the network traffic pattern with capturing the inbound traffic comes to the target host. The contributions of our approach are as follows; first, proposed model can present traffic's dispersibility, intensity, duration and rate effectively through network traffic matrix in real-time. Second, the model can not only detect DDoS attacks fast but also visualize network traffic streams in a real time basis. Third, our detection model is not dependent on the type of protocols. Therefore, it can detect the sophisticated DDoS attacks which use several protocols together. Forth, our detection model that analyzes the network traffic pattern through the traffic matrix is lightweight so it consumes less resource to detect DDoS attacks.

The remainder of the paper is organized as follows. Our proposed network traffic matrix and detection model are described in section 2. The evaluation of the proposed approach is presented in section 3. Finally, the paper concludes in section 4.

2 Proposed Approach

2.1 Overall Flow Proposed Approach

An overall flow of proposed DDoS attack detection model is depicted in Figure 1. The 1st dotted line box represents the process of traffic matrix initiation and it is performed before network monitoring. The second dotted line box presents construction of a traffic matrix. This process is repeatedly performed after starting network monitoring. At first, a traffic matrix for the traffic pattern analysis should be initiated; as setting a matrix size and time window size are determined depending on the network environments. Next, inbound traffic packets are captured and then, a traffic matrix is constructed using the captured packets information. The process of traffic matrix construction is described in next section 2.2 in more detail. The packets are captured during a given period of time window size and the detection model analyzes the traffic matrix and check whether the rate of captured traffics are more greater than some predefined threshold value (e.g., 1000pps) or not. This is a pre-processing phase for filtering out the meaningless irrelevant network traffic pattern since DDoS attack traffics are normally more than the threshold value. If the rate of capture traffic is less than the threshold value, then they are filtered out. The filtered traffic cannot badly affect the target system because the amount of the packets is negligible. The detection model continues to monitor the traffic through the traffic matrix. If the rate of the captured traffics is over the threshold value, then the model computes the variance of the matrix and Weighted Moving Average (WMA). Finally, it judges whether it is a spoofed DDoS attack, based on the variance and WMA of traffic matrix.

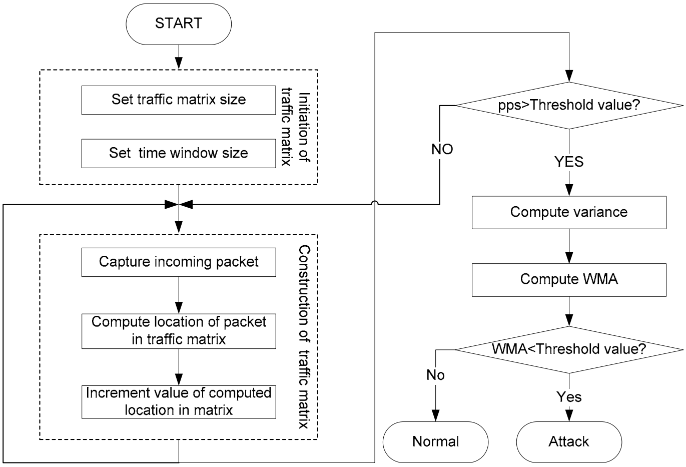


Fig. 1. Overall Flow of Proposed Detection Model

2.2 Constructing Traffic Matrix

In this section, we describe the process of constructing traffic matrix [9]. Figure 2 shows how to construct a traffic matrix using inbound traffic packets. Alphabets mean the packets that are coming from each different source IP addresses. ‘B’ packet is captured, the source IP address is divided into 4 octets and they are computed to determine the location of the matrix. Then, the value of location (i, j) is incremented by 1. The value of a specific location (i, j) becomes 4 by ‘B’ packets and the value of the other location became 2 since two ‘A’ packets were already captured. One traffic matrix could be constructed during a given time window. This traffic matrix design makes the packets coming from same bandwidth be mapped into same column. It is the characteristic of subnet spoofing which spoofs a random address from the address space assigned to the compromised host's subnet to avoid the ingress filtering. Consequently, we can present spoofed DDoS attack patterns using the traffic matrix. The detail of matrix construction is as follows; in order to build traffic matrix, each IP address of a captured packet is divided four octets as described in Eq. 1.

$$IP_1 \cdot IP_2 \cdot IP_3 \cdot IP_4 \tag{1}$$

For an example, assuming that B packet has the source IP address which is 192.168.103.101, then it is divided as $IP_1 = 192$, $IP_2 = 168$, $IP_3 = 103$, $IP_4 = 101$. And then, the IP is processed using two operations again; the first one is placement of a packet in matrix. The second one is to store traffic rate information. When a packet is captured in a monitoring network, the packet is mapped into a specific location of the matrix, which is determined by the source IP address of the packet. A placement function is described in Eq. 2.

$$\begin{aligned} i &= (IP_1 \times IP_2) \bmod n \\ j &= (IP_3 \times IP_4) \bmod m \end{aligned} \tag{2}$$

In Eq. 2, n and m indicate row and column of a matrix respectively. As the modular operations, the computed results of two IP octets; $(IP_1 \times IP_2)$, $(IP_3 \times IP_4)$, are within the range of n and m. Also, for storing traffic rate information, the value of that location (i, j) is the amount of packets coming from the source IP address, and it is represented as a numerical value.

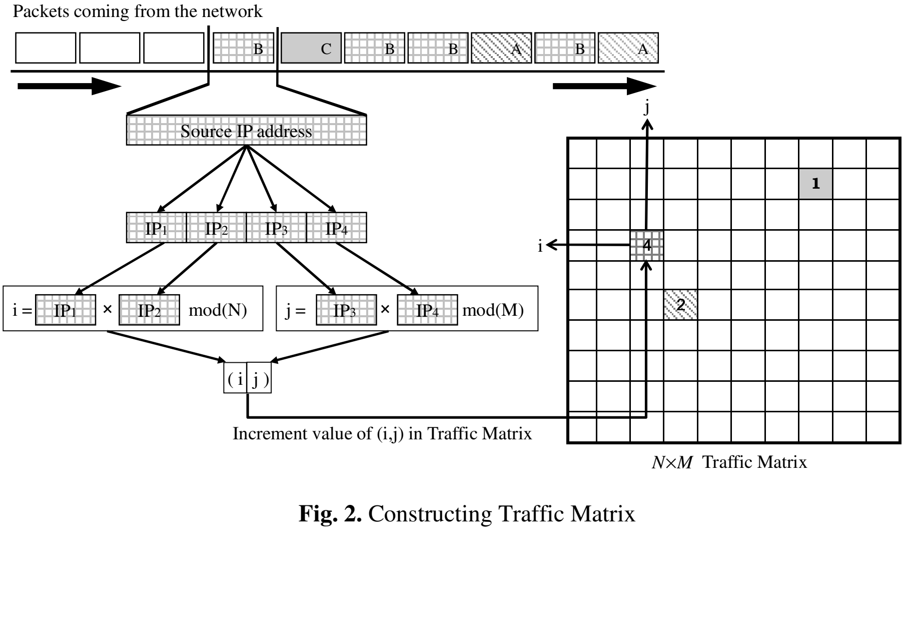


Fig. 2. Constructing Traffic Matrix

2.3 Variance of Traffic Matrix and DDoS Attacks

The source IP of attack traffic which is arbitrarily generated by random generator is one of the representative characteristics of spoofed DDoS attacks. In our proposed approach, we construct a traffic matrix with the source IP addresses and the number of packets to describe the dispersibility of network traffic that can be presented by the variance according to locations and their values in the matrix. Therefore, DDoS attack traffic is represented relatively equally distributed by spoofed source IP address as depicted in Figure 6(a). The variance of traffic matrix is much lower than that of normal traffic. The computation of variance of Matrix is represented in Eq. 3.

$$V = \frac{1}{k}\sum_{j=0}^{m}\sum_{i=0}^{n}(M_{(i,j)} - \mu)^2 \quad if \quad M_{(i,j)} \neq 0 \tag{3}$$

$M_{(i,j)}$ represents the value of location (i, j) in the matrix M. k represents the number of values which $M_{(i,j)}$ is not equal to 0, i.e., the number of sources coming into hosts. μ computed by Eq. 4 is the average packet(s) per one traffic.

$$\mu = \frac{1}{k}\sum_{j=0}^{m}\sum_{i=0}^{n}M_{(i,j)} \tag{4}$$

2.4 Moving Average and Weighted Moving Average

According to the special network state of the host, the variance of network traffic matrix can be extremely varying over time. The variance could be low when the amount of captured traffic data is small. For these two reasons, there are some relatively low variances even though they are normal traffics in Figure 3.

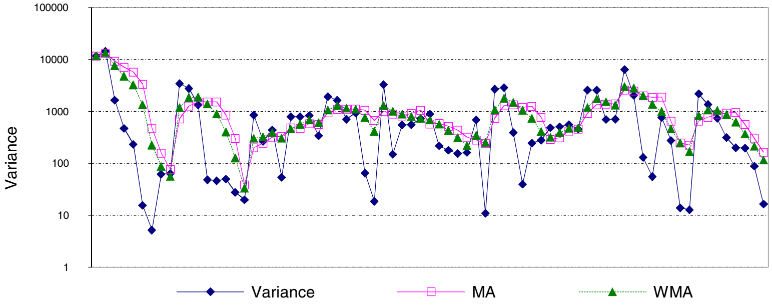


Fig. 3. Variance, MA, WMA

It means that the number of packets should be enough to analyze the traffic pattern using the variance, i.e., unless the number of packets is ensured, reliability of the variance can be degraded. For reducing such false alarm, we propose to utilize Moving Average (MA) and Weighted Moving Average (WMA). MA and WMA can make the extreme variation of data mitigate. In Figure 3, we can see that MA and WMA keep up the value in the points that the variance falls down significantly.

MA provides an advantage to reduce the false alarm with removing the significant variation of data. Mathematically, MA is the convolution of the data points with MA function in technical analysis. MA is the unweighted mean of the previous data samples. For example, if we have n data and the data are p_M, p_{M-1}, $\cdots$, $p_{M-(n-1)}$ then the MA can be formulated as;

$$MA = \frac{p_M + p_{M-1} + \cdots + p_{M-n+1}}{n} \tag{5}$$

Where, p_M is a variance during a given window size and n is the number of data for computing MA. If n is too large, it is difficult to present the accurate variation because of less influence of recent data. In order to cope with this problem of MA, WMA is adopted since it imposes more weight to the latest data. WMA is average that has multiplying factors to give different weights to different data points. WMA has the specific meaning of weights which decrease arithmetically. In an *n*-data, WMA the latest data has weight *n*, the second latest *n*-1, etc, down to zero.

$$WMA = \frac{np_M + (n-1)p_{M-1} + \cdots + 2p_{M-n+2} + p_{M-n+1}}{n + (n-1) + \cdots + 2 + 1} \tag{6}$$

3 Evaluation

In this section, we show the evaluation of proposed approach using DARPA 2000 data and real data from testbed. First, we start with matrix initialization that is represented as 1st dotted line box in Figure 1. It is important to determine the matrix size and time windows size of traffic matrix. We carry out experiment to determine them in next subsections.

3.1 Matrix Size

If the matrix size becomes bigger, it can present a large amount of network traffic at once, but if the matrix size is too big, it is useless in some cases, so that it is desirable to find out suitable matrix size with respect to the network environment. In this subsection, we show how to determine the matrix size and to efficiently reduce the traffic matrix size. To reduce the matrix size, we use a hash function and we can reduce the instances that the packets of different source IP addresses are located in same location (i, j). For the matrix size, a 50×50 matrix can describe the maximum 2500 different traffics simultaneously. In this case, if 100,000 connections are tried, 40 traffics are able to be mapped into same location. In case of a 100×100 matrix, it is able to present 10000 different traffics and it can decrease the number of overlapped traffics to 10. It is quite important to reduce the overlapped traffics since it can be an error when we analyze the traffic pattern.

Fig. 4 is the computed variance results with same network traffic data but three different matrix sizes; 100×100, 50×50 and 30×30. The big size of matrix can reduce the probability that packets coming from the different source IP address are mapped into the same location. Thus, we can see that the variance is low if the matrix size is big. Therefore, we need enough matrix size to present the traffic pattern to detect apparently. However, if the matrix size becomes bigger, we need more time and cost to analyze the traffic pattern. On the other hand, if the matrix size is too small, we cannot analyze the traffic pattern accurately so it is important to determine the matrix size which is suitable for the network state of the host. As the results, the variances between 30×30 and 50×50 matrixes have great differences in several times. Otherwise, the differences between 50×50 and 100×100 are little. The traffic data presented in Fig. 6 is captured traffics going to web server in testbed networks. In this network environment, 50×50 matrix is enough to present the traffic pattern.

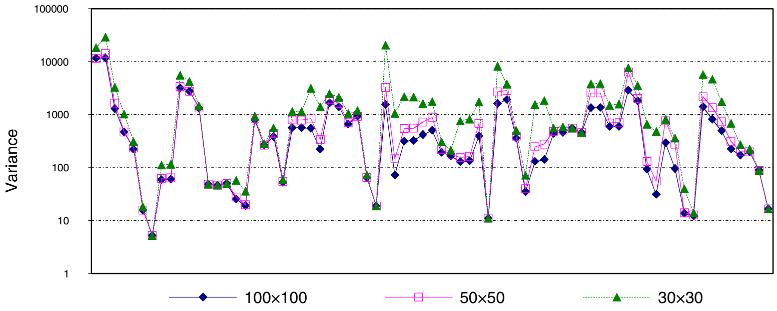


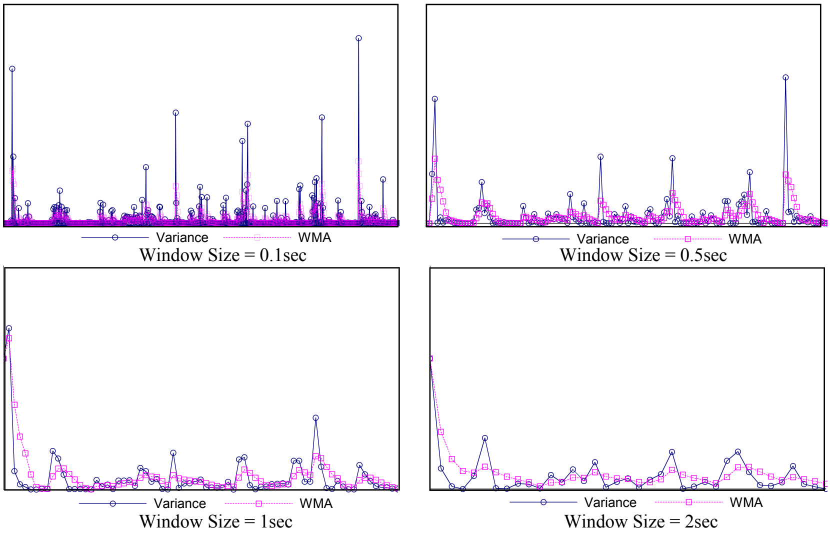
Fig. 4. Matrix size and variance

3.2 Window Size

In this subsection, we show how to determine window size. Traffic matrix M is constructed by traffic gathered for a given time period, called “window size”, then the matrix variance, number of packets are measured after passing every window size [9]. The suitable window size with the network state of the host can present traffic accurately in traffic matrix. If the window size is too large, traffic pattern is not described apparently because a lot of characteristics of traffic are in one matrix. On the other hand, if window size is too small, it is difficult to decide the characteristics of traffic pattern because of the small amount of traffic data.

Fig. 5 shows the computed variance results with same network traffic data but four different window sizes; 0.1, 0.5, 1 and 2 second(s). When the window size is 0.1 second, there are so many meaningless values that the variance is 0 because of the small number of captured data. Otherwise, when the window size is 2 seconds, it cannot present the variation of jumbled together. Thus, the reliability of variance in real-time traffic pattern in detail since a lot of network traffics are is degraded. Consequently, in our experiment environments, we can see that if window size is 1 second, the variation of WMA is clear and apparent, the noise is very small. Hence, it is also very indispensable to decide the proper window size according to the traffic rate.

We propose a victim based detection model which analyzes the network traffic pattern representing the inbound traffic comes to the host as a matrix. It can measure traffic’s dispersibility, intensity, duration and rate effectively through the constructed



Window Size = 0.1sec

Window Size = 0.5sec

Window Size = 1sec

Window Size = 2sec

Fig. 5. Window size and variance

network traffic matrix. The next subsection presents the way to build a traffic matrix and how to interpret the built matrix. After determining the size and window size of traffic matrix, we perform experiments on DARPA 2000 dataset and real network dataset collected from a university.

3.3 Experiments with DARPA 2000 Dataset

We used DARPA 2000 dataset as the first dataset to validate our approach. The 2000 DARPA Intrusion Detection Scenario Specific Data Set is used which includes a DDoS attack run by a novice attacker [12]. In phase. 5, even though DDoS attack time was few seconds, it is enough to verify the feasibility of our proposed detection model because the amount of data is enough. As it is very hard to collect DDoS attack type, DARPA 2000 dataset is used very commonly. Table 1 summarized the results of

Table 1. DARPA dataset experiment result

Window Size: 1sec		0.0~1.0		1.0~2.0		2.0~3.0		3.0~4.0		4.0~5.0		5.0~6.0	
Window Size: 0.5sec		0~0.5	0.5~1.0	1.0~1.5	1.5~2.0	2.0~2.5	2.5~3.0	3.0~3.5	3.5~4.0	4.0~4.5	4.5~5.0	5.0~5.5	5.5~6.0
Number of packets		5280		6267		6218		6221		6080		2772	
		1887	3993	3328	2939	3288	2930	3513	2708	3442	2638	1746	1026
Variance	MS:	96.339		137.824		116.3250		117.8680		117.0730		27.811	
	30×30	17.033	42.147	43.696	36.095	32.296	29.542	42.669	25.608	44.069	24.822	12.220	5.7116
	MS:	8.893		12.728		10.945		11.733		10.943		3.011	
	50×50	2.789	4.208	4.542	3.456	3.788	3.174	4.788	2.960	4.495	2.849	1.854	0.983
	MS:	1.828		2.511		2.219		2.305		2.227		0.723	
	100×100	0.504	0.899	0.936	0.815	0.842	0.741	1.056	0.682	0.988	0.678	0.366	0.197

experiments that use phase. 5 dataset. It presents the number of packets in each time and the variance of traffic matrix according to window size and matrix size. The variance when the matrix size is 30 is relatively higher than that in case of 50 and 100. This means the matrix size is not enough to present the traffic. Although the variance of normal network traffic is at least more than hundreds, the variance is less than maximum 13 when the matrix size is more than 50 in the experimental result. The results show that our approach is feasible.

3.4 Experiments in Testbed Network

Figure 6(a) and 9(b) present two 50×50 matrixes for one second window size. Figure 6(a) shows a DDoS attack traffic matrix which the source IP addresses are spoofed by random generator. Figure 6(b) shows a normal traffic matrix of a busy web server in our testbed network. The location in a matrix is determined by the source IP address of packets and value of the location is computed by the amount of packets in that location. The value of each element of the matrix is represented as a white-gray-black level color. If the value is high, the color becomes black whereas the value is low, it becomes white. DDoS attack traffics are evenly distributed because the source IP addresses are spoofed randomly. Thus, we can recognize that the variance of the traffic matrix is very low. On the other hand, the legitimate traffic of the web server has relatively less traffic sources and the intensity of traffic concentrates to a few sources even though they have a large amount of traffic. Thus, we can figure out the high variance of the traffic matrix.

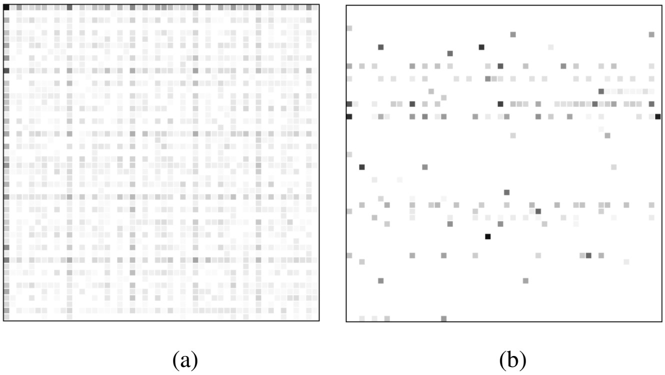
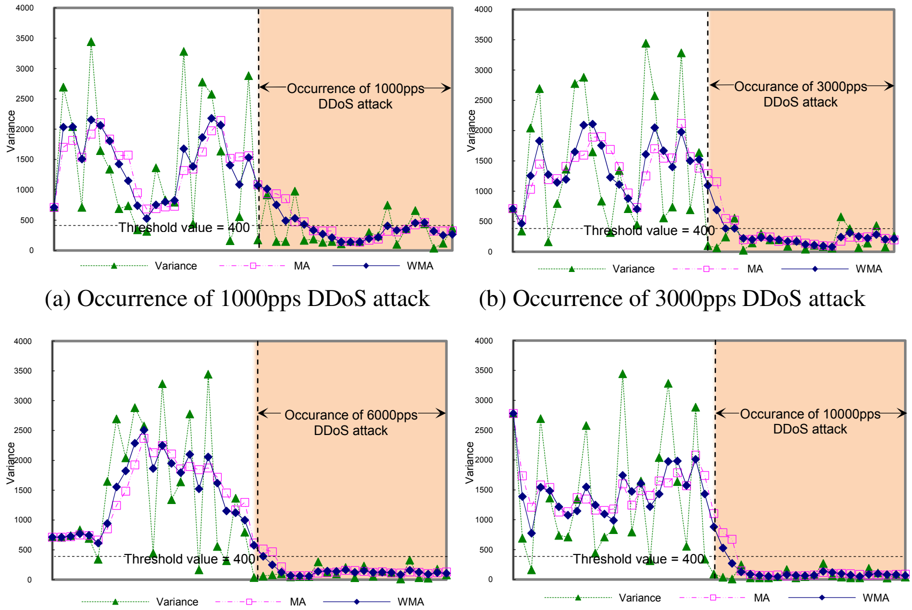


Fig. 6. DDoS attack traffic matrix(a) and normal web traffic matrix(b)

Our proposed approach is measured in real network. The traffic is captured in our testbed network and DDoS attack traffic is generated by several compromised hosts located in other networks. We carried out the experiments with changing the attack traffic rate, the number of compromised hosts and attack duration. Figure 7 presents the variation of variance of traffic matrix. We can see that WMA values of variance were going down below threshold value in few seconds after the host was attacked by DDoS attack. Even though the variance is below a threshold value in normal state, we can decrease such an error by using WMA. It means it is possible to detect accurately and reduce false alarm.



(a) Occurrence of 1000pps DDoS attack (b) Occurrence of 3000pps DDoS attack

(c) Occurrence of 6000pps DDoS attack (d) Occurrence of 10000pps DDoS attack

Fig. 7. Experimental results according to attack traffic rate

The parameters and experimental results are presented in Table 2. It shows that DDoS attack can be detected within several seconds. If the rate of DDoS attack traffic is higher, the dispersibility of network traffic is more apparent so that it is possible to detect the DDoS attack in very short period of time with low false alarm. In general, the rate of DDoS attack is launched in the rates of several thousands, it is expected to detect DDoS attacks in more accurate.

Table 2. The parameters and experimental results in real-networks

	(a)	(b)	(c)	(d)
Number of compromised hosts	10	20	30	50
Average of DDoS attack traffic rate	1000pps	3000pps	6000pps	10000pps
Detection time(sec)	6	2	1	1
False positive	0.2045	0.0454	0.0227	0.0254

4 Conclusion

In this paper, we have presented an efficient approach to detect DDoS attacks using traffic matrix and WMA. Considering the previous detection approach, there is commonly tradeoff between attack efficiency and cost [4]. Increasing the attack detection rate requires the increase of false alarm rate or increment of computational overheads or memory overheads. While detecting attacks as soon as possible is very important for preparing defense measures in DDoS attacks, most of the previous researches have been focused on the traffic generated by compromised host to extract detection parameters. However, our proposed detection model using traffic matrix can detect fast and decrease the false alarm through WMA. It is also efficient in terms of the cost. The contributions of our approach are (i) the network traffic analysis using traffic matrix can visualize the network traffic streams (ii) the traffic pattern analysis algorithm through the variance of traffic matrix is very efficient in terms of the cost (iii) fast detection of DDoS attack, so we can handle the DDoS attack proactively (iv) detection accuracy, speed and false alarm rate which have been validated through several experiments on DARPA 2000 dataset and real data in our testbed network environment.

Acknowledgments. This research was supported by the Advanced Broadcasting Media Technology Research Center (ABRC) in Korea Aerospace University, Korea, under the Gyeonggi Regional Research Center (GRRC) support program supervised by Gyeonggi Province.

References

1. Bezeq, R., Kim, H., Rozovskii, B., Tartakovsky, A.: A Novel Approach to Detection of Denial of-Service Attacks via Adaptive Sequential and Batch equential Change-Point Methods. In: IEEE Systems Man and Cybernetics Information Assurance Workshop, pp. 1–7 (2001)
2. Ferguson, P., Senie, D.: Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing, RFC 2827 (2000)
3. Gil, T., Poletto, M.: MULTOPS: A Data Structure for Bandwidth Attack Detection. In: USENIX Security Symposium, Washington D.C (2001)
4. Lee, K., Kim, J., Kwon, K., Han, Y., Kim, S.: DDoS attack detection method using cluster analysis. In: Expert Systems with Applications, vol. 34, pp. 1659–1665. Elsevier, Amsterdam (2008)
5. Li, J., Mirkovic, J., Wang, M., Reiher, P., Zhang, L.: SAVE: Source Address Validity Enforcement Protocol. In: INFOCOM 2002, vol. 3, pp. 1557–1566 (2002)
6. Mirkovic, J., Reiher, P.: A Taxonomy of DDoS Attack and DDoS Defense Mechanisms. In: SIGCOMM, vol. 34, pp. 39–53. ACM Press, New York (2004)
7. Mirkovic, J., Prier, G., Reiher, P.: Attacking DDoS at the Source. In: IEEE International Conference on Network Protocols, pp. 312–321 (2002)
8. Papadopoulos, C., Lindell, R., Mehringer, J., Hussain, A., Govindan, R.: COSSACK: Coordinated Suppression of Simultaneous Attacks. In: DARPA Information Survivability Conference and Exposition Washington DC, vol. 1, pp. 2–13 (2003)
9. Park, H., Lee, H., Kim, H.: Detecting Unknown Worms Using Randomness Check. IEICE Transactions on Communication E90(B4), 894–903 (2007)
10. Park, K., Lee, H.: On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets. In: ACM SIGCOMM (2001)
11. Zhang, G., Parashar, M.: Cooperative Defense Against DDoS Attacks. Journal of Research and Practice in Information Technology 38(1), 69–84 (2006)
12. MIT Lincoln Lab., DARPA intrusion detection scenario specific datasets (2000), http://www.ll.mit.edu/IST/ideval/data/2000/2000_data_index.html