The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 18, No. 5, pp.9-15, Oct. 31, 2018. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2018.18.5.9
JIIBC 2018-5-2

사물인터넷을 위한 침입탐지 및 자가 치료 시스템의 설계

Design of an Intrusion Detection and Self-treatment System for IoT

오선진*

Sun-Jin Oh*

요 약 본격 5G 통신시대의 도래와 더불어, 최근 사물인터넷과 연관된 융합기술의 발전이 급속도로 진행되고 있다. 일상생활의 여러 분야에서 다양한 센서 등을 이용한 사물인터넷 융합기술이 활발하게 응용되고 있으며, 많은 사람들 사이에서의 대중화가 성공적으로 이루어지고 있는 상황이다. 하지만, 많은 사물들이 네트워크에 연결되어 이루어지는 사물인터넷에서의 보안은 극히 취약하며 시급히 해결되어야 할 과제 중의 하나이다. 본 연구에서는 이러한 문제를 해결하기 위해 사물인터넷에 외부로 부터의 침입 또는 비정상적인 행위(anomaly)가 있는지를 실시간으로 탐지하고, 침입이 탐지되면 침입 유형에 따른 해당 치료 백신 프로그램을 가동시켜 자가 치료를 수행하도록 하는 사물 인터넷을 위한 침입탐지 및 자가 치료 시스템을 설계하고자 한다. 아울러, 사물인터넷으로의 침입 유행을 차단하기 위하여 유사 상황 빈도에 따른 침임 경고 메시지 방송 등을 고려한다.

Abstract With the advent of the 5G communication era recently, advancement of the convergence technologies related to IoT has been progressed rapidly. IoT convergence technologies using various sensors are actively applied many fields in our lives, and it contributes to the popularization of these convergence technologies among many people successfully. The security problem of the IoT which connects many things on the network is critically vulnerable and is one of the most important challenge to be solved urgently. In this paper, we design an intrusion detection and self-treatment system for IoT, which can detect external attacks and anomalies in order to solve the security problems in IoT, perform self-treatment by operating the vaccine program according to the intrusion type whenever it detects certain intrusion. Furthermore, we consider the broadcasting of intrusion alarm message according to the frequency of similar circumstances in order to block intrusion contagious in IoT.

Key Words : Intrusion Detection, IoT, Self-treatment

Ⅰ. 서 론

최근 정보화 사회는 주변의 모든 사물들이 유•무선 네트워크로 초 연결되어지는 경향으로 발전해 가고 있으며, 이러한 연결 네트워크를 통해 인간 간의 소통뿐만 아니라 인간과 사물 그리고 인간을 배제한 사물 간 직접 소통하는 형태의 새로운 패러다임으로 그 변화가 현실화되고 있다. 이와 같이 네트워크를 중심으로 주변의 모든 사물들이 서로 연결되어 “초 연결 사회(hyper- connected society)”를 구축하고, 이를 기반으로 기존의 인간과 인간 간의 연결뿐만이 아니라 인간과 사물 또는 사물과 사물 간에 다양한 형태의 대용량 데이터 정보를 생산·가공·처

*종신회원, 세명대학교 정보통신학부
접수일자 : 2018년 7월 6일, 수정완료 : 2018년 9월 23일
게재확정일자 : 2018년 10월 5일

Received: 6 July, 2018 / Revised: 23 September, 2018
Accepted: 5 October, 2018
**Corresponding Author: sjoh@semyung.ac.kr
Dept. of Computer & Information Science, Semyung University, Korea

리·유통 과정을 거쳐 기존 재화의 가치를 높일 수 있는 새롭고 창의적인 생산 방식으로 부를 창출하는 ICT 기술을 소위 “사물인터넷(Internet of Things)”이라 한다.[1] 사물인터넷은 주위의 사물 하나하나가 인터넷에 단순히 물리적으로 연결된 것만을 의미하는 것이 아니라 사물들이 서로 연결되어 사물 단독으로는 제공하지 못하던 새로운 기능이나 부가 가치를 창출해 낼 수 있음을 의미한다.[2] 이러한 패러다임의 변화는 우리의 기본적인 삶의 모습뿐만 아니라 주변의 환경, 안전, 공공 서비스 등 많은 다양한 분야의 모습을 급속도로 바꾸어 가고 있다. 사물인터넷 구현을 위해서는 최근의 다양한 첨단 ICT 기술들이 요구되며 그 주요 기술로는 주로 무선기반 통신기술, 경량 임베디드 네트워크 기술, 자율형·지능형 플랫폼 기술, 빅 데이터와 데이터 마이닝 기술, 센서 기술, 상황인식 기술, 칩 디바이스 기술, 사용자 중심 웹 서비스 기술 그리고 보안 및 프라이버시 보호 기술 등이 포함된다.[1, 3] 이러한 사물 인터넷 구현을 가능하게 하는 기저에는 사용자들이 자유롭게 이동하면서 시간과 장소에 구애 없이 언제 어디서나 필요한 경우 네트워크에 접속해서 서비스를 받을 수 있는 무선 기반의 모바일 컴퓨팅 환경, 즉 Ubiquitous Computing 환경이 만들어질 수 있기 때문이다. 사물인터넷과 같은 차세대 무선기반 통신망은 인프라 구조를 갖는 무선망과 인프라 구조가 없이 필요한 경우 일시적으로 형성되는 모바일 애드 혹 망(MANET)을 포함한다. 이러한 네트워크 환경에서는 무엇보다도 외부의 침입이나 해킹 공격 등에 매우 취약할 수밖에 없으므로 네트워크 보안은 사물인터넷 기반 응용들에 매우 민감하고 중요한 이슈가 아닐 수 없다. 암호화와 같은 유선망을 위한 현존하는 보안기술들은 여전히 무선 기반의 네트워크 환경에서도 사용될 수는 있으나 사물인터넷과 같은 오픈된 다양한 형태의 이질적인 무선기반 망에서는 노드들의 특징 때문에 기존의 보안 기술에 대한 적용에 있어서 극히 제한적이다. 한편, 유비쿼터스 망을 기반으로 하는 사물인터넷 응용에서는 무선 기반 네트워크에서의 중앙 집중화된 권한이 절대적으로 부족하므로 방화벽 같은 기존의 유용한 보안 기술들이 제대로 사용될 수 없다. 또한, 유선망에서와 마찬가지로 무선기반 애드 혹 망에서도 도청(passive eavesdropping), 위장(spoofing) 그리고 서비스의 거부와 같은 보안 위협에 더욱 쉽게 직면하게 되며, 망의 애드 혹 특징 때문에 더욱 보안 위협이 가중되게 된다. 이와 같이 사물인터넷은 기존의 유선기반 네트워크에 비해 외부 공격이나 침입 등에 매우 취약하며 심지어 외부로부터 침입을 당했는지에 대한 탐지조차 어려운 상황으로 이를 보완할 수 있는 연구가 절실하다고 할 수 있다.

본 연구에서는 사물인터넷과 같은 유•무선 기반 네트워크 환경에서 각 노드들이 다양한 형태의 데이터 정보를 생산·가공·처리·유통 하는 과정에서 외부로 부터의 침입이나 비정상적인 행위(anomaly)가 있는지를 실시간으로 탐지하고 이를 식별하여 치료를 할 수 있는 침입 탐지 및 자가 치료 시스템을 설계하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구를 살펴보았고, 3장에서는 제안한 사물인터넷을 위한 침입 탐지 및 자가 치료 시스템의 시스템 모델을 서술하였으며, 4장에서는 침입탐지 모듈과 자가 치료 및 침입 유행 방지 모듈을 설계하였고, 5장에서는 설계한 시스템에 대한 모의실험과 성능 평가 및 분석을 수행하였으며, 마지막으로 6장에서 향후 연구내용과 함께 결론을 맺는다.

II. 관련 연구

사물인터넷은 각종 사물들에 센서와 통신 기능을 삽입해서 인터넷에 연결하여 지금까지는 경험하지 못했던 새로운 융합 서비스를 제공하는 기술을 의미한다. 최근 사물인터넷 응용에 대한 관심의 증가로 M2M 사물 통신과 같은 기회적 애드혹 망에서 대용량의 데이터를 전달하는 방송은 매우 중요한 기술 중의 하나이다. 이렇듯 사물인터넷은 다양한 이질적인 특성을 갖는 네트워크들이 연합하여 수많은 센서와 같은 사물들이 네트워크에 연결되어 대용량의 실시간 데이터 전송을 효율적으로 처리해야 하는 기능을 수행해야 한다. 따라서 사물인터넷의 특성은 전송하는 대용량의 데이터 트래픽 패턴, 네트워크의 토폴로지와 크기, 이동성 정도의 측면에 따라 그 에너지 효율성과 확장성에 커다란 영향을 미치게 되며, 망 성능을 좌우하는 중요한 요인이 된다.[4] 사물인터넷 상에서의 효율적인 대용량 데이터 전송과 처리를 위한 연구들이 최근 활발하게 이루어지고 있으며, 데이터 가용성과 전달의 효율성을 증가시키기 위해 호스트 중심 보다는 콘텐츠 중심으로, IoT 장치들과 객체들에 의해 생성된 관련된 데이터를 글로벌하게 엑세스 할 수 있도록 클라우드 기반 계층적 데이터 전달 방법을 제안하기도 하였

다.[5] 다음으로 사물인터넷 관련 중요한 토픽은 보안 이슈로 유•무선 기반 네트워크 환경에서 이질적인 다양한 경량 장치 형태의 사물들이 서로 완전히 연결되어 실시간으로 데이터를 교환하는 환경에서 무엇보다도 외부로부터의 공격이나 침입 및 비정상행위 등과 같은 네트워크 보안에 취약할 수밖에 없는 상황이다. 따라서 이와 관련된 연구가 활발하게 진행되고 있다. 최근 고도화된 사이버 공격에 효과적으로 대응하기 위한 방안으로 IoT 백신[6] 개발 시도나 이종 시스템 로그 정보를 빅 데이터로 활용하여 패턴기반 탐지 방법과 비정상 행위 탐지 방법을 병합하여 사이버 침해시도 탐지 모델을 제안[7]하기도 하였고, 네트워크에 위협적인 악성 트래픽을 효율적으로 탐지할 수 있도록 악성 트래픽에서만 발견되는 비트패턴을 시그니처로 추출하는 기법을 사용하여 탐지규칙을 작성하여 네트워크 트래픽 분석에 적용할 수 있는 효율적인 침입탐지 시스템을 제안하기도 하였다.[8, 9] 또한 사물인터넷 경량장치에서 일련의 주기를 통해 연속적으로 발생되는 시계열 데이터를 통계적 기법을 활용하여 분석하고, 분석정보를 기반으로 장치의 이상 유무나 비정상 징후를 탐지할 수 있는 다단계 비정상 탐지 시스템을 제안하기도 하였다.[10] 다양한 무선 기반의 네트워크상에서의 상황정보 데이터를 인식하고 수집하기 위해 SNS 등 무선 기반의 소셜 네트워크 구조를 인지하고 컴퓨터 내에서의 표현하는 방법에 대한 연구[11]도 진행되고 있으며, 구글은 네트워크를 통해 접속하는 사용자의 접근 유형을 가진 로그 파일정보를 분석하여 이 사용자에 대한 최근 웹의 접근 빈도와 방법, 구매 형태 및 인기도 경향 등의 행위패턴 분석을 통해 이 사용자의 취향에 맞는 상품 추천 및 마케팅 활동을 위한 기본 자료를 유추해 내기 위한 웹 로그 분석 방법을 제안하였다.[12]

Ⅲ. 시스템 모델

본 연구에서는 유•무선 기반 사물인터넷 환경에서 각 노드들이 다양한 형태의 데이터 정보를 생산·가공·처리·유통 하는 과정에서 외부로 부터의 침입 또는 비정상적인 행위(anomaly)가 있는지를 탐지하고 이를 식별하여 자가 치료를 할 수 있는 침입 탐지 및 자가 치료 시스템을 설계하고자 한다. 그림 1은 본 논문에서 제안하는 침입 탐지 및 자가 치료 시스템의 시스템 모델을 보여준

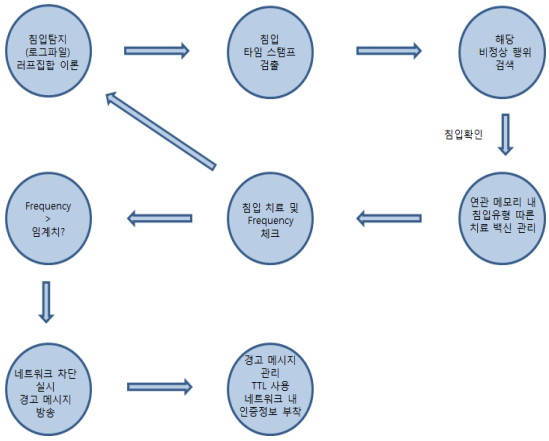

그림 1. 제안한 침입 탐지 시스템 모델
Fig. 1. Proposed Intrusion Detection System Model.

다. 무선기반의 사물인터넷 망에서의 효과적인 보안을 위해서 사물인터넷 망을 구성하고 있는 경량 장치나 센서로 부터 실시간으로 발생하는 상황정보를 수집하고 처리하는 백본 노드에서의 침입이나 비정상 행위가 발생했는지에 대한 정확한 탐지기법이 요구된다. 네트워크 환경에서의 다양한 침입이나 비정상 행위는 심각한 위협을 초래할 수 있으므로 이러한 침입을 효과적으로 탐지하기 위해 본 논문에서는 백본 노드에서의 네트워크 상태 로그 파일을 기반으로 하는 비정상 행위 탐지나 마이닝 기법을 이용한 침입 탐지 기법을 고려한다. 침입 탐지 시스템은 네트워크의 행위 데이터 로그 정보를 분석하여 오용 탐지나 비정상 행위 탐지 방식으로 판정하며 이때 러프 집합 이론을 적용한다. 이와 같은 침임 탐지 과정을 거쳐 실제 백본 노드 상에서 침입이나 비정상 행위가 탐지되면 정확한 침입 탐지시점을 기록하기 위해 타임스탬프를 검출하여 해당 비정상 행위를 검색해서 침입을 확인한 뒤, 침입 유형에 따른 해당 치료 백신 프로그램을 가동시켜 비정상 행위에 대한 자가 치료를 수행하게 된다. 침입에 대한 자가 치료가 달성되면 해당 비정상 행위 발생 빈도수를 갱신하고 다시 침입 탐지 모드로 복귀한다. 침입 탐지가 진행되는 동안 특정 비정상 행위에 대한 사물인터넷 망 내에서의 대유행을 방지하기 위해 이와 유사한 상황에 대한 비정상 행위 발생 빈도수를 단위 시간동안 측정하여 그 발생 빈도가 일정 임계치에 도달하면 해당하는 비정상 행위가 유행 단계에 접어들었다고 판단하여 이 시스템은 자가 치료에 이어 침입 유행을 제어하기 위해 현재의 통신망을 통해 주변의 이웃 노드들

에게 침입 경고 메시지를 방송하고, 일정 시간 간격동안 네트워크의 단절을 시도하여 침입 유행을 차단하도록 수행한다. 이때 침입 경고 메시지 방송으로 인한 네트워크 내의 혼잡을 방지하기 위한 트래픽 부하를 조절하기 위해 침입 경고 메시지에 대한 관리는 경고 메시지에 TTL 등을 부착하여 이 메시지의 전파 가능 최대 홉 수를 제한하여 네트워크 내의 경고 메시지 홍수를 방지하며, 또한 네트워크 침입자의 악의적인 용도로 네트워크를 통한 거짓 경고 메시지 방송으로 인한 피해에 대비하기 위해 방송되는 침입 경고 메시지에 대해 네트워크 내의 인증 정보를 부착하여 방송하는 방안을 고려한다.

Ⅳ. 침입탐지 및 자가 치료 시스템 설계

이 장에서는 본 논문에서 제안한 사물인터넷을 위한 침임 탐지 및 자가 치료 시스템을 설계하였다. 본 논문에서 제안한 시스템은 외부로 부터의 침입 또는 비정상적인 행위가 있는지를 실시간으로 탐지하는 모듈과 침입탐지가 감지되었을 때 이를 스스로 치료하고 사물인터넷 망을 통해 유행하는 것을 방지하기 위한 모듈로 구성된다.

1. 침입탐지 모듈 설계

사물인터넷을 구성하는 백본 노드에서의 침입 탐지를 위해 시간의 흐름에 따라 수집되는 노드 활동과 프로파일 정보를 기반으로 특정 이벤트에 대한 퍼지니스 정도에 따른 비정상 행위 정도를 나타내기 위해 러프 집합을 사용한다. 러프 집합의 기본 개념은 식별(classification)과 근사(approximation)이다. 러프 집합 이론은 어떤 집합에서 확실하게 분류되는 하한근사와 불확실하게 분류되는 상한근사 집합 이론을 통해서 나타낸다. 동치관계에 의해 정보 객체 집단은 동치류로 나뉘어 질 수 있고 상한근사에서 하한근사를 제외시키면 불확실한 객체들만 또 다른 부분집합으로 표현될 수 있으며 이를 경계영역이라 한다. 확률적으로 일정한 빈도 이상 나타나는 비일관적 데이터에 대해 일관적인 데이터로 간주하여 데이터에 대한 오차와 융통성을 부여함으로써 데이터에 포함된 불확실성의 영향을 최대한 줄이면서 효과적으로 규칙을 도출하고자 한다. 비정상 행위 탐지기법은 시스템 상태와 노드 행위의 정상 프로파일을 생성하고 그것을 현재 활동과 비교하여 만약 정상상태로부터 상당한 이탈이 관찰되면 그 이탈 정도에 따라 경고를 발령한다.

< IoT 백본노드에서의 비정상 행위 탐지 >

1. 백본노드에서의 데이터 전송 패턴으로부터 특징 추출

   단위 시간 동안 노드 내 데이터 크기 변화량(SZ),
   단위 시간 동안 유입되는 데이터 트래픽 변화량(TF),
   단위 시간 동안 노드의 라우팅 변화량(RT),
   각 엔트리의 신뢰도(RL)를 갖는 노드의 정상 특징정보 기초
2. IoT 백본노드에 대한 정상 특징정보 시스템 구축

   (RQ#, SZ, TF, RT, RL, TM)

   TM : 프로파일내의 엔트리 성숙도 등급
3. 러프집합 이용 프로파일 동치관계 클래스 추출

   1) 결정 동치 클래스 : $X = \{RL\}$

   2) 조건 동치 클래스 : $Y = \{SZ, TF, RT\}$

   3) 퍼지 포함관계 결정
4. 이탈정도(deviation number) 계산 (ω_{TM} : TM 가중치)

$$\mu(X,Y) = 1 - \frac{\sum_{TM=1}^{n} [Card(\overline{R}X \cap \overline{R}Y) \times \omega_{TM}]}{\sum_{TM=1}^{n} [Card(\overline{R}X \cup \overline{R}Y) \times \omega_{TM}]}$$

5. 허용 임계오차 ϵ과 비교

   if $\mu(X,Y) > \epsilon$, 노드 비정상 행위 탐지 경고 발령

그림 2. 러프집합 기반 비정상 행위 탐지 알고리즘
Fig. 2. Rough Set based Anomaly Detection Algorithm

여기서 TM은 사용자 프로파일 엔트리의 시스템 존속시간(즉 성숙도)을 나타내는 것으로 TM이 작을수록 시스템에 최근 입력된 새로운 프로파일 엔트리를 나타내며 그 신뢰도가 비교적 낮음을 의미하고, 상대적으로 TM이 큰 엔트리는 보다 높은 정상 신뢰도를 나타내는 것으로 노드 활동에 대한 정상 이탈 정도를 계산할 때 TM에 따른 차별화된 가중치를 부여한다.

2. 자가 치료 및 유행 방지 모듈 설계

사물인터넷을 구성하는 백본 노드에 대한 공격이나 비정상행위로 인한 침입이 감지되면 정확한 침입 탐지가 이루어진 시점을 기록하기 위해 타임스탬프를 검출하고, 어떤 형태의 침입인지 확인하여 해당 침입 유형에 따른 자가 치료를 수행하기 위해 치료 백신 프로그램을 가동시킨다. 이 때에는 침입으로 인한 침해사고 분석과 최근 유행하는 보안 공격 유형에 따른 보안 백신 프로그램을 구동하여 자가 치료를 수행하게 된다. 이와 더불어 침입이나 비정상 행위 유행을 가늠하기 위해 해당 침입에 대한 발생 빈도 카운터를 갱신하고 난 뒤 다시 침입 탐지

모드로 복귀한다. 침입에 대한 탐지와 치료뿐만 아니라 사물인터넷 망 내에서의 대유행을 방지하는 것도 매우 중요하기 때문에 유사 상황에 대한 비정상 행위 발생 빈도수를 단위 시간동안 측정하여 그 발생 빈도가 일정 임계치에 도달하면 해당 비정상 행위가 유행 단계에 접어들었다고 판단하여 시스템은 침입 유행을 제어하기 위해 통신망을 통해 이웃 노드에 침입 경고 메시지를 방송하고, 일정 시간 간격동안 네트워크의 단절을 시도하여 침입 유행을 차단하도록 수행한다. 이때 침입 경고 메시지 방송으로 인한 네트워크 내의 혼잡을 방지하기 위한 트래픽 부하 조절을 위해 경고 메시지에 TTL 등을 부착하여 이 메시지의 전파 가능 최대 홉 수를 제한하여 네트워크 내의 경고 메시지 홍수를 방지하는 것 이 필요하며, 또한 침입자의 망을 통한 악의적 거짓 경고 메시지 방송으로 인한 피해에 대비하기 위해 방송되는 침입 경고 메시지에 대해 네트워크 내의 인증 정보를 부착하여 방송하는 방안을 고려한다.

V. 평가 및 분석

본 논문에서 제안한 IoT를 위한 침입탐지 시스템에 대한 성능평가를 모의실험을 통해 허용 임계오차에 대한 침입 탐지율(detection rate)과 거짓 경고율(false alarm rate)로 하였다. 여기서 침입 탐지율은 모의실험 기간 중 발생한 총 비정상 행위 중에서 정상적으로 침입 행위를 탐지한 비율을 말하며, 거짓 경고율은 모의실험 기간 중 침입 행위가 아닌 활동을 침입으로 잘못 탐지한 비율을 말한다. 모의실험에 사용한 주요 파라미터는 다음의 표 1과 같다.

표 1. 모의실험 파라미터
Table 1. Parameters for a Simulation Study

Parameters	Value
Total # of Node in IoT	1000
Degree of SZ={S, M, L}	random(1, 3)
Degree of TF={L, M, H}	random(1, 3)
Degree of RT={L, M, H}	random(1, 3)
Degree of RL={1, 2, 3, 4}	random(1, 4)
Degree of TM={1, 2, 3}	random(1, 3)
Threshold ϵ	[0.2-0.6]
- simulation study on Intel Pentium PC, with Microsoft Visual Studio C++ Compiler	

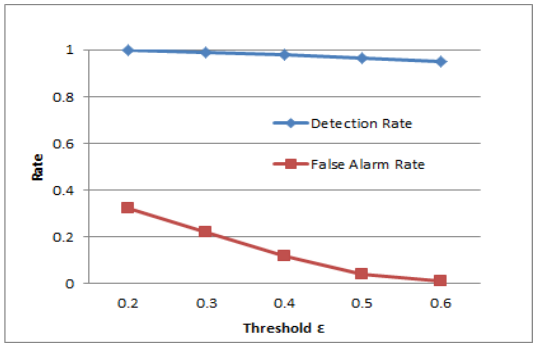

그림 3. 모의실험 결과
Fig. 3. Simulation Result

그림 3은 본 논문에서 제안한 사물인터넷을 위한 침입 탐지 시스템에 대한 모의실험 결과를 허용 임계오차에 따른 비정상 행위 탐지율과 거짓 경고율에 대하여 보여주고 있다. 그림에서 보인 바와 같이 허용 임계오차 ϵ이 작을 때 비교적 비정상 행위에 대한 탐지율이 높게 나타나고 있는데 이는 정상 행위에 대한 엄격한 행위 패턴을 적용함으로써 정상 활동에서 조금이라도 벗어나면 비정상 행위로 간주하였기 때문으로 생각되며, 하지만 이로 인해 정상 행위임에도 불구하고 비정상 행위로 간주되어 경고가 발령되는 경우 역시 늘어남에 따라 상대적으로 거짓 경고율이 비교적 높게 나타나고 있음을 알 수 있다. 허용 임계오차 ϵ이 커짐에 따라 비정상 행위에 대한 탐지율은 조금씩 낮아지는 것을 알 수 있는데 이는 넓어진 오차 범위내의 비정상 행위가 정상 행위로 판단되는 경우의 수가 증가하기 때문인 것으로 생각된다. 반면, 정상 행위에 대한 탐지 오류가 상대적으로 낮아지게 되므로 정상 행위에 대한 거짓 경고율은 낮아지는 것으로 판단된다. 그리고 허용 임계오차 ϵ의 변화율에 대해 비정상 행위 탐지율의 변화는 미미한 반면 거짓경고율의 변화율은 크게 영향을 미치는 것으로 나타났으며 특히 허용 임계오차 ϵ의 값이 0.4에서 0.5 사이에서 그 특징은 더욱 두드러지게 나타나고 있음을 알 수 있다.

VI. 결 론

21세기 정보통신 혁명은 5G기반 네트워크를 중심으로 주변의 모든 사물들이 서로 연결되어 “초 연결 사회”를 구축하고, 이를 기반으로 인간과 사물 또는 사물과 사물

간에 다양한 형태의 데이터 정보를 공유하며 기존 재화의 가치를 높일 수 있는 새롭고 창의적인 생산 방식으로부를 창출하는 “사물인터넷”시대라 할 수 있다. 하지만 사물인터넷은 기존의 유선기반 네트워크에 비해 외부 공격이나 침입 등에 매우 취약하며 심지어 외부로부터 침입을 당했는지에 대한 탐지조차 어려운 상황으로 이를 보완할 수 있는 연구가 절실하다고 할 수 있다.

본 연구에서는 사물인터넷과 같은 유•무선 기반 네트워크 환경에서 각 노드들이 다양한 형태의 데이터 정보를 생산·가공·처리·유통 하는 과정에서 외부로 부터의 침입 또는 비정상적인 행위가 있는지를 실시간으로 탐지하고 이를 식별하여 자가 치료를 할 수 있는 침입 탐지 및 자가 치료 시스템을 설계하고, 성능평가를 모의실험을 통해 허용 임계오차의 변화에 따른 침입 탐지율과 거짓 경고율로 분석하였다. 평가 결과 전반적으로 비정상 행위에 대한 탐지율은 허용 임계오차의 변화와는 무관하게 높게 나타났으며 반면, 거짓 경고율은 허용 임계오차의 변화율에 비교적 크게 영향을 받으며 상대적으로 높은 허용 임계오차에서 낮아지는 것을 알 수 있다. 향후 연구 과제는 실제 IoT 환경에서의 침입탐지 성능 평가와 백신 연구에 관한 것이다.

Ⅶ. References

[1] H. Y. Kim, Internet of Things: Concept, Implementation Technology, and Business, Hongrung Science Pub. Co., pp. 314, 2014.

[2] D. Lake, A. Rayes, M. Morrow, “The Internet of Things”, The Internet Protocol Journal, vol. 15, no. 3, September 2012.

[3] I. Jeon, S. Kang, H. Yang, “Development of Security Quality Evaluate Basis and Measurement of Intrusion Prevention System,” Journal of the Korea Academia-Industrial cooperation Society (JKAIS), Vol. 11, No. 1, pp. 81-86, 2010.

[4] I. H. Bae, C. H. Kim, H. T. Noh, “Design and Evaluation of a Fuzzy Logic based Multi-hop Broadcast Algorithm for IoT Application”, Journal of Internet Computing and Services, vol. 17, no. 6, pp. 17-23, 2016.
doi: 10.7472/jksii.2016.17.6.17.

[5] I. H. Bae, “Design and Evaluation of an Edge-Fog Cloud-based Hierarchical Data Delivery Scheme for IoT Application”, Journal of Internet Computing and Services, vol. 19, no. 1, pp. 37-47, 2018.
doi: 10.7472/jksii.2018.19.1.37.

[6] C. W. Lee, IoT Vaccine, Hanbit Media Inc., pp. 300, 2017.

[7] Y. B. Kwon, I. S. Kim, “A Study on Anomaly Signal Detection and Management Model using Big Data”, Journal of the Institute of Internet, Broadcasting and Communication(IIBC) vol. 16, no. 6, pp. 287-294, 2016.
doi: 10.7236/jiibc.2016.16. 6.287.

[8] S. I. Lee, S. C. Lee, J. R. Lee, H. Y. Youm, “Extraction of Network Threat Signatures using Latent Dirichlet Allocation”, Journal of Internet Computing and Services(JICS), vol. 19, no. 1, pp. 1-10, 2018.
doi: 10.7472/jksii.2018.19.1.1.

[9] S. J. Oh, “Design and Evaluation of a Weighted Intrusion Detection Method for VANETs”, The Journal of the Institute of Internet and Broadcasting and Communication (IIBC), vol. 11, no. 3, pp. 181-188, June 2011.

[10] M. C. Chae, H. Lim, N. H. Kang, “Design of Multi-level Abnormal Detection System Suitable for Time-Series Data”, Journal of the Institute of Internet, Broadcasting and Communication(IIBC) vol. 16, no. 6, pp. 1-7, 2016.
doi: 10.7236/jiibc.2016. 16.6.1.

[11] K. Y. Kwack, Social Network Analysis, 2ed. Chungram Pub., pp. 690, 2017.

[12] M. Akihiro, Google Analytics Access Kaiseki Kanzen Guide, Socym Co., pp. 239, 2014.

저자 소개

오 선 진(종신회원)

- 제 6권 제 2호 참조
- 현재 세명대학교 정보통신학부 교수

<주관심분야 : 스마트 응용, IoT, 빅데이터, 모바일컴퓨팅, USN 등>

※ 이 논문은 2017학년도 세명대학교 교내학술연구비 지원에 의해 수행된 연구임.