Journal of Universal Computer Science, vol. 15, no. 2 (2009), 488-504
submitted: 20/10/08, accepted: 25/1/09, appeared: 28/1/09 © J.UCS

A New Detection Method for Distributed Denial-of-Service Attack Traffic based on Statistical Test

Chin-Ling Chen
(Department of Information Management
National Pingtung Institute of Commerce
Pingtung, Taiwan 900
clchen@mail.npic.edu.tw)

Abstract: This study has proposed a new detection method for DDoS attack traffic based on two-sample t-test. We first investigate the statistics of normal SYN arrival rate (SAR) and confirm it follows normal distribution. The proposed method identifies the attack by testing 1) the difference between incoming SAR and normal SAR, and 2) the difference between the number of SYN and ACK packets. The experiment results show that the possibilities of both false positives and false negatives are very low. The proposed mechanism is also demonstrated to have the capability of detecting DDoS attack quickly.
Key Words: Security and protection, Network monitoring, Statistical computing
Category: C.2.0, C.2.3, G.3

1 Introduction

Denial of service (DoS) attack deluges the processing queue or link capacity of victim host with counterfeit packets. Distributed denial of service (DDoS) attack is a worse variant that an intruder may command the compromised computers to attack the same victim host at the same time. The difficult part of defending DDoS is that the flooding packets from numerous attackers are launched by an unknown intruder. TCP is the most important traffic in the Internet and 90 % of DDoS attack traffic uses TCP [Moore et al. 2006].

Many methods to defense servers from SYN flooding attacks have been proposed. We may categorize them into three main approaches: packet marking, proactive and reactive. Packet marking approach marks the suspicious packets with some bits at distributed routers, and then filters them in case of violating rule or exceeding threshold. Some IP Traceback schemes [Xiang and Zhou 2005, Muthuprasanna and Manimaran 2005] employ packet marking to trace attacks that use source address spoofing. Proactive approach usually 1) modifies the existing protocol to prevent DDoS attack from happening [Duwairi and Manimaran 2006], or 2) differentiates malicious traffic from normal one with the use of PacketScore [Ayres 2006] or test probability [Gao and Ansari 2006] or with the deployment of intelligent framework [Tupakula et al. 2004, Kong et al. 2003, Keromytis 2004]. On the other hand, reactive approach takes some response after the malicious traffic is detected. Much effort has been concentrated on reactive approach. Particular emphasis is on the designing of threshold algorithm and how they are affected by the parameters of the algorithm [Wang et al. 2002, Siris and Papagalou 2004, Siaterlis and Maglaris 2005, Zou et al 2006, You et al. 2007]. The combination of a coordinated detection and response framework is a more advanced way to mitigate the damage caused by DDoS [Haggerty et al. 2004, Lam et al. 2006]. The proposed framework composes of some heterogeneous defense systems which cooperate with each other to protect from attacks. There is growing interest in the use of statistical-based methods to defend against and mitigate the effect of DDoS attacks [Ohsita et al. 2004, Li et al. 2005, Jin and Yeung 2004, Chuah et al. 2004]. Packet statistics from on-line history data are monitored to classify normal and attack traffic.

Most researches in DDoS focus on designing of an effective countermeasure to detect flooding attack. However, low-rate attack may happen on condition that the rate difference between attackers and normal users is insignificant, thus making backlog queue full. The proposal [Jing et al. 2006] encounters SYN low-rate attack by providing IP traceback-based rate limit algorithm to identify and isolate the malicious traffic.

Unlike most of the previous DDoS defense schemes that only deal with either flooding or meek attack, the proposal uses two statistical tests to identify the malicious traffic. We first compare the differences between the overall means of incoming traffic arrival rate and normal traffic arrival rate by two-sample t-test. If the difference is significant, we may conclude that the traffic may include flooding attack packets. However, the low-rate attack traffic may pass the arrival rate test and makes the backlog queue full. We then compare two groups that contain different number of SYN and ACK packets by two-sample t-test. If there is significant difference, we may recognize that the attack traffic is mixed into the current traffic. It happens that normal traffic is mistaken for attack traffic (False Positives, FP) as well as attack traffic is mistaken for normal traffic (False Negatives, FN). We evaluate both FP and FN of the proposed scheme by conducting some experiments. We also compare the time to detect attack traffic between the proposed scheme and the other methods.

The rest of the paper is organized as follows. Section 2 presents Statistical analysis and detection scheme. We have performance evaluation in section 3. Finally, section 4 concludes this paper.

2 Statistical analysis and detection scheme

In this section, we first confirm the SYN arrival rates (SAR) sampling distribution of normal traffic is fitted to a normal distribution. The traffic from internet to campus network was monitored. We periodically measured SAR and calculated the sample means($\bar{X}$) and sample standard deviations ($\hat{S}$) of the SAR. Let X_1, X_2, ..., X_N be a sample of N measurements. We have

$$\bar{X} = \frac{\sum_{i=1}^{N} X_i}{N} \tag{1}$$

The sample variance($\hat{S}^2$) for a sample of N measurements is equal to the sum of the squared distances from the mean divided by $(N-1)$. Therefore,

$$\hat{S}^2 = \frac{\sum_{i=1}^{N}(X_i - \bar{X})^2}{N-1} \tag{2}$$

The reason we use the divisor $(N-1)$ instead of N is that using N tends to produce an underestimate of the population variance. So we use $(N-1)$ in the denominator to provide the appropriate correction for this tendency. We may rewrite equation (2) as

$$\hat{S}^2 = \frac{\sum_{i=1}^{N} X_i^2 - \frac{(\sum_{i=1}^{N} X_i)^2}{N}}{N-1} \tag{3}$$

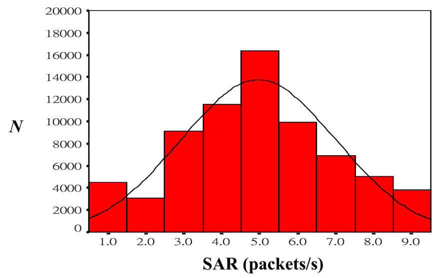
The sample standard deviation, $\hat{S}$, is defined as the positive square root of the sample variance, $\hat{S}^2$. Thus, $\hat{S}= \sqrt{\hat{S}^2}$. We use one-sample Kolmogorov-Smirnov (K-S) test to decide if the samples come from a population with a normal distribution. We have the following hypothesis test.

H_0: The data of normal SAR follow a normal distribution

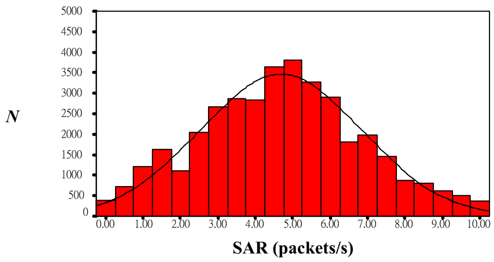
H_1: The data of normal SAR do not follow a normal distribution

We set the sampling Period (M) to be 1, 5 and 10 seconds and colleted SYN packets form 9:00 on October 22, 2007 to 17:00 November 9, 2007. SPSS plots the collected data based on three sampling periods (M=1, 5 and 10) to generate three histograms (Fig.1(a)-(c)) and Table 1. The P-values for three sampling periods are .438, .571 and .762, individually. The P-value of t or F test statistic is the probability, assuming that H_0 is true, of obtaining a value at least as extreme as the given point. Let the level of significant (α) be .05. We can see that all P-values are greater than α= .05, and thus accept the H_0 hypothesis. The data of normal SAR follow a normal distribution.

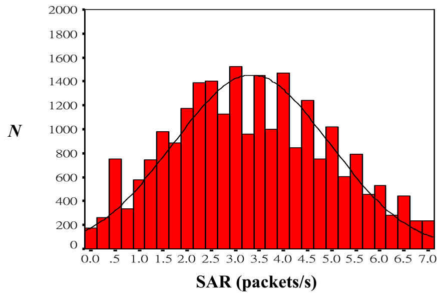
Now we know the sample mean $\bar{X}$ is normally distributed with unknown mean μ. In the real world, finding the standard deviation of an entire population is unrealistic. We may estimate population standard deviation from sample



(a) $M = 1$



(b) $M = 5$



(c) $M = 10$

Figure 1: Sampling distribution

Table 1: One-sample K-S test for SAR

	M=**1**	M=**5**	M=**10**
sample size (N)	70,408	37,533	23,646
sample mean ($\bar{X}$)	4.96	4.68	3.33
sample standard deviation ($\hat{S}$)	2.03	2.16	1.62
P-value	.438	.571	.762

standard deviation. The standard error is $\frac{\hat{S}}{\sqrt{N}}$. We standardize $\bar{X}$ by subtracting the mean and dividing by standard error as follows.

$$Z = \frac{\bar{X} - \mu}{\frac{\hat{S}}{\sqrt{N}}} \tag{4}$$

Now Z has a standard normal distribution. We define confidence interval for μ in the form $l \leq \mu \leq u$, where the end-points l and u are computed from the sample data. We know that different samples produce different values of l and u. The lower bound and upper bound end-points are values of random variables L and U, respectively. We have

$$P\{L \leq \mu \leq U\} = 1 - \alpha \tag{5}$$

where $0 \leq \alpha \leq 1$. There is a probability of $1 - \alpha$ of selecting a sample for which the confidence interval will contain the true value of μ.The end-points of l and u are called the lower and upper-confidence limits, individually. From equation (4), we know that Z has a standard normal distribution. We have

$$P\{-Z_{\alpha/2} \leq \frac{\bar{X} - \mu}{\frac{\hat{S}}{\sqrt{N}}} \leq Z_{\alpha/2}\} = 1 - \alpha \tag{6}$$

where $Z_{\alpha/2}$ is the upper $100\alpha/2$ percentage point of the standard normal distribution. We may rewrite equation (6) as

$$P\{\bar{X} - Z_{\alpha/2}\frac{\hat{S}}{\sqrt{N}} \leq \mu \leq \bar{X} + Z_{\alpha/2}\frac{\hat{S}}{\sqrt{N}}\} = 1 - \alpha \tag{7}$$

Therefore, a $100(1 - \alpha)\%$ confidence interval on μ is given by

$$\bar{X} - Z_{\alpha/2}\frac{\hat{S}}{\sqrt{N}} \leq \mu \leq \bar{X} + Z_{\alpha/2}\frac{\hat{S}}{\sqrt{N}} \tag{8}$$

The confidence interval in equation (8) gives both a lower and upper confidence bound for μ. In this work, we introduce a threshold, Maximum SYN packet Arrival Rates (MSAR), as the boundary between normal SAR and high-rate attack. In order to find out the threshold (D_x) of MSAR, we only obtain upper confidence bounds for μ by setting l = -∞ and replacing $Z_{\alpha/2}$ by Z_α. A 100 $(1 - \alpha)\%$ upper confidence bound for μ is, therefore,

$$\mu \leq D_x = \bar{X} + Z_\alpha\frac{\hat{S}}{\sqrt{N}} \tag{9}$$

where α is set to 0.025

In the following, we use t-test to verify 1) the difference between normal SAR and attack SAR, and 2) the difference between the number of SYN and

ACK packets. The characteristics of t-test are that it is robust and powerful. The robustness means that its assumptions may be violated to some extent, yet the correct statistical decision will still be made. The power of a statistical test refers to its ability to detect a real difference between two groups' means. ISR is defined to be the ratio of the number of incomplete packets (the difference between the number of SYN and ACK packets) to the number of normal SYN packets. We have

$$ISR = \frac{I}{T} \tag{10}$$

where I is the difference between the number of SYN and ACK packets, and T is the number of SYN packets. We set up the second threshold (D_y) to detect the possibility of low-rate attack traffic

A false positive (FP) occurs when the detection method mistakenly flags a normal traffic as being attacked. On the other hand, a false negative (FN) occurs when the attack traffic is classified as normal traffic. Assume s_n is the number of normal SYN packets whose SAR exceeding D_x, S_n is the number of normal SYN packets, s_a is the number of attack SYN packets whose SAR below D_x, and S_a is the total number of attack SYN packets. Both FP rate (P_1) and FN (P_2) rate are described as follows.

$$P_1 = \frac{s_n}{S_n} \tag{11}$$

$$P_2 = \frac{s_a}{S_a} \tag{12}$$

The relation between FP rate (P_1) of FN (P_2) rate of MSAR is shown at Fig.2. Let I_n be the number of normal SYN packets whose ISR exceeding D_y, and I_a be the number of attack SYN packets whose ISR below D_y. Both FP rate (P_3) and FN (P_4) rate of ISR are given as follows.

$$P_3 = \frac{I_n}{S_n} \tag{13}$$

$$P_4 = \frac{I_a}{S_a} \tag{14}$$

Fig. 3 depicts the flowchart of traffic identification. Upon receiving the incoming packets, the host calculates SAR based on the sampling period (M), where M= 1, 5 and 10. We compare incoming SAR and normal SAR with two-sample t-test. If there is significant difference between two groups, we may conclude that there is high-rate attack. Otherwise, we further identify the behavior of a flow by testing the significance of a difference between the number of SYN and ACK packets. If so, we may conclude that the flow has the possibility to attack.

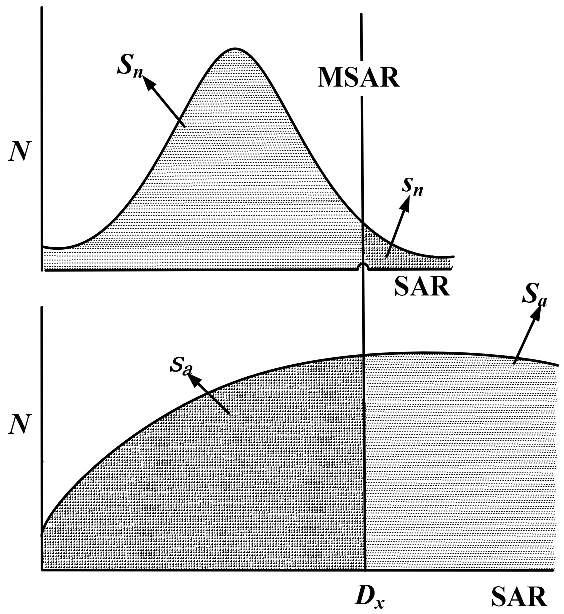


Figure 2: Relation between FP rate (P_1) and FN rate (P_2)

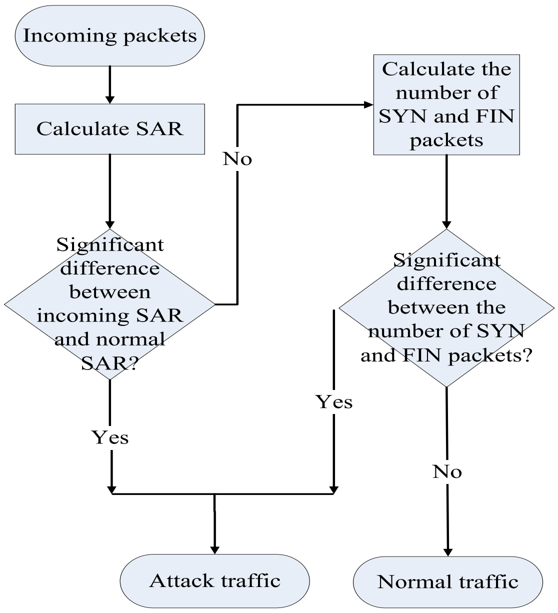


Figure 3: Flowchart of traffic identification

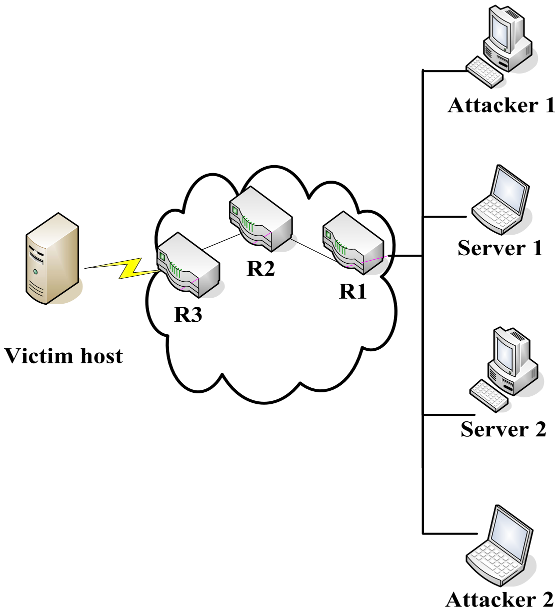


Figure 4: Experimental topology

3 Performance evaluation

Fig. 4 has shown the experimental topology. Suppose Group 1 is a collection of noraml SAR data from 9:00 to 17:00 on October 22, 2007 and Group 2 consists of the attack SAR data generated by attack software tool− Hoepelnuke v0.0.2. Since we do not have any assumptions about attack SAR population distribution, Group 1 and Group 2 are considered as two independent samples. SPSS plots the collected data to generate group statistics (Table 2 and Table 3) and independent sample test (Fig. 5). We use t-test to acertain the significanance of a difference between two population means ($\mu_1 - \mu_2$). Assume the difference between two sample means is ($\bar{X}_1 - \bar{X}_2$), and the standard deviation of the sampling distribution of differences is $\sqrt{(\frac{S_1^2}{N_1} + \frac{S_2^2}{N_2})}$. Therefore,

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{(\frac{S_1^2}{N_1} + \frac{S_2^2}{N_2})}} \tag{15}$$

Obviously, both groups contain different sample size ($N_1 \neq N_2$). We use the pooled variance estimate t-test which considers the difference in sample size by weighting the variance of each sample. The pooled variance estimate is

Table 2: Group 1 statistics

	M=**1**	M=**5**	M=**10**
sample size (N)	16,383	5,463	2,527
sample mean ($\bar{X}$)	142.95	155.70	157.31
sample standard deviation ($\hat{S}$)	33.61	15.19	10.35
standard deviation mean	.2626	.2056	.2059

Table 3: Group 2 statistics

	M=**1**	M=**5**	M=**10**
sample size (N)	13,774	5,572	2,799
sample mean ($\bar{X}$)	2.52	1.81	1.75
sample standard deviation ($\hat{S}$)	5.58	3.05	2.43
standard deviation mean	4.758E-02	4.085E-02	4.592E-02

$$\hat{S}^2 = \frac{(N_1-1)S_1^2 + (N_2-1)S_2^2}{N_1+N_2-2} \tag{16}$$

Therefore, equation (15) can be replaced by

$$t = \frac{\bar{X}_1 - \bar{X}_2}{\sqrt{(\frac{\hat{S}_1^2}{N_1} + \frac{\hat{S}_2^2}{N_2})}} \tag{17}$$

We have the following hyposthesis test.

H_2: μ_1=μ_2

H_3: $\mu_1 \neq \mu_2$

¿From both Table 2 and Table 3, we find that the means ($\bar{X}$)of the two examples are clearly different ((142.95, 2.52), (155.70, 1.81) and (157.31, 1.75)) with the M-value of 1, 5 and 10, individually. Next we need to test the difference is significant or not. Levene's test is used to assess the null hypothesis that the population variances are equal. If the resulting P-value of Levene's test is less than some critical value (0.05, in this study), the null hypothesis of equal variances is rejected. We may conclude that there is a difference between the variances in the population. Fig. 5(a)-(c) tabulate the value of t and its P-value (2-tailed) together with the 95% Confidence Interval of the Difference (CID) for both *Equal variance assumed* and *Equal variance not assumed* situations. We use Levene's test for Equality of Variances to assess the equality of variance assumption of a valid t-test. From Fig. 5, we find that the resulting P-value of Levene's test is 0 (< 0.05) in spite of the value of M. The equality of variance

	Levene test for equality of variances		t-test for equality of means						
								95% CID	
	F	Sig.	t	df	Sig. 2-tailed	Mean Diff.	Std Err. Diff.	lower	upper
Equal variance assumed	32158	.000	487.75	30155	.00	140.43	.2897	132.86	140.99
Equal variance not assumed			526.20	17453	.00	140.43	.2669	139.90	140.95

(a) *M* = 1

	Levene test for equality of variances		t-test for equality of means						
								95% CID	
	F	Sig.	t	df	Sig. 2-tailed	Mean Diff.	Std Err. Diff.	lower	upper
Equal variance assumed	10233	.000	740.98	11033	.00	153.89	.2077	153.49	154.30
Equal variance not assumed			134.26	5892.9	.00	.89	.2096	153.48	155.30

(b) *M* = 5

	Levene test for equality of variances		t-test for equality of means						
								95% CID	
	F	Sig.	t	df	Sig. 2-tailed	Mean Diff.	Std Err. Diff.	lower	upper
Equal variance assumed	1634.9	.000	772.04	5324	.00	155.56	.2015	155.17	155.96
Equal variance not assumed			737.49	2777.4	.00	155.56	.2109	155.15	155.98

(c) *M* = 10

Figure 5: Normal and attack SAR independent samples test

assumption has been violated and the normal t-test based on separate variance estimates is used (*Equal variance not assumed*). The obtained differences in sample variances are likely to have occurred. With a P-value of 0 the difference between means is significant. This is also confirmed by the 95% CID for the difference between means ((142.95, 2.52), (155.70, 1.81) and (157.31, 1.75)) in Table 2 and Table 3. We therefore rejects the H_2 mean difference of 0 between normal SAR and attack SAR. Since the P-value (0) is less than 0.05, the result

Table 4: Group 3 statistics

	M=**1**	M=**5**	M=**10**
sample size (N)	225,280	78,523	38,966
sample mean ($\bar{X}$)	.33	.34	.36
sample standard deviation ($\hat{S}$)	.37	.29	.27
standard deviation mean	7.80E-04	1.03E-03	1.34E-03

Table 5: Group 4 statistics

	M=**1**	M=**5**	M=**10**
sample size (N)	225,280	78,521	38,966
sample mean ($\bar{X}$)	.70	.66	.64
sample standard deviation ($\hat{S}$)	.37	.29	.27
standard deviation mean	7.80E-04	1.03E-03	1.34E-03

is significant beyond the 5-per cent level.

Assume Group 3 and Group 4 collect SYN and ACK packets from 9:00 to 17:00 on October 22-31, 2007, individually. Both groups have the same sample size. We use t-test equation (17) to test the significance of a difference between two population means ($\mu_3 - \mu_4$). Assume the difference between two sample means is ($\bar{X}_3 - \bar{X}_4$). We have the following hypothesis test.

H_4: μ_3=μ_4

H_5: $\mu_3 \neq \mu_4$

From both Table 4 and Table 5, we can find that the means ($\bar{X}$) of the two examples are slightly different ((.33, .70), (.34, .66), (.36, .64)) with the M-value of 1, 5 and 10, individually. We also use Levene's test to test the hypothesis that the variances in the two groups are equal. Fig. 6 has shown that Levene's test is not-significant (P-value = 1.0 > 0.05) regardless of M-value. We must accept the null hypothesis that the difference between the variance is 0. That is, the variance is roughly equal and the assumption is tenable. We should read the row labeled *Equal variance assumed.* In the case of M = 1, 5, 10, the two-tailed P-value are all 0 (< 0.05). We may conclude that there is significant difference between the number of SYN and ACK packets.

To illustrate the effects of an attack on the proposed method, we collect the SYN and ACK packets from 9:00 to 17:00, 11/26-27, with a simulated attack source. We set the sampling period (M) to be 1, 5 and 10 seconds individually and use the collected samples to obtain the threshold D_x and D_y (Table 6). We may identify high-rate attack by observing the traffic flow with SAR exceeding

	Levene test for equality of variances		t-test for equality of means					95% CID	
	F	Sig.	t	df	Sig. 2-tailed	Mean Diff.	Std Err. Diff.	lower	upper
Equal variance assumed	.000	1.000	-307.4	450558	.00	-.3391	1.1E-03	-.3413	-.3370
Equal variance not assumed			-307.4	450558	.00	-.3391	1.1E-03	-.3413	-.3370

(a) ***M*** **= 1**

	Levene test for equality of variances		t-test for equality of means					95% CID	
	F	Sig.	t	df	Sig. 2-tailed	Mean Diff.	Std Err. Diff.	lower	upper
Equal variance assumed	.000	1.000	-214	157042	.00	-.3124	1.4E-03	-.315	-.309
Equal variance not assumed			-214	157042	.00	-.3124	1.4E-03	-.315	-.309

(b) ***M*** **= 5**

	Levene test for equality of variances		t-test for equality of means					95% CID	
	F	Sig.	t	df	Sig. 2-tailed	Mean Diff.	Std Err. Diff.	lower	upper
Equal variance assumed	.000	1.000	-147.8	77930	.00	-.280	1.9E-03	-.284	-.277
Equal variance not assumed			-147.8	77930	.00	-.280	1.9E-03	-.284	-.277

(c) ***M*** **= 10**

Figure 6: SYN and ACK independent samples test

D_x. We define accuracy rate (AR) to be the possibility of not being erroneous identification. Table 7 and Table 8 list normal and attack SAR AR on 11/26 and 11/27, respectively. We find that the AR rate of normal traffic SAR is greater than 96% despite the value of M. Furthermore, the AR of attack traffic SAR is nearly 99.99%. Both FP rate and FN rate of normal traffic and attack traffic with their corresponding AR are shown in Table 9 and Table 10. We found that normal traffic with M=1 generates FP rate roughly between 5% and 7%. However, the

Table 6: The threshold value of D_x and D_y

	M=**1**	M=**5**	M=**10**
D_x	4.707	3.787	3.716
D_y	.6695	.6541	.6390

Table 7: SAR AR (11/26)

	M=**1**	M=**5**	M=**10**
S_n (packets)	41,875	41,875	41,875
S_a (packets)	3,330,019	3,330,019	3,330,019
s_n (packets)	909	652	386
s_a (packets)	25	0	0
FP (P_1)	2.17%	1.56%	.92%
FN (P_2)	.008%	0	0
Normal traffic AR (100% − P_1)	97.83%	98.44%	99.08%
Attack SAR AR (100% − P_2)	99.99%	100%	100%

Table 8: SAR AR (11/27)

	M=**1**	M=**5**	M=**10**
S_n (packets)	38,116	38,116	38,116
S_a (packets)	5,601,231	5,601,231	5,601,231
s_n (packets)	1,326	529	161
s_a (packets)	99	0	0
FP (P_1)	3.47%	1.38%	.42%
FN (P_2)	.0018%	0	0
Normal traffic AR (100% − P_1)	96.53%	98.62%	99.58%
Attack traffic AR (100% − P_2)	99.99%	100%	100%

FN rate of SAR is greater than 96% with the value of M=5, 10. The AR of attack traffic is also close to 99.99%. The proposed method is demonstrated to effectively catch attack traffic without generating false positives. Fig. 7 and Fig. 8 illustrate SAR AR and ISR AR, individuallly.

In Fig. 9, we compare the time needed to detect high-rate and low-rate attacks on the proposed scheme with the time on SYN-FIN method [Siris and Papagalou 2004] and SYN arrival method [Ohsita et al. 2004]. We vary the SYN rate of attack traffic and set SYN rate to be 20 as the boundary between high-rate and

Table 9: ISR AR (11/26)

	M=**1**	M=**5**	M=**10**
T_n (packets)	41,875	41,875	41,875
T_a (packets)	3,330,019	3,330,019	3,330,019
I_n (packets)	2,377	1,326	201
I_a (packets)	43	0	0
FP (P_3)	5.68%	3.17%	.48%
FN (P_4)	.0013%	0	0
Normal traffic AR (100% – P_3)	94.32%	96.83%	99.52%
Attack traffic AR (100% – P_4)	99.99%	100%	100%

Table 10: ISR AR (11/27)

	M=**1**	M=**5**	M=**10**
T_n (packets)	38,116	38,116	38,116
T_a (packets)	5,601,231	5,601,231	5,601,231
I_n (packets)	2,569	644	278
I_a (packets)	537	0	0
FP (P_3)	6.74%	1.69%	.73%
FN (P_4)	.0096%	0	0
Normal traffic AR (100% – P_3)	93.26%	98.31%	99.27%
Attack traffic AR (100% – P_4)	99.99%	100%	100%

low-rate attack. Both of the proposed scheme and SYN arrival method adopt parametric approach to identify high-rate attack, while SYN-FIN method uses a non-parametric approach. The parametric approach is capable of detecting high-rate attack faster and much more accurately than the non-parametric one since the data is fitted into the model. Moreover, the performance of the proposed scheme is better than that of SYN arrival method. SYN arrival method setup the threshold to detect all attacks. However, the computation of threshold value is very complicated. For each measurement of SYN arrival rate, the collected data needs to be sorted and labeled, and then the average of square differences from normal distribution is calculated. The proposed scheme uses the t-test to determine whether there is a significant difference between normal SAR and attack SAR. An attractive characteristic of t-test is responsiveness, which means that t-test works well regardless of the sample size. During the period of low-rate attack, the proposed scheme still outperforms the other two methods. SYN arrival method cannot detect low-rate attack efficiently since the low rate attack

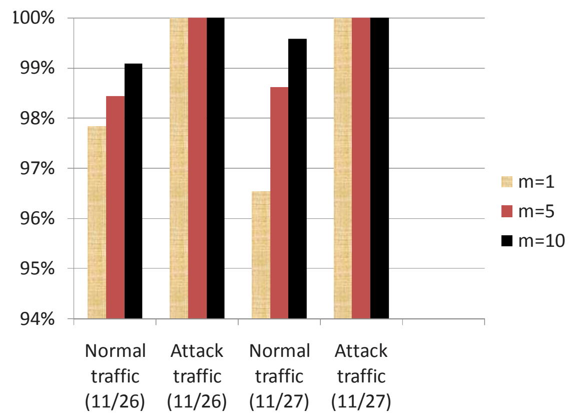


Figure 7: SAR AR

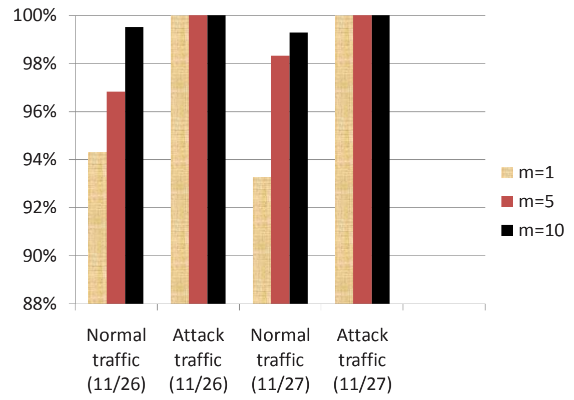


Figure 8: ISR AR

follows the normal distribution. SYN-FIN method calculates the traffic value by normalizing the difference between the number of SYN and FIN packets, thus leading more computation. The proposed scheme has the advantage of detecting low-rate attack by simply testing the difference between the number of SYN and ACK packets. The proposed scheme has the lowest detection time. The reason is the responsive characteristic of t-test, which is mentioned above. We also find that the time to detect high-rate attack is much faster than low-rate attack on our method. For high-rate attack detection only one SYN packet is needed to identified and processed. On the other hand, low-rate attack detection requires identification of both SYN and ACK packets, resulting in more computation

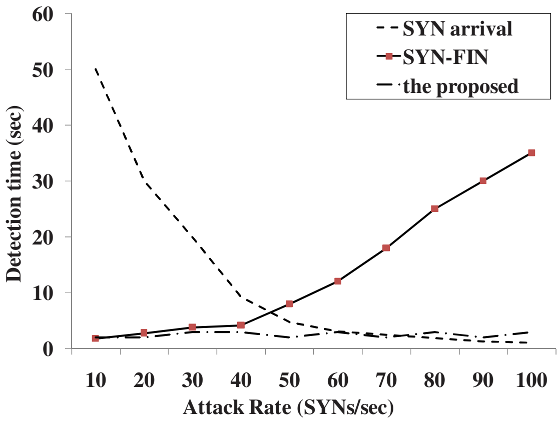


Figure 9: Detection time

time. This also explains why we deploy high-rate attack detection before low-rate attack detection at traffic identification flowchart (Fig. 3).

4 Conclusions

In this study, we have proposed a simple, robust and efficient DDoS detection mechanism. Two statistical t-tests are applied to detect the possible DDoS attack. This proposed method can effectively differentiate between normal and flooding traffic. Indeed, this method can detect even very subtle attacks only slightly different from normal behaviors. The proposed scheme does not hold the three-way handshaking states but only count the SYN and ACK packets, thus making low computation overhead. The efficacy of this detection mechanism is validated by experimental simulations. The evaluation results show that the detection mechanism has low false positive and false negative rate, and short detection time.

References

[Ayres 2006] Ayres, P. E., Sun, H., Chao, H. Jonathan, Lau, W. C.: "ALPi: A DDoS defense system for high-speed networks"; IEEE Journal on Selected Areas in Communications, 24, 10 (October 2006), 1864-1876.

[Chuah et al. 2004] Chuah, M. C., Lau, W. C., Kim, Y., Chao, H. Jonathan: "Transient performance of packetScore for blocking DDoS attacks"; ICC 2004-IEEE International Conference on Communications, 1 (June 2004), 1892-1896.

[Duwairi and Manimaran 2006] Duwairi, B. A., Manimaran, G.: "Intentional dropping: A novel scheme for SYN flooding mitigation"; IEEE INFOCOM 2006-IEEE International Conference on Computer Communications, 1 (April 2006), 3030-3034.

[Gao and Ansari 2006] Gao, Z., Ansari, N.: "Differentiating malicious DDoS attack traffic from normal TCP flows by proactive tests"; IEEE Communications Letters, 10, 11 (November 2006), 793-795.

[Haggerty et al. 2004] Haggerty, J., Berry, T., Shi, Q., Merabti, M.: "DiDDeM: A system for early detection of TCP SYN flood attacks"; GLOBECOM 2004-IEEE Global Telecommunications Conference, 1 (Dec 2004), 5011-5011.

[Jin and Yeung 2004] Jin. S., Yeung, D. S.: "A covariance analysis model for DDoS attack detection"; ICC 2004-IEEE International Conference on Communications, 1 (June 2004), 1882-1886.

[Jing et al. 2006] Jing, Y., Wang, X., Xiao, X., Zhang, G.: "Defending against meek DDoS attacks by IP traceback-based rate limiting"; GLOBECOM 2006-IEEE Global Telecommunications Conference, 1 (November 2006), 1475-1479.

[Keromytis 2004] Keromytis, D.: "Vishal Misra and Dan Rubenstein SOS: An architecture for mitigating DDoS attacks"; IEEE Journal on Selected Areas in Communications, 22, 1 (Jan 2004), 176-188.

[Kong et al. 2003] Kong, J., Mirza, M., Shu, J., Yoedhana, C., Gerla, M., Lu, S.: "Random flow network modeling and simulations for DDoS attack mitigation"; ICC 2003-IEEE International Conference on Communications, 1 (May 2003), 487-491.

[Lam et al. 2006] Lam, H. Y., Li, C. P., Chanson, S. T., Yeung, D. Y.: "A coordinated detection and response scheme for distributed denial-of-service attacks"; ICC 2006-IEEE International Conference on Communications, 1 (June 2006), 2150-2155.

[Li et al. 2005] Li, Q., Chang, E. C., Chan, M. C.: "On the effectiveness of DDoS attacks on statistical filtering"; IEEE INFOCOM 2005-IEEE International Conference on Computer Communications, 1 (March 2005), 1373-1383.

[Moore et al. 2006] Moore, D., Shannon, C., Brown, D. J., Voelker, G. M., Savage, S.: "Inferring Internet Denial-of-Service activity"; ACM Transactions on Computer Systems, 24, 2 (May 2006), 115-139.

[Muthuprasanna and Manimaran 2005] Muthuprasanna, M., Manimaran, G.: "Space-time encoding scheme for DDoS attack traceback"; GLOBECOM 2005-IEEE Global Telecommunications Conference, 1 (November 2005), 457-461.

[Ohsita et al. 2004] Ohsita, Y., Ata, S., Murata, M.: "Detecting distributed denial-of-service attacks by analyzing TCP SYN packets statistically"; GLOBECOM 2004-IEEE Global Telecommunications Conference, 1 (Dec 2004), 5012-5012.

[Siaterlis and Maglaris 2005] Siaterlis, C., Maglaris, B.: "Detecting DDoS attacks using a multilayer perception classifier"; IM 2005-IFIP/IEEE International Symposium on Integrated Network Management, 1 (May 2005), 1133-1136.

[Siris and Papagalou 2004] Siris, V. A., Papagalou, F.: "Application of anomaly detection algorithms for detecting SYN flooding attacks"; GLOBECOM 2004-IEEE Global Telecommunications Conference, 1 (Dec 2004), 5013-5013.

[Tupakula et al. 2004] Tupakula, U. K., Varadharajan, V., Gajam, A. K.: "Counteracting TCP SYN DDoS attacks using automated model"; GLOBECOM 2004-IEEE Global Telecommunications Conference, 1 (Dec 2004), 5071-5071.

[Wang et al. 2002] Wang, H., Zhang, D., Shin, K. G.: "Detecting SYN Flooding attacks"; IEEE INFOCOM 2002-The Conference on Computer Communications, 1 (June 2002), 1530-1539.

[Xiang and Zhou 2005] Xiang, Y., Zhou, W.: "Mark-aided distributed filtering by using neural network for DDoS defense"; GLOBECOM 2005-IEEE Global Telecommunications Conference, 1 (November 2005), 316-320.

[You et al. 2007] You, Y., Zulkernine, M., Haque, A.: "Detecting flooding-based DDoS attacks"; ICC 2007-IEEE International Conference on Communications, 1 (June 2007), 1229-1234.

[Zou et al 2006] Zou, C. C., Duffield, N., Towsley, D., Gong, W.: "Adaptive defense against various network attacks"; IEEE Journal on Selected Areas in Communications, 24, 10 (October 2006), 1877-1888.