정 보 보 호 학 회 지
제24권 제1호, 2014. 2

제어시스템 DNP3 프로토콜 취약점과 보안 현황

권 성 문*, 손 태 식**

요 약

과거의 제어 시스템은 외부 네트워크와 연결되지 않아 그 자체로 보안성을 보장 받을 수 있었다. 그러나 제어시스템의 디바이스들이 다양해지고 효율적인 제어를 필요로 하여 현재의 제어시스템은 기존 네트워크에 접속되어 효율적으로 관리되고 있다. 따라서 제어시스템 관리 효율은 증대 되었으나, 기존 네트워크가 가진 사이버 공격에 노출되어 보안적인 요소가 필요해 졌다. 본 논문은 많은 제어 시스템의 프로토콜 중 컨트롤 센터와 변전소간의 통신에 사용되는 DNP(Distributed Network Protocol)3 프로토콜을 중점으로 다루며 어떠한 취약점에 노출이 되어 있는지, 어떠한 보안 요소의 연구가 행해지고 있는지에 대해 다룬다.

Ⅰ. 서 론

과거의 제어시스템은 외부 네트워크와의 철저한 분리를 통해 외부의 접근을 차단하였으며 이를 통해 보안을 유지할 수 있었다. 그러나 현재의 제어시스템은 수천 개의 디바이스와 수백 개의 가동 시스템의 상호 운용하는 구조로 효율적인 관리 시스템이 필요해졌으며 결국 기존 네트워크에 연결하여 관리하게 되었다. 결과적으로 효율성은 증대 되었으나, 기존 네트워크가 가진 수많은 사이버 공격의 위험에 노출되었으며, 보안적인 요소를 고려하지 않았던 제어 시스템의 프로토콜에도 보안적인 요소가 필요해졌다. 따라서 제어 시스템의 여러 부분의 통신 프로토콜에 대한 보안연구 및 표준개발이 행해지고 있으며, 본 논문은 컨트롤 센터와 변전소간의 통신에 쓰이는 DNP3 프로토콜의 취약점과 보안 요소의 연구에 대해 알아본다.

2장은 DNP3 프로토콜에 대한 설명을 하며, 3장은 DNP3 프로토콜에 대한 보안사항을 설명하며, 4장은 DNP3 프로토콜에 대해 알려진 취약점을, 5장에서 이에 대한 분석과 대처방안을 설명한다.

Ⅱ. DNP3

2장에서는 DNP3 프로토콜의 표준과 관련된 개요 와 DNP3 프로토콜의 계층별 구조 및 특징을 설명한다.

2.1. DNP3 개요

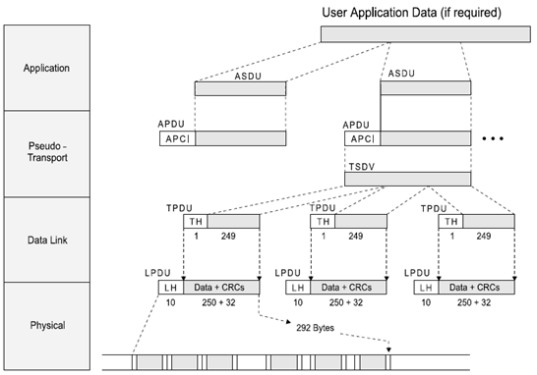
DNP3 프로토콜은 1993년 11월 캐나다 GE-Harris社가 SCADA(Supervisory Control and Data Acquisition) 시스템의 표준인 IEC 60870-5를 기반으로 만들었으며 컨트롤 센터와 변전소간의 통신을 위한 표준이다. 1998년, IEC 60870-5-101이라는 DNP3 프로토콜과 같은 역할을 하는 표준이 발표되었으나, 이는 DNP3 프로토콜과 근본만이 같을 뿐 구조 자체도 달라서 호환이 되지 않는 다른 프로토콜이다. 이 후, 기존 시리얼 기반 표준에서, 1998년 TCP/IP, UDP로 DNP3 프로토콜을 확장하였으며, IEC 또한 2000년 TCP/IP 기반 표준인 IEC 60870-5-104를 정의하였다. DNP3 프로토콜의 개발 책임과 소유권을 주장하기 위해 DNP 유저 그룹을 설립 후 개발과 유지 및 보수를 하였으며, 2010년 7월, IEEE에서 DNP3 프로토콜을 수용하여 IEEE 1815-2010표준이 발표되었다. 이 표준에서 보안을 강화하여 IEEE 1815-2012를 발표하였고, 이 표준이 현재

* 아주대학교 정보컴퓨터공학부(minter@ajou.ac.kr)
** 아주대학교 정보컴퓨터공학부(tsshon@ajou.ac.kr)

최신 버전이다. 보안과 관련된 부분은 다음 장에서 다루겠으며, DNP3의 구조에 대한 설명을 이어서 하며, 이는 모두 IEEE 1815-2012 표준을 참고한 내용임을 밝힌다.

2.2. DNP3 구조

2.1절에서 밝혔듯이, DNP3 프로토콜의 구조는 IEC 60870-5-101,104와 다른데, Pseudo-트랜스포트 계층을 추가로 가지고 있어 물리 계층, 데이터 링크 계층, 트랜스포트 계층(Pseudo-트랜스포트), 응용 계층으로 총 4계층 구조를 가진다.



〔그림 1〕 DNP3 구조

데이터 링크 계층은 최대 프레임 사이즈가 CRC(Cyclic Redundancy Check) 코드를 포함하여 292바이트이며, 이 중 상위 계층으로 부터의 메시지 정보를 담을 수 있는 최대 크기는 250바이트이다. 슬레이브 스테이션 또한 링크 계층 통신을 시작할 권한이 있는 Balanced 통신을 지원하며 Start, Length, Control, Destination Address, Source Address CRC 필드를 가진다. Start 필드는 시작을 나타내는 시그니처로 항상 0x0564 값을 가지며 Length 필드는 CRC를 제외한 프레임의 길이이며, Control 필드는 링크를 시작, 제어 테스트를 하기 위한 function 코드이다. 주소는 각 2바이트 크기로 최대 65,536개의 주소를 지정가능하다. 또한 이 주소는 논리적 주소이기 때문에 하나의 물리적 기기가 여러 개의 주소를 가질 수 있다.

트랜스포트 계층은 응용 계층 메시지에 대한 메시지 분해와 조립 기능을 수행하며 OSI 7 계층에서 정의하는 트랜스포트 계층에 비해 단순하여 Pseudo-트랜스포트 계층이라고 지칭한다. 응용 계층으로부터 TSDU(Transport Service Data Unit)을 받으면, 이것을 하위 데이터 링크 계층에서 다룰 수 있도록 250바이트 단위로 잘라서 데이터 링크로 전달한다.

응용 계층은 사용자 응용 프로그램과 직접 연결되는 계층으로 메시지를 받아서, ASDU(Application Server Data Unit) 단위로 쪼개어 각 ASDU에 제어정보를 추가해서 APDU(Application Protocol Data Unit)을 생성한다. 각 APDU 크기는 2048바이트로 제한되며 데이터 객체 정보와 제어 메시지를 포함한다. 통신 유형에는 Request-Response와 Unsolicited Response가 있는데, 오직 마스터만 요청을 보낼 수 있으며 아웃스테이션은 Unsolicited Response를 통해 요청 없이 상태에 대한 정보를 전달 가능하다. 요청 과정이 생략된 단순한 유형으로 상황에 따른 빠른 데이터의 전송이 가능하며 이와 함께 통신 관련 변수들을 다수 조작 가능한 특징 때문에 DNP3가 IEC 60870-5-101,104보다 유연하다고 볼 수 있다.

Ⅲ. DNP3 보안 현황

3장에서는 DNP3의 보안 현황에 대해 설명한다.

IEEE 1815-2010 표준에서부터 SA(Secure Authentication)을 포함하며, SA와 함께 트랜스포트 계층에는 TLS(Transport Layer Security)를 권고한다.

3.1. Secure Authentication

SA는 IEC 62351-2에 정의되어있는 spoofing, modification, repudiation, replay, eavesdropping와 같은 공격에 대응하기 위해 만들어졌다. DNP3와 IEC 60870-5-101,104의 보안 표준인 IEC 62351-5를 준수하며 인증 국제표준인 ISO/IEC 9798-4를 기반으로 하여 응용 계층만 변경하여 메시지 인증기능을 제공한다. 2007년 버전 1을 시작으로 버전 2에서 Pre-shared 키와 강도가 약한 해시를 포함하여 IEEE 1815-2010 표준에 포함되었으며, 현재의 버전인 버전 5에 오면서 기존의 버전 4까지의 구조적 문제점을 해결하기 위해 취약한 feature들을 삭제하여 보안성을 근본적으로 높였다. 따라서 Smart Grid Interoperability Panel Cyber Security Working Group가 제안한 스마트 그리드를 위한 보안

표준 요구사항을 충족 하였으나, 하위버전과는 호환이 되지 않는다. MD5 및 SHA-1과 같은 현재 안전하지 않은 알고리즘 또한 변경하여 HMAC-SHA256, AES-128,256 등을 포함하였으며 비대칭 키 관리 메커니즘 표준인 ISO/IEC 11770 표준을 준수하는 공개키 구조 또한 포함한다. 이 외 공격 패턴을 도출하기 위해 인증 실패 횟수와 같은 통계적인 자료를 수집하는 기능이 있으며 꾸준한 보완작업을 진행 중이며 IEEE 1815-2012에 포함되어 있다.

3.2. TLS(Transport Layer Security)

트랜스포트 계층에서 DNP3 프로토콜의 기밀성 및 인증 기능을 제공하기 위함이며 RSA, DSS(Digital Signature Standard)를 사용한 서명을 포함한다. 키 교환은 1024비트의 RSA나 Diffie-Hellman 알고리즘을 사용한다. 공개키 인증 및 인증 폐기에 관한 표준인 RFC 3280을 준수하며 IEC 62351-3 또한 준수한다. 그러나 NIST(National Institute of Standards and Technology)는 TLS를 2013년 3월부터 더 이상 지원하지 않기로 하여, 하나의 사용 가능한 옵션이라는 점을 밝혀둔다.

이러한 보안 사항을 IEEE 1815-2012 표준에서 권고하나 제어 시스템의 가용성이 우선시 되는 특성과 기존 디바이스들의 성능 문제로 실제 적용된 사례는 드물다. 현재 DNP 유저 그룹에 인증 받은 SAv5가 적용된 제품은 단 4개의 제품만이 존재할 정도이다.[3] 이 사항을 해결하기 위해 2013년 9월 DNP3 Secure Authentication Tutorial을 발표하였으며 더 나아가 DNP 제품을 생산하는 벤더들과 소비자단 까지 어떻게 SAv5를 공급할지에 대한 가이드라인을 2014년 2월 발표 할 예정이다. 그러나 이 외에도 처리가 빨라야 하는 명령이나 낮은 전송율의 링크를 가진 구역을 포함하는 통신구간 등의 문제가 있어 100% 안전하게 인증과 암호화가 이루어지기 힘들며 여전히 보안이 고려되지 않은 DNP3 프로토콜이 사용되고 있다.

Ⅳ. DNP3 취약점

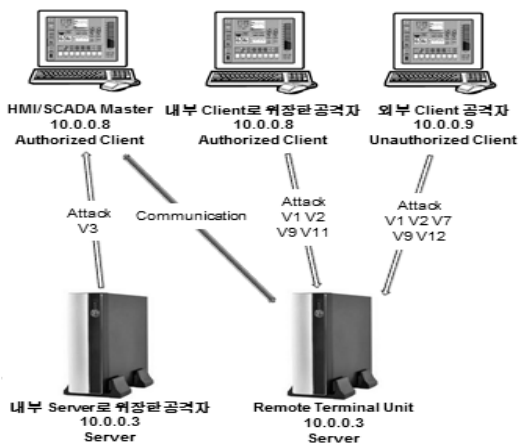
4장에서는 공개된 DNP3의 취약점과 ICS-CERT에서 발표에서 발표한 최신 Alert에 대해 알아본다.

인증과 암호화라는 보안 요소가 고려되지 않은 DNP3 프로토콜은 일반 네트워크의 spoofing, modification 등의 많은 공격 위험을 가지고 있다.

4.1. 공개된 DNP3 취약점

Digital Bond 社에서는 일반 네트워크의 취약점을 이용, DNP3 프로토콜에 적용하여 취약점 16가지를 공개하였으며 취약점의 내용은 [표 1]과 같다.

표의 취약성 중 단순 변경 명령 및 쉽게 탐지 가능한 체크섬 오류와 원활한 공격 실험을 위해 서버를 재시작 시키는 공격을 제외한 10개의 취약성을 아래 [그림 2]와 같은 환경에서 실험하였으며, 실제로 취약성이 유효함을 검증 할 수 있었다.



〔그림 2〕 DNP3 취약성 공격실험 환경

4.2. 최신 ICS CERT Alert

2013년 8월에서 2014년 1월 까지, 총 16건에 해당하는 DNP3 ICS CERT Alert가 있었다.[표 2]

이 ICS CERT Alert들은 SCADA/ICS 프로토콜의 취약점을 찾는 "Project Robus"[2]에 의해 찾아진 것으로, IOServer, Kepware, Triangle Microworks 등 많은 벤더의 DNP3 제품이 포함되어 있었으나, 입력 값의 타당성을 제대로 체크 하지 않아 일어나는 오류들로 서비스 거부 공격과 같은 결과를 초래하였다. DNP 유저 그룹은 표준에 입력 값의 타당성을 체크 하기 위한 정보가 부족한 부분에 대해 시인하고, 이를 바로 잡기 위해

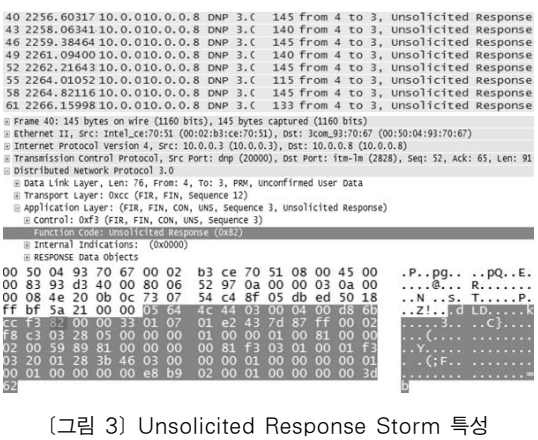
〔표 1〕 Digital Bond 社에서 공개한 DNP3 16가지 취약점

취약점명	내용	공격 유형	공격자 유형
Disable Unsolicited Response(V1)	공격자는 경보와 다른 주요 이벤트를 방해하기 위해 현장 제어장치의 unsolicited response 기능을 정지시킬 수 있음	불법수정, 방해	내부 Client 위장 외부 Client
Non-Dnp3 Communication on a DNP3 Port(V2)	제어시스템서버와 현장제어장치 사이에 확립된 연결은 어느 한쪽 장치로 다른 공격을 보내기 위해 하이재킹되거나 스푸핑 될 수 있음	불법수정, 방해	내부 Client 위장 외부 Client
Unsolicited Response Storm(V3)	제어시스템서버 또는 제어실 운영자가 처리하기 힘들 정도의 대량의 잘못된 unsolicited response를 보냄	불법수정, 방해	내부 Server 위장
Cold Restart from Authorized(V4) or Unauthorized Client(V5)	공격자는 제어시스템서버의 재시작 또는 정지를나타내는 패킷을 현장제어장치로 전달함으로써 현장제어장치를 서비스 불능 상태로 만들 수 있음	방해	V4:내부 Client 위장 V5:외부 Client
Unauthorized Read Request to a PLC(V6)	비인가된 제어시스템서버는 현장제어장치로부터 정보를 읽기위한 시도 가능	가로채기	외부 Client
Unauthorized Write Request to a PLC(V7)	비인가된 제어시스템서버는 현장제어장치의 정보를 쓰기 위한 시도 가능	불법수정, 방해	외부 Client
Unauthorized Miscellaneous Request to a PLC(V8)	비인가된 제어시스템서버는 현장제어장치에 읽기 또는 쓰기 요청외 다른 요청을 보냄	방해, 위조, 가로채기, 불법수정	외부 Client
Stop Application(V9)	현장제어장치상에 애플리케이션을 정지 시킴	방해	내부 Client 위장 외부 Client
Warm Restart(V10)	공격자는 현장제어장치의 구성을 초기화하고 이벤트를 삭제할 수 있음	불법수정	내부 Client 위장 외부 Client
Broadcast Request from an Authorized(V11) or Unauthorized Client(V12)	공격자는 다른 현장제어장치의 네트워크에 Broadcast 요청 패킷을 전송해서, 현장제어장치 주소 획득 및 서비스 거부 공격을 할 수 있음	가로채기, 불법수정, 방해	V11: 내부 Client 위장 V12: 외부 Client
Points List Scan(V13)	정보수집 단계에서 공격자는 가용한 DNP3 데이터 포인트 정보를 수집할 수 있음	가로채기	내부 Server 위장
Function Code Scan(V14)	정보수집 단계에서 공격자는 가용한 function code 정보를 수집할 수 있음	가로채기	내부 Server 위장
Time Change Attempt(V15)	Function code 2번과 object type 50으로 공격자가 시간 정보를 위조할 수 있음	불법수정	내부 Client 위장 외부 Client
Failed Checksum Error(V16)	체크섬을 검사한 결과 체크섬이 맞지 않는 경우로 공격자가 패킷을 위조했음을 알 수 있음	불법수정	내부 Client 위장 외부 Client

2013년 12월 20일 DNP3 데이터에 대한 입력 값의 타당성을 검사하기 위한 상세 문서를 공지하였다.

Ⅴ. 취약점 대처 방안

[표 1]의 취약점은 각 취약점의 특성으로 Snort Rule을 통해 공격 탐지가 가능하였다. [그림 3]은 V3 취약점인 Unsolicited Response Storm을 이용한 공격의 특징이다. Unsolicited Response 명령을 뜻하는 명령 코드 0x82의 패킷이 짧은 시간 다량 검출 된 것을 볼 수 있다. DNP3 프로토콜의 경우 2초간 응답을 받지 못하



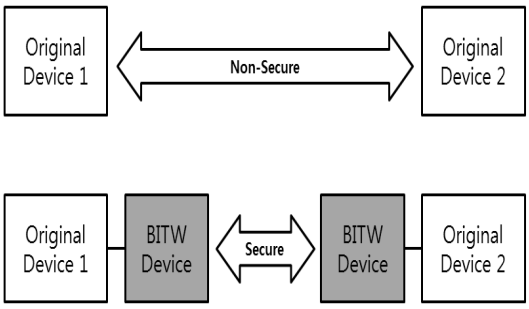
〔그림 3〕 Unsolicited Response Storm 특성

면 해당 연결이 끊긴 것으로 판단하기 때문에, 10초에 5개 이상의 Unsolicited Response 명령을 가진 패킷이 검출되면, 이는 정상적인 패킷의 흐름이 아니라고 판단할 수 있어 0x82명령코드와 10초간 카운팅을 하여 5개 이상인 경우라는 Snort Rule을 통해 탐지가 가능하였다. 이와 같이 각 취약점 별 Snort Rule을 통한 탐지가 가능 하였으나, 이러한 시그니쳐 기반 탐지에는 한계가 존재한다. 알려지지 않은 공격은 탐지가 불가능하며, 제어 시스템 프로토콜에 대해 알려진 공격의 시그니쳐가 적은 점은 시그니쳐 탐지 기술에 더욱더 한계를 가져다 준다. 따라서 이를 해결하기 Whitelist 기법과 Bump-In-The-Wire, 명령코드에 따른 각기 다른 수준의

〔표 2〕 DNP3 ICS CERT Alert (2013.08 ~ 2014.01)

Alert Number 날짜	내 용	해당 S/W 회사
ICSA-14-014-01 2014.01.14	다중 에러를 포함하게끔 조작된 Unsolicited 프레임을 전송하여 과도한 저널 이벤트 메시지를 로그에 기록하게 하여 자원을 모두 소비시켜 서비스 거부 증상을 발생시킴	Schneider Electric
ICSA-13-352-01 2013.12.18	인풋이 올바른지 테스트 하지 않아, 조작된 IP 패킷을 전송하여 마스터의 드라이버가 충돌, 프로세스를 재시작하게 유도 가능함	Novatech
ICSA-13-346-01 2013.12.18	인풋이 올바른지 테스트를 하지 않아, 조작된 TCP 패킷으로 통신 링크를 재시작 시키거나 불능으로 만들 수 있음(Serial 환경의 DNP3 에서도 동일한 취약성 공격이 가능)	Cooper
ICSA-13-346-02 2013.12.17	마스터 서버가 인풋이 올바른지 테스트를 하지 않아, 공격자가 정의되지 않은 예외를 발생시켜 프로세스를 크래시 시킬 수 있음	Cybectec/ Cooper
ICSA-13-282-01A 2013.11.22	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 마스터 스테이션에게 전송하여 무한 루프를 발생시켜 디바이스가 정지되고 루프 상태를 초기화 시키기 위해 재시작 하게 만듦(Serial환경의 DNP3 에서도 동일한 취약성 공격이 가능)	Alstom
ICSA-13-161-01 2013.11.22	TCP Connection Hijacking공격 기법을 사용하여 조작된 TCP/IP 패킷을 아웃스테이션에게 전송, 무한 루프를 발생시켜 디바이스가 정지되고 루프 상태를 초기화 시키기 위해 재시작 하게 만듦	IOServer
ICSA-13-297-02 2013.11.19	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 마스터에게 전송하여 무한 루프를 발생시켜 프로세스를 크래쉬 시키며 이 현상을 해결하기 위해 수동으로 재시작을 시켜줘야만 함(Serial환경의 DNP3 에서도 동일한 취약성 공격이 가능)	GE
ICSA-13-297-01 2013.11.19	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 전송해 HMI에게 DoS 공격을 하며 공격을 받은 HMI는 시스템이 정지되며 DoS로 부터 복구하기 위해 시스템을 재시작 하여야 함(Serial환경의 DNP3 에서도 동일한 취약성 공격이 가능)	Catapult
ICSA-13-213-04A 2013.10.03	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 마스터 스테이션으로 전송하여, 마스터 서버의 크래쉬, 어플리케이션의 종료, 아웃스테이션 디바이스와의 OPC 통신 방해를 유발	MatrikonOPC
ICSA-13-234-02 2013.9.22	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 마스터 스테이션에게 전송하여 무한 루프를 발생시켜 디바이스가 정지되고 루프 상태를 초기화 시키기 위해 재시작 하게 만듦(Serial환경의 DNP3 에서도 동일한 취약성 공격이 가능)	Toolbox
ICSA-13-240-01 2013.9.17	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 마스터로부터 아웃스테이션으로 전송하여 무한 루프를 발생시켜 디바이스가 정지되고 루프 상태를 초기화 시키기 위해 재시작 하게 만듦(Serial환경의 DNP3 에서도 동일한 취약성 공격이 가능)	Triangle MicroWorks
ICSA-13-226-01 2013.8.16	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 마스터 스테이션에게 전송하여 무한 루프를 발생시켜 디바이스가 정지되고 루프 상태를 초기화 시키기 위해 재시작 하게 만듦(Serial환경의 DNP3 에서도 동일한 취약성 공격이 가능)	Kepware
ICSA-13-219-01 2013.8.12	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 마스터 스테이션에게 전송하여 RTAC 마스터 디바이스에게 무한 루프를 발생시켜 디바이스가 정지되고 루프 상태를 초기화 시키기 위해 재시작 하게 만듦(Serial환경의 DNP3 에서도 동일한 취약성 공격이 가능)	Schweitzer
ICSA-13-252-01 2013.8.09	해당 취약점을 사용하여 서브 스테이션 서버의 DNP3 Slave 서비스의 가용성에 영향을 미침	Schweitzer
ICSA-13-213-03 2013.8.05	TCP Connection Hijacking공격 기법을 사용하여 조작된 TCP/IP 패킷을 마스터 스테이션에게 전송, 무한 루프를 발생시켜 디바이스가 정지되고 루프 상태를 초기화 시키기 위해 재시작 하게 만듦	IOServer
ICSA-13-213-03 2013.8.28	특정 필드의 값을 비정상으로 조작한 TCP/IP 패킷을 마스터로부터 아웃스테이션으로 전송하여 무한 루프를 발생시켜 디바이스가 정지되고 루프 상태를 초기화 시키기 위해 재시작 하게 만듦	IOServer

암호화 및 인증기법 적용을 제시한다. Whitelist 기법은 정상행위를 정의하여 이에 위반되는 행위를 탐지하는 기법으로, 시그니쳐 기반 탐지의 반대 격이다. 시그니쳐가 갈수록 늘어 부담이 되는 반면, Whitelist 기법은 한 번 정확히 정의된 Whitelist 규칙만 있으면 이것을 적용하면 되기 때문에 비교적 가벼운 특징을 가져 가용성에 민감한 제어 시스템에 효과적이다. Bump-In-The-Wire 기법은 [그림4]와 같이 기존 디바이스들 간 통신선로 사이에 추가적인 보안 장치를 연결함으로써 보안 채널을 형성하는 방식이다. 이 방법은 디바이스의 수정이 필요 없어 기존 전력망에 유연하게 적용할 수 있으며, 현장 기기의 성능저하 문제를 최소화 할 수 있다. 마지막으로, 빠르게 처리 되어야 하는 명령이나 느린 링크 구간을 가진 통신에 있어 암호화 및 인증 기법 보안의 강도를 다르게 하여 가용성에 큰 문제를 주지 않으면서 암호화 및 인증을 구현 하는 방법을 제시한다.



〔그림 4〕 Bump-In-The-Wire 기법 도식도

Ⅵ. 결론

DNP3 프로토콜을 위한 보안 사항은 SAv5, TLS의 암호 및 인증 기법이 있으나 가용성이 중요시 되는 제어 시스템에서 이를 적용하기는 쉽지가 않다. 따라서 명령코드 등의 환경에 따른 보안의 강도가 다른 암호 및 인증 기법을 택하면서 Whitelist 기법이나 Bump-In-The-Wire 기법을 추가적으로 적용하여 다계층적인 보안을 제공할 필요가 있다.

참고문헌

[1] IEEE Std 1815-2012, IEEE Standard for Electric Power Systems Communications

[2] Adam Crain, Chris Sistrunk, "Project Robus", http://www.automatak.com/ro bus/

[3] DNP3 Product, http://www.dnp.org/pag es/Dnp-ProductsDefault.aspx

[4] Digital Bond, http://www.digitalbond.co m

[5] Erfan Ibrahim, Overview of DNP3-SA, IEC 61850, IEC 62351, IEC 61970 and IEC 61968, Dec 2013

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

〈저자소개〉

권 성 문 (Sungmoon Kwon)
2013년 2월 : 아주대학교 정보컴퓨터컴퓨터공학부 졸업
2013년 3월~현재 : 아주대학교 컴퓨터공학과 석사과정
<관심분야> 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지

손 태 식 (Taeshik Shon)
정회원
2000년 2월 : 아주대학교 정보 및 컴퓨터공학부 졸업
2002년 2월 : 아주대학교 정보통신전문대학 공학석사
2005년 8월 : 고려대학교 정보보호대학원 공학박사
2004년 2월~2005년 2월 : Research Scholar, University of Minnesota
2005년 8월~2011년 2월 : 삼전전자 DMC 연구소 책임연구원
2011년 3월~현재 : 아주대학교 정보통신대학 정보컴퓨터공학과 조교수
관심분야 : 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지, ICT융합보안