Journal of the Korea Academia-Industrial cooperation Society
Vol. 20, No. 5 pp. 550-558, 2019

https://doi.org/10.5762/KAIS.2019.20.5.550
ISSN 1975-4701 / eISSN 2288-4688

스마트 홈 환경에서 C-PBFT 기반의 디바이스 인증 프로토콜 설계

김정호, 허재욱, 전문석*
숭실대학교 컴퓨터학과

Design of Device Authentication Protocol Based on C-PBFT in a Smart Home Environment

Jeong-Ho Kim, Jae-Wook Heo, Moon-Seog Jun*
Dept. of Computer Science and Engineering, Soongsil University

요 약 사물인터넷 환경에 대한 규모가 날이 갈수록 커지고 발전함에 따라서 사물인터넷 디바이스를 통해 수집하고 공유되는 정보들은 점점 다양해지고 더 많아지게 되었다. 하지만 사물인터넷 디바이스들은 소형화된 크기에 따라 연산능력의 한계점과 낮은 전력량을 가지고 있어 이전의 인터넷 환경에서 적용되어왔던 암호화, 인증 등의 보안 기술들을 사물인터넷에 직접적으로 적용하기 힘들어 취약점과 보안위협이 매우 크다. 이러한 문제점으로 인해 안전하고 정확하게 전달되어야 하는 필요성이 있는 중요한 정보들이 데이터 위변조나 개인정보 유출 및 침해 등 악의적으로 정보를 탈취하려는 위협들에 노출되었다. 이 위협을 극복하기 위해서 현재 사물인터넷 환경의 디바이스에 대하여 취약점들을 보완하고자 다양한 보안연구가 활발히 진행되고 있다. 특히 사물인터넷 환경에서 다양한 디바이스들이 상호동작하며 수집된 정보들을 공유하고 전달하기 때문에 각각의 디바이스들이 신뢰성을 가지고 통신할 수 있어야 한다. 이에 따라 디바이스 인증을 위한 다양한 기법의 연구들이 진행이 되었는데, 본 연구에서는 기존의 사물인터넷 디바이스들을 인증하기 위해 연구되어왔던 인증 기법에 대하여 한계 및 문제점을 알아보고 이를 해결하여 사물인터넷 환경에서 신뢰된 디바이스 간의 안전하게 통신을 할 수 있도록 사물인터넷 디바이스를 인증할 수 있는 기술을 제안한다.

Abstract As the scale of the Internet of Things (IoT) environment grows and develops day by day, the information collected and shared through IoT devices becomes increasingly diverse and more common. However, because IoT devices have limitations on computing power and a low power capacity due to their miniaturized size, it is difficult to apply security technologies like encryption and authentication that have been directly applied in the previous Internet environment, making the IoT vulnerable to security threats. Because of this weakness, important information that needs to be delivered safely and accurately is exposed to the threat of malicious exploitation, such as data forgery, data leakage, and infringement of personal information. In order to overcome this threat, various security studies are being actively conducted to compensate for the weaknesses in IoT environment devices. In particular, since various devices interact, and share and communicate information collected in the IoT environment, each device should be able to communicate with reliability. With regard to this, various studies have been carried out on techniques for device authentication. This study examines the limitations and problems of the authentication techniques that have been studied thus far, and proposes technologies that can certify IoT devices for safe communication between reliable devices in the Internet environment.

Keywords : IoT, Blockchain, PBFT, Device Authentication, Consensus Algorithm, Smart Home

*Corresponding Author : Moon-Seog Jun(Soongsil Univ.)
Tel: +82-2-820-0680 email: mjun@ssu.ac.kr
Received February 27, 2019 Revised March 28, 2019
Accepted May 3, 2019 Published May 31, 2019

1. 서론

사물인터넷(Internet of Things)은 자동차, 헬스 케어, 생활가전, 물류 같은 개인을 대상으로 하는 분야 뿐 아니라 농업, 공업 등의 산업분야, 그리고 보안관제, 환경과 같은 공공의 분야와 같은 다방면의 분야에서 무선 통신의 기능과 정보를 수집할 수 있는 다양한 센서들을 내장하여 실시간으로 인터넷을 통해 사람과 사물, 사물과 사물 간의 정보를 주고받는 지능형 기술과 서비스를 의미한다. 사물 인터넷의 핵심 기술에는 위치, 습도, 온도, 가스, 열, 속도 및 조도 등을 다양한 방법으로 측정하는 센싱 기술, 사물 인터넷의 주요 구성요소(사물, 인간, 서비스)를 이용해 특정 기능을 실행하는 응용서비스와 연동하는 인터페이스 기법 그리고 분산화된 환경에 존재하는 사물인터넷 디바이스들이 상호적으로 연결을 수행하는 유무선 네트워킹 기술이 있다. 일반 컴퓨팅은 몇 단계를 거쳐야 필요한 정보를 얻어오고 그 정보를 판단한 후에 행동하게 되지만, 사물인터넷을 사물 자체에 역할이 정해져서 필요한 정보를 전달받아 빠르게 필요로 하는 주체에게 제공하여 판단할 수 있게 해준다. 이러한 뛰어난 장점으로 인해서 사물인터넷 환경은 해를 거듭할수록 시장규모가 커지는 전망을 보여주고 있다.

Fig. 1. Smart Home Environment

사물인터넷 시장 규모가 지속적인 성장을 이룸에 따라 사물인터넷의 보안에 대한 취약점도 점차적으로 발견되고 있는데, 이는 사물인터넷 환경으로 나오는 다양한 사물들이 주고받는 통신 정보들이 해커의 공격 대상이 되기 때문에 보안에 대한 방어책의 필요성이 대두되고 있다. 예를 들면 사물들이 상호적으로 통신을 하면서 송수신하는 데이터에는 금융, 위치, 의료, 영상 등과 같은 사용자 개인의 프라이버시가 담긴 정보가 담겨 있어 다음과 같은 공격을 당한다면 정보의 유출이 가능해진다. 예를 들면, 인증되지 않은 디바이스에 대한 공격자의 수집 공격, 모방 공격, 개인정보 탈취 공격, 중간자 공격 등이 발생하고, 이러한 공격 기법들로 인하여 보안의 중요한 요소인 CIA, 즉 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability)에 대한 침해가 빈번히 발생하여 정상적인 서비스 제공 및 이용을 막는 보안 위협들이 발생하는 것이다[1-2].

정보를 수집하거나 공유하는데 활용되는 사물인터넷의 환경에서 각 사물간의 상호 통신과정이 빈번하게 발생하므로 안전하고 올바른 인증 방법이 필요하다. 게다가 사물인터넷에서 사용되는 디바이스들의 경우 소형화되도록 설계되어 있기 때문에 낮은 계산 능력을 가지는 특성상 경량화된 상태의 안전한 인증체계 방식을 적용해야 하는 한계가 있다. 이러한 한계점을 고려하여 위와 같은 보안 위협들로 발생하는 취약점을 해결하기 위하여 ID, 비밀번호 등을 활용하여 사물인터넷 디바이스의 인증 과정을 거친 후 서비스를 제공하는 연구와 다양한 인증 프로토콜(Authentication Protocol)들에 대한 연구가 다양하게 진행되고 있다[3].

블록체인 기술은 비트코인이라는 암호화폐가 최초로 등장하면서 전자상거래의 이중지불을 방지하기 위하여 Fig. 2와 같이 분산 데이터베이스의 형태로 제안된 핵심 기술로 지속적으로 데이터가 기록되는 리스트로 거래정보를 기록하는 원장을 중앙에서 관리하는 서버가 아닌 P2P 네트워크에 분산되어 네트워크상의 참가자들이 거래 내역을 공동으로 기록하고 보관하도록 설계되어 있고, 조금 넓은 의미로 분산 원장(Distributed Ledger)기술로 분류하기도 한다. 대표적인 응용사례로는 암호화폐의 거래과정을 기록하는 전자장부로 비트코인이 있다. 거래기록은 기본적으로 암호화되어 블록체인이 적용된 시스템에서 운용된다. 클라이언트와 서버가 자원을 공유하지 않고 Peer-to-peer 방식으로 자원을 공유하기 때문에 원하는 자원을 서버에서 허락해야 받을 수 있는 중앙 집중형태의 방식이 아니라 서로에게 도움을 요청하여 블록체인으로 연결되어 있는 상호적으로 연결되어 있는 공동체로써 자원을 손쉽게 공유할 수 있다.

Fig. 2. Blockchain Model

블록체인은 참여하는 네트워크들의 성격이나 범위 등에 따라 퍼블릭(Public)의 형태와 프라이빗(Private)의 형태로 구분된다. 퍼블릭 블록체인은 공개 형태의 방식으로 누구든지 자료에 대한 열람 및 거래가 가능하지만, 고도화된 암호화 검증 절차를 가져야 하며 네트워크의 확장성이 낮고 속도가 느리다는 단점이 있다. 또한 참여자가 익명성을 지니고 있기 때문에 중앙기관과 같이 제어를 필요로 하는 금융기관에서 활용하기에는 적합하지 않은 탈중앙화 방식의 구조이다.

상대적으로 프라이빗 형태의 블록체인은 자기 자신이 블록체인을 생성하고 관리할 수 있어 주체에 대한 식별이 가능하기 때문에 기업과 은행권에서 관심이 지대하다. 퍼블릭 블록체인은 작업증명(PoW), 지분 증명(PoS)같은 프로세스를 거쳐서 계약이나 거래에 대해 합의를 하게 된다. 반면에 프라이빗 블록체인의 경우, 승인 기관의 합의 알고리즘에 따라 합의하게 되며, 소수 기관의 권한으로 거래가 검증되고 처리되기 때문에, 일반적인 사용자가 임의로 참여할 수 없다. 보안적인 측면에서는 프라이빗 블록체인이 훨씬 높음을 알 수 있으며, 네트워크의 규칙이나 거래에 대한 내용을 변경 및 수정하는데 있어서 중앙기관의 개입을 통하여 빠르게 내용을 변경할 수 있는 이점을 가지고 있다[4-5].

Table 1. Blockchain Species

	Public Blockchain	Private Blockchain
Manager	All	Central organ
Transaction speed	Slow(10TPS)	Fast(1000TPS)
Identification	Anonymity	Identifiable
Transaction Certificate	PoW, PoS	Central organ
Data Accessibility	Accessible to all	Only authorized users
Use Case	Bitcoin, Etherium	Linq

본 연구에서는 사물인터넷을 기반으로 하는 스마트 홈 환경에서 다양한 사물인터넷 디바이스들이 통신을 하는데 있어 안전한 통신을 수립하기 위한 상호인증 방식의 사물인터넷 디바이스 인증 방식을 제안한다. 논문의 구성은 2장에서는 사물인터넷에서 디바이스 인증방식에서 대한 다양한 디바이스 인증 기술들에 대한 개념을 파악하고 각 인증기술별 한계점에 대해 알아본다. 3장에서는 C-PBFT 합의 알고리즘을 활용한 사물인터넷 디바이스 상호 인증 기법을 제안한다. 4장에서는 본 논문에 대한 결론을 제시한다.

2. 관련연구

2.1 사물인터넷 디바이스 인증 기법 사례

2.1.1 ID/PW 기반 디바이스 인증 기술

ID와 패스워드를 사용하는 인증기술은 전통적으로 사용되어왔던 기본적인 인증기술로써, 사물인터넷 단말기에 저장되어있는 ID와 패스워드를 사물인터넷 인증 서버와 연결하여 인증하는 방식이다. 이 방식은 사용하기가 편리하고 구현이 쉬운 편이며 사물인터넷 환경에서 보안 위협을 파악하기에 앞서 사물인터넷 서비스에 대한 인증 수준의 강도가 약하고 공격자에 의도에 의해 쉽게 우회될 수 있다는 단점이 있다. 공격자가 우회하기 위해서 전송과정에서 ID와 패스워드를 도청하여 재사용하는 방법이 일반적으로 이용된다[6].

2.1.2 MAC 주소 기반 디바이스 인증 기술

MAC(Media Access Control)은 네트워크의 데이터 링크 계층에서 통신하기 위해 해당 디바이스의 네트워크 인터페이스에 할당되어 있는 고유 하드웨어 주소를 말한다. 이 주소는 48비트로 구성이 되어있으며 48비트 중 앞에 위치한 24비트는 제조사의 고유번호를 나타내고 있고, 연이어 표시되어있는 24비트는 제조사에서 하드웨어를 생산하고 부여한 고유번호를 의미한다. 일반적으로 MAC 주소는 IP주소와 마찬가지로 특정 디바이스를 식별하는데 사용할 수 있다. 하지만 MAC 주소는 공격자의 의도로 프로그램을 사용해 손쉽게 변조할 수 있으며, 만약에 공격자가 사물인터넷 디바이스의 MAC 주소를 알게 된다면 해당 주소를 이용하여 위장하는 방식으로 디바이스 인증 메커니즘에 대한 우회가 가능해진다. 그렇기 때문에 MAC주소에 기반을 둔 디바이스 인증 방법은 인증의 강도가 약하고 공격자가 쉽게 우회할 수 있다는 단점이 있다[7].

2.1.3 암호 기반 디바이스 인증 기술

암호 기반의 디바이스 인증 기술은 무선인터넷 환경에서 디바이스 인증을 위해 사용되는 802.1x, EAP, WPA 등의 프로토콜 혹은 암호화 알고리즘을 이용하여 상호 인증하는 기술이다. 암호 기반의 인증 기술은 앞서 설명된 ID/PW 기반의 디바이스 인증기술과 MAC 주소 기반의 디바이스 인증기술에 대비하여 강도 높은 인증을 수행할 수 있기 때문에 많은 연구가 이루어지고 있다. 사물인터넷 환경에서 타원곡선 암호 알고리즘에 기반을 둔

디바이스 인증 프로토콜은 해를 거듭할수록 초기의 타원곡선 알고리즘에 대한 취약점을 분석하고 개선하는 심도 깊은 연구가 이루어지고 있다. Proambage [8-10]등이 제안한 디바이스 인증 기술은 센서 네트워크의 인증 프로토콜에서 공격자가 상대방의 식별자를 검증할 수 있는 단계가 존재하지 않아 정당한 서버로 위장하는 공격이 이루어질 수 있으며, 위장 공격에 성공했을 경우 합의된 인증키의 계산상 성질을 활용하여 사물인터넷 디바이스의 비밀 키 값에 대한 추측을 하는 공격이 이루어질 수 있다는 문제점이 있으나 개선된 연구에서는 대체식별자를 통해 서버와 클라이언트 간에 상호 인증이 이루어짐으로써 위장 공격에 대하여 대응이 가능해지며, 메시지를 주고받을 때 타임스탬프를 활용해서 재전송 공격을 사전에 방지할 수 있다. 이 방법에서는 위장 공격이 방지되므로 공격이 무효화되기 때문에 인증키 추측이 불가능해진다[11]. 하지만 마찬가지로 대체식별자를 교환하는 과정에서 중간자 공격을 받게 되면 도청을 받을 수 있는 문제점이 존재하고, 계산능력이 떨어지는 디바이스가 있는 환경에서는 운용하기 힘들다는 단점이 있다.

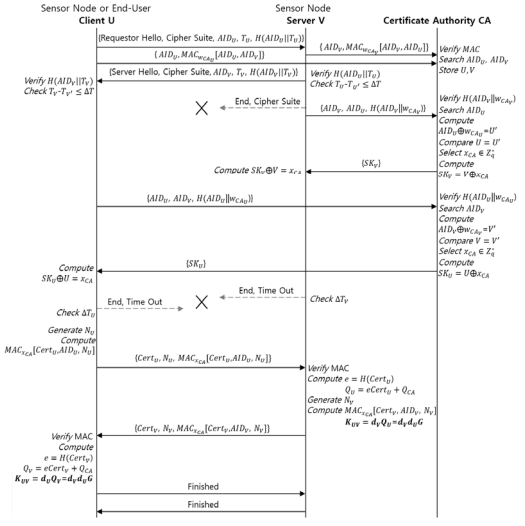


Fig. 3. ECC Based Device Authentication

2.1.4 시도-응답 기반 디바이스 인증 기술

시도-응답기반의 디바이스 인증 기술은 디바이스나 인증 서버가 임의의 랜덤 값을 생성하여 상대방에게 전달한 후 상대방은 전달받은 임의의 랜덤 값과 패스워드를 사용해 함수 알고리즘을 적용하여 도출된 결과 값을 반환하게 되고 응답을 받은 상대는 클라이언트와 동일한 해시단계를 거쳐 도출되는 결과 값과 비교하는 방법으로 인증 서버가 인증이 필요한 경우 사물인터넷 디바이스에 인증하고자 하는 정보를 요청하기 때문에 기존의 방식과 차이가 있다. SDN(Software Defined Network)기반의 환경에서 사물인터넷 디바이스를 인증하기 위해 제안된 시도-응답 기반의 디바이스 인증기술은 Fig. 4와 같이 SDN 장치의 프로그래밍이 가능한 특성을 활용하여 사물인터넷 디바이스의 인증정보를 요청하고 검증하는 방법을 사용한다. 그렇지만 이방법의 경우 사용되는 인증정보는 사물인터넷 디바이스 디바이스의 고유정보,ID,비밀번호 등은 정적인 정보로써 중간자에 의한 공격에 발생할 경우 공격자에 의해 재전송 및 위장공격이 발생할 우려가 있다[12].

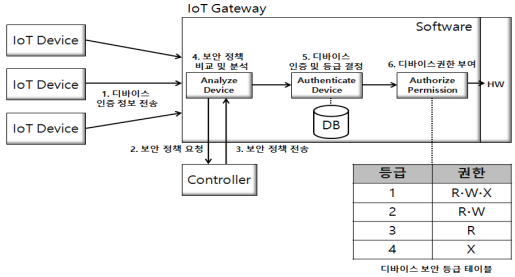


Fig. 4. SDN Based Device Authentication

또한 M2M 기반의 통신환경에서 안정성을 보장하는 상호적인 단말기 인증 방법은 마찬가지로 시도-응답 방식을 사용하고 있는데, Tag와 Reader에서 연산 알고리즘을 활용하여 인증 값을 생성한 후 상호적으로 비교하는 방법을 사용한다. 동일한 방식으로 Tag에서 고유한 값을 생성하여 Reader로 전송하면 Reader는 수신 값을 데이터베이스에 저장한다. 데이터베이스에서 Reader의 인증을 위한 값을 생성한 후 전송하면 Reader에서 Tag로 고정 길이 데이터 값을 생성하여 전송한다. Tag는 Reader가 송신한 값을 본인이 생성한 값과 상호 비교한 후, 동일할 시 자신의 ID를 해시연산 후 암호화하여 Reader에 전송하는 방법을 사용한다. 하지만 이방법도 위의 SDN 환경의 시도-응답 기반 인증기술과 마찬가지로 중간자 공격으로 인해 도청된다면 재전송 공격이 가능할 수 있다는 한계점이 있다.

2.1.5 일회용 패스워드 기반 디바이스 인증기술

일회용 패스워드 기반의 디바이스 인증기술은 단말기

와 인증서버에 동일한 알고리즘을 사용하여 상호적으로 암호를 생성하는 방법으로 상호 교환하는 임의의 랜덤 값이 동일할 경우에 같은 패스워드를 생성하여 인증하게 되는 방법이다. 일회용 패스워드는 한번만 사용되고 재사용하지 않기 때문에 강력한 인증 방법으로 알려져 있다. 하지만 기존의 환경에 이러한 방법을 적용하기에는 인증 값 생성을 위한 알고리즘이 적용되어야 하기 때문에 구조적인 변경이 필요하다. 실제로 사물인터넷 환경에서는 기존의 디바이스에 대하여 변경이 발생하는 것은 저전력, 경량화를 추구하는 단말기의 안정성을 해칠 수 있고, 기능저하 등의 문제가 발생할 수 있기 때문에 적용하는데 있어서 한계점이 있다[13].

2.2 사물인터넷 디바이스 인증 기술 한계점

앞서 설명한 다양한 사물인터넷 디바이스 인증 기술들은 실제 환경에서 적용함에 있어서 한계점이 존재하는데 정리하면 다음과 같이 인증 강도, 우회 가능성, 설계에 따른 디바이스 변경 여부로 구분하여 표로 나타낼 수 있다.

ID/PW 기반, MAC 주소 기반의 경우엔 인증강도가 낮고 우회 가능성이 높다는 문제가 있다는 단점이 있지만 디바이스의 변경이 불필요하다는 점이 있다. 암호 기반, 일회용 패스워드 기반의 경우 인증강도가 높고 우회 가능성이 낮지만 높은 계산능력의 암호화 기술은 디바이스를 변경해야 하는 단점이 있다. 마지막으로 시도-응답 방식 기반의 경우 인증 강도와 우회 가능성은 중간이지만 디바이스 변경을 필요로 하다는 단점이 있다.

Table 2. IoT Devices Authentication Comparison

Authentication	Certification Strength	Bypass potential	Device Change Status
ID/PW	Low	High	Not need
MAC	Low	High	Not need
Cipher	High	Low	Need
Challenge-Response	Middle	Middle	Need
One time password	High	Low	Need

2.3 사물인터넷 디바이스 인증 기술 개선방향

앞서 사물인터넷 디바이스를 인증하기 위해 연구했던 다양한 인증 기술들에 대한 한계점을 알아보고 이를 극복하기 위해 본 논문에서는 블록체인을 활용하여 복수의 디바이스가 함께 참여하여 인증과정을 수행할 수 있게 연구하였다. 소형화된 디바이스의 계산 능력을 감안하여 클라이언트-게이트웨이의 구간에서만 인증서를 사용하여 보안 능력을 강화하고 게이트웨이-디바이스 구간은 그룹화 시작단계에서 상호 협의된 암호화키를 생성하고 이를 활용하여 낮은 계산능력을 지닌 디바이스로도 안전하게 인증할 수 있도록 하여 인증강도를 높이고 디바이스 변경을 불필요하게 하였다. 또한 복수의 디바이스가 함께 참여하여 인증과정을 수행하기 때문에 우회 가능성도 낮도록 하였다[14-15].

다음 장에서 기존 연구의 한계점을 보완한 스마트 홈 환경에서 C-PBFT 기반의 안전한 디바이스 인증 기술에 대해 세부적으로 설명한다.

3. C-PBFT 디바이스 인증 프로토콜

사물인터넷이 나날이 발전하며 다양한 분야에서 활용됨에 따라 수요에 맞춰 디바이스의 수는 기하급수적으로 증가하고 있다. 하지만 사물인터넷 환경의 디바이스들은 소형화되기 때문에 보안적인 면에서 안전하지 않다. 따라서 사용자가 안전하게 사물인터넷을 이용하기 위해서는 디바이스에 대한 신뢰성이 필요하다.

앞서 2장 관련연구에서 언급되었던 다양한 디바이스 인증 기술들은 사물인터넷에 적용시키기에는 인증 강도, 우회 가능성 등에 대하여 한계점이 존재한다. 이러한 한계점을 해결하고자 다음과 같이 개선된 C-PBFT 합의 알고리즘을 활용하여 사물인터넷 디바이스를 효과적으로 인증하는 프로토콜을 제안한다.

3.1 제안하는 C-PBFT 알고리즘

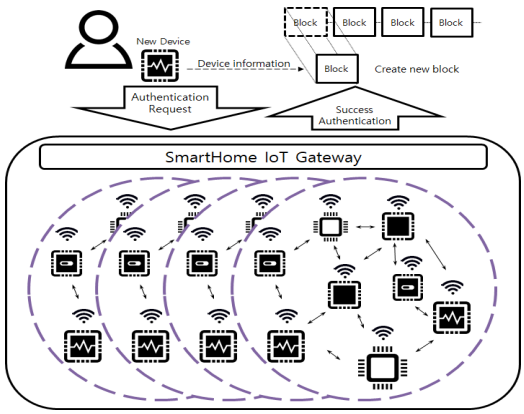


Fig. 5. Proposed Model

PBFT는 네트워크 상의 모든 노드들이 상호적으로 메시지를 주고받아 인증하여 신뢰를 보장하는 합의 알고리즘이다. 하지만 네트워크 내에서 메시지를 주고받아 인증하기 위한 노드의 개수가 늘어날수록 속도가 느려지는 단점이 있다. 이러한 단점을 개선하기 위해서는 전체 노드가 아닌 특정 목적에 맞추어 노드들을 그룹화하여 신뢰할 수 있는 디바이스 인증과정을 가지도록 해야 한다. 그룹화된 노드들로 새로운 디바이스에 대한 인증을 진행하게 되면 속도 저하를 우려하지 않고 신뢰된 스마트 홈 환경의 사물인터넷 디바이스들을 인증할 수 있다.

3.2 제안 프로토콜

Table 3. Proposed Protocol Symbol

Sign	Signification
R	Device Role Information
C	Device Group Information
D_{id}	Device Identification
T_c	Client Timestamp
$Sig_c()$	Client Certification
G_r	Group Cipher Key
$E_k()$	Message Encryption
$k_1 \cdots k_n$	Registration Key Value by Device
$S_1 \cdots S_{n+1}$	Approval value by device
$D(S_1 \cdots S_{n+1})$	Integrated Approval Message Digest
T_g	Gateway Timestamp
K_{n+1}	Registered key values for approved devices

첫 번째로 스마트 홈 네트워크 환경에서 신규 디바이스를 추가하기 위해 Request 단계를 수행한다. 이 때 클라이언트는 디바이스 아이디, 역할 정보, 그룹 정보, 사용자가 요청한 시간의 타임스탬프를 서명하여 IoT 게이트웨이에 전송한다.

$$Sig_c(R,C,D_{id},T_c)$$

두 번째로 클라이언트가 전송한 메시지를 수신한 IoT 게이트웨이는 메시지의 클라이언트 서명 내용을 검증한 후 그룹 내의 디바이스들에게 메시지를 전송하는 Pre-Prepare 단계를 수행한다. 게이트웨이는 인증하려는 디바이스의 역할 정보, 그룹 정보, 타임스탬프를 확인한 후 인증을 하기 위한 그룹 암호화 키를 생성한다. 확인한 그룹 정보를 색인하여 그룹에 속하는 각 디바이스별 암호화키를 이용하여 신규 디바이스를 검증하기 위해 전달받은 내용에 그룹 암호화키를 포함하여 암호화한 후 메시지를 전달한다.

$$E_{k1}(R,C,D_{id},G_r),\ E_{k2}(R,C,D_{id},G_r),\ E_{kn}(R,C,D_{id},G_r)$$

세 번째로 디바이스는 전달받은 메시지를 복호화하여 추가하려는 디바이스 정보를 확인하고 메시지를 전달하

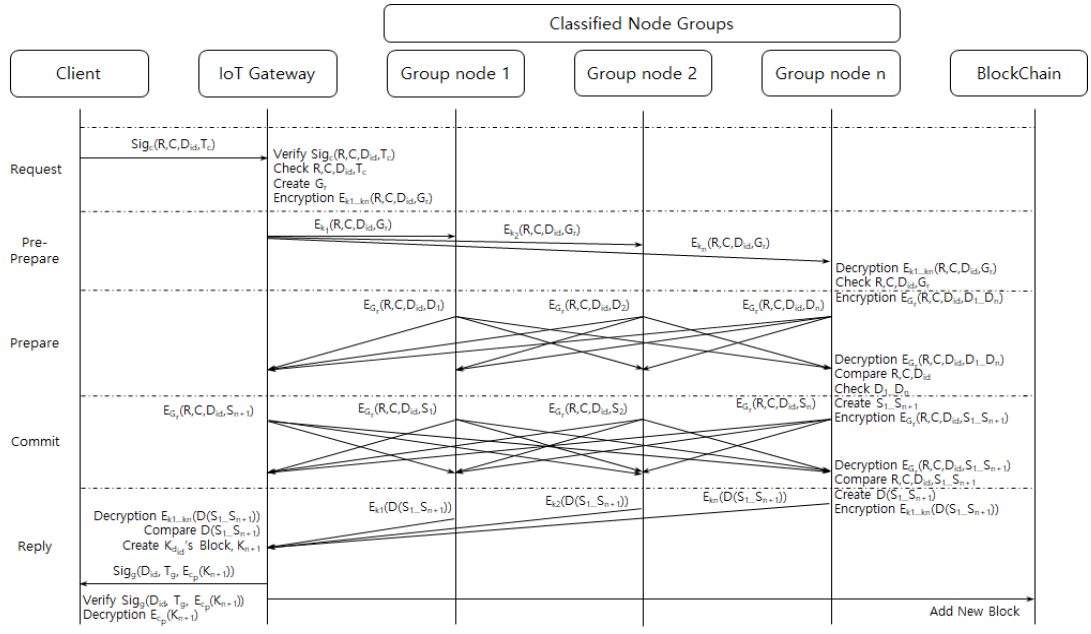


Fig. 6. Proposed Device Authentication Protocol

는 Prepare 단계를 수행한다. 확인이 완료되면 각 디바이스는 내용을 확인했음을 다른 디바이스들에게 알리기 위해 자신의 디바이스 정보값을 포함해 IoT 게이트웨이로부터 전달받은 그룹 암호화키로 메시지를 암호화해 다른 디바이스들에게 전달한다.

$$E_{Gr}(R,C,D_{id},D_1),\ E_{Gr}(R,C,D_{id},D_2),\ E_{Gr}(R,C,D_{id},D_n)$$

네 번째로 각 디바이스가 확인 메시지를 복호화해 추가하려는 디바이스 정보를 확인하고 승인 메시지를 전달하는 Commit 단계를 수행한다. 메시지를 확인한 각 디바이스들은 추가하려는 디바이스를 신뢰함을 승인하는 값을 생성한다. 해당 승인 값은 앞서 저장했던 디바이스의 아이디, 역할 정보, 그룹 정보와 함께 그룹 암호화키로 암호화하여 IoT 게이트웨이 및 그룹 내 디바이스들에게 메시지를 전달한다

$$E_{Gr}(R,C,D_{id},S_1),\ E_{Gr}(R,C,D_{id},S_2),\ E_{Gr}(R,C,D_{id},S_{n+1})$$

다섯 번째로 메시지들을 전달받고 IoT 게이트웨이가 생성한 값과 일치 여부를 검증하는 Reply 단계를 수행한다. 디바이스는 전달받은 메시지를 복호화하여 승인 메시지들을 확인 후 통합하여 승인 메시지 다이제스트를 생성한다. 생성한 다이제스트는 각 디바이스에서 자신의 암호화 키로 암호화해 IoT 게이트웨이에 전달한다.

$$E_{k1\cdots kn}(D(S_1\cdots S_{n+1}))$$

마지막으로 검증이 완료되면 IoT 게이트웨이는 블록을 생성하여 등록하고 클라이언트에게 알린다. 추가하고자 하는 디바이스가 승인되면 해당 디바이스의 아이디, 게이트웨이 타임스탬프, 디바이스 등록키, 클라이언트 공개키로 암호화한 정보를 클라이언트 개인키로 서명 후 클라이언트에게 보낸다. 또한 스마트 홈 환경에 디바이스가 등록되었음을 기록하기 위해 새로운 블록을 생성하여 블록체인에 등록한다.

$$Sig_g(D_{id},\ T_g,\ E_{cp}(K_{n+1}))$$

클라이언트는 전달받은 메시지를 검증하고 추가하려는 신규 디바이스에 값을 등록하여 스마트 홈 환경에서 사용한다.

4. 분석 및 보안평가

4.1 기존 블록체인과 성능 비교분석

Table 4. Comparison by Blockchain Types

	Public Blockchain	Private Blockchain	Proposed Blockchain
Consensus algorism	PoW,PoS	PBFT	C-PBFT
Time	10 min ~ 1 hour	Few seconds ~ minutes	Few seconds ~ minutes
Scalability	Low	Middle	High
Safety	Not Safe	Safe	Safe
Time of agreement	All	All	Short
Authorization	Difficulty	Middle	Easy
Compliance	Difficulty	Middle	Middle

퍼블릭 블록체인은 대표적으로 PoW, PoS 합의 알고리즘을 이용하기 때문에 블록체임 참여자나 분산원장들을 따로 관리할 필요가 없으나 합의 내용이 최종적으로 확정되기까지 최대 1시간 정도의 시간이 소요된다는 단점이 있지만, 프라이빗, 제안하는 블록체인 시스템의 경우 수초에서 수분의 시간이 필요하다.

확장성 면에 있어서는 일반적으로 블록의 크기를 증가시키거나 한 번에 처리하는 거래 처리량을 높여야 한다. 퍼블릭 블록체인의 경우에는 이 부분을 조정하는데 있어서 대부분의 노드에게 동의를 얻어야 하기 때문에 처리하기 쉽지 않아서 확장성이 낮은 편인데 반해, 프라이빗 블록체인의 경우에는 퍼블릭 블록체인보다 적은 수의 사전 협약이 되어있는 노드들에게 동의가 필요하기 때문에 중간 정도의 확장성을 지니고 있다. 제안 블록체인의 경우에는 프라이빗 블록체인에 비해 더 적은 노드의 동의가 필요하기 때문에 확장성이 상대적으로 높다고 이야기할 수 있다.

안정성 면에서는 퍼블릭 블록체인은 채굴자들의 채산성 및 수요에 따라 가상화폐의 가격이 급격하게 변동하여 안정성이 떨어지지만, 프라이빗 또는 제안형 블록체인의 경우 사전 협약된 노드들로 이루어져있기 때문에 수수료와 같은 가상화폐 생성없이 서비스가 이루어지기 때문에 안정적으로 이용이 가능하다.

합의 참여시간의 경우 퍼블릭 블록체인과 프라이빗 블록체인은 참여하고 있는 노드들이 분산원장을 상호공유하기 위하여 최초의 블록이 생성되었을 때부터 마지막 블록이 생성될 때까지 합의에 참여하거나, 참여 시점에서 전체 분산원장을 전달받아야 한다. 그러나 제안 블록체인은 특정 그룹의 노드들이 해당 디바이스 인증에 참여하기 때문에 참여시간이 짧다.

마지막으로 규제 준수면에 있어서는 퍼블릭 블록체인은 블록체인 네트워크에 참여하는 모든 노드들에 대한 엄격한 통제가 어렵기 때문에, 규제나 사용자 관리가 어렵다. 하지만 프라이빗 블록체인, 제안형 블록체인의 경우에는 사전 합의한 노드들로 구성이 되어있기에 규제 준수가 가능하다.

4.2 보안 평가

4.2.1 가장 공격

스마트 홈 환경에서 악의적인 공격을 시도하려는 디바이스는 정상적인 사물인터넷 디바이스로 가장하여 침투하려 할 수 있다. 하지만 제안하는 블록체인 환경 내에서 악의적인 공격을 시도하려는 디바이스가 임의의 사물인터넷 디바이스로 가장하여 침투하기 위해서는 우선적으로 블록체인 내에서 분류된 그룹의 대부분의 디바이스들에게 안정성을 검증받은 후, 블록체인에 해당 디바이스의 검증내역이 등록이 되어야 통신이 가능하기 때문에 가장 공격을 할 수 없다.

4.2.2 이중지불 공격

블록체인 환경에서 대표적인 공격 중 이중 지불 공격은 탈중앙화 형태의 블록체인 시스템에서 동시간대에 서로 다른 거래가 발생하게 될 경우 일어날 수 있는 공격방법이다. 퍼블릭 블록체인 시스템은 화폐 시스템 기반의 블록체인 환경이기 때문에 블록을 생성하는데 있어서 이자의 개념이 발생하여 화폐가 발생하게 되는데 해당 공격이 실제로 이루어질 경우 이중 지불이라는 치명적인 사고가 발생할 수 있다. 하지만 제안한 블록체인 시스템의 경우 사전에 내부에서 합의된 사물인터넷 디바이스들을 활용하여 C-PBFT 합의 알고리즘기반으로 블록이 생성되기 때문에 가상화폐가 발생하지 않아 이중지불 공격이 발생될 수 없다.

4.2.3 51% 공격

일반적으로 블록체인 시스템의 개념에서는 참여하는 모든 노드 중 절반 이상의 해시 파워를 지니고 있는 악의적인 행위자나 그룹이 시스템 노드의 절반 이상을 장악한 후, 해당 블록체인의 시스템 환경에서 악의적인 거래내역을 승인하도록 공격하는 행위를 51% 공격이라 하는데, 제안한 블록체인 시스템의 경우 중앙형태의 블록체인 시스템으로 이루어져있기 때문에 51% 공격은 발생할 수 없다.

5. 결론

본 논문에서는 스마트 홈 환경에서 다양한 사물인터넷 디바이스들이 상호적으로 협동하여 디바이스를 인증하여 안전한 통신을 만족할 수 있도록 C-PBFT 기반의 디바이스 인증 기술을 제안한다. 무선 인터넷 환경을 통하여 다양한 센서들을 활용해서 정보를 수집하고 전달하는 사물인터넷 디바이스들의 시장 환경이 시간이 지남에 따라 기기의 수가 급격하게 증가하며 규모가 커지면서 발전하고 있다. 이러한 사물인터넷 시장 규모가 나날이 성장함과 동시에 단순 계산능력을 가진 소형화된 사물인터넷 디바이스의 보안에 대한 문제점은 날이 갈수록 우려되고 있는데 이를 해결하기 위해서는 사물인터넷 디바이스에 대한 보안 문제점에 대한 연구가 활발히 이루어져야 한다. 특히 사물인터넷 디바이스에 대한 안전한 인증을 통해 신뢰성을 높이는 것이 매우 중요하다. 본 연구에서 제시한 C-PBFT 합의 알고리즘을 활용한 인증 기법을 바탕으로 기밀성, 무결성, 가용성 침해 발생을 일으키는 보안 위협들로부터 안전한 인증 방식을 가져다 줄 것으로 기대한다.

References

[1] Zhang, Zhi-Kai, “IoT security: ongoing challenges and research opportunities”, *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

[2] Seokung Yoon, Haeryong Park, HyeongSeon Yoo, “Security issues on Smarthome in IoT environment”, *Computer science and its applications*, Springer, Berlin, Heidelberg, pp.691-696, 2015.
DOI: https://doi.org/10.1007/978-3-662-45402-2_97

[3] Sivaraman Vijay, “Network-level security and privacy control for smart-home IoT devices”, *Wireless and Mobile Computing, Networking and Communications (WiMob)*, 2015 IEEE 11th International Conference on. IEEE, pp.163-167, 2015.
DOI: https://doi.org/10.1109/wimob.2015.7347956

[4] Konstantinos Christidis, Michael Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things”, *IEEE Access*, IEEE, pp.2292-2303, 2016
DOI: https://doi.org/10.1109/ACCESS.2016.2566339

[5] Chul-Jin Kim, "A Static and Dynamic Design Technique of Smart Contract based on BlockChain" *Korea Academy Industrial Cooperation Society*, vol. 19, no. 6, pp. 110-119, Jun. 2018
DOI: https://doi.org/10.5762/KAIS.2018.19.6.110

[6] Atwady Yahya, Hammoudeh Mohammed, "A survey on authentication techniques for the internet of things", *Proceedings of the International Conference on Future Networks and Distributed Systems*, ACM, NY, USA, p. 8, 2017.
DOI: https://doi.org/10.1145/3102304.3102312

[7] X. Yao, X. Han, X. Du, X. Zhou, "A lightweight multicast authentication mechanism for small scale IoT applications", *IEEE Sensors Journal*, vol 13, no. 10, pp.3693-3701, Oct, 2013.
DOI: https://doi.org/10.1109/JSEN.2013.2266116

[8] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov and M. Ylianttila, "Two-phase Authentication Protocol for Wireless Sensor Networks in Distributed IoT Applications", *2014 IEEE Wireless Communications and Networking Conference(WCNC)*, Istanbul, Turkey, pp. 2728-2733, Apr. 2014.
DOI: https://doi.org/10.1109/WCNC.2014.6952860

[9] Thomas Kothmayr, Corinna Schmitt, Wen Hu, Michael Brunig and Georg Carle,. "DTLS based security and two-way authentication for the Internet of Things", *AD Hoc Networks*, vol. 11, issue 8, pp. 2710-2723, Nov. 2013.
DOI: https://doi.org/10.1016/j.adhoc.2013.05.003

[10] N. Mahalle, B. Anggorojati, N. R. Prasad and R. Prasad, "Identity Authentication and Capability Based Access Control(IACAC) for the Internet of Things". *Journal of Cyber Security and Mobility*, vol. 1, no. 4, pp. 309-348, Mar. 2013.

[11] Deuk-hun Kim, Jin Kwak, "Design of Improved Authentication Protocol for Sensor Networks in IoT Environment" *Journal of the Korea Institute of Information Security & Cryptology*, vol. 25, no. 2, pp. 467-478, April, 2015.
DOI: https://doi.org/10.13089/JKIISC.2015.25.2.467

[12] O. Flauzac, C. González, A. Hachani and F. Nolot, "SDN based architecture for IoT and improvement of the security", *2015 IEEE 29th International Conference on Advanced Information Networking and Applications Workshops*, Gwangju, p. 688-693, 2015.
DOI: https://doi.org/10.1109/WAINA.2015.110

[13] V. L. Shivraj, M. A. Rajan, M. Singh and P. Balamuralidha, "One time password authentication scheme based on elliptic curves for Internet of Things (IoT)", *2015 5th National Symposium on Information Technology: Towards New Smart World (NSITNSW)*, IEEE, Riyadh, p. 1-6, 2015.
DOI: https://doi.org/10.1109/NSITNSW.2015.7176384

[14] Castro Miguel, "P*ractical Byzantine fault tolerance", Appears in the Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)*, p. 173-186, 1999.

[15] H. Sukhwani, J. M. Martínez, X. Chang, K. S. Trivedi and A. Rindos, "Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (Hyperledger Fabric)", *2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS)*, Hong Kong, p. 253-255, 2017.
DOI: https://doi.org/10.1109/SRDS.2017.36

김 정 호(Jeong-Ho Kim) [정회원]

- 2013년 8월 : 평택대학교 컴퓨터학과 (공학사)
- 2015년 8월 : 숭실대학교 정보과학대학원 정보보안학과 (공학석사)
- 2015년 9월 ~ 현재 : 숭실대학교 컴퓨터학과 (박사수료)

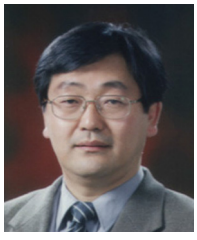
〈관심분야〉
블록체인, 클라우드, IoT 보안, 네트워크 보안

허 재 욱(Jae-Wook Heo) [준회원]

- 2017년 8월 : 국가평생교육진흥원 컴퓨터공학 (공학사)
- 2018년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 (석사과정)

〈관심분야〉
정보보호, 블록체인, 인공지능

전 문 석(Moon-Seog Jun) [정회원]



- 1981년 2월 : 숭실대학교 전자계산학과 (공학사)
- 1986년 2월 : University of Maryland Computer Science (공학석사)
- 1989년 2월 : University of Maryland Computer Science (공학박사)
- 1986년 9월 ~ 1989년 12월 : University of Mary 강사
- 1989년 3월 ~ 7월 : Morgan State University 조교수
- 1989년 9월 ~ 1991년 2월 : NMSU, PSL 연구소 책임연구원
- 1991년 3월 ~ 현재 : 숭실대학교 정교수

〈관심분야〉
정보보호, 네트워크 보안, 전자여권, 암호학