논문 2019-2-14 http://dx.doi.org/10.29056/jsav.2019.12.14

스마트미터와 데이터 집중 장치간 인증 및 암호화 통신을 위한 Cortex M3 기반 경량 보안 프로토콜

신동명*† , 고상준*

Cortex M3 Based Lightweight Security Protocol for Authentication and Encrypt Communication between Smart Meters and Data Concentrate Unit

Dong-Myung Shin*† , Sang-Jun Ko*

요 약

기존 스마트그리드 기기 인증 체계는 DCU와 검침 FEP 및 MDMS에 집중되어 있으며 스마트미터에 대한 인증체계는 확립되지 않은 상황이다. 현재 몇몇 암호칩이 개발되었지만, 낮은 강도의 단순 암호화 수준에 머물러 있어 PKI 인증체계를 완성하기에는 어려움이 있다. 스마트그리드는 기존 전력망과 달리 개방형 양방향 통신을 기반으로 함에 따라 정보보안 취약성이 높아지면서 사고 위험 증가하고 있다. 하지만 스마트미터에는 PKI가 적용되기 어려워, 조작한 패킷을 보내 운영시스템에 거짓 정보 전송으로 시스템 정지 등의 사고가 발생할 가능성 존재한다. 하드웨어 제약사항이 많은 스마트미터에 기존 PKI 인증서를 발급할 경우 인증 및 인증서 갱신이 어렵기 때문에 스마트미터의 열악한 성능(Non-IP 네트워크, 프로세서, 메모리 및 저장소 공간 등)에서도 작동 가능한 초 경량 암호 인증 프로토콜을 설계 구현하였다. 실험 결과 Cortex-M3 환경에서도 경량 암호 인증 프로토콜을 빠른 시간 내에 수행 할 수 있었으며, 앞으로 스마트그리드 산업에서의 더 안전한 보안성을 갖춘 인증 시스템을 마련하는데 도움을 줄 수 있을 것으로 기대한다.

Abstract

The existing smart grid device authentication system is concentrated on DCU, meter reading FEP and MDMS, and the authentication system for smart meters is not established. Although some cryptographic chips have been developed at present, it is difficult to complete the PKI authentication scheme because it is at the low level of simple encryption. Unlike existing power grids, smart grids are based on open two-way communication, increasing the risk of accidents as information security vulnerabilities increase.

However, PKI is difficult to apply to smart meters, and there is a possibility of accidents such as system shutdown by sending manipulated packets and sending false information to the operating system. Issuing an existing PKI certificate to smart meters with high hardware constraints makes authentication and certificate renewal difficult, so an ultra-lightweight password authentication protocol that can operate even on the poor performance of smart meters (such as non-IP networks, processors, memory, and storage space) was designed and implemented. As a result of the experiment, lightweight cryptographic authentication protocol was able to be executed quickly in the Cortex-M3 environment, and it is expected that it will help to prepare a more secure authentication system in the smart grid industry.

* 엘에스웨어(주)
† 교신저자: 신동명(email: roland@lsware.com)
접수일자: 2019.11.29. 심사완료: 2019.12.12.
게재확정: 2019.12.20.

한글키워드 : 스마트미터기, 데이터집중장치, 인증서버, 저사양 암호 프로토콜, 타원곡선 알고리즘

keywords : Smart meter, Data Concentrator Unit, Trusted Agent, Low specification crypto-graphic protocol, Elliptic curve algorithm

1. 서 론

스마트그리드는 기존 전력망과 달리 개방형 양방향 통신을 기반으로 함에 따라 정보보아 취약성이 높아지면서 사고 위험성이 날이 갈수록 증가하고 있다. 이에 국내 스마트그리드 PKI 인증센터에서는 다양한 스마트그리드 분야 및 기기를 대상으로 PKI 인증을 실증하였다. 하지만 스마트미터에는 여러 문제로 인하여 PKI가 적용되기 어렵다. 조작한 패킷을 보내 운영시스템에 거짓 정보 전송으로 시스템 정지 등의 보안 사고가 발생할 수 있으며, 하드웨어 제약사항이 많은 스마트미터에 기존 PKI 인증서를 발급할 경우 인증 및 인증서 갱신이 어려운 문제 또한 발생한다. 이러한 문제점을 극복하고자 국,내외에서 많은 연구 및 기술개발이 진행되고 있다.

한전 KDN은 국제표준 기술에 기반하여 PKI 기반 기기 인증서를 발급하고 인증할 수 있는 인증시스템을 개발하였다. 또한 DCU(데이터집중장치)와 AMI 상위관리 시스템인 MDMS간 PKI인증 실증시험을 완료하였다. 그러나 스마트미터와 DCU구간의 PKI인증체계는 하드웨어적인 성능 이슈로 완전하지 못한 상태이다. 따라서, 스마트미터와 DCU 사이에는 내부가 아닌 외부 모뎀을 설치해 보안 시험이 이루어졌다. 또한 스마트미터의 제조단계에서 인증서를 주입하므로 인증서 갱신의 어려움이 존재하였다[1.2.3].

미국 SafeNet의 PKI 기반 스마트그리드 보안 기술[4]에서도 AMI, DR, EVCI 등 새로운 스마트그리드 서비스를 위한 PKI 기반의 암호인증 기술을 개발하고 PKI 기반의 인증서가 탑재된 스마트그리드 기기를 전력회사로 납품하였지만, 별도의 외부 보안 모뎀(게이트웨이)을 사용하여 비용이 상승하였고 결국 많은 보급이 되지 못하였다. 또한 인증서 갱신이 어려운 문제도 존재하였다[5,6,7.8].

본 연구에서는 스마트미터에 적합한 인증체계 연구 개발을 통해 저사양 IoT 환경인 스마트미터에 적합한 알고리즘을 연구 개발하였다. 신뢰기관 기반의 간편 기기인증 체계를 개발하여 스마트미터와 DCU간의 기기 인증 서비스를 제공하였으며, 기존의 시스템들과는 다르게 저사양에서 높은 암호강도를 갖는 타원곡선 알고리즘을 최적화하여 Cortex M3칩에 적용하였다[9,10]. 스마트미터와 DCU간의 안정한 통신채널을 구축하므로써 최종적으로 지능형 원격검침 인프라에 대한 End-to-End 보안체계를 확립하였다.

2. 타원곡선 알고리즘 기반 간편 인증 프로토콜

개발한 프로토콜은 다수의 스마트미터와 DCU, 인증서버(TA)에서 시험되었다. 스마트미터는 건물 내외부에 설치되어 사용자의 전력 사용량을 계측하여 ST32(Modem)을 이용하여 DCU로 전송한다. DCU는 스마트미터로부터 전력 사용량 등의 데이터를 수집 및 저장하고, 이를 전력 공급자 측의 계량 데이터 관리 시스템(MDMS)로 전송한다. TA는 신뢰할 수 있는 기관이 운영하는 것으로, DCU와 Meter 간의 상호 인증을 제공한다.

DCU와 TA는 에러율이 낮고 속도가 빠른 이더넷 네트워크를 통해 연결되지만, 스마트미터와 DCU는 전력선 통신 네트워크(RS-485)과 같이 이더넷 통신 환경에 비해 에러율이 높고 속도가 느린 통신 네트워크를 통해 연결된다[11]. 따라서 원격 검침 시스템 및 스마트 미터 인증 방법은 스마트미터와 DCU간 저품질의 통신 환경과 스마트미터의 낮은 컴퓨팅 파워에 적합하게 설계하였다. 그림 1은 타원곡선 알고리즘 기반의 간편 인증 프로토콜의 시나리오를 도식화한 것이다.

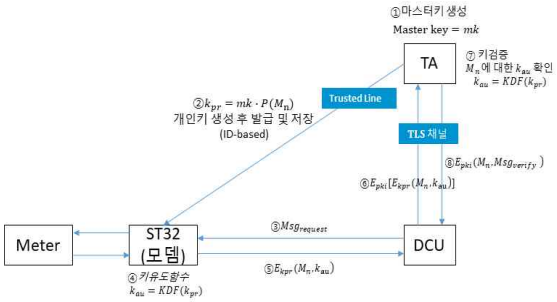

그림 1. 스마트미터 간편 기기 인증 시나리오
Fig. 1. Smart Meter Simple Device Authentication Scenario

- mk : 마스터키
- M_n : 미터 고유번호
- $P(M_n)$: 미터 고유번호로 공개키 생성
- k_{pr} : 개인키
- k_{au} : 미터 인증키
- $E_{pkr}()$: 개인키로 암호화한 메시지
- $E_{pki}()$: pki로 암호화한 메시지
- $Msg_{request}$: 인증 요청 메시지
- Msg_{verify} : 인증 검증 메시지

2.1 마스터키 생성

인증서버(TA)는 전체 마스터키를 생성한다. TA는 서버급의 PC로 운영 가능하므로 난수 발생기를 무리 없이 사용할 수 있고, 따라서 해당 난수발생기를 이용하여 안전한 마스터키를 생성한다.

2.2 개인키 생성 및 발급

TA에서 각 Meter별 개인키(k_{pr})를 생성하고 개발 보드에(Modem)에 각각의 개인키(k_{pr})를 발급한다. 이때 TA와 Modem은 완전히 신뢰 가능한 구간이라는 가정이 존재하며, 본 과제에서는 Meter별 발급된 개인키(k_{pr})를 직접 주입하였다. 개인키는 본 과제에서 개발한 ID-based 타원곡선 연산 알고리즘을 통해 생성되었으며 식은 다음과 같다.

$$k_{pr} = mk \circ P(M_n)$$

TA에서 가지고 있는 마스터키(mk)와 미터 고유번호로 생성된 공개키($P(M_n)$)를 기반으로 각 Meter별 개인키를 생성한다. 이때 각각의 데이터 크기는 미터 고유번호(M_n) 32byte, 미터의 공개키($P(M_n)$)는 32byte, Meter의 개인키(k_{pr})는 32byte로 구현되었다.

2.3 스마트미터 인증 요청

DCU에서 Meter로부터 전력 사용량을 송신받기 전에 해당 스마트미터가 안전한 스마트미터기인지 안전하지 않은지 확인인하기 위해서 인증요청($Msg_{request}$)을 보낸다. 여기서 DCU는 일반 PC환경이라 가정하고, Meter의 전력 사용량을 송신받기 위해 개발 보드를 통해 Meter의 전력 사용량을 받고, Modem은 DCU에게 전달하게 된다. Modem과 DCU는 시리얼 통신(RS-485)으로 연결되어 있으며 RS-485통신의 특성상, 하나의 DCU는 여러개의 Modem의 데이터를 전송받을 수 있다. DCU에서 Modem으로 보내는 인증 요청 payload는 다음과 같다.

*패킷 Header	*Msg Type 정보
Byte 1 : Magic Number	01 : 미터 인증 요청
Byte 2 : Packet Size	02 : 미터 인증 응답
Byte 3 : Msg Type	03 : 미터 데이터 값 요청
Byte 4 : MCC(Msg Check)	04 : 미터 데이터 값 응답

2.4 키 유도 함수

인증 요청($Msg_{request}$)을 받은 Modem은 TA로부터 주입되었던 Meter의 개인키(k_{pr})와 키유도함수(KDF())를 이용하여 인증키(k_{au})를 유도하며, 해당 식은 다음과 같다[12.13].

$$K_{au} = KDF(k_{pr})$$

키유도함수(KDF())는 SHA256을 사용하였으며, 개인키(k_{pr})를 직접 통신상에서 전송할 수 없기 때문에 해쉬함수를 이용하여 인증키(k_{au})를 만들어 전송하게 된다.

2.5 모뎀인증 응답

DCU로부터 Meter 인증 응답을 받은 Modem은 키유도함수를 이용하여 개인키(k_{pr})로부터 인증키(k_{au})를 만들고, Meter의 미터 고유번호(M_n)와 인증키(k_{au})를 전송한다.

여기에서 미터 고유번호(M_n)와 인증키(k_{au})도 평문으로 전송하는 것이 아니라, ARIA 대칭키 알고리즘으로 암호화하여 전송하게 되고, ARIA 대칭키 알고리즘[14]의 키로는 Meter의 개인키(k_{pr})를 사용하게 된다. 즉, $M_n, E_{kpr}(k_{au})$를 전송한다.

2.6 DCU에서 TA로 모뎀 인증 요청

DCU는 값을 전달받은 Meter의 개인키(k_{pr})를 알지 못하기 때문에, Modem으로부터 전달받은 데이터 $M_n, E_{kpr}(k_{au})$를 복호화 할 수 없고 인증 여부조차 알 수 없다. 따라서 DCU는 Modem으로부터 전달받은 데이터를 그대로 TA로 전송한다. DCU와 TA는 PC와 PC의 연결로 가정하기 때문에 TLS 채널을 이용하여 PKI 기반으로 데이터를 전송할 수 있다. 즉, DCU는 TA로 $E_{pki}[M_n, E_{kpr}(k_{au})]$를 전송한다.

2.7 TA에서의 키 검증

TA는 DCU와의 PKI 기반으로 통신되기 때문에 D_{pki}를 할 수 있고, 마스터키로 DCU로부터 전달받은 $E_{pki}[M_n, E_{kpr}(k_{au})]$를 복호화하면 $M_n, E_{kpr}(k_{au})$이 나온다. 여기서 나온 미터 고유번호(M_n)와 TA에 저장되어 있는 마스터키(mk)를 이용하여 2단계에 있는 $k_{pr} = mk \circ P(M_n)$ ID-based 타원곡선 연산 알고리즘으로 전송받은 Meter의 개인키(k_{pr})를 구할 수 있다. 또한 SHA256을 이용하여 키유도함수(KDF())로 인증키(k_{au})를 도출하여 전달받은 인증키와 일치/불일치 여부를 판단할 수 있다.

2.8 DCU로 인증값 전달

TA는 요청받은 키값을 검증하여 DCU로 다시 PKI 기반 암호화하여 $E_{pki}(M_n, Msg_{verify})$를 전송한다.

인증검증 메시지(Msg_{verify})는 성공시와 실패시로 나뉘며 성공시에는 해당 Meter의 개인키(k_{pr})를 전송해주어 DCU가 앞으로 Modem과 전력 사용량 등 데이터 송수신을 할 때 ARIA 대칭키 암호화 알고리즘의 키값으로 사용할 수 있게 해준다. 실패시에는 fail 메시지를 전송하므로써 해당 Meter가 올바른 Meter가 아니라는 것을 알려주어 연결을 차단하거나 통신상의 오류로 패킷 손실이 생겨 값이 바뀔것에 대비하여 재요청한다.

3. RS485 기반 암호 인증 통신 프로토콜

스마트 미터의 인증 방법의 시나리오는 다음과 같다. TA(인증서버)는 난수 발생기를 이용하여 엔트로피(불확실성)가 충분히 높은 마스터 키를 생성한다. 마스터 키는 다른 기기나 사용자에게는 공개되지 않으며, TA만이 보유할 수 있다.

TA는 Modem 고유의 식별 정보를 생성한다. 이 식별 정보는 원격 검침 시스템 상에서 유일한 것으로, Modem을 식별하고, Modem의 개인키를 생성하는데 사용됨. 고유 식별 정보는 식별 정보

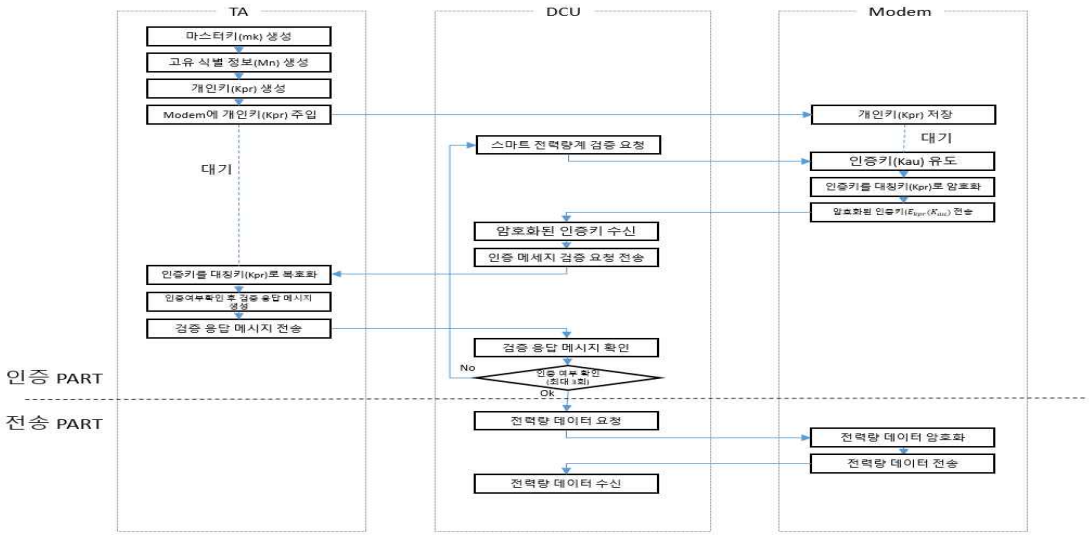

그림 2. 기기간 암호인증 통신 구조
Fig. 2. Password authentication communication structure between devices

를 생성하는 대신에, Modem에 이미 부여된 고유한 식별 정보를 활용할 수도 있다.

TA는 마스터 키와 식별 정보를 이용하여 Modem을 위한 개인키를 생성한다. 이때 TA는, RSA(Rivest-Shamir-Adleman), 디피-헬만(Diffie-Hellman) 암호화 알고리즘, 해쉬함수, 타원곡선 점연산(ECC Point Multiplication) 중 적어도 하나를 이용하여 마스터 키와 식별 정보를 연산함으로써 개인키를 생성할 수 있으며, 본 과제에서는 ID-based 타원곡선 알고리즘을 사용한다.

생성된 개인키는 Modem에 주입됨. 인증키의 주입은, 원격 검침 시스템의 운영자 또는 사용자 등에 의해 Modem에 물리적으로 주입될 수 있다.

TA는 생성한 개인키를 즉시 삭제하므로써 TA는 개인키를 보유하지 않으며, 마스터 키와 Modem 고유의 식별 정보를 보유한다. 따라서 Modem의 개인키는 오직 해당 Modem만이 보유하게 된다.

DCU가 Modem으로부터 전력 사용량 등의 데이터를 받아야 하는 등 DCU와 Modem 간의 통신이 요구되면, DCU는 Modem이 유효한 장비인지 인증하기 위해 Modem에게 인증 요청 메시지를 전송한다.

인증 요청 메시지를 수신한 Modem은 자신이 보유하고 있는 개인키를 소정의 암호화 방식으로 암호화하여, 암호화된 인증키를 생성한다. 여기서 암호화 방식은 공개키 기반 암호화가 아닌, 비교적 적은 컴퓨팅 자원으로도 가능한 해시 암호화(예컨대 SHA-224, SHA-256, SHA-384, SHA-512 등)와 같은 단방향 암호화 알고리즘을 사용할 수 있으며, 본 과제에서는 SHA-256 해시를 사용한다.

Modem은 생성한 암호화된 인증키를 포함하는 응답 메시지를 DCU로 전송한다. Modem이 응답 메시지를 전송할 때, 응답 메시지를 공개키 기반 암호화가 아닌 비교적 적은 컴퓨팅 자원으로도 가능한 대칭키 암호화 알고리즘(예컨대 ARIA, SEED, LEA, HIGHT 등)를 이용하여 암호화하여 전송할 수 있으며, 본 과제에서는 ARIA 대칭키 암호화 알고리즘을 사용한다.

응답 메시지를 수신한 DCU는 응답 메시지가 대칭키 암호화 알고리즘으로 암호화되어 있다면, DCU는 해당 대칭키 복호화 알고리즘으로 응답 메시지를 복호화하여 그로부터 암호화된 인증키를 추출할 수 있지만, 현재 DCU는 해당 Modem이 사용한 ARIA 대칭키 알고리즘의 키값을 알지 못하므로 복호화 할 수 없다. 따라서 Modem의 암호화된 인증키를 포함하는 인증키 검증 요청 메시지를 TA로 전송한다. DCU는 컴퓨팅 자원의 제약이 덜하고 TA와는 이더넷 통신망을 통해 통신하므로, 인증키 검증 요청 메시지를 공개키 기반 암호화를 이용해 암호화하여 전송할 수 있다.

인증키 검증 요청 메시지를 수신한 TA는, 인증키 검증 요청 메시지로부터 Modem의 암호화된 인증키를 추출한다. 인증키 검증 요청 메시지가 공개키 기반 암호화를 이용해 암호화되어 있지만, TA는 해당 공개키 기반 복호화를 이용해 인증키 검증 요청 메시지를 복호화하여 그로부터 암호화된 인증키를 추출할 수 있다.

TA는 기 보유하고 있는 마스터 키와 Modem의 식별 정보를 이용하여 개인키를 생성한다. 이때 이전에 Modem의 개인키를 만들었을 때와 동일하게 RSA(Rivest-Shamir-Adleman), 디피-헬만(Diffie-Hellman) 암호화 알고리즘, 해쉬함수, 타원곡선 점연산(ECC Point Multiplication) 중 적어도 하나를 이용하여 상기 마스터 키와 상기 식별 정보를 연산함으로써 개인키를 생성한다.

TA는 생성한 개인키를 통해 이전에 Modem에서 수행한 암호화 방식과 동일한 암호화 방식으로 암호화하여, 암호화된 인증키를 생성한다. 암호화 방식은 Modem과 TA가 사전에 공유하고 있다고 가정한다.

TA는 DCU로부터 받아서 추출된 암호화된 인증키와 생성된 암호화된 인증키를 비교하여 인증키의 유효성을 검증한다. 만일 두 암호화된 인증키가 일치한다면 인증키 검증 요청 메시지에 포함된 인증키는 유효한 것으로서 해당 스마트 미터는 유효한 장비로 볼 수 있고, 만일 두 암호화된 인증키가 일치하지 않는다면 인증키 검증 메시지에 포함된 인증키는 정상적인 인증키가 아닌 것으로 해당 스마트 미터는 유효하지 않은 장비로 볼 수 있다.

TA는 인증키 유효성 검증 결과를 포함하는 인증키 검증 메시지를 DCU로 전송한다. TA 역시 컴퓨팅 자원의 제약이 덜하고 DCU와는 이더넷 통신망을 통해 통신하므로, 인증키 검증 메시지를 공개키 기반 암호화를 이용해 암호화하여 전송할 수 있다.

인증키 검증 메시지를 수신한 DCU는 인증키 유효성 검증 결과를 확인하여 Modem의 유효성을 인증한다. Modem이 유효한 것으로 인증되면, DCU는 Modem과의 통신을 통해 전력 사용량 등의 데이터를 수신하고, Modem이 유효하지 않다면, DCU는 Modem과의 통신을 차단하거나 재전송을 요청한다.

4. 프로토콜 시험 및 검증

본 장에서는 제안한 프로토콜을 구현하고 암호화된 값들이 올바르게 생성되어 전달되는지 확인하였다.

4.1 실험 환경

본 프로토콜은 C언어를 활용하여 개발하였고, 모뎀은 Cortex M3 코어에서 72MHz, 256Kbyte Flash memory, 64Kbyte SRAM 환경에서 실험하였으며, DCU와 TA는 각각 i3-7100 3.9GHz CPU와 8G RAM, ubuntu 16.04 OS로 이루어진 PC 환경에서 실험하였다.

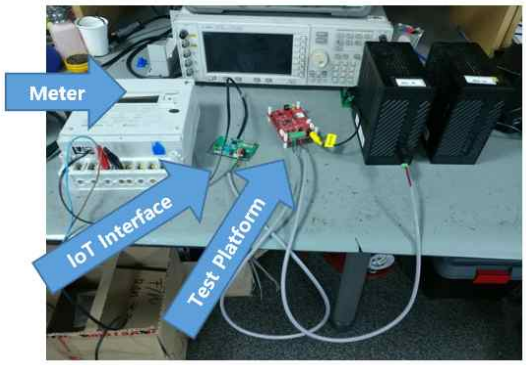

그림 3. 실험환경 구성도
Fig. 3. Experimental Environment

그림 3은 해당 실험의 테스트베드를 구성한 사진이다. TA와 DCU는 두 대의 미니PC를 이용하여 구성하였고, DCU와 스마트미터를 연결하여 보안 모듈을 적용할 Modem을 따로 IoT Interface와 Test Platform 두 가지로 나누어 개발하였으며, 추후에 두 모듈을 하나로 합쳐서 하나의 Modem으로 개발하여 스마트미터 안에 탑재할 예정이다.

4.2 구현

그림 4는 TA에서 마스터키 및 미터기별 개인키를 생성한 화면이다. 난수 발생기를 사용하여 마스터키(mk) Master_key를 생성하고 미터기 고유번호(M_n)을 입력받아 미터기 고유번호로 공개키($P(M_n)$)을 생성한 후 ID-based 타원곡선 알고리즘을 사용하여 미터기의 개인키(k_{pr}) dev_secret_key를 생성한다. 즉, 위의 데모화면에서 사용될 미터기 고유번호(M_n)는 'ST123123123'을 사용했고, 그에 맞는 개인키(k_{pr}) 가 생성되었다.

DCU와 Modem은 115200 통신 속도로 RS-485 시리얼 통신으로 연결되었으며 Modem에서는 이전 단계에서 만든 Meter의 개인키가 주입되어

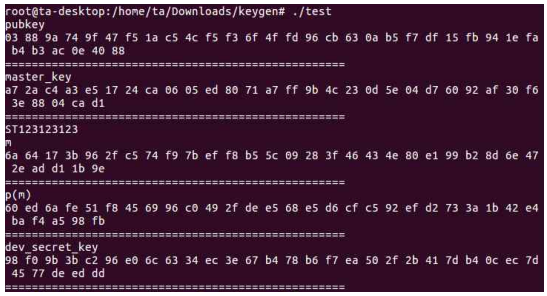

그림 4. 마스터 키 및 미터기별 개인키 생성
Fig. 4. Create master key and private key per meter

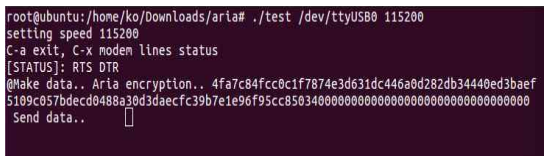

그림 5. 인증 요청 메시지를 받은 Modem
Fig. 5. Modem Receives an Authentication Request Message

있는 상태이다. DCU에서 인증 요청($Msg_{request}$) 메시지를 전송하면 Modem에서는 그림 5에서볼 수 있듯이, 미터기 고유번호(M_n)를 해쉬한 값(32byte)에 키유도함수를 통해 개인키를 인증키로 변환하여 ARIA 대칭 알고리즘으로 암호화한 값(32byte)가 붙여 전송됨을 확인할 수 있다.

DCU는 전송받은 미터기 고유번호(M_n)의 해쉬값 32byte와 인증키를 ARIA 대칭 알고리즘으로 암호화한 값(32byte)를 복호화 할 수 없으므로 전송받은 데이터를 그대로 TLS 채널을 통해 대기하고 있는 TA로 전송하게 된다.

대기하고 있는 TA에 DCU가 Meter의 인증키를 검증하기 위한 메시지를 보내게 되면 TA는 그림 6처럼 DCU에서 보낸 메시지를 PKI 기반의 암/복호화를 수행하여 Meter가 보낸 메시지인 미터기 고유번호(M_n)의 해쉬값 32byte와 인증키를 ARIA 대칭 알고리즘으로 암호화한 값(32byte)를 그대로 수신받게 된다.

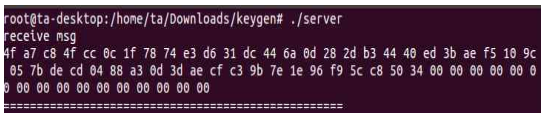

그림 6. TA에서 인증 검증 메시지 수신
Fig. 6. Receive Authentication Verification Message from TA

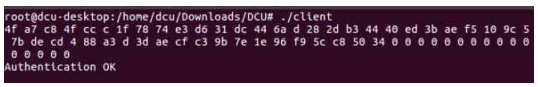

그림 7. DCU에서 인증 성공 메시지를 수신
Fig. 7. Receive authentication success message from DCU

TA는 가지고 있는 미터기 고유번호(M_n)의 해쉬값으로부터 미터기 고유번호(M_n)를 추측하고, 1단계에서 진행했던 미터기 고유번호로 공개키($P(M_n)$)을 생성한 후 ID-based 타원곡선 알고리즘을 사용하여 미터기의 개인키(k_{pr})를 생성한다. 생성한 개인키(k_{pr})를 기반으로 ARIA 대칭 알고리즘으로 복호화한 값을 키유도함수를 통해 인증키(k_{au})와 비교하여 올바른 Meter기의 값이 전송되었는지 확인 후 DCU로 결과값을 전송한다.

그림 7은 Modem으로부터 받은 값을 TA로 전송하여 인증 완료 메시지를 전송받은 화면으로 인증이 완료된 것을 확인할 수 있다.

5. 결 론

스마트그리드의 End-to-End 보안체계를 완성하기 위하여, 스마트미터와 DCU구간의 암호인증 프로토콜을 설계 개발하였다. 신뢰기관(TA) 기반의 인증체계를 통해 스마트미터와 DCU간의 안전한 통신채널을 설계하였으며, 스마트미터의 낮은 성능 및 제한된 메모리를 고려하여 암호 인증 프로토콜을 설계하였다. 또한 소프트웨어적으로 경량암호화에 적합한 타원곡선기반 알고리즘의 하드웨어 칩 최적화 과정을 통해 Cortex M3에서 동작 가능한 프로토콜이 개발되었다. 현재 전자서명을 통한 부인봉쇄 서비스가 가능한 프로토콜 개선이 완료되어 테스트가 진행되고 있으며 확장된 기능으로 늘어난 메모리 소요를 줄이기 위한 2차 최적화 작업이 마무리 단계에 와 있으며, 추후에는 저사양 IoT 기기에서도 적용 가능한 전자서명 기능을 포함한 프로토콜을 개발하므로 써 스마트그리드 산업에서의 더 안전한 보안성을 갖춘 인증 시스템을 마련하는데 도움을 줄 수 있을 것으로 기대된다.

본 연구는 과학기술정보통신부 및 정보통신기획평가원(IITP)의 2019년 연구지원금으로 수행되었음(과제명:스마트그리드 환경에서 PKI와 연동 가능한 간편 암호인증 기술 개발)

참 고 문 헌

[1] Joshitta, R. Shantha Mary, “Device authentication mechanism for IoT enabled healthcare system”, Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET), 2017 International Conference on 2017 Feb ,pp.1-6, 2017. DOI : https://doi.org/10.1109/icammaet.2017.8186646

[2] Vaidya, Binod, Makrakis, Dimitrios, Mouftah, Hussein, “Device authentication mechanism for Smart Energy Home Area Networks”, Consumer Electronics (ICCE), 2011 IEEE International Conference on 2011 Jan ,pp.787-788, 2011, 2158-3994 DOI: https://doi.org/10.1109/icce.2011.5722864

[3] Kim, Young-Sam, Heo, Joon, “Device Authentication Protocol for Smart Grid Systems Using Homomorphic Hash”, Journal of communications and networks v.14 no.6, pp. 606 - 613, 2012, 1229-2370

DOI: https://doi.org/10.1109/jcn.2012.00026
[4] Zhao, Shushan, Akshai Aggarwal, and Robert D. Kent, “PKI-based authentication mechanisms in grid systems”, 2007 International Conference on Networking, Architecture, and Storage (NAS 2007). IEEE, 2007. DOI: https://doi.org/10.1109/nas.2007.42
[5] Khurana, Himanshu, et al., “Smart-grid security issues”, IEEE Security & Privacy 8.1 (2010): 81-85. DOI: https://doi.org/10.1109/msp.2010.49
[6] McDaniel, Patrick, and Stephen McLaughlin, “Security and privacy challenges in the smart grid”, IEEE Security & Privacy 7.3 (2009): 75-77. DOI: https://doi.org/10.1109/msp.2009.76
[7] Metke, Anthony R., and Randy L. Ekl, “Smart grid security technology”, 2010 Innovative Smart Grid Technologies (ISGT). IEEE, 2010. DOI: https://doi.org/10.1109/isgt.2010.5434760
[8] Aloul, Fadi, et al., “Smart grid security: Threats, vulnerabilities and solutions”, International Journal of Smart Grid and Clean Energy 1.1 (2012): 1-6. DOI: https://doi.org/10.12720/sgce.1.1.1-6
[9] Schroeppel, Richard, et al., “A low-power design for an elliptic curve digital signature chip”, International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2002. DOI: https://doi.org/10.2172/802030
[10] Luca, Florian, and Igor E. Shparlinski, “Elliptic curves with low embedding degree”, Journal of Cryptology 19.4 (2006): 553-562. DOI: https://doi.org/10.1007/s00145-006-0544-0
[11] Lin, Ying, et al., “Serial Communication Based on RS485 Bus between PC and Multisinglechip System”, Machinery & Electronics 1 (2006). URL: http://en.cnki.com.cn/Article_en/CJFDTotal-JXYD200601013.htm
[12] Percival, Colin, “Stronger key derivation via sequential memory-hard functions”, (2009). URL: https://www.bsdcan.org/2009/schedule/attachments/87_scrypt.pdf
[13] Chen, Lily, “Recommendation for key derivation using pseudorandom functions”, No. NIST Special Publication (SP) 800-108 (Withdrawn). National Institute of Standards and Technology, 2008. DOI: https://doi.org/10.6028/nist.sp.800-108
[14] Kwon, Daesung, et al., “New block cipher: ARIA”, International Conference on Information Security and Cryptology. Springer, Berlin, Heidelberg, 2003. DOI: https://doi.org/10.1007/978-3-540-24691-6_32

저 자 소 개

신동명(Dong-Myung Shin)

2003년 대전대학교 컴퓨터공학과 박사
2001년-2006년 한국정보보호진흥원(KISA) 응용기술팀 선임연구원
2006년-2014년 한국저작권위원회 저작권기술팀 팀장
2014년-2016년 한국스마트그리드사업단 보안인증팀 팀장
2016년-현재 엘에스웨어(주) 연구소장/상무이사
<주관심분야> 오픈소스 라이선스, 시스템/네트워크보안, 스마트그리드 인증/보안, SW취약점분석·감정/블록체인

고상준(Sang-Jun Ko)

2016년 한국산업기술대 컴퓨터공학과 학사
2018년 성균관대 소프트웨어플랫폼학과 석사
2018년-현재 엘에스웨어(주) 선임
<주관심분야> 코드 유사도, 악성코드 탐지, 블록체인