대칭키 기반의 AMI 시스템 통신망 보안 설계*

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

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

Jieun Oh, Minku Kim, HoSung Jeon, 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 AMI 시스템의 문제점을 분석하고, 대칭키 기반의 보안으로 안전한 AMI 시스템의 통신망 구조를 제시하여 BSIM(Binary Subscriber Identity module)을 중심으로 인증 및 암호화를 위한 키 분배 프로토콜 등의 통합적인 관리를 제안한다.

1. 서론

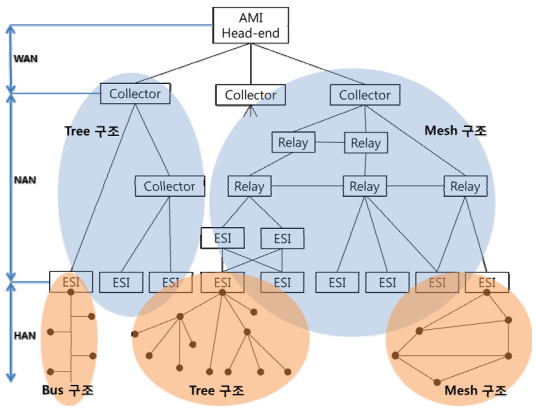
스마트 그리드(Smart Grid) 사업은 세계 각국에서 주목받는 사업일 뿐만 아니라 한국을 중심으로 저 탄소 녹색 성장의 표어 하에 추진되는 전력과 IT가 결합된 사업이다. 스마트 그리드 사업의 핵심인 AMI 시스템의 목적은 전력의 제공자와 소비자가 양방향 통신을 함으로써 능동적인 자원 소비로 불필요한 에너지의 소모를 감축하고 정전 사태 등의 잠재적 재난에 대비하기 위한 전력의 효율적인 관리를 위한 것이다. 그러나 IT의 결합으로 인해 IT상의 문제점이 AMI 시스템에 그대로 반영될 수 있는 가능성이 있다. 이에 대하여 공개키 기반의 AMI 보안 시스템에 대한 연구가 제시되고 있으나 인프라 구축에 막대한 비용이 들어가 현실적인 어려움이 따르며 연산속도가 느리기 때문에 서비스의 속도를 저하시킬 수 있는 가능성이 있다. 본 논문에서는 AMI 시스템의 문제점을 분석하고, 대칭키 기반의 보안으로 안전한 AMI 시스템의 통신망과 인증 및 키 일치 등의 통합적인 관리를 제안한다[1].

본 논문의 구성은 다음과 같다. 2장에서는 AMI의 구조와 통신에 대해 소개한다. 3장에서는 기존에 제시된 AMI 시스템의 구조에 따른 보안위협을 분석하고, 이에 대한 요구사항을 도출한다. 4장에서는 BSIM 기반의 AMI 통신망 구조와 통합적인 보안 관리를 위한 키 분배 프로토콜을 제안한다. 5장에서는 4장에서 제시한 구체적인 보안 프로토콜에 적용된 요구의 사항의 개선된 사항을 제시한다. 6장에서는 결론 및 차후 연구과제에 대해 언급한다.

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

2. AMI 시스템의 구조와 통신

2011년 6월 제주에서 개최된 '스마트 그리드 포커스 그룹 회의'에서 AMI 구조를 WAN(Wide Area Network), NAN(Neighborhood Area Network), HAN(Home Area Network)으로 확정지으며 Bus, Tree, Mesh 세 가지 유형의 네트워크 토폴로지를 제시하였다.



(그림 1) 스마트 그리드 구성 구조 모델

(그림 1)에서 볼 수 있는 AMI Head-end는 AMI 시스템을 제어, 관리하며 소비자에게 서비스를 제공하는 전력회사의 서버를 나타내며, Collector는 데이터 수집기 DCU(data concentrator unit)에 해당하며, 각 소비자로부터 데이터를 수집하여 한번에 AMI 서버로 전송하고, WAN과 NAN의 교량 역할을 한다. Relay는 NAN의 네트워크내의 교량역할을 한다. ESI(Energy Service Interface)는 각 소비자의 영역 네트워크의 입구에 해당하며 전력회

사로부터 전달된 서비스를 소비자에게 제공하는 역할을 하고, 전력회사와 소비자의 영역을 구분 짓는 실질적인 경계점이다. 스마트 미터기가 대개 ESI의 역할을 한다.

AMI 네트워크에서 WAN의 영역은 Wibro, D-TRS, 광 통신망 등 이동통신사의 네트워크를 활용할 수 있어 비용의 절감과 동시에 통신망의 확보가 손쉬우나, NAN과 HAN의 영역은 다양한 전송 기기 및 사업성에 따라 각기 다른 형태로 구축 운영되고 있어 통합적인 보안과 관리가 필요하다. NAN과 HAN의 사용될 통신 후보로 꼽히는 통신인 Binary-CDMA, PLC, ZigBee를 살펴보겠다.

2.1 Binary-CDMA(ISO/IEC SC6)

다양한 무선 기술의 주파수 할당문제와 QoS보장 문제를 해결한 무선 기술로 회로의 변조구조가 단순하여 칩 제작이 쉽다. Binary CDMA를 기반으로 한 Koinonia기술이 개발 완료되어 국제표준 채택되었으며, 유무선 네트워크 공공 망 모델로 Koinonia시스템에 ARIA적용이 가능한 BLAN(Binary CDMA LAN)제안된바 있다[2,3]. 현재까지 보안 문제점이 지적된 바 없는 NAN에 적합한 통신이다.

2.2 PLC(KS X 4600-2)

기존의 전력선에 데이터 신호를 커플링 시켜 전송하는 유선 통신 기술로 인프라 구축이 쉽다. 같은 그룹ID(GID)를 공유하고 있는 노드 간에 56-DES와 128-AES로 암호화를 하지만 표준에선 단편적으로 언급되어 있다[4]. 명확한 보안 표준 없이 사용하면 제품 간 상호호환의 문제가 발생하므로 AMI 통신으로는 아직 부적합 하다.

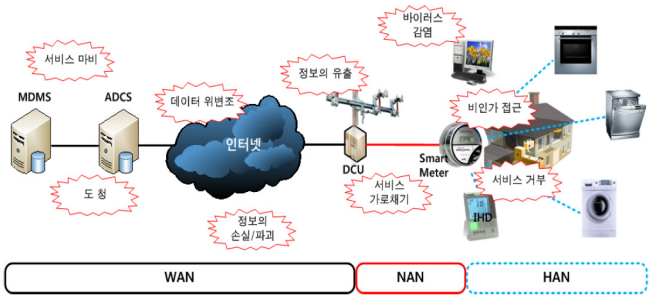
2.3 ZigBee(IEEE 802.15.4)

저전력, 저가격의 용이성을 가진 근거리 무선센서네트워크기술로 128비트 AES-CCM* 지원한고, 홈 네트워킹 서비스를 위한 기술로서 주목받는다[5]. 마스터키의 분배 및 갱신에 대한 이슈와, 코디네이터의 부담 등의 통신 기술상의 문제를 해결해야한다.

3. AMI 시스템의 보안위협 분석

AMI 시스템은 국가적 기간사업으로 보안상의 문제가 발생하면 개인의 프라이버시 침해는 물론, 사회적 혼란을 초래하는 등 막대한 피해가 발생한다. 따라서 AMI 시스템은 초기 구성부터 보안에 적합한 구조로 설계해야 한다. AMI 보안의 취약점은 두 가지 관점에서 분석할 수 있는데, 위에서 언급한 AMI에서 사용되는 통신 보안 문제와 AMI 네트워크 전체의 보안 문제이다.

기존의 전력망은 폐쇄적 단독 망 운영관리로 보안위협에 노출될 수 있는 가능성을 최소화 했지만 AMI 시스템은 전력 사업자와 소비자와의 양방향 통신이 그 핵심이므로 전력망에 IT가 접목되고, 외부 네트워크에 노출 될 수 밖에 없다. 따라서 기존의 IT의 보안문제가 AMI 시스템의 잠재적 보안문제가 될 수 있다. AMI의 망에서 예상되는 보안 위협 문제는 (그림 2)와 같다. MDMS(Meter Data Management System)는 정보를 처리하는 서버이고, ADCS(Automated Data Collection System)은 DCU의 정보를 수집하는 역할을 수행한다. IHD(In Home Display)는 전력회사가 제공하는 서비스와 댁내 정보를 소비자에게 표시해주고, 댁내 전력 및 에너지를 제어하는 역할을 한다.



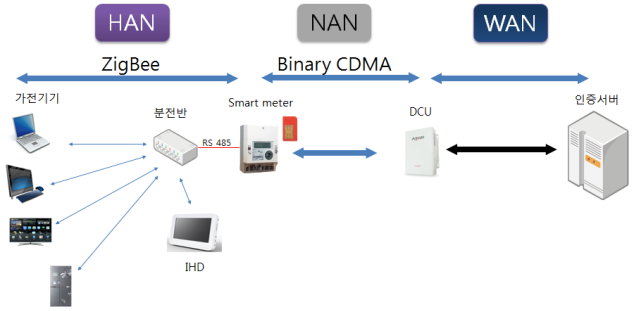
(그림 2) AMI시스템에서 예상되는 보안 위협의 사례

스마트 미터기로부터 생성되는 정보는 소비자의 전력 사용 패턴과 같은 개인 정보를 포함하고 있으므로 누출에 유의해야 한다. 스마트 미터기에서 측정된 전력 사용량 등의 정보는 과금과 같은 금전거래의 근거가 되므로 변조될 수 없도록 해야 한다. AMI 시스템은 악의적인 디바이스가 네트워크에 들어 왔는지, 디바이스가 조작되었는지 여부를 항상 감시하고 확인해야 한다. 그밖에 서비스의 마비, 도청, 서비스 가로채기, 바이러스 감염, 서비스 거부 등의 문제에 대한 대비책이 필요하다[7].

위의 여러 가지 보안 위협으로부터 안전한 AMI 시스템을 위해서 다음의 요건이 충족되어야 한다. 첫째, 기밀성, 무결성, 인증, 권한부여, 부인방지의 정보보안의 기본적인 요구사항을 갖추어야 한다. 둘째, 디바이스 인증 및 암호화에 필요한 안전한 키 분배 프로토콜이 필요하고 이를 위해 키를 관리할 서버가 존재해야 한다. 마지막으로 소비자의 감시 및 관리가 필요하다[6,7].

4. BSIM기반 AMI 네트워크 망

본 장에서는 안전한 AMI 네트워크를 위해 BSIM 기반의 통신기술을 적용한 AMI 구조를 제안하고 보안 아키텍처를 말하고자 한다. 본 논문에서 제안하는 AMI 구조는 (그림 3)과 같이 HAN에서 ZigBee를 사용하고 NAN에서 Binary CDMA를 사용한다.



(그림 3) 제안된 AMI 구조

스마트 미터기에서는 BSIM을 중심으로 인증 및 암호화가 이루어진다. BSIM은 핸드폰의 USIM과 같이 사용되는 Binary 통신을 위해 고안된 칩으로 사용자의 신원 정보와 보안키, 보안 모듈을 탑재할 수 있다. BSIM을 사용함으로써 전력 회사와 사용자간의 인증문제를 해결할 수 있고 키를 관리하는 인증서버와 BSIM간에 마스터키를 사전에 공유할 수 있다. 스마트 분전반은 물리적으로 스마트 미터기와 분리되어 있으나 RS485 통신으로 스마트 미터기와 논리적으로 하나로 볼 수 있다[9].

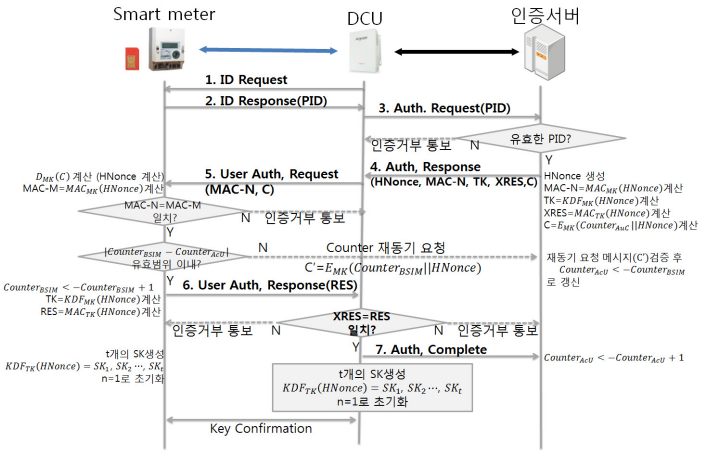
4.1 NAN의 AKA 프로토콜

NAN의 영역에서는 AKA(Authentication and Key Agreement) 프로토콜을 사용하여 기존의 이동통신망과 같은 인증 절차를 거친다. BSIM이 탑재되어 있는 스마트 미터기는 핸드폰과 같이 이동성이 필요하지 않기 때문에 사용 중에 재인증이 필요한 상황이 발생하지 않으므로 재인증을 위한 프로토콜은 정의하지 않는다. 암호화의 안전을 확보하려면 주기적으로 키를 교체해야 하므로 AKA과정이 끝나면 무선 구간의 암호화시 사용할 여러 개의 세션키 (SK)를 생성하여 주기적으로 교체한다[10].

<표 5> NAN 구성요소와 프로토콜 주요 약어

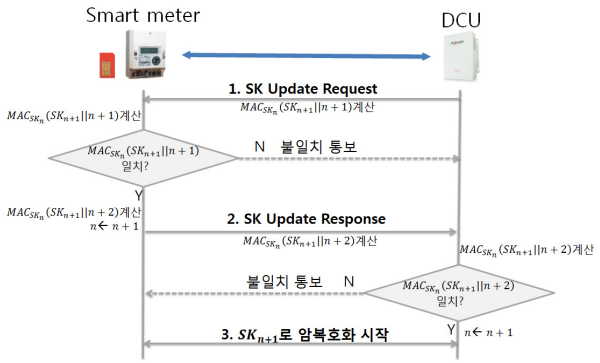
	용어	설명
AMI 구성요소	$SmartMeter$	스마트 미터기
	DCU	인증 서버와 스마트 미터기간 정보 교환을 중계,관리
	AuC	Authentication Center. 사용자를 인증하고 암호화하기 위한 서버
	$BSIM$	BCDMA Subscriber Identity Module. 사용자 신원 정보와 사전에 인증 서버와 공유한 MK를 저장하고 있으며, 인증을 수행하는 모듈
parameters	PID	$BSIM$에 부여된 영구 사용자 신원 (Permanent ID)
	MK	사전에 인증 서버와 약속한 공유된 킷값으로, 외부에 노출되지 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
	$counter_{BSIM}$	스마트 미터기의 $BSIM$이 유지하는 $counter$ 값
	C	$counter_{AuC}$를 암호화한 값
	C'	$BSIM$이 인증서버에 보내는 $counter$ 재동기 요청 메시지. $counter_{BSIM}$을 암호화한 값.
	$HNonce$	인증 서버에서 생성하는 난수
	$MAC-N$	인증 서버에서 계산되며 $BSIM$이 AMI 네트워크를 인증하는 데 사용
	$MAC-M$	$BSIM$이 $MAC-N$을 확인하기 위해 계산하는 값
	$XRES$	인증 서버에서 계산되며 DCU가 $BSIM$을 인증하는 데 사용
	RES	BSIM이 AMI Headend에서 인증받기 위해 $BSIM$에서 DCU로 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

위의 <표 5>는 다음 (그림 4, 5)의 구성요소와 약어를 정의한 것이다. (그림 4)는 NAN의 영역에서의 인증과 키 일치 과정이다. 프로토콜에 사용된 KDF(Key Derivation Function) 함수는 AKA과정에서 사용되는 임시키 (TK)와 세션키 (SK)를 생성할 때 사용된다[8].



(그림 4) NAN의 AKA 프로토콜

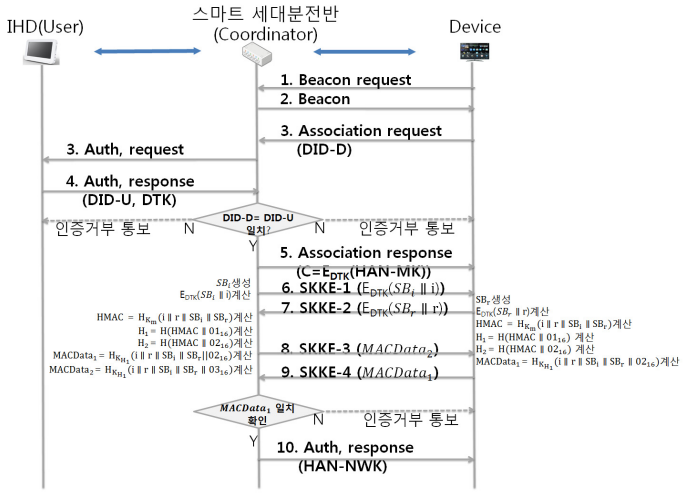
다음의 (그림 5)는 NAN영역의 인증과 키 일치 및 교체 프로토콜을 묘사한 것이다.



(그림 5) NAN에서의 키 일치 및 교체 과정

4.2 HAN의 AKA 프로토콜

ZigBee.는 새롭게 가입하는 디바이스에게 마스터키를 전송하는 과정에서 안전하지 않은 채널을 통해 전달되어 직접적으로 노출이 되는 위험이 존재한다.



(그림 6) HAN에서의 키 일치 및 교체 과정

제시된 (그림 6)의 프로토콜은 사용자가 직접 IHD를 사용하여 새롭게 가입하는 디바이스 정보와 키를 입력하여 입력 정보로 마스터키를 안전하게 전송할 수 있다. <표 6>은 HAN의 구성요소와 프로토콜의 주요 약어이다.

<표 6> HAN 구성요소와 프로토콜 주요 약어

	용어	설명
AMI 구성요소	*IHD*	In-Home Display. 댁내 전력정보표시장치
	Coordinator	ZigBee Coordinator. 댁내 네트워크를 관리 하는 스마트 세대분전반
	Device	ZigBee 종단기기. 댁내 네트워크에 속하는 가전기기 등의 단말장치
parameters	$DID-D$	Device에 부여된 영구 Device정보 (Device ID). Device에서 Coordinator에게 보내는 Device의 정보
	$DID-U$	사용자에 의해 입력되어지는 Device의 정보
	DTK	Device에 고정된 임시 키. HAN-MK를 안전하게 보내는데 사용
	$HAN-MK$	HAN에서 사용될 링크키를 생성할 마스터키
	$HAN-NWK$	HAN에서 사용되는 네트워크키
	SB_i	스마트 세대분전반에서 생성하는 난수
	SB_r	Device에서 생성하는 난수
	HMAC	링크키와 링크키 확인키를 만드는 데 사용
	H_1	Device와 Coordinator의 통신에 사용될 링크키
	H_2	링크키 확인키
표기법	$H(M)$	M의 해시 출력 값
	$H_K(M)$	키 K로 계산된 메시지 M의 해시 출력 값
	$E_K(M)$	키 K로 암호화된 메시지

5. BSIM기반 AMI 네트워크 망의 보안위협 해결 사항

국내의 WAN은 이미 통신망 확보가 손쉬운 상태로 본 망에서는 통신망 확보가 어려운 NAN과 HAN의 영역의 설계에 중점을 두었다. 본 망을 통해 해결할 수 있는 보안 요구사항은 다음과 같다.

5.1 AMI 통신 기술 요구사항 개선점

ZigBee의 노드간의 마스터키 전달이 노출될 수 있는 문제를 디바이스 출하 시 임시로 저장되어 있던 *DTK*를 사용하여 마스터키의 전달 노드의 안전성을 확보함으로써 인증 전 데이터에 대한 기밀성을 확보할 수 있다. 마스터키와 네트워크 키가 고정되어 있는 문제는 NAN에서 사용되는 BSIM의 도움으로 서버가 갱신을 유도하여 HAN에서의 마스터키와 네트워크 키의 주기적인 갱신을 유도할 수 있다.

5.2 AMI 네트워크 요구사항 개선점

NAN의 영역에서 BSIM 기반의 Binary CDMA의 AES- CCM, ARIA-CCM으로, HAN의 영역에서는 AES -CCM* 운영으로 기밀성과 무결성을 확보하고 사용자 인증을 할 수 있다.

무결성, 기밀성은 암호화를 하는 키의 안전을 통해 확보되는데 BSIM 기반의 대칭키 방식의 키 관리를 통해 해결할하였다. BSIM이 장착되어 있는 스마트 미터기가 사용자와 관리자를 연결하는 수단이 되며 이를 통해 상대적으로 보안이 취약한 사용자 영역의 HAN내의 키를 주기적으로 갱신하여 소비자의 보안을 확보할 수 있다.

디바이스의 인증은 NAN의 BSIM의 사용으로 사용자 인증 및 네트워크 인증이 가능하며 비인가 기기 접근 차단이 가능하다. HAN에서는 IHD에 디바이스 정보를 입력하여 인증문제를 해결하고, IHD를 통한 실시간 감시를 통해 비인가 기기 접근을 차단할 수 있다. 이런 과정을 통해 디바이스 인증뿐만 아니라 가용성, 식별, 인증, 인가, 검침 정보의 부인방지, 변종 탐지 서비스를 제공할 수 있다.

6. 결론 및 차후 연구과제

본 논문에서는 BSIM을 기반으로 Binary CDMA와 ZigBee를 적용하여 안전한 AMI 시스템을 구축하고 통합적인 보안 관리를 할 수 있는 전제조건인 AMI 네트워크 망의 구성과 인증 및 키 일치 등의 보안 프로토콜을 제시하였다. 무선 통신만으로는 효율적이지 못한 지역에 AMI 시스템을 구축하기에 한계가 있으므로 PLC통신의 명확하고 체계적인 보안 표준 확보를 통해 AMI 시스템의 유선망을 확보하는 연구가 진행되어야 한다.

참고문헌

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

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

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

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

[5] IEEE 802.15.4, "ZigBee Specification (Document 053474r17)",ZigBee Standard Organization,2007

[6] Document 075356r15, "ZigBee Smart Energy Profile Specification", ZigBee Alliance, 2008.10

[7] UCA International Users Group, "SECURITY PROFILE FOR ADVANCED METERING INFRA--STRUCTURE version 2.0",The Advanced Security Acceleration Project (ASAP-SG), 2010.06

[8] 강주성 외,“키 유도함수의 통계적 난수성 평가 방법”, 한국정보보호학회, 정보처리학회논문지 제 17권 제 1호, 2010.02, p.47-60

[9] 전력 기술인 교육 협력팀, “한국형 스마트 그리드”, 한국 전력기술인 협회 학술논문, 2010.07, p.26-31

[10]전재우, 임선희, 이옥연 “스마트 그리드를 위한 Binary CDMA 기반의 AMI 무선 네트워크 구조 및 AKA 프로토콜” 정보보호학회논문지 제20권 제5호, 2010.10, p.111-125