제36회 한국정보처리학회 추계학술발표대회 논문집 제18권 제2호 (2011. 11)

AMI 시스템의 무선 네트워크 보안 분석*

전호성, 오지은, 김민구, 이옥연
국민대학교 수학과, 정보보안연구소
{hsjeon, arhanaz, kmnine, oyyi}@kookmin.ac.kr

Analysis for Wireless Network Security on AMI System

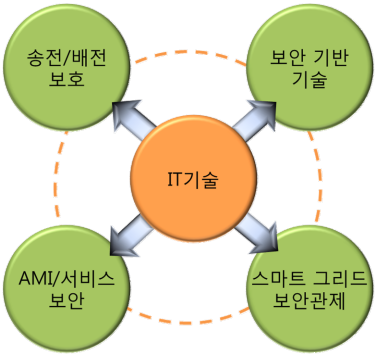
HoSung Jeon, Jieun Oh, Min-Ku Kim, Okyeon Yi,
Dept. of Mathematics. and CISI, Kookmin University

요 약

AMI 시스템은 정보통신 기술과 전력망의 융합으로 탄생한 새로운 형태의 차세대 전력망인 스마트그리드의 핵심기술 중 하나이다. AMI 시스템의 부하 제어 및 수요 측정, 미터링, 과금 등을 위한 다양한 유·무선 통신기술(ZigBee, PLC, Binary CDMA 등)을 적용함에 있어 기존에 제시된 AMI 네트워크 보안 위협에 따른 취약점은 스마트그리드 전체 네트워크의 보안사고를 유발할 수 있다. 본 논문은 AMI 시스템 상에서 ZigBee, Binary CDMA와 같은 무선 네트워크의 적용으로 인한 보안특성을 분석하고 보안 요구사항에 대한 대응방안을 제시한다.

1. 서론

스마트그리드는 기존의 전력망에 정보기술(IT)을 접목하여, 전력공급자와 소비자간 양방향 실시간 정보 교환 및 에너지 효율 최적화로 새로운 부가가치를 창출하는 차세대 전력시스템 및 관리 체계를 의미한다. 이러한 스마트그리드의 핵심기술 중 하나인 AMI(Advanced Metering Infrastructure) 시스템은 전력을 효율적으로 관리하기 위한 체계로써, 최근 다양한 연구와 개발이 이루어지고 있다. 소비자들은 AMI를 통한 실시간 전력 정보를 기반으로 에너지를 관리함으로써 가정 및 기업의 비용을 절감할 수 있으며 결과적으로 전체적인 전력 사용 효율을 높일 수 있다. (그림 1)은 스마트그리드에서 필요한 보안 요구사항을 나타내고 있다.



(그림 1) 스마트 그리드 보안 기술

* 이 논문은 2010년도 정부(교육과학기술부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (20100024870)

AMI 시스템의 구조를 네트워크 단위로 분류하면 HAN(Home Area Network), NAN(Neighborhood Area Network), WAN(Wide Area Network)으로 나누어지는데 이는 다양한 유·무선 통신기술로 구성되어있으며 주로 HAN에서는 ZigBee, PLC NAN에서는 Binary CDMA, PLC, WAN에서는 Wibro, D-TRS 인터넷 광통신망을 사용한다. 그러나 이러한 정보통신 기술의 융합은 단말 장치와 내부 운영 시스템 사이의 양방향 통신을 위한 스마트 미터, 센서 등의 기기에 대한 보안관리가 수반되어야 한다. 특히, HAN, NAN에서 사용하는 무선 네트워크는 기존 무선 네트워크가 갖고 있는 보안취약점이 동일하게 적용될 수 있으며 이는 전력망이라는 특성상 더욱 심각한 결과를 초래할 수 있다[1].

본 논문에서는 AMI 시스템에 사용되는 무선 네트워크의 보안특성을 분석하고 보안요구사항에 대한 대응방안을 제시한다.

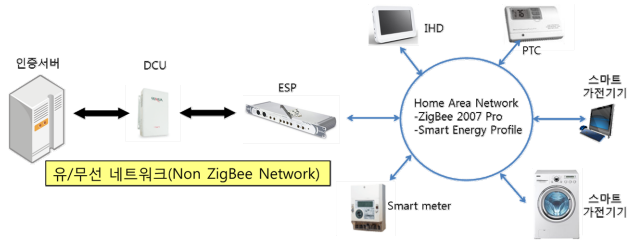
2. AMI(Advanced Metering Infrastructure) 시스템

AMI 시스템은 현재 전력망의 단방향·폐쇄적 에너지 공급이 아닌 양방향 에너지 종합관리시스템인 스마트 그리드를 위한 핵심기반 기술로써 전력 에너지를 효율적으로 관리할 수 있는 시스템 및 서비스이다. 소비자에게 전력 사용량, 과금 데이터 등의 정보를 실시간으로 제공하여 소비자 혹은 자동화된 기기의 제어를 통해 가정 및 기업의 에너지 비용을 절감할 수 있다. 또한, 에너지 생산 주체인 전력회사 역시 검침 및 유지 관리를 위한 비용의 절감뿐만 아니라 필요전력량에 대한 응답과 부하 제어를 통해 에너지 생산 비용 및 추가 인프라 확장을 방지하는 효과를 기대할 수 있다.

AMI 시스템의 도입 목적은 효율적인 전력 수요 관리를 통해 생산과 공급의 균형을 확보하기 위한 것이다. 현재 전력 사용 요금은 원단위로 전력량계에 표시된 누적치를 검침하여 이 값을 기준으로 부과되고 있는데 AMI 시스템이 구현되면 검침을 위해 가정을 직접 방문할 필요가 없을 뿐만 아니라, 실시간 검침이 가능해져 지금까지는 제공할 수 없었던 새로운 차원의 다양한 서비스를 제공할 수 있다[2].

3. AMI 시스템의 무선 네트워크 보안 분석

(그림 2)는 AMI 시스템의 구성을 보여준다. 각 구성요소는 ZigBee, PLC, Binary CDMA, Wibro, D-TRS 등의 다양한 통신망의 결합을 통해 연결되어있다. <표 1>을 보면 현재 사용하고 있는 무선 통신 기술을 비교·분석한 것이다[3].



(그림 2) AMI 시스템 구성

3.1 ZigBee

ZigBee란 IEEE 802.15.4를 기반으로 하는 근거리 무선 통신기술이다. ZigBee는 전력소모가 적고 칩 가격이 저렴하며 통신의 안정성이 높아 최근 급속한 발전을 하고 있다. 원격제어, 원격관리, 원격모니터링에 적합하기 때문에 가정 및 공장, 산업자동화에 활발하게 적용되고 있다. 반경 100m안 250kbps의 속도로 데이터를 전송하는 ZigBee는 멀티-홉(Multi-hop) 기능을 통해 65,000개 이상의 노드(Node)를 연결할 수 있어 확장성 있는 네트워크 구성에 용이하다.

ZigBee는 정보 유출이나 불법적인 침입자로 인한 도청 및 위·변조를 막기 위해서 128비트의 AES-CCM*를 이용하여 기밀성과 무결성을 보장하며 두 노드간의 키 관리(Key management), 키 설정(Key establishment), 키 전송(Key transport)과 인증(Authentication) 과정을 수행한다.

ZigBee는 트러스트센터(Trust center)라는 개념을 이용하여 네트워크상의 노드들이 SKKE(Symmetric Key Key Establishment) 프로토콜을 이용해 키를 분배하고 노드간의 단대단(End-to-end) 보안을 가능하게 한다. 노드 사이의 비밀 키는 중간 노드들의 중계에 의하여 전달되는데 ZigBee 보안시스템은 중간 통신채널의 안전성을 완벽히 보장하지 않아서 키의 노출 위험성이 존재한다[4]. 이는 비밀 키의 안전성 보장이 가장 중요한 대칭키 암호시스템의 손상을 의미한다. 또한 대칭키 암호시스템을 사용하는 ZigBee 시스템에서는 트러스트센터가 서로 통신하는 모든 노드들의 비밀 키를 관리하도록 되어 있기 때문에 트러스트센터에 대한 공격 성공 시 모든 노드들 간의 비밀키 유출을 비롯한 전체 네트워크의 위험을 초래한다.

3.2 Binary CDMA

Binary CDMA 기술은 WLAN이나 Bluetooth와 같은 다양한 무선기술들의 혼재에 따른 주파수 배정 문제나 QoS(Quality of Service) 보장 문제를 해결하기 위해 제안

<표 1> 무선 통신 기술 비교

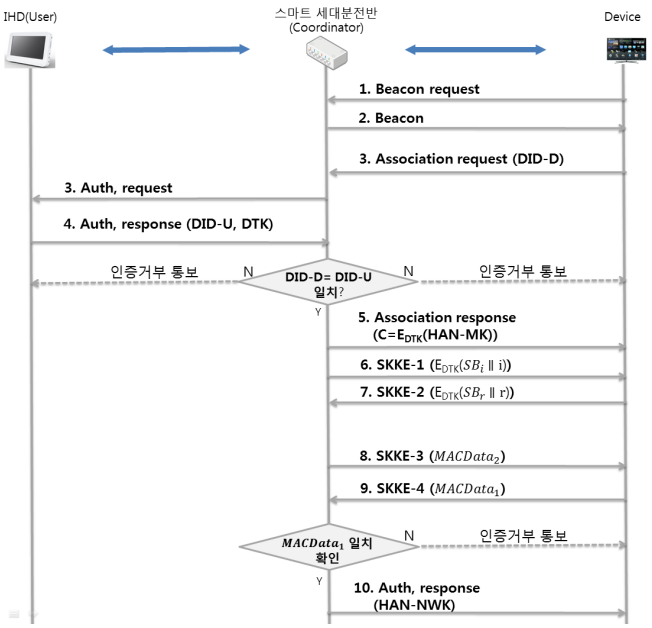
구분	ZigBee	WiFi	Binary CDMA	Wibro	WCDMA
통신 거리(m)	10 - 75	115 - 500	800 - 1000	100 - 1000	1000 - 2000
통신 속도(Mbps)	0.25	300	UP : 2 Down : 7.2	10	10
암호알고리즘	AES-CCM*	WEP, AES-CCM	AES-CCM (ARIA-CCM)	AES-CCM AES-CBC AES-CTR	MILENAGE Alg. KASUMI Alg.
AMI 구축 및 운영 편의성	저전력, 저속, 저가의 근거리 무선 통신으로 HAN 네트워크에 적합	단말기를 중심으로 하는 키 관리 체계로 AMI 적용 시 단말기와 사용자 정보를 연동하는 과정 필요	넓은 통신 범위와 속도 및 ARIA 탑재가 가능하여 공공 망에 적용 용이	현재 이동통신사를 중심으로 운영되고 있으므로 기존망 활용 시 전력 회사와 이동통신사 사이의 책임 문제 및 AMI 네트워크와 인터넷과의 분리 운영 문제가 번거로움	현재 이동통신사를 중심으로 운영되고 있으므로 기존망 활용 시 전력 회사와 이동통신사 사이의 책임 문제 및 AMI 네트워크와 인터넷과의 분리 운영 문제가 번거로움

된 무선기술이다. CDMA의 우수성과 TDMA의 경제성을 동시에 보유한 Binary CDMA 기술은 국내 독자 기술로서 국내 표준 KS-4650에 기반을 두고 국제 표준으로 채택된 무선 통신 기술이다. Binary CDMA는 무결성 및 기밀성 보장을 위해 AES-CCM을 사용하고 있으며 특히, 우리나라 공공망에서 무선 네트워크를 구축하려면 필수적으로 사용해야하는 ARIA를 적용시킬 수 있는 장점이 있다[5,6]. 하지만, Binary CDMA의 표준에서는 암호 알고리즘과 사용모드는 정의하고 있으나 인증 및 키 생성, 관리, 분배 프로토콜이 정의되어 있지 않기 때문에 보안위협에 대한 대응방법이 필요하다.

4. 제안하는 보안 요구 사항

4.1 ZigBee

ZigBee는 트러스트센터(Trust center)를 통해 새로 HAN에 가입하는 장치에 대한 키 분배에 대한 취약점을 지니고 있다. 새로운 장치가 접속할 때 트러스트센터는 자신이 가지고 있는 비밀키를 안전하지 않은 채널을 통해 전송하게 되는데 이는 공격자에게 노출되어 HAN 전체가 보안상 위협에 노출되어진다. 따라서 제안하는 프로토콜은 다음과 같다.



(그림 3) AKA in HAN

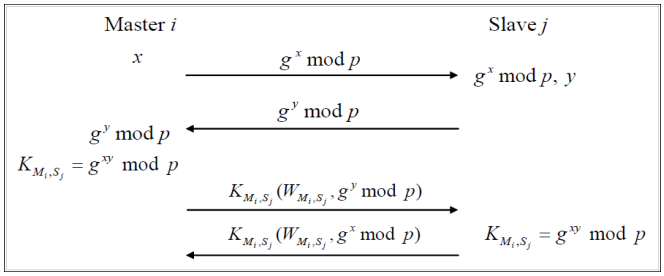
(그림 3)에서 보면 트러스트센터에서 새로운 장치로 비밀키를 안전하지 않은 채널을 통해 전송하여 링크키를 생성하는 대신, DID(Device ID)라는 장치 고유번호를 생성하여 영구적으로 장치 정보를 담게 한다. 그리고 DID를 이용해 링크키와 같은 역할을 하는 DTK(Device Temporary Key)를 생성하여 장치를 인증하는 데에 사용하고 장치 인증이 끝난 이후에는 사용하지 않는다. 그리고 또한 DTK는 HAN에서 사용되는 비밀키를 안전하게 전송하는 역할을 한다.

4.2 Binary CDMA

무선 네트워크에서는 장치의 인증과 키 생성, 관리, 분배가 매우 중요하다. 그러나 Binary CDMA 국내 표준(KS X 4650)에서는 인증 및 키 관리에 대해서 명확하게 언급하고 있지 않다. WPAN에서는 데이터를 안전하게 전송하기 위해서 암호화하여 전송해야하며, 암호화에 사용되는 암호키 또한 안전하게 전송되어야 한다. 기존의 발표되었던 대칭키 기반의 키 생성 및 교환, 분배 프로토콜을 이용한 암호키를 안전하게 전송하기 위해서 대칭 비밀키(Symmetric secret key) 생성 및 전송 방법이 있다[7]. 대칭 비밀키의 생성 및 전송을 위해서는 세션키(Session key)를 이용해야 하는데, 여기서 세션키란 모든 디바이스들을 컨트롤 하는 일시적인 비밀키이다. 따라서 생성된 세션키를 이용하여 바로 암호키를 전송하지 못하며, 암호키 전송을 위해서는 대칭 비밀키를 이용해야 한다. 대칭 비밀키를 이용하여 암호키를 전송할 경우 서버는 세션키를 이용하여 디바이스 간의 대칭 비밀키를 생성한다.

4.2.1 세션키 생성 및 인증 방법

대칭 비밀키 전송을 위해 사용되는 세션키 생성을 위하여 먼저 디바이스와 서버는 미리 정해진 패스워드(W_{M_i,S_j})를 공유하고 있다고 가정한다. 공유된 패스워드는 생성된 세션키의 인증과정에 사용된다. 세션키 생성 방법은 Diffie-Hellman 프로토콜에 기반 한다. 따라서 man-in-the- middle attack 문제가 발생할 수 있다. 이와 같은 문제를 보완하기 위한 인증 방법을 제시하고 이를 통하여 세션키를 생성하는 방법을 제안한다. 세션키 생성 방법은 그림 (그림 4)과 같다.



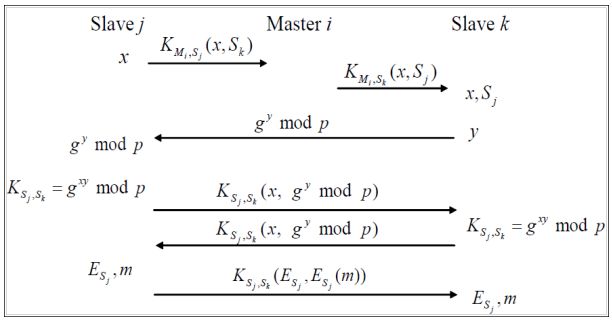
(그림 4) 세션키(K_{M_i,S_j}) 생성 및 인증과정

우선 서버 i-디바이스 j의 세션키 생성을 위해 마스터 i가 랜덤변수 x를 생성하고 $g^x \bmod p$ 를 계산하여 디바이스 j에게 전송하고, 이를 수신한 디바이스 j는 랜덤 변수 y를 생성, $g^y \bmod p$ 를 계산하여 서버 i에게 전송한다. 이와 같은 과정을 통하여 서버 i와 디바이스 j는 두개의 같은 파라미터를 공유하게 되고 이 공유된 파라미터를 이용하여 세션키 (K_{M_i,S_j})를 생성한다. 이와 같이 생성된 세션키를

사용하기 전에 서버 i-디바이스 j 간에 공유하는 패스워드 W_{M_i,S_j}를 이용하여 인증 과정을 거치게 된다. 즉, 서버 i는 공유하는 세션키로 서버 I-디바이스 j 사이에 공유하는 모든 파라미터(W_{M_i,S_j} 포함)를 암호화하여 전송하고 수신한 슬레이브 j는 복호화 후 소유하고 있는 자신의 파라미터와 비교한다. 이와 같은 인증 과정을 거친 후, 최종 세션 키 $K_{M_i,S_j}=g^{xy} \bmod p$를 공유하게 된다[7].

4.2.2 대칭 비밀키 교환 방법

데이터의 암호화를 위한 암호키의 안전한 전송을 위해 대칭 비밀키 이용 방법을 제안한다[7]. 즉, 위에서 생성한 세션키를 이용하여 통신을 원하는 디바이스 간 대칭 비밀키를 생성하고 분배하는 방법에 대하여 살펴본다. 서버는 KDC(Key Distribution Center)로 키를 생성하고 분배하는 역할을 수행한다. 서버에서의 통신은 두 디바이스 사이에 peer-to-peer통신 방식이 가능하므로 디바이스 사이에 비밀 통신을 하기 위해서는 이들만의 대칭 비밀키를 공유해야 한다. 이는 비밀 통신에 사용되는 데이터 암호키를 안전하게 전송하기 위해 필요한 키이다. 이와 같은 대칭 비밀키 생성과정은 (그림 5)와 같다. (그림 5)에서 보는 바와 같이 디비아스 j가 디바이스 k와 통신을 원할 경우, 디바이스 j는 서버 i에게 디바이스 k와 통신을 원한다는 메시지를 서버 i-디바이스 j 간의 세션키(K_{M_i,S_j})를 이용하여 암호화해서 보낸다. 이와 같은 요청 메시지를 전송할 때, 디바이스 j는 랜덤변수를 생성하여 함께 전송한다. 이 랜덤 변수는 디바이스 j와 디바이스 k의 대칭 비밀키 생성을 위해 사용된다. 메시지를 받은 서버 i는 생성된 랜덤변수 x를 서버 i-디바이스 k 간의 세션키(K_{M_i,S_k})를 이용하여 암호화 시킨 후, 디바이스 k에게 전송한다. 디바이스 k는 세션키(K_{M_i,S_k})로 이를 복호화하여 디바이스 j에 의해 생성된 랜덤 변수 x를 소유하게 된다. 이 과정이 끝나면 디바이스 간 세션키는 소멸되고 비밀 관계 설정을 위한 두 디바이스 간 대칭 비밀키 생성과정에 들어간다. 생성 방법은 Diffie- Hellman 프로토콜을 이용한다. 디바이스 k는 랜덤변수를 생성하여 $g^y \bmod p$를 계산, 디바이스 j에게 전송한다. 그리고 각 디바이스는 랜덤 변수 x를 이용하여 디바이스 j-k간 대칭 비밀키 $K_{S_j,S_k}=g^{xy} \bmod p$를 계산 할 수 있다. 디바이스 j와 k는 랜덤 변수 x와 $g^y \bmod p$를 서로 비교하는 인증 과정을 거친 후, 같을 경우 $K_{S_j,S_k}=g^{xy} \bmod p$를 두 디바이스 간 대칭 비밀키로 사용한다. 이와 같이 디바이스 j와 디바이스 k 간 생성된 대칭 비밀키를 이용하여 디바이스 j는 실제 데이터 암호에 사용되는 암호키 E_{S_j}를 디바이스 k에게 전송한다. 이때 디바이스 j는 디바이스 k에게 전송할 메시지 m을 암호키 E_{S_j}로 암호화하여 암호키 E_{S_j}와 함께 전송한다. 디바이스 k는 대칭 비밀키 K_{S_j,S_k}로 암호키 E_{S_j}와 메시지 m 을 수신하게 된다.



(그림 5) 대칭 비밀키(K_{S_i,S_k}) 생성, 분배 및 인증과정

5. 결론

전력망과 통신망이 융합되면서 정보통신 인프라에서 발생하고 있는 보안 문제가 차세대 전력망에서도 그대로 재현되고 있다. 특히 스마트그리드의 핵심기술을 이루고 있는 AMI 시스템의 무선 네트워크에서 보안에 대한 취약점이 발견되어 그에 따른 대응방안이 요구되고 있다. 본 논문에서는 AMI 시스템에서 무선 네트워크 보안요구사항 분석 및 방향을 제시 하였다.

이를 통해 AMI 시스템에서 보안의 필요성을 인식하여 장치와 네트워크를 보호하기 위한 대응방안을 지속적으로 연구하고 개발해야 할 것이다.

참고문헌

[1] 도윤미 외 “스마트 그리드 기술 동향 : 전력망과 정보통신의 융합기술“

[2] 전용희 “지그비 기반 AMI에서의 보안 특성 및 요구사항 분석” 한국정보보호학회, 정보보호학회지, 제20권 제5호

[3] 전재우, 임선희, 이옥연 “스마트 그리드를 위한 Binary CDMA 기반의 AMI 무선 네트워크 구조 및 AKA 프로토콜” 한국정보보호학회, 정보보호학회논문지, 제20권 제5호

[4] 정윤식, 김진철, 김영억 “ZigBee Smart Energy Profile 1.0v 기반의 보안이 적용된 AMI System에 관한 연구” 대한전자공학회, 대한전자공학회 2010년 하계종합학술대회

[5] 전선도, 이장연, 연규정, 이현석, 원윤재, 권대길 “무선 PAN 응용을 위한 Binary CDMA System” 한국인터넷정보학회, 인터넷정보학회지, 제5권 제3호

[6] 김용희, 박미애, 조진웅, 이현석, 이장연, 이옥연 “Binary CDMA 망을 위한 안전한 AKA 프로토콜” 한국정보보호학회, 정보보호학회논문지, 제20권 제1호

[7] 임순빈 외 “Koinonia 고속 WPAN에서 보안을 위한 대칭/비대칭 비밀 키 교환 방법” 한국통신학회, 한국통신학회논문지, 제31권 제6B호