The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 3, pp.1-6, Jun. 30, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.3.1
JIIBC 2015-3-1

사물인터넷의 경량화 장치를 위한 안전한 Pre-shared Key 설정 기술

Secure Configuration Scheme of Pre-shared Key for Lightweight Devices in Internet of Things

김정인*, 강남희**

Jeongin Kim*, Namhi Kang**

요 약 사물인터넷(IoT: Internet of Thing) 기술은 사용자 주변의 사물들이 상호 연결되어 정보를 공유할 수 있도록 해준다. IoT 환경에서 보안은 민감한 개인 정보 유출뿐만 아니라 생명에 직결 된 문제가 발생 할 수 있기 때문에 반드시 지원되어야하는 핵심 기술이다. 하지만 IoT 서비스를 구성하는 소형장치의 경우 자원이 제한적이며 배터리에 의존하기 때문에 기존 보안기술을 직접 적용하기는 어렵다. PSK(Pre-Shared Key)기반 방식은 통신 주체들이 사전에 안전하게 비밀키를 설정한 뒤 보안 기능을 수행하는 방식으로 경량화 장치에 적합하다. 공개키 알고리즘을 기반으로 세션 키를 설정하는 방식보다 적은 비용으로 보안 기술을 구축할 수 있기 때문이다. 그러나 경량화 된 장치는 입출력장치가 부재하기 때문에 PSK를 사전에 안전하게 설정하는 방식은 어렵다. 이를 해결하기 위해 본 논문에서는 자원이 제한적인 소형 장치들을 위한 안전한 초기 설정 기술을 제안하고 구현 결과를 보인다.

Abstract The IoT(Internet of things) technology enable objects around user to be connected with each other for sharing information. To support security is the mandatory requirement in IoT because it is related to the disclosure of private information but also directly related to the human safety. However, it is difficult to apply traditional security mechanism into lightweight devices. This is owing to the fact that many IoT devices are generally resource constrained and powered by battery. PSK(Pre-Shared Key) based approach, which share secret key in advance between communication entities thereafter operate security functions, is suitable for light-weight device. That is because PSK is costly efficient than a session key establishment approach based on public key algorithm. However, how to safely set a PSK of the lightweight device in advance is a difficult issue because input/output interfaces such as keyboard or display are constrained in general lightweight devices. To solve the problem, we propose and develop a secure PSK configuration scheme for resource constrained devices in IoT.

Key Words : Internet of Things, Secure bootstrapping, Pre-shared Key, Lightweight device

Ⅰ. 서 론

최근 센서나 액추에이터와 같은 소형 장치들까지 인터넷에 직접 연결하여 정보를 주고받을 수 있는 사물인터넷(IoT) 기술에 대한 관심이 높아지고 있다. 가트너(Gartner)는 IoT 기기가 2020년에는 약 250억 대에 도달

*준회원, 덕성여자대학교 디지털미디어학과
**정회원, 덕성여자대학교 디지털미디어학과(교신저자)
접수일자 2015년 5월 23일, 수정완료 2015년 6월 10일
게재확정일자 2015년 6월 12일

Received: 23 May, 2015 / Revised: 10 June, 2015 /
Accepted: 12 June, 2015
**Corresponding Author: kang@duksung.ac.kr
Dept. of Digital Media, Duksung Women's University, Korea

할 것이라고 전망했다[1]. IoT는 기존 통신에서 주류를 이루던 사람과 사람, 사람과 사물 간의 통신에서 생활 속 모든 것(물리 객체 및 가상 객체 포함)들을 상호 연결시키려는 기술이다.

IoT 환경에서 보안은 적용 환경에 따라 단순한 정보 보호의 차원을 넘어 사람의 생명에 직결될 수 있기에 반드시 제공되어야 하는 핵심기술이다. 그러나 IoT 환경의 모든 장치들에 적합한 보안 기술의 개발은 쉽지 않다[2]. 특히 IoT 환경에 신규로 적용되는 소형 장치들은 대부분 자원이 제한적이고 배터리에 의존한 에너지로 동작된다. 또한 장치 간 연결에 사용되는 통신 접속 기술도 저전력 사용을 목표로 설계되다보니 데이터 전송량이 작고, 무선 통신의 특성으로 인한 손실과 지연이 발생할 수 있다. 따라서 보안 기술의 경량화가 필요하다[3].

PSK(Pre-shared Key) 기반 방식은 계산 시간과 에너지 사용의 장점으로 인해 다양한 보안 시스템에 적용되고 있다. 특히 PSK 방식은 공개키 알고리즘을 기반으로 세션키를 설정하는 방식보다 적은 비용으로 보안 기술을 구축할 수 있으므로 경량화 장치로 구성되는 IoT환경에 적절하다. PSK 기반 방식의 주요한 전제는 사전에 통신 주체 간에 PSK가 안전하게 설정되어야 한다는 것이다. 그러나 대부분의 기존 연구들은 IoT 장치를 위한 PSK는 안전하게 설정되어 있다고 가정하고 시스템을 설계하고 있다[4].

작은 센서나 액추에이터의 경우 설정을 위해 필요한 입력장치(e.g. 키보드)나 출력장치(e.g. 모니터)가 부재하므로 IoT 환경에서 경량화 장치들에 PSK를 사전에 안전하게 설정하는 방식은 기존 인터넷 장치들에게 설정하는 것보다 어렵다. 특히 일반 사용자는 보안전문지식이 없기 때문에 설정이 어렵다. 따라서 공장에서 제조시 설정되는 기본 값을 사용하거나 장치의 설치자가 설정하는 경우가 일반적인 접근법이다. IoT 환경이나 응용 서비스에 따라 다수의 설치자와 다수의 제조사가 관여될 수 있다. 이 경우 모든 설치자들과 제조사들을 신뢰할 수 있는지는 (즉, 신용 설립(trust association) 방안 등) 어려운 문제이다.

이를 해결하기 위해 본 논문에서는 자원이 제한적인 소형 장치들을 위한 안전한 초기 설정 (secure bootstrapping) 기술을 제안한다. 즉, 기존 연구들에서 PSK가 안전하게 설정되어 있다고 가정했다면, 본 논문에서는 PSK를 안전하게 설정하거나 재설정 할 수 있는 방법론을 제시한다. 제안 기술의 기본 아이디어는 현실에서 사용하는 여행용 가방이나 잠금장치의 접근법과 유사하다. 일반적으로 여행용 가방 구입 시 '0000'이나 '1234'가 기본 비밀번호로 설정되어 있다. 구입 후 사용자는 자신이 원하는 비밀번호로 변경하여 사용한다. 이와 유사하게 제안 시스템에 적용되는 장치의 초기키(즉, 0000과 같은 초기 비밀 값)는 제조사나 설치자가 초기 단계에 설정한다. 이후 실제 사용하게 되는 PSK는 장치가 안전한 시점에 자동으로 재설정함으로써 사용자의 관여를 최소화하면서 안전하게 재설정 할 수 있는 방안을 제시한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대해서 기술하고 3장에서는 제안 시스템을 4장에서는 제안시스템의 동작시험 및 보안 분석을 기술한다. 끝으로 5장에서 본 논문의 결론을 맺는다.

II. 관련연구

서론에 기술했듯, IoT에 적용되는 소형장치들은 자원이 제한적이며 입출력 인터페이스가 부재하기 때문에 초기 설정 기술의 제공이 어렵다. 따라서 장치의 설치자나 제조사가 기본 설정을 수행한 후 시스템 관리자에게 전달해주는 방식이 일반적이다. 그러나 이러한 방식은 비밀 값 설정 등의 보안 관점을 배제한 경우에만 가능하다. 그리고 인터페이스의 부재로 인한 장치 설정 및 재설정 시 사용자의 관여를 최소화할 수 있어야 한다.

이를 해결하기 위한 방법 중 하나로 QR코드를 이용하는 방식이 제안되었다[5]. 이 시스템은 QR코드와 스마트폰을 이용하여 장치를 컨트롤러에 등록하는 방식이다. 그림 1은 [5]에서 제안한 시스템의 구성과 동작 과정을 나타낸다.

중재자(그림1의 Introducer)는 스마트폰과 같이 QR코드를 읽을 수 있는 장치를 말한다. 장치가 설치되면 중재자는 장치에서 QR코드를 스캔 하여 장치가 가지고 있는 OTP와 secret을 가져온다. OTP는 장치등록을 위해 제조자가 생성한 One Time Password이고 secret은 장치와 컨트롤러가 통신을 할 수 있도록 제조사가 생성한 비밀 값이다. 이후 중재자는 전송 에이전트(Transfer Agent)에게 장치가 사용 할 컨트롤러의 네트워크 정보를 전달한다(메시지 1,2). 중재자는 컨트롤러에게 secret(메

시지 3)을 전송 한다. 처음으로 장치가 부팅되고 네트워크연결을 하면 전송 에이전트와 연결을 하고 전송 에이전트는 장치에게 컨트롤러의 네트워크 정보를 전송한다 (메시지 4). 이후 장치가 작동될 때, 장치는 컨트롤러의 네트워크 정보를 알기 때문에 직접 통신을 할 수 있다 (메시지 5).

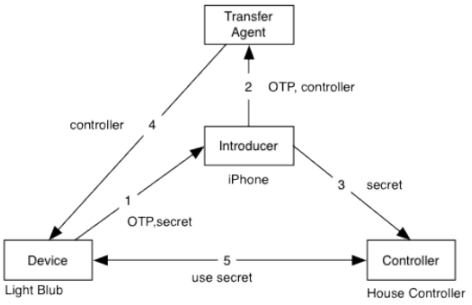


그림 1. 간단한 정보 흐름
Fig. 1. Simplified high-level information flow

그림 1에 나타낸 시스템은 제한된 메모리와 처리능력을 가지는 경량 장치에 사용 할 수 있으며 장치를 설치할 때 네트워크나 전원을 필요로 하지 않는다. 인증에 사용되는 OTP가 이미 사용된 경우에는 설치자가 감지 할 수 있다. 사용자가 QR코드를 스캔함으로써 장치 등록을 할 수 있도록 사용자의 관여를 최소화 하였지만 QR코드가 가지는 인증정보를 암호화하지 않고 그대로 제공하기 때문에 보안에 취약할 수 있으며 적용할 수 있는 환경이 제한적이다.

독일의 Olaf Bergmann은 IPv6와 CoAP을 기반으로한 무선 센서 네트워크에서 제한된 장치를 부트스트랩하기 위한 3단계의 프로토콜을 제안하였다[6]. 제안 시스템은 버튼이나 LED와 같은 저렴한 사용자 인터페이스를 사용한다.

제안 방식은 3단계로 설정이 수행 된다(discovery, imprinting, configuration) 첫 번째 단계에서 신규 노드와 연결할 수 있는 네트워크에서 신규 노드를 검출한다. 두 번째 단계에서 신규 노드는 서버와 보안 채널을 설정하기 위한 keying material을 제공 한다. 신규 장치의 실제 설정은 세 번째 단계 전에 설정 된 보안 채널을 사용하여 세 번째 단계 동안 수행된다. 본 시스템은 [7]에 정의 된 것처럼 네트워크는 적어도 하나의 CoAP Service Discovery Server(CSDS)를 구성하고 있다고 가정한다.

그 밖에도 보안 부트스트래핑에 사용될 수 있는 다양한 프로토콜을 [8]에서 언급하고 있으며 [9]에서는 무선 센서 네트워크에 대한 위협 분석과 보안 부트스트래핑 접근 방법에 대해 설명한다.

III. 제안 시스템

본 논문에서는 사물인터넷에서 자원이 제한된 장치들을 위한 안전한 PSK 설정 기술을 제안한다. 표 1은 본 논문의 제안시스템에서 사용하는 시스템 파라미터이다.

표 1. 시스템 파라미터
Table 1. Sysytem Parameters

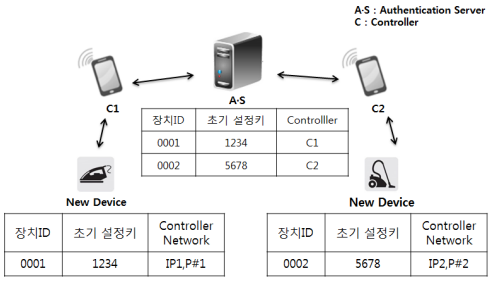
Parameter	Context
ID_d, ID_c	장치(d)와 컨트롤러(c)의 식별값 (32bit identifier)
RN_d, RN_c	장치(d)와 컨트롤러(c)의 랜덤숫자 (128bit identifier)
TS	타임스탬프
TID	트랜잭션 식별값(ID)
IK_i	신규장치를 위한 사전 설정키 128bit 대칭키
SK_{cs}	컨트롤러와 인증 서버를 위한 128bit 세션키
PSK	장치와 서버의 128bit pre-shared key
$E_K=(P)$	대칭키 k로 평문p를 암호화 하는 암호화 함수

본 논문에서 제안하는 시스템은 다음과 같은 가정 사항을 기반으로 한다.

- 시스템 관리자가 설치자나 제조사를 100% 신뢰하지 않음
- 신규 장치에는 장치의 식별 값인 ID, 통신 가능한 컨트롤러의 네트워크 정보, 초기 설정키가 사전에 안전하게 설정되어있음 (경우에 따라 제조사가 사전에 설정할 수도 있음)
- 시스템 관리자는 인증 서버에 신규 장치의 ID와 초기 설정키를 사전에 설정해둠
- 컨트롤러와 인증서버는 대칭키를 상호 공유

그림 2는 시스템 구성도이며 사전에 설정된 정보의 예

시를 나타낸다.



장치ID	초기 설정키	Controlller
0001	1234	C1
0002	5678	C2

장치ID	초기 설정키	Controller Network
0001	1234	IP1,P#1

장치ID	초기 설정키	Controller Network
0002	5678	IP2,P#2

그림 2. 시스템 구성도
Fig. 2. System Configuration

그림 3은 PSK 재설정을 위한 동작 과정을 나타낸다. 컨트롤러는 논리적으로는 인증서버와 분리되지만 물리적으로는 한 시스템에 구축 될 수 있다.

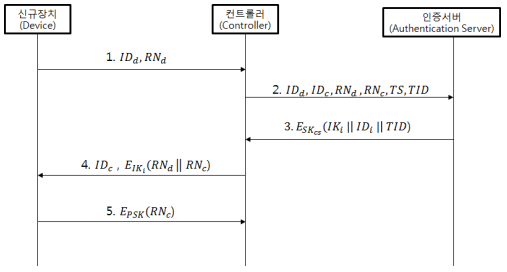


그림 3. PSK 설정을 위한 동작 과정
Fig. 3. Proposed system flow about PSK configuration

1) 신규장치가 운영 중인 네트워크에 설치되고 초기 설정이 수행 될 때, 신규장치는 RN_d를 생성하고 ID_d와 함께 컨트롤러에 전송한다.

2) 메시지를 수신한 컨트롤러는 RN_c와 TS, TID를 생성한 뒤, 신규장치로부터 수신한 메시지와 함께 인증서버에 전송한다. TS는 컨트롤러가 키의 유효시간과 메시지의 신선도를 확인할 수 있게 해준다. 이를 수신한 인증서버는 ID_d를 이용하여 사전에 설정해둔 IK_i를 찾아 수식(1)을 이용하여 PSK를 생성하여 초기키 IK_i를 대체한다.

$$PSK_i = E_{IK_i}(RN_d \oplus RN_c) \quad (1)$$

3) PSK를 재설정한 후, 컨트롤러는 IK_i를 가지고 있지 않기 때문에 인증서버는 SK_{cs}를 이용하여 IK_i, ID_d, TID를 암호화 하여 컨트롤러에 전송한다.

4) 컨트롤러는 SK_{cs}로 수신한 메시지를 복호화 하여 IK_i값을 알 수 있다. RN_d, RN_c를 IK_i로 암호화하여 컨트롤러의 ID_c값과 함께 신규장치에 전송한다.

5) 신규장치는 수신된 메시지를 초기키 IK_i로 복호화한다. 수식(1)을 이용하여 PSK를 설정하고 컨트롤러의 진위를 검증하기 위해 RN_c와 PSK를 암호화하여 컨트롤러에 전송한다.

Ⅳ. 동작 시험 및 보안 분석

1. 동작 시험

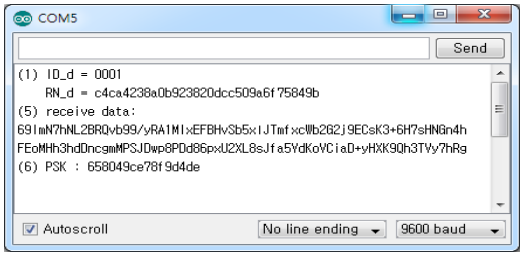
본 장에서는 제안 시스템을 구현하여 실험 한 결과를 기술한다. 동작 시험 및 보안 분석을 위해 표2에 기술된 오픈 하드웨어 플랫폼을 사용하였다.

표 2. 시험기기 사양
Table 2. specification of test device

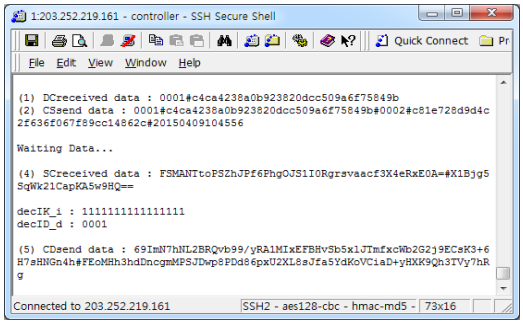
Device	Arduino Uno R3	Raspberry pi
Processor	ATmega328 (16 MHz)	ARM11 (700 MHz)
Flash Memory	32KB	SD Card
SRAM	2KB	512MB

제안시스템에서 PSK의 설정이 필요한 경량 장치로 Arduino 장치를 사용했고, 인증을 수행하는 컨트롤러로 Raspberry pi 장치를 사용하여 구현했다.

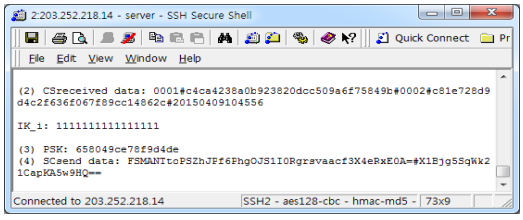
그림 4는 구현된 장치들의 동작 시험의 결과를 나타낸다. 그림4의 (a)는 경량 장치로 동작하는 Arduino에서 수행 된 결과를 콘솔로 연결하여 출력한 캡처화면이고, (b)는 컨트롤러의 출력 결과를 캡처한 화면, (c)는 인증 서버의 결과를 캡처한 화면이다.



(a) Arduino 캡처화면



(b) 컨트롤러 캡처화면



(c) 인증 서버 캡처화면

그림 4. 제안 시스템 동작 시험
Fig. 4. system operational test

장치의 초기 설정이 수행되면 Arduino는 (b)의 장치 ID와 랜덤넘버(1)를 전송한다.

컨트롤러는 장치로부터 받은 데이터와 컨트롤러의 ID와 컨트롤러가 생성한 랜덤넘버(2)를 (c)의 인증서버에 전송한다. 인증서버는 전송받은 데이터를 이용하여 PSK를 설정한다(3). 인증서버는 사전에 컨트롤러와 공유한 세션키를 이용하여 초기키, 장치의 ID, TID를 암호화하여(4) 컨트롤러에게 전송한다.

컨트롤러는 전송받은 데이터를 세션키로 복호화한다. 복호화하면 컨트롤러는 장치의 초기키를 얻을 수 있다. 컨트롤러는 장치의 랜덤넘버와 컨트롤러의 랜덤넘버를 초기키를 이용하여 암호화한 후, Arduino에게 전송한다(5).

Arduino는 전송받은 데이터를 초기키를 이용하여 복호화 한 뒤 PSK를 설정한다(6). PSK설정 후 Arduino는 컨트롤러가 생성한 랜덤넘버를 PSK로 암호화한 뒤 컨트롤러에게 전송한다.

본 논문에서는 장치와 컨트롤러의 성능 비교를 위해 암호화가 수행되는 시간을 측정하였다.

표 3. 성능 측정 결과
Table 3. Performance comparison

장치	Arduino		Raspberry pi	
input length(bit)	128	256	128	256
Processing time(μs)	12768	13108	7572	8200

Arduino를 센서의 장치로 사용하였고 라즈베리를 컨트롤러로 사용하였다. 두 장치 간 보안 알고리즘이 동작되는 속도는 표3과 같다. Arduino보다 라즈베리가 좀 더 빠르게 동작되는 것을 확인할 수 있다.

2. 보안 분석

제안하는 시스템의 안정성은 초기키에 의존한다. 초기키를 알고 있는 설치자를 완전하게 신임할 수 없으므로 키 설정이 수행되는 동안 설치자의 도청공격을 고려해야 한다. 하나의 대안으로 통신 반경이 작은 NFC(수십 cm 이내)와 같은 통신 기술을 적용하면 도청 공격에 대응하면서 안전하게 초기설정을 수행할 수 있다. 도청 공격 이외에 제안 시스템의 안전성을 분석하기 위해 인증 시스템을 대상으로 하는 대표적인 공격들에 대해 분석했다.

• 재전송 공격(Replay attack)

공격자는 장치가 컨트롤러에게 전송하는 정보를 가지고 있다가 일정시간 이후 재전송 할 수 있다.

본 제안 시스템은 공격자가 일정시간이 지난 후 재전송 공격을 하더라도 인증서버는 TS정보를 확인하여 재전송 공격임을 감지할 수 있다. 또한 장치는 PSK 설정 시 매번 새로운 랜덤넘버를 컨트롤러에게 넘겨주기 때문에 재전송 공격에 대응할 수 있다.

• 중간자 공격 (Man-In-The-Middle Attack)

장치와 컨트롤러 사이에 공격자가 존재할 수 있다. 장치가 컨트롤러에게 전송하는 ID_d와 RN_d값을 공격자가 가로챈 뒤, 공격자가 RN_c를 임의로 생성하여 인증서버에 전송하고 인증 서버는 공격자에게 PSK 생성을 위한 정보를 보내주게 된다. 이에 대응하기 위해 인증서버는 공격자에게 정보를 보낼 때 컨트롤러와 인증서버만 알고 있는 세션키 SK_{cs}로 암호화하여 전송한다. 공격자

는 세션키 SK_{cs}를 알지 못하기 때문에 암호화된 정보를 풀 수 없어 응답메시지를 생성 할 수 없다.

• **스푸핑 공격 (Spoofing Attack)**

제안 시스템은 공격자가 신규 장치나 컨트롤러로 위장(IP spoofing, 거짓 서버 등)한 스푸핑 공격에도 대응한다. 공격자가 신규 장치로 위장하여 랜덤 넘버를 생성할 수 있지만, 초기키로 암호화되는 컨트롤러의 랜덤 넘버를 복호화 하지 못하므로 PSK를 취득할 수 없다. 또한 컨트롤러로 위장하기 위해서도 초기카를 알고 있어야 가능하므로 불가하다.

V. 결 론

본 논문에서는 자원이 제한적인 소형 장치의 안전한 키 설정을 위한 방식을 제안하였다. 제안 기술을 통해 재전송 공격, 중간자 공격에 대응하면서 PSK를 안전하게 설정할 수 있다. 또한 운영 중인 네트워크에 연결할 때 자동으로 재설정되기 때문에 사용자의 관여를 최소화 할 수 있다.

References

[1] Gartner, http://www.gartner.com/newsroom/id/2905717, Nov. 2014.

[2] J. Part, N. Kang, "SSM: Secure Service Manager for the Internet of Things", Int. J. of Security and Its Applications, Vol.8, No.3, pp.39-48, 2004.

[3] Namhi Kang, "Survey on standard technologies for Internet of Things security", Information and Communications Magazine, Vol.31, No.9, pp. 40-45, 2014.

[4] P. Eronen, H. Tschofenig, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", IETF Standard, RFC4297

[5] C. Jennings, "Transitive Trust Enrollment for Constrained Devices", IETF Internet Draft, draft-jennings-core-transitive - trust -enrollment-01, 2012.

[6] O. Bergmann, S. Gerdes, S. Schafer, F. Junge, C. Bormann, "Secure Bootstrapping of Nodes in a CoAP Network", Pro. of IEEE WCNC, Apr. 2012.

[7] C. Bormann, "CoRE Simple Server Discovery", Internet-Draft (work in progress), Mar. 7, 2011. http://tools.ietf.org/html/draft-bormann-core-simple-server-discovery

[8] B. Sarikaya, Y. Ohba, R. Moskowitz, Z. Cao, and R. Cragie, "Security Bootstrapping of Resource-Constrained Devices", Internet-Draft (work in progress), Jun. 2011. http://tools.ietf.org/html/draft-sarikaya-core-sbootstrapping

[9] O. Garcia-Morchon, S. Keoh, R. Hummen, and R. Struik, "Security Considerations in the IP-based Internet of Things", Internet-Draft (work in progress), Jul. 2011. http://tools.ietf.org/html/draft-garcia-core-security

저자 소개

김 정 인(준회원)

• 2015년 2월 : 덕성여자대학교 디지털미디어학과 졸업
• 2015년 ~ 현재 : 덕성여자대학교 디지털미디어학과 석사과정
<주관심분야 : 네트워크 보안, 사물인터넷 보안>

강 남 희(정회원)

• 1999년 3월 ~ 2001년 2월 : 숭실대학교 공학석사
• 2004년 12월 : University of Siegen, 공학박사
• 2009년 3월 ~ 현재: 덕성여자대학교 디지털미디어학과 부교수
<주관심분야 : 유무선 인터넷통신, 네트워크 보안, 사물인터넷보안>

※본 연구는 덕성여자대학교 2014년도 교내연구비 지원에 의해 수행되었음