SDN에서 기계학습과 P4를 결합한 DoS 공격 탐지에 대한 연구

김수연[1], 박태준[2]
[1]전남대학교 인공지능학부 학부생
[2]전남대학교 인공지능학부 교수
rlatndus6205@jnu.ac.kr, taejune.park@jnu.ac.kr

A Study on DoS Attack Detection in SDN Combining Machine Learning and P4

SooYeon Kim[1], Taejune Park[2]
[1]Dept. of Artificial Intelligence, Chonnam National University
[2]Dept. of Artificial Intelligence, Chonnam National University

요 약

현대 사회는 네트워크의 규모가 증가하고 있으며 이러한 대규모의 트래픽을 보다 편하게 관리하고자 SDN이 등장했다. 허나, 대규모 트래픽의 등장으로 인해 DoS 공격의 규모 또한 더욱 커지고 있다. 이러한 공격을 완화하기 위한 다양한 연구가 진행되었으나, SDN에서 기계학습을 활용하여 DoS 공격을 탐지하는 기존의 연구는 제어평면 측에 상당한 부담을 주거나 공격에 대한 대처 부족 등의 문제점이 있다. SDN에서 기계학습과 P4를 결합한 DoS 공격 탐지는 이러한 문제를 해결하기 위해 등장했다. 이 논문에서는 SDN 환경에서 기존의 기계학습 기반의 DoS 공격 탐지에 대한 문제점과 한계에 대해 언급한 이후 기계학습과 P4를 결합한 DoS 공격 탐지에 대한 필요성을 언급한다. 이후, 기계학습 및 P4 기반의 DoS 공격 탐지와 관련된 연구를 살펴보고, 향후 연구 방향을 제시함으로써 네트워크 보안 분야에 새로운 가능성을 제시한다.

1. Introduction

현대 네트워크 패러다임으로 SDN(Software Defined Network)이 널리 쓰인다. SDN은 제어평면과 데이터평면을 분리하고 제어평면을 하나로 모아 여러 데이터평면을 중앙 집중식으로 관리하는 방식을 말한다. 이러한 방식은 네트워크의 가시성을 높이고, 개발자가 네트워크를 보다 편하게 관리할 수 있도록 해준다. 허나, 이러한 시스템에도 단점이 있다. 그 중 하나를 살펴보기 위해 우선 DoS 공격과 관련 연구에 대해 알아보고자 한다.

네트워크 기반 Denial of Service 공격은 공격자가 서버나 장치들에 수많은 패킷을 단기간에 전송함으로써 네트워크를 과포화시켜 사용자가 정상적으로 서비스를 사용하지 못하게 하는 공격으로, 공격이 탐지되면 그 이후에 패킷을 차단하거나 경로를 수정하는 등 신속한 대처가 매우 중요하다. 그러나, 오늘날 네트워크 규모가 증가함에 따라 이러한 패킷을 수동적으로 일일이 검토하는 것은 한계가 있으며, 특히 여러 시스템을 사용하여 타겟 시스템을 마비시키는 공격인 DDoS(Distributed Denial of Service) 공격은 동시에 여러 호스트와 경로를 고려해야하므로 그 탐지와 대처가 매우 어렵다. 이러한 문제를 해결하기 위해 SDN 환경에서 기계학습을 활용한 DoS 공격 탐지와 관련된 연구가 진행되었다.

2. SDN에서 기계학습을 활용한 DoS 공격 탐지

SAHOO et al. [1]은 SVM(Support Vector Machine)과 GA(Genetic Algorithm)를 활용해 SDN에서 DoS 공격을 탐지했다. 위 연구는 기계학습 모델에서 패킷을 추출하는데 이는 하드웨어에서 직접 추출하는 것보다 속도가 느리고 SDN의 제어평면에 상당한 부담을 준다는 문제가 있다. Ma et al. [2]은 엣지 컴퓨팅과 분산 컴퓨팅의 아이디어를 통합한 EDRFS (Edge-Distributed-Random Forest-Feature Selection) 프레임워크를 제안했다. 이 프레임워크는 랜덤 포레스트 모델을 엣지 스위치에 배포하고 스위치에서 DoS 공격을 탐지함으로써 제어평면 측에 대한 부담을 줄인다. 하지만, DoS 공격에 대한 대처가 스위치에서 바로 이루어지지 않는다는 한계가 있다. 또한, 위 연구들은 패킷에서 특징을 추출하는 과정이 스위치에서 바로 이루어지지 않아 추가적인 속도 저하가 발생한다는 문제가 있다.

기계학습을 활용하여 DoS 공격을 탐지하는 시스템에서 이러한 특징 추출 속도는 전반적인 시스템의 효율성에 영향을 미친다. 패킷의 특징을 추출하는 속도를 높임으로써 DoS 공격 탐지의 효율성을 높이기 위해 P4 (Programming Protocol-Independent Packet Processors) [3,4] 스위치를 이용한 하드웨어 기반 DoS탐지 기법이 제시되고 있다. P4 [3,4]는 프로그래밍 가능한 데이터평면 및 그에 대한 언어로, 들

어오는 트래픽을 캡쳐하고 서버로 전달할 필요 없이 바로 하드웨어에서 특징을 추출하므로 추출 속도가 향상된다. 또한, 하드웨어 수준에서 패킷을 처리하므로 패킷의 헤더를 직접 수정할 수 있다. 이는 DoS 공격에 대한 신속한 대처가 가능하다는 것을 의미한다. 또한, 하드웨어 수준에서 패킷을 처리할 수 있기 때문에 SDN 컨트롤러의 부담을 줄일 수 있다. 이러한 이유로 인해 P4 데이터평면과 기계학습을 결합하여 SDN 환경에서 DoS 공격을 탐지하려는 시도가 등장했다. 다음으로는 이러한 SDN에서 P4와 기계학습을 결합한 DoS 공격 탐지와 관련된 연구에 대해 살펴보고자 한다.

3. SDN에서 기계학습과 P4를 결합한 DoS 공격 탐지

Musumeci et al.이 작성한 [6]은 P4 언어를 사용해 상태 유지 데이터평면을 활용하여 데이터평면에서 DoS 공격 탐지를 수행했다. 이때, 데이터평면에서 바로 공격 탐지를 수행하기 때문에 SDN 컨트롤러의 부담이 줄어든다. 또한, 기계학습 기반의 분류기를 사용하여 DoS 공격 탐지를 수행함으로써 탐지의 정확성과 속도를 향상시켰다. 허나, 위 연구는 TCP flood 공격만 탐지할 수 있다는 한계가 있다.

[7]은 위 연구에서 SDN 컨트롤러의 부담을 최소화하기 위해 이상 패턴을 탐지하는 기계학습과 트래픽 정보를 수집하고 처리하는 P4 스위치를 결합했다. 여기서 기계학습은 특징을 기반으로 스위치를 거치는 트래픽이 악성 트래픽인지 탐지하는 역할을 수행하며, 스위치는 들어오는 패킷에서 특징을 추출하고 패킷을 처리함으로써 공격을 완화하는 역할을 수행한다. 허나, 이러한 연구도 공격 유형을 분류하는 다중 클래스 분류를 수행할 수 없다는 한계가 있다.

또 다른 연구인 [8]은 P4 스위치와 기계학습을 결합하여 SDN 환경에서 다양한 유형의 응용 계층 DDoS 공격을 탐지했다. SDN의 제어평면에서 랜덤 포레스트 분류기를 학습시킨 후 모델을 P4 스위치에 매핑했다. 이후 데이터평면 수준에서 바로 패킷 특징 추출과 분류를 수행함으로써 지연이 낮고 처리량이 높은 분류를 달성했다. 이는 회선 속도로 응용 계층 DoS 공격을 탐지했다는 것에 의의가 있다.

허나, 세 연구 모두 데이터평면에서 패킷 헤더를 수정하거나 패킷을 처리하는 방식을 수정하는 방식과 같이 실시간으로 DoS 공격을 완화하는 과정은 부족하다.

4. Conclusion

네트워크의 규모가 커져가고 있는 현대 사회에서 소프트웨어만으로는 수많은 트래픽을 빠르게 처리하기 어렵다. 또한, DoS 공격과 같이 대규모 공격에 대한 대처를 수행하기에는 소프트웨어에 부담이 많이 간다는 문제점이 존재한다. 이러한 문제를 해결하기 위해 기계학습과 P4를 결합하여 DoS 공격을 탐지하고자 하는 연구가 진행되고 있다. 허나, 공격을 단순히 탐지만 하는 것에 그치지 않고 나아가 이에 대해 능동적으로 신속하게 대처까지 수행하는 연구가 수행될 경우 네트워크 보안에 큰 기여를 할 것으로 보인다. 또한, 현대 사회에서는 점점 더 공격이 다양해지고 정교해지고 있다. 이러한 상황에서 DoS 공격 외에도 퍼징, 중간자 공격, 원격 코드 실행, 백도어와 같이 널리 알려진 공격 뿐만 아니라 기존에 알려지지 않은 새롭게 등장한 공격도 빠르게 탐지하여 대처를 수행한다면 네트워크 보안이 더욱 안전해질 것으로 기대한다. 기계학습과 P4를 결합하여 이러한 연구를 수행할 경우 기계학습의 능동성과 신속성, P4의 신속성과 자원 절약과 같은 장점을 결합해 효율적으로 네트워크 보안을 수행할 수 있을 것이다.

acknowledgement

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 인공지능융합혁신인재양성사업 연구 결과로 수행되었음(IITP-2023-RS-2023-00256629)

참고문헌

[1] SAHOO, Kshira Sagar, et al. An evolutionary SVM model for DDOS attack detection in software defined networks. IEEE access, 2 020, 8: 132502-132513.

[2] MA, Ruikui, et al. Real-Time Detection of DDoS Attacks Based on Random Forest in SDN. Applied Sciences, 2023, 13.13: 7872.

[3] BOSSHART, Pat, et al. P4: Programming protocol-independent packet processors. ACM SIGCOMM Computer Communication Review, 2014, 44.3: 87-95.

[4] P4, "P4 Open Source Programming Language", (https://p4.org/)

[5] 오일석, "기계학습(MACHINE LEARNING)", 서울, 한빛아카데미, 2021

[6] MUSUMECI, Francesco, et al. Machine-learning-assisted DDoS attack detection with P4 language In: ICC 2020-2020 IEEE International Conference on Communications (ICC). IEEE, 2020. p. 1-6.

[7] MUSUMECI, Francesco, et al. Machine-learning-enabled ddos attacks detection in p4 programmable networks. Journal of Network and Systems Management, 2022, 30: 1-27.

[8] LAHOZ TORRES, Aleix. Application-Layer DoS attacks detection in Data-Plane-Programmable Networks using Machine Learning and P4. 2023. Master's Thesis. Universitat Politècnica de Catalunya.