Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 12 pp. 76-82, 2019

https://doi.org/10.5762/KAIS.2019.20.12.76
ISSN 1975-4701 / eISSN 2288-4688

# IoT 환경에서 안전한 통신을 위한 인증 및 그룹 키 관리 기법

민소연[1*], 이재승[2]
[1]서일대학교 정보통신공학과, [2]숭실대학교 컴퓨터공학과

# Authentication and Group Key Management Techniques for Secure Communication in IoT

So-Yeon Min[1*], Jae-Seung Lee[2]
[1]Dept. of Information and Communication Eng., Seoil University
[2]Dept. of Computer Science and Eng., Soongsil University

**요 약** 인터넷의 기술의 발전과 스마트 디바이스의 보급은 사람들에게 편리한 환경을 제공해 주고 있으며, 이는 IoT라는 기술로 보편화 되고 있다. 그러나 IoT 기술의 발전과 수요는 이를 악용한 해커들의 공격으로 인해 개인 정보 유출과 같은 다양한 문제를 야기시키고 있다. 수많은 디바이스들이 네트워크에 연결되는 환경이 조성되었고, 기존 PC 환경에서 악용되던 네트워크 공격이 IoT 환경에서 발생하고 있다. 실제 IP 카메라의 경우 해킹을 통해 DDoS 공격을 진행하거나, 개인정보 유출, 동의 없이 모니터링 하는 등의 보안사고가 발생하고 있다. 이제는 IP카메라나 태블릿 등 IoT 환경에서 활용되는 다양한 스마트 기기가 네트워크 공격에 활용될 수 있음을 확인할 수 있다. 하지만, IoT 환경에서 소형 디바이스들이 가지는 특성상 Memory 공간이나 Power 등이 제한되어 있어 기존 보안 솔루션 설치 및 실행에 어려움을 가지고 있다. 따라서 본 논문에서는 IoT 환경에서 발생할 수 있는 보안 위협에 대해 살펴보고 이를 방지할 수 있는 보안 프로토콜을 제안한다. 제안하는 프로토콜은 보안평가를 통해 네트워크에서 발생할 수 있는 다양한 보안 위협에 대응 가능함을 확인할 수 있었다. 또한, 에너지 효율성 분석을 기존 보안 알고리즘으로 활용되는 ECC, RSA, Kerberos 등에 비해 디바이스 증가에 따른 인증 속도에서 최소 2배 이상의 속도가 개선되는 등 디바이스 수의 증가에 따라 인증 시간이 가파르게 감소함을 확인할 수 있었다. 따라서 본 프로토콜을 IoT 환경에 적용한다면 효율적인 운영이 가능할 것으로 기대 된다.

**Abstract** The development of Internet technology and the deployment of smart devices provide a convenient environment for people, and this is becoming common with the technology called the Internet of Things (IoT). But the development of, and demand for, IoT technology is causing various problems, such as personal information leaks due to the attacks of hackers who exploit it. A number of devices are connected to a network, and network attacks that have been exploited in the existing PC environment are occurring in the IoT environment. When it comes to IP cameras, security incidents (such as distributed denial of service [DDoS] attacks, hacking someone's personal information, and monitoring without consent) are occurring. However, it is difficult to install and implement existing security solutions because memory space and power are limited owing to the characteristics of small devices in the IoT environment. Therefore, this paper proposes a security protocol that can look at and prevent IoT security threats. A security assessment verified that the proposed protocol is able to respond to various security threats that could arise in a network. Therefore, it is expected that efficient operation of this protocol will be possible if it is applied to the IoT environment.

**Keywords :** Internet of Things, IoT, IoT Authentication, IoT Security, IoT Device Authentication

본 논문은 2019년도 서일대학교 학술연구비에 의해 연구되었음.
*Corresponding Author : So-Yeon Min(Seoil Univ.)
email: symin@seoil.ac.kr
Received September 25, 2019 Revised October 17, 2019
Accepted December 6, 2019 Published December 31, 2019

## 1. 서론

무선 통신 기술 및 디바이스의 발전은 오늘날 사물인터넷으로 발전하여 우리 사회에 손쉽게 찾아보고 활용하고 있다. 이러한 사물인터넷은 1999년 용어 및 개념으로 처음 등장하였으며, 지속적 발전을 통해 2018년에는 약 80억 이상의 사물인터넷 디바이스가 인터넷에 연결되어 있는 등 고속 성장이 진행되고 있다. 이러한 사물인터넷의 발전은 우리 사회에 다양한 형태로 보급되어 사람들은 시간과 공간 등에 제약 없이 디바이스를 제어하고 활용함으로서 일상생활의 편리성이 증가되고 있다. 단, 이러한 발전에 맞춰 이를 악용하는 사례들도 등장하고 있다. 사물인터넷이 가지는 네트워크나 디바이스 자체의 취약점 등을 악용해 해킹을 하거나 개인정보를 유출하고, DDoS 공격에도 악용하는 등 다양한 보안 사고를 발생시키고 있다. 실제 현재 사용 하는 사물인터넷 디바이스들은 기존 PC 및 모바일, 태블릿 등에 비해 상당히 낮은 수준의 Process Power 및 Memory 등을 활용하고 있어, 기존의 보안 프로토콜을 적용하는데 한계를 가지고 있다[1,2]. 실제로, 인터넷 도메인을 서비스하는 딘(Dyn)에 IoT 디바이스를 이용한 대규모 디도스(DDoS) 공격이 발생하였으며, 이 공격으로 인해서 수요가 높은 넷플릭스나 아마존, 트위터와 같은 수많은 주요 인터넷 사이트들이 오랜 시간 서비스를 하지 못하는 사건이 있었다. 디도스 공격의 경우 기존에 자주 사용되는 공격 방법이었지만, 주로 PC를 이용한 공격 방법이었다. 하지만, 이번사례를 통해 일상생활에서 사용하고 있는 가전용 홈 IoT 기기들이나 IP 카메라, CCTV(Closed Circuit TeleVision) 등 스마트 기기를 이용한 공격이 가능함을 확인할 수 있었다. 또한, Internet Explorer에 연결된 임베디드 디바이스를 통한 전통적인 HTTP 결함공격도 발견되었다, 이는, 클라우드 서비스에 자원의 과부하를 일으키는 것을 목표로 하였다. 여기서 사용된 공격의 경우 기존의 전통적인 컴퓨터 봇넷이 아니라, 전 세계의 IP 카메라에서 나왔으며, 최대 초당 2만 개의 요청을 만들었으며, 리눅스 임베디드 버전과 비지박스 툴킷을 사용한 약 900여대의 CCTV에서 만들어졌다고 한다. 컴퓨터의 경우 악성 코드에 감염시키기 위해서 소프트웨어 자체 취약점이나 소셜엔지니어링 등의 방법을 활용하지만, 앞서 설명한 사례에서 공격한 방법의 경우 Telnet, SSH를 통해 인터넷으로 액세스 할 수 있어 쉽게 공격이 가능 하다. 관리적 측면에서도 문제들이 발생하는데, 기존 초기 인증 값으로 ID와 Password 조합에 “ID : root, Password : admin"과 "ID : admin, Password"등이 빈번하게 사용되는 경우가 많았으며, 이는 제품 출시 후 기본으로 설정된 ID와 Password를 변경하지 않아서 발생하였다. 이렇듯 현재 사물인터넷 디바이스의 취약점을 이용한 문제가 다양하게 발생하고 있으며, 이러한 문제를 방지하기 위해 디바이스 보안 내재화 적용을 해야 하지만 쉽지가 않다. 활용 용도에 따라 디바이스 크기가 제한돼 있어서 충분한 메모리나 파워를 탑재하기 힘들고, 이로 인해 보안 솔루션 설치를 실행하기가 어렵고 물리적 접근이 쉬워서 인증·암호키를 보호하기도 더욱더 어렵다. 이에 따라, 사물인터넷 디바이스를 이용한 개인정보 유출이나 DDoS 공격은 앞으로도 지속적으로 발생될 것으로 보인다. 사물인터넷은 지속적으로 발전하여 2022년에는 약 350억 개의 디바이스가 인터넷에 연결될 것으로 예측되고 있으며, 취약점 관리를 하지 않는다면, 지속적인 혼란이 야기 될 수 있다[3~5].

따라서 본 논문에서는 사물인터넷 환경에서 안전하게 통신을 위한 인증 및 키 교환 기법을 제안하며, 메모리나 연산 능력의 한계로 기존의 보안 프로토콜 적용이 어려운 디바이스들에 대한 적용 가능한 인증 기법을 제안한다.

## 2. 관련 연구

### 2.1 Internet of Things

사물인터넷은 디바이스들에 네트워크 연결 기능을 내장하여 사람과 사물, 사물과 사물 등을 인터넷에 연결하여 무선 네트워크를 통해 사물을 연결하여 통신하는 기술을 의미한다. 각각의 디바이스들은 네트워크에 연결되어 데이터를 수집하고, 전달하며 최근에는 수집된 데이터를 분석하고 학습하여 의미 있는 가공된 데이터를 사용자에게 제공하는 등 다양한 형태로 발전되고 있다. 사물인터넷 디바이스의 범주에는 네트워크가 가능한 무선 센서, 모바일 장비, 홈 네트워크에 사용되는 디바이스, 웨어러블 디바이스 등 네트워크를 통해 통신 가능한 모든 디바이스를 통칭 하며, 따라서 이러한 디바이스들은 각각 고유의 IP Address를 통해 인터넷에 연결되고 있다. 다만, 대부분 이러한 사물인터넷 디바이스들은 24시간 네트워크에 연결되어 있고, 기존 PC나 모바일 디바이스와 다르게 메모리나 파워, 연산 능력 등에 한계를 지니고 있어 쉽게 해킹 대상으로 노출되고 있다[6].

실제 Symantec에 따르면, 사물인터넷이 우리 사회에 보편화됨에 따라 발생 가능한 보안 취약에 대해 지적하였다. 현재까지 대부분의 사물인터넷 디바이스 들은 리눅스 운영체제 기반에서 적절한 보안 프로토콜을 적용하지 않거나, 신규 취약점들에 대한 보안 업데이트가 이루어지지 않을 시 지속적인 해킹 위험에 노출될 것이라고 경고했다. 사물인터넷 특성상 Symantec가 우려하는 적절한 업데이트나 보안 프로토콜 적용은 어려운 상황이며, 실제 이러한 취약점을 이용한 공격 사례는 지속적으로 증가하고 있다. 또 다른 우려 사항은  표준의 문제이다. 사물인터넷의 급격한 성장에 비해 보안 기술이 따라가지 못하고 있으며, 여러 보안 표준과 프레임워크가 등장하고 있지만, 전 세계적으로 공통의 규정이나 방법론을 확립하지 못하고 있다[7]. 2017년 초에는 National Security Council에서 Interagency International Cybersecurity Standardization Working Group를 신설하고 보안에 대해 검토하였지만 아직까지 '현황 파악'에만 그쳐 있다.

### 2.2 OWASP IoT 10대 취약점

2.1을 통해 사물인터넷 보편화에 따라 보안 위협이 지속적으로 증가할 것이라 설명하였으며, OWASP(Open Web Application Security Project)가 발표한 OWASP Top 10을 통해 주의해야할 요소들에 대해 정의하였다.

먼저, OWASP에서 첫 번째 취약점으로 쉬운 암호와 유추할 수 있는 암호, 그리고 하드코딩된 암호 등 암호 취약점에 대해 언급하였다. 이는 디바이스가 가지는 한계로 인해 brute force attack 이나 소프트웨어를 통한 백도어 등으로 발생할 수 있다. 두 번째는 네트워크 안전성 문제로서 가용성을 훼손하거나 인가되지 않은 사용자에 대한 제어 허용 등으로 인해 발생하는 문제를 의미한다. 세 번째는 사용자에 대한 인증 및 승인 기능의 부재, 암호화의 부재 또는 빈약함, 입출력 필터링의 부재 등의 문제를 지적하였으며, 네 번째는 업데이트 메커니즘에 대해 언급하였다. 다섯 번째는 안전하지 않거나 오래된 소프트웨어를 지속적으로 사용하여 발생하는 문제들을 포함하였으며, 그 다음으로는 불충분한 개인정보에 대한 부분과 안전하지 않은 데이터 통신에 대해 정의하였다. 또한, 디바이스 관리의 부재와 기본 설정의 문제, 물리적 보호 수단의 부재에 대해 정의하였다[8~10].

## 3. 제안 내용

### 3. 제안 내용

본 논문에서 디바이스, 사용자 및 인증센터 입장에서 사용자 코드(User Code)와 랜덤(Random Data), 실시간 요청 시간(Real Time) 값 등을 활용하여 안전한 인증 프로토콜을 제안한다.

본 논문의 절차는 3단계로 나누어진다. 첫 번째는 사용자와 IoT 디바이스가 등록하는 과정으로 디바이스 활용을 위해 인증센터에 사용자 등록을 위한 ID/PW 기반 등록 절차를 진행하며, 이 과정에서 제품의 시리얼 넘버와 랜덤한 값, 이후 인증 과정에서 활용하게 될 다항식 전송 과정을 거친다. 두 번째는 인증 센터에 접근 권한 획득을 위한 절차로 사용자와 인증 센터, 디바이스의 인증 과정을 진행한 후 적합한 사용자라 판단되면 접근을 허용하는 방식이다. 세 번째, 디바이스의 실시간 접근 및 제어 과정으로 사용자는 디바이스에 접속하여 적합한 사용자임을 증명받고 권한을 받아 직접적으로 제어하는 방식이다. 제안하는 프로토콜의 경우 안전한 보안 통신을 위해 디바이스와 인증 센터, 사용자간 그룹 키 방식을 적용하였다. 또한, 디바이스를 포함한 기타 IoT 디바이스 장치들이 많은 수록 인증 절차의 신뢰성이 향상 될 수 있도록 설계하였다. 따라서, IoT 장비를 다수 사용하는 현 시대를 반영하여 강력한 인증 체계를 구축하도록 하였다.

Table 1. Proposed Notation

| Notation | Meaning |
|---|---|
| Ek | Encrypt a using key k |
| Dk | Encrypt ciphertext using key k |
| R | Random Number |
| f(k) | Polynomial for secret sharing |
| SN | Serial Number |
| lj(x) | Formula for secret combinations |

### 3.1 내부 연결 프로토콜

본 논문에서는 일정 그룹을 형성한 후 키를 분배하고 내부적으로 접근 요청이 들어왔을 경우 일정 수 이상이 동의했을 때 키를 복원하여 영상을 열람할 수 있는 방법을 제안하고 있다. 키를 교환하는 과정에서는 그룹 키를 사용하며 주기적으로 그룹 키를 갱신함으로서 키에 대한 안전성도 보장 한다.

### 3.2 등록 절차

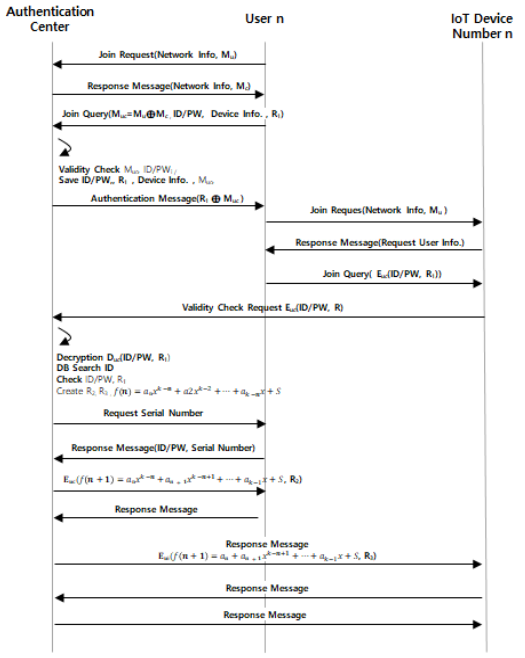


Fig. 1. Registration process

(1) 사용자는 등록 절차를 위해 인증 센터에 Join Request를 전송한다.
(2) 인증센터는 사용자에 응답메시지를 전송하며, 사용자는 ID/PW 기반의 회원 가입 절차를 진행하며, 랜덤한 값을 생성하여 함께 전송한다.
(3) 인증센터는 사용자의 가입 정보를 데이터베이스에 저장하며 마무리한다.
(4) 사용자는 원하는 디바이스의 등록을 위해 네트워크를 통해 디바이스에 접속을 요청한다.
(5) 디바이스는 사용자 정보를 요청하고, 사용자는 요청에 대한 응답으로 인증센터 등록 절차에서 생성한 ID/PW 및 랜덤 한 값을 전송한다.
(6) 디바이스에 해당하는 인증 센터에 사용자의 유효성을 확인을 위한 요청을 전송한다.
(7) 인증센터는 사용자의 적합성 판단 및 이후 인증을 위해 다항식을 전송하며, 다항식 키 분배 방법을 기술하였다.
(8) 사용자와 디바이스의 등록 절차를 마무리 한다.

### 3.3 디바이스 접근 개요

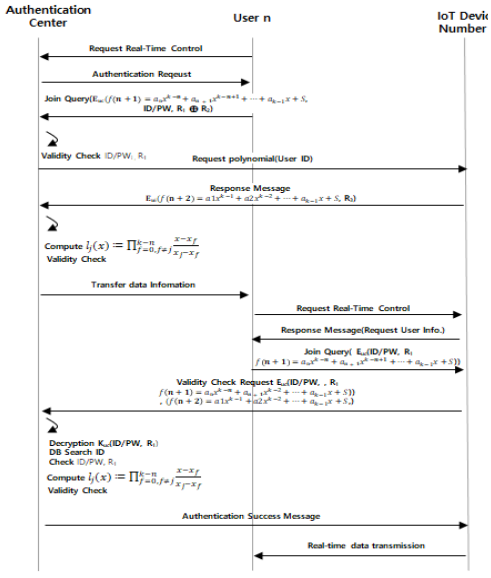


Fig. 2. Authentication process

(1) 사용자는 접근 요청 메시지를 전송 한다.
(2) 본 논문은 인증 센터의 그룹 매치에 따라 n개 이상의 디바이스 동의를 통해 권한을 획득하도록 한다.

각각의 디바이스는 사용자 요청의 적합성을 판단 후 적절하다고 판단되면 본인이 소유한 다항식 정보를 운영서버로 전송한다.

(3) 일정 수 이상의 다항식 키 값이 모이면 검증 후 접근을 허용 한다.

### 3.4 다항식 키 분배 및 전송 방법

키를 분배하는 방법은 k-1차 다항식을 이용한다. 본 논문에서는 가장 간단한 구조인 사용자, 인증센터, 디바이스 3개의 요소를 기반으로 예시를 들고 있으며, 그룹이 형성될수록 강력한 인증 체계를 가질 수 있다

(1) 관제센터는 s를 상수항으로 하는 k-1차의 다항식 f(k)를 선택한다.
(2) 관제센터는 j의 값을 정하고 f(j)를 전송한다. 본 논문은 사용자는 n, 인증센터는 n+1, IoT 디바이스

들은 n+2이상의 값으로 j 값을 지정하며 전송할 때 Predistribution and local Collaboration-based Group Rekeying[11]그룹 키 생성 방식을 통해 생성한 그룹 키를 통해 암호화를 한다.

(3) 인증센터에서 키를 전송할 때, 그룹 키로 암호화 하여 전송한다.

(4) 인증센터는 k개 이상의 분배키가 모이면 라그랑주 다항식을 이용하여 원본 키를 복원한다[12].

### 3.5 안전성 확보를 위한 키 교환

공격자가 인증센터에서 전송하는 암호문을 탈취하여 상황을 방지하기 위해서 본 논문에서는 암호화 과정에서 랜덤 값을 생성해서 사용함으로서 공격자의 중간자 공격 및 재사용 공격이 불가능 하도록 상호인증에 기반하여 설계하였다.

(1) 각 초기 전송 과정에서는 랜덤 값 R을 생성하여 암호화 후 전송을 진행 한다.

(2) 각각의 노드들은 복호화 후 R값을 획득하며, XOR 연산을 통해 키 사용에 이용한 후 인증 절차를 거친다.

(3) 노드간 난수를 위한 키 생성 및 인증 절차는 앞선 프로토콜의 다항식 기반 함수를 이용한다.

### 3.6 실시간 접근 제어

(1) 디바이스 제어를 위해 사용자는 IP 카메라에 접속을 요청하며 ID/PW 및 다항식 키 값을 그룹 키로 암호화 하여 전송한다.

(2) 디바이스는 전송 받은 로그인 정보에 대한 다항식 키 값을 관제 센터 및 보안 요구사항 정도에 따라 주변 디바이스에 요청을 한다.

(3) 다항식 키 값의 적합성이 확인되면 접근을 허가한다.

(4) 사용자가 세션을 종료하면 다항식 키 값을 폐기하며, 다항식 키 값은 일정 주기에 따라 갱신을 진행한다.

## 4. 성능 평가

### 4.1 보안성 평가

본 절에서는 보안성 평가를 위해 네트워크상에서 사용되는 잘 알려진 취약점 공격에 대한 안전성을 평가하고, 기존 연구와의 비교를 통해 우수성을 검증 하였다.

#### 4.1.1 상호 인증

본 논문에서는 인증 센터 가입을 위해 암호화 방식을 이용한 ID/PW 가입 절차를 진행한다. 이 과정에서 난수 값을 교환하며, 이는 나중에 키 및 인증 값 갱신을 위해 활용 된다. 또한 인증 센터의 경우 이후 인증 과정을 위해 다항식 f(k)를 각각 사용자와 IoT디바이스에 전송하며 초기 인증 이후에는 이 다항식 값을 가지고 검증 절차를 가짐으로서 상호 인증이 가능하다. 의 경우 이후 인증 과정을 위해 다항식 f(k)를 각각 사용자와 IoT 디바이스의 직접적인 인증 과정에서도 인증 센터가 인증 과정에 대한 제어 역할을 해 줌으로서 안전한 인증이 가능하다.

#### 4.1.2 재사용 공격

인가되지 않은 사용자가 디바이스-디바이스 및 사람-디바이스 등이 통신하는 과정에서 생성되는 메시지를 탈취하여 재사용하는 공격으로, 메시지를 탈취 하더라도 지속적인 난수 교환을 통해 이전의 전송 값이 활용되지 못하도록 인증하는 것이 가능하다. 또한, 본 논문에서는 인증 절차 과정에서 타임스탬프를 전송하도록 가정하고 있으므로, 이전 시간에 보내진 정보에 대해 검증이 가능하다.

#### 4.1.3 메시지 위변조 공격

인가되지 않은 사용자가 디바이스-디바이스 및 사람-디바이스 등이 통신하는 과정에서 생성되는 메시지를 탈취하여 공격자가 원하는 목적으로 메시지를 위·변조하는 메시지를 전송하는 방식의 공격으로, 데이터 전송 과정에서 암호화 키를 통해 암호문을 생성한 후 전송하고 있어, 공격자가 키를 탈취하지 않는 한 메시지 위변조 공격에 대해 안전성을 가지고 있다.

#### 4.1.4 스니핑

네트워크 상에 전송되는 메시지를 엿보는 공격 방법중 하나로서, 통신 과정에서 발생하는 메시지들에 대해 비밀키를 이용하여 암호화하고 있으며, 또한 지속적으로 키를 갱신함으로서 스니핑을 통한 메시지 엿보기를 시도하더라도 암호화된 메시지만을 볼 수 있기 때문에 해당 공격에 안전성을 가진다.

#### 4.1.5 스푸핑

네트워크상에서 사용자 및 디바이스의 식별 정보들을 인가된 사용자처럼 위장하여 상대방을 속이는 공격 방식으로, 이미 사전 통신 과정에서 인증 절차를 진행하며, 스푸핑 공격을 받더라도 초기 인증 절차에서 공유하고 있는 각 노드 간 비밀 값을 알지 못하기 때문에 해당 공격에 대하여 안전성을 가진다.

Table 2. Security Analysis

| | Wu | porambage | Li | Proposed |
|---|---|---|---|---|
| Mutual Authentication | X | O | O | O |
| Replay Attack | X | O | X | O |
| data integrity | O | X | X | O |
| Man in the Middle Attack | X | O | X | O |
| Sniffing & spoofing | O | O | O | O |

### 4.2 안전성 비교 분석

기존의 IoT 환경에서 제안된 보안 프로토콜과의 비교를 위해 네트워크 공격에 대한 안전성 여부를 Table 2를 통해 정리하였다. 분석 결과 먼저 Wu 프로토콜의 경우 각각 IoT 디바이스간의 상호 인증 및 재사용 공격, 중간자 공격 등에 취약점을 가지고 있으며, Li 프로토콜의 경우 재사용 공격과 데이터 무결성, 중간자 공격에 취약점을 가지고 있었다. 또한 Proamb 프로토콜의 경우 데이터 무결성 측면에서 위험성을 가지고 있었으며, 보안 통신에서 활용되는 세션키에 대한 위험에도 노출되어 있었다. 본 논문의 경우 잘 알려진 취약점에 대한 보안성을 4.1 보안성 평가를 통해 안전성을 가지고 있음을 확인하였다.

### 4.3 에너지 효율성

제안하는 프로토콜의 인증 및 재인증 과정에서 연산속도에 대한 성능평가를 기존 환경에서 활용되는 잘 알려진 암호화 알고리즘과 함께 비교 분석하여 Table 3, Table4 에 정의하였다. 제안하는 프로토콜은 적은 수의 디바이스 상황에서는 기존 알고리즘과 큰 차이가 없지만, 디바이스 수의 증가에 따라 그룹 키 활용에 따른 효율성이 증대됨을 확인할 수 있었다. 특히, 초기 인증의 경우 기존에 빠르다고 알려진 ECC 알고리즘과 거의 차이가 없지만, 재인증 과정에서는 그룹 키 활용을 통해 수치적으로 큰 차이를 나타내고 있다. 이는 디바이스의 수가 기하급수적으로 늘어나는 IoT 환경에서 적합할 것으로 기대 된다.

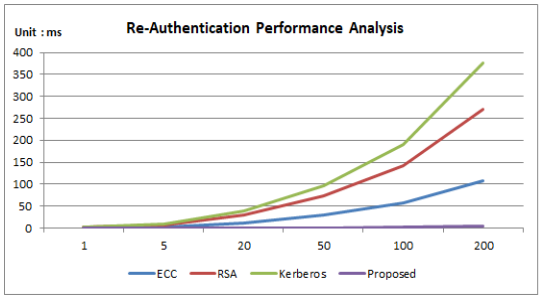


Fig. 3. Re-Authentication Performance

Table 3. Performance Analysis

| Number of Device | ECC | RSA | Kerberos | Proposed |
|---|---|---|---|---|
| 1 | 0.62321 | 1.54231 | 1.41233 | 0.56013 |
| 5 | 2.99140 | 7.573513 | 6.86393 | 2.80066 |
| 20 | 11.2177 | 29.74191 | 26.8625 | 11.2026 |
| 50 | 27.1813 | 71.79453 | 64.9672 | 25.0066 |
| 100 | 53.1037 | 142.201 | 124.129 | 50.0132 |
| 200 | 102.331 | 274.9106 | 234.729 | 98.0264 |

Table 4. Re-Authentication Performance Analysis

| Number of Device | ECC | RSA | Kerberos | Proposed |
|---|---|---|---|---|
| 1 | 0.62321 | 1.54231 | 2.01233 | 0.0232 |
| 5 | 2.99764 | 7.6113 | 9.93085 | 0.10672 |
| 20 | 11.7562 | 29.67404 | 39.0794 | 0.42363 |
| 50 | 28.7112 | 72.56569 | 96.8937 | 1.05676 |
| 100 | 56.7744 | 142.0468 | 189.360 | 2.05784 |
| 200 | 107.690 | 271.826 | 375.098 | 4.01824 |

## 5. 결론

기술의 발전에 따라서 현재 대부분이 일상생활에서 쉽게 스마트 디바이스를 접할 수 있다. 인터넷 기술과 하드웨어 기술의 발전은 사람들에게 수많은 편의를 제공해주고 있지만, 안타깝게도 이와 동시에 수많은 보안 위협 사례들이 발생하고 있는 상황이다. 기존 PC환경에서 활용되던 악성코드나 해킹의 방법들이 대상을 확대하여

IoT 디바이스들에 번번히 시도되고 있으며, 수많은 피해를 야기시켰지만, IoT디바이스들이 가지고 있는 성능 및 메모리, 파워 등의 한계로 인해 기존 PC환경의 보안 프로토콜을 적용하는데 어려움을 가지고 있다. 따라서, 본 논문은 IoT환경이 가지는 특성을 고려하여 보안 프로토콜을 설계하였으며, 성능평가를 통해 보안성 및 퍼포먼스의 적합성을 확인하였다. 그러므로, 제안하는 프로토콜을 적용한다면 미래 인터넷 환경에서 효율적인 보안 시스템 제공이 가능할 것으로 기대 된다.

## References


[1] KOLIAS, Constantinos, et al. DDoS in the IoT: Mirai and other botnets. Computer, 2017, 50.7: 80-84.
DOI : https://doi.org/10.1109/mc.2017.201

[2] YANG, Yuchen, et al. A survey on security and privacy issues in internet-of-things. IEEE Internet of Things Journal, 2017, 4.5: 1250-1258.
DOI : https://doi.org/10.1109/jiot.2017.2694844

[3] FRUSTACI, Mario, et al. Evaluating critical security issues of the IoT world: Present and future challenges. IEEE Internet of Things Journal, 2017, 5.4: 2483-2495.
DOI : https://doi.org/10.1109/jiot.2017.2767291

[4] KHAN, Minhaj Ahmad; SALAH, Khaled. IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 2018, 82: 395-411.
DOI : https://doi.org/10.1016/j.future.2017.11.022

[5] BKAMBLE, Ashvini; BHUTAD, Sonali. Survey on Internet of Things (IoT) security issues & solutions. In: 2018 2nd International Conference on Inventive Systems and Control (ICISC). IEEE, 2018. pp. 307-312.
DOI : https://doi.org/10.1109/icisc.2018.8399084

[6] SAMIE, Farzad; BAUER, Lars; HENKEL, Jörg. IoT technologies for embedded computing: A survey. In: Proceedings of the Eleventh IEEE/ACM/IFIP International Conference on Hardware/Software Codesign and System Synthesis. ACM, 2016. p. 8.
DOI : https://doi.org/10.1145/2968456.2974004

[7] SAHA, Himadri Nath; MANDAL, Abhilasha; SINHA, Abhirup. Recent trends in the Internet of Things. In: 2017 IEEE 7th annual computing and communication workshop and conference (CCWC). IEEE, 2017. pp. 1-4.

[8] SØHOEL, Halldis; JAATUN, Martin Gilje; BOYD, Colin. OWASP Top 10-Do Startups Care?. In: 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security). IEEE, 2018. pp. 1-8.
DOI : https://doi.org/10.1109/cybersecpods.2018.8560666

[9] RAY, Partha Pratim. Internet of things for smart agriculture: Technologies, practices and future direction. Journal of Ambient Intelligence and Smart Environments, 2017, 9.4: 395-420.
DOI : https://doi.org/10.3233/ais-170440

[10] PONTA, Serena Elisa; PLATE, Henrik; SABETTA, Antonino. Beyond metadata: Code-centric and usage-based analysis of known vulnerabilities in open-source software. In: 2018 IEEE International Conference on Software Maintenance and Evolution (ICSME). IEEE, 2018. pp. 449-460.
DOI : https://doi.org/10.1109/icsme.2018.00054

[11] ZHANG, Wensheng; ZHU, Sencun; CAO, Guohong. Predistribution and local collaboration-based group rekeying for wireless sensor networks. Ad hoc networks, 2009, 7.6: 1229-1242.
DOI : https://doi.org/10.1016/j.adhoc.2008.11.004

[12] FELDMAN, Paul. A practical scheme for non-interactive verifiable secret sharing. In: 28th Annual Symposium on Foundations of Computer Science (sfcs 1987). IEEE, 1987. pp. 427-438.
DOI : https://doi.org/10.1109/sfcs.1987.4



민 소 연(So-Yeon Min) [종신회원]

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

〈관심분야〉
통신 및 신호처리, 임베디드 시스템

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