한국정보전자통신기술학회논문지(jkiiect)'20-12, Vol.13 No.6
논문 20-13-06-605 http://dx.doi.org/10.17661/jkiiect.2020.13.6.605

소프트웨어-정의 네트워크에서 CNN 모델을 이용한 DDoS 공격 탐지 기술

고광만*

A DDoS Attack Detection Technique through CNN Model in Software Define Network

Kwang-Man Ko*

요 약 소프트웨어 정의 네트워크가 확장성, 유연성, 네트워크상 프로그래밍이 가능한 특징으로 네트워크 관리에서 표준으로 자리잡아 가고 있지만 많은 장점에도 불구하고 하나의 컨트롤러에 대한 사이버 공격이 전체 네트워크를 영향을 주는 문제점을 가지고 있다. 특히, 컨트롤러에 대한 DDoS 공격이 대표적인 사례로서 다양한 공격 탐지 기술에 대한 연구가 진행되고 있다. 본 논문에서는 최초로 84개 DDoS 공격 Feature 데이터셋을 Kaggle에서 획득한 후 Permutation Feature Importance 알고리즘을 이용하여 상위 20의 중요도를 갖는 Feature를 선택하여 딥 러닝 기반의 CNN 모델에서 학습과 검증을 수행하였다. 이를 통해, 최적의 공격 탐지율을 갖는 상위 13개의 DDoS Feature 선택이 DDoS 공격 탐지율 96%을 유지하면서 적정한 공격 탐지 시간, 정확성 등에서 매우 우수한 결과를 제시하였다.

Abstract Software Defined Networking (SDN) is setting the standard for the management of networks due to its scalability, flexibility and functionality to program the network. The Distributed Denial of Service (DDoS) attack is most widely used to attack the SDN controller to bring down the network. Different methodologies have been utilized to detect DDoS attack previously. In this paper, first the dataset is obtained by Kaggle with 84 features, and then according to the rank, the 20 highest rank features are selected using Permutation Importance Algorithm. Then, the datasets are trained and tested with Convolution Neural Network (CNN) classifier model by utilizing deep learning techniques. Our proposed solution has achieved the best results, which will allow the critical systems which need more security to adopt and take full advantage of the SDN paradigm without compromising their security.

Key Words : CNN, Deep Learning, DDoS Attack, Permutation Importance Algorithm, Software Defined Network

1. 서론

최근 확장성과 유연성이 우수한 SDN(Software Defined Network) 기반 네트워크 서비스로 빠르게 전환중이다[1]. SDN은 트래픽 전송을 수행하는 컨트롤 플레인과 트래픽 경로를 지정하는 데이터 플레인으로 분리하고 개방형 API인 OpenFlow 프로토콜을 통해 네트워크 트래픽 전달을 소프트웨어 기반 콘트롤러에서 제어하는 특징을 가지고 있다. 하지만, SDN에서 DDoS 공격의 효과는 매우 신속하고 전체 네트워크 서비스에 중요한 피해를 유발하므로 공격 탐지 및 완화와 같은 보안 문제가 지속적인 연구 주제로 제기되고 있다[2]. 특히, SDN이 네트워크 통제에 있어서 단일 컨트롤러에 집중되어 있기 때문에 이 지점에 대한 공

This Paper was supported by research Fund of Sang-Ji University in 2018.
Department of Computer Engineering, Sang-Ji University
Received December 02, 2020 Revised December 13, 2020 Accepted December 26, 2020

격 또는 비정상적 작동은 전체 네트워크에 막대한 영향을 끼친다. 최근에는 SDN 컨트롤러에서 DDoS 공격을 방어하기 위해 머신 러닝 기반으로 패킷 검사 등을 통한 공격 감지 및 완화 연구가 진행되었다.

본 논문에서는 딥 러닝 기반으로 DDoS 공격 방어(탐지 및 완화)하기 위해 첫째, Kaggle에서 획득한 84개의 DDoS 공격 Feature 데이터 셋으로부터 의미있는 64개의 Feature와 Permutation Importance(PFI)을 통해 상위 20개의 Feature를 선택하였다. 둘째, 64개와 20 Feature 선택을 Mininet 시뮬레이터의 SDN 토폴리지의 RYU 컨트로내에 컨볼로션 신경망 네트워크(CNN) 분류기 모델에서 실험한 최적의 13개의 Feature에 대한 평가 결과를 제시하였다.

2. 관련연구

시간 특성 기반 기술에서는 시간 특성을 DDoS 공격을 탐지하는 중요한 요소로 활용하여 Nugraha, M., Paramita[3] 연구에서 패킷 특성과 흐름 시간을 기반으로 통계적 방법을 제안한 후 sFlow[4]를 사용하여 시간 흐름을 수집하고 임계값을 적용하여 DDoS 패킷을 인식하였다. Dharma, N.G.[5] 연구에서는 공격 탐지를 위해 지속 시간을 사용하여 발생될 수 있는 공격을 방어하기 위해 시간 패턴을 사용하였다. Huseyin Polat[6]과 Ye, J.[7] 연구에서는 전통적인 네트워크에서 엔트로피 기반 DDoS 탐지를 위해 일정한 크기의 윈도우를 지정하고 임의의 시간동안 엔트로피를 이용하여 측정하였으며 초기단계에서 DDoS 공격을 탐지할 수 있는 특징을 가지고 있다.

머신 러닝 기반 SDN에 대한 DDoS 공격 탐지 연구는 Braga, R.[8]에서 선행되었다. SOM을 기반으로 일정 시간 동안 OpenFlow 스위치의 플로우 항목에서 패킷 정보를 추출하기 위해 네트워크에 NOX 등록 스위치를 설정하여 사용하였다. 이러한 머신 러닝 기반의 플로우 통계 정보는 SOM 분류기 모듈을 통해 악의적인 트래픽과 정상적인 트래픽을 판별하는데 적용하였다.

엔트로피 기반 DDos 공격 탐지 연구는 Wang R.[9]에서 진행되었으며 공격 탐지 스키마는 소스 포트, 착신 포트, 소스 IP, 착신 IP의 4개 요소에 근거하고 있다. Mousavi S.M.[10] 연구에서도 DDoS 공격 탐지를 위해 엔트로피 기반으로 무작위성을 활용하여 특정 호스트로 가는 수신 패킷의 수를 계산한 후, 이를 기준값과 비교한다. 이 연구에서는 수신되는 패킷을 측정하는 무작위성을 활용하였으며 무작위성을 측정하는 좋은 방법으로서 엔트로피를 활용하였다. 엔트로피는 총 이벤트 수에 대해 하나의 이벤트가 발생할

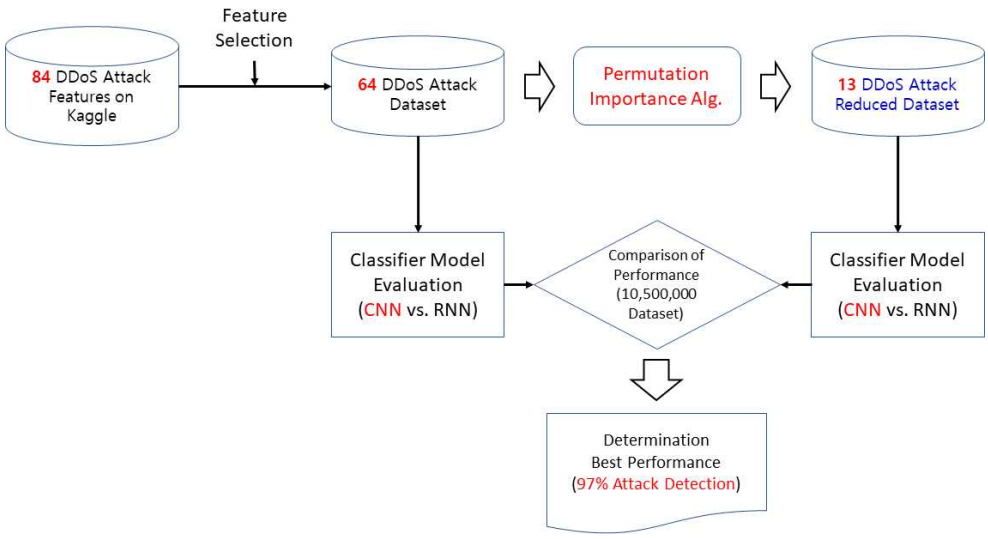

그림 1. CNN Future 선택을 이용한 DDoS 탐지 시스템 개요
Fig. 1. Overview of DDoS Detection System using CNN Future Selection

표 1. PFI를 이용한 13 Feature 선택
Table 1. 13 Feature Selection using 13 PFI

#	Feature	Importance	Description
1	fl_iat_avg	0.5334	Average time between two flows
2	fw_iat_max	0.3351	Maximum time between two packets sent in the forward direction
3	fw_win_byt	0.3248	Number of bytes sent in initial window in the forward direction
4	fw_iat_tot	0.3231	Total time between two packets sent in the forward direction
5	fl_dur	0.3162	Flow duration
6	fl_iat_min	0.2778	Minimum time between two flows
7	bw_iat_min	0.2655	Minimum time between two packets sent in the backward direction
8	fl_iat_max	0.2426	Maximum time between two flows
9	fw_iat_avg	0.2203	Mean time between two packets sent in the forward direction
10	Bw_pkt_l_max	0.2139	Maximum size of packet in backward direction
11	bw_iat_max	0.2077	Maximum time between two packets sent in the backward direction
12	bw_win_byt	0.1944	Number of bytes sent in initial window in the backward direction
13	bw_iat_tot	0.1942	Total time between two packets sent in the backward direction

확률을 도출하며 무작위성이 감소하면 엔트로피가 감소한다는 것을 의미하고 있다. 또한 Kim[11] 연구에서도 시간 속성을 이용한 엔트로피 기반의 유사연구 선행되었다.

3. CNN 기반 DDoS 공격 탐지

3.1 DDoS 공격 탐지 모델 및 방법

이 논문은 SDN에서 DDoS 공격을 탐지하기 위해 첫째, Kaggle에서 수집된 84개의 DDoS 공격 패턴중 의미있는 64개의 유형에 대해 PFI 알고리즘을 활용하여 가장 의미있는 13개의 Feature를 선택했다. 둘째로, 64개의 공격과 13개의 특징을 가진 10,500,000개의 데이터셋에 대해 러닝 기반 CNN 모델에 적용하여 97% 이상의 공격 탐지 적중률을 보장하면서 공격 탐지 시간 우수성을 갖는 결과를 그림 1과 같은 과정을 통해 제시하였다.

기존 연구에서는 머신 러닝 기반 네트워크 침입 탐지 시스템에서 Random Forest 알고리즘을 적용하여 DDoS 공격을 탐지하는 연구 진행되었지만 본 논문에서는 딥 러닝 기반에서 지도 및 비지도 학습이 가능한 CNN 분류기 모델을 적용하였다.

3.2 PFI 알고리즘을 통한 Feature 선택

PFI 알고리즘의 중요한 특징은 재학습 과정없이특정 Feature를 제거하고 중요도를 파악하는 것이다. Feature 값들을 무작위로 섞어서 Feature에 대한 노이즈를 만들어 목표 변수와 연결 고리를 제거하는 방법이며 예측값이 실제 값보다 얼마나 차이가 더 생겼는지를 통해 해당 Feature의 영향력을 파악할 수 있다. 학습한 모델과 데이터만 있으면 변수 중요도를 뽑아주는 방법이기 때문에, 모델의 학습 과정, 내부 구조에 대한 정보가 필요 없어서 어느 모델이든 적용할 수 있는 장점을 가지고 있다. 오버헤드를 줄이기 위해 PI 알고리즘을 통해 DDoS 공격 탐지율 96% 이상을 감지하면서 네트워크 지연을 감소시킬 수 있는 13개의 패턴을 반복적인 실험을 통해 표1과 같이 획득하였다. 즉, 64개의 공격 패턴을 적용했을 경우와 같은 공격 탐지율을 유지하면서 공격 탐지 시간을 현저히 줄일 수 있는 최적을 Feature를 중요도에 따라 결정하였다. 최소 Future 선택을 거친 64개의 DDoS 공격 패턴보다 PFI를 통해 선택된 13개의 DDoS 공격 패턴의 효율성 검증을 위해 딥 러닝 기반 CNN 모델에 적용하여 실행 시간, 정밀도, 재현율 등을 3.3절의 실험을 통해 입증하였다.

본 논문에서 DDoS 공격 탐지 시스템의 실험 검증

을 위해 Mininet 시뮬레이터상에서 그림 2와 같은 SDN 토폴로지를 구성하였다. SDN 토폴로지는 6대의 PC, OpenFlow 스위치, RYU SDN 컨트롤러로 구성되어 있다.

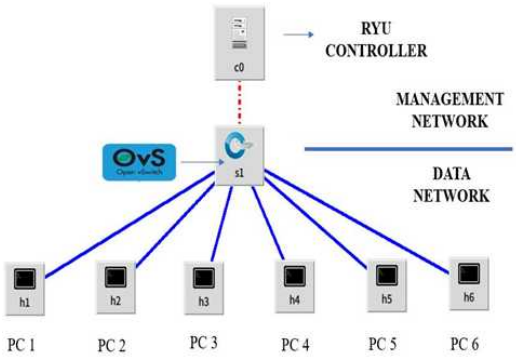

그림 2. DDoS 탐지 시스템을 위한 네트워크 토폴로지
Fig. 2. Network Topology for DDoS Detection System

6대의 PC중 1대의 PC는 DDoS 공격자이며 나머지는 정상적인 네트워크 흐름을 유지하도록 했다. DDoS 공격자 PC를 탐지하게 위해 RYU 컨트롤러에 딥 러닝 기반 CNN 분류기 모델을 구현하였다. 이러한 토폴로지의 설정은 기존 머신 러닝 기반의 DDoS 공격 탐지를 위한 설정과 동일하게 구성한 후 적용하였다. Mininet은 가상 네트워크 환경을 설정하는 에뮬레이터로서 본 논문의 실험 환경 구성을 위해 파이썬 기반의 RYU SDN 컨트롤러 기능, OpenFlow 프로토콜 지원을 활용할 수 있다.

표 2. 실험 환경
Table 2. Experimental Environment

Operating System	Ubuntu (18.10)
Simulator	Mininet (2.3)
Network Switch	RYU (4.3) controller
Hardware	2G RAM / 20G SSD

실험을 통해 공격 탐지 평가 시간(Evaluation time), 정확도(Accuracy), 재현율(Sensitivity), 정밀도(Precision), 특이도(Specificity), F1_Score 값을 측정하였다. 재현율은 DDoS 공격으로 예측한 집단에서 실제로 DDoS 공격으로 탐지하는 비율로서 100%에 근접해야 적중률이 높다고 판정한다. 특이도는 정상적인 네트워크 흐름으로 예측한 집단중 실제로 정상적인 네트워크 흐름으로 탐지하는 비율로서 100%에 근접해야 정확도가 높다고 판정한다. 정밀도는 실험에 적용된 모든 데이터셋에 대해 DDoS 공격으로 예측한 네트워크 흐름을 실제로 DDoS 공격으로 판정되는 비율을 의미한다. 마지막으로 F1_Score를 통해서 재현율과 정밀도의 안정적인 평균값을 구해 지나치게 DDoS 공격 또는 정상적인 네트워크 흐름에 데이터 셋이 치우치는 정도를 방지하게 위해 평가한다.

표 3. 실험 평가 지표
Table 3. Experimental Evaluation Index

Pred. / Exp.	DDoS (1)	Normal (0)	
DDoS (1)	True Positive	False Negative	Sensitivity
Normal (0)	False Positive	True Negative	Specificity
	Precision		

첫 번째 실험은 PFI 알고리즘을 이용한 Feature 선택없이 77개와 64개의 Feature에 대해 SDN에서 정상적인 네트워크 흐름(46%)과 DDoS 공격(54%)이 혼합되어 있는 일반적인 상황을 실험하였다. 77개의 Feature 보다는 64개의 Feature를 적용한 경우가 유사한 공격 탐지 평가 시간에도 불구하고 정확도에서 2배 정도 높은 적중률을 보여주고 있지만 다른 평가 요소에서는 다소 불안정한 결과를 보여주고 있다. 이 실험을 통해 Feature 선택의 수를 줄여서 탐지 평가 시간을 줄이고 다른 평가 요소값이 100%에 근접하는 값을 찾는 최적의 PFI 알고리즘의 필요성이 도출되었다.

최적의 Feture 수를 찾기 위해 두 번째 실험에서는 PFI 알고리즘을 적용하여 반복적인 실험을 진행하였다. Future 수를 13, 12, 11, 10, 9, 8 부근에서 90% 이상의 정확도를 유지하면서 탐지 평가 시간을 적정하게 유지하는 구간을 찾은 후 반복적으로 트레이닝을 CNN 분류기 모델을 통해 상위 13 Future가 최적임을 확인했다. 최적의 상위 13 Future를 적용하여 DDoS 공격이 없는 경우는 그림 3과 같다.

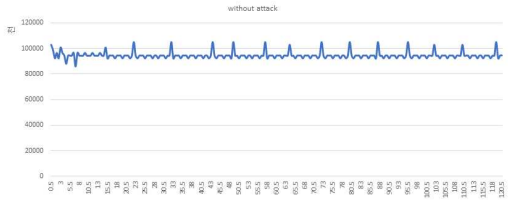

그림 3. DDoS 공격이 없는 네트워크 트래픽 성능
Fig. 3. The Performance of Network Traffic without DDoS Attack

또한, 최적의 상위 13 Future를 적용하여 DDoS 공격이 발생한 후 탐지를 통한 DDoS 공격 발신을 차단하는 완화 메카니즘을 적용한 경우는 그림 4와 같다.

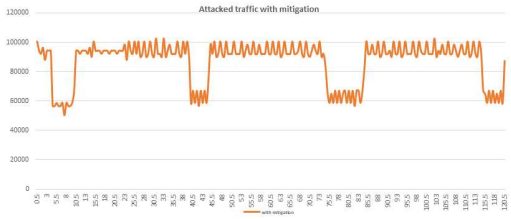

그림 4. DDoS 공격에 대해 탐지 및 완화 메커니즘을 적용한 네트워크 트래픽 성능
Fig. 4. The Performance of Network Traffic of DDoS Attacked with Detection and Mitigation

마지막으로, 최적의 상위 13 Future를 적용하여 DDoS 공격이 발생했지만 탐지를 통한 완화 메카니즘을 적용하지 않는 경우는 그림 5와 같은 실험 결과를 확인하였다.

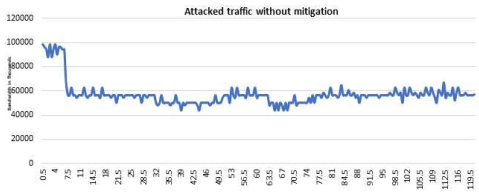

그림 5. DDoD 공격에 대해 탐지 및 완화 메커니즘을 적용하지 않은 네트워크 트래픽 성능
Fig. 5. The Performance of Network Traffic of DDoS Attacked without Detection and Metigation

4. 결론 및 향후연구

본 논문에서는 SDN 환경에서 DDoS 공격을 탐지하고 완화하기 위해 딥 러닝 기반 CNN 모델을 적용하여 실험한 결과를 제시하였다. 이 실험을 통해 논문에서 적용한 연구 방법의 타당성과 성능의 우수성을 확인하였다. 특히, SDN 환경에서 딥 러닝 기반으로 DDoS 공격을 탐지하는 시도가 기존 연구보다 네트워크 흐름에 적은 오버헤드를 가지고 있으며 적정한 Future 선택은 공격 탐지율을 기존 95%정도에서 평균적으로 97% 이상, 기존 97% 정밀도를 98%까지 높였으며, 선행 연구들과 같이 F1_socre 96% 이상을 유지하면서 공격 탐지 시간을 2%이상 줄이는 것을 확인하였다. 향후에는 Mininet 시뮬레이터에서 구현하고 검증한 결과를 실제 SDN 컨트롤러에 적용하여 성능 평가를 진행하고 다양한 사이버 공격에도 활용하여 안정적인 네트워크 흐름을 유지할 수 있는 연구를 진행할 예정이다.

REFERENCES

[1]"Toward an Optimal Solution Against Denial of Service Attacks in Software Defined Networks-ScienceDirect." [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X18302930 #bb40. [Accessed: 30-Mar-2019].

[2]O. Rahman, M. A. G. Quraishi, C.-H. Lung, "Ddos attacks detection and mitigation in sdn using machine learning," IEEE World Congress on Services, Vol. 2642, pp.184-189, 2019.

[3]Nugraha, M., Paramita, I., Musa, A., Choi, D. and Cho, B., "Utilizing OpenFlow and sFlow to Detect and Mitigate SYN Flooding Attack," Journal of Korea Multimedia Society, 17(8), pp.988-994, 2014.

[4]sFlow Version 5. [Online]. http://sflow.org/sflow version 5.txt, 2017.

[5]Dharma N.G., Muthohar M.F., Prayuda J.A. Priagung, K., Choi, D., "Time-based DDoS detection and mitigation for SDN controller. Network Operations and Management

Symposium, pp.550-553, 2015.
[6]Huseyin Polat, Onur Polat, Aydin Cetin, "Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models," MDPI Sustainability, 2020.
[7]Ye, J., Cheng, X. Zhu, J., Feng, L., Song, L., "A DDoS attack detection method based on SVM in software-defined network," Secure Communication Network. pp.1-8, 2018.
[8]Braga R., Mota E., Passito A., "Lightweight DDoS flooding attack detection using NOX/OpenFlow. Local Computer Networks (LCN2010), pp.408-415, 2010.
[9]Wang R., Jia Z., Ju, L., "An Entropy-Based DDoS Detection Mechanism in SDN", Trustcom/BigDataSE/ISPA 2015, Vol. 1, pp. 310-317, 2015.
[10]Mousavi S.M., St-Hilaire M., "Early detection of DDoS attacks against SDN controllers", In Computing Networking and Communications, pp.77-81, 2015.
[11]Soon-Gohn Kim, "A Study on the Detection Technique of DDoS Attacks on the Software-Defined Networks," The Journal of KIIECT, Vol. 13, No.1, pp.81-87, 2020.

저자약력

고 광 만(Kwang-Man Ko) **[정회원]**

- 1991년 2월 원광대학교 컴퓨터공학과(공학사)
- 1993년 2월 동국대학교 컴퓨터공학과(공학석사)
- 1998년 2월 동국대학교 컴퓨터공학과(공학박사)
- 1998년 3월 ~ 2001년 8월 광주여자대학교 컴퓨터과학과 전임강사
- 2001년 9월 ~ 현재 상지대학교 컴퓨터공학과 교수

관심분야: 프로그래밍언어론 및 컴파일러, 모바일 엣지 컴퓨팅.