Journal of the Korea Academia-Industrial cooperation Society
Vol. 21, No. 10 pp. 602-608, 2020

https://doi.org/10.5762/KAIS.2020.21.10.602
ISSN 1975-4701 / eISSN 2288-4688

IoT 환경에서 IP카메라의 효율적 운용을 위한 키 관리 및 보안 설계 프로토콜

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

Authentication and Key Management Techniques for Secure Communication in IP Camera

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

요 약 인터넷의 기술의 발전과 다양한 스마트 기기의 보급은 많은 사람들에게 편리성을 제공해 주며, 이는 IoT라는 이름의 기술로 보편화 되고 있다. 그러나 이러한 상황을 악용하는 해커들의 공격으로 인해 개인 정보 유출이나 사생활 침해를 받는 등의 다양한 문제를 야기 시키고 있다. IoT 환경에서는 다양한 스마트 디바이스들이 네트워크에 연결되고 있으며, 이로 인해 기존 PC 환경에서 악용되던 네트워크 공격이 IoT 환경에서 빈번하게 발생하고 있다. 실제로 IoT 디바이스인 IP 카메라에 불법적인 접근을 통해 DDoS 공격을 시도하거나, 개인정보 유출, 동의 없는 모니터링 등의 보안 사고가 발생하고 있다. 기존 인터넷 환경에서의 공격이 PC 위주였다면, 이제는 IP카메라나 태블릿 등의 스마트 기기들이 네트워크 공격에 활용될 수 있음을 확인할 수 있었다. 이러한 IoT환경에서 발생할 수 있는 문제를 방지하기 위해 디바이스들에 대한 보안 솔루션 적용을 해야 하지만 PC와 다르게 메모리나 파워 등이 제한되어 있어 기존에 사용하던 보안 솔루션 설치 및 실행에 어려움을 가지고 있다. 따라서 본 논문에서는 IoT 환경에서 IP 카메라의 특징 및 보안 위협들에 대해 살펴보고 이를 방지할 수 있는 보안 프로토콜을 제안한다. 제안하는 프로토콜은 성능평가를 통해 RSA 보다 서버 기준 11%, Kerberos 보다 클라이언트 기준 8배 이상 에너지 효율성을 보였으며, 디바이스의 개수가 늘어남에 따라 효율이 높아짐을 확인하였다. 또한, 네트워크에서 발생할 수 있는 다양한 보안 위협에 대응 가능함을 확인할 수 있어 IoT 환경에 적용한다면 효율적인 운영이 가능할 것으로 기대 된다.

Abstract Development of Internet technology and the spread of various smart devices provide a convenient computing environment for people, which is becoming common thanks to the Internet of Things (IoT). However, attacks by hackers have caused various problems, such as leaking personal information or violating privacy. In the IoT environment, various smart devices are connected, and network attacks that are used in the PC environment are occurring frequently in the IoT. In fact, security incidents such as conducting DDoS attacks by hacking IP cameras, leaking personal information, and monitoring unspecified numbers of personal files without consent are occurring. Although attacks in the existing Internet environment are PC-oriented, we can now confirm that smart devices such as IP cameras and tablets can be targets of network attacks. Through performance evaluation, the proposed protocol shows 11% more energy efficiency on servers than RSA, eight times greater energy efficiency on clients than Kerberos, and increased efficiency as the number of devices increases. In addition, it is possible to respond to a variety of security threats that might occur against the network. It is expected that efficient operations will be possible if the proposed protocol is applied to the IoT environment.

Keywords : IoT Authentication, IoT Security, IP Camera Security, Key management, Home Network

본 논문은 2020년도 서일대학교 학술지원비에 의해 연구되었음
*Corresponding Author : So-Yeon Min(Seoil Univ.)
email: symin@seoil.ac.kr
Received August 12, 2020 Revised September 1, 2020
Accepted October 5, 2020 Published October 31, 2020

1. 서론

최근 인터넷의 기술의 발전과 보급률이 높아짐에 따라 인터넷 환경은 인간과 밀접한 관계를 가지고 있으며, 이는 IoT(Internet of Things) 기술로 보편화 되고 있다. 그러나 이러한 IoT 기술의 발전과 수요가 증가함에 따라, 이를 악용한 보안 위협이 증가하여 다양한 보안 사고들이 발생하고 있다. IoT 의미에서 알 수 있듯이 다양한 디바이스들이 네트워크에 연결되어 네트워크를 활용한 보안 공격이 다양하게 발생하고 있으며, IoT 환경에서 PC, Server, Network 에 적용했던 기존의 백신, 방화벽과 같은 보안 솔루션이 IoT에 적용하기에 한계성을 지님에 따라, IoT 환경에 맞는 디바이스 보안의 필요성이 대두 되고 있는 상황이다.

보안 사고의 사례로 인터넷 도메인 서비스 업체 인 딘(Dyn)에 대규모 디도스 공격에 수많은 IoT 기기가 감염되어 활용된 것이 대표적인 사례이며, 이러한 DDoS 공격으로 인해 유명 웹 사이트인 뉴욕타임즈, 트위터, 넷플릭스, 아마존 등 수십 개의 웹 사이트가 몇 시간 동안 접속이 불가능 사태가 발생하였다. 디도스 공격의 경우 새로운 공격이 아니라 기존의 PC 환경에서 자주 악용되던 공격 중 하나로서, 이전 까지 PC를 감염시켜 공격을 하는 방식 이었는데, 이러한 공격 사례를 통해 일상생활에서 사용하고 있는 DVR, 태블릿, CCTV(Closed Circuit TeleVision)등 IoT 환경에서 활용되는 다양한 스마트 기기가 네트워크 공격에 활용될 수 있음을 확인할 수 있었다.

또한, 인터넷 익스플로러에 연결된 IoT 디바이스가 해킹되어 공격에 활용되고 있다. 이에 대한 최신 사례는 보안 전문업체 임페르바가 발견하였는데, 탐지된 공격의 경우 기존 PC 인터넷 환경에서 공격에 사용된 전통적인 HTTP 결함공격으로, 클라우드 서비스상 자원을 과부하 주는 것을 목표로 설정 하였다[1,2].

하지만 이번 공격에서 주목해야 할 점은 기존에 전통적으로 사용된 컴퓨터 봇넷이 아닌 IP카메라에서 나왔으며, 최대 초당 2만 개의 요청을 만들어서 약 900대의 CCTV 카메라를 활용한 공격이었다고 임페르바는 설명하였다. 기존의 환경에서 공격을 위해 컴퓨터를 감염시키기 위한 방법으로 소프트웨어 상의 취약점이나 소셜 엔지니어링 등의 방법을 이용했지만, 이번 공격은 Telnet, SS를 통하여 인터넷으로 액세스가 가능하여 쉽게 공격할 수 있는 환경 이였다. 또한, IoT 디바이스들을 공격하기 위해 ID와 Password 조합에 각각root, admin과 admin, Password를 가장 많이 사용 했으며, 이는 제품 출시 기본 설정된 값들을 변경하지 않는 점을 악용하는 공격에 활용할 수 있었다. 이렇게 IoT 환경에서 발생할 수 있는 문제를 방지하기 위해 디바이스들에 대한 보안 솔루션 적용을 해야 하지만 녹록치 않은 상황[3]이며, PC와 다르게 메모리나 파워 등이 제한되어 있어 기존 PC환경의 보안 솔루션 설치 및 실행에 어려움을 가지고 있다. 따라서 본 논문에서는 IoT 환경에서 위 사례에 활용된 IP 카메라의 동향 및 보안 문제에 대해 살펴보고, NVR 네트워크 보안 설계 시스템 구성을 통한 안전한 통신 방법에 대해 제안 한다.

2. 관련 연구

2.1 IP 카메라 동향

기존 CCTV 시스템의 경우 보안의 목적으로나 Closed Circuit TeleVision이 가지는 의미 그대로 폐쇄적인 구성을 가지며, 따라서, 주로 특정 지역에 카메라들을 설치하여 정해진 장소에서 영상을 감시하고 필요에 따라 저장 및 검색하는 구성이 보편적이었다. 반면 IT 기술의 발전에 따라 IP 카메라가 등장하였고, 이 디바이스는 네트워크에 기반하여 영상을 전송하는 개념을 활용함으로서 기존CCTV와 반대로 개방적이며 확장성이나 유연성 측면에서 강점을 가지고 있다.

또한, 네트워크 연결을 통해, 인터넷을 기반으로 사용할 수 있으므로 인터넷만 가능하다면 언제 어디서든 활용 가능하다는 큰 특징을 가지고 있다. 이러한 특징은 현 시대에 Network의 구성은 저렴하고 간편하며 또한 대부분의 장소에 네트워크 설치구성이 되어 있는 경우가 많아 추가 비용 없이 일상생활에 적용하는데 어려움이 없다는 장점을 가지고 있다.

기존 아날로그 CCTV에서는 비디오만 카메라가 보냈던 반면에, IP 카메라의 경우 영상과 함께 음성을 압축하여 전송이 가능하며, 대부분의 IP카메라가 음성 녹음 및 전송을 지원하고 있다. 이는 기존의 CCTV의 역할이 단순 영상감시에서 상호 커뮤니케이션 기능으로 확장 하는 것이 가능해졌으며, 음성을 통해 보안감시 목적의 활용도 가능하다[4,5].

간단하게 현재 출시되고 있는 IP 카메라의 종류를 살펴보면, CCTV에서 IP 카메라로 넘어오는 등장 초기에는 용어가 확립되지 않아 Web 카메라, Network 카메라, IP 카메라 등이 혼용되어 사용되었지만, 이후에는 이름

에 의미의 구분을 두고 불리고 있다. 제안하는 논문에서 대상 디바이스는 네트워크에 연결되어 실시간 영상 제어가 가능한 카메라 제품을 의미한다.

2.2 IP 카메라 보안 사례

IP 카메라 시장의 증가는 테러 및 범지 방지, 재난 및 재해에 대한 모니터링 등의 긍정적인 요소만 존재하는 것은 아니다. 지난 몇 년간 IP 카메라에 대한 악의적인 공격으로 수많은 문제가 발생하였다. 먼저, 오스트리아의 보안 연구 결과에 따르면, 약 80개 이상의 소니사의 카메라에서 백도어를 발견하였으며, 이스라엘에서도 같은 기종 내 IP 카메라 모델에서 취약점을 발견했다[6].

또한, 오스트리아의 보안 회사에서는 소니의 IPELA Engine IP 카메라에서 서로 다른 두 가지 백도어를 찾았으며, Telnet을 통해서 'primana'와 'debug'의 원격 조정을 할 수 있다고 밝혔다. 사용자들은 취약점에 대응하기 위해 펌웨어를 업데이트하고 있지만, 원천적인 해결방안이 필요한 상황이다.

Cybereason사가 eBay나 Amazon을 통해서 구매한 12종류의 IP 카메라의 모든 패스워드가 '888888'이었고, 이로 인하여 방화벽에서의 방어가 힘들었으며, 카메라를 만든 회사에서는 이러한 취약점에 대응 가능한 펌웨어 업데이트 및 패치를 하지 않았다.
SWANN 사의 카메라에서도 보안 취약점이 발견되었는데, 흔히 무료로 사용가능한 보안 툴을 통해 SWANN 카메라 앱으로 전송되는 메시지를 탈취 하는게 가능했다. 탈취 가능한 메시지에는 각각의 카메라가 공장에서 부여받는 제조번호도 포함되어 있었으며, 이 제조번호를 통해 유럽의 보안 컨설턴트 다섯 명의 연구진은 다른 카메라에서 나오는 영상을 획득할 수 있었다. 이 과정에서 다른 사용자 아이디 및 패스워드를 입력할 필요는 없었다. 또한, 스완의 카메라가 사용하고 있는 제조번호를 확인하는 방법도 발견했다. 이론적으로는 어떠한 계정의 영상이든 빠르게 훔쳐볼 수 있게 되는 것이며, 이는 개인영상정보의 유출이라는 큰 문제를 야기 시키고 있다.

IP 카메라를 이용한 DDoS 공격을 시도한 사례들도 존재 한다. 지난 2016년 10월 21일에는 DNS 서비스를 제공하는 Dyn이 대규모 DDoS 공격을 받아 뉴욕타임즈, 트위터, 넷플릭스 등의 유명 사이트를 포함하여 총 76개의 사이트의 서비스가 지연되거나 마비되는 사건이 발생했다.

DDoS 공격 원인으로는 출시 당시의 IoT기기(공장에서 출하할 당시에 기본 ID/PW가 설정된 채 방치된 기기)가 미라이(Mirai) 악성코드에 감염됨으로서 해커의 명령을 통해 DDoS 공격을 시도한 것으로 확인되었다. 수많은 IoT 디바이스들이 공장 출하 상태에서 취약한 ID/PW를 유지한 채 온라인에 연결되어 있으며, 이는 공격에 쉽게 노출될 수 있다. 이러한 점을 악용하여 디바이스의 악성코드 감염시도가 매년 증가하고 있으며, 이에 대한 보안대책 마련이 시급한 상황이다.

앞에서 이야기한 대규모 DDoS 공격에 사용된 Mirai 악성코드의 경우 Source Code가 누구나 쉽게 접근 가능하도록 공개되어 있으며, 따라서, 사용자들은 이 소스코드 수정함으로서 변종 악성코드 제작이 가능한 상황이다.

IoT 장비는 제조사마다 다양한 CPU를 사용하고 있으며, CPU 환경에 맞춰서 적합한 운영체제 리눅스를 적용하고 있다. 리눅스의 경우 크로스 컴파일로 다양한 CPU 환경에서도 실행이 가능 하며, 이 때문에 거의 대부분의 IoT 기기들이 공격의 대상이 된다. 실제 발견된 악성코드를 살펴보면 거의 기능은 동일하지만 ARM, MIPS, PowerPC 등 다양한 환경에서 실행 가능하도록 만들어진 것을 확인할 수 있다[7,8].

3. 제안 내용

본 장에서는 앞서 살펴본 보안 위협에 대응하고 효율적인 IP 카메라 운용이 가능한 관제센터 설계 방안을 제안 한다. 앞서 설명한 NVR 시스템에 결합한 IP 카메라의 경우 네트워크에 연결됨에 따라 네트워크에서 발생할 수 있는 다양한 보안위협 - 사용자 인증과 접근 보안 등에 취약하다. 본 논문에서 IP 카메라 사용자 및 관제센터 입장에서 사용자 정보와 랜덤 난수, 실시간 요청 값, 검증 값 등을 활용 하여 안전한 인증 프로토콜을 제안한다.

본 논문에서는 먼저 사용자가 IP 카메라를 등록하는 과정으로 IP 카메라 활용을 위해 관제 센터에 사용자 등록을 위한 ID/PW 기반 등록 절차를 진행하며, 이 과정에서 랜덤 난수와 사용자 인증 정보를 통해 이후 인증 과정에서 활용하게 될 bit stream 검증과정을 거친다. 다음으로 관제 센터에 저장된 영상의 열람을 위한 절차로 사용자와 관제 센터, IP 카메라의 인증 과정을 진행한 후 적합한 사용자라 판단되면 열람을 허용한다. 마지막으로 IP 카메라의 실시간 모니터링 과정으로 사용자는 IP 카메라에 접속하여 적합한 사용자임을 증명 받고 영상을 실시간으로 전송받는 방식으로 진행된다.

Table 1. Proposed Notation

Notation	Meaning
R	Random Number
f(k)	Polynomial for secret sharing
SN	Serial Number
v^i, v^j	Verify Value

3.1 등록 절차

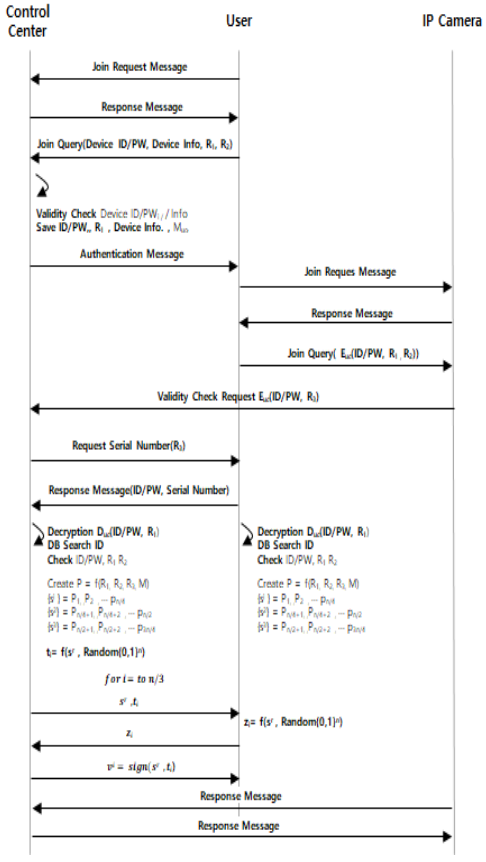

Fig. 1. Registration process

(1) 사용자는 등록 절차를 위해 관제 센터에 Join Request를 전송한다.
(2) 관제센터는 요청에 대한 응답을 사용자에게 전송하며, 사용자는 ID/PW 기반의 회원 가입 절차를 진행하며, 랜덤 난수를 생성하여 함께 전송한다.
(3) 관제센터는 사용자의 가입 정보를 데이터베이스에 저장한다.
(4) 사용자는 원하는 IP카메라의 등록을 위해 네트워크를 통해 IP 카메라에 접속을 요청한다.
(5) IP 카메라는 사용자의 요청이 들어왔을 때, 해당 사용자에 대한 정보를 관제센터에 요청하고, 사용자는 요청에 대한 응답으로 관제센터 등록 절차에서 생성한 ID/PW 및 랜덤한 값을 전송한다.
(6) IP 카메라는 제품에 해당하는 관제 센터에 사용자의 유효성을 확인을 위한 요청을 전송한다.
(7) 관제센터는 사용자의 적합성 판단(해당 IP 카메라의 시리얼 넘버는 사용자에게 요청하고 그에 대한 응답을 받는 과정) 한다.
(8) 사용자와 관제센터는 함수와 난수를 통해 3n bits의stream을 생성하며 이는 각각 s^1, s^2, s^3로 나뉜다. 이후 Challenge/Response 과정을 통해 검증된 v^i bit stream을 생성하며, 이는 추후 인증 과정에 활용된다.
(9) 사용자와 IP카메라의 등록 절차를 마무리 한다.

3.2 디바이스 접근 개요

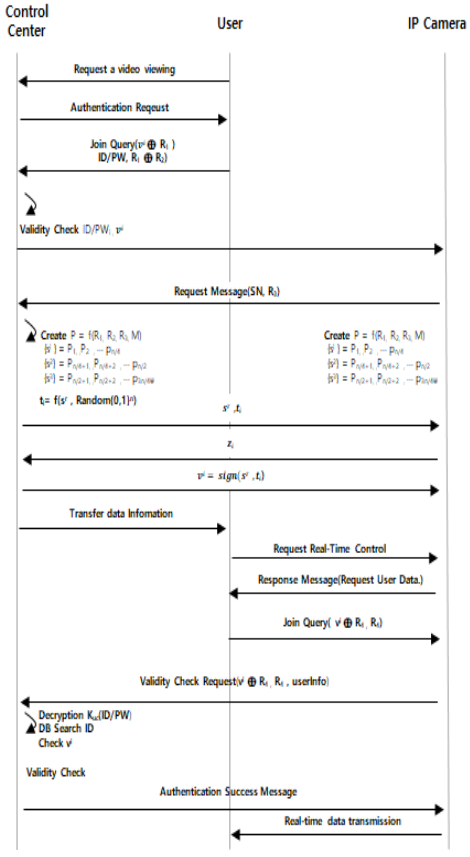

Fig. 2. Authentication process

(1) 사용자는 디바이스에 접근이 필요할 경우 접근 요청을 한다.

(2) 관제센터에서 응답이 오면 사용자는 검증된 v^i값가 랜덤 난수를 XOR 하여 랜덤 난수와 함께 전송한다.

(3) 관제센터는 ID/PW 와 매칭되는 검증된 v^i값을 확인하고 디바이스에 해당 유저에 대한 접근 요청 메시지를 전송한다.

(4) 첫 인증 과정이라면, 3.1의 유저와 관제센터의 인증 과정과 동일한 절차로 검증 값 v^j를 생성하고 추후 인증과정에서는 v^j를 통해 인증절차를 간소화 한다.

4. 성능 평가

4.1 보안성 평가

본 장에서는 제안하는 프로토콜의 보안성과 성능에 대해 비교 분석 한다. 제안하는 프로토콜의 사용자-센터-카메라 인증 시 발생할 수 있는 잘 알려진 취약점과 OneM2M 표준에서 정의된 디바이스의 보안 요구사항을 기준으로 분석하였다.

4.1.1 Authentication

본 논문에서는 관제센터 초기 등록을 위해 암호화 방식을 이용한 가입 절차를 진행한다. 이 과정에서 랜덤 난수를 교환하며, 이는 나중에 키 재생성 및 인증 절차에 활용된다. 또한 인증 센터의 경우 이후 인증 과정을 위해 검증 값 v^i, v^j를 활용하며, 초기 인증 이후에는 이 검증 값과 난수를 통해 검증 절차를 가짐으로서 상호 인증이 가능하다. 이후 인증 과정을 사용자와 - IP 카메라 인증 과정에서도 인증 센터가 인증 과정에 대한 제어 역할을 함으로서 안전한 인증이 가능하다.

4.1.2 Replay attack and Relay attack

공격자가 통신과정에서 생성 및 전송하는 정보를 탈취하여 재사용하는 공격으로, 중간에 정보를 가로채더라도 지속적인 난수 교환과 검증 값 v^i, v^j를 통해 이전의 전송 값이 활용되지 못하도록 인증하는 것이 가능하다. 또한, 본 논문에서 제안하는 프로토콜은 기본적으로 타임스탬프를 보냄을 전재하고 있다, 따라서 특정 시간이 지난 메시지들에 대한 검증이 가능하다.

4.1.3 Message Forgery Attack

공격자가 통신과정에서 생성 및 전송하는 메시지를 탈취하여 특정 목적을 위한 메시지의 위·변조하는 행위를 의미하며, 데이터는 기본적으로 암호화 되고 있어, 공격자가 키를 탈취하지 않는 한 메시지 위변조 공격에 대해 안전성을 가지고 있다.

4.1.4 Sniffing

통신과정에서 생성 및 전송되는 메시지를 엿보는 공격으로, 통신 과정에서 발생하는 메시지들은 기본적으로 비밀 키를 통해 암호화 하고 있으며, 지속적으로 키 갱신을 통해 안전성을 유지한다. 스니핑을 통한 메시지 엿보기를 시도하더라도 키가 없는 이상 복호화가 불가능하기 때문에 해당 공격에 안전성을 가진다.

4.1.5 Spoofing

통신과정에서 사용자 및 디바이스의 식별 정보들을 인증된 사용자처럼 위장하여 속이는 방식으로, 제안하는 프로토콜의 경우 초기 등록 과정에서 인증 절차를 진행하며, 스푸핑 공격을 받더라도 초기 등록 과정에서 공유하고 있는 사용자와 디바이스의 공유 값을 알지 못하기 때문에 해당 공격에 대하여 안전성을 가진다.

4.2 에너지 효율성

성능 분석을 위해서 IP 카메라의 수를 10개부터 100개 사이로 순차적으로 설정하였으며. 디바이스의 배치는 50m×50m 지역에 랜덤 하게 분포하였다. Control Center는 배치 영역을 고려하여 특정 위치에 지정하였다. 배치에 따라 모든 IoT 디바이스들과 Control Center는 40m 내에 존재하도록 한다. 디바이스의 랜덤 분포에 상관없이 효율성을 가지는지 판단하기 위해, 같은 조건으로 30번 이상 테스트를 진행하였으며, 아래의 도표는 평균값에 대한 결과이며, 자세한 테스트 환경은 Table 2와 같다.

제안하는 프로토콜에서는 에너지 효율성을 위해 클라이언트(IP 카메라)의 경우 단순 해시 연산 정도만을 진행하도록 하였으며, 암·복호화나 다항식의 연산 등은 Control Center에서 계산이 집중 되도록 인증 프로토콜을 제안하였다. 이러한 점은 단순 IP Camera뿐만 아니라 기존 IoT 및 스마트 홈 환경에서 경량화 보안 기술 방

안들이 가지는 한계점인 이기종 IoT 환경에서 암호화 모듈을 탑재하지 못하는 초경량 장치들에 대해 모두 활용 가능할 것으로 기대 된다.

성능분석을 통해 제안하는 인증 프레임워크는 클라이언트 측면에서 이전에 잘 알려진 보안 인증기술보다 경량화 되었음을 확인할 수 있었으며, 디바이스 측면에서도 적은 에너지 소모로 기존의 인증기술보다 보안성 및 에너지 효율성 측면에서 크게 향상됨을 확인할 수 있다.

Table 2. Simulation Initial Settings

Simulation Initial Settings	
Number of Device	10~50
Placement Area	50m*50
Control Center Location	X=30m, y=30
ETX, ERX	40 nanoJ
Packet Size	5000 bit

Table 3. Performance Analysis(Server, Unit : ms)

Number of Device	ECC	RSA	Kerberos	Proposed
10	66.8321	111.7614	0.37141	91.4791
30	202.184	329.2248	1.00873	282.116
50	332.132	556.804	1.65175	431.395
80	529.412	880.0219	2.81265	703.328
100	649.341	1118.414	3.5149	876.281

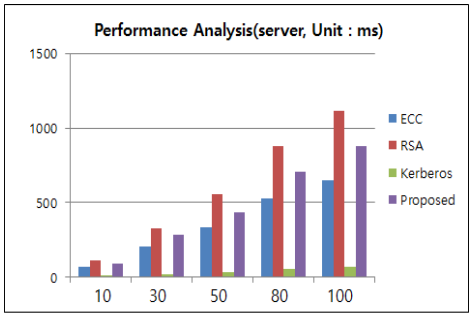

Fig. 3. Performance Analysis(server)

Table 4. Performance Analysis(Client, Unit : ms)

Number of Device	ECC	RSA	Kerberos	Proposed
10	47.9416	95.41287	4.33601	0.34571
30	142.455	288.1291	12.1876	1.01214
50	243.767	462.2417	21.1987	1.6841
80	392.663	768.2161	34.6871	2.7317
100	481.617	957.6178	43.2097	3.5622

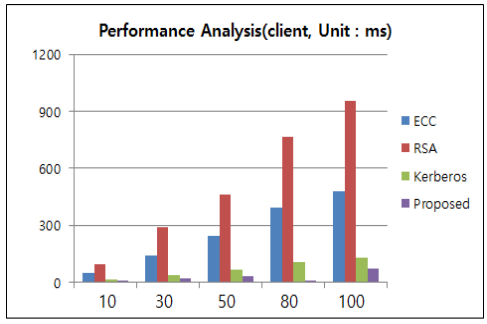

Fig. 4. Performance Analysis(client)

5. 결론

기술의 발전으로 누구나 쉽게 스마트 기기를 활용할 수 있으며, 이는 많은 사람들에게 편의를 제공해 주고 있다, 하지만 이러한 부분을 악용하는 수많은 보안 위협 사례들이 발생하고 있는 상황이다. 기존에 컴퓨터 환경을 대상으로 만든 악성코드나 해킹의 방법들이 이제는 스마트 기기를 대상으로 시도하고 있으며, 현재에도 수많은 피해를 발생시키지만, 스마트 기기들이 가지고 있는 성능 및 메모리, 파워 등의 한계로 인해 기존 컴퓨터 환경의 보안 프로토콜을 그대로 적용하기에는 어려움 있다. 따라서, 본 논문에서는 스마트 기기가 가지는 특성을 고려하여 보안 프로토콜을 설계하였으며, 성능평가를 통해 RSA보다 서버 기준 11%, Kerberos 보다 클라이언트 기준 8배 이상의 에너지 효율성을 확인하였으며, 추후 IoT환경에 적용 가능할 것으로 기대된다.

References

[1] TEKEOGLU, Ali; TOSUN, Ali Saman. Investigating security and privacy of a cloud-based wireless IP camera: NetCam. In: 2015 24th International Conference on Computer Communication and Networks (ICCCN). IEEE, 2015. pp. 1-6.
DOI : https://doi.org/10.1109/icccn.2015.7288421

[2] SINGH, Sneha, et al. IP camera video surveillance using Raspberry Pi. International Journal of Advanced Research in Computer and Communication Engineering, 2015, 4.2: 326-328.
DOI : https://doi.org/10.17148/ijarcce.2015.4272

[3] SUMAN, M. Chaitanya; PRATHYUSHA, K. Wireless camera based online examination security. International Journal of Engineering Research and

Applications (IJERA) Vol, 2012, 2: 1432-1435.

[4] KAPUR, Shyam. Systems and methods for search query processing using trend analysis. U.S. Patent No 7,562,076, 2009.

[5] POPOVIC, Gradimirka, et al. Overview, characteristics and advantages of IP Camera video surveillance systems compared to systems with other kinds of camera. Int. J. Eng. Sci. Innov. Technol, 2013, 2.5: 356-362.

[6] 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

[7] HWA, Kuo Yuan, et al. A GHS-based intelligent management platform with IP-camera security system. Wireless Personal Communications, 2011, 56.1: 85-96.
DOI : https://doi.org/10.1007/s11277-009-9877-y

[8] SERALATHAN, Yogeesh, et al. IoT security vulnerability: A case study of a Web camera. In: 2018 20th International Conference on Advanced Communication Technology (ICACT). IEEE, 2018. pp. 172-177.
DOI : https://doi.org/10.23919/icact.2018.8323686

민 소 연(So-Yeon Min) [종신회원]

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

〈관심분야〉
통신 및 신호처리, 정보통신, 임베디드 시스템

이 재 승(Jae-Seung Lee) [정회원]

- 2013년 2월 : 평생교육진흥원 컴퓨터학과(공학사)
- 2015년 2월 : 숭실대학교 컴퓨터학과(공학석사)
- 2015년 3월 : 숭실대학교 컴퓨터학과 박사수료
- (주)IOSYS 연구소 연구원

〈관심분야〉
시큐어코딩, Sensor Network, IoT Security