IEICE TRANS. INF. & SYST., VOL.E101–D, NO.6 JUNE 2018

LETTER

Source-Side Detection of DRDoS Attack Request with Traffic-Aware Adaptive Threshold

Sinh-Ngoc NGUYEN[†a)], **Van-Quyet NGUYEN**[†b)], **Giang-Truong NGUYEN**[†c)], **JeongNyeo KIM**[††d)], ***Nonmembers***, ***and*** **Kyungbaek KIM**[†e)], ***Member***

SUMMARY Distributed Reflective Denial of Services (DRDoS) attacks have gained huge popularity and become a major factor in a number of massive cyber-attacks. Usually, the attackers launch this kind of attack with small volume of requests to generate a large volume of attack traffic aiming at the victim by using IP spoofing from legitimate hosts. There have been several approaches, such as static threshold based approach and confirmation-based approach, focusing on DRDoS attack detection at victim's side. However, these approaches have significant disadvantages: (1) they are only passive defences after the attack and (2) it is hard to trace back the attackers. To address this problem, considerable attention has been paid to the study of detecting DRDoS attack at source side. Because the existing proposals following this direction are supposed to be ineffective to deal with small volume of attack traffic, there is still a room for improvement. In this paper, we propose a novel method to detect DRDoS attack request traffic on SDN(Software Defined Network)-enabled gateways in the source side of attack traffic. Our method adjusts the sampling rate and provides a traffic-aware adaptive threshold along with the margin based on analysing observed traffic behind gateways. Experimental results show that the proposed method is a promising solution to detect DRDoS attack request in the source side.

key words: *DRDoS request detection, source-side detection, software defined network, traffic-aware adaptive threshold*

1. Introduction

Distributed Reflective Denial of Service (DRDoS) attacks pose a serious threat to the internet services. The attacker exploits the malformed hosts and uses protocols, like Network Time Protocol (NTP) or Domain Name Server (DNS), to send small DRDoS attack request to reflector servers, then they response large amount of attack traffic to victim in a short period of time. For instance, the attacker flooded a victim on CloudFlare's network by generating approximately 400Gbps using 4,529 NTP servers running on 1,298 different networks [1]. It is possible that a DRDoS attacker can use only a single server running on a network to send many requests to a victim by using IP address spoofing.

The most common approaches for dectecting DRDoS attack are based on analyzing traffic at victim side, such as threshold-based approach and confirmation-based approach [2]–[4]. Kawahana et. al. [2] investigated how to detect network anomalies using flow statistics. The basic idea of this approach is if the number of sampled flows exceeds a predefined static threshold, the abnormal network traffic can be detected. However, a static threshold is not efficient for detecting DRDoS attack in case of complex traffic with wavelet form. To address this issue, Zhang et. al. [4] proposed an adaptive sampling technique based on group similarity, which reflects the fact that abnormal network traffic could belong to the same group sharing similar characteristics. Tsunoda et. al. [3] proposed a simple method for detecting DRDoS attack by using response packet confirmation mechanism, which focused on the fact that the types of the response packets received by a victim are predictable based on the corresponding types of the request packets. However, these victim-side approaches have significant disadvantages: (1) they are only passive defenses after the attack and (2) it is hard to trace back the attackers.

The focus of recent researches has been changed to source side situated DRDoS attack detection. The traditional threshold-based techniques applied for victim side detection are not effective enough to be employed on this direction because they are only suitable to detect abnormal traffic with large volume. Meanwhile, considering the source side, the volume of attack traffic is quite small comparing to the victim one. Confirmation-based approach can be still applied to DRDoS attack detection in the source side, but this approach has a limitation when dealing with the trade off between delay time of request-response packets and false positive rate of detection. Recently, a machine learning based approach for DDoS attack detection from source side in cloud has been proposed in [5]. The authors used both supervised learning and unsupervised learning algorithms to classify the network traffic into 2 output labels: attack or not-attack. However, there is still a room for improvement, because classification techniques are inefficient in case of DRDoS detection where the attack traffic itself has a small volume. Moreover, they are quite similar and can be mixed up with legitimate traffic.

In this paper, we propose a novel method for source-side detection of DRDoS attack request by using traffic-aware adaptive threshold. Initially, the proposed method collects the samples of network traffic related to a network service protocol, which may be maliciously exploited as attack requests, to obtain observed traffic. Afterwards, we cal-

Manuscript received January 25, 2018.
Manuscript publicized March 12, 2018.
[†]The authors are with the Department of Electronics and Computer Engineering, Chonnam National University, Gwangju, Korea.
[††]The author is with the Electronics and Telecommunications Research Institute, Korea.
a) E-mail: sinhngoc.nguyen@gmail.com
b) E-mail: quyetict@utehy.edu.vn
c) E-mail: truongnguyengiang.bk@gmail.com
d) E-mail: jnkim@etri.re.kr
e) E-mail: kyungbaekkim@jnu.ac.kr (Corresponding author)
DOI: 10.1587/transinf.2018EDL8020

culate an adaptive threshold for DRDoS detection based on observed traffic in every time window (e.g., 5 seconds). This threshold will be used for determining whether DRDoS attacks are occurring or not. Finally, we shall re-calculate parameters: threshold and margin, then update them for the next time window based on observed traffic. Through experiments, we demonstrate that the proposed method can accurately detect DRDoS attack packets in a short duration.

2. Rationale of the Proposed Approach

Regarding the characteristic of DRDoS attack, it employs only some specific known protocols, such as DNS or NTP, among many others. Therefore, the traffic containing these specific ones could be filtered to support capturing the attack. Moreover, considering the situation that it is launched from the source side, although the attack's volume is quite small, it still generates transient peaks of traffic with specific protocols at some short periods, which could be exploited to be detected.

In the reality, as mentioned before, the number of DRDoS requests are much smaller than the amplified attack traffic's one. Meanwhile, the diversity of services and protocols used by many different devices makes the legitimate traffic fluctuate. Therefore, it is better to use an adaptive threshold instead of the old fixed one. Furthermore, sometimes, legitimate traffic could fluctuate dramatically, which creates itself some peaks. This change could cause high false positive rate of detection, if an adaptive threshold is solely used. Consequently, there is a need to add a margin to the proposed adaptive threshold to reduce the number of false positive cases.

3. Souce-Side Detection of DRDoS Attack Requests with Traffic-Aware Adaptive Threshold

3.1 Overview of the Proposed Method

Figure 1 depicts the overview of our source side DRDoS attack request detection operation with traffic-aware adaptive threshold. For conducting the proposed method, we need an SDN-enabled gateway, an SDN controller with network configured application and a DRDoS attack request detection module.

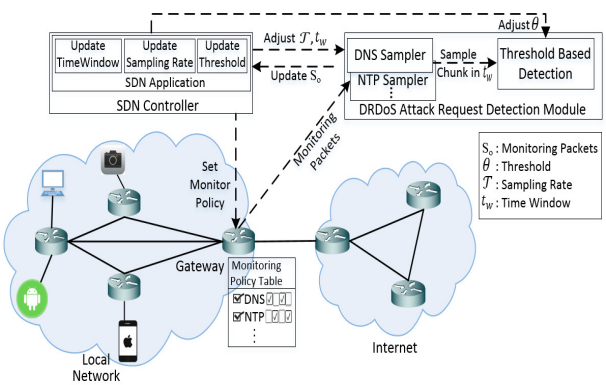

Fig. 1 Network system model.

The proposed gateway is an essential component, which captures all of network traffic from local network heading to the internet. This monitored traffic will be mirrored with some specific protocols, such as DNS or NTP, and forwarded to DRDoS attack request detection module. The chosen protocols will be decided by the monitoring policies set by the SDN controller.

In the DRDoS detection module, based on the chosen forwarded protocols, the corresponding sampler, such as DNS sampler and NTP sampler, will receive their monitored traffic, which is defined by S_R, and formalize it into a unit of observed traffic S_o with a given time window t_w. To avoid the overloading case, we employ sampling method with sampling rate parameter τ, which could be adjusted by the SDN application on the SDN controller based on the information of the observed traffic S_R.

With the observed traffic, the threshold based detection module determines whether a DRDoS attack request occurs or not. The adaptive detection threshold θ is also adjustable according to the current observed traffic and previous detecting threshold. Furthermore, the threshold is also affected by the so-called margin, which is also controllable by the SDN application. Both sampling rate and margin are described more specifically in the next section.

3.2 DRDoS Detecting with Traffic-Aware Adaptive Threshold

In this section, we describe our novel algorithm for efficiently obtaining adaptive threshold to detect DRDoS attack. The basic idea is adjusting the threshold based on observed traffic in every period of time (t_w), so the proposed system could obtain high detection rate when dealing with various types of network traffic such as flat or strongly wavelet one. To do this, we first consider obtaining the observed traffic in our system. We then propose an approach to calculate and adjust the threshold based on observed traffic. Finally, the important parameters will be updated into detection module for the next time window detection.

At the gateway, the monitored network traffic S_R is mirrored to samplers on the DRDoS attack request detection module. In this case, samplers may have limitation of handling large amount of packets. To resolve this limitation, sampling technique can be applied to the monitored network traffic. Assuming that the sampling capacity of a sampler is C_d, and the sampling ratio is defined for the observed traffic as τ. In Eq. (1), if the monitored traffic is less than capacity of the sampler, all of traffic will be forwarded. Otherwise, only a portion of traffic (C_d/S_R) will be handled instead.

$$\tau = \begin{cases} 1 & \text{if } S_R \leq C_d \\ \frac{C_d}{S_R} & \text{Otherwise} \end{cases} \quad (1)$$

The observed traffic is the key of the proposed detecting method, which includes both legitimate traffic and DRDoS attack request traffic. The monitored traffic at the gate-

Algorithm 1 DRDoS Attack Request Detection

Require: Sampling capacity (C_d), monitored traffic (S_R), time window (t_w), threshold (θ_t), margin of threshold (δ), degree of weighting of moving average (μ)
Ensure: Notification of DRDoS attack request
1: $t \leftarrow 1$;
2: $\theta_1 = S_{o_1} \leftarrow$ GetNormalTraffic();
3: **while** *true* **do**
4: / *Detection Phase* /
5: $t \leftarrow t + 1$;
6: $S_{o_t} \leftarrow$ GetObservedTraffic(τ, t_w, S_R); / Number of packets /
7: **if** $S_{o_t} > \theta_{t-1} * (1 + \delta)$ **then**
8: NotifyDRDoSAttackRequestEvent(S_{o_t}, θ_{t-1});
9: $\theta_t = \theta_{t-1}$
10: **else**
11: $\theta_t = \mu\, \theta_{t-1} + (1 - \mu)\, S_{o_t}$
12: / *Reconfiguration Phase* /
13: $\tau \leftarrow$ RecomputeSamplingRate(C_d, S_R);
14: changes $\leftarrow$ UpdateDetectingConfiguration(t_w, τ, S_o,);
15: **if** changes ! = 0 **then**
16: AdjustParameters(t_w, τ, θ_t);

way is S_R, which is the total traffic of a specific protocol mirrored to a sampler. When the samplers of DRDoS attack request detection module receives the monitored traffic, they take samples from the received traffic with the given sampling ratio τ and generate a chunk of the sampled network traffic for a time window unit t_w. According to this, the sampled traffic from the monitored traffic is defined as the observed traffic S_o (which is shown in Eq. (2)). This one will be used to generate traffic chunks as the input to the threshold based detection module.

$$S_o = S_R * \tau * t_w \tag{2}$$

Algorithm 1 depicts our idea in this proposal. Firstly, at $t = 1$, the value of the threshold is set to the same value with the initial observed traffic, and it is assumed that there is no attack occurring at that time (lines 1-2). Next, in the detection phase, observed traffic is gotten in a time window t_w from monitored traffic S_R (lines 5-6). Then, the appearance of attack traffic in the considered time window is checked (line 7). In which, if the observed traffic is greater than the sum of the threshold and the margin, this traffic is detected as attack traffic. It is supposed that there is no simple way to determine the best value for the margin because it depends on the real monitored network traffic as well as observed traffic. Consequently, using a fixed value of margin is not the best approach. We therefore use the margin value as a portion of the threshold which is decided by the coefficient δ, whose value is between 0 and 1. Clearly, the margin value of situation whose network traffic fluctuates should be higher than the one whose traffic is flat.

Next, if the attack traffic is detected, a notification about DRDoS attack request is generated, and the threshold is kept unchanged with the previous one (lines 8-9). Otherwise, this threshold is updated based on current observed traffic and previous threshold (line 11) by using Eq. (3):

$$\theta = \mu * S_o + (1 - \mu) * \theta_{t-1} \tag{3}$$

where the coefficient μ represents the weight degree of moving average [6] and its value is a constant smoothing factor between 0 and 1. For example, in case attack happens in flat network traffic, the μ value could be close to 0, while in other cases, the μ value could be chosen at 0.5. We can see that the smaller μ values make the choice of previous threshold relatively more important than the larger μ values.

In the reconfiguration phase, if any important parameters (sampling rate, time window, and threshold) change is recorded, they are updated to the detector (lines 13-16). The sampling rate is needed to be recomputed because it could be changed depending on monitored traffic in each time window. Also, the time window value can be changed somehow by the system administrator, which could affect the observed traffic, leading to the threshold change.

4. Evaluation

To evaluate the viability of our proposed system, we conducted experiments with two types of traffic (flat and fluctuated). Firstly, we implemented an event-based simulator for generating DNS request traffic. Duration of the traffic is one hour and it includes 20 events of DNS DRDoS attack requests. For a DRDoS event, malicious bots generate attack request packets with a given attack traffic rate for a given attack duration. Then our proposed method is applied to detect the attack traffic. To evaluate the detecting ability of our proposed system, we measure the detection rate and the the false positive rate of traffic samples captured by every time window. The detection rate is defined as the portion of the detected attack samples out of the total number of real attack samples. The false positive rate is defined as the portion of the mis-detected samples out of the total number of detected attack samples.

Exp-1: Detecting ability in flat traffic

In this case, we evaluate the detection rate under the change of attack ratio, attack period, and time window size. In the experiment setting, the attack ratio, which is the fraction of attack request packets over total packets in the observed traffic, changed in different time window size (t_w). This shift would affect the result of detection. As shown in the Fig. 2, the detection rate increases when the attack ratio increases because it would be easier to capture the attack when there is much attack traffic.

As mentioned before, detection rate is affected by the time window size, and both of attack period and time win-

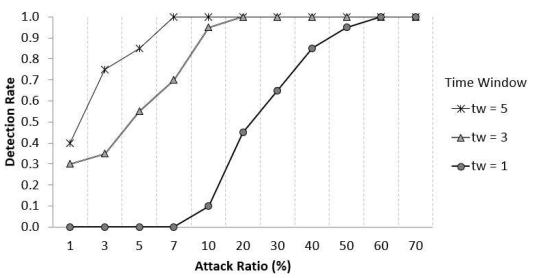

Fig. 2 Flat traffic case: detection rate with various attack ratio

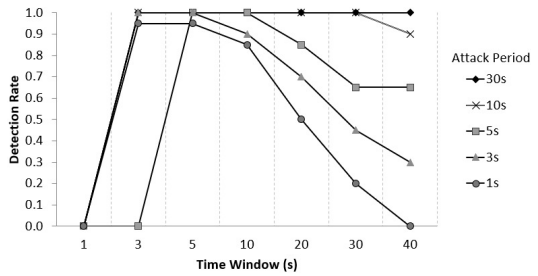

Fig. 3 Flat traffic case: Detection rate with various time window size

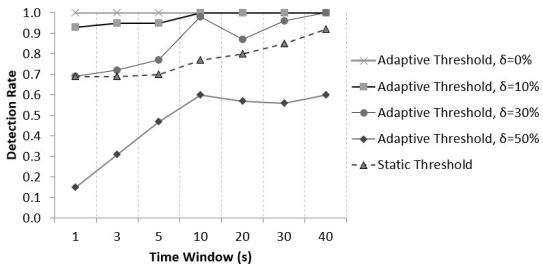

Fig. 4 Detection rate in fluctuated traffic case with 30% attack ratio

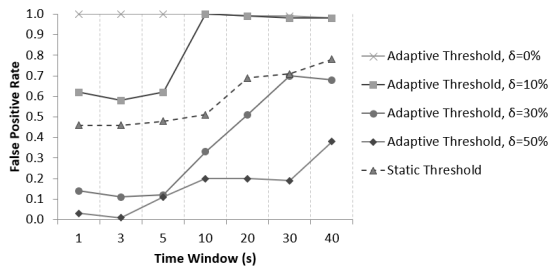

Fig. 5 False positive rate of detection in fluctuated traffic case with 30% attack ratio

dow size changed with different values to evaluate detection rate. Figure 3 shows the trade off between detection rate and time window size. If the time window is too large and attack traffic is small, the peak of attack traffic could blend with the legitimate traffic. According to the result, with 5 seconds of time window, attacks are detected most. The false positive rate in this case is not considered because the legitimate traffic does not have much change in each time window, which makes the false positive rate of detection be too small.

Exp-2: Detecting ability in fluctuated traffic

In this case, we evaluate both of the detection rate and false positive rate of our proposed method. The evaluation is conducted under the change of time window and margin. In the experiment setting, attack ratio is set to 30% of all the traffic, and each attack event occurs from 20 seconds to 30 seconds.

Overall, as the result shown in Fig. 4 and Fig. 5, when time window value increases, both of the detection rate and false positive rate also increase together. Therefore, there is a need to choose a suitable value for time window to balance the trade-off between detection rate and false positive rate.

Figure 4 depicts the detection rate by using static threshold and adaptive threshold with different margins. When the margin increases, the detection rate decreases, because employing the large margin could make the small attack peak be considered as the normal one. The detection rate by using static threshold is higher than the adaptive one with 50% value of margin, but is lower than other adaptive ones with other margin values (0%, 10%, and 30%).

As seen from Fig. 5, the false positive rate decreases when the margin for adaptive threshold increases. Specifically, with time window being equal to 10 seconds, the false positive rate is 1.0 in case margin being equal to 0%, and nearly 0.2 for the case margin being equal to 50%. Comparing to using the static threshold, it is better than the adaptive threshold with margin being smaller than 10%, but with larger than 30%, the adaptive one provides a better result with lower false positive rate.

In summary, there is a trade-off between detection rate and false positive rate based on the margin value and time window value. Through the experiments, we found that with 10 seconds of time window and 30% value of margin accompanied with the adaptive threshold, the best result is recorded with detection being equal to 1.0 and false positive rate being equal to 0.3. Clearly, our proposed adaptive threshold with margin outperforms the static threshold for detecting DRDoS attack requests.

5. Conclusion

In this paper, we proposed a method of detecting DRDoS attack requests from source side of attack by using traffic aware adaptive threshold. By using an SDN-enabled gateway, it is possible to filter specific packet samples easily and adjust threshold properly. Through extensive evaluation, we showed that the viability of the proposed method under various types of traffic.

Acknowledgments

This work was supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIP)(R0110-16-1001). This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(NRF-2017R1A2B4012559). This research was supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2018-2016-0-00314) supervised by the IITP.

References

[1] L. Rudman and B. Irwin, "Characterization and analysis of ntp amplification based ddos attacks," Information Security for South Africa (ISSA), 2015, pp.1–5, IEEE, 2015.

[2] R. Kawahara, T. Mori, N. Kamiyama, S. Harada, and S. Asano, "A study on detecting network anomalies using sampled flow statistics," Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on, pp.81–81, IEEE, 2007.

[3] H. Tsunoda, K. Ohta, A. Yamamoto, N. Ansari, Y. Waizumi, and Y. Nemoto, "Detecting drdos attacks by a simple response packet confirmation mechanism," Computer Communications, vol.31, no.14,

pp.3299–3306, 2008.

[4] J. Zhang, X. Luo, R. Perdisci, G. Gu, W. Lee, and N. Feamster, "Boosting the scalability of botnet detection using adaptive traffic sampling," Proc. 6th ACM Symposium on Information, Computer and Communications Security, pp.124–134, ACM, 2011.

[5] Z. He, T. Zhang, and R.B. Lee, "Machine learning based ddos attack detection from source side in cloud," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), pp.114–120, 2017.

[6] W. contributors, "Moving average," 2017. [Online; accessed 21-November-2017].