情報保護學會論文誌
第 21 卷 第 1 號, 2011. 2

원격 검침용 PLC 기술(KS X 4600-1 / ISO IEC 12139-1) 보안성 분석*

홍 정 대,[1†] 천 정 희,[1] 주 성 호,[2] 최 문 석[2]
[1]서울대학교 수리과학부, [2]한국전력공사 전력연구원

Security Analysis of KS X 4600-1 / ISO IEC 12139-1*

Jeongdae Hong[1†] , Jung Hee Cheon[1], Seong-ho Ju,[2] Moon-suk Choi[2]
[1]Seoul National University, [2]Kepco Research Institute

요 약

전력선통신(Power Line Communication: PLC)은 기존의 전력선에 고주파 신호를 중첩하는 방법으로 데이터를 전송하는 통신기술이다. 전력선통신은 연결의 편리성과 확장성 때문에 통신선로 보급이 낮은 지역의 대체 통신수단 뿐 아니라 옥내 가전기기(Home appliances)간의 통신 등으로도 주목받고 있으며, 최근 한국 전력에서도 전력선 통신 기술을 이용하여 검침값을 전송하는 원격검침시스템을 구축하고 있다.

대부분의 전력선 통신 기술은 하위 계층의 보안 프로토콜을 이용하여 안전성을 확보하고 있는데, 이는 전력선 통신의 물리적인 특성과 여러 가지 난수요소로 인해 실질적인 검침값 획득 및 변조 등의 공격이 어려울 것이라는 예측에 기반을 두고 있다. 이 논문에서는 전력선 통신의 정확한 보안성을 평가하기 위해, 먼저 하위 계층 보안 프로토콜을 포함한 전력선 통신의 동작 방식을 분석한다. 이를 통하여 검침값 데이터가 현재 상태로 전송될 경우 전력선 통신의 여러 가지 임의성에도 불구하고 검침값 변조와 같은 실질적인 공격이 가능함을 보인다. 또한 이를 보완하기 위해 다른 통신 프로토콜과 마찬가지로 상위 계층에서 보안 프로토콜이 필요함을 지적한다. 이 논문에서 제시한 전력선 통신의 동작방식 분석은 본 논문의 결론과 더불어 향후 스마트 그리드 등 대규모 사업에 사용될 전력선 통신의 표준 보안 기술 설계에 유용하게 활용될 수 있을 것으로 기대된다.

ABSTRACT

Power Line Communication (PLC) is a system for carrying data on a conductor used for electric power transmission. Recently, PLC has received much attention due to connection efficiency and possibility of extension. It can be used for not only alternative communication, in which communication line is not sufficient, but also for communication between home appliances. Korea Electronic Power Cooperation (KEPCO) is constructing the system, which automatically collects values of power consumption of every household.

Due to the randomness and complicated physical characteristics of PLC protocol (KS X4600-1), it has been believed that the current PLC is secure in the sense that it is hard that an attacker guesses or modifies the value of power consumption. However, we show that the randomness of the protocol is closely related to state of the communication line and thus anyone can easily guess the randomness by checking the state of the communication line. In order to analyze the security of PLC, we study the protocol in detail and show some vulnerability. In addition, we suggest that PLC needs more secure protocol on higher layers. We expect that the study of PLC help in designing more secure protocol as well.

Keywords: Power Line Communication (PLC), Data Encryption Standard (DES), Tone Map

접수일(2009년 11월 3일), 수정일(2010년 4월 18일)
게재확정일(2010년 9월 24일)
* 본 연구는 2005년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구과제입니다. (R-2005-1-397-004)
† 주저자, jdhong@gmail.com

I. 서 론

전력선통신(Power Line Communication: PLC)은 기존의 전력선에 고주파 신호를 중첩하는 방법으로 전력선을 통신매체로 활용하여 데이터를 전송하는 통신기술이다. 연결의 편리성과 확장성, 경제성 때문에 통신선로 보급이 낮은 지역의 대체 통신수단 뿐 아니라 옥내 가전기기(home appliances)간의 통신수단 등으로도 주목받고 있다. 2009년 7월 한국전력공사에서 개발한 고속 PLC(Power Line Communication) 기술[1]이 국제 표준화 기구(ISO) 표준[2]으로 채택되면서 전력선 통신에 대한 수요는 더욱 높아 질 것으로 기대된다.

현재 한국전력은 이 기술을 5만 6천 호의 저압 원격검침, 전기·가스·수도 통합 검침 등에 활용하고 있으며, 제주도 스마트 그리드 시범 사업지역에 전기료, 사용기록, 안내 메시지와 같은 필수 정보들을 보여주는 IHD(in-home display), 전기차, 태양광 등 스마트 그리드 기반시스템의 통신망으로도 활용할 계획이다. 또한 한국전력은 2009년 7월 초 착수한 사우디아라비아 전력청 약 400만호 원격검침 컨설팅 계약 사업에도 PLC 국제표준 규격을 권고할 예정이다.

대부분의 전력선 통신 기술은 하위 계층의 보안 프로토콜을 이용하여 안전성을 확보하고 있는데, 이는 전력선 통신의 물리적인 특성과 여러 가지 난수요소로 인해 실질적인 검침값 획득 및 변조 등의 공격이 어려울 것이라는 예측에 기반을 두고 있다. PLC 기술(KS X 4600-1)은 채널 환경에 따라 주기적으로 톤맵(tone map)을 변경하기 때문에 송신자와 수신자가 통신개시 전 톤맵을 일치시키는 과정을 거치도록 하였다. 이러한 톤 맵의 변경은 통신 환경 변화에 맞춰 좋은 통신경로를 탐색하는 과정이기도 하지만 톤맵을 모르면 신호를 얻을 수 없기 때문에 보안성에 도움을 줄 것이라고 기대되기도 한다. 또한 PLC(KS X 4600-1)기술은 데이터 보안을 위해 클래스 A(고속 PLC를 이용한 옥내 및 옥외 데이터 네트워크)와 클래스 B(고속 PLC를 이용한 A/V 엔터테인먼트 네트워크)에 각각 DES(Data Encryption Standard)와 AES(Advanced Encryption Standard) 암호시스템을 사용하도록 하고 있다.

한편 검침값은 개별 가구의 전력 사용량을 나타내고 비용과 직접적으로 관련되기 때문에 무결성(integrity), 부인방지(non-repudiation), 인증(authentication) 뿐 아니라 재사용 공격(replay attack) 방지 등의 보안요건까지 갖춘 통신망을 통해 전송되어야 한다. 현재 PLC 기술(KS X 4600-1)은 보안을 위해 상위계층에서 DES 암호시스템[3]또는 AES 암호시스템[4]만을 사용하고 있는데, 블록암호시스템 단독으로는 무결성, 부인방지, 인증 등의 보안요건을 만족하지 못할 뿐 아니라 DES 암호시스템은 이미 1999년에 안전하지 않은 것으로 분류되어 있어서 보안에 취약한 것으로 판단된다. 또한 통신의 효율성을 위해 통신 개시 전 확인 및 변경하는 톤 맵도 보안성 향상에는 거의 도움이 되지 않는 것으로 보인다. 본 논문에서는 DES와 톤 맵에 의지하는 원격 검침용 PLC 기술의 보안성과 개선 가능성을 분석하고 그 대안을 제시한다.

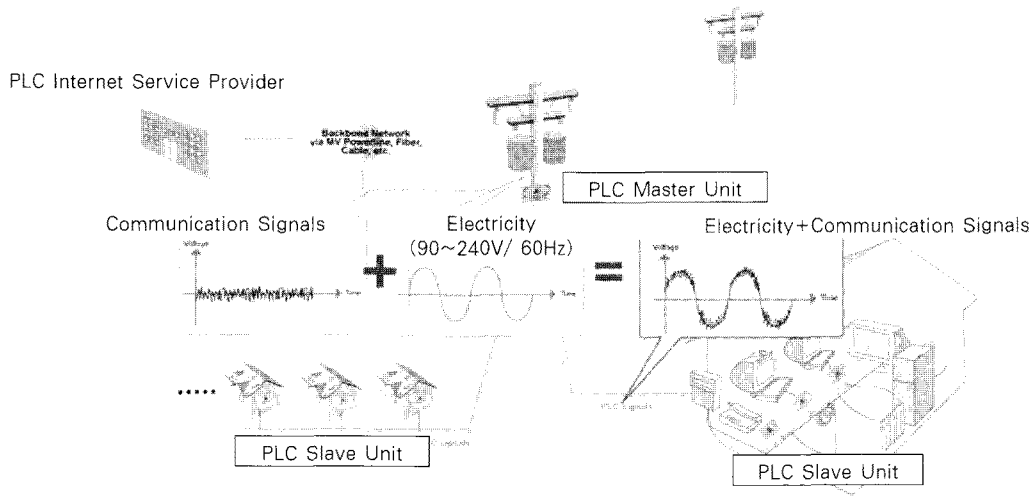
논문의 구성은 다음과 같다. 먼저 2장에서 물리계층의 프로토콜을 포함한 전력선 통신의 동작 방식을 소개 및 분석한다. 3장에서는 검침값 데이터가 현재 상태로 전송될 경우 전력선 통신의 여러 가지 임의성에도 불구하고 검침값 변조와 같은 실질적인 공격이 가능함을 보인다. 4장에서는 이를 보완하기 위해 다른 통신 프로토콜과 마찬가지로 상위 계층에서 보안 프로토콜이 필요함을 지적한다.

II. 전력선 통신 개요

전력선 통신 기술은 향후 스마트그리드, AMI(Advanced Metering Infrastructure)등에 광범위하게 활용될 중요한 기술이기 때문에 보안성 분석 뿐 아니라, 보다 향상된 표준 보안 프로토콜 설계를 위해 현재 통신 프로토콜의 동작방식을 정확히 이해할 필요가 있다. 따라서 보안성 분석에 앞서 PLC 통신기술에 대해 간략히 살펴본다.

전력선 통신(PLC)이란 [그림 1]과 같이 기존의 전력선 (90~240V/ 60Hz)에 통신 신호(Communication signals)를 결합하여 데이터를 송·수신하는 통신방식을 말한다. 한국전력의 원격 전력량 검침은 각 가구의 전력 사용량을 15분 단위로 측정하여 전력선 통신을 이용하여 통보하는 시스템이다. 기존의 전신주를 중심(Master Unit)으로 하나의 그룹을 형성하며, Master Unit들은 이들을 한국전력으로 재전송한다.

먼저 측정된 전력 사용량(검침값)을 송·수신하는데 사용되는 전력선 통신기술(전기통신과 시스템 간의 정보교환-전력선 통신(PLC)-고속 PLC 매체접근제어(MAC) 및 물리층(PHY): KS X 4600-1 또는



〔그림 1〕 전력선 통신

ISO IEC 12139-1 클래스 A)의 PHY 계층에 대한 기술 특징 및 사양을 살펴보면 다음과 같다.

2.1 변·복조 방식

고속 PLC를 이용한 옥내 및 옥외 데이터 네트워크를 위한 클래스 A 장치의 변·복조 방식으로는 다중반송파(Discrete Multi Tone: DMT) 방식을 사용한다. 다중 반송파 방식은 한 채널의 대역폭(bandwidth)을 여러 개의 작은 대역폭을 갖는 부채널(sub-channel)로 분할하고, 다수의 협대역 부반송파(sub-carrier)를 부채널로 하여 신호를 전송하는 기술을 말한다. 다중 반송파 방식은 작은 대역폭으로 인해 단일 반송파 변조 방식에 비해 고속 데이터 전송에 유리한 것으로 알려져 있다. 〔표 1〕에는 전력선 통신의 PHY 계층에 대한 기본적인 규격이 나타나 있다. 이때 순환접두부는 다중 반송파 변조방식에서 각 심볼이 다중 경로 채널을 통해 전송되는 동안 상호 심볼 간 간섭을 방지하기 위해 연속된 심볼 사이에 채널의 최대 지연확산 보다 긴 보호구간을 삽입하는 방법 중의 하나인데, 순환접두부는 유효 심볼구간의 마지막 구간 신호를 프레임의 앞부분에다 붙이는 방법이다.

규격에서 제시하는 DMT 시스템은 2.15~23.15 MHz의 대역을 사용하며, 한 번의 통신에는 총 256개의 서브채널(톤)이 존재하고 각 톤은 97.65625 kHz(이론치)의 대역폭을 갖는다. 전력선 채널에서 DMT 심볼 간의 간섭을 없애기 위해 128 샘플의 순환 접두부를 사용한다. 또 전력선 채널 상에서 발생하는 노이즈에 의한 패킷 에러 확률을 줄이기 위해 컨볼루셔널 부호와 리드-솔로몬(Reed-Solomon) 부호가 결합된 FEC(Forward Error Correction)를 적용한다.

〔표 1〕 PHU 계층 규격

항 목	값
사용대역폭(Bandwidth)	2.15~23.15 MHz
톤 간격(25MHz/256)	97.65625 kHz
샘플링 주파수	50 MHz
IFFT 간격	512 샘플
순환 접두부 간격	128 샘플
롤 오프 간격	16 샘플
심볼 간격	624 샘플
심볼 속도	80.1282 kHz
심볼 길이 (순환접두부가 없는 경우)	10.24 μs
심볼 길이 (순환접두부가 있는 경우)	12.48 μs
톤(또는 부채널) 변조 방식	DBPSK, DQPSK, D8PSK

2.2 물리계층 서비스 데이터 단위 (PSDU)

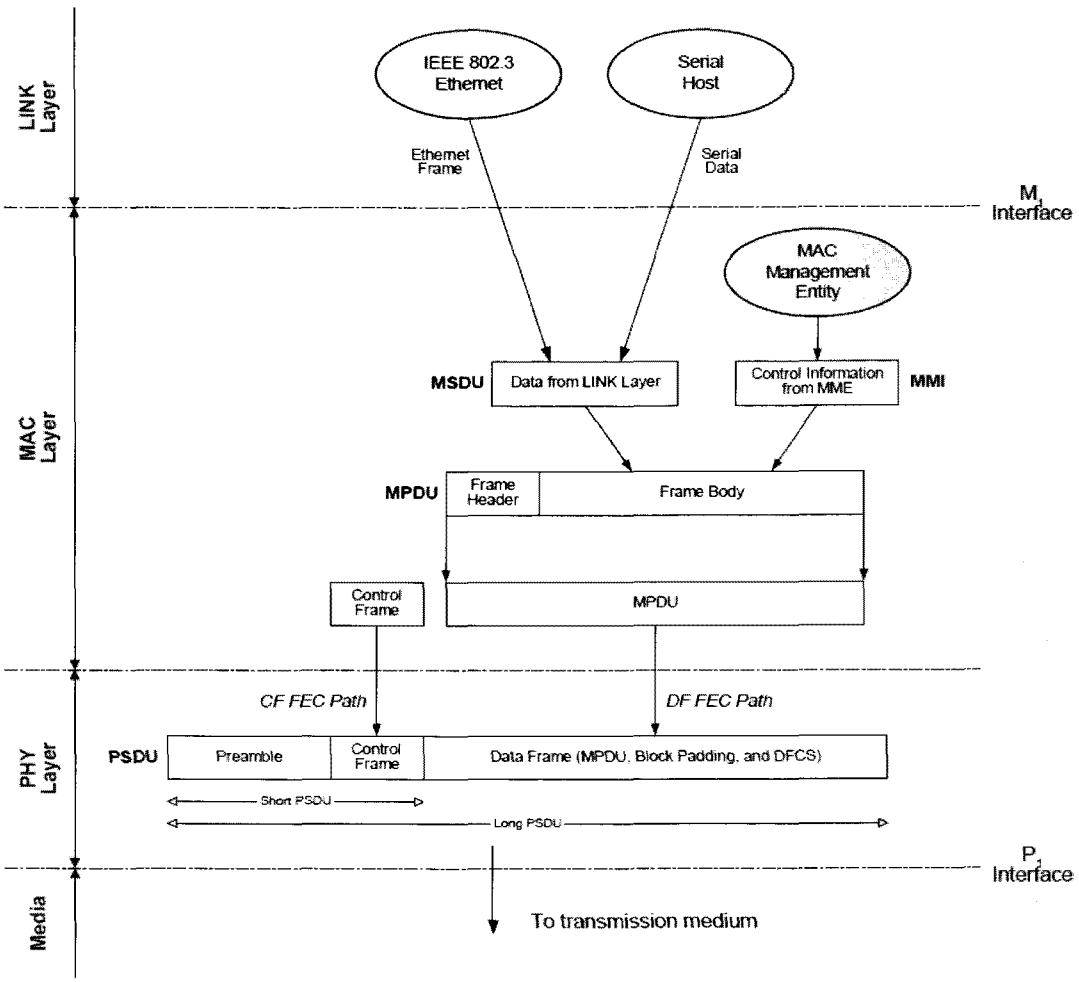
규격에서 사용하는 물리계층 서비스 데이터 단위(PHY Service Data Unit: PSDU)의 캡슐화 과정 및 구조는 〔그림 2〕와 같다. 링크 레이어(link layer)로부터 내려 받는 데이터는 IEEE 802.3 이더넷(ethernet) 데이터 일 수도 있고 검침값과 같은 데

이터 일 수도 있다. 이 데이터는 MAC 관리 실체(MAC management entity), 프레임 헤더와 함께 MAC 프로토콜 데이터 단위(MAC protocol data unit)를 구성한다. 여기에 MAC 레이어에서 결정된 제어 프레임(Control Frame: CF)과 프리앰블(preamble)을 추가하여 PSDU를 구성한다. 이때 제어 프레임(Control Frame: CF)과 프리앰블을 구분자(delimiter)라고 부르는데 프레임의 특성에 따라서는 데이터 프레임(data frame) 없이 구분자만으로 구성된 PSDU가 존재하기도 한다.

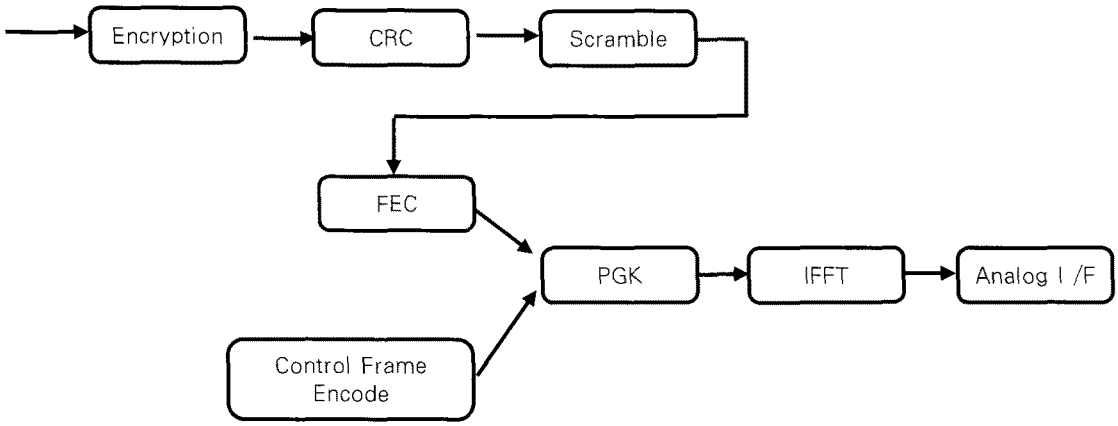
이중 제어프레임은 데이터 프레임의 전달을 도와주는 부분으로 MAC 계층에서의 신뢰성을 지원하고 무선매체로의 접근을 관리하는 역할을 하며, PLC 통신의 제어프레임은 순환접두부(cyclic prefix)가 붙은 4개의 다중반송파 심볼로 구성된다. 프리앰블은 시스템간에 전송 타이밍을 동기화하기 위해 사용되는 신호를 말하는데, 프리앰블은 순환접두부가 없는 7개의 트레이닝 신호와 2개의 역 트레이닝 신호로 구성된다. 수신단에서는 이를 이용하여 물리적 반송파 감지와 자동이득 조절 및 동기화 등의 작업을 수행한다.

2.3 다중반송파 송신 메커니즘

캡슐화된 PSDU는 [그림 3]과 같은 메커니즘을 통해 상대방 노드로 송신된다. 56비트 DES를 사용하여 암호화한 데이터에 순환 잉여 검사 (cyclic redundancy Check :전송된 데이터에 오류가 있는지 확인하기 위해 체크값을 결정하는 방식), 스크램블



[그림 2] PSDU 서식 및 캡슐화 과정



〔그림 3〕 다중반송파 송신기 블록도

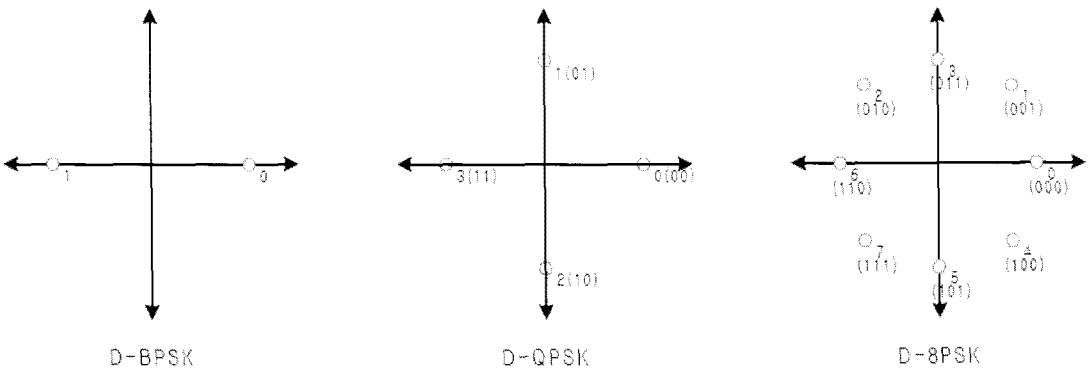
(scramble : 교란), 순방향 에러정정(Forward Error Correction: FEC)등을 수행하여 데이터의 보안성과 정확성을 향상시킨다. 그리고 인코딩된 제어프레임과 결합시켜 톤별로 정의된 위상편이 변조(Phase Shift Keying: PSK)과정을 통과시킨 후 역급속 푸리에 변환(Inverse Fast Fourier Transform: IFFT)시켜 전송한다.

2.4 위상편이 변조(PSK)

각 서브채널 혹은 톤에 사용되는 변조 방식은 채널 상황에 따라 DBPSK, DQPSK 및 D8PSK를 사용한다. 〔그림 4〕는 각 변조 방식의 성상도를, "〔표 2〕"는 부호화값을 보여준다. 서브 채널별로 선택된 변조 방식에 따라 전송될 수 있는 비트의 수도 결정된다.

〔표 2〕 변조방식별 부호화 값
(θ :이전 심볼의 동일한 톤에서 전송된 위상값)

변조방식	입력비트	출력값
D-BPSK	0	θ
	1	θ+π
D-QPSK	00	θ
	01	θ+π/2
	11	θ+π
	10	θ+3π/2
D-8PSK	000	θ
	001	θ+π/4
	011	θ+π/2
	010	θ+3π/4
	110	θ+π
	111	θ+5/4
	101	θ+3π/2
	100	θ+7π/4



〔그림 4〕 위상편이 변조 성상도

2.5 톤 맵 인덱스(Tone Map Index: TMI) 설정

통신 개시 전 송신측 노드와 수신측 노드는 채널 상황에 적합한 톤별 변조방식을 결정하는데, 이는 제어프레임에 포함되는 톤 맵 인덱스로 공유된다. 톤 맵 인덱스는 다음과 같은 방법으로 결정된다. 톤 맵 인덱스는 자신의 송 · 수신 톤 맵을 저장한 주소인 MTMI (My Tone Map Index)와 상대 송 · 수신 톤 맵을 저장한 PTMI(Parter's Tone Map Index)로 구분된다. 통신을 개시하고자 하는 노드가 상대방 노드

〔표 3〕 각 톤별 기준 위상값

톤 번호	위상값 (x π/8)	톤 번호	위상값 (x π/8)	톤 번호	위상값 (x π/8)	톤 번호	위상값 (x π/8)	톤 번호	위상값 (x π/8)	톤 번호	위상값 (x π/8)	톤 번호	위상값 (x π/8)	톤 번호	위상값 (x π/8)
0	15	1	15	2	13	3	8	4	11	5	2	6	9	7	1
8	14	9	6	10	8	11	10	12	3	13	4	14	3	15	8
16	7	17	6	18	7	19	1	20	9	21	8	22	1	23	2
24	9	25	12	26	13	27	12	28	7	29	12	30	7	31	1
32	4	33	11	34	11	35	13	36	15	37	8	38	8	39	11
40	4	41	0	42	12	43	9	44	13	45	10	46	8	47	8
48	13	49	13	50	13	51	11	52	2	53	15	54	8	55	3
56	1	57	3	58	8	59	1	60	15	61	10	62	6	63	2
64	10	65	3	66	9	67	0	68	2	69	8	70	0	71	3
⋮															
184	2	185	10	186	14	187	10	188	10	189	13	190	14	191	4
192	6	193	3	194	13	195	7	196	6	197	1	198	8	199	4
200	15	201	10	202	0	203	11	204	7	205	4	206	2	207	2
208	0	209	3	210	9	211	13	212	1	213	2	214	15	215	5
216	0	217	11	218	12	219	14	220	5	221	10	222	13	223	5
224	14	225	1	226	11	227	0	228	1	229	1	230	13	231	2
232	6	233	1	234	14	235	13	236	2	237	13	238	11	239	9
240	5	241	15	242	11	243	12	244	5	245	15	246	13	247	5
248	8	249	8	250	6	251	7	252	10	253	3	254	15	255	9

〔표 4〕 제어 프레임용 톤 번호

톤순서	톤번호									
1번~10번	47	48	59	50	51	52	53	54	55	56
11번~20번	57	58	59	60	61	62	63	64	78	79
21번~30번	80	81	82	88	95	96	97	98	99	107
31번~40번	108	109	110	111	112	113	114	115	116	117
41번~50번	118	119	120	121	122	128	124	125	126	127
51번~60번	128	129	130	131	132	133	150	151	152	153
61번~70번	154	155	156	157	158	159	160	161	162	163
71번~80번	164	165	166	167	168	169	170	171	172	173
81번~90번	174	175	176	177	178	179	180	189	190	191
91번~100번	192	193	194	195	196	197	198	199	200	201
101번~110번	202	203	204	205	206	207	208	209	210	211
111번~120번	212	223	224	225	226	227	228	229	230	231
121번~124번	232	234	235	-	-	-	-	-	-	-

에게 트레이닝 시퀀스(Training Sequence: TS)를 보낸다. 그러면 상대방 노드는 채널 추정을 하는데 TS를 받은 시점의 전력선 상태를 고려하여 적절한 TMI를 결정(1~63)하고 이를 통보한다. TS에 대한 응답으로 수신한 톤 맵 인덱스는 TS를 보낸 노드의 PTMI가 된다. 채널 추정(Channel Estimation) 결과의 TMI 필드에는 이렇게 저장된 PTMI가 포함된다. 동일한 방법으로 상대방 노드도 TS를 보내고 CE 결과를 수신하는 방법으로 PTMI와 MTMI를 결정한다. CE결과를 수신한 노드가 같은 상대 노드로부터 TS를 수신하였을 경우에는 상대방 노드에게 동일한 MTMI를 부여한다. 각 톤 맵 인덱스는 각 톤의 위상값을 나타내는데 각 톤 별 기준 위상값은 미리 결정되어 있는데 각 톤별 기준 위상값은 [표 3]과 같다.

이중 [표 4]의 124개의 톤은 제어 프레임 전송에 사용되고 나머지 톤은 기준 위상값에 대해 동일한 혹은 180도 위상 반전된 값을 임의로 발생시켜 전송한다.

III. 전력선 통신 기술의 보안성 분석

KS X 4600-1 또는 ISO IEC 12139-1 클래스 A의 PHY 계층의 보안성은 DES 암호시스템에 의지하고 있으며, 주기적인 톤 맵의 변경도 보안성에 다소 도움을 준다고 기대할 수 있다. 여기서는 DES와 톤 맵의 보안성을 분석한다.

3.1 DES의 안전성

DES(Data Encryption Standard: Federal Information Standards Publication 46-3)는 1976년 미국 NBS(National Bureau of Standards)에 의해 미국 표준으로 선정된 이래 가장 널리 사용되어온 블록 암호이다. 송신 노드와 수신 노드가 공유하는 56 비트 비밀키를 사용하여 64비트 단위로 암·복호화를 진행한다. 기본적인 암·복호화 방법은 [그림 6]과 같다.

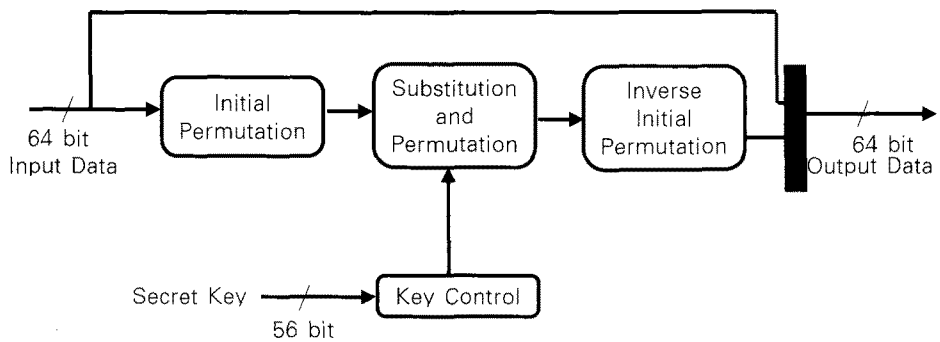
그러나 DES는 더 이상 안전하지 않은 암호시스템으로 분류되며 미국정부는 2001년부터 AES(Advanced Encryption Standard)를 블록암호 표준으로 선정하여 사용하고 있다.

DES에 대한 대표적인 공격으로는 차분공격(differential cryptanalysis)과 선형공격(linear cryptanalysis)이 알려져 있다. 차분공격[5]은 1991년 Eli Biham과 Adi Shamir에 의해 제안된 공격방법으로 최소 2^{47}개의 일정한 차분을 갖는 평문쌍(chosen plaintexts)과 암호문쌍을 이용하여 키를 찾는 공격이며, 선형공격[6]은 1998년 Mitsuru Matsui에 의해 제안된 공격방법으로 2^{43}개의 이미 알고 있는 평문(known plaintexts)이 있을 때 이를 이용하여 공격하는 방법인데 두 가지 공격 모두 전수조사(exhaustive attack)에 비해 빠른 시간 내에 공격이 성공할 수 있음을 보여준다. 또한 1999년에는 distrubuted.net과 Electronic Frontier Foundation이 협력하여 선택 또는 기지 평문 없이 무차별 대입 공격(brute force attack)으로 22시간 15분 만에 56비트 키를 찾아낸 바 있다.

3.2 원격 검침용 PLC의 보안성 분석

3.2.1 차분공격 또는 선형공격에 취약

원격 검침용 전력선 통신에서 송·수신하는 데이터인 검침값은 이미 알고 있거나 추측할 수 있는 값이



[그림 6] 56-비트 DES 블록도

[표 5] 각 톤별 주파수 값

톤 번호	주파수 (MHz)	톤 번호	주파수 (MHz)	톤 번호	주파수 (MHz)	톤 번호	주파수 (MHz)	톤 번호	주파수 (MHz)	톤 번호	주파수 (MHz)
0	0	1	0.0977	2	0.1953	3	0.2930	4	0.3906	5	0.4883
6	0.5859	7	0.6836	8	0.7813	9	0.8789	10	0.9766	11	1.0742
12	1.1719	13	1.2695	14	1.3672	15	1.4648	16	1.5625	17	1.6602
18	1.7578	19	1.8555	20	1.9531	21	2.0508	22	2.1484	23	2.2461
24	2.3438	25	2.4414	26	2.5391	27	2.6367	28	2.7344	29	2.8320
30	2.9297	31	3.0273	32	3.1250	33	3.2227	34	3.3203	35	3.4180
36	3.5156	37	3.6133	38	3.7109	39	3.8086	40	3.9063	41	4.0039
42	4.1016	43	4.1992	44	4.2969	45	4.3945	46	4.4922	47	4.5898
⋮											
198	19.3359	199	19.4336	200	19.5313	201	19.6289	202	19.7266	203	19.8242
204	19.9219	205	20.0195	206	20.1172	207	20.2148	208	20.3125	209	20.4102
210	20.5078	211	20.6055	212	20.7031	213	20.8008	214	20.8984	215	20.9961
216	21.0938	217	21.1914	218	21.2891	219	21.3867	220	21.4844	221	21.5820
222	21.6797	223	21.7773	224	21.8750	225	21.9727	226	22.0703	227	22.1680
228	22.2656	229	22.3633	230	22.4609	231	22.5586	232	22.6563	233	22.7539
234	22.8516	235	22.9492	236	23.0469	237	23.1445	238	23.2422	239	23.3398
240	23.4375	241	23.5352	242	23.6328	243	23.7305	244	23.8281	245	23.9258
246	24.0234	247	24.1211	248	24.2188	249	24.3164	250	24.4141	251	24.5117
252	24.6094	253	24.7070	254	24.8047	255	24.9023	-	-	-	-

다. 따라서 보다 상위 계층에서 적절한 보안대책을 강구하지 않고 PHY계층의 DES에만 보안성을 의지한다면 앞서 설명한 기지평문(known plaintexts) 또는 선택평문(chosen plaintexts) 공격에 취약하다. 즉, 검침값은 기존의 검침값에 어느 정도의 값이 추가되는 값일 것이기 때문에 기존의 전력량을 알고 있는 공격자는 그 값에 오차 범위내의 값을 더하는 방법으로 새로운 검침값을 예상할 수 있다. 때문에 충분한 양의 평문을 모을 수 있다. 충분한 양의 평문을 모으면 공격자는 선형공격이나 차분공격을 적용할 수 있다. DES 암호시스템의 공격자에게 2^{43} 개 이상의 기지평문 또는 2^{47}개 이상의 선택평문이 주어진 경우 공격자는 선형공격 또는 차분공격을 이용하여 전수조사보다 빠른 시간 내에 비밀키를 찾을 수 있게 된다.

3.2.2 재사용 공격(replay attack)에 취약

검침값은 각 가정의 전력 사용량이기 때문에 검침되는 전력량이 기존 전력량에 추가되는 형태이든 단위시간에 사용된 전력량이든 재사용 공격을 시도할 가능성이 크다. 따라서 타임스탬프(time stamp) 또는 동기화(synchronization) 등의 방법을 추가하지 않는다면 사용자가 동일한 검침값을 계속 전송하더라도 한국전력 측에서는 이를 정당한 검침값으로 이해할 수 밖에 없다. 제안된 전력선 통신에서는 보안성을 위해 DES 암호시스템을 사용하고 있는데, 블록 암호 시스템으로는 이러한 재사용공격을 막을 수 없다.

3.2.3 암호키(encryption key) 관리 문제

현재의 시스템에서는 하나의 master unit을 중심으로 다수의 원격검침 장비(가구)가 동일한 비밀키를 사용하고 있으며, 키의 변경 주기는 고려하지 않고 있는데 위의 차분 또는 선형 공격 등에 의해 하나의 비밀키가 누설되면 동일한 비밀키를 사용하는 다른 모든 장비도 동시에 비밀키가 누설되게 된다. 또한 하나의 master unit를 중심으로 다수의 장비가 동일한 키를 사용하기 때문에 공격자가 앞서 설명한 기지평문 또는 선택평문을 수집할 가능성도 높아진다.

3.2.4 tone map 변경

현재 한국전력에서 추진 중인 검침값 전송 시스템에서는 검침값을 송·수신하는 두 노드가 매 통신 개시 전(15분 간격) 톤 맵 인덱스를 재설정하도록 되어 있다. 송신 노드는 설정된 톤 맵 인덱스에 따라 각 서브 채널(톤 맵)의 변조방식에 맞는 방법으로 데이터를 변조 및 암호화하여 보내며, 수신 노드는 이 톤 맵에

따라 암호화된 검침값을 추출하고 이를 복호화하여 실제 검침값을 알 수 있게 된다.

이때 톤 맵 인덱스는 서브 채널(톤)의 개수가 256개이고 각 톤이 가질 수 있는 변조 방식이 3가지이기 때문에 이론상 3^{256}가지가 존재할 수 있으나 표준에서는 63가지만 존재한다.

따라서 톤 맵 인덱스를 모르는 공격자라도 63가지 톤 맵 인덱스를 테스트해 봄으로써 톤 맵을 알아낼 수 있다. 더구나 [표 4]에 제시된 124개 톤은 제어프레임을 위해 할당되어 있기 때문에, 공격자는 이 124개의 톤을 높은 확률로 추측할 수 있으며 [표 5]의 각 톤 별 주파수 또한 이미 알고 있기 때문에 해당 톤의 주파수에서 감지한 신호를 기준 위상값과 비교하는 방법으로 정확한 톤 맵 인덱스를 알아낼 수 있게 된다.

그리고 톤 맵 인덱스를 결정하는 주요 변수가 채널의 상태이기 때문에 채널의 상태를 알 수 있는 공격자는 높은 확률로 하나의 톤 맵 인덱스를 추측할 수 있다. 이는 톤 맵 인덱스는 거의 공개된 정보로 간주 할 수 있음을 의미한다.

톤 맵 인덱스의 정보를 숨기기 위해 종류를 늘리거나 기존의 톤 맵 인덱스에 난수를 추가하는 방법을 고려할 수 있는데, 이는 테스트 횟수를 크게 향상시키지 못할 뿐 아니라(N개의 톤 맵 인덱스에 대한 테스트 횟수는 $\log_2 N$) [그림 7]과 같은 제어프레임의 골격을 변경해야하는 문제를 유발하기 때문에 바람직하지 않아 보인다.

IV. 검침용 PLC 기술을 위한 보안 대책

전력선 통신으로 검침값과 같이 고유하면서도 변경값이 의미를 가지는 정보를 송·수신하는 데는 보다 상위계층에서의 보안 대책이 요구되는데 본 절에서는 이러한 보안대책을 제안한다.

4.1 보안성이 강한 블록 암호 시스템 사용

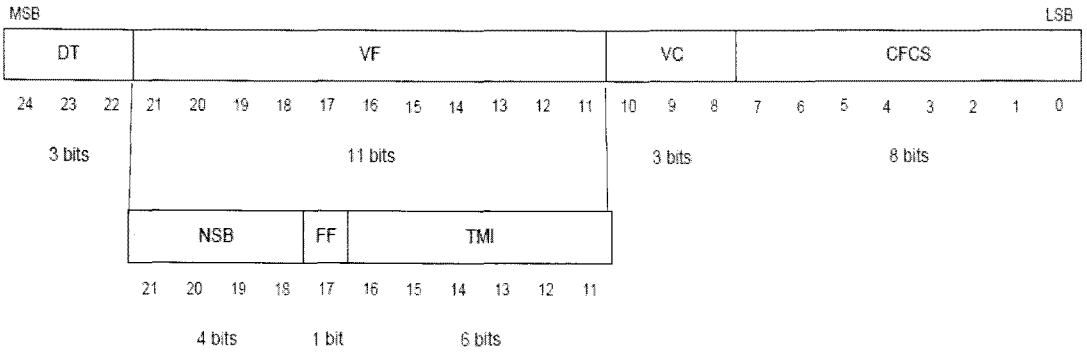
전송하고자 하는 정보가 검침값과 같은 개별 정보가 아니라도, 암호학적 관점에서 DES 암호 시스템은 이미 보안성에 도움을 주지 않는 걸로 간주 된다. 따라서 미국의 전력선 통신 표준 HomePlug AV와 같이 AES 암호시스템을 사용하거나 국내 표준인 ARIA[7]의 사용을 권고한다.

4.2 키 관리 시스템 보완

ARIA 등의 암호시스템을 사용하면 128비트 이상의 키를 사용할 수 있으므로, 개별 장비(가구)별로 서로 다른 비밀키를 부여 할 것을 권장한다. 또한 비밀키가 누설되지 않은 상황이라도 안전한 비밀키 주입·주기적인 교체 등과 같은 키 관리(key management) 방안이 강구되어야 할 것으로 판단된다.

4.3 상위 계층에서 보안대책 강구

전력선 통신 기술(KS X 4600-1)은 물리계층에서 DES 암호 시스템을 사용하여 데이터를 암호화하고 있지만, 블록 암호 단독으로는 무결성(integrity), 부인방지(non-repudiation), 인증(authentication)과 같은 다른 보안요건을 충족하지 못한다. 그런데, 검침값은 비용과 직결되기 때문에 데이터를 변조하거나 전기를 추가적으로 사용하지 않은 것처럼 이전 검침값을 전송하려 할 재사용 공격의 가능성이 내재되어 있다. 따라서, 검침값과 같이 특정 가구(노드)



[그림 7] 제어프레임 서식

와 밀접하게 연결된 값을 안전하게 전달하기 위해서는 보다 상위 계층에서 공개키(public key) 암호 시스템과 타임스탬프(time stamp) 등을 사용하여 무결성, 부인 방지 및 인증 기능과 같은 보안요건 들을 추가해야 한다.

V. 결 론

전력선 통신은 연결의 편리성, 경제성 및 확장 가능성으로 인해 갈수록 수요가 증대할 것을 보인다. 그러나 현재 표준에서 제시하는 보안대책 즉, 클래스 A에서의 DES 암호시스템 사용 및 클래스 B에서 AES 암호시스템을 사용하는 것만으로는 무결성(integrity), 부인방지(non-repudiation), 인증(authentication) 등과 같은 다른 보안요건을 충족하지 못한다. 또한 통신의 효율성을 위해 매 통신 개시 전 변경하는 톤 맵도 보안성에 어떠한 도움을 준다고 볼 수 없다.

따라서 본 논문에서 살펴본 바와 같이 보안성을 요구하는 데이터를 전력선 통신 기술을 이용하여 송·수신하기 위해서는 보다 상위 계층에서 공개키 암호시스템과 타임스탬프 사용 등의 보다 강화된 보안대책이 요구되며 물리계층(PHY)에서도 보다 안전한 블록암호의 사용이 필요하다.

참고문헌

[1] "정보기술-전력통신과 시스템 간의 정보교환-전력선통신(PLC)-고속 PLC 매체접근제어(MAC) 및 물리층(PHY)-제 1부: 일반요구사항," KS X 4600-1, 산업자원부 기술표준원, 2007년.

[2] "Information technology — Telecommunications and information exchange between systems — Powerline communication (PLC) — High speed PLC medium access control (MAC) and physical layer (PHY) — Part 1: General requirements," ISO/IEC 12139-1, 2009.

[3] FIPS 46-3: The official document decribing the DES standard.

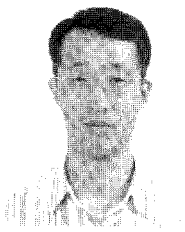
[4] FIPS PUB 197: the official AES standard.

[5] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems," Journal of Cryptology, vol. 4, no. 1, pp. 3-72, 1991.

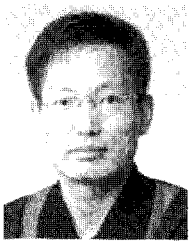
[6] M. Mastsui, "Linear Cryptanalysis Method for DES Cipher, Advances in cryptology-EUROCRYPT '93, LNCS 765, pp. 386-397, 1994.

[7] D. Kwon, J. Kim, and S. Park et al., "New block cipher: ARIA," Proceedings of the Information Security and Cryptology-ICISC'03, LNCS 2971, pp. 432-445, 2003.

〈著者紹介〉

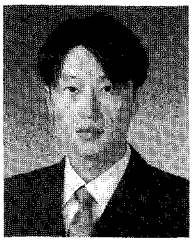


홍 정 대 (Jeongdae Hong) 정회원
1993년 3월: 육군사관학교 기계공학부 졸업
2005년 2월: 서울대학교 전기컴퓨터공학부 석사
2010년 2월: 서울대학교 전기컴퓨터공학부 박사
2010년 3월~현재: 국방부
〈관심분야〉 그룹 복호화, 네트워크 보안



천 정 희 (Jung Hee Cheon) 정회원
1997년 2월: 한국과학기술원 수학과 박사
1997년 3월~2000년 1월: 한국전자통신연구원 선임연구원
2000년 1월~2000년 12월: 브라운 대학 박사후 연구원
2000년 12월~2003년 2월: 한국 정보통신 대학교 공학부 조교수
2003년 3월~현재: 서울대학교 수리과학부 교수
〈관심분야〉 계산 수론, 암호론, 응용 암호

주 성 호 (Seong-ho Ju) 정회원
2001년 2월: 연세대학교 전기공학과 졸업
2004년 2월: 서울대학교 전기컴퓨터공학부 석사
2004년 1월~현재: 한국전력공사 전력연구원 선임연구원
〈관심분야〉 원격검침, SCADA 보안, 스마트그리드 보안



최 문 석 (Moon-suk Choi) 정회원
2003년 2월: 충남대학교 전자공학과 졸업
2005년 2월: KAIST 전기전자공학부 석사
2005년 2월~현재: 한국전력공사 전력연구원 선임연구원
〈관심분야〉 망관리, SCADA 보안, 스마트그리드 보안