Journal of Korea Society of Industrial Information Systems Vol.28 No.5, Oct. 2023 :41-54
http://dx.doi.org/10.9723/jksiis.2023.28.5.041 ISSN:1229-3741

스마트 그리드 환경에서 블록체인 기반 스마트 미터 인증 프로토콜+

(Blockchain-based Smart Meter Authentication Protocol in Smart Grid Environment)

김 종 현[1], 김 명 현[2]*, 박 영 호[2]*
(Jonghyun Kim, Myeonghyun Kim, and Youngho Park)

요 약 스마트 그리드는 효율적인 에너지 생산과 소비, 관리를 지원해주는 전력망 시스템으로 다양한 분야와 산업에서 활용되고 있다. 그러나 공개된 네트워크를 통해 서비스가 제공되는 환경에서는 보안 취약점과 개인정보 침해에 대한 신뢰 문제 해결은 필수적이다. 특히, 스마트 미터 단말의 식별정보는 중앙화된 서버를 통해 일괄적으로 관리되며, 중앙화된 관리 구조는 단말기 탈취, 데이터 위조 및 변조, 삭제 등 공격에 취약하다. 본 논문은 이러한 문제점을 해결하기 위해 탈중앙 분산원장 기술인 블록체인을 활용한 스마트 미터 인증 프로토콜을 제안한다. 제안된 방식은 블록체인을 통한 개별 스마트 미터 단말의 고유한 분산식별자(DID) 발급과 물리적복제방지기술(PUF)을 기반한 난수 값을 사용하여 데이터의 무결성과 신뢰성을 강화한다. 또한 비정형 보안 분석 및 AVISPA 시뮬레이션을 이용하여 제안한 방식의 안전성을 분석하고 관련 연구들과 비교하여 효율적인 방식임을 보인다.

핵심주제어: 블록체인, 인증, 분산식별자, PUF

Abstract Smart grid that supports efficient energy production and management is used in various fields and industries. However, because of the environment in which services are provided through open networks, it is essential to resolve trust issues regarding security vulnerabilities and privacy preservation. In particular, the identification information of smart meter is managed by a centralized server, which makes it vulnerable to security attacks such as device stolen, data forgery, alteration, and deletion. To solve these problems, this paper proposes a blockchain based authentication protocol for a smart meter. The proposed scheme issues an unique decentralized identifiers (DIDs) for individual smart meter through blockchain and utilizes a random values based on physical unclonable function (PUF) to strengthen the integrity and reliability of data. In addition, we analyze the security of the proposed scheme using informal security analysis and AVISPA simulation, and show the efficiency of the proposed scheme by comparing with related work.

Keywords: Blockchain, Authentication, Decentralized identifier, PUF

* Corresponding Author: kimmyeong123@knu.ac.kr, parkyh@knu.ac.kr
+ 이 논문은 2023년도 중소벤처기업부의 기술개발사업 지원에 의한 연구임 [RS-2023-00255607].
Manuscript received September 05, 2023 / revised October 04, 2023 / accepted October 05, 2023
1) 경북대학교 정보보호학과, 제1저자
2) 경북대학교 전자전기공학부, 교신저자

1. 서 론

스마트 그리드(Smart grid)는 전기 및 정보통신 기술을 활용하여 전력망을 고도화함으로써 고품질의 전력서비스를 제공하고 에너지 이용효율 극대화를 가능하게 하는 차세대 지능형 전력망이다. 이런 스마트 그리드 환경에서 전력 및 에너지 시스템과 인프라의 효율적인 운영을 위해 스마트 장치를 통해 관련 정보를 수집하고 적절한 서비스를 제공한다. 특히, 사물인터넷(IoT)은 스마트 그리드와 결합하여 다양한 응용 프로그램과 서비스를 지원하며 수집되는 데이터의 신뢰성과 안정성을 담당하는 스마트 미터는 중요한 감지 기능과 높은 연결성을 특징으로 발전하였다. 그러나 스마트 그리드 시스템에서 유선 네트워크와 무선통신 기술의 결합으로 광범위한 제어, 자동화 및 연결성이 가능하게 되었지만 기존 무선통신과 소프트웨어, 가상화 운영 환경이 가지고 있는 보안 취약점과 악의적 공격에 대한 위협에 쉽게 노출될 수 있다(Park et al., 2011; Park and Park, 2015; Mirzaee et al., 2022). 따라서, 스마트 미터의 신뢰성 향상과 보안 확보를 위한 단말 인증에 대한 지속적인 연구가 활발히 이루어지고 있다(Paul et al., 2014; Barai et al., 2015; Odelu et al., 2018; Islam et al., 2019; Sureshkumar et al., 2020).

Odelu et al.(2018)는 스마트 그리드 환경에서 스마트 미터의 자격증명과 개인정보 보호를 위한 키 보안 기술을 제안하였으나 단말 구현의 높은 복잡성이 요구되며, Islam et al.(2019)이 제안한 스마트 미터의 고급키 생성, 단말 보안 강화를 위한 물리계층 보안기술은 추적 공격에 취약해 개인정보 보호에 문제점이 발생한다.

Sureshkumar et al.(2020)은 GNY 논리와 ProVerif 자동화 도구를 활용한 프로토콜로 스마트 미터와 서비스 제공자 간 보안통신 방법을 제안하였으나 단말 인증과 가장 공격에는 취약한 문제점이 있다.

이러한 문제는 스마트 미터의 자원 제약적인 사항으로 물리적 위협과 외부 공격에 취약한 단말을 통해 시스템 전체적인 장애와 붕괴를 초래하며(Alsuwian et al., 2022) 서비스 확대에 따른 신규 보안 문제와 스마트 미터의 광범위한 제어를 위한 효율적인 연구가 필요하다.

본 논문에서는 스마트 그리드를 위한 탈중앙 분산원장을 활용한 스마트 미터 인증체계와 방법을 제안한다. 제안한 인증 방식은 블록체인을 통해 개별 단말에 고유 분산식별자인 DID (decentralized identifier)(W3C, 2022)를 발급하여 분산식별자를 이용한 탈중앙화된 인증 방식을 제공하고, 물리적 복제 방지기술 PUF(physical unclonable function)(Gao et al., 2020)을 이용하여 생성한 비밀 값을 기반으로 데이터의 무결성 및 기밀성을 보장한다. 또한 제안한 방식과 관련 연구들과의 계산량 및 통신량을 비교분석하여 제안한 인증 방식이 스마트 그리드 환경에서 효율적이고 안전한 인증방식임을 증명한다.

2. 관련 연구

2.1 스마트 그리드

스마트 그리드 환경에서 전송되는 데이터의 양이 방대해지며 다양한 보안 위협으로부터 안전한 데이터 인증을 위한 연구가 지속적으로 제안되고 있다. Lee and Kim(2016)은 블록체인을 이용한 스마트 그리드 시스템의 기기 인증 방안을 제안하였다. 그러나 그들의 방식은 다양한 보안 공격으로부터 안전할 수 있는 구체적인 인증방안에 대한 분석을 다루고 있지 않다. Zhang et al.(2019)은 스마트 그리드를 위한 블록체인 기반의 탈중앙화되고 안전한 key-less 서명 기법을 제안하였다. 그러나 스마트 미터가 수집한 데이터를 보낼 때 마다 블록체인에 기록하기 때문에 통신과정과 별도로 블록체인 합의과정을 위한 비용이 발생할 수 있어 시스템 운영 효율성이 떨어지는 취약성을 가지고 있다. Xiong et al.(2020)은 스마트 그리드를 포함한 IoT 환경에서 스마트 장치가 개방형 무선 통신 채널을 통해 데이터를 전송하는 것은 악의적인 보안 공격에 취약할 수 있으므로, certicateless signature 방식을 사용하여 스마트 장치에서 전송되는 데이터의 신뢰성을 보호하는 방법을 제시하였다.

그러나 그들의 방식은 스마트 장치가 일괄 인증을 직접 수행해야 하는 부담이 존재한다.

또한 최근 기존의 시스템 구조에서 데이터를 이용하는 서버의 데이터 검증 및 관리 등에 의한 부담을 줄이고 스마트 그리드 환경에 기기 관리의 효율성을 높이고 노드간 통신 및 서비스 지연을 줄이기 위한 엣지 컴퓨팅 기술을 결합하는 연구가 진행되면서 관련된 안전한 인증 프로토콜 연구가 함께 진행되고 있다. Cui et al. (2021)은 기존의 엣지 컴퓨팅 기반 시스템 구조에서 사용자의 민감한 개인정보 등을 포함한 데이터를 중간에서 수집하는 엣지 서버가 신뢰할 수 없는 개체일 때 사용자의 개인정보 유출 등의 프라이버시 문제가 발생할 수 있으므로 그룹 서명 기술 및 프록시 재암호화 기술을 활용한 데이터의 기밀성과 무결성을 보장하는 메시지 인증 방식을 제안하였다. 그러나 그들이 제안하는 방식은 제한된 성능을 가진 스마트 장치에 많은 오버헤드를 발생시킬 수 있다. Cui et al. (2023)은, 제한된 계산능력을 가진 스마트 장치를 고려하여 효율적인 메시지 인증을 위한 엣지 컴퓨팅 기반 일괄 인증 방식을 제안하였다. Cui et al.(2023)은 전송되는 데이터의 기밀성을 보장하기 위해 ECC기반의 암호화 키를 이용하여 데이터를 암호화한다. 그러나 ECC기반의 암호화 키를 생성하는 과정은 제한된 성능을 가진 스마트 장치에 부담이 되는 문제가 여전히 남아있다.

본 논문에서는 스마트 그리드 환경에서 제한된 성능을 가진 스마트 미터의 효율적인 메시지 인증을 위해 일괄 인증 방식을 사용하고 데이터의 기밀성을 보장하기 위해 XOR 연산과 hash 연산을 이용한 암호화키를 이용한 효율적인 블록체인 기반 스마트 미터 인증 방식을 제안한다.

2.2 분산식별자 (decentralized identifier, DID)

분산 식별자 DID는 새로운 유형의 고유 식별자로써, 사용자가 신뢰할 수 있는 기관에 의존하지 않고도 자신의 신원과 주권을 통제할 수 있도록 지원한다. 사용자는 전자서명 등 암호화 폐 증명을 통해 DID의 소유권을 증명할 수 있으며, 분산원장에서 DID를 관리할 수 있다. DID 주체의 데이터는 블록체인에 DID 문서(DID document) 형태로 저장된다. DID 문서는 DID 주체가 자신을 인증하고 주체와 DID 간의 관계를 증명하는 데 사용할 수 있다.

2.3 물리적 복제방지 기술 (physical unclonable function, PUF)

물리적 복제방지 기술 PUF는 집적 회로(IC) 제조의 무작위성과 불확실성으로 인해 중복이 발생할 가능성이 낮아져서 각 IC는 고유하며 완전한 설계가 알려져 있더라도 두 개의 동일한 회로를 생성할 수 없는 특징을 가진다. 사용자가 PUF에 챌린지 c를 입력하면 c에 해당하는 응답 r이 출력되며 PUF에 다른 챌린지 c'가 입력되면 항상 다른 응답이 나온다. 그리고 이 응답은 각 PUF에 따라 다르게 출력된다.

2.4 퍼지 추출기 (fuzzy extractor)

퍼지 추출기는 사용자의 생체정보에서 키 정보를 추출할 수 있고 추출된 키값은 사용자 인증에 사용할 수 있다(Burnett et al., 2007; Lee et al. 2019). 퍼치 추출기의 동작 알고리즘은 (Gen, Rep) 쌍으로 구성된다.

Gen(Generation) 알고리즘은 키 정보를 생성하기 위한 알고리즘으로, 생체 데이터(R)를 입력하여 임의의 문자열인 비밀 키값(smr)과 보조 문자열 데이터(δ)를 출력한다. $\{smr,\delta\} = Gen(R)$.

Rep(Reproduction) 알고리즘은 생체정보(R)와 보조 문자열 데이터(δ)를 입력받고 비밀 키값(smr)을 재현합니다. 동일한 비밀 키값을 복구하려면 입력된 생체정보의 노이즈가 허용 오차 이내여야 합니다. $\{smr\} = Rep(R,\delta)$.

3. 시스템 모델

3.1 시스템 모델

Fig. 1은 스마트 그리드 환경에서의 제안하는 시스템 모델을 나타낸다. 제안하는 시스템 모델

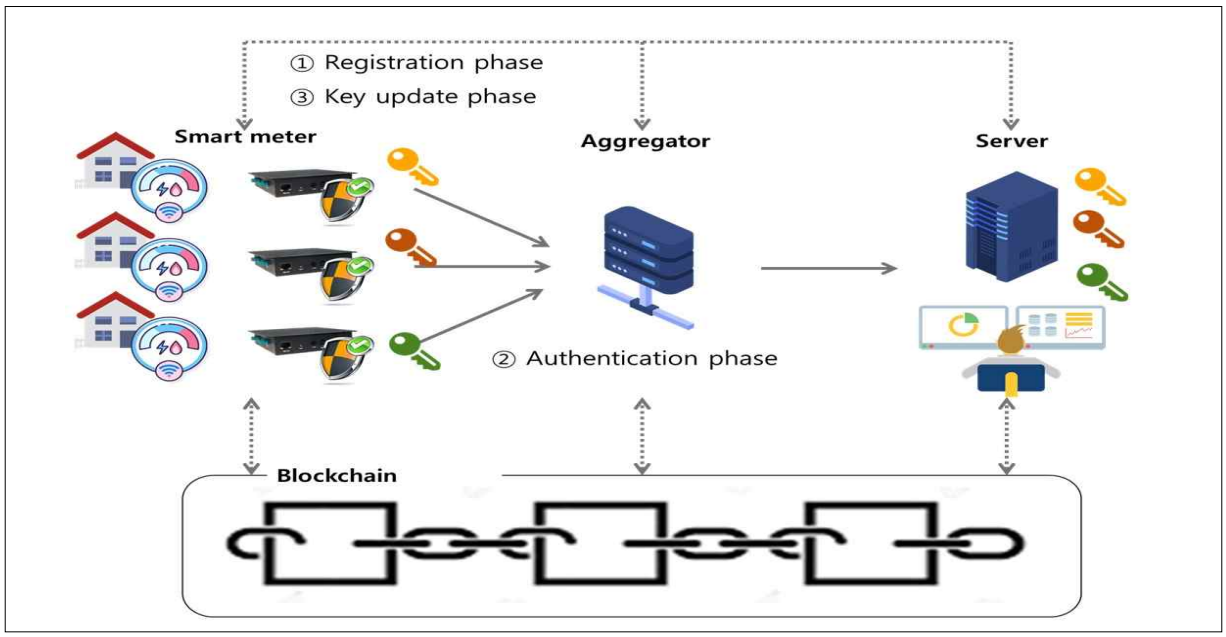

Fig. 1 Proposed System Model

은 서버(server), 어그리게이터(aggregator), 스마트 미터(smart meter), 블록체인(blockchain)으로 구성되며 각 개체의 역할 및 보안적 특성에 대한 정의는 다음과 같다.

- 서버(server): 서버는 스마트 그리드 환경에서 스마트 미터로부터 수집한 데이터를 분석하여 효율적인 전력 배분 등의 서비스를 제공한다. 서버는 완전히 신뢰할 수 있는 개체로써, 시스템의 공개 변수들을 초기화하고, 시스템 노드들의 등록을 책임진다. 서버는 각각의 스마트 미터와 데이터 기밀성을 보장하기 위한 암복호화 키를 공유하며 일정 기간마다 키를 업데이트 한다.
- 어그리게이터(aggregator): 어그리게이터는 엣지 서버로써, 스마트 미터와 서버 사이에 위치하여 서버의 부담을 줄여주기 위해 스마트 미터가 보내온 메시지를 검증한다. 어그리게이터는 효율적인 메시지 검증을 위해 서버가 보내온 스마트 미터 정보와 블록체인에 저장된 각각의 스마트 미터의 정보를 이용하여 스마트 미터들이 보낸 메시지를 일괄 검증한다. 검증이 올바르면 수신받은 메시지들과 함께 서버에게 결과를 전달한다. 어그리게이터는 준시뢰기관으로 시스템의 정상적인 동작을 수행하지만 스마트 미터에서 전송되는 개인정보를 획득하기 위한 시도를 시행할 수 있다.
- 스마트 미터(smart meter): 스마트 미터는 제한된 성능을 가진 IoT 장치로써, 사용자의 정보나 센싱한 정보를 서버에게 전달한다. 스마트 미터는 서버와 공유하는 암호화 키를 사용하여 데이터를 암호화하여 어그리게이터에게 전송한다. 전송되는 데이터는 오직 서버만 복호화 할 수 있다.
- 블록체인(blockchain): 블록체인은 스마트 미터와 어그리게이터의 분산식별자와 이에 대응하는 공개키 정보를 저장하고 있으며, 저장된 정보의 높은 무결성을 제공한다.

Fig. 2는 스마트 그리드 환경에서의 제안하는 시스템 모델의 흐름도를 나타낸다.

3.2 공격자 모델

제안한 방식에서 공격자는 DY공격 모델(Dolev and Yao, 1983)에 따라 다음의 능력을 가진다.

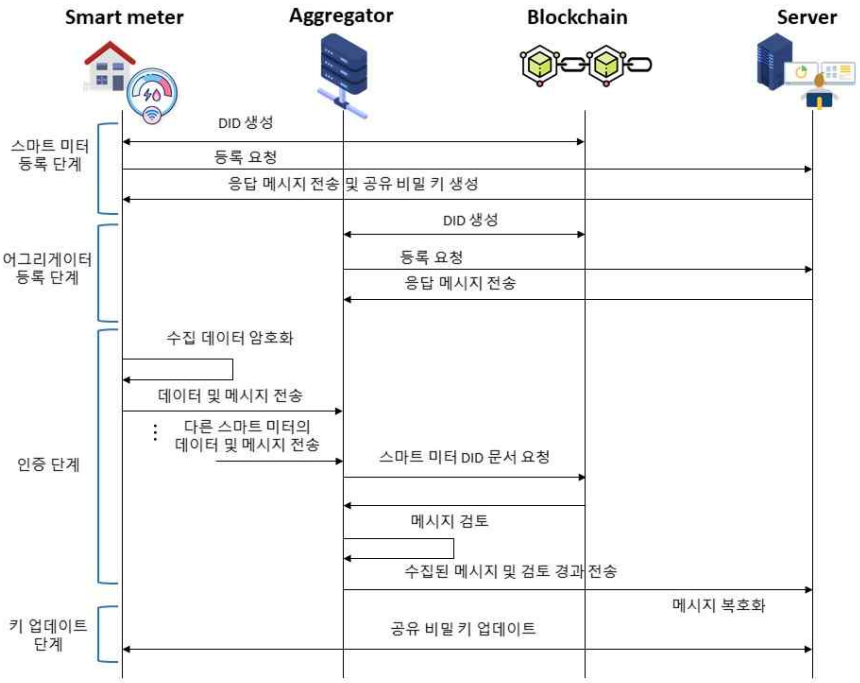

Fig. 2 Proposed System Flow

- 악의적인 공격자는 공개된 무선 통신 채널에서 전송되는 메시지를 도청, 탈취, 수정, 제거 등을 수행할 수 있다.
- 악의적인 공격자는 탈취한 IoT장치에서 Power analysis 분석을 통해 저장된 정보를 추출할 수 있다(Mandal et al. 2020; Kim et al. 2021; Cho et al. 2022).
- 악의적인 공격자는 위장공격, 재전송공격 등을 수행할 수 있다.

4. 제안한 인증 방식

제안하는 스마트 그리드 환경을 위한 블록체인 기반 스마트 미터 인증방식은 1)초기화 단계, 2)등록 단계, 3)인증 단계로 구성된다. 제안하는 인증 방식에서 사용된 시스템 매게 변수는 다음과 같다.

Table 1 System notations

Notation	Description
SM_i	Smart meter
$Sever$	Server
Agg_j	Aggregator
p,q	Large prime numbers
$G,EC(F_p),P$	A additive group, Elliptic curve on field F_p, Generator
sk_x, PK_x	A private key and public key of entity X
ID_i, PW_i	SM_i's identity and password
$h()$	Hash function
$PUF()$	PUF function
$Gen(), Rep()$	Algorithms of fuzzy extractor
T	Timestamp
$\|\|$	Concatenation
$\oplus$	Exclusive-OR operation

4.1 초기화 단계

이 단계는 신뢰할 수 있는 개체인 서버가 시스템 공개 변수를 초기화하는 단계이다. 서버는 개인 키 sk_{TA}와 공개 키 PK_{TA}를 생성하고 시스템 공개 변수 $para = \{p, q, G, P, PK_{TA}, h()\}$를 설정한다.

4.2 등록 단계

제안하는 등록 단계는 스마트 미터 등록단계, 어그리게이터 등록단계로 구성된다.

■ 2단계: SM_i는 $Re_i = PUF(C_i)$, $\{smr_i, \delta_i\} = Gen(Re_i)$, $HID_i = h(ID_i \| \| smr_i)$, $HPW_i = h(ID_i \| \| PW_i \| \| smr_i)$ 를 계산하고 $Server$에게 $\{DID_i, HID_i, C_i\}$를 전송한다.

■ 3단계: $Server$는 DID_i를 확인하고, 임의의 랜덤 값 r_i를 선택한다. 또한, $Server$는 $R_i = r_i \cdot P$, $PHID_i = h(HID_i \| \| r_i)$, $EK_i = h(PHID_i \| \| C_i \| \| R_i \| \| sk_{TA})$, $SI_i = r_i + h(DID_i \| \| PK_{TA} \| \| R_i) \cdot sk_{TA}$를 계산한 후 $\{PHID_i, HID_i, DID_i, R_i, C_i\}$를 안

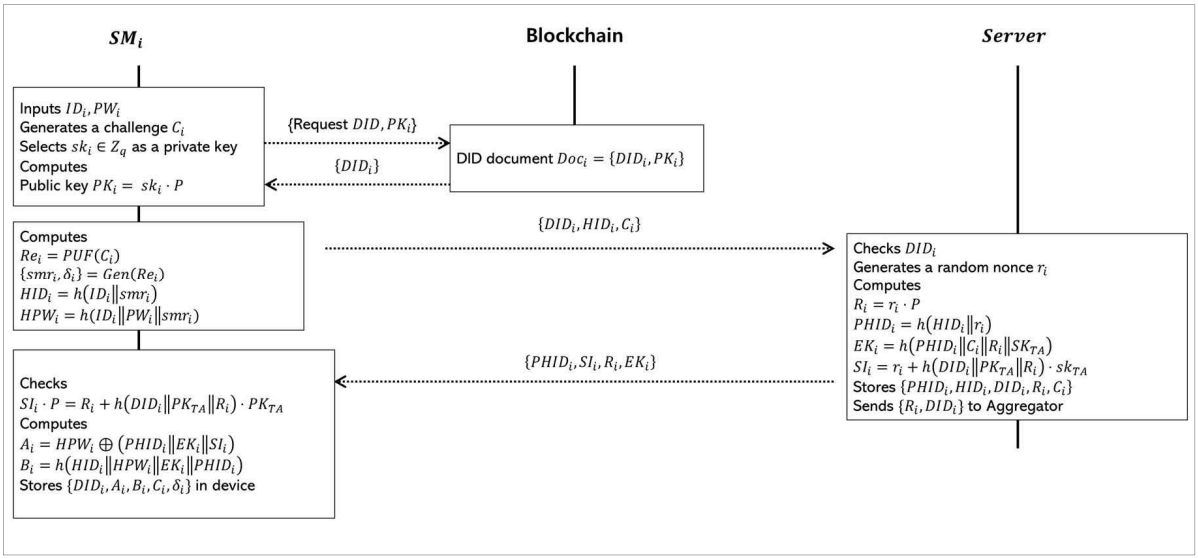

Fig. 3 Smart Meter Registration Phase

4.2.1 스마트 미터 등록 단계

스마트 미터 등록단계는 Fig. 3와 같으며 구체적인 단계는 다음과 같다.

■ 1단계: 스마트 미터SM_i는 ID_i,PW_i, 임의의 챌린지 값 C_i 및 개인 킷값 sk_i을 선택하고 공개 키 값 $PK_i = sk_i \cdot P$를 계산한다. 이후 SM_i은 분산식별자 DID_i를 생성하기 위해 블록체인에 PK_i를 포함한 요청을 보내면 블록체인에서 PK_i 값과 DID_i가 저장된 $Doc_i = \{DID_i, PK_i\}$를 만든 후 DID_i를 반환한다.

전한 데이터베이스에 저장하고, $\{R_i, DID_i\}$를 Agg_j에게 $\{PHID_i, SI_i, R_i, EK_i\}$를 SM_i에게 안전한 통신 채널을 통해 전달한다.

■ 4단계: SM_i는 $SI_i \cdot P = R_i + h(DID_i \| \| PK_{TA} \| \| R_i) \cdot PK_{TA}$를 검증한 후 $A_i = HPW_i \oplus (PHID_i \| \| EK_i \| \| SI_i)$, $B_i = h(HID_i \| \| HPW_i \| \| EK_i \| \| PHID_i)$를 계산하고 $\{DID_i, A_i, B_i, C_i, \delta_i\}$를 메모리에 저장한다.

4.2.2 어그리게이터 등록 단계

제안하는 어그리게이터 등록단계는 Fig. 4과 같으며 구체적인 단계는 다음과 같다.

■ 1단계: Agg_j는 ID_j, 개인 키 sk_{ag}, 임의의 챌린지 값 C_i를 선택하고 공개 키 $PK_j = sk_j \cdot P$를 계산한다. 이후 Agg_j는 분산 식별자 DID_j를 생성하기 위해 블록체인에 PK_j를 포함한 요청을 보내면 블록체인에서 PK_j 값과 DID_j가 저장된 $Doc_j = \{DID_j, PK_j\}$를 만든 후 DID_j를 반환한다.

■ 2단계: Agg_j는 $Re_j = PUF(C_j)$, $\{smr_j, \delta_j\} = Gen(Re_j)$, $HID_j = h(ID_j \| \| smr_j)$를 계산하고 $Server$에게 $\{DID_j, HID_j, C_j\}$를 전송한다.

■ 3단계: $Server$는 DID_j를 확인하고, 임의의 랜덤 값 r_j를 선택한다. 또한, $Server$는 $R_j = r_j \cdot P$, $PHID_j = h(HID_j \| \| r_j)$, $SI_j = r_j + h(DID_j \| \| PHID_j \| \| PK_{TA} \| \| R_j) \cdot sk_{TA}$를 계산한 후 $\{PHID_j, HID_j, DID_j, R_j, C_j\}$를 안전한 데이터베이스에 저장하고, $\{PHID_j, SI_j, R_i\}$를 안전한 통신 채널을 통해 Agg_j에게 전달한다.

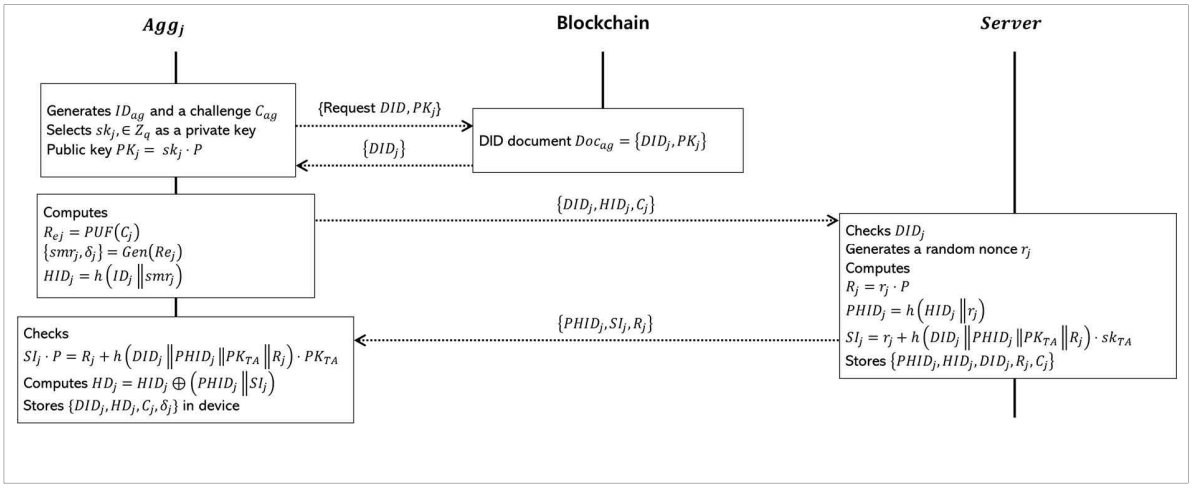

Fig. 4 Aggregator Registration Phase

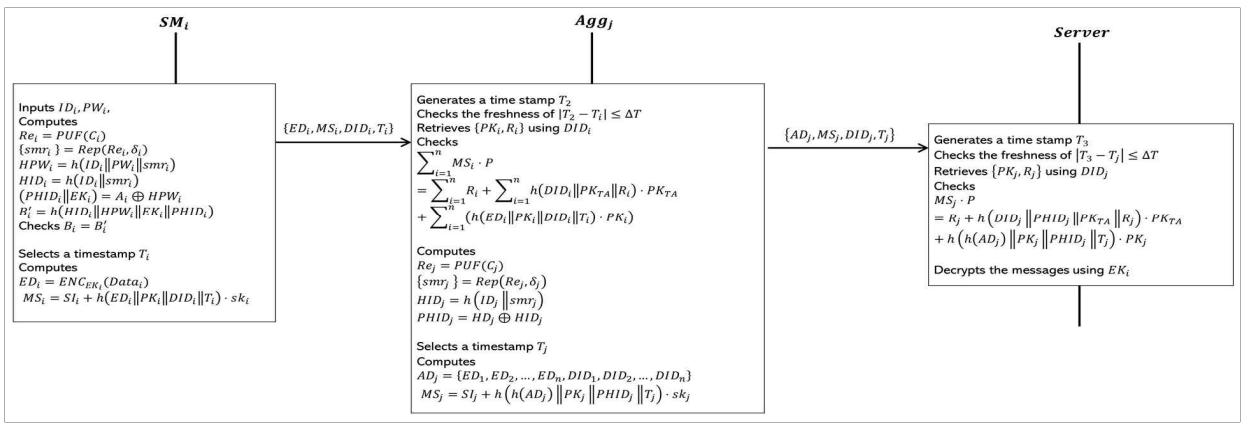

Fig. 5 Authentication Phase

■ 4단계: Agg_j는 $SI_j \cdot P = R_j + h(DID_j \| \| PHID_j \| \| PK_{TA} \| \| R_i) \cdot PK_{TA}$를 검증한 후, $HD_j = HID_j \oplus (PHID_j \| \| SI_j)$를 계산하고 $\{DID_j, HD_j, C_j, \delta_j\}$를 데이터베이스에 저장한다.

4.3 인증 단계

제안하는 인증 단계는 Fig. 5와 같으며 구체적인 단계는 다음과 같다.

■ 1단계: SM_i 사용자가 ID_i, PW_i을 입력하면, SM_i는 $Re_i = PUF(C_i)$, $\{smr_i\} = Rep(Re_i, \delta_i)$, $HPW_i = h(ID_i \| \| PW_i \| \| smr_i)$, $HID_i = h(ID_i \| \| smr_i)$, $(PHID_i \| \| EK_i \| \| SI_i) = A_i \oplus HPW_i$, $B_i' = h(HID_i \| \| HPW_i \| \| EK_i \| \| PHID_i)$를 계산하고 $B_i = B_i'$의 검사하여 합법적인 사용자의 접근을 확인한다.

■ 2단계: SM_i은 현재 타임스탬프 T_i를 생성한 후, 수집한 데이터 $Data_i$를 암호화 키 EK_i를 사용하여 암호화 $ED_i = Enc_{EK_i}(Data_i)$하고 $MS_i = SI_i + h(ED_i \| \| PK_i \| \| DID_i \| \| T_i) \cdot sk_i$를 계산한다. 이후, SM_i는 $\{ED_i, MS_i, DID_i, T_i\}$를 Agg_j에게 전달한다.

■ 3단계: n개의 SM_i로부터 메시지를 수신받은 Agg_j는 각 메시지에서 타임스탬프를 검사한다 $|T_2 - T_i| \leq \Delta T$. 이후, Agg_j는 각각의 DID_i로를 이용하여 블록체인과 데이터베이스에서 DID_i에 대응하는 $\{PK_i, R_i\}$를 가져오고 메시지 일괄 검증을 수행한다.

$$\sum_{i=1}^{n} MS_i \cdot P = \sum_{i=1}^{n} R_i + \sum_{i=1}^{n} h(DID_i \| \| PK_{TA} \| \| R_i)$$

$$\cdot PK_{TA} + \sum_{i=1}^{n} (h(ED_i \| \| PK_i \| \| DID_i \| \| T_i) \cdot PK_i)$$

■ 4단계: 메시지 일괄 검증 이후, Agg_j는 타임스탬프 T_j를 생성하고 $Re_j = PUF(C_j)$, $\{smr_j\} = Rep(Re_j, \delta_j)$, $HID_j = h(ID_j \| \| smr_j)$, $(PHID_j \| \| SI_j) = HD_j \oplus HID_j$, $AD_j = \{ED_1, ED_2, ..., ED_n, DID_1, DID_2, ..., DID_n\}$,

■ $MS_j = SI_j + h(h(AD_j) \| \| PK_j \| \| PHID_j \| \| T_j) \cdot sk_j$

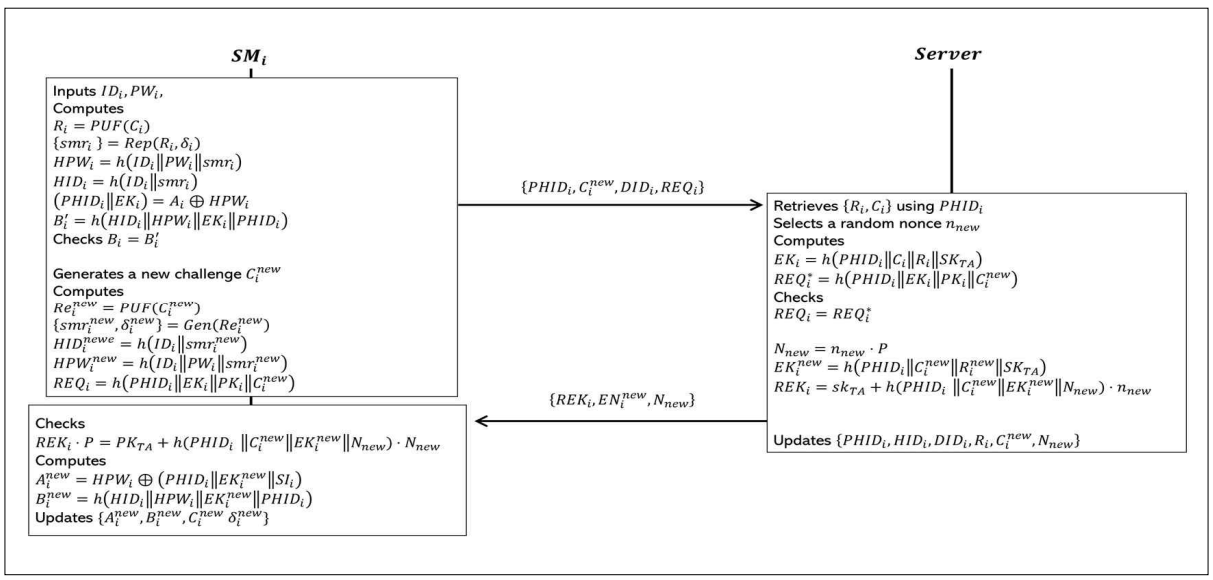

Fig. 6 Key Update Phase

를 계산한다. 이후, $\{AD_j, MS_j, DID_j, T_j\}$를 $Server$에게 전달한다.

- 5단계: $Server$는 메시지의 타임스탬프를 검사하고 $|T_3 - T_{ji}| \leq \Delta T$, DID_j를 이용하여 $\{PK_j, R_j\}$를 가져온다. 이후, $Server$는 메시지 검증을 수행한다.

$$MS_j \cdot P = R_j + h(DID_j \| \| PHID_j \| \| PK_{TA} \| \| R_j)$$

$$\cdot PK_{TA} + h(h(AD_j) \| \| PK_j \| \| PHID_j \| \| T_j) \cdot PK_j$$

메시지 검증 결과가 올바르면, 각 DID_i의 메시지를 EK_i를 이용하여 복호화한다.

4.4 키 업데이트 단계

제안하는 키 업데이트 단계는 Fig. 6와 같으며 구체적인 단계는 다음과 같다.

- 1단계: SM_i 사용자가 ID_i,PW_i을 입력하면, SM_i는 $Re_i = PUF(C_i)$, $\{smr_i\} = Rep(Re_i, \delta_i)$, $HPW_i = h(ID_i \| \| PW_i \| \| smr_i)$, $HID_i = h(ID_i \| \| smr_i)$, $(PHID_i \| \| EK_i) = A_i \oplus HPW_i$, $B_i' = h(HID_i \| \| HPW_i \| \| EK_i \| \| PHID_i)$를 계산하고 $B_i = B_i'$의 검사하여 합법적인 사용자의 접근을 확인한다.
- 2단계: SM_i는 새로운 임의의 챌린지 값 C_i^{new}을 생성한 후 $Re_i^{new} = PUF(C_i^{new})$, $\{smr_i^{new}, \delta_i^{new}\} = Gen(Re_i^{new})$, $HPW_i^{new} = h(ID_i \| \| PW_i \| \| smr_i^{new})$, $HID_i^{new} = h(ID_i \| \| smr_i^{new})$, $REQ_i = h(PHID_i \| \| EK_i \| \| PK_i \| \| C_i^{new})$를 계산하고 $\{PHID_i, C_i^{new}, DID_i, REQ_i\}$를 $Server$에게 전달한다.
- 3단계: $Server$는 $PHID_i$를 이용하여 데이터베이스에서 $\{R_i, C_i\}$를 가져오고 임의의 랜덤 값 n_{new}를 선택한 후, $EK_i = h(PHID_i \| \| C_i \| \| R_i \| \| sk_{TA})$, $REQ_i^* = h(PHID_i \| \| EK_i \| \| PK_i \| \| C_i^{new})$를 계산하고 방정식 $REQ_i = REQ_i^*$를 검사한다. 결과가 올바르면, $Server$는 $N_{new} = n_{new} \cdot P$, $EK_i^{new} = h(PHID_i \| \| C_i^{\neq w} \| \| R_i^{\neq w} \| \| sk_{TA})$, $REK_i = sk_{TA} + h(PHID_i \| \| C_i^{new} \| \| EK_i^{new} \| \| N_{new}) \cdot n_{new}$를 계산한 후, 데이터베이스에 $\{PHID_i, HID_i, DID_i, R_i, C_i^{new}, N_{new}\}$를 업데이트하고 $\{REK_i, EN_i^{new}, N_{new}\}$를 SM_i에게 전달한다.
- 4단계: SM_i은 $REK_i \cdot P = PK_{TA} + h(PHID_i \| \| C_i^{new} \| \| EK_i^{new} \| \| N_{new}) \cdot N_{new}$를 검사하여 메시지를 검증하고 $A_i^{new} = HPW_i \oplus (PHID_i \| \| , EK_i^{new})$, $B_i^{new} = h(HID_i \| \| HPW_i \| \| EK_i^{new} \| \| PHID_i)$를 계산하고 메모리에서 $\{A_i^{new}, B_i^{new}, C_i^{new}, \delta_i^{new}\}$를 업데이트 한다.

5. 보안 분석

5.1 비정형 분석

비정형 분석을 통해 제안한 방식이 악의적인 공격자의 보안 공격으로부터 안전함을 보인다.

5.1.1 IoT장치 탈취 공격

IoT장치 탈취 공격은 Power analysis 분석을 통해 IoT장치에 저장된 데이터를 이용하여 사용자의 정보를 얻으려고 시도하는 공격이다. 공격자는 스마트 미터에 저장된 $\{DID_i, A_i, B_i, C_i, \delta_i\}$를 추출하더라도 실제 사용자의 ID_i, PW_i와 PUF함수를 통해 출력되는 smr_i를 알 수 없기 때문에 SI_i, $PHID_i$와 같은 중요한 값을 계산할 수 없다. 따라서 제안한 방

식은 IoT장치 탈취 공격에 안전하다.

5.1.2 스마트 미터 위장공격

공격자는 Power analysis 분석을 통해 스마트 미터에 저장된 $\{DID_i, A_i, B_i, C_i, \delta_i\}$와 공개된 통신 채널에서 전송되는 $\{ED_i, MS_i, DID_i, T_i\}$, $\{AD_j, MS_j, DID_j, T_j\}$를 획득할 수 있다. 공격자는 합법적인 IoT 장치인 것처럼 위장하기 위해서는 유효한 $\{ED_i, MS_i, DID_i, T_i\}$ 메시지를 만들 수 있어야 한다. 그러나 SI_i는 XOR 연산과 Hash 함수를 이용하여 마스킹 되어 있으며, sk_i는 안전하게 관리되기 때문에 공격자는 유효한 메시지를 만들기 어렵다. 따라서 제안한 방식은 스마트 미터 위장 공격에 안전하다.

5.1.3 어그리게이터 위장 공격

공격자는 합법적인 어그리게이터로 위장공격하기 위해 공개된 통신 채널에서 전송되는 $\{ED_i, MS_i, DID_i, T_i\}$, $\{AD_j, MS_j, DID_j, T_j\}$를 이용하여 유효한 $\{AD_j, MS_j, DID_j, T_j\}$ 메시지를 만들 수 있다. 그러나 SI_j는 PUF함수를 기반한 XOR 연산과 Hash 함수를 이용하여 마스킹 되어 있으며, sk_j는 안전하게 관리되기 때문에 공격자는 유효한 메시지를 만들기 어렵다. 따라서 제안한 방식은 어그리게이터 위장 공격에 안전하다.

5.1.4 재전송 공격

공격자는 과거에 공개된 통신 채널을 통해 전송되는 메시지를 이용하여 현재의 세션에서 다시 재전송하여 중ㅇ요한 정보를 획득하거 인증을 수행할 수 있다. 그러나 세션마다 생성되는 메시지에는 타임스탬프 값 T_x이 포함되어 있고 메시지 수신측에서 타임스탬프의 유효성을 검증하기 때문에 공격자는 이전에 전송되었던 메시지를 재사용할 수 없다. 따라서 제안한 방식은 재전송 공격에 안전하다.

5.1.5 중간자 공격

중간자 공격은 통신하는 개체 사이에서 데이터 도청, 위조 및 변조를 시도하는 공격이다. 제안한 방식에서 공격자는 개인 키 sk_i와 비밀 값 SI_x를 알 수 없으므로 인증 메시지 $\{ED_i, MS_i, DID_i, T_i\}$, $\{AD_j, MS_j, DID_j, T_j\}$를 성공적으로 생성할 수 없다. 따라서 제안한 방식은 중간자 공격에 안전하다.

```
%%%%%%% Role smartmeter %%%%%
role smartmeter(SM,AG,SV: agent, SKsmsv,SKagsv,SKsmag: symmetric_key, H,ADD,MUL:
hash_func, SND, RCV : channel(dy))
played_by SM
def=
local State: nat,
      IDi,PWi,DIDi,CHAi,REi,SKi,PKi,SMRi,HIDi,HPWi,RRi,Ri,PHIDi,EKi,SIi,Ai,Bi,Ti,EDi,DATAi:t
ext,
      MSi,P,SKta,PKta,SKj,PKj,IDj,DIDj,CHAj,REj,SMRj,HIDj,RRj,Rj,PHIDj,SIj,HDj,MSj,Tj:  text

      const sp1,sp2,sp3,sp4,sp5,ag_sv_rj,sm_ag_ri: protocol_id
init State:=0
transition

%%%%% Registration phase %%%%%%%
1. State=0 /\RCV(start)=|>
State':=1 /\CHAi':=new()
      /\SMRi':=new()
      /\HIDi':=H(IDi.SMRi')
      /\HPWi':=H(IDi.PWi.SMRi')
      /\SND{{DIDi.HIDi'.CHAi'}_SKsmsv)
      /\secret{{HIDi'.CHAi'},sp1,{SM,SV}}
      /\secret{{SMRi'},sp2,{SM}}


2. State=1
/\RCV({H(H(IDi.SMRi').Ri').ADD(Ri'.MUL(H(DIDi.MUL(SKta.P).MUL(Ri'.P)).SKta)).MUL(Ri'.P
).H(H(H(IDi.SMRi').Ri').CHAi'.MUL(Ri'.P).SKta)}_SKsmsv)=|>
State':=2
      /\Ai':=xor(HPWi,(H(H(IDi.SMRi').Ri').H(H(H(IDi.SMRi').Ri').CHAi'.MUL(Ri'.P).SKta)))%
is it need?

%%%%% authentication phase %%%%%%%
      /\Ti':=new() /\DATAi':=new()
/\EDi':=xor(DATAi',H(H(H(IDi.SMRi').Ri').CHAi'.MUL(Ri'.P).SKta))
      /\MSi':=ADD(ADD(Ri'.MUL(H(DIDi.MUL(SKta.P).MUL(Ri'.P)).SKta)).MUL(H(EDi'.PKi.DI
Di.Ti').SKi))
      /\SND(EDi'.MSi'.DIDi.Ti')
      /\witness(SM,AG,sm_ag_ri,Ri')%Ri(by server)? or ski?

end role
```

Fig. 7 Role of the Smart Meter in AVISPA

5.1.6 데이터 기밀성 및 무결성

제안한 방식에서 스마트 미터에서 전송하는 데이터의 기밀성을 보장하기 위해 스마트 미터는 데이터를 서버와 공유하는 대칭 키 EK_i로 암호화한다. 암호화된 데이터는 데이터를 이용하는 서버만이 EK_i를 이용하여 복호화할 수 있다. 뿐만 아니라 전송되는 데이터는 Hash 함수를 이용하여 메시지 검증을 통해 데이터의 무결성을 보장할 수 있다. 따라서 제안한 방식은 데이터 기밀성 및 무결성을 보장한다.

5.2 AVISPA 시뮬레이션

AVISPA는 설계한 인증 프로토콜의 재전송공

```
%%%%%%%%%  session  %%%%%%%
role session(SM,AG,SV: agent, SKsmsv,SKagsv,SKsmag :symmetric_key, H,ADD,MUL:
hash_func)

def=
local SN1, SN2, SN3, RC1, RC2, RC3: channel(dy)
composition
smartmeter(SM,AG,SV,SKsmsv,SKagsv,SKsmag,H,ADD,MUL,SN1,RC1)
/\aggregator(SM,AG,SV,SKsmsv,SKagsv,SKsmag,H,ADD,MUL,SN2,RC2)
/\server(SM,AG,SV,SKsmsv,SKagsv,SKsmag,H,ADD,MUL,SN3,RC3)

end role

%%%%%  environments and goals  %%%%%%%
role environment()

def=
const sm, ag, sv : agent,
      sksmsv,skagsv,sksmag: symmetric_key,
      h,add,mul: hash_func,
      idi,idj: text,
      ag_sv_rj,sm_ag_ri: protocol_id,
      sp1,sp2,sp3,sp4,sp5: protocol_id

intruder_knowledge = {sm,ag,sv,idi,idj,h,add,mul}%intruder knows the information in
MDs
composition
session(sm,ag,sv,sksmsv,skagsv,sksmag,h,add,mul)
/\session(i,ag,sv,sksmsv,skagsv,sksmag,h,add,mul)
/\session(sm,i,sv,sksmsv,skagsv,sksmag,h,add,mul)
/\session(sm,ag,i,sksmsv,skagsv,sksmag,h,add,mul)
end role

goal
secrecy_of sp1,sp2,sp3,sp4,sp5
authentication_on ag_sv_rj
authentication_on sm_ag_ri
end goal

environment()
```

Fig. 8 The Session, Goals and Environments in AVISPA

격과 중간자 공격에 안전함을 분석하는데 널리 사용되는 보안 시뮬레이션 툴이다(Park et al. 2019; Jangirala et al., 2020; Yu et al., 2020). AVISPA 시뮬레이션을 사용하여 제안한 방식이 안전성을 확인한다. Fig. 7은 HLPSL언어 기반의 스마트 미터의 역할을 정의한 AVISPA 코드를 나타낸다. 작성된 코드는 State 0에서 스마트 미터는 등록을 위한 메시지를 만들어 서버에 등록요청을 하고 State 1에서 서버로부터 응답 메시지를 받는다. State 2에서 어그리게이터로 메시지를 보내는 것으로 구성되어 있다. 또한, 어그리게이터와 서버의 코드는 스마트 미터와 유사하다. Fig. 8은 프로토콜의 세션, 악의적인 공격자에 대한 설정을 표기한 환경 및 보안 목표가 정의된 코드이다. Fig. 9은 AVISPA 시뮬레이션 결과를 나타내며, “SAFE”를 통해 제안한 인증방식이 재전송 공격과 중간자 공격에 안전함을 보인다.

```
SUMMARY
  SAFE

DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
  TYPED_MODEL

PROTOCOL
  /home/span/span/testsuite/results/code2.if

GOAL
  As Specified

BACKEND
  CL-AtSe

STATISTICS

  Analysed  : 0 states
  Reachable  : 0 states
  Translation: 0.11 seconds
  Computation: 0.00 seconds
```

```
% OFMC
% Version of 2006/02/13
SUMMARY
  SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL

/home/span/span/testsuite/results/code2.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 11.86s
  visitedNodes: 1040 nodes
  depth: 9 plies
```

Fig. 9 The Result of AVISPA Simulation

6. 성능 분석

제안한 방식과 관련 연구들의 메시지 인증단계의 성능 분석을 통해 제안한 방식이 관련 연구들(Xiong et al., 2020; Cui et al., 2021; Cui et al., 2023)과 비교하여 효율적인 방식임을 보인다.

Table 2 Computation Comparison

Scheme	Message Generation	Batch Verification
Xiong et al.	$T_{sm}+T_{am}$ $+2T_{mm}+2T_h$ ≈ 1.5354[ms]	$(3n+1)T_{sm}$ $+2nT_{am}$ $+nT_{mm}+2nT_h$ $\approx 1.4658+$ $4.4415n$[ms]
Cui et al.(2021)	$12T_{sm}+7T_{am}$ $+5T_{mm}+T_h$ $+3T_p$ ≈ 51.5178[ms]	$12nT_{sm}+nT_h$ $+5nT_p$ $\approx 73.8077n$ [ms]
Cui et al.(2023)	$2T_{sm}+T_{am}$ $+2T_{mm}+4T_h$ ≈ 3.0024[ms]	$(2n+1)T_{sm}$ $+4T_a+2nT_{mm}$ $+2nT_h$ ≈ 1.489 $+2.9954n$[ms]
Our scheme	$T_{am}+T_{mm}$ $+4T_h$ ≈ 0.0395 [ms]	$(n+2)T_{sm}$ $+3T_{am}+2nT_h$ ≈ 2.949 $+1.467n$ [ms]

6.1 계산량 분석

계산량 분석을 위한 실험 환경 및 각 연산자의 계산량은 Xiong et al.(2020) 방식을 이용한다. 계산에 사용된 함수 ECC multiplication (T_{sm}), ECC point addtion(T_{am}), modular multiplication(T_{mm}), hash(T_h)의 동작시간은 1.4658ms, 0.0058ms, 0.0313ms, 0.0006ms이다. 제안한 방식과 관련 논문들의 계산량 분석은 Table 2과 같다. 제안한 방식은 메시지를 생성하는 IoT기기 단에서 계산량이 높은 ECC multiplication 사용하지 않음으로써 관련 논문들과 비교하여 매우 효율적임을 확인할 수 있다.

6.2 통신량 분석

제안한 방식과 관련 연구와의 통신량 비교 분석을 위해 아이디, 임의의 난수, 타임스탬프, 해시값, 그룹 G요소의 비트 크기를 128, 160, 32, 256, 1024 bits로 설정한다. 제안한 방식과 관련 논문들의 통신량 분석은 Table 3과 같다. 제안한 방식은 IoT기기 단에서 전송하는 메시지에서 타원곡선상의 좌표정보를 포함하지 않음으로써 관련 논문들과 비교하여 매우 효율적임을 확인할 수 있다.

Table 3 Communication Comparison

Scheme	Costs
Xiong et al.	2848 bits
Cui et al.(2021)	3616 bits
Cui et al.(2023)	5408 bits
Our scheme	1744 bits

7. 결 론

스마트 그리드는 효율적인 에너지 생산과 소비, 관리를 지원해주는 전력망 시스템으로 다양한 분야와 산업에서 활용되고 있다. 그러나 공개된 네트워크를 통해 서비스가 제공되는 환경에서는 보안 취약점과 개인정보 침해에 대한 신뢰 문제 해결은 필수적이며 탈중앙 분산원장 기술인 블록체인을 활용한 스마트 미터 인증체계 및 방법을 제안하였다. 제안된 방법은 블록체인을 통한 개별 스마트 미터 단말의 고유한 분산식별자(DID) 발급과 물리적 복제방지 기술(PUF)을 기반한 난수 값을 사용하여 탈중앙화된 인증방식과 데이터의 무결성및 기밀성을 보장한다. 또한 비정형 보안 분석 및 AVISPA 시뮬레이션을 이용하여 제안한 방식의 안전성을 분석하고 관련 연구들과 비교하여 제안한 방식이 효율적인 방식임을 확인하였다.

References

Alsuwian, T., Butt, A. S. and Amin, A. A. (2022) Smart Grid Cyber Security Enhancement: Challenges and Solutions-A Review, *Sustainability*, 14(21), 14226.

Barai, G. R., Krishnan, S. and Venkatesh., B. (2015) Smart Metering and Functionalities of Smart Meters in Smart Grid - A Review, *2015 IEEE Electrical Power and Energy Conference (EPEC)*, Oct. 26-28, London, ON, Canada.

Burnett, A., Byrne, F., Dowling, T. and Duffy, A. (2007) A Biometric Identity based Signature Scheme, *International Journal of Network Security*, 5(3), 317-326.

Cho, Y., Oh, J., Kwon, D., Son, S., Lee, J. and Park, Y. (2022) A Secure and Anonymous User Authentication Scheme for IoT-Enabled Smart Home Environments Using PUF, *IEEE Access*, 10, 101330-101346.

Cui, J., Wang, F., Zhang, Q., Xu, Y. and Zhong, H. (2021) Anonymous Message Authentication Scheme for Semitrusted Edge-Enabled IIoT, *IEEE Transactions on Industrial Electronics*, 68(12), 12921-12929.

Cui, J., Wang, F., Zhang, Q., Gu, C. and Zhoong, H. (2023) Efficient Batch Authentication Scheme Based on Edge Computing in IIoT, *IEEE Transactions on Network and Service*

Management, 20(1), 357-368.

Dolev, D. and Yao, A. C. (1983) On the Security of Public Key Protocols, *IEEE Transactions on Information Theory*, 29(2), 198-208.

Gao, Y., Sarawi, S. F. AI. and Abbott, D. (2020) Physical Unclonable Functions, *Nature Electronics*, 3, 81-91.

Islam, S. N., Baig, Z. and Zeadally, S. (2019) Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures, *IEEE Transactions on Industrial Informatics,* 15(12), 6522-6530.

Jangirala, S., Das, A. K. and Vasilakos, A. V. (2020)Designing Secure Lightweight Blockchain-Enabled RFID-Based Authentication Protocol for Supply Chains in 5G Mobile Edge Computing Environment, *IEEE Transactions on Industrial Informatics*, 16(11), 7081-7093.

Kim, M., Lee, J., Park, K., Park, Y., Park, K. and Park, Y. (2021) Design of Secure Decentralized Car-Sharing System Using Blockchain, *IEEE Access*, 9, 54796-54810.

Lee, J., Yu, S., Park, K., Park, Y. and Park, Y. (2019) Secure Three-Factor Authentication Protocol for Multi-Gateway IoT Environments, *Sensors*, 19(10), 2358.

Lee, S. and Kim, K. (2016) Device Authentication in Smart Grid System using Blockchain, *Conference on Information Security and Cryptography-Winter 2016*, Dec. 03, Seoul, Korea.

Mandal, S., Bera, B., Sutrala, A. K., Das, A. K. Choo, K. K. R., Park, Y. (2020) Certificateless-Signcryption-BasedThree-Factor User Access Control Scheme for IoT Environment, *IEEE Internet of Things Journal*, 7(4), 3184-3197.

Mirzaee, P. H., Shojafar, M., Cruickshank, H. and Tafazolli, R. (2022) Smart Grid Security and Privacy: From Conventional to Machine Learning Issues (Threats and Countermeasures), *IEEE access,* 10, 52922-52954.

Odelu, V., Das, A. K., Wazid, M. and Conti, M. (2018) Provably Secure Authenticated Key Agreement Scheme for Smart Grid, *IEEE Transactions on Smart Grid*, 9(3), 1900-1910.

Park, K., Park, Y., Das, A. K., Yu, S., Lee, J. and Park, Y. (2019) A Dynamic Privacy-Preserving Key Management Protocol for V2G in Social Internet of Things, *IEEE Access*, 7, 76812-76832.

Park, Y. H., Park, Y. H. and Moon, S. J. (2011) Security Improvement of ID-based Multiple Key Management Scheme for Scalable Ad Hoc Networks, *Journal of the Korea Industrial Information Systems Research*, 16(2), 13-18.

Park, Y. H. and Park, Y. H. (2015) Secure and Scalable Key Aggregation Scheme for Cloud Storage, *Journal of the Korea Industrial Information Systems Research*, 20(2), 11-18.

Paul, S., Rabbani, M. S., Kundu, R. K. and Zama, S. M. R. (2014) A Review of Smart Technology (Smart Grid) and Its Features, *2014 1st International Conference on Non Conventional Energy (ICONCE 2014)*, Jan. 16-17, Kalyani, India, pp. 200-203.

Sureshkumar, V., Anandhi, S., Amin, R. and Madhumathi, R. (2021) Design of Robust Mutual Authentication and Key Establishment Security Protocol for Cloud-Enabled Smart Grid Communication, *IEEE Systems Journal* 15(3), 3565-3572.

Yu, S., Park, K., Lee, J., Park, Y., Park, Y., Lee, S. and Chung, B. (2020) Privacy-Preserving Lightweight Authentication Protocol for Demand Response Management in Smart Grid Environment, *Applied Sciences*, 10(5), 1758.

Xiong, H., Wu, Y. Su, C. and Yeh, K. H. (2020) A Secure and Efficient Certificateless Batch Verification Scheme with Invalid

Signature Identification for The Internet of Things, *Journal of Information Security and Applications*, 53, 102507.

World Wide Web Consortium (W3C) (2022) Decentralized Identifiers (DIDs) v1.0 Core Architecture, Data Model, and Representations, https://www.w3.org/TR/did-core/(Accessed on Sep. 1st, 2023)

Zhang, H., Wang, J. and Ding, Y. (2019) Blockchain-based Decentralized and Secure Keyless Signature Scheme for Smart Grid, *Energy*, 180, 955-967.

김 종 현 (Jonghyun Kim)

- 계명대학교 경영정보학과 학사
- 계명대학교 경영정보학과 석사
- 경북대학교 정보보호학과 박사 수료
- (현재) ㈜루트랩 대표 총괄관리
- 관심분야: 정보보호, 블록체인, 사물인터넷

김 명 현 (Myeonghyun Kim)

- 경북대학교 전자공학부 공학사
- 경북대학교 전자공학부 공학 석사
- (현재) 경북대학교 전자전기 공학부 박사 수료
- 관심분야: 정보보호, 블록체인, 인증, 사물인터넷, 차량보안

박 영 호 (Youngho Park)

- 경북대학교 전자공학과 공학사
- 경북대학교 전자공학과 공학 석사
- 경북대학교 전자공학과 공학 박사
- (현재) 경북대학교 전자전기 공학부 교수
- 관심분야: 정보보호, 블록체인, 인증, 사물인터넷, 차량보안, 빅데이터