논문 15-40-05-06 The Journal of Korean Institute of Communications and Information Sciences '15-05 Vol.40 No.05
http://dx.doi.org/10.7840/kics.2015.40.5.815

DNP3에 적합한 발신 부인 방지 기법 제안과 그 구현

유 기 순◆, 송 경 영*, 장 민 호°

Proposal and Implementation on Non-Repudiation of Origin for DNP3

Ki-Soon Yu◆, Kyoung-Young Song*, Min-Ho Jang°

요 약

DNP3는 SCADA 시스템의 대표적인 프로토콜 중 하나이다. IEC 62351에서는 기밀성, 무결성, 가용성, 부인방지·책임추적성을 보안 요구사항으로 들고 있다. 하지만 DNP3 표준인 IEEE Std. 1815에서는 부인방지·책임추적성에 대한 메커니즘을 정의하고 있지 않다. 이에 본 논문에서는 DNP3의 발신자 부인방지 기법을 제안하고, OpenSSL과 스카다시스템 라이브러리를 이용하여 DNP3 발신 부인방지를 구현한다.

Key Words : DNP3, Non-Repudiation of Origin, SCADA, Smart grid, Time synchronization

ABSTRACT

DNP3(Distributed Network Protocol) is one of the most representative protocols which is used in SCADA(Supervisory Control and Data Acquisition) system. IEC 62351 is listing the integrity, confidentiality, availability and non-repudiation or accountability as the security requirement. However, IEEE Std. 1815 that is DNP3 standards does not define a mechanism for non-repudiation or accountability. In this paper, we propose a non-repudiation of origin technique about the sender of critical ASDU and implement the proposed scheme using software such as OpenSSL and SCADA source code library.

Ⅰ. 서 론

정보통신 기술(ICT)의 급속한 발전은 기존의 다른 산업에 많은 영향을 끼치며 발전적 형태의 융합 학문으로 진화했다. 스마트그리드는 종래의 전력기술(Grid)과 정보통신 기술(Smart)을 접목한 것으로 사용자와 공급자가 실시간으로 전력 정보를 교환함으로써 에너지 효율을 최적화하는 차세대 전력망이다. 스마트그리드를 통해 사용자와 공급자간의 양방향 통신이 가능해져 사용자는 합리적 에너지 소비를 할 수 있으며, 공급자는 고품질의 에너지 및 다양한 부가서비스를 제공할 수 있다. 또한, 스마트그리드는 풍력과 태양광 등의 신재생에너지와 전기차 등 녹색기술의 접목 및 확장이 용이한 개방형 시스템으로, 산업간 새로운 융·복합 비즈니스를 창출할 수 있다[1].

스카다(SCADA; Supervisory Control and Data Acquisition) 시스템은 산업 제어시스템으로 전력, 가스, 상하수도, 교통시스템 등 주요 기반시설에 적용되

※ 본 연구는 2013년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (No. 20131020400760)
◆ First Author : Division of Information Communication Engineering, Dongguk University, ykscj39@naver.com, 정회원
° Corresponding Author : School of Electrical and Electronic Engineering, Ulsan College, mhjang@uc.ac.kr, 종신회원
* School of Electrical and Electronic Engineering, Ulsan College, kysong@uc.ac.kr, 종신회원
논문번호 : KICS2015-01-009, Received January 13, 2015; Revised April 20, 2015; Accepted May 11, 2015

어 사용되고 있기 때문에 사고 발생 시 국가 전반에 악영향을 미칠 수 있다. 이러한 이유로 최근 산업 제어시스템에 대한 다양한 침입 및 사이버 공격 가능성에 대한 연구가 활발하게 진행되고 있다[2]. 본 논문에서는 스마트그리드에서 제어신호 전송을 위해 사용되는 스카다 시스템의 보안강화를 위해 발신 부인방지 기법을 제안하고 이를 구현하고자 한다.

DNP3(Distributed Network Protocol)는 스카다 시스템에서 중앙제어장치(Master)와 현장제어장치(Outstation) 간의 데이터와 제어 메시지 전송을 위해 IEEE에서 설계한 표준 전력 프로토콜로 IEC 62351을 기반으로 만들어 졌다. IEC 62351에서는 전력 프로토콜의 보안 요구사항으로 기밀성, 무결성, 가용성, 부인방지·책임추적성을 들고 있다[3]. 이에 반해 DNP3 표준 문서인 IEEE Std 1815에서는 부인방지를 위한 메커니즘을 제공하지 않는다[4].

이에 본 논문에서는 중앙제어장치와 현장제어장치 사이의 통신 중 DNP3 보안 인증(DNP3 Secure Authentication)에서 인증이 필요한 메시지로 지정한 Critical ASDU(Critical Application Service Data Unit) 발신자에 대한 발신 부인방지 기법을 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 부인방지와 관련된 기존의 연구 결과를 소개하고, Ⅲ장에서 DNP3에 적용 가능한 발신 부인방지 기법을 제안한다. 또한, Ⅳ장에서는 본 논문에서 제안한 부인방지 기법을 소프트웨어적으로 구현한다. 마지막으로 Ⅴ장에서 결론을 맺고 향후 연구 계획에 대해 설명한다.

Ⅱ. 관련 연구

2.1 부인방지 메커니즘 분석

부인방지란 통신 참여자 중 하나가 참여 사실을 부인하는 것에 대한 보안 서비스를 말한다. 부인방지의 목적은 사건이나 행위에 대한 증명을 제공하는 것이다. 증명이 제공되기 위해서는 통신 당사자의 식별과 데이터의 무결성이 확인되어야 한다. 부인방지는 다음과 같은 4단계로 구성된다[5].

1) 1단계: 증거생성
2) 2단계: 증거전송, 저장과 검색
3) 3단계: 증거확인
4) 4단계: 논쟁해결

증거는 분쟁을 해결하는 데 사용되는 정보로 부인할 가능성이 있는 통신 당사자가 생성한다. 증거는 증거의 사용자 또는 제3 신뢰 기관(Trusted Third Party; TTP)이 보관할 수 있다. 증거는 메시지 내용, 시간, 날짜, 부인할 가능성이 있는 통신 당사자의 식별 정보를 포함해야 한다.

발신자와 수신자가 직접 통신할 때 제공되는 부인방지로는 발신 부인방지와 수신 부인방지가 있다. 발신 부인방지는 메시지 발신자가 수신자에게 증거를 제공하는 것으로, 수신자는 발신자가 메시지 발신 사실을 부인할 때 증거를 이용해 발신자의 부인 사실을 증명할 수 있다. 수신 부인방지는 메시지 수신자가 발신자에게 증거를 제공하는 것이다. 발신자는 수신자가 메시지 수신 사실을 부인할 때 증거를 이용해 수신자의 부인 사실을 증명할 수 있다[6].

보안 요구사항을 위해 타임스탬프나 전자서명과 같은 보안메커니즘과 대칭 및 비대칭 암호 기술을 부인방지에 사용할 수 있다. KS X ISO/IEC 10181-4에서 다음과 같이 부인방지 메커니즘을 소개하고 있다. 이 메커니즘은 부인방지에 필요한 증거생성과 관련된 것으로 발신 부인방지를 위해 메시지 발신자는 부인방지 메커니즘을 이용해 증거를 생성 후 메시지와 생성한 증거를 함께 전송한다.

가. 제3 신뢰 기관 토큰을 사용하는 부인방지

메시지 발신자는 메시지를 제3 신뢰 기관에게 보내 증거 생성을 요청한다. 제3 신뢰 기관은 자신만이 알고 있는 비밀키로 해당 메시지에 대한 증거를 생성한다.

나. 보안 토큰과 변형 억제 모듈을 사용한 부인방지

변형 억제 모듈은 증거 생성 및 확인하는 제한된 기능만을 수행하는 것으로 메시지 발신자의 변형 억제 모듈은 증거를 생성하는 데 사용된다. 메시지 수신자와 판결관의 변형 억제 모듈은 발신자가 생성한 증거를 확인하는 데 사용된다.

다. 전자서명을 이용한 부인방지

전자서명은 서명키로 생성된다. 수신자는 확인키를 사용해 생성된 전자서명을 확인할 수 있다. 확인키는 인증서에서 얻을 수 있으며, 인증서는 제3 신뢰 기관의 전자서명으로 보증 받는다. 그러므로 인증서의 유효성 확인을 위해 제3 신뢰 기관의 인증서도 필요하다.

라. 타임스탬프를 이용한 부인방지

제3 신뢰 기관이 전자서명한 타임스탬프를 제공하는 것으로 부인방지를 위해 신뢰할 수 있는 시간 참조값을 요구할 때 사용된다. 타임스탬프는 메시지 발신자의 서명키가 노출되기 전에 서명되었음을 보장한다.

표 1. 부인방지 메커니즘 비교
Table 1. Comparison of non-repudiation mechanisms

mechanism / items[7]	security envelope	trusted platform module	digital signatures	time stamp	using TTP	notarization
role of TTP	evidence generation	verification evidence	certificate generation and assurance	time stamp generation	delivery	notary
involvement of TTP	on-line	off-line	off-line	on-line	in-line	on-line
number of messages exchanged	3	1	1	2	3	-
non-Repudiation of receipt	×	×	×	×	×	○
fairness	×	×	×	×	×	×

마. 제3 신뢰 기관을 이용한 부인방지

메시지 발신자와 메시지 수신자 사이에서 제3 신뢰 기관은 모든 데이터를 중개하는 중개자 역할을 한다. 제3 신뢰 기관은 부인방지에 필요한 증거를 직접 관리하므로 분쟁 발생 시 해결을 위한 증거를 제공한다.

바. 공증을 이용한 부인방지

메시지의 특성을 확보하여 기록함으로써 증거를 생성한다. 공증인은 분쟁 발생 시 증거의 정당성을 확인해 준다.

표 1은 부인방지 메커니즘을 비교한 표이다. 제3 신뢰 기관의 통신 참여도를 나타내는 제3 신뢰 기관에 대한 의존도는 3단계로 다음과 같이 나눌 수 있다[8].

- In-line : 제3 신뢰 기관이 중개자 역할을 하며 부인방지에 필요한 증거를 직접 생성 및 관리
- On-line : 공증인처럼 제3 신뢰 기관은 증거 생성에 직접 참여
- Off-line : 인증서 발행자처럼 제3 신뢰 기관은 부인방지를 간접적으로 지원

본 논문에서는 발신 부인방지를 위해 제3 신뢰 기관에 대한 의존도와 프로토콜 통신량이 적은 부인방지 메커니즘을 사용하고자 한다. 보안 토큰과 변형 억제 모듈을 사용한 부인방지 메커니즘의 경우 별도의 소프트웨어적 설치나 하드웨어가 필요하므로 전자서명을 이용한 부인방지 메커니즘을 이용한 발신 부인방지 기법을 제안하고자 한다.

2.2 DNP3 분석

지리적으로 떨어진 위치에 있는 중앙제어장치와 현장제어장치는 시간동기화를 통해 동일한 시간을 유지하고 있다. 그림 1은 LAN환경에서 현장제어장치의 시간동기화 방법을 보여주고 있다[4].

1) 중앙제어장치는 RECORD_CURRENT_TIME 전송 시 메시지의 마지막 옥텟이 이더넷 하드웨어를 떠나는 시간을 기록한다. 시점 [A]가 이를 나타낸다.
2) 현장제어장치는 메시지의 마지막 옥텟이 이더넷 하드웨어에 도착하는 시간을 기록한다. 시점 [B]가 이를 나타낸다.
3) 현장제어장치는 NULL로 응답한다.
4) 중앙제어장치는 시점 [A]의 시간을 기록한 WRITE 메시지를 전송한다.
5) 현장제어장치는 WRITE 메시지에 기록된 시간과 시점 [B]와 시점 [C]사이의 시간차를 이용하여 수식 (1)과 같이 현재 시간을 설정한다.

$$\text{설정시간} = \text{WRITE 시간정보} + (\text{시점 [C]} - \text{시점 [B]}) \quad (1)$$

위와 같은 과정을 통해 현장제어장치는 주기적으로 시간동기화를 수행한다[9]. IIN(Internal Indications) 필드는 어플리케이션 헤더에서 현장제어장치의 특정 상태 또는 오류 상태를 나타내는데 사용된다. 현장제어장치가 시스템을 재시작하였거나 임의 시간동기화가 필요한 경우 어플리케이션 헤더 값인 IIN1.4비트를 설정해 중앙제어장치에게 시간동기화를 요청할 수 있다. 여기서 IIN1.4비트를 설정한다는 것은 IIN 필드

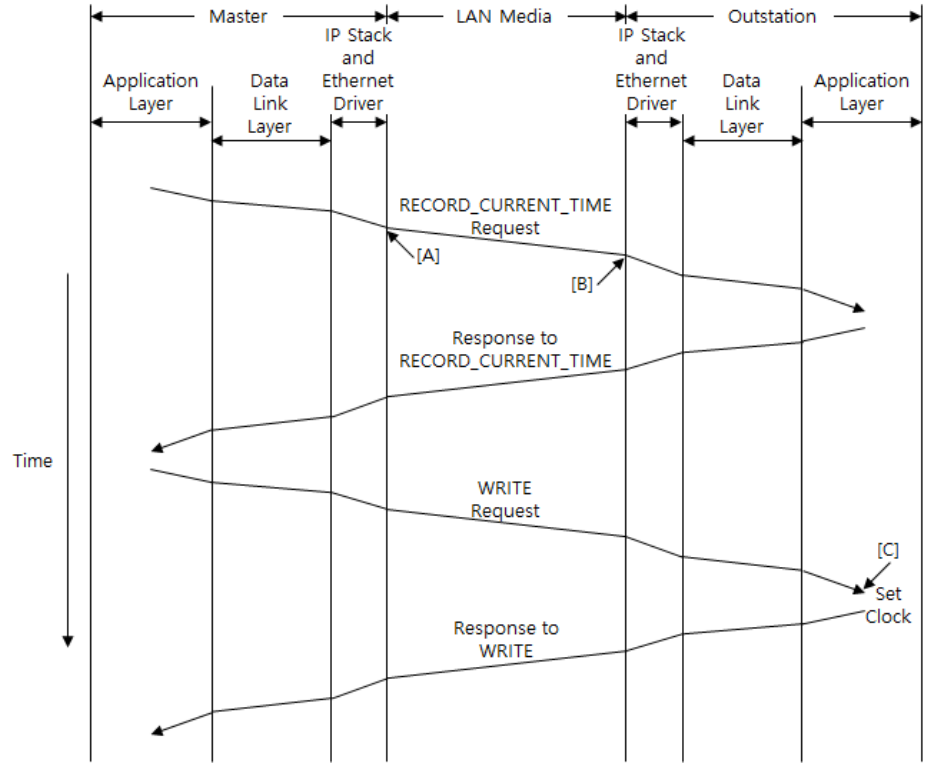


그림 1. LAN 환경에서 시간동기화 방법
Fig. 1. Timing of LAN time synchronization

의 첫 번째 옥텟, 네 번째 비트(NEED_TIME)의 설정을 의미한다. 하지만 빈번한 시간동기화 요청은 시스템의 부하를 발생시키기 때문에 발신 부인방지에서 시간동기화를 위한 임계치 값을 적정하게 설정해야 한다[4].

DNP3 보안 인증에서는 Critical ASDU 발신자에 대한 인증과정을 시도 응답 모드(Challenge Response Mode)(그림 2)와 적극적 모드(Aggressive Mode)(그림 3)로 설명하고 있다[4].

시도 응답 모드에서 Critical ASDU를 수신한 인증 요구자(Challenger)는 해당 메시지에 대한 인증 요청 메시지(Authentication Challenge)를 전송한다. 그림 4는 인증 요청에 사용되는 오브젝트 구조를 보여준다.

1) Challenge Sequence Number : 인증 시퀀스
2) User Number : 사용자 정보
3) MAC Algorithm : HMAC (Keyed-Hash Message Authentication Code) 알고리즘 정보

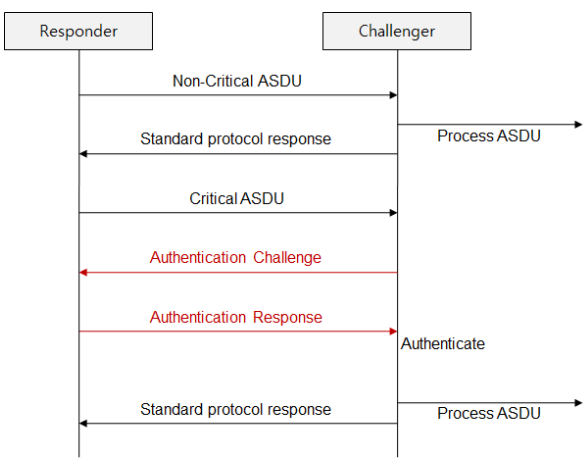


그림 2. 시도 응답 모드
Fig. 2. Challenge Response Mode

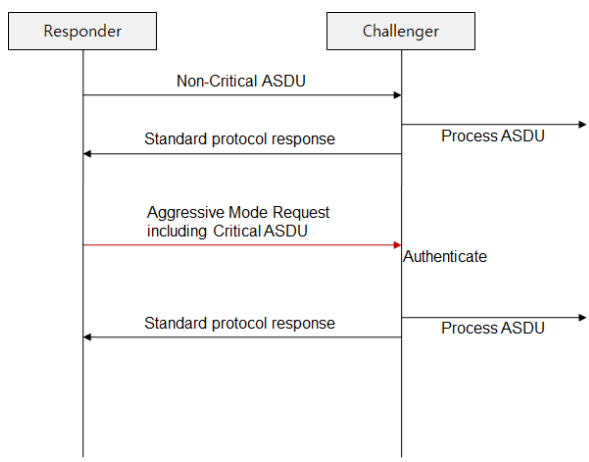


그림 3. 적극적 모드
Fig. 3. Aggressive Mode

Challenge Sequence Number	User Number	MAC Algorithm	Reason for Challenge	Challenge Data
4byte	2byte	1byte	1byte	4byte 이상

그림 4. 인증 요청에 사용되는 오브젝트 구조
Fig. 4. Object structure of Authentication Challenge

Challenge Sequence Number	User Number	Critical ASDU	MAC Value
4byte	2byte	...	16byte 이상

Fig. 5. Object structure of Aggressive Mode Request
그림 5. Aggressive Mode Request에 사용되는 오브젝트 구조

4) Reason for Challenge : HMAC 계산에 사용할 데이터 지정, 1인 경우 인증 요청 메시지와 Critical ASDU를 이용해 HMAC을 계산
5) Challenge DATA : 랜덤 값, 최소 4바이트 이상 사용

인증 요청 메시지를 수신한 인증 검증자(Responder)는 지정된 데이터로 HMAC을 계산한 후 인증 응답 메시지(Authentication Response)를 전송한다. 인증 요구자는 수신한 HMAC과 직접 계산한 HMAC을 비교하여 일치하는 경우 Critical ASDU를 처리한다.

적극적 모드에서 인증 검증자는 Critical ASDU 전송 시 인증정보도 함께 전송한다. 적극적 모드에서 세션키 변경 후 첫 번째 Critical ASDU는 시도 응답 모드로 인증을 거쳐야 한다. 인증 검증자는 이 때 수신한 인증 요청 메시지와 전송하고자 하는 적극적 모드에서의 요청 메시지(Aggressive Mode Request)를 이용해 HMAC을 계산한다[4]. 그림 5는 적극적 모드에서의 요청 메시지의 오브젝트 구조를 보여주고 있다.

다음 장에서 2가지 인증모드를 사용한 발신 부인방지 기법을 제안하고자 한다.

Ⅲ. DNP3의 발신 부인방지 기법 제안

현재 DNP3 보안 인증에서는 HMAC을 사용해 메시지의 인증 및 사용자 인증 기능을 제공하고 있다. HMAC 생성 시 메시지 발신자는 메시지 수신자와 공유하고 있는 비밀키를 이용해 HMAC을 생성함으로 자신이 올바른 메시지 생성자임을 증명 할 수 있어 공격자의 위장 공격을 예방 할 수 있다. 또한, 메시지의 무결성을 증명 할 수 있어 공격자의 변조 공격을 예방할 수 있다. 하지만, HMAC을 통한 메시지 인증 코드만으로는 발신자를 식별할 수 없어 제3자에게 발신자가 보낸 메시지임을 증명하는 것과 부인방지를 지원할 수 없다. 본 장에서는 전자서명을 이용해 Critical ASDU 발신자에 대한 발신 부인방지를 기법을 제안하고자 한다. 발신 부인방지는 2가지 인증모드에서 제공된다. 표 2는 발신 부인방지에 사용할 표기법을 정

표 2. 표기법
Table 2. Notation

Notation	Explanation
REQU	Request
RESP	Response
CASDU	Critical Application Service Data Unit
AUCH	Authentication Challenge
LAUCH	Recently received Authentication Challenge
AURE	Authentication Response
AMR	Aggressive Mode Request
CSQ	Challenge Sequence Number
USR	User Number 0 : Outstation 1 : Master
MAL	Hash algorithm
RFC	Reason for Challenge 1 : Critical 2, …, 255 : reserved value
r	Pseudo-Random Challenge Data
t_C	Challenger's present time, 'YYYYMMDDhhmmss'
t_R	Responder's present time, 'YYYYMMDDhhmmss'
TH	Threshold of time difference
TD	Time difference between Challenger and Responder
$H()$	Hash function, Computes a message digest of the n bytes
h	Hash value
$E()$	Encryption function
$D()$	Description function
K_S	Session key
$PRIV\_R$	Responder's private key
PUB_R	Responder's public key
$PRIV\_C$	Challenger's private key
PUB_C	Challenger's public key
AH	Application Header
OH	Object Header

리한 것이며 다음 사항들을 가정하고 있다.

1) 중앙제어장치와 현장제어장치는 각각 인증기관(Certificate Authority; CA)으로부터 발급받은 공개키와 개인키 쌍을 가지고 있다.
2) 중앙제어장치와 현장제어장치는 서로의 인증서를 가지고 있다.
3) 중앙제어장치와 현장제어장치의 인증서는 유효한 상태이다.
4) 중앙제어장치의 시간은 조작할 수 없는 신뢰할 수 있는 시간이다.
5) 현장제어장치는 중앙제어장치로부터 시간동기화 정보를 얻고 있다.
6) 중앙제어장치와 현장제어장치는 부인방지에 사용할 시간차의 임계치를 공유하고 있다.

3.1 시도 응답 모드의 발신 부인방지

시도 응답 모드에서 발신 부인방지를 위한 메시지 교환은 그림 6과 같은 단계로 이루어진다.

CASDU를 수신한 인증 요구자는 RFC 필드 값을 2로 설정해 인증 검증자가 AUCH, CASDU, TD를 이용해 해시 값을 계산 할 수 있도록 한다. 인증 검증자가 TD를 계산하기 위해서는 인증 요구자의 시간정보가 필요하므로 'YYYYMMDD hhmmss' 형태의 t_C를 추가하여 전송한다. 그림 7과 그림 8은 각각 AUCH와 AURE의 메시지 구조를 나타낸 것이다.

인증 검증자는 수신한 t_C와 자신의 현재시간 정보를 이용해 TD를 계산한다. AUCH, TD, CASDU를 이용해 해시를 계산하고 개인키로 전자서명한 후 AURE를 전송한다. 전자서명은 인증기능을 포함하므로 HMAC이 아닌 해시 값으로 계산한다. 인증 요구자는 수신한 해시 값과 직접 계산한 해시 값을 비교하여 일치하면 CASDU를 처리한다. 단, 인증 요구자가 현장제어장치이고, TD가 TH보다 큰 경우 현장제어장치는 자신의 현재시간과 수신한 TD를 이용해 임의의 시간동기화를 아래 수식 (2)와 같이 진행한 다음 CASDU를 처리한다.

$$\text{설정시간} = \text{현재시간} \pm TD \tag{2}$$

3.2 적극적 모드의 발신 부인방지

적극적 모드에서 발신 부인방지를 위한 메시지 교환(그림 9)은 다음과 같은 단계로 이루어진다.

1) 현재 전달하고자 하는 CASDU로 구성된 REQU에 인증 검증자는 발신 부인방지를 위해 메시지에

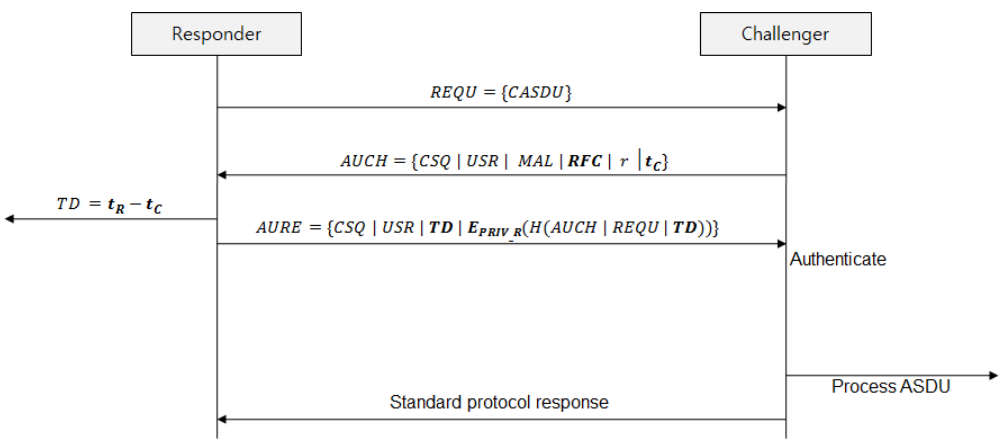


그림 6. 시도 응답 모드에서 발신 부인방지를 위한 메시지 교환
Fig. 6. Non-repudiation of origin of Challenge Response Mode

AH	OH	*CSQ*	*USR*	*MAL*	*RFC*	*r*	t_C
4byte	...	4byte	2byte	1byte	1byte	4byte	14byte

그림 7. AUCH 메시지 구조
Fig. 7. Message structure of AUCH

AH	OH	*CSQ*	*USR*	*TD*	*E(h)*
4byte	...	4byte	2byte	2byte	256byte

그림 8. AURE 메시지 구조
Fig. 8. Message structure of AURE

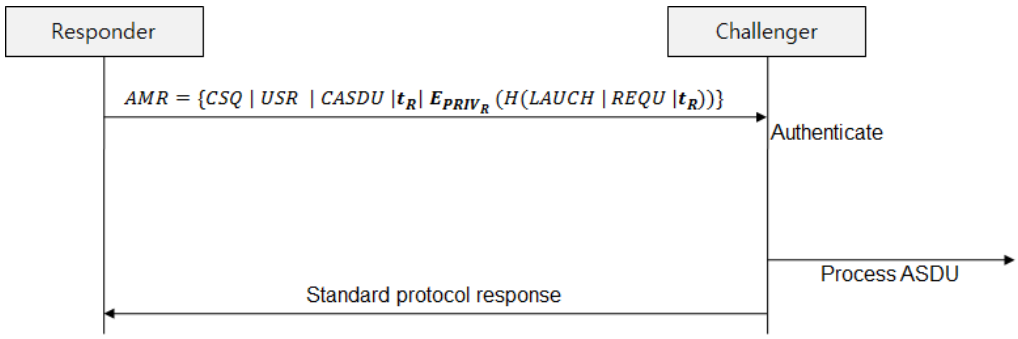


그림 9. 적극적 모드에서 발신 부인방지를 위한 메시지 교환
Fig. 9. Non-repudiation of origin of Aggressive Mode

'YYYYMMDDhhmmss' 형태의 t_R를 추가한 후 LAUCH와 REQU 그리고 t_R을 이용해 해시 값을 계산한 다음 개인키로 암호화하여 전자서명을 한다. 이렇게 만들어진 AMR을 인증 요구자에게 전송한다. 그림 10은 AMR의 메시지 구조를 나타낸다.

2) 인증 요구자는 수신한 해시 값과 직접 계산한 해시 값을 비교하여 이 값들이 일치하면 수신한 CASDU를 처리하게 된다. 단, 인증 요구자가 현장제어장치이고 인증 검증자의 인증이 완료되면, 수신한 t_R과 자신의 현재시간 정보를 이용해 TD를 계산한다. 계산한 TD가 TH보다 크면, 시도 응답 모드와 마찬가지로 수신한 t_R을 이용해 임의의 시간동기화를 다음 수식 (3)과 같이 진행한 다음 CASDU를 처리한다.

$$\text{설정시간} = t_R \tag{3}$$

위와 같이 2가지 모드에서 증거를 수신한 인증 요구자는 텍스트 파일을 이용해 증거를 저장한다. 저장 방식은 선입선출(FIFO; First-In First-Out) 방식을 따르며 저장 가능한 증거의 개수를 사용자 임의로 지정할 수 있다. 저장 가능한 증거의 개수가 100개라고 할 때 101번째의 증거를 저장하기 위해 1번째의 증거를 삭제하고 101번째 증거를 저장한다.

증거자료로 해시 값과 해시 값 생성 시 사용했던 메시지, 암호문을 복호화할 때 사용한 인증서 정보를 저장한다.

Ⅳ. DNP3의 발신 부인방지 구현

본 장에서는 TRIANGLE MICROWORKS사의 Source Code Library와 OpenSSL 1.0.1g를 이용해 발신 부인방지를 구현하고자 한다. DNP3 Secure Authentication은 Version 5(SAv5)를, 해시 알고리즘은 SHA-256, 공개키는 RSA 2048를 사용한다.

4.1 시도 응답 모드의 발신 부인방지 구현

시도 응답 모드에서 인증 요구자의 발신 부인방지 과정을 그림 11에서 보여주고 있다. 그림 11에서 06:35:52.948은 장치의 로컬시간으로 밀리 세컨드 단위까지 나타낸다. 앞서 설명한 바와 같이, 시도 응답 모드에서 발신 부인방지를 위해 인증 요구자는 AUCH 전송 시 RFC 필드 값을 2로 설정하고, t_C를 추가하여 전송한다. 이는 그림 11의 [A]에 해당되며, 기존의 인증 요청 메시지에 시간 정보를 추가하고 RFC 필드 값을 변경한 것이다.

인증 검증자는 수신한 t_C와 자신의 현재시간 정보로 계산한 TD와 AUCH, CASDU로 해시 값을 계산하여 전자서명을 한 다음 AURE를 전송한다. 이는 그림 11의 [B]에 해당되며, 기존의 인증 응답 메시지에 인증 요구자와 인증 검증자의 시간 차이 정보인 TD를 추가하고, HMAC 대신 해시 값을 얻은 뒤 인증 검증자의 개인키로 전자서명한다.

검증을 위해 인증 요구자는 인증 검증자의 공개키로 복호화한 해시 값과 직접 계산한 해시 값을 비교한다. 이 값이 일치하면 인증 요구자는 증거자료를 저장하고 CASDU를 처리한다. 이는 그림 11의 [C]에 해

AH	OH	*CSQ*	*USR*	*CASDU*	*t*	*E(h)*
2byte	...	4byte	2byte	...	14byte	256byte

그림 10. AMR 메시지 구조
Fig. 10. Message structure of AMR

```
06:35:52.948: ===> Slave      Application Header, Select
06:35:52.948:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 11
06:35:52.948:                 cb 03 0c 01 28 01 00 00 00 03 01 00 00 00 00 00
06:35:52.948:                 00 00 00 00
06:35:52.948:       Slave     Outstation Authentication Event, state=IDLE  event=CRITICAL_RCVD

06:35:52.948: <+++ Slave      Build DNP3 Message: Authentication Challenge

06:35:52.948:                 Tx Object 120(Authentication), variation 1, qualifier 0x5b(16 Bit Free Format)
06:35:52.948:                 Tx Authentication Challenge, User = 0, Sequence = 4,
                              Algorithm = 4-SHA256 16 OCTET, Reason 2-NONREPUDIATION |

06:35:52.948: <+++ Slave      Insert request in queue: Authentication Challenge

06:35:52.948: <=== Slave      Application Header, Authentication Response
06:35:52.948:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 11
06:35:52.948:                 cb 83 00 00 78 01 5b 01 1a 00 04 00 00 00 00 00
06:35:52.948:                 04 02 34 22 7e ac 32 30 31 35 30 34 30 36 30 36
06:35:52.948:                 33 35 35 32

06:35:53.962: ===> Slave      Application Header, Authentication Request
06:35:53.962:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 11
06:35:53.962:                 cb 20 78 02 5b 01 08 01 04 00 00 00 64 00 00 01
06:35:53.962:                 08 92 5a 6e 2b 56 42 50 15 5b c3 13 31 a0 10 91
06:35:53.962:                 9f 60 4b 51 0a 6a ed 4c fd 4b 74 a6 60 11 6b 9f
06:35:53.962:                 c0 3e 85 f4 c2 a8 ae bb ad 13 44 73 b5 bd de 3c
06:35:53.962:                 f1 1d 56 10 03 58 24 8c 70 ec 2c d4 4b 14 96 07
06:35:53.962:                 12 68 15 e8 36 c6 f9 5b 81 f5 02 b2 ab db a2 18
06:35:53.962:                 d1 0d 01 99 d5 ef 00 20 08 af 6e d4 cc 58 57 24
06:35:53.962:                 29 9b f6 01 85 af 5f 3d 3f a5 7a 77 47 f2 a6 4c
06:35:53.962:                 1e 68 90 85 3d b4 d9 81 74 a7 89 b9 2f 5a ba 8a
06:35:53.962:                 70 df e9 d4 bb 40 54 8f 23 10 f0 42 0b a8 6e 1b
06:35:53.962:                 87 b6 f0 16 21 47 a7 c7 5d 74 41 09 41 1a 43 01
06:35:53.962:                 cb 63 8a 8f ad 0f e7 94 b3 e2 35 70 d7 9f 59 37
06:35:53.962:                 93 3b 8d e0 1a fa 30 e7 84 c7 a2 38 8e 3e 49 d1
06:35:53.962:                 cc 2e a9 d3 1e 50 e7 f7 af cc 19 5f 40 e6 94 48
06:35:53.962:                 e2 c4 4e 06 9d 7f c6 e4 c3 55 a8 89 02 90 2d ff
06:35:53.962:                 9a ab 43 b9 cb 8f d9 fe 52 f2 13 90 80 87 37 d8
06:35:53.962:                 d6 df d0 df 38 17 60 ee e7 a0 3f d1 91 83 2a 61

06:35:53.962:                 Rx Object 120(Authentication), variation 2, qualifier 0x5b(16 Bit Free Format)
06:35:53.962:       Slave     Outstation Authentication Event, state=WAITFORREPLY  event=CHALLENGE_REPLY
06:35:53.962:                 Authentication, plain text
06:35:53.962:                 cb 83 00 00 78 01 5b 01 1a 00 04 00 00 00 00 04
06:35:53.962:                 02 34 22 7e ac 32 30 31 35 30 34 30 36 30 36 33 35
06:35:53.962:                 35 32 00 01 cb 03 0c 01 28 01 00 00 00 03 01 00 00
06:35:53.962:                 00 00 00 00 00 00 00

06:35:53.962:                 Authentication, hashed text
06:35:53.962:                 de 43 92 37 6e d9 d0 85 fc df ec ba 40 ca 19 7b

06:35:54.962:                 Rx Authentication Reply, User = 100, Sequence = 4 SUCCESS

06:35:54.962: <+++ Slave      Insert request in queue: Select Response

06:35:54.962: <=== Slave      Application Header, Response
06:35:54.962:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 11
06:35:54.962:                 cb 81 00 00 0c 01 28 01 00 00 00 03 01 00 00 00
06:35:54.962:                 00 00 00 00 00 00
```

[A] [B] [C] [D]

그림 11. 시도 응답 모드에서 인증 요구자의 발신 부인방지 과정
Fig. 11. Process of doing Non-repudiation of origin of the challenger in Challenge Response Mode

No	AUCH	TD	CASDU	Digital Signature	Certification Serial Number	Writing Time
062	cc 83 00 00 78 01 ... 35 35	00 00	cc 04 ... 00	8e 5a ... 29 62	A13A02F8C2937C0E	06Apr15 06:35:56.990
061	cb 83 00 00 78 01 ... 35 32	00 01	cb 03 ... 00	08 92 ... 2a 61	A13A02F8C2937C0E	06Apr15 06:35:53.962
060	c7 83 10 00 78 01 ... 34 31	00 00	c7 02 ... 01	0a b0 ... 6b 59	A13A02F8C2937C0E	06Apr15 06:35:42.760

그림 12. 시도 응답 모드에서 발신부인 방지의 증거
Fig. 12. Evidences of Non-repudiation of origin in Challenge Response Mode

당되며, 해시 값을 비교하여 동일한 경우에는 증거자료를 저장한 뒤 CASDU를 처리하고, 동일하지 않은 경우에는 에러 처리를 하게 된다. 이때, 인증 요구자가 현장제어장치이고 TD가 TH보다 큰 경우에는 임의로 시간동기화를 수행한 다음 CASDU를 처리한다.

그림 12는 발신 부인방지의 증거자료를 저장한 결과를 보여주고 있다. 증거자료 순번, AUCH, TD, CASDU, 전자서명 값, 인증서의 시리얼 넘버, 증거 기록 시간을 저장하였다. 그림 11의 [D]는 CASDU를 모두 처리한 다음 응답 메시지를 전송하는 부분이다.

4.2 적극적 모드의 발신 부인방지 구현

그림 13은 적극적 모드에서 인증 검증자의 발신 부인방지 과정을 나타낸 것이다. 발신 부인방지를 위해 적극적 모드에서 인증 검증자는 전송하고자하는 CASDU로 이루어진 REQU에 인증 검증자의 시간 정보인 t_R을 추가한다. 그림 13의 [A]가 이를 나타낸다. LAUCH, REQU, t_R을 이용해 계산한 해시 값을 개인키로 암호화한 다음 AMR을 전송한다. 그림 13의 [B]가 이것을 나타낸다. 그림 13의 [C]는 인증 요구자에게 전송 받은 응답 메시지이다.

인증 요구자는 직접 계산한 해시 값과 수신한 해시 값이 일치하는 경우 증거자료를 저장하고 CASDU를 처리한다. 시도 응답 모드와 마찬가지로 인증 요구자가 현장제어장치이고 TD가 TH보다 크면 현장제어장치는 임의로 시간동기화를 수행한 후 CASDU를 처리한다.

그림 14는 적극적 모드에서 증거를 저장한 결과이다. 증거자료 순번과 LAUCH, CASDU, t_R, 전자서명 값으로 구성된 AMR, 인증서의 시리얼 넘버, 증거 기록 시간을 저장하였다. 본 장에서는 전자서명과 DNP3 보안 인증을 기반으로 한 발신 부인방지가 시도 응답 모드와 적극적 모드에서 정상적으로 작동되는 것을 확인하였다.

메시지 발신자와 수신자가 공유하고 있는 비밀키를 사용해 생성한 HMAC을 이용하여 수신자는 제3자에게 이것이 발신자가 보낸 메시지임을 증명 할 수 없었다. 하지만, 메시지의 해시 값을 발신자가 개인키로 전자서명함으로써 메시지의 무결성이 확인되고, 통신 당사자를 식별할 수 있게 되어 메시지 수신자는 발신자의 메시지 발신 사실을 검증자에게 증명할 수 있게

```
Issue Binary Output Command for Session 0
size : 305

08:57:33.888: <+++ DNP Master Build DNP3 Message: Binary Command

08:57:33.888:                 Tx Object 120(Authentication), variation 3,
                              qualifier 0x07(8 Bit Limited Quantity)

08:57:33.888: <+++ DNP Master Insert request in queue: Binary Command                    [A]

08:57:33.888:                 Tx Object 120(Authentication), variation 9, qualifier 0x5b(16 Bit Free Format)
08:57:33.888:                 Authentication, plain text
08:57:33.888:                 c7 83 10 00 78 01 5b 01 0c 00 03 00 00 00 00 00 04
08:57:33.888:                 01 05 9e d5 cf cb 03 78 03 07 01 04 00 00 00 64 00
08:57:33.888:                 0c 01 28 01 00 00 00 03 01 00 00 00 00 00 00 00
08:57:33.888:                 00 78 09 5b 01 10 00 32 30 31 35 30 34 30 38 30 38
08:57:33.888:                 35 37 33 33

08:57:33.888:                 Authentication, hashed text
08:57:33.888:                 be 16 16 03 bb 8c 20 c9 8f b8 5a 4a a8 3c 9d 3b

08:57:33.997:                 Tx Authentication Aggressive Mode Request, User = 100, Sequence = 4

08:57:33.997: <=== DNP Master Application Header, Select
08:57:33.997:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 11
08:57:33.997:                 cb 03 78 03 07 01 04 00 00 00 64 00 0c 01 28 01
08:57:33.997:                 00 00 00 03 01 00 00 00 00 00 00 00 00 78 09
08:57:33.997:                 5b 01 10 00 32 30 31 35 30 34 30 38 30 38 35 37
08:57:33.997:                 33 33 30 02 21 d5 0e 70 64 42 f1 b5 e1 b7 10 06
08:57:33.997:                 ee 62 44 95 eb 88 be 7a 4c f9 44 6d 4f 0a 95 b4
08:57:33.997:                 f3 49 e2 01 a0 b0 dd ab 96 44 67 62 4c 80 14 c3
08:57:33.997:                 58 c5 68 df d5 07 dd fb c3 08 c2 a5 a5 d6 d2 fe
08:57:33.997:                 60 ea 58 1b e1 0f 4c c0 d5 1b 92 c1 a7 e2 37 92   [B]
08:57:33.997:                 74 e4 43 64 32 d3 ee 13 01 7c a7 a3 f9 62 bc bb
08:57:33.997:                 41 0d 4e 20 72 04 69 46 47 74 3f b0 d3 a8 6c 30
08:57:33.997:                 b3 ba 2a 34 a5 a6 02 db 0f e1 e1 f3 c9 cc 54 65
08:57:33.997:                 c7 c8 41 05 fa 77 54 76 48 68 b3 0f d3 2a 92 60
08:57:33.997:                 d5 29 89 68 ed 50 5e 43 13 29 90 08 3f f7 92 78
08:57:33.997:                 bb 0d b9 87 cf 66 68 2f d3 79 bf 28 59 52 36 c0
08:57:33.997:                 73 87 33 7a 94 a6 97 fc 8a ee 14 42 c5 ed 4c 85
08:57:33.997:                 0a 60 74 d2 c6 96 23 87 bd c1 26 1d de 60 6d bc
08:57:33.997:                 25 1a 4e 73 2a 4f b6 de 2f af 03 db 23 67 4b 0f
08:57:33.997:                 68 02 45 66 bf a5 4a d9 84 67 86 22 2e 2f 6d 0f
08:57:33.997:                 b7 eb 43 68 1c f7 64 fa 20 7c 13 a6 20 b0 f4 d3
08:57:33.997:                 6b fe
Event Poll for Session 0

08:57:34.075: <+++ DNP Master Build DNP3 Message: Event Class Poll

08:57:34.075: <+++ DNP Master Insert request in queue: Event Class Poll

08:57:34.574: ===> DNP Master Application Header, Response
08:57:34.574:                 FIR(1) FIN(1) CON(0) UNS(0) SEQ# 11
08:57:34.574:                 cb 81 00 00 0c 01 28 01 00 00 00 03 01 00 00 00   [C]
08:57:34.574:                 00 00 00 00 00 00
08:57:34.574:       DNP Master Master Authentication Event, user=0 state=IDLE  event=NONCRITICAL_RCVD
```

그림 13. 적극적 모드에서 인증 검증자의 발신 부인방지 과정
Fig. 13. Process of doing Non-repudiation of origin of the responder in Aggressive Mode

No	AMR				Certification Serial Number	Writing Time
	LAUCH	CASDU	t_R	Digital Signature		
005	c7 83 10 00 78 01 ... d5 cf	c5 03 ... 00	32 30 ... 33	56 24 ... 8f 78	A13A02F8C2937C0E	08Apr15 08:58:13.949
004	c7 83 10 00 78 01 ... d5 cf	c0 03 ... 00	32 30 ... 33	42 a2 ... d8 14	A13A02F8C2937C0E	08Apr15 08:57:53.746
003	c7 83 10 00 78 01 ... d5 cf	cb 03 ... 00	32 30 ... 33	30 02 ... 6b fe	A13A02F8C2937C0E	08Apr15 08:57:33.575

그림 14. 적극적 모드에서 발신부인 방지의 증거
Fig. 14. Evidence of Non-repudiation of origin in Aggressive Mode

되었다. 또한, 증거 생성 시 메시지 내용 및 시간 정보를 포함으로써 수신자는 향후 발생할 수 있는 메시지 발신자의 부인을 예방할 수 있게 되었다.

V. 결 론

IEC 62351에서는 전력 통신 프로토콜의 보안 요구사항으로 기밀성, 무결성, 가용성, 부인방지·책임추적성을 들고 있다. 하지만 DNP3 표준에서는 부인방지를 위한 기법이 소개되어 있지 않다. 이에 본 논문에서는 DNP3의 발신 부인방지 기법을 찾아보고자 하였으며, 공개키 기반의 전자서명과 DNP3 보안 인증을 이용한 발신 부인방지를 제안하였다. 이 기법은 기존 프로토콜에서 인증을 위해 사용하였던 2가지 인증모드를 이용해 발신 부인방지 기법을 제안하였다. 제안된 기법은 기존 DNP3의 변경을 최소화한 형태로 Critical ASDU 발신자에 대한 부인방지를 제공한다. 발신자가 Critical ASDU에 대한 증거를 생성해 수신자에게 전송하면, 수신자는 전송받은 증거를 저장함으로써 앞으로 발신자가 발신 사실을 부인함으로 발생할 수 있는 분쟁을 해결할 수 있게 된다.

하지만 제안된 기법은 시도 응답 모드에서는 인증 요구자의 시간을 기준으로 증거를 생성하고 적극적 모드에서는 인증 검증자의 시간을 기준으로 증거를 생성한다는 문제점을 가지고 있다. 또한, 인증 요구자가 현장제어장치인 경우 잦은 임의의 시간동기화가 발생할 수 있으며, 적극적 모드에서 임의의 시간동기화를 할 경우 전송지연으로 인해 잘못된 시간으로 시간동기화를 할 수 있다는 문제점을 가지고 있으므로, 이를 해결하기 위한 추가적인 연구가 필요하다.

References

[1] S.-I. Hwang, T.-J. Park, Y.-K. Sohn, and G.-P. Jeon, "Smart grid use case and service requirement based on M2M: Energy management system for public buildings," *J. KICS,* vol. 38C, no. 7, pp. 612-620, Jul. 2013.

[2] H. Yoo, J.-H. Yun, and T. Shon, "Whitelist-based anomaly detection for Industrial control system," *J. KICS,* vol. 38B, no. 8, pp. 641-653, Aug. 2013.

[3] IEC, *IEC/TS 62351-1:2007(E),* 2007.

[4] IEEE Power and Energy Society, *IEEE Std. 1815:2012,* 2012.

[5] KATS, *KS X ISO/IEC 10181-4:2013,* 2013.

[6] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[7] M. Seo, et al., "On the standard mechanism for non-repudiation services," in *Proc. CISC'99,* vol. 9, no. 1, pp. 228-240, Nov. 1999.

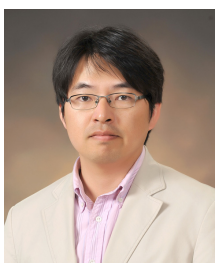
[8] J. Zhou and D. Gollmann, "An efficient non-repudiation protocol," *Computer Security Foundations Workshop,* pp. 126-132, Jun. 1999.

[9] J.-H. Lee and S.-J. Lee, "An accuracy improvement on acquisition time of SCADA RTU status event," *Trans. KIEE,* vol. 62, no. 3, pp. 332-341, 2013.

유 기 순 (Ki-Soon Yu)

2007년 2월 : 안동대학교 전자공학과 졸업
2015년 2월 : 동국대학교 국제정보대학원 정보보호학과 석사
2015년 3월~현재 : 동국대학교 정보통신공학과 박사과정
<관심분야> 정보통신, 정보보호

송 경 영 (Kyoung-Young Song)



2004년 2월 : 고려대학교 전기전자전파공학부, 수학과 졸업
2010년 8월 : 서울대학교 전기컴퓨터공학부 박사
2010년 8월~2012년 2월 : LG 전자 선임연구원
2012년 3월~현재 : 울산과학대학교 전기전자공학부 조교수
<관심분야> 스마트그리드 보안, 생체신호처리, MIMO 통신

장 민 호 (Min-Ho Jang)

2002년 8월 : 연세대학교 전기전자공학부 공학사
2004년 8월 : 서울대학교 전기컴퓨터공학부 공학석사
2009년 2월 : 서울대학교 전기컴퓨터공학부 공학박사
2009년 3월~2011년 8월 : 삼성전자 DMC연구소 책임연구원
2011년 9월~현재 : 울산과학대학교 전기전자공학부 조교수
<관심분야> 디지털통신, 이동통신시스템, 오류정정부호, OFDM, 정보보호