재전송 공격에 안전한 개선된 AMI 네트워크 인증 프로토콜

황문영*, 곽진**
*순천향대학교 정보보호학과 정보보호응용및보증연구실
**순천향대학교 정보보호학과
e-mail : myhwang@sch.ac.kr, jkwak@sch.ac.kr

Improved AMI Network Authentication Protocol to Secure on Replay Attack

Moon-Young Hwang*, JinKwak**
*ISAA Lab, Department of Information Security Engineering, Soonchunhyang University
**Dept of Information Security Engineering, Soonchunhyang University

요 약

스마트그리드는 에너지 고갈과 지구온난화 등의 환경문제를 해결하기 위한 방안으로 IT와 통신기술을 접목하여 에너지 활용의 효율성을 높이는 기술이다. 스마트그리드는 기존의 전력망에 비하여 소비자와 전력 공급자간 양방향 통신으로 이동하는 정보가 많은데 그 중에서도 스마트미터와 사업자의 정보수집 디바이스인 AMI Headend의 통신영역의 보안이 중요하다. 위와 같은 이유로 스마트미터와 AMI Headend의 통신영역의 보안에 대한 연구들이 많이 이루어지고 있지만 아직 미흡한 실정이다. 따라서 본 논문에서는 스마트그리드의 스마트미터와 AMI Headend 통신영역의 보안을 위한 인증 프로토콜을 제안한다.

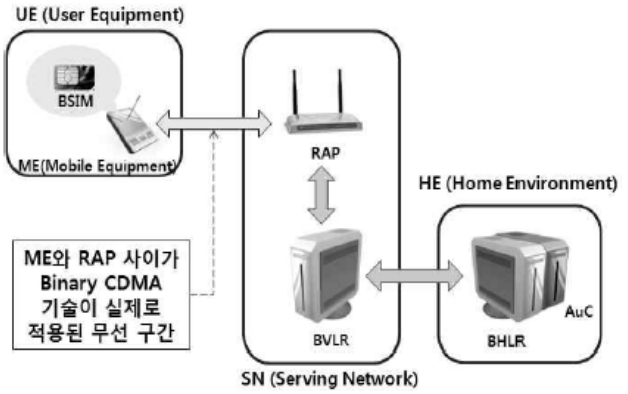
1. 서론

현재 에너지 고갈과 지구온난화 등 환경 문제로 인하여 에너지를 효율적으로 관리하고 친환경 에너지를 사용하자는 '녹색성장(Green Growth)'이 국내외에서 주목을 받고 있다. 이러한 노력의 일환으로 IT 산업에서는 Green IT 개념의 '스마트그리드(Smart Grid)'가 등장을 하였고 이 기술에 대한 관심이 고조되고 있다. 실제로 우리나라를 비롯한 세계 각 국은 스마트그리드의 개발과 보급에 힘을 쓰고 있다. 스마트그리드는 차세대 전력망에 IT 기술을 도입하여 기존의 전력생산, 관리, 송신, 소비의 과정에서 발생할 수 있는 에너지의 불필요한 낭비를 줄이고 에너지를 효율적으로 관리할 수 있는 시스템을 말한다[1][2]. 스마트그리드 기술은 소비자의 에너지 사용을 실시간으로 감시하고 그 결과를 취합하여 분석한 후 그 결과를 다시 소비자에게 전송해줌으로써 소비자와 전력 공급자 사이에 쌍방향 통신을 가능하게 하고 이를 통해 전력 에너지의 소비가 효율적으로 이루어질 수 있게 해준다. 하지만 스마트 그리드는 기존의 전력전송 시스템과 비교하여 쌍방향 통신을 통해 전송되는 민감한 데이터가 증가하였기 때문에 보안적인 측면이 이슈가 되고 있다. 스마트그리드의 중요한 통신 영역 중 하나는 각 가정의 정보를 취합하는 스마트미터와 스마트미터와 전력 공급자 사이에 위치하여 정보를 취합하고 통신을 중계하는 AMI Headend간의 통신 영역이다[3]. 때문에 국내외에서 스마트미터와 AMI Headend의 보안에 대한 연구가 활발히 진행되고 있다. 그 중 전재우 등은 기존의 WCDMA 및 WiBro보다 열악한 환경에서 통신 품질이 우수하고 24시간 동안 중단 없는 서비스를 제공할 수 있는 BLAN(Binary CDMA Lan)를 사용하여 AKA 프로토콜을 제안하였다[4]. 이는 BSIM(Binary CDMA Subscriber Identity Module)을 사용하여 사용자 중심의 서비스 제공이 쉬우나 공격자가 정당한 AMI Headend로 가장하기 위해 AMI Headend와 AuC의 통신을 도청하여 전송하는 재전송 공격에 대한 취약성이 존재한다. 즉, BSIM이 AMI Headend과 AuC의 통신에 대한 보안성을 안전성이 보장된다고 가정하기 때문에 공격자는 BSIM이 AMI Headend를 인증할 때 사용되는 메시지를 이용하여 BSIM에게 정당한 AMI Headend로 인증이 가능하다. 이러한 문제점을 해결하기 위해 본 논문에서는 재전송 공격에 안전한 개선된 AMI 네트워크 AKA 프로토콜을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 BLAN의 구조에 대하여 알아보고 3장에서는 AMI Headend와 AuC 유선구간의 보안 문제점을 분석한다. 4장에서는 개선된 AMI 네트워크 인증 프로토콜을 제안하며 마지막으로 5장에서는 결론을 맺는다.

2. BLAN(Binary CDMA) 구조

BLAN은 유무선 네트워크 공공망을 위한 구조로 (그림 1)과 같이 유무선으로 이루어져 있다. BLAN은



(그림 1) BLAN의 구조

UE(User Equipment), SN(Serving Network), HE(Home Environment)로 구성되며, UE와 SN 사이는 무선 구간, SN과 HE 사이는 유선구간이다. 여기서 UE는 BLAN의 사용자 영역으로, BSIM(Binary CDMA Subscriber Identity Module)과 ME(Mobile Equipment)로 구성된다. SN은 사용자에게 여러 가지 서비스를 제공하기 위한 주체로 RAP(Radio Access Point)와 BVLR (BLAN Visitor Location Register)로 구성된다. HE는 사용자의 개인 정보 및 권한 정보를 저장하며, BLAN-AKA 메커니즘을 지원한다. HE는 BHLR (BLAN Home Location Register)과 인증 서버 (AuC)로 구성된다. 비록 BHLR과 AuC가 논리적으로 서로 다른 개체이지만, 실제로는 물리적으로 같이 구현될 수 있다.

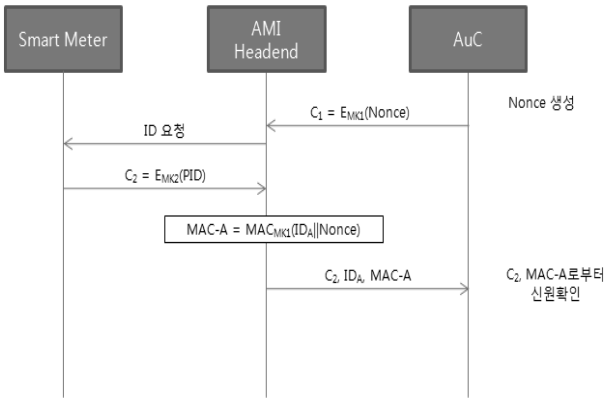
3. AMI Headend와 AuC 유선구간의 보안 문제점

BLAN을 적용한 AMI 네트워크 프로토콜은 AMI Headend와 AuC 유선 구간의 통신은 안전한 채널이 형성되어 안전성이 보장된다고 가정을 하였지만 현재 발전소, 전력통신망, 폐쇄된 형태의 네트워크에서 Stuxnet 등의 공격을 통해 폐쇄네트워크에 침입하여 피해를 입는 사례가 빈번히 보고되고 있다. 이러한 사실에서 AMI Headend와 AuC사이의 유선 구간이 완전히 안전한 채널이 아니라는 것을 알 수 있다. 따라서 AMI Headend와 AuC사이에는 일차적으로 도청공격이 이루어질 수 있고 도청공격을 통하여 BLAN을 적용한 AMI 네트워크 프로토콜에서는 공격자의 재전송 공격으로 이어질 수 있다. 또한 이는 위장공격으로 이어져 스마트미터와 공격자는 정상적인 통신이 가능하게 된다.

4. 개선된 AMI 네트워크 프로토콜

3.1.1 BSIS과 AMI Headend의 신원 확인

AuC는 스마트미터와 AMI Headend의 신원을 확인하기 위하여 다음과 같은 절차를 수행한다.



(그림 2) BSIM과 AMI Headend의 신원확인 과정

1) AuC는 AMI Headend의 신원을 확인하기 위한 Nonce값을 생성하여 AMI Headend와 공유하고 있는 비밀키 MK_1으로 암호화한 C_1을 전송한다.

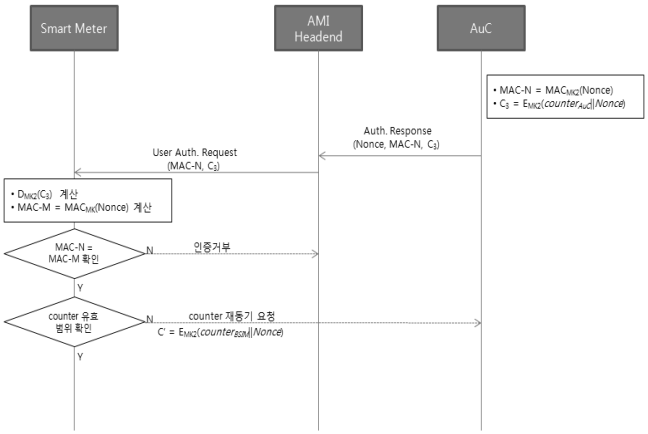
2) AMI Headend가 스마트미터에 ID를 요청을 하고 스마트미터는 AuC와 공유하고 있는 비밀키 MK_2으로 PID를 암호화한 C_2를 전송한다.

3) AMI Headend는 자신이 정당한 디바이스라는 것을 검증하기 위해 1)에서 전송받은 Nonce값에 자신의 ID를 연접하여 MAC_{MK1}를 연산한 후 스마트미터에게 전송받은 C_2, AMI Headend의 고유 ID, MAC-A 값을 AuC에게 전송한다.

4) AuC는 C_2를 복호화해서 얻은 PID와 MAC-A로부터 전송받은 IDA를 통해 스마트미터와 AMI Headend의 신원이 유효한지 확인한다.

3.1.2 스마트미터의 AMI Headend 인증

스마트미터는 AMI Headend를 인증하기 위하여 다음과 같은 절차를 수행한다.



(그림 3) 스마트미터의 AMI Headend 인증 과정

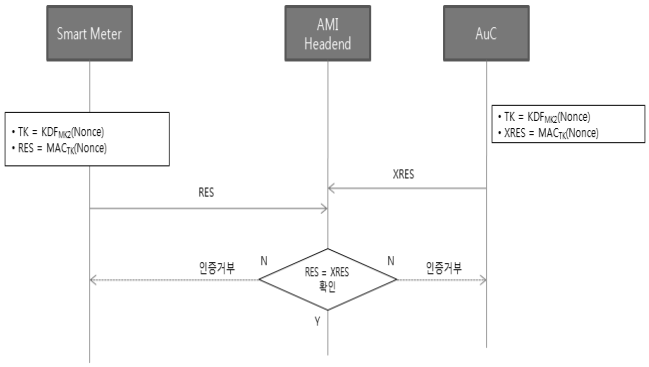
1) AuC는 스마트미터와 공유하고 있는 비밀키 MK_2값으

로 MAC_{MK2}(Nonce)값과 freshness를 위한 카운터 값을 포함한 C_3을 계산한다.

2) AMI Headend는 스마트미터에게 AuC로부터 전송받은 값 MAC-N과 C_3값을 전송한다.
3) 스마트미터는 자신이 가지고 있는 MK_2값으로 C를 복호화하여 Nonce값과 Counter값을 알아낸 후 MAC_{MK2}(Nonce)값을 계산한다.
4) 전송받은 MAC-N값과 자신이 계산한 MAC-M값을 비교하여 같으면 인증을 하고 자신이 보유한 Counter값과 전송 받은 Counter값을 비교하여 재동기 여부를 결정한다.
5) Counter값이 사전에 설정된 유효범위를 벗어나게 되면 AuC와 공유하고 있는 비밀키 MK_2를 사용하여 카운터 값을 암호화 후 AuC에게 전송하여 재동기 요청을 한다.

3.1.3 AMI Headend의 스마트미터 인증

AMI Headend는 스마트미터를 인증하기 위하여 다음과 같은 과정을 거친다.



(그림 4) AMI Headend의 스마트미터 인증

1) AuC는 Nonce값을 이용하여 스마트미터 인증을 위한 임시키 TK를 비밀키 MK_2를 이용하여 생성하고 TK를 이용하여 MAC_{TK}(Nonce)를 계산하여 AMI Headend에게 전송한다.
2) 스마트미터는 비밀키 MK_2를 이용하여 임시키 TK를 생성하고 사전에 전송받은 Nonce값을 이용해 MAC_{TK}(Nonce)를 계산하여 AMI Headend에게 전송한다.
3) AMI Headend는 AuC에게 전송받은 MAC_{TK}(Nonce)값 XRES와 스마트미터에게 전송받은 MAC_{TK}(Nonce)값 RES를 비교하여 스마트미터를 인증한다.

위의 AuC의 BSIM, AMI Headend의 신원확인 과정, 스마트미터의 AMI Headend 인증 과정, AMI Headend의 스마트미터 인증과정을 통하여 스마트미터와 AMI Headend는 상호인증이 가능하게 되고 상호인증 후의 키 교환을 통하여 스마트미터와 AMI Headend 구간의 무선통신 AMI Headend 구간의 유선통신을 포함한 AMI 네트워크의 전반적인 영역에서 안전한 통신이 가능하다.

5. 시서점 및 결론

AMI Headend에서는 스마트그리드 사용자의 에너지 사용 정보, HAN(Home Network Area) 망 상태 정보, AMI 장치 상태 정보, 에너지 상태 정보, 에너지 가격 정보, AMI 망 제어 정보 등 여러 가지 정보의 교환이 지속적으로 발생한다. 만약 공격자가AMI Headend로 위장을 한 후 위와 같은 정보들을 수집할 수 있다면 공격자와 연결된 하위의 모든 AMI 장치들이 피해를 입을 수 있다. 또한 AMI 장치 뿐 아니라 과금 정보의 변경이 이루어진다면 스마트그리드의 사용자는 인터넷 뱅킹의 수준과 비슷한 금전적인 피해를 입힐 수 있다.

본 논문에서는 위와 같은 피해를 막기 위하여 기존의 Binary CDMA를 이용한 AMI 네트워크 구조의 AMI Headend와 AuC의 유선구간에서 발생할 수 있는 도청, 재전송 공격, 위장 공격 등의 문제점을 보완할 수 있는 프로토콜을 제안하였다. 제안된 프로토콜은 AMI 네트워크 구간에 필요한 기밀성 및 무결성을 보장하며 BLAN의 장점을 그대로 적용이 가능하다.

참고문헌

[1] U. S. Department of Commerce, "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0 (Draft)," pp.83-84, 2009

[2] P. McDaniel, S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," IEEE Security and Privacy, Vol.7, No.3, pp.75-77,2009

[3] F.M. Cleveland Senior, "Cyber Security Issues for Advanced Metering Infrastructure" IEEE, 2008

[4] 전재우, 임선희, 이옥연, "스마트 그리드를 위한 Binary CDMA 기반의 AMI 무선 네트워크 구조 및 AKA 프로토콜", 정보보호학회논문지, 2010

[5] Coalton Bennet, Darren Highfill, "Networking AMI Smart Meters", IEEE Energy, 2008

[6] 최승환, 정남준, 조랑훈,, "스마트그리드 환경의 AMI 구현을 위한 요구사항 분석", 한국전력공사, 2010

[7] Andrew Wright, Daniel Thanos et al, "Bottom-Up Security Analisys of the Smart Grid", 2011