대칭키 기반의 한전KDN AMI 통신망 보안 설계*

오지은, 이옥연
국민대학교 수학과
e-mail:arhanaz@kookmin.ac.kr , oyyi@kookmin.ac.kr

Designing communication network security of KEPCO AMI System based on Symmetric-key

Jieun Oh, Okyeon Yi
Dept. of Mathematics and CISI, Kookmin University

요 약

지능형 전력망인 AMI(Advanced Metering Infrastructure)에 대한 관심이 높아지고 있다. AMI 시스템은 전력의 제공자와 소비자가 양방향 통신을 함으로써 전력의 효율적인 관리를 위한 것이지만 기존의 전력망에 통신망인 IT의 결합으로 인한 보안 문제에 대한 대응방안이 필요하다. 본 논문에서는 한전KDN(주)가 규정하여 추진하고 있는 AMI 시스템의 문제점을 분석하고, 한전의 규정상에서 적용 가능한 대칭키 기반의 보안으로 안전한 AMI 시스템의 통신망 구조를 제시하여 암호화 및 메시지인증을 통해 기밀성, 무결성, 가용성 등의 보안 요건을 만족시킬 수 있는 통합적인 관리를 제안한다.

1. 서론

스마트 그리드(Smart Grid)는 기존의 전력망에 정보기술(IT)를 접목하여 전력 공급자와 소비자가 양방향으로 실시간 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 지능형 전력망으로 세계 각국에서 주목받고 있으며, 한국의 경우 저 탄소 녹색성장의 표어 하에 추진되는 사업으로, 송・배전, 신재생 에너지, 전기자동차, SCADA, AMII(Advanced Metering Infrastructure) 서비스 등으로 다양한 분야를 포괄한다. 스마트 그리드의 핵심은 에너지를 효율적으로 사용하는 것으로 수요・공급자 간의 양방향 통신을 이용한 정확한 실시간 가격정보 교환 및 전력공급을 가능케 하여 능동적인 자원 소비로 불필요한 에너지의 소모를 감축하고 정전 사태 등의 잠재적 재난에 대비하기 위한 전력의 효율적인 관리를 위한 것이다. 이것이 바로 원격 검침 인프라(AMI) 시스템이다[1].

그러나 IT의 결합으로 인해 IT상의 문제점이 AMI 시스템을 포함한 스마트 그리드에 그대로 반영될 가능성이 있기 때문에 보안문제가 함께 고려되며 개발되어야 한다. 현재 기술적인 개발에 거의 완성단계임에도 불구하고 보안 등의 여러 이슈의 문제로 AMI 시스템의 현실 도입은 어려운 상태이다[2]. 특히 국내에서는 단지 사이버 보안 정보의 공유역할만을 담당하고 있는 수준이기 때문에 실질적인 보안 연구가 미흡하다는 지적을 받고 있다[3].

본 논문에서는 보안문제로 당장 인프라를 구축하여 서비스를 수행할 수 없는 한전의KDN(주)가 규정하여 추진하는 AMI 시스템 규격을 토대로 취약점을 분석하고, 현재의 한전의 규정상에서 적용 가능한 대칭키 기반의 보안으로 안전한 AMI 시스템의 통신프로토콜 구조를 제시하여 암호화 및 메시지인증을 통해 기밀성, 무결성, 가용성 등의 보안 요건을 만족시킬 수 있는 통합적인 관리를 제안한다.

2. 대칭키 기반 AMI 시스템 특징

물리적인 공격 가능성을 제쳐두고서도 AMI 기기는 낮은 컴퓨팅 능력과 통신 대역폭을 갖고 있어 암호화 등의 적용이 어려워 보안 구현이 어렵다. 기술발전으로 저가의 암호화 연산능력을 갖춘 반도체가 등장하여 암호화 등의 제약사항을 상당히 완화시켰지만, 리소스 등의 제약사항이 모두 해소된 것은 아니기에 현재 금융권에서 사용하는 PKI 방식 즉, 공개키 기반 방식이 가장 유력한 대안으로 떠오르고 있으나, PKI 인증의 경우에도 인증서 유효기간이 길수록 증가하는 위험에 대한 대응책 마련이 필요하며 이를 위해 주기적인 키 업데이트, 폐지에 대한 라이프사이클을 지원해야 하는 등 많은 요구가 따른다[4]. 게다가 공개키 방식은 보안상의 문제 이외에도 인프라 구축에 막대한 비용이 들어가 현실적인 어려움이 따르며 연산속도가 느리기 때문에 즉각적으로 반응해야하는 서비스의 속도를 저하시킬 수 있는 가능성이 있다.

대칭키 기반의 AMI 보안 시스템은 낮은 성능인 AMI 기기에 공개키 기반 보안 시스템보다 부담이 덜하여 빠르게 실시간 서비스를 제공해야 하는 AMI서비스에 적용하기에 적합하다. 공개키에 비하여 암호화 구현 및 적용이 쉽고, 키 관리에 있어서도 AKA 프로토콜 등의 검증 및 실제로 응용하고 있는 관리방법들로 복잡하고 데이터 관리가 큰 인증서를 사용하지 않고 인증 및 키 공유 문제를

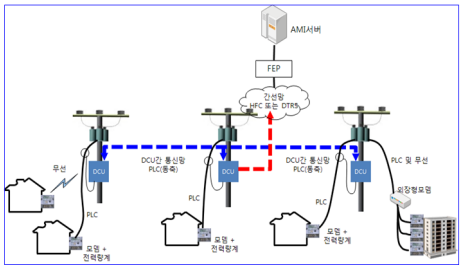
* 본 연구는 국토해양부 첨단도시개발사업의 연구비지원(07첨단도시 A01)에 의해 수행되었습니다.
이 논문은 2011년도 정부(교육과학기술부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원을 받아 수행된 연구임(No.2011-0029927)

해결할 수 있다.

3. 한전 AMI 시스템의 구조와 통신

3.1 AMI 시스템 통신과 보안

AMI 시스템은 보통 세 구간의 통신 구간을 가지며 각 구간이 통합적으로 보안이 제공되어야 한다. (그림 1)은 한전이 규정한 시스템 구성의 예이다.



(그림 1) 한전의 AMI 시스템 구성도

우선 통신 구간은 댁내에서 기기들 간에 통신망인 HAN(Home Area Network), 각 가정의 스마트 미터에서 정보를 수집하는 DCU와 스마트 미터 간의 통신망인 NAN(Neighborhood Area Network), 그리고 DCU부터 통신 사업자가 제공하는 공중망을 이용해 DCU의 정보를 수집하고 정보를 처리하는 AMI head-end간에 통신망인 WAN(Wide Area Network)으로 구성된다.

통신 종류는 스마트 미터기의 E-type, G-type여부에 따라 다음의 [표 1]과 같이 분류된다.[5,6].

[표 1] 한전의 구간별 통신 종류

	E-type	G-type
HAN	RS-485	적외선
NAN	통신모듈 설치에 따라(PLC, Binary-CDMA)	PLC
WAN	광(HFC)간선망 또는 D-TRS	

실질적으로 고려해야 하는 구간은 NAN과 WAN으로 스마트 미터기에서 AMI서버(혹은 FEP)까지의 보안이다. WAN의 구간은 이동 통신사의 네트워크를 활용할 수 있어 비용의 절감과 동시에 통신망의 확보가 손쉬운 편이다. 한전에서 구축한 D-TRS 시스템은 TETRA로 변압기 감시, 배전 자동화, 신 기동배전보수 등의 전력 IT응용 시스템을 연동하여 사용하고 있다[7]. 하지만 NAN의 영역에서는 다양한 무선기술의 주파수 할당문제와 안전하다 검증된 보안 모듈의 표준상의 부재로 현실적으로 bypass로 사용된다. Binary-CDMA는 Koinonia시스템에 ARIA적용이 가능한 BLAN(Binary CDMA LAN)이 제안된바 있다[8,9]. PLC의 경우에는 같은 그룹ID(GID)를 공유하고 있는 노드 간에 56-DES와 128-AES로 암호화를 하지만 표준에선 단편적으로 언급되어 있다[10].

3.2 DLMS/COSEM과 AMI시스템 프로토콜

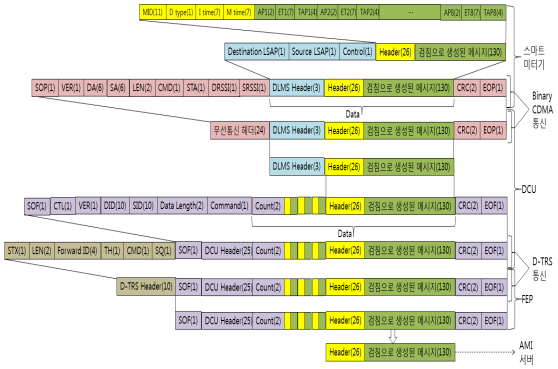
NAN의 영역에서 전자식 계기의 통신을 위해서 국제 통신 규격인 DLMS/SOSEM의 규정을 적용한다. DLMS/SOSEM (IEC 62056)통신 프로토콜은 IEC 62056국제 규격을 기반으로 하는 차세대 전력량계 통신 프로토콜로 데이터의 상호 호환성 확보를 목적으로 계량기가 다루고 있는 각종 데이터들을 논리적인 객체로 모델링하고, 표준화된 자료구조로 데이터 메시지를 정의하고, 다양한 전송매체로 전송방법을 규정한 원격검침용 통신 프로토콜 국제 규격이다. 전송되는 표준화된 자료구조는OBIS(Object Identification System)을 따른다[11]. OBIS는 전기 계량장치에서 일반적으로 사용되는 자료 항목을 위한 인식코드를 정의하며 [표 2] 같은 구조다.

[표 2] OBIS 코드 구조

A 그룹	B 그룹	C 그룹	D 그룹	E 그룹	F 그룹	Resister
에너지 종류	채널	물리량	처리 방법	분류	시간 분류	검침값
1byte	2bytes	2bytes	2bytes	2bytes	2bytes	Variable

Register는 OBIS가 의미하는 실제 측정값은 Resister에 저장하며 그 크기는 double long unsigned6, float32 등으로 다양하다[6].

다음의 (그림 2)는 현재의 한전의 규정상에서 미터기에서 AMI 서버까지 전달되는 과정을 단계별로 묘사한 것이다. 미터기에서 생성된 데이터는 가장 데이터가 큰 경우인 최대 수요데이터 전송의 경우이며, 미터기와 DCU사이의 통신은 Binary CDMA를 사용하고 DCU에서 각 미터기에서 보낸 자료가 취합되어 AMI서버로 보내진다. DCU와 FEP(AMI 서버)사이의 통신은 D-TRS인 경우를 예로 들었다[5,6,8,11,12,13].



(그림 2) 한전 규격에 따른 검침 데이터 전달 과정

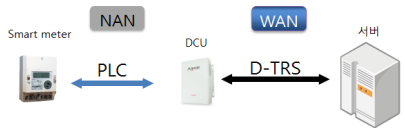
다음의 [표 3]는 위의 (그림 2)로 표현한 패킷 중에서 미터기에서 생성되어 AMI서버에 보내질 데이터에 대한 간략한 설명이다[7]. 통신기술상의 패킷 정보는 생략하도록 한다.

[표 3] 한전 규정상 데이터 패킷 설명

패킷 위치	패킷 이름	내용
스마트 미터기 데이터 생성	MID(11)	스마트 미터기 ID
	D type(1)	데이터 종류
	I time(7)	해당 미터기의 검침 수신 시 DCU 시간
	M time(7)	수집 시 미터시간
	API(2)	유효 수요전력
	ET(7)	발생시간
	TAP(4)	누적 유효수요전력

4. 데이터 암호화 최적 지점과 암호화 방법

한전의 보안에 대한 규정을 종합하면, 통신에서는 AES-128이상의 암호화를 해야 하며, DLMS에서는 low security level로 설정하는 것이 전부라고 할 수 있다. low security level 역시 암호화라기보다는 확인절차에 불과한 인증 버전으로 보안이 없는 것이나 다름없다[12]. 명확한 규정과 세세한 언급이 부족하여 암호화를 어디서 구현할 것인지 어떻게 구현할 것인지 논란이 될 수 있으며 이로 인해 개발된 상품들 간에 호환성의 문제가 발생할 수 있다. 이를 명확히 하게 제시하기 위해 한전이 제시하는 AMI 망을 다시 간략히 나타내면 (그림 3)와 같다. 서버가 의미하는 것은 한전의 FEP에 해당할 수도 있으며 인증서버의 기능이 있거나 인증 서버가 도와주어 데이터를 암복호화 할 수 있는 키를 나누어갖고 관리할 수 있어야 한다. 우선은 미터기와 인증 서버가 서로 인증되고 키를 안전하게 분배하여 정상적인 세션키를 생성하고 있다는 가정 하에 암호화가 이루어져야 할 위치를 검토해 보고 어떤 방식으로 암호화가 이루어 져야 기밀성뿐만 아니라 무결성을 보장할 수 있을지에 대하여 논하겠다.



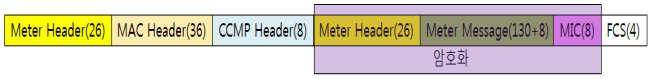
(그림 3) 한전의 AMI 시스템

PLC와 D-TRS에서 암호화를 한다고 하자. 즉, 통신구간마다 암호화를 한다고 하면 DCU에서 반드시 복호화하여 평문 상태가 된 데이터를 다시 D-TRS방식으로 암호화해야 한다. 평문상태가 드러나는 security hole이 발생하여 공격자의 타깃이 될 수 있다. security hole 없이 스마트 미터와 서버가 end-to-end 보안이 되기 위해서는 통신보다 더 높은 애플리케이션 단에서 암호화 되어야 한다. 즉 검침 데이터가 생성된 직후 송신을 위한 프로토콜에 encapsulation되기 전에 AES-128bit 또는 ARIA-128bit이상 수준의 알고리즘을 통해 암호화해야 한다. 3장의 패킷 구조 (그림 4)에서 알 수 있듯, 미터기에서 생성된 최대의 데이터가 156byte 이므로 총 9 블록으로 나누어 수행되며 이보다 데이터가 작은 경우에는 암호 알고리즘의 블록 사이즈에 맞춰 패딩 하는 기술이 필요하다.

이렇게 암호화를 한 것만으로는 여전히 여러 가지 문제가 남아있다. 복호화한 후에도 전송된 검침 정보가 사실인지 중간에 바꿔치기 당하거나 변동되지 않았는지 증명할 방법이 없기 때문이다. 이 문제를 해결하는데 있어 무선 랜의 암호화 알고리즘에 사용되는 AES-CCMP를 사용한다. CCM은 데이터의 기밀성을 위한 counter 모드와 데이터의 무결성과 사용자의 인증을 위한 CBC-MAC (Cipher Block Chaining - Message Authentication Code)의 조합으로 구성되어 있다. CBC-MAC 모드를 사용하여 MIC(Message Integrity Code)를 생성해 데이터의 무결성을 검사할 수 있다.

4.1 end to end 암호화 적용 위치와 적용 대상 패킷

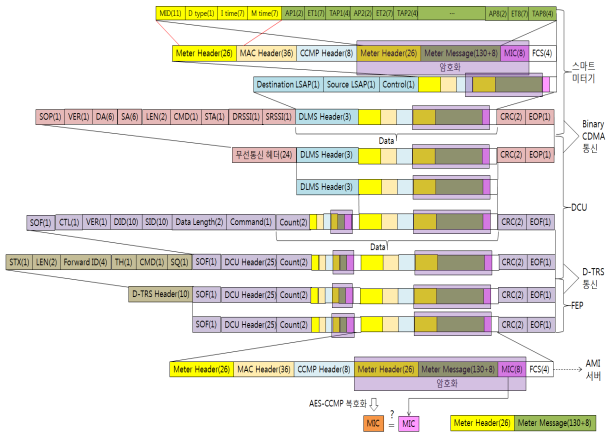
앞서 살펴본 AES-CCMP를 이용하여 한전의 규정에 영향을 끼치지 않으면서 암호화의 기능을 추가하기 위해서는 미터기에서 생성된 최종 데이터는 다음(그림 4)과 같은 구조가 되어야 한다.



(그림 4) 스마트 미터기의 암호화된 최종 데이터

AES-CCMP에서 무결성을 체크하는 MIC을 데이터와 함께 암호화 하는 것처럼 미터기에서 생성된 데이터만 암호화 하면 미터기 헤더의 정보가 위조 될 수 있으므로 미터기 헤더 역시 함께 암호화 되어야 한다. 이때 암호화된 상태의 미터기 헤더로는 미터기 헤더의 정보를 알 수 없기 때문에 전송이 불가능 하며 한전의 규정과도 맞지 않으므로 미터기 헤더를 복사하여 AES-CCMP 헤더 앞에 위치 시켜 암호화와 메시지 인증 기능을 추가시키되 결과적으로 한전의 규정과 유사한 형식을 유지할 수 있다. 미터기에서 생성된 데이터는 AMI 서버까지 전송되는 과정에서 암호화된 채로 encapsulation과 decapsulation만을 반복하여 전송되기 때문에 도중에 평문정보가 드러나거나 위조될 수 없고, AMI 서버는 결과적으로 (그림 4)과 동일한 패킷을 받게 된다. 이와 같이 AES-CCMP를 적용할 시에 추가되는 데이터는 미터기 한 대를 단위로 하여, 복사되는 미터기 헤더 26bytes, AES-CCMP적용으로 인해 부가 데이터와 블록 암호알고리즘 위해 패딩된 추가데이터 8byte를 포함하여 64byte로, 총 90bytes가 추가된다. DCU에서 수집하여 FEP까지 전송할 때 미터기를 17개로 묶어 전송하는 것을 감안 할 때 DCU가 수집하여 생성하는 데이터에선 총 1530bytes가 추가된다. 다음의 (그림 5)은 AES-CCMP가 적용됐을 시에 한전의 규격에 따라 AMI 서버까지 전송되는 과정을 묘사한 것이다.

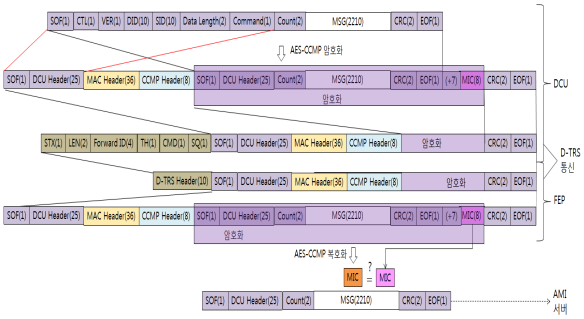
본 논문에서는 AES-CCMP를 예로 들었지만 AMI는 국가 기간산업이므로 국내에 적용을 위해 AES-CCMP를 ARIA-CCMP로 변경하여 사용하는 것이 알맞다.



(그림 5) 암호화가 적용된 패킷의 전송 과정

4.2 DCU에서 AMI 서버까지 보안 시 데이터 암호화 최적 지점과 암호화 방법

end-to-end 보안이 가장 안전한 데이터 전송 방법 이지만 현실적으로 각 가정 또는 건물마다 보안을 적용하는 것은 서비스를 원활히 제공하는 입장에서도 커다란 부담이며 비용 적으로도 불가능 할 수도 있다. 그렇지만 최소한 대량의 데이터를 수집하고 다루는, 기업적으로 투자가 가능할 수 있는 영역에서도 보안이 이루어지지 않는다면 대량의 데이터가 평문 상태로 노출되는 만큼 피해도 클 것으로 예상된다. 더욱이 DCU에서 AMI 서버(혹은 FEP)까지 전송되는 과정을 공중망을 통한 통신을 사용하기 때문에 유선 통신을 적용할 때보다 공격자의 접근이 용이할 수도 있다. 따라서 end-to-end의 차선책으로서 DCU에서 AMI 까지의 데이터 보안을 위해 DCU 또는 AMI 서버에서는 다음의 (그림 6)와 같이 AES-CCMP 혹은 ARIA-CCMP가 적용되어 암호화된 데이터 패킷이 전송되어야 한다.



(그림 6) WAN에서 암호화가 적용된 패킷의 전달 과정

DCU에서 암호화까지 완료되어 생성된 최종 데이터는 복사되는 미터기 헤더 29bytes, AES-CCMP로 인해 추가되는 헤더와 MIC이 52bytes, 블록암호 연산을 위해 추가로 패딩되는 7bytes로, 총 88bytes가 추가된다.

7. 결론

스마트 그리드의 핵심 기술인 AMI는 기존의 전력망에 IT의 결합으로 인해 보안적인 대응이 필요하다. 이런 AMI에서 효과적으로 보안을 함과 동시에 이미 상당수 추진되고 있는 사업 규정을 바탕으로 실질적으로 적용이 가능한 암호화 기술이 필요하며 이것은 보안의 요소를 충족시킬 수 있어야 한다.

본 논문에서는 가용성에 도움이 되기 위해 무거운 공개키 기반의 보안 대신 빠른 처리와 서비스 제공에 도움이 되는 대칭키 방식의 보안을 설계하였다. 기밀성을 위해 AES또는 ARIA 블록암호를 사용하며, 암호화된 메시지의 무결성을 위해 AES-CCM, ARIA-CCMP의 방식을 사용한다. 이는 보안이 적용되는 단에 보안 모듈을 추가하는 것만으로 한전의 규격을 준수하면서 보안을 적용했다.

이 외에도 본 논문에서 제시한 암호화의 바탕이 되는 기기 인증과 키 분배 프로토콜 등 전방위적인 안전성의 확보를 위한 연구가 필요하다.

참고문헌

[1] 장두석, “스마트 그리드 산업의 동향 및 산업화 방안”, 산업이슈, 2010.05, p.11-33

[2] 박찬국, “전력인프라 사이버보안 이슈와 정책 대응”, 주간기술동향 통권 1398호, 2009.12, pp.1-166

[3] 김영준, 스마트 그리드 시스템에서의 고객 데이터 공유 및 관리 방식 제안, 대한전기학회, 2010.7

[4] 김진철 한전KDN 전력IT 연구원, “스마트그리드 기기 인증 기술과 발전 방향”,IT정보마당 DATANET, 오현식 기자 2011.12.01. http://www.datanet.co.kr/news/articleView.html?idxno=58111

[5] RS-6625-0029, “E-Type 저압 전자식전력량계”,한전 등록 구매 규격, 2011. 07 개정

[6] “G-Type 저압 전자식 전력량계”, 한전 등록 구매 규격, 2010.10 제정

[7] 송병권, 정태의 “전력 IT용 D-TRS 접속을 위한 게이트웨이 플랫폼”,한국철도학회논문집 제 12권 제 1호, 2009, pp.45-54

[8] KS X 4650-2,"정보기술-전기통신과 시스템간의 정보교환-이진부호분할다중접속(Binary CDMA)-고속 Binary CDMA 매체접근제어(MAC) 및 물리계층(PHY)",2007

[9] 대우전자부품(주), “Koinonia 표준규격서: 물리계층과 데이터링크 계층 규격 버전1.1”,2004

[10] KS X 4600-1, "정보기술-전기통신과 시스템간의 정보교환-고속 PLC 개치접근제어(MAC) 및 물리층(PHY)-제 1부 일반요구사항“,2007

[11] IEC 62056-61."OBIS Object Identification System", 2006

[12] IEC 62056-53, "전기 계량 - 검침과 종별계량, 부하 제어를 위한 데이터 교환 - 제 53부 : COSEM 응용 계층.",2010.12 개정

[13] IEC 62056-46, "Data Link Layer using HDLC-Protocol", 2007