KNOM Review '20-01 Vol.23 No.01
https://doi.org/10.22670/knom.2020.23.1.10

통계적 가중치를 이용한 협력형 소스측 DDoS 공격 탐지 기법 성능 평가

염 성 웅◆, 김 경 백°

Assessment of Collaborative Source-Side DDoS Attack Detection using Statistical Weight

Sungwoong Yeom◆, Kyungbaek Kim°

요 약

최근 보안이 취약한 IoT 장치를 악용하는 분산 서비스 거부 공격의 위협이 확산됨에 따라 신속하게 공격을 탐지하고 공격자의 위치를 찾기 위해 소스측 서비스 거부 공격 탐지 연구가 활성화되고 있다. 또한, 소스측 탐지의 지역적 한계를 극복하기 위해 개별 사이트에 위치한 소스측 네트워크들의 탐지 결과를 공유하는 협력형 소스측 공격 탐지 기법도 활성화되고 있다. 이 논문에서는 통계적 가중치를 이용하는 협력형 소스측 분산 서비스 거부 공격 탐지 기법의 성능을 평가한다. 통계적 가중치는 개별 소스측 네트워크의 시간대에 해당하는 탐지율과 오탐지율을 기반으로 계산된다. 제안된 기법은 여러 지역에서 발생한 소스측 서비스 거부 공격 탐지 결과들을 수집하고 가중치를 부여하여 결과를 도출하고, 이를 통해 DDoS 공격 발생 여부를 결정한다. 실제 DNS 요청 트래픽을 기반으로 실험한 결과, 제안된 기법은 높은 공격탐지율을 유지하면서, 공격오탐율을 2% 줄일 수 있음을 확인하였다.

Key Words : Network Security, DDoS Attack, Software-Defined Networking (SDN), Collaborative Source-side detection

ABSTRACT

As the threat of Distributed Denial-of-Service attacks that exploit weakly secure IoT devices has spread, research on source-side Denial-of-Service attack detection is being activated to quickly detect the attack and the location of attacker. In addition, a collaborative source-side attack detection technique that shares detection results of source-side networks located at individual sites is also being activated to overcome regional limitations of source-side detection. In this paper, we evaluate the performance of a collaborative source-side DDoS attack detection using statistical weights. The statistical weight is calculated based on the detection rate and false positive rate corresponding to the time zone of the individual source-side network. By calculating weighted sum of the source-side DoS attack detection results from various sites, the proposed method determines whether a DDoS attack happens. As a result of the experiment based on actual DNS request to traffic, it was confirmed that the proposed technique reduces false positive rate 2% while maintaining a high attack detection rate.

※이 논문은 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2017R1A2B4012559)
※본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터지원사업의 연구결과로 수행되었음 (IITP-2020-2016-0-00314)
◆ First Author : Chonnam National University, Department of Electronics and Computer Engineering, yeomsw0421@gmail.com
° Corresponding Author : Chonnam Ntional University, Department of Electronics and Computer Engineering, kyungbaekkim@jnu.ac.kr, 정회원
논문번호 : KNOM2020-01-03, Received July 15, 2020; Revised July 30, 2020; Accepted August 16, 2020

Ⅰ. 서 론

IoT 환경 활성화에 따라, 여러 지역에 분산된 IoT 디바이스의 취약점을 악용한 분산서비스거부(DDoS) 공격 위협이 급증하고 있다.[2,15] 이렇게 악용된 IoT기기가 만들어내는 트래픽의 양은 소량이지만 피해자측 네트워크에서 대량의 트래픽이 유입이 된다. 그러나 피해자측 공격 탐지 방법은 탐지 지연, 공격자 추적의 어려움 등의 단점이 있다. 최근, 이러한 단점을 완화하기 위해 소스측 DoS 탐지 기법이 연구되고 있다.[1]

소스측 네트워크에서 관찰되는 트래픽의 양은 피해자측 네트워크에 비해 비교적 적기 때문에 공격 트래픽과 일반트래픽이 쉽게 혼합될 수 있다. 적은 양의 공격 트래픽을 감지하기 위해, 관찰되는 트래픽을 이용하여 공격 탐지 임계값을 동적으로 변경하는 기법이 연구되었다[3]. 그러나 관찰된 트래픽이 공격 트래픽과 섞일 경우, 이 기법은 새로운 임계값을 계산하기 위해 관찰된 트래픽과 공격 트래픽을 분리해야 한다. 관찰 트래픽과 공격 트래픽을 분리하기 위해 네트워크 트래픽 계절성을 활용하여 정상 트래픽의 양을 추정하는 기법이 연구되었다[4]. 이 기법은 정상 트래픽을 추정하기 위해 통계적으로 네트워크 트래픽 계절성을 식별하였다. 통계적으로 계산된 계절적 패턴은 공격 트래픽으로부터 작은 영향을 받아 정상 트래픽을 추정하는데 유용하다. 또한, 정상 트래픽 추정에 대한 성능을 개선하기 위해 시계열 딥러닝 분석을 사용한 트래픽 볼륨 추정 기법이 활발하게 연구되고 있다. 특히, LSTM은 네트워크 트래픽 볼륨 추정과 같은 시계열 딥러닝 분석에서 높은 성능을 보여준다[5,6].

하지만, 시간대가 다른 여러 사이트에서 대규모 공격이 동시적으로 개시되는 경우 소스측 네트워크에서는 공격 트래픽을 탐지하지 못할 수 있다. 피해자측 네트워크에 비해 소스측 네트워크에서는 소량의 트래픽을 분석하여 공격을 탐지하기 때문에, 시간대별 정상 트래픽의 변화는 공격 트래픽 탐지 성능에 영향을 미칠 수 있다. 다시 말해, 다른 시간대에 위치한 소스측 DoS 탐지 기법은 공격이 발생할 때 탐지 성능이 다를 수 있다. 또한, 각 소스측 네트워크에서 사용한 DoS 탐지 기법의 종류에 따라 탐지 성능이 다를 수 있다. 따라서 여러 지역에서 분산되어 개시된 대규모 DDoS 공격 탐지와 성능 저하를 완화시키기 위해서는 소스측 네트워크 간에 공격 탐지 결과를 공유할 필요가 있다.

이 논문에서는 서로 다른 시간대에 위치한 소스측 서비스 공격 탐지 모듈의 성능을 통계적으로 계산한 가중치와 탐지결과를 공유하여 최종적으로 공격여부를 판단하는 협력형 소스측 분산 서비스 거부 공격 탐지 기법을 제안한다. 개별 소스측 탐지 모듈의 성능을 표현한 가중치는 해당 시간 인덱스에서 공격탐지율과 공격오탐율을 고려하여 계산한다. 다시 말해 통계적 가중치는 소스측 공격 탐지 모듈이 해당 시간 인덱스에 공격 트래픽과 정상트래픽을 정확하게 분류할 확률을 의미한다. 협력형 공격 탐지 모듈은 공유된 가중치들을 통해 가중치 산술 평균을 계산하고 평가를 통해 설정된 임계값과 비교하여 공격 유무를 판단한다. 또한, 협력형 공격 탐지 기법은 개별 소스측 네트워크에 위치한 DoS 탐지 기법에 따라 그 성능이 다를 수 있다.

제안된 기법의 실효성 검증을 위해, 실제 DNS 트래픽 데이터에 기반한 실험을 수행하여 소스측 DoS 탐지 기법에 따른 협력형 소스측 DDoS 탐지 기법의 공격탐지율(Detection Rate)과 공격오탐율(False Positive Rate)을 확인한다. 특히, 개별 소스측 공격 탐지 기법의 종류와 탐지 기법에 참여하는 사이트의 수의 변화에 따른 협력형 소스측 DoS 탐지 기법의 성능을 평가한다.

이 논문은 다음과 같이 구성된다. 2장에서 소스측 DoS 공격 탐지를 위한 시스템 및 기법에 대한 설명과 협력형 DDoS 공격 관련 연구를 소개한다. 3장에서는 제안하는 협력형 소스측 DDoS 탐지 기법에 대한 자세한 내용을 소개하고, 4장에서 실제 DNS요청 트래픽에 기초하는 제안 기법의 성능평가 결과를 기술한다. 5장에서 이 논문의 결론 및 향후 연구 내용에 관해 기술한다.

Ⅱ. 연구 배경 및 관련 연구

1. 소스측 DoS 공격 탐지 기법

최근 대규모의 트래픽과 함께 대용량의 데이터 통신의 기술 발달에 따라 기존의 하드웨어 중심의 네트워크에서 소프트웨어 중심의 네트워크로 변화함으로써 논리적으로 네트워크를 관리하고 제어할 수 있게 되었다. 이러한 변화는 분산 네트워크를 중앙집중형으로 관리할 수 있게 되었으며 이에 따라 IoT와 같은 분산형 네트워크와 빅데이터 기반의 대용량 네트워크에서 SDN(Software-Define Networking)

은 필수적이다.

SDN 컨트롤러는 게이트웨이를 통과하는 네트워크 트래픽 중 DNS 또는 NTP와 같은 특정 프로토콜을 미러링(mirroring)하여 DoS 탐지 모듈로 전달한다. DoS 탐지 모듈은 관찰하고자 하는 프로토콜을 선택하고, 선택된 프로토콜을 기반으로 모니터링되는 트래픽을 동일한 단위시간 동안 수신하고 관찰된 트래픽 볼륨을 생성한다. 트래픽 볼륨의 시간창(time window) 크기는 단위시간의 배수로 표현되며 t_w으로 설정한다. z^{th} 시간 창에서 관찰된 트래픽 볼륨은 S_z로 정의된다. z^{th} 시간 창에서 관찰된 트래픽 볼륨 S_z은 DoS 탐지 모듈에서 임계값 θ과 비교하여 DoS 공격 여부를 결정한다. 이때, 임계값 θ의 계산 방법은 소스측 공격 탐지 모듈에 적용되는 개별 검출 방법에 따라 달라진다. 주요 개별 검출 방법으로는 OTAT[3], STBAT[4] 그리고 L-STBAT[6] 가 있다.

1) Observed Traffic Aware Threshold(OTAT): OTAT는 관찰된 트래픽 볼륨을 기반으로 임계값을 설정하는 알고리즘이다.[3] OTAT 기반 소스측 DoS 감지 모듈은 z^{th} 시간 창에서 관찰된 트래픽 볼륨 S_z과 공격 트래픽 볼륨이 혼합되어 있는지 여부를 결정한다. z^{th} 시간대의 관찰된 트래픽 볼륨 S_z에서 공격 트래픽 볼륨이 검출되면 OTAT는 현재의 임계값 θ을 유지한다. z^{th} 시간대의 관찰된 트래픽 볼륨 S_z에서 공격 트래픽 볼륨이 검출되지 않으면 OTAT는 관찰된 트래픽 볼륨 S_z에 근거한 Exponential Smoothing 함수를 사용하여 다음 트래픽 볼륨 $\overline{S}_{z+1}$을 예측한다. $\overline{S}_{z+1}$에 대한 수식은 아래와 같다.

$$\overline{S}_{z+1} = \mu * S_z + (1-\mu) * \overline{S}_z \qquad (1)$$

다음 임계값 θ_{z+1}은 예측 트래픽 볼륨 $\overline{S}_{z+1}$에 정상트래픽의 허용 변화량을 고려하는 마진(Margin) δ를 추가하여 갱신된다. θ_{z+1}에 대한 수식은 아래와 같다.

$$\theta_{z+1} = \overline{S}_{z+1} * (1+\delta) \qquad (2)$$

2) Seasonality Traffic Behavior Aware Threshold(STBAT): STBAT는 관찰된 트래픽 계절성을 기반으로 임계값을 설정하는 알고리즘이다.[4] STBAT 기반 소스측 DoS 감지 모듈은 z^{th} 시간대에서 관찰된 트래픽 볼륨 S_z과 공격 트래픽 볼륨의 혼합 여부를 결정한다. z^{th} 시간 창에서 관찰된 트래픽 볼륨 S_z에서 공격 트래픽이 감지되지 않는 경우, 식 (1)과 같이 관찰된 트래픽 볼륨 S_z에 기반하여 Exponential Smoothing을 사용하여 다음 트래픽 볼륨 $\overline{S}_{z+1}$을 예측하고, 다음 임계값 θ_{z+1}은 식 (2)와 같이 예측 트래픽 볼륨 $\overline{S}_{z+1}$과 마진 δ를 추가하여 갱신된다.

하지만, z^{th} 시간 창에서 관찰된 트래픽 볼륨 S_z에서 공격 트래픽이 검출되면, 트래픽 계절성을 기반으로 현재 트래픽 볼륨에서 정상 트래픽 볼륨 $S_{predict\,z}$를 추정하여, 다음 트래픽 볼륨 $\overline{S}_{z+1}$을 예측한다. 정상 트래픽 볼륨 $S_{predict\,z}$은 식 (3)와 같이 현재 트래픽 볼륨 S_z에 트래픽 계절성을 기반으로 관찰된 트래픽 변화율 $\triangle_z$을 곱하여 만든다.

$$S_{predict\,z} = S_z * \triangle_z \qquad (3)$$

이렇게 예측된 정상 트래픽 볼륨 $S_{predict\,z}$을 사용하여 식(4)와 같이 다음 트래픽 볼륨 $\overline{S}_{z+1}$을 예측한다.

$$\overline{S}_{z+1} = \mu * S_{predict\,z} + (1-\mu) * \overline{S}_z \qquad (4)$$

다음 임계값 θ_{z+1}은 예측 트래픽 볼륨 $\overline{S}_{z+1}$에 마진 δ를 추가하여 갱신된다.

3) LSTM-based Seasonality Traffic Behavior Aware Threshold(L-STBAT): L-STBAT는 트래픽의 계절성을 시계열 딥러닝 분석 모델인 LSTM으로 학습하고 이를 이용하여 정상 트래픽 볼륨을 예측하고 임계값을 조정하는 알고리즘이다.[6] 이때, LSTM은 트래픽의 변화율을 예측하는 데 사용된다. L-STBAT 기반

소스측 DoS 감지 모듈은 z^{th} 시간 창에서 관찰된 트래픽 볼륨 S_z에서 공격 트래픽이 감지되지 않는 경우, 식 (1)과 식 (2)를 사용하여 다음 트래픽 볼륨 $\overline{S}_{z+1}$ 및 다음 임계값 θ_{z+1}을 갱신한다.

하지만, z^{th} 시간 창에서 관찰된 트래픽 볼륨 S_z에서 공격 트래픽이 검출되는 경우, 식 (3)과 같이 현재 트래픽 볼륨에서 정상 트래픽 볼륨 $S_{predict\,z}$를 추정하고, 식 (4)와 같이 다음 트래픽 볼륨 $\overline{S}_{z+1}$을 예측한다. 다만, L-STBAT에서는 트래픽 볼륨 변화율 $\triangle_z$를 트래픽 계절성에 관련된 시계열 데이터를 학습한 LSTM 모듈을 통해 추정한다. 다음 임계값 θ_{z+1}은 예측된 트래픽 볼륨 $\overline{S}_{z+1}$에 마진 δ를 추가하여 갱신된다.

2. 협력형 공격 탐지 기법

과거에도 서비스 거부공격 탐지를 위한 협력형 공격 탐지 모델은 연구되어 왔다[7-14]. 논문[8]는 여러 라우터를 통해 트래픽 분포를 모니터링하여 DDoS를 조기 탐지할 수 있는 CAT(Change-Aggregation Tree)를 제안하였다. 논문[9]은 CAT를 이용한 DCD(Distributed Change-Point Detection) 아키텍처를 개발하였다. 이 기법은 페더레이션된 네트워크 환경에서 DDoS 공격에 대응하기 위해 라우터를 협력하여 조기 경고를 발생시킨다. 논문[10] 기존의 중앙 집중화된 구조에서 네트워크의 여러 부분에 공격 탐지기를 설치하는 분산 방법론을 제안하였다. 이 기법은 발생한 경보 수와 공격 흐름의 경로에 대한 정보가 포함된 트리 구조가 만들어지며, 컨스트럭트가 특정 패턴을 보이면 DDoS 공격으로 판단한다. 논문[11]은 공격 피해자 에지 라우터의 공격을 감지하고 경고 메시지를 인접 노드로 전송하는 능동적인 방어 기법을 제안하였다.

이 연구들은 주로 네트워크 구조를 이해하여 네트워크 트래픽이 공격자가 위치한 네트워크에서 피해자가 위치한 네트워크로 유입되는 과정에서 발생하는 공격 네트워크 트래픽의 결집 정도 및 유입 정도를 활용하여 DDoS를 탐지하는 알고리즘 또는 동적으로 자원 할당을 통해 협업 네트워크를 용이하게 하는 시스템을 제안하였다. 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 DoS 탐지를 위한 협력형 공격 탐지 모델 또한 연구되어 왔다.[2,7,12,13] 이 연구들은 소스측 네트워크에 공격 탐지 모듈을 위치시키고 결과를 공유함으로써 연결된 소스측 네트워크의 시너지 효과를 통해 거짓 경보 발생률을 크게 방지하였다. 하지만, 이러한 기법들은 공격 트래픽으로 오탐지 된 결과들이 정상적으로 탐지된 결과들과 함께 공유되기 때문에 최종적으로 공유하여 결과를 도출할 때 협력형 공격 탐지 모듈의 오탐율이 증가할 수 있다.

또한, 각 사이트별 탐지 성능의 차이에 따라 협력형 공격 탐지 기법의 성능이 영향을 받을 수 있다. 즉, 소스측 공격 탐지 기법에 따라 협력형 공격 탐지 기법의 성능이 영향을 받을 수 있다.

Ⅲ. 통계적 가중치를 고려한 협력형 소스측 DDoS 탐지 기법

시간대가 다른 소스측 네트워크에서는 시간대별 정상 트래픽 추세가 다르기 때문에, 서로 다른 시간대에 위치한 소스측 공격 탐지 모듈들의 성능은 각각 다를 수 있다. 제안된 협력형 공격 탐지 기법은 서로 다른 시간대에 위치한 소스측 공격 탐지 모듈들의 탐지된 결과와 탐지 결과 통계 가중치를 활용하여 최종 결과를 도출한다. 이때, i번째 소스측 공격 탐지 모듈의 시간 창 t_i에 대한 탐지 결과를 $d_i^{t_i}$이라 한다. 시간 창 t_i는 1분 간격으로 설정되며, 공격이 탐지될 경우 탐지 결과 $d_i^{t_i}$의 값은 1의 값을 가지고 공격이 탐지되지 않을 경우 0의 값을 가진다. 각 사이트 별 소스측 공격 탐지 모듈은 시간 창 t_i에 해당하는 탐지 결과 $d_i^{t_i}$와 탐지 결과에 대한 가중치 W_{t_i}를 협력형 공격 탐지 모듈에 공유한다. 협력형 탐지 모듈은 각 사이트 별 소스측 공격 탐지 모듈에서 공유된 탐지 결과 $d_i^{t_i}$와 탐지 결과에 대한 가중치 W_{t_i}를 이용하여 최종적으로 결과를 판단하기 위해 가중치 산술 평균 A^t을 사용한다. 사용된 수식은 아래와 같다.

$$A^t = \sum_{i=1}^{L} \frac{W_{t_i} * d_i^{t_i}}{W_{t_i}} \quad (5)$$

가중치 산술 평균값 A^t이 임의로 지정된 임계값 θ 보다 클 경우, 최종적으로 해당 시간 창 t에서 공격이 탐지되었다고 판단한다.

협력형 공격 탐지 모듈의 가중치 기법으로 EW(Equal Weight)와 SW(Statistical Weight)두가 방법을 제안한다.

EW는 서로 다른 시간대에 위치한 소스측 공격 탐지 모듈의 시간 창 t_i에 대한 탐지 결과 $d_i^{t_i}$에 대해 동등한 가중치를 부여하는 기법이다. 각 사이트 별 소스측 공격 탐지 모듈의 성능에 동등한 가중치를 부여하기 위해 W_{t_i}를 1로 설정한다. 이때, 최종적으로 결과를 판단하기 위해 가중치 산술 평균 A^t를 아래의 수식과 같이 수정한다.

$$A^t = \sum_{i=1}^{L} \frac{d_i^{t_i}}{L} \quad (6)$$

가중치 산술 평균값 A^t이 임의로 지정된 임계값 θ 보다 클 경우, 최종적으로 해당 시간 창 t에서 공격이 탐지되었다고 판단한다. 하지만, 이러한 기법은 서로 다른 시간대에 위치한 소스측 공격 탐지 모듈의 성능과 상관없이 결과들을 공유하기 때문에 최종적으로 결과를 도출할 때 협력형 공격 탐지 모듈의 오탐율이 증가할 수 있다. 따라서 최종적으로 결과를 도출할 때 소스측 공격 탐지 모듈의 성능을 고려하기 위해, 탐지 결과에 탐지된 결과 기반 통계 가중치를 부여하는 과정이 필요하다.

SW는 서로 다른 시간대에 위치한 소스측 공격 탐지 모듈에서 시간 창 t_i에 대해 통계적 가중치를 부여하는 기법이다. 가중치 W_{t_i}는 N일 동안 가상의 공격을 부여하였을 때 탐지 확률 D_{t_i}와 N일 동안 가상의 공격을 부여하지 않았을 때 오탐지 확률 F_{t_i}들의 비중을 달리하여 더한 값, 즉, 소스측 공격 탐지 모듈이 통계적으로 시간 창 t_i에 공격 트래픽과 정상트래픽을 정확하게 분류할 확률로 설정한다. 확률 D_{t_i}와 F_{t_i}에 대한 수식은 아래와 같다. 여기서 K는 일별 탐지 여부를 표현하기 위한 미지수이다.

$$D_{t_i} = F_{t_i} = \sum_{k=1}^{N} \frac{d_i^{t_i-(N-K)*1440}}{N} \quad (7)$$

최종적인 가중치 W_{t_i}를 계산하는 수식은 아래와 같다.

$$W_{t_i} = \alpha * D_{t_i} + (1-\alpha) * F_{t_i} \quad (8)$$

여기서 계수 α 는 D_{t_i}와 F_{t_i}의 비중을 나타내며 0과 1 사이의 일정한 값을 가진다. 계수 α값이 1에 가까울수록 임의의 시간 창 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 설정한다.

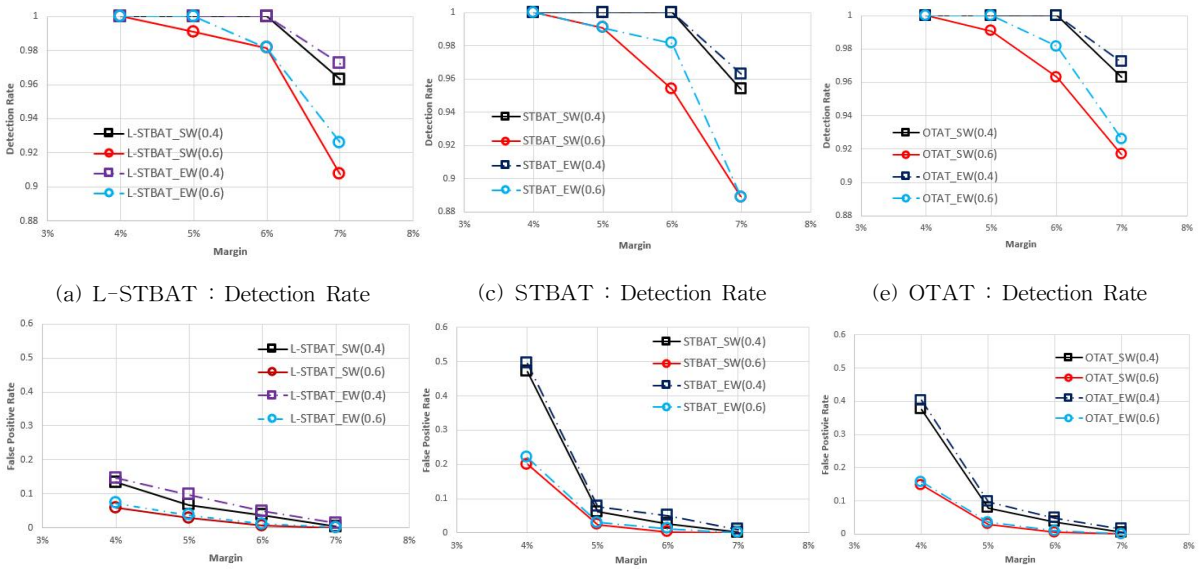
SW기법을 적용한 협력형 공격 탐지 모듈은 각 사이트 별 소스측 공격 탐지 모듈에서 시간 창 t_i에 대한 탐지 결과 $d_i^{t_i}$와 탐지된 결과에 대한 통계 가중치 W_{t_i}를 공유하고 최종적으로 가중치 산술 평균 A^t을 사용한다. 가중치 산술 평균값 A^t이 임의로 지정된 임계값 θ 보다 클 경우, 최종적으로 해당 시간 창 t에서 공격이 탐지되었다고 판단한다.

Ⅳ. 성능 평가 결과 및 분석

제안하는 협력형 공격 탐지 기법은 각 사이트에서 사용되는 개별 탐지 기법에 따라 협력형 공격 탐지 기법의 전체적인 성능이 변할 수 있다. 또한, 서로 다른 시간대에 위치한 소스측 공격 탐지 모듈의 개수에 따라 협력형 공격 탐지 모듈의 성능이 달라질 수 있다. 따라서, 이 논문에서는 제안하는 통계적 가중치를 이용한 협력형 소스측 DDoS공격 탐지 기법의 성능을 여러 가지 환경에서 평가한다.

1. 성능 평가 실험 환경

이 실험은 DNS-STAT: Hedgehos의 DNS 요청 트래픽을 사용하여 수행한다. 제안된 통계적 가중치를 이용한 협력형 공격 탐지 기법의 성능 평가를 위해 서로 다른 시간대에 위치하는 10개의 사이트에서 각각 39일간의 DNS 요청 트래픽을 수집하였다. 수집된 트래픽의 Outlier를 제거한 후, 해당 트래픽을 정상트래픽으로 정의한다.



(a) L-STBAT : Detection Rate (c) STBAT : Detection Rate (e) OTAT : Detection Rate

(b) L-STBAT : False Positive Rate (d) STBAT : False Positive Rate (f) OTAT : False Positive Rate

그림 1. 협력형 소스측 DDoS 공격 탐지 기법 성능 비교
Fig. 1. Performance Comparison of Collaborative Source-side DDoS Attack Detection Methods

서로 다른 시간대에 위치하는 소스측 공격 탐지 모듈의 적응형 임계값이 트래픽 계절성을 인식하게 만들기 위해, 각 사이트당 2018년 첫 30일에 해당하는 DNS 쿼리 트래픽을 사용한다. 이 트래픽 계절성 인식을 위한 데이터는 STBAT 모델에서 사용하는 통계적 방법에 적용되고, L-STBAT 모델에서 사용하는 LSTM 모듈 학습에 사용된다. LSTM 모듈의 경우, Gradient descent optimization 알고리즘과 100 사이즈의 배치를 사용하고 1000회의 학습 시간을 반복한다.

서로 다른 시간대에 위치하는 10개의 사이트에서 매분마다 캡처된 트래픽 샘플의 탐지와 오탐지를 측정하기 위해, 각 도시별로 2018년 8일에 해당하는 DNS 쿼리 트래픽을 사용한다. 이와 같이 매분마다 캡처된 트래픽의 마지막 1일에 해당하는 기간이 추가되었으며, 서비스 공격 트래픽은 서로 다른 시간대의 시간 창에서 동시에 발생하도록 하였다.

2. 성능 평가 결과 및 분석

우리는 서로 다른 시간대에 위치하는 소스측 공격 탐지 모듈의 성능과 상관없이 현재 탐지된 결과에 동등한 가중치를 부여하는 EW기법과 해당 시간대에 탐지되었던 결과들과 오탐지 되었던 결과들에 대한 통계 가중치를 탐지된 결과에 부여하는 SW기법을 비교한다. 이때, 각 소스측 공격 탐지 기법으로 L-STBAT, STBAT, OTAT를 사용한다. 각 소스측 공격 탐지 기법의 임계값에 영향을 주는 마진은 4%~7%까지 적용하고, 협력형 공격 탐지 모듈의 임계값은 0.1씩 변화시키면서 테스트한다. 각 소스측 공격 탐지 모듈의 마진 별 EW기법과 SW기법의 공격탐지율과 공격오탐율를 측정한다.

그림 1은 각 사이트별 탐지 기법과 마진의 변화에 따른 협력형 소스측 DDoS공격 탐지 기법에 대한 성능을 나타낸다. 이때, 공격탐지율 (Detection Rate)는 각 소스측 공격 탐지 모듈에서 사용하는 탐지 기법에 따라 결과와 가중치를 공유하여 최종적으로 결과를 도출하였을 때 전체 공격 수 중 탐지된 공격 횟수를 뜻한다. 또한, 공격오탐율(False Positive Rate)는 각 소스측 공격 탐지 모듈의 결과와 가중치를 공유하여 최종적으로 결과를 도출하였을 때 정상 트래픽 수 중 공격으로 오 탐지된 공격 수를 뜻한다.

그림 1에서 협력형 공격 탐지 기법을 사용할 때, 개별 사이트별로 소스측 공격 탐지 모듈의 성능을 고려하여 가중치를 부여한 SW기법이 EW기법에 비해 전반적으로 우수한 성능을 보임을 확인하였다. 세가지 소스측 공격 탐지 기법 L-STBAT, STBAT, OTAT 모든 경우에 대해, SW기법의 공격탐지율은

EW의 공격탐지율과 비슷하다. 그리고 SW기법의 공격오탐율은 EW기법의 공격오탐율에 비해 전반적으로 2%정도 낮다.

각 소스측 공격 탐지 기법에 따른 협력형 공격 탐지 기법들의 공격탐지율과 공격오탐율을 좀 더 자세히 분석하였다. L-STBAT 기법이 사용되는 경우, SW기법은 임계값이 0.4일 경우 마진 6%에서 높은 공격탐지율을 유지하면서 약 4%의 공격오탐율을 보여주고, EW기법은 임계값이 0.6일 경우 마진 5%에서 높은 공격탐지율을 유지하면서 약 4%의 공격오탐율을 보여준다. STBAT 기법이 사용되는 경우, SW기법은 임계값이 0.4일 경우 마진 6%에서 높은 공격탐지율을 유지하면서 약 3%의 공격오탐율을 보여주고, EW기법은 임계값이 0.4일 경우 마진 6%에서 높은 공격탐지율을 유지하면서 약 5%의 공격오탐율을 보여준다. OTAT 기법이 사용되는 경우, SW기법은 임계값이 0.4일 경우 마진 6%에서 높은 공격탐지율을 유지하면서 약 3%의 공격오탐율을 보여주고, EW기법은 임계값이 0.4일 경우 마진 6%에서 높은 공격탐지율을 유지하면서 약 5%의 공격오탐율을 보여준다. 즉, 모든 기법에 대해서 SW기반 협력형 소스측 공격 탐지 기법이 높은 공격탐지율과 낮은 공격오탐율을 달성할 수 있음을 확인하였다.

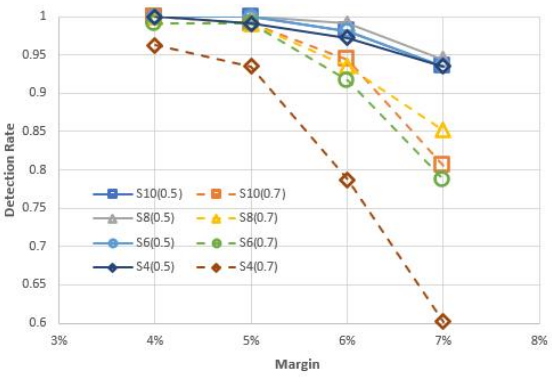
그림 2는 서로 다른 시간대에 위치한 소스측 공격 탐지 사이트의 수에 따른 통계적 가중치 기반 협력형 공격 탐지 기법의 성능평가 결과를 나타낸다. 이때, 각 사이트에서는 L-STBAT를 사용하고 협력형 공격 탐지 기법은 SW 가중치 기법을 사용한다고 가정한다. 그림 2의 SN(M)은 N개의 사이트에서 협력형 탐지 기법이 M의 임계값을 사용하는 것을 의미한다. 예를 들어 S10(0.5)는 10개의 사이트에서 0.5 임계값을 이용해 협력형 공격 탐지를 수행하는 것을 의미한다.

그림 2에서 서로 다른 시간대에 위치한 소스측 공격 탐지 모듈의 수가 많아질수록, 공격탐지율이 높아지고 공격오탐율이 낮아지는 것을 확인할 수 있다. 특히, 모듈의 수의 증가는 공격오탐율 감소에 큰 효과를 보이는 것으로 확인되었다. 그리고 높은 임계값을 사용할수록, 보다 보수적으로 공격 탐지 결과를 도출하는 것을 확인 할 수 있었다.

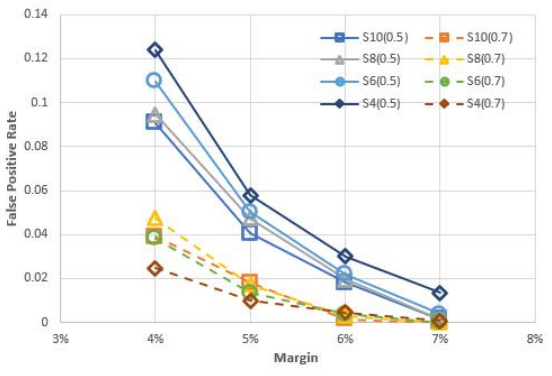
V. 결 론

이 논문에서는 개별 소스측 공격 탐지 성능의 통계적 가중치를 부여하고, 이를 공유하여 최종적으로 공격 유무를 판단하는 통계적 가중치를 고려하는 협력형 소스측 DDoS 공격 탐지 기법을 제안하였다. 실제 네트워크 트래픽을 사용한 성능평가 결과, 각 사이트별 탐지결과에 동등한 가중치를 부여하는 협력형 공격 탐지 기법에 비해 제안된 통계적 가중치 기반 협력형 공격 탐지 기법은 높은 탐지율을 유지하지면서 약 2% 더 낮은 공격오탐율을 달성함을 확인하였다. 특히, L-STBAT을 개별 소스측 공격 탐지 기법으로 사용할 경우, 협력형 공격 탐지 기법을 보다 효과적으로 사용할 수 있음을 확인하였다. 또한, 협력적 공격 탐지 모듈의 수가 많아질수록 탐지 기법의 성능이 향상되는 것을 확인하였다.

향후, 소스측 네트워크의 특징, 개별 공격 탐지 기법의 종류와 시간대별 성능에 따라 탐지 결과를 분석할 수 있는 협력형 탐지 기법을 연구하고자 한다.



(a) Detection Rate



(b) False Positive Rate

그림 2. 사이트 수에 따른 협력형 공격 탐지 기법 성능
Fig. 2. Performance of Collaborative Source-side DDoS Attack Detection Method by Number of Sites

References

[1] Yeom, Sungwoong, et. al. “Assessing Convolutional Neural Network based Malicious Network Traffic Detection Methods.” KNOM Review, vol.22, no.1, pp.20-29, 2019

[2] Choi, Jintae, et. al. “Assessing the impact of DoS Attack on SDN based IoT Gateway.” KNOM Review, vol.20, no.1, pp.24-33, 2017

[3] Nguyen, Sinh-Ngoc, et al. ″Source-Side Detection of DRDoS Attack Request with Traffic-Aware Adaptive Threshold.″ IEICE Transactions on Information and Systems, vol.E101-D, no.6, pp.1686-1690, 2018.

[4] Nguyen, Giang-Truong, et al. ″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.

[5] Ramakrishnan, Nipun, and Tarun Soni. ″Network traffic prediction using recurrent neural networks.″ 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA), pp.187-193, 2018.

[6] Nguyen, Giang-Truong, et al. ″LSTM based Network Traffic Volume Prediction.″ 2018 KIPS Spring Conference, pp.362-364, 2018

[7] Sungwoong Yeom, Kyungbaek Kim. ″A Study on Collaborative Source-Side DoS Attack Detection.″ 2019 KICS Summer Conference, pp.478-479, 2019

[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). pp. 401-410, 2006.

[9] Chen, Yu, et al., ″Collaborative detection of DDoS attacks over multiple network domains.″ IEEE Transactions on Parallel and Distributed Systems, vol.18, no.12, pp.1649-1662, 2007.

[10] Shalinie, S. Mercy, et al. ″CoDe—An collaborative detection algorithm for DDoS attacks.″ 2011 International Conference on Recent Trends in Information Technology (ICRTIT), pp.113-118, 2011.

[11] Tariq, Usman, et al. ″Collaborative peer to peer defense mechanism for ddos attacks.″ Procedia Computer Science, vol.5, pp.157-164, 2011.

[12] Song, ByungHak, et al., “Collaborative Defense Mechanism Using Statistical Detection Method against DDoS Attacks.” IEICE Transactions on Communications, vol.E90-B, no.10, pp. 2655-2664, 2007.

[13] Gamer, Thomas. ″Collaborative anomaly-based detection of large-scale internet attacks.″ Computer Networks, vol.56, no.1, pp.169-185, 2012.

[14] Abou El Houda, et. al., ″Co-IoT: A Collaborative DDoS Mitigation Scheme in IoT Environment Based on Blockchain Using SDN.″ 2019 IEEE Global Communications Conference (GLOBECOM), pp.1-6, 2019.

[15] Kim, Young-pin, etl. al. “DDoS Detection System Based on Multiple Machine Learning Combination for Software Defined Networking.” The Journal of Korean Institute of Communications and Information Sciences, vol.42, no.8, pp.1581-1590, 2017

염 성 웅 (Yeom Sungwoong)

2019년 2월 : 전남대학교 전자컴퓨터공학과 학사 졸업

2019년 3월~현재 전남대학교 전자컴퓨터공학과 석사과정

<관심 분야> 네트워크, 빅데이터, 데이터 스트리밍

김 경 백 (Kim Kyungbaek)

1999년 : 한국과학기술원 전기 및 전자공학과 학사 졸업

2001년 : 한국과학기술원 전기 및 전자공학과 석사 졸업

2007년 : 한국과학기술원 전기 및 전자공학과 박사 졸업

2007년~2011년 : University of California Irvine, 박사 후 연구원

2012년~ 현재 : 전남대학교 전자컴퓨터공학부 교수

<관심분야> 분산시스템, 소프트웨어 정의 인프라스트럭쳐, 빅데이터 플랫폼, 소셜 네트워킹 시스템, 블락체인, AI기반 CPS