http://dx.doi.org/10.14400/JDC.2016.14.11.313

스마트 팜에서의 보안 취약점 및 대응 방안에 관한 연구

채철주*, 한상균*, 조한진**
한국농수산대학*, 극동대학교 스마트모바일학과**

Security Vulnerability and Countermeasures in Smart Farm

Cheol-Joo Chae*, Sang-Kyun Han*, Han-Jin Cho**
Korea National College of Agriculture and Fisheries*, Dept. of Smart Mobile, Far East University**

요 약 FTA 대응 및 농업 경쟁력 향상을 위해 농장을 PC, 스마트 폰을 이용하여 원격으로 자동·제어할 수 있는 스마트 팜 기술 개발이 활발하게 진행되고 있다. 스마트 팜에서는 RFID, Wi-Fi, ZigBee, Wireless LAN 등 다양한 ICT 기술들을 이용하여 작물과 가축의 생육환경을 원격·자동으로 관리할 수 있다. 스마트 팜에 설치된 각 디바이스들은 생육환경 데이터를 TCP/IP 기반의 유선 네트워크뿐만 아니라 ZigBee, Wireless LAN 등과 같은 무선 네트워크를 사용하여 서버에 전송하기 때문에 스마트 팜 환경에서는 기존 정보통신 환경에서 발생하는 보안 위협들을 가지고 있다. 그러므로 본 논문에서는 스마트 팜에서 발생할 수 있는 보안 취약점에 대해 분석하고 스마트 팜에서의 보안 취약점에 대응하기 위해 사용자 인증정보를 스마트 팜의 디바이스에 분산하여 저장하고 복화화하여 인증하는 방법을 제안한다.

주제어 : Smart Farm, Smart Farm Control, Secret Share, Authentication, Security

Abstract Recently, the smart farm development using a PC and smart phone to manag the farm for improving competitiveness is in progress. In the smart farm, by using the various ICT technology including RFID, Wi-Fi, ZigBee, Wireless LAN, and etc., the growing environment of the crop and animals can be managed with the remote. By using the network including not only the TCP/IP based wired network but also ZigBee, Wireless LAN, and etc., each of the devices installed in the smart farm transmits the growing environment data to the server. So, smart farms have information and network security vulnerability. Therefore, we propose the method that analyzes the security vulnerability which can begenerated in the smart farm and user authentication method.

Key Words : Smart Farm, Smart Farm Control, Secret Share, Authentication, Security

1. 서론

최근 ICT 기술을 온실·축사·과수원 등에 접목하여 원격으로 생육환경을 적정하게 관리할 수 있는 스마트 팜에 대한 관심이 높아지고 있다. 이러한 스마트 팜 기술은 유럽의 농업 선진국을 중심으로 개발되고 있으며 그 중에서도 네덜란드의 스마트 농업은 세계최고 수준이다. 우리나라에서도 농촌진흥청을 중심으로 중·소 비닐하우스 중심의 국내 시설원예 측성에 맞는 한국형 스마트 팜 모델을 개발하고 있다[1]. 스마트 팜이란 ICT 기술을 온

Received 30 September 2016, Revised 2 November 2016
Accepted 20 November 2016, Published 28 November 2016
Corresponding Author: Han-Jin Cho
(Dept. of Smart Mobile, Far East University)
Email: hanjincho@hotmail.com

ISSN: 1738-1916

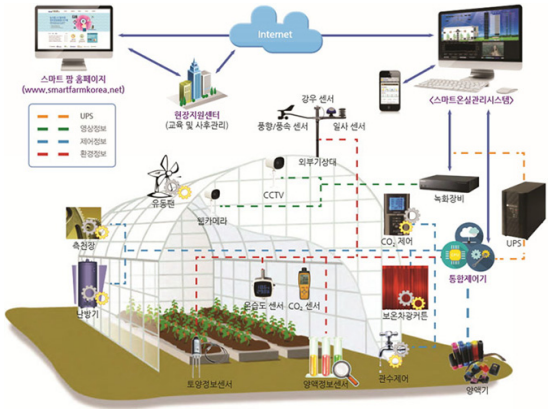
실·축사·과수원 등에 접목하여 원격·자동으로 작물과 가축의 생육환경을 적정하게 유지·관리할 수 있는 농장을 의미한다. 스마트 팜에서 디바이스들은 특정 위치에 설치되어 온도, 습도, CO_2 등의 데이터를 추출하여 네트워크를 통해 다른 디바이스나 게이트웨이로 전송한다. 스마트 팜에서 사용되는 디바이스는 RFID, 센서 노드, 스마트 기기 등이 있으며, 게이트웨이는 이러한 디바이스들로부터 수집한 데이터를 송수신하는 역할을 수행한다. 이러한 스마트 팜에서 데이터 송수신은 TCP/IP 기반의 유선 네트워크뿐만 아니라 ZigBee, Wireless LAN 등과 같은 무선 네트워크를 사용한다[2].

그러므로 스마트 팜 환경에서는 기존 정보통신 환경에서 발생할 수 있는 보안 취약점들을 가지고 있다. 스마트 팜에서는 기존 농장 관리와는 달리 온도, 습도, CO_2 등의 생육환경 데이터를 자동으로 컴퓨터에 저장하고 관리하기 때문에 공격자는 보안 취약점을 이용해 스마트 팜 시설의 온도, 급도, 급수, 배수 등을 원격으로 제어하여 큰 피해를 입힐 수도 있다. 최근 유럽에서는 스마트 팜 시설을 해킹하여 스마트 팜 환경 제어 시설을 공격하려는 시도가 있었다. 이러한 스마트 팜에서 보안 취약점은 공격자가 한번 인증에 성공하게 되면 스마트 팜의 모든 서비스를 이용할 수 있기 때문에 심각한 보안 문제점을 야기할 수 있다.

이러한 보안 문제점을 극복하기 위해 스마트 팜에서 발생할 수 있는 보안 취약점에 대해 분석하고 스마트 팜에서의 사용자 인증 방법을 제안한다. 논문의 구성은 다음과 같다. 2장에서는 스마트 팜에서 데이터 송수신을 위해 사용하는 네트워크 기술에 대해 분석하고 3장에서는 스마트 팜에서 발생할 수 있는 보안 취약점에 대해 분석한다. 그리고 4장에서는 3장에서 분석한 보안 취약점을 극복할 수 있는 사용자 인증 방법을 제안하고 5장에서 결론을 맺는다.

2. 스마트 팜에서의 네트워크 기술

스마트 팜이란 ICT 기술을 온실·축사·과수원 등에 접목하여 원격·자동으로 작물과 가축의 생육환경을 적정하게 유지·관리할 수 있는 농장을 의미한다. 스마트 팜에서는 IoT(Internet of Thing) 기술[3, 4]을 이용하여 온도, 습도, CO_2 등의 생육환경 정보를 모니터링하고 생육환경에 최적화된 상태를 유지할 수 있는 환경을 제어할 수 있다. 스마트 팜에 부착되어 있는 센서들은 생육환경 데이터를 획득하여 유·무선 네트워크를 통해 센서들을 관리하는 게이트웨이로 전송한다. 스마트 팜에서 센서가 생육환경 데이터를 전달하기 위해 사용하는 유·무선 네트워크는 유선의 경우에는 IEEE802.3, PLC, RS-232C 등을 사용하고 무선의 경우에는 IEEE802.15.4, IEEE802.15.4e, IEEE802.11n 등을 사용한다. 스마트 팜에서 생육환경을 제어하기 위해서는 각 시설별 제어 장비가 있으며, 최적의 생육환경을 제공하기 위해 정보관리시스템이 포함되어 있다. [Fig. 1]은 시설원예 분야 스마트 팜 구성을 보여주고 있다[5].

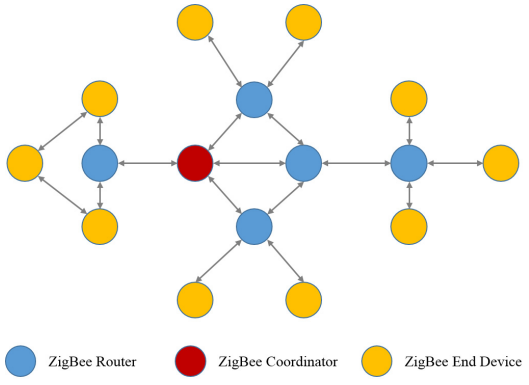


[Fig. 1] Example of Smart Farm

2.1 ZigBee

ZigBee는 낮은 가격과 전력 소비량 때문에 스마트 팜 같은 근거리 통신에 적합한 무선 네트워크 기술이다. ZigBee는 반경 100m 안에서 250kbps의 속도로 데이터를 전송할 수 있고, 네트워크 구성을 그물형(Mesh)으로 할 경우, 한 개의 무선 네트워크에 약 65,000개의 디바이스를 연결할 수 있다. 그러므로 스마트 팜에 설치된 여러 센서들은 Zigbee를 이용하여 생육환경 정보를 전송할 수 있다. 또한 ZigBee는 낮은 전력을 사용함으로 일반적으로 배터리 사용 기간이 최대 2~3년 정도 사용할 수 있다는 장점이 있다. ZigBee 네트워크는 일반적으로 ZigBee Coordinator, ZigBee Router, ZigBee End Device로 구성된다. ZigBee Coordinator는 네트워크 트리를 형성하고

다른 네크워크와 연계시키는 역할을 수행할 뿐만 아니라 보안키 저장 등 네트워크의 정보를 저장하는 기능을 수행한다. ZigBee Router는 다른 디바이스로부터 들어오는 데이터를 전달하는 중계라우터 역할을 수행한다. ZigBee End Device는 ZigBee Coordinator 또는 ZigBee Router와 통신이 가능하도록 구성된다[6,7,8,9,10]. [Fig. 2]는 ZigBee를 이용한 네트워크 구성 예시 이며, <Table 1>은 ZigBee의 특징을 보여주고 있다.



[Fig. 2] ZigBee Network

〈Table 1〉 characteristic of ZigBee

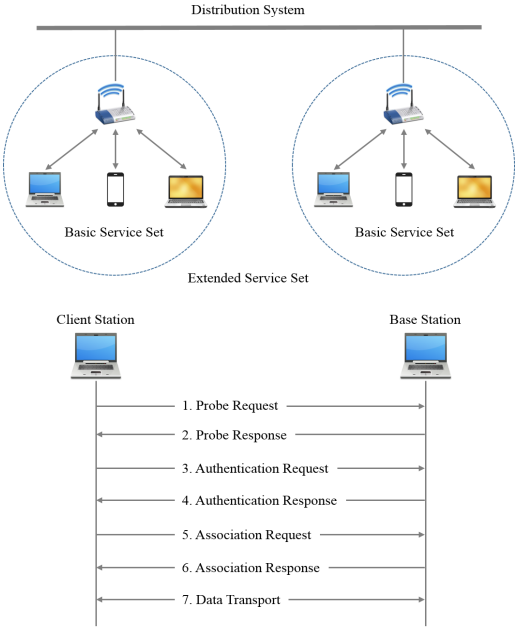
Classification	2.4GHz	868MHz	915MHz
Data Rate	250Kbps	20Kbps	40Kbps
Channel	11~26Channel	1Channel	10Channel
DSSS	32-chip PN codes	15-chip PN codes	
Chip Modulation	O-QPSK	BPSK	
Symbol Rate	62.5Ksym/s	20Ksym/s	40Ksym/s
Chip Rate	2.0Mchips/s	300Mchips/s	600Mchips/s
Sensitivity	-52dBm	-92dBm	
RF Linearity	-10dBm(IIP3), -4dBm(Output PldB)		
Transmit Power	0dBm(1mW)		
Adjacent Channel Rejection	0dB		
Altermating Channel Rejection	30dB		

2.2 Wireless LAN

Wireless LAN은 무선으로 네트워크를 이용할 수 있도록 하는 기술을 말하며 1997년부터 IEEE 802.11 그룹에서 표준화를 진행하고 있다. 그리고 Wi-Fi Alliance에서는 IEEE에서 제정한 Wireless LAN 표준을 만족하는 장치에 대해 인증마크를 부여하는 역할을 담당하고 있다. Wireless LAN은 공공 주파수 대역을 사용하므로 전파 사용료 지불 및 송출 허가가 불필요 하고 무선 AP의 가격이 저렴하여 단기간에 구축하기 적합하다. 또한 사용자 입장에서도 기존 이동통신 네트워크보다 빠른 속도와 저렴한 이용료로 이용할 수 있는 장점이 있다. 그러므로 스마트폰, 노트북 등 단말 기기에서 데이터 전송을 위한 필수 기술로서 사용되고 있으며, 스마트 팜에서도 데이터 전송을 위해 많이 사용하고 있다. <Table 2>은 Wireless LAN 기술의 특징을 보여주고 있다[11].

〈Table 2〉 characteristic of Wireless LAN

Wireless LAN	Frequency Band	Speed
802.11	2.4GHz	2Mbps
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4/5GHz	540Mbps



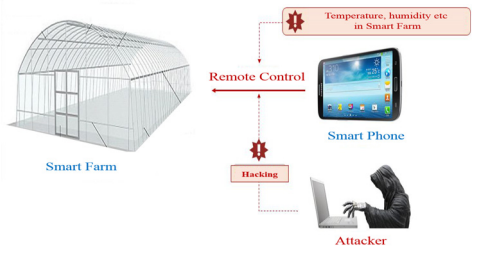
[Fig. 3] Network and Process of Wireless LAN

Wireless LAN은 IBSS(Independent Basic Service Set), BSS(Basic Service Set), ESS(Extended Service Set)의 네트워크 구조를 가지고 있다. IBSS는 Wireless LAN Device간의 통신이 직접적으로 이루어지는 네트워크이다. BSS는 AP(Access Point)를 이용하여 통신을 할 수

있는 네트워크이며 ESS는 여러 개의 BSS로 구성되어 있는 네트워크를 말한다. [Fig. 3]은 Wireless LAN에서의 네트워크 구조와 기본적인 동작 프로세스를 보여주고 있다[12].

3. 스마트 팜에서의 보안 위협

스마트 팜에서는 온도, 습도, CO_2 등 생육환경에 대한 데이터를 자동으로 제어하기 때문에 공격자는 네트워크를 통해 공격 대상 농장의 데이터를 외부로 유출할 수 있다. 그리고 공격자는 공격 대상 농장의 온도, 습도, CO_2 등을 원격으로 제어어할 수 있는 권한을 획득하여 공격할 수 있다. 스마트 팜이 많이 보급되어 있는 유럽에서는 공격자가 원격제어를 해킹하여 농장의 온도, 급수, 사료 공급 등의 생육환경 정보를 변경하여 농장에 피해를 주려는 시도가 있었다. [Fig. 4]는 스마트 팜 서비스에서의 보안 위협을 보여주고 있다[13].

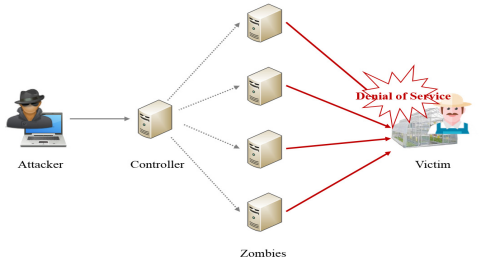


[Fig. 4] Security Vulnerability of Smart Farm

스마트 팜에 설치된 센서들로부터 데이터를 획득하고 제어하기 위해서는 다양한 IoT 기술들이 사용된다. 그러므로 스마트 팜 환경에서는 기존 정보통신 환경에서 발생할 수 있는 보안 위협들을 가지고 있다[2, 14]. 본 절에서는 네트워크 환경에서 발생할 수 있는 서비스 거부 공격 취약점을 이용한 공격과 재전송 공격 취약점을 이용하여 인증 권한을 획득하여 스마트 팜의 제어 시설을 공격할 수 있는 취약점에 대해 분석한다.

3.1 서비스 거부 공격 취약점

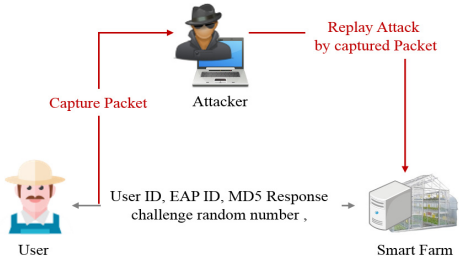
스마트 팜에 설치된 센서들은 서비스 확인, 위치 확인 등을 위해 게이트웨이를 통해 원격지에서 연결 요청을 수행한다. 공격자는 이러한 점을 이용하여 비인가 센서를 설치하여 수용할 수 있는 능력 이상의 데이터나 네트워크 트래픽을 발생시켜 정상적인 서비스를 할 수 없게 할 수 있다. 그리고 임의로 대량의 연결 요청을 수행하거나 확인 응답을 전송하여 센서의 자원을 소모시킬 수 있다. 결국 스마트 팜에 설치된 센서들의 전력을 지속적으로 소모시키기 때문에 서비스를 불가능하도록 할 수도 있다. 서비스 거부 공격을 위해 공격자는 컨트롤러를 이용해 다수의 좀비 디바이스를 이용하여 공격을 수행하기 때문에 공격자의 위치와 구체적인 발원지를 파악하기가 어렵다. [Fig. 5]는 스마트 팜에서의 서비스 거부 공격을 보여주고 있다.



[Fig. 5] Denial of Service Attack Vulnerability

3.2 재전송 공격 취약점

공격자는 스마트 팜의 무선 구간을 스니핑(sniffing)하여 트래픽을 가로채 사용자 ID, EAP ID, 챌린지 난수, MD5 응답 값을 사전으로 만든다. 공격자는 사전으로 만들어 놓은 사용자 ID를 이용하여 인증을 시도하고 인증을 위해 EAP-Response/Identity 메시지를 전송한다. 그리고 서버에서 전송한 EAP-Request/MD5 챌린지 값을 사전을 이용하여 일치하는 값을 찾아 인증을 시도한다. 이러한 방법으로 공격자는 스마트 팜 인증 권한을 획득한 후 공격을 시도할 수 있다. [Fig. 6]은 스마트 팜에서의 재전송 공격을 부여주고 있다.

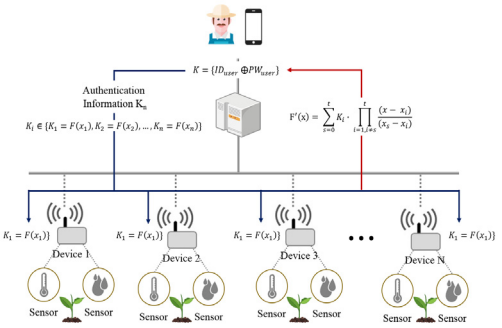


[Fig. 6] Replay Attack Vulnerability

4. 스마트 팜에서 보안 위협 대응 방법

스마트 팜 서비스를 사용하기 위해서는 먼저 사용자 인증을 수행한 후 생육환경 데이터를 모니터링하고 제어 장치들을 제어할 수 있다. 스마트 팜에서 PC, 스마트 폰에서 사용자 인증을 위해 사용하는 인증정보(ID, Password)는 공격자가 탈취당할 가능성이 있다. 스마트 팜에서는 한 번의 사용자 인증으로 스마트 팜에 설치되어 있는 다수의 센서, 제어기들을 이용할 수 있기 때문에 심각한 보안 문제를 발생할 수 있다. 그러므로 사용자 인증정보 값을 Shamir의 t-n 비밀분산 기법[15]을 이용하여 스마트 팜을 구성하는 디바이스에 분산하여 저장하여 사용자 인증정보의 일부가 탈취되더라도 인증에 사용할 수 없는 인증 알고리즘을 제안한다. Shamir의 비밀분산 기법(t,n)에서 t, n은 사용자의 인증정보를 n개의 비밀조각(secret share)로 나누어서 각기 저장하였다가, t개 이상의 비밀조각으로 사용자의 인증정보를 복호화 할 수 있는 기법이다.

먼저 스마트 팜에서 사용자 인증정보인 ID, Password를 분산시키기 위하여 사용자 인증정보 $K = ID_{user} \oplus PW_{user}$를 생성한다. 그리고 사용자 인증 정보 K를 n개로 분산시키기 위해 임의의 t-1차 Lagrange 다항식 $F(x) = ax + bx^2 + ... + cx^{t-1} + K \bmod p$를 생성한다. 이때 a, b, c …와 K는 상수이고, $t \le n$, $p(> n+1)$는 소수이다. 각각의 비밀조각(secret share)를 계산하고 (x_i, k_i)의 값으로 나누어 저장하면, $k_i \in k_1 = (x_1), k_2 = (x_2), ..., k_n = (x_n)$와 같이 사용자 인증 정보 K가 스마트 팜의 디바이스(Device 1, Device 2, … Device N)에 분산 저장된다. 그리고 사용자가 스마트 팜에 서비스를 이용하기 위해 분산된 사용자 인증정보 K를 복호화 하기 위해서는 t개의 비밀조각이 필요하다. 그러므로 최소 t개 이상의 서버에서 $K_n = F(x_n)$을 수집한다. 그리고 라그랑지 보간법(Lagrange Interpolation) $F'(x) = \sum_{s=0}^{t} K_i \cdot \prod_{i=1, i \neq s}^{t} \frac{(x - x_1)}{(x_s - x_i)}$을 이용하여 사용자 정보를 복호화 하여 사용자 인증을 수행한다. [Fig. 7]은 제안하는 스마트 팜 환경에서의 사용자 인증 방법을 보여주고 있다.



[Fig. 7] Proposed User Authentication in Smart Farm

제안 방법에서는 사용자 인증정보 K를 사용하기 때문에 ID가 유출되어도 인증에 사용할 수 없다. 그리고 사용자 인증정보 K를 분산하여 저장하기 때문에 공격자가 사용자 인증정보 K 일부를 획득하더라고 인증을 할 수 없다는 장점이 있다. 공격자는 재전송 공격과 서비스 거부 공격을 위해 스마트 팜에 접근하기 위해서는 t개 이상의 디바이스에서 비밀조각을 획득해야하기 때문에 재전송 공격과 서비스 거부 공격을 예방할 수 있다.

5. 결론

우리나라는 FTA에 대응하기 위하여 농업 경쟁력 향상과 수출산업 발전을 위해 ICT 융·복합 적용사업을 추진하고 있다. 최근에는 ICT 기술을 활용한 스마트 팜 확산 정책을 추진하여 한국형 스마트 팜을 개발하고 있다. 스마트 팜에서는 ICT 기술을 이용하여 생육환경에 대한 데이터를 획득하고 제어하기 때문에 사용자의 스마트 팜 서비스 인증 과정에서 여러 보안 취약점을 가지고 있다. 논문에서는 스마트 팜에서 발생할 수 있는 보안 취약점을 극복하기 위해 사용자 인증정보 K를 스마트 팜 디바이스에 분산하여 저장하고 복화화 하여 인증하는 방법을 제안하였다. 제안 방법에서 공격자가 사용자 인증정보 K를 일부 탈취하더라고 t개 이상의 비밀조각을 획득해야 하기 때문에 불법적인 인증을 예방할 수 있다. 제안 방법을 이용하여 스마트 팜에서의 보안 사고를 예방할 수 있으며 현재 활발하게 연구되고 있는 IoT 인증 서비스에 적용할 수 있다.

REFERENCES

[1] Yong-Byum Lee, “Smart farm policy and trend of technology in korea”, Institute of Control, Robotics and Systems, Vol. 22, No.3, pp. 58-64, 2016.

[2] Dong-Hee Kim, “The Security for IoT Service”, Korea Institute Of Communication Sciences, Vol. 30, No. 8, pp. 53-59, 2013.

[3] Ji-Eun Lee, WoonCheol Cha, “An Analysis of the Professional's Cognition Regarding the Plant”, Journal of Digital Convergence, Vol. 13, No. 12, pp. 89-97, 2015.

[4] Yong-Kyu Lee, Ku-Hong Youn, “Searching Role of Government for Promoting IoT Industry -Utilizing Importance of Individual Sub-Policies using AHP”, Journal of Digital Convergence, Vol. 14, No. 5, pp. 47-55, 2016.

[5] http://www.smartfarmkorea.net

[6] Hyun-Woo Je, Oh Yang, “Remote Monitoring System of Photovoltaic Inverter using Zigbee Communication”, Korean Institute Of Information Technology, Vol. 10. No. 2, pp. 94-101, 2012.

[7] Moonsik Kang, “Design of Multi-node Real-time Diagnostic and Management System Using Zigbee Sensor Network”, Institute of Electronics Engineers of Korea, Vol. 51, No. 6, pp. 1280-1289, 2014.

[8] Chenyan Zhang, et al, “Topology Performance Analysis of Zigbee Network in the Smart Home Environment”, 2013 5th IHMSC International Conference, Aug. 2013.

[9] Liu Yanfei, et al, “An improved design of ZigBee Wireless Sensor Network”, 2nd ICCSITIEEE International Conference, Aug. 2009.

[10] Mei-Sung Kang, et al, “ZigBee Wireless Network for Transformer Load Monitoring and Temperature Sensitivity Analysis”, 2011 IEEE IAS Conference, Oct. 2011.

[11] Jonghyun Baek, SoonTai Park, “The wireless LAN (WiFi) status of security operation and direction of policy in Korea”, Korea Institute Of Information Security And Cryptology, Vol. 21, No. 1, pp.44-50, 2011.

[12] Young-Jin Kim, “A complementary plan to vulnerable enterprise WLAN through analysis of security mechanism and threat“, Graduate School of Information & Telecommunications, 2008.

[13] Personal Information Protection Commission, “The Personal Information threat and case study in IoT”, 2015.

[14] Park, Dong Hyun, “A Study on Intrusion Patterns and Countermeasures in Wireless LAN Environment”, Department of Electrical ComputerEngineering, Graduate School of Industry & Technology, 2006.

[15] Shamir, How to share a secret, Communications of the ACM, Vol. 22, No. 11, 612-613, 1997.

채 철 주(Chae, Cheol Joo)

- 2006년 2월 : 한남대학교 컴퓨터공학과(공학석사)
- 2009년 8월 : 한남대학교 컴퓨터공학과(공학박사)
- 2009년 9월 ~ 2013년 4월 : 한국전자통신연구원 선임연구원
- 2013년 4월 ~ 2016년 8월 : 한국과학기술정보연구원 선임연구원
- 2016년 9월 ~ 현재 : 한국농수산대학 교수
- 관심분야 : 정보보호, 바이오 보안, 네트워크 보안
- E-Mail : chae.cheoljoo@gmail.com

한 상 균(Han, Sang Kyun)

- 2006년 8월 : 미국 아이다호주립대학교 자연자원대학 (임학석사)
- 2011년 3월 : 미국 오래건주립대학교 산림과학대학 (산림공학박사)
- 2013년 3월 ~ 현재 : 한국농수산대학 교수
- 관심분야 : 산림생산 및 경제성 분석, 산불방지간벌 및 산림복원작업, 소형 임업기계를 이용한 산림작업시스템 개발
- E-Mail : hsk5311@korea.kr

조 한 진(Cho, Han Jin)

- 1999년 2월 : 한남대학교 컴퓨터공학과(공학석사)
- 2002년 8월 : 한남대학교 컴퓨터공학과(공학박사)
- 2002년 8월 ~ 현재 : 극동대학교 스마트모바일학과 교수
- 관심분야 : 정보보호, 스마트폰 보안, 모바일 콘텐츠
- E-Mail : hanjincho@hotmail.com