Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.3, Jun. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.3.313

스마트 그리드 환경에서 변조 방지 디바이스를 사용하지 않는 안전한 사용자 인증 및 키 합의 방식*

박 기 성,[1†] 윤 대 근,[1] 노 성 기[2‡]
[1,2]한국전자통신연구원 (연구원, 책임연구원)

A Secure Authentication and Key Agreement Scheme for Smart Grid Environments without Tamper-Resistant Devices*

Ki-Sung Park,[1†] Dae-Geun Yoon,[1] SungKee Noh[2‡]
[1,2]Electronics and Telecommunications Research Institute (Researcher, Principal Researcher)

요 약

최근 스마트 그리드 관련 기술의 발전으로 사용자는 다양한 환경에서 보다 안전하고 신뢰성 있는 전력 서비스를 제공 받을 수 있다. 그러나 이러한 서비스들은 인터넷을 통하여 제공되므로 공격자의 데이터 주입, 변경, 삭제 및 추출 등 다양한 잠재적인 공격에 취약하다. 따라서 올바른 사용자에게만 서비스를 제공하기 위한 사용자 인증하고 키를 합의 하는 것은 반드시 이루어져야 하는 보안 필수요소 이다. 본 논문에서는 Zhang 등이 제안한 인증 및 키 합의 방식이 안전성을 tamper-resistant 디바이스에 의존하는 문제가 있으며 스마트 미터 도난 및 위장 공격, 세션 키 노출 공격 등 다양한 공격에 취약함을 밝히고 이를 개선한 스마트 그리드 환경에서 변조 방지 디바이스를 사용하지 않으며 안전한 사용자 인증 및 키 합의 방식을 제안한다. 또한 제안된 인증 방식의 안전성 및 성능을 분석하고 BAN(Abadi-Burrow-Needham) logic 분석을 통하여 제안한 방식이 안전한 상호 인증을 제공함을 입증하였다. 따라서 제안된 방식은 효율적이고 안전하며 실제 스마트 그리드 환경에서 효율적으로 적용 가능한 인증 방식이다.

ABSTRACT

With the development of smart grid technologies, a user can use the secure and reliable power services in smart gird environments. However, the users are not secure against various potential attacks because the smart gird services are provided through the public channel. Therefore, a secure and lightweight authentication and key agreement scheme has become a very important security issue in smart grid in order to guarantee user's privacy. In 2019, Zhang et al. proposed a lightweight authentication scheme for smart gird communications. In this paper, we demonstrate that Zhang et al.'s scheme is vulnerable to impersonation and session key disclosure attacks, and then we propose a secure authentication and key agreement scheme for smart grid environments without tamper-resistant devices. Moreover, we perform the informal security and the BAN logic analysis to prove that our scheme is secure various attacks and provides secure mutual authentication, respectively. We also perform the performance analysis compared with related schemes. Therefore, the proposed scheme is efficiently applicable to practical smart gird environments.

Keywords: Smart grid, Authentication, Key agreement, BAN logic, tamper-resistant device

Received(03. 03. 2020), Modified(05. 13. 2020), Accepted(05. 14. 2020)

* 본 연구는 한국전자통신연구원 연구운영비지원사업의 일환으로 수행되었음. [20ZR1300, 지능형 사이버 보안 및 신뢰 인프라 기술 연구]

* 본 논문은 2019년도 동계 학술대회에 발표한 우수논문을 개선 및 확장한 것임

† 주저자, ks.park@etri.re.kr
‡ 교신저자, sknoh@etri.re.kr(Corresponding author)

I. 서 론

스마트 그리드(smart gird)는 기존의 전력망에 정보통신기술을 융합하여 전력의 효율적인 생산 및 분배를 가능하게 하는 차세대 지능형 전력망이다. 그러나 이러한 스마트 그리드 환경의 다양한 서비스들은 공개 네트워크를 통하여 제공되므로 악의적인 공격자에 의한 데이터 주입, 위조 및 변조, 삭제 등 다양한 공격에 쉽게 노출될 수 있다. 또한 스마트 그리드 네트워크가 공격자에게 공격 받을 경우 개인 및 기업의 손실뿐만 아니라 국가적인 손실까지 일으킬 수 있다. 따라서 스마트 그리드 환경에서 올바른 사용자에게 서비스를 제공하기 위한 올바른 사용자 인증 및 키 합의 방식이 필요하다.

최근 스마트 그리드 환경에서 사용자의 데이터를 안전하게 보호하고 신뢰성 있는 전력 서비스를 제공하기 위한 인증 방식에 대한 연구가 활발히 이루어지고 있다[1-6].

2016년 Tasi 등[1]은 스마트 그리드 환경을 위한 익명성을 보장하는 안전한 키 분배 방식을 제안하였으며 2018년 Odelu 등[2]은 스마트 그리드 환경에서 안전한 인증 및 키 합의 방식을 제안하였다. 그러나 Tasi 등의 방식은 세션 키 노출 공격에 취약하고 Odelu 등의 방식은 가장 공격 및 추적 공격에 취약한 문제점이 있다. 이를 해결하기 위하여 2017년 Chen 등[3]은 bilinear map을 이용한 인증 방식을 제안하였으나 Chen 등의 방식 또한 높은 연산량을 요구하는 문제점이 있다.

이러한 자원이 제약적인 스마트 그리드 환경을 고려하여 2016년 He 등[4]은 타원곡선을 사용하여 경량화된 익명 키 분배 방식을 제안하였으며 2018년 Kmuar 등[5]은 스마트 미터링을 위한 경량화된 인증 및 키 합의 방식을 제안하였다. 또한 2018년 Mood 등[6]은 타원곡선암호 기반의 스마트 그리드 환경을 위한 키 분배 방식을 제안하였으며 2019년 Zhang 등[7]은 프라이버시 보호를 위한 경량화 인증 방식을 제안하였다. 그러나 제안된 경량화 방식[4-6]들의 전체적인 연산량은 줄어들었으나 스마트 미터에게 과도한 연산을 요구하고 있으며 스마트 미터를 안전한 디바이스로 가정하고 이에 안전성을 의존하는 문제점이 있다. 이러한 가정은 스마트 미터가 공격자에게 노출될 경우 개인의 피해뿐만 아니라 전체적인 시스템의 붕괴를 초래할 수 있으므로 스마트 미터가 공격자에게 노출되어도 안전한 시스템에 대한 연구가 필요하다[8-9].

본 논문에서는 스마트 그리드 환경에서 안전한 전력 서비스를 제공하기 위한 경량화 인증 및 키 합의 방식을 제안한다. 제안한 인증 방식은 스마트 미터의 tamper-resistant 특성에 안전성을 의존하지 않으며 내부자 공격, 재전송 공격, 위장 공격 등 다양한 잠재적인 공격에 안전하며 사용자의 익명성 및 안전한 상호 인증을 제공한다. 또한 자원이 제한적인 스마트 그리드 환경에서 스마트 미터의 연산량을 고려하여 설계하였으며 BAN(Burrow-Abadi-Needham) logic[8]을 동하여 안전성을 분석하였으므로 실제 스마트 그리드 환경에 효율적으로 적용 가능하다.

본 논문의 구성은 다음과 같다. 2장에서는 Zhang 등의 인증 방식에 대하여 설명하고 3장에서는 Zhang 등이 제안한 방식의 보안 취약점을 분석한다. 4장에서는 본 논문에서 제안하는 변조 방지 디바이스를 사용하지 않는 사용자 인증 및 키 합의 방식을 제안하고 5장에서 제안한 방식의 안전성 및 성능을 분석한다. 최종적으로 6장에서는 본 논문에 대한 결론을 제시한다.

II. 관련 연구

2.1 스마트 그리드

스마트 그리드는 전력의 생산, 운반 및 소비 과정에서 초소형센서, 모바일 디바이스 및 대형기기 등 다양한 통신 기기를 활용하여 공급자와 소비자가 서로 상호작용하고 효율적인 전력을 공급하는 전력망시스템이며 국제표준화기구(IEC)를 통하여 표준화 추진 중에 있다.

스마트 그리드 시스템은 모바일 디바이스와 스마트 미터, 서비스 제공자, 전력 시스템으로 구성되며 인증 프로토콜의 수행단계는 Fig. 1과 같고 각 수행단계는 아래와 같다.

1)초기화 단계: 서비스 제공자가 효율적인 전력 서비스 제공을 위한 초기 시스템 매개변수 및 자신의 개인키를 생성한다.

2)등록 단계: 사용자는 서비스 제공자로부터 요청한 자신의 신원정보에 대한 인증 파라미터를 발급 받는다. 사용자는 스마트 미터의 메모리에 인증 파라미터를 저장하고 모바일 디바이스와 연결하여 등록한 신원정보를 기반으로 스마트 미터를 관리한다.

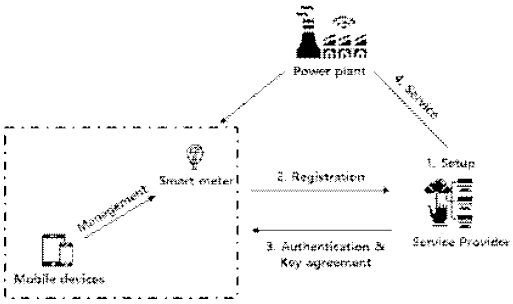

Fig. 1. System model of smart grid

3)인증 및 키 합의 단계: 사용자는 효율적인 전력 서비스를 제공받기 위하여 서비스 제공자와 서로 올바른 개체인지 확인하고 추후 사용할 세션 키를 생성한다.

4)서비스 단계: 상호인증이 완료된 후 사용자는 스마트 미터 및 모바일 디바이스를 활용하여 서비스 제공자 및 전력시스템으로부터 전력 서비스를 제공받는다.

2.2 Zhang 등이 제안한 방식

2019년 Zhang 등[7]은 사용자의 프라이버시를 보호하기 위하여 해시 함수와 XOR 함수 기반 경량화 인증 방식을 제안하였다. 그러자 제안한 방식은 스마트 미터를 tamper-proof 디바이스로 안전하다고 가정하고 이에 안전성을 전적으로 의존하는 문제가 있다. Zhang 등이 제안한 방식은 스마트 미터

Smart Meter (SM_i) **Service Provider** (SP_j)

Selects a random number r_1

$\{ID_i, r_1\}$

$\Rightarrow$

Computes
$M_i = E_S((ID_i \oplus h(ID_j||s))||(r_1 \oplus ID_i))$,
$Q_i = h((ID_i||ID_j) \oplus s \oplus r_1)$
Stores Q_i **into database**

$\{SmartCard\}$

$\Leftarrow$

Stores
M_i, ID_i, r_1 **in the tamper-resistant device**

$\Rightarrow$ **Secure Channel**

Fig. 2. Smart meter registration phase of Zhang et al.'s scheme

Smart Meter (SM_i) **Service Provider** (SP_j)

Selects a random number r_2
Computes $X_i = r_2 \oplus h(ID_i||r_1)$

$\{M_i, X_i\}$

$\rightarrow$

Computes
$D_S(M_i) = (ID_i' \oplus h(ID_j'||s'))||(r_1' \oplus ID_i')$, $ID_i^* = ID_i' \oplus h(ID_j'||s') \oplus h(ID_j||s)$, $r_1^* = r_1' \oplus ID_i' \oplus ID_i^*$, $Q_i' = h((ID_i^*||ID_j) \oplus s \oplus r_1^*)$
Checks $Q_i' = Q_i$ **or** $Q_i' = Q_{io}$
Computes
$r_2' = X_i \oplus h(ID_i^*||r_1^*)$, $M_i' = E_S((ID_i^* \oplus h(ID_j||s))||(r_2' \oplus ID_i^*))$
Selects a random number r_3
Computes $k = h(ID_i^*||r^{*1}||r_2')$, $Auth_{ji} = E_k((h(ID_i^*||r_2'||r_1^*) \oplus r_3)||h(ID_i^*||r_1^*||r_2'||M_i')$,
$SK_{sp} = h(ID_i^*||r_1^*||r^{*2}||r_3)$

$\{Auth_{ji}\}$

$\leftarrow$

Computes $k' = h(ID_i \oplus r_1 \oplus r_2)$,
$D_{k'}(Auth_{ji}) = ((h(ID_i^{**} \oplus r_2^*)||r_1^{**}) \oplus r_3')||h(ID_i^{**}||r_i^{**}||r_2^*)||M_i^*)$
Checks
$h(ID_i||r_1||r_2) = h(ID_i^{**}||r_i^{**}||r_2^*)$
Computes
$r_3^* = h(ID_i^{**} \oplus r_2^*)||r_i^{**}) \oplus r_3' \oplus h((ID_i \oplus r_2)||r_1)$, $SK_{sm} = h(ID_i||r_1||r_2||r_3^*)$,
$Auth_{ij} = h(SK_{sm}||r_3^*)$

$\{Auth_{ij}\}$

$\rightarrow$

Checks $Auth_{ij} = h(SK_{sp}||r_3)$
Computes
$Q_{\in ew} = h((ID^*||ID_j) \oplus s \oplus r_2)$
Replaces Q_i, Q_{io} **with** Q_{inew}, Q_i
$Ack_{ji} = h((r_2' \oplus r_3||r_1^*)$

$\{Ack_{ji}\}$

$\leftarrow$

Checks $Ack_{ji} = h((r_2 \oplus r_3^*)||r_1)$
Replaces r_1, M_1 **with** r_2, M_i^*

$\rightarrow$ **Public Channel**

Fig. 3. Authentication and key agreement phase of Zhang et al.'s scheme

등록 단계, 인증 및 키 합의 단계로 구성되며 각 단계는 Fig. 2, Fig. 3과 같고 상세 수행절차는 다음과 같다.

2.2.1 등록 단계

1 단계: 스마트 미터(SM_i)는 랜덤 넘버 r_1을 선택하고 자신의 신원 ID_i를 서비스 제공자(SP_j)에게 전송한다.

2 단계: SP_j는 전송받은 ID_i와 r_1을 사용하여 $M_i = E_i((ID_i \oplus h(ID_j \| s)) \| r_1 \oplus ID_i))$, $Q_i = h((ID_i \| ID_j) \oplus s \oplus r_1)$ 를 계산한 후 Q_i를 데이터베이스에 저장하고 M_i를 SM_i에게 전송한다.

3 단계: SM_i는 SP_j로부터 전송받은 M_i와 ID_i 및 r_1을 메모리에 저장한다.

2.2.2 인증 및 키 합의 단계

- 1 단계: 스마트 미터(SM_i)는 랜덤 넘버 r_2를 선택하고 $X_i = r_2 \oplus h(ID_i \| r_1)$ 을 계산한 후 M_i와 X_i를 SP_j에게 전송한다.
- 2 단계: SP_j는 M_i와 X_i를 전송받은 후 비밀키 s를 사용하여 M_i를 복호화한다. 또한 SP_j는 $ID_i^* = ID_i' \oplus h(ID_j' \| s')) \oplus h(ID_j \| s)$, $r_1^* = r_1' \oplus ID_i' \oplus ID_i^*$, $Q_i' = h((ID_i^* \| ID_j) \oplus s \oplus r_1^*$을 계산하고 데이터베이스에 해당 값이 저장되어 있는지 확인한다. SP_j는 $r_2' = X_i \oplus h(ID_i^* \| r_1^*)$를 계산하고 M_i를 M_i'로 업데이트한 후 랜덤 넘버 r_3와 새로운 대칭키 $k = h(ID_i^* \oplus r_i^* \oplus r_2')$를 계산한다. 그 후 SP_j는 인증 메시지 $Auth_{ji} = E_k((h((ID_i^* \oplus r_2') \| r_1^*) \oplus r_3) \| h(ID_i^* \| r_i^* \| r_2') \| M_i')$ 및 세션 키 $SK_{sp} = h(ID_i^* \| r_1^* \| r_2' \| r_3)$를 계산하고 $Auth_{ji}$를 SM_i에게 전송한다.
- 3 단계: SM_i는 인증 메시지를 전송받은 후 자신의 ID_i를 사용하여 세션 키 $k' = h(ID_i \oplus r_1 \oplus r_2)$, $h((ID_i^{**} \oplus r_2^* \| r_1^{**}) \oplus r_3')$, $h(ID_i^{**} \| r_1^{**} \| r_2^*)$를 계산하고 세션 키로 암호화된 메시지 $Auth_{ji}$를 복호화한다. 그 후 SM_i는 복호화 된 값의 유효성을 검증하고 $r_3^* = h((ID_i^{**} \oplus r_2^* \| r_1^{**}) \oplus r_3' \oplus h((ID_i \oplus r_2 \| r_1)$를 계산한 후 세션 키 $SK_{sm} = h(ID_i \| r_1 \| r_2 \| r_3^*)$ 계산한다. 최종적으로 SM_i는 검증 메시지 $Auth_{ij} = h(SK_{sm} \| r_3^*)$를 계산한 후 SP_j에게 전송한다.
- 4 단계: SP_j는 응답 메시지를 수신한 후 $Auth_{ij}$의 유효성을 검증하고 세션 키 SK_{sp}를 계산한다. 그 후 SP_j는 $Q_{inew} = h((ID_i^* \| ID_j) \oplus s \oplus r_2)$를 계산하여 데이터베이스의 저장된 (Q_i, Q_{io})값을 $(Q_{i \neq w}, Q_i)$로 갱신하고 응답 메시지 $Ack_{ji} = h((r_2' \oplus r_3) \| r_1^*)$을 SM_i에게 전송한다.
- 5 단계: SM_i는 응답 메시지 Ack_{ji}를 수신하고 Ack_{ji}의 유효성을 검증한다. 그 후 SM_i는 (r_1, M_i)값을 (r_2, M_i^*)로 업데이트하여 tamper-resistant 디바이스에 저장한다.

III. Zhang 등이 제안한 방식의 보안 취약점 분석

본 장에서는 Zhang 등이 제안한 방식이 tamper-resistant 디바이스에 안전성을 의존하고 상호 인증을 제공하지 못하며 스마트 미터 도난 공격, 세션 키 노출 공격, 스마트 미터 위장 공격에 취약함을 보였다. 각 공격은 다음과 같다.

3.1 단일 요소 안전성 의존 문제

Zhang 등의 인증 및 키 합의 방식에서 시스템의 안전성은 이상적인 tamper-resistant 디바이스에 전적으로 의존하고 있으며 사용자의 중요한 정보 ID_i, r_1를 디바이스에 평문으로 저장하고 있다. 그러나 이러한 강한 가정은 tamper-resistant 디바이스가 공격자에 의하여 노출될 경우 시스템 전체의 안전성을 침해할 뿐만 아니라 국가적인 손실을 발생시킬 수 있다[8,9].

3.2 스마트 미터 도난 공격

스마트 미터 도난 공격은 악의적인 공격자가 사용자의 스마트 미터를 획득하고 스마트 미터 안의 저장된 값을 활용하여 사용자의 민감한 개인정보를 탈취 및 변조하는 공격이다. Zhang 등의 방식에서 공격자는 스마트 미터에 저장된 값 M_i, ID_i, r_1을 획득하고 이를 활용하여 스마트 미터 위장 공격, 세션 키 노출 공격 등을 시도할 수 있다.

3.3 스마트 미터 위장 공격

악의적인 공격자는 스마트 미터 도난 공격으로부터 사전에 획득한 정보 M_i, ID_i 및 r_1을 사용하여 로그인 요청 메시지 M_i $X_i = r_2 \oplus h(ID_i \| r_1)$과 응답 메시지 $Auth_{ij}$를 성공적으로 생성할 수 있으므로 Zhang 등의 방식은 스마트 미터 위장 공격에 취약하다.

3.4 세션 키 노출 공격

악의적인 공격자는 스마트 미터 도난 공격으로부터 사전에 획득한 정보 M_i, ID_i, r_1 및 공개 채널로 전송되는 값 X_i, $Auth_{ji}$을 이용하여 해당 세션에서 사용된 세션 키를 생성할 수 있다. 먼저 공격자는 스마트 미터안의 저장된 값 ID_i, r_1을 이용하여 랜덤 넘버 r_2를 획득하고 대칭키 $k = h(ID_i \oplus r_1 \oplus r_2)$를 생성한 후 $Auth_{ji}$를 복호화한다. 따라서 공격자는 세션 키에 사용되는 모든 중요 파라미터 값 ID_i, r_1, r_2, r_3를 얻을 수 있으므로 Zhang 등이 제안한 방식은 세션 키 노출 공격에 취약하다.

3.5 상호 인증

Zhang 등이 제안한 방식에서 악의적인 공격자는 스마트 미터 도난 공격으로 합법적인 사용자로 위장할 수 있으며 세션 키 노출 공격을 통하여 성공적으로 세션 키를 얻을 수 있으므로 Zhang 등의 방식은 안전한 상호 인증을 제공하지 않는다.

IV. 제안한 방식

본 논문에서는 2019년 Zhang 등이 제안한 경량화 인증 방식의 보안 취약점을 개선한 경량화 인증 및 키 합의 방식을 제안한다. 제안한 방식은 사용자 및 스마트 미터 등록 단계, 인증 및 키 합의 단계로 구성되며 각 단계는 Fig. 4, Fig. 5와 같고 상세 수행절차는 다음과 같다.

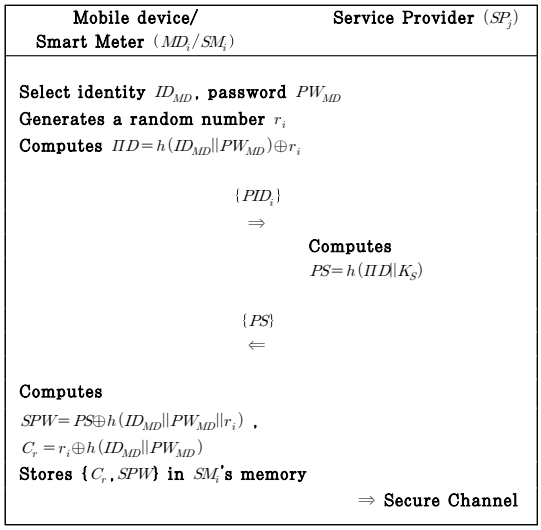

Fig. 4. Mobile device and smart meter registration phase of the proposed scheme

4.1 시스템 매개 변수

본 논문에서 사용하는 제안하는 방식의 시스템 매개변수는 표 1과 같다.

Table 1. Notations

Parameters	Descriptions
MD_i	Mobile device
SM_i	Smart meter
SP_j	Service provider
ID_{MD}	Identity of mobile device
PW_{MD}	Password of mobile device
ID	Pseudo-identity
K_S	Master key of service provider
r	Random number
SK	Session key
$h()$	One-way hash function
$\|$	Concatenation operation
$\oplus$	Bit-wise XOR operation

Mobile device/ Smart Meter (MD_i/SM_i)	Service Provider (SP_j)
Inputs ID_{MD}, PW_{MD} **Generates** r_{new}, r_1 **Computes** $r_i = C_r \oplus h(ID_{MD}\|\|PW_{MD})$, $PID = h(ID_{MD}\|\|PW_{MD}) \oplus r_i$, $PS = SPW \oplus h(ID_{MD}\|\|PW_{MD}\|\|r_i)$, $PID_{new} = h(ID_{MD}\|\|PW_{MD}) \oplus r_{new}$, $Cr_{new} = r_{new} \oplus h(ID_{MD}\|\|PW_{MD})$, $C_{MD} = PID_{new} \oplus h(PS\|\|r_1)$, $V_{MD} = h(PID_{new}\|\|PS\|\|r_1)$	
$\{PID, V_{MD}, C_{MD}, r_1\}$ →	**Computes** $PS' = h(PID\|\|K_S)$, $PID_{new} = C_{MD} \oplus h(PS'\|\|R_1)$, $PS_{new} = h(PID_{new}\|\|K_S)$ **Checks** $V_{MD} = h(PID_{new}\|\|PS'\|\|r_1)$ **Generates a random number** r_2 **Computes** $V_{SP} = h(PID\|PS_{new}\|\|r_2)$, $C_{SP} = PS_{new} \oplus h(PS'\|\|r_2)$, $SK = h(r_1\|\|r_2\|\|PS'\|\|PS_{new})$
← $\{V_{SP}, C_{SP}, r_2\}$	
Computes $PS_{new} = C_{SP} \oplus (PS\|\|r_2)$, **Checks** $V_{SP} = h(PID\|PS_{new}\|\|r_2)$ **Computes** $SPW_{new} = PS_{new} \oplus h(ID_{MD}\|\|PW_{MD}\|\|r_{new})$, $SK = h(r_1\|\|r_2\|\|PS\|\|PS_{new})$	
	→ **Public Channel**

Fig. 5. Authentication and key agreement phase of the proposed scheme

4.2 사용자 및 스마트 미터 등록 단계

- 1 단계: 모바일 디바이스 사용자(MD_i)는 자신의 신원 ID_i 및 비밀번호 PW_i를 설정하고 랜덤 넘버 r_i를 생성한 후 $PID = h(ID_{MD}\|PW_{MD}) \oplus r_i$를 계산하여 SP_j에게 전송한다.
- 2 단계: SP_j는 전송받은 PID_i와 자신의 마스터 키 K_s를 사용하여 $PS = h(PID\|K_s)$를 계산하고 MD_i에게 전송한다.
- 3 단계: MD_i는 SP_j로부터 전송받은 PS_i를 사용하여 $SPW = PS \oplus h(ID_{MD}\|PW_{MD}\|r_i)$, $Cr = r_i \oplus h(ID_{MD}\|PW_{MD})$ 을 계산하고 Cr 및 SPW를 스마트 미터(SM_i)에 저장한다.

4.3 인증 및 키 합의 단계

- 1 단계: MD_i는 자신의 디바이스에 ID_i, PW_i를 입력하고 랜덤 넘버 r_{new}, r_1을 선택한 후 $r_i = Cr \oplus h(ID_{MD}\|PW_{MD})$, $PS = SPW \oplus h(ID_{MD}\|PW_{MD}\|r_i)$, $PID_{new} = h(ID_{MD}\|PW_{MD}) \oplus r_{new}$, $Cr_{new} = r_{new} \oplus h(ID_{MD}\|PW_{MD})$, $C_{MD} = PID_{new} \oplus h(PS\|r_1)$, $V_{MD} = h(PID_{new}\|PS\|r_1)$ 를 계산하고 PID, V_{MD}, C_{MD}, r_1을 SP_j에게 전송한다.
- 2 단계: MD_i로부터 PID, V_{MD}, C_{MD}, r_1을 전송받은 후 SP_j는 $PS = h(PID\|K_s)$, $PID_{new} = C_{MD} \oplus h(PS\|r_1)$, $PS_{new} = h(PID_{new}\|K_s)$를 계산하고 V_{MD} 값이 유효한지 검증한다. 만약 V_{MD} 값이 유효한 값이라면 SP_j는 랜덤 넘버 r_2를 생성하고 $V_{SP} = h(PID\|PS_{new}\|\|r_2)$, $C_{SP} = PS_{new} \oplus h(PS\|r_2)$ 를 계산한 후 V_{SP}, C_{SP}, r_2를 MD_i에게 전송한다.
- 3 단계: MD_i는 $PS_{new} = C_{SP} \oplus h(PS\|r_2)$를 계산하고 V_{SP} 값이 유효한 값인지 검증한다. 만약 V_{SP}가 유효한 값이라면 MD_i는 $SPW_{new} = PS_{new} \oplus h(ID_{MD}\|PW_{MD}\|r_{\neq w})$을 계산하고 SM_i의 메모리에 SPW_{new} 및 r_{new}를 업데이트 한다.
- 4 단계: 최종적으로 SM_i와 SP_j는 세션 키 $SK = h(r_1\|r_2\|PS\|PS_{new})$ 를 계산하고 추후 안전한 통신을 위하여 사용한다.

V. 안전성 및 성능 분석

본 장에서는 제안한 경량화 인증 및 키 합의 방식의 안전성을 분석하고 Zhang 등의 방식과 성능을 비교 분석하였다. 또한 BAN logic 분석을 통하여 제안한 방식이 안전한 상호 인증을 제공함을 입증하였다.

5.1 안전성 분석

본 논문에서 제안한 인증 및 키 합의 방식의 안전성을 informal 분석을 통하여 분석하였으며 제안한 방식은 안전성을 tamper-resistant 디바이스에 의존하지 않으며 스마트 미터 도난 및 위장 공격, 세션 키 노출 공격, 재전송 공격 등에 안전하고 상호 인증 및 불추적성을 보장한다.

5.1.1 스마트 미터 도난 및 위장 공격

제안한 방식에서 인증에 필요한 주요 파라미터 PS 및 r_i 등은 올바른 ID와 PW를 알고 있는 경우에만 얻을 수 있으며 악의적인 공격자가 스마트 미터의 저장된 데이터 $Cr = r_i \oplus h(ID_{MD} \| PW_{MD})$ 및 $SPW = PS \oplus h(ID_{MD} \| PW_{MD})$ 를 획득하더라도 합법적인 사용자의 ID, PW 없이 전체 시스템 및 개인의 안전성에 영향을 줄 수 없다. 따라서 제안한 인증 및 키 합의 방식은 tamper-resistant 성질에 의존하지 않고 시스템의 안전성을 보장하고 스마트 미터 도난 및 위장 공격에 안전하다.

5.1.2 세션 키 노출 공격

제안한 방식에서 공격자는 사전에 스마트 미터로부터 획득한 정보 Cr, SPW와 공개 채널로 전송되는 값 PID, V_{MD}, C_{MD}, r_1, V_{SP}, C_{SP}, r_2를 이용하더라도 해당 세션에서 사용하는 세션 키를 생성할 수 없다. 스마트 미터의 메모리에 저장된 값은 사용자의 올바른 ID, PW 없이 사용될 수 없으며 공개된 채널로 전송되는 모든 파라미터들은 매 세션마다 갱신되므로 세션 키 노출 공격에 안전하다.

5.1.3 재전송 공격

제안한 방식에서 SP_j 및 SM_i는 $V_{MD} = h(\Pi D_{new} \| PS \| r_1)$ 와 $V_{SP} = h(PID \| PS_{new} \| r_2)$ 으로 메시지의 유효성을 각각 검증한다. 또한 검증 메시지 V_{MD}, V_{SP}는 랜덤 넘버 r_1, r_2를 포함하고 있으므로 한 번 전송된 메시지를 재사용하는 것은 불가능하다. 따라서 제안한 방식은 재전송 공격에 안전하다.

5.1.4 상호 인증 및 불추적성

제안한 인증 및 키 합의 방식에서 공격자는 로그인 요청 메시지 PID, V_{MD}, C_{MD}, r_1 및 응답 메시지 V_{SP}, C_{SP}, r_2를 성공적으로 생성할 수 없다. 또한 인증 및 키 합의 단계에서 사용되는 모든 파라미터들은 매 세션마다 새로운 값으로 갱신되므로 공격자는 사용자를 추적할 수 없다. 따라서 제안하는 방식은 안전한 상호 인증 및 불추적성을 보장한다.

5.1.5 패스워드 추측 공격

제안한 방식에서 공격자는 패스워드와 랜덤넘버를 동시에 추측할 수 없다고 가정한다. 만약 공격자가 올바른 패스워드를 추측했다고 가정하더라도 사용자의 인증 파라미터 r_i를 추측할 수 없으며 인증 파라미터 r_i를 추측하더라도 올바른 패스워드를 추측할 수 없으므로 제안한 방식은 패스워드 추측 공격에 안전하다.

5.2 BAN logic 안전성 분석

BAN(Burrows-Abadi-Needham) logic[10]은 보안 프로토콜의 안전성을 증명하기 위하여 1990년 제안된 방식으로 현재 상호 인증의 안전성을 입증하기 위하여 사용되는 대표적인 분석 방법이다. 본 논문에서는 제안하는 방식이 상호 인증을 가능함을 BAN logic을 통하여 분석하였다. 또한 BAN logic 분석을 위하여 분석에 필요한 규칙, 가정, 목표, 이상화 형태를 먼저 정의하고 안전성을 분석한다.

5.2.1 BAN logic 표기법

BAN logic 분석에 사용하는 표기법은 다음 표 2와 같다.

Table 2. Notations of BAN logic

Notation	Description
$A \mid\Rightarrow B$	A controls B
$\#K$	K is fresh
$A \lhd B$	A sees B
$A \mid\sim B$	A once said B
$A \mid\equiv B$	A believes X
$(K)_K$	K is encrypted by the statement K
$A \overset{SK}{\longleftrightarrow} B$	A and B use the shared secret key to communicate each other

5.2.2 BAN logic 규칙

- MMR(Message meaning rule): 만약 A와 B가 비밀키 K를 공유하고 있는 사실을 신뢰하고 암호화된 메시지 K를 본다면 A는 B가 X를 언급한 사실을 신뢰한다. MMR은 식 (1)과 같다.

$$\frac{A \mid\equiv A \overset{SK}{\longleftrightarrow} B,\ A \lhd (X)_K}{A \mid\equiv B \mid\sim X} \tag{1}$$

- NVR(Nonce Verification rule): 만약 A가 X를 이전에 사용한 적 없는 변수임을 신뢰하고 B가 X를 언급한 것을 신뢰한다면 A는 B가 X를 신뢰하고 있다는 사실을 신뢰한다.

$$\frac{A \mid\equiv \#(X),\ A \mid\equiv B \mid\sim X}{A \mid\equiv B \mid\equiv X} \tag{2}$$

- JR(Jurisdiction rule): 만약 B가 X를 제어하는 사실을 A가 신뢰하고 B가 X를 신뢰하고 있다는 사실을 신뢰한다면 A는 X를 신뢰한다.

$$\frac{A \mid\equiv \mid\Rightarrow X,\ A \mid\equiv B \mid\equiv X}{A \mid\equiv X} \tag{3}$$

- FR(Freshness rule): 만약 A가 X를 이전에 사용한 적이 없는 변수임을 신뢰한다면 A는 변수 (X, Y)도 사용한 적이 없는 변수로 신뢰한다.
- $$\frac{A \mid\equiv \#(X)}{A \mid\equiv \#(X, Y)} \tag{4}$$

5.2.3 보안 목표

보안 목표 1: $SM \mid\equiv (SM \overset{SK}{\longleftrightarrow} SP)$

보안 목표 2: $SP \mid\equiv (SM \overset{SK}{\longleftrightarrow} SP)$

보안 목표 3: $SM \mid\equiv SP \mid\equiv (SM \overset{SK}{\longleftrightarrow} SP)$

보안 목표 4: $SP \mid\equiv SM \mid\equiv (SM \overset{SK}{\longleftrightarrow} SP)$

5.2.4 가정

가정 1: $SP \mid\equiv (SM \overset{PS}{\longleftrightarrow} SP)$

가정 2: $SP \mid\equiv \#(r_2)$

가정 3: $SM \mid\equiv (SM \overset{PS}{\longleftrightarrow} SP)$

가정 4: $SM \mid\equiv \#(r_1)$

가정 5: $SM \mid\equiv SP \mid\Rightarrow (SM \overset{SK}{\longleftrightarrow} SP)$

가정 6: $SP \mid\equiv SM \mid\Rightarrow (SM \overset{SK}{\longleftrightarrow} SP)$

5.2.5 메세지 이상화 형태

메세지 1. $SM \rightarrow SP : (PID, PID_{new}, r_1)_{PS}$
메세지 2. $SP \rightarrow SM : (PS_{new}, r_2)_{PS}$

5.2.6 BAN logic 증명

- 1 단계: SP_j는 SM_i로부터 받은 이상화 형태의 메시지 1로부터 다음 식을 (5)를 얻는다.

$$SP \lhd (PID, PID_{new}, r_1)_{PS} \quad (5)$$

- 2 단계: 식 (5)와 가정 1로부터 MMR을 적용하여 다음 식 (6)을 얻는다.

$$SP| \equiv SM| \sim (PID, PID_{new}, r_1)_{PS} \quad (6)$$

- 3 단계: 식 (6)과 가정 2로부터 FR을 적용하여 식 (7)을 얻는다.

$$SP| \equiv SM| \equiv \#(PID, PID_{new}, r_1)_{PS} \quad (7)$$

- 4 단계: 식 (5)와 식 (6)으로부터 NVR을 적용하여 식 (8)을 얻는다.

$$SP| \equiv SM| \equiv (PID, PID_{new}, r_1)_{PS} \quad (8)$$

- 5 단계: SM_i는 SP_j로부터 받은 이상화 형태의 메시지 2로부터 다음 식을 (9)를 얻는다.

$$SM \lhd (PS_{new}, r_2)_{PS} \quad (9)$$

- 6 단계: 식 (9)와 가정 3로부터 MMR을 적용하여 다음 식 (10)을 얻는다.

$$SM| \equiv SP| \sim (PS_{new}, r_2)_{PS} \quad (10)$$

- 7 단계: 식 (10)과 가정 4로부터 FR을 적용하여 식 (11)을 얻는다.

$$SM| \equiv SP| \equiv \#(PS_{new}, r_2)_{PS} \quad (11)$$

- 8 단계: 식 (9)와 식 (10)으로부터 NVR을 적용하여 식 (12)을 얻는다.

$$SM| \equiv SP| \equiv (PS_{new}, r_2)_{PS} \quad (12)$$

- 9 단계: 제안한 방식에서 세션 키는 $SK = h(r_1 \| r_2 \| PS \| PS_{new})$ 로 계산되며 BAN logic 분석을 통하여 해당 중요 파라미터들에 대한 신뢰 관계를 모두 구축하였으므로 식 (13), (14)를 얻을 수 있다.

$$SM| \equiv SP| \equiv (SM \overset{SK}{\longleftrightarrow} SP) \quad (13)$$

$$SP| \equiv SM| \equiv (SM \overset{SK}{\longleftrightarrow} SP) \quad (14)$$

- 10 단계: 식 (13)과 가정 5로부터 JR을 적용하여 식 (15)를 얻는다.

$$SM| \equiv (SM \overset{SK}{\longleftrightarrow} SP) \quad (15)$$

- 11 단계: 식 (14)와 가정 6로부터 JR을 적용하여 식 (16)을 얻는다.

$$SP| \equiv (SM \overset{SK}{\longleftrightarrow} SP) \quad (16)$$

BAN logic 분석 결과의 식 (13), (14), (15), (16)을 통하여 요구하는 모든 보안 목표를 얻었으므로 제안하는 방식은 안전한 상호 인증을 제공한다.

5.3 성능 분석

제안한 인증 방식과 Zhang 등이 제안한 인증 방식의 연산량 분석을 등록 단계와 인증 및 키 합의 단계로 구분하여 분석하였으며 분석 결과는 표 3과 같다.

Zhang 등의 방식은 경량화 인증을 위하여 대칭키 암호화 방식을 사용하였으며 총 0.052s의 연산 시간이 소요되었다. 그러나 제안한 방식은 대칭키 암호화를 사용하지 않고 해시 함수와 XOR 연산만을

Table 3. Performance comparison

	Zhang et al. scheme[7]	Proposed scheme
Registration phase	2H+1E ≈ 0.0092s	4H ≈ 0.002s
Authentication and key agreement phase	16H+2D+2E ≈ 0.0428s	13H ≈ 0.0065s

H: hash operation(≈ 0.0005s)[11],
E/D:symmetric encryption/decrpyion (≈ 0.87s)[11]

이용하여 설계되었으며 총 0.0085s의 소요시간을 요구하므로 Zhang 등이 제안한 방식보다 더 효율적이다. 따라서 제안한 인증 방식은 실제 스마트 그리드 환경에서 보다 효율적인 인증 및 키 합의 방식이다.

VI. 결 론

스마트 그리드 환경에서 사용자는 시간 및 공간에 제약 받지 않고 언제나 편리하게 서비스 제공자로부터 전력 서비스를 받을 수 있다. 그러나 이러한 전력 시스템의 보안 취약점이 공격자에게 노출될 경우 사용자의 프라이버시 침해 및 국가적인 손실을 일으킬 수 있으므로 스마트 그리드 환경에서 안전한 통신을 위한 인증 및 키 합의 방식에 대한 연구는 반드시 필요하다. 또한 스마트 그리드 환경에서 사용되는 스마트 미터는 저사양 디바이스이므로 연산량을 고려하여 기존의 공개키 기반 인증 방식이 아닌 경량화된 인증 방식을 사용하여야 한다.

본 논문에서는 최근 Zhang 등이 제안한 인증 방식이 스마트 미터의 tamper-resistant 성질에 시스템의 안전성을 전적으로 의존하고 있으며 이는 스마트 미터의 정보가 노출될 경우 심각한 보안 문제를 발생시킬 수 있음을 보이고 이를 개선한 인증 및 키 합의 방식을 제안하였다. 또한 제안한 방식이 스마트 미터 도난 및 위장 공격, 세션 키 노출 공격, 재전송 공격, 추적 공격 등에 안전함을 입증하고 BAN logic 분석을 통하여 제안한 방식이 안전한 상호 인증을 제공함을 증명하였을 뿐만 아니라 Zhang 등의 방식과 성능을 비교 분석하여 보다 효율적인 방식임을 보였다. 따라서 제안하는 인증 및 키 합의 방식은 실제 스마트 미터의 저사양을 고려하여 제안되었으며 tamper-resistant 성질에 안전성을 의존하지 않으므로 실제 스마트 그리드 환경에서 효율적으로 활용 가능한 방식이다.

References

〔1〕 J. Tasi and N. Lo, "Secure anonymous key distribution scheme for smart grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906-914, March 2016.

〔2〕 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, May 2018.

〔3〕 Y. Chen, J. Martinez, P. Castillejo, and I. Lopez, "An anonymous authentication and key establish scheme for samrt grid: FAuth," *Energies*, vol. 10, no. 9, pp. 1354-1376, Sept. 2017.

〔4〕 D. He, H. Wang, M. K. khan, and L. Wang, "Lightweight anonymous key distribution scheme for smart grid using elliptic curve cryptography," *IET Communications* vol. 10, no. 14, pp. 1795-1802, Sept. 2016

〔5〕 P. Kumar, A. Gurtov, M. Sain, A. Mrtin, and P. Ha, "Lightweight authentication and key agreement for smart metering in smart energy networks," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 4349-4359, July 2019.

〔6〕 D. Abbasinezhad-Mood and M. Nikooghadam, "An anonymous ECC-based self-certified key distribution scheme for smart grid," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 7996-8004, Oct. 2018.

〔7〕 L. Zhang, L. Zhao, S. Yin, C. Chi, R. Liu, and Y. Zhang, "A lightweight authentication scheme with privacy protection for smart grid communications," *Future Generation Computer Systems*, vol. 100, pp. 770-778, Nov. 2019.

〔8〕 Z. Liu, L. Xiong, T. Peng, D. Peng, and H. Liang, "A realistic distributed conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Access*, vol. 6, pp. 26307-26317, May 2018.

〔9〕 H. Zhong, S. Han, J. Cui, J. Zhang, and Y. Xu, "Privacy-preserving au-

thentication scheme with full aggregation in VANET," Information Sciences, vol. 476, pp. 221-221, Feb. 2019.

[10] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM trans. Comput. Syst.*, vol. 8, pp. 18-36, Feb. 1990.

[11] C. -C. Lee, C. -T, Chen, P. -H. Wu, and T. -Y. Chen, "Three-factor control protocol based on elliptic curve cryptosystem for universal serial bus mass storage devices," *IET Comput. Digit. Tchn.*, vol. 7, pp. 48-56, Jan. 2013.

〈저자소개〉

박 기 성 (KiSung Park) 정회원
2015년 2월: 경북대학교 산업전자전기공학부 졸업
2017년 2월: 경북대학교 전자공학부 석사
2017년 3월~현재: 경북대학교 전자공학부 박사과정
2019년 9월~현재: 한국전자통신연구원 연구원
〈관심분야〉 블록체인, 분산신원, 인증, 보안프로토콜

윤 대 근 (Dae-Geun Yoon) 정회원
2014년 12월: 뉴욕주립대(Stony Brook University) 컴퓨터공학과 학사 졸업
2015년 12월: 뉴욕주립대(Stony Brook University) 전자공학과 석사 졸업
2016년 1월~현재: 한국전자통신연구원 재직 중
2019년 3월~현재: KAIST 전자공학과 박사과정
〈관심분야〉 정보보호, 네트워크, 블록체인

노 성 기 (Sungkee Noh) 정회원
1990년 2월: 한양대학교 산업공학과 졸업
1992년 2월: 포항공과대학교 산업공학과 석사
2004년 3월: 충남대학교 컴퓨터과학과 박사
1992년 1월~현재: 한국전자통신연구원 책임연구원
〈관심분야〉 블록체인, 분산신원, 네트워크