STDP 를 이용한 DDoS 공격 패킷 분석

허정윤, 임재한*
광운대학교, *광운대학교

jylemon1128@kw.ac.kr, *ljhar@kw.ac.kr

DDoS attack packet analysis using STDP

Jeong-Yun Heo, Jae-Han Lim*
Kwangwoon Univ., * Kwangwoon Univ.

요 약

IoT 와 모바일 기기가 대중화되고 있다. 그러나 소형화가 함께 이루어지면서 할당할 수 있는 자원이 적어 외부 공격에 취약함을 보인다. 이를 보완하기 위해 ANN 이나 CNN 같은 뉴로모픽 인공지능이 사용되고 있으나 높은 연산량으로 인하여 IoT 및 모바일 기기에서 모델을 사용하는 것이 아니라 클라우드 기반 탐지방법을 사용한다. 그러나 이는 서버와의 연결이 끊기거나 서버에 공격이 들어오면 클라이언트가 보안에 취약해짐을 보인다. 그래서 본 논문에서는 IoT 및 모바일 기기처럼 제한된 환경에서 강점을 가지는 SNN 의 STDP 모델을 이용하여 DDoS 공격을 검출하는 실험을 진행하였다. 총 5 가지의 공격에 대해 실험을 진행하였으며 모두 90%이상의 검출 능력을 보여주었으며 TFTP 와 DrDoS UDP 는 99%이상의 검출 능력을 보인다.

I. 서 론

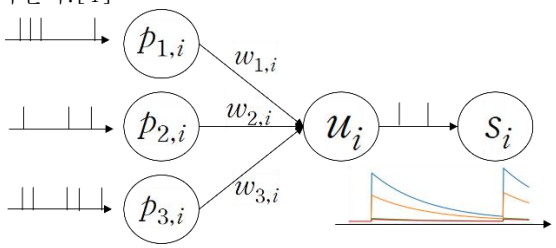
IoT 기술이 발달하고 관련 기기들이 대중들에게 급속도로 퍼지고 있다. 그러나 대부분의 IoT 기기들이 사용자의 편의를 위하여 소형화 되어 있고 이는 기기의 보안을 위해 할당할 수 있는 자원이 적음을 의미한다.[1] 특히 가장 일반적인 네트워크 공격방식인 분산 네트워크 서비스 공격(Distributed DoS attack)에도 IoT 기기들은 무척이나 취약함을 보인다.[2] 이러한 부족한 보안성을 채우기 위해서 Artificial Neural Network (ANN)과 Convolution Neural Networks (CNN)을 이용한 딥러닝 기반 패킷 분석 등을 통한 공격 감지에 대한 연구가 활발하게 이루어지고 있다.[3] 그러나 이는 클라우드 기반 탐지기법에 치중된 경향이 있다. ANN 이나 CNN 은 상당한 연산량과 높은 전력을 사용하여 초소형-모바일 기기에는 적합하지 않다. 그래서 모바일 기기나 초소형 IoT 기기(클라이언트)에서 데이터를 수집하고 서버로 데이터를 전송하여 분석한다. 그후 서버가 연산결과를 클라이언트로 전달한다. 그러나 이 방식은 통신시간이 소요되어 실시간 분석이 필요한 DDoS Detection 에 적합하지 않다. 또한 데이터베이스가 있는 클라우드 서버가 공격을 받거나 네트워크 이상이 생긴다면 클라이언트에 가해진 공격을 분석하지 못한다. 이를 보완하기 위해서 서버와의 통신없이 초소형-모바일 기기 자체에서 실시간 분석이 가능한 패킷 탐지 시스템을 운영할 필요가 있다.

따라서 본 논문에서는 IOT 기반 초소형 모바일 기기에서 SNN 을 적용한 DDoS 탐지 방법을 제안한다. SNN 은 전력소모를 최소화할 수 있어서 IOT 기반 초소형 모바일 기기와 같이 제한적인 환경에서 강점을 가진다. 또한 본 논문의 탐지 방법에서 사용한 STDP 학습 규칙은 빠른 학습 속도를 가지고 있어 실시간으로 수신되는 패킷들을 탐지하는데 유리하다.

II. 배경 지식

2.1 Spiking Neural Network

SNN 은 스파이킹 뉴런(Spiking Neuron)과 시냅스(Synapse)로 이루어져 있다. 스파이킹 뉴런의 막전위는 인풋 스파이크가 입력될 때마다 가중치에 비례하여 증가한다.[4]



[그림 1] SNN 의 작동 구조

[그림 1]과 같이 설정된 막전위 값에 도달하면 아웃풋 스파이크를 출력하여 다음 뉴런으로 전달한다. 그후 휴지 전위에 들어가서 일정 기간 동안은 인풋 스파이크가 들어와도 막전위를 올리지 않는다. 이를 설계된 계층(Layer)만큼 반복한다.

2.2 Spike-Timing-Dependent Plasticity

STDP 는 시냅스 전 뉴런에서 발생한 스파이크와 시냅스 후 뉴런에서 발생된 스파이크 간의 시간간격에 따라 시냅스의 가중치를 조절하는 SNN 학습방법이다. 가중치의 강화 및 약화는 Long-Term Potentiation (LTP)와 Long-Term Depression (LTD)를 사용한다. 시냅스 전 뉴런이 발화한 후 시냅스 후 뉴런이 발화하면 LTP 가 발생한다. 반면 시냅스 후 뉴런이 발화하고 시냅스 전 뉴런이 발화하면 LTD 가 발생한다. 따라서 STDP 는 신호를 스파이크의 세기가 아닌 발생 시각으로 구분한다. 이러한 특징으로 STDP 는 빠른 학습속도를 가진다.

2.3 Distributed DoS Attack

DDoS 공격은 가용성을 악화시키는 공격 방식이다. 크게 시스템의 취약점 및 약점을 공격하는 방법, 피해자가 가용할 수 있는 자원을 소모시키는 방법, 피해자가 가용할 수 있는 대역폭을 소모시키는 방법이 있다. OSI 7 계층으로 DDoS 공격을 분류하면 대표적으로 L7(응용) 공격으로는 HTTP Get Flooding, SQL 이 있고 L4(TCP, UDP) 공격으로는 TCP SYN, UDP Flooding 이 있으며 L3(IP, ARP, ICMP) 공격으로는 ARP Spoofing, ICMP Flooding 이 있다.[5]

III. 실험 결과

3.1 Dataset

DDoS Dataset(CIC-DDoS2019)는 실제 패킷 데이터를 time stamp, destination IP, source, ports, protocols 등과 함께 CICFlowMeter-V3 로 가공한 데이터들을 85 개의 feature 를 통하여 csv 파일로 제공한다. DDoS 공격을 MSSQL. DNS, UDP Flood 등 13 개의 공격과 Benign 으로 분류하여서 label 을 제공한다. [6]

3.2 BindsNET

BindsNET 은 SNN 시뮬레이션을 위해 개발된 파이썬 패키지이다. 기존의 소프트웨어 framework 는 광범위한 뉴럴 기능들을 지원하지만 기계학습 문제를 해결하는 데에는 적합하지 않다.[7] 그래서 본 실험에서는 추가적인 작업 없이 CPU 나 GPU 가속 계산을 할 수 있으며, SNN 시뮬레이션을 지원하는 모듈 및 메소드를 제공하여 BindsNET 을 사용하였다.

3.3 학습 모델 설계

우선, CIC-DDoS2019 에서 제공하는 feature 중에서 flow ID, source IP, source port, destination IP, destination port, protocol, similar HTTP 와 같이 가공하기 어렵고 flow bytes/s, flow packets/s 과 같이 중복된 의미를 가지고 있는 feature 를 제외하였다.

실험의 원활한 피드백을 위해 attack dataset 과 따로 추출한 normal dataset 에서 랜덤으로 50,500 개를 추출하여 dataset 을 제작한다. 76 개의 feature 각각이 가지는 값의 범위는 매우 달라서, 실험의 용의성을 위해 Min-Max scaler 로 normalization 하였다. 제작한 dataset 에서 attack 과 normal 를 train dataset 에서는 각각 500 개씩, test dataset 에서는 각각 50,000 씩 랜덤 추출하여 실험을 진행하였다.

이후 최적화를 위해 실험 결과를 분석하면서 영향력을 행사하지 못하는 feature 를 제외하였다. 최종적으로 fwd PSH flags, packet length mean, packet length std, packet length variance, fwd packets/s 을 비롯한 11 개의 feature 로 최적화를 하였다.

3.4 결과

본 논문에서는 Proportion Weighting Accuracy (Accuracy), Probability of Detection(PD), False Negative probability(FN), False Positive probability (FP)로 성능을 확인하였다. Accuracy 는 뉴런별로 지정된 스파이크가 튄 개수를 측정한고 스파이크 개수가 가장 많은 label 을 정답으로 지정한다. PD 는 attack 을 막은 정도, FN 은 attack 을 normal 로 잘못 구분한 정도, FP 는 normal 을 attack 으로 잘못 구분한 정도이다.

Syn Flood, DrDos UDP, TFTP, UDP Lag, DrDos DNS 총 5 개의 공격에 대하여 분석을 하였다.

Attack	Accuracy	PD	FN	FP
SYN Flood	91.24	0.9999	0.0001	0.1750
DrDoS UDP	99.84	99.84	0.9977	0.0023
TFTP	99.58	0.9996	0.0004	0.0000
UDP Lag	92.93	0.8657	0.1343	0.0071.
DrDoS DNS	97.66	0.9995	0.0005	0.0464

[표 1] Attack 방식별 탐지 정확도

[표 1]을 보면 설계한 STDP 가 매우 높은 성능을 보임을 확인하였다. DrDoS UDP 와 TFTP 는 99% 이상의 정확도를 보이며 타 공격방식 또한 90% 이상의 감지효과를 보인다.

IV. 결론

본 논문에서는 SNN 을 기반으로 DDoS 패킷의 탐지를 하기위해 CIC-DDoS2019 을 사용하였다. 위에서 획득한 87 개의 feature 를 실험 결과를 통해 11 개의 feature 로 최적화하였다. Syn Flood, DrDoS UDP, TFTP, UDP Lag, DrDoS DNS 총 5 개의 공격에 대한 감지 실험을 진행하였으며 90%이상의 높은 감지 능력을 보였다. Hyper parameter 를 일괄적으로 적용한 점을 고려하였을 때 미세 조정을 거친다면 DrDoS UDP 와 TFTP 와 같이 99%이상의 감지 정확도를 보일 거라 기대된다.

ACKNOWLEDGMENT

본 연구는 한국연구재단 신소자원천기술개발사업 (grant no. NRF-2021M3F3A2A01037962)의 지원을 받아 수행된 연구입니다.

참 고 문 헌

[1] Dong-hee Kang, Jae-Deok Lim. (2022). “Network Security Protocol Performance Analysis in IoT Environment.” Journal of the Korea Institute of Information Security & Cryptology, 32(5):955-963.

[2] Young-Taek Oh, In-June Jo. (2021). "Data Modeling for Cyber Security of IoT in Artificial Intelligence Technology." Journal of the Korea Contents Association, 21(12):57-65.

[3] Siddiqui S, Nesbitt R, Shakir MZ, Khan AA, Khan AA, Khan KK, Ramzan N. (2020). "Artificial Neural Network (ANN) Enabled Internet of Things (IoT) Architecture for Music Therapy" Electronics, 9(12):2019.

[4] D.V. Buonomano, T.P. Carvalho. (2009). "Spike-Timing-Dependent Plasticity (STDP)" Editor(s): Larry R. Squire, Encyclopedia of Neuroscience, Academic Press, pp. 265-268.

[5] Yong-Hee Jeon, Jong-Soo Jang, Jin-Tae Oh. (2009). "DDoS 공격 및 대응 기법 분류." Review of KIISC, 19(3):46-57.

[6] I. Sharafaldin, A. H. Lashkari, S. Hakak and A. A. Ghorbani. (2019). "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy" International Carnahan Conference on Security Technology (ICCST), Chennai, India, pp. 1-8.

[7] Hazan H, Saunders DJ, Khan H,Patel D, Sanghavi DT, Siegelmann HT and Kozma R. (2018). "BindsNET: A Machine Learning-Oriented Spiking Neural Networks Library in Python." Frontiers in Neuroinformatics, 12:89, DOI=10.3389/fninf.2018.00089.