협력형 소스측 서비스 거부 공격 탐지 기법 연구

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

A Study on Collaborative Source-Side DoS Attack Detection

Sungwung Yeom, Kyungbaek Kim
Dept. Electronics and Computer Engineering, Chonnam National University

요 약

최근 IoT의 활성화에 따라 IoT 기기를 악용하는 분산 서비스 거부 공격 위협이 급격히 증가하고 있다. 이에 따라, IoT 환경이 구축된 소스측 네트워크에서 발생하는 트래픽을 분석하여 서비스 거부 공격을 탐지하는 소스측 서비스 거부 공격 탐지 기법에 대한 연구가 활발히 진행되고 있다. 분산 서비스 거부 공격 탐지의 경우, 공격대상이 연결된 네트워크에는 대량의 트래픽이 탐지되어 손쉽게 공격을 감지할 수 있는 반면, 공격자가 위치한 소스측에서의 공격 트래픽 탐지는 보다 세밀하고 정교한 트래픽 분석이 필요하다. 그러나, 소스측 네트워크에서는 공격트래픽이 손쉽게 일반 트래픽과 섞일 수 있어서, 공격 탐지에 사용되는 트래픽의 상태에 따라 탐지 성능이 영향을 받을 수 있다. 이 논문에서는 이러한 소스측 서비스 거부 공격의 탐지 성능의 편차를 극복하기 위해, 여러개의 소스측 공격 탐지 모듈이 협력하여 서비스 거부 공격여부를 판단하는 방법을 제안한다. 각 소스측 네트워크에서 공격탐지를 위해 LSTM기반 소스측 서비스 거부공격 탐지 모듈을 사용하고, 각 사이트의 공격 탐지 결과를 상호 공유하여 각 시간 인덱스에 해당하는 협력형 탐지 결과를 도출한다. 제안된 기법의 검증을 위해, 다수의 사이트의 DNS 요청 트래픽을 수집하였고, 이 트래픽을 이용해 제안된 기법의 성능을 평가하였다. 성능평가를 통해, 협력형 기법을 사용할 경우 단독으로 소스측 공격 탐지 기법에 비해 공격탐지율은 5% 상승하고 오탐율도 5% 줄일수 있음을 확인하였다.

Ⅰ. 서 론

IoT 환경의 활성화에 따라, 다양한 IoT기기를 악용하는 분산 서비스 거부 공격 위협이 급격히 증가하고 있다. 최근 미라이 봇넷 기반 서비스 거부 공격 및 스턱스 넷 기반 서비스 거부 공격 등이 IoT기기를 악용한 분산 서비스 거부 공격의 대표적인 사례이다. 이러한 공격에서 여러 지역에 퍼져 있는 IoT기기들은 소량의 공격트래픽을 생성하는 반면, 피공격자 주변의 네트워크에는 대량의 공격트래픽이 유입된다.

IoT 환경 활성화와 함께 에지 컴퓨팅 환경 또한 활성화 되고 있다. 에지 컴퓨팅의 발달에 따라 다양한 네트워크 서비스들이 네트워크 에지에서 구현되고 있다. 서비스 거부 공격 탐지의 경우, 클라우드 내의 네트워크 트래픽을 분석하거나 네트워크 게이트웨이의 트래픽을 분석하여 공격자가 위치한 소스측에서 공격을 탐지하는 연구가 수행되고 있다.[1] 이러한, 소스측 서비스 거부 공격 탐지는 공격 트래픽의 총량이 확연히 다르게 되는 피공격자측 서비스 거부 공격 탐지와는 상이한 기법을 적용하는 것이 필요하다. 소스측에서 발생되는 공격 트래픽은 그 총량이 상대적으로 작아서 정상적으로 발생되는 네트워크 트래픽에 쉽게 섞일 수 있게 되어, 소스측 서비스 거부 공격 탐지를 위해서는 보다 세밀하고 정교한 탐지 기법의 개발이 필요하다.

최근, 소스측 서비스 거부 공격 탐지 기법을 위해 소스측 네트워크 트래픽의 시간적 변화를 세밀히 분석하여 서비스 거부 공격 탐지를 위한 네트워크 임계값을 능동적으로 조절하는 기법들이 연구되었다.[2,3,4] 이 연구들은 소스측 네트워크 트래픽의 특성, 특히 시간별 네트워크 트래픽 변화의 계절성(Seasonality)를 이용하여 각 시간별 네트워크 트래픽을 예측하거나, LSTM을 이용하여 네트워크 트래픽의 변화를 학습하고 각 시간대별 네트워크 트래픽을 예측하는 기법 등을 활용해 임계값을 능동적으로 조절하여 소스측 서비스 거부 공격 탐지를 수행하는 모듈을 제안하였다. 하지만, 이러한 모듈들은 네트워크 트래픽의 현재의 특성 값에 따라 탐지 성능이 달라질 수 있다는 한계가 있다.

이러한 동적 네트워크 임계값에 기반한 소스측 서비스 거부 공격 탐지 기법의 성능을 향상시키기 위해, 우리는 여러 사이트에서 운용되는 소스측 서비스 거부 공격 탐지 모듈들이 협력하여 해당 결과를 상호 교환하는 협력형 서비스 거부 공격 탐지 기법을 제안한다.

Ⅱ. 관련연구

과거에도 서비스 거부공격 탐지를 위한 협력형 모델은 연구되어 왔다.[5,6,7,8] 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 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.

본 논문에서는 피공격자 측은 고려하지 않고, IoT 기기와 같이 보안에 취약한 기기들이 활용되는 소스측 네트워크에서 서비스 거부 공격 트래픽을 탐지하는 기법에 주안점을 둔다.

Ⅲ. 협력형 소스측 서비스 거부공격 탐지 기법 및 검증

제안하는 협력형 소스측 서비스 거부공격 탐지 기법은 각 사이트에 위치한 네트워크 트래픽 예측 기반 능동적 임계값 조절을 통한 소스측 서비

스 거부 공격 모듈에서 제공하는 탐지 결과를 협력적으로 활용하여 최종 결과를 도출하도록 한다. 특히, 이 논문에서는 탐지 결과의 평균값을 활용한 협력형 탐지 기법을 제안하고, 실험을 통해 제안하는 기법의 성능을 평가 한다.

전체 사이트의 개수, 즉 소스측 서비스 거부 공격 모듈의 개수를 L 이라 한다. 각 소스측 서비스 거부 공격 모듈의 일정 타임윈도우 t 에 대한 탐지 결과를 d_i^t ,$i \in L$ 이라 한다. 임의의 타임윈도우 t 에 대한 탐지 결과의 평균값은 $A^t = \sum_{i=1}^{L} d_i^t / L$ 과 같이 계산되고, 이 평균값이 지정된 임계값 θ 보다 클 경우, 최종적으로 해당 타임윈도우 t 에서 공격이 탐지되었다고 판단한다.

제안된 협력형 소스측 서비스 거부 공격 탐지 기법의 검증을 위해, 10개의 사이트에 해당하는 10일간의 DNS 요청 트래픽을 수집하였다. 수집된 트래픽의 Outlier를 제거한 후, 해당 트래픽을 정상트래픽으로 정의하였다. 서비스 거부 공격 트래픽은 해당 트래픽의 마지막 2일에 해당하는 기간에 추가되었으며, 서비스 공격 트래픽은 모든 사이트에서 동일한 타임윈도우에서 발생하도록 하였다. 각 사이트에는 LSTM 트래픽 예측 기반 소스측 서비스 공격 탐지 모듈을 운용하도록 하여 마지막 2일에 해당하는 공격 탐지 결과를 추출하였고, 해당 결과를 공유하는 협력형 공격 탐지 결과도 함께 추출하였다.

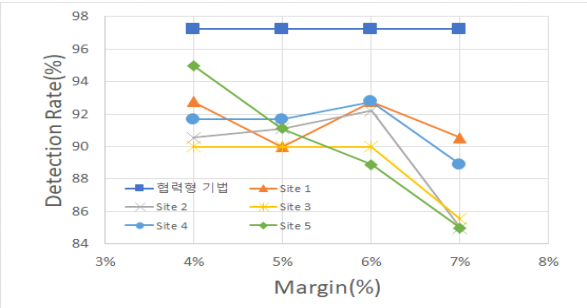

그림 1. 각 사이트 및 협력형 기법에 대한 공격 탐지율

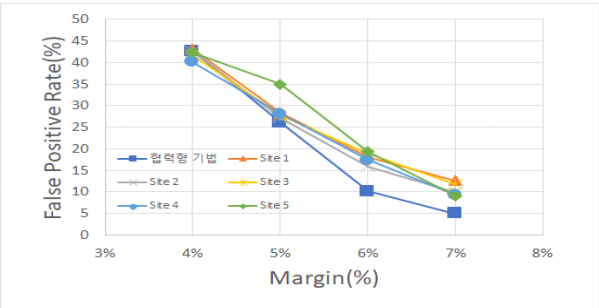

그림 2. 각 사이트 및 협력형 기법에 대한 오탐율

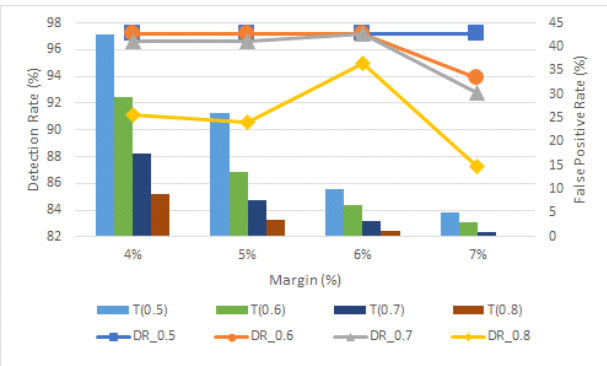

그림3. 임계값 θ 에 따른 협력형 기법 성능

그림 1, 2에서 알 수 있듯이, 협력형 기법을 사용할 경우, 단위 사이트에서의 공격 탐지에 비해 탐지율은 약 5% 상승하여 97%를 유지하고, 오탐율은 약 5%를 줄여 5~10%를 유지할 수 있다. 제안하는 협력형 탐지 기법은 최종 탐지 결과의 판단을 위한 임계값 설정에 따라 그 성능이 달라진다. 그 결과는 그림 2에서 확인할 수 있다.

Ⅳ. 결론

본 논문에서는 트래픽 볼륨 예측 기반 능동형 임계값 조절기법을 이용하는 소스측 서비스 거부 공격 탐지 기법의 성능을 향상시키기 위한 협력적 기법을 제안하고, 실제 네트워크 트래픽에 이용한 평가를 통해 제안된 기법의 성능을 검증하였다. 향후, 보다 다양한 분산 서비스 거부 공격 모델을 고려하는 탐지 기법을 제안하고자 한다.

ACKNOWLEDGMENT

이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2017R1A2B4012559). 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터 지원사업의 연구결과로 수행되었음 (IITP-2019-2016-0-00314).

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] Giang-Truong Nguyen, Van-Quyet Nguyen, Sinh-Ngoc Nguyen and Kyungbaek Kim, "Traffic Seasonality aware Threshold Adjustment for Effective Source-side DoS Attack Detection," KSII Transactions on Internet and Information Systems, vol. 13, no. 5, pp. 2651-2673, 2019. DOI: 10.3837/tiis.2019.05.023

[3] 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.

[4] 염성웅, 뉘엔 지앙 즈엉, 뉘엔 반 퀴엣, 김경백, LSTM기반 소스 측 DoS공격 탐지에서 특징벡터 영향 평가. In Proceedings of 2019년도 한국스마트미디어학회(KISM) 춘계학술대회, April 26-27, 2019, 한국교통대학교, 충주.

[5] 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.

[6] 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.

[7] Jingle, I. Diana Jeba, and Elijah Blessing Rajsingh. "ColShield: an effective and collaborative protection shield for the detection and prevention of collaborative flooding of DDoS attacks in wireless mesh networks." Human-centric Computing and Information Sciences 4.1 (2014): 8.

[8] 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.