情報保護學會論文誌
第20卷 第5號, 2010. 10

스마트 그리드를 위한 Binary CDMA 기반의 AMI 무선 네트워크 구조 및 AKA 프로토콜*

전 재 우,[1†] 임 선 희,[2] 이 옥 연[3‡]
[1]고려대학교 정보경영공학전문대학원, [2]한국전자통신연구원, [3]국민대학교 자연과학대학 수학과

A Wireless Network Structure and AKA(Authentication and Key Agreement) Protocol of Advanced Metering Infrastructure on the Smart Grid based on Binary CDMA*

Jae-woo Jeon,[1†] Sun-Hee Lim,[2] Okyeon Yi[3‡]
[1]Graduate School of Information Management and Security, Korea University,
[2]Electronics and Telecommunications Research Institute,
[3]Demartment of Mathematics, Kookmin University,

요 약

원격 검침 시스템(AMI : Advanced Metering Infrastructure)은 최근 활발히 추진 중인 스마트그리드의 핵심 인프라로, 구축비용 절감 및 운영의 효율성을 위해 무선 통신 기술 도입이 적극적으로 검토되고 있다. 하지만, AMI에 무선 통신 기술 적용 시 무선 통신의 보안 취약점 때문에 다양한 보안 위협이 발생 가능하기 때문에 이에 대한 대응책이 필요하다. 본 논문에서는 Binary CDMA 망을 이용한 AMI 네트워크 무선망 구조를 제시하고, 이에 대한 보안 대책으로 BSIM(Binary Subscriber Identity Module)을 중심으로 사용자 인증 및 무선 구간 암호화를 수행함으로써 AMI 무선 구간의 보안 위협을 감소시키는 방안에 대해 연구한다.

ABSTRACT

AMI (Advanced Metering Infrastructure) is a core infrastructure of Smart Grid, and is promoting in various country. Wireless network is considered for cost savings and operational efficiencies in AMI. But various security problems are expected in wireless networks of AMI, so we should solve these problems. In this paper, we suggest a wireless network of AMI by using Binary CDMA and security countermeasures of AMI wireless network. Proposed security architecture is using BSIM (Binary Subscriber Identity Module) to perform user authentication and key agreement for the encryption and decryption over radio network to reduce security threats.

Keywords: Smart Grid, Advanced Metering Infrastructure, AMI, Binary CDMA, Wireless Security

접수일(2010년 4월 19일), 수정일(2010년 7월 28일), 게재확정일(2010년 9월 20일)
* 본 연구는 2010년도 국민대학교 교내연구비를 지원받아 수행된 연구임
† 주저자, jjwkma61@korea.ac.kr
‡ 교신저자, oyyi@kookmin.ac.kr

I. 서 론

원격 검침 시스템(AMI : Advanced Metering Infrastructure)은 에너지를 효율적으로 관리하기 위한 체계로써[1], 최근 활발히 추진 중인 스마트그리드의 핵심 인프라이다. 소비자들은 AMI를 통해 실시간 에너지 사용량 정보를 기반으로 에너지를 관리함으로써 가정 및 기업의 에너지 비용 절감할 수 있으며, 결과적으로 전체적인 에너지 사용 효율을 높일 수 있다. 이러한 AMI 구축은 현재 미국을 중심으로 활발히 전개되고 있으며 2009년에 투자된 오바마 행정부의 스마트그리드 관련 투자액 상당 부분이 스마트미터와 AMI 기반 구축에 우선하여 사용될 것으로 나타난다. 이외에도 호주와 유럽지역에서도 AMI 기반 또는 AMI를 염두에 둔 AMR(Automated Meter Reading)의 구축이 활발히 진행되고 있고 한국에서도 AMR 사업이 한전을 중심으로 시범 사업으로 시행되었다[2]. 특히 AMI 네트워크 구축 및 운영의 효율성을 위해 무선 통신 기술 도입이 적극적으로 추진되고 있는 현실이다[3].

그러나 AMI 기술이 IT 체계로 구성되기 때문에 기존 IT에 존재하는 보안 위협과 더불어 다양한 보안 위협이 예상된다[4-6]. AMI를 통해 생성된 소비자의 에너지 사용 패턴 정보의 노출은 프라이버시 문제를 일으킬 수 있으며, 사이버 공격 등으로 말미암아 AMI 체계가 마비되어 그 피해가 전체 전력망으로 확대되면 기존 인터넷 등에서 발생한 피해 이상의 손실이 발생한다. 따라서 AMI 서비스를 대비한 발생 가능한 보안 위협에 대응하는 대책 마련이 선행되어야 한다.

본 논문에서는 AMI 네트워크에 Binary CDMA 기술[7]과 BSIM(Binary Subscriber Identity Module)을 적용한 AMI 네트워크 구조 제안 및 그에 대한 효과를 도출하며, AMI 네트워크의 무선 구간에 대한 보안 대책을 제시한다. 제안하는 AMI 네트워크 구조 및 AKA(Authentication and Key Agreement) 과정은 AMI 네트워크 무선 구간에 요구되는 기밀성 및 무결성을 보장하기 위한 기반 구조를 제시하는 것을 목적으로 하며, 기존의 BLAN (Binary CDMA LAN)의 AKA 과정을 AMI 네트워크 특성에 적합하도록 개선한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존에 제시된 AMI 네트워크의 논리적 구조와 현재까지 도출된 AMI 보안 요구 사항들을 살펴보고, 3장에서는 AMI 네트워크에 적용할 수 있는 무선 통신 기술에 대해 비교분석한다. 4장에서는 Binary CDMA 기술 및 이를 기반으로 한 BLAN-AKA 과정을 살펴보고 5장에서는 Binary CDMA를 적용한 AMI 네트워크 구조 및 AKA 프로토콜을 제안한다. 6장에서는 제안된 AMI 네트워크에 대한 분석 및 이를 바탕으로 한 서비스 시나리오를 제안하고 7장에서는 결론 및 차후 연구과제에 대해 언급한다.

II. AMI 논리적 구조 및 보안요구 사항

미국 국립표준기술연구소(NIST)에서는 스마트 그리드의 전반적인 논리적 구조 및 보안 요구 사항을 제시하고 있다[8]. 본 장에서는 AMI와 관련된 기술에 대해 논의한다.

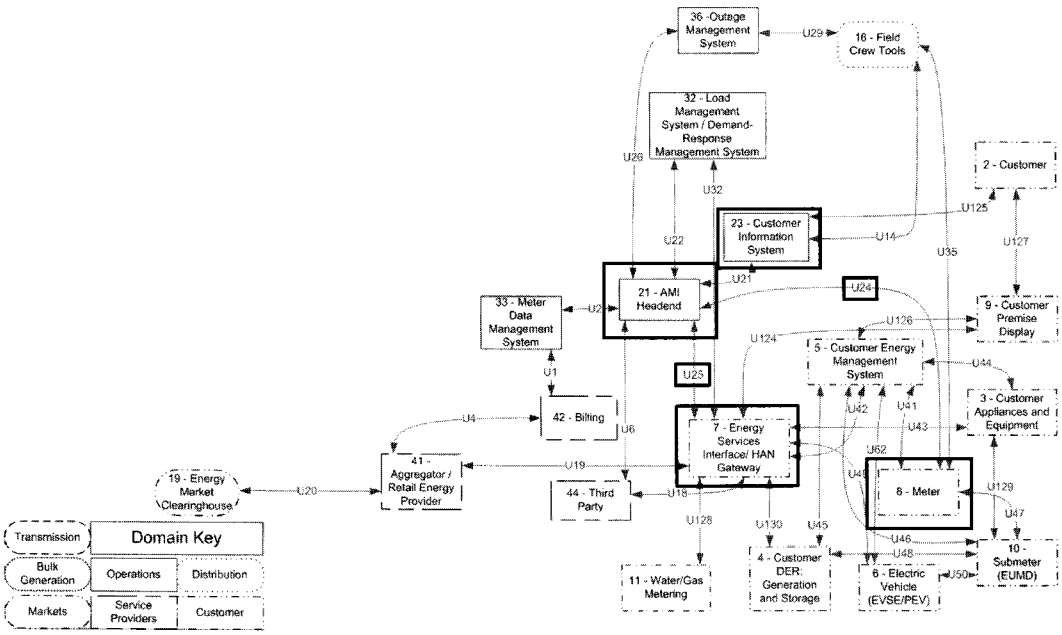
2.1 AMI 논리적 구조

NIST에서는 스마트 그리드의 논리적 구조를 6개의 애플리케이션 영역으로 분류하고, 이 중 전력 공급자와 지능형 계량기 사이의 구간은 Home Area Network/Business Area Network(HAN/BAN) 영역에서 정의되고 있다. NIST에서 제시하고 있는 HAN/BAN 영역의 논리적 구조는 [그림 1]과 같다.

특히 AMI 서비스를 위해 전력 공급자와 지능형 계량기가 연결되는 부분은 계량기(8번)와 AMI Headend(21번)가 연결되는 U24 인터페이스와 Energy Service Interface/HAN Gateway(7번)와 AMI Headend(21번)가 연결되는 U25 인터페이스이다. AMI 서비스에서 계량정보의 전달은 U24 인터페이스를 통해 이루어지며, AMI 서비스를 제공, 운용은 U25 인터페이스를 통해 이루어진다. U24와 U25 인터페이스는 본 논문에서 정의하고 있는 무선 통신 기술을 적용한 구간으로, AMI에서 소비자와 전력 공급자 사이에 이루어지는 대부분의 통신은 이 구간을 통해 이루어진다.

2.2 AMI 보안 요구 사항

NIST에서는 스마트 그리드의 논리적 구조 인터페이스를 여러 개의 카테고리로 분류하였고, 카테고리별로 예상되는 보안 위협에 따른 보안 요구 사항을 제시하였다. 다음은 U24 및 U25 인터페이스에 필요한 보안 요구 사항을 정의한 것이다.



〔그림 1〕 HAN/BAN 논리적 구조

- 기밀성 : 지능형 계량기로부터 생성되는 정보는 소비자의 전기 소비 패턴과 같은 개인 정보를 포함하고 있으므로 이 구간에서 유통되는 정보는 기밀로 취급되어야 한다.
- 무결성 : 지능형 계량기가 전기 사용량을 측정한 정보는 과금과 같은 금전 거래의 근거가 되므로 중간에 변조되어서는 안 된다.
- 키 관리 : 전력 공급자는 수백만 개의 지능형 계량기를 관리해야 하며, 또한, 위 구간에 필요한 키 관리 방안이 필요하다.

이 외에 중단 없는 전력 서비스를 위한 가용성과 외부 네트워크를 통한 위협을 줄이기 위해 인터넷과 같은 공공망과 분리된 형태의 네트워크 구축을 요구한다.

III. 무선 통신 기술 비교

AMI 네트워크 구축 방안 중 하나로 다양한 무선 통신 기술 도입이 고려되고 있다. 하지만, 무선네트워크들이 가지는 특성들 때문에 이를 AMI에 적용하면 각각 장단점이 존재한다. 〔표 1〕에서는 무선 통신 기술별 주요 특징들에 대해 알아보고 다양한 무선네트워크들을 AMI에 적용할 때의 장단점에 대해 도출한다.

3.1 ZigBee

ZigBee는 저전력, 저가격, 사용의 용이성을 가진 근거리 무선센서네트워크의 대표적 기술 중 하나이다〔9〕. 모듈의 가격이 저렴하여 비교적 적은 비용으로 무선 근거리 네트워크를 구축할 수 있으며, 보안 특성으로 128bit 키의 AES-CCM*를 지원하여 데이터의 기밀성과 무결성을 보장한다〔10〕. 또한, 스마트 그리드에서의 활용을 위해 HAN(Home Area Networks) 영역에서의 지능형 에너지 관리를 위한 무선 통신 기술 연구가 진행되고 있다〔11〕.

3.2 WiFi

WiFi는 최근 가장 대중적으로 사용되고 있는 무선 통신 기술이며, 802.11n의 등장으로 유선 랜 못지않은 빠른 속도의 통신이 가능해졌다〔12〕. 또한, 802.11i의 최근 표준인 WPA2에서는 128비트 AES-CCM를 지원하며〔13〕, 최근에는 3GPP에서 3GPP-WLAN 연동을 위한 USIM 기반의 AKA 보안 기술을 표준화하고 있다〔14〕.

3.3 WCDMA

WCDMA는 3세대 이동통신 기술 표준의 하나로 국내를 비롯하여 세계적으로 널리 쓰이고 있는 이동통신 기술이다[15]. WCDMA에 적용된 보안 구조는 USIM 중심의 사용자 영역 및 서비스 네트워크 영역, 홈 환경 영역으로 구분되며 사용자 신원 기밀성 및 사용자 인증, 데이터 기밀성 및 무결성 등을 보장하도록 구성되어 있으며[16], 영역별 암호화 수행 절차에 따라 MILENAGE 및 KASUMI 등 다양한 암호 알고리즘이 사용된다[17]. 그러나 현재 KASUMI는 보안상 취약점이 발견되었다[18].

3.4 WiBro

와이브로는 4G 통신 기술 중 하나로 국제 표준으로 채택되어 현재 수도권을 중심으로 서비스 범위를 점차 늘려나가고 있다. 비교적 빠른 통신 속도와 이동성 지원으로 차세대 통신 기술로 주목받고 있다. 암호 알고리즘으로 128비트 AES-CCM/CBC/CTR 등을 지원하고 있으며, 기존의 3G 통신망과 유사하게 USIM을 사용하여 사용자를 인증하기 때문에[19] 사용자 중심의 서비스가 상대적으로 쉬운 장점이 있다.

3.5 Binary CDMA

Binary CDMA 기술은 WLAN이나 Bluetooth와 같은 다양한 무선 기술들의 혼재에 따른 주파수 할당 문제나 QoS 보장 문제를 해결하기 위해 제안된 무선 기술이다. 특히 직진성이 보장되지 않거나 전송채널이 포화되는 등의 열악한 환경에서 기존의 CDMA보다 우수한 성능을 보이며, 회로의 변조구조가 단순하여 칩 제작이 쉽다[7]. 현재 Binary CDMA 기술을 기반으로 한 Koinonia 기술이 개발 완료되었고[20-21], Guardian 등의 기술이 개발 중에 있으며[22], 특히 Koinonia는 2009년 1월에 ISO/IEC JTC SC6에서 국제 표준으로 채택되기도 하였다[23]. 또한, 새로운 유무선 네트워크 공공망 모델로 Koinonia 시스템을 기반으로 하고 ARIA 적용이 가능한 BLAN(Binary CDMA LAN)이 제안되기도 하였다[24].

3.6 비교 분석 결과

Zigbee는 통신거리가 짧고 통신 속도가 느려 AMI와 같은 광역화된 네트워크에 적용은 부적절하며, WiFi의 인증 및 키 관리 체계는 아직 단말기를 중심으로 이루어지고 있어 단말기별로 키가 유지, 관리되어야 하는데 AMI 네트워크에서는 단말기 역할을 하

[표 1] 무선 통신 기술 비교

구 분	Zigbee	WiFi	WCDMA	Wibro	BCDMA
통신거리	10~75m	115~500m	1~2km	100m~1km	800~1km
통신속도	~250Kbps	~300Mbps	Up : ~2Mbps Down : ~7.2Mbps	~10Mbps	~10Mbps
암호 알고리즘	128bit AES-CCM*	128bit AES-CCM	128bit KASUMI	128bit AES-CCM	128bit AES-CCM ARIA-CCM
키 관리	단말기 중심	단말기 중심	USIM 중심	USIM 중심	BSIM 중심
이동성	○	△	○	○	○
공공성	× (ARIA 미지원)	× (ARIA 미지원)	× (ARIA 미지원)	× (ARIA 미지원)	○ (ARIA 지원)
AMI 구축 및 운영 편의성	통신거리가 짧고 통신 속도가 느려 AMI와 같은 광역화된 무선 네트워크에 적용하기에는 부적절함	단말기를 중심으로 하는 키 관리 체계로 AMI 적용 시 단말기와 사용자 정보를 연동하는 과정이 필요함	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	BSIM 중심의 인증 체계와 이를 바탕으로 한 AMI 전용 네트워크 구축으로 전력 사업자의 운영 및 관리가 편리

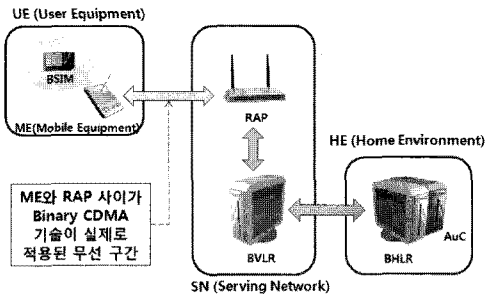
는 지능형 계량기까지 전력 사업자의 소유로 있기 때문에 WiFi를 AMI 네트워크에 적용하기 위해서는 지능형 계량기의 정보와 사용자 정보를 수동으로 연동시키는 과정이 필요하다. 또한, WCDMA 및 WiBro는 이미 구축 완료된 이동통신사의 네트워크를 활용할 수 있으므로 초기 AMI 네트워크 구축비용을 절감할 수 있지만, 이동통신사의 네트워크를 같이 사용하면 이동통신사와 전력 회사 사이에 사용자 인증 등과 같은 보안 관리 책임에 관한 문제가 발생할 수 있으며, 기존의 인터넷과 분리되어야 하는 AMI 네트워크의 특성상 무선 구간을 AMI 구간과 인터넷으로 나누어서 운영하는 문제도 해결해야 한다. 또한, 전력망은 공공망으로써 공공기관에 적용하는 암호화 기술은 국가 표준을 적용해야 하는데, 현재 WCDMA 및 WiBro가 국가 표준 암호 알고리즘인 ARIA[25]를 지원하지 않아 ARIA를 적용하기 위한 별도의 방안이 정의되어야 하는 문제도 있다.

이에 반해 Binary CDMA 기술은 WCDMA 및 WiBro보다 열악한 환경에서의 통신 품질이 우수하여 [7] 24시간 동안 중단 없는 실시간 서비스가 이루어져야 하는 AMI 서비스의 품질 향상에 도움이 될 것으로 기대된다. 특히 Binary CDMA의 BLAN-AKA 과정은 BLAN에서 ARIA, AES 겸용으로 지원하므로 국내 환경 및 국제적 활용도가 매우 높으며, 전력망과 같은 공공망에 적용할 수 있는 장점이 있다. 또한, WCDMA나 WiBro처럼 사용자 신원 모듈인 BSIM(Binary CDMA Subscriber Identity Module)을 중심으로 한 인증 프로토콜이기 때문에 사용자 중심의 서비스 제공이 쉽다.

결과적으로 AMI네트워크에 무선 네트워크를 적용하면 Binary CDMA 통신 기술이 타 무선 네트워크와 비교 시 많은 장점이 있다.

IV. Binary CDMA LAN(BLAN) 구조

기존에 제안된 Binary CDMA LAN(BLAN) [24]은 유무선 네트워크 공공망을 위한 구조로써, [그림 2]와 같이 유무선으로 이루어져 있다. BLAN은 UE(User Equipment), SN(Serving Network), HE(Home Environment)로 구성되며, UE와 SN 사이는 무선 구간, SN과 HE 사이는 유선 구간이다. 여기서 UE는 BLAN의 사용자 영역으로, BSIM(Binary CDMA Subscriber Identity Module)과 ME(Mobile Equipment)로 구성된



[그림 2] BLAN(Binary CDMA) 구조

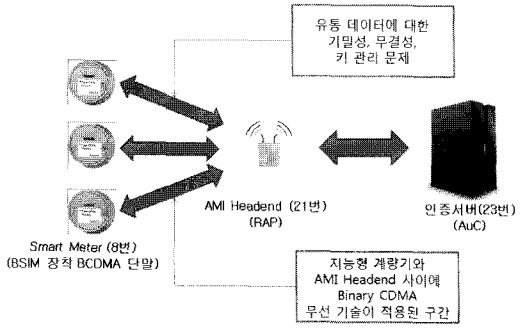
다. SN은 사용자에게 여러 가지 서비스를 제공하기 위한 주체로 RAP(Radio Access Point)와 BVLR (BLAN Visitor Location Register)로 구성된다. HE는 사용자의 개인 정보 및 권한 정보를 저장하며, BLAN-AKA 메커니즘을 지원한다. HE는 BHLR (BLAN Home Location Register)과 인증 서버 (AuC)로 구성된다. 비록 BHLR과 AuC가 논리적으로 서로 다른 개체이지만, 실제로는 물리적으로 같이 구현될 수 있다.

V. Binary CDMA를 적용한 AMI 네트워크

기존에 정의된 BLAN 구조를 AMI 네트워크에 그대로 적용하면 BLAN-AKA 과정을 통해 AMI 네트워크 무선 구간의 기밀성 및 무결성을 확보할 수 있으나 AMI 환경에서는 여러 가지 불필요한 요소들이 존재한다. 이 장에서는 Binary CDMA를 적용한 AMI 네트워크 구조를 제안하고, AMI 구조에 적합한 AKA 프로토콜 과정을 제안한다. 본 논문에서 제안한 AKA는 무선 구간에서의 인증과 키 일치를 위한 것으로, 유선 구간인 AMI Headend와 인증 서버 사이의 보안은 안전하다는 가정한다. 즉, AMI Headend와 인증 서버 사이의 유선 구간은 안전한 채널이 형성되어 있어서 이 구간의 인증 및 통신은 안전성이 보장된다고 가정하며, 또한, 기존에 보안성이 검증된 스마트카드가 많이 활용되고 있고, 지능형 계량기의 안전한 설계 등을 통해 BSIM의 물리적 보안 위협도 예방할 수 있으므로 BSIM의 보안성도 안전하다고 가정한다.

5.1 Binary CDMA를 적용한 AMI 네트워크 구조

Binary CDMA를 적용한 AMI 네트워크 구조는 NIST에서 제시한 [그림 1]의 HAN/BAN 논리적 인터페이스 구조를 바탕으로 구성된다. HAN/BAN



〔그림 3〕 Binary CDMA가 적용된 AMI 네트워크 구조

논리적 구조에 BLAN 구조를 적용하면 ME는 Meter(8번), RAP는 AMI Headend(21번), AuC는 Customer Information System(23번) 구실을 하며, 따라서 Meter(ME)↔AMI Headend (RAP) 구간에 Binary CDMA를 적용한 형태로 구성된다. 또한, BLAN의 ME와 마찬가지로 Meter에도 BSIM이 장착된다. 여기서 AMI 네트워크의 무선 구간은 Meter(ME)↔AMI Headend(RAP) 사이 구간이고, AMI Headend(RAP)↔Customer Information System(AuC) 구간은 유선으로 가정한다. 전체 구조는 〔그림 3〕과 같고 각 구성 요소별 대응 관계는 〔표 2〕와 같다.

제안된 AMI 네트워크에서도 기존의 BLAN-AKA와 같이 BSIM을 중심으로 인증 및 암호화가 이루어지며, 지능형 계량기가 BSIM을 장착한 형태의 단말기가 된다. 지능형 계량기에 BSIM을 장착하는 이유는 기존의 무선통신망과 달리 AMI에서는 지능형 계량기, 즉 단말기의 영역이 사용자 영역이 아니고 네트워크 영역에 포함되어 있기 때문이다. 기존의 무선통신망은 사용자가 단말기를 소유하고 있고, 단일 무선통신망에 여러 사용자의 단말기가 접속하는 형태라 단말기가 사용자를 구별할 수 있는 수단이 될 수 있지만, AMI 네트워크에서는 단말기의 구실을 하는 지능형 계량기가 전력 사업자의 소유로 되어 단말기 자체로 사용자를 구별하는 것은 부적절하다. 따라서 단말기를 중심으로 사용자를 구별하기 위해서는 단말기와 사용자를 연결하는 별도의 수단이 필요하며, 제안한 AMI 네트워크에서는 BSIM이 이러한 구실을 한다.

또한, 기존에 제안된 BLAN 구조와 다른 점은 기존 BLAN 구조에서 BVLR, BHLR을 제외한 것이다. BLAN의 경우 원래 빈번한 이동을 전제로 구성되었기 때문에 이를 효과적으로 지원하기 위해서는 BVLR과 BHLR이 있어야 하나, AMI에서는 이동통신망보다 단말기(지능형 계량기)의 이동이 빈번하지 않으므로 이를 처리하는 장치가 불필요하다. 따라서 기존 BLAN에 있는 UE-SN-HE 구조에서 각각 BSIM을 포함하는 ME, RAP, AuC만 AMI 네트워크에 적용하는 것이 효과적이다.

〔표 2〕 AMI와 BLAN 구성 요소 관계

	AMI	Binary CDMA
구성요소	Meter (8번)	ME(BSIM 장착)
	AMI Headend (21번)	RAP
	Customer Information System (23번)	AuC(인증 서버)

5.2 AMI 네트워크 AKA 프로토콜

AMI 네트워크에는 BVLR과 BHLR이 생략된 구조로 기존 BLAN-AKA 과정에서 BVLR과 BHLR이 수행하던 역할은 각각 RAP와 AuC가 수행한다. 그리고 기존 BLAN-AKA와 달리 재인증을 위한 프로토콜을 별도로 정의하지 않는다. 그 이유는 AMI 네트워크에서 재인증이 필요한 상황은 기존의 이동통신망의 핸드오버와 같이 사용 중에 재인증이 필요한 상황이 아닌 사용자가 바뀌었거나 의도적/비의도적인 장애 발생 시 등 인증 서버가 인지해야 할 상황이 대부분이기 때문이다. 따라서 재인증이 필요하면 처음부터 AKA 과정을 다시 수행하도록 요구한다. 그러나 AMI 특성상 지능형 계량기와 AMI Headend는 항상 연결이 유지되어 있어야 하고 비교적 고정된 상태로 통신이 이루어지기 때문에 일정 주기별로 키를 교체해야 하며, 이를 위해 AKA 과정이 끝나면 무선 구간의 암호화 시 사용할 여러 개의 세션키 SK를 생성하고 주기적으로 SK를 교체한다.

그리고 본 프로토콜에 사용된 KDF(Key Derivation Function) 함수는 AKA 과정에서 사용되는 임시키 TK와 세션키 SK를 생성할 때 사용되며, 난수성이 검증된 블록암호 기반 키 유도 함수가 사용된다. 특히 SK를 생성할 때 사용되는 KDF는 NIST에서 제안한 키 유도 함수의 Counter 모드〔26〕 등과 같이 블록 한 개로 구성된 입력 값이 내부 함수를 통해 여러 개의 블록으로 확장되어 출력되는 구조이며, 이를 통해 한 번의 AKA 과정으로 여러 개의 SK를 유도하여 키 freshness를 유지할 수 있다.

MAC(Message Authentication Code) 함수는 본 AKA 과정에서 사용자 및 네트워크가 상호 인

〔표 3〕 AMI 구성요소 및 프로토콜에 사용되는 주요 약어 및 표기법

	용 어	설 명
AMI 구성요소	Smart Meter	지능형 계량기
	AMI Headend	인증 서버와 지능형 계량기 사이의 정보 교환을 중계, 관리
	AuC	Authentication Center. 사용자를 인증하고 암호화하기 위한 서버
	BSIM	BCDMA Subscriber Identity Module. 사용자 신원 정보와 사전에 인증 서버와 공유한 MK를 저장하고 있으며, 인증을 수행하는 모듈
Parameters	PID	BSIM에 부여된 영구 사용자 신원 (Permanent ID)
	MK	사전에 인증 서버와 약속한 공유된 킷값으로, 외부에 노출되지 않음 (Master Key)
	TK	SK를 생성하기 위한 임시키 (Temporary Key)
	SK	무선 구간을 암호화하기 위한 세션키 (Session Key)
	n	현재 사용되는 SK를 나타내는 인덱스 값
	$counter$	프로토콜의 freshness를 보장하기 위해 인증 과정에서 인증 서버와 BSIM이 갱신하는 값
	$counter_{AuC}$	인증 서버가 유지하는 counter 값
	$counter_{BSIM}$	지능형 계량기의 BSIM이 유지하는 counter 값
	C	$counter_{AuC}$를 암호화한 값
	C'	BSIM이 인증서버에 보내는 counter 재동기 요청 메시지. $counter_{BSIM}$을 암호화한 값.
	$HNonce$	인증 서버에서 생성하는 난수
	MAC_N	인증 서버에서 계산되며 BSIM이 AMI 네트워크를 인증하는 데 사용
	MAC_M	BSIM이 MAC-N을 확인하기 위해 계산하는 값
	$XRES$	인증 서버에서 계산되며 AMI Headend가 BSIM을 인증하는 데 사용
	RES	BSIM이 AMI Headend에서 인증받기 위해 BSIM에서 AMI Headend로 전송하는 값
표기법	$MAC_K(M)$	키 K로 계산된 메시지 M의 메시지 인증 코드 출력 값
	$KDF_K(M)$	키 K로 계산된 메시지 M의 키 유도 함수 출력 값
	$E_K(M)$	키 K로 암호화된 메시지
	$D_K(M)$	키 K로 복호화된 메시지

증을 하기 위한 값을 얻기 위해 사용되며, 본 프로토콜에서는 MK 및 TK가 비밀키, 인증 서버가 생성한 난수 HNonce가 파라미터가 되어 계산된다.

〔표 3〕은 제안한 프로토콜에 사용된 주요 용어들이며, 〔그림 4〕는 AMI 네트워크 AKA 과정이다.

message 1 : ID Request
AMI Headend → BSIM

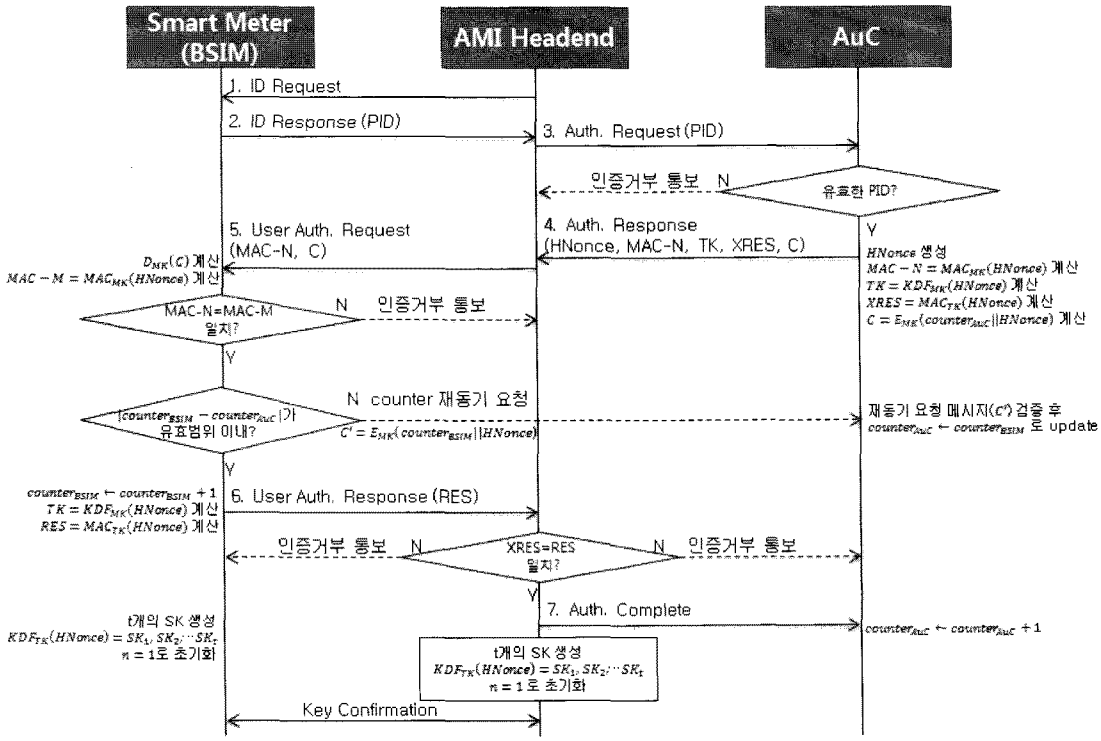
AMI Headend가 지능형 계량기에 Identity Request를 전송함으로써 AKA 과정이 시작된다. 지능형 계량기는 AMI Headend로부터 받은 Identity Request를 BSIM에 전달한다. 이후 지능형 계량기는 AKA 과정에서 AMI Headend와 BSIM 사이의 통신을 단지 중계만 하며, AKA 과정이 모두 끝나면 BSIM으로부터 SK를 받아 무선구간의 암, 복호화를 수행한다.

message 2 : ID Response (PID)
BSIM → AMI Headend

Identity Request를 수신한 BSIM은 Identity Response로 PID(Permanent ID)를 전송한다. PID는 BSIM이 인증 서버에 등록한 사용자의 영구 신원이다.

message 3 : Authentication Request (PID)
AMI Headend → AuC

AMI Headend는 AKA를 위해 필요한 사용자의 데이터를 얻기 위해, BSIM으로부터 수신한 PID를 인증 서버로 전송하며, PID를 수신한 인증 서버는 수신한 PID의 유효성을 검사하여 유효하지 않으면 AMI Headend에 인증 거부를 통보하고 AKA 과정을 종료한다. 유효한 인증 서버일 경우 HNonce를 생성하고, 사전에 BSIM과 공유한 마스터 키 MK와 HNonce를 이용하여 MAC을 통해 BSIM이 네트워크를 인증하기 위한 MAC-N을 계산한다. 그리고 MK와 HNonce를 이용하여 KDF를 통해 차후 SK 생성 시 사용할 임시키 TK를 계산하고, TK와 HNonce를 이용하여 MAC을 통해 차후 AMI Headend가 BSIM을 인증하기 위한 XRES를 계산한다. 또한, 인증 서버가 유지하는 counter ($counter_{AuC}$)도 HNonce와 함께 MK로 암호화한다. counter는 freshness를 보장하기 위해 사용되는 값으로, 상호 인증이 끝나면 BSIM과 인증 서버가 각각 갱신한다.



〔그림 4〕 AMI 네트워크 AKA 프로토콜

$MAC-N = MAC_{MK}(HNonce)$
$TK = KDF_{MK}(HNonce)$
$XRES = MAC_{TK}(HNonce)$
$C = E_{MK}(counter_{AuC} \| HNonce)$

message 4 : Authentication Response
(HNonce,MAC-N,TK,XRES,C)
AuC → AMI Headend

AuC는 앞서 계산한 HNonce, MAC-N, TK, XRES, C를 AMI Headend로 전송한다.

message 5 : User Authentication Request
(MAC-N,C)
AMI Headend → Smart Meter

AMI Headend는 MAC-N, C를 User Authentication Request로 BSIM에 전송한다. BSIM은 수신한 C를 복호화하여 HNonce값을 획득하고, HNonce와 MK를 이용하여 MAC-M을 계산한 후에 이를 수신한 MAC-N과 비교하여 네트워크를 인증한다. 인증에 실패하면 인증 거부를 통보하고 연결을 종료한다. 인증에 성공하면 BSIM은 인증 서버로부터 받은 $counter_{AuC}$의 값과 자신이 유지하는 $counter_{BSIM}$을 비교하여 $counter_{AuC}$가 허용 범위에 있는지 확인한다. 허용 범위를 벗어나면 BSIM은 counter 재동기를 위해 재동기 요청 메시지를 AMI Headend에 전송하고 AMI Headend는 이를 인증 서버에 통보한다. 이때 전송되는 재동기 요청 메시지에 포함된 $counter_{AuC}$는 노출을 막기 위해 HNonce와 함께 MK로 암호화한다. 재동기 요청 메시지를 수신한 인증 서버는 이를 복호화 후에 HNonce를 검증하여 정상적인 재동기 요청 메시지로 확인되면 $counter_{AuC}$를 갱신하고 새로운 AKA 과정을 시작할 수 있다. counter 검증에 성공하면 BSIM은 $counter_{BSIM}$을 갱신한다. 이후 KDF를 통해 MK와 HNonce를 이용하여 TK를 계산하고, MAC을 통해 TK와 HNonce를 이용하여 RES를 계산한다.

$MAC-M = MAC_{MK}(HNonce)$
$counter_{BSIM} \leftarrow counter_{BSIM} + 1$
$TK = KDF_{MK}(HNonce)$
$RES = MAC_{TK}(HNonce)$

message 6 : User Authentication Response
(RES)
BSIM → AMI Headend

BSIM은 앞서 계산한 RES를 User Authentication Response로 AMI Headend에 전달한다. AMI Headend는 앞서 message 4에서 인증 서버로부터 받은 XRES와 BSIM으로부터 수신한 RES가 같은지 확인하여 사용자의 BSIM을 인증한다. 인증에 실패하면 BSIM와 인증 서버에 인증 거부를 통보하고 연결을 종료한다.

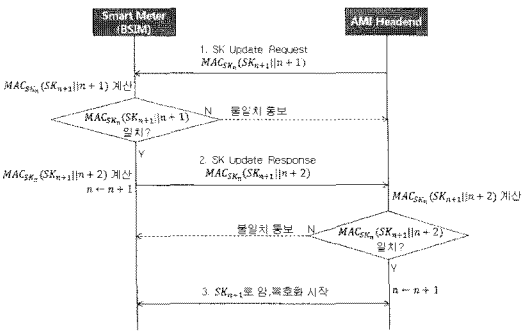
message 7 : Authentication Complete
AMI Headend → BSIM, AuC

인증에 성공하면 인증 서버에 인증 완료를 통보하고, 인증 서버는 $counter_{AuC}$를 갱신한다. 또한, BSIM과 AMI Headend는 KDF를 통해 TK와 HNonce를 이용하여 여러 개의 SK를 생성하며, 이후 키 일치 과정을 수행한다.

$$counter_{AuC} \leftarrow counter_{AuC}+1$$
$$KDF_{TK}(HNonce) = SK_1, SK_2, \ldots, SK_t$$

상호 인증 과정이 정상적으로 완료되면 BSIM과 AMI Headend는 각각 생성한 여러 개의 SK를 이용해 키 일치 과정을 수행한다. 또한, 일정 주기가 되면 기존에 사용하던 SK를 다른 SK로 교체하며, 이 과정에서도 키 일치 과정을 수행한다. 따라서 상호 인증 후 최초 키 일치 과정과 일정 주기별로 수행하는 키 교체 과정은 같으며, 이를 통해 인증 서버의 개입을 줄이면서 SK 갱신이 가능하다. 세부적인 키 일치 및 교체 과정은 아래와 같고, [그림 5]는 키 일치 및 교체 과정을 나타낸다.

message 1 : SK Update Request
$(MAC_{SK_n}(SK_{n+1}\|n+1))$
AMI Headend → BSIM



[그림 5] 키 일치 및 교체 과정

최초 인증이 완료되거나 SK 교체 주기가 되면 AMI Headend는 $MAC_{SK_n}(SK_{n+1}\|n+1)$을 계산하여 BSIM에 전송한다. 여기서 SK_n은 현재 사용하고 있는 SK이며, 키 일치 및 교체 과정이 끝나면 SK는 SK_n에서 SK_{n+1}로 교체된다. 따라서 상호 인증 후 처음으로 키 일치 과정이 수행되면 SK_n은 첫 번째 SK인 SK_1이 사용된다. 즉, SK_1은 상호 인증 후 최초 키 일치 시에만 사용되며, 실제로 무선 구간의 암, 복호화에 사용되는 키는 SK_1 이후$(SK_2, SK_3, \ldots, SK_t)$부터이다.

message 2 : SK Update Response
$(MAC_{SK_n}(SK_{n+1}\|n+2))$
BSIM → AMI Headend

AMI Headend로부터 $MAC_{SK_n}(SK_{n+1}\|n+1)$을 수신한 BSIM은 $MAC_{SK_n}(SK_{n+1}\|n+1)$을 계산하여 수신한 $MAC_{SK_n}(SK_{n+1}\|n+1)$과 일치 여부를 확인하며, 일치하지 않으면 불일치를 통보하고 키 일치 과정을 종료한다. $MAC_{SK_n}(SK_{n+1}\|n+1)$이 일치하면 BSIM은 $MAC_{SK_n}(SK_{n+1}\|n+2)$를 계산하여 이를 AMI Headend에 전송하고 인덱스 n을 $n+1$로 갱신한다.

message 3 : SK_{n+1}로 암, 복호화 시작

BSIM으로부터 $MAC_{SK_n}(SK_{n+1}\|n+2)$를 수신한 AMI Headend는 $MAC_{SK_n}(SK_{n+1}\|n+2)$를 계산하여 수신한 $MAC_{SK_n}(SK_{n+1}\|n+2)$와 일치 여부를 확인하며, 일치하지 않으면 불일치를 통보하고 키 일치 과정을 종료한다. 일치하면 BSIM과 AMI Headend의 SK_{n+1}이 서로 일치하는 것이므로 인덱스 n을 $n+1$로 갱신하고 새로운 SK인 SK_{n+1}으로 무선 구간의 암, 복호화를 진행한다. 이때 BSIM은 지능형 계량기에게 SK_{n+1}을 전달하며, 지능형 계량기는 전달받은 SK_{n+1}을 이용해 암, 복호화를 수행한다.

그리고 생성한 SK를 모두 사용하면 AMI Headend는 지능형 계량기에 Identity Request를 전송하여 새롭게 AKA 과정을 시작한다. 또한, 키 일치 과정에서 이나 MAC 값이 일치하지 않으면 처음부터 다시 AKA 과정을 시작한다.

VI. 분석 및 보안 서비스 시나리오

6.1 제안된 AKA 프로토콜 안전성 분석

앞서 제안한 AKA 프로토콜은 1. 지능형 계량기의

BSIM이 AMI 네트워크 인증 2. AMI 네트워크가 지능형 계량기의 BSIM 인증. 3. 키 일치 및 무선 구간 암, 복호화 순이다. 본 절에서는 프로토콜 진행 단계별로 안전성을 분석하였다.

6.1.1 지능형 계량기가 AMI 네트워크 인증 시의 안전성

지능형 계량기의 BSIM이 AMI 네트워크를 인증할 때 BSIM은 AMI Headend로부터 수신한 MAC-N을 확인하여 AMI 네트워크를 인증한다(단계 5). 이때 MAC-N은 MK와 HNonce를 이용하여 계산된다. 그리고 BSIM 또한, 인증 서버와 같은 방식으로 MK와 수신한 HNonce를 이용해 MAC-M을 계산하여 수신한 MAC-N과 계산한 MAC-N이 일치하는지 확인하여 네트워크를 인증하게 된다. 이때 MAC-N을 계산할 때 필요한 MK 및 HNonce가 무선상에 직접 노출되지 않으므로 BSIM에 대해 비인가된 네트워크의 접근은 불가능하다. 또한, 인증 과정에서 counter를 사용하여 공격자의 재생 공격을 방지하고 프로토콜의 freshness를 보장한다.

6.1.2 네트워크가 BSIM 인증 시 안전성

AMI 네트워크가 BSIM을 인증할 때 AMI Headend가 인증을 수행하게 되는데, AMI Headend는 이전에 수신한 XRES(단계 4)과 BSIM으로부터 수신한 RES(단계 6)를 비교하여 BSIM을 인증한다. 이때 XRES 및 RES를 계산할 때 필요한 TK와 HNonce가 무선상에 직접 노출되지 않으므로 공격자가 AMI 네트워크에 접근하는 것은 불가능하다.

6.1.3 키 일치 및 교체 시 안전성

상호 인증 과정이 끝나면 지능형 계량기와 AMI Headend는 여러 개의 SK를 생성하여 이를 무선 구간의 암, 복호화에 사용하며 일정 주기가 되면 이를 다음 SK로 교체한다. AMI 특성상 지능형 계량기는 같은 AMI Headend와 항상 연결되어 있으므로 주기적으로 무선 구간의 비밀키를 교체해야 하는데, 인증 과정이 끝난 후 생성한 여러 개의 SK를 일정 주기별로 교체하면서 사용하면 이러한 문제를 해결할 수 있으며, AKA 과정에서 생성된 여러 개의 SK들은 난수성이 검증된 KDF를 사용하여 생성되었으므로 일부 SK만 가지고 다른 SK를 알아내기는 어렵다. 그리고 키 일치 및 교체 과정이 모두 암호화되어 진행되므로 키 일치 및 교체 과정 또한, 안전하다. 또한, 암, 복호화 시 기존의 BLAN과 같이 ARIA-CCM을 사용하면 무선 구간에 대한 기밀성과 함께 무결성도 보장할 수 있다.

〔표 4〕 기존 BLAN-AKA와 AMI 네트워크 AKA 비교

	구 분		BLAN-AKA	AMI 네트워크 AKA	비 고
구성 요소	UE		ME, BSIM	지능형 계량기, BSIM	지능형 계량기가 ME 역할 수행
	SN		RAP, BVLR	AMI Headend(RAP)	AMI Headend가 RAP와 BVLR 역할 동시 수행
	HE		BHLR, AuC	AuC	AuC가 BHLR 역할 동시 수행
프로토콜	TID		○	×	위치 기밀성을 위해 사용되는 변수 생략
	MAC-N		MAC(TK, VNonce, counter)	MAC(TK, HNonce)	VNonce를 생략하여 HNonce 사용
	SK		KDF(TK, VNonce, counter) 하나의 SK 생성	KDF(TK, HNonce) 여러 개의 SK 생성	한 번의 AKA로 여러 개의 SK 생성
계산량	메시지 전송 횟수		12회 (무선구간 5회)	8회 (무선구간 5회)	BVLR 및 BHLR 제거로 유선구간 메시지 전송횟수 감소
	알고리즘연산 횟수	KDF	4회(TK,SK)	4회(TK, SK)	
		MAC/mac	8회 (RES/XRES,MAC-N, MAC1,MAC2)	8회 (RES/XRES, MAC-N,MAC-M, SK update)	
		암호화	·	2회(C,D)	counter 암,복호화

6.2 기존 BLAN-AKA와 비교

앞서 제안한 AMI 네트워크에는 BVLR과 BHLR이 생략된 구조로 기존 BLAN-AKA 과정에서 BVLR과 BHLR이 수행하던 역할은 각각 RAP와 AuC가 수행한다. 또한, 본 논문에서 제안한 AMI 네트워크 AKA 프로토콜은 기존의 BLAN-AKA 과정을 준용하면서 AMI에 맞게 일부를 수정하였다. 기존 BLAN-AKA와 AMI 네트워크 AKA 비교 내용은 [표 4]와 같다.

6.2.1 이동성 보장을 위한 요소 제거

기존 BLAN과 AMI 네트워크의 가장 큰 차이점은 단말기의 빈번한 이동 여부이다. AMI는 비교적 고정된 형태의 네트워크이지만 기존 BLAN의 경우 단말기의 빈번한 이동을 전제로 구성되었다. 따라서 상대적으로 단말기의 이동이 빈번하지 않은 AMI에서는 이동성을 보장하기 위한 장치인 BVLR과 BHLR이 생략되었으며, BVLR과 BHLR의 역할은 각각 RAP와 AuC가 같이 수행한다. 또한, BVLR과 BHLR이 생략되어 유선 구간의 메시지 전송 횟수가 기존 BLAN-AKA에 비해 감소하였다. 그리고 위치정보보호를 위한 TID를 제거하였으며, 이동성 보장 및 재인증을 위해 BVLR이 생성하던 VNonce, ANonce도 제거하였다. 따라서 AMI Headend는 암, 복호화 모듈과 난수 생성 모듈이 모두 필요한 기존 BVLR과 달리 KDF 및 암, 복호화 기능만을 수행하므로 별도의 난수 생성 모듈이 불필요하다.

6.2.2 한 번의 AKA 과정으로 여러 개의 SK 생성

기존 BLAN-AKA는 SK를 생성할 때마다 인증 및 재인증 절차를 수행하였으나, 제안된 AKA에서는 한 번의 AKA를 통해 여러 개의 SK를 생성한 후 주기적으로 SK를 교체하므로 AKA 종료 후에도 무선 구간의 Key freshness를 유지한다. 또한, SK 교체 과정이 인증 서버 없이 진행되므로 인증 서버의 부하도 감소한다.

6.3 충족 가능한 보안 요구 사항

제안된 네트워크 구조 및 프로토콜을 적용하면 기존에 제기되었던 AMI 네트워크에 대한 보안 요구 사항을 만족하게 할 수 있으며, 비교 내용은 [표 5]에 정리하였다. 세부적인 사항은 아래와 같다.

- 기밀성/무결성 : 통신 전 BSIM을 이용해 상호 인증 키 일치 완료 후 기밀성/무결성이 보장된 암호알고리즘을 사용하여 무선 구간을 암호화하면 무선 구간 데이터에 대한 기밀성/무결성을 보장할 수 있다. 또한, 차후 스마트 그리드와 관련된 서비스가 제공되면 서비스 과정에서 HAN 영역에서 발생한 에너지 사용 통계 정보는 과금에 필수적인 자료를 제외하고 모두 BSIM에 저장할 수 있기 때문에 개인 정보 유출에도 상대적으로 안전하다.
- 키 관리 문제 : BSIM을 이용하기 전에 전력 회사의 사용자 키 관리 서버에 BSIM을 먼저 등록하기 때문에 사용자 키 관리가 간편해진다.

6.4 BSIM 적용시 장점

제안된 AMI 네트워크의 특징 중 하나는 BSIM을 도입한 것으로, AMI에 BSIM을 적용함으로써 다양한 장점이 존재한다.

- 보안성 향상 : BSIM을 통한 인증 및 암호화를

[표 5] 제안된 AMI 구조 분석 및 BSIM 적용 시 장점

	구 분	설 명
보안 요구 사항	기밀성/무결성	• BSIM을 이용한 상호 인증 후 암호화로 무선 구간 기밀성/무결성 보장 • 차후 HAN 영역에서 발생한 개인 정보를 모두 BSIM에 저장하여 개인 정보 유출에 안전
	키 관리	• BSIM을 사용자별로 발급/관리하여 키 관리 과정이 간편해짐
BSIM 적용 시 장점	보안성	• 비인가자 접근이 쉬운 지능형 계량기 대신 BSIM이 보안 기능을 수행하여 보안성 향상
	사용자 중심의 서비스	• 사용자별로 발급/관리되는 BSIM 중심의 서비스이므로 사용자 중심의 서비스 제공 가능
	유연성	• 장소와 무관하게 BSIM을 통한 인증 및 서비스로 더욱 유연한 서비스 제공 가능
	프라이버시	• BSIM의 저장 공간을 통해 서비스 과정에서 발생한 개인정보 보관 가능

할 때 사용자를 직접 인증하는 것과 유사한 과정을 수행하게 된다. 만약 AMI 네트워크를 BSIM이 없는 형태로 운영하려면 전력 운영자가 지능형 계량기를 중심으로 인증 및 암호화를 수행해야 하는데, 지능형 계량기는 소비자와 가까운 곳에 있어 물리적 보안에 취약하다. 따라서 비인가자의 접근이 쉬운 환경에 있는 지능형 계량기가 직접 보안에 관련된 기능을 수행하는 것은 부적절하며, 보안성이 검증된 스마트카드 형태의 BSIM에서 보안 기능을 수행하는 것이 상대적으로 안전하다.

- 사용자 중심의 서비스 : AMI 네트워크에서 지능형 계량기와 AMI Headend 사이 구간의 암호화는 필수적이며, 최소한 사용자 수만큼 암호키가 유지, 관리되어야 한다. 하지만, BSIM이 없다면 인증 서버에서 지능형 계량기 자체를 인증하고 암호화하게 되는데, 이 경우 지능형 계량기의 암호키와 사용자 정보를 연동시키는 과정이 있어야 하며, 또한, 지능형 계량기의 사용자가 바뀌면 연동 정보도 같이 변경해줘야 하는 번거로움이 따른다. 하지만,BSIM을 중심으로 인증 및 암호화를 수행하면 자연스럽게 사용자 정보와 암호키의 연동이 이루어지며, 차후 사용자의 이동 및 신규 가입, 서비스 해지 등의 절차를 수행 시에도 인증 서버에서 해당 BSIM의 이동 및 등록, 해지만 수행하면 되므로 사용자 중심의 서비스가 쉽다.
- 유연성 : 이동통신망과 달리 AMI 네트워크에서는 이동이 빈번하지 않지만, 본 논문에서 적용한 BSIM 중심의 인증 및 서비스 구조는 사용자를 중심으로 한 유연한 서비스 제공이 가능하다. 예를 들어 사용자가 이사 등으로 말미암아 타 장소에서 전력 서비스를 받고자 하는 경우 기존에 있던 BSIM을 새로운 장소에 있는 지능형 계량기에 삽입하여 새로 인증 과정을 거치면, 전력 사업자도 기존의 사용자가 이동한 위치를 쉽게 파악하고 연속적인 전력 서비스를 제공할 수 있다.
- 프라이버시 문제 해결 : HAN 영역의 서비스가 개발되면 필연적으로 사용자별 전기 사용 패턴 데이터가 생성될 수밖에 없으며 이는 개인정보로 취급되어야 한다. 차후 BSIM이 대용량 저장 공간이 있는 스마트카드로 구현되면 이러한 개인정보를 전력 회사 서버가 아닌 대용량 BSIM에 관련 로그 기록을 저장한다면 프라이버시 문제에도 대응할 수 있다.

6.5 보안 서비스 시나리오

제안된 AMI 네트워크에서 BSIM을 활용하면 전력과 관련된 다양한 보안 서비스를 할 수 있다.

6.5.1 전력 서비스의 신규가입, 이동, 해지

제안된 AMI 네트워크 구조는 BSIM을 중심으로 한 보안 구조이므로 사용자의 전력 서비스 신규가입 및 이동, 해지 등의 절차는 기존 3G 이동통신망의 신규가입 및 이동, 해지 절차와 유사하게 처리할 수 있다. 신규가입은 사용자에게 BSIM을 발급하여 이를 지능형 계량기에 삽입하면 되고, 이사 등으로 말미암은 이동 시에는 이동통신망의 USIM을 통한 기기변경과 같이 기존에 사용했던 BSIM을 가지고 새로운 장소에 있는 지능형 계량기에 삽입하면 된다. 서비스 해지 시에는 기존에 발급된 사용자 BSIM을 인증 서버에서 무효로 하면 되며, 기타 BSIM 훼손 및 분실 등으로 말미암은 재발급 시에도 기존에 발급된 BSIM을 무효화시킨 후 새로운 BSIM을 발급, 등록하면 된다.

6.5.2 임시 전기 신청 및 사용

현재도 사용자가 전력 사업자에게 임시 전기 사용을 신청하는 절차가 있지만, BSIM을 활용하면 이러한 절차를 간소화할 수 있다. 예를 들어 야외공연, 행사, 공사장 등 특정 기간에 특정 장소에서 전력을 사용할 때 BSIM을 이용한 사용자 인증을 통해 과금 및 기타 서비스를 하는 것이다. 이를 위해 우선 지능형 계량기 내부에 장착하는 BSIM과 별도로 이동형 BSIM 발급하여 필요한 소비자에게 분배하고 행사장 전력이 공급되는 곳에 있는 스마트 미터에 BSIM 장착한 후에 사용자 인증을 수행한다. 그리고 행사 기간에 전기를 사용한 후 행사 종료 후에 BSIM 제거하면 서비스가 종료되며, 차후 이를 근거로 BSIM 명의자에게 전기요금을 부과하면 될 것이다. 또한, 필요하면 이동형 AMI Headend(RAP)를 추가하여 이를 이용한 사용자 인증 및 서비스 수행도 가능하다.

VII. 결론 및 차후 연구과제

본 논문에서는 Binary CDMA를 이용한 AMI 무선 네트워크 보안 구조를 제안하였다. 제안된 구조를

적용하면 효율적인 AMI 네트워크 구축이 가능해지며, 특히 BSIM을 중심으로 한 인증 및 암호화를 통해 AMI 네트워크 무선 구간의 기밀성 및 무결성을 보장함과 동시에 수많은 지능형 계량기에 대한 키 관리 문제도 해결할 수 있다. 그리고 기존의 무선장치는 공공망의 성격을 가진 전력망에 적용하면 ARIA를 수용할 수 없다는 매우 현실적인 어려움이 있지만, Binary CDMA는 ARIA와 AES를 겸용으로 쓸 수 있으므로 스마트그리드 무선 환경에 적합하며, 또한, Binary CDMA가 가진 유연성을 살려 다양한 서비스를 제공할 수 있게 된다.

한편, 이러한 기반체계를 이용한 다양한 보안 서비스 시나리오에 대한 연구가 필요하다. 스마트카드 기술의 발전으로 BSIM에 대용량의 데이터를 안전하게 보관할 수 있으므로 서비스 과정에서 발생하는 개인정보를 BSIM에 저장, 관리하는 방안과 인증 서버와 Binary CDMA의 이동성을 활용한 원격 제어 서비스 시나리오 설계에 관한 연구들이 앞으로 더욱 진행될 것이다. 또한, BSIM이 외부 노출에 취약한 지능형 계량기에 장착되므로 외부자에 의한 BSIM 탈취에 의한 문제도 예상되는데, 이에 대비하여 BSIM을 분리할 때 비밀번호를 입력하거나 임의로 분리된 BSIM은 재사용이 불가능하도록 하는 등의 보안 대책도 구체적인 연구가 진행되어야 할 것이다.

참 고 문 헌

[1] 김선진, 서정해, 전종암, 표철식, "USN 기반 AMI 서비스 및 기술동향:전력 산업과 USN 산업의 융합기술", 한국전자통신연구원 전자통신동향분석, 23(5), 2008년 10월.

[2] 이정준, "AMI 국제 표준화 동향", 전기신문, 2010년 3월.

[3] Motorola, "AMI and Beyond:How Wireless Broadband Enables the Smart Grid Today and Tomorrow" Motorola Solution Brief, 2009.

[4] Wayne F. Boyer and Scott A. McBride, "Study of Security Attributes of Smart Grid Systems - Current Cyber Security Issues" Idaho National Laboratory Critical Infrastructure Protection/Resilience Center, pp. 12-13, Apr. 2009.

[5] Patrick McDaniel and Sean W. Smith, "Security and Privacy Challenges in the Smart Grid", IEEE Computer and Reliability Societies, pp. 72-74, Jun. 2009.

[6] 전용희, "지능형 전력망(Smart Grid)과 정보보호" 한국정보보호학회지, 19(4), pp. 65-71, 2009년 8월.

[7] 류승문, "Binay CDMA 소개," 한국전자파학회 전자파기술, 13(4), pp.13-24, 2002년 10월.

[8] Gary Locke and Patric D. Gallagher, "Guidelines for Smart Grid Cyber Security : Vol. 3, Supportive Analyses and References", NISTIR 7628, The Smart Grid Interoperability Panel - Cyber Security Working Group, Aug. 2010.

[9] 한국 ZigBee 포럼 홈페이지, "http://zigbee-forum.or.kr/forum_info/info04_1.html"

[10] ZigBee Standards Organization, "ZigBee Specification", Document 053474r17, Jan. 2008.

[11] Brent Hodges, Craig Rodine, Craig Tinder, and Ivan O'Neill, "Smart Energy Profile Marketing Requirements" Document Draft Revision 1.0, ZigBee+HomePlug Joint Working Group, Mar. 2009.

[12] IEEE 802.11 Standard "Wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) Specifications Amendment 5: Enhancements for Higher Throughput," Oct. 2009.

[13] IEEE 802.11 Standard "Amendment 6: Medium Access Control(MAC) Security Enhancements," Jul. 2004.

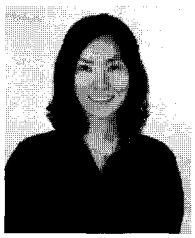
[14] 3rd Generation Partnership Project, "Technical Specification Group Service and System Aspects;3G Security;Wireless Local Area Network(WLAN) interworking security(Release 9)," 3GPP TS 33.234 V9.2.0 Jun. 2010.

[15] Aymem I. Zreikat, Khalid Al-Begain and Kevin Smith, "A Comparative Capacity/Coverage Analysis for CDMA Cell in Different Propagation Environments," Wireless Personal Communications 28: pp. 205 - 231, 2004.

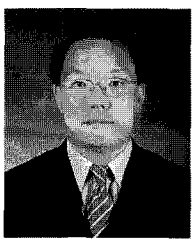
[16] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects:3G Security:Security architecture(Release 9)," 3GPP TS 33.102 V9.2.0, Mar. 2010.
[17] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects:3G Security:Cryptographic algorithm requirements(Release 9), "3GPP TS 33.105 V9.0.0, Dec. 2009.
[18] IACR eprint archive: Orr Dunkelman, Nathan Keller, and Adi Shamir, "A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony," IACR ePrint 2010-013, Jan. 2010.
[19] 이재일, 원유재, 지승구, 이태진, "와이브로 보안기술 안내서," KISA 안내·해설 제2010-26호, 한국인터넷진흥원, 2010년 1월.
[20] KETI, "Koinonia 표준규격서, 물리 계층과 데이터링크 계층 규격 버전 1.0," 2003년 5월.
[21] 강성진, 홍대기, 이현석, 조진웅, "Design methodology : Binary CDMA를 기반으로 하는 Koinonia 시스템의 모뎀 설계," IT SOC magazine, 15, pp. 44-50, 2006년 11월.
[22] 임순빈, 정쌍봉, 이태진, 전선도, 이현석, 권대길, 조진웅, "Koinonia 고속 WPAN에서 보안을 위한 대칭/비대칭 비밀 키 교환 방법," 한국통신학회논문지, 31(6B), pp. 551-560, 2006년 6월.
[23] 지식경제부, "Binary CDMA 특허기술 ISO 국제표준 확정," 지식경제부 기술표준원 정보통신표준과 보도자료, 2009년 1월.
[24] 김용희, 박미애, 조진웅, 이현석, 이장연, 이옥연, "Binary CDMA 망을 위한 안전한 AKA 프로토콜," 한국정보보호학회논문지, 20(1), pp. 51-61. 2010년 2월.
[25] 산업자원부 기술표준원, "128비트 블록 암호 알고리즘 ARIA," KS X 1213:2004, 2004년 12월.
[26] 강주성, 이옥연, 염지선, 조진웅, "키유도함수의 통계적 난수성 평가 방법," 정보처리학회논문지C, v.17C, no.1, pp.47-60, 2010년 2월.

〈著者紹介〉

전 재 우 (Jae-woo Jeon) 학생회원
2005년 3월: 육군사관학교 전산학과 학사
2009년 3월~현재: 고려대학교 정보경영공학전문대학원 석사과정
〈관심분야〉 무선이동통신 보안, 스마트그리드 보안



임 선 희 (Sun-Hee Lim) 정회원
1998년 2월: 고려대학교 컴퓨터학과 학사
2005년 2월: 고려대학교 정보보호대학원 석사
2010년 8월: 고려대학교 정보보호대학원 박사
2010년 9월~현재: 한국전자통신연구원 소프트웨어연구부문 (선임연구원)
〈관심분야〉 무선이동통신 보안, 네트워크 보안, Quality of Protection



이 옥 연(Okyeon Yi) 종신회원
1988년 2월 : 고려대학교 이과대학 수학과 학사
1990년 2월 : 고려대학교 대학원 수학과 석사
1996년 8월 : University of Kentucky 수학과 박사
1999년 7월~2001년 8월 : 한국전자통신연구원 팀장
2001년 9월~현재 : 국민대학교 자연과학대학 수학과 교수
〈관심분야〉 이동통신 보안, 암호알고리즘, 스마트그리드보안 등