The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 20, No. 3, pp.1-7, Jun. 30, 2020. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2020.20.3.1
JIIBC 2020-3-1

네트워크 침입탐지를 위한 세션관리 기반의 LSTM 모델

LSTM Model based on Session Management for Network Intrusion Detection

이민욱*

Min-Wook Lee*

요 약 증가하는 사이버공격에 대응하기 위하여 머신러닝을 적용한 자동화된 침입탐지기술이 연구되고 있다. 최근 연구결과에 따르면, 순환형 학습모델을 적용한 침입탐지기술이 높은 탐지성능을 보여주는 것으로 확인되었다. 하지만 단순한 순환형 모델을 적용하는 것은 통신이 중첩된 환경일수록 연관된 통신의 특성을 반영하기 어려워 탐지성능이 저하될 수 있다. 본 논문에서는 이 같은 문제점을 해결하고자 세션관리모듈을 설계하여 LSTM(Long Short-Term Memory) 순환형 모델에 적용하였다. 실험을 위하여 CSE-CIC-IDS 2018 데이터 셋을 사용하였으며, 정상통신비율을 증가시켜 악성통신의 연관성을 낮추었다. 실험결과 통신연관성을 파악하기 힘든 환경에서도 제안하는 모델은 높은 탐지성능을 유지할 수 있음을 확인하였다.

Abstract With the increase in cyber attacks, automated IDS using machine learning is being studied. According to recent research, the IDS using the recursive learning model shows high detection performance. However, the simple application of the recursive model may be difficult to reflect the associated session characteristics, as the overlapping session environment may degrade the performance. In this paper, we designed the session management module and applied it to LSTM (Long Short-Term Memory) recursive model. For the experiment, the CSE-CIC-IDS 2018 dataset is used and increased the normal session ratio to reduce the association of mal-session. The results show that the proposed model is able to maintain high detection performance even in the environment where session relevance is difficult to find.

Key Words : Anomaly Session Inspection, IDS, Long Short-Term Mmemory, Machine Learning

Ⅰ. 서 론

다양한 서비스들이 네트워크 기반으로 연결됨에 따라 네트워크 사이버 위협도 지속해서 증가하고 있다. 보안 전문 업체 Mcafee의 2019년 위협 동향 보고서에 따르면 RDP Brute force, Web Attack, SMB, Webshell 등 다양한 방식을 이용한 네트워크 기반의 사이버공격이 계속하여 급증하고 있음이 확인되었다.[1]

이 같은 네트워크 공격 증가에 대응하기 위해 수동적인 탐지 기술에서 자동적인 탐지 기술 연구로 발전하고

*정회원, 국방과학연구소 기술원
접수일자 2020년 3월 9일, 수정완료 2020년 5월 7일
게재확정일자 2020년 6월 5일

Received: 9 March, 2020 / Revised: 7 May, 2020 / Accepted: 5 June, 2020
*Corresponding Author: zwmin1616@add.re.kr
Dept of Information Security, Agency for Defense Development, Korea

있다. 기존 수동적인 탐지기술 연구로 전통적인 IPS, 방화벽부터 통합로그분석을 위한 SIEM(Secrity Information Event Management) 기술이 있다.[2] 하지만 이 같은 방식은 패턴을 제작하기 위하여 기술자의 전문성뿐만 아니라 많은 시간이 필요하기 때문에 급증하는 네트워크 사이버 공격과 변화하는 대응 환경에 대처하기 어렵다. 반면 머신러닝 모델은 데이터만 정제하면 어떤 분야들 적용이 가능하기에 네트워크 공격 탐지뿐만 아니라, 악성코드 탐지나 데이터유출과 같은 영역에서도 다양하게 연구가 이루어지고 있다.[3][4]

머신러닝을 이용한 연구는 전통적인 모델인 kNN, Naive Bayesian, Random Forest부터 RNN(Recurrent Neural Network)과 LSTM(Logn Short-Term Memory) 등 최신 순환형 학습모델이 적용되어 많은 연구가 이루어졌다.[5][6][7][8][9] 특히 순환형 모델은 네트워크 침입탐지에 있어서 높은 정확도와 탐지율을 보여주어, 통신의 시간 특성이 침입탐지 성능을 높이는데 밀접한 관련이 있음을 보여주었다. 이는 정보수집, 침투, 권한 획득 등 시간 순에 따른 네트워크 사이버 공격의 특징을 순환형 학습모델에 반영하였을 때, 더 높은 탐지 정확도를 얻을 수 있음을 의미한다. 하지만 기존 네트워크 침입탐지 기술에 적용한 순환형 모델은 통신의 시간적인 특성을 온전히 반영하지 못하고 있다.

기존의 순환형 학습모델이 적용된 침입탐지기술은 통신세션을 단순히 시간 순으로 학습하고 있다. 이 같은 방식에 따라 통신세션을 학습할 경우, 서로 관련 없는 세션임에도 영향을 주고 있는 것으로 학습될 수 있고, 반대로 관련 있는 세션의 연관관계가 약하게 학습될 수 있다. 결과적으로 이 같은 현상은 통신이 더욱 많이 중첩된 환경에서 탐지율의 저하 또는 오탐률의 증가를 발생시킬 수 있다.

이를 방지하기 위하여 연관성 있는 세션을 구분하여 학습하는 것이 필요하다. 연관성 있는 세션이란 특정 공격자가 발생시킨 일련의 세션을 의미한다. 본 논문에서는 이를 위해 LSTM 모델에 세션관리모듈을 적용한 SM-LSTM(Session Management based LSTM) 모델을 설계하였다. 세션관리모듈은 동일한 사용자가 발생시킨 일련의 세션을 구분하여 저장하고 출력 시켜 LSTM 모델에 학습시킨다.

본 논문은 총 5장으로 구성되어 있다. 2장은 네트워크 침입탐지 기술에 머신러닝을 적용한 연구사례를 소개하며, 3장에서는 SM-LSTM 모델을 제안한다. 4장은 제안한 모델을 사용하여 실험 및 결과를 분석하고, 5장에서는 결론과 향후 연구과제에 대하여 제시하였다.

II. 관련연구

네트워크 침입탐지에서 머신러닝모델 연구는 적용하고자 하는 통신계층에 따라 구분된다. 네트워크 통신 계층에 따라 활용 가능한 Feature의 범위가 다르므로 어떤 네트워크 계층에서 학습시킬 것인가는 네트워크 침입탐지 연구에서 중요한 부분이다. 네트워크 침입탐지에서 머신러닝에 활용되는 Feature는 Packet 수준의 네트워크 계층과 Session 수준의 전송계층으로 구분할 수 있다.

Packet 계층의 연구는 Chan, P. K., et al.에 의하여 수행되었고, IP, Port, Flag, data size, window size 등 Packet 수준의 Header 정보를 Feature로 활용하여 침입탐지모델을 설계하였다.[10] 또한, Perdisci, R., et al.과 Liu, H., et al., Wang, K.,et al. 는 Packet Header 보다 실질적인 데이터(Payload)에 초점을 맞추어 Payload의 Feature 활용 가능성을 증명하였다.[11][12][13]

Session 계층에서 머신러닝연구는 Zhang, C, et al.과 Chadza, T., et al.에 의해 수행되었었으며, Packet 계층 Feature에 세션시간, 송수신 바이트, 패킷의 송수신 간격 등 Session에서 관측 가능한 메타데이터를 머신러닝 학습에 활용하였다.[14][15] 또한, Yu, Y., et al. 는 Session 계층에서 발생하는 큰 사이즈의 Payload를 부분적으로 학습 시켜 악성통신을 탐지할 수 있음을 증명하였다.[16]

특히 Yin C., et al.은 침입탐지기술에 RNN 모델을 적용하여 시계열 학습모델의 가능성을 확인하였으며,[8] Kim, J., et al.은 RNN의 장기간 통신에 대한 학습 영향력 약화(Vanishing Problem) 문제를 해결하기 위하여 LSTM을 적용하여 98.88% 탐지율과 96.93% 정확도의 성능을 보여주었다.[9]

침입탐지에 대한 머신러닝 적용은 Packet 계층에서 Session 계층으로 확대되었으며, 비순환형 학습모델보다 순환형 학습모델을 적용하였을 때 더욱 효과적인 침입탐지가 가능한 것이 확인되었다. 하지만 기존 순환형 학습모델은 통신의 시간특성을 반영하였으나, 각 통신의 주체에 대해서는 구분하고 있지 않다. 결국 이것은 정상통신이 중첩된 환경에서 서로 다른 통신이 연관된 것으로 오학습 시킬 수 있고, 간헐적으로 발생하는 악성통신 간에 연관성을 잃어 탐지성능이 저하될 수 있다. 따라서 본 논문에서는 수많은 통신세션이 공존하는 환경에서도 연관된

세션을 구분하여 성능저하를 방지할 수 있는 SM-LSTM을 제안한다.

Ⅲ. 네트워크 침입탐지를 위한 세션관리 LSTM 모델

1. SM-LSTM(Session Management based LSTM)

SM-LSTM은 기존 LSTM 모델에 세션관리모듈을 추가한 모델이다. 새로운 세션이 입력되었을 때, 입력된 세션은 세션관리모듈에 저장된 뒤 LSTM 학습을 위해 출력된다. 그림 1은 SM-LSTM의 전체적인 동작과정을 도식화한 그림이다. 세션관리모듈은 새로운 세션을 입력받고, 서로 연관된 세션끼리 구분되어 저장된다. 저장이 완료되면 연관된 세션을 함께 출력하여 LSTM 모델에 입력(학습)시키고, 악성여부를 출력한다. 이 같은 방식으로 서로 관련 있는 일련의 세션을 차례대로 학습시킴으로써 관련 없는 세션이 서로 미칠 수 있는 영향을 최소화하고, 연관 세션의 영향력을 강화하였다. 세션관리모듈과 LSTM의 구체적인 구조와 동작 방식은 3.2절과 3.3절에서 설명한다.

2. 세션관리모듈

세션관리모듈은 특정 IP에서 발생한 일련의 세션을 관리하여 서로 관계있는 세션만 모아주는 역할을 한다. 세션관리모듈은 세션을 저장하는 Session Storage가 존재하며, Storage 내부는 Session Array로 구성된다. Array는 서로 연관된 세션의 Feature를 저장한다. 또한 관리하는 세션을 구분하기 위하여 Array는 각각 Header를 보유하고 있다. Header에는 출발지 IP, 목적지 IP, 목적지 Port가 기록되어있어, 새로운 세션이 유입되었을 때 Header 정보로 연관 Array를 찾아 유입된 세션을 저장할 수 있다.

그림 2는 세션관리모듈의 동작과정과 Session Storage를 도식화한 그림이다. 새로운 세션이 입력되면, Session Storage에서 Session Array를 검색한다. 입력된 세션의 출발지 IP, 도착지 IP, 도착지 Port와 동일한 Array가 존재할 경우, 해당 Array에 유입된 세션의 Feature를 추가한다. 만약, Session Array가 가득 찰 경우 Array에 저장된 Feature를 삭제하고 신규 세션의 Feature를 저장한다. 삭제할 Feature는 현재 유입된 Feature와 시간적인 연관성이 가장 떨어지는 오래된 Feature이다. 저장이 완료된 후 Array에 저장된 Feature는 학습을 위하여 순차적으로 출력된다. 이 같은 과정을 통해 세션관리모듈은 서로 다른 통신세션이 섞인 환경에서도 연관된 세션을 하나로 묶어 학습을 강화할 수 있다.

3. LSTM(Long Short-Term Memory) 학습모델

LSTM은 Hochreiter와 Schmidhuber에 의해 제안된 학습모델이다.[17] LSTM은 기존 RNN의 긴 의존 기간의 문제점을 해결하기 위하여 개발되었다. LSTM은 각각의 학습 단계를 의미하는 Cell이 있으며, Cell 내부에는 입력, 삭제, 출력 함수가 존재하여 학습된 데이터가 언제 삭제될 것인지 모델링할 수 있다.

본 논문에서는 기존 LSTM 모델을 차용하였으며, 네

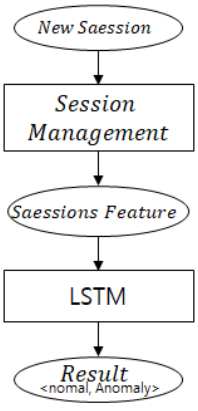


그림 1. SM-LSTM 탐지 흐름도
Fig. 1. SM-LSTM Detection Flow

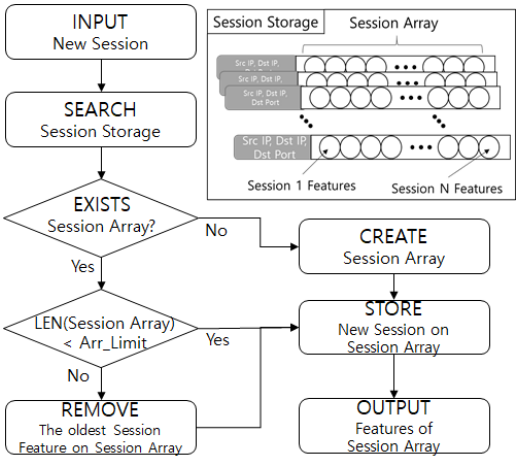


그림 2. 세션관리모듈
Fig. 2. Session Management

트워크 Feature를 학습할 수 있게 학습 데이터 입력 값을 변경하여 구성하였다. 그림 3은 LSTM의 구조를 보여주고 있다. Cell의 입력 값으로 〈이전 상태 값(C_{t-1})〉, 〈이전 결과 값(h_{t-1})〉, 〈현재 학습 데이터(x_t)〉를 입력받는다. 현재 학습 데이터는 단일 세션의 Feature값을 의미한다. 세션관리모듈에서 출력된 세션들의 Feature가 시간 순으로 각 Cell의 학습데이터로 입력된다. 탐지 결과 값은 마지막 Cell에서 출력된 값을 사용한다.

Cell은 〈결과 값(h_t)〉과 〈현재 상태 값(C_t)〉을 출력한다. 각각의 값은 Input Gate(i_t)와 Forget Gate(f_t), Output Gate(o_t) 함수에 의해 생성되며, 각 Gate는 bias(b), Weight(W)로 구성된 Sigmoid(σ) 함수이다.

$$f_t = \sigma(W_f \bullet [h_{t-1}, x_t] + b_f) \quad (1)$$

$$i_t = \sigma(W_i \bullet [h_{t-1}, x_t] + b_i) \quad (2)$$

$$o_t = \sigma(W_o \bullet [h_{t-1}, x_t] + b_o) \quad (3)$$

〈현재 상태 값(C_t)〉과 〈출력 값(h_t)〉은 (4)~(6) 수식에 의해 계산된다. 〈현재 상태 값(C_t)〉은 Forget Gate와 Input Gate 비율에 따른 〈중간 상태 값($\widetilde{C_t}$)〉과 〈과거 상태 값(C_{t-1})〉의 합으로 결정되며, 〈출력 값(h_t)〉는 $\tanh(C_t)$ 와 Output Gate(o_t) 값의 곱으로 결정된다.

$$\widetilde{C_t} = \tanh(W_C \bullet [h_{t-1}, x_t] + b_C) \quad (4)$$

$$C_t = f_t * C_{t-1} + i_t * \widetilde{C_t} \quad (5)$$

$$h_t = o_t * \tanh(C_t) \quad (6)$$

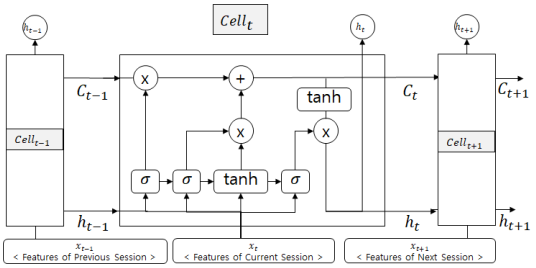


그림 3. LSTM 모델 구조
Fig. 3. LSTM Model Architecture

Ⅳ. 실험 및 결과

4장에서는 세션관리를 통해 순환형 학습모델의 성능 저하를 방지할 수 있음을 증명하기 위한 실험을 수행하였다. 이를 위해 정상 통신 비율을 서로 다르게 구성한 데이터 셋을 생성하였으며, 생성된 데이터 셋을 사용하여 기존 학습모델과 제안하는 SM-LSTM 모델의 성능을 비교하는 실험을 수행하였다.

1. 실험 데이터 셋 및 Feature 소개

SM-LSTM 모델의 테스트를 위하여 케나다 사이버보안연구소에서 제공하는 CSE-CIC-IDS 2018의 데이터 셋을 활용하였다.[18] 전체 데이터 셋에서 세션 기반의 침입탐지 모델에 적합한 네트워크 공격 데이터를 선정하였고, 선정된 네트워크 데이터에 정상 통신 비율을 조정하여 Original 데이터 셋과 Noise 데이터 셋을 생성하였다.

IDS 2018 데이터 셋의 원본 데이터는 DoS, Brute Force, Web attack , Infiltration attack, DDoS로 공

표 1. 실험 & 테스트 데이터 셋
Table 1. Train & Test Dataset

Category		Original Dataset (Train / Test)	Noise Dataset (Train / Test)	Description
Normal		3786027 / 420670	37860273 / 4206697	Normal Dataset Count
Mal	Web Attack	342854 / 38095		Web Attack Dataset Count (SQL Injection, XSS, Web Based Brute Force etc.)
	Brute Force	588870 / 65430		Brute Force Dataset Count (SSH, FTP Brute Force)
	DoS	835 / 93		DoS Attack Dataset Count (Hulk, Slowloris etc.)
Mal Data Ratio		20%	2%	Malicious Data(Web Attack, Brute Force, DoS) Ratio compared with Normal Data

격 카테고리가 구성되어있다. 이 중 세션 기반의 공격 방식인 Web Attack, Bruete Force, DoS 데이터를 선정하였다.

다음 선정한 데이터에 정상 통신세션을 추가하였다. 전혀 다른 양상을 보이는 통신세션을 추가할 경우 잘못된 학습과 탐지결과를 보일 수 있다. 따라서 기존 데이터 셋에 존재하는 정상 값의 범위를 측정한 뒤, 해당 범위 내에서 정상 값과 동일하거나 유사한 값을 생성하였다. Feature의 속성에 따라 Port, Protocol 등 원본 데이터와 동일해야하는 Feature값은 유지하였고, 전송바이트, 초당 전송 패킷 등 변경 가능한 Feature 값에 대해서만 정상범위 내로 변경하여 생성된 데이터의 신뢰성과 원본 데이터와의 유사성을 높였다. 생성한 데이터를 원본 데이터 셋에 추가하였으며, 공격세션이 전체 데이터 셋에서 균일하게 분포하되, 순서는 동일하도록 데이터 셋을 구성하였다. 최종적으로 생성된 데이터 셋을 학습용과 테스트용 데이터 셋으로 분리하였다. 이 같은 과정에 따라 생성된 데이터 셋은 표 1과 같다. 최종적으로 Original Dataset에는 20%의 높은 빈도로 공격 데이터가 포함되어있으며, Noise Dataset에는 2%로 낮은 빈도로 공격 데이터가 포함되어있다.

마지막으로 데이터 셋에서 학습에 사용될 Feature와 세션관리를 위한 Feature를 선정하였다. 출발지 IP, 목적지 IP와 목적지 Port는 세션관리를 위한 Feature로 선정하였으며, 학습을 위한 Feature는 Sung, A. H., et al. 이 제안하는 Feature[19] 중 5개를 선정하였다. 선정된 Feature는 source bytes(출발지에서 보낸 데이터 크기, flag(연결 에러 등의 상태 값), rerror_rate(서버 거부 에러), service(ftp, http 등), dst_host_diff_srv_rate (다른 서비스에 접근한 비율)이다.

2. 실험 및 결과

구성된 Original 및 Noise 데이터 셋을 사용하여 SM-LSTM을 포함한 총 6개의 모델을 실험하였다. 비교군 학습모델은 비순환형 학습모델 kNN, NB(Naive Bayesian), RF(Random Forest)과 순환형 학습모델 RNN, LSTM을 선정하였다. 모델의 성능변화를 관측하기 위하여 (7)~(8) 수식에 따라 모델의 정탐률(DR), 오탐률(FAR), 정확도(Accuracy)를 측정하였다.

$$DR = \frac{TP}{TP + FN} \tag{7}$$

$$FAR = \frac{FP}{TN + FP} \tag{8}$$

$$Accuracy = \frac{TP + TN}{FP + FN + TP + TN} \tag{9}$$

$$TP: True Positive, TN: True Negative$$
$$FP: False Positive, FN: False Negative$$

표 2는 전체 실험결과를 보여주고 있다. 비교를 위하여 Noise Dataset 실험결과 하단에 Diff를 추가하였다. Diff 값은 Original 데이터 셋 실험결과 값과 비교하여 Noise 데이터 셋 실험결과 값이 증가되었거나 감소된 수치를 의미한다.

Original 및 Noise 데이터 셋의 통신 특징에 따라 비

표 2. 실험결과
Table 2. Experiment Result

Model	Original Dataset			Noise Dataset		
	DR(%)	FAR(%)	Accuracy(%)	DR(%) (Diff)	**FAR(%) (Diff)**	Accuracy(%) (Diff)
kNN	71.37	37.15	69.69	72.04 (0.68)	39.31 (2.15)	71.77 (2.09)
NB	76.50	56.15	70.05	75.87 (-0.63)	57.32 (1.17)	75.08 (5.03)
RF	82.59	24.04	81.28	80.73 (-1.86)	23.66 (-0.38)	80.62 (-0.66)
RNN	85.15	15.45	85.03	86.70 (1.55)	28.37 (12.93)	86.34 (1.31)
LSTM	90.52	16.24	89.18	87.98 (-2.54)	**31.88 (15.64)**	87.50 (-1.68)
SM-LSTM	89.66	15.25	88.69	89.69 (0.02)	**16.12 (0.87)**	89.55 (0.86)

순환형 학습모델과 순환형 학습모델은 서로 다른 결과를 보여주었다. 비순환형 학습 모델(kNN, NB, RF)에서는 데이터 셋 특징에 따라 성능에 변화가 없었으나, 순환형 학습모델(RNN, LSTM)에서는 오탐률 증가로 인한 성능 저하가 발생된 것을 확인할 수 있었다. 반면, 본 논문에서 제안하는 SM-LSTM 모델은 순환형 학습모델을 이용함에도 연관된 세션을 구분하여 학습시킴으로써 높은 탐지 성능을 유지할 수 있음을 확인하였다.

V. 결 론

본 논문에서는 연관된 세션을 고려하지 않은 학습모델에서 발생하는 침입탐지 성능저하를 실험하였고, 이를 방지하기 위한 SM-LSTM 모델을 제안하여 성능을 검증하였다. 실험을 위하여 데이터 셋에 정상세션 비율을 높이고, 정상세션들 간에 공격세션이 균일하게 분포되도록 구성하였다. 이같이 통신 중첩이 증가된 환경에서 일반적인 순환형 학습모델은 연관된 세션을 제대로 학습하지 못하고, 오탐률 증가로 인한 성능저하가 발생하였다. 반면, SM-LSTM은 세션관리를 통해 공격세션에 서로 다른 세션이 섞이더라도 높은 탐지성능을 유지하는 것에 성공하였다.

향후 연구로는 세션관리와 학습 Feature에 관한 최적화 연구가 필요하다. 또한, 정상통신이 많은 일반적인 네트워크 서비스 환경에서 SM-LSTM모델을 실험하여 실제 서비스 환경이 탐지성능에 미치는 영향에 대해 연구가 필요하다.

References

[1] Christiaan Beek, Taylor Dunton, John Fokker, Steve Grobman, Tim Hux, Tim Polzer, Marc Rivero Lopez, Thomas Roccia, Jessica Saavedra-Morales, Raj Samani,Ryan Sherstobitof, ,McAfee Labs Thread Report 2019, Aug 2019
DOI:https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

[2] Um, J.G., Kwon, H. Y., "Model Proposal for Detection Method of Cyber Attack using SIEM", The journal of the institute of internet, broadcasting and communication(JIIBC), vol. 16, no. 6, pp. 43-54, Dec. 2016.
DOI: http://dx.doi.org/10.7236/JIIBC.2016.16.6.43

[3] Jeon, D. J., Park, D.G., "Real-time Linux Malware Detection Using Machine Learning," The Journal of Korean Institute of Information Technology(JKIIT), vol. 17, no. 7, pp. 111-122, Jul. 2019.
DOI: http://dx.doi.org/10.14801/jkiit.2019.17.7.111

[4] Lim, W. G., Kwon, K. H., Kim, J. J., Lee, J. E., Cha, S. H., "Comparison and Analysis of Anomaly Detection Methods for Detecting Data Exfiltration" Journal of the Korea Academia Industrial cooperation Society(JKAIS), vol. 17, no. 9, pp. 440-446, Sep. 2016.
DOI: http://dx.doi.org/10.5762/KAIS.2016.17.9.440

[5] Muda, Z., Yassin, W., Sulaiman, M. N., & Udzir, N. I., A K-Means and Naive Bayesian learning approach for better intrusion detection. Information technology journal, 10(3), pp. 648-655, 2011
DOI: https://doi.org/10.3923/itj.2011

[6] Liao, Yihua, and V. Rao Vemuri, Use of k-nearest neighbor classifier for intrusion detection, Computers & Security 21.5, pp.439-448, 2002.
DOI : https://doi.org/10.1016/S0167-4048(02)00514-X

[7] Farnaaz, N., & Jabbar, M. A. Random forest modeling for network intrusion detection system. Procedia Computer Science, 89(1), pp. 213-217. 2016.
DOI: https://doi.org/10.1016/j.procs.2016.06.047

[8] Yin, C., Zhu, Y., Fei, J., & He, X. A deep learning approach for intrusion detection using recurrent neural networks. Ieee Access, 5, pp. 21954-21961, 2017.
DOI: https://doi.org/10.1109/ACCESS.2017.2762418

[9] Kim, J., Kim, J., Thu, H. L. T., & Kim, H, Long Short-Term memory recurrent neural network classifier for intrusion detection. In 2016 International Conference on Platform Technology and Service (PlatCon) pp. 1-5, Feb, 2016.
DOI: https://doi.org/10.1109/PlatCon.2016.7456805

[10] Chan, P. K., & Mahoney, M. V. Detecting Novel Attacks by Identifying Anomalous Network Packet Headers. Florida Tech., 2001
DOI: http://hdl.handle.net/11141/87

[11] Perdisci, R., Ariu, D., Fogla, P., Giacinto, G., & Lee, W. McPAD: A multiple classifier system for accurate payload-based anomaly detection. Computer networks, 53(6), pp. 864-881, 2009.
DOI: https://doi.org/10.1016/j.comnet.2008.11.011

[12] Liu, H., Lang, B., Liu, M., & Yan, H. CNN and RNN based payload classification methods for attack detection. Knowledge-Based Systems, 163, pp. 332-341. 2019.
DOI: https://doi.org/10.1016/j.knosys.2018.08.036

[13] Wang, K., & Stolfo, S. J. Anomalous payload-based network intrusion detection. In International workshop on recent advances in intrusion detection pp. 203-222. Sep, 2004.
DOI: https://doi.org/10.1007/978-3-540-30143-1_11

[14] Zhang, C., Ruan, F., Yin, L., Chen, X., Zhai, L., & Liu, F. A Deep Learning Approach for Network Intrusion

Detection Based on NSL-KDD Dataset. In 2019 IEEE 13th International Conference on Anti-counterfeiting, Security, and Identification (ASID) pp. 41-45. Oct, 2019.
DOI: https://doi.org/10.1109/ICASID.2019.8925239

[15] Chadza, T., Kyriakopoulos, K. G., & Lambotharan, S. Contemporary Sequential Network Attacks Prediction using Hidden Markov Model. In 2019 17th International Conference on Privacy, Security and Trust (PST) pp. 1-3, Aug 2019.
DOI: https://doi.org/10.1109/PST47121.2019.8949035

[16] Yu, Y., Long, J., & Cai, Z. Session-based network intrusion detection using a deep learning architecture. In International Conference on Modeling Decisions for Artificial Intelligence, pp. 144-155. Oct, 2017.
DOI: https://doi.org/10.1007/978-3-319-67422-3_13

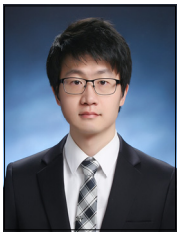
[17] Hochreiter, S., & Schmidhuber, J. Long short-term memory. Neural computation, 9(8), pp. 1735-1780. 1997.
DOI: https://doi.org/10.1162/neco.1997.9.8.1735

[18] Communications Security Establishment & Canadian Institute for Cybersecurity ,CSE-CIC-IDS2018 DATASET,
https://www.unb.ca/cic/datasets/ids-2018.html

[19] Sung, A. H., Mukkamala, S. The feature selection and intrusion detection problems. In Annual Asian Computing Science Conference, pp. 468-482. Dec, 2004.
DOI: https://doi.org/10.1007/978-3-540-30502-6_34

저 자 소 개

이 민 욱(정회원)



- 2014년 : 경기대학교 전자공학과 졸업 (이학사)
- 2016년 : 고려대학교 정보보호대학원 정보보호학과 졸업(공학석사)
- 2017년 ~ 현재 : 국방과학연구소 기술원