AMI 보안적용을 위한 기기보안 기술에 관한 연구

온인석*, 이성훈*, 이승원*
*한전KDN
e-mail : jse315.tm@kdn.com

A Study on Device Security Technique for AMI System

Inn-Seok Onn*, Seong-Hun Lee*, Seung-Won Lee*
*KEPCO KDN

요 약

AMI 기술은 스마트 미터의 검침 데이터를 수집하고 이에 대한 전력사용 정보를 수용가에게 제공하는 지능화된 전력 네트워크 시스템이다. AMI 네트워크는 공개된 통신망에서 양방향 네트워크 기술을 사용하기 때문에 데이터 전송에 대한 데이터의 신뢰성이 무엇보다 중요하다. 일반적인 AMI 통신망 구조에서는 악의적인 사용자의 공격에 노출되어 다양한 종류의 피해 사례가 발생할 수 있다. 따라서 본 논문에서는 AMI 시스템 기기에 대하여 안전한 데이터 송수신을 위한 보안적용 기술에 대하여 기술한다.

1. 서론

스마트그리드는 기존의 발전, 송변전, 배전 및 수용가에 이르기까지 전력에너지 공급의 단위별 전력공급체계에 정보통신기술이 결합된 상호 유기적이고 지능화된 전력 네트워크 시스템이다.

스마트그리드의 최말단 수용가 측과의 연결고리는 AMI (Advanced Metering Infrastructure)시스템이 담당하게 되며, 이때 AMI 시스템에 대한 보안 기능은 필수로 요구된다. 본 논문에서는 AMI 기기에 대한 기기간 상호인증, 키 교환 및 암복호화 통신을 연구함으로써 AMI기기 적용을 위한 보안모델을 제안하고자 한다.

AMI 시스템은 수용가 측에 설치되어 있는 Smart Meter, 변대주에 설치되어있는 DCU(데이터집중장치), 검침센터에 설치되어 있는 FEP(Front-End Processor)서버를 포함한 서버류들로 구성되어진다. Smart Meter와 DCU간은 PLC(Power Line Communication), ZigBee, Binary CDMA등의 다양한 통신방식으로 Meter의 검침데이터를 DCU가 수집하며, DCU가 수집한 검침데이터는 HFC망, TRS망 등의 WAN구간을 통하여 상위서버로 전송되어진다. DCU로부터 전송된 데이터는 FEP서버를 거쳐 AMI서버등으로 전송되어진다.

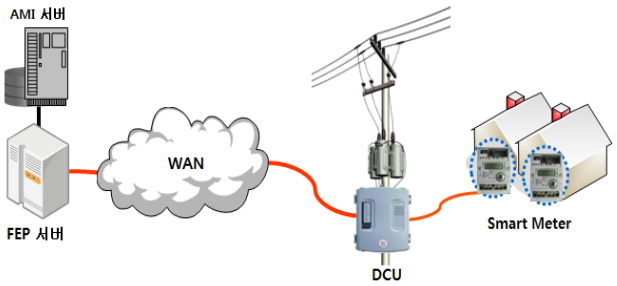
2-1. AMI 시스템의 보안위협

AMI 시스템은 스마트그리드의 근간을 이루며 또한 동시에 악의적인 행위의 공격대상이자, 스마트그리드망에 연계된 다른 시스템으로의 침입경로가 되며, 이는 스마트그리드의 치명적인 약점이 될 수 있으며 있으며, 이로 인한 스마트그리드의 보안취약성 증가 요인이 된다.[1] 이와 같은 보안위협에 따른 주요 취약성으로는 사이버 공격으로 인한 전력시스템 제어권의 상실이다. WAN구간과 연계되는 AMI망은 기존 인터넷망이 가지고 있는 보안취약성으로 인해 외부 공격에 쉽게 노출되어질 수 있다. 또한 기존 네트워크 망에서 사용되는 범용적인 통신장비 및 서버시스템을 사용함으로써 이들 시스템이 가지고 있는 보안 취약성이 스마트 그리드 취약성으로 연결되는 것이다.

이로 인한 가장 큰 공격 위협은 스마트그리드망에 침투하여 전력시스템의 제어권을 획득한 후 전력공급의 차단등 전력 통제권의 상실로 직결되어질 수 있다는 것이다.[1] 또한 2009년 미국에서 수행된 스마트그리드 모의해킹(CNN 2009. 3)에서 내부로의 손쉬운 침투가 가능함이 확인 되었으며 침투한 해커는 대규모의 스마트 미터 조작이 가능할 수 있었는데 이는 전기 수요 증감을 통한 전력망 불안정을 유도해 대도시를 대상으로한 정전 사태 유발까지 이루어질 수 있으며, 나아가 사이버 무기화로서의 가능성을 말해주는 것이다.[2]

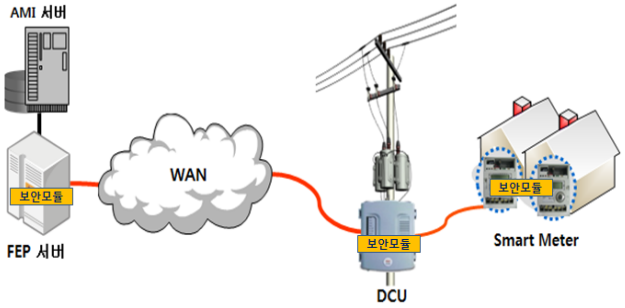
2-2. AMI 시스템 기기적용 보안모델

본 논문에서는 AMI 시스템의 대상 기기간 상호인증, 키교환 및 암복호화 통신을 기반으로한 AMI 보안적용 기술을 논하고자 하며, [그림1]은 AMI 시스템의 구성개요이다.



[그림1] AMI 시스템 개요

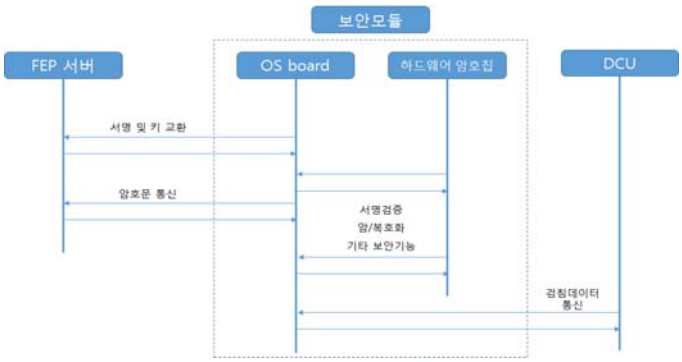
AMI 시스템의 보안 모델의 적용 대상 기기는 [그림2]에서와 같이 수용가측에 설치된 Smart Meter, 변대주에 설치된 DCU, 검침센터에 설치된 FEP서버를 그 대상으로 하며, 각각의 대상에 대하여 보안모듈을 적용하여 기기 상호간 인증, 키교환 및 암복호화 통신을 수행한다.



[그림2] AMI 시스템 기기 적용 보안 모델 개요

2-3. H/W 암호칩을 이용한 보안모듈 구현

[그림3]은 AMI 시스템 보안적용에 대하여 H/W 암호칩을 이용하여 DCU 연동 보안모듈을 구현한 구성도이다.



[그림3] H/W암호칩을 이용한 DCU연동 보안모듈 구현

보안모듈은 AMI 보안프로토콜에 따라 DCU와 연동하여 FEP과의 상호인증, 서명검증 및 키 교환, 데이터 암복호화를 수행한다.

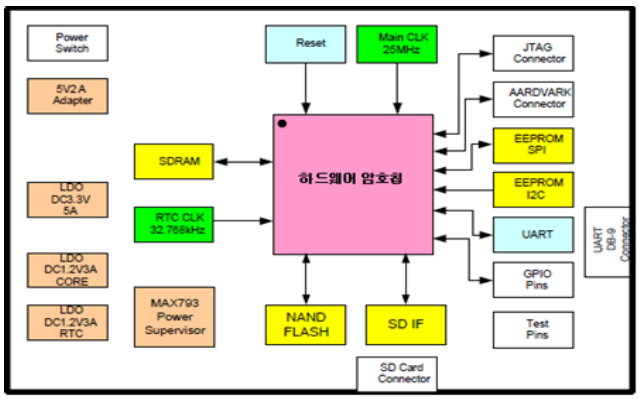
구분	알고리즘	
비밀키 암호	ARIA	Mode : ECB, CBC, CFB(128), OFB(128), CTR Key Size: 128, 192, 256 bit
	AES	Mode : ECB, CBC, CFB(128), OFB(128), CTR Key Size: 128, 192, 256 bit
MAC	HMAC	Hash : SHA-256
해쉬함수	SHA-256	SHA 해시함수
난수발생기	CTR-DRBG	ARIA 기반
전자서명	ECDSA	ECC
키공유	ECDH	ECC

<표 1> H/W 암호칩 대상 알고리즘

H/W암호칩을 이용한 보안모듈 구현시의 대상 암호알고리즘은 위의 <표 1>과 같다.

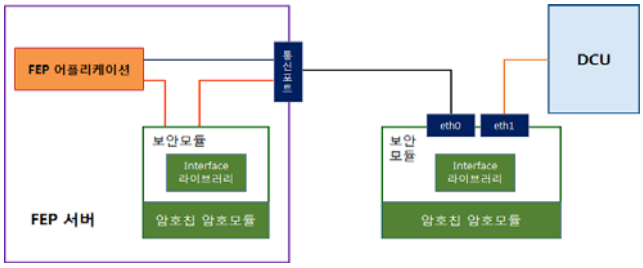
암복호화시의 비밀키는 ARIA, AES를 사용하며, MAC은 HMAC, 해시함수는 SHA-256, 난수발생기는 CTR-DRBG, 전자서명은 ECDSA, 키공유 방식은 ECDH방식을 사용한다.

[그림4]는 H/W 암호모듈 기능 블록도이다.



[그림4] 암호모듈 기능 블록도

[그림5]는 DCU 연동 보안모듈과 FEP간의 시험환경 구축 구성을 나타난 것이며, AMI 보안프로콜에 따라 기기 인증서 검증, 키토큰 생성, 키토큰 전달, 키토큰 확인, 세션키 생성, 서명 생성, 서명 전달, 서명검증, 메시지 암복호화 통신을 수행하게 된다.



[그림5] DCU연동 보안모듈 시험환경 구축

5. 결론

본 논문은 AMI 기기적용을 위한 보안에 있어 기기간 상호인증 및 데이터 암·복호화를 통한 AMI 보안 적용 모델에 대하여 언급하였지만, 이것만으로는 악의적인 사용자의 행위에 대해서는 그 이상의 보안사항이 요구되어질 것이며 이에 대한 보안성 강화를 위하여 물리적 보안 등 추가적인 보안시스템 도입과 개선이 필요하다.

참고문헌

[1] 한국방송통신전파진흥원, “스마트 그리드에서의 취약성 보안 기술”, 2013년

[2] 국가보안기술연구소, “스마트그리드 보안 추진현황 및 이슈”, 2014년