Journal of the Korea Academia-Industrial cooperation Society
Vol. 19, No. 11 pp. 303-309, 2018

https://doi.org/10.5762/KAIS.2018.19.11.303
ISSN 1975-4701 / eISSN 2288-4688

IoT 환경에서 해시 체인 기반 센서 상호 인증 기법

이광형[1*], 이재승[2]
[1]서일대학교 소프트웨어공학과, [2]숭실대학교 컴퓨터공학과

Mutual Authentication Method for Hash Chain Based Sensors in IoT Environment

Kwang-Hyoung Lee[1*], Jae-Seung Lee[2]
[1]**Dept. of Software Eng., Seoil University**
[2]**Dept. of Computer Science and Eng., Soongsil University**

요 약 사물인터넷 기술은 모든 사물을 인터넷에 연결하고 상호 작용하는 지능형 서비스로 군사지역의 탐색 목적은 물론 산업시스템에서의 디바이스 관리, 공정 관리, 비인가 지역의 모니터링 등 다양한 분야에 활용 가능한 기술이다. 하지만, 모든 기기들이 인터넷에 연결됨에 따라, 보안 취약점을 이용하는 다양한 공격으로 경제적 손실이나 개인정보 유출 등 다양한 피해를 발생 시키고 있으며, 추후 의료 서비스나 군사적 목적의 취약점 공격을 이용할 경우 인명 피해까지 발생할 수 있다. 따라서, 제안하는 논문에서는 통신 과정에서 해시체인 기반의 S/Key기술을 적용하여 디바이스간 상호인증과 키 생성과 갱신 등의 시스템을 도입함으로서 다양한 보안위협에 대응할 수 있는 상호인증 방법에 대해 연구 하였다. 제안하는 프로토콜은 이기종간 보안 통신에 적용 가능하며, IoT 환경에서 잘 알려진 공격인 재사용 공격, 중간자 공격, 데이터 무결성 등에 안전함을 확인할 수 있었다.

Abstract Internet of Things technology is an intelligent service that connects all objects to the Internet and interacts with them. It is a technology that can be used in various fields, such as device management, process management, monitoring of restricted areas for industrial systems, as well as for navigation in military theaters of operation. However, because all devices are connected to the Internet, various attacks using security vulnerabilities can cause a variety of damage, such as economic loss, personal information leaks, and risks to life from vulnerability attacks against medical services or for military purposes. Therefore, in this paper, a mutual authentication method and a key-generation and update system are applied by applying S/Key technology based on a hash chain in the communications process. A mutual authentication method is studied, which can cope with various security threats. The proposed protocol can be applied to inter-peer security communications, and we confirm it is robust against replay attacks and man-in-the-middle attacks, providing data integrity against well-known attacks in the IoT environment.

Keywords : Hash Chain, Internet of Things, IoT, IoT Authentication, IoT Security, S/Key Authentication, S/Key Protocol

1. 서론

사물인터넷(Internet of Things)은 모든 사물을 인터넷을 통해 연결함으로서 사람과 사물, 사물과 사물 간의 정보의 통신 및 교환을 통해 상호 작용하는 지능형 기술 및 서비스를 말한다. 이러한 사물인터넷 환경에서는 지

본 논문은 2018년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : Kwang-Hyoung Lee(Seoil Univ.)
Tel: +82-2-490-7226 email: dreamace@seoil.ac.kr
Received September 17, 2018 Revised (1st October 2, 2018, 2nd October 4, 2018)
Accepted November 2, 2018 Published November 30, 2018

능형 서비스를 제공하기 위해 다양하고 방대한 양의 디바이스 정보를 수집하며, 사람이나 동/식물, 공간이나 특정 프로세스 등의 정보를 기반으로 서비스를 제공받고 디바이스를 제어한다. 이러한 IoT 서비스의 핵심 포인트는 언제 어디서나 지속적으로 서비스가 제공되어야 한다는 점이다[1-2]. 또한, 다양한 디바이스를 통해 정보가 전송되고 제어되기 때문에 올바른 표준을 기반으로 통신이 이루어져야 한다. 또한, 이 때 정보를 전송하는 디바이스 별 보안방안을 제공하여 디바이스 하드웨어 제한에 따른 각기 다른 보안이 제공되어야 하며 그렇지 않을 경우 경제적 피해는 물론 의료 서비스나 군사적 목적으로 활용할 경우에는 인명 피해까지 발생 시킬 수 있다. 또한, 일상의 모든 사물이 인터넷에 연결되어 있으므로 개인의 프라이버시나 금융 피해 등 다양한 범죄의 표적이 될 수 있다[3-5].

이에 따라, 최근에는 국내는 물론 미국, 유럽, 중국 등 국내·외에서 IoT 기술의 전략적 육성을 위해 연구단체 및 다양한 기업들이 참여하여 표준 통신 프로토콜 연구를 진행하고 있으며, 기존 무선 센서 네트워크(Wireless Sensor Network)의 기술을 환경에 맞게 응용하여 적용하는 등 다양한 개발이 진행되고 있다.

하지만, 지속적인 서비스를 위해서는 경량화 되고 안전한 통신 규약이 필요하지만, 기존 연구들의 대부분 공개키 통신을 하는 등 에너지 효율이 떨어지는 보안 통신을 하고 있다. 현재 IoT 서비스에서는 이미 취약점이 들어난 커버로스나 에너지 효율성을 고려하지 않은 PKI 시스템 등을 보안기술로서 활용하고 있으며, 따라서 스마트 더스트(Smart Dust)등과 같은 초소형 센서 등에 적용 가능한 경량화 인증 기술이 필요한 상황이다.

2. 관련 연구

2.1 Internet of Things

사물인터넷(Internet of Things)은 도처의 모든 사물들이 인터넷에 연결되어 커뮤니케이션을 통해 정보를 주고받는 지능형 기술 및 서비스를 말한다. 인간의 제어 및 간섭 없이도 디바이스 스스로 대화하고 주변 환경을 분석하여 정보를 통해 서비스를 제공하는 개념으로 디지털 혁명의 기술로 떠오르고 있다.

1999년에 MIT Auto-ID Center를 설립한 Kevin Ashton이 처음 사물 인터넷에 대한 개념과 용어를 처음 제안하면서 사용되기 시작한 이후 지속적으로 발전을 거듭해 왔다. 최근의 사물인터넷은, 다양한 기기들과 소프트웨어, 서비스 등의 개발로 실생활 속에서 손쉽게 접하고 활용할 수 있다[6].

사물인터넷을 활용한 디바이스 및 서비스 등의 제품은 다양한 루트로 시장에 나와 있다. 특히 스마트 홈과 스마트 카, e-헬스 등 실생활에 밀접한 관련이 있는 분야에서 사물인터넷을 제공하는 서비스 및 제품에 대한 기술 개발이 한창인 상황이다. 사물인터넷에서는 디바이스들 간의 네트워크를 이요한 통신이 이루어져야 하며, 이를 지원하는 기술로서 기기간 통신 (Machine-to-Machine Communication)이 활용되고 있다. 실제로 현재 사용되어 지고 있는 구글 글라스나 컨넥티드 자동차 등은 M2M 기술을 사용하고 있다[7-8].

현재 개발 되어진 많은 사물인터넷 서비스 그리고 디바이스들은 동일 제조사나 동일 서비스 영역에서만 동작을 하는 경우가 대부분이다. 서로 다른 제조사로부터의 사물들, 그리고 다른 사업 영역에서 사용되어지는 사물들 (예를 들어, 스마트 홈의 가전과 스마트 카) 간의 사물 통신이 이루어지기 위해서는 표준화된 방식이 절대적으로 필요한 상황이며, 또한 그에 맞는 보안 기술로 필요하다[9].

2.2 S/Key Algorithm

S/Key 알고리즘 방법은 해시 체인 기반의 도청 및 재사용 공격 등에 안전한 인증 방법으로서 단 방향 해시 함수와 배타적 논리합을 사용하는 단순한 인증 기법으로 사용하기에 간단하고 쉬워 경량화 인증에 활용이 가능하다[10-11].

먼저, 클라이언트는 임의의 키를 만들어 서버로 전송하며, 서버는 클라이언트로 받은 키를 이용하여 해시 체인 방법과 같이 해시 값을 구하는 작업을 n번 진행하여 서버에 저장한다.

이후, 인증을 요구할 때, 클라이언트는 n-i번 해시 함수를 중첩 하여 서버로 전송한다(이때, i는 i번째 인증을 요구할 때의 값으로 가정함). 서버에서는 클라이언트가 전송한 값의 해시 함수를 계산하여 기존에 저장해 둔 n-i+1번째의 해시 값과 일치하는지 확인하며, 일치할 경우 인증에 성공한 것으로 적용하여 카운트 값을 1씩 증가 시킨다. S/Key 알고리즘은 해시 함수가 가지고 있는

역연산의 어려움에 기반한 알고리즘으로 중간에 해시 값이 노출된다 하더라도, 인증을 위한 일회용 해시 값이므로 재사용이 불가능하다. 또한, 인증을 위해 전송된 값보다 이전의 해시 값을 사용해야 하는데, 해시 함수의 특성상 역연산의 어려움을 가지고 있어 유추하기 어렵다는 장점이 있다[12].

2.3 기존 연구 분석

Porambage 등은 ECC(Elliptic Curve Cryptography)에 기반하는 인증서 기반 키 교환 프로토콜을 제안하였다. Porambage 등은 인증서를 인증기관을 통해 등록하고, 인증기관에서 발급한 인증서를 이용하여 디바이스를 인증하며, 그 과정에서 타원 곡선의 점을 이용한 인증 값, 인증기관을 통해 공개된 공개 키, 랜덤한 값 등을 활용하여 인증 과정을 걸친다. 다만 Porambage 등의 프로토콜의 경우 식별 과정이 존재하지 않고, 악의 적인 사용자가 인증기관을 위장할 경우 대처할 수 없다. 또한, 공격에 성공할 경우 $(d_u Q_{v'} = d_v Q_u)$의 계산을 이용하여 개인키를 추측할 수 있는 등의 문제가 존재 한다[13].

Farash 등의 프로토콜의 경우 기존 3PAKE 프로토콜의 비밀번호 추측에 대해 취약함을 증명하고 이를 보안하며, 공개키 없이 서버의 인증이 가능한 프로토콜은 제안하였지만, 세션 키를 성립하기 이전 서로 다른 디바이스들의 인증이 불가능하여 온라인 패스워드 공격 등 보안 위협을 가지고 있다[14].

Baruah 등이 제안한 프로토콜의 경우 ID와 Password 및 생체 정보를 활용한 인증 방법으로, 등록 과정을 통해 게이트웨이에 ID, Password, 생체 정보를 등록하고 hash 과정을 거쳐 hash 값을 이용하는 인증 절차를 가진다. 이때, Password와 생체 정보를 이용하여 만들어진 R1 값이 유출 될 경우 악의 적인 사용자가 별다른 과정 없이 인증이 가능한 등 데이터 위변조와 중간자 공격 등에 취약점을 가지고 있다[15].

3. 제안 내용

본 연구에서는 군사 지역 등과 같이 사람의 진입이 어려워 소형 센서를 기반으로 하는 IoT 환경에서 S/Key 프로토콜을 이용한 상호인증 기법을 제안한다. 제안하는 기법은 에너지 효율성을 위해 특정 클러스터 내에서 중간 역할을 하는 MN(Middle Node)를 특정 시간마다 선출하며, MN을 통해 센서들이 경량화 상호 인증함으로서 에너지 효율성을 높였다.

Table 1. Proposed Notation

Notation	Meaning
ID_i	Node i ID
R_i	Node i Random Number
N_n	Hash Value
E_m	Key m Encryption
$H()$	Hash Function

3.1 S/Key를 활용한 기본 구조

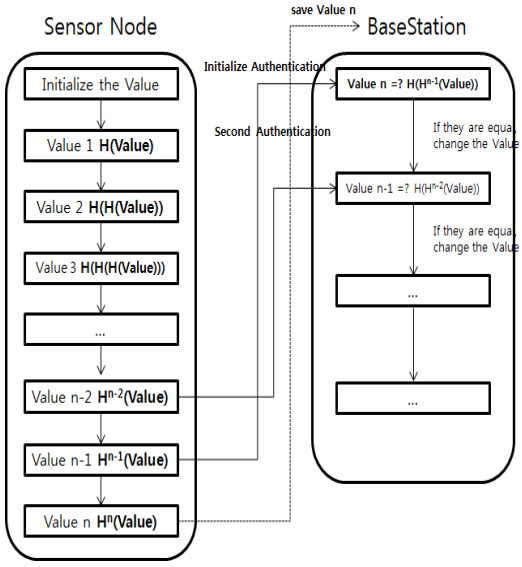

Fig. 1. Initial design based on hash chain

센서 노드들은 사전에 BS와 대칭키 암호 알고리즘에 기반한 Key를 공유하고 있으며, 센싱 지역에 배치되기 전 특정 Value를 이용한 해시 체인 기반의 해시 값들을 생성하여 저장하고, 마지막 생성된 해시 값 $H^n(Value)$를 BS에 공유 한다.

[그림 1]과 같이 센서 노드는 Value 값을 이용하여 순차적으로 해시를 진행하며, 마지막으로 얻은 $H^n(Value)$ 값을 공유한다. 이후, 인증이 필요할 때, 센서 노드는 $H^{n-1}(Value)$를 BS에 전송하며, BS는 $H^{n-1}(Value)$에 해시 함수를 적용하여 $H^n(Value)$와

비교하여 검증한다. 이후, 검증에 성공하며 카운트 값을 감소하고, 이전에 사용한 해시 값은 폐기한다.

3.2 Sensor Node 와 MN 인증 과정

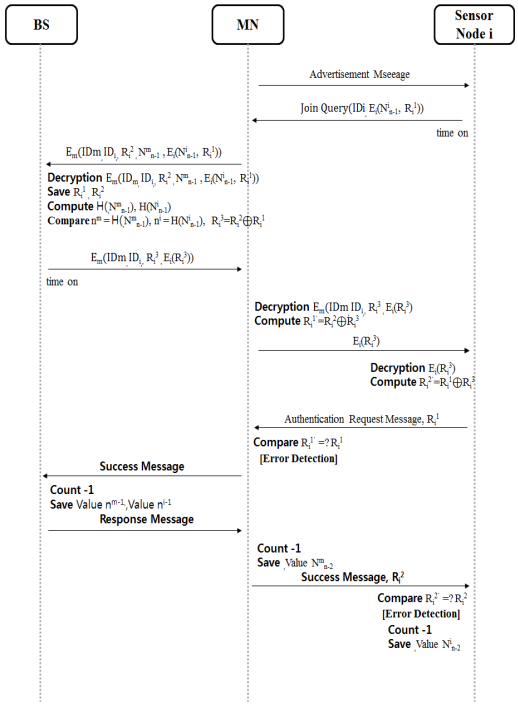

Fig. 2. Sensor Node -MN Authentication Protocol

MN에 선출된 노드는 주변 센서 노드들에게 광고메시지를 보내며, 센서 노드는 두 개 이상의 MN 광고 메시지를 수신할 경우 가까운 MN에게 조인 쿼리를 본인의 ID와 BS와의 대칭키를 통해 암호화하여 해시 값 N_{n-1}^{i}, 난수 R_i^1 를 생성하여 전송한다. 이를 수신한 MN은 BS와의 대칭키를 통해 암호화 하여 노드와 MN의 ID, MN이 생성한 난수 R_i^2 , 해시 값 N_{n-1}^{m} 과 노드로부터 받은 암호화된 값을 BS에게 전송한다.

BS는 전송받은 값을 복호화 하여 R_i^1, R_i^2를 저장하고 $H(N_{n-1}^{m})$와 $H(N_{n-1}^{i})$, $R_i^1 \oplus R_i^2$를 계산한다.

이후, $n^m = H(N_{n-1}^{m})$, $n^i = H(N_{n-1}^{i})$를 통해 전송된 값을 검증하고, MN과 센서 노드의 ID, R_i^3를 암호화 하여 MN에게 전송한다.

BS로부터 암호화된 값을 수신 받은 MN은 이를 복호화하고 $R_i^1 = R_i^2 \oplus R_i^3$를 통해 R_i^1을 추론한다. 이후 BS로부터 받은 $E(R_i^3)$값을 센서 노드로 전송한다.

센서 노드는 전송 받은 값 $E(R_i^3)$을 복호화 하고 $R_i^2 = R_i^1 \oplus R_i^3$값을 추론 한다. 이후 R_i^1값을 MN에게 보내고 MN은 기존에 생성한 R_i^1 값과 비교하여 검증한다. 이후, BS에게 인증 성공 메시지를 전송하면 BS는 다음 인증을 위해 Value 값을 감소시키고 저장한다. 이후 응답 메시지를 전송하면, MN도 Value값을 한 단계 감소시키며, 센서 노드에게 인증 완료 메시지와 함께 R_i^2 값을 전송한다. 센서 노드는 R_i^2값을 검증하고 Value 값은 감소시키며 인증 과정을 종료 한다.

3.3 Sensor Node 와 MN 통신 과정

센서 노드는 데이터 통신 및 전송이 필요할 때, 본인의 ID와 BS와의 대칭키를 통해 암호화하여 해시 값 N_{n-a}^{i}, 난수 R_i^i 를 생성하여 전송한다. 이때, a는 현재까지의 통신 횟수를 의미 한다. 이를 수신한 MN은 BS와의 대칭키를 통해 암호화 하여 노드와 MN의 ID, MN이 생성한 난수 R_i^j , 해시 값 N_{n-a}^{m} 과 노드로부터 받은 암호화된 값을 BS에게 전송한다.

BS는 전송받은 값을 복호화 하여 R_i^i, R_i^j를 저장하고 $H(N_{n-a}^{m})$와 $H(N_{n-a}^{i})$, $R_i^i \oplus R_i^j$를 계산한다.

이후, $n^{m-a+1} = H(N_{n-a}^{m})$, $n^{i-a+1} = H(N_{n-a}^{i})$를 통해 전송된 값을 검증하고, MN과 센서 노드의 ID, R_i^z, $E_i(R_i^z)$를 암호화 하여 MN에게 전송한다.

이를 수신한 MN은 복호화 이후 $R_i^z \oplus R_i^j$를 이용하여 R_i^i를 생성하고, $E_i(R_i^z)$값을 센서 노드에게 전송한다. 센서 노드는 복호화 이후 $R_i^z \oplus R_i^i$를 계산하여 R_i^j를 생성 후 R_i^i를 MN에게 전송한다. MN은 자신이 생성한 R_i^i의 유효성 검사 후 새로운 키를 생성하고, BS에게 인증 사실을 알리며, BS는 Value n을 감소시키고 응답하며, MN도 Value n값을 감소시킨 후 R_i^j값을 센서 노드에게 전송한다. 센서 노드는 R_i^j 값의 유효성 검사 이후 새로운 키를 생성하고, 이후 이 키를 이용하여 MN과 데이터 통신을 진행 한다.

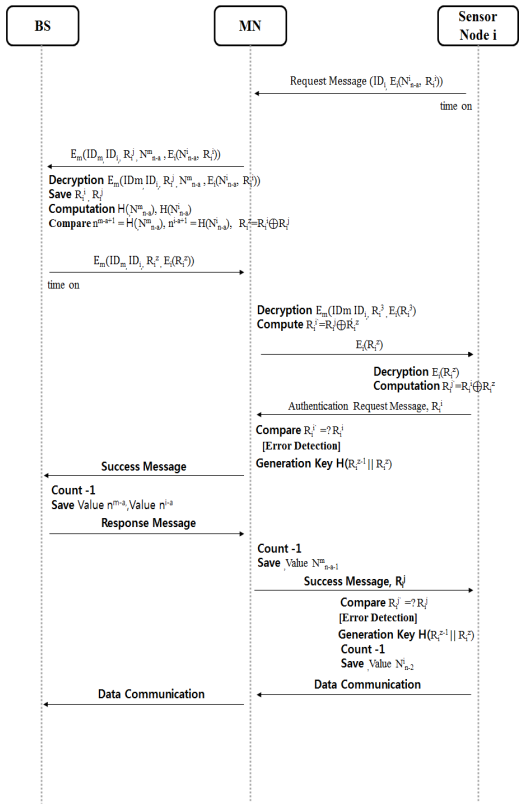

Fig. 3. Sensor-MN Communication Protocol

4. 보안성 평가

4.1 보안성 비교 평가

본 절에서는 디바이스 인증 및 등록, 키 교환 과정 등 IoT 환경에서 가능한 보안위협과 요구사항을 파악하고 그에 대한 안전성을 평가 하며 기존 IoT 환경에서 보안 기술을 적용한 인증 기법들과 비교 평가 한다.

Table 2. Security Analysis

	farash	porambage	baruah	Proposed
Mutual Authentication	X	O	O	O
Replay Attack	O	O	X	O
data integrity	O	X	O	O
Man in the Middle Attack	O	O	X	O
Session Key Management	X	X	X	O

4.2 안전성 비교 분석

기존 사물인터넷 환경에서 제안하는 보안 스킴에서 farash 스킴의 경우 재사용 공격과 데이터 무결성, 중간자 공격에 대해 보안성을 제공하지만, 디바이스간 상호 인증, 세션 키 관리 측면에서 취약점을 가지고 있다. Proamb 스킴의 경우 데이터 무결성, 세션 키 관리 측면에 취약점을 가지고 있으며, baruah 스킴의 경우 재사용 공격과 중간자 공격, 세션키 관리 측면에 취약점이 존재하고 있다.

본 연구에서는 베이스 스테이션이 Middle Node, Sensor Node 간 통신을 진행할 때, OTP 인증 프로토콜 중 하나인 해시 체인에 기반한 S/Key 프로토콜을 이용하여 인증과정을 설계 하였다. 해시 체인의 경우 해시 함수의 역연산 어려움에 기반하고 있으며, 공격자에 의해 노출 되는 경우가 생기더라도 Value n이 일회용으로 사용되므로 공격자는 이후 인증에 사용되는 해시 값을 유추하기 어려워 안전한 인증이 가능하다. 또한, Middle Node, Sensor Node 간에도 베이스 스테이션을 이용한 1차 인증과 임의의 수 R_x^y 값을 이용한 인증을 진행하고 있어 안전한 상호 인증이 가능하다. 또한, 재사용 공격의 경우, 본 연구에서는 해시 체인을 기반으로 설계하여 일회용 값을 사용하고 있으므로 다시 사용하는 것이 불가능하다. 그리고, 값이 노출 되더라도 다음 인증을 위해서는 탈취한 해시에 해시 함수를 적게 적용된 해시 값을 유추해야 하는데 이는 매우 어렵다. Middle Node, Sensor Node간 데이터 통신을 할 경우, 인증 과정 이후 $H(R_i^{z-1}||R_i^x)$ 계산을 통해 세션 키를 생성하고 이후 통신에는 갱신함으로서 탈취한 메시지는 유효성을 가지지 않는다. 데이터 위변조에 의한 무결성 공격의 경우 1차적으로 세션 성립 당시의 키를 추측하는 것이 매우 어려워 원하는 메시지로의 위변조는 사실상 불가능 하다. 지속적으로 키가 갱신되어 $H(R_i^{z-1}||R_i^x)$를 사용하기 때문에 메시지의 위·변조로 인한 공격에 대하여 안전하다.

중간자 공격의 경우 각 디바이스들은 상호 인증된 상태에서, 난수 R과 N 등 해당 디바이스들이 아니면 알 수 없는 값들을 암호화 하여 전송하고 인증하기 때문에 중간자 공격에 대한 검증이 가능하다. 또한, 세션 키는 디바이스가 추가되거나 특정 영역마다 갱신됨으로서 세션 키 유출이나 추측 공격에 대해 안전성을 가진다.

5. 결론

본 논문에서는 IoT 환경에서 해시 체인 기반의 S/Key Protocol을 이용하여, 센서와 센서, 베이스 스테이션과의 안전한 상호 인증 방법을 제안하였으며, 소형 센서 디바이스를 이용하여 정보를 수집하는 환경에서 중간 센서 노드를 활용함으로서 에너지 효율성을 향상 시킬 수 있도록 제안하였다.

제안하는 방식은 IoT 환경에서 발생 가능한 재사용 공격이나 위변조 공격, 키 탈취 등 다양한 보안 위협에 대응할 수 있으며, 센서 노드들이 특정 확률과 시간에 따라 중간 노드를 선출하고, 중계자 역할을 하도록 함으로서 기존 환경에 비해 에너지 효율성을 증가 시켰다.

제안하는 방법을 통해 군사 지역이나 산간 지역 등 사람의 출입이 제한된 환경에서 소형 센서 디바이스를 이용한 안전한 데이터 수집이 가능할 것으로 기대 된다.

References

[1] YICK, Jennifer; MUKHERJEE, Biswanath; GHOSAL, Dipak. Wireless sensor network survey. Computer networks, 52.12: 2292-2330. 2008.
DOI: https://doi.org/10.1016/j.comnet.2008.04.002

[2] ZHANG, Zhi-Kai, et al. IoT security: ongoing challenges and research opportunities. In: Service-Oriented Computing and Applications (SOCA), 2014 IEEE 7th International Conference on. IEEE, pp. 230-234. 2014.
DOI: https://doi.org/10.1109/soca.2014.58

[3] XU, Teng; WENDT, James B.; POTKONJAK, Miodrag. Security of IoT systems: Design challenges and opportunities. In: Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design. IEEE Press, pp. 417-423. 2014.
DOI: https://doi.org/10.1109/iccad.2014.7001385

[4] RIAHI, Arbia, et al. A systemic approach for IoT security. In: Distributed Computing in Sensor Systems (DCOSS), 2013 IEEE International Conference on. IEEE, pp. 351-355. 2013.
DOI: https://doi.org/10.1109/dcoss.2013.78

[5] MAHMOUD, Rwan, et al. Internet of things (IoT) security: Current status, challenges and prospective measures. In: Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for. IEEE, pp. 336-341. 2015.
DOI: https://doi.org/10.1109/icitst.2015.7412116

[6] ZHAO, Kai; GE, Lina. A survey on the internet of things security. In: Computational Intelligence and Security (CIS), 2013 9th International Conference on. IEEE, pp. 663-667. 2013.
DOI: https://doi.org/10.1109/cis.2013.145

[7] WURM, Jacob, et al. Security analysis on consumer and industrial iot devices. In: Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific. IEEE, pp. 519-524. 2016.
DOI: https://doi.org/10.1109/aspdac.2016.7428064

[8] RIAHI, Arbia, et al. A systemic and cognitive approach for IoT security. In: Computing, Networking and Communications (ICNC), 2014 International Conference on. IEEE, pp. 183-188. 2014.
DOI: https://doi.org/10.1109/iccnc.2014.6785328

[9] YAO, Xuanxia, et al. A lightweight multicast authentication mechanism for small scale IoT applications. IEEE Sensors Journal, 13.10: 3693-3701. 2013.
DOI: https://doi.org/10.1109/jsen.2013.2266116

[10] N. Haller, Bellcore, The S/KEY One-Time Password System, February 1995.
DOI: https://doi.org/10.17487/rfc1760

[11] PARK, Joonggil. The development of a one-time password mechanism improving on S/KEY. Korea Institute of Information Security & Cryptology, 9.2: 25-35. 1999.

[12] ZHANG, Yuan, et al. Training Demand Analysis for Airlines Safety Manager Based on Improved OTP Model. In: International Conference on Human-Computer Interaction. Springer, Cham, pp. 334-342. 2018.
DOI: https://doi.org/10.1007/978-3-319-92285-0_46

[13] Pawani Porambage, Corinna Schmitt, Pardeep Kumar, Andrei Gurtov, Mika Ylianttila, “Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications”, IEEE Wireless Communications and Networking Conference (WCNC), 04. 06. 2014.
DOI: https://doi.org/10.1109/wcnc.2014.6952860

[14] Farash, Mohammad Sabzinejad, Turkanović Muhamed, Kumari Saru, and Marko Hölbl. "An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the internet of things environment." Ad Hoc Networks 36, 152-176. 2016.
DOI: https://doi.org/10.1016/j.adhoc.2015.05.014

[15] Baruah, Khanjan Ch, Banerjee Subhasish, Dutta Manash P, Bhunia Chandan T. "An improved biometric-based multi-server authentication scheme using smart card." International Journal of Security and Its Applications 9.1, 397-408. 2015.
DOI: https://doi.org/10.14257/ijsia.2015.9.1.38

이 광 형(Kwang-Hyong Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 (공학사)
- 2002년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 소프트웨어공학과 부교수

<관심분야>
멀티미디어 보안, 사물인터넷, 학습콘텐츠, 영상처리

이 재 승(Jae-Seung Lee) **[정회원]**

- 2013년 2월 : 평생교육진흥원 컴퓨터학과(공학사)
- 2015년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2015년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사수료

<관심분야>
시큐어코딩, Sensor Network, IoT Security