JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

기반 기술

J. Adv. Navig. Technol. 18(4): 353-358, Aug. 2014

DNP3 프로토콜 보안 현황 및 공격 탐지 방안

DNP3 Protocol Security and Attack Detection Method

권 성 문[1] · 유 형 욱[1] · 이 상 하[2] · 손 태 식[3*]
[1]아주대학교 컴퓨터공학과
[2]동서울대학 정보통신과
[3]아주대학교 정보컴퓨터공학과

Sung-moon Kwon[1] · Hyung-uk Yoo[1] · Sang-ha Lee[2] · Tae-shik Shon[3*]

[1]Department of Computer Engineering, Ajou University, Gyeonggi-do, 443-749, Korea

[2]Department of Information Communication, DongSeoul University, Gyeonggi-do, 461-714, Korea

[3]Department of Information and Computer Engineering, Ajou University, Gyeonggi-do, 443-749, Korea

[요 약]

과거의 제어 시스템은 제어 시스템의 망을 외부의 망과 분리함으로써 외부의 접근을 원천 차단하여 외부공격에 대한 보안을 보장받았다. 그러나 제어 시스템의 디바이스들이 다양해지고 디바이스 간의 상호 운용이 필요해짐에 따라 효율적인 관리 시스템이 필요해 졌으며 이는 제어 시스템 또한 외부의 망과 연결되는 요인이 되었다. 따라서 효율적인 관리는 용이해졌으나 보안 사항이 포함되지 않은 다수의 제어 시스템의 프로토콜이 각종 사이버 공격의 위험에 놓이게 되어 각 프로토콜에 대한 보안 기능 추가 및 공격 탐지에 관한 연구가 활발히 진행 되어 왔다. 본 논문에서는 컨트롤 센터와 변전소간 통신에 쓰이는 DNP(distributed network protocol)3 프로토콜을 중점으로 다루며 프로토콜의 특징과 보안 현황 분석 및 현재까지 공개된 취약점 분석과 취약점을 이용한 공격 탐지 방안을 제시한다.

[Abstract]

In the past, security on control system was guaranteed by isolation of control system networks from external networks. However as devices of the control systems became more various and interaction between the devices became necessary, effective management system for such network emerged and this triggered connection between control system networks and external system networks. This made management of control system easier but also made control system exposed to various cyber attack threats, Therefore researches on appending security measures on each protocols are in progress. This paper focused on DNP(distributed network protocol)3 protocol which is used for communication between control center and substations. It describes characteristics of DNP3 protocol and research on adding security elements to the protocol. It also analyzed known vulnerabilities of DNP3 protocol and proposed data mining methodology for detecting such vulnerabilities.

Key word : DNP3, Control system, Attack detection, Cyber attack, Data mining.

http://dx.doi.org/10.12673/jant.2014.18.4.353

Received 11 July 2014; **Revised** 26 August 2014
Accepted (Publication) 23 August 2014(30 August 2014)

***Corresponding Author; Tae-shik Shon**

Tel: +82-31-219-3321
E-mail: tsshon@ajou.ac.kr

Ⅰ. 서 론

과거의 제어 시스템은 외부의 망과 분리된 독립된 망을 사용하였기 때문에 외부의 접근을 원천 차단하여 외부공격에 대한 보안을 보장받을 수 있었다. 따라서 제어 시스템을 위해 설계되는 프로토콜은 보안적인 요소는 중요한 요소로 고려되지 않았으며 효율적인 운용을 위한 프로토콜들이 설계되었다. 그러나 제어 시스템의 디바이스들이 다양해지고 디바이스 간의 상호 운용이 필요해짐에 따라 효율적인 관리 시스템이 필요해졌으며 제어 시스템 또한 외부의 망과 연결되게 되었다. 따라서 효율적인 관리는 용이해졌으나 기존 외부의 망이 가진 사이버 공격에 대한 위험 또한 상속받게 되어 보안 사항이 고려되지 않았던 많은 프로토콜 또한 보안 기능의 추가가 필요해 졌다. 이에 많은 연구가 행해지고 있으며 본 논문에서는 전력계통 제어시스템의 컨트롤 센터와 변전소 간의 통신에 주로 사용되는 DNP(distributed network protocol)3를 중점으로 다루며 2장에서는 DNP3의 전반적인 특징과 보안 기능을 다루며 3장에서는 DNP3의 공개된 취약성을 분석하며 4장에서는 3장에서 분석한 취약성을 이용한 공격을 탐지하기 위한 방안을 제시하며 마지막 5장에서는 결론 및 향후 연구 방향을 논의하며 논문을 마무리한다.

Ⅱ. DNP3

2-1 DNP3 개요

DNP3 프로토콜은 1992-1994년 캐나다 Westronic社(현재 Harris Corporation에 합병됨)에 의해 만들어졌으며 특정 환경, 단체, 개인 등을 위해 특화된 수백 개의 프로토콜을 표준화 하고자 만들었다. 그 당시 IEC 60870-5와 UCA 1.0(UCA 2.0이 현재의 IEC 61850)이 개발 중에 있었다. 그러나 IEC 60870-5는 진행 속도가 너무 더뎠으며 많은 옵션을 포함하여 표준이 충분히 제한적이지 못할 우려가 있었으며 UCA 1.0의 경우 SCADA(supervisory control and data acquisition) 시스템에 대해 정의되어 있지 않았다. 이러한 이유로 Westronic社가 IEC 60870-5의 개발에 참여 중이었음에도 불구하고 직접 프로토콜을 만들게 되었다. 또한 IEC 60870-5와 UCA 1.0의 결과물중 당시의 IEC 60870-5의 작업이 더 완성적이었기에 IEC 60870-5를 바탕으로 DNP3를 제작하였으며 이 때문에 IEC 60870-5와 DNP3는 같은 연구바탕을 기반으로 하여 비슷한 부분이 상당 부분 존재한다.

그러나 그림 1에서 보이는 바와 같이 프로토콜 스택에서 차이점이 있다. DNP3 프로토콜의 경우 transport layer를 포함하는데, 이는 낮은 속도의 전송 구간을 포함한 환경을 고려하여 패킷을 분할 전송 가능하게하기 위해 설계한 계층이며 이 계층 덕분에 그림 2와 같이 application layer의 메시지를 최대 249

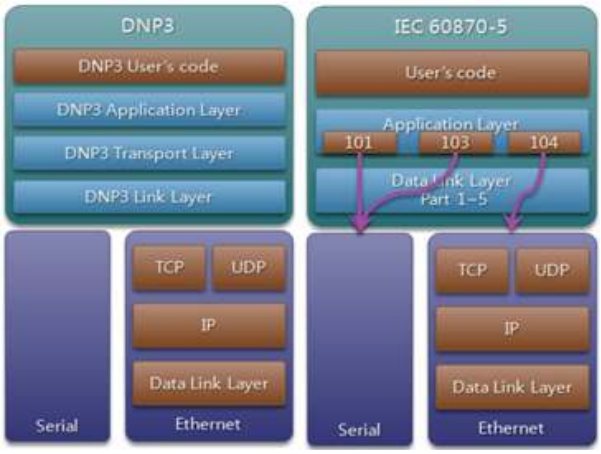

그림 1. DNP3와 IEC 60870-5의 구조
Fig. 1. Architecture of DNP3 and IEC 60870-5.

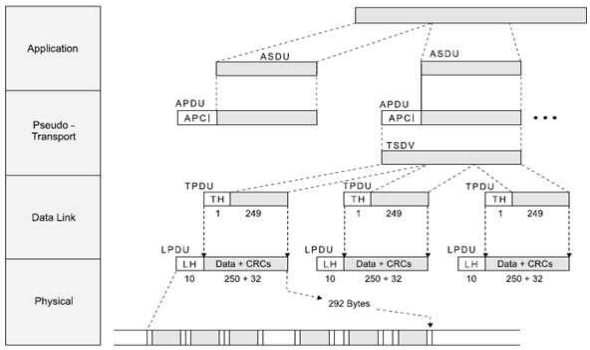

그림 2. DNP3 메시지 포맷
Fig. 2. Message format of DNP3.

byte로 분할하여 전송이 가능하다. 이 계층은 다른 프로토콜과 상호 운용을 고려하여 1바이트의 단순한 태그와 비슷하게 설계되어 pseudo-transport layer으로 불리나 구조적 차이로 인해 IEC 60870-5와는 호환이 불가능하다. 가장 낮은 계층부터 link 계층은 최대 프레임 사이즈가 CRC(cyclic redundancy check) 코드를 포함하여 292바이트이며, 이 중 상위 계층으로 부터의 메시지 정보를 담을 수 있는 최대 크기는 250바이트이다. start, length, control, destination address, source address CRC 필드를 가진다. start 필드는 시작을 나타내는 시그니쳐로 항상 0x0564 값을 가지며 length 필드는 CRC를 제외한 프레임의 길이이며, control 필드는 링크를 시작, 제어 테스트를 하기 위한 function 코드이다. transport 계층은 application 계층 메시지에 대한 메시지 분해와 조립 기능을 수행하며 OSI 7 계층에서 정의하는 트랜스포트 계층과 달리 1바이트의 단순한 구조를 하여 앞서 설명 했듯이 pseudo-transport 계층이라고 지칭한다. application 계층으로부터 TSDU (transport service data unit)을 받으면, 이것을 하위 link 계층에서 다룰 수 있도록 250바이트 단위로 잘라서 link 계층으로 전달한다. application 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 데이터객체 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.

초기 serial 기반에서 1998년 TCP/IP, UDP로 프로토콜을 확장하였으며 DNP3의 프로토콜의 개발 책임과 소유권을 주장하기 위해 DNP 유저 그룹을 설립, 2010년 7월 IEEE에서 DNP3 프로토콜을 수용하여 IEEE 1815-2010표준이 되었으며 현재 북미에서 널리 사용되고 있는 프로토콜이 되었다. IEEE 1815-2010에서 보안을 강화하여 IEEE 1815-2012가 발표되었으며 현재 IEEE 1815-2012 표준이 최신이며 그 이상 버전에 대한 계획은 아직 발표되지 않았다.

2-2 DNP3 보안

IEEE 1815-2010 표준에서부터 SA(secure authentication)을 포함하며 SA와 함께 transport 계층에서는 TLS(transport layer security)를 권고한다.

1) secure authentication

SA는 IEC 62351-2에 정의되어있는 spoofing, modification, repudiation, replay, eavesdropping와 같은 공격에 대응하기 위해 만들어진 인증 체계이다. 2007년 버전 1을 시작으로 버전 2가 IEEE 1815-2010에 포함, 보안성을 높인 버전 5가 현재의 최신버전으로 IEEE 1815-2012에 포함되었다. 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. 버전 2에서 pre-shared 키와 강도가 약한 해시를 포함했었으나 버전 5에 오면서 기존의 버전 4까지의 구조적 문제점을 해결하기 위해 취약한 요소들을 삭제하여 보안성을 근본적으로 높였다. 또한 공격을 나타내는 패턴을 감지하기 위해 통계적 자료를 유지하고 보고하는 기능인 security statics를 추가하였으며 MD5 및 SHA-1과 같은 현재 안전하지 않은 알고리즘 또한 변경하여 HMAC-SHA256, AES-256을 기본 설정으로 하는 등 암호화 알고리즘의 강도를 높였다. 비대칭키 관리 메커니즘 표준인 ISO/IEC 11770 표준을 준수하는 공개키 구조 또한 포함하였다. 따라서 smart grid interoperability panel cyber security working group가 제안한 스마트 그리드를 위한 보안 표준 요구사항을 충족 하였으나, 하위버전의 SA와는 호환이 되지 않는다.

2) TLS

transport 계층에서 DNP3 프로토콜의 기밀성 및 인증 기능을 제공하기 위해 TLS를 권고하며 IEEE 1815-2010에서는 TLS 버전 1.0이상을 권고하였으나 TLS 버전 1.0의 취약성이 공개되어 IEEE 1815-2012에서 TLS 버전 1.2 이상으로 권고하였다. RSA, DSS(digital signature standard)를 사용한 서명을 포함하며 키 교환은 1024비트의 RSA나 Diffie-Hellman 알고리즘을 사용한다. 공개키 인증 및 인증 폐기에 관한 표준인 RFC 3280을 준수하며 전력 시스템의 TCP/IP 관련 보안 표준인 IEC 62351-3 또한 준수한다.

이와 같은 보안을 IEEE 1815-2012 표준에서 권고하나 가용성이 우선시 되는 제어시스템의 특성과 이미 동작하고 있는 제어시스템의 디바이스들의 성능 문제로 실제 인증 및 암호화 과정이 적용된 사례는 드물다. 현재 DNP 유저 그룹에 인증 받은 SAv5가 적용된 제품은 단 4개의 제품 밖에 없으며 SA를 좀더 보급하고자 2013년 9월 DNP3 secure authentication tutorial을 배포하였으나 빠른 전송과 처리를 요구하는 중요한 명령 모두에 SA를 적용하기에 무리가 있으며 또한 낮은 전송율의 링크를 가진 구역을 포함하는 통신구간에서는 인증과 암호화를 적용 시 인증 과정에 따른 통신 딜레이가 상당히 증가하기 때문에 인증과 암호화의 도입이 힘들다. 따라서 여전히 보안이 고려되지 않은 DNP3 프로토콜이 많은 지역에서 사용되고 있다.

Ⅲ. DNP3 취약점 분석

3-1 최신 ICS-CERT Alert

최신 ICS-CERT Alert는 Adam Crain, Matthew Luallen 이 주도하는 project “Robus”라 불리는 SCADA 프로토콜 Fuzzing 테스트로 밝혀진 취약점으로 일반적으로 생각하는 공격의 반대 방향이라는 특이점을 가지고 있다. 그림 3의 B방향과 같이 마스터에서 필드 디바이스로의 공격이 아닌 그 반대 방향인 필드 디바이스로 조작된 패킷을 통해 마스터를 공격하는 방향으로, 현재까지 28개의 DNP3, 1개의 Modbus, 1개의 Telegyr 취

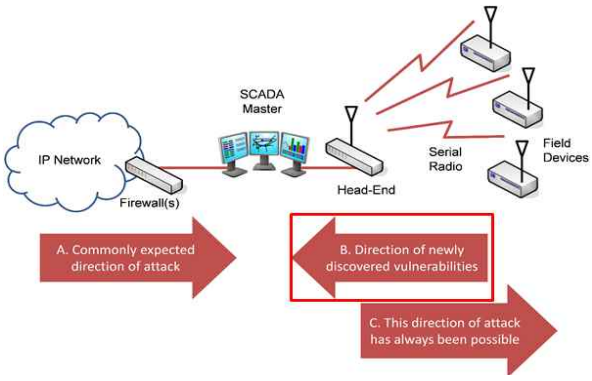

그림 3. project “Robus”의 fuzzing 테스트 방향
Fig. 3. Fuzzing test direction of project “Robus”.

표 1. 2014년에 공개된 DNP3 ICS-CERT alert
Table 1. DNP3 ICS-CERT alert published in 2014.

alert number 날짜	내 용	해당 S/W 회사
ICSA-14-098-01 2014.04.08	다수의 에러를 포함하게 조작한 IP 프래임을 마스터에 전송해 과도한 저널 메시지를 로그에 남기게 유도, 컴퓨팅 자원을 소모시켜 DNP3 프로세스에 DoS 공격을 함	OSISoft
ICSA-14-006-01 2014.01.30	gateway device에서 input에 대한 validation을 하지 않아 master에게 조작된 패킷을 보내 단시간 동안 높은 CPU 과부하를 유도, 통신을 불능으로 만듦	Schneider / Telven
ICSA-14-014-01 2014.01.14	DNP master OPC server에서 input에 대한 validation을 하지 않아 master에게 조작된 패킷을 보내 unhandled exception으로 유도, master의 프로세스 crash를 일으킴	Schneider Electric

약점이 발견되었으며 DNP3의 취약점 20개가 현재 보완되고 공개되어졌다. 아래 표 1은 2014년에 공개된 취약점 3개 항목이며, DNP 유저 그룹은 이러한 공격을 예방하기 위해 각 필드의 값의 타당성을 검사하는 문서인 “validation of incoming DNP3 data”를 2013년 12월에 발표하였다.

3-2 공개된 DNP3 취약점

Digital Bond 社에서는 일반 네트워크의 취약점을 이용, DNP3 프로토콜에 적용하여 취약점 16가지를 공개하였으며 취약점의 내용은 표 2와 같다. 또한 각 취약점을 탐지하기 위한 snort rule을 공개하였다. 취약점 V1 경우 unsolicited response 기능을 쓰지 못하게 만드는 명령 코드가 0x15인 특징을 이용하여 필드 디바이스에게 보내는 패킷 중 DNP3 패킷의 12번째 바이트(명령 코드의 위치)가 0x15라는 snort rule을 제시하였다. 단일 패킷만으로는 탐지하기 힘든 DDoS 공격의 일종인 unsolicited response storm 공격을 탐지하기 위해서는 단위 시간당 특정 패킷의 개수를 사용하는 snort rule을 제시하였다. SA나 TLS가 적용 되지 않은 DNP3 프로토콜을 사용 중인 제어 시스템에서는 이와 같은 공격이 유효하여 탐지 기법을 도입하여야 한다. 그러나 Digital Bond 社에서 제안한 snort rule은 blacklist 기반의 기법이며 새로운 취약점에 새로운 rule이 필요하며 rule이외의 공격은 탐지 할 수 없다. 또한 rule이 많아질수록 연산이 많이 요구되기 때문에 제어 시스템에 적합하지 않다고 판단된다. 따라서 본 노문에서는 데이터 마이닝 기법을 활용한 공격 탐지 방안을 제시한다.

Ⅳ. 제안하는 공격 탐지 방안

본 논문에서 제안하는 공격 탐지 방안은 데이터 마이닝 기법을 활용한 공격 탐지 방안으로 사용한 알고리즘과 탐지 모델을 어떻게 생성하였는지 설명한다.

우선 Digital Bond 社에서 공개한 취약점들로부터 중요한 필

표 2. Digital Bond 社에서 공개한 DNP3 16가지 취약점
Table 2. DNP3 16 vulnerabilities exposed by Digital Bond.

취약점명	내 용	공격 유형	공격자 유형
disable unsolicited responses (V1)	공격자는 경보와 다른 주요 이벤트를 방해하기 위해 현장제어장치의 unsolicited response 기능을 정지시킬 수 있음	불법 수정, 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 하이재킹 되거나 스푸핑 될 수 있음	불법 수정, 방해	내부 client 위장 외부 client
unsolicited response storm(V3)	제어시스템서버 또는 제어실 운영자가 처리하기 힘들 정도의 대량의 잘못된 unsolicited response를 보냄	불법 수정, 방해	내부 server 위장
cold restart from authorized (V4)or unauthorized client(V5)	공격자는 제어시스템서버의 재시작 또는 정지를 나타내는 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	가로 채기	외부 client
unauthorized write request to a PLC(V7)	비인가된 제어시스템서버는 현장제어장치의 정보를 쓰기위한 시도 가능	불법 수정, 방해	외부 client
unauthorized miscellaneous request to a PLC(V8)	비인가된 제어시스템서버는 현장제어장치에 읽기 또는 쓰기 요청외 다른 요청을 보냄	방해, 위조, 가로 채기, 불법 수정	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	불법 수정	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 서비스거부 공격을 할 수 있음	가로 채기, 불법 수정, 방해	V11: 내부 client 위장 V12 : 외부 client
points list scan(V13)	정보수집 단계에서 공격자는 가용한 DNP3 데이터 포인트 정보를 수집할 수 있음	가로 채기	내부 server위장
function code scan(V14)	정보수집 단계에서 공격자는 가용한 function code 정보를 수집할 수 있음	가로 채기	내부 server위장
time change attempt(V15)	function code 2번과 object type 50으로 공격자가 시간 정보를 위조할 수 있음	불법 수정	내부 client 위장 외부 client
failed checksum error(V16)	체크섬을 검사한 결과 체크섬이 맞지 않는 경우로 공격자가 패킷을 위조했음을 알 수 있음	불법 수정	내부 client 위장 외부 client

드들을 추출한다. snort rule에서 사용된 필드는 총 7개로 source/destination IP주소와 port 번호, DNP 시작 2바이트, DNP 목적지, DNP 명령 코드이다. 실제 변전소에서 캡처한 하루 분량의 DNP3 패킷과 공격 특성에 맞게 생성한 패킷을 필요한 필드만 추출하여 arff형식에 맞게 출력하는 c코드를 작성하여 전처리하였다. classification에 사용된 알고리즘은 alternating decision tree로 decision tree에서 decision node에 prediction node가 추가된 특징을 가지고 있다. 각 decision node의 분기마다 prediction node를 가지고 있으며 각 instance가 decision node에 의해 분기되고 분기된 prediction node의 값

표 3. 공격 패킷의 탐지 결과
Table 3. Result of attack packet detection.

공격 유형	탐지 결과	신뢰도(%)
disable unsolicited responses	공격	80.2
non-DNP3 communication on a DNP3 port	공격	58.3
cold restart from authorized client	공격	80.2
cold restart from unauthorized client	공격	95.5
unauthorized read request to a PLC	정상	61.9
unauthorized write request to a PLC	공격	95.5
unauthorized miscellaneous request to a PLC	공격	95.5
stop application	공격	80.2
warm restart	공격	80.2
broadcast request from an authorized client	공격	80.2
broadcast request from an unauthorized client	공격	95.5

을 총합하여 1과 -1에 어디에 가까운지에 따라 최종 classification된다. training set과 test set으로 각각 하루치의 실제 제어시스템에서 캡처한 DNP3 패킷과 단일 패킷으로 탐지할 수 있는 11가지의 공격 패킷을 생성하여 사용하였으며 탐지 결과는 표 3과 같다. 1000여개의 정상 패킷을 공격 패킷으로 분류한 경우는 없었으나 unauthorized read request to a PLC(programmable logic controller) 공격이 정상으로 오탐 되었다. 이는 공격의 특징이 source IP 주소만 다르며 다른 필드는 모두 정상과 같은 값을 가지기 때문에 IP 주소의 값을 내부망에 존재하지 않는 값을 넣어 공격 패킷을 생성 하였으나 IP 값이 기존 망의 IP와 차이가 아주 적은 흡사한 값인 경우 탐지가 불가능하였다. 따라서 IP 주소를 4자리를 모두 나누어 attribute로 설정한다면 1/1억의 변동치가 1/255로 늘어 확연한 차이를 보여 탐지 가능할 것으로 보인다.

Ⅴ. 결 론

DNP3 프로토콜을 위한 보안 사항은 SAv5, TLS의 암호 및 인증 기법이 있으나 가용성이 중요시 되는 제어 시스템에서 이를 적용하기는 쉽지 않으며 따라서 현재 보안 사항 없이 운행되고 있다. 본 논문에서는 데이터 마이닝 기법을 이용하여 공개된 취약점을 이용한 공격을 탐지 할 수 있는 탐지 방안을 제시 하였으며 유효성에 대해 검증하였다. 제어 시스템의 보안은 이러한 탐지 기법을 포함하여 bump-in-the-wire 기법, whitelist 기법 등을 추가적으로 적용 하여 다계층적인 보안이 필요할 것이다.

감사의 글

본 연구는 2013년도 산학협동재단의 학술연구 지원에 의하여 이루어진 연구로서, 관계부처에 감사드립니다.

참고문헌

[1] IEEE Standard for Electric Power Systems Communications-Distributed Network Protocol (DNP3), IEEE Standard Association, IEEE Std 1815-2012, 2012.10.10.

[2] G. Clarke, D. Reynders, *Practical Modern SCADA Protocol,* Newnes, pp. 66-142, 2004.

[3] DNP3 Product. [Internet]. Available: http://www.dnp.org/Pages/DnpProductsDefault.aspx?conf=y

[4] Tim Polk, Santosh Chokhani, Kerry McKay, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, NIST, U.S. Department of Commerce, NIST Special Publication 800-52 Revision 1, pp. 16-21, Sep. 2013.

[5] Adam Crain, Chris Sistrunk. Project Robus [Internet]. Available: http://www.automatak.com/robus/.

[6] Digital Bond. [Internet]. Available: http://www.digitalbond.com.

권 성 문 (Sung-moon Kwon)
2013년 2월 :아주대학교 정보 및 컴퓨터공학부 (공학사)
2013년 3월 ~ 현재 : 아주대학교 컴퓨터공학과 석사과정
※관심분야 : 스마트그리드 보안, 디지털 포렌식, 비정상행위 탐지

유 형 욱 (Hyung-uk Yoo)
2011년 8월 : 아주대학교 정보 및 컴퓨터공학부 (공학사)
2011년 9월 ~ 현재 : 아주대학교 컴퓨터공학과 통합과정
※관심분야 : 스마트그리드 보안, 디지털 포렌식, 비정상행위 탐지, 리눅스 및 안드로이드 보안

이 상 하 (Sang-ha Lee)
1987년 2월 :울산대학교 전자계산학과 (공학사), 1991년 2월 : 아주대학교 컴퓨터공학과 (공학석사)
2002년 8월 : 아주대학교 컴퓨터공학과 (공학박사), 1991년 ~ 1992년 : (주)큐닉스 컴퓨터
1993년 ~ 1999년 : (주)케이엔아이시스템,
2000년 ~ 현재 : 동서울대학 정보통신과 근무
※관심분야 : 정보통신 보안, 네트워크 관리, IPTV QoS/QoE

손 태 식 (Tae-shik Shon)
2000년 2월 : 아주대학교 정보컴퓨터공학부 (공학사), 2002년 2월 : 아주대학교 정보통신공학 (공학석사)
2005년 8월 : 고려대학교 정보보호대학원 (공학박사),
2004년 2월 ~ 2005년 2월 : University of Minnesota, Research Scholar
2005년 8월 ~ 2011년 2월 : 삼성전자 DMC 연구소 책임연구원
2011년 2월 ~ 현재 : 아주대학교 정보컴퓨터공학과 조교수
※관심분야 : 무선/모바일 네트워크 보안, WSN/WPAN, 비정상행위 탐지/기계 학습