ISSN 2586-1816
Journal of Convergence for Information Technology
e-ISSN 2586-4440
Vol. 8. No. 6, pp. 149-157, 2018
DOI : https://doi.org/10.22156/CS4SMB.2018.8.6.149

IoT 계층별 보안위협 분석 및 대응기술 개선 방안 연구

원종혁[1], 홍정완[2], 유연우[3*]
[1]한성대학교 스마트융합컨설팅학과 외래교수, [2]한성대학교 산업경영공학과 교수, [3]한성대학교 스마트융합공학부 교수

A Study on the Improvement of Security Threat Analysis and Response Technology by IoT Layer

Jong-Hyuk Won[1], Jung-Wan Hong[2], Yen-Yoo You[3*]
[1]Adjunct Professor, Dept. of Smart Convergence Consulting, Hansung University
[2]Professor, Dept. of Industrial Management Engineering, Hansung University
[3]Professor, Faculty of Smart Management, Hansung University

요 약 최근 급격히 증가하고 있는 IoT 환경에서의 보안위협 대응방안에 관한 연구를 위해서 SDN Controller 기능을 활용한 침입감시 대응기술 방안을 연구하고자 한다. 연구방법은 IoT 계층별 보안위협에 따른 대응기술 및 적용되는 보안기술의 연구 동향 분석을 통해 향상된 IoT 보안위협 대응기술 구현 방안을 수립하였다. 연구결과는 기존의 IoT망의 네트워크스위치 장비에 OpenFlow 기반의 SDN Controller를 추가하여 샘플링 기법을 통한 탐지방법의 실효성을 연구하였다. 이 방법은 기존 IoT 기기의 성능에 영향을 미치지 않으면서도 IDS 및 IPS와의 연동만으로도 네트워크 전체의 모니터링 및 공격에 대한 탐지가 가능해 졌다. 이와 같이 향상된 보안위협 대응기술을 적용하면 IoT 보안위협 불안감 해소와 서비스 신뢰를 높일 수 있을 것으로 기대 한다.

주제어 : IoT 보안, IoT 프레임워크, IoT 보안기술, 오픈플로우, SDN 콘트롤러, IDS

Abstract In this paper, we propose an attack detection technology using SDN Controller to study security threats in IoT environment. The research methodology has been developed by applying IoT security threat management technology to the IoT layer and analyzing the research trend of applied security technology. The study results show that the effectiveness of the detection method using the sampling method is studied by adding OpenFlow based SDN Controller to the network switch equipment of the existing IoT network. This method can detect the monitoring and attack of the whole network by interworking with IDS and IPS without affecting the performance of existing IoT devices. By applying such improved security threat countermeasure technology, we expect to be able to relieve anxiety of IoT security threat and increase service reliability.

Key Words : IoT security, IoT framework, IoT security technology, OpenFlow, SDN Controller, IDS

1. 서론

정보통신기술(ICT)을 활용한 융·복합 기술의 발달로 인해 우리는 역사상 유례없는 편리함을 제공받고 있다. 이러한 편리함은 IoT 시대에 접어들면서 그 필요성이 더욱 높아져 가고 있다. 사람과 사물들, 그리고 사물과 사물 간의 네트워크 통신을 통한 인터넷 연결은 방대한 데이터를 주고받으면서 그 중요성이 커지게 되었다. 데이터 정보자산의 중요성이 높아지면서 이러한 정보를 악의적인 목적으로 사용하려는 IoT 보안위협도 함께 증가하게 되었다.

2016년 9월 발생한 '미라이(Mirai)' 악성코드의 공격으

*Corresponding Author : Yen-Yoo You(threey0818@hansung.ac.kr)
Received October 8, 2018 Revised October 31, 2018
Accepted December 20, 2018 Published December 31, 2018

로 IoT 기기 약 10만대가 해킹 되어 페이팔, 트위터, 아마존, 뉴욕타임즈 등 세계적 주요 호스팅 업체가 서비스 분산 공격(DDos)을 받게 되었다. 이와 같이 IoT 기기는 단순한 해킹에도 사이버 보안에 큰 위협이 된다는 것을 암시하였다. 최근에는 IoT 기기의 취약점을 이용한 개인정보 유출 등 보안 침해사고 발생으로 재산상의 피해 또한 증가하게 되었다.

이러한 보안위협에 대응하기 위해서 여러 기관과 기업에서는 다양한 대응전략을 수립하고 개선된 대응기술 개발을 위해 많은 노력을 하고 있다. 그러나 IoT 기기들은 저 전력, 경량화 기준으로 설계되는 구조적 특성의 한계점으로 인해 현실적으로는 제대로 된 보안 알고리즘을 탑재하지 못하고 있다[1]. 이러한 취약한 구조의 문제점을 파악하고 보안위협을 줄이기 위해서 Device와 제어할 수 있는 Application에 대한 접근 정책 및 규정이 제정되어야 한다. 그리고 기존의 IoT환경에서 발생하는 공격기법 분석과 신규 및 변종공격을 방지할 수 있는 차단 할 수 있는 연구가 시급한 상황이다[2]. 본 연구에서는 기존 구축되어 운영 중인 네트워크 스위치에 SDN Controller를 탑재시키고 침입감시시스템과 연동한 향상된 대응기술 방안을 제시하고자 한다.

2. IoT 기술 프레임워크

2.1 IoT 공통 프레임워크

사물인터넷 세계 포럼에서 정의한 “사물인터넷 기술 스택” 에 따르면 데이터 분석과 수직적 애플리케이션 연동은 사물인터넷의 핵심 동력으로서 데이터의 가치를 높이는 것이 IoT 시대의 가장 중요한 목적임을 강조 하고 있다. 그리고 사물인터넷 세계 포럼 아키텍처 위원회 에서는 IoT 데이터에 대한 큰 과제로서 데이터의 흐름이 느려지는 경향이 데이터의 가치를 급격히 떨어뜨린다는 점을 강조 하고 있으며, 이를 극복하는 방법으로서 네트워크 종단에서 실시간 분석 기능을 활용하여 보완점을 찾고 해결방안을 모색해야 한다고 하였다[3,4].

Table 1. 사물인터넷 기술 스택에서 정의한 내용은 다음과 같다. 먼저 Level 1 단계 에서는 사람들과 비즈니스의 참여를 통한 협업 프로세스를 갖추어야 하며, Level 2 단계 에서는 애플리케이션 상태를 제어하고 그 내용에 대한 보고 및 분석을 하고, Level 3단계 에서는 데이터 추상화를 위해 데이터 병합 및 데이터 액세스 처리 역할을 수행하게 된다. 그리고 Level 4단계 에서는 축적된 데이터를 저장하게 되며, Level 5단계 에서는 축적된 데이터의 분석과 변환 임무를 수행하게 된다. 그다음 Level 6 단계 에서는 통신기기들을 활용해서 네트워크 연결을 한 후 데이터를 처리하게 된다. 마지막으로 Level 7단계 에서는 사물인터넷 디바이스 기기들과 컨트롤러와의 연결을 통해 사물인터넷 기술을 완성 시키게 된다.

그리고 IoT 디바이스 장치들은 보안위협에 대응하기 위한 높은 수준의 암호화 알고리즘과 같은 대응기술을 집적시키기 어렵기 때문에 종단에서 침입감시 시스템을 활용해서 보안위협에 적절히 대응해야 하는 게 바람직하다고 정의하고 있다.

Table 1. Internet of Things Technical stack [3,4]

Step	Subject	Perform and Role
Level 7	Physical devices and controllers	Things ‘Things’ on the Internet
Level 6	Connectivity	Communication and processing equipment
Level 5	Edge computing	Data Element Analysis and Transformation
Level 4	Data accumulation	Save
Level 3	Data abstraction	Data Merging and Data Access
Level 2	Application	Reporting, analysis, control
Level 1	Collaboration and Process	Participation in business with people

2.2 IoT 기술 요소

가트너는 사물인터넷의 발전 가능성이 매우 높음을 강조하며 다음과 같은 방향성을 제시하였다. 그리고 사물인터넷(IoT)은 데이터 센터 모니터링 및 유지 관리, 공급망 관리 및 홈오토메이션에 이르기까지 연결성 및 추적 가능성이 무한하기 때문에 IoT 관련 비즈니스 전략 활성화를 위해서는 새로운 주요 기술을 습득하고 관리능력을 향상시켜야 한다고 하였다.[4]. Table 2와 같이 가트너가 발표한 IoT 관련 2017년과 2018년의 상위 10대 기술 요소에 대한 설명으로서 IoT 표준화 API 정립 및 플랫폼, 운영체제 및 프로세서, 저 전력 통신, 단거리 및 광역 네트워크 연결방식, IoT 디바이스 관리 및 데이터 분석, 그리고 IoT 보안기술에 대해 정의하고 있다.

Table 2. IoT Top Ten Technologies [4]

No	Technology	Technical Overview
1	IoT security	• Improved information intrusion protection • Improved physical infringement protection • Troubleshooting encryption, battery drain attacks • H / W and S / W are required for continuous security update
2	IoT analysis	• New Analytical Approach Needed • Need to improve analytical methods against increasing amount of data
3	IoT Device Management	• Device monitoring, firmware, SW update, complementary management, and monitoring management system needs to be upgraded
4	Low-power, short-range IoT network	• Balanced communication range, battery life, bandwidth and operating costs • Expansion of low-power, short- range network connections
5	Low power, wide area network	• Enable wide area IoT network • Battery life 10 years • Fast transmission speed • Lower hardware costs
6	IoT processor	• Determining features such as security and encryption capabilities, power consumption, software sophistication, and firmware characteristics • Improved HW design and functional implementation
7	IoT operating system	• IoT dedicated OS developed separate from existing OS • Developed OS for IoT hardware function requirement
8	Event stream processing	• Requires large data processing capabilities for real-time analysis • Development of Parallel Distributed Stream Computing Platform for High-Speed Data Stream Processing
9	IoT Platform	• Communication, device monitoring and management • Data collection, transformation, and management • Event-driven logic, application programming, visualization, analysis, and IoT application development
10	IoT standards and ecosystems	• Establish API for IoT standardization • Emergence of commercial and technical ecosystems to dominate the smart technology domain

상위 10대 기술 중에서 IoT 보안 기술의 문제를 가장 우선시 해결해야 한다고 강조 하였다. IoT 보안기술 이슈로는 향상된 정보침입 보호기능과 물리적 침해 보호능력이 필요하며 IoT 디바이스의 암호화 기능구현 과 보안위협 공격으로 인한 배터리 소모에 대한 문제 해결이 필요하다. 그리고 지속적인 보안 업데이트가 가능한 H/W 및 S/W 구현이 필수적으로 이행되어야 한다[5]. 그러나 IoT 디바이스는 저 전력, 경량화의 트렌드를 따라가느라 현실적으로 보안기술에 대해 만족할 만한 기능을 구현하지 못하고 있다.

3. IoT 보안위협 및 대응기술 동향

3.1 IoT 보안 요구사항

IoT 환경으로 변화하면서 각각의 연결된 IoT 장치들은 서로 간에 개인 정보 등 정보보안 침해의 위협요소가 발생 되었다. IoT 서비스의 대중화, 고성능화는 다양한 기능의 서비스를 제공하게 되면서 IoT 보안 메커니즘의 복잡성도 함께 증가하게 되었다. 이러한 복잡성으로 인해 서비스 제공에 대한 취약점이 증가하게 되었으며 보안 위협은 더욱 커지게 되었다. 따라서 IoT의 보안 요구사항은 기본적으로 법적 문제에 위배되지 않는 범위에서 설계가 고려되어야 하며 합법적이고 윤리적인 범위에서 설계되어야 한다. 그리고 체계적인 접근을 통한 기술적 과제 및 비즈니스 과제를 고려해서 구축하되 사회적 이슈를 반영하고 정치적으로 수용 가능한 방식으로 구현되어야 한다고 정의하였다[6-10].

IoT보안 요구사항은 국제적으로 ITU-T, IETF 등 표준화 단체를 중심으로 논의되고 있으며 ITU-T는 IoT 표준 참조모델을 통하여 디바이스, 어플리케이션, 네트워크 등에서 고려되어야 할 보안 요구사항들을 제시하고 있다. 그리고 IETF의 CoRE 워킹그룹에서는 IP기반의 IoT 서비스들을 위험수준에 따라 분류하고, 각각의 분류 체계별로 고려되어야할 보안 요구사항들을 논의 중이다. 한편, 전기·전자, 통신, 인터넷 등의 표준화 단체는 IoT 환경에 적합한 경량 인증・암호화 기술에 대한 연구 추진하고 있다[11].

3.2 IoT 계층별 보안위협 및 대응방안

IoT 환경에서의 계층별 보안위협은 한국인터넷진흥원의 보고에 따르면 Fig. 1과 같이 센서/디바이스 계층, 네트워크 계층, 플랫폼/서비스(애플리케이션) 계층과 같이 3가지 계층으로 분류해서 보안위협에 대해 대응방안을 마련해야 한다고 정의 하고 있다[12].

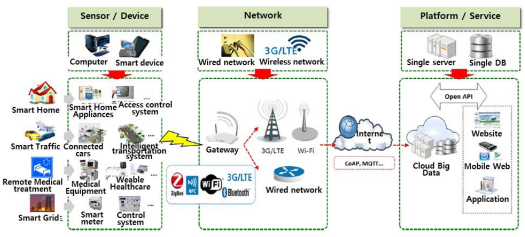

Fig. 1. IoT Environment Security Threats by Hierarchy [12]

기존의 M2M 기반에서의 IoT 디바이스 장치들 간에는 보안적으로 안전한 유무선 통신 프로토콜을 적용시켰으며 난수, 해시연산, 세션키, 공개키, 비밀키 등을 이용하여 설계를 하였다. 그리고 보안성을 더 높이기 위해 상호인증을 접목하는 방안을 적용시켰다[13]. 한편, IoT 계층별 보안 요구사항에 대한 정의로서 국외에서는 영국 잉글랜드 대학교의 산츠앙리 교수와 미국 올드 도미니언 대학의 리다쉬 교수가 Table 3과 같이 정의 하였다.

Table 3. Security Requirements by IoT Tier [14]

Step	Hierarchy	Security threats and countermeasures
Level 4	Application Interface Layer	• Complement SQL injection • Prevent viruses and malware • Prepare for scanning attacks • Secure Coding
Level 3	Service layer	• Privacy Protection Measures • Interception and manipulation defenses • False Forgery Defense • Wife Defense • Resend attack
Level 2	Network layer	• malware, DDOS attack defense • Guaranteed QoS • Data forgery attack defense • Hacking, unauthorized access control • Spoofing defense • Routing Failure Defense
Level 1	Sensing layer	• Lack of implementation of security functions due to minimization of cost and weight • Requires mounting of sensing devices such as RFID, sensors, and actuators • Designed for seamless communication between IoT devices • Requires wireless network, supervisory control, and data collection capabilities

3.2.1 센서/디바이스 계층

저사양의 취약한 디바이스에 대한 해킹으로서 초경량, 저 전력 디바이스에 대한 적절한 보안기술 적용이 어려운 약점을 보이고 있다. IoT 디바이스 수는 급속도로 증가하고 있으며 이에 따른 보안패치 적용, 관리, 모니터링의 어려움이 커지면서 관리 취약점이 증가하고 있다[15,16].

3.2.2 네트워크 계층

IoT 서비스의 통신 연결은 중간거점인 기지국 까지는 유선망을 사용하고 있으며, 디바이스와의 연결은 Wi-Fi, LoRa, 3G, LTE 등 무선네트워크 기반의 통신방식을 주로 사용 하고 있다. 최근 들어서 네트워크 트래픽이 증가하게 되면서 보안 침해 공격 시 디바이스가 악성코드 및 서비스 거부 공격에 감염되면 대규모 트래픽의 공격을 받게 되는 위험이 있다[15,16].

3.2.3 플랫폼/서비스/애플리케이션 계층

IoT 애플리케이션 계층은 서비스를 제공하는 계층으로서 openAPI 와 같은 오픈 플랫폼의 취약점을 악용하여 디바이스 및 서스비간에 데이터 위변조 및 탈취, 오작동을 유발시킨다. 그리고 디바이스로부터 수집된 정보를 가지고 조합하여 새로운 정보를 만들게 되면 개인정보 유출 및 프라이버시 침해 사고에 대한 우려가 커진다[15,16].

3.3 IoT 보안위협 대응기술 연구동향

IoT 계층별 보안위협에 따른 대응기술에 대한 연구는 Table 4와 같이 정부기관과 학계 및 보안 전문기업에서 활발히 이루어지고 있다.

Table 4. IoT security technology research trend [17]

Applied technology	Implement function
AES password design	• Implementation of AES-128 for RFID (ETRI) • Implementation of AES-256 MD5 based DTLS mutual authentication (Duksung Women's University)
Lightweight encryption algorithms and	• LEA, HIGHT, SEED (SHORT) • HB-family Protocol (Yonsei University) • OWL Model Context-aware Smart Home Control Technology (Kyunghee University)
End security	• Implementation of DTLS-based security technology (ETRI) • VPN Implementation for Devices (ETRI) • Implementation of PKI, IEEE1609.2- based vehicle communication security technology (Penta Security)
Device Security	• MTM Security Technology Development (ETRI) • Development of Open IoT Device Platform with Lightweight IP Protocol (KETI) • Smart IoT middleware platform development (ETRI)
Intrusion monitoring	• WSN sensor code integrity verification (Inha University) • WIPS (ETRI, Samsung Electronics, Konig Glory, Unet System) • NFV / SDN security vulnerability analysis and experiment (KAIST, Sungkyunkwan University)
SDN Controller	• Ator Research / NIM Networks / ETRI • SDN switch equipment (Pioneer) • Secure SDN / NFV building element technology (SKT / Samsung Electronics)

AES 암호설계 기술은 AES-128bit / AES-256bit 설계를 한국전자통신연구원(ETRI)과 덕성여대에서 구현

성과를 보였으며 경량 암호화 알고리즘 및 프로토콜 연구는 한국인터넷진흥원(KISA)과 연세대, KAIST, 경희대에서 활발한 연구 활동을 통해 구현을 성공하였다. 그리고 종단보안에 대한 기술 연구는 ETRI에서 DTLS 기반 보안기술과 디바이스에 대한 VPN 구현 기술을 확보하고 있으며 보안전문기업인 펜타시큐리티는 차량통신 보안 기술 구현을 보유하고 있다. 또한, 디바이스 보안은 ETRI와 전자부품연구원(KETI)에서 관련 플랫폼 개발을 완료하였으며 추가적인 보안 기능 개발에 노력을 하고 있는 중이다.

한편, 침입감시 및 탐지 기술연구와 SDN Controller에 대한 연구는 학계와 통신사, 보안전문기업에서 활발한 연구개발을 통해 어느 정도 요소 기술력을 확보하고 있지만 현재까지는 큰 성과를 얻지 못하고 있으며 아직까지는 활발한 연구단계 정도라고 할 수 있다[17].

4. 향상된 대응기술 구현

4.1 SDN Controller 활용기술 개요

IoT 디바이스는 저 전력, 경량화가 우선적인 목표로 설계되어지고 있다. 사물인터넷 시장의 확대로 인해 관심을 끌고 있는 방식으로는 IETE에서 발표한 Low Power WPAN (6LoWPAN)의 개념인 “인터넷 프로토콜이 가장 작은 장치에도 적용될 수 있어야 하고 적용되어야 한다.” 는 정의와 제한된 처리능력을 갖춘 저 전력 장치가 사물의 인터넷에 참여할 수 있어야 한다는 연구가 활발히 이루어지고 있다[18].

하지만 IoT 디바이스는 많은 연산이 필요한 암호화 알고리즘과 같은 보안기술을 접목시킨 복잡한 구조로 설계를 하지 못하기 때문에 디바이스 계층에서 보안위협에 취약한 구조를 보이고 있다.

이에 하드웨어 기능을 소프트웨어로 구현할 수 있는 일종의 가상화 기술인 SDN Controller를 접목시킨 후 침입감시 및 탐지기능을 활용한 보다 능동적으로 보안위협에 대응하는 방안이 이슈화 되고 있다.

IoT 기반의 관련 산업의 발전으로 인해 사용된 java, C 언어, xcode의 오픈소스 기반 소스프로그램을 만들고 개발하기 위하여 많은 투자개발이 이루어지고 있으며 이를 응용하여 다양한 분야에서 추가적인 개발이 가능하다[19]. 이에 본 연구에서는 Java로 개발된 오픈소스 기반의 OpenFlow Controller 개발하여 출력정보, QoS, ACL 기능구현이 가능하도록 설계하였다.

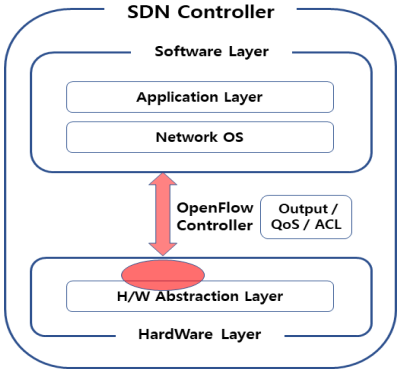

Fig. 2. SDN Controller Architecture

SDN Controller 구조는 Fig. 2와 같이 크게 소프트웨어 계층과 하드웨어 계층으로 구분되며 소프트웨어 계층은 어플레케이션과 네트워크 운영체제로 구성이 된다. 그리고 하드웨어 추상화 계층과의 사이에는 OpenFlow Controller를 접목시켜서 SDN Controller를 구현시키게 된다. 그리고 네트워크상의 모든 네트워크스위치에서 샘플링 수집을 수행한 경우보다 네트워크상의 플로우에 대한 악의적인 트래픽의 비율 값에 따라 샘플링 수집을 하게 되면 결손률이 훨씬 적게 측정이 되어 IDS 및 IPS에서 공격에 대한 감지율이 높아지게 된다. 최종 구현시 네트워크 계층에서의 제어를 통해 소프트웨어 계층인 어플레케이션 구간에서의 보안위협 탐지에 있어서 높은 성과를 보이는 것으로 성과를 보여주게 된다.

4.2 SDN Controller 활용기술 구현

4.2.1 SDN Controller 처리 구조

IoT 네트워크 환경에서 SDN Controller 기능 흐름도는 Fig. 3과 같이 설명할 수 있다. 첫 번째, IoT 기기가 보안침해 위협을 당하여 비정상 트래픽을 발생하게 되면 그 트래픽은 네트워크에 연결되어 있는 네트워크스위치 장비로 흘러간다. 두 번째, 네트워크스위치 장비에 흐르고 있는 비정상 트래픽을 SDN Controller에서 샘플링 기법을 통해 IoT관제센터 내 SDN Controller Server로 송신한다. 세 번째, SDN Controller Server 에서는 전달받은 트래픽을 IDS(또는 IPS)로 전달한다. 적용시킬 정책에 대한 명령을 전달한다. 네 번째, 전달받은 DB중에서

비정상 트래픽의 패턴을 분석하여 유해하다고 판단이 되는 트래픽을 선별하여 보안침해위협을 받고 있는 IoT기기와 연결되어 있는 네트워크 스위치의 비정상 패킷을 차단시킴으로서 트래픽의 정상화를 유지시킨다. 그리고 SDN Controller 서버에서는 해당 네트워크스위치 장비에 QoS 및 ACL 명령을 실행시켜서 트래픽 부하율을 줄이게 된다.

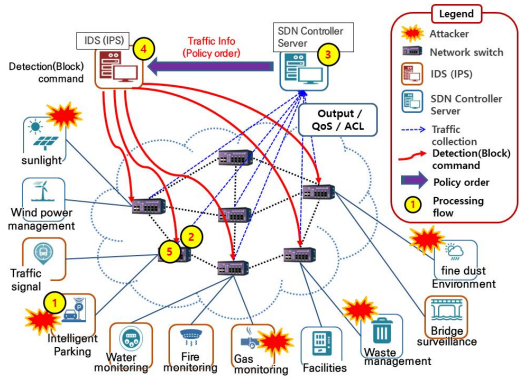

Fig. 3. SDN Controller Process Flow Diagram [12]

이 방안은 데이터를 송수신하는 복수개의 노드와 상기 노드 간의 플로우 송수신을 중계하는 네트워크스위치 및 침입탐지시스템(IDS)이 결합된 시스템에서 공격 데이터를 탐지하는 방법으로서 침해를 당한 IoT기기를 빠르게 찾아내어 다른 지역으로의 확산을 지연시키는 방법이다[12,13]. 기존의 네트워크스위치 장비에 Javascript 로 작성된 SDN Controller를 접목시켜서 IoT 디바이스와 연결되는 네트워크스위치에서 지정된 샘플링 패킷을 도출한 후 기존에 설치되어 운영 중인 IoT 관제센터 내의 침입탐지시스템(IDS) 및 침입차단시스템(IPS)에 발송해서 침입 판단에 따른 필요한 조치를 하는 구현 방식이다.

4.2.2 SDN Controller 처리 흐름도

SDN 기반에서 IDS는 네트워크상에서 흐르는 모든 패킷에 대해 검사가 가능하며 각각의 스위치에 대한 샘플링 비율을 설정함으로써, 악의적인 공격에 대한 감지를 효과적으로 수행할 수 있다. Fig. 4와 같이 SDN Controller 구현방식은 단계별로 다음과 같다[20].

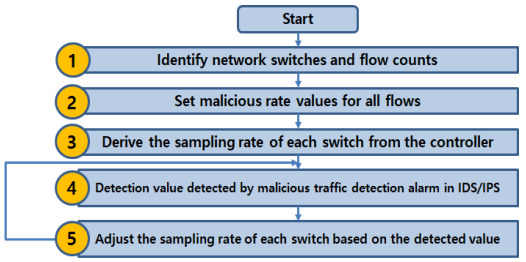

Fig. 4. SDN Controller utilization technology flow chart [20,21]

가. 구현 1단계

1) 각각의 플로우는 특정한 악의적인 공격 비율을 가진다고 가정
2) 어떤 플로우가 악의적인 패킷을 포함하고 있지 않다면, 악의적인 공격 비율은 “0”이 됨
3) 각 스위치의 플로우 위치는 SDN 컨트롤러가 파악
4) 이 정보를 통해서 기존 네트워크의 루팅 테이블과 같은 플로우 경로 정보를 도출

나. 구현 2단계

1) 부정 오류율(false negative rate)을 측정 (결손률이라고도 함)
2) 부정 오류 : IDS가 공격이 발생함에도 불구하고 어떠한 의심스런 공격을 감지하지 못하는 것

다. 구현 3단계

1) IDS에서 얼마나 많은 악의적인 의도가 담긴 데이터를 감지할 수 있는지 여부를 판단
2) IDS로 전송되는 모든 악의적인 패킷들이 감지된다고 가정하면, 악의적인 공격이 포함된 트래픽의 결손률을 최소화하도록 샘플링 비율을 설정함으로써 공격 탐지 시스템의 성능 강화
3) SDN 컨트롤러로부터 스위치 플로우 테이블 배당
4) 각각의 스위치에 대해 샘플링 비율을 설정
5) IDS가 악의적인 트래픽을 감지하는 경우에 경보를 발생하고, 감지 경보에 의한 검출 값을 도출
6) 각각의 악의적인 공격이 포함된 트래픽에 대해 악의적인 공격이 나타나는 비율을 계산

라. **구현 4단계**

1) IDS가 악의적인 트래픽을 감지하는 경우에 경보를 발생하고, 감지 경보에 의한 검출 값을 도출

2) 각각의 악의적인 공격이 포함된 트래픽에 대해 악의적인 공격이 나타나는 비율을 계산
3) 각 플로우에 대해 IDS로 전송된 데이터 패킷을 계산하고, 임의의 플로우에서 감지된 악의적인 패킷 의양을 비교하여 악의적인 공격이 발생하는 비율을 계산하여 검출 값을 업데이트
4) 각각의 스위치에 대해 샘플링 비율을 변경(Proposed sampling)한 경우에는 악의적인 공격의 트래픽이 IDS로 전달될 확률이 높아짐에 따라서 악의적인 공격에 대한 결손률이 점차 줄어듦

바. **구현 5단계**

1) 평균값에 의해 악의적인 공격이 나타나는 비율 값이 재설정되면 공격에 대한 결손률의 최댓값을 최소화하는 함수를 계산하고 이에 대한 샘플링 비율 벡터 값을 계산하여 샘플링 비율을 새롭게 설정
2) 악의적인 공격이 나타나는 비율의 재설정을 반복함에 따라서, 악의적인 공격이 나타나는 비율 벡터는 더욱 실제 값과 유사하게 설정될 수 있음

4.3 SDN Controller 적용한 결손률 측정

본 연구에서는 결손율 측정을 위해 30대의 네트워크 스위치를 구성하여 실험을 하였다. 실험방법은 네트워크 상의 모든 스위치에 대해 동일하게 샘플링을 수행한 경우와, 각각의 스위치에 대해서 특정구간에 대해 샘플링 비율을 변경한 경우를 나타낸다. Fig. 5와 같은 결과를 분석하면 모든 네트워크스위치에서 동일하게 샘플링(Fixed sampling)을 수행한 경우에는 결손률(missing rate)이 100%에 근접하게 나타나며 IDS 처리용량이 증가함에 따라 60% 이상의 값을 가짐을 알 수 있다. 이는 네트워크에 악의적인 공격이 발생했음에도 불구하고, 스위치에서 샘플링된 데이터 패킷이 악의적인 공격에 대한 패킷을 결손 함으로써 IDS에서 공격에 대한 감지가 제대로 이루어지지 않았음을 의미한다. 그러나 각각의 스위치에 대해 샘플링 비율을 변경(Proposed sampling)한 경우에는 악의적인 공격의 트래픽이 IDS로 전달될 확률이 높아짐에 따라서 악의적인 공격에 대한 결손률이 35% 수준에서 IDS 처리용량의 증가함에 따라 급속하게 0%에 가까워진다는 것을 알 수 있었다.

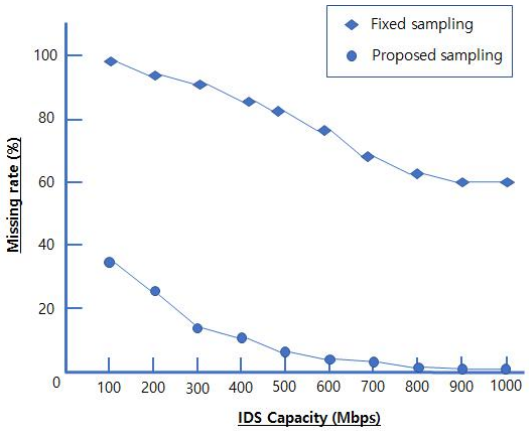

Fig. 5. Measurement of defect rate by sampling application ratio change using SDN controller

5. 결론

최근 IoT 환경에서의 디바이스 설계에 있어서 저 전력, 경량화가 우선 고려되고 있는 실정이다. 이러한 구조의 설계는 보안위협에 대한 기능추가를 고려하지 않기 때문에 이용자의 개인정보 유출에 대한 불안감 증가와 서비스 저하로 이어지게 된다. 만약 IoT 디바이스에 보안기능을 적용 시키면 외형이 다소 커지게 되며 중량 또한 증가하게 된다. 그리고 많은 연산처리 과정으로 인해 전력소모가 커져서 배터리 수명이 급격히 줄어들게 되어 제품 교체 수명도 함께 줄어드는 단점이 발생하게 된다. 이로 인해 제품 가격이 상승하게 되고 전반적으로 제품이 우수하지 못하다는 평가를 받게 될 수 있다.

이러한 문제 해결을 위한 방법 중에 SDN Controller 기능을 탑재한 IoT망의 네트워크스위치를 통해 관제센터의 IDS와 서로 연동하는 방법이 이슈화 되고 있다.

동작 방식은 네트워크망에 흐르는 패킷을 네트워크스위치에 적용시킨 SDN Controller에서 관제센터의 IDS 및 IPS 에 전달을 해주게 된다. 전달받은 트래픽 속에서 해킹 및 악의적인 패킷을 감지하여 관리자에게 즉시 알려주거나 스스로 차단시키는 방법이다.

이는 기존의 IoT 디바이스 성능에 영향을 주지 않으면서도 보안위협 요소를 사전에 탐지해서 차단할 수 있는 방법으로서 활발한 연구가 진행되고 있다. 최근에는 IoT망에서 동작되는 모든 네트워크스위치의 샘플링 비율을 트래픽 흐름양의 정도에 따라 자동으로 조절할 수

있기 때문에 악의적인 패킷이 IDS로 전달될 확률을 높일 수 있게 되었다. 또 다른 장점으로는 네트워크망의 크기에 비례해서 IDS의 수량을 증가시키지 않고도 특정 위치에 마련된 IDS에서 네트워크 전체 트래픽에 대해 공격 데이터의 유무를 검사할 수 있어 보다 효율적으로 네트워크에 대한 감시를 수행할 수 있게 되었다.

본 연구는 네트워크망의 전체 트래픽에 대해 공격 데이터의 유무를 검사할 수 있어 효율적으로 네트워크에 대한 감시를 수행할 수 있는 장점이 있다. 샘플링 패킷이 증가하여도 네트워크스위치 및 전송망 구간에서의 사용량에만 미비하게 영향을 미칠 뿐 IoT 디바이스에는 부하가 전혀 생기지 않기 때문에 전력공급 문제와 경량화에 문제가 되지 않는다.

한편, IoT 환경은 옥외 환경이 많기 때문에 온도, 습도, 먼지 환경 등에 강한 옥외용 산업용스위치 장비에 적용을 해야 한다. 산업용스위치 장비도 Ethernet 기반의 네트워크스위치 장비이기 때문에 향후 동일한 실험이 가능하며 만족할만한 결과를 예측해 볼 수 있다.

이와 같이 향상된 보안위협 대응기술의 개발을 통해서 기존의 IoT 기기에 SDN Controller 만을 추가하여 샘플링을 통한 네트워크 전체의 모니터링 및 공격 탐지가 가능해 졌으며 디바이스 자체에 대해 보안 기능을 추가하지 않고도 IoT 보안위협 불안감 해소와 서비스 신뢰를 높일 수 있을 것으로 기대 한다.

REFERENCES

[1] S. H. Hong & H. J. Shin. (2017). Analysis of the Vulnerability of the IoT by the Scenario. *Journal of the Korea Convergence Society, 8(9),* 1-7.

[2] J. O. Park. (2016). A Study of Message Communication Method Using Attribute Based Encryption in IoT Environment. *Journal of Digital Convergence, 14(10),* 295-302.

[3] Maciej Kranz. (2017). *The Core Objects of the Fourth Industrial Revolution The Future of the Internet IoT Innovation* : First Books Publishing. ISBN 979-11-7022-121-0 03320 / 2017.7.24.001

[4] *Things Internet World Forum Architecture Committee* 2015. http://iotforum.kr

[5] Gartner. *Top 10 Internet of Things Technologies for 2017 and 2018.* https://www.gartner.com

[6] R. Di Pietro, S. Guarino, N. Verde & J. Domingo-Ferrer. (2014). Security in wireless ad-hoc networks-a survey. *Comput. Commun. 51,* 1-20.

[7] H. Gaur. (2013). *Internet of things: thinking services.*

[8] D. Miorandi, S. Sicari, F. De Pellegrini & I. Chlamtac. (2012). Internet of things: vision, applications and research challenges. *Ad Hoc networks, 10(7),* 1497-1516.

[9] R. Roman & J. Zhou. (2013). On the features and challenges of security and privacy in distributed internet of things. *Comput. Networks, 57(10),* 2266-2279.

[10] R. H. Weber. (2013). internet of things-governance quo vadis. *Comput. Law Security Rev, 29(4),* 341-347.

[11] J. H. Kim, H. M. Jung & H. J. Cho. (2017). Design Plan of Secure IoT System based Common Criteria. *Journal of the Korea Convergence Society, 8(10),* 61-66.

[12] K. S. Jeon. (2016). *IoT Security.* https://kisa.or.kr

[13] J. O. Park. (2015). Verifying a Safe P2P Security Protocol in M2M Communication Environment. *Journal of Digital Convergence, 13(5),* 213-218.

[14] S. Li & L. Xu. (2017). *Securing the Internet of Things* : Acorn Publishing. ISBN 979-11-6175-039-2 / 2017.8.30.001

[15] B. Russell & D. V. Duren. (2017). *Things Security Guide for the Internet Age* : Acorn Publishing. ISBN 979-11-6175-041-5 / 2017.8.30.001

[16] S. S. Jang (2016). *General Information Protection* : Saengneung Publishing. ISBN 978-89-7050-848-1 93000 / 2016.10.31.001

[17] J. N. Kim & H. H. Jin. (2017). Internet(Iot) Security Technology for Security Threats in Second Connection Environment. *The Journal of The Korean Institute of Communication Sciences, 34(3),* 57-64.

[18] S. H. Hong. (2017). Research on IoT International Strategic Standard Model. *Journal of the Korea Convergence Society, 8(2),* 21-26.

[19] J. S. Lee. (2018). A Study of protective measures of the source program for the development of the Internet of Things (IoT). *Journal of the Korea Convergence Society, 9(4),* 31-45.

[20] H. Im, J. W. Kim, J. Na, T. J. Ha & C. Jung. (2016. 7). *Intrusion detection method in network.* Seoul : Metrocomnet Co., Ltd. ICT Research Institute

[21] M. H. Kang (2016). *Completion of IDS and security control* : Wowbooks Publishing. ISBN 978-89-94405-14-8 13560 / 2016.3.8.00

원 종 혁(Won, Jong Hyuk) [정회원]

- 2013년 8월 : 서울시립대학교 전기전자컴퓨터공학과 (공학석사)
- 2015년 8월 : 한성대학교 융합기술학과 (융합기술학석사)
- 2017년 8월 : 한성대학교 스마트융합컨설팅학과 (컨설팅학박사 수료)
- 2017년 9월 ~ 현재 : 한성대학교 외래교수 (정보보안 컨설팅 전공)
- 2002년 6월 ~ 현재 : (주)메트로컴넷 ICT연구소장
- 관심분야 : Information security, IoT security, Convergence security, System & Network security, Video security, Consulting
- E-Mail : smart@hansung.ac.kr

홍 정 완(Hong, Jung Wan) [정회원]

- 1994년 2월 : 서울대학교 대학원 산업공학과 (공학박사)
- 1994년 7월 ~ 1996년 2월 : 한국전자통신연구소 선임연구원
- 1996년 3월 ~ 현재 : 한성대학교 산업경영공학과 교수
- 관심분야 : Process Innovation, Consulting Methodology, Performance Evaluation, Service Science
- E-Mail : jwhong@hansung.ac.kr

유 연 우(You, Yen Yoo) [정회원]

- 1996년 2월 : 숭실대학교 산업경영학과 (경영학석사)
- 2007년 2월 : 한성대학교 행정학과 (행정학 박사)
- 1981년 7월 ~ 2002년 1월 : 해외건설협회 (기획, 전전략/IT컨설팅)
- 2002년 2월 ~ 2008년 8월 : 중소기업기술정보진흥원 (컨설팅, 경영혁신, CSR, IT, 서비스R&D, 기술혁신)
- 2008년 9월 ~ 현재 : 한성대학교 스마트융합공학부 교수
- 관심분야 : Consulting (Strategy, PM, 성과평가, MOT), CSR, Technology Innovation, Management Innovation, Service R&D, Franchise, 지식재산, 장애인 기업지원
- E-Mail : threey0818@hansung.ac.kr