통계적 가중치를 이용한 협력형 소스측 분산 서비스 거부 공격 탐지 기법

염성웅, 김경백
전남대학교 전자컴퓨터공학부
yeomsw0421@gmail.com, kyungbaekkim@jnu.ac.kr

Collaborative Source-Side DDoS Attack Detection using Statistical Weight

Sungwoong Yeom, Kyungbaek Kim
Dept. Electronics and Computer Engineering, Chonman National University

요 약

최근 보안이 취약한 IoT 기기를 악용하는 분산 서비스 거부 공격을 보다 빠르게 감지하고 공격자의 위치를 확보하기 위해, 소스측 서비스 거부 공격 탐지 기법이 연구되었다. 또한, 대규모 분산 서비스 거부 공격의 효과적인 탐지를 위해 여러 사이트의 소스측 탐지결과를 공유하여 탐지 성능을 향상시키는 협력형 소스측 서비스 거부 공격 탐지 기법도 연구 되었다. 이러한, 협력형 탐지 기법에서는 서로 다른 시간대에서 수행된 공격 탐지 성능 편차에 의해 전체적인 공격 탐지 성능이 영향을 받을 가능성이 있다. 이 논문에서는 공격 탐지 기법의 각 시간대별 탐지 성능을 통계적으로 분석한 가중치를 이용하는 협력형 소스측 분산 서비스 거부 공격 탐지 기법을 제안한다. 특히, 공격을 오탐지하는 거짓 양성률(false positive rate)를 고려하여, 협력형 탐지 기법의 오탐율을 낮출 수 있도록 하였다. 실제 DNS요청 트래픽을 수집하고, 이를 기반으로 실험한 결과, 제안하는 가중치를 사용하였을 때, 공격탐지율은 높게 유지하면서, 오탐율을 약 30% 줄일 수 있음을 확인하였다.

Ⅰ. 서 론

IoT 환경의 활성화에 따라, 이기종 네트워크 엔티티로 구성된 협업 네트워크 시스템(CNS)도 커지는 추세이다. 하지만, 여러 지역에 분포한 IoT 기기의 보안이 취약함을 악용한 분산 서비스 거부 공격의 위협이 급격히 증가하고 있다. 이렇게 악용된 IoT 기기들이 생산한 트래픽의 량은 소량이지만 피공격자 측 네트워크에서는 대량의 공격 트래픽이 유입된다. 또한 피공격자 측 네트워크는 지연된 탐지 및 공격자 추적의 어려움과 같은 몇 가지 단점이 드러난다. 최근 에지 컴퓨팅의 발달됨으로써 소스측에서 네트워크 공격 트래픽 탐지 기법을 위해 다양한 연구들이 진행되고 있다.

소스측에서 발견되는 공격 트래픽의 총량은 피해자 측에서 발견되는 공격 트래픽에 비해 상대적으로 작기 때문에 공격 트래픽이 정상적인 네트워크 트래픽에 쉽게 섞일 수 있다. 이와 같은 공격트래픽을 탐지하기 위해 관찰된 트래픽의 양을 이용하여 동적으로 공격 탐지 임계 값을 변경하는 기법이 연구되었다.[1] 하지만, 특정 지역에 고정되어 있는 소스측 공격 탐지 모듈은 대규모로 분산되는 공격의 특징을 포착할 수 없다. 또한, 소스측 공격 탐지 모듈의 성능은 시차가 위치한 지역의 네트워크 에지에서 관찰되는 시간과 트래픽의 특징에 따라 성능이 다를 수 있다.

이 소스측 공격 탐지 모듈별 성능 편차를 극복하기 위해, 각 소스측 공격 탐지 모듈의 시간 인덱스 별 탐지 결과를 공유하여 최종 탐지 결과를 도출하는 연구가 진행되었다.[2] 이 기법은 공격이 탐지된 모듈의 수가 주어진 임계값보다 높을 경우 공격을 탐지하도록 한다. 하지만, 이러한 기법은 정상적인 트래픽을 공격 트래픽으로 오탐지된 결과들 또한 함께 공유되기 때문에 최종적으로 공유하여 결과를 도출할 때 협력형 공격 탐지 모듈의 오탐율이 증가할 수 있다.

이 논문에서는 여러 사이트에 위치한 소스측 서비스 공격 탐지 모듈의 시간 인덱스 별 탐지 성능을 통계적으로 계산한 가중치와 탐지결과를 공유하여 공격여부를 판단하는 협력형 소스측 분산 서비스 거부 공격 탐지 기법을 제안한다. 각 소스측 공격 탐지 모듈은 적응형 임계를 사용하여 공격을 탐지한다. 소스측 공격 탐지 모듈의 시간 인덱스 별 탐지 성능을 통계적으로 계산한 가중치는 해당 시간 인덱스에 공격이 존재하였을 때 탐지될 확률과 공격이 존재하지 않았을 때 잘못 탐지되지 않을 확률의 합, 즉, 소스측 공격 탐지 모듈이 통계적으로 해당 시간 인덱스에 공격 트래픽과 정상트래픽을 정확하게 분류할 확률로 설정한다. 협력형 공격 탐지 모듈은 서로 다른 시간대에 위치한 소스측 공격 탐지 모듈의 탐지 결과와 가중치들을 공유하고 가중치 산술 평균을 계산한다. 최종적으로 가중치 산술 평균과 임의의 임계값과 비교하여 공격을 판단한다.

제안된 기법의 실효성 검증을 위해, 실제 DNS 트래픽 데이터에 기반한 실험을 수행하여 제안된 기법이 공격탐지율(Detection Rate)과 공격오탐율(False Positive Rate)에서 기존의 공격탐지 기법의 성능을 능가하는 것을 확인하였다.

Ⅱ. 관련 연구

과거에도 서비스 거부공격 탐지를 위한 협력형 공격 탐지 모델은 연구되어 왔다. [4,5,6,7,8,9] 이 연구들은 주로 네트워크 구조를 이해하여 네트워크 트래픽이 공격자가 위치한 네트워크에서 피공격자가 위치한 네트워크로 유입되는 과정에서 발생하는 공격 네트워크 트래픽의 결집 정도 및 유입 정도를 활용하여 분산 서비스 거부 공격을 탐지하는 알고리즘 또는 동적으로 자원 할당을 통해 협업 네트워크를 용이하게 하는 시스템을 제안하고 있다. 그러나, 이 논문들은 공격 네트워크 트래픽의 볼륨이 정상 네트워크 트래픽 볼륨과 확연히 차이나는 상황을 주로 가정하고 있으며, 소스측 보다는 피공격자 측에 가까울수록 탐지가 더 잘되는 알고리즘을 제안하고 있다.

이와 반대로 공격원이나 피해자 네트워크 근처에 위치하여 서비스 거부

공격 탐지를 위한 협력형 공격 탐지 모델 또한 연구되어 왔다. [2,3] 이 연구들은 각 소스측 네트워크에 공격 탐지 모듈을 위치시키고 결과를 공유함으로써 연결된 소스측 네트워크의 시너지 효과를 통해 거짓 경보 발생률을 크게 방지하였다. 하지만, 이러한 기법들은 공격 트래픽으로 오탐지된 결과들이 정상적으로 탐지된 결과들과 함께 공유되기 때문에 최종적으로 공유하여 결과를 도출할 때 협력형 공격 탐지 모듈의 오탐율이 증가할 수 있다.

Ⅲ. 통계적 가중치를 이용한 협력형 소스측 분산 서비스 거부공격 탐지 기법

제안된 협력형 소스측 분산 서비스 거부공격 탐지 기법은 서로 다른 시간대에 위치한 소스측 거부 공격 탐지 모듈에서 탐지된 결과와 탐지 결과 통계 기반 가중치를 활용하여 최종 결과를 도출한다.[2] 이때, 각 소스측 거부 공격 탐지 모듈은 관찰되는 트래픽 기반 적응형 임계값 조정 기법을 사용한다.[1] 이 적응형 임계값 조정 기법은 일정한 시간 간격동안 관찰되는 트래픽의 양을 사용하여 예측한 트래픽 양에 Margin을 더하여 동적으로 공격 탐지 임계 값을 조정한다. 이때, 적응형 임계값 조정 기법이 공격에 대한 영향을 받지 않는다는 가정을 적용한다. i번째 소스측 서비스 거부 공격 모듈의 타임윈도우 t_i에 대한 탐지 결과를 $d_i^{t_i}$이라 한다. 타임윈도우 t_i는 1분 간격으로 구성되며 탐지 결과 $d_i^{t_i}$의 값은 공격이 탐지될 경우 1의 값을 가지고 공격이 탐지되지 않을 경우 0의 값을 가진다.

i번째 소스측 서비스 거부 공격 모듈의 타임윈도우 t_i의 탐지 결과 통계 기반 가중치는 N일 동안 가상의 공격을 부여하였을 때 탐지할 확률 D_{t_i}과 N일 동안 가상의 공격을 부여하지 않았을 때 오탐지할 확률 F_{t_i}들의 비중을 달리하여 더한 값, 즉, 소스측 공격 탐지 모듈이 통계적으로 타임윈도우 t_i에 공격 트래픽과 정상트래픽을 정확하게 분류할 확률로 설정한다. 이때, 확률 D_{t_i}와 확률 F_{t_i}의 정의는 $\sum_{k=1}^{N} \frac{d_i^{t_i-(N-k)*1440}}{N}$로 설정한다. 최종적인 가중치를 계산하는 수식은 아래와 같다.

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

여기서 계수 α는 D_{t_i}와 F_{t_i}의 비중을 나타내며 0과 1사이의 일정한 값을 가진다. 계수 α 값이 1에 가까울수록 임의의 타임윈도우 t_i에 공격이 존재하였을 때 공격을 탐지할 확률의 비중을 둔다고 할 수 있다. 우리는 계수 α를 0.5로 설정하여 공격이 존재하였을 때 공격을 탐지할 확률과 공격이 존재하지 않을 때 공격을 탐지하지 않을 확률의 비중을 같게 한다. 가중치 산술 평균은 각 사이트 별 소스측 서비스 거부 공격 모듈의 타임윈도우 t_i에 해당하는 탐지 결과 통계 기반 가중치와 탐지 결과를 공유하고 최종적으로 결과를 판단하기 위해 사용된다. 수식은 아래와 같다.

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

가중치 산술 평균값이 임의로 지정된 임계값 θ 보다 클 경우, 최종적으로 해당 타임윈도우 t에서 공격이 탐지되었다고 판단한다.

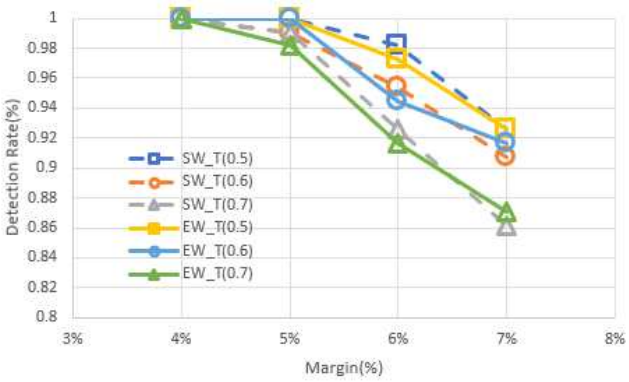

그림 1. Detection Rate for Collaborative DDoS Attack Detection

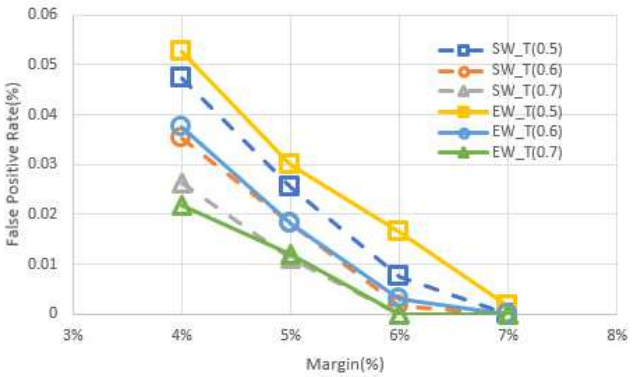

그림 2. False Positive Rate for Collaborative DDoS Attack Detection

Ⅳ. 실험 및 검증

제안된 협력형 소스측 분산 서비스 거부 공격 탐지 기법의 검증을 위해, 서로 다른 시간대에 위치하는 10개의 사이트에서 각각 9일간의 DNS 요청 트래픽을 수집하였다. 수집된 트래픽의 Outlier를 제거한 후, 해당 트래픽을 정상트래픽으로 정의하였다. 각 사이트의 9일간의 DNS 요청 트래픽 중 8일은 가중치를 계산하기 위해 사용되었다. 서비스 거부 공격 트래픽은 해당 트래픽의 마지막 1일에 해당하는 기간에 추가되었으며, 서비스 공격 트래픽은 서로 다른 시간대의 타임 윈도우t_i에서 동시에 발생하도록 하였다. 우리는 서로 다른 시간대에 위치하는 소스측 거부 공격 탐지 기법의 성능과 상관없이 공격 탐지가 된 사이트 수에 결과를 판단한 EW(Equal Weight) 기법[2]과 탐지된 결과 통계 기반 가중치 SW(Statistical Weight) 기법을 비교한다. 이때, 각 소스측 거부 공격 탐지 기법의 임계 값에 영향을 주는 Margin은 4% ~ 7%까지 적용하고, 협력형 공격 탐지 기법의 임계 값θ은 0.1씩 변화 시키면서 테스트한다. 각 소스측 거부 공격 탐지 모듈의 Margin 별각 기법별로 EW 기법과 SW 기법의 공격 탐지율(Detection Rate)과 공격 오탐율(False Positive Rate)를 측정한다.

그림 1의 Margin의 변화에 따른 각 협력형 공격 탐지 기법의 공격 탐지율(Detection Rate)은 각 소스 측 공격 탐지 모듈의 결과와 가중치를 공유하여 최종적으로 결과를 도출하였을 때 전체 분산 서비스 거부 공격 수 중 탐지된 공격 횟수를 뜻한다. 그림 2의 Margin의 변화에 따른 각 협력형 공격 탐지 기법의 공격 오탐율(False Positive Rate)은 각 소스 측 공격 탐지 모듈의 결과와 가중치를 공유하여 최종적으로 결과를 도출하였을 때 정상적인 트래픽 수 중 공격으로 오 탐지된 공격 수를 뜻한다. 그림 1과

그림 2에서 T(x)는 임계값 θ 를 x로 설정하는 것을 의미한다.

실험 결과에서 SW기법은 EW기법과 비슷한 Detection Rate 값을 보이면서도, 전반적으로 낮은 False Positive Rate 값을 가지는 것을 확인할 수 있다. 특히, 완벽한 detection rater를 가지는 설정인 Margin 4% 또는 5%에서 임계값이 0.5 또는 0.6인 경우, SW 기법은 EW 기법에 비해 공격 오탐율을 최대 30%정도 낮출 수 있음을 확인하였다.

Ⅴ. 결론

본 논문에서는 적응형 임계값 조절 기법을 이용하는 소스측 서비스 거부 공격 탐지 기법의 성능을 향상시키기 위한 협력적 기법을 제안하고, 실제 네트워크 트래픽에 이용한 평가를 통해 제안된 기법의 성능을 검증하였다. 검증된 결과로 SW 기법은 EW 기법에 비해 전반적으로 공격 오탐율을 낮추며 최종적으로 30%정도 낮출 수 있음을 확인하였다. 향후, 서로 다른 시간대에 위치한 소스측 공격 탐지 모델의 Margin 값을 관찰되는 트래픽 량과 특징에 따라 동적으로 수정하는 기법을 제안하고자 한다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2017RIA2B4012559). 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음" (IITP-2020-2016-0-00314).

참 고 문 헌

[1] Nguyen, Sinh-Ngoc, Nguyen, Van-Quyet, Nguyen, Giang-Truong, Kim, JeongNyeo, Kim, and Kyungbaek, "Source-Side Detection of DRDoS Attack Request with Traffic-Aware Adaptive Threshold." IEICE Transactions on Information and Systems 101.6 (2018): 1686-1690.

[2] 염성웅, and 김경백. "협력형 소스측 서비스 거부 공격 탐지 기법 연구." 한국통신학회 학술대회논문집 (2019): 478-479.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] Nguyen, Giang-Truong, Nguyen, Van-Quyet, Nguyen, Huu Duy, and Kim, Kyungbaek,. "LSTM based Network Traffic Volume Prediction.", In Proceedings of 2018 KIPS Spring Conference, 2018.