논문 21-46-06-13 The Journal of Korean Institute of Communications and Information Sciences '21-06 Vol.46 No.06
https://doi.org/10.7840/kics.2021.46.6.1040

AMI 보안 적용에 따른 원격검침 성능분석

명 노 길◆, 은 창 수°

Remote Meter Reading Performance Analysis According to Applying AMI Security

No-Gil Myoung◆, Chung-Soo Eun°

요 약

AMI는 원격검침이 주목적인 AMR에 가까웠으나 BTM 및 분산전원 연계와 같은 신규서비스 수용과 개인정보 보호를 위해 사회적으로 요구하고 있는 사이버 보안이 강화된 AMI 2.0으로 진화하고 있다. 특히 AMI 보안 적용에 따라 추가로 생성되는 트래픽이 원격검침에 미치는 영향을 분석하고자 보호 방식별 DLMS 패킷 오버헤드 크기를 분석하고, 현장의 AMI 통신환경을 고려하여 원격검침 모의시험을 시행하였다. 모의시험 결과 DCU가 15분 동안 원격검침 해야 하는 지능형 전력량계를 200대에서 50대 수준으로 재설정해야 한다는 결론을 얻었다.

Key Words : AMI, DLMS, AMI security, smart meter, remote meter-reading

ABSTRACT

Current AMI is close to AMR but it is developing into AMI 2.0, which expands for accommodating new services such as BTM and DER connection, and strengthens cyber security which is socially required for protection of personal information. In particular, to analyze the effect of additionally generated traffic on remote meter reading by applying AMI security, we analyzed the size of DLMS packet overhead for each protection method, and conducted a remote meter reading simulation considering the AMI communication field environment. As a result of the simulation, it is concluded that the maximum number of smart meters that the DCU remotely reads should be reset from 200 to 50.

Ⅰ. 서 론

최근 전력 분야에서의 4차 산업혁명은 지능형 전력망 구축이며, 지능형 전력망의 핵심인프라는 단연코 AMI(Advanced Metering Infrastructure)를 손꼽고 있다. 이에 따라 주요 전력회사는 원격검침, 체계화된 정전 및 수요관리를 통한 피크 전력을 낮춰 설비투자 비용을 최소화할 수 있는 AMI를 적극적으로 구축하고 있다[1-3]. 전 세계적으로 태양광 및 풍력과 같은 간헐성과 변동성이 큰 신재생에너지 확대 정책으로 발생할 수 있는 전력 시스템의 신뢰도 저하 문제를 극복하고 궁극적으로는 신재생 에너지원의 수용력을 확대할 수 있는 핵심인프라로 AMI를 주목하고 있다[4,5].

국내의 경우 2024년까지 1.7조 원을 투자하여 2,250만 호 저압 고객을 대상으로 AMI를 구축하고 있다[6,19]. 2020년 연말 기준으로 1,020만 호 규모의 AMI를 구축하여 운영하고 있으나, 구축된 AMI는 원격검침이 주목적인 AMR(Automatic Meter Reading)

※ 본 연구의 일부는 충남대학교 학술연구비에 의해 지원되었습니다.
◆ First Author : Convergence Laboratory, Korea Electric Power Research Institute, ng-myoung@kepco.co.kr, 정회원
° Corresponding Author : Department of Radio and Information Communications Engineering, Chungnam National University, eun@cnu.ac.kr, 종신회원
논문번호 : 202101-004-C-RN, Received January 3, 2021; Revised March 20, 2021; Accepted March 25, 2021

에 가깝다. 따라서, BTM(Behind The Meter), 정전관리, 분산전원 연계 등과 같은 신규서비스를 수용할 수 있는 서비스 플랫폼으로의 확장과 사이버 보안이 강화된 AMI 2.0 버전으로 진화하고 있다[7]. AMI 2.0에서의 보안성 강화는 “지능형 전력망 정보 보호조치에 관한 지침(이하 지침)”을 준수하여 사회적으로 요구하고 있는 개인정보를 보호하고, 통신 네트워크로 연결된 지능형 전력량계를 해킹하여 발생할 수 있는 원격부하 차단 및 과금 정보의 위·변조와 같은 사이버 공격에 대응하기 위해서이다[8,20].

AMI는 구축사업 초창기부터 IEC 국제표준인 DLMS(Device Language Message Specification) 프로토콜을 원격검침 프로토콜로 채택하여 사용하고 있다[1]. 따라서 AMI 보안 요구사항을 충족시키는 구체적인 방법 또한 DLMS 프로토콜 기능과 범위 안에서 수행되어야 한다. 특히 DLMS 보안을 적용함에 따라 발생하는 추가 트랜잭션과 패킷 오버헤드가 원격검침 성능에 얼마나 영향을 미치는지에 관한 분석이 필요하다. 이러한 분석은 DCU(Data Concentrator Unit)와 지능형 전력량계 구간인 SUN(Smart Utility Network) 통신 네트워크 구축방안과 DCU가 최대로 검침 가능한 지능형 전력량계의 대수를 이론적으로 산정할 수 있게 하여 AMI 사업을 추진하는 정책 결정자와 현장 설치 작업자에게 유용한 정보를 제공할 것이다.

본 논문은 서론에 이어 Ⅱ장에서는 정부 지침의 보안 요구사항 분석과 AMI 보안 정책을 설명 후 이를 구현하기 위한 DLMS 보호 방식별 APDU (Application Protocol Data Unit) 패킷 구조와 오버헤드 크기를 설명한다. Ⅲ장에서는 DCU가 주기적으로 수집하고 있는 원격검침 항목을 대상으로 DLMS 보호 방식별 HDLC(High-level Data Link Control) 프레임 크기를 계산하고 이를 이용한 원격검침 모의시험과 그 결과를 분석한다. 마지막 Ⅳ장에서는 결론과 향후 과제를 제시한다.

Ⅱ. AMI 보안 요구사항 분석 및 적용방안

2.1 AMI 보안 요구사항

지능형 전력망 정보의 신뢰성과 안정성을 확보하기 위해 지능형 전력망 사업자가 준수해야 할 보호조치의 세부적인 기준을 제시하고자, 지식경제부 고시로 “지능형 전력망 정보의 보호조치에 관한 지침(2012.6.20.)”이 제정되었다[9]. AMI는 지능형 전력망에 포함되는 하위 시스템이므로 이를 반드시 준수해야 한다. 정부 지침에는 지능형 전력망 정보에 대한 기술적/물리적/관리적 보호조치가 제시되었는데, AMI 장치와 시스템 관점의 요구사항을 표 1에 요약 정리하였다[9].

IT보안인증사무국의 검정필 암호 모듈 사용은 KCMVP(Korea Cryptographic Module Validation Program) 검증을 획득한 암호 모듈 사용을 의미한다. 가장 많이 사용하는 대칭 키 암호 알고리즘인 AES(Advanced Encryption Standard)는 KCMVP 검증대상 알고리즘이 아니므로, 국내표준인 SEED 또는 ARIA(Academy, Research Institute, Agency)만 사용해야 하는 제약사항을 내포하고 있다. 안전한 암호키 생성 및 주기적인 갱신과 더불어 만료 시 공격자가 암호키를 획득하여 재사용할 수 없도록 파기 의무가 있으며, 보안 강도를 고려하여 128 비트 이상의 키 길이 사용을 요구한다. 시스템 또는 기기 간 통신을 수행하기 위해서는 반드시 사전에 상호인증을 수행해야 한다. 지능형 전력망 사업자의 기기는 위·변조, 도·감청 방지기능과 과금과 직접적으로 관련이 있는 월 전력사용량과 같은 중요 검침 정보에 대해서는 무결성을 제공해야 한다. 마지막으로 기기는 서비스 제공에 필요한 최소 정보를 필요기간만 저장해야 하며, 중요 정보에 대해서는 암호화 저장을 수행해야 한다.

표 1. 장치와 시스템 관점의 주요 보안 요구사항
Table 1. Security requirements in the view of devices/systems.

Items	Requirements	Remark
Crypto module	· Using a KCMVP module · Use more than 128 bits	Article 10
key management	· Periodic updates · Destroy after expiration	Article 11
Mutual authentication	· Communicate with authenticated parties	Article 12
Device communication security	· Prevention of forgery/ eavesdropping · Data integrity	Article 13
Device data security	· Storage for required period · Encrypted storage	Article 14

2.2 AMI 2.0 보안 기능

DLMS 표준에서는 보안 강도와 세부 지원기능에 따라 다양한 security suite를 정의했다[11]. 2.1절에서 분석한 AMI 요구사항을 종합적으로 고려하면, “ECDH-ECDSA-AES-GCM-128-SHA-256”의 security suite ID 1번이 가장 적합하다. 그러나 정부 지침에 명시된 KCMVP 검증필 암호 모듈 사용 의무

때문에 AES 알고리즘을 사용하는 security suite ID 1번을 사용할 수 없다. 따라서 AMI 2.0에서는 AES 알고리즘 대신 ARIA 알고리즘을 사용하는 "ECDH-ECDSA-ARIA-GCM-128-SHA-256"을 security suite ID 8번인 제조사 규격으로 정의하였다. 정의한 security suite ID 8번은 key wrapping과 APDU 압축방식은 사용하지 않는다. 표 2에 security suite ID 1번과 8번의 기능을 비교하여 명시하였다.

표 3은 AMI 1.0과 2.0 버전의 보안 기능과 수준을 보여준다. AMI 1.0 버전에서는 AA(Application Association) 체결 시 사전 공유 키 방식을 사용하는 LLS(Low Level Security) 기반의 상호인증 방식을 사용한다. 패킷 암호화와 무결성 기능을 사용하지 않기 때문에 비밀키 생성을 위한 키 합의와 전자서명을 사용하지 않는다[15]. 그러나 AMI 2.0 버전에서는 AA 체결 시 인증서를 이용하는 HLS(High Level Security) ECDSA(Elliptic Curve Digital Signature Algorithm) 방식을 사용한다. 비밀키를 생성하기 위해서 사용하는 키 합의 알고리즘은 DLMS client 및 server 각각 키 쌍 생성기능이 필요한 ephemeral unified model(2e, 0s, ECC CDH)을 사용한다[11]. ECC CDH 알고리즘을 이용하여 shared secret을 우선 생성하고, 사전에 합의된 HMAC(Hash Message Authentication Code) 기반의 KDF(Key Derivation Function) 알고리즘과 부가정보를 사용하여 비밀키를 생성한다[11]. 생성한 32 바이트의 비밀키는 상위 16 바이트는 인증키로, 하위 16 바이트는 암호키로 사용하여, 모든 DLMS 패킷에 대해서 인증암호 방식을 적용한다.

표 2. DLMS 보안 세트 비교
Table 2. Comparison DLMS security suites.

ID	Name	AE	DS	KA	Hash	KW	C	R
1	ECDH-ECDSA-AES-GCM-128-SHA-256	AES-GCM-128	ECDSA (P256)	ECDH (P256)	SHA-256	AES-128 key wrap	V.44	DLMS std
8	ECDH-ECDSA-ARIA-GCM-128-SHA-256	ARIA-GCM-128	ECDSA (P256)	ECDH (P256)	SHA-256	-	-	AMI 2.0

AE(Authenticated Encryption), DS(Digital Signature), KA(Key Agreement), KW(Key Wrapping), C(Compression), R(Remark)

표 3. AMI 버전에 따른 보안 기능 비교
Table 3. Comparison of AMI security features according to AMI version.

Classification (year)	MA (Packet size)	KA	Encryption	DS
AMI 1.0 (~2021)	LLS (213 bytes)	-	-	-
AMI 2.0 (2022~)	HLS ECDSA (1,271 bytes)	Ephemeral unified model (2e, 0s, ECC CDH)	SSGC	GS

MA(Mutual Authentication), SSGC(Service-specific global ciphering), DS(Digital Signature), GS(General signing)

AMI 2.0은 다양한 DLMS APDU 암호 방식 중에서 DLMS server-client 간에만 적용할 수 있고, 패킷 오버헤드가 상대적으로 적은 SSGC(Service-specific Global Ciphering) APDU 방식을 사용한다. 월 전력 사용량 또는 LP(Load Profile)와 같이 과금과 직접 관련된 중요 정보는 무결성 확보를 위해서 GS(General Signing) APDU 방식을 사용한다.

2.3 DLMS 보안 APDU 오버헤드 크기 분석

DLMS 표준에서 제공하는 보안 적용으로 발생하는 APDU 패킷 오버헤드는 AA 수행 과정, 키 합의 과정, ciphering APDU 및 signing APDU를 생성할 때 발생한다. 키 합의 과정은 한 달에 한 번 수행하는 것을 가정하여 패킷 오버헤드 크기 계산은 AA 수행과 ciphering 및 signing APDU 생성으로만 국한하였다. 8 바이트 크기의 사전공유 비밀키를 사용하는 LLS 기반의 AA 수행 시 총 213 바이트를 사용한다[14]. 338 바이트 크기를 갖는 X.509 기반의 인증서와 각각 32 바이트 크기의 CtoS/StoC를 사용하는 HLS ECDSA 기반의 AA 수행 시 총 1,271 바이트를 사용하기 때문에 LLS 방식보다 5.97배 많은 패킷을 사용한다[14]. 상기 AA 수행 시 선택사항인 세부 패킷 구성 항목과 관련 파라미터의 크기 설정에 따라서 총 패킷 크기는 가변 될 수 있다.

Ciphering과 signing을 적용할 때 발생하는 패킷 오버헤드 크기를 분석하기 위해서 그림 1, 그림 2 및 그림 3에 각각 평문을 전송하는 xDLMS APDU, ciphering만 지원하는 SSGC APDU 및 signing만 지원하는 GS APDU의 패킷 구조를 도시하였다. 평문인 xDLMS APDU와 비교하여, SSGC APDU와 GS APDU는 각각 23(1+1+1+8+12) 바이트와 101(1+8+8+8+12+64) 바이트의 오버헤드가 추가로 발생

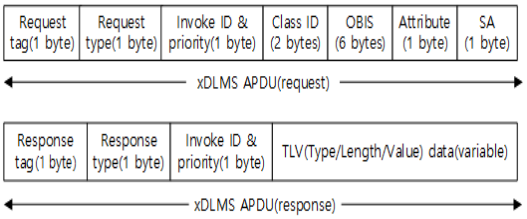

그림 1. xDLMS APDU 필드(보호 방식 적용 없음)
Fig. 1. xDLMS APDU fields(No protection)

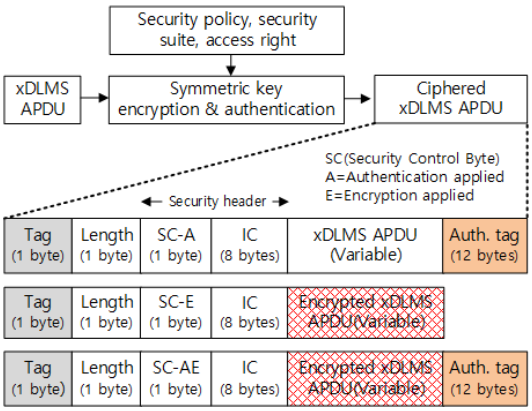

그림 2. SSGC APDU 필드 및 크기
Fig. 2. SSGC(Service-specific Global Ciphering) APDU field and size

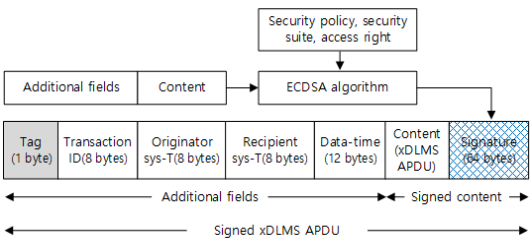

그림 3. GS(General Signing) APDU 필드 및 크기
Fig. 3. GS(General Signing) APDU field and size

함을 확인할 수 있다. 다중 보호(Multi-protection) 방식을 사용하면 ciphering과 signing을 동시에 적용할 수 있으며 전체 오버헤드는 각 오버헤드 크기의 합인 124(23+101) 바이트 크기만큼 증가한다.

Ⅲ. 모의환경 구성 및 검침 성능분석

3.1 DCU 검침 항목 및 주기

SUN 통신 네트워크 방식으로는 best-effort 통신방식인 고속 PLC(Power Line Communication) 또는 WiSUN 방식을 선호한다[7,13]. DCU와 AMI HE(Head End) 구간의 백홀 통신 네트워크는 신뢰성이 우수한 광통신 방식을 사용한다. 따라서 검침 등의 응용서비스 관점에서 보면, SUN 통신 네트워크 구간에서 발생하는 트래픽 병목 현상이 AMI 전체 서비스 성능을 좌우하기 때문에 상기 SUN 통신 네트워크 구간으로만 한정하여 모의시험을 시행한다.

표 4와 같이 DCU는 15분마다 주기적으로 현재시간, 전력량계 제조사 ID, 전력량계 고객 ID, LP, 평균 전압/전류 이력, 순시 전압/전류 이력 항목을 원격 검침한다. 또한, 하루에 한 번씩 월 사용전력량, 최대 수요전력 및 정전/복전 이력 항목을 원격 검침한다[15]. 향후 분산전원 및 수요관리 서비스를 위해서 검침 주기는 10분 및 5분 등으로 단축될 가능성이 크다. 항목별 데이터 크기는 단위를 포함하지 않는 값이며, DLMS 프로토콜에서 사용하고 있는 데이터형의 크기를 의미한다.

표 4. 검침 항목, 주기 및 크기
Table 4. Remote meter-reading items, period and data size.

Period	Reading items	Total size(bytes)
15 minutes	Date-time	12
	Manufacture ID	13
	Customer ID	13
	LP entry	13
	LP(Last 4 entry)	47×4=187
	AVCP entry	13
	AVCP(Last 4 entry)	36×4=144
	IVCP entry	13
	IVCP(Last 4 entry)	72×4=288
24 hours	Monthly energy usage	20
	Maximum demand power	40
	Outage/restoration profile (each 10 EA)	28×10=280

AVCP(Average Voltage Current Profile),
IVCP(Instantaneous Voltage Current Profile)

3.2 HDLC 프레임 오버헤드 크기 계산

국내 AMI는 다양한 DLMS 통신 프로파일 중에서 범용성이 우수한 HDLC 통신 프로파일을 사용하고 있다[15]. 그림 4는 DLMS에서 채택한 HDLC 프레임 포맷 3의 구조를 보여준다[17]. 프레임의 시작과 종료는 각각 1 바이트 크기를 갖는 식별자 “7E”를 사용한다. 프레임의 세부 구성은 FF(Frame Format), DA(Destination Address), SA(Source Address),

Control, HCS(Header Check Sequence), I(information), FCS(Frame Check Sequence) 필드로 구성된다.

그림 2와 3에 명시한 보호 방식을 적용할 경우 ciphered xDLMS APDU 및 signed xDLMS APDU는 그림 4의 HDLC의 I 필드를 구성하는 xDLMS APDU와 대체된다. E6E600 및 E7E700은 LLC(Logical Link Control)의 헤더 역할을 하며, 송·수신에 따라 구분된다. HDLC 프레임 크기는 ciphered xDLMS APDU 및 signed xDLMS APDU의 크기보다 항상 15(1+2+2+1+1+2+3+2+1) 바이트가 크다. 표 5는 평문을 사용하는 xDLMS APDU를 기준으로 보호 방식별 APDU의 오버헤드 크기 증가와 HDLC 프레임 크기와의 관계를 수식적으로 표현하였다. SSGC+GS APDU 방식은 SSGC APDU와 GS APDU의 보호 방식을 중복하여 적용한 경우를 의미한다.

그림 1~3에서 명시한 필드 구성과 표 5에 정리한 계산방식을 이용하여 표 6에 DCU의 검침 항목에 대하여 Tx/Rx 별 HDLC 프레임 크기를 계산하여 정리하였다. 평문 프레임의 크기는 그림 4에 명시한 xDLMS APDU를 포함하는 HDLC 프레임의 크기를 의미한다. SSGC APDU, GS APDU 및 SSGC+GS APDU의 프레임 크기는 각각 그림 2와 3에 명시한 인증암호, 전자서명, 인증암호/전자서명을 적용한 보호

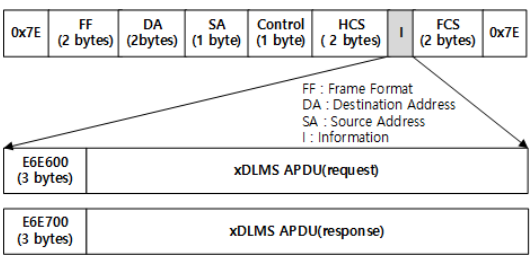

그림 4. HDLC 프레임 구조
Fig. 4. HDLC frame structure

표 5. 보호 방식 적용에 따른 오버헤드 크기(평문 기준)
Table 5. Overhead size analyses according to protections (Referring Plain text).

Protections	APDU(Bytes) size	HDLC frame(Bytes) size
SSGC APDU	(xDLMS APDU)+23	(xDLMS APDU+23)+15
GS APDU	(xDLMS APDU)+101	(xDLMS APDU+101)+15
SSGC+GS APDU	(xDLMS APDU)+124	(xDLMS APDU+124)+15

표 6. 보호 방식별 DCU가 수집하는 검침 항목의 패킷 크기 (HDLC 프레임 기준)
Table 6. Packet sizes of DCU meter-reading item according to protections(HDLC frame size).

Num	Classification (size, bytes)		Plain text APDU	SSGC APDU	GS APDU	SSGC +GS APDU	Reading period (s)
1	Date-time	Tx	28	51	129	152	900
		Rx	33	56	134	157	
2	Manufacture ID	Tx	28	51	129	152	
		Rx	28	51	129	152	
3	Customer ID	Tx	28	51	129	152	
		Rx	28	51	129	152	
4	LP entry	Tx	28	51	129	152	
		Rx	24	47	125	148	
5	LP (Last 4 entry)	Tx	47	70	148	171	
		Rx	275	298	376	399	
6	AVCP entry	Tx	28	51	129	152	
		Rx	24	47	125	148	
7	AVCP (Last 4 entry)	Tx	47	70	148	171	
		Rx	261	284	362	385	
8	IVCP entry	Tx	28	51	129	152	
		Rx	24	47	125	148	
9	IVCP (Last 4 entry)	Tx	47	70	148	171	
		Rx	367	390	468	491	
10	Monthly energy usage	Tx	28	51	129	152	86,400
		Rx	148	171	249	272	
11	Maximum demand power	Tx	28	51	129	152	
		Rx	503	526	604	627	
12	Outage profile (10 EA)	Tx	28	51	129	152	
		Rx	249	272	350	373	
13	Restoration profile(10 EA)	Tx	28	51	129	152	
		Rx	249	271	350	373	
	Total		2,634	3,231	5,260	5,858	

방식별 APDU을 포함하는 HDLC 프레임의 크기를 의미한다.

3.3 원격검침 모의환경 구성

보안 적용에 따른 AMI의 원격검침 성능을 분석하기 위해서 Contiki OS에서 제공하는 cooja 시뮬레이터를 사용하였다. Contiki OS는 WSN(Wireless Sensor Network) 및 IoT(Internet of Things) 분야에서 많이 사용하는 에너지 효율적 초소형 임베디드 OS로 다양한 인터넷 표준 네트워크 스택과 RF 모델링을 지원한다[18]. Cooja에서 제공하는 다양한 wireless

radio model 중에서 MRM(Multi-path Ray-tracer Medium)을 사용했다. PL(Path Loss) 모델에 따른 AMI 검침 성능을 분석하는 목적이 아니므로, 모의시험에서 구성한 WiSUN 네트워크는 외부의 주파수 간섭이 없고 전송오류 없이 정상 동작한다고 가정하였다. WiSUN MAC은 CSMA/CA(Carrier Sense Multiple Access /Collision Avoidance) 방식으로 동작하지만, DCU에서 동작하는 DLMS client는 N개의 (N은 최대 200개) 지능형 전력량계를 대상으로 순차적인 polling 방식으로 검침을 수행하기 때문에 실효적으로는 스케줄링 방식으로 동작한다.

그림 5는 모의시험을 시행하기 위해 구성한 통신 스택을 보여준다. DCU와 WiSUN 모뎀 구간은 스타 구조의 단일 홉 방식으로 구성하였다. DCU와 WiSUN 모뎀 구간은 UDP/IP 통신을 수행하며, WiSUN 모뎀과 지능형 전력량계 구간은 RS-485 시리얼 통신을 사용한다. 다세대 주택과 같은 집합 고객의 경우 한 대의 WiSUN 모뎀은 RS-485의 멀티 드랍 방식을 이용하여 최대 30개의 지능형 전력량계와 통신한다. HDLC 패킷이 하위 계층으로 전송됨에 따라 캡슐화에 필요한 추가적인 UDP/IP/MAC/PHY 헤더 크기를 그림 5에 명시하였으며 모의시험에서 활용하였다.

WiSUN 모뎀은 수신한 UDP/IP 패킷을 역 캡슐화하여 HDLC 프레임의 목적지 주소를 확인 후 해당 지능형 전력량계로 전송한다. DLMS server 역할을 하는 지능형 전력량계는 수신한 HDLC 프레임의 I 필드에 있는 xDLMS APDU를 해석하고 이에 대한 응답 xDLMS APDU를 생성 후 HDLC의 I 필드에 삽입 후 역전송하는 과정으로 동작한다. 표 7은 모의시험에 사용한 파라미터의 값을 보여준다. WiSUN 모뎀은 2-FSK로 동작하여 50kbps의 전송속도를 제공한다[13]. WiSUN 모뎀과 지능형 전력량계 구간의 RS-485 전송속도는 지능형 전력량계의 기본 설정값인 9.6kbps를 적용하였다[16].

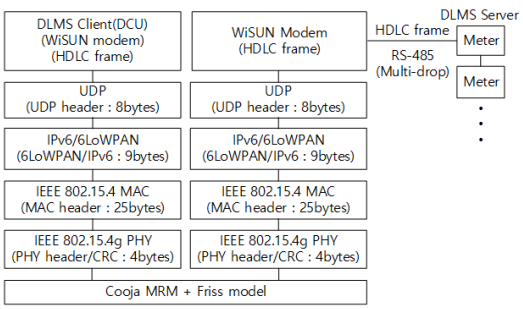

그림 5. 모의실험을 위한 통신 스택 구조 및 헤더 크기
Fig. 5. Communication stacks and header sizes for simulation

표 7. 모의시험 파라미터 설정값
Table 7. Parameter values for simulation.

Parameter	Value	Remark
Frequency(MHz)	917	IoT/AMI services
Channel bandwidth(KHz)	25	Semtech IC
WiSUN data rate(Kbps)	50	Semtech IC
RS-485 data rate(Kbps)	9.6kbps	Meter default
MAC algorithm	CSMA/CA	IEEE 802.15.4
The maximum number of meters per a DCU	200	KEPCO AMI requirement
WiSUN modems(EA)	20	10 meters per one WiSUN modem
Meter reading items	9 or 13	Table 6

3.4 원격검침 성능분석

그림 6은 표 6에서 명시한 모든 항목에 대해서 지능형 전력량계의 개수를 200개까지 변경하면서 보호 방식별 원격검침 소요 시간을 보여준다. “LLS+plain text” 방식은 현장에서 사용하고 있는 방식으로 원격검침에 562초가 소요되었다. AA 체결 시 인증서를 사용하고 모든 패킷에 대해서 인증암호를 적용한 “HLS ECDSA+SSGC” 방식은 원격검침에 989초가 소요되어 요구사항인 15분 검침이 불가능함을 확인하였다. 보안 패킷 오버헤드가 더 큰 “HLS ECDSA+GS”

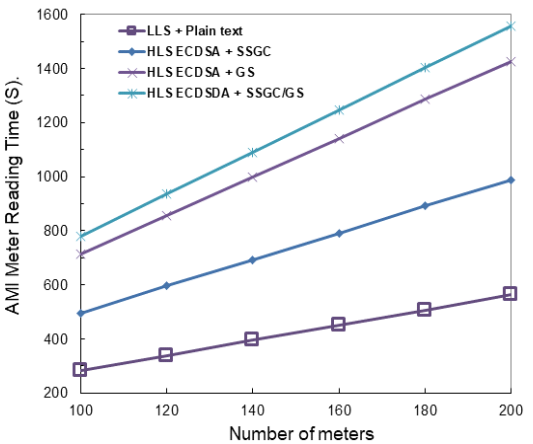

그림 6. 보호 방식별 보안 적용에 따른 200대 지능형 전력량계 원격검침 소요 시간 비교(표 6의 13개 검침 항목 대상)
Fig. 6. Comparisons of meter reading time for 200 smart meters according to protections(13 meter reading items in table 6)

및 "HLS ECDSA+SSGC/GS 방식은 원격검침에 각각 1,427초 및 1,558초가 소요되었다.

모의시험에서는 암호 모듈에서 필요한 암·복호화, 전자서명 생성 및 검증 등의 연산 시간은 제외하였다. 그러나 USIM 기반의 암호 모듈과 같이 외장형태로 연동되는 경우 전자서명 생성 및 검증과 저속 통신에 따른 패킷 지연시간을 고려하면 최소 수백ms 이상의 동작 시간이 필요하므로 이에 대한 추가적인 고려가 필요하다. 보호 방식별 원격검침 모의시험 결과와 현장에서 발생할 수 있는 통신오류 및 이를 고려한 재검침 횟수와 암호 모듈의 연산 소요 시간 등을 종합적으로 고려하면 DCU가 수용할 수 있는 지능형 전력량계 대수를 200대에서 50대 수준으로 변경하는 정책이 필요하다고 판단된다. 특히 향후 검침 주기가 15분에서 10분 및 5분 등으로 단축되면 DCU가 수용할 수 있는 지능형 전력량계의 개수는 더욱더 줄어들 수밖에 없다.

따라서, 현장에서는 이러한 신규보안 기능과 검침 주기 단축 등을 고려하여 신뢰성 있는 통신방식 선정과 최적의 SUN 통신 네트워크 구축이 필요하다. 추가적인 연구내용으로는 주파수 간섭에 의한 WiSUN 통신 장애와 이에 따른 재검침 영향, 암호 모듈 연산 시간 반영과 polling과 대비되는 event-notification 방식의 원격검침의 장단점을 분석하고 상호 간의 성능을 비교 및 분석할 계획이다.

Ⅳ. 결 론

AMI는 단순 원격검침뿐만 아니라 다양한 서비스 수용을 위한 플랫폼으로의 확장과 사회적으로 요구하고 있는 사이버 보안을 강화한 AMI 2.0 버전으로 진화하고 있다. 특히 AMI가 국가 단위로 구축됨에 따라 통신 네트워크로 연결된 2,250만 개의 지능형 전력량계는 사이버 공격에 대한 취약성이 대두되어, AMI에 대한 선제적 보안 정책 수립과 기술적 대책을 마련하고 있다.

본 논문에서는 정부의 지능형 전력망 보안 지침 요구사항을 분석 후 AMI 보안 정책과 이를 구현하기 위한 세부내용을 DLMS 프로토콜의 보안 기능을 이용하여 설명하였다. 신규보안 적용에 따른 오버헤드 크기를 보호 방식별로 분석하고, 분석한 오버헤드 크기에 따른 원격검침 소요 시간을 확인하고자 DCU가 현장에서 수집하는 계량 항목을 대상으로 원격검침 모의시험을 시행하였다.

모의시험 결과 신규보안 적용에 따른 프로토콜 오버헤드와 현장의 통신환경을 고려하면 DCU가 수용할 수 있는 지능형 전력량계 대수를 현재 기준인 200대에서 50대 수준으로 변경하는 것이 필요하다고 판단된다. 본 논문의 결과가 AMI 사업을 추진하는 정책결정자와 현장에서 AMI를 구축하는 현장 작업자에게 DCU의 원격검침 용량 산정과 SUN 통신 네트워크 구축 시 유용한 정보가 될 수 있을 것이다.

References

[1] N. G. Myoung, Y. H. Kim, and S. Y. Lee, "A study on AMI system of KEPCO," *J. KICS*, vol. 35, no. 8, pp. 1251-1258, 2010.

[2] N. Matanov and A. Zahov, "Remote electricity metering system" in *Proc. IEEE Electrical Eng. Faculty Conf.*, 2019.

[3] H. Sui, et al., "An AMI system for the deregulated electricity markets," *IEEE Trans. Industry Appl.*, vol. 45, no. 6, pp. 2104-2018, Nov. 2009.

[4] H. Padull, et al., "*Considerations for AMI based Operation for Distribution Feeders*," Retrieved Aug., 30, 2020, from http://www.nrel.gov/docs/fy19osti/72773.pdf.

[5] R. R. Mohassel, et al., "A survey on advanced metering infrastructure," *JEPE*, vol. 63, pp. 473-484, 2014.

[6] Y. I. Kim, et al., "Development of AMI NMS using SNMP for network monitoring of meter reading devices," *KEPCO J. Electric Power and Energy*, vol. 2, no. 2, pp. 259-268, Jun. 2010.

[7] B. Y. Park, "*AMI 2.0 and Emerging IoT PLC Technology*," Retrieved Mar. 14, 2021, from https://www.itfind.or.kr/publication/regular/weeklytrend/weekly/list.do?selectedId=1099

[8] S. K. Kim, et al., "A study on AMI security vulnerability," *KIISC*, vol. 22, no. 5, pp. 73-78, Aug. 2012.

[9] MOTIE, "*Guidance on Smart Grid Information Protections*," Retrieved Aug., 25, 2020, from http://www.motie.go.kr.

[10] D. D. Vyas and H. N. Pandya, "Advanced metering infrastructure," *IJERT*, vol. 1, no. 10, pp. 1-5, Dec. 2012.

[11] DLMS User Association, *Green Book* (Technical Report) Ed. 9.
[12] DLMS User Association, *Blue Book*(Technical Report) Ed. 13.
[13] B. Y. Park, "*Wi-SUN Protocol and Usage Trends*," Retrieved Mar. 14, 2021, from https://www.itfind.or.kr/WZIN/jugidong/1864/file47785453494121234 28-186402.pdf
[14] N. G. Myoung, B. S, Park, and C. S. Eun, "Development of secure SW update technology for smart meters," *J. KICS*, vol. 42, no. 12, pp. 2326-2339, 2017.
[15] KEPCO, "*Communication equipment for low voltage AMI using Wi-SUN specifications*," Retrieved Mar., 14, 2021, from https://srm.kepco.net/index.do(Specification number : GS-5895-0051)
[16] KEPCO, "*Communication protocol specification for G-type static meters for low voltage*," Retrieved Mar., 14, 2021, from https://srm.kepco.net/index.do (Specification number : GS-6625-0087)
[17] IEC 62056-46, "*Data Link Layer Using HDLC Protocol*," Ed.1.1, 2007
[18] G. Tanganelli, A. Virdis, and E. Mingozzi, "Implementation of software-defined 6LoWPANs in Contiki OS," in *Proc. IEEE Int. Sym. WoWMoM*, pp. 201-205, Washington, USA, Jun. 2019.
[19] MOTIE, "*The Second SmartGrid Master Plan*," Retrieved Sep., 4, 2020, from http://www.motie.go.kr.
[20] F. M. Cleveland, "Cyber security issues for AMI," in *Proc. IEEE Power and Energy Soc. General Meeting Conf.*, 2008.
[21] I. S. Yang, "*Smart metering technology* (security)" Retrieved Mar., 14, 2021, from http://procon.co.kr/pdf/2017%201/11-01.pdf

명 노 길 (No-Gil Myoung)

2003년 : 충북대 전기전자공학부 졸업 (학사)
2003년 : 한국무선관리사업단 근무
2006년 : KAIST 전기 및 전자공학부 졸업 (석사)
2006년~현재 : 한전전력연구원 근무 (책임연구원)
<관심분야> 전력IoT, AMI/통합검침, 전력망 시각동기, 분산전원 출력제어

은 창 수 (Chang-Soo Eun)

1985년 : 서울대 전자공학과 졸업 (학사)
1987년 : 서울대 전자공학과 졸업 (석사)
1995년 : 텍사스 오스틴 주립대 전기·컴퓨터 공학과 졸업 (박사)
1987년~1995 : ㈜ 대우전자 중앙연구원 근무 (선임연구원)
1997년~현재 : 충남대학교 전파정보통신공학과 교수
<관심분야> 신호처리, 아날로그 회로설계, IoT, 무선통신기술