Improving Performance of Collaborative Source-Side DDoS Attack Detection

Sungwoong Yeom, Kyungbaek Kim
Department of Computer Engineering
Chonnam National University
Gwangju City, South Korea
yeomsw0421@gmail.com, kyungbaekkim@jnu.ac.kr

Abstract— **Recently, as the threat of Distributed Denial-of-Service attacks exploiting IoT devices has spread, source-side Denial-of-Service attack detection methods are being studied in order to quickly detect attacks and find their locations. Moreover, to mitigate the limitation of local view of source-side detection, a collaborative attack detection technique is required to share detection results on each source-side network. In this paper, a new collaborative source-side DDoS attack detection method is proposed for detecting DDoS attacks on multiple networks more correctly, by considering the detecting performance on different time zone. The results of individual attack detection on each network are weighted based on detection rate and false positive rate corresponding to the time zone of each network. By gathering the weighted detection results, the proposed method determines whether a DDoS attack happens. Through extensive evaluation with real network traffic data, it is confirmed that the proposed method reduces false positive rate by 35% while maintaining high detection rate.**

Keywords— Network Security, DDoS Attack, SDN IDPS, Collaborative Source-side detection

I. INTRODUCTION

Depending on the activation of IoT environment, the threat of Distributed Denial of Service (DDoS) attacks that exploit the weakness of IoT devices distributed in multiple regions is rapidly increasing. Even though the amount of traffic produced by these abused IoT devices is small, the amount of traffic observed in the victim-side network is a large and it is easy to detect it. However, victim-side attack detection methods reveal several disadvantages, such as delayed detection and difficulty in tracking attackers. To mitigate these disadvantages, source-side DoS detection methods are being studied.

In a source-side network, the amount of traffic observed is relatively small compared to a victim-side network, so attack traffic can easily mix with normal traffic. To detect this small amount of attack traffic, methods for dynamically changing attack detection threshold using observed traffic were studied [1]. However, if the observed traffic is mixed with attack traffic, this method requires separating attack traffic from observed traffic for calculation of new threshold. To separate this attack traffic from the observed traffic, estimating the amount of normal traffic by utilizing network traffic seasonality was studied [2]. This study identified the seasonal behavior through network traffic volume statistics to estimate normal traffic. For example, the volume of network traffic is characterized by increasing in the morning and gradually decreasing from afternoon to evening. This seasonal pattern has a small impact on the attack traffic volume and helps to estimate normal traffic. Recently, to improve the performance of estimating an amount of normal traffic, methods of estimation through time series deep learning analysis has been actively studied. Consequently, LSTM demonstrates high performance in time-series deep learning analysis, such as predicting the volume of network traffic using multivariate data and seasonality features [3,4].

However, the source-side DoS detection method fixed in one region may not detect the attack traffic from the source-side network when a large-scale DDoS attack is initiated from multiple sites with different time region. A source-side network only observes small amount of traffic for detecting an attack compared to a victim-side network. Due to this, a change in the amount of normal traffic over time, which is relatively much bigger than attack traffic in source-side network, may affect the performance of detecting an attack. In other words, the source-side DoS detection method located at different time zones may have different detection results when a large-scale DDoS attack occurs. In addition, the detection result may be different depending on types of DoS detection methods used in each source-side network. Therefore, in order to mitigate the degradation of performance for detecting large-scale DDoS attack detection on every source-side network, it is necessary to share the results of attack detection among the every source-side network. In addition, if more accurate detection results are mainly shared, more accurate attack detection may be possible in every network.

In this paper, we propose a collaborative source-side DDoS attack detection method that determines whether an attack is made, by sharing the detection result which is weighted with the statistically calculated detection performance of each source-side DoS attack detection module located in different time zones. The weight for each detection result is calculated by considering the probability of detecting an attack correctly and the probability of false positives in the corresponding time index of a detection result. That is, the statistical weight means the probability that the source-side attack detection module accurately classifies attack traffic and normal traffic in the corresponding time index. The collaborative source-side attack detection module shares detection results and weights of the source-side attack detection modules located at different time zones, and finally compares the weighted arithmetic average with an arbitrary

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-2020-2016-0-00314) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation). This research was one of KOREN projects supported by National Information Society Agency (No.1711117098).
*Prof. Kyungbaek Kim is the corresponding author.

threshold to determine an attack. To improve the performance of these methods, we evaluate the performance of the collaborative source-side DDoS detection method according to the individual source-side DoS detection method [1,2,4]. To verify the effectiveness of the proposed method, we performed experiments based on actual DNS traffic data to check the detection rate and false positive rate of the collaborative source-side DDoS detection method according to the source-side DoS detection method.

The rest of this paper is arranged as follows. Chapter II describes the work associated with a collaborative DDoS attack detection model. Chapter III describes the proposed SDN-based source-side DoS detection method. Chapter IV describes the proposed collaborative source-side DDoS detection method. Chapter V presents the results of the experiment, and Chapter VI provides conclusions and future research directions.

II. Related Work

In the past, collaborative attack detection models for DoS attacks have been studied [7,8,9,10,11,12]. These studies mainly understand the network structure and dynamically allocate resources or algorithms to detect DDoS using the degree of aggregation and inflow of attack network traffic that occurs when the network traffic flows from the attacker's network to the victim's network. Through this, a system that facilitates a collaborative network is proposed. However, these papers mainly assume a situation in which the volume of attack network traffic is significantly different from the volume of normal network traffic, and propose an algorithm that detects better as it is closer to the victim than the source.

Conversely, collaborative attack detection models for DoS attack detection near the attack source or source-side network have also been studied [5,6]. By sharing the results of the attack detection module with each source-side network, these studies prevented the false positive rate through the synergy effect of connected source-side network greatly. However, these methods share detection with false positive as attack traffic. Accordingly, the false positive rate of the collaborative attack detection module may be increased when the results of each site are finally shared. In addition, the performance of the collaborative source-side DDoS detection method may be affected by the difference in detection performance for each site. In other words, the performance of the collaborative source-side DDoS detection method may be affected by individual source-side DoS detection methods such as OTAT (Observed Traffic Aware Threshold)[1], STBAT (Seasonality Traffic Behavior Aware Threshold)[2] and L-STBAT (LSTM-based STBAT)[4].

III. Collaborative Source-Side DDoS Detection

Because of the difference in the usage of normal traffic for each different time zone, the performance of the source-side attack detection modules located in different time zones may be different. As shown in Figure 1, the proposed collaborative source-side DDoS attack detection method determines the final result using the detected results and statistical weights of the source-side attack detection modules located in different time zones [2]. At this time, the detection result $d_i^{t_i}$ of the i^{th} source-side attack detection module in the time window t_i.

The time window t_i is composed of 1 minute intervals. As a result of detection, the value of $d_i^{t_i}$ has a value of 1 when an

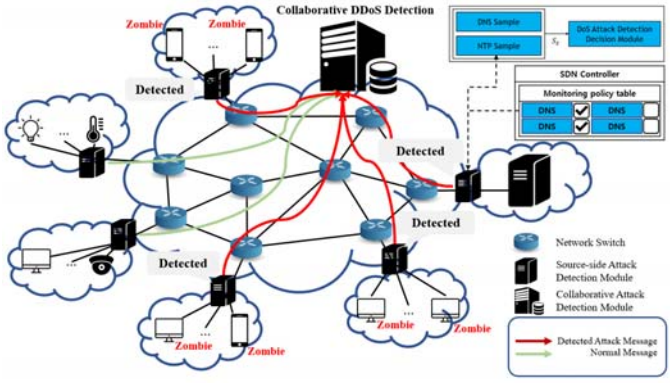

Figure 1. Architecture of Collaborative source-side DDoS Detection

attack is detected, and has a value of 0 when no attack is detected. The source-side attack detection module for each site shares the detection result $d_i^{t_i}$ corresponding to the time window t_i and the statistical weight W_{t_i} based on the detection result to the collaborative attack detection module. The collaborative attack detection module uses the weighted arithmetic mean A^t to determine the final result by using the detection result $d_i^{t_i}$ and statistics weight W_{t_i} shared by each site of the source-side attack module. The weighted arithmetic mean A^t formula is shown below:

$$A^t = \sum_{i=1}^{L} \frac{W_{t_i} * d_i^{t_i}}{W_{t_i}} \quad (1)$$

If this weighted arithmetic average A^t is greater than the specified threshold θ, the attack is finally determined to have been detected at that time window t.

Here, the performance of attack detection can be affected by the method of assigning weight for each detection result, three different statistical weighting W_{t_i} methods are proposed : EW (Equal Weight), DW (Detection Weight) and MW (Mixed Weight).

EW method is a method to give equal weight to the detection result $d_i^{t_i}$ for the time window t_i of the source-side attack detection module located in different time zones. The weight W_{t_i} of this method is set to 1. At this time, to determine the final result, the weighted arithmetic mean A^t is modified as shown in the following formula.

$$A^t = \sum_{i=1}^{L} \frac{d_i^{t_i}}{L} \quad (2)$$

This method shares results regardless of the performance of the source-side attack detection modules located at different time zones. So the false positive rate of the collaborative source-side attack detection module may increase when the result is finally obtained. In order to consider the performance of the source-side attack detection module when finally determines the result, it is necessary to provide a detection result based statistical weight to the detection result.

DW method gives reliability to the result by giving the statistical weight W_{t_i} for the detected result to the detection result $d_i^{t_i}$ for the time window t_i of the source-side attack detection module located in different time. The weight W_{t_i} of

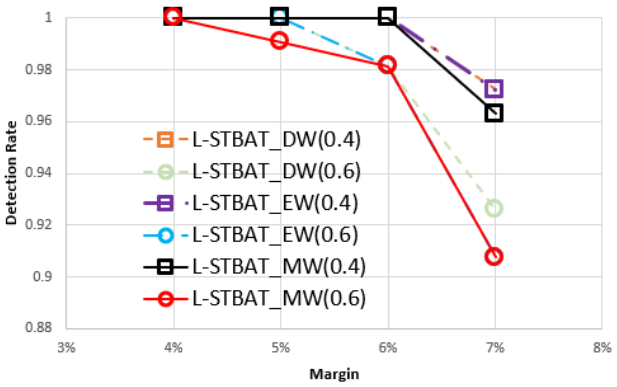

Figure 2. Detection Rate for L-STBAT based Collaborative DDoS Attack Detection

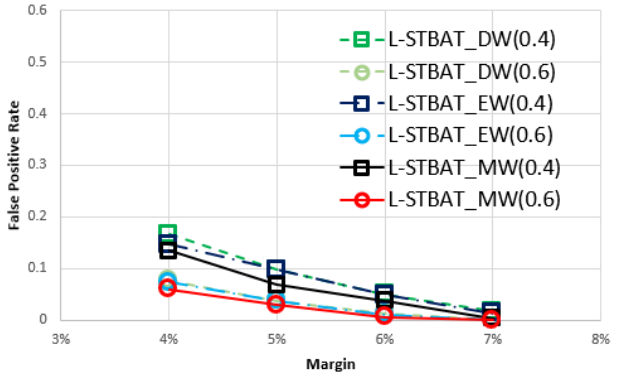

Figure 3. False Positive Rate for L-STBAT based Collaborative DDoS Attack Detection

this method is designated as the probability D_{t_i} to be detected when a virtual attack is given for N days. The formulas for probability D_{t_i} and weight W_{t_i} are as follows:

$$D_{t_i} = \sum_{k=1}^{N} \frac{d_i^{t_i-(N-k)*1440}}{N} \quad (3)$$

$$W_{t_i} = D_{t_i} \quad (4)$$

The collaborative attack detection module applying DW method shares the detection result $d_i^{t_i}$ for the time window t_i and the statistical weight W_{t_i} for the detected result in the source-side DoS module for each site, and finally calculates the weight for A^t. This method may increase the false positive rate of the collaborative source-side attack detection module when finally determining the result. It is because the weight of detection results does not consider the results of false positives. Therefore, in order to give the reliability of the detection result when the result is finally determined, it is necessary to provide a statistical weight to detections and false positives.

MW method provides statistics on detections and false positives in the detection result $d_i^{t_i}$ of the time window t_i of the source-side attack detection module located in different time zones to give reliability to the result. The weight W_{t_i} is obtained by adding the probability detection D_{t_i} when a virtual attack is given for N days and the probability of false positive F_{t_i} when the virtual attack is not given for N days, properly. In other words, the weight W_{t_i} is probability that the source-side attack detection module classifies the attack traffic and the normal traffic in the time window t_i. The formulas for

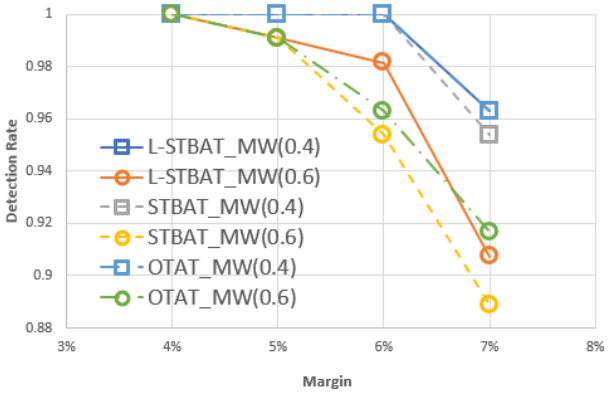

Figure 4. Detection Rate Comparison between Different individual Source-Side DoS Detection Methods

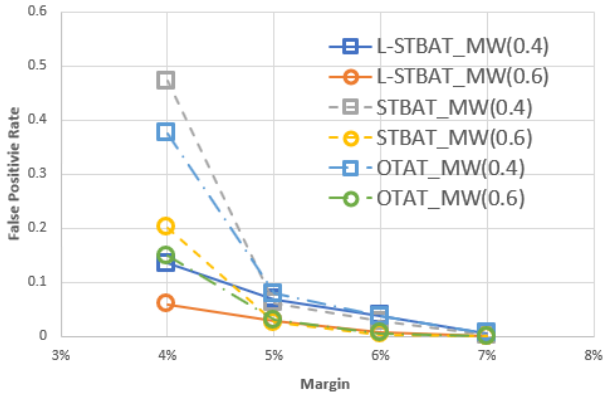

Figure 5. False Positive Rate Comparison between Different individual Source-Side DoS Detection Methods

probability D_{t_i} is shown in equation (3), and F_{t_i} and W_{t_i} are as follows :

$$F_{t_i} = \sum_{k=1}^{N} \frac{d_i^{t_i-(N-k)*1440}}{N} \quad (5)$$

$$W_{t_i} = \alpha * D_{t_i} + (1-\alpha) * F_{t_i} \quad (6)$$

The collborative attack detection module using the MW method hares the detection result $d_i^{t_i}$ for the time window t_i and the statistical weight W_{t_i} for the detected result in the source-side attack module for each site. The coefficient α represents the specific importance of D_{t_i} and F_{t_i}. These coefficient α has a constant value between 0 and 1. It means that the closer the value of the coefficient α is to 1, the greater probability of detecting an attack of source side attack detection module when attack traffic is detected. We set the coefficient α to 0.5 to equalize probability of detecting an attack by source side attack detection module when attack traffic is detected and probability of not detecting an attack by source side attack detection module when attack traffic is not detected.

IV. EVALUTATION

To show the effectiveness of the proposed collaborative method with different weighting method, the real-world DNS traffic obtained from DNS-STAT: Hedgehog. For verification of the proposed collaborative source-side DDoS attack detection technique, DNS request traffic of 39 days was collected from 10 sites located at different time zones. After

removing the outlier of the collected traffic, the traffic is defined as a normal traffic. To make adaptive thresholds of the source-side attack detection modules located at different time zones aware of traffic seasonality, DNS query traffic corresponding to the first 30 days of 2018 per site is used. In the case of LSTM network learning used in the L-STBAT model, a gradient descent optimization algorithm and a batch of 100 sizes are used and 1000 training times are repeated. To measure detection and false positive of traffic samples captured every minute from 10 sites located at different time zones, we use DNS query traffic equivalent to 8 days of 2018 per site. In this way, a period corresponding to the last 1 day of captured traffic is added per minute, and service attack traffic occurs simultaneously in time windows t at different time zones.

We compare the performance of the proposed weighting methods for collaborative source-side DoS attack detection: EW, DW, and MW. EW method gives equal weight to current detection regardless of the performance of the source-side attack detection modules located in different time zones. DW method assigns weights generated through statistics of previous detections in the corresponding time window to current detection. MW method assigns weights generated through statistics of previous detections and false positives in the corresponding time window to current detection. For comparing the weighting technique, it is assumed that every source-side detection module uses only one of L-STBAT, STBAT, and OTAT. In these individual detection technuques, a margin affects the threshold value and their detection performance, and it is applied from 4% to 7%. The threshold value of the collaborative attack detection module is varied between 0.4 and 0.7. We measure detection rate and false positive rate of each technique per margin.

Figure 2 shows the detection rate of L-STBAT according to individual weighting technique. Figure 3 shows the false positive rate of L-STBAT according to individual weighting technique. We compare the performance of individual weighting technique using L-STBAT-based source-side attack detection method at each site. At margin 6% and threshold 0.4, the MW method shows a false positive rate 4% while maintaining a high detection rate. At margin 5% and threshold 0.6, the DW method and EW method show 4% false positive rate while maintaining a high detection rate. When the MW method is used as the weighting technique, the overall false positive rate can be lowered by 2% compared to other weighting technique. However, collaborative attack detection modules may have different overall performance depending on the source-side detection methods used at each site.

Figure 4 shows the detection rate of the collaborative attack detection method based on the MW method according to the individual source-side attack detection method. Figure 5 shows the false positive rate of the MW method-based collaborative attack detection method according to each source-side attack detection method. In Figures 4 and 5, the case of using L-STBAT, STBAT, and OTAT as a source-side attack detection method used in each site was compared. As shown in Figures 4 and 5, L-STBAT maintains the best detection rate and achives a low false positive rate overall. If L-STBAT is used as source-side attack detection method, it is possible to detect detailed attacks in the source-side network and achives low false positive rate.

V. Conclusion

In this paper, we propose a new collaborative source-side DDoS attack detection method which shares detections and false positives of the source-side network over time. In detail, we proposed different weighing method to improve the reliability of the detection results of each source-side DoS detection module located in different time zone. The performance of the proposed method was verified through evaluation by using actual network traffic. Accordingly, when the MW (mixed weight) method is applied to a collaborative source-side DDoS attack detection, it reduces the false positives significantly and achieves reasonably high detection rate. Moreover, among different individual source-side DoS attack detection modules, L-STBAT achieves highest detection rate and the lowest false positive rate. Finally, it was confirmed that the L-STBAT+MW method can lower false positive rate by up to 35% while maintaining a higher detection rate than the OTAT+EW technique. In the future, we would like to propose a method that dynamically modifies the Margin according to the observed traffic volume and features according to the error rate of the source-side attack detection modules located in different time zones.

References

[1] Nguyen, Sinh-Ngoc, et al. "Source-Side Detection of DRDoS Attack Request with Traffic-Aware Adaptive Threshold." IEICE Transactions on Information and Systems 101.6 (2018): 1686-1690.

[2] Nguyen, Giang-Truong, et al. "Traffic Seasonality aware Threshold Adjustment for Effective Source-side DoS Attack Detection." KSII Transactions on Internet & Information Systems 13.5 (2019).

[3] Ramakrishnan, Nipun, and Tarun Soni. "Network traffic prediction using recurrent neural networks." 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA). IEEE, 2018.

[4] Nguyen, Giang-Truong, et al. "LSTM based Network Traffic Volume Prediction." Proceedings of 2018 KIPS Spring Conference. 2018.K. Elissa, “Title of paper if known,” unpublished.

[5] Sungwoong Yeom, Kyungbaek Kim. "A Study on Collaborative Source-Side DoS Attack Detection." KICS (2019): 478-479.

[6] Song, ByungHak, Heo, Joon, and Hong, Choong Seon, “Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks.” IEICE Transactions 90-B (2007): 2655-2664.

[7] Shalinie, S. Mercy, et al. "CoDe—An collaborative detection algorithm for DDoS attacks." 2011 International Conference on Recent Trends in Information Technology (ICRTIT). IEEE, 2011.

[8] DChen, Yu, Kai Hwang, and Wei-Shinn Ku. "Collaborative detection of DDoS attacks over multiple network domains." IEEE Transactions on Parallel and Distributed Systems 18.12 (2007): 1649-1662.

[9] Chen, Yu, and Kai Hwang. "Collaborative change detection of DDoS attacks on community and ISP networks." International Symposium on Collaborative Technologies and Systems (CTS'06). IEEE, 2006.

[10] Tariq, Usman, et al. "Collaborative peer to peer defense mechanism for ddos attacks." Procedia Computer Science 5 (2011): 157-164.

[11] Rashidi, Bahman, Carol Fung, and Elisa Bertino. "A collaborative DDoS defence framework using network function virtualization." IEEE Transactions on Information Forensics and Security 12.10 (2017): 2483-2497.

[12] Rashidi, Bahman, and Carol Fung. "CoFence: A collaborative DDoS defence using network function virtualization." 2016 12th International Conference on Network and Service Management (CNSM). IEEE, 2016.