논문 17-42-10-18 The Journal of Korean Institute of Communications and Information Sciences '17-10 Vol.42 No.10
https://doi.org/10.7840/kics.2017.42.10.1973

# 사물인터넷에서 장치 사이의 부가 채널에 대한 안전도를 고려한 비밀키 설정 방법

반 효 진◆, 강 남 희°

# Secure Key Agreement Method Considering Secure Strength of Out-of-Band Channel between Devices in Internet of Things

Hyo Jin Ban◆, Namhi Kang°

요 약

IoT(Internet of Things) 서비스를 안전하게 제공하기 위해서는 IoT 장치 간 전송되는 데이터를 안전하게 보호할 필요가 있다. 이를 위해서는 두 통신 주체 사이에 비밀키가 안전하게 설정되어야 하는데, 주로 PSK(Pre-Shared Key) 방식을 기반으로 안전한 키 설정 방법들이 제안되고 있다. 그러나 처음 연결되는 장치들의 경우 사전에 설정되어 있는 PSK가 부재되어 PSK 기반 방식을 적용하기는 현실적으로 어렵다. 이를 해결하기 위해 본 논문에서는 DH(Diffie-Hellman) 키 교환 알고리즘과 부가(OOB: Out-Of-Band) 채널을 이용한 방식을 제안한다. OOB 채널을 이용함에 있어 기존의 연구들은 통신하고자 하는 두 장치의 OOB 채널이 다른 경우, OOB 채널의 안전함의 강도가 다른 경우, OOB 채널의 통신 범위가 다른 경우 등과 같이 다양한 상황을 고려하지 않았다. 따라서 본 논문에서는 OOB 채널을 환경 및 통신 수단에 따라 안전도를 분류하고, 분류된 안전도에 기반을 두어 비밀키를 설정할 수 있는 방법들을 제시하고 안전도를 분석한다.

**Key Words** : Internet of Things, Security, Key Agreement, OOB Channel, Lightweight device

ABSTRACT

To provide secure IoT(Internet of Things) services, it is required to protect the data securely that is delivered between IoT devices. To do so, a secret key between the two communication devices has to be configured securely. For the purpose several secure key agreement methods based on PSK(Pre-Shared-Key) have been proposed in the literatures. However, it is practically difficult to apply the PSK based methods for devices that are connected in the first time because there is no pre-configured PSK between the two devices. To solve the problem, we propose methods utilizing the DH(Diffie-Hellman) key exchange algorithm and OOB(Out-of-Band) channel. Most related work did not considerer various cases, where two devices utilize different OOB channel, the security strength of OOB channel is different, the communication range of the OOB channel is different, and others. In this paper, however, we categorize the security strength of OOB channels according to environments and communication means, then we suggest protocols based on the categorized OOB channel.

※ 본 논문은 덕성여자대학교 2017년도 교내연구비 지원에 의해 수행되었습니다.
◆ First Author : Duksung Women's University Department of Digital Media, hj.ban64@gmail.com, 학생회원
° Corresponding Author : Duksung Women's University Department of Digital Media, kang@duksung.ac.kr, 정회원
논문번호 : KICS2017-05-155, Received May 25, 2017; Revised July 22, 2017; Accepted July 24, 2017

## Ⅰ. 서 론

IoT(Internet of Things) 기술의 발전에 따라 기존에 고려되지 않았던 일상의 사물들이 인터넷에 연결되고 있으며 그 수는 급증하고 있다. 이에 따라 IoT 기술이 적용되는 새로운 응용 서비스의 수는 증가하고 있으며 스마트 카, 스마트 홈, 스마트 빌딩 그리고 스마트 시티 등 서비스 범위 또한 점차 확장되고 있다.

IoT 서비스가 발전하는 데 있어 가장 큰 토대는 두 장치 간 데이터를 교환함에 있다. 장치 간 주고받는 데이터를 통해 각 상황에 따른 조치가 결정되고 인간은 자신에게 적절한 서비스를 받을 수 있다. 그러나 IoT가 일상생활과 밀접한 관련이 있는 만큼 교환되는 데이터는 사용자의 민감한 정보를 담고 있을 수 있으며 경우에 따라서는 민감한 정보를 가지고 있지 않더라도 해커가 유추해낼 수 있는 특정 정보를 흘릴 수 있다. 공격자는 이러한 정보를 공격에 이용할 수 있으며 사용자에게 물리적인 피해까지 입힐 수 있다. 따라서 두 장치 사이에서 이루어지는 통신은 IoT 환경에 있어 중요한 요소이며 이에 따라 교환되는 데이터는 안전하게 보호되어야 한다.

두 장치 사이에서 교환되는 데이터를 보호하기 위해서는 데이터 암호화에 필요한 비밀키가 가장 먼저 안전하게 설정되어야 한다. 그러나 IoT 환경에서는 대부분의 장치가 제한된 입출력 인터페이스를 가지기 때문에 사용자가 직접 키를 입력하는 등의 설정이 어렵다[13]. 더불어 대부분의 장치가 CPU, 메모리, 배터리 등 자원의 제약성을 가지기 때문에 공개키에 비해 적은 계산을 수행하는 PSK(Pre-Shared Key) 방식을 이용한다. 그러나 PSK 방식은 처음 연결되는 두 주체가 사용하기에는 적합하지 않다. 따라서 본 논문에서는 이를 해결하기 위한 방법으로 DH(Diffie-Hellman) 키 교환 알고리즘을 이용한다.

DH 키 교환 알고리즘은 통신하고자 하는 두 장치가 서로에 대한 사전 정보를 가지고 있지 않을 때 키를 교환할 수 있게 하는 알고리즘이다. 따라서 처음 연결되는 두 장치를 다루고자 하는 본 논문의 목적에 적합하다. DH 키 교환 알고리즘을 이용하면 두 장치는 안전하지 않은 채널을 통해 서로 값을 주고받아 비밀키를 만들 수 있다. 그러나 키를 교환하는 상대방에 대한 인증이 이루어지지 않아 중간자(Man-In-The-Middle) 공격에 취약하다는 단점이 있다. 대부분의 기기들이 무선 통신을 이용하는 IoT 환경에서는 인증의 문제가 더욱 커진다[3]. 따라서 상기 문제점을 해결하기 위해 기본 통신 채널 외의 부수적인 채널인 OOB(Out-of-Band) 채널을 이용한다.

IoT 환경에서의 OOB 채널은 장치가 가지고 있는 빛, 소리, 진동 등 다양한 매체가 될 수 있다. IoT 장치는 자원이 제한되어 있기 때문에 모든 기기가 공통적으로 특정 매체를 가지고 있는 것은 아니다. 그러나 대부분의 선행 연구들은 두 통신 주체가 동일한 매체를 사용하는 환경을 다루고 있으며 두 기기에 적용되어있는 OOB 채널이 다른 경우를 고려하지 않았다. 또한 전송 매체는 통신 수단 및 환경에 따라 안전함의 강도가 달라지지만 기존의 연구들은 매체 자체에 대해서 안전도를 가정하였다. 따라서 본 논문에서는 매체의 안전도를 통신 수단 및 환경을 모두 고려하여 분류하고 각 상황에 맞는 프로토콜을 제시함으로써 상기 문제점들을 해결한다. 특히 두 장치의 OOB 채널의 안전도가 다른 경우는 개인 장치(예, 스마트폰)를 중재자로 이용함으로써 문제를 해결한다.

본 논문은 다음과 같이 구성되어 있다. 먼저 본 논문과 관련된 선행 연구들을 2장에서 알아본 후 해결하고자 하는 주요 문제를 3장에서 제시한다. 4장에서는 OOB 채널로 사용될 전송 매체의 보안 특성을 기술하고 이에 기반 한 보안키 설정 프로토콜을 제안한다. 5장에서는 제안하는 프로토콜의 보안 및 성능 분석을 수행한다. 마지막으로 6장에서는 결론을 내린다.

## Ⅱ. 관련 연구

### 2.1 OOB 채널을 활용한 비밀키 설정 기술

빛, 소리, 진동, 가속도계, 제스처 등 다양한 매체를 OOB 채널로 이용하는 방법이 제안되어 왔다. 그 중에서 빛, 소리를 이용한 방법들을 중점적으로 알아보고자 한다. 먼저 OOB 채널로 사용되는 매체 중에서도 빛은 가장 많이 이용되어왔다. X. Huang et al.은 BSN 환경에서 기본 무선 통신 채널로 전송되는 키를 검증하는 데 LED를 이용하였다[1]. T. Kovacevic et al.은 다수의 자원이 제한된 기기를 한 번에 안전하게 초기 설정하는 방법을 제안하였다[2]. 해당 방법은 스마트폰, 랩탑 등의 디스플레이 위에 다수의 기기를 한 번에 올려놓는다. 그 다음 디스플레이에서 흘러나오는 빛을 통해 각 기기에 아이디와 비밀 키를 전송하고 기본 무선 통신 채널에서 키 검증을 수행한다.

J. Han은 차량 환경에서 스마트폰과의 안전한 블루투스 페어링을 위해 빛 또는 소리를 OOB 채널로 이용하였다[3]. 빛을 OOB 채널로 이용하는 경우 차량의 글러브 박스에 스마트폰을 넣는다. 글러브 박스에서 나오는 빛은 외부로부터 차단되기 때문에 안전하다고

보아 빛을 통해 스마트폰에 길이가 짧은 임시키를 전송한다. 다음으로 해당 임시키를 이용하여 블루투스 페어링을 수행한다. 반면 소리를 OOB 채널로 이용하는 경우에는 소리의 근원지는 알 수 있으나 전송되는 메시지의 비밀(secrecy)은 제공하지 않기 때문에 빛을 이용하는 것보다 약하다고 본다. 따라서 블루투스를 통해 먼저 키를 교환하고 해당 키를 인증하는 용도로 소리를 이용한다.

OOB 채널로 소리를 이용하여 키를 교환하는 방법으로 자가 전파 방해(self-jamming)를 적용한 방법이 있다[4]. 해당 제안 방식은 NFC 하드웨어가 없어도 NFC를 가능하게 하기 위해 폰의 마이크와 스피커를 이용하는 소리 기반 시스템이다. 자가 전파 방해 방법은 송신자가 수신자에 데이터를 전송할 때 수신자가 임의의 노이즈를 만들어 전파시킨다. 즉, 수신자는 자신이 만든 노이즈를 알기 때문에 송신자가 전송한 데이터를 추출할 수 있다. 반면 공격자는 송신자와 수신자의 전파를 합쳐서 듣기 때문에 도청이 불가능하다. 이 방법을 이용하면 초기 설정을 위해 사전 공유 값이나 인증서(certificate) 없이도 키를 교환할 수 있다. 해당 방식은 소리를 통해 키 교환이 가능하게 만듦으로써 IoT 환경에도 소리를 이용하여 안전한 키 설정을 수행할 수 있음을 보여주고 있다.

### 2.2 스마트폰을 이용한 비밀키 설정 기술

IoT 기기 간 OOB 채널을 활용한 페어링 시 스마트폰을 이용하는 방법 또한 제안되어 왔다. J. Suomalainen은 통신하고자 하는 두 주체 사이의 거리가 멀거나 두 주체가 가지고 있는 OOB 채널이 호환되지 않는 경우를 다루었다[5]. 상기 문제점들을 해결하기 위해 먼저 OOB 채널을 인증만 제공 혹은 인증과 기밀성을 제공하는 채널로 구분하였다. 이에 따라 각 경우에 따른 프로토콜을 제안하였고 스마트폰을 중재자로 이용하였다. 스마트폰은 통신하고자 하는 두 IoT 기기 사이에서 사용되는 키를 생성하는 역할을 하는데 이는 IoT 기기들에 키를 생성하는 부담을 덜 수 있다는 장점이 있다. 그러나 스마트폰이 키를 생성하는 만큼 보안이 전적으로 스마트폰에 달린다는 문제점이 있다.

A. Coppa는 입출력 인터페이스가 제한된 IoT 기기의 안전한 초기 설정을 위해 게이트웨이와의 연결 시 BLE 환경에서 OOB 페어링 모드를 이용한다[6]. 이때 사용되는 OOB 채널은 NFC이다. 해당 제안은 IoT 기기를 움직일 수 있는 것과 그렇지 않은 것으로 분류하였다. 움직일 수 있는 IoT 기기의 경우 사용자가 해당 기기를 게이트웨이에 가까이 이동시켜서 OOB 채널을 이용한 BLE 통신을 수행한다. 반면 크기가 크거나 고정되어 있는 기기의 경우에는 스마트폰을 이용하여 두 번의 BLE 통신을 수행하거나 NFC와 BLE 터널을 만든다. 먼저 두 번의 BLE 통신 수행 방법은 스마트폰이 기기와 게이트웨이 각각에 OOB 채널을 이용한 BLE 연결을 수행한다. 스마트 폰을 중간에 두고 연결된 BLE 통신 채널은 일종의 OOB 채널로 이용되며 게이트웨이와 IoT 기기는 이 OOB 채널을 이용하여 BLE 통신을 수행한다. 다음으로 NFC와 BLE를 이용한 터널은 IoT 기기와 스마트폰 사이의 연결을 NFC로 대체하는 것이다. 스마트폰은 IoT 기기와 NFC 연결을, 게이트에이와 BLE 연결을 통해 하나의 터널을 이루고, 이를 OOB 채널로 이용한다.

A. Lakshminarayanan은 두 기기 사이의 페어링을 위해 중재자로 계산 능력이 있는 간편한 기기를 이용하였다[11]. 이 중재자는 TAP(Touch mediated Association Protocols)이라고 불리며 기기를 탐색하고 키를 안전하게 분배하는 용도로 사용된다. 이는 USB와 같은 기기를 이용하며 해당 기기를 가볍게 두드리기만 하면 된다. 그러나 이 방법은 개인 기기에만 적용할 수 있으며 USB와 같은 추가적인 물리적 기기 또는 중재자와 기기 사이에 칩 카드(chip card) 인터페이스를 필요로 한다.

## Ⅲ. 문제 제기

본 논문에서는 사전 정보가 없는 두 사물 기기가 처음 통신하고자 하는 경우를 고려하여 DH 키 교환 알고리즘을 이용한다. 그러나 DH 키 교환 알고리즘은 주체 인증이 이루어지지 않기 때문에 중간자 공격이 가능하다는 취약점을 가지고 있다.

중간자 공격을 막기 위해서는 키를 교환하는 두 주체간의 상호 인증이 필요하다. 이를 해결하기 위한 방법으로 인증된 DH 키 교환 프로토콜, STS (Station-to-Station) 프로토콜과 같은 상호 인증을 포함하는 프로토콜을 이용하거나 OOB 채널을 이용하는 등의 방법이 있다. 본 고에서는 인증 문제를 해결하기 위해 OOB 채널을 이용한다.

IoT 기기는 유무선 통신 장치 이외에도 LED, 스피커, 마이크와 같이 다양한 데이터 전송 가능 장치를 가지고 있으며 이에 따라 기기들은 빛, 소리, 진동 등 다양한 매체를 OOB 채널로 사용할 수 있다. 그러나 OOB 채널로 이용되는 전송 매체는 기본 통신 채널에 비해 전송 가능한 데이터의 양, 전송 속도 등의 성능

이 낮다. 따라서 IoT 환경에서의 OOB 채널은 기본 통신 채널에서 전송되는 데이터를 인증하는 용도로 사용되거나 길이가 짧은 임시 키와 같은 데이터를 전송하는 용도로 사용된다.

OOB 채널은 데이터 무결성, 데이터 인증, 그리고 경우에 따라 데이터 기밀성까지 제공한다[10]. 그렇기 때문에 DH 키 교환 알고리즘 사용 시 발생하는 문제점을 OOB 채널에 위임함으로써 해결할 수 있다[6, 10]. 또한 OOB 채널은 IoT 장치 내 포함되어 있는 입출력 인터페이스를 이용하기 때문에 무선 채널의 보이지 않는 특성으로 인해 커지는 기기 인증의 문제 또한 해결할 수 있다[3]. 그러나 IoT 기기는 자원의 제약성으로 인해 대부분이 입출력 인터페이스가 부재하거나 제한되어 있다. 따라서 기존의 OOB 채널을 활용한 제안 방안들을 적용하기에는 다음과 같은 문제점들이 있다.

첫 번째 문제점은 OOB 채널을 이용하여 키를 설정하는 방법을 제안해 온 기존 연구들은 동일 OOB 채널을 기반으로 하고 있다는 점이다. 그러나 IoT 기기는 다양한 이종 기기들을 포함하고 있으며 모든 기기들이 특정 OOB 장치를 공통적으로 가지고 있는 것은 아니다.

두 번째로 통신하고자 하는 두 주체가 동일한 OOB 매체를 가지고 있더라도 전송 가능한 통신 범위에 제한이 따른다[5]. 예를 들어, 다른 방에 있는 두 기기 사이에 빛을 OOB 매체로 사용할 수 없다. 또한 IoT 기기 내 사용될 수 있는 OOB 채널들은 대부분 통신 반경이 작기 때문에 거리가 먼 경우 활용이 어렵다.

IoT 기기의 크기나 무게와 같은 특성으로 한 지점에 고정되어 있는 경우(예, 냉장고, TV 등)에는 직접적으로 OOB 채널을 사용할 수 없다는 문제도 있다[5]. 즉, 통신하고자 하는 두 기기가 상기와 같은 이유로 움직일 수 없다면 OOB 채널을 이용한 키 설정 방안을 적용하는 것은 어렵다.

마지막으로, 기존 선행 연구들은 OOB 매체 자체에 강함/약함의 특성을 부여하고 특정 환경에서 적용될 수 있는 방안을 제안하였다. 예를 들어 J. Han의 경우 차량 환경에서 자동차와 스마트폰 사이의 OOB 채널을 이용한 안전한 키 설정을 다루었는데, 차량 내 글러브 박스에서 흘러나오는 빛은 밀폐되어 있으므로 빛이란 매체는 강하다고 결정했다[1]. 또 다른 OOB 채널로 이용하는 소리는 소리의 근원지는 알 수 있으나 비밀은 보장되지 않으므로 빛보다는 약하다고 결정하였다. 그러나 매체 자체를 두고 강약을 결정해서는 무리가 있고 매체 및 환경을 모두 고려해야 한다.

## Ⅳ. 제안 시스템

제안 시스템은 처음 연결을 시도하는 두 기기를 대상으로 한다. 또한 두 기기의 OOB 채널이 다른 문제와 두 기기 사이의 거리가 멀거나 특정 위치에 고정되어 있어 이용되는 OOB 채널의 통신 범위를 벗어나는 문제를 해결하기 위해 스마트폰과 같은 개인 장치(P·D)를 중재자로 이용한다. 따라서 그림 1과 같이 동일한 서비스 환경에 있지 않은 두 기기가 연결되고자 하는 경우에도 적용할 수 있다. 본 제안 시스템에서 OOB 채널의 Strong과 Weak의 의미는 매체 자체에 기반을 둔 안전도가 아닌 환경 및 통신 수단을 고려한 안전도이다.

제안 시스템에서 이용하고자 하는 DH 키 교환 알고리즘은 공개키 기반 방식이기 때문에 자원이 제한된 IoT 환경에서는 부담이 될 수 있다. 이를 해결하기 위해서 많은 연구들이 선행되어 왔다.

A. Liu et al.은 무선 센서 네트워크 환경에서 공개키 암호화를 이용하기 위해 경량화된 ECC를 제안하였다[7]. R. Watro et al.은 무선 센서 네트워크 환경에서 인증과 키 합의를 가능하게 하는 공개키 기반 프로토콜을 제안하였으며[8], S. Misra et al.은 대칭키 암호화 방식을 제공하는 Zigbee 환경에서 공개 키 기반 구조(PKI)를 이용할 수 있는 방법을 제안하였다[9]. 이와 같이 자원이 제한된 환경에서 공개키를 사용하기 위한 방안들을 활용하면 DH 키 교환 알고리즘을 IoT 환경에서 사용할 수 있다. 또한 DH 키 교환 알고리즘은 모든 전송 데이터를 대상으로 하지 않고 간헐적으로 수행되는 키 교환에만 적용되므로 IoT 기기의 부담은 크지 않다.

제안 시스템에서는 DH 키 교환 알고리즘의 중간자 공격에 대한 취약점을 해결하기 위해 OOB 채널을 이용한다. OOB 채널은 기본 통신 채널에서 전송되는

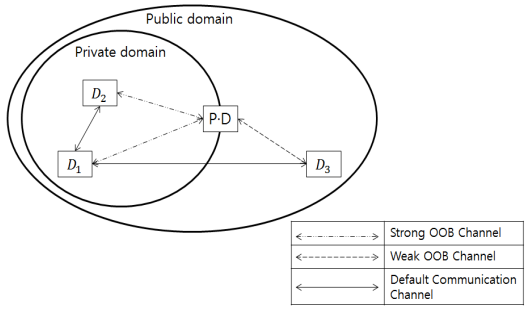



그림 1. 제안 시스템 환경
Fig. 1. Proposed system environment

데이터의 인증 용도와 임시키와 같은 짧은 데이터 전송에 사용된다. 즉, 키 교환 시 기본 통신 채널에서 발생하는 중간자 공격에 대한 방어를 OOB 채널에 위임함으로써 주체 인증 및 중간자 공격에 대한 문제점을 해결한다. 또한 제안하는 시스템은 개인 장치를 중간 매개체로 활용하여 2장에서 제시한 다양한 문제점을 해결한다.

OOB 채널로 이용되는 통신 매체들은 각기 서로 다른 보안 속성을 지니고 있고, 적용되는 환경에 따라 매체들의 위협 요소 또한 다르다. 이에 본 장에서는 OOB 채널의 보안 특성을 먼저 분류하고 분류된 매체에 기반을 두어 안전한 키 설정을 위한 프로토콜을 제시한다.

### 4.1 매체 분류

제안 시스템에서는 빛과 소리를 주요 매체로 고려한다. OOB 채널로 사용되는 빛과 소리의 안전도는 매체의 수단 및 환경을 기반으로 다음 표 1과 같이 분류된다. 제시된 매체 분류법은 매체의 안전함의 강도를 쉽게 파악할 수 있게 해준다.

빛의 경우 두 장치의 키 교환이 글러브 박스 또는 방과 같이 폐쇄된 공간에서 이루어진다거나 사용자가 육안으로 확인 가능한 짧은 길이의 케이블을 이용하게 된다면 보안 강도는 높다고 할 수 있다. 빛은 폐쇄된 공간을 투과할 수 없기 때문에 외부로 흘러나오지 않는다. 그렇기 때문에 전송되는 데이터의 안전을 보장하며 사용자가 두 장치를 육안으로 확인 할 수 있으므로 강하다고 본다. 반면 공공장소와 같은 개방된 공간에서 디스플레이나 LED와 같은 통신 수단을 이용하게 된다면 공격자도 전송되는 데이터를 확인할 수 있으므로 빛이라도 보안 강도가 약하다고 볼 수 있다.

소리의 경우에도 빛의 경우와 같이 폐쇄된 공간에서 키 교환이 이루어진다거나 사용자가 확인할 수 있는 길이의 케이블을 이용한다면 공격자가 전파를 획득하기 어려워지기 때문에 보안 강도는 강하다. 또한 두 장치가 개방된 환경에 있더라도 자가 전파 방해(예, 재밍 신호 입력) 방법을 이용하는 경우에도 보안 강도는 높다. 그러나 주변이 매우 시끄러워 노이즈가 크게 생긴다거나 마이크, 스피커와 같이 열린 통신 수단을 이용한다면 사용자는 통신하고 있는 두 장치를 확인 할 수는 있지만 공격자도 데이터를 확인할 수 있기 때문에 비밀을 보장하지 않는다. 따라서 해당 매체의 보안 강도는 보다 낮아진다.

제시된 매체 분류법에 따라 두 장치 간 키 설정에 대한 적절한 프로토콜이 필요하게 된다. 프로토콜 제시에 앞서 OOB 채널에 관한 문제점들을 먼저 해결해야 하며 이를 해결하기 위해 개인 장치를 이용한다. 개인 장치는 사용자가 가지고 있는 스마트폰, 태블릿, 노트북과 같이 통신이 가능하며 대부분의 입출력 인터페이스를 가지고 있는 기기를 의미한다. 개인 장치는 자원이 제한된 IoT 기기들이 가지고 있는 입출력 인터페이스를 거의 포함하고 있기 때문에 서로 다른 OOB 채널을 가지고 있는 두 기기 사이에서 중간 매개체 역할을 할 수 있다. 사용자가 이미 가지고 있는 기기를 중재자로서 이용하기 때문에 별도의 기기가 필요하지 않으며 각 기기들은 키 교환을 위해 불필요한 입출력 인터페이스를 탑재하지 않아도 된다. 또한 한쪽 또는 양쪽 기기 모두 크기 및 거리상의 문제가 있는 경우에도 이동이 편리한 개인 장치를 이용하여 문제점을 해결할 수 있다.

### 4.2 제안 프로토콜

매체의 보안 특성을 반영하고 OOB 매체의 약점을 보완해 줄 개인 장치를 이용하여 각 기기의 조건에 쉽게 적용 가능한 프로토콜을 제안한다. 제안되는 프로토콜은 두 기기의 매체 A, B가 모두 강한 경우, A(B)는 강하고 B(A)는 약한 경우 그리고 A, B 모두 약한 경우로 총 3가지로 분류될 수 있다. 제안 프로토콜에서 이용되는 주요 파라미터는 표 2를 따른다.

표 1. 환경 및 통신 수단을 고려한 매체의 보안 강도 분류법
Table 1. security strength of media classification based on environments or communication means

| Classification | Light | | Audio | |
|---|---|---|---|---|
| | Strong | Weak | Strong | Weak |
| Environment | - Glove box in Car [3], Closed space (e.g. room) | - Open space (e.g. office, public space) | - Glove box, Closed space (e.g. room)<br>- case of self-jamming possibility [4], [12] | - Open space (e.g. office, public space)<br>- case of noisy surrounding |
| Media | User-Identifiable Optical Cable | Display panel, camera, LED, optical sensor, etc. | User-Identifiable Cable | Microphone, speaker |

표 2. 제안 시스템 파라미터
Table 2. Parameters using in proposed system

| Parameter | Description |
|---|---|
| $ID_A$ | Identifier of device A |
| $g^a$ | DH public value of device A, where a is an private integer value |
| $R_A$ | Random number generated by of device A |
| $K_A$ | Temporary encryption key generated by device A |
| $K_{AB}$ | DH shared key between devices A and B |
| $H(m)$ | Result value of hashing message m |
| $S\_H(m)$ | Short have value of $H(m)$ (i.e. truncation of $H(m)$) |
| $\{m\}_{K_A}$ | Encrypted message m with key $K_A$ |

4.2.1 두 기기의 OOB 매체 A, B의 안전도가 모두 강한 경우

먼저 OOB 채널에 이용되는 두 기기의 매체 A, B가 모두 강한 경우를 살펴본다. 매체 A, B가 동일한 통신 수단이라면 두 기기가 직접적으로 통신할 수 있다. 그러나 두 기기 중 하나라도 OOB 채널의 통신 범위를 벗어나는 경우에는 중재자가 필요하다. 이 때 중재자가 되는 개인 장치는 단순한 전달 역할만 수행하면 된다. 또한 매체의 안전도는 동일하나 통신 수단이 다른 경우에는 중재자가 각 기기의 OOB 채널에 맞게 신호만 바꾸어주면 된다. 매체 A, B가 모두 강한 경우 제안되는 키 교환 프로토콜을 그림 2에 나타냈다.

기기 $D_A$은 OOB 채널로 중재자 M을 통해 임시키 $K_A$를 $D_B$에 전송한다. 이용되는 OOB 채널은 환경 및 통신 수단으로 보아 안전하다고 보기 때문에 해당 채널로 임시키를 전송할 수 있다. 공유된 임시키는 기본 통신 채널에서 전송되는 데이터를 암호화하는 용도로 이용한다. 두 주체는 이를 이용하여 각각 자신의 아이디와 DH 공개값 그리고 랜덤값을 암호화한 값을 상대방과 교환한다. 여기에서 각 기기는 DH 키 교환 알고리즘을 이용하여 공유키 $K_{AB}$를 생성한다. 그 다음 키를 검증하기 위해 $D_B$는 자신과 상대방의 DH 공개값과 랜덤값 $R_A$를 해시 및 암호화여 $D_A$에 전송한다. $D_A$는 이를 확인 한 후 상대방이 보낸 해시 값에 상대방의 랜덤값 $R_B$를 해시 및 암호화하여 $D_B$에 전송한다.

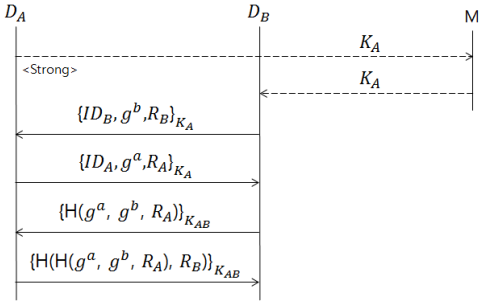



그림 2. 두 OOB 채널의 안전도가 모두 강한 경우의 키 교환 프로토콜
Fig. 2. Key agreement protocol in case security strength of two OOB channels is strong

4.2.2 두 기기의 OOB 매체 A, B의 안전도가 모두 약한 경우

두 기기의 매체 A, B가 모두 약한 경우도 모두 강한 경우와 마찬가지이다. 중재자는 매체 A, B가 동일한 통신 수단이라면 단순 전달을, 통신 수단이 다르다면 신호만을 변경하여 보내주면 된다. 그러나 현재 고려되는 매체들은 안전도가 약하다고 보기 때문에 공격자의 도청과 같은 공격이 가능하다. 따라서 매체 A, B가 모두 강한 경우와 달리 OOB 채널을 길이가 짧은 해시 값을 전송하는 용도로 이용하였다. 제안 프로토콜은 그림 3과 같다.

각 기기는 자신의 아이디, DH 공개값, 랜덤값을 해시한 값을 OOB 채널로 전송하기 위해 truncation과 같은 방법을 이용하여 길이를 짧게 만든다. 중재자를

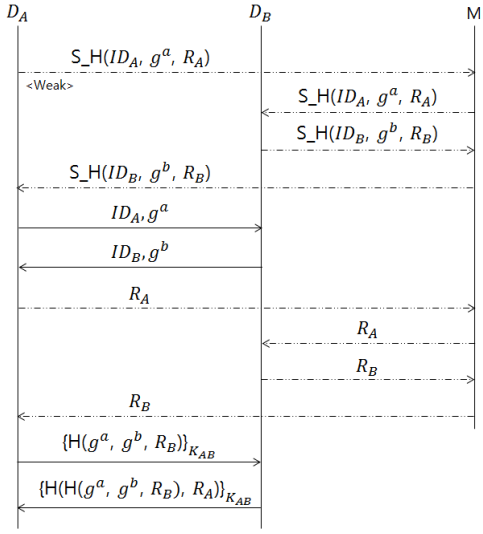



그림 3. 두 OOB 채널의 안전도가 모두 약한 경우의 키 교환 프로토콜
Fig. 3. Key agreement protocol in case security strength of two OOB channels is weak

통해 길이가 짧은 해시 값을 교환한 후 기본 통신 채널을 통해 각자의 아이디 값과 DH 공개 값을 교환한다. 다시 중재자를 통해 각자의 랜덤값을 OOB 채널을 이용하여 전달한다. 각 기기는 상대방으로부터 받은 아이디 값, DH 공개값 그리고 랜덤값을 이용하여 길이가 짧은 해시 값을 만들고 맨 처음 받았던 값과 같은지 비교한다. 이후 첫 번째 프로토콜과 같은 방식으로 키 검증을 수행한다.

#### 4.2.3 두 기기의 OOB 매체 A, B의 안전도가 상이한 경우

매체 A, B의 안전도가 상이한 경우에는 앞선 경우보다 복잡한 구조를 가지게 된다. A(B)는 강하고 B(A)는 약한 경우 강한 매체로부터 전송되는 값들은 약한 매체로 전송될 때 안전하게 보호되어야 할 필요가 있다. 따라서 이를 해결하기 위해 매체 A, B의 안전도가 동일한 경우와 달리 중재자의 역할을 가중시킨다. 즉, 그림 4에서 보이는 바와 같이 약한 OOB 채널을 가진 기기와 중재자 사이에 키를 생성한다. 생성된 키는 중재자가 강한 OOB 채널을 통해 전송받은 임시키 $K_A$를 암호화하여 약한 OOB 채널을 가진 기기에 전송하기 위한 목적으로 사용된다. 중재자는 키 검증 시 약한 매체를 가진 기기에 대한 검증이 끝나면 $K_A$와 함께 자신의 검증 값을 전송한다. 이후 각 기기가 임시키를 이용하여 키 생성 관련 데이터를 교환하는 동작들은 매체 A, B가 모두 강할 때와 동일하다.

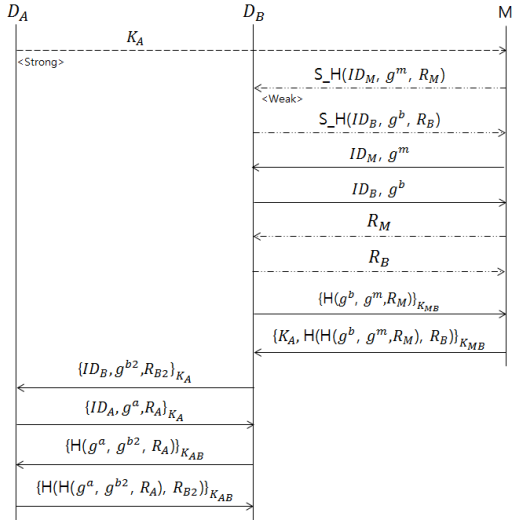



그림 4. 두 OOB 채널의 안전도가 상이한 경우의 키 교환 프로토콜
Fig. 4. Key agreement protocol in case security strength of two OOB channels are different

## V. 보안 및 성능 분석

표 1에 제시된 매체의 보안 강도 분류법을 통해 매체는 상황 및 전송 수단에 따라 안전도가 달라짐을 확인할 수 있었다. 또한 표 1에 기반을 두어 이용되는 매체의 보안 강도에 따라 총 세 가지의 프로토콜을 제안하였다. 이에 따라 본 장에서는 각 프로토콜의 보안을 분석한 후 성능을 분석한다.

먼저 각 프로토콜의 보안을 분석한다. 첫 번째 제안 프로토콜은 두 OOB 매체의 안전도가 모두 강한 경우로 공격자의 중간자 공격, 가로채기 등의 공격을 막을 수 있다. 예를 들어, 장치가 글러브 박스와 같은 폐쇄된 공간에 있다면 각 매체의 신호는 외부로 흘러나오지 않는다. 따라서 전송되는 데이터의 안전을 보장하며 사용자가 육안으로 확인 할 수 있기 때문에 인증을 제공한다.

이후 기본 통신 채널을 통해 전달되는 데이터들은 안전한 OOB 채널을 이용하여 공유된 임시키로 암호화된다. 따라서 공격자는 두 주체 사이에서 전송되는 메시지를 도청할 수 없으며 키를 알아내지 않는 이상 중간자 공격, 수정, 위조 등의 어떠한 적극적인 공격도 수행할 수 없다. 또한 DH 키 교환 알고리즘을 이용하여 생성된 키를 통해 데이터의 무결성을 검사한다.

두 기기의 OOB 매체의 안전도가 모두 약한 경우는 공공장소와 같은 개방된 공간이나 모니터, 스피커 등을 이용하는 경우를 예로 들 수 있다. 이 경우 사용자는 이용되는 OOB 채널을 통해 어느 장치와 올바르게 통신되고 있는지를 확인할 수 있다. 그러나 공격자도 데이터를 확인할 수 있기 때문에 비밀을 보장하지는 않는다. 따라서 두 장치의 OOB 채널의 안전도가 모두 강한 경우와는 달리 OOB 채널을 통해 임시키를 전송할 수 없으며 기본 통신 채널에서는 더욱 복잡한 구조를 가지게 된다.

두 매체의 안전도가 모두 약한 경우는 OOB 채널을 통해 길이가 짧은 해시 값을 가장 먼저 보낸 후 이를 기본 통신 채널을 통해 전송된 값들로 검증한다. 이때 해시를 만드는 데 이용된 모든 값들은 기본 통신 채널로만 전송되는 것이 아니라 OOB 채널로도 전송된다. 따라서 공격자는 OOB 채널과 기본 통신 채널을 모두 공격하지 않는 이상 해시 구성 값들을 알 수 없으며 결국 중간자 공격을 수행하지 못한다. 또한 랜덤넘버를 이용함으로써 재전송 공격을 막을 수 있다. 이후 한쪽에서 새로운 해시를 만들어 그 값을 암호화하여 보내면 다른 한 쪽이 해당 메시지를 확인한다.

그 다음 해시 값을 상대방의 랜덤값과 다시 해시 및 암호화하여 자신을 인증한다.

마지막으로 두 장치의 OOB 채널의 안전도가 상이한 경우를 살펴본다. 먼저 안전도가 강한 OOB 채널로부터 전송된 값을 안전도가 약한 OOB 채널을 가진 기기에 전송하기 위해서 해당 기기와 개인 장치 사이에서 기본 통신 채널을 위한 키를 만들었다. 키 생성에 이용되는 값을 전송하는 방식은 두 장치의 OOB 채널의 안전도가 모두 약한 경우와 같이 길이가 짧은 해시 값을 OOB 채널로 보낸 후 나중에 검증하였다.

개인 장치는 생성된 키를 이용하여 안전도가 강한 OOB 채널을 가진 장치가 보낸 임시키를 안전도가 약한 OOB 채널을 가진 장치에 안전하게 보낼 수 있다. 이로써 두 장치는 임시키를 공유하게 되고 임시키를 이용하여 두 장치가 직접 기본 통신 채널을 통해 키를 설정할 수 있다. 두 장치의 키 설정에 대한 안전도는 두 장치의 OOB 채널이 모두 강한 경우와 동일하다.

다음으로 각 프로토콜의 성능을 분석한다. 각 프로토콜의 연산량 분석 결과는 다음 표 3과 같다. E는 암호화를 의미하고 H는 해시를 의미한다. 두 OOB 채널의 안전도가 모두 강한 경우(P1)는 OOB 채널을 통해 기본 통신 채널로 전송되는 데이터를 암호화하기 위한 임시 키를 교환한 후 암호화된 데이터를 전송하기 때문에 장치의 식별값과 DH 공개 키 그리고 랜덤 넘버를 전송하기 위한 암호화와 DH 공유 키를 이용한 암호화가 수행된다. 따라서 OOB 채널의 안전도가 모두 약한 경우에 비해 암호화가 한 번 더 수행된다. 또한 키 검증 단계에서 해시를 한 번 수행하므로 각 장치는 한번의 해시와 두 번의 암호화를 수행한다.

두 OOB 채널의 안전도가 모두 약한 경우(P2) 두 장치는 맨 처음 길이가 짧은 해시 값을 만들기 위해 해시를 한 번 수행하고 키 검증 단계에서 해시와 암호화를 한 번 수행한다. 따라서 총 4번의 해시와 2번의 암호화를 수행하게 된다.

두 OOB 채널의 안전도가 상이한 경우(P3)에는 P1, P2보다 더 많은 계산을 수행하게 되는데 이는 안전도가 약한 OOB 채널을 안전하게 만드는 단계가 수행되기 때문이다. 이 단계에서는 중재자의 역할이 가중되어 중재자 또한 단순 전달만이 아닌 계산이 필요한 작업을 수행하며 안전도가 약한 OOB 채널을 가진 장치도 보다 더 많은 계산 작업을 수행하게 된다. 따라서 안전도가 약한 OOB 채널을 가진 장치와 중재자 각각 두 번의 해시와 한 번의 암호화를 수행한다. 이후 통신하고자 하는 두 장치 사이에 임시 키가 공유되면 각 장치는 한 번의 해시와 두 번의 암호화를 수행하게 된다. 따라서 P3의 총 연산량은 6H+6E이다.

표 3. 프로토콜 연산량 비교
Table 3. Comparison of Calculation Amount of protocols

| | Operation amount of $D_1$ | Operation amount of $D_2$ | Operation amount of M | Total operation amount |
|---|---|---|---|---|
| P1 | 1H+2E | 1H+2E | none | 2H+4E |
| P2 | 2H+1E | 2H+1E | none | 4H+2E |
| P3 | 1H+2E | 3H+3E | 2H+1E | 6H+6E |

## Ⅵ. 결 론

본 논문은 기존에 제안된 OOB 채널을 이용한 키 교환 방법들이 지니는 문제점들을 제기하였다. 또한 OOB 채널의 통신 수단 및 환경에 따른 분류법을 제안하였으며 각 경우에 따른 프로토콜을 제시하였다. 이는 IoT 장치가 다른 OOB 채널을 가진 장치와 키를 교환할 때 OOB 채널을 부수적으로 탑재하지 않아도 된다는 이점을 준다. 또한 제시된 각각의 프로토콜은 주어진 상황에 따라 유동성 있게 적용이 가능하다. 즉, 다양한 이종 장치들이 포함되어 있는 IoT 환경에서 이용하기에 실용적이다.

## References

[1] X. Huang, X. Gao, and Z. Yan, "Security protocols in body sensor networks using visible light communications," *Int. J. Commun. Syst.*, vol. 29, no. 16, pp. 2349-2363, Nov. 2016.

[2] T. Kovačević, T. Perković, and M. Čagalj. "Flashing displays: user friendly solution for bootstrapping secure associations between multiple constrained wireless devices," *Secur. Commun. Netw.*, vol. 9, no. 10, pp. 1050-1071, Jul. 2016.

[3] J. Han, Y. H. Lin, A. Perrig, and F. Bai, "MVSec: Secure and easy-to-use pairing of mobile devices with vehicles," in *Proc. Secur. and Privacy in Wireless & Mob. Netw. 2014(WiSec 2014)*, pp. 51-56, Oxford, UK, Jul. 2014.

[4] R. Nandakumar, K. K. Chintalapudi, V.

Padmanabhan, and R. Venkatesan, “Dhwani: secure peer-to-peer acoustic NFC,” *ACM SIGCOMM Comput. Commun. Rev.*, vol. 43, no. 4, pp. 63-74, Oct. 2013.

[5] J. Suomalainen, “Smartphone assisted security pairings for the internet of things,” in *Wireless Commun., Veh. Technol., Inf. Theory and Aerospace & Electron. Syst. 2014 (VITAE 2014)*, pp. 1-5, Aalborg, Denmark, May 2014.

[6] A. Coppa, *Secure and User-Friendly Commissioning and Bootstrapping of Constrained Devices*(2015), Retrieved Apr., 10, 2017, from https://brage.bibsys.no/xmlui/handle/11250/2388270

[7] A. Liu and P. Ning, “TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks,” in *Proc. IPSN 2008*, pp. 245-256, Washington DC, USA, Apr. 2008.

[8] R. Watro, D. Kong, S. Cuti, C. Gardiner, C. Lynn, and P. Kruus, “TinyPK: Securing sensor networks with public key technology,” in *Proc. SASN 2004*, pp. 59-64, Washington DC, USA, Oct. 2004.

[9] S. Misra, S. Goswami, C. Taneja, and A. Mukherjee, “Design and implementation analysis of a public key infrastructure enabled security framework for ZigBee sensor networks,” *Int. J. Commun. Syst.*, vol. 29, no. 13, pp. 1992-2014, Nov. 2014.

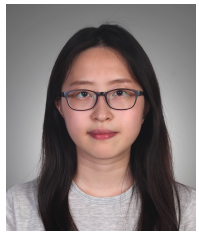
[10] S. Mirzadeh and H. Cruickshank, “Secure device pairing: A survey,” *IEEE Commun. Surveys & Tuts.*, vol. 16, no. 1, pp. 17-40, Dec. 2014.

[11] A. Lakshminarayanan, “Tap - Practical security protocols for wireless personal devices,” in *PIMRC 2004*, vol. 4, pp. 2884-2888, Barcelona, Spain, Sept. 2004.

[12] B. Zhang, Q. Zhan, S. Chen, M. Li, K. Ren, C. Wang, and D. Ma, “PriWhisper: Enabling keyless secure acoustic communication for smartphones,” *IEEE Internet of Things J.* vol. 1, no. 1, pp. 33-45, Jan. 2014.

[13] J. Kim and N. Kang, “Secure configuration scheme for internet of things using NFC as OOB channel,” *J. IIBC*, vol. 16, no. 3, pp. 13-19, Jun. 2016.

**반 효 진** (Hyo Jin Ban)



2015년 8월 : 덕성여자대학교 컴퓨터학과 졸업

2015년 8월~현재 : 덕성여자대학교 디지털미디어학과 석사과정

<관심분야> 인터넷 및 시스템 보안, 사물인터넷 보안

**강 남 희** (Namhi Kang)

2001년 2월 : 숭실대학교 정보통신대학원 공학석사

2004년 12월 : University of Siegen 컴퓨터공학과 공학박사

2009년 3월~현재 : 덕성여자대학교 디지털미디어학과 부교수

<관심분야> 유무선 인터넷통신, 통신보안프로토콜, 시스템 보안, 사물인터넷 보안