IP와 연동되는 PLC 네트워크에서의 기기간 인증 메커니즘

°조용준[1], 허준[1], 홍충선[1], 최문석[2], 주성호[2]
[1]경희대학교 컴퓨터공학과
°ejcho@networking.khu.ac.kr, heojoon@khu.ac.kr, cshong@khu.ac.kr
[2]한국전력공사 전력연구원
cms96@kepri.re.kr, shju1052@kepri.re.kr

Device authentication mechanism on PLC network linked with IP network

°EungJun Cho, Joon Heo, ChoongSeon Hong, Moon Seok Choi, Seong Ho Ju
[1]Department of Computer Engineering, Kyung Hee University
[2]KEPRI KEPCO, Korea

요 약

IP 네트워크(공중망)에 새로운 네트워크 기술들의 결합, 예를 들면 IP-USN, IP-Mesh, IP-PLC 등의 이종 네트워크가 생겨나면서 이러한 네트워크를 안전하게 관리하기 위한 보안 기술의 개발이 요구되고 있다. 기존 IP 네트워크가 가지는 다양하고 견고한 보안 기술들이 이종 네트워크에 그대로 사용될 수 없으면서 생겨나는 문제 중 PKI 기반 인프라를 적용할 수 없다는 것이 가장 현실적이고 중요한 문제로 여겨지고 있다. 이러한 문제로 인해, 새로운 네트워크 기술들은 주로 내부에서 사용하는 대칭키 방식의 암호화, 복호화만을 정의하고 있다. 본 논문에서는 이러한 문제를 해결하고자 하는 노력으로, 이종 네트워크 환경에서 디바이스간 인증을 하는 메커니즘을 제안한다.

1. 서 론

정보의 다양성과 중요성이 증가하면서, 보안 기술의 적용을 통해 안전한 통신망을 구축하는 것이 네트워크 운용에 있어 기본적인 요구사항이 되었다. 이는 이종 네트워크와 같은 기술 간의 융합에 있어서도 중요한 요소라고 할 수 있다. 그러나 이종 네트워크는 이를 구성하는 기술들의 특징으로 인해, IP네트워크에서 사용되는 보안 기술의 적용이 불가능하다. 네트워크의 확장에 따른 관리 개체의 증가에도 효율적으로 디바이스를 관리할 수 있고, 안전한 통신망 구축을 위해 필수적인 보안키 관리 프레임워크의 구축이 필요하다고 할 수 있다. 따라서 본 논문에서는 이러한 이종 네트워크의 제약조건을 고려할 때, 기존 PKI 인프라를 활용할 수 없는 환경에서 공개키를 활용한 보안키 관리 프레임워크 방식에 관하여 기술한다. 인증서 기반의 공개키 사용을 위해 신원 기반 암호화 방식의 개념을 사용하며 이에 따르는 보안키 관리 프레임워크를 위해 구체적인 메커니즘을 제안한다.

본 논문은 다음과 같이 구성 되어있다. 2장에서는 관련 연구를 살펴 볼 것이고 3장에서는 IP와 연동되는 PLC 네트워크의 특징을, 4장에서는 보안이슈 그리고 5장에서는 기기인증 메커니즘을 설명 할 것이고 마지막으로 6장에서는 해당 메커니즘의 보안성을 분석하여 볼 것이다.

2. 관련연구

현재 사용되고 있는 대부분의 전력선 통신은 몇가지 주요 표준기술을 따르고 있다. 국내외 대표적 표준기술은 아래와 같다.

- Homeplug [1]

대표적인 전력선 관련 국제 표준으로서 전력선 통신 활용 분야에 따라 5가지 보안 모드 (Security Mode: Insecure, User-confirm, Secure, Lock-down)를 정의하고 있으며, 각 모드는 서로 다른 보안 정책을 가진다. 암호화 키 및 패스워드를 사용하는데 있어 매우 다양한 종류의 보안 키 (DAK, DPW, PPK 등)의 생성 방식 및 절차를 정의하고 있다. 또한, 암호 알고리즘으로는 AES-CBC 또는 1024비트 RSA 방식을 사용하도록 정의하고 있다.

- KS X4600-1 [2]
고속 전력선 통신을 위한 국내 표준으로서 동일한 셀(Cell)내의 장비들은 같은 암호화 키를 사용한다. 데이터 네트워크를 위한 클래스 A의 경우 PHY레이어와 MAC레이어에서 56비트 DES 알고리즘을 사용하여 암호화/복호화를 수행한다. AV 네트워크를 위한 클래스 B의 경우 PHY레이어에서 3-DES 또는 AES 알고리즘을 사용해 암호화/복호화를 수행한다.

- OPERA [3,4]
대표적인 전력선 관련 국제 표준으로서 전력선 통신의 활용 분야에 따라 5가지 보안 모드 (Security Mode, Insecure, User-confirm, Secure, Lock-down)를 각각 정의하고 있으며, 각 모드는 서로 다른 보안 정책을 가진다. 암호화 키 및 패스워드를 사용하는데 있어 매우 다양한 종류의 보안 키 (DAK, DPW, PPK 등) 생성 방식 및 절차를 정의하고 있다. 또한, 암호화 알고리즘으로는 AES-CBC 또는 1024비트 RSA 방식을 사용하도록 정의하고 있다.

이러한 표준 기술들은 보안의 관점에서 각각의 사용환경을 고려하여 정의하고 있으나, 대부분 대칭키를 활용하는 데이터 암호화에 초점을 맞추고 있다. 따라서 통신이 일어나기 전 기기 간에 인증을 수행한다면 보다 높은 수준의 보안성을 부여 할 수 있을 것이다.

3. IP와 연동되는 PLC 네트워크의 특징

전력 시스템의 광범위하고 계층적인 인프라가 통신 매체로 사용될 경우 그 활용 범위 및 비용의 절감은 매우 크다고 할 수 있을 것이다. 전력선 통신 (Power Line Communication) 기술은 매체 특성으로 인한 몇 가지 단점을 가지고 있지만, 계측 시스템 및 자동 제어 시스템을 위한 가장 유력한 기술로 여겨지고 있다. 유비쿼터스 시대를 위한 통신 기술의 융합 및 발전에 초점이 맞추어져 있는 최근의 개발 동향으로 볼 때 전력선 통신 기술은 매우 중요한 부분을 담당하게 될 것으로 기대되고 있다. UPLC (Ubiqutious Power Line Communication) 프로젝트는 기존에 존재하는 전력선 인프라를 활용해 전력 공급회사에서 소비 가정까지 이르는 계측 및 자동제어 통신 시스템을 설계하고 개발하는데 목적을 두고 있다. 이러한 시스템을 구축함으로써 전력 공급회사는 각 소비 가정의 계측 데이터 (전기, 가스, 수도 등)를 원격에서 수집할 수 있으며, 나아가서는 전력을 포함하는 에너지 소비를 자동 제어할 수 있게 된다.

전신주에 설치되는 IRM은 IP와 PLC 기술을 지원하는 연결 포인트로서의 역할을 하며 기존 IP망과 연결되어 전력회사에 위치하는 관리서버의 제어를 받게 된다. 또한 IRM에 연결되는 모든 Master와 PLC 모뎀은 동일 그룹으로 간주되며, 그룹키를 사용하여 패킷을 암호화한 후 통신한다. 이러한 특징을 반영하여 대칭키 기반의 보안 메커니즘의 관한 연구가 진행되고 있다.

4. IP와 연동된 PLC 네트워크의 보안이슈

IP 네트워크는 그동안 잘 정의된 다양한 보안기술들의 적용으로 어느 정도의 안전성이 확보되었다고 할 수 있다. 그러나, PLC 기술과 같은 새로운 네트워크와 결합될 때 다음과 같은 보안 이슈들이 새롭게 발생하게 된다.

- 인증기관의 부재
- 사용자 인터페이스
- 디바이스 인증

위의 여러 이슈 중에서도 특히 디바이스 인증의 경우 보안적인 측면에서 중요하게 생각되어야 할 부분이다. 즉, 통신이 이루어지기 전에 인가받은 디바이스 인지 상호 확인할 수 있는 기술이 필요하며 이 논문에서는 이부분에 대한 메커니즘을 제안하고자 한다.

5. 기기간 인증 메커니즘

IP와 연동되는PLC네트워크의 특징은 그림 1과 같이 모든 장치들이 직접 혹은 간접적으로 IRM에 접속하고 있다는 것이다.

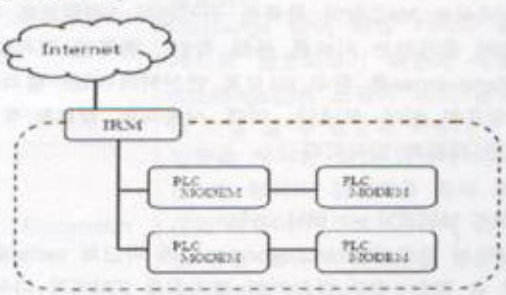

그림 1 IP-PLC 네트워크 구성도

즉 PLC모뎀이 IRM에 직접 접속하거나 다른 PLC모뎀을 리피터로 거쳐서 IRM에 접속하고 있는 것이다. 이것을 이용하여 인증 단계를 2단계로 나누어 설계하였다.

1단계에서는 IRM에 PLC모뎀이 인증을 받는 과정이며, 2단계는 서로 통신을 장치간에 인증을 하는 과정이다. 2단계의 인증에는 1단계의 인증에서 발급받은 비 대칭 키를 사용하여 기기간의 인증을 하도록 하였다.

그림2는 1단계의 인증 메커니즘의 구성도이다.

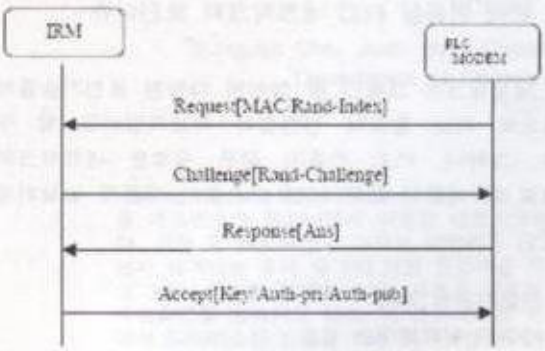

그림 2 IRM-PLC 인증

각 단계별의 세부 동작은 다음과 같다. 여기서 IRM은 사전에 각 모뎀의 MAC과 serial 값을 알고 있다. 그리고 IRM과 각각의 기기는 사전에 합의된 해쉬 함수 H1, H2를 각각 가지고 있으며 암호화 복호화를 위한 비대칭/대칭 키 방식의 알고리즘을 사용 할 수 있다.

① PLC MODEM -> IRM : *MAC/Rand-Index*
PLC 모뎀이 자신의 MAC값과 키 생성에 쓰일 Rand-Index 값을 IRM에게 전송하여 인증을 요청한다.

② IRM -> PLC MODEM : *Rnad-challenge*
IRM에서는 MAC값이 등록된 기기인지 1차적으로 판단(IP망에 존재하는 서버를 통해 확인), 등록된 기기일 경우 Rand-Index를 함수 H1으로 연산하여 나온 결과값으로 암호화 하여 보낸다. 이때 사용되는 암호화/복호화 방식은 대칭키 방식이다.

③ PLC MODEM -> IRM : *Ans*
IRM에서 받은 Rand-challenge 값과 자신의 serial을 더하여 을 함수 H2로 연산하여 결과값을 IRM에게 다시 전송하여 준다.

④ IRM -> PLC MODEM : *Key/Auth-pub/Auth-pri*
Ans값을 확인하여 값이 유효하다면 기기간 인증 시 사용될 key 값과 Auth-pub/AuthPri값을 모뎀에게 전송하여 준다.

여기에서 나온 key값과 Auth-pub/Auth-pri 값은 차후 2단계 인증, 즉 기기간 인증 시 사용될 값이다. 이 key 값과 Auth 값의 갱신 주기를 설정하면 인증의 유효기간을 설정 할 수 있다. Auth-pri는 해당 장치만이 사용할 비밀 키이고 Auth-pub는 공개 키이다.

2단계 인증 메커니즘은 그림 3과 같다.

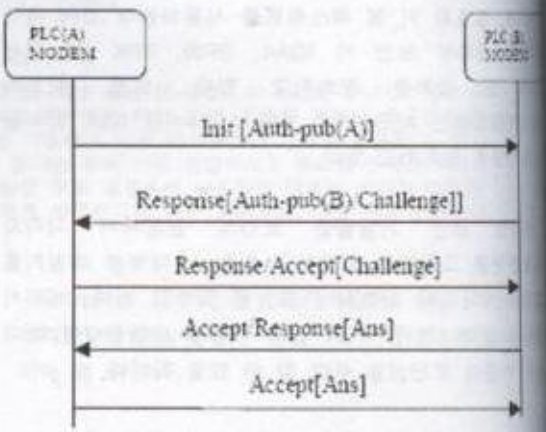

그림 3 기기간 인증

각 기기에는 IRM과 같이 MAC정보가 없기 때문에 MAC를 이용한 1차적인 인증을 사용 할 수 없다. 따라서 1단계 인증에서 발급 받은 key 값을 이용해 대칭 키 방식으로 암호화를 하여 통신을 한다. 그리고 Challenge - Response시 앞서 발급 받은 Auth값을 연산 시 사용하여 유효기간을 판단한다. 즉 Auth값이 서로 다를 경우 올바른 Ans 값을 연산 할 수 없어 서로 인증이 불가능하게 된다. 각각 단계의 자세한 설명은 다음과 같다.

① A -> B : *Auth-pub(A)*
통신을 시작하는 기기 측에서 자신의 Auth-pub값을 수신 측으로 전송하여 준다. 이때 모든 통신은 대칭 키 방식으로 미리 발급받은 key로 암호화 하여 이루어 진다.

B -> A : Auth-Pub(B)/Challenge

신 측에서 넘겨받은 Auth-pub(A)값으로 challenge1 을 암호화 하여 보내준다. 이때 자신의 공개키인 uth-pub(B)도 함께 전송하여 준다. 장치 A는 B의 공개 를 서버에 조회, 현재 받은 공개키가 장치 B가 사용중 인 확인을 한다.

A -> B : *Challenge*

는 Challenge 값을 복호화 하고 자신의 challenge2값 에게 B의 공개키 암호화하여 전송한다.

B -> A : *Ans*

는 넘겨받은 Challenge2값과 challenge1값을 더하여 함수를 거쳐 Ans값을 도출 이를 A로 전송한다. 이 과정은 그림 4와 같다.

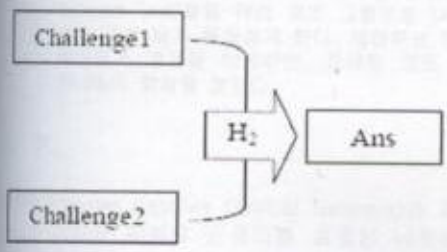

그림 4 Challenge값을 통한 Ans 도출

A -> B : *Ans*

는 Ans를 확인하여 값이 맞을 경우 B와 마찬가지로 Challenge1, Challenge2값을 H2연산을 거쳐 B로 송신 한다.

와 B 인증 시 위의 설명처럼 서로의 challenge값을 공개키로 암호화 하여 교환한뒤 그것을 복호화 후 사전 합의된 H_2 함수를 거쳐 Ans에 입력을 하도록 하였 다. 즉 최종 Ans값은 다음 식과 같이 나타 날 수 있다.

표 1 용어 정의

용어	설명
H	해쉬 함수
$Challenge_A$	A기기의 random challenge 값
$A_{Contents}$	A의 공개 키로 암호화한 Contents
$H(Contents)$	H 해쉬로 연산된 Contents

$$Ans = B_{H(Challenge_A + Challenge_B)}$$
$$\text{or } A_{H(Challenge_A + Challenge_B)}$$

그림 5 Ans 값 계산

Ans 값은 위의 식에서처럼 각 기기에서 생성한 Challenge값에 기반하여 생성이 된다. 그러나 이 값들이 네트워크에 노출 될 경우 replay 공격이나 relay 공격에 취약점을 드러내게 된다. 따라서 본 메커니즘에서는 서버에서 부여받은 비 대칭키를 사용하여 challenge 값을 암호화 하였다. 기기 간에 인증 시 challenge값은 인증 중인 상대방 외에는 아무도 알 수 없는 것이다.

6. 보안성 분석

본 논문에서 제안하고 있는 기기간 인증 메커니즘을 보안적인 측면에서 표 2과 같이 분석할 수 있다.

표 2 제안된 메커니즘의 분석

항목	설명
Freshness	기기간 인증이 수행될 때마다 랜덤한 값을 통한 Challenge-Response 과정을 사용하므로 replay 공격등에 효과적으로 대처 할 수 있다
Authentication	공유하는 해쉬함수를 사용하여 랜덤 값을 결과를 비교하는 방식을 사용한다. 기본적으로 동일한 해쉬함수를 가지고 있는 장비만이 인증을 받을 수 있으나, 공유함수의 노출 및 공격자에 의한 함수의 노출에 추가적인 대비가 필요하다.
Integrity	Challenge 값이 해당 기기의 공개키로 암호화되기 때문에 해당 challenge값이 노출이 되어 공격에 이용 될 수 없도록 하였다.
Encryption	인증을 제외한 모든 단계에서 대칭 키 방식의 암호화를 통해 통신이 이루어 지므로, 기존의 전력선 통신 방식의 취약점인 평문전송 문제를 해결할 수 있다.

Overhead	IRM에서 MAC 리스트를 관리해야 하는 부담이 있으며 주기적으로 Auth 비대칭 키의 값을 갱신해야 하므로, 관리적인 오버헤드가 발생할 수 있으나, 안전한 네트워크를 구축하기 위한 trade-off 과정이라 할 수 있다.

인증 시에만 두 기기가 비 대칭키 방식의 인증을 사용하여 다른 기기에 의한 위장을 방지 할 수 있고 각 모든 기기가 다른 Auth값으로 비 대칭키를 사용하여 인증을 하게 됨으로 기기간 구별이 확실해 진다. 그리고 상대방 기기의 신원을 서버를 통해 확인을 하여 악의적인 기기와의 통신을 사전에 방지 할 수 있다.

7. 결론 및 향후 계획

이상에서 IP와 연동되는 PLC 네트워크에서 기기를 인증하는 메커니즘을 설명 하였다. IP망과 연동이 될 경우 장점은 대량의 MAC관리나 짧은 시간 안에 복잡한 키 생성과 같이 부하가 큰 작업의 경우 IP망에 따로 서버를 두어 IRM에서 직접 처리하지 않고 연산의 결과를 받아오는 식으로 처리가 가능하다는 것이다. 그리고 최초 인증시에만 비 대칭키를 사용하고 나머지 통신에서는 대칭 키를 사용하는 만큼, PLC 기기 상에서도 충분히 구현 가능 하리라 생각된다.

향후 연구로는 본 논문에서 제안한 기기간 인증메커니즘을 시뮬레이션 해보고 실제 장비에 구현하여, 성능을 평가하고 적용가능성을 검토하는 것이다. 또한, 적용과정에서 발생할 수 있는 보안적 문제점의 요구사항을 도출하여 이를 바탕으로 제안된 메커니즘에 반영하는 것이다.

앞으로 위에서 제안된 메커니즘을 구현하여 보고 보완점을 찾아보며, 나아가 인증 이외에 비 대칭 키 생성 및 분배, 그리고 ZigBee 네트워크나 다른 무선 비 IP망과의 연동도 제안, 연구한다.

8. 참고 문헌

[1] HomePlug Specification Version 1.0, http://www.homeplug.org

[2] Standard, "High Speed Power Line Communication MAC and PHY", KS X4600-1, 2006.

[3] Opera Alliance, "OPERA Specification : Technology", Jan. 2006.

[4] Opera Alliance, "OPERA Specification : Syste Jan. 2006.

[5] Man Young LEE, "Internet Security Cryptograp principles, algorithms and protocols", WILEY, 2002.

[6] Albert Treytl, Noel Roberts and Gerhard P. Hancke, "Security Architecture for Power-line Metering System", In proceedings of IEEE Factory Communication Systems 2004, pp. 393-396, September 2004.