The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 16, No. 6, pp.1-7, Dec. 31, 2016. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2016.16.6.1
JIIBC 2016-6-1

시계열 데이터에 적합한 다단계 비정상 탐지 시스템 설계

Design of Multi-Level Abnormal Detection System Suitable for Time-Series Data

채문창*, 임혁*, 강남희**

Moon-Chang Chae*, Hyeok Lim*, Namhi Kang**

요 약 새로운 정보통신 기술의 발전과 더불어 보안 위협도 나날이 지능화 고도화되고 있다. 본 논문은 네트워크 장치나 사물인터넷 경량 장치에서 일련의 주기를 통해 연속적으로 입력되는 시계열 데이터를 통계적 기법을 활용하여 분석하고, 분석 정보를 기반으로 장치의 이상 유무나 비정상 징후를 탐지할 수 있는 시스템을 제안한다. 제안 시스템은 과거에 입력된 데이터를 기반으로 1차 비정상 탐지를 수행하고, 시간 속성이나 그룹의 속성을 기반으로 저장되어있는 시계열 데이터를 기반으로 신뢰구간을 설정하여 2차 비정상 탐지를 수행한다. 다단계 분석은 판정 데이터의 다양성을 통해 신뢰성을 향상시키고 오탐율을 줄일 수 있다.

Abstract As new information and communication technologies evolve, security threats are also becoming increasingly intelligent and advanced. In this paper, we analyze the time series data continuously entered through a series of periods from the network device or lightweight IoT (Internet of Things) devices by using the statistical technique and propose a system to detect abnormal behaviors of the device or abnormality based on the analysis results. The proposed system performs the first level abnormal detection by using previously entered data set, thereafter performs the second level anomaly detection according to the trust bound configured by using stored time series data based on time attribute or group attribute. Multi-level analysis is able to improve reliability and to reduce false positives as well through a variety of decision data set.

Key Words : Abnormal, Intrusion Detection System, Multi-level, Time-Series, Security

Ⅰ. 서 론

클라우드 컴퓨팅, 빅데이터 및 사물인터넷 등 새로운 정보통신기술의 발전으로 보안위협이 나날이 지능화되고 고도화되어 가고 있다. 사물인터넷의 경우 과거 인터넷과의 연결을 고려하지 않았던 주변의 많은 장치들이 상호 연결되어 초연결 사회가 구축될 것으로 기대되고 있다[1].

인터넷에 연결되는 개체의 수가 증가할수록 공격될 수 있는 대상의 수도 증가하게 되고, 공격에 대응할 수 있는 보안 기술의 적용은 더욱 복잡해지게 된다[2, 3]. 새로운 기술을 적용하여 다양한 융복합 시장을 활성화하기 위해서는 개인의 정보를 보호하고 시스템의 신뢰성을 향상시킬 수 있는 보안 기술은 반드시 제공되어야한다. 기존 정보 보호 시스템 운용 방법의 한계를 극복하고 최근의 사이버 위협에 효율적으로 대응할 수 있는 방안이 필

*정회원, (주)퓨쳐시스템 보안기술연구소
**종신회원, 덕성여자대학교 디지털미디어학과(교신저자)
접수일자 : 2016년 11월 16일, 수정완료 : 2016년 12월 6일
게재확정일자 : 2016년 12월 9일

Received: 16 November, 2016 / Revised: 6 December, 2016 / Accepted: 9 December, 2016
**Corresponding Author: kang@duksung.ac.kr
Dept. of Digital Media, Duksung Women's University, Korea

요하다.

최근 국내외에서 이슈화되었던 금융권, 국가기관, 기업의 침해 사례들은 기관을 보호하기 위해 설치되어있는 보안 장비들이 공격을 탐지할 수 없도록 치밀하게 수행되었다. 특히, 2011년 농협과 SK컴즈 공격 사례 그리고 2013년 3.20 사이버 테러의 경우는 탐지가 어려운 APT(Advanced Persistent Threat) 공격을 기반으로 하고 있다[4]. APT는 기술적 공격과 사회공학적인 공격들을 다양하게 조합하여 장기간 지속적으로 목표 기관에 공격을 준비하고 최종 공격을 수행하는 보안 공격이다[5]. 장기간 다양한 공격 루트를 활용하므로 사전에 공격에 대응하거나 침입을 탐지하기가 어렵다.

네트워크나 시스템의 보안 공격을 사전에 탐지하는 방식은 시그너처 기반 방식과 비정상(Abnormal) 탐지 기반 방식으로 일반적으로 구분할 수 있다. 시그너처 기반 탐지는 알려진 보안 공격을 쉽게 탐지할 수 있고 공격 시 대응 방안의 설정이 용이하지만 알려지지 않은 신종 공격에 대응기 어렵다는 단점이 있다. 비정상 탐지 기반 방식은 신종 공격에도 대응할 수 있지만 비정상 행위의 판단 기준 설정이 어렵고 공격 이후에 대응할 수 있는 방안을 자동화하기 어렵다는 단점이 있다[6].

본 논문에서는 네트워크 구성 장치로부터 주기적으로 연속되어 입력되는 시계열 데이터에 통계적 기법을 활용하여 이상 유무를 판단하여 지정된 사용자에게 알려 줄 수 있는 비정상 시계열 데이터 탐지 방법을 제안한다.

네트워크 구성 장비나 보안 장비들은 다양한 종류의 데이터를 일정한 시간 간격으로 발생하게 된다. 센서와 같은 사물인터넷 초경량 장치도 적용되는 서비스에 맞게 데이터를 주기적으로 발생하게 된다. 이러한 데이터는 일반적으로 일정 주기를 갖고 발생되며 각각의 목적에 맞는 활용을 위해 저장 및 관리되고 있다.

본 논문에서는 이렇게 시간의 흐름에 따라 일정한 간격마다 관측된 데이터를 "시계열 데이터"로 지칭한다. 즉, 시계열 데이터는 주기적으로 연속되어 측정되는 수치 데이터로서, 시간(연, 월, 주, 일, 시 등)이나 시즌(계절, 명절, 바캉스, 크리스마스, 연말, 연초, 공휴일 등)과 같은 시간적 주기에 따라 반복되는 특성을 갖는다.

예를 들어, 평일 오전 10시부터 오후 5시 사이의 지하철 이용 고객 수는 출퇴근 시간대에 비해 감소하는 주기적인 특성을 가질 수 있다. 또한, 웹사이트에 접속하는 웹 트래픽은 주말에 낮게 기록되다가 월요일 오전 9시부터 높아지는 주기적인 특성을 가질 수 있다. 또한, 산불 감시 센서의 측정값은 습한 여름에 낮다가 가을, 겨울과 같이 건조한 계절에 높아지는 주기적인 특성을 가질 수 있다. 또한, 매년 설, 추석과 같은 명절을 앞두고 귀성표 판매 서비스를 제공하는 웹사이트에서 웹 트래픽이 증가하는 주기적인 특성을 가질 수 있다.

이러한 시계열 데이터의 이상 유무를 판단하기 위해 기존에 적용되고 있는 방식은 정상 시계열 데이터에 정상 범위로 허용될 수 있는 임계치를 설정하거나 일정시간 동안의 학습기간을 통해 획득한 측정값을 기반으로 데이터의 정상을 판단하는 방식들이 이용되고 있다. 그러나 이러한 방식을 통해 비정상으로 탐지된 시계열 데이터 중에는 실제로 정상인 시계열 데이터가 포함되는 경우가 많아 탐지 결과에 대해 실효성과 신뢰성이 적은 단점이 있다 [6]. 예를 들어, 1에서 100 사이의 값이 입력되는 임의의 장치로부터, '20,30,40,30'이 입력된 후, '60'이라는 값이 입력되는 경우 정상과 비정상을 판단할 근거를 제시하기 어렵다. 또한, 사용자에 의해 시계열 데이터의 정상 비정상이 판단되는 경우, 오인 탐지가 발생할 우려가 있다.

오탐을 최소화하기 위해 본 논문에서 제안하는 시스템에서는 다단계 탐지를 수행한다. 현재 입력된 시계열 데이터를 과거에 입력된 시계열 데이터를 기반으로 1차 판정한다. 1차 단계에서 비정상으로 판별되는 경우 대상 시계열 데이터와 시간적 속성 또는 그룹적 속성이 동일한 시계열 데이터를 이용하여 비정상 여부를 확정하는 다단계 탐지를 수행하여 시계열 데이터의 비정상 탐지율을 보다 향상시켰다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해서 기술한다. 이어서 3장에서는 제안 시스템의 개요를 기술한다. 이어서 4장에서는 제안시스템을 적용한 시나리오를 기술하고, 5장에서 본 논문의 결론을 맺는다.

II. 관련연구

네트워크와 시스템을 보호하고 악의적 공격에 대응하는 기본적인 방식은 방화벽과 같은 침입 방지 기술이다. 그러나 고도화되고 지능적인 공격자의 모든 공격을 방지할 수는 없다. 따라서 IDS(Intrusion Detection System)와 같이 공격 행위를 침입 전, 침입 도중, 그리고 침입 사

후에 탐지할 수 있는 기술이 필요하다[6, 12].

IDS와 같은 공격 탐지 기술의 기본은 비정상적 행위를 찾는 일이다. 일반적으로 비정상적 행위의 알려진 패턴(혹은 시그너처)을 기반으로 탐지하는 시그너처 기반 기술과 비정상 행위 기반 탐지 기술로 구분된다. 시그너처 기반 방식의 경우 알려진 공격을 막기 위해 자주 공격 흔적 정보를 갱신해야 하고 패턴의 종류가 많아질수록 탐지에 소요되는 시간과 필요한 자원은 증가하게 되는 단점이 있다. 비정상 기반 탐지 기술의 경우 정상과 비정상을 판단할 수 있는 정확성의 설정이 가장 중요하고 설정된 근거를 우회하기 위해 노력하는 공격자의 기술에 신속하게 대응해야 한다. 또한 순간적으로 발생하는 이상 징후와 공격으로 인한 이상 징후를 구분해야 하는 어려움이 있다[8].

정보의 가치가 증가할수록 장기적이고 지속적으로 목적 기관을 공격하는 APT 공격이 문제로 대두되면서 다양한 APT 대응 시스템이 제안되고 있다. 기존 보안 시스템과 달리 APT 공격 대응 시스템은 많은 사항들을 고려해야 한다[11]. 사물인터넷과 같은 경우는 경량 센서가 클라이언트이자 동시에 서버로 동작될 수 있으므로 공격에 대응하기 위한 정보 수집의 범위는 점차 커지고 있다. 또한 물리적으로 고정된 시스템을 보호하는 기존의 네트워크 기반 보호 장치로는 스마트폰과 같이 이동하는 장치를 통해 전파되는 악성 코드에 대응하기 어렵고 이어지는 APT에 대응하기는 더욱 어렵다[7].

APT와 같은 고도화된 보안 공격에 대응하기 위해 빅데이터 분석 기술을 적용한 기술이 제안되고 있고 제품들도 출시되고 있다. 빅데이터 분석 기반 보안 기술은 대량의 보안 로그를 효율적으로 처리하고 분석하는 방식에 중점을 두거나[8], 기존 규칙(Rule) 기반 방식과 조합되어 미래의 보안 공격을 예측하는 방식에 중점을 둔 기술 등 다양하다. 통합 보안 관제 환경에서 빅데이터 분석 방법을 적용할 수 있는 방법도 제안되고 있는데, 블랙리스트 IP 정보를 빅데이터로 분석하여 APT 공격 전조 현상을 분석하고 DNS 로그를 이용한 악성코드를 분석하는 방식을 제안하고 있다[9].

시스템 로그의 분석도 중요하지만 신종 보안 공격에 대응하는 또 다른 방식은 이상 징후를 공격받기 전과 공격 과정에 탐지하는 것이다. 탐지를 위한 데이터 수집 방식은 다양하다. 침입 탐지를 위한 실험 데이터에 의존하지 않고 네트워크의 과거 상황 정보를 기록하고 현 시점의 네트워크가 정상인지를 판단하는 방법도 있다[10]. 제안 방식은 네트워크 전반에 대한 상태를 기록하고 공격을 판단하므로 세부 장치에 대한 공격 징후를 판단하기에는 무리가 있다. 호스트 비정상 행위 탐지 시스템도 제안되고 있다[4]. 제안 시스템은 사전에 공격을 탐지하기 위한 패스트 데이터 기반의 탐지 시스템으로 공격의 실시간 탐지를 위해 특성 인자 벡터 트리를 구축하여 프로세스 실행 이력을 추적하고 프로세스 행위의 변경을 상관 분석하는 방법을 사용한다.

Ⅲ. 제안 시스템 개요

사물인터넷 환경의 경량 센서, 전력 측정 장치, 네트워크 인프라 장비, 보안 장비 등 대부분의 장치들은 주기적으로 수치 데이터를 생성한다. 이런 시계열 데이터를 생성하는 장치는 단일일 수도 있고 다수 개로서 속성에 따라 그룹을 형성할 수도 있다. 예를 들어, 동일한 지역(속성)에 분포되어 있는 다수 개의 해수 온도 센서는 그룹을 형성할 수 있으며 비정상 시계열 데이터 탐지 시스템은 동일 그룹에 속하는 해수 온도 센서들로부터 각기 상이한 시계열 데이터를 입력받을 수 있다. 그밖에, 비정상 시계열 데이터 탐지 시스템은 동일한 네트워크(속성)에 다단계로 연동되는 다수의 하위 네트워크 또는 다수의 보안 장비(게이트웨이, 모뎀, 서버 등)로부터 각기 상이한 시계열 데이터를 입력 받을 수 있다. 그림 1은 제안 시스템의 구성도를 나타낸다.

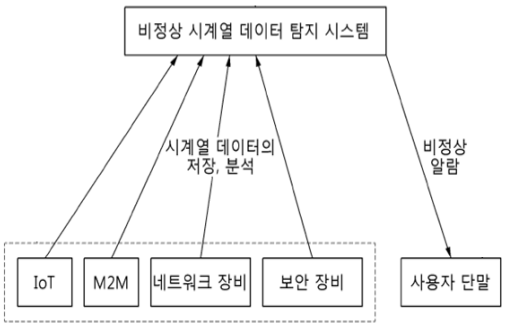

그림 1. 제안 시스템 구성도
Fig. 1. Proposed system architecture

비정상 시계열 데이터 탐지 시스템은 다양한 네트워크 구성 장치로부터 주기적으로 연속되어 입력되는 시계

열 데이터를 분산 저장한다. 입력 데이터는 다양한 유무선 네트워크를 활용하여 전달되거나 관리자로부터 직접 입력받을 수도 있다. 그림 1에서 사용자 단말은 탐지의 대상 장치를 등록하고 비정상 상태의 알림을 전달받는 관리 장치를 의미한다. 시계열 데이터 탐지 시스템을 통해 저장된 정보는 통계적 기법을 활용하여 다단계 분석되어 비정상 데이터를 탐지하게 된다.

제안하는 시계열 데이터 탐지 시스템은 다단계로 탐지를 수행하는데, 1차 단계로는 대상 장치에서 가장 최근에 입력된 복수 개의 시계열 데이터를 기준으로 입력되는 시계열 데이터가 산출된 신뢰구간에 포함되는지 여부를 확인한다. 1차 판정 후 2차 판정 단계를 수행하여 대상 장치에서 입력한 데이터의 정상 여부를 확정하게 된다.

2차 단계에서는 탐지하고자 하는 시계열 데이터와 동일한 속성(시간적 동일 속성)으로 분류되는 시계열 데이터를 이용하여 비정상 여부를 확정하게 된다. 즉, 1차 단계는 최근의 시계열 데이터를 사용하고 2차 단계에는 데이터 속성을 기반으로 데이터를 사용한다. 예로 시간의 속성을 사용할 경우 1일 전, 1주일 전, 2주일 전, 한 달 전, 또는 일 년 전 등과 같은 해당 주기에 입력된 시계열 데이터를 기준으로 산출한 신뢰구간을 기준으로 판단한다. 이 후 판정의 정확성을 높이기 위해 3단계 판정을 수행할 수 있다. 이 경우 신뢰구간 산출에 사용되는 시계열 데이터는 탐지하고 하는 대상 장치와 동일 그룹(예컨대, 동일 지역, 동일 네트워크, 동일 대상 감지 센서 등)에 속하는 다른 장치들로부터 취득된다.

게이트웨이 장치로부터 특정 웹 사이트의 트래픽 데이터(시계열 데이터)가 매분 연속되어 입력되는 경우를 가정하여 설명하면 다음과 같다.

1단계 판단을 위해 제안시스템은 현재 입력된 트래픽 데이터(대상 시계열 데이터)에 대한 비정상 여부 판별 시 가장 최근에 입력된 N개의 트래픽 데이터를 선택할 수 있다. 정규분포에 가까워지는 수치를 고려할 때 N은 일반적으로 100으로 설정될 수 있다. 게이트웨이에서 이전에 입력된 트래픽 데이터 중에서 가장 최근 100개의 트래픽 데이터를 이용하여 1단계 탐지에 적용되는 신뢰 구간은 다음 수식과 같이 산출될 수 있다. 현재 입력된 트래픽 데이터가 수식 (1)의 신뢰구간에 포함되면 정상으로 판별하고 포함되지 않으면 비정상으로 판별한다.

신뢰구간 = 평균값 ± 표준 편차 * R (1)

수식 (1)에서 상수 R은 비정상 시계열 데이터가 나타나는 확률과 연관될 수 있으며 관리자에 의해 2 또는 3으로 사전에 설정될 수 있다. 'R=2'인 경우, (평균값 ± 표준편차 * 2)의 신뢰구간 안에 대상 시계열 데이터가 포함되지 않으면 표준 정규 분포 확률 상 4.6% 정도로 예외 값(비정상 시계열 데이터)이 나타날 수 있다. R의 값이 2보다 커질수록 비정상 시계열 데이터가 나타날 확률은 낮아진다. 'R=3'인 경우, 신뢰구간 안에 대상 시계열 데이터가 포함되지 않으면 표준 정규 분포 확률 상 0.4% 정도의 예외 값이 나타나므로, 'R=2'인 경우에 비해 비정상 시계열 데이터가 나타나기 어렵다는 것을 의미한다.

1차 판별 결과가 비정상일 경우 수행되는 2단계 탐지에서는 현재 입력된 트래픽 데이터의 이전에 입력된 트래픽 데이터 중에서 시간 속성 값이 일치하는 트래픽 데이터(예, 1일 전, 1주일 전, 1달 전의 현재 시각에 입력된 데이터)를 판단 근거로 사용한다. 또는 현재 입력된 트래픽 데이터와 시즌값(귀성 시즌)이 일치하는 트래픽 데이터(예, 설, 추석 등의 귀성 시즌에 입력된 트래픽 데이터)를 신뢰구간 산출에 적용할 데이터로서 선택할 수도 있다. 신뢰구간 산출 및 산출에 사용되는 저장 데이터 수는 1단계와 동일하다.

제안하는 탐지 시스템에서는 2단계 분석을 통해 1단계에서는 비정상처럼 보이는 값이라 해도 특정 반복 시점에는 정상일 수 있다는 점을 이용하여 대상 시계열 데이터를 재판별할 수 있다. 예를 들어, 매주 월요일 오전 9시만 되면 높은 값의 시 계열 데이터가 입력되는 경우, 오늘(월요일)에 입력된 대상 시계열 데이터에 대해 정상으로 확정할 수 있다. 따라서 제안 시스템에서는 단순히 최근에 입력된 복수 개의 시계열 데이터에 기초하여 현재 입력된 시계열 데이터의 비정상 여부를 판별하는 것이 아니라 대상 시계열 데이터와 시간적 속성이 동일한 복수 개의 2 단계 데이터를 추출하여 통계적으로 분석하고 이에 기초하여 비정상 여부를 최종 판별 함으로써 비정상 시계열 데이터의 탐지 성능을 높일 수 있다.

3단계는 대상 장치와 상이한 타 장치들로부터 입력 된 시계열 데이터 중에서 대상 시계열 데이터와 동일 주기에 입력되는 시계열 데이터를 그룹적 동일 속성으로 분류하여 사용할 수 있다.

그림 4는 시계열 데이터 탐지 방법의 순서를 도시한 흐름도로 95%의 신뢰도를 갖는 신뢰구간을 산출하는 것을 가정하여 나타냈다.

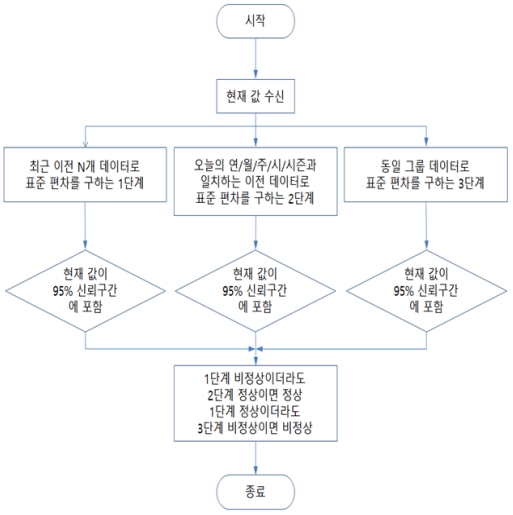

그림 2. 비정상 탐지 순서 흐름도
Fig. 2. Flow chart for abnormal detection

Ⅳ. 적용 시나리오

본 장에서는 제안하는 시계열 데이터 탐지 시스템이 웹 서비스를 제공하는 네트워크 장비를 대상으로 비정상 트래픽 발생을 탐지하는 적용 시나리오를 설명한다. 그림 3은 대상 장치에서 입력되는 시계열 데이터에 대한 1단계 분석 과정을 나타낸다.

그림 3의 (ⅰ)는 비정상 탐지를 수행하기에 직전 입력의 개수(즉, 100개 미만)가 부족한 상황을 나타낸다. 그림의 (ⅱ)는 1단계의 분석 결과가 정상인 예시를 나타내는데 네트워크 장비로부터 입력된 현재 트래픽 데이터의 직전에 입력된 100개의 트래픽 데이터(점선 네모 박스)를 이용하는 예를 보인다. 본 예에서는 기존에 입력된 100개의 트래픽 데이터에 따라 산출한 95%의 신뢰구간 내에 현재 입력 데이터가 포함될 경우 정상으로 판별한다. 그림 (ⅲ)은 입력 데이터가 산출된 95%의 신뢰구간 내에 포함되지 않아 비정상으로 판별된 경우를 나타낸다. 신뢰구간에 대한 신뢰도는 95%와 같이 상수로 지정될 수도 있고 신뢰도 CI(Confidence interval)와 같은 변수로 지정될 수도 있다.

그림 4는 입력된 시계열 데이터에 대한 2단계 분석을 실시하는 예를 나타낸다.

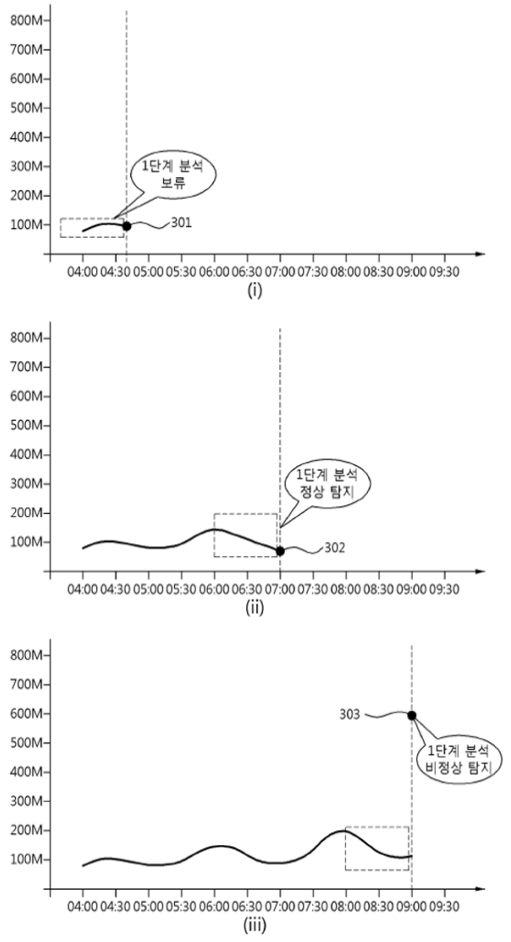

그림 3. 1단계 분석 과정
Fig. 3. First phase of analysis

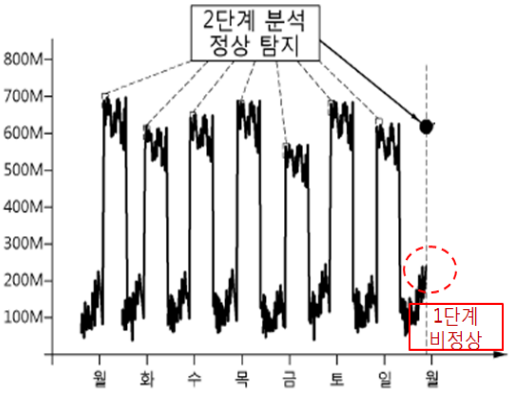

그림 4. 2단계 분석 과정
Fig. 4. Second phase of analysis

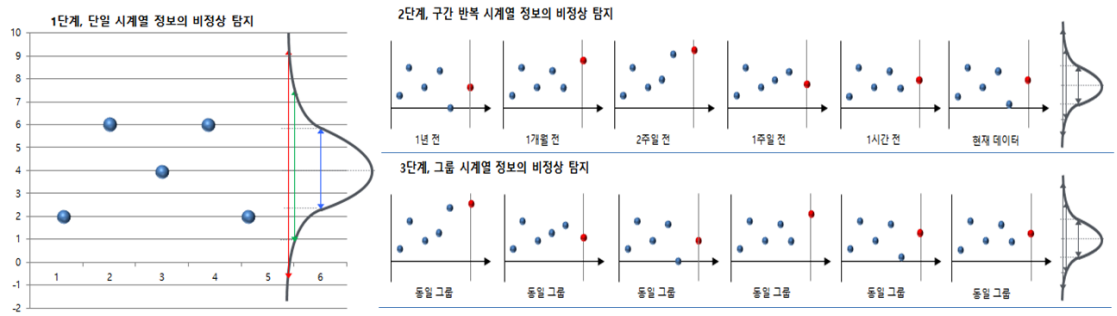

그림 5. 다단계 비정상 탐지
Fig 5. Multi-phase abnormal detection

제안하는 탐지 시스템은 1단계에서 비정상처럼 보이는 값이라 해도 특정 반복 시점에는 정상일 수 있다는 점을 이용한다. 트래픽이 급증하는 월요일 오전 입력 데이터를 주말 데이터를 기준으로 판정할 경우 비정상으로 나오지만 일주일 전 동일 시간대의 데이터와 비교할 경우 정상으로 판정되는 예를 들 수 있다.

더 나아가 동일 장치가 아닌 그룹 속성이 유사한 상의한 장치의 데이터를 기반으로 3단계 판정을 수행 할 수도 있다. 즉, 3단계 분석을 통해 동일 주기에 입력된 서로 다른 시계열 데이터 간의 관계를 더 고려하여 대상 시계열 데이터에 대한 비정상 여부를 확정할 수 있으며 비정상 정도까지 파악할 수 있다. 탐지 시스템은 1단계 분석 결과 정상이지만 3단계 분석에서 비정상으로 판별되면 비정상으로 확정할 수 있다.

V. 결 론

본 논문에서는 알려지지 않는 보안 공격에 대응할 수 있도록 입력된 데이터를 단계별로 판정할 수 있는 비정상 탐지 기술을 제안하였다. 입력되는 데이터의 1차 비정상 탐지를 수행하고 비정상으로 판정된 경우 시간이나 그룹의 속성을 판단하여 속성이 동일한 시계열 데이터를 이용하여 2차 비정상 여부를 확정하는 방식을 수행하여 오탐율을 최소화할 수 있었다. 제안 시스템은 판정 단계와 적용 방식의 확장이 용의하고, 탐지 결과에 대한 실효성을 극대화하도록 설계되어 다양한 영역에 적용될 수 있을 것으로 기대된다.

References

[1] S. Li, L. D. Xu, and S. Zhao, “The internet of things: a survey,” Information Systems Frontiers, Springer, Vol. 17, No. 2, pp. 243-259, April 2015. DOI: https://doi.org/10.1007/s10796-014-9492-7.

[2] Jeongin Kim, Namhi Kang, "Secure Configuration Scheme for Internet of Things using NFC as OOB Channel," The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 16, No. 03, pp.13-19, June 2016.
DOI: https://doi.org/10.7236/JIIBC.2016.16.3.13

[3] Jiye Park, Namhi Kang, “Design of Smart Service based on Reverse-proxy for the Internet of Things,” The Journal of the Institute of Internet, Broadcasting and Communication, Vol. 14, No. 06, pp.1-6, Dec. 2014.
DOI: https://doi.org/10.7236/JIIBC.2014.14.6.1

[4] Myungcheol Lee, Daesung Moon, Ikkyun Kim, “Real-time Abnormal Behavior Detection System based on Fast Data,” Journal of the Korea Institute of Information Security and Cryptology, Vol. 25, No. 5, pp.1027-1041, Oct. 2015.
DOI: https://doi.org/10.13089/JKIISC.2015.25.5.102

[5] Colin Tankard, “Advanced persistent threats and how to monitor and deter them,” Network Security, Vol. 2011, No. 8, pp. 16-19, Aug. 2011.
DOI: https://doi.org/10.1016/S1353-4858(11)70086-1

[6] Mark Stamp, “Information Security, Principles and Practice,” Wiley, ISBN 978-0-470-62639-9, May

2011.

[7] Z. Zulkefli, M. M. Singh, N. H. A. H. Malim, "Advanced Persistent Threat Mitigation Using Multi Level Security - Access Control Framework," Vol. 9158, LNCS, Springer, pp 90-105, June 2015.
DOI: https://doi.org/10.1007/978-3-319-21410-8_7

[8] Elshoush. H. Tagelsir. and I. M. Osmank, "Alert correlation in collaborative intelligent intrusion detection systems - A survey." Applied Soft Computing In Press, Vol. 11, No. 7, pp.4349-4365, Oct. 2011.
DOI: https://doi.org/10.1016/j.asoc.2010.12.004

[9] Chan-young Choi, Dea-woo Park, "The Analysis of the APT Prelude by Big Data Analytics," Journal of the Korea Institute of Information and Communication Engineering, Vol. 20, No. 6, pp.1129-1135, June 2016.
DOI : https://doi.org/10.6109/jkiice.2016.20.6.1129

[10] Ho-sub Lee, Eung-ki Park, Jung-taek Seo, "A New Method to Detect Anomalous State of Network using Information of Clusters," Journal of the Korea Institute of Information Security and Cryptology, Vol. 22, No. 3, pp. 545-552, June 2012.

[11] Kyungho Son, Taijin Lee, Dongho Won, "Design for Zombie PCs and APT Attack Detection based on traffic analysis," Journal of The Korea Institute of Information Security & Cryptology, VOL.24, NO.3, Jun. 2014.
DOI : https://doi.org/10.13089/JKIISC.2014.24.3.491

[12] Poonam Sinai Kenkre, Anusha Pai, Louella Colaco, "Real Time Intrusion Detection and Prevention System," Proc. of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA), pp. 405-411, 2014.
DOI: https://doi.org/10.1007/978-3-319-11933-5_44

저자 소개

채 문 창(정회원)

- 1991년 2월 : 아주대학교 전자계산학 학사
- 2012 ~ 현재 : ㈜퓨쳐시스템 보안기술연구소 연구소장(상무)

<주관심분야 : 보안제품 개발, 네트워크 보안, 사물인터넷 보안>

임 혁(정회원)

- 1998년 2월 : 순천향대학교 컴퓨터공학과 학사
- 2014년 10월 ~ 현재 : ㈜퓨쳐시스템 보안기술 연구소 수석연구원

<주관심분야 : 유무선 인터넷통신, 네트워크 보안, 사물인터넷보안>

강 남 희(종신회원)

- 1999년 2월 : 숭실대학교 공학사
- 2001년 2월 : 숭실대학교 공학석사
- 2004년 12월 : University of Siegen, 공학박사
- 2009년 3월 ~ 현재 : 덕성여자대학교 디지털미디어학과 부교수

<주관심분야 : 유무선 인터넷통신, 네트워크 보안, 사물인터넷보안>

※ 본 연구는 미래창조과학부 및 정보통신기술진흥센터의 SW컴퓨팅산업원천기술개발사업(GCS과제 3차)의 연구결과로 수행되었음 (R7117-16-0090)