Detecting TCP-based DDoS Attacks in Baidu Cloud Computing Data Centers

Jiahui Jiao[1], Benjun Ye[1], Yue Zhao[1], Rebecca J. Stones[1],
Gang Wang[1]*, Xiaoguang Liu[1]*, Shaoyan Wang[2], Guangjun Xie[2]
[1]*Nankai-Baidu Joint Lab, College of Computer and Control Engineering, Nankai University*
[2]*Cloud Business Unit, Baidu Inc.*
{*jiaojh, yebj, zhaoyue, becky, wgzwp, liuxg*}*@nbjl.nankai.edu.cn*
{*wangshaoyan, xieguangjun*}*@baidu.com*

***Abstract*—Cloud computing data centers have become one of the most important infrastructures in the big-data era. When considering the security of data centers, distributed denial of service (DDoS) attacks are one of the most serious problems. Here we consider DDoS attacks leveraging TCP traffic, which are increasingly rampant but are difficult to detect.**

To detect DDoS attacks, we identify two attack modes: fixed source IP attacks (FSIA) and random source IP attacks (RSIA), based on the source IP address used by attackers. We also propose a real-time TCP-based DDoS detection approach, which extracts effective features of TCP traffic and distinguishes malicious traffic from normal traffic by two decision tree classifiers.

We evaluate the proposed approach using a simulated dataset and real datasets, including the ISCX IDS dataset, the CAIDA DDoS Attack 2007 dataset, and a Baidu Cloud Computing Platform dataset. Experimental results show that the proposed approach can achieve attack detection rate higher than 99% with a false alarm rate less than 1%. This approach will be deployed to the victim-end DDoS defense system in Baidu cloud computing data center.

Paper Type: Poster Abstract

I. Introduction

TCP traffic has recently been exploited broadly in DDoS attacks. At present, half of all network DDoS attacks are SYN flood attacks which are considered one of the most powerful flooding methods [1]. At the same time, Challenge Collapsar (HTTP flood) attacks have been emerging frequently. TCP-based DDoS attacks can utilize multiple attack types and different attack modes, which makes it extremely difficult to detect these attacks.

There are two different attack modes depending on the source IP address(es) used by attackers: fixed source IP attacks (FSIA) and random source IP attacks (RSIA). Generally, attackers spoof their IP address(es) to launch attacks for the sake of hiding their own hosts [2]. The spoofed IP address(es) could be fixed or random. Moreover, to avoid possible anti-spoofing mechanisms, the attackers can also launch the attacks from a botnet using non-spoofed IP addresses (fixed IP addresses) [3]. While detecting attacks based on IP addresses is crucial for defending against DDoS attacks, many detection methods do not defend against both attack modes (FSIA and RSIA).

Several recent DDoS attack detection approaches [4], [5], [6], while successfully identifying DDoS attacks, fail to identify the attack source. As a result, the victims cannot initiate appropriate defensive measures. The approaches in [7] and [8] detect DDoS attacks based on connections between two network hosts, but they are not suited to detecting RSIA-mode DDoS attacks.

Motivated by above challenges, we concentrate on how to detect TCP-based DDoS attacks under the two attack modes. In this paper, a victim-end detection approach is proposed, which uses the decision tree technique to achieve a high detection rate and low false alarm rate. The following are the contributions of this work:

a) Generality: The proposed approach provides two different detection modules corresponding to RSIA and FSIA. Moreover, for FSIA, the malicious fixed IP address can be identified, allowing the victims to take immediate countermeasures.

b) Real-time: The proposed approach extracts important features from inbound and outbound TCP traffic flows every second for the purpose of detecting attacks real-time.

c) Accuracy: The proposed approach can detect various TCP-based DDoS attacks with an attack detection rate higher than 99% and false alarm rate less than 1%.

II. Method

The overall architecture of our proposed TCP-based DDoS detection system is shown in Figure 1. It consists of four main phases: Data Collection, Sample Generation and Feature Selection, Classification, and Attack Alarm.

A. Data Collection Phase

In the Data Collection phase, we use a packet sniffer to capture every packet from TCP traffic flows. After extracting TCP/IP header from the captured packets, the proposed system partitions them according to every pair of IP addresses (local IP, the address of the local host, and remote IP, the address of the remote host that communicates with the local host), and counts the number of inbound (remote IP to local IP) packets of each IP pair every second.

B. Sample Generation and Feature Selection Phase

According to the two attack modes, we design different sample generation method and select different features.

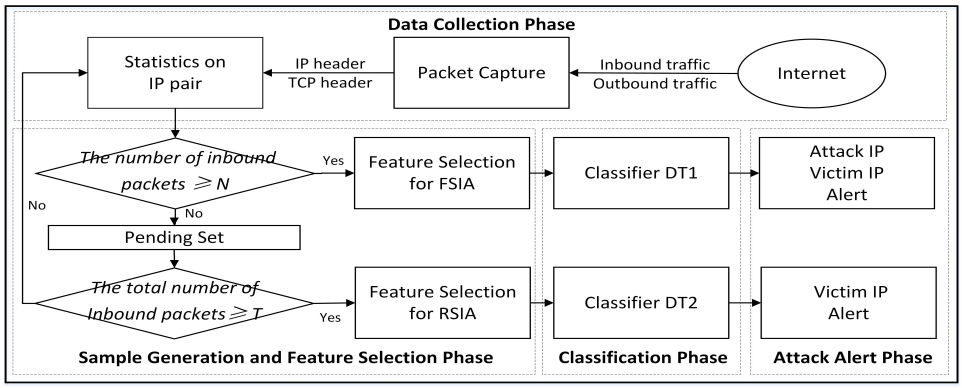

Fig. 1: Architecture of the proposed TCP-based DDoS detection system.

.

1) Sample generation: To develop a practical real-time detection system, we begin by detecting abnormal traffic flows. To this end, we set a threshold N on the number of IP-pair inbound packets per second (PPS). Once the inbound PPS for an IP pair exceeds N, the system will generate a FSIA detection event.

This method is aimed to only detect fixed source IP attacks, since a spike in IP-pair inbound PPS will not necessarily occur for RSIAs. RSIAs are comparatively harder to detect because of its similarity with that of legitimate traffic. To detect RSIAs, we set a second threshold T which we use on the total number of inbound packets, only counting packets between IP pairs which don't meet the first threshold N.

2) Feature selection:

a) FSIA: Through analyzing the characteristics of the TCP protocol and TCP-based attacks, we select two categories of features: 15 basic statistical features and 16 ratio features (Table I), which can give identifying information about the occurrence of malicious traffic. TCP traffic has various control flags which represent the communication state. Thus we select a large proportion of features related to them (e.g., SYN, ACK, PUSH, RST, FIN). For instance, under a SYN flood, a target server receives enormous SYN packets. The ratio of the number of inbound SYN packets and the total number of inbound packets per second will be extremely high.

b) RSIA: In this setting, we need to select general features. The similarity of traffic rates during RSIAs is stronger than legitimate flows [9]. Therefore, the features designed for RSIA magnify this kind of similarity based on the number of inbound packets. We define 10 simple, but effective features, where the i-th feature is the number of remote hosts which sends at least $(i/10)N$ and less than $((i+1)/10)N$ packets to a local host, for $i \in \{0, 1, \ldots, 9\}$, where N is the threshold on the number of inbound packets per second.

c) Chi-squared test: The number of feature affects the classification efficiency directly. We use a χ-squared test to generate an optimal feature set which is expected to be adequate for classifying the legitimate traffic and malicious traffic. For FSIA mode, we select the top-k features from χ-squared test ranking in order to achieve a faster and more accurate classification.

TABLE I: Statistical Features for FSIA.

No.	Feature	Description
1	in_pps	number of inbound TCP packets per sec.
2	out_pps	number of outbound TCP packets per sec.
3	syn_in_pps	number of inbound syn packets per sec.
4	synack_out_pps	number of outbound syn-ack packets per sec.
5	ack_in_pps	number of inbound ack packets per sec.
6	ack_out_pps	number of outbound ack packets per sec.
7	push_in_pps	number of inbound push packets per sec.
8	push_out_pps	number of outbound push packets per sec.
9	fin_in_pps	number of inbound fin packets per sec.
10	fin_out_pps	number of outbound fin packets per sec.
11	rst_in_pps	number of inbound rst packets per sec.
12	rst_out_pps	number of outbound rst packets per sec.
13	other_in_pps	number of inbound non-flag packets per sec.
14	port_num_RIP	number of port used by remote IP
15	port_num_LIP	number of port used by local IP

No.	Feature
16	in_pps / (in_pps + out_pps)
17	syn_in_pps / in_pps
18	syn_in_pps / (syn_in_pps + syn-ack_out_pps)
19	syn_in_pps / (syn_in_pps + ack_in_pps)
20	ack_in_pps / in_pps
21	ack_in_pps / (ack_in_pps + ack_out_pps)
22	ack_in_pps / (ack_in_pps + rst_out_pps)
23	push_in_pps / in_pps
24	push_in_pps / (push_in_pps + push_out_pps)
25	push_in_pps / (push_in_pps + rst_out_pps)
26	push_in_pps / (push_in_pps + ack_in_pps)
27	rst_in_pps / in_pps
28	rst_out_pps / out_pps
29	fin_in_pps / in_pps
30	fin_in_pps / (fin_in_pps + fin_out_pps)
31	other_in_pps / in_pps

C. Classification Phase

In the Classification phase, we also provide two decision tree classifiers which are trained with our experimental data. One is designed for FSIA, another for RSIA. They can be used to label traffic flow as normal or attack.

D. Attack Alert Phase

During FSIA detection, the IP-pair method enables us to raise an alert, giving the fixed-source IP address, which is the malicious user. This enables the operator to react with an appropriate defense mechanism.

III. Evaluation and Discussion

A. Experimental Data

We use four different datasets, two public datasets (ISCX dataset [10] and CAIDA dataset [11]), a Baidu dataset, and one simulated dataset, to evaluate our method. The attack mode (FSIA and/or RSIA) used in the dataset determines which experiments we use the dataset for. Specifically, the simulated dataset, ISCX dataset, Baidu dataset are used for testing FSIA detection. And the simulated dataset, and the benign data of ISCX together with the malicious data of CAIDA dataset (because the CAIDA dataset contains little normal data) are applied for testing RSIA detection.

B. Threshold selection

In this detection system, the thresholds N and T play an important role, affecting both the detection time and detection accuracy directly. The thresholds should be chosen according to specifics of the network under consideration.

We analyze normal data of our simulated dataset for choosing the thresholds N and T. The normal data contains three scenarios: low-rate traffic, medium-rate traffic, and high-rate traffic. First, we perform a statistical analysis on inbound PPS of every IP pair in these three scenarios, and calculate the ninth decile(empirical value) of numbers of inbound PPS of IP pairs, respectively. We then use these three values as thresholds N for the experiment, respectively. Then, for each hour, we calculate the number of inbound packets in each one-second period, including only those from remote IPs which send fewer than N, and compute the moving value (over the 3600 one-second intervals) as time varies. Then, we calculate an overall average as T.

C. Results

We evaluate the detection results by estimating the Attack Detection Rate (ADR) and False Alarm Rate (FAR) on these datasets. The results are given in Tables II and III.

TABLE II: Detection results (%) for FSIA

rate	Simulated Dataset		ISCX IDS Dataset		Baidu Dataset	
	ADR	FAR	ADR	FAR	ADR	FAR
low	99.71	0.13	99.92	0.34	99.09	0.02
middle	99.69	0.10	99.95	0.23	99.41	0.01
high	99.16	0.17	99.94	0.10	99.76	0.02

IV. Conclusion

In this paper, we describe and test a TCP-based DDoS attack detection method. It focuses on two identified attack modes (fixed source IP attacks and random source IP attacks) and provides a different detection strategy for each. We examine the proposed method with four datasets: one simulated dataset, one ISP dataset and two public datasets. The experimental results demonstrate it can identify the different attack modes and distinguish benign network traffic from main TCP-based attacks with high attack detection rates and low false alarm rates. We test the proposed method in Baidu data centers, and it will be deployed to the Baidu Cloud Computing Platform to detect TCP-based DDoS attacks.

TABLE III: Detection results (%) for RSIA

scenario	Simulated Dataset		CAIDA+ISCX Dataset	
	ADR	FAR	ADR	FAR
low-rate	100	0.00	100	0.49
middle-rate	100	0.00	100	0.74
high-rate	100	0.00	100	0.33

Acknowledgment

This work is partially supported by NSF of China (grant numbers: 61373018, 61602266, 11550110491, 4117JCY-BJC15300). Stones was also supported by the Thousand Youth Talents Plan in Tianjin.

References

[1] "The top 10 DDoS attack trends," http://www.imperva.com/docs/DS_Incapsula_The_Top_10_DDoS_Attack_Trends_ebook.pdf.

[2] N. Long and R. Thomas, "Trends in denial of service attack technology," *CERT Coordination Center*, 2001.

[3] L. Colace, G. Masini, V. Cencelli, F. Denotaristefani, and G. Assanto, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Surveys*, vol. 39, no. 3, pp. 273–302, 2007.

[4] M. L. Sang, S. K. Dong, J. H. Lee, and J. S. Park, "Detection of DDoS attacks using optimized traffic matrix." *Computers & Mathematics with Applications*, vol. 63, no. 2, pp. 501–510, 2012.

[5] T. Thapngam, S. Yu, W. Zhou, and S. K. Makki, "Distributed denial of service (DDoS) detection by traffic pattern analysis," *Peer-to-Peer Networking and Applications*, vol. 7, no. 4, pp. 346–358, 2014.

[6] M. H. Bhuyan, A. Kalwar, A. Goswami, and D. K. Bhattacharyya, "Low-rate and high-rate distributed DoS attack detection using partial rank correlation," in *Fifth International Conference on Communication Systems and Network Technologies*, 2015.

[7] H. J. Kashyap and D. K. Bhattacharyya, "A DDoS attack detection mechanism based on protocol specific traffic features," in *International Conference on Computational Science, Engineering and Information Technology*, 2012, pp. 194–200.

[8] P. Xiao, W. Qu, H. Qi, and Z. Li, "Detecting DDoS attacks against data center with correlation analysis," *Computer Communications*, vol. 67, no. C, pp. 66–74, 2015.

[9] S. Behal and K. Kumar, "Detection of DDoS attacks and flash events using novel information theory metrics," *Computer Networks*, vol. 116, pp. 96–110, 2017.

[10] A. Shiravi, H. Shiravi, M. Tavallaee, and A. A. Ghorbani, "Toward developing a systematic approach to generate benchmark datasets for intrusion detection," *Computers & Security*, vol. 31, no. 3, pp. 357–374, 2012.

[11] "The CAIDA UCSD DDoS attack 2007 dataset," http://www.caida.org/data/passive/ddos-20070804_dataset.xml.