https://doi.org/10.33778/kcsa.2022.22.1.071

스마트 그리드 기반 엣지 컴퓨팅 환경에서 블록체인을 이용한 사용자 인증 기법

이 학 준*, 이 영 숙**

요 약

정보기술과 전력 공급 시스템을 결합하여 전력 공급자와 소비자 간의 실시간 정보 교환을 통해 에너지 효율을 극대화하는 스마트 그리드 시스템이 등장했다. 중앙 클라우드 서버와 스마트 그리드 IoT 기기 사이에서 전력 관련 정보 수집 및 데이터 저장 처리하는 엣지 서버를 활용하여 스마트 그리드 시스템을 위한 블록체인 기반의 사용자 인증 기법이 제안되고 있다. 최근, 스마트 그리드 환경에서 보안을 강화하기 위해 인증 방식이 제안되고 있지만 여전히 많은 취약점이 보고되고 있다. 본 논문은 블록체인을 이용한 엣지 컴퓨팅 기반의 스마트 그리드에서 사용자의 프라이버시와 익명성을 보장하기 위한 새로운 상호 인증 기법을 제시한다. 제안된 방식에서는 키 자료 업데이트 및 폐기와 같은 키 관리의 효율성을 위해 스마트 계약을 사용합니다. 마지막으로 제안하는 기법이 사용자의 스마트 그리드-IoT 기기와 에지 서버 간의 세션 키를 안전하게 설정함과 동시에 익명성을 보장함을 증명한다.

A User Authentication Scheme using Blockchain in Smart Grid-based Edge Computing Environments

Hakjun Lee*, Youngsook Lee**

ABSTRACT

The smart grid system has emerged to maximize energy efficiency through real-time information exchange between power providers and consumers by combining information technology and power supply systems. The authentication schemes using blockchain in a smart grid system have been proposed, which utilize an edge server's architecture to collect and store electric power-related information and process data between a central cloud server and smart grid-IoT devices. Although authentication schemes are being proposed to enhance security in the smart grid environment, many vulnerabilities are still reported. This paper presents a new mutual authentication scheme to guarantee users' privacy and anonymity in a smart grid based on edge computing using blockchain. In the proposed scheme, we use the smart contract for the key management's efficiency, such as updating and discarding key materials. Finally, we prove that the proposed scheme not only securely establishes a session key between the smart grid-IoT device of the user and the edge server but also guarantees anonymity.

Key words : Smart Grid, Smart Contract, Blockchain, User Authentication

접수일(2022년0 2월 15일), 게재확정일(2022년 3월 29일)

* 호원대학교 IT소프트웨어보안학과(주저자)

** 호원대학교 IT소프트웨어보안학과(교신저자)

1. 서 론

정보통신기술과 전력 공급 시스템을 결합하여 전력 공급자와 소비자 간의 실시간 정보 교환을 통해 에너지 효율을 극대화하는 스마트 그리드 시스템이 등장했다. 인터넷과 연결된 전력공급시스템 기기를 활용하여 지능형 전력 수요 관리, 신재생 에너지, 전기차 충전 등이 가능해졌으며 스마트 그리드 시스템을 다양한 산업과 융·복합하여 신 비즈니스 모델 창출이 가능해졌다[1, 2].

스마트 그리드 시스템과 클라우드 기반 엣지 컴퓨팅(Edge Computing) 기술을 결합하는 연구가 진행되고 있다. 이를 통해 품질, 신뢰성, 에너지 전송의 유연성 향상과 스마트 그리드 전용 사물인터넷(IoT) 기기의 이기종성, 이동성, 지리적 분산성을 극복하고 기기 관리의 효율성을 높여 노드 간의 통신 지연(Latency)을 줄일 수 있다[3].

최근에는 중앙 클라우드 서버와 스마트 그리드 IoT 기기 사이에서 전력 관련 정보 수집 및 데이터 저장·처리하는 엣지 서버를 활용하여 스마트 그리드 시스템을 위한 블록체인 기반의 사용자 인증 기법이 제안되고 있다[4, 5]. 사용자 인증 기법을 통해 스마트 미터 같은 스마트 그리드 IoT 기기와 엣지 서버 간의 세션키를 수립한다. 세션키는 사용자의 신분, 전력량, 전력 요금 등 사용자의 민감한 정보를 숨기고 상호 보안 통신을 위해 사용된다.

공개키 기반 인증 시스템은 인증서를 발급, 폐기, 서명, 검증하는 과정에서 오버헤드가 크기 때문에 제한적인 시스템 자원을 지닌 IoT 기기 기반 네트워크 환경에서는 적합하지 않다. 최근에는 사용자의 신원 및 키 생성 관련 파라미터와 같은 민감한 정보를 암호화하여 블록체인에 안전하게 저장하고, 키 생성 과정을 스마트 컨트랙트(Smart Contract)와 연계한 사용자 인증 기법이 제안되고 있다[6, 7].

이렇게 스마트 그리드 환경에서 보안성을 강화하기 위한 인증 기법들이 제안되고 있음에도 불구하고, 여전히 사용자 프라이버시를 위협하는 취약점들이 보고되고 있다. 본 논문에서는 이러한 문제점을 보완하기 위해 블록체인을 이용하는 엣지 컴퓨팅 기반 스마트 그리드 환경에서 사용자의 프라이버시와 익명성을 보장하는 사용자 인증 기법을 제안한다. 제안하는 기법에서 사용되는 키 생성 관련 파라미터 생성, 갱신, 폐기 등의 키 관리 과정은 스마트 컨트랙트를 통해 동작한다. 그런 다음, 제안하는 기법에서 사용자 전력 기기와 엣지 서버는 상호적으로 안전한 세션키를 수립함과 동시의 익명성을 보장한다는 것을 보여줌으로써 제안하는 기법의 보안성을 증명한다.

본 논문의 구성은 다음과 같다. 2장에서 기존 스마트 그리드 환경을 위한 인증 기법의 문제점과 배경 및 관련 지식에 대해 설명한다. 3장에서는 제안하는 인증 기법에 대해 설명한다. 4장에서는 제안하는 기법의 안전성과 성능을 분석하고 5장에서 결론을 맺는다.

2. 관련연구

2.1 기존 연구의 문제점

최근 다양한 네트워크 환경에서 사용자 인증 기법들이 제안되고 있으며[8, 9], 스마트 그리드 환경에서도 사용자의 프라이버시를 보호하기 위해 많은 연구가 진행되고 있다.

2015년, Tsai와 Lo는 Bilinear Pairing을 사용하여 스마트 미터와 전력 공급자 간의 익명 접근 서비스 제공을 위한 키 교환 기법을 제안했다[10]. 하지만, 이 인증 기법에서는 공격자가 스마트 미터의 비밀키를 추출하여 사용자의 개인정보를 침해할 수 있다는 것이 밝혀졌다[11]. 2017년, Wazid 등은 스마트 미터의 익명성을 보장하고 패스워드 및 생체정보를 동적 업데이트할 수 있는 경량 사용자 인증 기법을 제안했다[12]. 하지만, 이 인증 기법은 악의적이거나 오동작하는 스마트 미터를 네트워크에서 제외하는 폐기 과정을 지원하지 않는다. 2018년, Mahmood 등은 엣지 컴퓨팅 기반 스마트 그리드 환경에서 익명성을 보장을 위한 키 교환 프로토콜을 제안했다[13]. 하지만, Liang

등은 Mahmood 등의 프로토콜에서 공격자가 스마트 미터의 비밀키를 유출하여 정당한 사용자처럼 가장할 수 있다는 것을 보고했다[14].

최근, Wang 등은 스마트 미터의 비밀키 유출을 방지하고 키 관리의 효율성을 높이기 위해 블록체인 적용하여 엣지 컴퓨팅 기반 스마트 그리드 환경에서의 상호 인증 기법을 제안했다[6]. 하지만, 이 기법에서 공격자는 부채널 공격(Side-channel attack)을 통해 스마트 기기에 저장된 비밀키를 추출하고 사용자 가장 공격에 성공할 수 있다. 이뿐만 아니라 엣지 서버의 ID가 보호되지 않아 공격자는 블록체인에 저장된 엣지 서버의 키 관련 정보들을 손쉽게 변경할 수 있다.

스마트 그리드 환경에 블록체인 및 엣지 컴퓨팅 기술이 도입된 환경을 위해 새로운 인증 기법이 계속해서 제안되고 있지만, 이에 대한 취약점 역시 계속해서 보고되고 있다. 이러한 문제점을 보완하고 보안성을 강화한 인증 기법이 필요한 실정이다. 따라서, 본 논문에서는 Wang 등이 제안한 스마트 그리드 환경을 기반으로 스마트 미터와 엣지 서버의 익명성을 보장하고 안전한 키 세션키 수립을 할 수 있는 새로운 인증 기법을 제안한다.

2.2 Bilinear Pairing

G_1을 위수(Order)가 소수(Prime) q인 덧셈군(Additive Group)이라 두고 G_2를 동일한 위수 q의 곱셋군(Multiplicative Group)이라 할 때 $e: G_1 \times G_1 \rightarrow G_2$는 다음과 같은 성질을 만족하면 Bilinear Pairing이라고 한다.

① Bilinearity : 생성자(Generator) $P_1, P_2 \in G_1$와 $\forall x, y \in Z_q^*$에 대해, $e(xP_1, yP_2) = e(P_1, P_2)^{xy}$이다.

② Non-degeneracy : $e(P_1, P_2) \neq 1$을 만족하는 $P_1, P_2 \in G_1$가 존재한다.

③ Computablity : 모든 $P_1, P_2 \in G_1$에 대하여 $e(P_1, P_2)$를 효율적으로 계산할 수 있다.

본 논문에서는 타원곡선 상에서 P, xP, yP이 주어졌을 때 xyP를 계산하는 ECDH(Elliptic Curve Diffie-Hellman)문제를 기반으로, 제 3자간 상호 인증을 위하여 $P \in G_1$과 $x, y \in Z_q^*$인 P, xP, yP가 주어졌을 때 $e(P, P)^{xy}$를 계산하는 BDH(Bilinear Diffie-Hellman Problem) 문제를 사용한다[15].

2.3 네트워크 모델

본 논문에서 소개하는 스마트 그리드 네트워크 환경에는 등록 기관(Register Authority, RA), 스마트 미터 (Smart Meter, SM), 엣지 서버(Edge Server, ES)로 구성된다.

① *RA*: *RA*는 전력 공급자이며 모든 스마트 그리드 시스템 참가자의 신뢰기관이다. *RA*는 스마트 컨트랙트를 사용하여 *SM*의 ID, 키 갱신 및 폐기 등 네트워크 참가자를 관리할 수 있는 권한 갖는다.

② *SM*: *SM*은 사용자의 에너지 소비량 같은 전력 관련 정보를 *ES*에게 보고한다. 일반적으로 *SM*은 지리적으로 가장 가까운 *ES*와 연결된다.

③ *ES*: *ES*는 *SM*으로부터 정보를 수집할 뿐만 아니라 제어를 할 수도 있다. 데이터 저장 및 처리를 담당하는 중앙 클라우드 서버와 연결되어 있으며, *SM*과의 인증을 수행하기 위해 블록체인 네트워크에도 연결되어 있다.

2.4 스마트 컨트랙트

블록체인상에서 키 생성을 위한 정보들을 관리한다. 블록체인에 기록되는 정보들은 사용자에게 키를 발급, 갱신, 폐기를 위하여 사용되며 이러한 과정은 스마트 컨트랙트를 통해 수행된다. 스마트 컨트랙트 알고리즘은 키 관련 정보 테이블을 관리하는 작업을 수행할 때 호출된다. 블록체인을 기반으로 키 관련 정보들을 관리하기 때문에 통신 참가자들의 익명성을 보호하고 효율적으로 비동기 문제들을 방지할 수 있다. 본 논문에서 제안하는 기법은 (그림 1)에 설명된 스마트 컨트랙트 알고리즘을 사용한다.

Algorithm 1: KMT_Initialization

```
1.  contract KMT{
2.    address owner
3.    struct KMTS {
4.      bytes32 HID;
5.      bytes32 EID;
6.      DataTime ET; }
7.    KMTS[ ] public KMT; {
8.    constructor KMT() {
9.      owner=msg.sender;
10.      len=0;
11.      return 1; }
12.  }
```

(a)

Algorithm 2: KMT_Update

```
1.  function update KMT(oldHID, HID, EID, ET){
2.    if owner≠msg.sender then
3.      return 0
4.    else {
5.      if Exist(KMTS[i].HID == oldHID) then
6.        KMTS[i].HID=HID;
7.        KMTS[i].EID=EID;
8.        KMTS[i].ET=ET;
9.        return 1; }
10.     else {
11.       len++;
12.       KMTS[len].HID=HID;
13.       KMTS[len].EID=EID;
14.       KMTS[len].ET=ET;
15.     return 1; }
16.  }
```

(b)

Algorithm 3: KMT_Query

```
1.  function query KMT(HID){
2.    if Exist(KMTS[i].HID == HID) then
3.      return KMTS;
4.    else;
5.      return 0;
6.  }
```

(c)

Algorithm 4: KMT_Revoke

```
1.  function revoke KMT(HID){
2.    if owner≠msg.sender then
3.      return 0 ;
4.    else {
5.      if Exist(KMTS[i].HID == HID) then
6.        for; i<len; i++;
7.          KMTS[i]=KMTS[i+1];
8.        len−;
9.        return 1; }
10.     else {
11.       return 0; }
12.  }
```

(d)

(그림 1) Algorithm of smart contract used in the proposed scheme. (a) Key material initialization, (b) Key material update, (c) Query for key material and (d) Revocation of key material

3. 제안 기법

본 장에서는 블록체인을 이용한 엣지 컴퓨팅이 적용된 스마트 그리드 환경에서 세션키를 안전하게 생성하기 위한 새로운 인증 기법을 제안한다. 제안되는 인증 기법은 Wang 등이 제안한 인증 기법과 동일한 방식으로 등록, 인증, 갱신 및 폐기 단계 등 3단계로 구성된다. 아래 (그림 2)는 제안한 기법 중 인증 단계를 나타낸다.

3.1 Systen Setup

시스템 설정 과정에서 RA는 자신의 비밀키와 공개 파라미터를 생성하기 위해 다음과 같은 작업을 수행한다. RA는 위수가 소수 q인 타원 곡선 $E(F_q)$상에서 P가 생성자인 덧셈 순환군 G를 선택한다. 그런 다음, 보안 파라미터가 $\kappa = \log_2 q$인 2개의 일방향 해시 함수 $h_1 = \{0,1\}^* \rightarrow Z_q$와 $h_2 = \{0,1\}^* \rightarrow \{0,1\}^\kappa$를 선택한다. 그런 다음, 비밀키 $s_{RA} \leftarrow Z_q^*$를 선택한 뒤 공개키 $P_{pub} = s_{RA} \cdot P$를 계산한다. 마지막으로 s_{RA}를 안전한 메모리 공간에 보관하고 공개 파라미터 $(G, P, q, h_1, h_2, P_{pub})$를 배포한다.

3.2 Registration Phase

등록단계에서 SM_i와 ES_j는 보안 채널을 통해 RA에 등록하고 블록체인상에서 상호 인증을 위해 사용할 공개 파라미터와 비밀 파라미터를 발급받는다.

3.2.1 Registration Phase of EU

① SM_i는 자신의 아이디 ID_i와 패스워드 PW_i

를 선택한 후 등록 요청 메시지를 ID_i와 $h(ID_i \| PW_i)$를 함께 RA에게 전송한다. 이를 수신한 RA는 EU_i가 사전에 등록되어 있었는지 확인한다. RA는 $HID_i = h(ID_i), SID_i = h(ID_i \| PW_i \| s_{RA})$, $X_i = SID_i \oplus h(HID_i \| PW_i)$, $EID_i = Enc_{P_{pub}}(ID_i)$를 계산한 다음 키 관련 정보들의 만료 기한 ET_i를 설정한다. 그런 다음, Algorithm 2를 이용하여 $KMT_Update(null, HID_i, EID_i, ET_i)$를 호출한다. 즉, 블록체인에 SM_i의 키 관련 정보 (HID_i, EID_i, ET_i)이 등록된다. 마지막으로, RA는 SID_i와 X_i를 SM_i에게 전송한다.

② SM_i는 수신한 파라미터 SID_i와 X_i를 메모리에 저장한다.

3.2.1 Registration Phase of ES

① ES_j는 자신의 ID_j를 RA에게 전송한다. 이를 수신한 RA는 ES_j가 이미 등록되어 있는지 확인한다. 등록되지 않은 ES_j라면, RA는 $SID_j = h(ID_j)$와 $s_j = \frac{1}{s_{RA} \cdot SID_j} \cdot P_1$을 계산하고 s_j를 ES_j에게 전달한다.

② RA에게 비밀 파라미터를 수신한 ES_j는 이를 안전하게 메모리에 저장한다.

3.3 Authentication Phase

① SM_i는 먼저 $HID_i = h(ID_i)$, $SID'_i = X_i \oplus h(HID_i \| PW_i)$를 계산한 다음, SID_i와 SID'_i가 동일한지 검사한다. 만약 두 값이 같지 않으면, 로그인 단계를 종료한다. 그렇지 않으면 SM_i는 난수 $r_i \in Z_q^*$를 선택하고, , $R_i = g^{r_i}$, $K_i = r_i \cdot P$, $V_i = r_i \cdot (P_{pub} + SID_j \cdot P)$, $Q_i = h(HID_i \| V_i \| r_i \| K_i \| TS_i)$, $Auth_i = HID_i \oplus R_i$를 계산한다. 그런 다음, 인증 요청 메시지 $M_1 = < V_i, K_i, Auth_i, TS_i >$를 ES_j에게 전송한다.

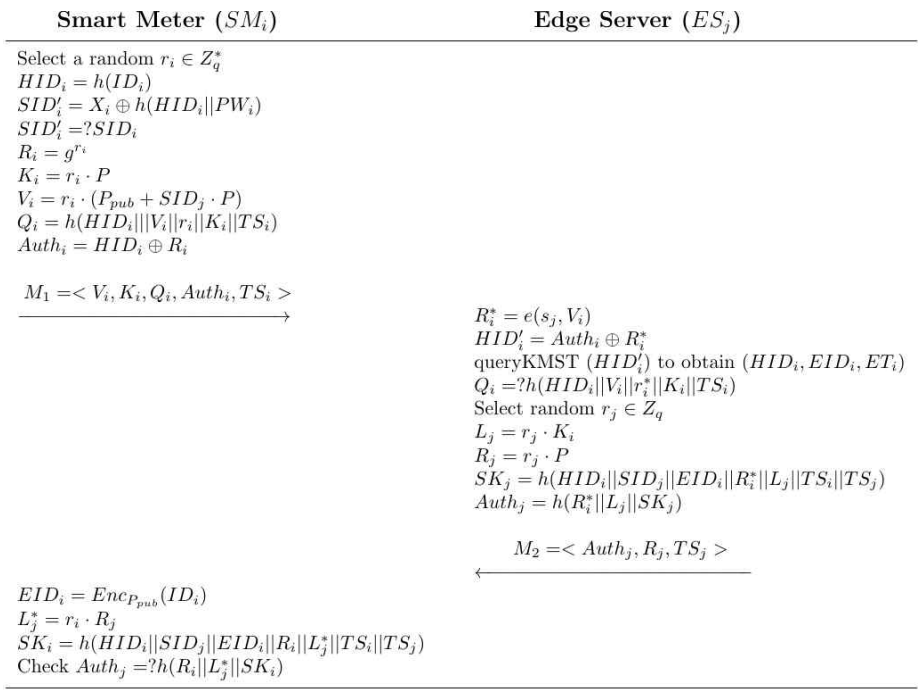
② M_1을 수신한 ES_j는 $R_i^* = e(s_j, V_i)$와 $HID_i' = Auth_i \oplus R_i^*$를 계산한다. 이를 통해 얻은 HID_i'를 이용하여 $KMT_Query(HID_i')$를 호출하면 블록체인에 저장된 인증용 파라미터 (HID_i, EID_i, ET_i)를 수신하게 된다. 먼저 ET_i를 확인하여 수신한 파라미터들의 유효기간을 검사한다. 파라미터들이 유효하면 ES_j는 $Q_i^* = ? h(HID_i \| V_i \| r_i^* \| K_i \| TS_i)$인지 검사한다. 만약 두 값이 같으면 ES_j는 난수 $r_j \in Z_q^*$를 선택하고 $L_j = r_j \cdot K_i$, $R_j = r_j \cdot P_1$, $SK_j = h(HID_i \| SID_j \| EID_i \| R_i^* \| L_j \| TS_i \| TS_j)$, $Auth_j = h_2(R_i^* \| L_j \| SK_j)$를 계산한다. 그런 다음 $M_2 = \langle Auth_j, R_j, TS_j \rangle$를 SM_i에게 전송한다.

③ SM_i는 자신의 ID_i를 이용하여 $EID_i = Enc_{P_{pub}}(ID_i)$를 계산하고 $L_j^* = r_i \cdot R_j$를 구한 다음 세션키 $SK_i = h(HID_i \| SID_j \| EID_i \| R_i \| L_j \| TS_i \| TS_j)$를 도출해낸다. 도출한 세션키의 유효성을 확인하기 위해 $Auth_j = ? h(R_i \| L_j^* \| SK_i)$인지 검사한다. 이 검사가 통과하면 SM_i와 ES_j는 성공적으로 세션키를 공유한 것이다.

3.4 Revocation Phase

SM_i의 키 관련 정보들에 대한 ET_i가 만료되었거나 보안적인 이유로 SM_i가 RA에 재등록해야 하는 경우가 있다. 이때 공개키와 비밀 파라미터들을 새로 갱신하기 위한 업데이트가 필요하다. 이를 위해 RA는 스마트 컨트랙트 알고리즘 $KMT_Update(oldHID_i, HID_i, EID_i, ET_i)$를 호출하여 새로 갱신한 정보들을 블록체인에 등록한다.

RA는 SM_i의 악의적인 행동을 탐지하게 되면 $KMT_Revocation()$을 이용하여 폐기 트랜잭션을 생성한다. 이를 통해 키 관련 정보인 (HID_i, EID_i, ET_i)를 삭제한다. 또한, SM_i가 스마트 그리드 시스템에 더 이상 참여하지 않아 키 관련 정보 폐기를 위한 요청할 때에도 RA는 동일한 방법으로 관련 정보들을 삭제한다.



(그림 2) Authentication phase of the proposed scheme

4. 검증

4.1 보안 분석

4.1.1 Mutual Authentication

Authentication phase에서 공격자가 공개 채널 상에서 메시지 M_1을 도청하더라도, 정당한 ES_j만이 자신의 비밀키를 이용하여 다음 식 (1)과 같이 $g^{r_i} = R_i$를 계산할 수 있다.

$$\begin{aligned} R_i &= e(s_j, V_i) \\ &= e(\frac{1}{s_{RA} \cdot SID_j} \cdot P,\ r_i \cdot (s_{RA} \cdot P + SID_j \cdot P)) \\ &= e(P,P)^{\frac{1}{s_{RA} \cdot SID_j} \cdot SID_j \cdot s_{RA} \cdot r_i} \\ &= e(P,P)^{r_i} \\ &= g^{r_i} \end{aligned} \tag{1}$$

이렇게 성공적으로 R_i 값을 계산한 ES_j만이 $Auth_i$를 복호화하여 HID_i를 얻을 수 있다. 이때, HID_i는 $KMT\_Query()$ 알고리즘을 통해 블록체인으로부터 사용자의 키 관련 정보들을 얻는 데 사용된다. 그런 다음, K_i는 Q_i^*값 검증을 통해 블록체인에 등록된 정당한 사용자인지 검증하는 데 사용되므로 본 논문에서 제안하는 기법은 상호 인증을 보장한다.

4.1.2 Session key agreement

공격자가 세션키를 계산하기 위해서는 두 개의 난수 r_i와 r_j가 필요하다. 하지만 이 두 개의 값은 공개채널을 통해 직접 전송되지 않으며 ECDH문제 아래에서 보호된다. ES_j와 SM_i가 세션키를 수립하기 전에, ES_j는 $Auth_j = h(R_i^* \| L_j \| SK_i)$를 생성하여 SM_i에게 전송한다. SM_i는 $Auth_i = h(R_i \| L_j^* \| SK_i)$를 계산하여 $Auth_j$와 동일한지 검사한다.

$$L_j = r_j \cdot K_i = r_i \cdot R_j = r_i \cdot r_j \cdot P_1 \tag{2}$$

식 (2)가 위와 같이 만족하므로, 복호화 연산을 통

해 유효한 Q_i^*값을 계산한 정당한 ES_j만이 자신의 세션키 검증 값 $Auth_j$를 생성하여 SM_i와 키 합의를 달성할 수 있다.

4.1.3 Anonymity

SM_i와 ES_j의 ID가 노출되면 공격자는 가장 공격 또는 SM_i의 키 정보를 변경하려는 공격을 시도 할 수 있다. 이로부터 보호하기 위해 제안하는 기법에서는 실제 ID를 직접적으로 노출하지 않고 $HID_i = h_1(ID_i)$와 $SID_j = h_1(ID_j)$와 같이 해시화 한다. 따라서, 제안한 기법은 익명성을 보장한다.

4.1.4 Untraceability

인증단계에서 공개 채널을 통해 전송되는 메시지 M_1과 M_2를 공격자가 도청할 수 있다. 하지만 여기에 포함되어 있는 V_i, K_i, Q_i, $Auth_i$, R_j, $Auth_j$에는 매 세션마다 변하는 난수가 포함되어 있다. 따라서, 공격자는 메시지 M_1과 M_2를 통해 사용자의 행동을 추적할 수 없으므로 제안하는 기법은 비 추적성을 제공한다.

4.1.5 Perfect forward secrecy

전방향 안전성을 만족하기 위해서는 각 세션의 세션키들의 관계를 공격자가 유추할 수 없어야 한다. 제안하는 기법에서 생성되는 세션키는 매 세션마다 변하는 난수가 포함되어 있다. 만약 비밀 파라미터들이 노출되어 공격자가 이전 세션의 세션키를 알아내려고 하더라도, 공격자가 난수를 얻기 위해서는 ECDH 문제를 해결해야 한다. 따라서, 공격자는 ECDH문제를 해결하기 어려우므로 제안한 기법은 전방향 안전성을 만족한다.

4.1.6 Resistance to the stolen-device attack

공격자가 스마트 그리드 IoT 디바이스를 임의로 획득하거나 탈취하여 이로부터 SID_i와 X_i값을 추출했다고 가정하자. 공격자는 디바이스 탈취 공격을 통해 SM_i로 가장하기 위해서는 ID_i 또는 PW_i가 필요한데 이는 해시화되어 보호되고 있다. 즉, 공격자는 SM_i에 저장되어 있는 파라미터들을 추출하더라도 SM_i의 민감한 정보를 알아낼 수 없으므로 제안된 기법은 디바이스 탈취 공격으로부터 안전하다.

4.1.7 Resistance to the user impersonation attack

제안하는 기법에서 SM_i는 자신이 유효한 HID_i를 계산할 수 있다는 것을 보여줌으로써 ES_j에게 자신의 신분을 증명한다. 5.6절에서 설명했듯이 공격자가 SM_i로 위장하기 위해서는 사용자의 ID_i와 PW_i 필요하다. 하지만, 공격자는 이를 계산할 수 없으므로 제안하는 기법은 사용자 위장 공격으로부터 안전하다.

4.1.8 Resistance to the replay attack

제안하는 기법에서는 SM_i의 타임스탬프 TS_i와 ES_j의 타임스탬프 TS_j를 이용하여 각 단계마다 메시지를 검사한다. 공격자가 메시지 M_1과 M_2를 도청 또는 가로채 재전송하더라도 타임스탬프 값을 검사하기 때문에 세션이 종료된다. 따라서 제안하는 기법은 재전송 공격으로부터 안전하다.

4.1.9 Resistance to the denial-of-service attack

제안하는 기법에서는 인증 단계에서 SM_i는 SID_i값을, ES_j는 Q_i를 값을 유효하게 계산할 수 있는지 검사하여 값이 다를 경우 세션을 종료한다. 따라서 제안하는 기법은 서비스 공격으로부터 안전하다.

4.2 성능 분석

본 장에서는 스마트 컨트랙트를 적용한 관련 연구인 Wang 등이 제안한 인증 기법과 성능 분석을 실시한다. <표 1>은 등록단계와 인증단계별로 EU와 ES가 수행하는 연산량을 비교한다. T_H는

<표 1> The performance analysis of the proposed scheme

	Wang et al.'s scheme			Proposed		
	RA	*EU*	*ES*	*RA*	*EU*	*ES*
Registration	$T_E=3$ $T_H=2$ $T_S=1$	$T_E=2$ $T_H=2$		$T_E=2$ $T_H=2$ $T_S=1$		
Authentication		$T_E=6$ $T_H=4$	$T_E=6$ $T_H=5$		$T_E=4$ $T_H=5$ $T_S=1$	$T_E=2$ $T_H=3$ $T_B=1$
Total	$18T_E+13T_H+1T_S$			$8T_E+10T_H+1T_S+1T_B$		

일방향 해시 함수이며 T_S는 대칭키 암호화, T_B는 Bilinear Paring, T_E는 타원곡선에서의 곱셈 연산을 의미한다. 본 논문에서 제안하는 방식과 Wang 등이 제안한 방식과 비교할 때 *RA*, *EU*, *ES* 각각의 연산량에서 제안한 방식이 상대적으로 T_E 연산 횟수가 적지만, Bilinear Paring 연산이 추가되면서 전체적으로 비슷한 연산 소모량을 가지는 것을 알 수 있다.

5. 결론

본 논문에서는 기존 스마트 그리드 환경에서의 인증 기법의 취약점을 파악하고 보안성을 강화하기 위해 블록체인에서 동작하는 스마트 컨트랙트를 적용한 새로운 인증 기법을 제안했다. 기존 관련 연구에서 보고되었던 취약점인 디바이스 탈취 공격을 통한 사용자 가장 공격을 방어하고, 갱신 및 폐기 과정을 지원하기 위해 스마트 컨트랙트를 적용했다. 또한, 기존 스마트 컨트랙트를 적용한 관련 연구에서 사용자의 ID가 노출되어 키 관련 정보들이 악의적으로 변경될 수 있다는 문제점 또한 해결하였다. 안전성 분석을 통해 제안된 기법이 익명성, 상호 인증, 전방향 안전성을 만족함과 동시에 디바이스 탈취 공격에 안전함을 증명했다. 본 논문에서 제안하는 기법과 성능 측면에서 Wang 등이 제안한 기법과 비교하여 거의 동등한 연산 소모량을 갖는다는 것을 보였다. 따라서 본 논문에서 제안하는 기법은 실제 스마트 그리드 환경에서 사용자의 프라이버시를 보호함과 동시에 성능적 측면에서 효율적으로 사용될 수 있다.

참고문헌

[1] KEPCO. https://home.kepco.co.kr/kepco/KO/C/htmlView/KOCDHP001.do?menuCd=FN05030501 (accessed Febuary 24, 2021).

[2] Korea Smart Grid Institute. https://www.smartgrid.or.kr/bbs/content.php?co_id=sub5_1 (accessed Febuary 24, 2021).

[3] J. Lee, and J. Lee, "Mobile Edge Computing based Charging Infrastructure considering Electric Vehicle Charging Efficiency," Journal of the Korea Academia-Industrial cooperation Society, Vol. 18, No. 10, pp. 669-674, 2017.

[4] W. Wang, H. Huang, L. Zhang, and C. Su, "Secure and Efficient Mutual Authentication Protocol for Smart Grid under Blockchain," Peer-to-Peer Networking and Applications, pp.1-13, 2020.

[5] H. Zhang, J. Wang, and Y. Ding, "Blockchain-based Decentralized and Secure Keyless Signature Scheme for Smart Grid," Energy, Vol. 180, pp. 955-967, 2019.

[6] Y. H. Kang and W. H. Park, "A Study on

Concurrency Control Scheme for Scalability of Blockchain", Jouranl of Information and Security, Vol. 20, No. 3, pp. 71-78, 2020.

[7] J. Wang, L. Wu, K.K.K.R. Choo, and D. He, "Blockchain-based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure," IEEE Transactions on Industrial Informatics, Vol. 16, No. 3, pp. 1984-1992, 2019.

[8] J. W. Jung and S. J. Lee, "The Security Vulnerabilities of 5G-AKA and PUF-based Security Improvement", Jouranl of Information and Security, Vol. 19, No. 1, pp. 3-10, 2019.

[9] J. Y. Park, J. Y. Lee, H. S. Lee, J. W. Kang, H. J. Kwon, and D. S. Shin, "Design of Military Information System User Authentication System Using FIDO 2.0-based Web Browser Secure Storage", Jouranl of Information and Security, Vol. 19, No. 4, pp .43-53, 2019.

[10] J.L. Tasi, and N.W. Lo, "Secure Anonymous Key Distribution Scheme for Smart Grid," IEEE Transactions on Smart Grid, Vol. 7, No. 2, pp. 906-914, 2015.

[11] V. Odelu, A.K. Das, M. Wazid, and M. Conti, "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," IEEE Transactions on Smart Grid, Vol. 9, No. 3, pp. 1900-1910, 2016.

[12] M. Wazid, A. K. Das, N. Kumar, and J. J. Rodrigues, "Secure Three-factor User Authentication Scheme for Renewable-energy-based Smart Grid Environment," IEEE Transactions on Industrial Informatics, Vol. 13, No. 6, pp. 3144-3153, 2017.

[13] K. Mahmood, S.A. Chaudhry, H. Naqvi, S. Kumari, X. Li, and A.K. Sangaiah, "An Elliptic Curve Cryptography based Lightweight Authentication Scheme for Smart Grid Communication," Future Generation Computer Systems, Vol. 81, pp. 557-565, 2018.

[14] X.C. Liang, T.Y. Wu, Y.Q. Lee, C.M. Chen, and J.H. Yeh, "Cryptanalysis of A Pairing-based Anonymous Key Agreement Scheme for Smart Grid," In Advances in Intelligent Information Hiding and Multimedia Signal Processing, pp. 125-131, 2020.

[15] D. Boneh, and M. Franklin, "Identity-based Encryption from The Weil Pairing," In Annual International Cryptology Conference, pp. 213-229, 2001.

[저 자 소 개]

이 학 준 (Hakjun Lee)
2015년 2월 한국교통대학교 소프트웨어공학 학사
2018년 2월 성균관대학교 전자전기컴퓨터공학 석사
2020년 2월 성균관대학교 전자전기컴퓨터공학 박사 수료
2021년 4월~현재 호원대학교 IT소프트웨어보안학과 조교수
email : hjlee@security.re.kr

이 영 숙 (Youngsook Lee)
2009년 3월~현재 호원대학교 IT소프트웨어보안학과 교수
2008년 8월 성균관대학교 컴퓨터공학 박사
2005년 2월 성균관대학교 석사
1987년 2월 성균관대학교 정보공학사
email : ysooklee@howon.ac.kr