J. Internet Comput. Serv.
ISSN 1598-0170 (Print) / ISSN 2287-1136 (Online)
http://www.jics.or.kr

알려지지 않은 위협 탐지를 위한 CBA와 OCSVM 기반 하이브리드 침입 탐지 시스템☆

A hybrid intrusion detection system based on CBA and OCSVM for unknown threat detection

신 건 윤[1] 김 동 욱[1] 윤 지 영[2] 김 상 수[3] 한 명 묵[2*]
Gun-Yoon Shin Dong-Wook Kim Jiyoung Yun Sang-Soo Kim Myung-Mook Han

요 약

인터넷이 발달함에 따라, IoT, 클라우드 등과 같은 다양한 IT 기술들이 개발되었고, 이러한 기술들을 사용하여 국가와 여러 기업들에서는 다양한 시스템을 구축하였다. 해당 시스템들은 방대한 양의 데이터들을 생성하고, 공유하기 때문에 시스템에 들어있는 중요한 데이터들을 보호하기 위해 위협을 탐지할 수 있는 다양한 시스템이 필요하였으며, 이에 대한 연구가 현재까지 활발히 진행되고 있다. 대표적인 기술로 이상 탐지와 오용 탐지를 들 수 있으며, 해당 기술들은 기존에 알려진 위협이나 정상과는 다른 행동을 보이는 위협들을 탐지한다. 하지만 IT 기술이 발전함에 따라 시스템을 위협하는 기술들도 점차 발전되고 있으며, 이러한 탐지 방법들을 피해서 위협을 가한다. 지능형 지속 위협(Advanced Persistent Threat : APT)은 국가 또는 기업의 시스템을 공격하여 중요 정보 탈취 및 시스템 다운 등의 공격을 수행하며, 이러한 공격에는 기존에 알려지지 않았던 악성코드 및 공격 기술들을 적용한 위협이 존재한다. 따라서 본 논문에서는 알려지지 않은 위협을 탐지하기 위한 이상 탐지와 오용 탐지를 결합한 하이브리드 침입 탐지 시스템을 제안한다. 두 가지 탐지 기술을 적용하여 알려진 위협과 알려지지 않은 위협에 대한 탐지가 가능하게 하였으며, 기계학습을 적용함으로써 보다 정확한 위협 탐지가 가능하게 된다. 오용 탐지에서는 Classification based on Association Rule(CBA)를 적용하여 알려진 위협에 대한 규칙을 생성하였으며, 이상 탐지에서는 One Class SVM(OCSVM)을 사용하여 알려지지 않은 위협을 탐지하였다. 실험 결과, 알려지지 않은 위협 탐지 정확도는 약 94%로 나타난 것을 확인하였고, 하이브리드 침입 탐지를 통해 알려지지 않은 위협을 탐지 할 수 있는 것을 확인하였다.

☞ 주제어 : 알려지지 않은 위협, 하이브리드 침입 탐지, 연관 규칙 기반 분류, 단일 클래스 서포트 벡터 머신

ABSTRACT

With the development of the Internet, various IT technologies such as IoT, Cloud, etc. have been developed, and various systems have been built in countries and companies. Because these systems generate and share vast amounts of data, they needed a variety of systems that could detect threats to protect the critical data contained in the system, which has been actively studied to date. Typical techniques include anomaly detection and misuse detection, and these techniques detect threats that are known or exhibit behavior different from normal. However, as IT technology advances, so do technologies that threaten systems, and these methods of detection. Advanced Persistent Threat (APT) attacks national or companies systems to steal important information and perform attacks such as system down. These threats apply previously unknown malware and attack technologies. Therefore, in this paper, we propose a hybrid intrusion detection system that combines anomaly detection and misuse detection to detect unknown threats. Two detection techniques have been applied to enable the detection of known and unknown threats, and by applying machine learning, more accurate threat detection is possible. In misuse detection, we applied Classification based on Association Rule(CBA) to generate rules for known threats, and in anomaly detection, we used One-Class SVM(OCSVM) to detect unknown threats. Experiments show that unknown threat detection accuracy is about 94%, and we confirm that unknown threats can be detected.

☞ keyword : Unknown Threat, Hybrid Intrusion Detection, Classification based on Association Rule, One-Class SVM

1 Department of Computer Engineering, Gachon University, Sungnam-si, 13120, Korea.
2 Department of Software, Gachon University, Sungnam-si, 13120, Korea.
3 Agency for Defense Development, Songpa P.O Box 132, Seoul, 05661, Korea.

* Corresponding author (mmhan@gachon.ac.kr)
[Received 12 March 2021, Reviewed 3 May 2021(R2 2 June 2021), Accepted 10 June 2021]
☆ 이 논문은 2020년도 한국인터넷정보학회 추계학술대회 (최)우수 논문 추천에 따라 확장 및 수정된 논문임.
☆ 이 논문은 2018년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(NRF-2018R1D1A1B07050864).
☆ 이 논문은 국방과학연구소 지원을 받아 수행된 연구임(UD200020ED)

1. 서 론

IT 기술이 발전함에 따라 소셜 네트워크, IoT, 보안 등 다양한 분야에서 IT 기술을 사용하고 있으며, 특히 최근 활발한 연구가 진행되고 있는 기계학습과 인공지능을 접목한 기술들이 점차 많아지고 있다. 이처럼 IT 기술의 발전은 우리들에게 다양한 이점을 안겨주었지만, 반대로 이를 악용한 기술들 또한 많아지고 있다. 대표적인 공격으로 제로 데이 공격이 있으며, 해당 공격은 네트워크 시스템 방어자를 포함하여 대중적으로 알려지지 않은 취약점을 찾아 공격한다. 이처럼 발전된 IT기술을 악용하여 공격에 적용하는 방법은 컴퓨터 네트워크 보안에서 꾸준히 연구되어야 하는 주요 도전과제라고 할 수 있다[1].

알려지지 않은 위협은 제로 데이 공격과 같이 기존의 파악하지 못했던 취약점, 시스템의 허점, 탐지 기술로 탐지되지 않는 부분 등을 찾아 공격을 수행하는 방법과 같은 새로운 위협을 포함한 방어자가 이전에 알지 못했던 다양한 공격 방법, 악성코드 및 취약점을 의미하며, 이러한 알려지지 않은 위협은 기존 위협들과 다른 악성 행위를 하기 때문에 구축되어 있는 탐지 시스템에서 정확하게 탐지하기 어렵다.

침입 탐지 시스템은 의심스러운 행위나 알려진 위협에 대한 알람을 생성한다[2]. 침입 탐지 시스템의 목표는 컴퓨터 시스템에 있는 비정상적인 행위를 탐지하는 것이고, 최근에는 기계학습과 데이터 마이닝을 적용한 침입 탐지 방법이 연구되고 있다. 침입 탐지는 이상 탐지와 오용 탐지 그리고 이 두 가지 방식을 혼합한 하이브리드 방식으로 구분할 수 있다. 이상 탐지는 정상 행위를 학습한 시스템에 새로운 데이터가 입력되었을 때 시스템이 가지고 있는 정상 정보의 기준을 근거로 새로운 데이터가 정상인지 이상인지를 판단한다. 이상 탐지에서는 군집화 또는 분류에서 2-class 문제(0 또는 1)에 적용할 수 있는 기계학습 방법이 사용된다. 오용 탐지는 기존에 알려진 공격들을 기반으로 시그니처 또는 규칙을 생성하고, 새로운 데이터에 이를 대조하여 매칭이 되는 지를 확인한다. 오용 탐지에서는 분류 문제에 적용할 수 있는 기계학습 방법들이 자주 사용된다. 이상 탐지는 새롭거나 알려지지 않은 공격을 탐지하기에 적합하나, 정상 데이터와 유사한 공격을 탐지하기 어렵고 거짓 알람이 많고, 오용 탐지는 시그니처 또는 규칙을 생성하기 때문에 거짓 알람이 적으나, 오직 알려진 공격만 탐지할 수 있다.

하이브리드 탐지는 이상 탐지와 오용 탐지를 결합하여 공격을 탐지하는 방법으로, 이상 탐지와 오용탐지가 가지고 있는 문제점을 해결하기 위해 제안되었다. 이를 통해 이상 탐지가 가지고 있는 거짓 알람이 많이 발생한다는 문제와 오용 탐지가 가지고 있는 알려진 공격만 탐지하는 문제점을 해결하고자 하였으며, 기계학습과 데이터 마이닝을 적용하여 고도화 하고자 하였다.

따라서 본 연구에서는 알려지지 않은 위협을 탐지하기 위한 하이브리드 침입 탐지 시스템을 제안한다. 오용 탐지에서는 CBA를 사용하여 알려진 위협에 대한 규칙을 생성하고, 이를 사용자에게 제공함으로써 알려진 위협에 대한 탐지를 수행 및 정확한 규칙이 생성되었는지를 사용자가 확인할 수 있게 하였다. 또한 이상 탐지에서는 OCSVM을 사용하여 정상과 섞여있는 알려지지 않은 위협을 탐지한다. 하이브리드 침입 탐지를 적용함으로써, 기존의 알려진 위협과 알려지지 않은 위협을 전부 탐지할 수 있게 하였다.

본 논문에서 제안하는 방식이 기여하는 바는 다음과 같다. 1) 하이브리드 침입 탐지 기반 알려지지 않은 공격 탐지 프레임워크를 제안한다. 하이브리드 방법을 적용하여 오용 및 이상 탐지가 가지고 있는 단점을 극복하였다. 2) 실제 네트워크 환경을 기반으로 생성된 IDS-2018 데이터 셋을 사용하여 제안하는 방법이 실제 환경에서 적용 가능함을 보였다. 실험을 통해 정확도를 확인하였고, 이를 통해 실제 환경에서도 사용 가능함을 증명하였다.

2. 관련 연구

2.1 하이브리드 침입 탐지

기존에 제안한 침입 탐지 방법들은 알려지지 않은 공격을 탐지하기 위해 이상 행위 식별, 공격 및 정상 규칙 생성 등과 같은 방법을 제안하였다. 하지만 대부분의 침입 탐지들은 알려지지 않은 위협을 탐지하는데 있어, 많은 거짓 알람을 생성하고 이로 인해 탐지 정확도가 낮았다. 이러한 문제를 극복하기 위해 하이브리드 침입 탐지가 제안되었다. 하이브리드 침입 탐지는 이상 탐지와 오용 탐지가 가지고 있는 문제점을 상호 보완하여 알려지지 않은 공격을 탐지하기 위해 제안된 방법으로 이상 탐지가 가지고 있는 많은 수의 거짓 알람 생성과 오용 탐지가 가지고 있는 알려진 공격만을 탐지하는 문제를 해결하고자 하였다.

[2]에서는 하이브리드 방식인 Decision Tree(DT)와 Support Vector Machine(SVM)을 이용한 하이브리드 침입

탐지 시스템을 제안했다. C5를 사용하여 고차원 데이터를 효과적으로 다룰 수 있게 하였고, SVM을 통해 알려지지 않은 위협을 탐지하였다. [3]에서는 DT와 SVM을 이용한 하이브리드 침임 탐지 시스템을 통해 알려지지 않는 위협을 탐지하는 시스템을 제안하였다. 트래픽을 캡쳐해 의미있는 특징들을 추출하고 DT를 통해 기존 공격에 포함되는지를 확인하였다. SVM을 통해 알려지지 않은 위협과 정상으로 분류하였다. [4]에서는 위협과 관련된 프로필을 생성하여 탐지를 수행하는 오용 탐지 부분과 1-NN을 이용한 이상 탐지를 결합한 방법을 제안하였다. 오용 탐지에서는 조건부 엔트로피를 이용해 과거 데이터로부터 위협들의 프로필을 생성하여 새로 들어오는 데이터와 매칭하였고, 매칭이 완전하지 않을 경우 1-NN 기반 이상 탐지를 수행하였다. [5]에서는 DT를 이용해 오용 탐지를 하고 SVM을 이용해 이상탐지를 하는 프레임워크를 제안했다. DT를 사용하여 알려진 위협에 대한 규칙을 생성하고, SVM을 사용하여 정상 데이터에 대한 바운더리를 생성하여 알려지지 않은 위협을 분류하였다. [6]에서는 CART를 사용해 규칙을 생성해 알려진 공격을 분류하고 Extreme Learning Machine(ELM)을 이용해 정상과 비정상을 분류하는 모델을 제안하였다. [7]에서는 SVM과 ELM을 사용한 하이브리드 침입탐지 시스템을 제안했다. 일반적인 하이브리드 침입 탐지 시스템의 두 단계 탐지가 아닌 5단계 분류기를 구축하여 알려지지 않은 공격 탐지를 하였다.

2.1.1 Classification based on Association Rule

CBA는 연관 규칙을 분류(Classification) 문제에 적용하기 위한 방법으로 분류 문제에 존재하는 클래스에 적합한 규칙을 찾는 것을 의미한다. 연관 규칙을 분류 문제에 적용함으로써 분류에 대한 성능을 향상시킨다. CBA는 먼저 모든 클래스에 대한 연관 규칙을 생성하고, 생성된 규칙을 기반으로 분류기를 구축한다. 생성되는 규칙은 조건문과 그에 따른 클래스로 구성되어 있다. 조건문에서는 특징과 그에 대한 조건이 포함되어 있고, 그 다음 조건문들에 부합하는 클래스에 대해서 명시되어 있다. 이때 조건문들의 경우 'or'이 아닌 'and'로 적용되기 때문에 모든 조건에 부합해야지만 해당 클래스로 정의된다.

최적화된 규칙과 높은 성능의 정확도를 얻기 위해서는 최소 지지도(minimum support)와 최소 신뢰도(minimum confidence)라는 파라미터를 사용자가 설정하여 분류에 적합하지 않는 규칙이 정의되는 것을 방지하여야 한다. 아이템 빈도수 기반의 Apriori 방법을 적용하여 분류를 수행하기도 하고[8], 다중 클래스 분류를 하기 위해 Rule Ranking을 적용한 방법[9], 규칙 중복 방지와 충돌 방지를 위해 정보 이득(Information Gain)을 적용한 방법[10] 등이 있다.

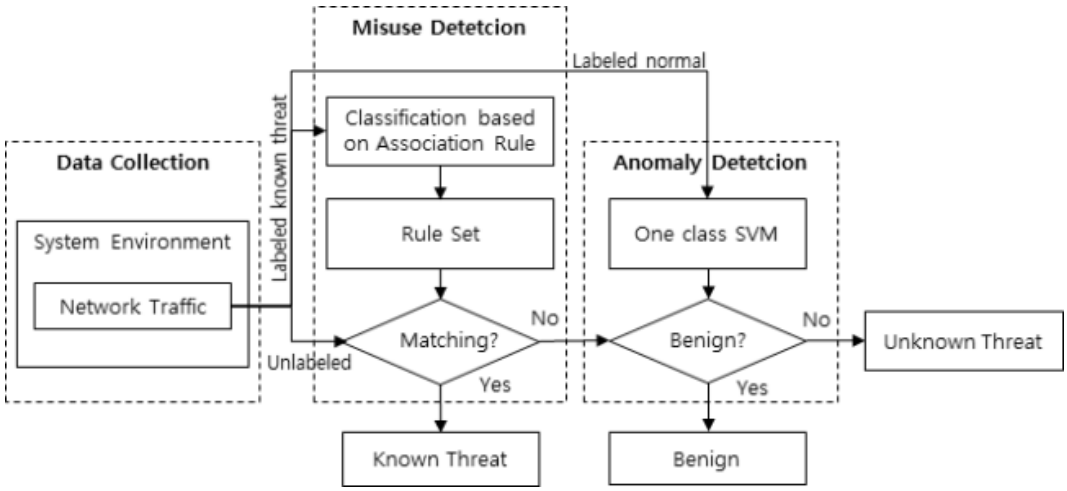
2.1.2 One-Class SVM(OCSVM)

OCSVM은 이상 탐지에서 자주 사용되는 지도 학습 방법으로, 비선형 커널 함수를 이용하여 주어진 데이터를 특징 공간에 매핑하고, 데이터가 존재하는 공간을 서포트 벡터라고 정의한다. 정의된 영역은 결정 경계가 생성되고, 결정 경계 안의 데이터들은 정상으로, 경계 밖의 데이터들은 비정상 또는 아웃라이어(Outlier)로 간주하게 된다[11]. 이상 탐지에서 이와 유사한 방식으로 사용되는 방법으로는 Isolation Forest나 Histogram-based Outlier Score(HBOS)등이 존재한다. [12]에서는 이메일에 존재하는 이상 행위를 탐지하기 위해 OCSVM을 사용하였으며, Polynomial, Radial basis, STIDE와 Markov Chain 등의 커널 비교를 통한 탐지 성능을 확인하였다. 또한 OCSVM의 경우, 알려지지 않은 위협을 탐지하는데 있어 단일로 사용되기 보다는 오용 탐지에서는 식별할 수 없는 알려지지 않은 위협을 탐지하기 위한 이상 탐지에 사용하기 위해 주로 사용되었다[2,3,5,7].

2.2 알려지지 않은 위협 탐지

알려지지 않은 위협 탐지는 이전에 보지 못했던 위협과 이와 관련된 데이터들을 탐지하는 것을 의미한다. 탐지를 통해 알려지지 않은 위협이 기존의 어떤 위협과 유사한지를 식별하거나, 그렇지 않다면 알려지지 않은 위협이 가지고 있는 특성을 확인한다. 이와 관련된 방법으로 이상 탐지가 있으며, 해당 방식에서는 알려지지 않은 위협이 정상과 얼마나 다른지, 다른 위협들과 얼마나 유사한지 또는 어떤 차이가 있는 지 등을 탐지한다.

알려지지 않은 위협 탐지에 대한 연구 방법은 크게 2가지 방법으로 나뉜다. 첫 번째 방법은 알려지지 않은 위협 또는 변종을 생성하고 탐지를 수행하는 방법으로 일반적으로 Generative Adversarial Network(GAN)을 통해 위협을 생성한다. 해당 방법은 알려지지 않은 위협을 생성하기 때문에 기존에 수집된 위협과는 다른 알려지지 않은 위협을 식별하고 탐지할 수 있다는 장점을 가지고 있지만, 알려지지 않은 위협을 생성하는 것이 어렵고 생성



(그림 1) 제안하는 알려지지 않은 위협 탐지 시스템
(Figure 1) Proposed Unknown Threat Detection System

된 위협이 실제적으로 악의적인 행위를 수행하지 않을 수도 있다는 문제점을 가지고 있다. 즉, 생성된 위협이 데이터로써는 다른 위협 데이터와 유사하지만 생성된 위협을 실제 네트워크 시스템에 올려놓고 악성 행위를 하는지를 확인해보면 악성 행위를 수행하지 않을 수도 있다는 것이다.

두 번째 방법으로는 수집한 데이터 셋의 특정 클래스를 알려지지 않은 위협으로 정의하는 방법이다. 해당 방법은 대부분의 연구에서 적용하는 방법으로 수집한 데이터 셋의 일부 클래스를 알려지지 않은 공격으로 명시하고 이에 대한 레이블을 제거하여 연구를 진행한다. 해당 방법은 다양한 데이터 셋 활용이 가능하고, 다양한 위협에 대해서 연구가 가능하다는 장점을 가지고 있지만, 이미 알려진 위협이기 때문에 실제 네트워크 시스템에서 발생하는 알려지지 않은 위협을 탐지할 수 있는지가 불분명하다는 한계점을 가지고 있다.

[13]에서는 알려지지 않은 위협을 탐지하기위해 오토인코더와 1차원 CNN을 적용한 이상 탐지 방법을 제안하였다. [14]에서는 GAN을 사용하여 악성코드 기반의 적대적 샘플을 생성하는 MalGAN을 제안하고 이를 통해 생성된 적대적 샘플을 탐지한다. [15]에서는 Long Short Term Memory(LSTM)과 Attention Mechanism(AM)을 적용한 하이브리드 기반의 알려지지 않은 위협을 탐지하는 방법을 제안하였다. [16]에서는 클래스들의 특징을 추출하고 이를 이용해 SVM의 성능을 개선하는 모델을 만들어 알려지지 않은 위협을 판단하는 방법을 제안하였다. [17]에서는 메시지를 이용해 알려지지 않은 위협을 탐지하는 모델을 제안하였다. 메시지 내 데이터 추출 및 정규화, 특징 추출, 유사도 계산, 이상 탐지를 통해 알려지지 않은 위협을 탐지하였다.

3. 알려지지 않은 위협 탐지 시스템

본 연구에서는 그림 1과 같이 오용 탐지와 이상 탐지를 결합한 하이브리드 기반의 알려지지 않은 위협 탐지 방법을 제안한다. 먼저 네트워크 시스템 상에 존재하는 트래픽 데이터를 수집하고, 수집한 데이터를 전처리하여 기계학습에 적합한 형태로 구축한다. 이렇게 생성된 데이터를 가지고 오용 탐지를 수행하게 되며, 해당 단계에서는 CBA를 적용하여 탐지를 수행한다. 기존에 수집된 알려진 위협 클래스 맞는 규칙을 생성하고 생성된 규칙을 기반으로 레이블이 되지 않은 네트워크 데이터를 매칭하여 오용 탐지를 수행한다. 매칭된 데이터들은 기존의 알려진 위협으로 판단되고 매칭되지 않은 데이터들은 알려지지 않은 위협인지 또는 정상 인지를 판별하기 위해 이상 탐지 단계로 전달된다. 이상 탐지에서는 OCSVM을 기반으로 알려지지 않은 위협을 탐지한다. 정상 데이터를 기반으로 OCSVM 기반 이상 탐지 모델을 구축하고, 정상과 알려지지 않은 위협을 판별한다. 해당 과정을 통해 위협으로 분류되는 데이터의 경우 기존에 수집된 위협에 없는 알려지지 않은 위협으로 정의된다.

3.1 데이터 수집

본 단계에서는 네트워크 시스템 상에 존재하는 데이터 수집 및 이를 하이브리드 침입 탐지에 적용하기 위한 전처리를 수행한다. 하이브리드 침입 탐지 및 기계학습에 적용하기 위해 노이즈, 결측값 제거 및 tabular 데이터로 변환, 정규화 등의 방법을 적용한다. 또한 각 데이터의 활용도에 맞게 클래스가 명시되어 있는 데이터는 라벨이 있는 데이터 셋에 저장되고, 클래스가 명시되어 있지 않은 데이터는 오용 탐지의 입력 데이터로 사용하기 위해 분리한다. 또한 상호의존정보(Mutual Information)를 활용하여 각 특징들이 사이에 존재하는 정보량을 정량화하여 서로 유사한 특징을 파악하고 제거한다. 이를 통해 모델 학습에 대한 시간을 줄이고, 중요한 정보만을 학습함으로써 모델의 정확성을 높일 수 있다.

3.2 오용 탐지

오용 탐지 단계에서는 알려진 위협 데이터에 대한 규칙을 생성하고 이를 통해 새로 들어오는 네트워크 데이터와 매칭하여 그 사이에 포함되어 있는 알려진 위협을 탐지한다. 규칙을 생성하기 위해서 CBA 기반 연관 규칙 알고리즘을 적용하였다. CBA는 Item set의 높은 빈도수를 기반으로 규칙을 생성하는 Apriori 알고리즘을 기반으로 구축되었으며, 수집된 데이터 중에서 알려진 위협으로 분류된 데이터들을 기반으로 규칙을 생성하였다.

생성된 규칙을 기반으로 새로 들어오는 네트워크 데이터와 매칭을 수행하였으며, 매칭이 되면 기존에 알려진 위협 클래스로 정의하고 매칭이 되지 않으면 클래스가 판별되지 않음으로 정의하고 그 다음 단계인 이상 탐지 단계로 넘어가게 된다.

또한 생성된 규칙을 사용자가 확인할 수 있게 제공함으로써 알려진 위협을 탐지하는데 있어 어떠한 특징들을 사용되었고, 어떠한 기준으로 판단을 내리는 지를 확인할 수 있게 하였다. 이를 통해 사용자에게 모델 판단에 대한 근거를 제공 및 설명성을 제공하였으며, 이러한 방식은 사용자에게 모델에 대한 신뢰성을 높일 수 있다.

3.3 이상 탐지

이상 탐지 단계에서는 오용 탐지 단계에서 매칭이 되지 않은 데이터들에 대한 판별을 수행하게 된다. 해당 단계에서는 기존에 수집된 정상 데이터를 학습 데이터로 사용한 OCSVM 기반 이상 탐지 모델을 구축하고, 오용 탐지에서 넘어온 데이터들을 입력 데이터하여 그 안에 포함되어 있는 정상과 알려지지 않은 위협을 판별한다. 해당 단계를 통해 위협으로 분류되는 데이터의 경우 기존에 수집된 위협에 없는 알려지지 않은 위협 즉, 일려지지 않은 위협으로 탐지된다.

4. 실험 결과

4.1 데이터 셋

본 연구에서는 IDS 2018 데이터 셋을 사용하여 실험을 진행한다. 해당 데이터 셋은 Canadian Institute for Cyber security에서 실제 네트워크 환경을 참고하여 네트워크 망을 구축하고 이를 통해 PCAP과 윈도우 이벤트 로그로 구성되어 있는 데이터 셋을 추출하였다[18]. 10일 동안 공격을 수행하였으며, 그와 관련된 Raw 데이터를 생성하였다. 79개의 특징이 포함되어 있고, 악성 행위에 대한 라벨이 포함되어 있다. 8개의 악성 행위가 수행되었으며, 각 공격에 사용한 도구, 소프트웨어 피해 PC 및 사용 IP 주소 등에 대한 정보가 포함되어 있다. 본 연구에서는 섹션 2.2에서 정의한 알려지지 않은 위협 연구 방법 중에서 두 번째 방법인 알려지지 않은 위협을 따로 생성하는 것이 아닌, 기존 데이터 셋에서 특정 클래스를 알려지지 않은 위협으로 정의하고 클래스 라벨을 제거한 데이터 셋을 가지고 실험을 진행한다.

해당 데이터 셋에서 약 60만개의 샘플을 임의로 선택하였으며, 공격 유형은 FTP-BruteForce, DoS attacks-Hulk, DoS attacks-SlowHTTPTest, Bot, DDOS attack-HOIC으로 구성되어 있다. 학습 데이터와 테스트 데이터의 비율은 8대 2로 정의하여 실험을 진행하였다.

4.2 알려지지 않은 위협 탐지

본 실험에서는 먼저 데이터 전처리를 수행하여 중요한 특징들을 선별하였다. 이를 통해 학습 시간을 단축시키고, 불필요한 정보로 인해 잘못 학습되는 문제를 해결한다. 그 다음 오용 탐지를 통해 알려진 위협을 탐지한다. 특징 전처리를 수행하기 위해 Random Forest 특징 중요도 평가와 상호의존정보을 적용하여 특징 중요도 분석을 수행하고, 오용 탐지에서는 CBA를 사용하여 규칙을 생성한다. 이상 탐지에서는 OCSVM, Isolation Forest 등의 아웃라이어 탐지 알고리즘을 사용한 비교 연구를 진행한다. 실험에서는 각각의 공격 유형을 알려지지 않은 공격으로

정의하고 성능평가를 진행하였으며, 섹션 4.2.1와 섹션 4.2.2에서 수행한 연구들은 오용 탐지 및 이상 탐지에 적합한 알고리즘 비교 검증을 수행하였기 때문에 공격 유형에 대한 평균 성능 결과를 가지고 검증을 수행하였다.

4.2.1 알려진 위협 탐지를 위한 오용 탐지

학습 시간 단축 및 불필요한 특징을 제거하기 위해 특징 선택을 수행하였다. 해당 연구에서는 의사결정나무 기반 특징 중요도 산출 및 선택과 Mutual Information 기반 특징 선택방법을 사용하였으며, 이를 통해 선택된 특징을 기반으로 CBA를 적용하여 규칙을 생성하고, 매칭을 통해 오용 탐지를 수행하였다. 표 1은 Mutual Information을 사용하여 특징 선택을 수행하고, 이를 통해 선택된 특징들을 사용하여 CBA 기반 규칙 생성을 수행한 결과이다. 표 2는 특징 선택에 따른 오용 탐지 정확도를 나타낸 표로 실험 결과 Mutual Information 기반 특징 선택 방법이 0.8435로 의사결정나무 기반 특징 중요도 산출 및 선택 방식의 0.7297 보다 높은 성능을 보인 것을 확인하였다.

(표 1) Mutual Information 기반 특징 선택을 통한 CBA 규칙 생성
(Table 1) Creating a CBA rule by selecting features based on mutual information

(8, < 0.288675), (19, < 0.5), (4, < 0.5), (15, < 4) -> (class:Brute Force -Web, sup:0.534, conf:1.0)
(7, < 0.144338), (8, < 0.288675), (15, < 4), (19, < 0.5), (21, < 0.5), (24, < 0.52439), (28, < 2.5), (30, < -0.5) -> (class:Brute Force -Web, sup:0.534, conf:1.0)
(0, 8062.5 - 8080.5), (4, < 0.5), (13, < 0.353553), (30, < -0.5) -> (class:Bot, sup:0.501, conf:1.0)
(0, 8062.5 - 8080.5), (4, < 0.5), (28, < 2.5), (31, 14 - 22) -> (class:Bot, sup:0.501, conf:1.0)
(0, 8062.5 - 8080.5), (4, < 0.5), (30, < -0.5), (31, 14 - 22) -> (class:Bot, sup:0.501, conf:1.0)
(0, 79.5 - 80.5), (5, < 0.5), (9, < 0.0344222), (23, < 0.186131), (26, < 0.5), (27, < 0.5), (28, < 2.5) -> (class:Brute Force -XSS, sup:0.538, conf:1.0)
(0, 79.5 - 80.5), (4, < 0.5), (6, < 2.5), (9, < 0.0344222), (23, < 0.186131), (28, < 2.5) -> (class:Brute Force -XSS, sup:0.538, conf:1.0)

4.2.2 알려지지 않은 위협 탐지를 위한 이상 탐지

오용 탐지를 통해 산출된 결과를 바탕으로 이상 탐지를 수행하였다. 표 3은 이상 탐지에 사용되는 알고리즘에 대한 비교 결과를 나태나며, 해당 결과에 나와 있는 바와 같이 KNN(K-Nearest Neighbor) HBOS(Histogram-based Outlier Score), iForest(Isolation, Forest), OCSVM 순서로 이상 탐지 정확도가 높게 산출되는 것을 확인하였다. 이를 통해 OCSVM이 94.15%로 가장 성능이 좋은 것을 확인하였다.

(표 2) 특징 선택 방법에 따른 오용 탐지 정확도 비교
(Table 2) Comparison of misuse detection accuracy by feature selection method

특징 선택 방법	정확도
DT 기반 특징 중요도(Top 10)	0.7297
DT 기반 특징 중요도(Top 20)	0.7297
Mutual Information	0.8435

(표 3) 특징 선택 방법에 따른 CBA 기반 이상 탐지 정확도 비교
(Table 3) Comparison of CBA-based anomaly detection accuracy by feature selection method

알고리즘	탐지 정확도	학습 시간
OCSVM	94.1580	436.4462
iForest	90.4762	7.6408
HBOS	70.5050	1.6630
KNN	53.5716	4.0611

4.2.3 하이브리드 기반 알려지지 않은 위협 탐지

최종적으로 Mutual Information 기반 특징 선택을 수행한 데이터를 적용하여 CBA 기반 오용 탐지와 OCSVM 기반 이상 탐지를 결합한 하이브리드 침입 탐지 시스템에 대한 각각 공격 유형에 따른 탐지 정확도를 측정하였다. 실험 결과는 표 4와 같으며, DoS attacks-Hulk의 경우 97.2%로 가장 높은 성능을 보였고, 탐지한 모든 공격들이 약 90% 이상의 알려지지 않은 공격 탐지가 가능한 것을 확인하였다.

(표 4) 알려지지 않은 공격 유형에 따른 탐지 결과
(Table 4) Detection results based on unknown attack types

알려지지 않은 공격 유형	탐지 정확도
DoS attacks-SlowHTTPTest	0.9353
DoS attacks-Hulk	0.9720
Bot	0.9628
FTP-BruteForce	0.9343
DDOS attack-HOIC	0.9034
Average	0.9415

5. 결 론

본 연구에서는 알려지지 않은 위협을 탐지하기 위하여 오용 탐지와 이상 탐지를 적용한 하이브리드 방식을 제안하였다. 해당 방식에는 다양한 특징에서 의미없는 특징들을 제거하기 위해 특징 선택을 수행하였고, CBA와 OCSVM 기반 침임 탐지 시스템을 구축하였다. 실험 결과 알려지지 않은 위협들의 탐지 정확도가 평균 94%를 나타내었고, 이를 통해 제안하는 방법이 알려지지 않은 위협을 탐지하는데 사용될 수 있다는 것을 확인하였다.

오용 탐지에서 생성되는 규칙이 특정 클래스에서는 중복되는 문제가 발생하였고, 이상 탐지의 경우 결정 경계에 분포해 있는 데이터들에 대한 정확한 판별이 어렵다는 문제점이 발생하였다. 특히 오용 탐지의 경우, 연관 규칙에 사용되는 지지도와 신뢰도 파라미터에 따른 생성되는 규칙이 다르기 때문에 이에 대한 최적화 연구도 필요한 것을 확인하였다. 따라서 향후 연구에서는 이러한 문제를 보완하기 위한 방법에 대해서 연구를 진행하고, 이를 통해 개선된 하이브리드 침입 탐지 시스템을 구축 할 것이다.

참고문헌(Reference)

[1] X. Sun, J. Dai, P. Liu, A. Singhal, and J. Yen, "Using Bayesian networks for probabilistic identification of zero-day attack paths," IEEE Transactions on Information Forensics and Security, vol. 13, no. 10, pp. 2506-2521, 2018. https://doi.org/10.1109/tifs.2018.2821095

[2] A. Khraisat, I. Gondal, P. Vamplew, J. Kamruzzaman, and A. Alazab, "Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine," Electronics, vol. 9, no. 1, pp. 173, 2020. https://doi.org/10.3390/electronics9010173

[3] G. Kim, S. Lee, and S. Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," Expert Systems with Applications, vol. 41, no. 4, pp. 1690-1700, 2014. https://doi.org/10.1016/j.eswa.2013.08.066

[4] A. AlEroud, and G. Karabatis, "A contextual anomaly detection approach to discover zero-day attacks," In 2012 International Conference on Cyber Security, pp. 40-45, 2012. https://doi.org/10.1109/cybersecurity.2012.12

[5] J. Hussain, and S. Lalmuanawma, "Fusion of misuse detection with anomaly detection technique for novel hybrid network intrusion detection system," In Recent Developments in Intelligent Computing, Communication and Devices, pp. 73-87, 2017. https://doi.org/10.1007/978-981-10-3779-5_10

[6] J. Lekha, and P. Ganapathi, "Detection of illegal traffic pattern using hybrid improved CART and multiple extreme learning machine approach," International Journal of Communication Networks and Information Security, vol. 9, no. 2, pp. 164-171, 2017. https://www.ijcnis.org/index.php/ijcnis/article/view/2053

[7] W. L. Al-Yaseen, Z. A. Othman, and M. Z. A. Nazri, "Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system," Expert Systems with Applications, vol 67, pp. 296-303, 2017. https://doi.org/10.1016/j.eswa.2016.09.041

[8] B. Liu, W. Hsu, and Y. Ma, "Integrating classification and association rule mining," In Kdd, vol. 98, pp. 80-86, 1998. https://dl.acm.org/doi/10.5555/3000292.3000305

[9] F. Thabtah, P. Cowling, and Y. Peng, "MCAR: multi-class classification based on association rule," In The 3rd ACS/IEEE International Conference onComputer Systems and Applications, p. 33, 2005. https://doi.org/10.1109/aiccsa.2005.1387030

[10] G. Chen, H. Liu, L. Yu, Q. Wei, and X. Zhang, "A new approach to classification based on association rule mining," Decision Support Systems, vol. 42, no. 2, pp. 674-689, 2006. https://doi.org/10.1016/j.dss.2005.03.005

[11] S. M. Erfani, S. Rajasegarar, S. Karunasekera, and C. Leckie, "High-dimensional and large-scale anomaly detection using a linear one-class SVM with deep learning," Pattern Recognition, vol. 58, pp. 121-134, 2016. https://doi.org/10.1016/j.patcog.2016.03.028

[12] Y. Wang, J. Wong, and A. Miner, "Anomaly intrusion detection using one class SVM," In Proceedings from the Fifth Annual IEEE SMC Information Assurance

Workshop, pp. 358-364, 2004.
https://doi.org/10.1109/iaw.2004.1437839

[13] C. Hwang, D. Kim, and T. Lee, "Semi-supervised based Unknown Attack Detection in EDR Environment," KSII Transactions on Internet & Information Systems, vol. 14, no. 12, pp. 4909-4926. http://itiis.org/digital-library/24150

[14] W. Hu, and Y. Tan, "Generating adversarial malware examples for black-box attacks based on gan," arXiv preprint arXiv:1702.05983, 2017. https://arxiv.org/abs/1702.05983

[15] P. Lin, K. Ye, and C. Z. Xu, "Dynamic network anomaly detection system by using deep learning techniques," In International Conference on Cloud Computing, pp. 161-176, 2019. https://doi.org/10.1007/978-3-030-23502-4_12

[16] S. Huda, S. Miah, M. M. Hassan, R. Islam, and J. Yearwood, et al., "Defending unknown attacks on cyber-physical systems by semi-supervised approach and available unlabeled data," Information Sciences, vol. 379, pp. 211-228, 2017. https://doi.org/10.1016/j.ins.2016.09.041

[17] P. Duessel, C. Gehl, U. Flegel, S. Dietrich, and M. Meier, "Detecting zero-day attacks using context-aware anomaly detection at the application-layer," International Journal of Information Security, vol. 16, no. 5, pp. 475-490, 2017. https://doi.org/10.1007/s10207-016-0344-y

[18] CSE-CIC-IDS2018 https://www.unb.ca/cic/datasets/ids-2018.html

◐ 저 자 소 개 ◑

신 건 윤(Gun-Yoon Shin)
2017년 가천대학교 인터랙티브 미디어 융합학과 학사
2018년 가천대학교 일반대학원 컴퓨터공학과(공학석사)
2018년~현재 가천대학교 컴퓨터공학과 박사과정
관심분야 : 기계 학습, 악성코드 분석, 공격자 식별, 저자 분석, 인공지능
E-mail : tlsrjsdbs@gmail.com

김 동 욱 (Dong-Wook Kim)
2015년 가천대학교 컴퓨터공학과(공학사)
2017년 가천대학교 일반대학원 컴퓨터공학과(공학석사)
2017년~현재 가천대학교 컴퓨터공학과 박사과정
관심분야 : Cyber Security, Data Mining, Artificial intelligence
E-mail : kog7306@naver.com

◐ 저 자 소 개 ◑

윤 지 영(Jiyoung Yun)
2020년 가천대학교 컴퓨터공학과(공학사)
2020년~현재 가천대학교 일반대학원 소프트웨어학과 석사과정
관심분야 : XAI, Machine Learning, Statistics, Intrusion Detection
E-mail : apfhd9043@naver.com

김 상 수(Sang-Soo Kim)
1997년 경북대학교 전자공학과(공학사)
2003년 경북대학교 컴퓨터공학과(공학석사)
2003년~현재 국방과학연구소 연구원
관심분야 : Cyber Security, Cyber Situation Awareness, Artificial Intelligence
E-mail : wisdory@naver.com

한 명 묵(Myung-Mook Han)
1980년 연세대학교 공과대학(공학사)
1987년 뉴욕공과대학교 대학원 컴퓨터과학과(이학석사)
1997년 오사카시립대학교 대학원 정보공학부(공학박사)
1998년~현재 가천대학교 소프트웨어학과 교수
관심분야 : 정보보호, 데이터 마이닝, 기계 학습
E-mail : mmhan@gachon.ac.kr