한국항행학회 논문지 제17권 제6호 2013년 12월 (JKONI 17(6): 736-748, Dec. 2013)

스마트그리드 AMI 환경을 위한 전방 보안성이 강화된 ID기반 인증 기법

ID-based Authentication Schemes with Forward Secrecy for Smart Grid AMI Environment

박대일*, 여상수**0

Dae-il Park*, Sang-Soo Yeo**0

요 약

본 논문에서는 기존에 연구된 AMI망 환경에서 동적 ID기반 인증 프로토콜 KL기법의 취약점을 분석하였고, 기존 연구의 보안요구사항을 만족하면서도 추가적으로 전방 보안성을 가지도록 하는 기법 두 가지를 제안한다. 첫번째 기법에서는 전력사 내의 상위 시스템인 MDMS를 시간동기화 서버로 사용하여 댁내의 스마트그리드 기기와 시간동기화 하여, 매 세션마다 OTP함수로 만들어지는 새로운 비밀값으로 인증을 진행한다. 두 번째 기법에서는 비공개 값의 해시체인을 사용하여 인증을 진행함으로써, 매 세션마다 새로운 비밀값을 사용한다. 제안하는 두 가지 기법은 지역 및 통신 환경에 따른 장·단점이 있을 것으로 보이며 이를 통해 AMI망 환경에 따라 제안기법을 효율적으로 선택하여 적용할 수 있을 것으로 예상한다.

Abstract

In this paper, we analyse the vulnerabilities of KL scheme which is an ID-based authentication scheme for AMI network, and propose two kinds of authentication schemes which satisfy forward secrecy as well as security requirements introduced in the previous works. In the first scheme, we use MDMS which is the supervising system located in an electrical company for a time-synchronizing server, in order to synchronize smart grid devices in home, and we process device authentication with a new secret value generated by OTP function every session. In the second scheme, we use a secret hash-chain mechanism for authentication process, so we can use a new secret value every session. The proposed two schemes have strong points and weak points respectively and those depend on the services area and its environment, so we can select one of them efficiently considering real aspects of AMI environment.

Key words : Smart Grid, AMI Network, Authentication, Forward Secrecy

I. 서 론

스마트그리드란 기존 전력망에 정보기술(IT)을 융

* 목원대학교 컴퓨터공학부(Mokwon University.)
** 목원대학교 컴퓨터공학부 교수(Division of Computer Engineering., Mokwon University)
· 제1저자 (First Author) : 박대일(Dae-il Park)
0 교신저자 (Corresponding Author) : 여상수(Sang-Soo Yeo, tel : +82-42-829-7636, email: sangsooyeo@gmail.com)
· 접수일자 : 2013년 9월 11일 · 심사(수정)일자 : 2013년 9월 12일 (수정일자 : 2013년 12월 17일) · 게재일자 : 2013년 12월 30일
http://dx.doi.org/10.12673/jkoni.2013.17.6.736

합하여 발전소에서 생산된 전력을 핵심 인프라인 첨단 검침 인프라 AMI (Advanced Meter Infrastructure)를 통해 사용자에게 양방향으로 실시간 전력정보를 주고받음으로 양방향으로 교환 및 활용함으로써 에너지 효율성을 증진시키기 위한 융합 기술이다 [1].

소비자들은 AMI를 통해 실시간으로 전력 사용량 정보를 모니터링 하여 가정 및 기업의 에너지 비용을 절감할 수 있으며, 적정량의 에너지 생산으로 생산비용을 줄이고 에너지 공급의 신뢰도를 높여 보다 안정적으로 전력을 공급할 수 있다. 또한, 신재생 에너지의 이용 비율을 높여 지구 환경 문제 극복에 일조한다 [2],[3]. 이와 같은 스마트그리드 환경으로 인해 스마트그리드의 보안 또한 중요해졌다 [4].

기존 전력망은 폐쇄망으로 운영되어 악의적인 공격자가 접근하기 어려운 환경이었으나 스마트그리드는 소비자 영역에 스마트그리드 기기를 두어 악의적인 공격자가 온-오프라인으로 전력망에 쉽게 접근이 가능해졌다는 점이다 [3]. 악의적인 공격자는 스마트그리드 기기를 통해 전력망 상위 시스템에 침투하거나, 사용자 영역의 디바이스를 탈취하여 허위 정보를 보내거나, 사용자의 전력소비패턴을 통해 개인정보 침해 등의 다양한 공격이 가능하게 된다 [5].

악의적인 공격자의 공격을 막기 위해 사용자 영역에 설치되는 기기와 전력공급자 내에 있는 시스템과의 안전한 통신을 위해 사용자 영역의 기기와 전력공급자 내에 있는 시스템과의 인증을 통해 적법한 사용자일 경우 데이터 전송을 허락하도록 하는 기법의 연구가 필요하다 [6],[7],[8].

본 논문은 [9]의 암호화 프로토콜 KL기법을 개선하여 전방 보안성을 가지도록 하는 기법을 제안한다. 먼저, 기존연구에 대해 알아보고, 기존연구의 취약점인 전방 보안성 (Forward Secrecy)을 해결할 수 있는 기법을 제안한다. 전방 보안성을 해결하기 위해 비공개 값이 변화되도록 시간동기화 OTP 기법과 해시체인 기법을 사용하여 두 가지 기법을 제안한다. 제안하는 기법들은 KL기법의 보안요구사항을 모두 만족하며 전방 보안성을 위한 해시연산 및 통신횟수가 추가된다. 시간동기화 OTP 기법의 경우 MDMS (Meter Data Management System)에 시간동기화 서버로서의 기능을 추가하여 시간동기화 서버를 두어야 하는 문제를 해결하였으나 시간동기화를 위한 통신이 1회 추가되어 총 4회의 통신이 이루어진다. 해시체인 기법은 통신횟수의 변화가 없으며 연산량 또한 해시체인 형성을 위한 연산을 각 기기마다 1회씩 추가하여 KL기법과 큰 차이가 없도록 설계하였다. 제안하는 시간동기화 OTP 기법과 해시체인을 사용하는 기법을 분석하여 어느 환경에서 사용하면 효율적인지에 대해서도 제시하였다.

본 논문의 구성은 다음과 같다. 2, 3장에서 기존연구에 대한 분석 및 문제점에 대하여 고찰하고, 4장에서 기존연구의 문제점을 개선하는 프로토콜에 대해 제안하고, 5장에서는 기존연구 및 제안연구를 분석하고, 마지막으로 6장에서 결론을 맺는다. 특히 5장에서 제안된 기법 중 시간동기화 OTP 기법에 대한 선행연구는 논문[10]에 게재된 내용을 보완정리해서 설명한다.`

Ⅱ. 기존연구

본 장에서는 기존연구의 AMI 구성요소에 대해 알아보고, 기존연구의 인증기술에 대하여 분석한다.

2-1 AMI 구성요소

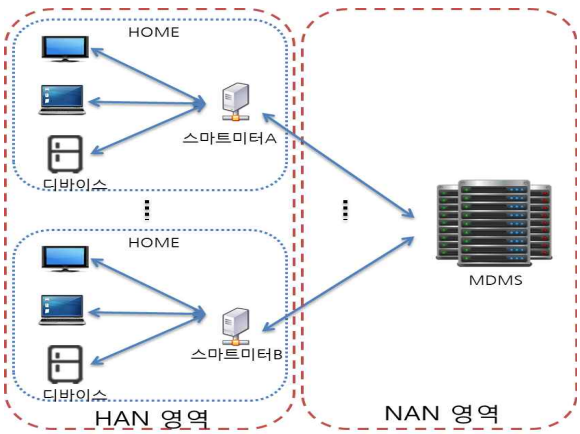

그림 1. AMI 구조[9]
Fig. 1. AMI Structure

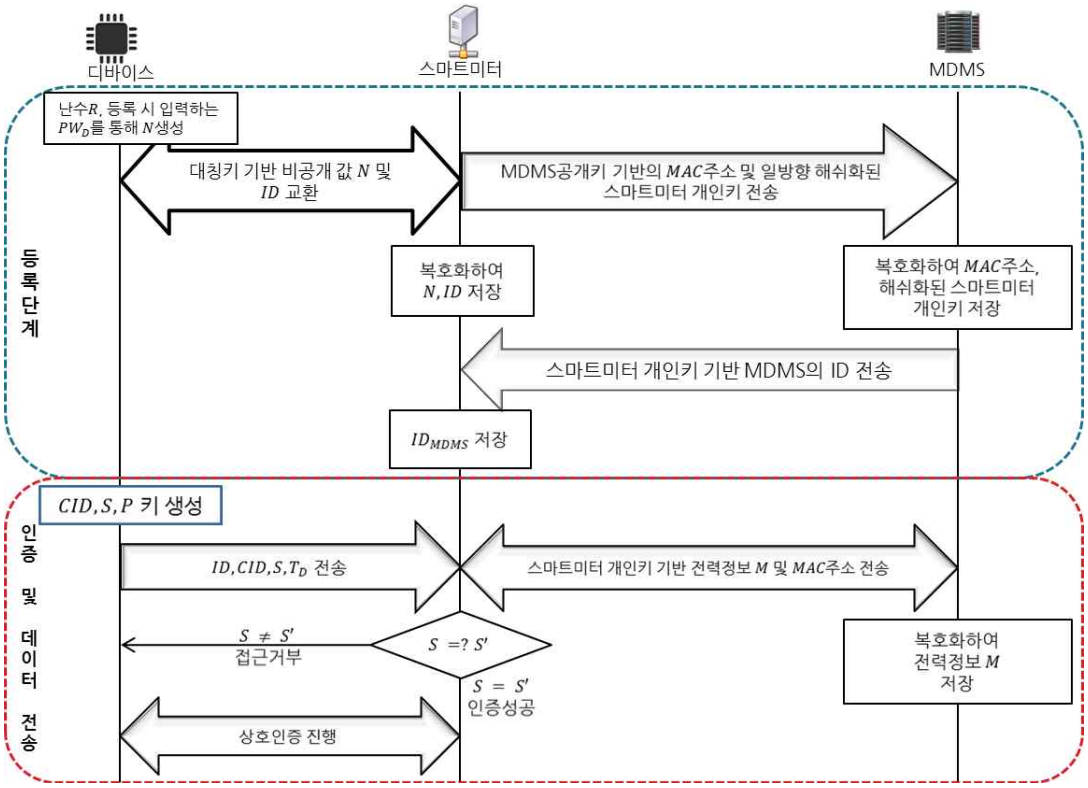

그림 2. KL기법 등록 및 인증단계
Fig. 2. Initial Setup and Authentication of KL Scheme

AMI 구성요소는 그림 1과 같이 MDMS를 중심으로 전력사 내의 상위 시스템, 전력사와 수용가의 스마트미터 간의 연결시켜주는 통신 시스템, 스마트미터 (Smart Meter), 가정용 디바이스 (Device) 등으로 구분된다. 디바이스와 스마트미터 간 인증기법에는 HAN (Home Area Network)를 통해 전력선 통신인 PLC (Power Line Communication)와 ZigBee를 사용하고 있고, 스마트미터와 MDMS간 통신에서는 NAN (Neighborhood Area Network)를 사용하여 데이터를 전송하고 있다 [9],[11].

2-2 KL 기법 [9]

2011년 발표된 김홍기 등의 KL기법[9]은 디바이스에서 생성한 비공개 값인 N을 암호화하여 디바이스와 스마트미터에 저장하여 N값의 안전성을 바탕으로 인증에 필요한 정보를 생성하여 인증을 수행하고 확인할 수 있도록 하는 방식이다. 디바이스는 스마트미터로 인증을 진행할 때 등록단계에서 전송한 비공개 값인 N값에 포함된 난수 R값을 유추할 수 있도록 인증키를 생성하여 스마트미터로 전송하여 인증을 진행하며 식별자 ID를 통해 디바이스를 식별한다. 통신상에 P값을 노출하지 않아 N값을 유추하기 어렵게 하였으며 상호인증을 위해 디바이스로부터 받은 데이터와 이전 정보들을 조합하여 스마트미터에서 생성한 P'을 이용하여 V'값을 생성하여 상호인증을 수행하도록 고안되었다.

스마트미터와 MDMS 간 인증 및 데이터 전송은 스마트미터의 MAC_{Addr}와 해시 연산된 개인키를 이용하여 자신이 등록하고자 하는 MDMS에게만 개인키를 전송하여 데이터를 암호화하므로 부인방지 (Non-Repudiation)가 가능하며, 전송받은 MDMS는 자신의 ID를 스마트미터에게 전송하여 전력량을 전송할 때 MDMS의 ID를 식별하여 올바른 MDMS로 전력정보를 전송하도록 한다.

KL기법의 디바이스, 스마트미터, MDMS 간 등록 및 인증단계는 그림 2와 같다.

Ⅲ. KL기법의 취약점 분석

KL기법은 스마트그리드 AMI망 환경에서의 외부 디바이스가 사용자 스마트미터에 접근하여 전력 사용량을 증가시키거나, 과금을 높이는 문제점들을 해결하기 위해 디바이스와 스마트미터, MDMS 간의 인증 및 데이터 전송을 다루고 있다. 또한, 스마트미터와 MDMS 간 주기적인 통신을 수행하므로 다수의 스마트미터에서 MDMS로의 일괄적인 데이터가 전송될 경우에 빠른 데이터 처리를 위한 적은 연산량과 통신횟수를 통해 안전하게 스마트미터를 인증하고 데이터를 전송하는 기법을 제안하였다. 그러나 디바이스와 스마트미터 간 인증 및 데이터 전송을 위해 사용하는 비공개 값인 N이 고정되어 세션마다 수행되기 때문에 공개키 혹은 N값이 유추될 경우 세션을 수행하여 전송이 완료된 이미 사용된 값들을 악의적인 공격자가 확인할 수 있게 되는 전방 보안성에 취약점을 갖게 된다.

전방 보안성은 악의적인 공격자가 어떠한 순간에 공격이 성공하여 현재 통신상의 정보를 알게 되었을 때 공격이 성공한 시점의 현재 통신상의 정보만으로 과거의 정보를 추적하지 못하는 것을 말한다.

KL기법의 비공개 값인 N은 등록단계에서 디바이스와 스마트미터가 교환하여 안전성을 확보하였으나 악의적인 공격자가 어느 시점에서 N값이나 대칭키를 알게 될 경우, 인증단계 통신상의 공격에 성공하여 통신상의 정보들을 알게 될 경우에 비공개 값인 N을 유추할 수 있게 되며 과거 정보에 대한 이력들을 악의적인 공격자가 손쉽게 확인할 수 있게 되는 취약점을 갖고 있다.

Ⅳ. 전방 보안성이 강화된 ID기반 인증기법

본 장에서는 KL기법에서 보여준 ID기반 인증 기법을 이용하되 기본 설계 프로토콜이 전방 보안성을 보장하지 못하는 점을 개선한 보안 기법 두 가지를 제안한다.

제안기법1은 시간동기화를 통해 동기화 된 시간을 기준으로 하는 현재시간과 비공개 값을 OTP 함수로 연산하여 비공개 값이 변화되도록 암호화하는 방식이다.

제안기법2는 디바이스가 스마트미터로 등록을 진행할 때 전송하는 비공개 값이 매 세션마다 바뀌어 해시체인을 형성하도록 하여 인증을 진행하는 방식이다. 제안하는 ID기반 인증 기법은 KL기법에서 제시하는 필수보안요건을 모두 보장하면서도 전방 보안성 또한 지킬 수 있도록 하는 향상된 기법이다.

4-1 용어 정의

앞으로 프로토콜에 사용될 기호와 용어에 대한 정의이다.

M : 전력량데이터
ks :각각의 개체 간 공유된 세션 키
MAC_{Addr} : 스마트미터의 MAC Address
ID_* : *의 이름
T_* : *의 전송시간 값
R_* : *에서 생성한 난수
PW_* : 동기화 시 *에서 입력한 비밀번호
$B_*[\,]$: *의 키를 이용한 암호화
$h()$: 단방향 해시함수
$g()$: 단방향 해시함수, 스마트미터와의 비밀값 동기화를 위해 사용
$OTP()$: OTP 함수
T_{MDMS} : MDMS의 글로벌시간동기화 값
T_{SYN} : 스마트미터의 시간동기화 값
K_{SMP} : 스마트미터의 개인키
$||$: 비트결합

4-2 제안기법 1 : 시간동기화 OTP 기법[10]

KL기법의 구성요소 중 MDMS를 글로벌시간동기화 서버로 활용하여 시간 동기화 OTP 기법을 통한 전방 보안성 문제를 해결하기 위한 제안기법이다. 본 제안기법은 스마트미터 등록단계에서 시간동기화 서버인 MDMS로 시간동기화 값인 T_{MDMS}를 요청하여 스마트미터의 시간동기화를 진행한다. 동기화가

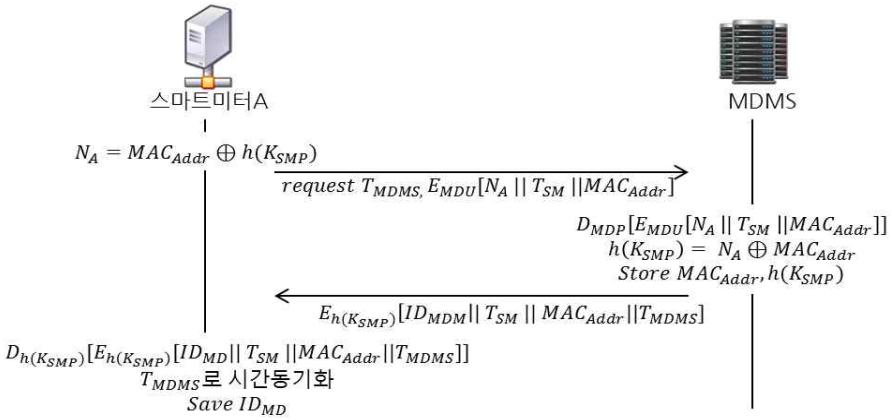

그림 3. 시간동기화 OTP기법의 스마트미터 등록 및 시간동기화 단계
Fig. 3. Registration and Synchronization between SmartMeter & MDMS in Time Synchronized OTP Scheme

완료된 스마트미터는 디바이스의 등록요청이 들어올 경우 스마트미터와의 시간동기화를 위한 T_{SYN}를 디바이스로 전송하여 스마트미터와 디바이스의 시간 동기화를 진행한다. 스마트미터와 디바이스의 시간 동기화가 완료되면 디바이스는 동기화 된 시간의 현재 시간 $Time$과 비공개 값 N_{seed}를 OTP 함수로 연산하여 암호화하는 방식이다. 시간동기화 OTP 기법의 수행절차는 다음 단계와 같다.

단계 1. 스마트미터 등록 및 시간동기화 단계

등록 및 시간동기화 단계에 사용되는 MDMS는 글로벌시간동기화 서버의 역할을 한다. 스마트미터는 등록을 진행할 때 MDMS로 시간동기화 값 요청 $request\ T_{MDMS}$를 보낸다. MDMS는 스마트미터로부터 요청이 들어온 시점의 글로벌시간을 T_{MDMS}으로 생성하여 스마트미터로 전송한다. 스마트미터는 T_{MDMS}로 시간동기화 하여 스마트미터와 MDMS간 시간동기화를 마친다. 스마트미터 등록 및 시간동기화 절차는 다음 그림 3과 같다.

① 스마트미터 A는 자신의 개인키 K_{SMP}의 해시연산된 값 $h(K_{SMP})$를 스마트미터의 MAC_{Addr}와 연산하여 N_A를 생성한다. 생성된 N_A값과 $T_{SM,}\ MAC_{Addr}$을 비트결합한 후에 MDMS의 공개키를 이용하여 암호화 하고 시간동기화를 위한 요청 $request\ T_{MDMS}$를 포함한 정보를 MDMS로 전송한다.

$$\begin{aligned} &SM: N_A = MAC_{Addr} \oplus h(K_{SMP}) \\ &SM \rightarrow MD: request\ T_{MDMS,} \\ &\qquad E_{MDU}[N_A || T_{SM} || MAC_{Addr}] \end{aligned} \tag{1}$$

② MDMS는 $request\ T_{MDMS}$에 대한 시간동기화 값인 T_{MDMS}를 생성하고, MDMS의 공개키로 암호화되어 전송된 데이터를 개인키를 이용하여 복호화한다. 복호화 된 값 N_A와 MAC_{Addr}을 이용하여 스마트미터의 해시연산 된 개인키 $h(K_{SMP})$를 추출한다. 인증단계에서 식별자 MAC_{Addr}를 이용하여 $h(K_{SMP})$를 찾을 수 있도록 MAC_{Addr}와 $h(K_{SMP})$를 MDMS에 저장한다.

$$\begin{aligned} &MD: \\ &D_{MDP}[E_{MDU}[N_A || T_{SM} || MAC_{Addr}]] \\ &h(K_{SMP}) = N_A \oplus MAC_{Addr} \\ &Store\ h(K_{SMP}), MAC_{Addr} \end{aligned} \tag{2}$$

③ MDMS는 스마트미터의 개인키를 저장한 후 MDMS의 ID인 ID_{MD}와 스마트미터로부터 전송받은 $T_{SM,}\ MAC_{Addr}$와 시간동기화 값인 T_{MDMS}를 비트결합한 후, 추출된 스마트미터의 해시연산 된 개인키 $h(K_{SMP})$를 이용하여 암호화한 후 스마트미터로 전송한다.

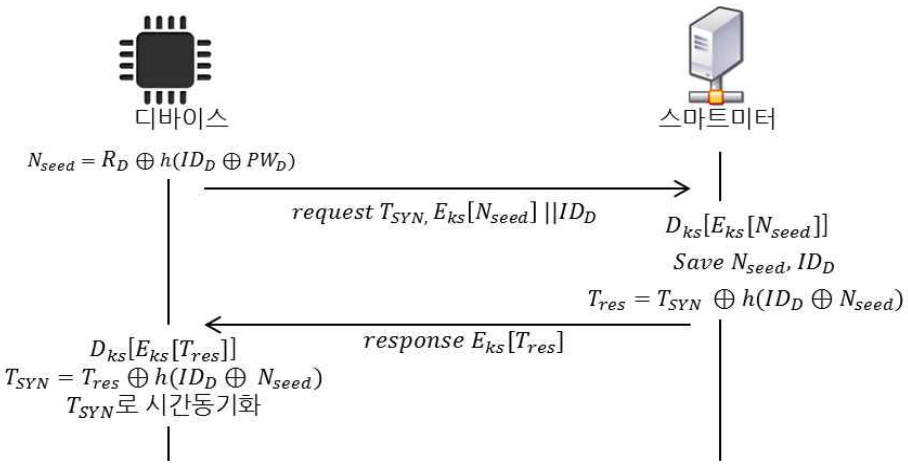

그림 4. 시간동기화 OTP기법의 디바이스 등록 및 시간동기화 단계
Fig. 4. Device Registration & Time Synchronization between Device and SmartMeter in Time Synchronized OTP Scheme

$$MD \rightarrow SM: \\ E_{h(K_{SMP})}[ID_{MD} || T_{SM} || MAC_{Addr} || T_{MDMS}] \quad (3)$$

④ 스마트미터는 전송받은 값을 해시연산 된 개인키 $h(K_{SMP})$를 이용하여 복호화하고 시간동기화 값인 T_{MDMS}을 통해서 시간동기화를 진행한다. 시간동기화가 완료된 후 MDMS의 ID인 ID_{MD}를 스마트미터에 저장하여 스마트미터와 MDMS간 등록단계를 마친다.

$$SM: \\ D_{h(K_{SMP})}[E_{h(K_{SMP})}[ID_{MD} || T_{SM} || T_{MDMS}]] \quad (4) \\ T_{MDMS}\text{으로 시간동기화} \\ Store\ ID_{MD}$$

단계 2. 디바이스 등록 및 시간동기화 단계

디바이스는 스마트미터와의 등록단계에서 비공개 값을 대칭키로 암호화하여 전송하며 동시에 시간동기화 값을 요청한다. 스마트미터는 대칭키를 사용하여 비공개 값을 복호화하고 비공개 값과 디바이스를 식별하기 위한 디바이스의 ID를 저장한다. 스마트미터는 시간동기화 값 T_{SYN}을 생성하여 디바이스로부터 전송받아 저장하고 있는 비공개 값 N_{seed}와 디바이스의 식별자 ID_D을 통해서 T_{res}를 생성한다. 생성된 T_{res}를 대칭키로 암호화하여 디바이스로 전송해준다. 디바이스는 전송받은 T_{res}값을 복호화해서 T_{SYN}값을 추출하여 저장하고 시간동기화 및 등록단계를 마친다. 등록 및 시간동기화 절차는 그림 4와 같다.

① 디바이스는 비공개 값 N_{seed}를 생성하기 위해 디바이스 초기 구동시 입력하는 패스워드 PW_D와 디바이스의 ID인 ID_D를 해시연산한 후 디바이스에서 생성한 난수 R_D값과 연산하여 N_{seed}값을 생성한다.

$$N_{seed} = R_D \oplus h(ID_D \oplus PW_D) \quad (5)$$

② 디바이스는 스마트미터로 비공개 값을 안전하게 보내기 위해 상호공유하고 있는 대칭키를 이용하여 N_{seed}을 암호화한다. 암호화 된 값에 디바이스 식별자 ID_D와 비트결합하여 시간동기화 값 요청과 함께 스마트미터로 전송한다.

$$D \rightarrow SM: request\ T_{SYN,}\ E_{ks}[N_{seed}] || ID_D \quad (6)$$

③ 스마트미터는 전송받은 값에서 ID_D값을 추출하고 암호화 된 비공개 값인 N_{seed}를 대칭키를 통해 복호화하여 스마트미터에 ID_D와 N_{seed}값을 저장한다.

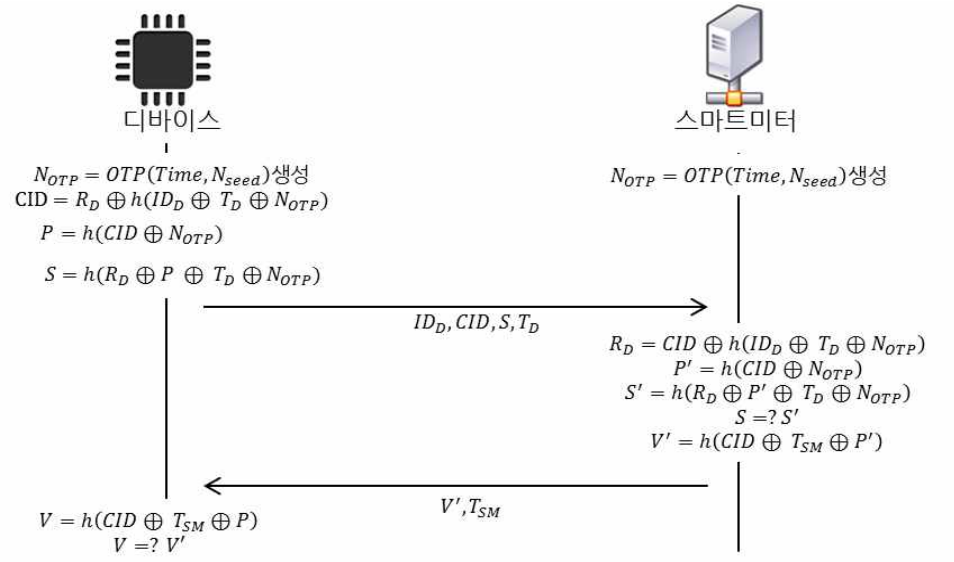

그림 5. 시간동기화 OTP기법의 인증단계
Fig. 5. Authentication in Time Synchronized OTP Scheme

$$SM: D_{ks}[E_{ks}[N_{seed}]] \quad (7)$$
$$SM: Store\, N_{seed,}\, ID_D$$

④ 스마트미터는 시간동기화 값을 디바이스가 복호화 할 수 있도록 디바이스의 ID인 ID_D와 N_{seed}를 이용하여 해시연산 한 후 시간동기화 값인 T_{SYN}와 연산하여 T_{res}를 생성한다. 생성된 T_{res}값을 공유된 대칭키로 암호화하여 스마트미터에서 디바이스로 전송한다.

$$SM: T_{res} = T_{SYN} \oplus h(ID_D \oplus N_{seed}) \quad (8)$$
$$SM \rightarrow D: response\, E_{ks}[T_{res}]$$

⑤ 디바이스는 전송받은 값을 대칭키를 이용하여 복호화하고 T_{res}값에서 시간동기화 값인 T_{SYN}값을 추출하여 스마트미터와 디바이스 간의 시간 동기화를 진행한다. 이때 시간동기화 값인 T_{SYN}을 기준으로 하여 일정한 주기로 생성되는 현재 시간 값은 $Time$이다.

$$D: D_{ks}[E_{ks}[T_{res}]]$$
$$T_{SYN} = T_{res} \oplus h(ID_D \oplus N_{seed}) \quad (9)$$
$$D: T_{SYN}\text{으로 시간 동기화}$$

단계 3. 인증단계

디바이스 등록 및 시간동기화 단계에서 비공개 값 전송 및 시간동기화가 완료된 디바이스와 스마트미터는 비공개 값인 N_{seed}와 디바이스를 식별할 수 있는 ID_D를 저장하고 있다. 디바이스와 스마트미터는 T_{SYN}으로 시간동기화 되어 일정한 주기를 갖는 현재 시간 값인 $Time$을 생성하여 $OTP(N_{seed,}\, Time)$함수를 통해서 N_{OTP}값을 생성한다.

생성된 N_{OTP}값을 이용하여 디바이스는 CID, P, S값을 생성하고 ID와 CID, S, T_D값을 스마트미터에게 전송하게 된다. 스마트미터는 전송받은 값과 마찬가지로 N_{OTP}값을 이용하여 통신상에 전송되지 않은 P값을 생성하여 인증을 진행하고, 인증이 성공할 경우 P'값을 통하여 V'값을 생성한다. 디바이스와 스마트미터 간 상호인증은 통신상에 P값을 주고받지 않도록 하여 안전성을 유지한다.

만일 N_{OTP} 값이 유추된다 하더라도 매 세션마다 $Time$값이 변하므로 생성되는 N_{OTP}의 값은 매 세션마다 달라져 전방 보안성을 만족한다. 인증단계는 다음 그림 5와 같다.

① 디바이스는 매 세션마다 T_{SYN}를 통해 동기화된 디바이스의 현재 시간 값 $Time$과 N_{seed}값을 OTP함수로 연산하여 N_{OTP}값을 생성하고, 등록

단계에서 생성한 난수 R_D, 비공개 값 N_{OTP}, 디바이스의 ID 값 ID_D, 매 세션마다 값이 고정되지 않도록 하는 타임스탬프 값 T_D를 이용하여 CID, P, S 값을 생성한다.

$$\begin{aligned} &N_{OTP} = OTP(N_{seed,}\, Time) \\ &D\colon\ CID = R_D \oplus h(ID_D \oplus T_D \oplus N_{OTP}) \\ &\qquad P = h(CID \oplus N_{OTP}) \\ &\qquad S = h(R \oplus P \oplus T_D \oplus N_{OTP}) \end{aligned} \tag{10}$$

② 디바이스는 생성한 값 중에 P값을 제외한 ID_D, CID, S, T_D를 스마트미터로 전송한다. 스마트미터는 디바이스와 마찬가지로 N_{OTP}값을 생성한다.

$$\begin{aligned} &D \rightarrow SM : ID, CID, S, T_D \\ &\qquad SM : N_{OTP} \text{생성} \end{aligned} \tag{11}$$

③ 스마트미터는 전송받은 값 중에 CID와 스마트미터에서 생성한 N_{OTP}값을 해시연산하여 P'을 생성하고, CID값을 이용하여 난수 R_D를 추출하여 인증에 필요한 값인 S'값을 연산한다.

$$\begin{aligned} &SM\colon\ R = CID \oplus h(ID \oplus T_D \oplus N_{OTP}) \\ &\qquad P' = h(CID \oplus N_{OTP}) \\ &\qquad S' = h(R \oplus P' \oplus T_D \oplus N_{OTP}) \end{aligned} \tag{12}$$

④ 스마트미터에서 전송받은 S값과 생성한 S'값을 비교한 후 인증을 완료하며, 인증이 성공할 경우 CID, P'값과 스마트미터의 타임스탬프 값인 T_{SM}을 통해 상호인증에 사용될 값인 V'값을 생성하여 디바이스에게 스마트미터의 타임스탬프 T_{SM}을 포함하여 전송한다.

$$\begin{aligned} &SM\colon\ S' = ?\ S \\ &SM\colon\ V' = h(CID \oplus T_{SM} \oplus P') \\ &SM \rightarrow D\colon\ V',\ T_{SM} \end{aligned} \tag{13}$$

⑤ 디바이스는 전송받은 T_{SM}값을 이용하여 V값을 생성하고 전송받은 V'값과 비교하여 상호인증을 수행한다.

$$\begin{aligned} &D\colon\ V = h(CID \oplus T_{SM} \oplus P) \\ &D\colon\ V = ?\ V' \end{aligned} \tag{14}$$

4-3 제안기법 2 : 단방향 해시체인 기법

KL기법의 ID기반 디바이스와 스마트미터의 인증 및 데이터 전송 기법에 해시체인 기법을 적용하여 전방 보안성 문제를 해결하기 위한 제안기법이다. 본 제안기법은 등록단계에서 디바이스가 생성하는 N_1 값을 활용하여 매 세션마다 단방향 해시함수를 통한 $N_i(i < 1, N_1 = N_{seed})$값이 생성되도록 하는 방식이다. 생성된 해시값은 세션마다 진행되며 해시체인 $N_{1,} N_{2,} N_{3,} \cdots N_i$ 을 형성한다. 해시의 연산에 필요한 정보는 등록단계에서 전송되며 이후 해시연산은 각각의 디바이스와 스마트미터에서 진행한다. 단방향 해시체인 기법의 수행절차는 다음 단계와 같다.

단계 1. 등록단계

등록단계에서는 디바이스에서 생성한 난수 R_D값과 디바이스 ID_D, 스마트미터와 동기화 시 사용자가 입력한 패스워드를 이용하여 N_1값을 생성한다. 이를 스마트미터에 디바이스 ID_D와 N_1의 값을 저장한다. 저장한 N_1값은 후에 디바이스의 최초 인증 시 사용하고 ID_D는 N_1의 값을 확인하기 위한 식별자로 사용한다. 등록단계는 그림 6과 같은 단계로 진행된다.

① 디바이스는 해시체인을 형성할 최초 비공개 값인 $N_!$을 생성하기 위해 디바이스 초기 구동 시 입력하는 PW_D와 디바이스의 ID인 ID_D를 해시연산한 후, 디바이스에서 생성한 난수 R_D값을 연산하여 N_1값을 생성한다.

$$D\colon\ N_1 = R_D \oplus h(ID_D \oplus PW_D) \tag{15}$$

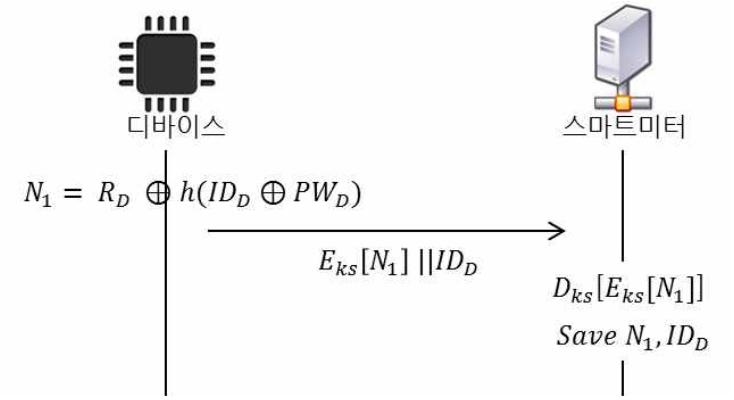

그림 6. 단방향 해시체인기법 등록단계
Fig. 6. Registration between Device and SmartMeter in One-way hash chain-base Scheme

② 디바이스는 스마트미터로 비공개 값을 안전하게 전송하기 위해 상호공유하고 있는 대칭키를 이용하여 N_1을 암호화한다. 암호화 된 값에 디바이스의 ID값인 ID_D를 비트결합하여 스마트미터로 전송한다.

$$D \rightarrow SM: E_{ks}[N_1] \,||\, ID_D \tag{16}$$

③ 스마트미터는 전송받은 값에서 ID_D값을 추출하고 암호화 된 비공개 값 N_1을 대칭키를 통해 복호화하여 스마트미터에 디바이스의 식별자로 사용할 ID_D와 함께 N_1값을 저장한다.

$$SM: D_{ks}[E_{ks}[N_1]] \tag{17}$$
$$Save\ N_1, ID$$

단계 2. 인증단계

등록단계를 수행하면 스마트미터는 디바이스의 아이디와 N_1값을 저장하고 있다. 저장한 값을 이용하여 디바이스는 CID, P, S값을 생성하고 ID_D와 CID, S, T_D값을 스마트미터에게 전송하게 된다. N_1값이 노출되지 않고, 스마트미터에게 전송하고 있는 값 중 P의 값이 노출되지 않고 있기 때문에 N_1값을 추측하기 어려우며, 이를 통해 안전성을 보장한다.

만일 N_i값이 유추되더라도 최초의 N_1값이 단방향 해시함수를 통해 매 세션마다 바뀌기 때문에 수행된 N_i값을 유추하기 어려워 전방 보안성을 만족하며, 통신상에 N_i값을 교환하지 않고 등록단계에서 교환한 N_1값을 이용해 N_i값을 디바이스와 스마트미터에서 단방향 해시연산하여 생성하기 때문에 디바이스와 스마트미터는 물리적으로 공격하기 전에는 비공개 값인 N_i값을 유추하기 어렵다. 또한 스마트미터에서 인증 후 생성한 P'값을 이용하여 V'값을 생성하고 디바이스에서 이를 확인하여 상호인증을 수행한다. 디바이스와 스마트미터의 통신세션이 끊기는 등의 문제로 동기화 실패로 인한 인증에 실패할 경우 인증에 실패한 기기는 최근 성공한 인증 이후의 해시체인 값을 차례대로 연산하여 비교함으로써 에러제어를 수행하도록 한다. 만일 에러제어에 실패할 경우에는 디바이스 재등록과정을 수행하여 인증단계를 진행한다. 인증단계는 그림 7과 같은 단계로 진행된다.

① 디바이스는 i번째 세션마다 N_{i-1}값을 이용하여 새로운 N_i를 해시연산하여 해시체인이 형성되도록 비공개 값 N_i을 생성하고, 등록단계에서 생성한 난수 R_D, 비공개 값인 N_i, 디바이스의 ID인 ID_D, 매 세션마다 값이 고정되지 않도록 하는 타임스탬프 값 T_D를 이용하여 CID, P, S값을 생성한다. N_i값 생성에 대한 점화식은 다음과 같다.

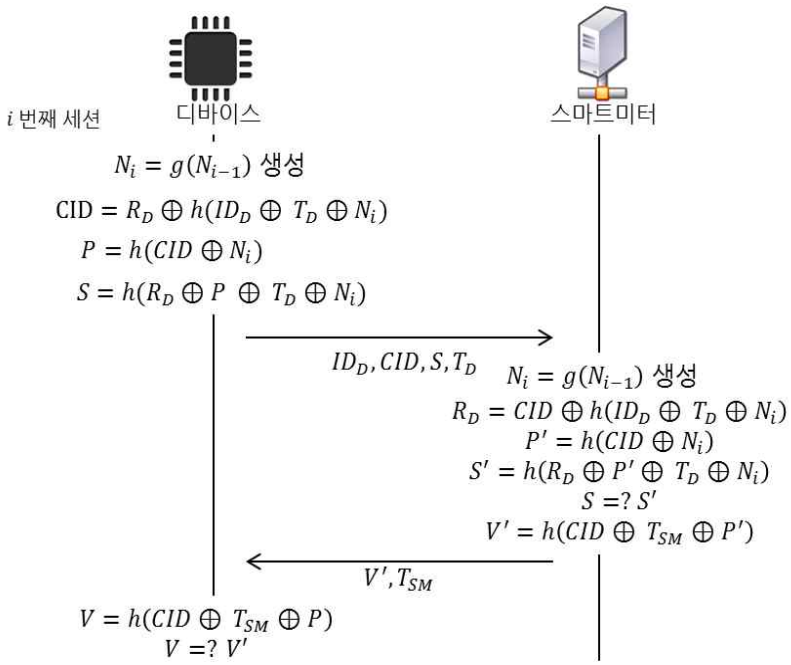

그림 7. 단방향 해시체인기법 인증단계
Fig. 7. Authentication between Device and SmartMeter in One-way hash chain-base Scheme

$$N_i = g(N_{i-1}) \quad (1 < i, N_1 = N_{seed}) \tag{18}$$

$$D:\ CID = R_D \oplus h(ID_D \oplus T_D \oplus N_i)$$
$$P = h(CID \oplus N_i)$$
$$S = h(R_D \oplus P \oplus T_D \oplus N_i) \tag{19}$$

② 디바이스는 생성한 값 중에 P값을 제외한 ID_D, CID, S, T_D를 스마트미터로 전송한다. 스마트미터는 디바이스와 마찬가지로 N_i값을 연산한다.

$$D \rightarrow SM:\ ID, CID, S, T_D$$
$$SM:\ N_i \text{ 생성}$$
$$N_i = g(N_{i-1}) \quad (1 < i,\ N_1 = N_{seed}) \tag{20}$$

③ 스마트미터는 전송받은 값 중에 CID와 N_i를 이용하여 P'값을 생성하고, CID값을 이용하여 난수 R_D값을 추출하여 인증에 필요한 값인 S'값을 만든다.

$$SM:\ R = CID \oplus h(ID \oplus T_D \oplus N_i)$$
$$P' = h(CID \oplus N_i)$$
$$S' = h(R \oplus P' \oplus T_D \oplus N_i) \tag{21}$$

④ 전송받은 S값과 스마트미터에서 생성한 S'값을 비교하여 인증을 진행하며, 인증이 성공할 경우 CID, P'값과 스마트미터의 타임스탬프 값인 T_{SM}를 통해 상호인증에 필요한 값인 V'을 생성하고, V'생성에 사용된 스마트미터의 타임스탬프 값 T_{SM}과 함께 디바이스로 전송한다.

$$SM:\ S' = ? S$$
$$SM:\ V' = h(CID \oplus T_{SM} \oplus P')$$
$$SM \rightarrow D:\ V',\ T_{SM} \tag{22}$$

⑤ 디바이스는 전송받은 T_{SM}값을 이용하여 V값을 생성하고 전송받은 V'값과 비교하여 상호인증을 한다.

$$D:\ V = h(CID \oplus T_{SM} \oplus P)$$
$$D:\ V = ?\ V' \tag{23}$$

표 1. 성능 비교
Table 1. Performance Comparison

구분			KL기법	제안기법1 (OTP사용)	제안기법2 (해시체인사용)
기밀성			○	○	○
무결성			○	○	○
상호인증			○	○	○
전방 보안성	통신내용만 disclosure되는 공격에 대해		×	○	○
	디바이스까지 disclosure되는 공격에 대해		×	×	○
연산량	디바이스 인증	등록단계	1H+2E	3H+4E	1H+2E
		인증단계	8H	10H	10H
	스마트미터 인증	등록단계	2H+2E+2U	2H+2E+2U	2H+2E+2U
		인증단계	2H+4E	2H+4E	2H+4E
통신 횟수	디바이스	등록단계	1	2	1
		인증단계	2	2	2
	스마트미터	등록단계	2	2	2
		인증단계	1	1	1
동기화 문제			-	간단함	어려울 수 있음

○ : 제공, × : 제공안함, H:해시연산, E:대칭키 연산, U:공개키 연산

단계 3. 동기화 실패 처리

인증단계 수행 중 디바이스와 스마트미터의 통신 세션이 끊기는 등의 문제로 인해 N_i값의 동기화가 실패하여 인증을 실패하는 경우가 발생할 수 있다. 이러한 경우, 인증에 실패한 기기는 최근 성공한 인증 이후의 해시체인 값을 차례대로 연산하여 비교함으로써 에러제어를 수행하도록 한다. $MaxError$번의 해시체인 값의 연산을 통하여 에러제어를 수행하며, 만일 $MaxError$번 이후에도 동기화 실패가 일어나는 경우에는 디바이스 재등록과정을 수행하여 인증단계를 진행하도록 한다. $MaxError$는 시스템에서 상황에 따라 설정할 수 있도록 한다.

Ⅴ. 효율성 및 안전성 비교

KL기법과 제안기법 1, 2의 효율성 및 안전성 비교는 다음과 같다.

KL기법의 디바이스 인증방식은 등록단계에서 암호화 처리를 통해 N값을 공유하고 N값의 안전성을 기반으로 인증을 수행하고 있다. 주요 정보인 N을 통신 중간에 공유하지 않아 기밀성이 보장되며, 비밀키 K_A를 해시연산하여 무결성을 보장하고 있다. 또한 생성되는 CID, P, S값에 타임스탬프를 추가하여 매 세션마다 변화되도록 하여 재사용공격에 대비하였으며 디바이스와 스마트미터는 서로 통신하는 기기가 맞는지 확인하는 상호인증이 포함되어 있다[9]. 그러나 비공개 값을 암호화하는 대칭키 혹은 비공개 값 N이 유추될 경우 현재의 정보뿐만 아니라 이전에 사용된 정보들까지 유추할 수 있는 전방 보안성의 취약점이 존재한다. 또한, 연산량 계산에서 누락된 부분이 있어 해시연산의 연산량을 다시 계산하였으며, 암호화에 대한 복호화 과정을 연산량에 포함하지 않아 이 부분을 다시 계산하여 표 1에 제시하였다.

제안기법 1, 2는 비공개 값이 유추될 경우를 상정하여 전방 보안성을 위협하는 요인인 N값이 고정되

지 않도록 생성해주어 인증을 수행하도록 한다. 주요 정보인 N_{seed}값은 등록 시 암호화되어 스마트미터로 전송되어지며 최초의 N_{seed}값이 유추된다 하더라도 이후 인증에 사용된 N_i값을 유추하기 어렵도록 설계하여 전방 보안성을 해결하도록 설계하였다 [9].

제안기법 1은 MDMS를 시간동기화서버로 이용하여 최초의 스마트미터 등록단계에서 시간동기화 값을 MDMS로부터 수신하여 스마트미터의 동기화를 수행한다. 시간동기화가 완료된 스마트미터는 디바이스가 스마트미터로 등록을 요청할 때에 전송하는 비공개 값과 디바이스의 ID를 이용하여 스마트미터의 시간동기화 값을 암호화해 디바이스에게 전송해준다. 디바이스는 시간동기화 값을 복호화하여 시간동기화를 수행한다. 디바이스는 동기화 된 시간을 기준으로 하는 현재 시간 $Time$값과 비공개 값인 N_{seed}값을 OTP 함수에 넣어 N_{OTP}를 생성하여 인증에 사용한다. 만일 N_{seed}값이 유출된다 하더라도 디바이스-스마트미터 인증에 사용되는 값인 N_{seed}값과 동기화 된 시간을 기준으로 한 현재시간인 $Time$을 알고 있어야 최초 인증 정보를 확인할 수 있으며 인증에 사용되는 N_{OTP}값은 매 세션마다 변화하는 $Time$값으로 인해 유추하기 어려워 인증에 대한 정보를 확인하기 어려우며 $Time$값 또한 시간동기화 값인 T_{SYN}를 통신상에 주고받지 않아 인증정보를 확인하기 어렵도록 설계하였다.

제안기법 2의 디바이스 인증방식은 등록단계에서 해시체인을 형성할 주요 정보인 N_1값을 암호화하여 스마트미터로 전송하여 매 세션마다 N_i값을 해시연산하여 인증을 수행한다. 만일 N_i값이 유추된다 하더라도 N_1값을 통해 형성된 해시체인의 값을 유추하기 어려울 뿐만 아니라 매 세션마다 다른 N_i값을 통하여 인증 및 데이터 교환하여 전방 보안성을 지킬 수 있으며 인증을 위한 값을 생성하기 위해 디바이스와 스마트미터에 각 1회의 해시연산을 추가하므로 KL기법과 연산속도가 큰 차이가 없도록 설계하였다.

Ⅵ. 결과 및 검토

제안기법1은 시간동기화가 비교적 간편하나 디바이스 및 스마트미터를 물리적으로 공격할 경우 최초의 비공개 값이 변화하지 않고 동기화 된 시간을 기준으로 하여 주기를 갖는 시간값이 인증에 사용되기 때문에 비공개 값의 유추가 비교적 쉽게 이루어질 수 있어 폐쇄된 구조 등의 물리적 공격에 비교적 안전한 구조에서 일괄적으로 디바이스 또는 스마트미터의 동기화 및 관리해야 하는 환경에서 효율적일 것으로 보인다.

제안기법2는 해시체인을 사용하여 등록 시 주고받는 비공개 값이 매 세션마다 해시함수를 통해 변화하도록 설계되어 제안기법1의 문제점인 물리적 공격에 대한 대비도 이루어진 방식이다. 또한 인증단계 수행 중 디바이스와 스마트미터의 통신세션이 끊기는 등의 문제로 동기화 실패로 인해 인증에 실패하는 경우가 발생하게 될 경우에는 실패한 기기에서 최근 성공한 인증 이후의 해시체인 값을 차례대로 연산하여 비교함으로써 에러제어를 수행하도록 하여 동기화 문제가 발생할 경우를 해결하도록 설계하였다. 또한 기기를 물리적으로 공격할 경우에 대한 안전성을 갖도록 설계하였으므로 사용자 댁내의 디바이스 및 스마트미터에 사용할 경우 효율적일 것으로 보인다.

Ⅶ. 결 론

기존의 연구된 AMI망 환경을 보호하는 기법은 디바이스와 스마트미터 간의 최초 등록 시 전송되는 비공개 값을 이용하여 상호인증을 지원하고 연산속도를 향상시키는 기법을 제안하였다. 그러나 이 기법은 비공개 값이 어느 시점에서 유추될 경우 악의적인 공격자가 모아둔 데이터와 비공개 값을 이용하여 유추된 시점 이전의 데이터를 확인할 수 있는 전방 보안성에 문제가 발생한다. 따라서 본 논문에서는 전방 보안성 문제를 해결하기 위해 MDMS를 시간동기화 서버로 활용하여 스마트미터가 최초 등록 시 MDMS로부터 시간동기화 값을 받아와 디바이스의 등록단계에서 시간동기화 값을 주고받아 디바이스와 스마트미터에 있는 시간동기화 값을 기준으로 하는 현재 시간 값과 비공개 값을 OTP 함수에서 연산하여 동기

화를 진행하는 방식1과 해시체인을 사용하여 디바이스와 스마트미터 간에 등록단계에서 주고받은 비밀값을 이용하여 해시함수로 하여 최초의 비밀값을 유추할 수 없도록 인증에 사용하는 비공개 값이 계속 바뀌도록 하는 방식 두 가지를 제안하였다.

감사의 글

이 논문은 2013년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (2011-0014394).

Reference

[1] J. D. Choi, J. T. Seo, “Separate networks and an authentication framework in AMI for secure smart grid,“ *Journal of the Korea Institue of Information Security and Cryptology,* vol. 22, no. 3, pp. 525-536, June 2012.

[2] J. W. Jeon, S. H. Lim, and O. Y. Yi, “A wireless network structure and AKA(authentication and key agreement) protocol of advanced metering infrastructure on the smart grid based on binary CDMA,“ *Journal of the Korea Institute of Information Security and Cryptology,* vol. 20, no. 5, pp. 111-124, Oct 2010.

[3] J. D. Lee, J. T. Seo, and C. W. Lee, “Smart Grid and Cyber Security,” *The Journal of The Korean Institute of Communication Sciences*, vol. 27, no. 4, pp. 23-30, Mar 2010.

[4] K. B. Lee, J. E. Dokko, J. Y. Yoo, S. Y. Lee, and J. I. Lim, “Consumer Participation and Security Issues in Smart Grid,” *Review of KIISC,* vol. 19, no. 4, pp. 21-35, Aug 2009.

[5] W. G. Nam, H. J. Jo, K. T. Cho, and D. H. Lee, “Study on Smart Grid Security,“ *Review of KIISC,* vol. 20, no. 5, pp. 20-30, Oct 2010.

[6] M. J. Kim, M. Y. Yoon, H. C. Jung, and H. Y. Youm, “Standardization Trend for Smart Grid Security,” *Review of KIISC,* vol. 22, no. 2, pp. 15-22, Apr 2012.

[7] NIST, “Guidelines for Smart Grid Cyber Security,“ *NISTIR 7626*, Aug 2010.

[8] J. Naruchiptparames. M. H Gunes, and C.Y Evrenosoglu, “Secure Communications in the Smart Grid,“ *IEEE Consumer Communications and Networking Conference (CCNC) 2011,* pp. 1171-1175, Jan 2011.

[9] H. K. Kim, I. Y. Lee, “A Study on ID-based authentication scheme in AMI SmartGrid environment,“ *The KIPS transactions. Part C,* vol. 18C, no. 6, pp. 397-404, Dec 2011.

[10] S.-S. Yeo, D. I. Park, and Y. A. Jung, “Enhanced ID-based Authentication Scheme using OTP in Smart Grid AMI Environment,” *Journal of Applied Mathematics, Hindawi, 2014 (to appear).*

[11] G. T. Lee, J. Y. Oh, and Y. K. Kim, “Smart Grid Home Service,” *The Journal of the Korean Institute of Communication Sciences,* vol. 27, no. 4, pp. 38-42, Mar 2010.

박 대 일 (Dae-il Park)

2014년 2월 : 목원대학교 컴퓨터공학부(졸업예정)학과(공학사)
관심분야 : 스마트그리드 보안, 알고리즘, 정보보호 기술

여 상 수 (Sang-Soo Yeo)

2005년 8월 : 중앙대학교 공학박사
2007년 2월~2008년 1월 : 큐슈대학교 정보공학부 방문연구원
2008년 2월~2009년 2월 : ㈜비티웍스 연구개발본부 부장
2009년 3월~현재 : 목원대학교 컴퓨터공학부 조교수
관심분야 : 정보보호 기술 및 정책, 멀티미디어 시스템, 임베디드 시스템, 유비쿼터스 보안 등