



(19) 대한민국특허청(KR)
(12) 등록특허공보(B1)

(45) 공고일자 2012년04월06일
(11) 등록번호 10-1133378
(24) 등록일자 2012년03월28일

(51) 국제특허분류(Int. Cl.)
H04L 9/14 (2006.01) H04L 29/06 (2006.01)
H04L 12/12 (2006.01)

(21) 출원번호 10-2010-0082673

(22) 출원일자 2010년08월25일

심사청구일자 2010년08월25일

(65) 공개번호 10-2012-0019322

(43) 공개일자 2012년03월06일

(56) 선행기술조사문헌

KR1020060025547 A

KR1020100053900 A

KR1020100078559 A

Luigi Lo Iacono, Christoph Ruland, Norbert Zisky, "Secure transfer of measurement data in open systems," Computer Standards & Interfaces, Vol. 28, Issue 3, pp. 311-326. (2006.01.)

(73) 특허권자

삼성전기주식회사

경기도 수원시 영통구 매영로 150 (매탄동)

(72) 발명자

김민규

인천광역시 남구 낙섬중로 102, 유원아파트 2동 501호 (용현동)

한영진

경기도 용인시 수지구 성북2로 126, 성동마을LG빌리지3차아파트 307동 2002호 (성북동)

(74) 대리인

특허법인씨엔에스

전체 청구항 수 : 총 4 항

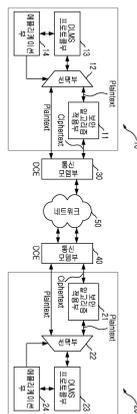
심사관 : 이형일

(54) 발명의 명칭 **보안 기능이 적용된 원격 통신 장치 및 이를 이용한 보안 기능이 적용된 원격 전력 미터링 시스템**

(57) 요약

보안 기능이 적용된 원격 통신 장치 및 이를 이용한 보안 기능이 적용된 원격 전력 미터링 시스템이 개시된다. 상기 보안 기능이 적용된 원격 통신 장치는, 통신 네트워크로부터 수신된 수신 신호가 암호화된 신호인 경우 상기 수신 신호를 복호화하고, 상기 통신 네트워크로 송신하고자 하는 송신 신호를 암호화하는 보안 알고리즘 적용부; 및 상기 수신 신호 또는 상기 보안 알고리즘 적용부에 의해 복호화된 수신 신호를 사전 설정된 통신규약에 따라 변환하고, 상기 사전 설정된 통신규약에 따라 상기 송신 신호를 생성하는 프로토콜부를 포함할 수 있다.

대표도 - 도1



특허청구의 범위

청구항 1

삭제

청구항 2

삭제

청구항 3

원격 미터링을 위한 애플리케이션을 포함하는 제1 애플리케이션부와, 상기 제1 애플리케이션부에서 원격 전력량 계로 전송하고자 하는 제1 데이터 및 상기 원격 전력량계에서 제1 애플리케이션부로 전송된 제2 데이터에 DLMS(Device Language Message Specification) 프로토콜의 규약을 적용하는 제1 프로토콜부와, 상기 DLMS 프로토콜의 규약을 따르는 제1 데이터를 선택적으로 암호화하고, 상기 제2 데이터가 암호화된 데이터인 경우에 상기 제2 데이터를 복호화하는 보안 알고리즘 적용부를 갖는 원격 미터링부;

상기 원격 미터링부에서 통신 네트워크로 상기 제1 데이터를 송신하고 상기 통신 네트워크로부터 상기 제2 데이터를 수신하여 상기 원격 미터링부로 제공하는 제1 통신 모듈부;

전력량 측정을 위한 애플리케이션을 포함하며, 상기 제1 데이터를 입력받고 상기 제2 데이터를 생성하는 제2 애플리케이션부와, 상기 제1 데이터 및 상기 제2 데이터에 상기 DLMS 프로토콜의 규약을 적용하는 제2 프로토콜부와, 상기 DLMS 프로토콜의 규약을 따르는 제2 데이터를 선택적으로 암호화하고, 상기 제1 데이터가 암호화된 데이터인 경우에 상기 제1 데이터를 복호화하는 보안 알고리즘 적용부를 갖는 상기 원격 전력량계; 및

상기 원격 전력량계에서 상기 통신 네트워크로 상기 제2 데이터를 송신하고 상기 통신 네트워크로부터 상기 제1 데이터를 수신하여 상기 원격 전력량계로 제공하는 제2 통신 모듈부를 포함하고,

상기 원격 미터링부는 상기 DLMS 프로토콜이 지원하는 OBIS(object identification system) 코드 중 하나를 암호화 지원 확인용 코드로 작성하여 상기 원격 전력량계로 전송하고, 상기 원격 전력량계가 사전에 상기 암호화 지원 확인용 코드를 갖는 경우 암호화 통신 가능함을 상기 원격 미터링부로 응답하여 암호화 통신을 수행하는 것을 특징으로 하는 보안 기능이 적용된 원격 전력 미터링 시스템.

청구항 4

제3항에 있어서, 상기 원격 미터링부는,

상기 제1 통신 모듈부에서 수신된 상기 제2 데이터가 암호화되지 않은 신호인 경우 상기 제1 통신 모듈부로부터 직접 상기 제2 데이터를 입력받아 상기 제1 프로토콜부로 제공하고, 상기 DLMS 프로토콜의 규약이 적용된 상기 제1 데이터를 상기 제1 보안 알고리즘 적용부 또는 상기 제1 통신 모듈부로 제공하는 제1 신호 선택부를 더 포함하는 것을 특징으로 하는 보안 기능이 적용된 원격 전력 미터링 시스템.

청구항 5

제3항에 있어서, 상기 원격 전력량계는,

상기 제2 통신 모듈부에서 수신된 상기 제1 데이터가 암호화되지 않은 신호인 경우 상기 제2 통신 모듈부로부터 직접 상기 제1 데이터를 입력받아 상기 제2 프로토콜부로 제공하고, 상기 DLMS 프로토콜의 규약이 적용된 상기 제2 데이터를 상기 제2 보안 알고리즘 적용부 또는 상기 제2 통신 모듈부로 제공하는 제2 신호 선택부를 더 포함하는 것을 특징으로 하는 보안 기능이 적용된 원격 전력 미터링 시스템.

청구항 6

제3항에 있어서,

상기 원격 미터링부는 상기 원격 전력량계로 암호화 응답 설정 메시지를 전송하고, 상기 원격 전력량계로부터 상기 암호화 설정 메시지에 대한 응답 준비 메시지를 수신함으로써 암호화 통신을 수행하는 것을 특징으로 하는

보안 기능이 적용된 원격 전력 미터링 시스템.

청구항 7

삭제

명세서

기술분야

[0001] 본 발명은 원격 미터링 기술에 관한 것으로, 더욱 상세하게는 보안 기능이 적용된 원격 통신 장치 및 이를 이용한 보안 기능이 적용된 원격 전력 미터링 시스템에 관한 것이다.

배경기술

[0002] 최근 이슈화되고 있는 스마트 그리드에 관련하여 전력의 효율화 및 보다 진보된 형태의 전력 사용 모니터링을 위한 전자식 전력량계의 개발이 활발하게 진행되고 있다.

[0003] 현재 국내 한국전력을 비롯한 많은 전력회사들이 전자식 전력량계의 보급과 관련하여 원격검침을 위해 국제 통신 프로토콜 규격인 DLMS(Sevice Language Message Specification) 프로토콜을 사용하고 있다. 하지만 DLMS 프로토콜을 사용하는 종래의 전력량계는, 전력량계와 원격 미터링 기기 간의 통신 선로를 통해 데이터 조작 및 변경과 같은 보안상의 문제점을 갖는다.

[0004] 다시 설명하면, DLMS 프로토콜을 이용하여 송수신 되는 데이터는 모두 별도의 가공 없이 분석 가능한 로 데이터 (Raw Data)이다. 따라서, 악의의 목적을 위해 통신이 이루어지는 선로 간의 개입을 통해 로 데이터의 조작 및 변경이 가능한 보안이 취약한 구조를 갖는다. 예를 들어, 통신이 이루어지는 선로에 임의의 단말장치를 연결하여 계량 항목 중 하나인 유효 전력량값을 변경하여 원격 미터링 장치에 송신하게 되는 경우 한국전력과 같은 전력회사는 실제 사용 전력량보다 적은 전력량에 대한 사용요금을 부과하는 경우가 발생하는 문제점이 있다.

발명의 내용

해결하려는 과제

[0005] 본 발명은, 데이터 조작 및 변경과 같은 보안상의 문제를 해결할 수 있는 보안 기능이 적용된 원격 통신 장치 및 이를 이용한 보안 기능이 적용된 원격 전력 미터링 시스템을 제공하는 것을 해결하고자 하는 기술적 과제로 한다.

과제의 해결 수단

[0006] 상기 기술적 과제를 해결하기 위한 수단으로서 본 발명은,

[0007] 통신 네트워크로부터 수신된 수신 신호가 암호화된 신호인 경우 상기 수신 신호를 복호화하고, 상기 통신 네트워크로 송신하고자 하는 송신 신호를 암호화하는 보안 알고리즘 적용부; 및

[0008] 상기 수신 신호 또는 상기 보안 알고리즘 적용부에 의해 복호화된 수신 신호를 사전 설정된 통신규약에 따라 변환하고, 상기 사전 설정된 통신규약에 따라 상기 송신 신호를 생성하는 프로토콜부

[0009] 를 포함하는 보안 기능이 적용된 원격 통신 장치를 제공한다.

[0010] 본 발명의 일 실시형태는, 상기 수신 신호가 암호화되지 않은 신호인 경우 상기 수신 신호를 상기 프로토콜부로 제공하고, 상기 프로토콜부에서 생성된 송신 신호를 선택적으로 상기 보안 알고리즘 적용부 또는 상기 통신 모듈부로 제공하는 신호 선택부를 더 포함할 수 있다.

- [0011] 상기 기술적 과제를 해결하기 위한 다른 수단으로서 본 발명은,
 원격 미터링을 위한 애플리케이션을 포함하는 제1 애플리케이션부와, 상기 제1 애플리케이션부에서 원격 전력량 계로 전송하고자 하는 제1 데이터 및 상기 원격 전력량계에서 제1 애플리케이션부로 전송된 제2 데이터에 DLMS(Device Language Message Specification) 프로토콜의 규약을 적용하는 제1 프로토콜부와, 상기 DLMS 프로토콜의 규약을 따르는 제1 데이터를 선택적으로 암호화하고, 상기 제2 데이터가 암호화된 데이터인 경우에 상기 제2 데이터를 복호화하는 보안 알고리즘 적용부를 갖는 원격 미터링부;
 상기 원격 미터링부에서 통신 네트워크로 상기 제1 데이터를 송신하고 상기 통신 네트워크로부터 상기 제2 데이터를 수신하여 상기 원격 미터링부로 제공하는 제1 통신 모듈부;
 전력량 측정을 위한 애플리케이션을 포함하며, 상기 제1 데이터를 입력받고 상기 제2 데이터를 생성하는 제2 애플리케이션부와, 상기 제1 데이터 및 상기 제2 데이터에 상기 DLMS 프로토콜의 규약을 적용하는 제2 프로토콜부와, 상기 DLMS 프로토콜의 규약을 따르는 제2 데이터를 선택적으로 암호화하고, 상기 제1 데이터가 암호화된 데이터인 경우에 상기 제1 데이터를 복호화하는 보안 알고리즘 적용부를 갖는 상기 원격 전력량계; 및
 상기 원격 전력량계에서 상기 통신 네트워크로 상기 제2 데이터를 송신하고 상기 통신 네트워크로부터 상기 제1 데이터를 수신하여 상기 원격 전력량계로 제공하는 제2 통신 모듈부를 포함하고,
- [0012] 상기 원격 미터링부는 상기 DLMS 프로토콜이 지원하는 OBIS(object identification system) 코드 중 하나를 암호화 지원 확인용 코드로 작성하여 상기 원격 전력량계로 전송하고, 상기 원격 전력량계가 사전에 상기 암호화 지원 확인용 코드를 갖는 경우 암호화 통신 가능함을 상기 원격 미터링부로 응답하여 암호화 통신을 수행하는 것을 특징으로 하는 보안 기능이 적용된 원격 전력 미터링 시스템을 제공한다.
- [0013] 삭제
- [0014] 삭제
- [0015] 삭제
- [0016] 삭제
- [0017] 본 발명의 일 실시형태에서, 상기 원격 미터링부는, 상기 제1 통신 모듈부에서 수신된 상기 제2 데이터가 암호화되지 않은 신호인 경우 상기 제1 통신 모듈부로부터 직접 상기 제2 데이터를 입력받아 상기 제1 프로토콜부로 제공하고, 상기 DLMS 프로토콜의 규약이 적용된 상기 제1 데이터를 상기 제1 보안 알고리즘 적용부 또는 상기 제1 통신 모듈부로 제공하는 제1 신호 선택부를 더 포함할 수 있다.
- [0018] 이와 유사하게, 본 발명의 일 실시형태에서, 상기 원격 전력량계는, 상기 제2 통신 모듈부에서 수신된 상기 제1 데이터가 암호화되지 않은 신호인 경우 상기 제2 통신 모듈부로부터 직접 상기 제1 데이터를 입력받아 상기 제2 프로토콜부로 제공하고, 상기 DLMS 프로토콜의 규약이 적용된 상기 제2 데이터를 상기 제2 보안 알고리즘 적용부 또는 상기 제2 통신 모듈부로 제공하는 제2 신호 선택부를 더 포함할 수 있다.
- [0019] 본 발명의 일 실시형태에서, 상기 원격 미터링부는 상기 원격 전력량계로 암호화 응답 설정 메시지를 전송하고, 상기 원격 전력량계로부터 상기 암호화 설정 메시지에 대한 응답 준비 메시지를 수신함으로써 암호화 통신을 수행할 수 있다.
- [0020] 본 발명의 다른 실시형태에서, 상기 원격 미터링부는 상기 DLMS 프로토콜이 지원하는 OBIS(object identification system) 코드 중 하나를 암호화 지원 확인용 코드로 작성하여 상기 원격 전력량계로 전송하고,

상기 원격 전력량계가 사전에 상기 암호화 지원 확인용 코드를 갖는 경우 암호화 통신 가능함을 상기 원격 미터링부로 응답하여 암호화 통신을 수행할 수 있다.

발명의 효과

[0021] 본 발명에 따르면, 전자 전력량계와 원격 검침 장치 사이에 암호화 통신이 가능하므로 데이터 조작 및 변경과 같은 보안상의 문제를 해결하고 안전한 전자 전력량계의 원격 검침이 가능한 효과가 있다.

도면의 간단한 설명

[0022] 도 1은 본 발명의 일 실시형태에 따른, 보안 기능이 적용된 원격 통신 장치 및 이 보안 기능이 적용된 원격 통신 장치로 구현된 보안 기능이 적용된 원격 전력 미터링 시스템을 도시한 블록 구성도이다.

도 2 및 도 3은 본 발명의 일 실시형태에 따른 보안 기능이 적용된 원격 미터링 시스템의 운용 방법을 도시한 타이밍도이다.

발명을 실시하기 위한 구체적인 내용

[0023] 이하, 첨부된 도면을 참조하여 본 발명의 다양한 실시형태를 보다 상세하게 설명한다. 그러나, 본 발명의 실시 형태는 여러 가지 다른 형태로 변형될 수 있으며, 본 발명의 범위가 이하 설명되는 실시형태로 한정되는 것은 아니다. 본 발명의 실시 형태는 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 본 발명을 보다 완전하게 설명하기 위해서 제공되는 것이다. 따라서, 도면에 도시된 구성요소들의 형상 및 크기 등은 보다 명확한 설명을 위해 과장될 수 있다는 점을 유념해야 할 것이다.

[0024] 도 1은 본 발명의 일 실시형태에 따른 보안 기능이 적용된 원격 통신 장치 및 이 보안 기능이 적용된 원격 통신 장치로 구현된 보안 기능이 적용된 원격 전력 미터링 시스템을 도시한 블록 구성도이다.

[0025] 도 1을 참조하면, 본 발명의 일 실시형태에 따른 보안 기능이 적용된 원격 통신 장치(10, 20)는 보안 기능이 적용된 원격 전력 미터링 시스템에 채용될 수 있다.

[0026] 본 발명의 일 실시형태에 따른 보안 기능이 적용된 원격 통신 장치(10, 20)는 보안 알고리즘 적용부(11, 21)와 프로토콜부(13, 23)를 포함할 수 있다. 더하여, 본 발명의 일 실시형태에 따른 보안 기능이 적용된 원격 통신 장치(10, 20)는 신호 선택부(12, 22)를 더 포함할 수 있다.

[0027] 상기 보안 알고리즘 적용부(11, 21)는 외부의 통신 네트워크(50)로부터 수신된 수신 신호가 암호화된 신호인 경우 상기 수신 신호를 복호화하고, 상기 통신 네트워크로 송신하고자 하는 송신 신호를 암호화하여 원격 통신 장치(10, 20)의 외부로 출력한다. 예를 들어, 상기 보안 알고리즘 적용부(11, 21)는 AES(Advanced Encryption Standard)와 같은 보안 알고리즘을 송신신호에 적용하여 암호화하고, AES 알고리즘을 통해 암호화된 수신 신호를 복호화할 수 있다.

[0028] 상기 프로토콜부(13, 14)는 통신 규약에 따라 수신 신호와 송신 신호를 변환하거나 생성하는 기능을 수행할 수 있다. 본 발명의 일 실시형태에 따른 원격 통신 장치(10, 20)가 원격 미터링 분야에 적용되는 경우, 상기 프로토콜부(13, 14)는 DLMS(Device Language Message Specification) 프로토콜을 적용할 수 있다. DLMS 프로토콜은 원격 미터링에 관한 IEC(International Electrotechnical Commission: 국제전기표준회의)의 국제표준으로 상호 호환성 확보를 목적으로 계량기가 다루고 있는 각종 데이터들을 논리적인 객체로 모델링하고, 이를 표준화된 자료구조로 데이터 메시지를 정의해 다양한 전송매체로 전송방법을 규정한 원격검침용 통신 프로토콜 IEC 국제표준이다.

[0029] 상기 신호 선택부(12, 22)는, 프로토콜부(13, 23)에서 출력되는 송신 신호에 선택적으로 보안 알고리즘을 적용

할 수 있도록, 보안 알고리즘이 필요한 송신 신호를 보안 알고리즘 적용부(11)로 제공하고 보안 알고리즘이 필요하지 않은 송신 신호를 원격 통신 장치(10, 20) 외부로 바로 출력할 수 있다. 또한, 수신 신호 중 복호화가 필요하지 않은 신호를 프로토콜부(13, 23)로 직접 전달할 수 있다.

- [0030] 도 1에서 통신 모델부(30, 40)는 각 원격 통신 장치(10, 20)에서 출력되는 신호를 통신 네트워크(50)를 통해 전달될 수 있도록 신호의 변조 및 복조를 수행하는 블록이다. 또한, 각 원격 통신 장치(10, 20)에 구비된 애플리케이션부(24)는 각 원격 통신 장치가 적용되는 용도에 적합한 기능을 수행하는 블록이다. 예를 들어, 원격 통신 장치(10)가 원격 미터링에 적용되는 경우, 애플리케이션부(14)는 원격 미터링에 필요한 데이터 요청 신호 생성, 수집 데이터 분석, 수집 데이터 집계, 통계 작성 등의 기능을 수행하는 블록이 될 수 있다. 또한, 원격 통신 장치(20)가 전력량계에 적용되는 경우, 애플리케이션부(24)는 전력선으로부터 검출된 전압, 전류를 이용하여 사용되는 전력량(유효, 무효 등)을 검출하고 이를 저장하는 블록이 될 수 있다.
- [0031] 도 1에 도시된 바와 같이, 전술한 것과 같은 원격 통신 장치(10, 20)는 보안 기능을 갖는 원격 검침 시스템에 적용될 수 있다. 도 1을 참조하여, 보안 기능을 갖는 원격 검침 시스템을 설명하면 다음과 같다.
- [0032] 본 발명의 일 실시형태에 따른 원격 검침 시스템에서, 원격 통신 장치 중 하나(10)는 원격 미터링부(10)가 되고 나머지 하나의 원격 통신 장치(20)는 원격 전력량계(20)가 된다. 또한, 본 발명의 일 실시형태에 따른 원격 검침 시스템은, 통신 네트워크(50)를 이용하여 상기 원격 미터링부(10)와 원격 전력량계(20)가 상호 통신할 수 있도록 통신을 위한 제1 및 제2 통신 모델부(30, 40)를 포함할 수 있다.
- [0033] 상기 원격 미터링부(10)는, 원격 미터링을 위한 애플리케이션을 포함하는 제1 애플리케이션부(14)와, 상기 제1 애플리케이션부(14)에서 원격 전력량계(20)로 전송하고자 하는 제1 데이터 및 상기 원격 전력량계(20)에서 제1 애플리케이션부(14)로 전송된 제2 데이터에 DLMS(Sevice Language Message Specification) 프로토콜의 규약을 적용하는 제1 프로토콜부(13)와, 상기 DLMS 프로토콜의 규약을 따르는 제1 데이터를 선택적으로 암호화하고, 상기 제2 데이터가 암호화된 데이터인 경우에 상기 제2 데이터를 복호화하는 보안 알고리즘 적용부(11)를 가질 수 있다.
- [0034] 더하여, 원격 미터링부(10)는, 제1 통신 모델부(30)에서 수신된 상기 제2 데이터가 암호화되지 않은 신호인 경우 제1 통신 모델부(30)로부터 직접 상기 제2 데이터를 입력받아 상기 제1 프로토콜부(13)로 제공하고, 상기 DLMS 프로토콜의 규약이 적용된 상기 제1 데이터를 상기 제1 보안 알고리즘 적용부(11) 또는 상기 제1 통신 모델부로 제공하는 제1 신호 선택부(12)를 더 포함할 수 있다.
- [0035] 상기 원격 전력량계(20)는, 전력량 측정을 위한 애플리케이션을 포함하며, 상기 제1 데이터를 입력받고 상기 제2 데이터를 생성하는 제2 애플리케이션부(24)와, 상기 제1 데이터 및 상기 제2 데이터에 상기 DLMS 프로토콜의 규약을 적용하는 제2 프로토콜부(23)와, 상기 DLMS 프로토콜의 규약을 따르는 제2 데이터를 선택적으로 암호화하고, 상기 제1 데이터가 암호화된 데이터인 경우에 상기 제1 데이터를 복호화하는 보안 알고리즘 적용부(21)를 가질 수 있다.
- [0036] 더하여, 원격 전력량계(20)는, 상기 제2 통신 모델부(40)에서 수신된 상기 제1 데이터가 암호화되지 않은 신호인 경우 상기 제2 통신 모델부(40)로부터 직접 상기 제1 데이터를 입력받아 상기 제2 프로토콜부(23)로 제공하고, 상기 DLMS 프로토콜의 규약이 적용된 상기 제2 데이터를 상기 제2 보안 알고리즘 적용부(21) 또는 상기 제2 통신 모델부로 제공하는 제2 신호 선택부(22)를 더 포함할 수 있다.
- [0037] 상기 제1 통신 모델부(30)는, 상기 원격 미터링부(10)에서 통신 네트워크(50)로 상기 제1 데이터를 송신하고 상기 통신 네트워크(50)로부터 상기 제2 데이터를 수신하여 상기 원격 미터링부(10)로 제공할 수 있다.
- [0038] 이와 유사하게, 상기 제2 통신 모델부(40)는, 상기 원격 전력량계(20)에서 상기 통신 네트워크(50)로 상기 제2 데이터를 송신하고 상기 통신 네트워크(50)로부터 상기 제1 데이터를 수신하여 상기 원격 전력량계(20)로 제공할 수 있다.

- [0039] 도 2 및 도 3은 본 발명의 일실시형태에 따른 보안 기능이 적용된 원격 미터링 시스템의 운용 방법을 도시한 타이밍도이다.
- [0040] 이하, 본 발명의 원격 미터링 시스템의 운용방법에 대해 상세하게 설명한다.
- [0041] 먼저, 도 2를 참조하면, 클라이언트(10), 즉 원격 미터링부에서 연결 요청이 발생하면, 애플리케이션부(14)에서 선택부(12) 및 통신 모듈부(30)를 거쳐 비암호 데이터로 암호화 통신이 가능한지 문의하는 메시지를 서버(20), 즉 원격 전력량계로 전송한다(SSRM: set secure response mode). 이어, 그에 대한 응답으로 서버(20)의 애플리케이션부(24)는 선택부(22) 및 통신 모듈부(40)를 통해 응답 가능하다는 메시지를 비암호화 된 상태로 클라이언트(10)에 전송한다(RR: response ready).
- [0042] 이어, 애플리케이션간 연결을 위한 요청(AARQ: application association request)이 발생하면, 클라이언트(10)에서 암호화된 데이터, 즉 프로토콜부(13)와 신호 선택부(12) 및 보안 알고리즘 적용부(11)를 거친 파라미터 메시지를 서버(20)로 전송하고, 서버(20)에서는 전송받은 상호 연결에 필요한 파라미터를 복호화하여 수신하고 그에 대한 확인 메시지를 암호화하여, 즉 프로토콜부(230), 신호 선택부(22) 및 보안 알고리즘 적용부(21)를 거쳐 클라이언트(10)로 전송한다.
- [0043] 이어, 클라이언트(10)는 DLMS 프로토콜에서 지원하는 OBIS(object identification system) 코드를 암호화하여 데이터를 요청하고 그에 대한 응답으로 서버(20)는 암호화된 데이터, 레지스터값 등을 클라이언트(10)로 전송한다.
- [0044] 이어, 필요한 정보를 모두 수신한 클라이언트(10)는 암호화된 데이터로 연결종료를 요청하고(DISC: disconnection), 서버는 이에 대한 응답을 암호화된 데이터로 클라이언트(10)에 전송함으로써 원격 미터링부와 원격 전력량계의 통신이 종료된다.
- [0045] 한편, 도 3은 도 2와는 다른 형태의 보안 통신 방법을 도시한다. 도 3을 참조하면, 클라이언트(10)는 먼저 비암호 데이터를 이용하여 일반적인 즉 암호화 하지 않는 응답 모드(SNRM: set normal response mode)를 요청하고 서버(20)는 이에 암호화되지 않는 메시지로 응답한다(RR: response ready).
- [0046] 이어, 클라이언트(10)는 통신을 위해 필요한 파라미터를 비암호 데이터로 서버(20)에 전송하고 서버는 이에 대해 암호화 되지 않은 확인 메시지로 응답하여 클라이언트(10)와 서버(20)의 연결이 이루어진다.
- [0047] 이어, 클라이언트(10)는 암호화 통신을 요청하는 OBIS 코드를 비암호화 된 상태로 서버(20)로 전송한다. OBIS 코드는 새로운 기능이 추가되는 경우 이를 지원할 수 있는 구조로 되어 있다. 도 3의 실시형태는 이 OBIS 코드에서 새로운 기능의 확장을 위해 비워둔 코드를 이용하여 암호화를 요청하는 코드로 활용한다. 서버(20)는 암호화 관련 OBIS 코드를 갖고 있는 경우 암호화 통신이 가능하다는 데이터 응답을 하게 되며, 서버(20)가 암호화 통신이 불가능한 경우 비암호화 모드로 통신한다.
- [0048] 이어, 암호화 통신이 가능한 경우, 이어, 클라이언트(10)는 DLMS 프로토콜에서 지원하는 OBIS(object identification system) 코드를 암호화하여 데이터를 요청하고 그에 대한 응답으로 서버(20)는 암호화된 데이터, 레지스터값 등을 클라이언트(10)로 전송한다.
- [0049] 이어, 필요한 정보를 모두 수신한 클라이언트(10)는 암호화된 데이터로 연결종료를 요청하고(DISC: disconnection), 서버는 이에 대한 응답을 암호화된 데이터로 클라이언트(10)에 전송함으로써 원격 미터링부와 원격 전력량계의 통신이 종료된다.
- [0050] 도 2 및 도 3에 도시된 바와 같이, 본 발명은 별도의 암호화 요청 메시지를 송수신하여 암호화 통신을 수행하는 기법과, DLMS 프로토콜이 지원하는 OBIS 코드를 이용하여 암호화 요청을 수행함으로써 암호화 통신을 수행하는 기법으로 구현될 수 있다.
- [0051] 이상에서 설명한 바와 같이, 본 발명은, 전자 전력량계와 원격 검침 장치 사이에 암호화 통신이 가능하므로 데이터 조작 및 변경과 같은 보안상의 문제를 해결하고 안전한 전자 전력량계의 원격 검침이 가능하게 한다.

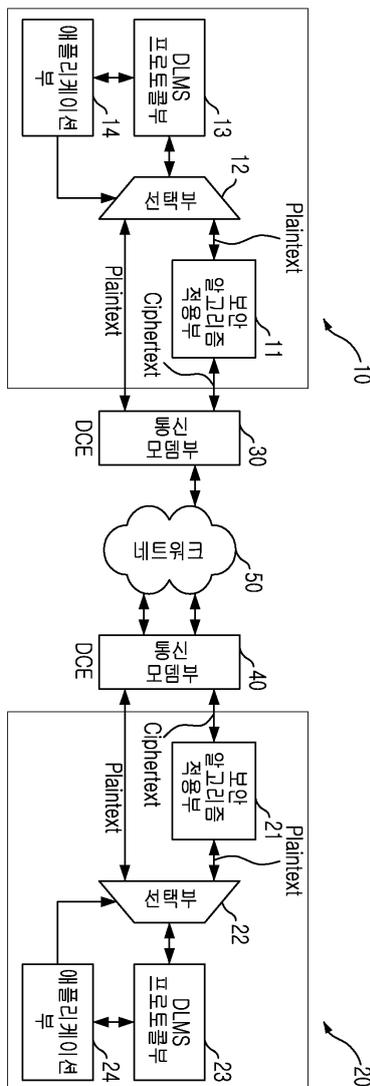
[0052] 발명의 상세한 설명에서는 구체적인 실시예에 관하여 설명하였으나 본 발명의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다. 그러므로 본 발명의 범위는 설명된 실시예에 국한되지 않으며, 후술되는 특허청구의 범위 및 이 특허청구의 범위와 균등한 것들에 의해 정해져야 한다.

부호의 설명

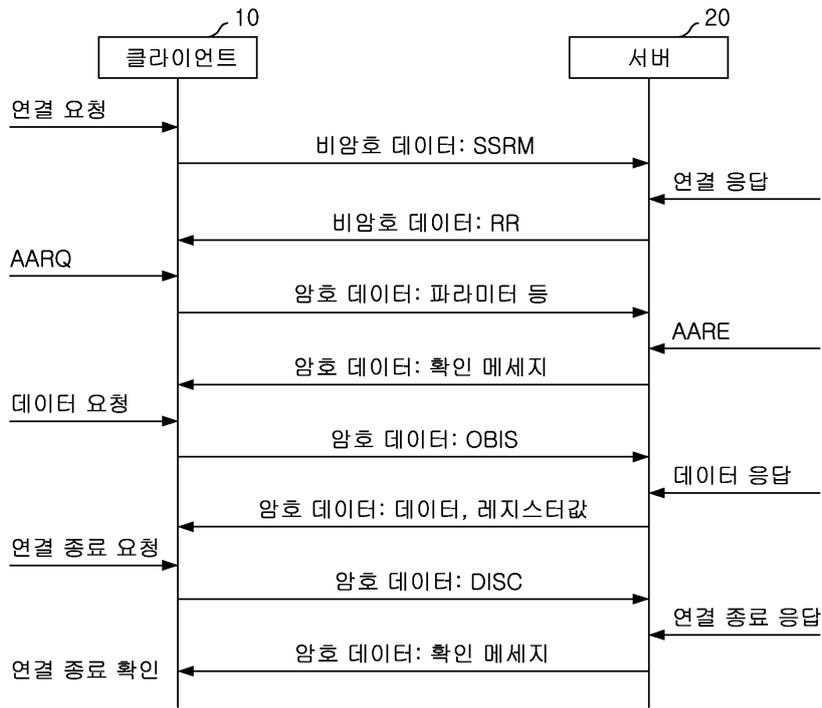
- | | | |
|--------|---------------------|-----------------|
| [0053] | 10: 클라이언트(원격 미터링부) | 20: 서버(원격 전력량계) |
| | 11, 12: 보안 알고리즘 적용부 | 12, 22: 신호 선택부 |
| | 13, 23: 프로토콜부 | 14, 24: 애플리케이션부 |
| | 30, 40: 통신 모듈부 | 50: 통신 네트워크 |

도면

도면1



도면2



도면3

