정 보 보 호 학 회 지
제24권 제3호, 2014. 6

전력 제어시스템에서 안전한 보안 인증을 위한 메커니즘 소개

박 준 용*, 민 남 홍**, 하 기 웅**, 유 기 순**, 송 경 영***

요 약

최근 전력 제어시스템의 자동화 효율(Automation Efficiency)과 상호운용성(Interoperability)을 높이기 위해 공개된 표준 프로토콜과 상용 시스템을 사용하게 되었고 외부망과의 연결 필요성이 증가됨에 따라 SCADA 시스템에 대한 공격 위협성이 증가하고 있다. 그러나 전력 제어시스템의 중앙제어장치(Master)와 현장 운영장치(Outstation) 간 데이터를 교환하기 위한 통신 규격인 DNP(Distributed Network Protocol) 프로토콜은 보안을 고려하지 않고 개발되어 통신규격 자체에 보안 취약점을 가지고 있었고, 제어시스템에 대한 사이버 위협 요소도 크게 증가하고 있다. 정보통신 기술의 발전과 개방형 망이 갖는 장점을 취하기 위하여 DNP3 프로토콜은 TCP/IP 네트워크를 지원하게 되었고, TCP/IP 네트워크가 가지고 있는 기존의 보안 취약점(Vulnerability)이 전력 제어시스템 및 통신망에 그대로 이전되고 있어 중앙제어장치와 현장운영장치 간에 DNP3 표준에서 제시한 사항 외에 추가적인 보안 메커니즘이 요구된다. 본 논문에서는 SCADA 시스템이 보안성을 갖고 안전하게 운용되기 위한 IEEE DNP3 표준과 ISO/IEC TC57 WG15에서 권고하고 있는 IEC 62351 표준의 인증 및 암호화 메커니즘을 소개한다.

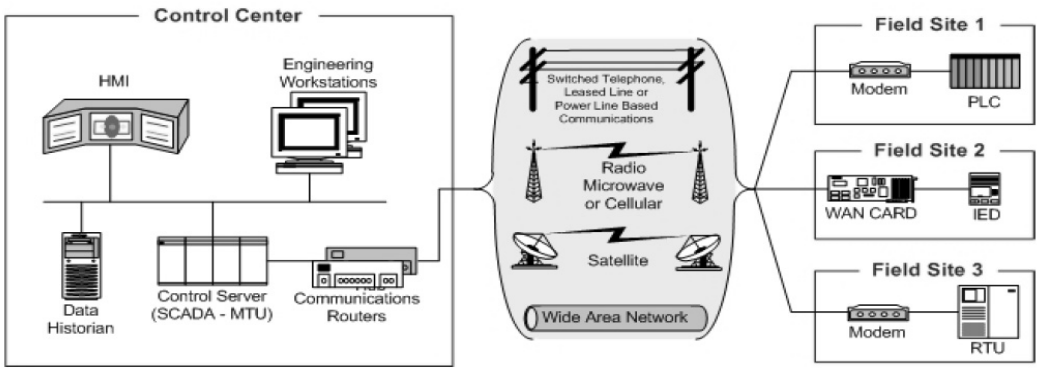
Ⅰ. 서 론

전력 제어시스템(Power Control System)은 SCADA (Supervisory Control and Data Acquisition) 시스템을 통해 전기, 가스, 수도, 교통 등 국가기반 핵심시설에 연계된 전력설비의 운전 상태를 감시하고 설비에 부착된 센서를 통해 실시간으로 여러 데이터를 취득 및 제어할 수 있다.

전력 제어시스템의 주요 구성은 [그림 1]에서처럼 통신 경로상의 아날로그 또는 디지털 신호를 사용하여 중앙통제센터(Master Terminal Unit : MTU)와 필드 사이트에 연계된 원격 장치의 상태정보 데이터를 원격소장치(Remote Terminal Unit : RTU), 지능형 전력 장비(Intelligence Electronic Device : IDE), 자동화제어장치(Programmable Logic Controllers : PLC)로부터 수집, 기록, 표시하여 중앙 제어시스템이 현장에 운영되는 원격장치를 감시하고 제어하는 시스템이다[1].

과거의 SCADA시스템은 특화된 제어시스템 전용 프로토콜을 사용하여 외부망과 분리된 독립·폐쇄형 망을 구성하여 사이버 공격으로부터 안전하다고 판단하였으나, 비즈니스 목적상 자동화 효율과 상호운용성을 높이기 위해 외부망과의 연결 필요성이 대두됨에 따라 공개된 표준과 상용 시스템을 사용하면서 SCADA시스템에 대한 공격 위협성이 증가하고 있다. 또한, 사이버 테러로 인해 전력 제어시스템 장애가 발생 시 그 파급효과는 사회적, 경제적 대규모 혼란을 야기할 수 있어 사이버 테러의 주요 목표가 되고 있으며 지속적으로 공격시도가 증가하는 추세이다. 전력 제어시스템의 중앙 제어장치(Master)와 현장 운영장치(Outstation) 간 데이터를 교환하기 위한 통신 규격인 DNP(Distributed Network Protocol) 프로토콜은 보안을 고려하지 않고 개발되어 통신규격 자체에 보안 취약점을 가지고 있었고, 2010

본 연구는 2013년도 산업통상자원부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다.
(No. 20131020400760)
* 동국대학교 공과대학 정보통신공학과 (park1jun@naver.com)
** 동국대학교 국제정보대학원 정보보호학과 모바일 클라우드보안 전공 (gsiai@dongguk.edu)
*** 울산과학대학교 전기전자공학부 (kysong@uc.ac.kr), 교신저자



〔그림 1〕 전력 제어시스템의 일반적인 구성

년과 2012년의 개정을 통해 IEEE Std. 1815(DNP3) 표준은 보안 인증과 키 교환 메커니즘을 제시하고 있다. DNP3 프로토콜이 TCP/IP 네트워크를 기반으로 동작하는 경우, 기존 다른 연구자들에 의해 DNP3의 보안 취약점에 대한 연구들이 발표된 바와 같이 [2, 3] TCP/IP 네트워크가 가지고 있는 기존의 보안 취약점(Vulnerability)이 전력 제어시스템 및 통신망에 그대로 이전되고 있어 중앙 제어장치와 현장 운영장치 간에 DNP3 표준에서 제시한 사항 외에 추가적인 보안 메커니즘이 요구된다.

본 논문에서는 전력 제어시스템에서 보안 인증에 관련된 프로토콜 및 취약점을 알아보고 DNP3 프로토콜의 패킷을 분석한 다음 전력 제어시스템에 안전하게 접속하기 위한 인증 및 암호화 메커니즘을 소개하고자 한다. 이를 위한 본 논문은 다음과 같이 구성된다. Ⅱ장에서는 보안 인증 프로토콜 및 전력 제어시스템 취약점에 대해 알아보고, Ⅲ장에서는 DNP3 제어 프로토콜의 패킷 구조를 분석한 후, Ⅳ장에서는 보안 인증 및 암호화 메커니즘을 소개하고 Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 연구

2.1 보안 인증 구현 프로토콜

보안 인증 구현 프로토콜이란, 네트워크망에서 사용자 인증 또는 기기 인증과 관련되는 보안서비스를 제공하는 프로토콜로써 현재까지 네트워크 시스템에서 사용되는 주요 인증 방식은 Challenge-Response, Digital Signature, Transformed Passwords, Time Synchronous 방식이 있다[4].

- Challenge-Response

사용자의 인증을 위해 User의 ID와 패스워드를 사용하는 대신 질문(Challenge)과 응답(Response)을 이용한다. 사용자는 인증서버에 PIN(Personal Identification Number)을 전송하고 서버는 난수(Challenge)를 생성하여 사용자에게 전송한다. 이때 사용자는 암호화키를 미리 지정된 패스워드로 해싱(Hashing)하여 재전송(Response)하고 서버는 원래 질문을 본인의 패스워드로 해싱하여 사용자가 보낸 값(Response)과 비교하여 동일할 때 사용자를 인증하는 방식이다.

- Digital Signature

인감 날인, 사인(서명) 같은 기능을 전자적으로 구현한 디지털 기술로 메시지마다 계산에 의해 디지털 서명을 다르게 만들어 서명 효과를 구현하는 방식이다. 또한 문서에 기재되는 서명의 위조 방지 보다는 서명이 된 후 그 문서에 대해 변경행위의 검출에 주안점을 둔 것이며, 전자문서 내용에 대한 암호화가 아닌 서명자가 진짜 서명자임을 증명하고 작성 내용이 위·변조되지 않았음을 작성자가 부인할 수 없도록 증명하는 방식이다. 디지털 서명의 주요 조건은 인증(Authentication), 위·변조 불가능성(Integrity), 부인의 불가능성(Non-repudiation), 재사용 불가능성(Uniqueness), 진위확인 가능성(Availability)이 갖추어져야 한다.

〔표 1〕 전력 제어시스템의 위협 분석

구 분	설 명
공격자 (Attacker)	실력 과시 및 스릴을 위해 네트워크 침입을 시도할 수 있다. 현재 공격 스크립트 및 프로토콜을 인터넷을 통해 쉽게 구할 수 있기 때문에 전문적인 지식 없어도 쉽게 공격을 수행할 수 있다.
봇-넷 (Bot-network)	공격을 조직화하고 피싱, 스팸, 악성코드를 유포하여 해커가 마음대로 제어할 수 있는 좀비 PC들이다.
피셔 (Phishers)	금전적 이익을 목적으로 스팸, 스파이웨어/멀웨어를 이용하여 계정 탈취 및 정보 취득을 시도한다.
스팸 전파자 (Spammers)	상품 판매, 피싱 수행, 스파이웨어/멀웨어 유포, DoS 공격 수행을 위해 수신인이 원하지 않는 잘못된 정보 및 정보를 숨긴 이메일을 퍼뜨린다.
내부자 (Insiders)	불만을 품은 내부 직원은 사이버 범죄의 주요근원이다. 내부자는 목표 시스템에 제한 없이 접근을 할 수 있기 때문에 풍부한 지식 없이도 정보를 획득하거나 시스템 침해를 야기할 수 있다. 내부 위협은 내부 직원뿐 아니라 아웃소싱 벤더 및 비즈니스 파트너 등도 포함되며, 불완전한 정책, 절차, 테스팅은 제어시스템에 영향을 줄 수 있다. 제어시스템의 침해사고는 내부자의 실수로 인해서도 높은 확률로 발생한다.
범죄 조직 (Criminal groups)	조직적인 범죄조직이나 산업스파이 등은 신원도용 및 온라인 도용을 위해 스팸, 피싱, 스파이웨어/멀웨어를 이용하여 금전적 이익을 목적으로 공격을 수행할 수 있다
테러리스트 (Terrorists)	국가안보를 위협하기 위해 제어시스템을 파괴하거나 불능상태로 만든다. 이것은 다수의 사상자를 유발하고, 국가 경제에 타격을 주며, 국가 신뢰도에 영향을 미친다.
산업스파이 (Industrial spies)	기업 기밀에 대한 지적자산 및 노하우 취득을 목적으로 한다.

• Transformed Passwords

로그인 할 때마다 그 세션에서만 사용 가능한 일회성 패스워드를 생성하여 사용자에 대한 로그인 정보 유출을 최소화하기 위한 방식이다. 변형 패스워드 방식은 단방향 해시함수 H를 도입하여 위 패스워드 방식의 문제점을 해결하고 있다. 즉 사용자의 식별 정보 ID와 패스워드를 해시함수 H를 이용하여 해시 한 후 전송함으로서, 제 3자에 의한 도청(Eavesdropping)을 방지하고 동시에 전송 시 노출에 대한 예방을 하고 있다. 또한 패스워드 재전송(Replay)을 방지함과 위해 랜덤값 R을 사용하고, 서버 인증 정보 공격을 막기 위해 해시된 정보를 그대로 저장함으로서 안전성을 획득하고 있다. 현재 변형된 패스워드를 제공하는 솔루션은 OTP(One Time Password)가 있다.

• Time Synchronous

특정한 시각을 나타내는 문자열로써 통상적으로 세계표준시(UTC)의 자정으로부터 밀리 초(ms) 단위로 표시하며, 특정한 시각을 나타낼 때 마다 64bit의 비밀키가 생성되어 각각의 사용자에게는 특정키가 할당되어지고 지능형 토큰과 인증서버 데이터베이스에 저장되어진다. 사용자가 로그인 할 때 PIN과 6개의 숫자로 된 난수를 전달하면 난수는 토큰 내부에 저장되어 있던 비밀키와 T를 초기 값으로 하여 토큰 내부의 알고리즘을 통해 인증키를 생성하며 서버는 PIN을 인덱스로 하여 해당 비밀키를 찾고 생성된 6개의 난수들을 수신한 것과 시간 일치 여부를 통하여 사용자를 인증하는 방식이다.

2.2 전력 제어시스템의 보안 위협 분석

전력 제어시스템에 대한 보안 위협은 공격자, 봇넷, 피셔, 스팸 전파자, 테러리스트, 산업스파이, 내부자 등에 의한 악의적인 위협과 시스템 복잡성, 사람에 의한 실수 및 사고, 장치 고장 및 자연재해와 같은 다양한 위협 인자에 의해 발생할 수 있다. 이러한 위협으로부터 제어시스템을 보호하기 위해서는 심층 방어(defense-in-depth) 전략을 수립할 필요가 있다. 전력 제어시스템에 공격을 수행할 가능성이 있는 악의적인 위협의 유형은 [표 1]과 같다[5].

〔표 2〕 제어 프로토콜 보안 취약점

구 분	설 명
DNP3	특정 통신 프로토콜이 제한한 최대 길이를 초과하거나 길이 필드의 값과 다르게 설정된 패킷을 보냄으로써 메모리 용량이 초과됨(Buffer overflow)
Modbus	인증 또는 암호화 메커니즘이 없기 때문에 다양한 function code들을 이용하여 Victim을 제어함
MMS/ICCP	인증 또는 암호화 메커니즘이 없기 때문에 메시지 변조 공격, 중간자 공격, 재생공격이 가능함
GOOSE	메시지 인증 및 암호화를 제공하지 않기 때문에 중간자 공격이나 메시지 변조가 가능함

2.3 전력 제어시스템의 보안 취약점 분석

전력 제어시스템이 가지는 취약점은 아래와 같이 네 가지 분류의 취약성으로 구분할 수 있다[4].

• 정책 및 절차

제어시스템 보안에 관한 정책 및 구현가이드(절차)가 불완전/부적절하거나 없는 경우에서 오는 취약성이다. 보안 정책 및 절차, 관리 지원은 보안의 기초다. 보안 정책은 패스워드 정책 또는 제어시스템에 연결되는 모뎀 등에 대한 보안 요구사항을 권고함으로써 취약성을 완화시킬 수 있다.

• 플랫폼

하드웨어, OS, 제어시스템 애플리케이션을 포함하는 플랫폼의 결함, 잘못된 구성 또는 부실한 유지보수에서 오는 취약성이다. 이러한 취약성은 OS 및 애플리케이션 패치, 물리적 접근통제와 보안 소프트웨어(예를 들어, 백신)와 같은 다양한 보안 통제를 통해 완화될 수 있다.

• 네트워크

제어시스템의 네트워크의 결함, 잘못된 구성 또는 부실한 관리와 다른 네트워크와의 연결성으로 인하여 발생하는 취약점이다. 이러한 취약성은 심층 네트워크 설계, 통신 암호화, 네트워크 트래픽 제한, 네트워크 컴포넌트에 대한 물리적인 접근통제와 같은 보안 통제를 통해 제거 또는 완화될 수 있다[5].

• 제어 프로토콜

SCADA에서 사용되는 제어 프로토콜(DNP3, Modbus, MMS/ICCP, GOOSE 등) 별 다양한 보안 취약점이 존재한다. [표 2]는 상용 제어 프로토콜에 대한 보안 취약점을 정리한 것이다[6].

Ⅲ. DNP3 패킷 구조 및 분석

DNP3는 주로 원격지에 위치한 현장 운영장치로부터 정보수집, 제어명령 송신을 목적으로 하는 SCADA시스템에 최적화되어 설계된 표준 통신 프로토콜이다. DNP3는 중앙 제어장치[1]와 현장 운영장치[2]의 통신 흐름을 정의한 표준으로 전력, 수도, 가스 등 국가주요 기반시설간의 상호운용성(Interoperability) 확보를 위해 개발되었다.

DNP3는 전력산업에 사용할 목적으로 Harris사[3]에 의해 IEC 60870-5 프로토콜을 기반으로 개발된 최초의 전력시스템 전용 프로토콜이었으나 그 소유권이 1993년 DNP 사용자 그룹으로 이전되면서 공개적으로 사용되기 시작했다. 2010년, DNP3는 IEEE Standard for Electric Power System Communications로 제정되어, IEEE Std 1815™-2010으로 배포되었고, 2012년 재개정되었다[7].

DNP3는 초기 DNP 버전을 시장 환경의 변화에 맞게 개선하고 전 세계 전력회사의 90%가 사용하고 있을 정도로 가장 보편적으로 사용되고 있는 산업 표준(De

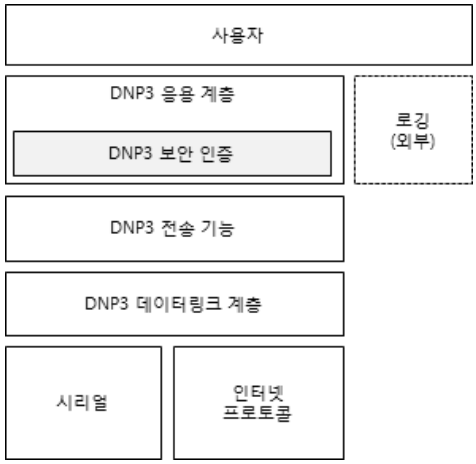
1) 중앙 제어장치(Master) : HMI, Control System
2) 현장 운영장치(Outstation) : PLC, RTU, IED
3) Harris Corporation : 1895년에 미국 Ohio Cleveland에서 설립되어 1960년대 후반부터 전자, 통신 등을 중심으로 현재 RF Communications, Government Communications Systems, Broadcast Communications의 3개로 분류되어 있는 통신 단말 전문회사 (http://www.harris.com/)

Facto Industry Standard)프로토콜이다.

DNP3는 [그림 2]의 구조로 구성되어 있으며, IEC TC57 WG3에서 SCADA 통신을 위해 제안한 EPA(Enhanced Performance Architecture)를 사용한다. EPA는 OSI 7 Layer 중 물리 계층, 데이터 링크계층 및 응용 계층의 3계층으로 구성된다. DNP3는 초기에는 Serial 통신을 지원하는 형태로 개발되었으나 이더넷 및 네트워크 기술이 고도화되면서 UDP나 TCP/IP를 지원하는 버전이 개발 되었다.

Ⅳ. DNP3 인증 메커니즘

전력 제어시스템에서의 인증은 사용자 인증과 기기 인증으로 구분할 수 있다.



〔그림 2〕 DNP3 Protocol Stack

• 사용자 인증

SCADA 시스템에서는 기기 인증 외에 장치 사용자의 신원확인을 위한 사용자 인증 기능이 반드시 필요하다. 사용자 인증 방법으로는 생체인식, 패스워드, 인증서, 스마트카드 등 다양한 것들이 있지만 제어시스템의 성능과 호환성, 활용성, 유용성 등을 고려하여 사용자 인증 기술의 적용성이 검토되어야 한다.

• 기기 인증

안정된 SCADA 시스템을 구현하기 위해서는 기본적으로 기기간의 상호 인증이 요구된다. 불가피하게 기기간의 인증이 어려울 경우에는 네트워크 장비 앞 단에 별도의 보안 장비를 설치하여 인증하는 방안을 고려할 수 있다.

표준에서 언급하고 있는 인증방식은 사용자가 인증되지 않은 또는 인증된 DNP3 메시지를 모두 보낼 수 있다는 가정하에 인증메시지를 구별할 수 있는 능력이 필요하며 인증메시지에는 추가적인 DNP function code와 object가 포함되어 있기 때문에 구현할 때 인증 실패 등의 보안 이벤트(Security event) 로깅(Logging) 및 감사(Audit)가 정보보호의 중요한 부분임을 반드시 인식해야 한다. 또한 전력 제어시스템은 이기종의 네트워크 인프라[4]와 다양한 프로토콜의 속성을 통해 실시간 정보를 주고 받기 때문에 기존 인터넷에서 발생되고 있는 보안 취약성 외에도 추가적으로 고려해야 할 보안 취약성이 많다. 특히 SCADA 시스템에 연결되어 있는 Master와 Outstation에서 사용자 및 기기 인증을 통해 접근통제의 신뢰성 확보한 뒤, 권한을 부여하는 것은 아주 중요한 메커니즘이라고 할 수 있다. 따라서 이번 장에서는 SCADA 시스템의 보안성 향상을 목표로 ISO/IEC TC57 WG15에서 권고하고 있는 IEC 62351 표준의 인증 및 암호화 메커니즘을 소개하고자 한다. IEC 62351 표준은 IEC 60870-5, IEC 61850, IEC 61970, IEC 61980을 기반으로 하는 전력자동화 프로토콜의 정보보안을 위한 표준으로 전자서명, 인증 엑세스, 도청 예방, 침입탐지, 네트워크 및 시스템 관리, 역할기반 접근제어(RBAC), 인증 및 보안 키 관리 등 스마트그리드 및 연계 정보의 보호방안을 제시하고 있다 [8].

IEC 62351 표준은 [표 3]과 같이 구성되어 있으며, 기존 보안표준 및 기술을 적극 활용하면서 타 표준과의 호환성 확보를 위한 표준이라고 할 수 있다. TCP/IP를 사용하는 전력 제어통신망에서 보안 강화를 위해 Packet filtering을 구현하고 있으며, 소개 하고자 하는 IEC 62351 권고안은 전력 제어시스템의 정보보안에 관한 포괄적인 표준으로 Application level security에 관한 인증, 침입탐지, 접근통제 등의 내용을 포함하고 있다.

IEC 62351은 정보통신기술(ICT) 분야에서 발전되어 온 정보보안기술을 전력 제어시스템에 적용하여 전력통신 보안을 구현하였다. 예를 들어 IEC 62351-4는 제어

4) 이기종 네트워크 인프라 : (유·무선)인터넷 및 인트라넷, 비즈니스 및 (폐쇄망을 포함한) 기업 내부망

〔표 3〕 IEC 62351 Family

구 분	설 명	비 고
IEC 62351-1	Introduction to the standard	
IEC 62351-2	Glossary of terms	
IEC 62351-3	Security for any profiles including TCP/IP	
IEC 62351-4	Security for any profiles including MMS (e.g., ICCP-based IEC 60870-6, IEC 61850, etc.)	
IEC 62351-5	Security for any profiles including IEC 60870-5 (e.g., DNP3 derivative)	
IEC 62351-6	Security for IEC 61850 profiles (e.g., GOOSE, RFC2030)	
IEC 62351-7	Security through network and system management	
IEC 62351-8	Role-based access control(RBAC)	
IEC 62351-9	Key Management	DRAFT
IEC 62351-10	Security Architecture	
IEC 62351-11	Security for XML Files	DRAFT

시스템의 무결성 유지를 위해 해시(Hash)알고리즘과 디지털서명기술(DSS)을 도입하고 접근통제(Access Control)와 도청(Eavesdropping) 방지를 위해 IETF RFC2246 TLS(Transport Layer Security)를 채택하였다.

중앙 제어장치(Master Station)와 현장 운영장치간(Outstation)의 인증 및 암호화 메커니즘을 위해 2006년 발표된 IEC 62351-3과 IEC 62351-5에서의 권고사항인 TCP/IP에서 TLS 암호화 방식 및 메시지 인증 방식에 관련된 DNP3 profile을 수용하고 이를 실제적으로 구현하기 위한 통신흐름, function code, object group, variation 등을 구체화하여 2007년 3월에 DNP3 Secure Authentication 첫 번째 규격을 발표하였다. DNP3 Secure Authentication 규격은 기존의 DNP 규격에 인증과 암호화를 위한 메커니즘을 추가한 것이다.

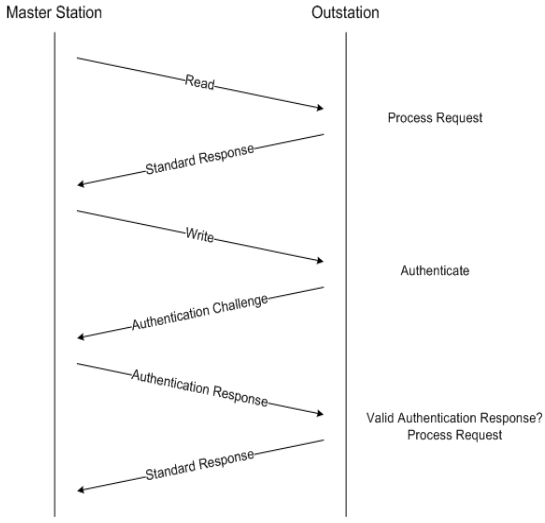
본 논문에서는 중앙 제어장치와 현장 운영장치 간의 연결이 요구될 때 보안성을 고려한 상호 인증(Authentication)과 연결된 보안채널 내 전송되는 제어명령에 대한 무결성(Integrity)을 검증하기 위한 암호화 메커니즘을 소개하고자 한다.

DNP3 Secure Authentication 규격의 가장 큰 특징은 기존의 DNP를 그대로 수용하면서 응용계층만 변경하여 보안기능을 구현한 것이다.

본 표준에서는 다음의 4가지 시나리오에 대해서는 인증을 수행해야 한다고 명시하고 있다[7].

- Initialization : 세션 초기화시 spoofing, replay, hijacking 등의 공격 방지를 위해 인증수행
- Periodic : 다른 공격(hijacking) 예방을 위해 주기적으로 인증 수행
- Critical Function Code Requests : 쓰기, 리셋 등과 같은 중요한 기능 수행 시 인증 수행
- Implementation Specific : DNP3를 통한 vendor와의 상호 인증을 위해 수행

Secure Authentication은 Challenge- Response



〔그림 3〕 Challenge-Response mode 인증 방식

〔표 4〕 DNP3 Critical Request Function Codes

Function codes		Description	Critical
Dec	Hex		
2	0x02	Write	MANDATORY
3	0x03	Select	MANDATORY
4	0x04	Operate	MANDATORY
5	0x05	Direct operate	MANDATORY
⋮	⋮	⋮	⋮
32	0x20	Authentication Request	Not applicable
33	0x21	Authentication Request－No Ack	Not applicable
34	0x22	Authentication Error	
131	0x83	Authentication Challenge	Not applicable
132	0x84	Unsolicited Authentication Challenge	

mode와 Aggressive mode 등 2가지의 인증 모드를 제공한다. [그림 3]은 Challenge- Response mode의 인증 방식을 나타낸 것으로 Master가 Outstation으로 [표 4]에 기술된 인증이 필요한 Function code를 포함한 request 메시지를 전송하면 Outstation은 난수를 포함하는 Authentication Challenge를 보내고 Master Station은 IEC 9798-4에 정의된 방법대로 Session키와 난수가 포함된 HMAC(Hash-based Message Authentication Code)을 보낸다. 이후, Outstation은 보유하고 있던 Session키로 HMAC을 검증하고 Response가 옳은지 여부를 판단하는 방식으로 인증을 수행한다. 또한 DNP3는 에러검출 메커니즘으로 CRC(Cyclical Redundancy Check)를 사용할 뿐만 아니라 전송 메시지의 중복 방지를 위해 Challenge, Reply, Error Message는 동일한 DNP3 애플리케이션 S/N(Sequence Number)을 사용하고 있다.

DNP3를 이용한 전력 제어시스템 또는 네트워크에 대한 주요 공격 대상은 중앙 제어장치 및 현장 운영장치이며 주요공격 유형은 아래와 같다[9].

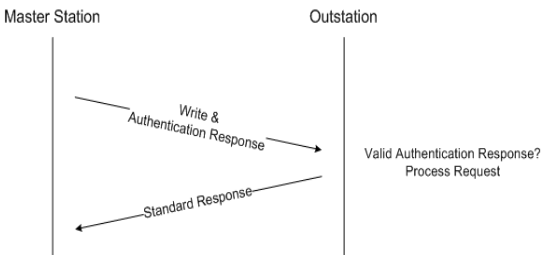
- 방해(Interruption) : 통신회선 절단 및 정보 전달 오류 등을 통해 서비스 거부를 유도하는 공격
- 가로채기(Interception) : 중요 제어데이터에 대한 비인가자들의 불법적인 접근에 대한 공격
- 변조(Modification) : 비인가자들의 불법적인 접근과 불법적인 변경에 의한 무결성에 대한 공격
- 위조(fabrication) : 비인가자들의 시스템에 대한 위조물 삽입에 의한 인증에 대한 공격

그러나 DNP3는 폐쇄망 기반에 맞추어 개발되었기 때문에 인증, 암호 및 키 관리 메커니즘을 제공하지 않고 있다. 하지만, 현장 운영장치에 대한 원격 접속 및 관리의 효율성을 위해 인터넷과 같은 외부망과의 연결이 점차 증가하고 있고 이로 인해 외부망을 통한 공격 경로가 다양해짐에 따라 DNP3 프로토콜에 대한 보안성 향상이 필요하다.

[그림 4]는 Aggressive mode에서 Master는 Request 메시지에 Authentication Response를 첨부하여 전송하기 때문에 일반적인 메시지 전송과 Challenge-Response 절차가 따로 수행되지 않아 Challenge-Response mode에서 발생하는 지연과 오버헤드를 제거할 수 있는 장점이 있다.

그러나 Authentication Challenge에 사용되는 난수는 Master에 의해 생성되기 때문에 Master가 해킹의 영향을 받으면 replay 공격에 악용될 수 있다는 단점이 있다.

Function Code는 제어 프로토콜과 함께 다른 표준 및 독점 제어시스템 프로토콜에 보안 기능을 추가하기



〔그림 4〕 Aggressive mode 인증 방식

〔표 5〕 암호(Session)키 업데이트 주기

형태	프로세스	메커니즘
모니터링 방향 Session key	Outstation으로부터 모니터링 방향으로 전송되는 인증 데이터를 인증하기 위함	마스터는 Update key를 이용하여 키 변경 메시지의 세션 키를 암호화한다.
컨트롤 방향 Session key	Master로부터 컨트롤 방향으로 전송되는 인증 데이터를 인증하기 위함	마스터는 Update key를 이용하여 키 변경 메시지의 세션 키를 암호화한다.
Update key	Master는 주기적으로 세션 키를 변경하기 위해 Update key를 사용함	Update key는 두 장치(Master / Outstation)로부터 사전에 공유되고 외부 프로토콜로부터 변경된다.

위해 사용될 수 있다. 물론 IEEE 1815™-2012에 많은 Function Code들이 제시되어 있지만 기존의 응답 기능 코드(0x81) 및 상태정보 쓰기코드(0x02) 등은 보안 기능을 위해 추가적으로 지정된다[10].

그리고 각 Challenge는 Critical ASDU[5]와 Non-Critical ASDU를 구별해야 한다. 특히 Critical ASDU는 Challenger를 인증하는데 중요한 메시지가 되며, IEC 62351-5는 다음과 같은 요구사항을 언급하고 있다.

- Outstation은 모든 output operation을 Critical하게 고려해야 한다.
- Challenger는 Critical한 최소 부분 집합을 추가 기능으로 선택할 수 있다.
- Outstation은 confirm 메시지가 Critical 할 수 있다는 것을 고려해야 한다.
- Security configuration parameter를 변경할 수 있는 모든 메시지는 Critical 한 것으로 간주한다.

또한 에러 메시지는 인증이 수행되는 것과는 다른 DNP3 프로토콜 연결시 전송될 수 있으며, 이것은 공격을 감지하는데 매우 유용하기 때문에 모든 에러(Error)는 기록(Logging)하는 것을 추천하고 있다.

DNP3는 무결성 보장을 위해 IEC 9798-4에 명시되어 있는 암호 알고리즘인 HMAC(keyed hashing with message authentication)을 이용한다. HMAC 연산 후 전송할 때 사용하는 세 가지 요소는 message data, challenge data와 비밀키가 사용되며 오직 수신자만이 HMAC의 검증을 통해 메시지 변조 여부를 확인할 수 있다. Master Station은 메시지와 키를 비밀키로 Hash 연산을 수행한 후 Hash 결과 값과 메시지를 Outstation으로 보낸다. Outstation은 가지고 있던 비밀키와 수신한 메시지를 Hash 연산을 수행한 후 수신한 Hash 결과 값과 대조하여 무결성을 확인한다. HMAC(Hash-based Message Authentication Code) 절차를 위해서는 Master Station과 Outstation은 사전에 비밀키를 공유하고 있어야 하는데 Secure Authentication에서는 이를 위해 2-level Key Management Scheme을 제공한다[11].

- Level 1 Pre-shared Key : Master Station과 Outstation에게 별도의 안전한 방법으로 배포된 비밀키로 Session key의 안전한 분배를 위해 사용된다.
- Level 2 Session Key : Session key란 Pre-shared Key를 이용하여 안전하게 배포되는 비밀키로 인증 메커니즘에 사용된다.

또한 인증 메커니즘에서 암호(Session)키가 어떻게 사용되고 Update 되는지를 [표 5]에 나타내었다.

Ⅴ. 결 론

현재 전력 SCADA 시스템에 대한 공격자의 동기와 목적이 커지면서 전력 제어시스템 사이버 공격이 크게 증가하고 있는 추세이며 사이버 공격으로 인해 전력 제어시스템 장애 발생 시 대규모 피해가 발생할 수 있어 SCADA 시스템에 대한 높은 수준의 사이버공격 대응 기술이 필요한 상황이다. 또한 전력 제어시스템 환경에서도 랜섬웨어(Ransomware)와 같은 몸값 요구형 악성코드 감염이 확인될 것으로 예상되어 산업제어 기기를

5) ASDU : Application Service Data Unit (응용 서비스 데이터 단위)

인질로 금전을 요구하는 경우도 부정할 수 없을 것으로 생각된다[12].

국가 중요기반시설을 보호한다는 측면에서 전력 제어시스템 보안기술개발의 필요성을 인식한 IEC, IEEE 등 국제 표준화기구는 보안 요구사항을 정의하고 전력 제어 데이터의 안전한 전송을 위한 보안 메커니즘을 연구 개발하고 있다.

국내의 경우 현재까지 대다수의 전력 제어시스템에서 보안 인증 기능이 없는 구 버전의 DNP3 프로토콜이 사용되고 있어 보안에 매우 취약한 상황이며, IEEE와 IEC에서 정의한 보안 메커니즘의 지원이 가능하고 국내 전력제어시스템의 구성에 특화된 보안시스템을 개발 및 보급이 절실히 요구된다.

참 고 문 헌

[1] NIST, “Special Publication 800-82, Revision 2 Draft : Guide to Industrial Control Systems (ICS) Security”, NIST SP 800-82, May 2014.

[2] 장문수, 이건희, 김신규, 민병길, 김우년, 서정택, “DNP3 제어시스템 프로토콜 취약점 실험,“ 보안공학연구논문지, 7(1), pp. 15-28, Feb 2010.

[3] 권성문, 손태식, “제어시스템 DNP3 프로토콜 취약점과 현황,” 정보보호학회지, 24(1), pp. 53-58, Feb. 2014.

[4] Jaebok Cha, “Information Communication Technology Glossary Book”, 2004 from http://www.ktword.co.kr/

[5] NIST, “Special Publication 800-82, Revision 1 Draft : Guide to Industrial Control Systems (ICS) Security”, NIST SP 800-82, 3-2 Threat, May 2013. http://dx.doi.org/10.6028/NIST.SP.800-82r1

[6] 유형욱, 윤정한, 손태식, “제어시스템 보안을 위한 whitelist 기반 이상징후 탐지 기법,” 한국통신학회 논문지, 38B(8), pp. 646-647, June 2013.

[7] IEEE, “IEEE Standard for Electric Power Systems Communications－Distributed Network Protocol (DNP3)”, 7.Secure authentication, pp.171-266, Oct 2012

[8] IEC, “IEC/TS 62351-2 TECHNICAL SPECIFICATION”, 2.Terms and definitions, Aug 2008

[9] Digital Bond, SCADA Security Portal, DNP3 User Group, 8. Feb. 2011 from http://www.digitalbond.com/DNP3UserGroupPolitics

[10] Digital Bond, SCADA Security Portal, DNP3 User Group, Function Code, Feb. 2011 from http://www.digitalbond.com/DNP3UserGroupPolitics

[11] Digital Bond, SCADA Security Portal, DNP3 User Group, Cryptography, Feb. 2011 from http://www.digitalbond.com/DNP3UserGroupPolitics

[12] Trend Micro, “TrandLabs SECURITY BLOG”, 産業制御システムに對するサイバー攻撃、攻撃を狙っているのは誰か？, Aug 2013 from http://www.trendmicro.co.jp/ics_cyberreport2

〈저 자 소 개〉

박 준 용 (Jun Yong Park)
학생회원

2000년 2월 : 동국대학교 반도체과학과 학사
2006년 2월 : 영남대학교 컴퓨터정보통신공학과 석사
2012년 2월 : 동국대학교 정보보호학과 석사
2012년 7월 ~ 2014년 2월 : (주) 한국IT컨설팅 보안사업부 선임연구원
2014년 2월 ~ 현재 : 동국대학교 엔터테인먼트 컴퓨팅 연구센터 연구원
2012년 3월 ~ 현재 : 동국대학교 정보통신공학과 박사과정
관심분야 : 융합보안, 스마트그리드보안, 개인정보보호, 위험평가

하 기 웅 (Gi-Ung Ha)
학생회원

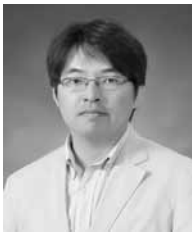
2012년 2월 : 동아대학교 컴퓨터공학과 학사
2013년 3월 ~ 현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 정보보호, 스마트그리드보안, 제어시스템보안, 침입탐지

민 남 홍 (Nam-Hong Min)
학생회원

2013년 2월 : 동국대학교 컴퓨터공학과 학사
2013년 3월 ~ 현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 정보보호, 스마트그리드보안, 제어시스템보안, 접근제어

유 기 순 (Ki-Soon Yu)
학생회원

2007년 2월 : 안동대학교 컴퓨터공학과 학사
2013년 3월 ~ 현재 : 동국대학교 정보보호학과 석사과정
관심분야 : 네트워크 보안, 모바일 보안



송 경 영 (Kyoung-Young Song)
정회원

2004년 2월 : 고려대학교 전기전자전파공학부/수학과 학사
2010년 8월 : 서울대학교 전기컴퓨터공학부 박사
2010년 8월~2012년 2월 : LG전자 차세대통신연구소 선임연구원
2013년 3월 ~ 현재 : 울산과학대학교 전기전자공학부 조교수
관심분야 : 스마트그리드 보안, MIMO 통신, 채널 부호화, 생체신호처리