Detection of Pulsing DoS Attacks at Their Source Networks

Ming Yu[1], Xiong-wei Li[2]

**[1]School of Information and Communication Engineering, Dalian University of Technology
Dalian, 116024, China**

**[2]Department of Computer Engineering, Ordnance Engineering College,
Shijiazhuang, 050081, China**

Abstract

Pulsing Denial of Service (PDoS) is a type of DoS attack. Its attacking behavior is intermittent rather than constant, which helps it avoid being detected. In this paper, an adaptive detection method is proposed for source-end detection of PDoS attacks. It has three distinctive features: (i) its detection statistic is based on the discrepancy in the aggregated outbound and inbound packets; (ii) a self-adaptive detection threshold adapts it quickly to the variations of network traffic and the latest detection result; (iii) random abnormalities in the normal network traffic can be filtered by consecutive accumulation of threshold violations. Experimental results show the minimum attack traffic that can be detected is less than 35% of the background traffic, under the requirements that probability of false alarms is less than 10^{-6}, probability of a miss during an attack is less than 10^{-2} and detection delay is within 7 sampling periods.

Keywords: *Pulsing DoS, Attack Detection, Adaptive Detection, Source-end Defense, Network Security.*

1. Introduction

At SIGCOMM 2003, Kuzmanovic and Knightly proposed a new generation of DoS attacks, which could decrease the throughput of normal TCP traffic by periodically sending high-volume traffic in a short period. They named it "shrew attack"[1]. By further and deep study on shrew attacks, X.Luo *et.al*. proposed a generic definition of PDoS (Pulsing Denial of Service)[2]. That is, a DoS attack can be called a PDoS attack only if its attack traffic is sent in a intermittent way. By this definition, a shrew attack is considered as a kind of PDoS attacks. Different from traditional DoS attacks, PDoS traffic is sent periodically and lasts for a short time within each attacking period. Thus, it is more difficult to detect PDoS attacks.

According to the different deployment locations, an autonomous DoS defense systems can be classified into source-end defense, victim-end defense and intermediate-network defense[3]. Among them, source-end refers to those networks that unwittingly host attacking machines; victim-end refers to the target network or the network that hosts the target machines; intermediate-network means the infrastructure between the attacking machines and the target. In recent years, source-end defense against DoS attacks has been a hotspot in network security. Several methods have been proposed for anomaly detection of the source-end traffic. Among them, the one used in the D-WARD system[4,5] is widely accepted. It adopts a set of legitimate traffic models to identify legitimate traffic and detect or constrain malicious traffic. Unfortunately, these models need to be updated periodically and therefore cannot adapt to the frequent changes in network traffic. This paper expatiates on our latest study on source-end defense against PDoS attacks.

Rest of this paper is organized as follows. Section 2 discusses the previous detection algorithms proposed for PDoS attacks. Section 3 presents the design of an adaptive method for source-end detection of PDoS attacks. Section 4 gives a performance analysis of the proposed method. Section 5 explains the parameter configuration in the proposed method. Section 6 presents the experiments and the detection results. Section 7 concludes this paper.

2. Related Work

Luo and Chang proposed a two-stage detection system to detect PDoS attacks on the receiver side[2]. Their method is based on the presence of two types of traffic anomalies induced by PDoS attacks: periodic fluctuations in the inbound TCP data traffic and a decline in the trend of the outbound TCP acknowledgement (ACK) traffic. In the first stage, the detection system monitors the inbound data and outbound ACK traffic using discrete wavelet transform. In the second stage, a nonparametric CUSUM algorithm is employed to detect the anomalies. Experiment results show the system is effective in detecting PDoS attacks with constant attack periods. However, it is ineffective in detecting flooding-based DoS attacks because such attacks will not cause periodic fluctuations in TCP traffic.

Hussain *et al*. proposed to differentiate between single-

source and multi-source DoS attacks[6] by analyzing spectrum of the network traffic. Chen *et al*. found the power spectrum density of a traffic stream containing shrew attacks has much higher energy in low-frequency band as compared with legitimate traffic. Based on this observation, they proposed a spectral template matching method to detect shrew attacks[7,8]. YU *et al*. proposed a similar method to detect SYN flooding attacks[9]. However, all these spectrum-based methods are ineffective in detecting PDoS attacks with different attacking frequencies and intervals.

Sun *et al*. proposed to detect shrew attacks using a dynamic time warping method which is divided into two stages[10]. In the first stage, autocorrelation is used to extract the periodic patterns in the inbound network traffic and eliminate the problem of time shifting. In the second stage, a slightly modified dynamic time warping algorithm is used to detect the signature of a shrew attack based on its autocorrelation coefficient. However, performance of this method is unsatisfactory when used in detecting PDoS attacks which are not separated by a constant interval. Moreover, such methods are ineffective in detecting flooding-based DoS attacks because the assumed square-wave patterns in such methods do not exhibit in the traffic under attack.

The D-WARD system is designed and implemented for source-end defense of DoS attacks. It adopts a useful metric that computes ratio of the inbound TCP traffic to the outbound TCP ACK traffic in detecting DDoS attacks [4]. Such a metric is also adopted in the Vanguard DoS detection system[11,12]. In both systems, however, a fixed ratio of the inbound TCP traffic to the outbound TCP ACK traffic is used to distinguish an attack flow from legitimate ones, which cannot adapt to the frequent changes in network traffic. Therefore, it is of crucial importance to design an "intelligent" detection method which can automatically adjust its detection parameters to adapt to the changing network conditions.

This paper expatiates on our latest study of source-end defense against PDoS attacks. Our main contribution is to propose an adaptive detection method for source-end detection of PDoS attacks.

3. Design of an Adaptive Method for Source-end Detection of PDoS Attacks

3.1 Problem Formulation

Let us begin by giving the problem formulation of PDoS detection before we go deep into the design of the proposed adaptive detection method.

Suppose $X=\{x_n, n=1,2,\cdots\}$ is a sequence of independent random variables observed sequentially, and $x_n=(O_n+1)/(I_n+1)$. Respectively, O_n and I_n denote the number of outbound requests and inbound replies collected within the n^{th} observation period. For legitimate traffic, O_n is approximately equal to I_n, thus we have $x_n \approx 1$. Normally, the mean of X (denoted by μ_X) is stable and close to 1. This conclusion has been referred by Mirkovic[4]. It is also supported by our analysis on some real traffic datasets collected at Dalian University of Technology. Fig. 1 gives the result of our analysis on one of those datasets.

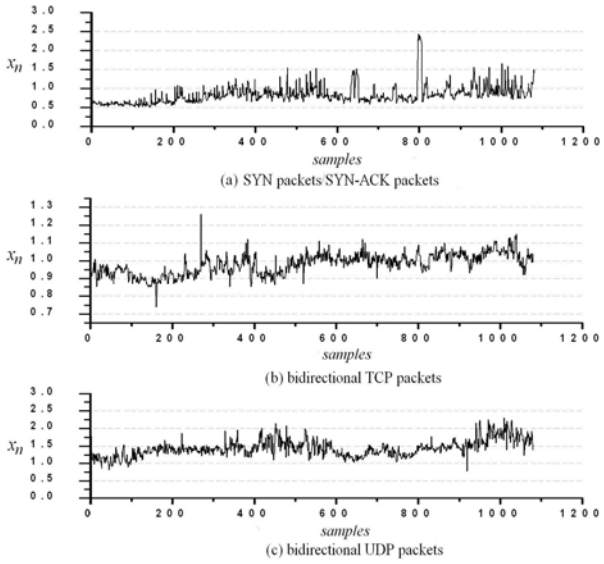

Fig.1 Analysis on x_n based on one of the real traffic dataset.

At a certain moment (random and unknown), an anomalous event occurs and μ_X is increased. When the anomaly ends, the mean of X is decreased to normal. Fig. 2 illustrates this process. However, no prior knowledge is known about the probability distribution function of X. The aim of a PDoS detection method is to accurately detect the start and the end of the PDoS attack as soon as possible.

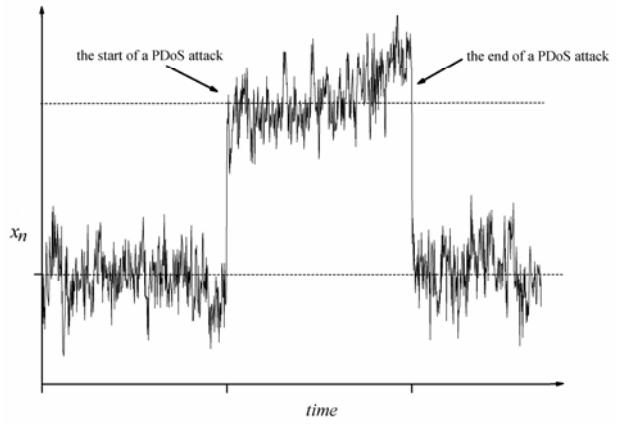

Fig.2 Illustration of PDoS detection.

3.2 Design of the Method

Essentially, the proposed method belongs to the area of sequential change-point detection[13,14]. It monitors network traffic at a regular interval and analyzes it to determine if any abnormalities are in the traffic. As we know, sequential change-point detection has to employ smaller amounts of data in order to keep such detection simple and efficient. At the same time, the data can not be so few that meaningful statistical characters can hardly be drawn. In the proposed method, data smoothing algorithms are considered to tradeoff these considerations. In addition, sequential change-point detection may also require that any alarms on attacks or anomalies be raised with a delay as short as possible. This is statistically guaranteed in the proposed method.

Three measures in design of the proposed method distinguish it from others. Respectively, they are as follows.

(i) Adopt the simple moving average algorithm in processing $X=\{x_n, n=1,2,\cdots\}$. Consequently, a new series, $U=\{u_n, n=1,2,\cdots\}$, is obtained. Here, u_n is used as the detection statistic and N is the sliding window size. Moreover, $u_n=\frac{1}{N}\sum_{i=n-N+1}^{n} x_i$.

(ii) Adopt the exponentially-weighted moving average (EWMA) algorithm in estimation of the mean of U after the n^{th} sampling period (denoted by $\hat{\bar{u}}_n$) when there are no alarms. We get $\hat{\bar{u}}_n = p\hat{\bar{u}}_{n-1} + (1-p)u_n$, where p is the EWMA factor. Once an alarm is raised, update of $\hat{\bar{u}}_n$ is suspended and the current $\hat{\bar{u}}_n$ is referred until the alarm is canceled.

(iii) Make consecutive estimations of the standard deviation of U after the nth sampling period (denoted by $\hat{\sigma}_n$) when there are no alarms. We get

$$\hat{\sigma}_n = \sqrt{2\sum_{i=N}^{n}(u_i - \bar{u}_{i-1})^2/(n-1)}$$

Once an alarm is raised, update of $\hat{\sigma}_n$ is suspended and the current $\hat{\sigma}_n$ is referred until the alarm is canceled.

To reduce disturbance of random abnormalities in the normal network traffic, two variables are set. Respectively, they are AI for accumulation of threshold violations, and d_n for alarm decisions. The decision rules for threshold violations are as follows. Here, $\eta(\eta > 0)$ is a parameter indicating PDoS attacks in the network traffic.

IF $u_n \geq \hat{\bar{u}}_{n-1} + \eta\hat{\sigma}_n$
  AI=AI+1;
  IF AI equals K
    AI=K-1;
ELSE
  IF AI>0
    AI=AI-1;
END

The decision rules for raising alarms are as follows. Here, '0' is for no alarms and '1' is for raising alarms.

$$d_n = \begin{cases} 0, & \text{if } AI < K \\ 1, & \text{if } AI \geq K \end{cases}$$

To reduce miss of alarms during an attack, η is set as a function of d_n, that is,

$$\eta = \begin{cases} \eta_H, & \text{if } d_n \text{ equals } 0 \\ \eta_L, & \text{if } d_n \text{ equals } 1 \end{cases}$$

In summary, the proposed method is described in Fig.3.

4. Performance Analysis

As is mentioned in section 3, no prior knowledge is known about the probability distribution function of X. However, it is generally accepted that the discrepancy between the numbers of outbound packets and inbound packets is due to some transmission failures and the subsequent

retransmissions. And usually, transmission failures are caused by various random network anomalies, such as network congestion, routing loops, link failures and server failures. To date, there is little evidence indicating these anomalies are closely correlated. Thus, it is a reasonable assumption that U is a stochastic series following Gaussian distribution $p_0 = N(\mu_0, \sigma_0)$ under normal conditions and $p_1 = N(\mu_1, \sigma_1)$ during a PDoS attack. Due to the data smoothing measure, we assume $\hat{\bar{u}}_n = u_0$ and $\hat{\sigma}_n = \sigma_0$ under normal conditions.

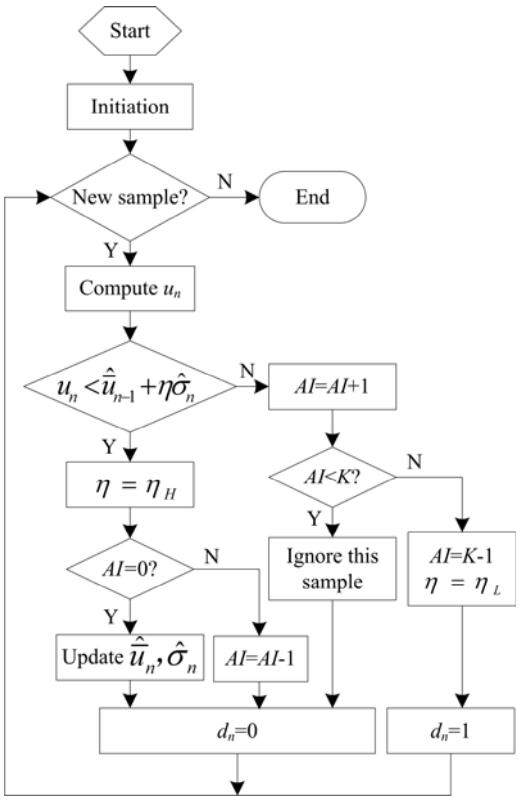

Fig.3 Flowchart of the proposed method.

For convenience of subsequent analysis, we define the following variables.

(i) O_N: the averaged number of outbound packets under normal conditions in one sampling period.

(ii) O_M: the averaged number of outbound packets sent by attacking machines in one sampling period during a PDoS attack.

(iii) I_N: the averaged number of inbound packets under normal conditions in one sampling period.

(iv) $\lambda(\lambda>0)$: the proportion of O_M to O_N, and $\lambda = O_M/O_N$.

And we get

$$\mu_1 = E[\frac{O_M + O_N + 1}{I_N + 1}] \approx (1+\lambda)E[\frac{O_N}{I_N}] = (1+\lambda)\mu_0 \quad (1)$$

$$\sigma_1^2 = D[\frac{O_M + O_N + 1}{I_N + 1}] \approx D[(1+\lambda)\frac{O_N}{I_N}] = (1+\lambda)^2\sigma_0^2 \quad (2)$$

$$\sigma_1 = (1+\lambda)\sigma_0 \quad (3)$$

Based on Eq. (1)~Eq.(3), following results on performance of the proposed method can be obtained.

(i) Probability of false alarms (P_f)

According to the proposed method, false alarms are raised mainly by random network anomalies which last K sampling periods at least. Thus, we get

$$P_f = [\int_{\mu_0+\eta_H\sigma_0}^{\infty} p_0(x)dx]^K = Q^K(\eta_H) \quad (4)$$

Here, $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^{\infty} e^{-u^2/2}\,du$.

(ii) Probability of a miss during an attack (P_m)

$$P_m = \int_0^{\mu_0+\eta_L\sigma_0} p_1(x)dx \approx Q(\frac{\mu_1 - \mu_0 - \eta_L\sigma_0}{\sigma_1}) \quad (5)$$

(iii) Probability of detection (P_d) and detection delay (τ)

In PDoS detection, it is meaningless to talk about probability of detection without referring to the corresponding detection delay. In this paper, PDoS detection delay is defined as the time between the beginning of an attack and the first alarm of it. The unit of τ is the observation period t_s. If an attack is launched when $0<AI<K$, $\tau \geq 0$. In the design of the proposed method, we consider the worst case that an attack is launched when AI is zero. Then, τ can be expressed as $\{\tau = K + 2m, m=0,1,2,3,\cdots\}$. However, it is practical to focus on the probability of detection with $\tau \leq K+2$. Thus, we get

$$P_d(\tau = K) = [\int_{\mu_0+\eta_H\sigma_0}^{\infty} p_1(x)dx]^K = [1 - Q(\frac{\mu_1 - \eta_H\sigma_0 - \mu_0}{\sigma_1})]^K \quad (6)$$

Let $P_d(\tau = K) = P_{d(K)}$, then

$$P_d(\tau = K+2) = (K-1)P_{d(K)}\,P_{d(K)}^{1/K}(1 - P_{d(K)}^{1/K}) \quad (7)$$

$$P_d(\tau \leq K+2) = P_{d(K)} + (K-1)P_{d(K)}\,P_{d(K)}^{1/K}(1 - P_{d(K)}^{1/K}) \quad (8)$$

5. Parameter Specification

Suppose: the specified requirements for PDoS detection is $P_f \le \alpha$, $P_m \le \beta$, $P_d(\tau \le K+2) \ge \gamma$ and $\lambda_{min} = \rho$. By Eq. (4) and Eq. (5), we get

$$Q^K(\eta_H) \le \alpha \Rightarrow \eta_H \ge Q^{-1}(\sqrt[K]{\alpha}) \quad (9)$$

$$Q(\frac{\mu_1 - \mu_0 - \eta_L\sigma_0}{\sigma_1}) \le \beta \Rightarrow \frac{\mu_1 - \mu_0 - \eta_L\sigma_0}{\sigma_1} \ge Q^{-1}(\beta) \quad (10)$$

Here, $Q^{-1}(x)$ is the inverse function of $Q(x)$.

Based on Eq. (8), we get

$$P_{d(K)} + (K-1)P_{d(K)}P_{d(K)}^{1/K}(1 - P_{d(K)}^{1/K}) \ge \gamma \quad (11)$$

Suppose $\xi(K,\gamma)$ is the minimum value which satisfies inequation $x^K + (K-1)x^{K+1}(1-x) \ge \gamma$ and $0 < \xi(K,\gamma) < 1$, then $P_{d(K)}^{1/K} \ge \xi(K,\gamma)$. By Eq. (6), we get

$$\frac{\mu_1 - \eta_H\sigma_0 - \mu_0}{\sigma_1} \ge Q^{-1}(1 - \zeta(K,\gamma)) \quad (12)$$

Based on Eq. (3)、Eq. (9)、Eq. (10) and Eq. (12), we get

$$\eta_H \ge Q^{-1}(\sqrt[K]{\alpha}) \quad (13)$$

$$\eta_L \le \frac{\mu_1 - \mu_0}{\sigma_0} - (1+\lambda)Q^{-1}(\beta) \quad (14)$$

$$\frac{\mu_1 - \mu_0}{\sigma_0} \ge Q^{-1}(1 - \zeta(K,\gamma)) + \frac{\eta_H}{1+\lambda} \quad (15)$$

To fulfill the minimum value of the requirements, key parameters in the method can be set as follows.

$$\eta_H = Q^{-1}(\sqrt[K]{\alpha}) \quad (16)$$

$$\eta_L = Q^{-1}(1 - \zeta(K,\gamma)) + Q^{-1}(\sqrt[K]{\alpha}) - Q^{-1}(\beta) \quad (17)$$

6. Experiments

Five real traffic traces are used to validate the proposed method. These traces were all collected by a Endace® DAG card at Dalian university of technology with an OC-48c PoS link connected to CERNET. For each trace, two types of PDoS traffic were included. Respectively, they are SYN flooding traffic and UDP flooding traffic. All the attacks are launched every 10 minutes, and the bursting time of each attacking machines is 5 minutes. In order to reflect the advantages of the proposed method in detecting low intensity attacking traffic over those with a fixed detection threshold, a comparison is made on the detection results between the proposed method and a direct detection with a fixed threshold.

In order to make an impartial comparison, all experiments were done with the same requirements. Respectively, they are $P_f < 10^{-6}$, $P_m < 10^{-2}$ and $P_d(\tau \le 7) \ge 0.7$. Based on these requirements, we get $\eta_H = 1.6$, $\eta_L = 0.7$ and K=5 according to Eq. (8)、Eq. (16) and Eq. (17). Other parameters that are related to the proposed method are set as follows. The sliding window size N is set to 3. The sampling interval t_s is set to 20 seconds. The EWMA factor p is set to 0.1. Initiation of $\hat{\bar{u}}_n$ and $\hat{\sigma}_n$ is set as $\hat{\bar{u}}_2 = 2$, $\hat{\sigma}_2 = 0.2$. Configuration of these parameters is fit for various requirements on the proposed method, and they seldom change in our experiments. In the fixed threshold detection, the detection threshold is set to 1.2, 1.6 and 2 respectively.

The experiments were carried out with the intensity of attacking traffic varied from 10% to 10 times of the normal background traffic. Table 1~Table 8 give the detection results on pulsing SYN flooding traffic and pulsing UDP flooding traffic by the proposed method and fixed threshold detection respectively. These results are obtained after 300 experiments on each trace.

Table 1 Detection of pulsing SYN flooding traffic by the proposed method

	Trace-1	Trace-2	Trace-3	Trace-4	Trace-5
P_f	1.9×10^{-3}	0.0	0.5×10^{-3}	0.0	0.0
P_d	99.4%	96.9%	98.8%	100.0%	100.0%
$\tau(t_s)$	6.7	6.8	6.6	6.7	6.9
λ_{min}	0.59	0.20	0.38	0.34	0.29

Table 2 Detection of pulsing SYN flooding traffic by fixed threshold detection with the threshold set to 1.2

	Trace-1	Trace-2	Trace-3	Trace-4	Trace-5
P_f	3.0×10^{-2}	—	12.8×10^{-2}	12.1×10^{-2}	6.5×10^{-3}
P_d	99.7%	—	99.5%	99.2	100.0%
$\tau(t_s)$	0.1	—	0.1	0.1	0.1
λ_{min}	0.66	—	0.29	0.17	0.23

Table 3 Detection of pulsing SYN flooding traffic by fixed threshold detection with the threshold set to 1.6

	Trace-1	Trace-2	Trace-3	Trace-4	Trace-5
P_f	1.9×10^{-3}	10.2×10^{-2}	1.3×10^{-2}	2.2×10^{-3}	0.0
P_d	100.0%	88.2%	100.0%	100.0%	100.0%
$\tau(t_s)$	0.1	0.0	0.1	0.1	0.1
λ_{min}	1.15	0.13	0.84	0.71	0.78

Table 4 Detection of pulsing SYN flooding traffic by fixed threshold detection with the threshold set to 2

	Trace-1	Trace-2	Trace-3	Trace-4	Trace-5
P_f	0.9×10^{-3}	0.0	3.4×10^{-3}	0.0	0.0
P_d	100.0%	100.0%	100.0%	100.0%	100.0%
$\tau(t_s)$	0.1	0.1	0.1	0.1	0.1
λ_{min}	1.64	0.38	1.42	1.25	1.33

Table 5 Detection of pulsing UDP flooding traffic by the proposed method

	Trace-1	Trace-2	Trace-3	Trace-4	Trace-5
P_f	4.6×10^{-3}	0.0	2.0×10^{-3}	0.0	0.0
P_d	91.7%	100.0%	81.7%	96.6%	92.0%
$\tau(t_s)$	6.3	7.0	6.4	6.6	6.4
λ_{min}	0.31	0.69	0.32	0.65	0.74

Table 6 Detection of pulsing UDP flooding traffic by fixed threshold detection with the threshold set to 1.2

	Trace-1	Trace-2	Trace-3	Trace-4	Trace-5
P_f	6.0×10^{-2}	0.0	10.2×10^{-2}	4.4×10^{-2}	10.4×10^{-2}
P_d	31.5%	100.0%	81.7%	99.6%	100.0%
$\tau(t_s)$	0.0	0.2	0.1	0.2	0.3
λ_{min}	0.12	0.74	0.26	0.92	0.80

Table 7 Detection of pulsing UDP flooding traffic by fixed threshold detection with the threshold set to 1.6

	Trace-1	Trace-2	Trace-3	Trace-4	Trace-5
P_f	5.7×10^{-2}	0.0	1.1×10^{-2}	2.2×10^{-3}	7.4×10^{-3}
P_d	98.1%	100.0%	96.9%	100.0%	100.0%
$\tau(t_s)$	0.1	0.2	0.2	0.2	0.4
λ_{min}	0.36	1.32	0.63	1.56	1.42

Table 8 Detection of pulsing UDP flooding traffic by fixed threshold detection with the threshold set to 2

	Trace-1	Trace-2	Trace-3	Trace-4	Trace-5
P_f	1.6×10^{-2}	0.0	3.0×10^{-3}	0.0	0.0
P_d	100.0%	100.0%	98.6%	100.0%	100.0%
$\tau(t_s)$	0.0	0.3	0.2	0.3	0.4
λ_{min}	0.70	1.93	1.05	2.22	2.06

In these tables, "—" stands for invalid detections which occur when the detection threshold is too low to avoid false alarms. λ_{min} denotes the lowest intensity of the attacks that can be detected. Our explanation on all of the detection results are give as follows.

(i) As we can see, part of the results on P_f in Table 1 and Table 5 are between 0.5×10^{-3} and 4.6×10^{-3}. This is related to insufficiency of trace data in the corresponding traces. Analysis shows there are 1080 sample data (the traffic data was collected in 6 hours) in trace-1 and 2030 sample data (the traffic data was collected in 6 hours about 11 hours) in trace-3. Even if one or two false alarms occur, P_f will rise to 10^{-3}. In practice, this is acceptable. In our opinion, P_f will decrease if more traffic is collected. This opinion can be supported by trace-2、trace-4 and trace-5 which contain more traffic data than that in trace-1 and trace-3.

(ii) The detection results on P_d, τ and λ_{min} obtained by using the proposed method fulfill the requirements on the detection. Since the key parameters η_H、η_L and K configured in the proposed method are derived from Eq. (8)、Eq. (15) and Eq. (16), accuracy of the performance analysis in section 4 is proved.

(iii) Fixed threshold detection is not ideal for PDoS detection. A proper threshold is hard to determine in the detection. If the detection threshold is lower, P_f will increase to 10^{-2}. This can not be improved by gathering more traffic data. If the detection threshold is higher, attacks may be missed. This is reflected by λ_{min} which is higher in fixed threshold detection than in the proposed method.

7. Conclusions

Adaptive detection of PDoS attacks is a newly proposed research area. In this paper, an adaptive method is proposed based on the assumption of normal distribution of the detection statistic which is a ratio between the outbound packets and the inbound packets in the source-end networks of the attacking machines. Distinct characters in design of the proposed method include: (i) its detection statistic is based on the discrepancy in the aggregated outbound and inbound packets; (ii) a self-adaptive detection threshold adapts it quickly to the variations of network traffic and the latest detection result; (iii) random abnormalities in the normal network traffic can be filtered by consecutive accumulation of threshold violations. Performance analysis of the proposed method is made in terms of probability of false alarms, probability of a miss during an attack, probability of detection, and detection delay. Experiments on real traffic traces validate the accuracy of our performance analysis on the proposed method and show the efficacy of the proposed method in source-end detection of pulsing SYN flooding and pulsing UDP flooding.

Acknowledgments

This work is supported by (1) National Natural Science Foundation of China (Grant No.61172059); (2) the Scientific Research Foundation for Ph.Ds of Liaoning Province, China (Grant No.20111022).

References

[1] A.Kuzmanovic, and E.W.Knightly, "Low-rate TCP-targeted Denial of Service Attacks: the Shrew vs. the Mice and Elephants ", in ACM SIGCOMM 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, 2003, Vol.1, pp.75-86.

[2] X.Luo, and R.Chang, "On a New Class of Pulsing Denial-of-Service Attacks and the Defense", in Network and Distributed System Security Symposium, 2005, pp.67-85.

[3] Yu Ming, "A Nonparametric Adaptive CUSUM Method and Its Application in Source-End Defense against SYN Flooding Attacks", WuHan University Journal of Natural Science, Vol. 16, No. 5, 2011, pp.414-418.

[4] Jelena Mirkovic, and Peter Reiher, "D-WARD: A Source-End Defense Against Flooding Denial-of-Service Attacks", IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 3, 2005, pp. 216-232.

[5] Bekravi Masoud, Jamali Shahram, Shaker Gholam, "Defense against SYN-flooding Denial of Service Attacks Based on Learning Automata", International Journal of Computer Science Issues, Vol. 9, No. 3, 2012, pp.514-520.

[6] A. Hussain, J. Heidemann, and C. Papadopoulos, "A Framework for Classifying Denial of Service Attacks", in ACM SIGCOMM 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, 2003, Vol.1, pp.99–110.

[7] Y. Chen, and K. Hwang, "Collaborative Detection and Filtering of Shrew DDoS Attacks Using Spectral Analysis", Journal of Parallel and Distributed Computing, Vol. 66, No. 9, 2006, pp. 1137–1151.

[8] Y. Chen and K. Hwang, "Spectral Analysis of TCP Flows for Defense against Reduction-of-Quality Attacks", in IEEE International Conference on Communications, 2007, Vol.1, pp.1203-1210.

[9] Ming Yu, and Xi-yuan Zhou, "An Adaptive Method for Anomaly Detection in Symmetric Network Traffic", Computers & Security, Vol.26, No.6, 2007, pp.427-433.

[10] H. Sun, J. C. S. Lu, and D. K. Y. Yau, "Defending against Low-rate TCP Attacks: Dynamic Detection and Protection", in the 12th IEEE International Conference on Network Protocols, 2004, Vol.1, pp. 196–205.

[11] Xiapu Luo, Edmond W. W. Chan, and Rocky K.C.Chang, "Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals", EURASIP Journal on Advances in Signal Processing, Vol.2009, 2009, pp.1-13.

[12] C. W. Zhang, Z. P. Cai, W. F. Chen, et.al., "Flow Level Detection and Filtering of Low-rate DDoS", Computer Networks, Vol. 56, No.15, 2012, pp.3417-3431.

[13] M.Basseville, and I.V.Nikiforov, Detection of Abrupt Changes: Theory and Applications, New Jersey: Prentice Hall, 1993

[14] Ullah Fasee, Tariq Waqas, Arshad Muhammad, *et.al*., "Analysis of Security Techniques for Detecting Suspicious Activities and Intrusion Detection in Network Traffic", International Journal of Computer Science Issues, Vol. 9, No. 2, 2012, pp.259-265.

Ming Yu received the BS degree in electronics engineering in 1998 from Shandong University, China. He received the MS degree and Ph.D degree in information and telecommunication system in 2004 and 2008 from Xidian University, China. He is currently an associate professor in Dalian University of Technology, China. He is also a member of IEEE Computer Society. So far, he has 15 papers published in international journals. His research interests include network security, cloud computing and DoS defense.

Xiong-wei Li received the BS degree in electronics engineering in 1998 from Wuhan Air Force Radar Academy, China. He received the MS degree and Ph.D degree in information and telecommunication system in 2004 and 2008 from Ordnance Engineering College, China. He is currently an associate professor in Ordnance Engineering College, China. He is also a member of IEEE Computer Society. So far, he has 10 papers published in international journals and conferences. His research interests include network security, and DoS defense.