A Two-Tier Coordination System against DDoS Attacks

http://dx.doi.org/10.3991/ijoe.v9i4.2820

Chin-Ling Chen* and Chih-Yu Chang
National Pingtung Institute of Commerce, Pingtung, Taiwan

***Abstract*—We present a two-tier coordination approach for detecting and mitigating DDoS attacks. The first tier traffic filter (1st-TF) filters suspicious traffic for possible flooding. This is achieved by using proactive tests to identify and isolate the malicious traffic. The second tier traffic filter (2nd-TF), which is deployed on network routers, performs online monitoring on queue length status with RED/Droptail mechanism for any incoming traffic. The simulation shows that the scheme can detect attacks accurately and effectively.**

***Index Terms*—coordination, DDoS, queue length, rate control.**

I. INTRODUCTION

There is a growing international public discussion on DDoS attacks. DDoS attacks deliberately exhaust resources such as CPU, memory and bandwidth in computer systems or networks. The actions may deny access from other users. Recently, many methods of DDoS detection have been proposed. We may categorize them into two main approaches: TCP-based and IP-based detection. TCP-based detection [1-3] discovers the attacks by analyzing the ratio of TCP packets to its related flags, such as SYN, FIN, ACK and RST. For normal host, the number of TCP flags sent to and received from should be equivalent within a range of error tolerance. On the other hand, an attacker will hardly issue any corresponding response.

Most DDoS related studies have focused on the IP-based detection, which further classified into two approaches: volume-based and attribute-based. Conventional volume-based detections [4-5] usually define some rules and conditions to distinguish the difference between normal and abnormal traffic. The abnormal traffic refers to constant rate attack as well as increasing rate attack. However, a stealthy attack, also called shrew or pulsing attack [6-7], is found to be very difficult to be detected based on solely volume-based schemes. Such attack exhibit high peak rate periodically while maintaining low average rate. The attacker imposes significant damage to the victim host with small volume of traffic without being noticed. To deal with such attack requires a further analysis of TCP flags received at the destination.

Existing attribute-based detection schemes require header information, such as source IP address [8-12], time-to-live (TTL) [13-20] to distinguish between legitimate and attack traffics. However, some DDoS attacks could flood the victim by spoofing a legitimate source address. Distance-based schemes [13-14] work on the variation of the average distance value and detect the anomalous distance values. The distance of the packet is the final TTL value deducted from the initial value. Nevertheless, the attackers can distribute attack traffic for all distances with the same distribution of normal traffic. In this case, the average value of distance for both of the attacker and the legitimate will be the same. The concept behind stack marking [9] is very similar to that for TTL marking. In stack marking, each router along the path from source to destination must contribute some aggregate information to record the IP identification field. Each router treats the IP identification field as though it were a stack. Furthermore, the need to analyze the combination of multiple attributes surely complicates the computation, and, possibly increases false positive rate. To recognize an attack signature of incoming flow, apparently, is neither sufficient nor efficient for detecting DDoS attacks.

To reduce the workload of routers and perform the enhancement of protection, we propose a two-tier coordination architecture for detecting DDoS attacks. Two approaches, namely, Rate-based (RB) and queue-length-based (QLB) detection, are deployed at the routers of the first traffic filter (1st-TF) and the second traffic filter (2nd-TF), respectively. The 1st-TF router is defined as the router of the proposed architecture located closest to the attack source. On the other hand, the 2nd-TF router is the nearest possible point to the victim host. In the RB approach, the routers are assigned a flow list, which is maintained by Data Transit Agent (DTA). During a suspicious attack, the 1st-TF routers query the flow list by checking for specific source/destination address pairs. This approach is useful if the attack signature or attack pattern is identifiable. However, a wide range of spoofed addresses might not be captured by the routers. Therefore, we set up some thresholds, such as arrival rate, the number of passing and the number of failure to further examine the suspicious traffic. Unlike high-rate attacks, the low-rate attacks remain undetected, but impose significant damage to the victim with a small amount of flood. QLB approach is used to detect the possible attack traffic, especially low rate attack, by

observing the number of dropped packets by implementing two kinds of queue management- Droptail and RED [21]. In Droptail, the overflow packets are discarded once the buffer is full. It drops packets as the means for congestion notification. However, low throughput and high delay are the major shortcomings. RED, the emerging concept of Active Queue Management (AQM), is proposed as simple solution to above problems. When detecting impending congestion, RED uses a single linear drop function to calculate the drop probability of a packet. The heavier the overload is, the more packets it drops. The system keeps a history of the arrival rate and drop rate for each flow. A flow is declared to be the attack traffic when its arrival rate has not decreased in response to a substantial increase in its drop rate.

The rest of the paper is organized as follows. Section 2 presents the proposed system. We have simulation and results in section 3. Finally, section 4 concludes this paper.

II. THE PROPOSED SYSTEM

1st-TF: Fig. 1 is the proposed system. Table 1 describes the flow list. When a packet arrives, the 1st-TF first decides which flow the packet belongs by checking the tuple of (source address, destination address, source port number, destination port number, protocol). If it is a new one, the above information is added into flow list.

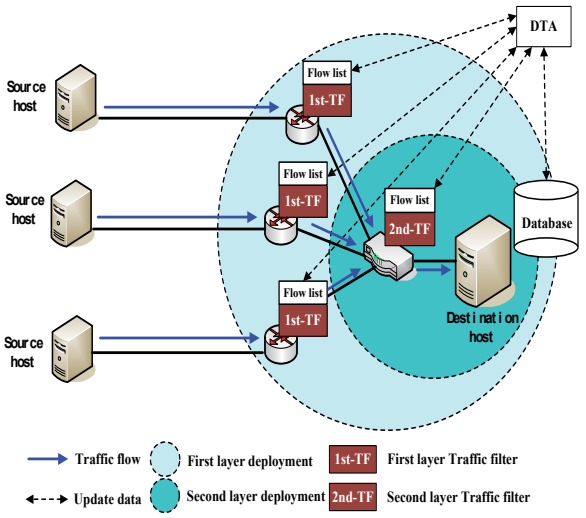

Fig. 1 System Architecture

The 1st-TF then determines whether the flow is aggressive traffic or not by checking the *aggressive traffic* filed in the flow list. If so, the packet is discarded. The decision of aggressive traffic comes from 2nd-TF, which will be mentioned later. We define flow i as ith flow receiving at the router. Assume N_i^s and N_i^f is the number of success and failure for flow i, respectively. If N_i^f is larger than a failure threshold (f), flow i is considered to be suspicious traffic by treating with prudence.

To accommodate high-rate legitimate traffic, we set up a success threshold (h) to define a maximal number of successful tests for a flow. Once flow i works well to pass the threshold, flow i is considered as normal traffic and is not needed to take the test again. Let G_i be a gap variable to represent the difference between the number of success and failure tests for flow i. That is, $G_i = N_i^f - N_i^s$. Assume $R_i(t)$ is the arrival rate of flow i at time t and T_i is the threshold of $R_i(t)$. The threshold T_i is adjusted based on the following equation.

$$T_i = R_i(t\text{-}1) * \left(k - \frac{G_i}{10}\right), \quad (1)$$

where k is an adjustable parameter, which is initiated to be 1.5. When the number of success tests is less than the number of failures ($G_i < 0$), we say that the system is a good possibility under attack by flow i. The threshold should be reduced to tighten the admission criteria and vice-versa. In the case that flow i conforms to that constraint ($R_i^t \le T_i$), $N_i^s$is incremented by 1. Otherwise, N_i^f is incemented by 1. Fig. 2 depicts the flowchart of 1st-TF detection.

Table 1 Description of flow list

Name	Data type	Example
Source address	char	203.64.123.56
Destination address	char	59.127.124.33
Source port number	int	80
Destination port number	int	80
Protocol	char	TCP
Suspicious traffic	boolean	True
Aggressive traffic	boolean	False

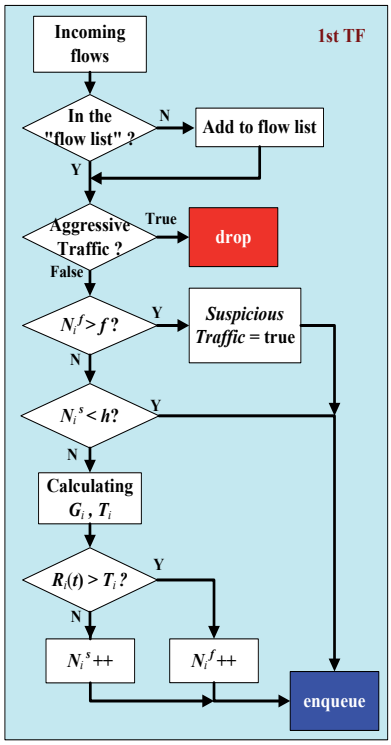

Fig. 2 Flowchart of 1st-TF detection

2nd-TF: 2nd-TF is used to evaluate the potential low-rate attack condition by observing the dropping rate based on queue-length management. Two detection schemes are proposed in 2nd-TF. The first one is Random early

detection (RED). RED randomly and early drops (eDrop) packets based on the average queue length by detecting the incipient condition.

Let P_i^T and P_i^{LD} denote the counter to count the number of enqueued packets and the number of enqueued packets after eDrop for flow i, respectively. Once an arriving packet is accepted, both P_i^T and P_i^{LD} are incremented by 1. Otherwise, the arriving packet is dropped with a probability that depends on the average queue size. The drop probability is calculated the same as in RED. We use the queue occupancy ratio (QOR) to indicate the possibility of low-rate attacks. QOR is expressed by

$$QOR = \frac{P_i^{LD}}{P_i^T} \quad (2)$$

Assume N_i^c is a counter to count the number of incipient congestion for flow i. Once QOR is below the threshold (c), N_i^c is incremented by 1. P_i^{LD} is then reset to 0. If N_i^c exceeds their threshold (q), the system further identifies whether flow i is suspicious traffic or not by examining *suspicious traffic* field of flow list through DTA. If so, the flow is considered as aggressive traffic. DTA then modifies the Boolean value of *aggressive traffic* field of flow list. The packet is discarded. Fig. 3 is the flowchart of 2nd-TF detection with RED.

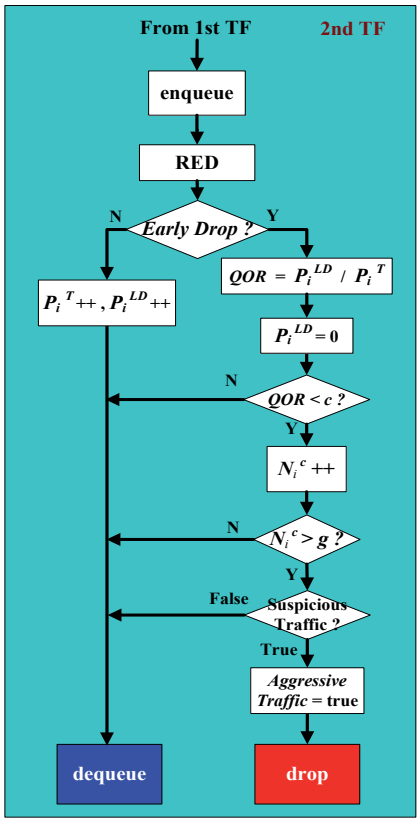

Fig. 3 Flowchart of 2nd-TF detection (RED)

The second one is Droptail. Assume $N^q(t)$ and $N_i^q(t)$ is the current queue length and the number of enqueued packets for flow i at time t. Let Q be the physical queue length, Q_{MAX} be the threshold of queue occupancy (0.8, recommended in this article), q_{limit} be the target queue length, individually. We have

$$q_{limit} = Q \times Q_{MAX} \quad (3)$$

If $N^q(t)$ is larger than q_{limit}, we analyze the queue length share of all flows to identify whether there is a possibility of low-rate attacks. Let PR_i represent the ratio of enqueued packets for flow i. We have

$$PR_i = \frac{N_i^q(t) - N_i^q(t-1)}{N^q(t) - N^q(t-1)} \quad (4)$$

Let pr and N_i^{PR} denote the threshold of queue length share and a counter to record the number of queue overlength for flow i, respectively. If PR_i is larger than pr, N_i^{PR} is incremented by 1. Once N_i^{PR} is equal to the threshold m, we further examine whether the flow is suspicious traffic, which is identified by 1st-TF. If so, we may consider the flow is attack traffic and update the value of *aggressive traffic* field of flow list through DTA. Fig. 4 is the flowchart of 2nd-TF detection with Droptail.

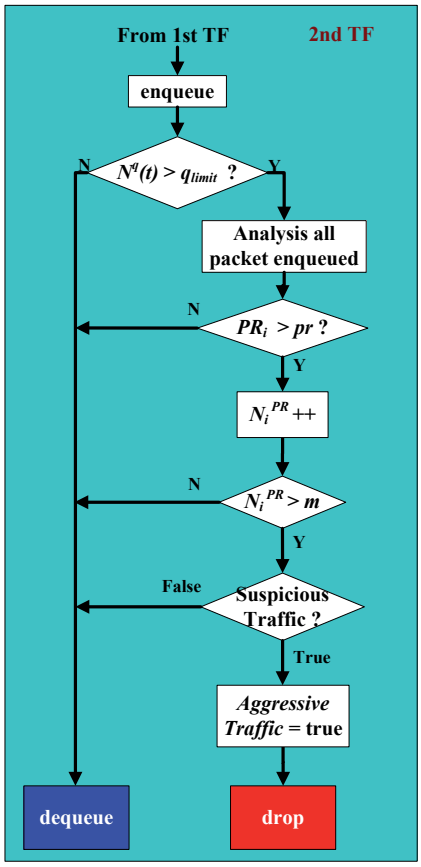

Fig. 4 Flowchart of 2nd-TF detection (Droptail)

III. EXPERIMENTS AND EVALUATION

Fig. 5 represents the simulation environment. We develop a simulation model in NS-2 [22]. Each source generates one or more flows. Table 2 represents the number of normal flows and attack flows in the experiment. Well-behaved sources generate UDP traffic at CBR or TCP traffic at a FTP of 6 Mbps as the normal traffic. Ill-behaved source generate UDP traffic at an on/off model

as the attack traffic. The parameters in the on/off source model are burst time, idle time, traffic rate. False Positive Rate (FPR) is the possibilities of identifying normal traffic as defective, while False Negative Rate (FNR) is the possibilities of identifying attack traffic as non-defective. We conduct four set of experiments to validate our scheme. In the first three experiments, we study FPR and FNR for the 1st-TF, 2nd-TF RED and 2nd-TF Droptail, individually, to find out the optimal parameter value. Finally, we use the selected parameter values to compare 2nd-TF alone and 1st-TF together with 2nd-TF.

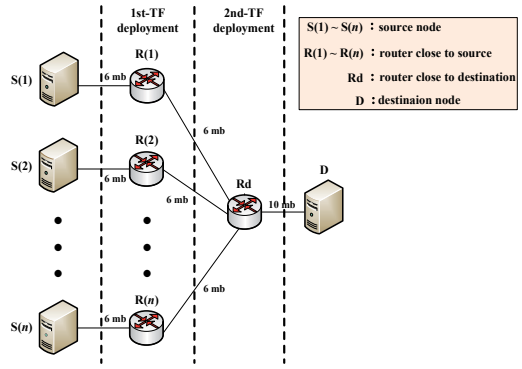

Fig. 5 Simulation environment

Table 2 Number of normal flows and attack flows

Total number of flows	Number of normal flows	Number of attack flows
100	90	10
200	190	10
300	285	15
400	380	20
500	480	20
600	580	20
700	680	20
800	780	20
900	880	20
1000	980	20

Experiment 1: Fig. 6(a) and (b) represent FPR and FNR for 1st-TF with increasing number of flows, individually. We fix the value of *h* as 10 while varying the value of *f* (3, 5 and 7). We found that a small *f* value will increase the possibility of identifying attack traffic, thus leading to lower FPR and FNR. We also vary the value of *h* (5, 10 and 15) while fixing the value of *f* to be 3. We can see from Fig. 7(a) and (b) that a small *h* value incurs lower FPR, but higher FNR. The reason is that both malicious and legitimate traffic will easily pass the success test in case of slacken threshold. Therefore, a moderate value (*h*=10) is recommended for further experimenting.

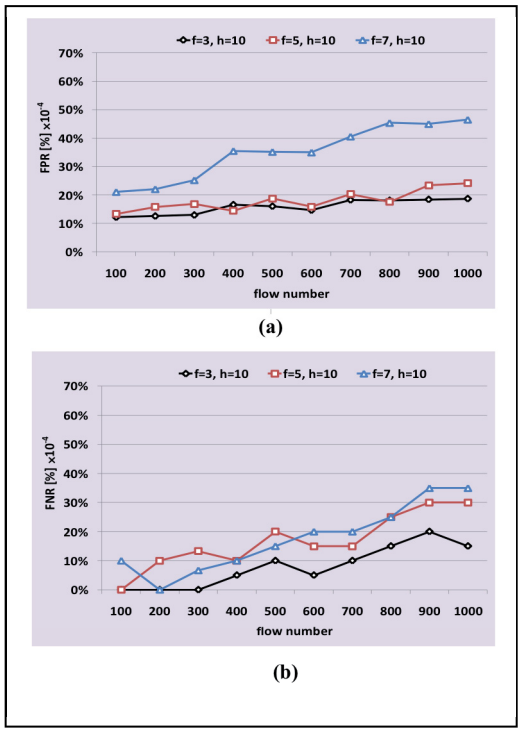

Fig. 6 (a) FPR and (b) FNR for 1st-TF with fixed value *h*

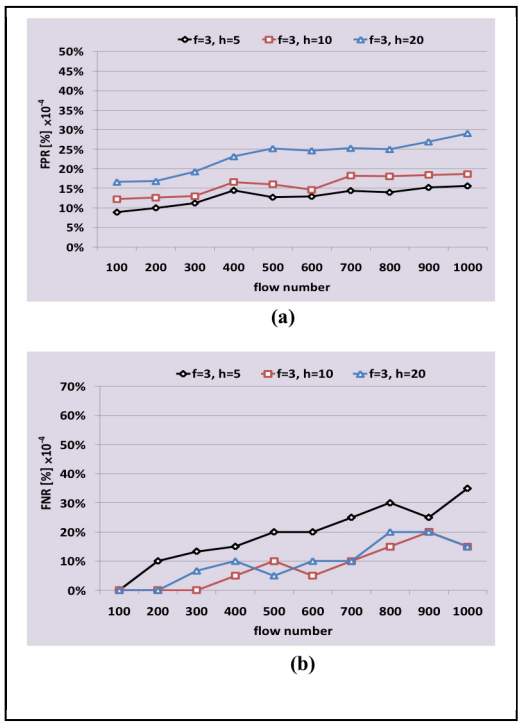

Fig. 7 (a) FPR and (b) FNR for 1st-TF with fixed value *f*

Experiment 2: Fig. 8(a) and (b) show FPR and FNR identified for varying number of flows using 2nd-TF RED, individually. We first take *g* as a constant and vary the value of *c* (0.1, 0.3 and 0.5). We found that a small *c* value (0.1) tends to reduce the effectiveness of system filtering and simply pass the normal traffic, thus causing low FPR and high FNR.

On the other hand, a large *c* value (0.5) has a tendency toward rigidness, hence achieving high FPR and low FNR. An optimal *c* value (0.3) therefore is selected for the following experiment. We fix the value of *c* to be 0.3 and change the value of *g* (3, 5 and 7). From Fig. 9(a) and (b), we can see that the effect of a large *g* value (7) is the same as that of a small *c* value. It is highly accurate to

identify the non-defective traffic as legal one (low FPR), but there is good possibility that the illlegal traffic ends up being not detected (high FNR). A medium *g* value (5) is, therefore, chosen.

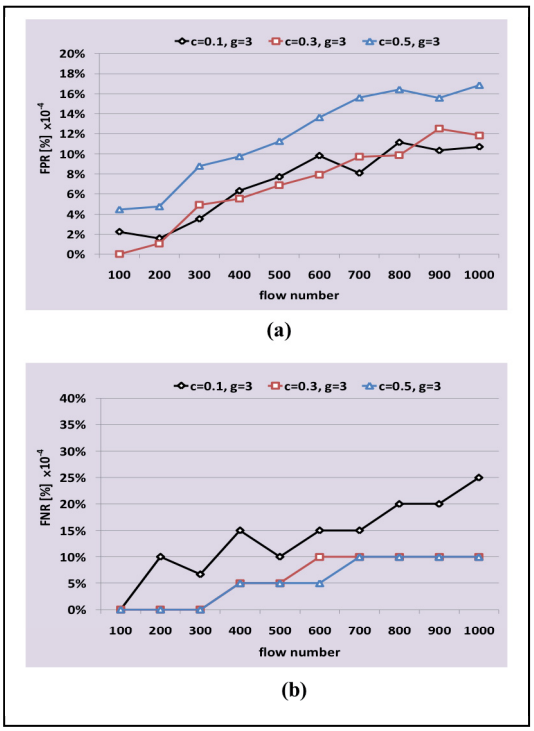

Fig. 8 (a) FPR and (b) FNR for 2nd-TF RED with fixed value *g*

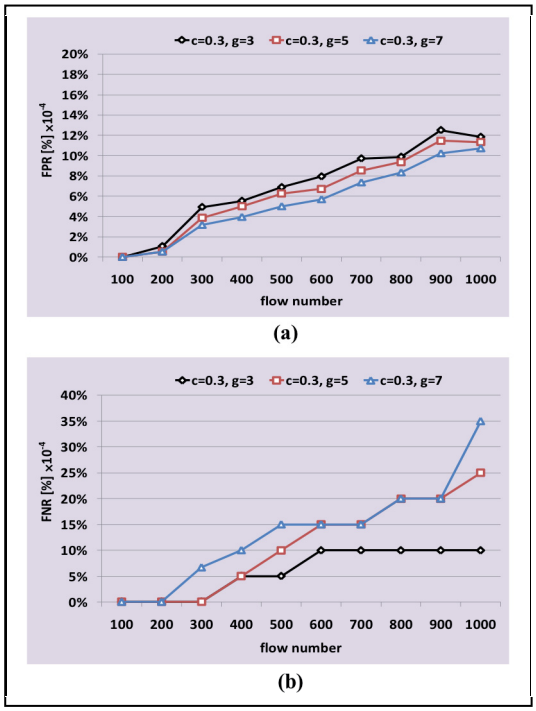

Fig. 9 (a) FPR and (b) FNR for 2nd-TF RED with fixed value *c*

Experiment 3: In this experiment, we examine two parameters of 2nd-TF Droptail, *m* and *pr*, to estimate the FPR and FNR in the presence of varying number of flows. We first take *m* as a constant (10) and adjust the threshold *pr* (0.3, 0.5 and 0.7). From Fig. 10(a) and (b), we can see that FPR is low but FNR is high in case of large *pr* value (0.7). A large percentage of attack traffic cannot be detected in this situation. The effect of raising the threshold value increases the possibility of admitting the traffic, regardless of legal and illegal ones, and vice-versa. A moderate *pr* value (0.5) seems to be better for the subsequent experiment. *pr* is, thereby, fixed to be 0.5 and *m* is varying from 5, 10 and 15. We found that the two curves (m =10 and m =15) have the same trend in FPR (Fig. 11(a)) and FNR (Fig. 11(b)). We may conclude that the effect of filtering makes no difference in case of $m \geq 10$.

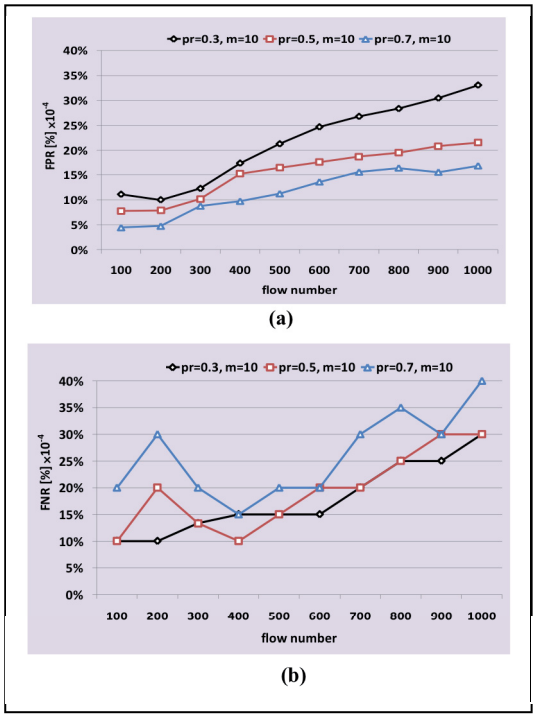

Fig. 10 (a) FPR and (b) FNR for 2nd-TF Droptail with fixed value *m*

Experiment 4: Finally, we experiment solely 2nd-TF as well as together 1-st TF and 2nd-TF with the parameter values recommended above. Fig. 12(a) shows that all four curves increase as the number of flows grows. The FPR for 2nd-TF RED has the worst performance. So does FNR for 2nd-TF RED in Fig. 12(b). The reason is that the arrival rate of a flow may not depend only on the drops at the router, but also on the demand from application, and the drops elsewhere along the path. Therefore, legal packet can be easily identified as illegal one, and vice-versa. However, both FPR and FNR of together 1st- TF and 2nd-TF RED outperform the other three schemes. For flows identified as suspicious by 1st-TF, 2nd-TF drops packets with a reasonably unbiased sample of the traffic. The packet drops from the RED has sent congestion indication by the router. If the discarded packet is legal, the sending rate will be reduced based on TCP

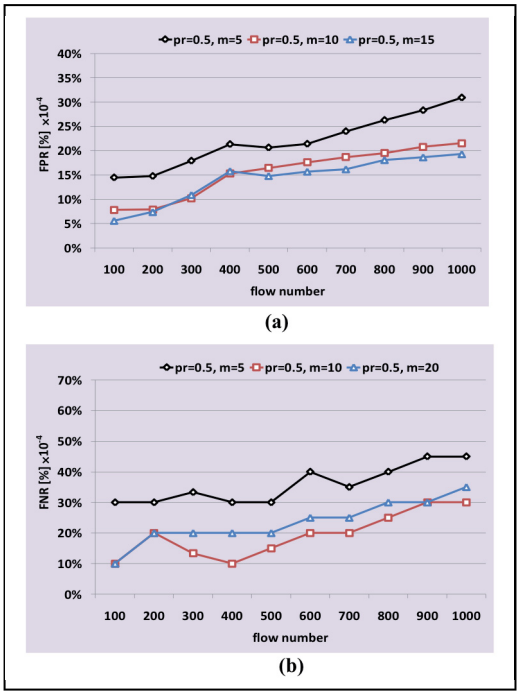

Fig. 11 (a)FPR and (b)FNR for 2nd-TF Droptail with fixed value *pr*

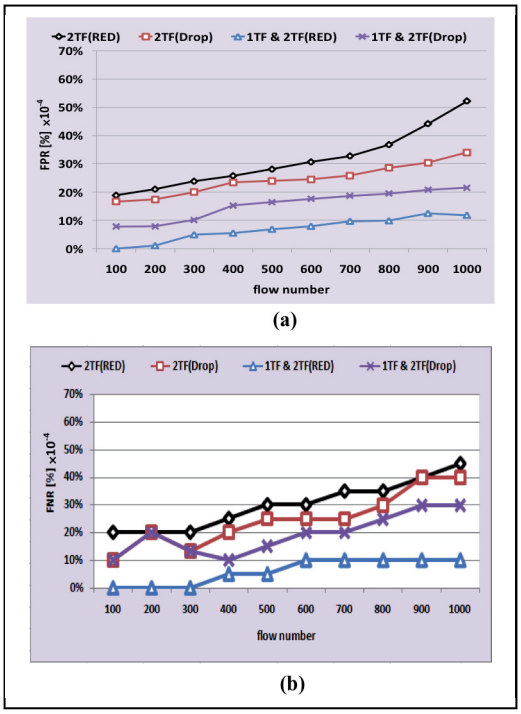

Fig. 12 Comparison of 2nd-TF and together 1-st TF with 2nd-TF

IV. CONCLUSION

In the paper, we have proposed a 2-tier DDoS detection system. The strengths of this scheme are its accuracy due to the distribution of processing workload and simple computation of arrival rate and queue length. Changes to the original data packets as well as the protocol are not required. Finally, we demonstrate the effectiveness of the proposed defense scheme which involves rate control and active queue management to detect the high-rate as well as potential low-rate attack.

REFERENCES

[1] Z. Gao and N. Ansari, "Differentiating malicious DDoS attack traffic from normal TCP flows by proactive tests," *IEEE Communications Letters*, vol.10, no.11, November 2006, pp.793-795. http://dx.doi.org/10.1109/LCOMM.2006.060669

[2] H. Y. Lam, C. P. Li, Samuel T. Chanson and D. Y. Yeung, "A coordinated detection and response scheme for distributed denial-of-service attacks," *ICC 2006 - IEEE International Conference on Communications*, no. 1, June 2006, pp.2150-2155.

[3] Shevtekar and N. Ansari, "Is it congestion or a DDoS attack?" IEEE Communications Letters, vol.13, no.7, July 2009, pp.546-548. http://dx.doi.org/10.1109/LCOMM.2009.090628

[4] Jerry C. Y. Chou, B. Lin, S. Sen and O. Spatscheck, "Proactive Surge Protection: A Defense Mechanism for Bandwidth-Based Attacks," *IEEE/ACM Transactions on Networking*, vol.17, no.6, December 2009.

[5] N. Kim., H. Lim, H. Park, and M. Kang, "Detection of Multicast Video Flooding Attack using the Pattern of Bandwidth Provisioning Efficiency," *IEEE Communications Letters*, vol.14, no.12, 2010, pp.1170-1172. http://dx.doi.org/10.1109/LCOMM.2010.101210.101053

[6] Y. Jing, X. Wang, X. Xiao and G. Zhang, "Defending against meek DDoS attacks by IP traceback-based rate limiting", *GLOBECOM 2006 - IEEE Global Telecommunications Conference*, no.1, November 2006, pp.1475-1479.

[7] V. A. Kumar, P. S. Jayalekshmy, G. K. Patra and R. P. Thangavelu, "On remote exploitation of TCP sender for low-rate flooding denial-of-service attack," *IEEE Communications Letters*, vol.13, no.1, January 2009, pp. 46-48. http://dx.doi.org/10.1109/LCOMM.2009.081555

[8] P. E. Ayres, H. Sun, H. J. Chao and W. C. Lau, "ALPi: A DDoS defense system for high-speed networks," *IEEE Journal on Selected Areas in Communications*, vol.24, no.10, October 2006, pp.1864-1876. http://dx.doi.org/10.1109/JSAC.2006.877136

[9] A. Yaar, A. Perrig and D. Song, "StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense," *IEEE Journal on Selected Areas in Communications*, vol.24, no. 10, October 2006, pp.1853-1863. http://dx.doi.org/10.1109/JSAC.2006.877138

[10] V. L. L. Thing, M. Sloman and N. Dulay, "Adaptive response system for distributed denial-of-service attacks," *IM 2009-11th IFIP/IEEE International Symposium on Integrated Network Management*, vol.11, no.1, June 2009, pp.809-814.

[11] K. Takemori, K. Wakasa, T. Kai, and H. Hazeyama, "Demonstration Experiments towards Practical IP Traceback on the Internet," *CCNC 2010 - 7th IEEE Consumer Communications and Networking Conference*, 2010.

[12] Y. Jing, X. Wang, L. Zhang and G. Zhang, "Stable Topology Support for Tracing DDoS Attackers in MANET," *GLOBECOM 2011 - IEEE Global Telecommunications Conference*, 2011.

[13] Y. You, M. Zulkernine and A. Haque, "Detecting flooding-based DDoS attacks," *ICC 2007- IEEE International Conference on Communications*, no.1, June 2007, pp. 1229-1234.

[14] S. Yu, W. Zhou and R. Doss, "Information theory based detection against network behavior mimicking DDoS attacks," *IEEE Communications Letters*, vol.12, no.4, April 2008, pp.319-321.

[15] H. Sun, Y. Zhaung and H. J. Chao, "A principal components analysis-based robust DDoS defense system," *ICC 2008 - IEEE International Conference on Communications*, vol.31, no.1, May 2008, pp. 1663-1669.

[16] A. Chonka, J. Singh and W. Zhou, "Chaos theory based detection against network mimicking DDoS attacks," *IEEE Communications Letters*, vol.13, no.9, September 2009, pp.717-719. http://dx.doi.org/10.1109/LCOMM.2009.090615

[17] S. Khor and A. Nakao, "MI: Cross-Layer Malleable Identity," *ICC 2011 - IEEE International Conference on Communications*, 2011.

[18] H. Liu, Y. Sun, V. Valgenti and M. Kim, "TrustGuard: A Flow-Level Reputation-Based DDoS Defense System," *CCNC 2011-*

8th IEEE Consumer Communications and Networking Conference, 2011.

[19] Y. Liu, W. Chen and Y. Guan, "A Fast Sketch for Aggregate Queries over High-Speed Network Traffic," *IEEE INFOCOM 2012 - 31th IEEE International Conference on Computer Communications*, 2012.

[20] K. Salah, K. Elbadawi, and R. Boutaba, "Performance Modeling and Analysis of Network Firewalls," *IEEE Transactions on Network and Service Management*, vol.9, no.1, 2012, pp.12-21. http://dx.doi.org/10.1109/TNSM.2011.122011.110151

[21] S. Floyd, V. Jacobson, "Random early detection gateways for congestion avoidance," *IEEE/ACM Transactions on Networking*, vol.1 no. 4, p.397-413, Aug. 1993. http://dx.doi.org/10.1109/90.251892

[22] The Network Simulator ns-2, see http://www.isi.edu/nsnam/ns/

AUTHORS

Chin-Ling Chen* and **Chih-Yu Chang** are with the Department of Information Management, National Pingtung Institute of Commerce, Pingtung, Taiwan.

This article is an extended and modified version of a paper presented at the 2013 Chinese Intelligent Automation Conference (CIAC2013), held in Yangzhou, Jiangsu Province, China, in August 2013. Submitted 22 May 2013. Published as re-submitted by the authors 23 July 2013.