JKIICE Journal of the Korea Institute of Information and Communication Engineering

한국정보통신학회논문지 Vol. 25, No. 1: 69~74, Jan. 2021

트래픽 속성 개수를 고려한 의사 결정 트리 DDoS 기반 분석

진민우[1] · 염성관[2*]

DDoS traffic analysis using decision tree according by feature of traffic flow

Min-Woo Jin[1] · Sung-Kwan Youm[2*]

[1]Graduate Student, Department of Information & Communication Engineering Department, WonKwang University, 54583 Korea
[2*]Associate Professor, Department of Information & Communication Engineering Department, WonKwang University, 54583 Korea

요 약

코로나19의 영향으로 온라인 활동이 늘어나면서 인터넷 접속량도 늘어나고 있다. 하지만 악의적인 사용자에 의해서 네트워크 공격도 다양해지고 있으며 그중에서 DDoS 공격은 해마다 증가하는 추세이다. 이러한 공격은 침입 탐지 시스템에 의해서 탐지되며 조기에 차단할 수 있다. 침입 탐지 알고리즘을 검증하기 위해 다양한 데이터 세트를 이용하고 있으나 본 논문에서는 최신 트래픽 데이터 세트인 CICIDS2017를 이용한다. 의사 결정 트리를 이용하여 DDoS 공격 트래픽을 분석하였다. 중요도가 높은 결정적인 속성(Feature)을 찾아서 해당 속성에 대해서만 의사 결정 트리를 진행하여 정확도를 확인하였다. 그리고 위양성 및 위음성 트래픽의 내용을 분석하였다. 그 결과 하나의 속성은 98%, 두 가지 속성은 99.8%의 정확도를 각각 나타냈다.

ABSTRACT

Internet access is also increasing as online activities increase due to the influence of Corona 19. However, network attacks are also diversifying by malicious users, and DDoS among the attacks are increasing year by year. These attacks are detected by intrusion detection systems and can be prevented at an early stage. Various data sets are used to verify intrusion detection algorithms, but in this paper, CICIDS2017, the latest traffic, is used. DDoS attack traffic was analyzed using the decision tree. In this paper, we analyzed the traffic by using the decision tree. Through the analysis, a decisive feature was found, and the accuracy of the decisive feature was confirmed by proceeding the decision tree to prove the accuracy of detection. And the contents of false positive and false negative traffic were analyzed. As a result, learning the feature and the two features showed that the accuracy was 98% and 99.8% respectively.

키워드 : 침입 탐지 시스템, 서비스 거부, 의사결정트리, 예측 중요도, CICIDS2017

Keywords : Intrusion detection system, DDoS, Decision tree, Predictor importance, CICIDS2017

Received 13 November 2020, **Revised** 5 December 2020, **Accepted** 16 December 2020

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

Open Access http://doi.org/10.6109/jkiice.2021.25.1.69 print ISSN: 2234-4772 online ISSN: 2288-4165

Ⅰ. 서 론

코로나19의 영향으로 비대면 활동이 활발해지면서 온라인으로 하는 작업들이 늘어나고 있다. 온라인이 활성화되면서 디지털 전환이 가속화되어 웹사이트, 온라인 쇼핑몰, 게임 및 교육 플랫폼의 트래픽이 증가하게 되었다. 하지만 이러한 온라인 서비스를 공격하는 보안 사고가 해마다 증가하고 있다. 예를 들어 서비스 거부를 유발하는 DDoS 공격이 다양하게 증가하고 있다. 최근 서비스 거부를 인질로 몸값을 요구하는 보이스 피싱이 발생하였다[1,2].

네트워크 혹은 특정 시스템에서 비정상적이거나 악의적인 행동을 찾아내는 기법을 침입 탐지(Intrusion Detection)라고 한다. 네트워크를 안정적으로 운영하기 위해 외부의 침입으로부터 네트워크 및 호스트를 보호하기 위해 망의 침입 탐지 시스템을 운영하고 있다. 침입 탐지 시스템은 통상적으로 네트워크에서 비정상적이나 악의적인 행위를 탐지하는 시스템으로, 네트워크 및 호스트 보안을 위해 매우 중요한 시스템이다. 대표적인 탐지 방식으로 패턴 기반 탐지와 비정상 행위 기반 탐지가 있다. 패턴 기반 탐지는 학습된 내용을 바탕으로 입력 트래픽을 분석해서 비정상 트래픽을 감지한다. 반면에 비정상 행위 기반 탐지는 일상적이지 않은 패턴의 트래픽이 유입되었을 때 감지한다[3,4].

이러한 패턴 기반 침입탐지는 비정상 트래픽을 감지하는 알고리즘을 적용하여 외부의 위협으로부터 사전에 차단하고자 한다. 많은 논문에서 효율적인 알고리즘을 검증하기 위해 실제 망에서 수집된 데이터에 적용해서 검증하고 있다. 가장 많이 사용하고 있는 데이터인 KDDCUP 99는 20년이 지났음에서 많은 연구에서 활용되고 있다. 네트워크 환경을 구성하여 시뮬레이션으로 얻어진 네트워크 트래픽을 tcpdump로 만들어진 공격 데이터이다. DARPA에서 네트워크 이상 탐지 또는 공격 판별 테스트를 위해 만든 데이터 셋으로써, 지속시간, 프로토콜 종류 등 41개의 속성과 공격여부를 라벨링한 정보까지 총 42개의 속성을 가지고 있다[5]. 그리고 CIC-IDS-2017는 캐나다 사이버보안연구소에서 전수공격(Brute force), Heartbleed, Botnet, DDoS 등 6가지 공격 시나리오를 생성하여 수집한 데이터 세트로써 80개의 속성을 가지고 있다[6].

공격 탐지 성능 향상을 위해 머신러닝을 이용한 탐지 기법이 많이 도입되고 잇다. 머신 러닝의 학습을 위해서 트래픽의 특징과 공격패턴을 사용하며 학습한 네트워크을 바탕으로 실제 네트워크에 적용하여 시험한다. 이때 주로 사용되는 데이터 세트가 KDDCUP99, CICIDS2017이다[7]. 본 논문은 가장 최근의 데이터 세트인 CICIDS2017를 이용하여 결정 트리 침입 탐지 알고리즘을 검증하고 데이터의 유효성에 관해서 확인하고자 한다.

본 논문은 2장에서 의사 결정 트리 알고리즘 및 예측 중요도에 대하여 설명한다. 3장에서는 의사 결정 트리를 이용한 침입 탐지 방법에 관하여 설명하고 CICIDS 2017로 학습 및 탐지한 내용을 기술한다. 그리고 마지막 장에서 결론을 맺는다.

Ⅱ. 의사 결정 트리 및 중요도 분석

본 장에서는 DDoS 공격 탐지를 하기 위해서 사용하고 있는 침입 탐지 알고리즘 및 예측 중요도에 관하여 설명한다.

2.1. 의사 결정 트리 알고리즘

의사 결정 트리 학습법은 기계 학습으로써 입력 및 목표 변수를 연결해주는 의사 결정 트리를 사용한다. 일반적으로 의사 결정 트리 방법으로 분류(Classification) 및 회귀(Regression)가 가능하다. 분류는 목표 값이 이산적일 경우 즉, 목표 값이 가질 수 있는 값이 유한한 경우에 적용하며 회귀는 목표 값이 실수인 경우에 적용한다. 트리는 가지와 노드로 구성되어 있으며 가지는 입력에 대한 참과 거짓을 가지는 논리연산으로 나타낸다. 노드는 출력으로 연속 또는 불연속 값이 될 수 있다. 결정 트리 중 종단 노드 변수가 연속하는 값, 일반적으로 실수를 가지는 것은 회귀 트리라 한다.

결정 트리 학습법은 지도 분류 학습에서 가장 유용하게 사용되고 있는 기법 중 하나이다. 본 연구에서는 공격 유형에 따라 유한한 이산값으로 정의한 출력값을 가지고 있으며, 분류를 단일 대상 속성으로 지니고 있다고 간주한다. 결정 트리의 모든 내부 노드들에는 트래픽 흐름(Traffic flow)의 속성으로 입력 속성이 일대일로 대응된다. 트리의 내부 노드에 연결된 가지에는 속성이 가질 수 있는 값들이 표시되며, 잎 노드에는 속성의 확률 분포가 표시된다.

결정 트리의 학습에 사용되는 트래픽 속성 집합을 적

절한 분할 기준에 따라 부분 집합들로 나누는 과정이다. 이러한 과정은 순환 분할이라 불리는 방식으로 각각 나눠진 숙성 부분 집합에 재귀적으로 반복되며, 분할로 인해 더 이상 새로운 공격유형의 목표 값이 추가되지 않거나 부분 집합의 노드가 목표 값과 같은 값을 지닐 때까지 계속된다. 이러한 하향식 의사 결정 트리 귀납법은 일반적인 알고리즘의 한 예시이며, 데이터로부터 결정 트리를 학습하는 방법이다. 입력 및 목표값을 아래와 같이 기술할 때,

$$(x, Y) = (x_{1,} x_{2,} x_{3,} \ldots, x_{k,} Y) \tag{1}$$

목표값 Y는 분류를 통해 학습하고자 하는 목표 변수로서 본 연구에서는 트래픽 공격유형이 되며, 벡터 x는 입력 변수로 트래픽 흐름 속성이다.

본 연구에서는 분류 및 회귀 트리(Classification And Regression Tree, CART)를 사용하였다. 분류 및 회귀 트리는 두 가지 기능의 트리를 아울러 일컫는 용어이다. 분류 및 회귀 트리는 일정 부분 유사하지만, 입력 및 목표값 자료를 나누는 과정 등에서 차이가 있다.

분류형 목표 변수에 대한 분리 기준은 다음과 같다. 지니 인덱스(Gini index)은 각 마디에서의 불순도(Impurity) 또는 다양도(diversity)를 재는 척도 중 하나로서 식 (2)과 같이 정의한다. 0에 가까운 값이 분류에 효과적이다. 식 (2)에서 n개 관측치 중에서 임의로 2개를 선택하였을 때, 선택된 2개가 서로 다른 범주에 속할 확률을 의미한다.

$$\begin{aligned} G &= \sum_{j=1}^{c} \sum_{i \neq j} P(i) P(j) = \sum_{j=1}^{c} P(i) [1 - P(j)] \\ &= 1 - \sum_{j=1}^{c} P(j)^2 = 1 - \sum_{j=1}^{c} (n_j / n)^2 \end{aligned} \tag{2}$$

여기서 $P(j)$는 각마디에서 한 속성이 목표변수의 j번째 범주의 속할 확률이다. 그리고 c, n, n_j는 각각 분류 수, 가지에 포함되어 있는 관측치의 수, 목표변수의 j번째 범주에 속하는 관측치의 수를 나타낸다. 의사결정 나무는 지니 인덱스가 작아지는 방향으로 움직이며 지니 인덱스 값을 가장 많이 감소시켜 주는 변수가 영향을 가장 많이 끼치는 변수가 된다. 그리고 이 변수를 기준으로 의사 결정 트리의 가지가 만들어진다. 모든 트래픽 흐름의 속성을 반복하면서 가지를 쳐나간다. 가지를 칠 때마다 지니 인덱스를 측정하여 가장 낮은 속성을 찾아서 가지를 치고 더는 분류가 필요하지 않을 때까지 학습한다.

2.2. 중요도 분석

지니 중요도(Gini Importance)를 측정하여 속성 중 가장 중요한 값을 찾아서 해당 속성에 대해서만 결정트리를 학습시켜 학습 시간을 최소화 할 수 있다. 지니 중요도로 중요한 속성을 파악하여 해당 속성을 분류의 기준으로 삼는다. 속성 중요도는 모든 속성 평균 X_j가 사용되는 모든 트리의 노드에 대해서 $p(t) \triangle i(s_t, t)$ 차감을 더한 후 평균을 구한다[8,9].

$$Imp(X_j) = \frac{1}{M} \sum_{m=1}^{M} \sum_{t \in \varphi_m} 1(j_t = j) [p(t) \triangle i(s_t, t)], \tag{3}$$

지니 지수를 불순도 함수로 사용하는 경우에 측정값을 지니 중요도라고 한다.

Ⅲ. 결정 트리를 이용한 DDoS 분석

CICIDS는 많은 트래픽 세트를 포함하고 있다[10]. 그 중에서 본 논문은 CICIDS2017 데이터 세트로 의사 결정 트리를 분석한다. 본 연구에서는 의사 결정 트리로 데이터 세트를 학습하여 탐지하지만 정확도뿐만 아니라 위양성 및 위음성의 트래픽 특징을 파악하고자 한다.

3.1. 전체 속성 학습 결과

트래픽 세트는 80개의 속성이 입력 변수로 제공된다. 이 속성들은 CICFlowMeter를 구동하여서 나온 결과이다. CICFlowMeter는 Raw 트래픽을 생성 및 분석하는 툴로서 트래픽 흐름에 대한 데이터를 생성한다. TCP 트래픽 흐름은 FIN으로 종료가 결정되고 UDP Flow의 경우 Timeout에 의해서 결정된다. Raw 트래픽 흐름로 부터 속성을 추출한다. 전체 트래픽 흐름 수는 225745이다. 이 흐름의 마지막 속성 열에 트래픽 라벨이 표기된다. 라벨은 BENIGN과 DDoS로 구분된다. 전체 79개 속성을 입력으로 의사 결정 분석 결과는 표 1과 같다. 트리의 구조는 그림 1과 같다. 정확도가 99.98%를 기록하였으며 위양성 2개의 경우 정상 트래픽을 차단하는 결과를 나타낼 수 있는 반면에 위음성 1개의 경우 네트워크

에 하나의 공격 트래픽이 전달되어 서비스에 미미한 영향을 미칠 수 있다.

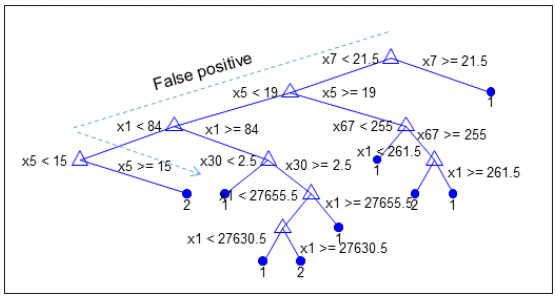

Fig. 1 Decision tree on DDoS dataset

Table. 1 Accuracy on decision tree on all features

Accuracy(%)	False positive	False negative
99.9867	2	1

의사 결정 트리에서 중요하지 않은 속성은 DDoS 공격 여부를 판단하는데 제거할 수 있다. 그래서 속성의 중요도를 확인하였다. 그림 2는 속성별 중요도를 나타낸다. 그림에서 보는 바와 같이 x축 속성 5, 7에서 결정적인 역할을 하고 있다. x5와 x7은 각각 'Total Length of Fwd Packets'와 'Fwd Packet Length Max'으로 중요도 값 0.0140 와 0.0146이다. 여기서 'Total Length of Fwd Packets'는 외부에서 내부 방향을 향하는 트래픽 흐름의 전체 사이즈를 말한다. 예를 들어, Sync 공격은 짧은 패킷으로 이루어지기 때문에 DDoS 공격에서 많이 사용되고 있다.

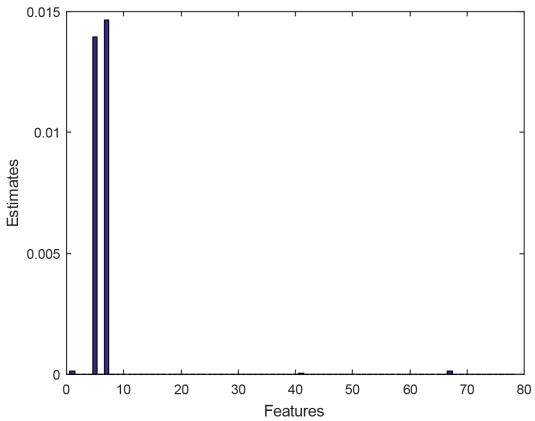

Fig. 2 Importance Estimate on the decision tree

그림 3은 전체 속성을 대상으로 의사 결정 트리를 구성했을 때 위양성과 위음성 트래픽을 나타내고 있다. 위양성이라 함은 BENIGN 트래픽인데 의사결정 트리에서 DDoS로 인식하는 트래픽을 말하고 위음성이라고 함은 DDoS 트래픽인데 BENIGN 트래픽으로 인식하는 것을 말한다. 의사 결정 트리에 의해서 오판되는 트래픽 흐름을 확인한 결과 글 상자와 같이 'Total Length of Fwd Packets'의 값 18을 위양성으로 판정하고 있으며 'Total Length of Fwd Packets'의 값 12를 위음성으로 판정하고 있다. 그림 1에서 위양성을 판단하는 경로는 점선으로 나타내고 있다. 데이터 셋의 DDoS 공격 포트은 80으로 인터넷 웹 서비스 공격로 이루어져 있다. 위음성의 경우 탐지를 통과할 경우 서비스에 자원 소진으로 이어지지만 치명적이지 않다.

< False positive >
80,153,3,0,18,0,6,6,6,0,0,0,0,0,117647.0588,19607.84314,76.5,40.30508653,105,48,153,76.5,40.30508653,105,48,0,0,0,0,0,0,0,0,0,60,0,19607.84314,0,6,6,6,0,0,0,0,0,0,1,0,0,0,0,8,6,0,60,0,0,0,0,0,0,0,3,18,0,0,256,-1,2,20,0,0,0,0,0,0,0,0,BENIGN
80,472,3,0,18,0,6,6,6,0,0,0,0,0,38135.59322,6355.932203,236,328.0975465,468,4,472,236,328.0975465,468,4,0,0,0,0,0,0,0,0,0,60,0,6355.932203,0,6,6,6,0,0,0,0,0,0,1,0,0,0,0,8,6,0,60,0,0,0,0,0,0,0,3,18,0,0,65535,-1,2,20,0,0,0,0,0,0,0,0,BENIGN
< False negative>
80,29,2,1,12,6,6,6,6,0,6,6,6,0,620689.6552,103448.2759,14.5,19.09188309,28,1,1,1,0,1,1,0,0,0,0,0,0,0,0,0,0,40,20,68965.51724,34482.75862,6,6,6,0,0,0,0,0,0,1,0,0,0,0,8,6,6,40,0,0,0,0,0,0,2,12,1,6,256,229,1,20,0,0,0,0,0,0,0,0,DDoS

Fig. 3 False positive and negative cases

3.2. 'Total Length of Fwd Packets' 사용 결과

전체 트래픽에 대해서 의사 결정 트리 분석 및 중요도를 평가한 결과 중요 속성이 5번과 7번 임을 확인하였다. 그래서 5번 속성인 'Total Length of Fwd Packets'에 대한 결정 트리를 분석하여 탐지 정확도를 파악하고자 한다. 의사 결정 트리를 학습시킨 결과 그림 4과 같은 의사 결정 트리를 구성하였다. 5번 속성에 의한 정확도는 표 2에서 보는 바와 같이 98.9% 이다. 그리고 위양성 및 위음성의 개수는 각각 200개 및 35개 이다. 위양성과 위

음성을 분석한 결과 모든 속성에 대해서 적용한 결과와 다른 위양성 및 위음성 트래픽 흐름이 나타났다. 이 결과를 보면 98.9%의 정확도는 유의미하다고 판단되며 5번 속성으로만 판단하면 되지만 이 데이터 세트에 대해서만 유한할 것으로 추정한다. 다른 특징의 트래픽 경우 Sync가 Forward 패킷이 크고 가변적일 때는 이 정도의 정확도를 얻기 힘들 것이다.

Table. 2 Accuracy on decision tree on Total Length of Fwd Packets feature

Accuracy(%)	False positive	False negative
98.9502	200	36

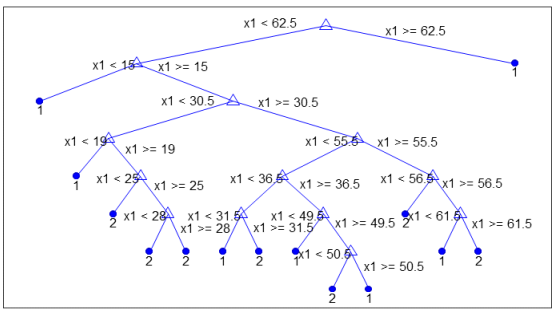

Fig. 4 Decision tree on 'Total Length of Fwd Packets' feature

3.3. 'Fwd Packet Length Max' 사용 결과

이번에는 7번 속성에 대해 적용한 결과를 보고자 한다. 7번의 경우 그림 5와 같이 아주 단순한 트리로 생성되며 트래픽 흐름의 Forward 최대 사이즈가 5보다 크고 6.5보다 작은 경우 또는 13.5보다 크거나 21.6보다 작은 경우 DDoS 공격 트래픽 흐름으로 판정한다. 이 조건이 다른 DDoS 공격에도 적용 가능한지 판단할 필요가 있다. 위 조건으로 의사결정트리를 했을 때 위음성의 개수가 발생하지 않았다는 것은 임의로 침투하는 트래픽이 발생하지 않았다는 의미이며 계정 공격과 같은 공격에서 필요한 결과이다. 표 3을 보면 정확도는 89.3%이며 위양성 및 위음성은 각각 2415 및 0개를 나타낸다. 위양성이 많아서 일반 트래픽에 영향을 미칠 수 있어 탐지 알고리즘으로 채택하기에 적합하지 않다.

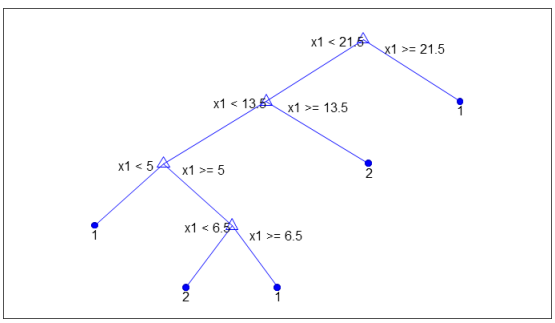

Fig. 5 Decision tree on Fwd Packet Length Max feature

Table. 3 Accuracy on decision tree on Fwd Packet Length Max feature

Accuracy(%)	False positive	False negative
89.3023	2415	0

3.4. 'Total Length of Fwd Packets'와 'Fwd Packet Length Max' 사용 결과

다음은 'Total Length of Fwd Packets'와 'Fwd Packet Length Max'을 모두 이용하여 의사 결정트리를 수행하면 트리는 그림 6와 같으며 성능은 표 4와 같이 얻을 수 있다. 그림에서 x1은 'Total Length of Fwd Packets'를 x2는 'Fwd Packet Length Max'를 나타낸다. 트리는 단순화 되어 있지만 표 4에서 보는 바와 같이 정확도가 99.8에 달한다. 속성이 많아지면 학습하는데 소비되는 자원이 많아지기 때문에 최소의 속성으로 최대의 성능을 달성해야 한다. 이처럼 2개의 속성만으로 전체 속성을 학습시킨 결과와 유사한 정확도를 얻을 수 있었다.

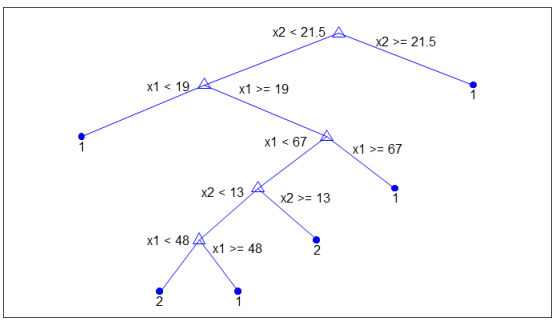

Fig. 6 Decision tree on 'Total Length of Fwd Packets and Fwd Packet Length Max' feature

Table. 4 Accuracy on decision tree on Fwd Packet Length Max feature

Accuracy(%)	False positive	False negative
99.8405	5	31

Ⅳ. 결 론

본 연구에서는 의사 결정 트리를 이용하여 CICIDS2017 데이터의 DDoS 공격를 분석하였다. 분석 방법으로 먼저 전체 트래픽 속성을 적용해서 분석한 후 예측 중요도로 다시 중요한 트래픽 속성을 파악한다. 해당 트래픽 속성으로 다시 의사 결정 트리를 학습하여 정확도, 위양성 및 위음성를 확인하였다. 2가지 트래픽 속성으로 분석하여도 99.8%의 정확도를 얻을 수 있었다. 하지만 위음성의 개수는 늘어나 탐지를 피하는 공격 트래픽이 늘어 날 가능성이 있다. 그리고 본 연구에서는 위양성 및 위음성 트래픽 흐름 특징에 대해서 분석하였다. 앞으로 패턴을 회피하는 공격이나 DDoS 트래픽 흐름의 가변적인 특징을 고려하여 비지도 학습을 통해서 DDoS 공격을 판별하는 기법에 대한 추가 연구가 필요하다.

ACKNOWLEDGEMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2018R1D1A1B07050277).

REFERENCES

[1] FotiGuard Labs. Global Threat Trend Report [Internet]. Available: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/ko_kr/threat-report-h1-2020-kr.pdf.

[2] KISA. Cyber Security Issue Report Q2 2020 [Internet]. Available: https://www.boho.or.kr/data/reportView.do?bulletin_writing_sequence=35506.

[3] H. J. Gil and S. H. Kim, "A Tree-based Intrusion Detection System (IDS) considering Data features," in *Conference Proceeding of The Korean Operations Research and Management Science Society*, Seoul: SU, pp. 605-608, Oct. 2009.

[4] I. Lee and S. Oh, "Optimization of Intrusion Detection Systems based on signature-based rules," *Communications of the Korean Institute of Information Scientists and Engineers*, vol. 33, no. 6, pp. 55-60, Jun. 2015.

[5] E. M. Yang and C. H. Seo, " A Study on Intrusion Detection in Network Intrusion Detection System using SVM," *Journal of Digital Convergence*, vol. 16, no. 5, pp. 399-406, May. 2018.

[6] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, " Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization," In *Proceeding of the 4th International Conference on Information Systems Security and Privacy*, Funchal: FNC, pp. 108-116, Jan. 2018.

[7] S. H. Choi, M. H. Jang, and M. S. Kim, "A Study on AI algorithms to Improve Precision Rate in a Managed Security Service," *The transactions of The Korean Institute of Electrical Engineers*, vol. 69, no. 7, pp. 1046-1052, Jul. 2020.

[8] B. H. Menze, B. M. Kelm, R. Masuch, R. U. Himmelreich, P. Bachert, W. Petrich, and F. A. Hamprecht, "A comparison of random forest and its Gini importance with standard chemometric methods for the feature selection and classification of spectral data," *BMC Bioinformat*, vol. 10, no. 213, pp. 1-16, Jul. 2009.

[9] G. Louppe, "Understanding random forests," Ph. D. dissertation, University of Liège, liège, Be, Jul. 2014.

[10] Intrusion Detection Evaluation Dataset (CIC-IDS2017) [Internet]. Available: https://www.unb.ca/cic/datasets/ids-2017.html.

진민우(Min-Woo JIN)

2019년 2월 : 원광대학교 전자공학과 졸업
2019년 3월 ~ 현재 : 원광대학교 전자통신공학과 석사과정
※관심분야 : 블록체인 및 부분방전분야

염성관(Sung-Kwan Youm)

2001년 2월 : 고려대학교 전자공학과 (공학석사)
2006년 2월 : 고려대학교 전자공학과(공학박사)
2006년 3월 ~ 2015년 2월 : 삼성전자 책임연구원
2015년 3월 ~ 2018년 2월 : 제주 한라대학교 조교수
2018년 3월 ~ 현재 : 원광대학교 부교수
※관심분야 : 사물인터넷, 빅데이터, 컴퓨터 통신, 인공지능