Journal of the Korea Academia-Industrial cooperation Society
Vol. 17, No. 9 pp. 440-446, 2016

http://dx.doi.org/10.5762/KAIS.2016.17.9.440
ISSN 1975-4701 / eISSN 2288-4688

데이터 유출 탐지를 위한 이상 행위 탐지 방법의 비교 및 분석

임원기[1], 권구형[1], 김정재[2], 이종언[3*], 차시호[4]
[1]국방과학연구소 2본부 3부, [2]광운대학교 컴퓨터과학과,
[3]한화시스템 전술통신팀, [4]청운대학교 멀티미디어학과

Comparison and Analysis of Anomaly Detection Methods for Detecting Data Exfiltration

Wongi Lim[1], Koohyung Kwon[1], Koohyung Kwon[2], Jong-Eon Lee[3*], Si-Ho Cha[4]
[1]The 2nd Institute 3rd Directorate, Agency for Defense Development
[2]Dept. of Computer Science, Kwangwoon University
[3]Tactical Communication Team, Hanwha Systems
[4]Dept. of Multimedia Science, Chungwoon University

요 약 군사 비밀이나 조직의 기밀 데이터는 그 조직의 매우 중요한 자원이며 외부로부터의 접근이 차단되어야 한다. 그러나 최근 인터넷의 접근성이 높아짐으로써 보안이 중요한 이슈로 부상하고 있다. 이를 위해 네트워크 내부에 대한 공격이나 침입 행위를 탐지하는 이상 행위 탐지 방법이 제안되었다. 그러나 대부분의 이상 행위 탐지는 외부로부터의 침입에 대한 측면만 다루고 있으며, 공격이나 침입보다 더 큰 피해를 입히는 내부 데이터의 유출에 대해서는 다루고 있지 않다. 또한 기존의 이상 행위 탐지 방법을 데이터 유출 탐지에 적용할 경우 네트워크 내부의 환경과 여러 가지 변수들이 고려되어 있지 않기 때문에 많은 문제점들이 발생한다. 따라서 본 논문에서는 데이터 유출 탐지를 위한 이상 행위 탐지(Data Exfiltrating Detection for Anomaly Detection : DEDfAD) 방법의 정확도 향상을 위하여 DEDfAD에서 고려되어야 하는 이슈 사항들에 대하여 기술하고, 프로파일 기반의 탐지 방법과 머신러닝 기반의 탐지 방법으로 분류하여 이들의 장단점을 분석한다. 또한 분류된 접근 방법을 중심으로 이슈들과의 비교분석을 통해 향후 연구 방향을 제시한다.

Abstract Military secrets or confidential data of any organization are extremely important assets. They must be discluded from outside. To do this, methods for detecting anomalous attacks and intrusions inside the network have been proposed. However, most anomaly-detection methods only cover aspects of intrusion from outside and do not deal with internal leakage of data, inflicting greater damage than intrusions and attacks from outside. In addition, applying conventional anomaly-detection methods to data exfiltration creates many problems, because the methods do not consider a number of variables or the internal network environment. In this paper, we describe issues considered in data exfiltration detection for anomaly detection (DEDfAD) to improve the accuracy of the methods, classify the methods as profile-based detection or machine learning-based detection, and analyze their advantages and disadvantages. We also suggest future research challenges through comparative analysis of the issues with classification of the detection methods.

Keywords : Data Exfilteration, Anomaly Detection, Information Leakage, Machine Learning, Insider Threat Prediction

1. 서론

최근 하드웨어 기술의 발전으로 다양한 디바이스들이 개발되었으며, 스마트 폰이나 태블릿 등과 같은 인터넷에 접속할 수 있는 다양한 디바이스들이 보급되고 있다. 이에 따라 사용자들은 언제 어디서나 인터넷에 쉽게 접

*Corresponding Author: Jong-Eon Lee(Hanwha Systems)
Tel: +82-31-8091-7405 email: jong-eon.lee@hanwha.com
Received August 8, 2016 Revised September 7, 2016
Accepted September 9, 2016 Published September 30, 2016

속할 수 있게 되었다. 인터넷의 사용이 쉬워진 만큼 사용자들은 보안 위협에 더 쉽게 노출되고 있으며, 이로 인해 보안의 중요성이 날로 증대되고 있다[1]. 이러한 배경으로 인하여 네트워크 내부에 대한 공격이나 네트워크 내부로의 침입 행위를 탐지하는 이상 행위 탐지 방법이 제안되었다[2-5]. 이상 행위 탐지는 네트워크에 대한 공격이나 침입을 일련의 행위로 가정하고, 이를 탐지하기 위해 활용하는 기법들을 총칭한다. 기존에는 네트워크에 대한 외부의 공격이나 침입이 이미 발생하고 난후(많은 피해를 입은 후)에 해당 IP 주소를 하드웨어적으로 블록킹하여 공격을 방어하는 블랙 리스트 방법을 사용하였다. 그러나 이상 행위 탐지 기법들이 발달함에 따라 공격이 발생한 시점에 탐지하여 방어함으로써 외부 사용자의 침입을 조기에 제거할 수 있는 효과를 얻을 수 있다. 이러한 이상 행위 탐지 기법의 발달로 인하여 네트워크 보안 측면에 상당한 발전이 있었으며, 하드웨어에 의존하던 네트워크 보안을 네트워크 모니터링 즉, 소프트웨어 측면에서 분담하게 되는 계기가 되었다. 그러나 이는 외부에서의 침입을 방어하는 측면에 제한되어 있고, 내부에서 외부로의 데이터 유출 측면의 보안은 전혀 고려되어 있지 않다[6-9].

데이터 유출은 현재 네트워크 보안에서 많은 관심을 받고 있다. 데이터 유출은 정보 누수라고도 불리며, 비인가된 사용자가 네트워크 내부의 정보(데이터 혹은 파일)를 악의적인 목적으로 외부로 유출하는 것을 의미한다. 데이터 유출은 침입에 비해 발견이 늦고 어렵기 때문에 유출이 발생한 후 한참 후에야 알 수 있어 그 피해가 외부에서의 공격 보다 더 크다[10-12]. 그러나 기존의 연구는 외부 사용자에 의한 내부 데이터의 안전성 측면에서만 연구되었다. 또한, 기존의 이상 행위 탐지 연구 방법을 데이터 유출 탐지에 그대로 적용할 경우에는 많은 문제점들이 발생한다. 따라서 데이터 유출에 대한 효율적인 탐지를 위해서는 데이터 유출과 네트워크 내부에 대한 여러 가지 변수를 고려해야만 한다. 데이터 유출 탐지를 위한 이상 행위 탐지(Data Exfiltrating Detection for Anomaly Detection : DEDfAD)는 인가 또는 비인가된 사용자가 네트워크 내부의 중요 정보를 외부로 유출하는 것을 탐지하여 관리자에게 알림을 주는 것을 주요 목적으로 하고 있다. 따라서 정보 유출을 얼마나 정확하게 탐지할 수 있느냐가 데이터 유출 탐지를 위한 이상 행위 탐지 기법의 성능 지표가 되며, 정확도 향상을 중심으로 연구되고 있다[13].

현재 제안되고 있는 DEDfAD 방법들은 파일 혹은 데이터가 담고 있는 콘텐츠가 중요하기 때문에 데이터 유출 탐지에 대한 성능 향상을 위해서는 구축된 네트워크의 특성뿐만 아니라 파일이나 네트워크 사용자의 특성을 함께 고려해야 한다. 이를 위하여 본 논문에서는 DEDfAD의 정확도 향상을 위해 DEDfAD에서 해결되어야 하는 이슈 사항들에 대하여 점검하고, 기존에 제안된 DEDfAD를 탐지 방법에 따라 프로파일 기반의 접근 방법과 머신러닝 기반의 접근 방법으로 분류하여 장단점을 분석한다. 또한 분류된 접근방법을 중심으로 해결되어야 할 이슈들과의 비교 분석을 통하여 DEDfAD의 향후 연구 방향을 제시한다.

본 논문의 2장에서는 DEDfAD를 개선하기 위해 해결해야 할 이슈 사항들에 대하여 기술하고, 3장에서는 기존에 제안된 각 DEDfAD 방법에 대한 장단점을 분석한다. 그리고 4장에서는 3장에서 분석된 각 기술의 장단점을 기반으로 해결 이슈를 중심으로 DEDfAD 방법을 비교한다. 마지막으로, 5장에서는 결론 및 향후 연구에 대하여 기술한다.

2. DEDfAD를 위한 이슈 분석

데이터 유출 탐지는 침입 탐지와 다른 특성을 갖는다. 2장에서는 데이터 유출 탐지의 효율적인 설계를 위하여 이상 행위 탐지 방법 설계 시 발생하는 이슈들에 대하여 기술한다.

2.1 경계 검출

네트워크상에서 데이터 유출을 탐지하는데 있어 일반적인 경우 정상 및 비정상 행위의 경계는 모호하다. 이러한 모호함을 방지하기 위하여 사용자가 행하는 모든 정상적인 동작을 정의하고, 이를 일반화하는 집합을 정의하는 것은 불가능에 가깝다(비정상 동작을 정의하는 경우에도 동일하다)[14]. 이는 정상과 비정상의 경계선 부근의 행위에서 관측되는 이상 행위는 정상으로 관측되더라도 비정상일 수 있고, 비정상으로 관측되더라도 실제로는 정상을 의미할 수 있다는 것이다. 이것은 어떠한 경계선을 긋는 가에 따라 같은 동작이 정상일 수도 있고 비정상일 수도 있다는 것을 의미한다. 따라서 데이터 유

출을 탐지하는데 있어서 이러한 모호한 상황에서의 행위에 대한 판단은 언제든지 변할 수 있어야 한다.

2.2 비적합성

사용자가 수행하는 특정 행위가 유출에 대한 이상 결과이고, 그 행위가 실제 유출로 나타났을 경우, 데이터를 유출하는 내부자는 그 행위가 비정상에서 정상으로 적응하도록 할 수 있다. 이는 의도적으로 이상 행위를 노출시켜 시스템이 정상 행위로 인지하도록 하는 경우이다. 이러한 일련의 행위는 정상 행위를 정의하는 것을 더욱 복잡하고 어렵게 만든다[7]. 따라서 데이터 유출을 효율적으로 탐지하기 위해서는 정상 혹은 비정상 행위에 대한 기준을 이상 행위 검출 시스템이 조절할 수 있어야 한다.

2.3 유연성

많은 환경에서 정상적인 동작은 고도화된다. 이는 현재의 정상적인 동작의 개념은 차후 혹은 미래에는 정상적인 동작을 충분히 대표하지 않을 수 있다는 것을 의미한다[15]. 따라서 효율적인 데이터 유출 탐지를 위해서는 정상적인 동작에 대한 정의 집합을 유연하게 새로 추가할 수 있어야 한다.

2.4 다양성

데이터 유출 탐지의 정확한 개념은 도메인마다 차이가 있다. 예를 들어, 주식 시장 영역에서의 유사한 편차(주식의 가격 변동)가 정상으로 간주 될 수 있는 반면, 의료 도메인의 작은 편차(체온 변동)는 이상 행위 일 수 있다는 것이다[8]. 이는 현재의 이상 행위 검출 탐지 방법이 각각의 도메인에서 적응하여 이상 행위를 탐지해야 함을 나타낸다.

2.5 유효성

트레이닝이나 검증을 위해 사용하는 데이터는 일반적으로 중요한 이슈이다[7-8]. 이는 이상 행위 탐지를 위해 전 처리 후 시스템에 입력하는 데이터가 얼마나 유효한지를 나타내는 지표가 된다.

2.6 민감성

데이터 유출 탐지에서 사용하는 데이터에는 언제나 실제의 이상 행위와 유사한 노이즈가 섞여 있다[8-9]. 이는 노이즈와 실제 행위를 구분하기가 어렵다는 것을 의미이다. 따라서 효율적인 데이터 유출 탐지 방법은 이와 같은 노이즈와 실제의 행위를 구분할 수 있어야 한다.

3. DEDfAD의 분류

현재 DEDfAD는 시그니처, 머신러닝, 피처, 프로파일, 그리고 행위 기반 검출 방법으로 분류된다. 본 논문에서는 DEDfAD를 효율적으로 분류하기 위해 네트워크 상의 정보를 다루는 방법에 따라 프로파일 기반 검출과 머신러닝 기반 검출로 분류하여 각각의 장단점에 대하여 분석한다.

3.1 프로파일 기반 검출

G. B. Magklaras[16]는 초기에 데이터 유출에 대한 문제점을 인식하고 ITPT(Insider Threat Prediction Tool)을 제안하였다. ITPT는 네트워크 오퍼레이터에 의해 네트워크 사용자의 행동을 프로파일화하고 네트워크 사용자의 어떤 행동이 데이터 유출을 유발하는지 그리고 어떤 영향을 미치는지에 대해 실험할 수 있는 툴이다. 즉 ITPT는 네트워크 오퍼레이터가 프로파일링 된 사용자의 정보를 ITPT에 넣어서 시뮬레이션을 통해 사용자의 행동에 의한 위협 수준을 비교할 수 있는 툴이다. 그림 1은 ITPT 툴의 구조를 보인 것으로 동작 절차는 간단하다.

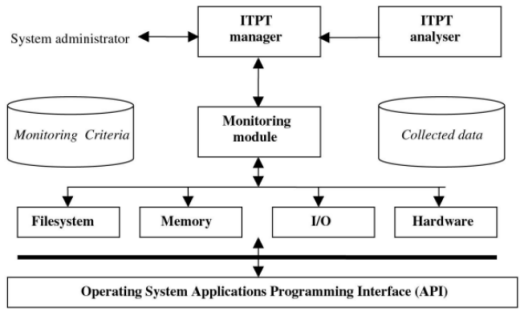

Fig. 1. High level Architecture of ITPT[16]

모니터링 모듈에 의해 사용자가 컴퓨터를 통해 접근하는 모든 것에 대한 정보들이 수집된 데이터에 저장된다. 이때 오퍼레이터가 GUI 환경을 통해 모니터링 기준에 추출 정책(파일 시그니처, 사용자 인가 정보)들에 대해 업데이트하면 ITPT 분석가 모듈에서 저장된 피처들에 대해 패턴 매칭을 통해 검사한 후 다시 ITPT 관리자

를 통해 관리자에게 결과를 통보한다.

Y. Liu[17]는 데이터 유출 탐지를 위해 SIDD (Sensitive Information Dissemination Detection)라는 프레임워크를 제안하였다. SIDD는 사용자나 사용자의 행동과 무관하게 네트워크의 내부에 있는 보호해야하는 콘텐츠에 초점을 맞추고 콘텐츠를 프로파일링 한다. SIDD의 간소화된 동작절차는 다음과 같다. 먼저 관리자에 의해 중요 콘텐츠를 식별하고, 식별된 콘텐츠에 대해 통계나 시그널 프로세싱을 사용하여 시그니처를 생성한 후 이를 CDR(Critical Data Repository)에 저장한다. 이러한 과정은 콘텐츠를 프로파일링 하는 과정으로 간주될 수 있다. 이후 네트워크 안에서 전송되는 패킷을 캡처하여 CDR의 데이터와 패턴 매칭을 통해 데이터 유출을 식별한다. SIDD는 네트워크에서 외부로 전송되는 모든 패킷을 캡처하므로 관리자에 의해 지정된 유출을 거의 완벽하게 탐지할 수 있고, 멀티미디어 콘텐츠의 유출에서 특히 좋은 성능을 보이고 있다. 그러나 암호화된 패킷이나 데이터에 대해서는 탐지를 수행할 수 없다는 단점이 있으며 프로파일 기반 검출의 단점인 새로운 유출 방법에 대해서 쉽게 적응하지 못하는 단점 또한 갖고 있다.

3.2 머신러닝 기반 검출

A. Al-Bataineh[18]는 데이터 유출에 있어 전송하는 콘텐츠나 파일을 암호화할 경우에는 패턴 매칭을 통해 식별하기가 어렵다는 문제점을 인식하였다. 따라서 Zeus라 불리는 봇넷에서 데이터를 가져와 데이터 유출자들의 행동들을 분석하였고, HTTP POST의 바이트 빈도 분포와 엔트로피를 특성으로 하는 행동 분류기를 사용하였다. 이를 위해 AdaBoost 행동 분류 알고리즘을 사용하였으며, 이를 통해 기존의 패턴 매칭 방법에 비해 약간의 좋은 성능을 보였다. 이러한 약간의 좋은 성능은 이상치에 대한 약간의 변화에 대해서 분류를 해 낼 수 있음을 의미한다. 그러나 이는 교사 학습과 파라메트릭 모델을 이용하기 때문에 기존에 정의 되지 않은 새로운 시나리오나 공격 방법에 대해서는 검출할 방법이 없다는 단점을 가지고 있다.

R. Ramachandran[19]은 기존의 침입 탐지 방법을 분석하였다. 침입탐지 방법은 침입이 발생한 후에 해당 공격 방법을 인지하고 차단하는 블랙 리스트 방식을 사용한다. 그러나 이를 데이터 유출 방법에 적용했을 때의 문제점을 해결하기 위하여 사용자의 정상 행동을 기반으로 데이터 유출에 대한 이상치를 찾아내는 방법을 설계하였다. Ramachandran가 제안한 행동 기반의 데이터 유출 탐지 모델은 그림 2와 같이 학습과 탐지의 2단계로 이루어진다. 첫 번째의 학습 단계에서는 사용자의 정상 행동을 비모수 검정법인 KDE(Kernel Density Estimation)을 통해 학습한다. 이러한 비교사학습을 통해 정상 행동에 대해 명확한 학습이 가능해진다. 두 번째 탐지 단계에서는 학습 단계에서 학습한 정상 행위를 바탕으로 상관 계수를 통해 정상 이외의 이상치를 탐지한다. 이러한 모델은 비교사학습을 사용하기 때문에 미리 정의되어 있지 않은 유출 시나리오에도 대응할 수 있는 장점이 있다. 그러나 이 모델은 초기 학습 단계에서 정상 행위를 어떻게 판단하느냐에 따라 매우 다른 결과를 나타낸다는 단점이 있다.

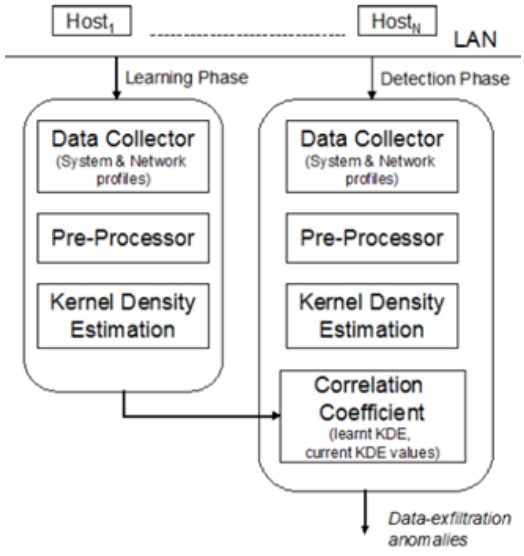

Fig. 2. Behavior based exfiltration detection model[19]

P. Parveen[20]은 네트워크의 특정 패킷 데이터로 데이터 유출 행위를 판단하는 것에는 한계가 있음을 인식하고 GBAD(Graph-Based Anomaly Detection) 방법을 제안하였다. GBAD는 그래프를 기반으로 사용자의 일련의 행동이 데이터 유출인지에 대해 판단하는 방법이다. GBAD는 데이터 유출 행위를 행동의 연속으로 가정하였고 일련의 패킷의 흐름으로 매칭할 수 있다. 따라서 먼저 패킷 스트림을 통해 유의미한 특성을 추출하기 위해 앙상블 메소드 기반의 스트림 마이닝 방법을 차용하였으

며, 모든 데이터 유출 방법에 대응하기 위하여 비교사학습을 수행한다. 또한 추출한 특성이 실제 유출 행위 인지 아닌지 판단하기 위해 그래프 기반의 이상 행위 탐지 방법을 사용해 내부 유출을 판단한다. 그래프를 통해 이상행위를 탐지하는 방법은 그림 3과 같다. 먼저 추출된 특성을 통해 패킷의 흐름에 따라 기준이 되는 규범 구조를 생성하고 기준과 다른 흐름이 생기면 해당 행위를 이상행위로 판단한다. GBAD 방법의 경우도 마찬가지로 비교사학습을 통해 정의되지 않은 시나리오에 대한 탐지가 가능하다는 장점이 있지만, 정상이지만 이상행위로 판단하는 긍정오류율이 높다는 단점이 있다.

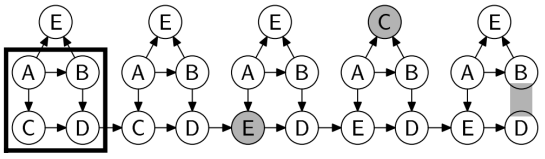

Fig. 3. A graph with a normative substructure (boxed) and anomalies (shaded)[20]

4. 비교 및 분석

표 1은 본 논문에서 살펴본 DEDfAD 이슈들에 대한 각 방법론들의 비교를 나타낸 것이다. 이상 행위 검출 방법은 이상치 검출을 목적으로 하고 있다. 이에 따라 표 1에서 보인 것과 같이 현재 연구되고 있는 모든 방법론들은 데이터 유출 방법을 위한 정확도 향상에 초점을 맞추고 있다. 프로파일 기반 검출 방법 중 ITPT[16]는 사용자를 프로파일링 하여 사용자가 하는 행위에 대해 위협수준을 표현하는 것에 목적을 두고 있다. 관리자의 입력에 따라서 도메인이 변경되어도 충분히 사용이 가능하며 관리자의 입력에만 영향을 받기 때문에 데이터의 노이즈 에는 비교적으로 영향을 덜 받는다. SIDD[17]의 경우 특성 추출 후 단순 패턴 매칭으로 동작하므로 데이터의 노이즈나 유효성에 거의 영향을 받지 않는다.

머신러닝 기반 검출 방법 중 Magklaras[18]가 제안한 방법의 경우 머신러닝을 활용하기 때문에 데이터의 형태에 따라 유연하고 모든 네트워크 환경과 도메인에 적용할 수 있다. 그러나 패턴 매칭과 교사학습으로 인한 한계가 분명하다. 그러나 비교사학습 방법으로 정상행위를 학습하는 Ramachandran[19]이 제안한 방법의 경우에는 내부자의 유출 방법이 기존의 정상 행위만큼 발생하지 않으면 이상치로 검출되기 때문에 적합성에 거의 영향을 받지 않는다고 할 수 있다. GBAD[20]는 패킷 하나만을 유출로 가정하고 판단하는 기존의 방법에 비해 정확도가 높고 그래프를 기반으로 하는 탐지 방법과 앙상블 메소드로 인해 다른 머신러닝 기반의 탐지방법에 비해 노이즈에 대한 민감도가 적은 편이다.

프로파일 기반 검출의 경우 위와 같이 패턴 매칭을 중심으로 활용하기 때문에 이미 알려진 시나리오(유출순서 및 방법)에 대해서는 거의 완벽한 탐지가 가능하다. 그러나 알려지지 않은 시나리오에 대해서는 전혀 탐지 할 수 없는 특성을 가지고 있다. 반면에 머신러닝 기반 검출의 경우 데이터를 기준으로 학습하기 때문에 데이터의 분포에 따라 이상치를 탐지하는 기준이 변한다. 이는 머신러닝 기반의 탐지방법은 새로운 유출 방법의 시도에도 반응할 수 있도록 사전조치의 특성을 가지고 있고 프로필 기반의 탐지 방법의 경우 패턴매칭 방법을 사용하기 때문에 사후조치의 특성을 가지고 있다.

5. 결론 및 향후과제

본 논문에서는 정보 유출 탐지를 위한 이상 행위 탐지 방법(DEDfAD)의 성능 향상을 위해 해결되어야 하는 이슈들과 DEDfAD 방법의 분류에 따른 장단점을 비교 분

Table 1. Comparison and analysis of DEDfAD

Methods		Boundary Detection	Inadaptability	Flexibility	Diversity	Availability	Sensitivity
Profile-based Detection	ITPT[16]				√		√
	SIDD[17]					√	√
Machine learning based Detection	Magklaras[18]	√			√		
	Ramachandran1[19]	√	√	√	√		
	GBAD[20]	√	√		√		√

석 하였다. 현재 많은 방법들이 정보 유출 탐지를 위해 제안되고 있지만 현재 연구되고 있는 프로파일 기반 검출 기법과 머신러닝 기반 검출 방법은 접근 방법이 다른 만큼 서로간의 특성과 이슈도 매우 다르다. 따라서 정보 유출 탐지에서의 높은 정확도 향상을 위해서는 두 가지 방법의 장점을 혼합할 필요가 있다. 예를 들어, 프로파일 기반 검출을 먼저 수행한 후에 정상으로 판단된 패킷들에 대해 머신러닝 기반 검출 방법을 적용하거나 반대로 머신러닝 기반 검출을 먼저 적용한 후에 이상 행위로 검출된 패킷들에 대해 프로필 기반의 탐지 방법을 적용하여 2단계로 이상 행위를 검출할 수 있는 시스템에 대한 연구도 가능하다. 그러나 이러한 방법들은 각각의 시간이 많이 걸리는 만큼 실시간 탐지를 보장하지 않을 수 있다. 따라서 보다 나은 탐지율 향상을 위해 두 가지 방법론을 함께 적용하면서도 실시간 탐지가 가능하도록 각자의 방법에 대한 계산 복잡도를 최소화하는 연구가 이루어져야 한다.

References

[1] B. J. Lee, H. S. Jeon, H. Y. Song, "Information-Centric Networking Research Trend", Electronics and Telecommunications Trends, 2012.

[2] S. J. Oh, "An Anomaly Detection Method for the Security of VANETs," The Journal of The Institute of Internet, Broadcasting and Communication, vol. 14, no. 6, pp. 175-185, 2014.

[3] S. J. Oh, "Design and Evaluation of a Weighted Intrusion Detection Method for VANETs," The Journal of The Institute of Webcasting, Internet and Telecommunication, vol. 11, no. 3, pp. 181-188, 2011.

[4] S. Kim, S.-J. Oh, "A Big Data Application for Anomaly Detection in VANETs," The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), vol. 14, no. 6, pp. 175-181, Dec. 2014.
DOI: http://dx.doi.org/10.7236/JIIBC.2014.14.6.175

[5] V. J. Hodge, J. Austin, "A Survey of Outlier Detection Methologies", Artificial Intelligence Review, vol. 22, no. 2, pp. 85-126, 2004.
DOI: http://dx.doi.org/10.1023/B:AIRE.0000045502.10941.a9

[6] W.-S. Kim, S. Kim, "A Study on Information Effluence State and Measure by Peer-to-Peer Programs in Korea and Japan," The Journal of The Institute of Webcasting, Internet Television and Telecommunication, vol. 9 no. 1, pp. 67-74, 2009.

[7] V. Chandola, A. Banerjee, Vipin Kumar, "Anomaly detection : A survey", ACM Computing Surveys(CSUR), vol. 41 no. 3, 2009.
DOI: http://dx.doi.org/10.1145/1541880.1541882

[8] F. Sabahi, A. Movaghar, "Intrusion Detection : A Survey", The Third International Conference on Systems and Networks Communications, pp. 23-26, 2008.
DOI: http://dx.doi.org/10.1109/icsnc.2008.44

[9] Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network Anomaly Detection : Methods, Systems and Tools", IEEE Communications Surveys & Tutorials, vol. 16, no. 1, 2014.
DOI: http://dx.doi.org/10.1109/SURV.2013.052213.00046

[10] M. R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore, “Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector”, CERT and the National Threat Assessment Center, Aug. 2004.

[11] E. D. Shaw, K. G. Ruby, and J. M. Post, “The insider threat to information systems: The psychology of the dangerous insider”, Security Awareness Bulletin, vol. 2-98, pp. 27-46, Sept. 1998.

[12] L. Spitzner, “Honeypots: catching the insider threat”, Proceedings of 19th Annual Computer Security Applications Conference, pp. 170-179, Dec. 2003.
DOI: http://dx.doi.org/10.1109/csac.2003.1254322

[13] M. B. Salem, S. Hershkop, S. J. Stoplfo, "A Survey of Insider Attack Detection Research", Insider Attack and Cyber Security, vol. 39, pp. 69-90, 2008.
DOI: http://dx.doi.org/10.1007/978-0-387-77322-3_5

[14] S. Y. Lim, A. Jones, "Network Anomaly Detection System : The State of art of Network Behaviour Analysis", International Conference on Convergence and Hybrid Information Technology, 2008.
DOI: http://dx.doi.org/10.1109/ichit.2008.249

[15] V. Chandola, A. Banerjee, V. Kumar, "Anomaly Detection for Discrete Sequences: A Survey", IEEE Transactions on Knowledge and Data Engineering, vol. 24, no. 5, May 2012.
DOI: http://dx.doi.org/10.1109/TKDE.2010.235

[16] G. B. Magklaras, “Insider Threat Prediction Tool: Evaluating the probability of IT misuse”, Elsevier Science C&C, 2002.

[17] Y. Liu, “SIDD: A Framework for Detecting Sensitive Data Exfiltration by an Insider Attack ”, IEEE HICSS, 2009.
DOI: http://dx.doi.org/10.1109/HICSS.2009.390

[18] A. Al-Bataineh, “Analysis and Detection of Malicious Data Exfiltration in Web Traffic”, IEEE Malicious and Unwanted Software, 2012.
DOI: http://dx.doi.org/10.1109/malware.2012.6461004

[19] R. Ramachandran, “Behavior model for Detecting data Exfiltration in Network Environment”, IEEE, 2011.
DOI: http://dx.doi.org/10.1109/imsaa.2011.6156340

[20] P. Parveen, “Insider Threat Detection using Stream Mining and Graph Mining”, IEEE ICSC, 2012.

임 원 기(Wongi Lim) **[정회원]**

- 1994년 2월 : 건국대학교 전자계산학과 (공학사)
- 1996년 2월 : 건국대학교 컴퓨터공학 (공학석사)
- 1996년 1월 ~ 현재 : 국방과학연구소 책임연구원

<관심분야>
정보보호, 내장형 실시간 시스템, 전술통신

이 종 언(Jong-Eon Lee) **[정회원]**

- 2003년 2월 : 광운대학교 컴퓨터과학과 (공학석사)
- 2007년 8월 : 광운대학교 컴퓨터과학과 (공학박사)
- 2008년 4월 ~ 현재 : 한화시스템 전술통신팀 전문연구원

<관심분야>
네트워크 관리, 차세대 네트워크, 사물 인터넷, 전술통신

권 구 형(Koohyung Kwon) **[정회원]**

- 2001년 2월 : 고려대학교 전기전자전파공학부 (공학사)
- 2003년 2월 : 고려대학교 전파공학과 (공학석사)
- 2006년 7월 ~ 현재 : 국방과학연구소 선임연구원

<관심분야>
정보통신, 사이버지휘통제

차 시 호(Si-Ho Cha) **[종신회원]**

- 1997년 8월 : 광운대학교 전자계산학과 (이학석사)
- 2004년 2월 : 광운대학교 컴퓨터과학과 (공학박사)
- 1997년 7월 ~ 2000년 2월 : 대우통신 종합연구소 선임연구원
- 2009년 3월 ~ 현재 : 청운대학교 멀티미디어학과 교수

<관심분야>
네트워크 관리, 차량 통신 네트워크, 지능형 IoT

김 정 재(Jung-Jae Kim) **[준회원]**

- 2013년 2월 : 광운대학교 컴퓨터소프트웨어학과 (공학사)
- 2015년 2월 : 광운대학교 컴퓨터과학과 (공학석사)
- 2015년 3월 ~ 현재 : 광운대학교 컴퓨터과학과 박사과정

<관심분야>
미래 인터넷, 정보 중심 네트워크, 사물 통신