Journal of The Korea Society of Computer and Information
Vol. 23 No. 2, pp. 45-51, February 2018
www.ksci.re.kr
https://doi.org/10.9708/jksci.2018.23.02.045

Small size IoT Device Monitoring System Modeling applying DEVS methodology

Se-Han Lee*, Hee-Suk Seo**, Yo-Han Choi***

Abstract

In this paper, we propose a Designed and Developed home router management system. Through the fourth industrial revolution and development of IoT technology, now people can experience a wide range of IoT related services at their workplace or daily lives. At the industrial site, IoT devices are used to improve productivity such as factory automation, and at home, IoT technology is used to control home appliances from a remote distance. Usually IoT device is integrated and controlled by the router. Home router connects different IoT devices together at home, however when security issues arise, it can invade personal privacy. Even though these threats exist, the perception for home router security is still insufficient.

In this paper, we have designed and developed home router management system using DEVS methodology to promote the safe use of home router. Through the DEVS methodology, we have designed the system and developed the mobile application. This management system enables users to set up security options for home router easily.

▸Keyword: Information Security, monitoring system, AP, IoT, DEVS methodology

I. Introduction

제4차 산업혁명에 대해서 전 세계적인 관심이 집중되고 있으며, 주요 기술인 IoT와 관련된 기술에 대한 다양한 연구가 진행되고 있다. 최근에는 IoT를 활용한 기술은 산업현장 뿐만 아니라 일상생활에서도 쉽게 접할 수 있게 되었다[1].

IoT기술 및 기기가 일상생활에 적용되어 다양한 IoT 서비스를 제공받을 수 있게 되었다[2]. 또한 IoT기기들이 점차 지능화되어 사용자와 더욱 밀접하게 연결될 것이다[3].

IoT기술이 일상생활의 다양한 부분에서 활용되면서 해킹 등의 보안 침해 사고 또한 급증하고 있다. 특히 IoT기기를 통합한 스마트홈(Smart Home)을 구축하는 가정용 공유에 대한사고가 증가하고 있다[4,5].

2016년 2월부터 6월까지 보안이 취약한 공유기를 통해 스마트폰이 악성코드에 감염된 피해가 발생했다. 이 기간 동안 감염된 스마트폰은 총 1만 3,501대이며, 악성코드를 통해 개인정가 유출되었다[6].

IoT기술은 의료, 교통, 에너지, 제조분야 등 사회기반 시설에도 다양하게 적용되고 있다. 사회기반시설에 적용된 IoT단말의 보안 사고가 발생하면 시민의 생명에 직/간접적인 위협이 될 수 있다[7,8].

본 논문에서는 안전하게 IoT기기를 관리할 수 있는 모니터링 시스템을 개발하였으며, 이를 통해서 사용자가 간편하게 IoT단말의 보안 설정과 안전한 IoT 서비스 환경을 구축할 수 있도록 IoT단말의 모니터링 서비스를 개발하였다.

• First Author: Se-Han Lee, Corresponding Author: Hee-Suk Seo
*Se-Han Lee (sehands@koreatech.ac.kr) Dept. of Computer Science & Engineering, Korea University of Technology and Education
**Hee-Suk Seo (histone@koreatech.ac.kr) Dept. of Computer Science & Engineering, Korea University of Technology and Education
***Yo-Han (yhchoi@koreatech.ac.kr), Dept. of Computer Science & Engineering, Korea University of Technology and Education
• Received: 2017. 12. 15, Revised: 2017. 12. 31, Accepted: 2018. 02. 02.
• This paper was supported by the education and research promotion program of KOREATECH.

II. Preliminaries

1. Related works

1.1 IoT Security Threats

IoT 서비스 및 단말은 단순한 터미널 및 시스템을 통해 운영되고 있으며, IoT기기의 하드웨어적 특성으로 인해 데이터 암호화 등 기존의 연산이 많이 필요로 하는 보안 기술을 적용하기 어렵다[9]. IoT요소는 IoT단말 자체, 데이터 서버, 센스 네트워크로 구분할 수 있으며, [Table 1]은 각 요소별 보안 취약성에 대해서 나타내고 있다[10].

Table 1. IoT Security Threats

Security Threat	Descriptions
IoT device vulnerability	Abnormal manipulation of input nodes and tags of information recognition Illegal wiretapping of data reader Illegal access of unauthorized users
Data server vulnerability	Unlawful wiretapping at the server Vulnerable to directory server attacks Vulnerable to illegal acquisition of data on servers
sensor networks Vulnerability	Difficult to apply and develop various security technologies due to characteristics of sensor network Security of physical location and accessibility of sensor is weak Security issues such as illegal data eavesdropping to sensor and physical removal of sensor and abnormal installation attempt

1.2 Case Study in IoT Security

IoT를 구성기기 중 가장 많은 피해가 발생하는 기기는 무선 공유기(Router)이다.

2016년 2월부터 6월 중순까지 보안에 취약한 공유기를 통해 스마트폰이 감염된 사례가 나타났으며, 이 기간 동안 총 1만 3,501대의 스마트폰이 감염되어 개인 정보가 유출되는 사고가 있었다[4]. 이 사례는 사용자가 IoT기기에 대한 보안에 무관심하다는 점을 악용한 사건으로 공유기의 기본 보안 설정만으로도 예방할 수 있었던 사건이다.

2017년 1월, 가정용 공유기의 DNS 설정 등을 변경하여 악성코드가 포함된 웹 사이트로 접속을 유도하는 트로이목마인 스위처(Switcher)로 인한 피해가 발생하였다[11].

정상적인 안드로이드 어플리케이션으로 위장하여 악성코드가 설치된 단말이 무선 AP에 접속할 경우 공유기의 관리자 계정을 탈취하기 위해 무차별 대입 공격(brute force attack)을 수행하고 관리자 계정 탈취가 성공하면 DNS 정보를 변경하는 방식으로 공격을 수행한다.

III. Management System for Home router

본 논문에서는 IoT기기를 사용하는 사용자를 대상으로 간편하게 보안설정을 수행하여 보안성을 강화하고, IoT기기의 모니터링 및 관리를 할 수 있는 IDASS(IoT Device Automatic Security Setting Sytstem)와 AMMS(AP Monitoring Management System)를 설계하였다.

설계한 IDASS와 AMMS는 안드로이드 애플리케이션으로 개발하여 사용자의 접근성화 활용도를 높였다.

1. IDASS and AMMS Modelling

1.1 DEVS methodology

B.P. Zeigler가 제안한 이산 사건 시스템 명세(discrete event system specifications; 이하 DEVS)는 계층적이고 모듈화 된 이산 사건 시스템을 표현하기 위한 방법론으로서, 집합이론을 기반으로 체계적으로 정립된 형식론이다. DEVS에서 대상 시스템은 시간을 기반으로 하는 입력, 상태, 출력, 상태 변환 함수들로 표현되며, 함수들은 현재 상태와 입력을 근거로 하여 다음 상태와 출력을 결정하게 된다. DEVS 형식론에서 시스템을 기술하기 위한 두 가지 모델 유형, 기본(basic)모델과 결합(coupled) 모델이 있다. 기본 모델(M)은 시스템의 동작(behavior)의 단위가 되는 시스템의 구성 요소들을 표현하기 위한 것이고, 결합 모델(DN)은 시스템의 구성 요소 간의 상호작용을 의미하는 구조(structure)를 표현하기 위한 것이다.

기본 모델 M은 < X, S, Y, δint, δext, λ, ta >로 정의되며,
X : 입력 이벤트들의 집합
S : 상태 이벤트들의 집합
Y : 출력 이벤트들의 집합
δint : 내부 상태 전이 함수
δext : 외부 상태 전이 함수
λ : 출력 함수
ta : 시간 전진 함수이다.
결합 모델 DN은 < D, {Mi}, {Ii}, {Zi,j}, select>로 정의되며,
D : 구성 요소가 되는 모델들의 이름 집합
Mi : 구성 요소가 되는 i번째 모델
Ii : 모델 I가 영향을 주는 다른 모델들의 집합
Zi,j : 모델 i에서 모델 j로의 연결 함수
select : 타이-브레이킹(tie-breaking) 함수이다.

1.2 IDASS Modelling

IDASS는 IoT 기기에 대한 보안 설정 정보를 파악하고, 보안에 취약하다면 자동으로 보안 설정을 하는 서비스를 제공하는 모델이다. IDASS를 통해 사용자는 손쉽게 IoT기기의 보안성을 향상 시킬 수 있으며, 다양한 보안 사고를 예방할 수 있다.

IDASS는 단말기 주변에 접속 가능한 무선 AP(Wireless Access Point)를 분석을 수행하는 AP List Viewer, IoT기기의 보안성 분석하는 IoT Device Setting Checker와 자동으로 보안설정을 수행하는 IoT Device Automatic Setter. IoT 단말기의 계정 패스워드 설정에 대한 점검을 수행하는 Password Checker로 구성되어 있다. IDASS의 구성은 [Fig. 1]과 같다.

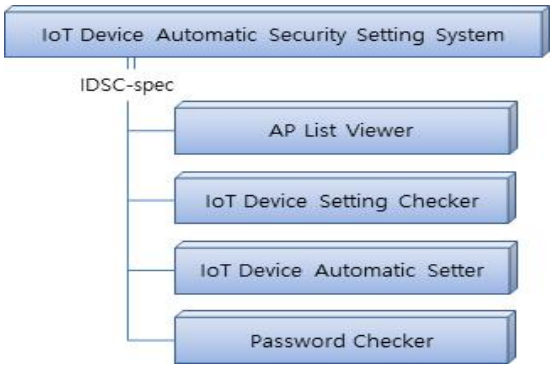


Fig. 1. IDASS Model

AP List Viewer는 주변의 AP에 대한 정보 수집과 분석을 위한 내부 모델로 [Fig. 2]과 같이 구성되어 있다.

주변에서 감지되는 AP에 대하여 새롭게 업데이트 하는 기능을 수행하는 AP Updater, 감지되어 얻은 AP에 대하여 정보를 분석하는 기능을 수행하는 AP Analyzer, 분석이 끝난 AP를 리스트로 만들어 사용자가 확인할 수 있도록 보여주는 기능을 수행하는 AP List Viewer로 구성된다.

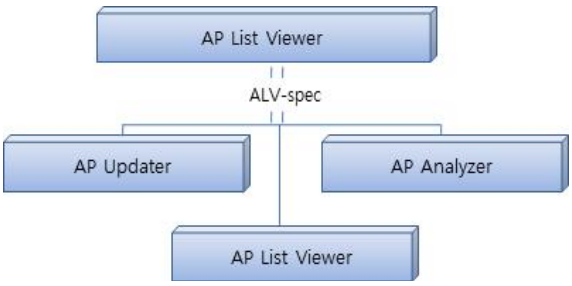


Fig. 2. AP List Viewer

IoT Device Setting Checker는 현재 연결된 디바이스(AP)에 대한 보안 설정 데이터를 가져오는 기능을 수행하는 Device Setting Data Getter와 디바이스 설정 정보를 사용자가 확인할 수 있도록 보여주는 기능을 수행하는 Device Setting Check Viewer로 구성되어 있으며, [Fig. 3] 같다.

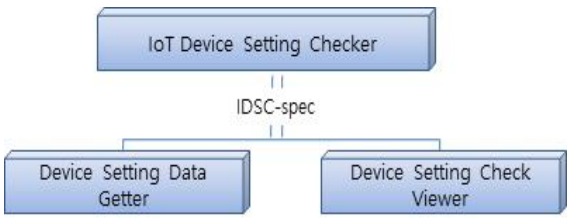


Fig. 3. IoT Device Setting Checker

IoT Device Automatic Setter는 디바이스 보안 설정에 필요한 데이터를 생성하는 Device Security Data Setter와 Device Security Data Setter에서 생성된 보안 설정 데이터를 이용하여 디바이스 보안 자동 설정을 하는 기능을 수행하는 Device Automatic Setter로 구성되어 있으며, [Fig. 4] 같다.

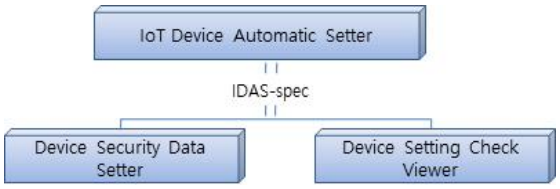


Fig. 4. IoT Device Automatic Setter

Password Checker는 IoT기기의 관리자 계정을 생성하거나 혹은 이미 만들어져 있는 관리자 계정을 확인하고 설정된 비밀번호의 안정성을 평가하는 Device Password Checker와 비밀번호 설정 시 안전한 비밀번호를 설정할 수 있도록 제시하는 Secure Password Advisor로 구성되어 있으며, [Fig. 5] 같다.

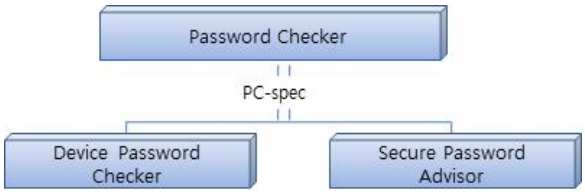


Fig. 5. Password Checker

1.3 AMMS Modelling

AMMS(AP Monitoring Management System)는 IoT 기기에 대한 보안 모니터링(관제) 및 관리를 쉽게 수행할 수 있는 서비스를 제공하는 모델이다. 사용자에게 IoT기기를 안전하게 유지/관리하기 위한 설정 방법에 제시한다.

AMMS는 사용자가 활용하는 공유기 이외에 주변에 존재하는 공유기의 정보를 수집하여, 주변에 존재하는 공유기에 대한 관리를 수행할 수 있으며, [Fig. 6]과 같이 구성되어 있다.

Periodic AP List Checker는 AP를 주기적으로 감지하는 기능을 수행하고 AP List를 갱신하는 역할을 수행한다. AP Encryption Checker는 감지된 AP에 대한 암호화 여부를 확인하고 정보를 사용자에게 전달한다. AP Bandwidth Checker는 감지되는 AP에 대한 대역폭에 대한 정보를 사용자에게 전달한다. AP RSSI Checker는 AP의 신호 세기(RSSI)값을 수집하고 -100에서 0사이의 값으로 사용자에게 제시한다.

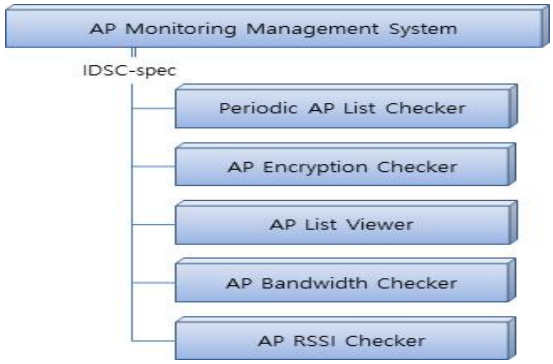


Fig. 6. AMMS Model

2. Development of IDASS and AMMS

본 논문에서는 IDASS와 AMMS를 하나의 모바일 어플리케이션으로 개발하였으며 [Fig. 7]과 같다. 사용자가 IoT기기에 대한 유지/관리를 효율적으로 수행할 수 있도록 하였다.

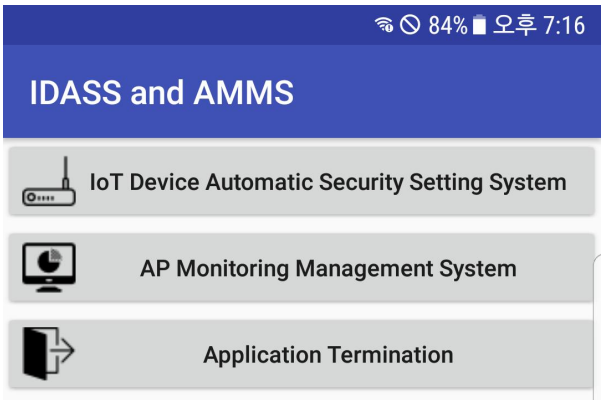


Fig. 7. Development screen of IDASS and AMMS

2.1 Development for IDASS

IDASS(IoT Device Automatic Security Setting System)는 IoT 기기 중 대표적인 기기인 가정용 공유기(Home Router)에 대한 자동 보안 설정을 목적으로 개발된 시스템이다. 개발된 화면은 [Fig. 8]과 같다.

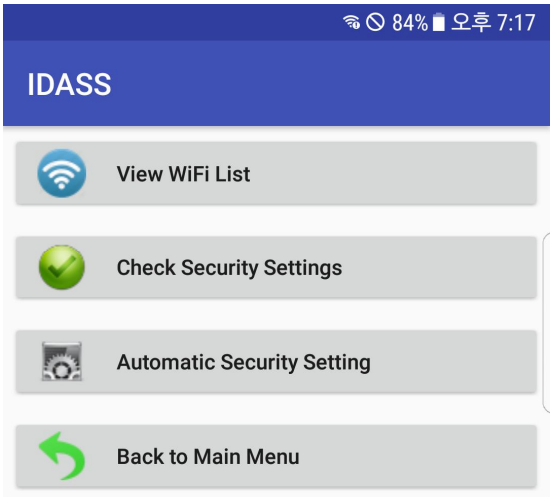


Fig. 8. Development screen of IDASS

IDASS에는 DEVS 모델링을 통해 설계한 3가지 기능을 포함하고 있으며, 스마트폰 주변에서 감지되는 Wi-Fi 정보를 보여주는 기능과 스마트폰과 연결된 가정용 공유기(Home Router)에 대한 보안 설정 확인 기능, 그리고 스마트폰과 연결된 가정용 공유기에 대한 보안 자동 설정 기능이다.

View WiFi List 메뉴를 통해 현 주변에서 감지되는 Wi-Fi 목록을 확인할 수 있게 된다. 개발된 화면은 [Fig 9]와 같다.

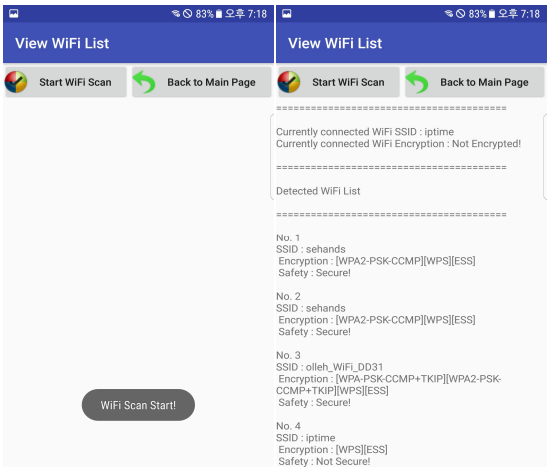


Fig. 9. Development screen of View WiFi List

Check Security Settings 메뉴를 선택하게 되면 현재 스마트폰과 연결된 가정용 공유기에 관리자 계정 설정이 되어있는지를 확인이 가능하다. 만약 공유기의 관리자 계정 설정이 되어있지 않다고 판단되면, 사용자에게 보안설정을 권고한다. 개발된 화면은 [Fig 10]과 같다.

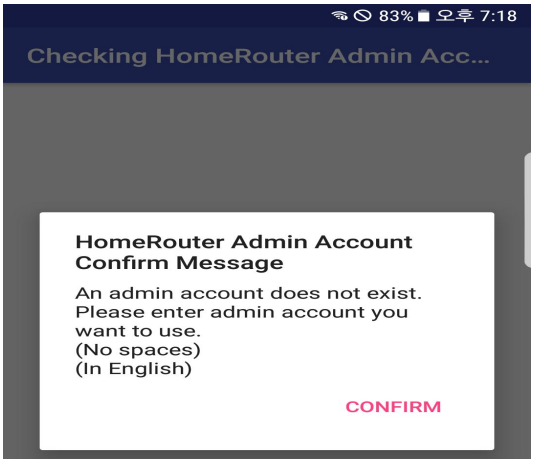


Fig. 10. Development screen of Check Security Settings

관리자 계정을 설정할 때는 보안성을 강화하기 위하여 [Fig. 11]과 같이 Password Checker를 통해 일정한 보안성 이상을 가지는 암호를 설정하도록 제시한다.

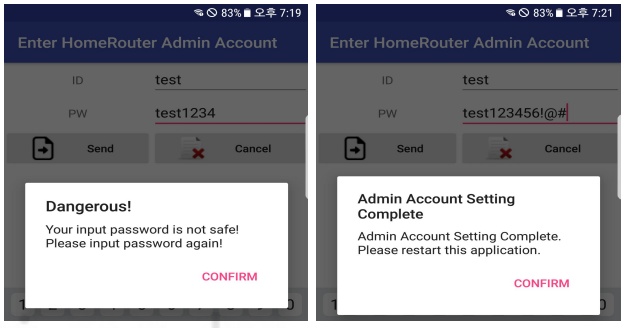


Fig. 11. Administrator account password setting screen

Check Security Settings 메뉴는 [Fig. 12]와 같이 공유기에 자체 보안 설정이 되어있는지를 확인하는 기능을 수행한다. 현재 사용 중인 공유기에 대한 자체 보안 설정 확인을 진행하게 되며, 사용자에게 현재 설정된 보안 설정이 되어 있는 항목과 설정되지 않은 항목을 보여준다.

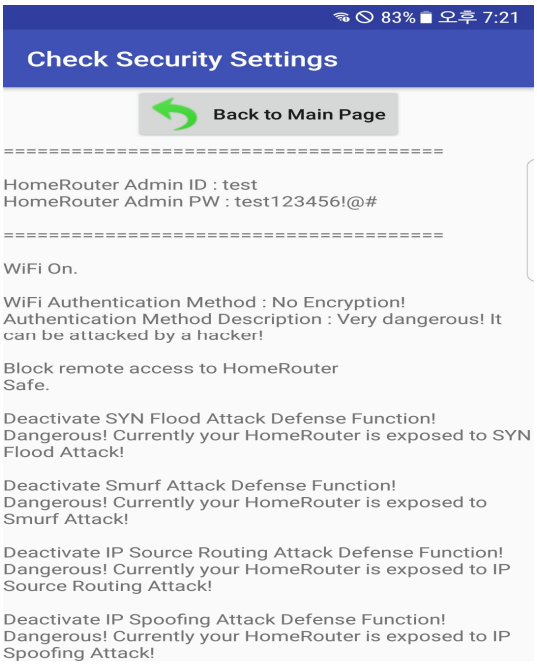


Fig. 12. Development screen of Check Security Settings

Automatic Security Setting 메뉴는 [Fig. 13]과 같이 현재 접속된 공유기에 대한 자동 보안 설정을 수행하기 위한 관리자 계정에 대한 설정 여부를 확인하고, 입력한 관리자 계정 정보를 활용하여 보안설정을 자동으로 수행한다.

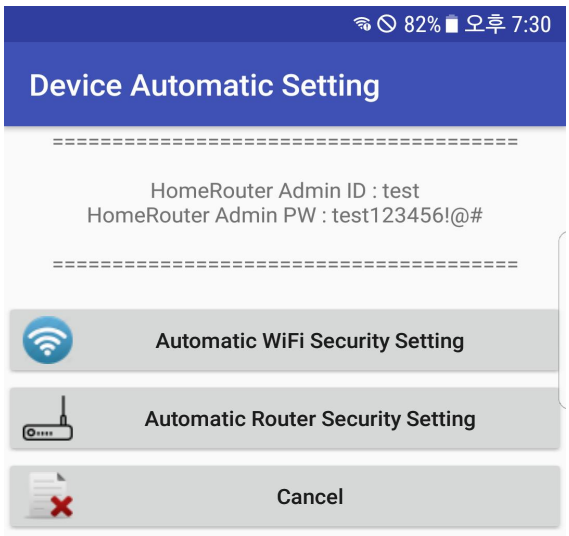


Fig. 13. Development screen of Automatic Security Setting

Automatic WiFi Security Setting메뉴는 공유기 Wi-Fi 설정을 하는 기능을 수행한다.

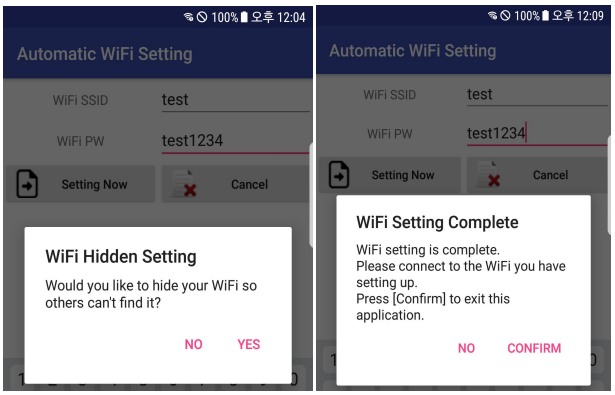


Fig. 14. Development screen of Automatic WiFi Security Setting

Automatic WiFi Security Setting를 통해 설정한 정보 [Fig. 15]과 같이 실제 공유기의 관리자 화면에서 확인이 가능하다.

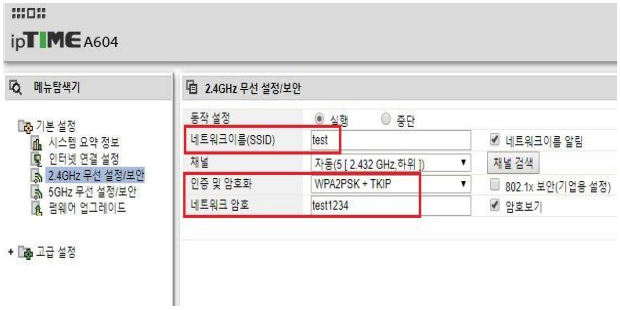


Fig. 15. Screen of Router security setting

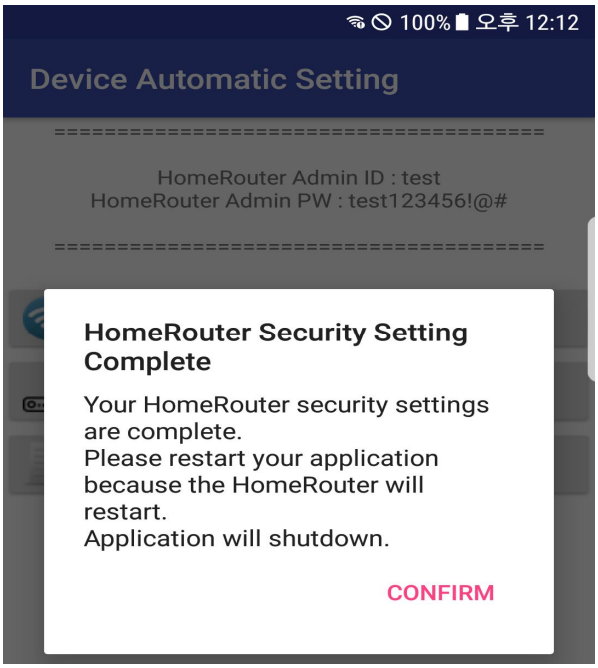


Fig. 16. Development screen of Automatic Router Security Setting

Automatic Router Security Setting 메뉴는 [Fig. 16]과 같이 공유기의 자체 보안 설정을 자동으로 수행하는 기능을 제공한다.

[Fig. 17]과 같이 Automatic Router Security Setting 메뉴를 통해 보안설정이 완료되면, Check Security Settings 메뉴를 통해서 확인할 수 있다.

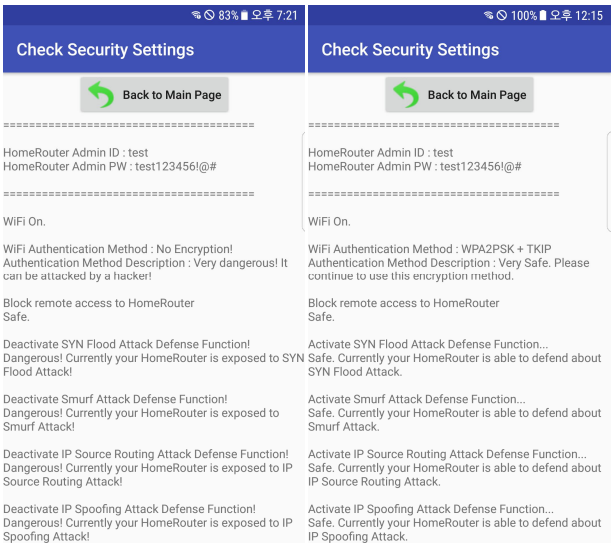


Fig. 17. Check Security Settings

2.2 Development of AMMS

AMMS는 공유기 관리자가 활용할 수 있는 시스템이며, 관리하고자 하는 AP들에 대한 정보들을 파악하고, 어떤 정보가 어떻게 변화를 추적할 수 있는 모니터링 시스템이다.

관리하고 하는 AP이 SSID를 입력함으로서 관리 리스트를 구축할 수 있다.

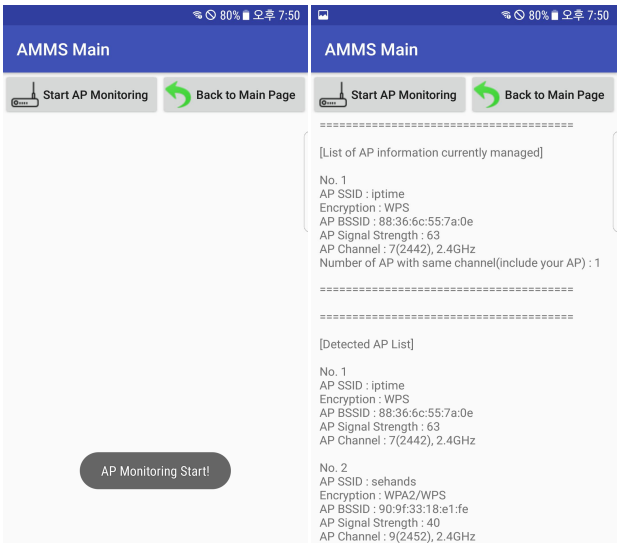


Fig. 18. Development screen of AMMS

모니터링을 실행 시 [Fig. 19]과 같이 AP의 정보를 모니터링 할 수 있다. 표시되는 정보는 [Table 2]와 같다.

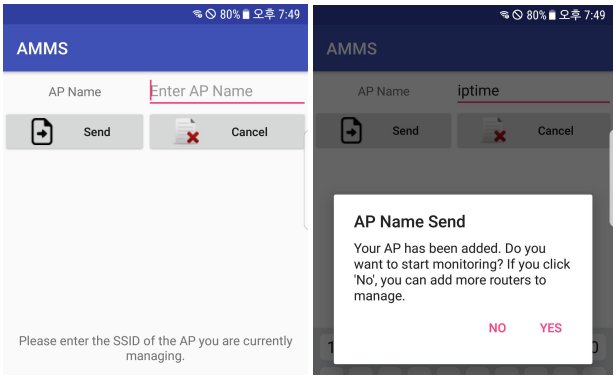


Fig. 19. Development screen of AMMS

Table 2. Monitoring Items and Descriptions

Items	Descriptions
AP SSID	SSID information provided by the router (AP)
Encryption	Information indicating the encryption of WiFi provided by the router (AP)
AP BSSID	Hardware address information of router (AP)
AP Signal Strength	Signal strength (strength) of the router (AP)
AP Channel	Channel information provided by the router (AP)
Number of AP with same channel	Number of other APs that use the same channel as the current AP

모니터링 시스템은 실시간으로 주변에서 감지되는 AP와 관리자가 입력한 관리할 AP들에 대한 정보를 보여주게 되며, 경고 모듈을 통해 어떤 정보가 변경되었는지 확인할 수 있다.

IV. Conclusions

본 논문에서는 제4차 산업혁명과 함께 IoT기기들이 증가하고 있는 상황에서 IoT 기기 편리하게 관리를 할 수 있는 시스템을 개발하였다.

개발한 IoT 기기 모니터링 시스템(IDASS 및 AMMS)을 통해 기기의 보안 상태 분석 및 자동 보안 설정을 수행할 수 있으며, 안전한 IoT 기기 환경 구축 서비스를 제공하고, 보안 모니터링을 통해 지속적인 관리가 가능하다.

또한, IoT 기기에 대한 전문적인 보안 인력을 양성하는 과정에서 이 시스템을 사용할 수 있으며 이를 통해 IoT 기기 보안 관제(모니터링) 및 관리를 할 수 있는 전문 인력을 양성할 수 있다.

안전한 IoT 기기 운영 환경을 구축하고, IoT 기기들에 대한 보안 관리 및 운영을 할 수 있는 인력을 양성하고자 한다.

REFERENCES

[1] Bharadia, Dinesh, et al. "Backfi: High throughput wifi backscatter." ACM SIGCOMM Computer Communication Review 45.4, pp.283-296. 2015

[2] Joosang Youn, Hun Choi, "CoAP-based Reliable Message Transmission Scheme in IoT Environments" Journal of the Korea Society of Computer and Information 21, pp.79-84, jun, 2016

[3] Jun Jong Am, Kim Nae Soo, Park Jeong Kil, Park Tae Jun, Kang Ho Yong, "IoT device products and technology trends," The Journal of The Korean Institute of Communication Sciences 31(4), pp.44-52, Mar. 2014.

[4] Jie, Y., Pei, J. Y., Jun, L., Yun, G., & Wei, X. "Smart home system based on iot technologies." Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on (pp. 1789-1791). IEEE.

[5] Yoon-Hwan Shin, "A Study on the Security Technology of Real-time Biometric Data in IoT Environment" Journal of the Korea Society of Computer and Information 21, pp.79-84, jun, 2016

[6] http://www.boannews.com/media/view.asp?idx=52023

[7] Kang Nam Hee, "Standard Technology Trends for Internet Security of Things," The Journal of The Korean Institute of Communication Sciences 31(9), pp.40-45, Aug. 2014.

[8] Namje Park, "Analysis of Privacy Weakness and Protective Countermeasures in Smart Grid Environment," Journal of Korean Institute of Information Technology 8(9), pp. 189-197, Sep. 2010.

[9] Nguyen, K. T. and Lauret, M., and Oualha, N. "Survey on Secure Communication Protocols for the Internet of Things," Ad Hoc Networks 32, 2015

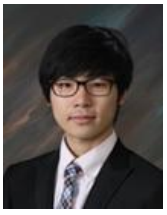
[10] Si-Jung Kim, Do-Eun Cho, "Technology Trends for IOT Security", The Korea Contents Association Review 13(1), pp.31-35, Mar. 2015.

[11] http://www.ddaily.co.kr/news/article.html?no=151522

Authors

Se Han Lee received the B.S. degrees in the Department of Computer Science and Engineering from Korea University of Technology and Education, Korea, in 2017. He received the B.S. degrees in the Department of Computer Science and Engineering from Korea University of Technology and Education, Korea, in 2017. He is currently a Master's course student in the Department of Computer Science and Engineering, Korea University of Technology and Education. He is interested in Offensive Security, User Authentication, Social Engineering, Malware Analysis.

Hee Suk Seo is now a Professor in Department of Computer Science and Engineering, Korea University of Technology and Education, Korea. His research interests include malicious code analysis, modeling & simulation, network security and intelligent system.



Yo-Han Choi received the B.S and M.S. degree in the Department of Computer Science and Engineering from Korea University of Technology and Education in 2012, 2014, respectively Now He is a Ph.D. course student at the Interdisciplinary Program in Creative Engineering from Korea University of Technology and Education, Cheonan, Korea.
His current research interests include mobile Security, Information Security, User Authentication,