JKIICE

Short Paper

한국정보통신학회논문지 Vol. 24, No. 1: 138~140, Jan. 2020

에지 클라우드 환경에서 사물인터넷 트래픽 침입 탐지

Intrusion Detection for IoT Traffic in Edge Cloud

Kwang-Seong Shin[1] · Sungkwan Youm[2*]

[1]Associate Professor, Department of Digital Contents Engineering, WonKwang University, 54538 Korea
[2*]Associate Professor, Department of Information & Communication Engineering Department, WonKwang University, 54538 Korea

ABSTRACT

As the IoT is applied to home and industrial networks, data generated by the IoT is being processed at the cloud edge. Intrusion detection function is very important because it can be operated by invading IoT devices through the cloud edge. Data delivered to the edge network in the cloud environment is traffic at the application layer. In order to determine the intrusion of the packet transmitted to the IoT, the intrusion should be detected at the application layer. This paper proposes the intrusion detection function at the application layer excluding normal traffic from IoT intrusion detection function. As the proposed method, we obtained the intrusion detection result by decision tree method and explained the detection result for each feature.

Keywords : Edge Computering, IoT, Intrusion Detection, Supervised Learning, Application Layer

Ⅰ. 서 론

오늘날 IoT 서비스는 데이터 수집 및 분석과 같은 다양한 요구 사항을 만족해야 한다. 대부분의 경우 다양한 IoT 서비스를 지원하기 위해 클라우드 및 에지 컴퓨팅의 조합으로 동작한다. 클라우드 컴퓨팅은 일반적으로 특정 애플리케이션과 프로세스를 실행하고 원격 측정 데이터를 시각화하기 위해 스토리지 및 컴퓨팅 기능이 필요할 때 사용된다. 반면에 에지 컴퓨팅은 대기 시간이 짧고 로컬 자치 작업이 적고 백엔드 트래픽이 감소하고 기밀 데이터와 관련된 경우에 적합하다. 에지 및 클라우드 컴퓨팅은 상호 배타적인 접근 방식으로 여겨지지만 대규모 IoT 프로젝트는 두 가지의 조합이 필요하다 [1-2].

불행히도 네트워크 침입 방지 시스템 및 방화벽과 같은 기존의 네트워크 보안 솔루션은 이러한 IoT 장치에서 생성된 악성 트래픽을 구별하고 필터링하는 데 부족하다. 첫째로, 장치 및 펌웨어 버전의 이질성으로 인해 이러한 장치에 대해 가능한 모든 네트워크 상호 작용에 대한 특징을 수집 할 수 없다. 실제로 장치의 네트워크 동작은 펌웨어 릴리스마다 크게 다를 수 있다. 둘째로, 기존의 네트워크 침입 방지 시스템을 구축하고 유지 관리하는 비용은 소규모 사무실 및 홈 네트워크에서 높다. 마지막으로, 처리해야 하는 네트워크 트래픽 데이터양은 트래픽 분석을 수행하는 네트워크 침입 방지 시스템을 압도 한다. 따라서 자체 적응적이고 비용 효율적이며 특수 하드웨어가 필요 없는 트래픽 모니터링 및 분류를 위한 새로운 솔루션이 필요하다 [3-4].

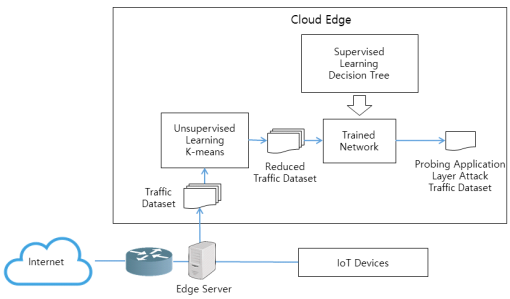

Fig. 1 Intrusion Detection System for Edge Cloud

에지 네트워크에서 IoT 트래픽을 분류하고 침입 트래픽을 분류할 필요가 있다. 에지 클라우드에서 사물인터넷 트래픽은 어플리케이션 계층에서 발생한다 [5-6].

Received 8 November 2019, **Revised** 15 November 2019, **Accepted** 18 November 2019

* **Corresponding Author** Sungkwan Youm(E-mail:skyoum@gmail.com, Tel:+82-63-850-6342)
Associate Professor, Department of Information & Communication Engineering Department, Wonkwang University, 54538 Korea

Open Access http://doi.org/10.6109/jkiice.2020.24.1.138 print ISSN: 2234-4772 online ISSN: 2288-4165

그래서 어플리케이션 계층의 트래픽을 분류하고 침입을 탐지해야 한다. 본 논문에서는 이렇게 에지 클라우드에서 IoT 트래픽 침입 탐지 방법을 제안하고 분석한다. 2장에서는 제안하는 IoT 트래픽 탐지 방법에 대해서 설명하고 실험 결과를 분석한 후 마지막 장에서 결론을 맺는다.

Traffic Feature	Attack Pattern					
	satan	multihop	warezmast	warezclien	spy	rootkit
duration	0	50	0	9	100	0
service	0	0	0	0	0	0
src_bytes	9	0	0	85	0	100
dst_bytes	0	0	50	26	100	0
land	0	0	0	0	0	0
wrong_fragment	0	0	0	0	0	0
hot	0	0	0	28	0	0
num_failed_logins	0	0	0	0	0	0
logged_in	0	0	0	0	0	0
num_compromised	0	0	0	0	0	0
num_root	0	0	0	0	0	50
count	3	0	0	0	0	0
srv_count	0	0	0	0	0	0
serror_rate	87	0	0	0	0	0
rerror_rate	90	0	0	0	0	0
diff_srv_rate	92	0	0	0	0	0
dst_host_diff_srv_rate	90	0	0	0	0	0
dst_host_same_src_port_rate	0	0	0	0	0	0
dst_host_srv_diff_host_rate	0	0	0	0	0	0
dst_host_serror_rate	64	0	0	2	0	0
dst_host_rerror_rate	80	0	0	0	0	0
dst_host_srv_rerror_rate	0	0	0	0	0	0

Fig. 2 Detection Rate for Normal and Attack Types

Ⅱ. IoT 침입 탐지 시스템

2.1. IoT 침입 탐지 시스템

제안하는 침입 탐지 과정은 그림 1의 라우터에서 먼저 k-mean 비지도 학습으로 정상 트래픽을 분류한다. 분류하는 방법은 임의의 시험 트래픽을 송수신하여 해당 트래픽이 비지도 학습의 클러스터에 포함되면 해당 클러스터의 트래픽을 정상 트래픽으로 분류하여 침입 탐지 알고리즘에서 제거한다. 그리고 침입 탐지 트래픽이 포함되어 있다고 판단이 되는 트래픽에 대해서 Decision Tree 지도 학습을 통해서 공격 유형을 분류하는 과정을 거친다.

2.2. IoT 침입 탐지 시스템 실험 결과 분석

제안하는 침입 탐지를 시험하기 위해 KDDCUP99 데이터를 사용하였다 [7]. 제안하는 IoT 침입 탐지 시스템에서는 탐지할 트래픽을 줄여서 공격 유형 판별 시간을 줄이고 탐지율을 높이고자 한다. 그림 2는 제안하는 침입 탐지를 통해서 IoT 응용 계층에서의 침입 탐지를 분류한 내용이다. 왼쪽은 트래픽의 feature를 나타내고 상단은 공격 타입을 나타낸다. 과정은 그림 1의 라우터에서 먼저 비지도 학습으로 정상 트래픽을 분류한다. 그림 1의 에지 서버에서 지도학습을 통해서 정상 트래픽을 제거한 트래픽에 대해서 각 feature 별 탐지율을 구한다. 그림 2의 count feature는 정상 트래픽을 분류하는 중요한 기준이 되고 perl 공격을 탐지하기 위한 중요한 feature는 dst_bytes와 num_root이다. 에지 클라우드에 guess_password 공격을 탐지하기 위해 점검해야 하는 feature는 src_bytes와 dst_bytes이다. 그림 2에서 보는 바와 같이 각 feature는 특정 공격을 검출하기 위한 중요한 판단 기준이 되므로 에지 클라우드에서 침입 탐지하기 위한 중요한 파라미터가 된다.

Ⅲ. 결 론

사물인터넷이 가정용 및 산업용 네트워크에 적용되면서 사물인터넷이 생성하는 데이터는 클라우드 에지에 처리하려고 하고 있다. 이렇게 클라우드 에지를 통해서 사물인터넷 기기에 침입하여 기능을 조작하는 경우가 발생할 수 있어 침입 탐지 기능이 매우 중요하다. 클라우드 환경에 에지 네트워크로 전달되는 트래픽은 응용계층의 트래픽이다. 이러한 사물인터넷에 전달되는 패킷에 대한 침입 여부를 판별하기 위해서는 application 계층에서 침입을 탐지해야 한다. 본 논문은 정상 트래픽을 사물인터넷 침임 탐지 기능에서 제외하고 응용계층에서 침입 탐지하는 기능을 제안하였다. 제안하는 지도학습 방식으로 침입 탐지 결과를 얻고 각 feature 별 탐지 결과에 대해 설명하였다.

ACKNOWLEDGEMENT

This paper was supported by Wonkwang university in 2018

REFERENCES

[1] Y. Ai, M. Peng, and K. Zhang, “Edge cloud computing technologies for internet of things: A primer,” *Digital Communications and Networks*, vol 4, no. 2, pp. 77-86, 2017.

[2] A. Alnoman, S. K. Sharma, W. Ejaz, and A. Anpalagan, “Emerging Edge Computing Technologies for Distributed IoT Systems,” *IEEE Network*, vol. 33, no. 6, pp. 140-147, 2019.

[3] S. Raponi, M. Caprolu, and R. D. Pietro “Intrusion Detection at the Network Edge: Solutions, Limitations, and Future Directions,” in *International Conference on Edge Computing*, San Diego : SD, 2019.

[4] B. B. Zarpelão, R. S. Miani, C. T. Kawakani, and S. C. de Alvarenga, “A survey of intrusion detection in Internet of Things,” *Journal of Network and Computer Applications*, vol. 84, no. 15, pp. 25-37. 2017.

[5] M. F. Elrawy, A. I. Awad, and H. F. A. Hamed, “Intrusion detection systems for IoT-based smart environments: a survey,” *Journal of Cloud Computing: Advances, Systems and Applications*, vol. 7, no. 21, pp 1-20, 2018.

[6] M. Hasan, Md. M. Islam, Md I. I. Zarif, and M. M. A. Hashem, “Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches,” *Internet of Things*, vol. 7, 2019.

[7] UCI. 2009. The 3rd International Knowledge Discovery and Data Mining Tools Competition. [Internet]. Available: http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.