Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.34, NO.4, Aug. 2024 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2024.34.4.615

DNP3 over TCP/IP 환경 전력 제어시스템에서의 상태추정 기반 침입 탐지 연구

최 현 호,[1†] 이 중 희[2‡]
[1,2]고려대학교 (대학원생, 교수)

A Study on State Estimation Based Intrusion Detection in Power Control Systems Using DNP3 over TCP/IP

Hyeonho Choi,[1†] Junghee Lee[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

전력계통의 변화 및 IT 기술 발전 등에 따라 통신 방식 변경에 대한 요구가 커지고 있어 시리얼 기반 통신에서 TCP/IP 기반 통신으로의 변경은 불가피하다. 하지만 TCP/IP 기반 통신의 경우 보다 다양한 보안 위협이 존재하기 때문에 정보보안 측면에서 많은 고려가 필요하다. 인증 및 암호화 등의 보안대책은 원격소 장치(RTU : Remote Terminal Unit)의 교체, 암호 알고리즘의 성능 요건 충족 등의 문제로 단기간에 적용은 불가능하다. 본 논문에서는 이러한 상황 속에서 전력 제어시스템으로의 위협을 식별하고 효과적으로 탐지하기 위해 상태추정 기반의 침입 탐지 모델을 제안하였다. 제안된 모델은 시그니처 탐지 방식에 더해 취득 데이터의 유효성을 검증함으로써 데이터 위변조 등 기존의 방법으로 탐지하기 어려운 공격들을 탐지할 수 있었다.

ABSTRACT

With the evolution of power systems and advancements in IT technology, there is an increasing demand to shift from serial-based communication to TCP/IP-based communication. However, TCP/IP communication entails various security threats, necessitating extensive consideration from an information security perspective. Security measures such as authentication and encryption cannot be rapidly implemented due to issues like the replacement of Remote Terminal Units (RTUs) and the performance requirements of encryption algorithms. This paper proposes a state estimation-based intrusion detection model to identify and effectively detect threats to power control systems in such a context. The proposed model, in addition to signature detection methods, verifies the validity of acquired data, enabling it to detect attacks that are difficult to identify using traditional methods, such as data tampering.

Keywords: DNP3, Intrusion Detection System, State Estimation, Energy Management System

I. 서 론

전력은 현대 사회에서 필수적인 요소로 길거리, 공장, 병원 등 우리가 생활하는 모든 곳에 사용되고 있다. 만약 전력 공급이 중단된다면 국가 기능 마비까지도 초래할 수 있기 때문에 전력 관련 기반시설은 중요도가 매우 높다고 할 수 있다[1].

최근 사이버 공격에 의한 전력 공급 중단 사고로는 우크라이나 사례를 들 수 있다. 2015년 BlackEnergy 악성코드 감염 및 사이버 공격으로

Received(04. 30. 2024), Modified(06. 04. 2024), Accepted(06. 05. 2024)
† 주저자, chh1124@korea.ac.kr
‡ 교신저자, j_lee@korea.ac.kr(Corresponding author)

인해 전력 공급이 중단 되었으며[2], 2016년에는 Industroyer 악성코드가 발견되었다. 다른 악성코드와 다른 점은 변전소에서 스위치나 차단기를 직접 제어할 수 있도록 설계되었다는 것이다[3]. 전력 분야 외에도 2021년에 다크사이드로부터 콜로니얼 파이프라인이 랜섬웨어 공격을 받아 석유 공급이 중단되었다[4]. 이처럼 전력망 등 기반시설이 공격을 받는다면 우리 생활에 막대한 지장을 초래하기 때문에 안정적인 운영을 위해 위협으로부터 보호가 필요하다.

과거에 이러한 기반시설은 폐쇄망으로 운영되기 때문에 공격이 어렵다고 인식되어져 왔다. 하지만 최근 다양한 기술의 도입으로 외부와의 연계 접점이 증가하고 있다. 특히 전력망의 경우 신재생 에너지 보급 및 가상 발전소 도입 등으로 인해 외부와의 연계 접점이 증가할 수 밖에 없는 구조이다[1]. 신재생에너지 발전 비중은 2030년 21.6%에서 2036년 30.6%로 증가할 것으로 전망되어 분산형 전원의 보급이 점점 확대되고 있음을 알 수 있다[5].

우리나라는 경제적인 전력 생산과 안정적인 전력 공급을 위해 계통운영시스템(EMS : Energy Management System)을 통해 전국의 발전소, 변전소의 운전 상태를 실시간 감시 및 제어하고 있으며, 전국의 중앙급전발전기 및 345kV 이상 변전소의 데이터를 시리얼 기반 DNP3 통신 및 9600bps 이상 전용선을 통해 실시간으로 취득하고 있다[6].

최근 신재생 발전기 증가 및 IT 기술 발전 등에 따라 시리얼 기반 통신에서 TCP/IP 기반 통신으로 변경에 대한 요구가 커지고 있지만, TCP/IP 기반 통신의 경우 다양한 보안 위협이 존재하고 있어 인증, 암호화 등 정보보안 측면에서 많은 고려가 필요하다.

TCP/IP 기반 통신은 시리얼 기반 통신에 비해 소수의 네트워크 장비로 여러 장치와 통신할 수 있으며 속도 또한 빠른 장점이 있지만, 시리얼 방식에서 부각되지 않았던 인증 및 암호화에 대한 문제가 단점이라고 할 수 있다. 기존 시리얼 방식은 9600bps의 저속 및 원격소 장치(RTU : Remote Terminal Unit)와 일대일 통신을 하기 때문에 인증과 암호화를 고려하지 않은 상태에서도 활용해 왔지만, TCP/IP 기반 통신으로 변경 할 경우 중간자 공격, 메세지 재전송 공격 등에 취약하다.

인증과 암호화를 적용한다 하더라도 계통운영시스템과 원격소 장치 둘 다 적용할 수 있어야 가능하며, 적용 시 통신 지연시간 발생 등의 문제가 있어 단기간에 적용은 어렵다. 하지만 빠른 속도로 주변 환경이 변화함에 따라 시리얼 기반 통신에서 TCP/IP 기반 통신으로의 전환은 불가피하기 때문에 TCP/IP 기반 통신을 적용하더라도 보안성을 확보할 수 있는 대책이 필요하다.

본 논문에서는 TCP/IP 기반 DNP3 통신을 사용하는 전력 제어시스템으로의 보안위협을 식별하고, 이를 이용한 공격을 탐지하는 침입 탐지 모델을 제안한다. 전력 제어시스템은 장애로 인한 자료 미취득 또는 설비 성능저하로 인한 오차 발생 등에 대비하여 상태추정(SE : State Estimation)을 통해 취득 데이터를 보정하여 사용하고 있다[6]. 이를 활용해 중간자 공격 등을 통한 패킷 조작 및 데이터 위변조 공격을 탐지할 수 있으며, 기존의 시그니처 기반의 탐지 방식과 함께 사용하여 식별된 보안위협에 대응할 수 있다.

본 논문의 구성은 다음과 같다. 본 논문의 2장과 3장에서는 관련 연구와 배경 지식을 기술하였으며, 4장에서는 전력 제어시스템으로의 공격 유형에 대해 서술하였다. 5장과 6장에서는 제안하는 침입 탐지 모델 및 실험 결과에 대해 설명하고, 마지막으로 결론 및 한계점에 대해 기술하였다.

II. 관련 연구

DNP3는 1990년대부터 사용된 산업용 프로토콜로 현재까지 관련 취약점 및 침입 탐지를 위한 다양한 방안들이 연구되었다.

장문수 등은 Digital Bond社에서 발표한 취약점 정보를 토대로 시리얼 기반 테스트 베드를 구성하여 실제 공격 가능 여부를 검증하였으며, 12개 취약점 중 5개 취약점이 공격 가능함을 확인하였다. 나머지 취약점은 이더넷 통신 환경 미구성 또는 현장제어장치가 기능을 지원하지 않아 확인이 불가하였으며, DNP3 프로토콜의 보안 취약점을 이용한 공격에 대응하기 위해 침입탐지시스템 도입 등을 제안하였다[7].

고폴린 등은 SCADA 시스템의 일정하고 규칙적인 트래픽 패턴에 착안하여 자기 유사성 기반의 침입 탐지 방법론을 제안하였다. 해당 연구에서는 알려지지 않은 공격도 탐지가 가능한 장점이 있으나 어떤 공격이 발생했는지는 알 수 없는 한계가 있었다. 또한 자기 유사성의 변화를 주지 않는 공격은 탐지하기

가 어렵기 때문에 시그니처 기반의 오용탐지를 결합한 하이브리드 침입탐지시스템을 제작하였다[8].

윤정한 등은 버스트 특성을 기반으로 이상 탐지 화이트리스트 모델을 제안하였으며, 실제 스카다 시스템의 네트워크 트래픽으로 화이트리스트 규칙을 추출하였다. 공격 트래픽은 화이트리스트 규칙에 포함되지 않은 버스트를 생성하기 때문에 화이트리스트 모델을 이용하여 탐지할 수 있음을 확인하였다[9].

권성문 등은 데이터 마이닝 기법을 활용한 공격탐지 방안을 제안하였다. 실제 변전소 패킷에서 중요 필드를 추출하여 Digital Bond社에서 발표한 11가지 취약점에 대해 탐지를 시도하였고, 대부분의 공격을 탐지하여 유효성을 검증하였다. 하지만 정상 패킷에서 출발지 IP만 변조한 공격은 탐지하지 못하는 한계가 있었다[10].

김명종 등은 화이트리스트 기반의 침입 탐지 방안을 제안하였다. Digital Bond社에서 발표한 취약점을 토대로 Snort 화이트리스트 룰을 만들어 실험환경에서 테스트하였다. 테스트 결과 탐지는 성공적이었지만 다른 공격도 탐지하기 위해서는 분석을 통해 규칙을 추가해야 하는 한계가 있었다[11].

Egger 등은 IEC 60870-5-104 기반 테스트 변전소 패킷을 이용하여 지도 학습, 준지도 학습, 비지도 학습, 시그니처 기반 탐지 등 네 가지 방법론을 비교하였다. 준지도 학습이 일부 오탐을 제외하면 성능이 제일 훌륭했고 시그니처 기반 탐지와 지도 학습의 경우 오탐은 전혀 없었으나, 새로운 공격을 탐지할 수는 없었다. 특히 시그니처 기반 탐지의 경우 Nessus 공격의 패킷이 TLS(Transport Layer Security)로 암호화 되어 전혀 탐지를 못하는 문제가 있었다. 해당 연구에서는 여러 원격소 장치 및 스카다 시스템으로 구성된 복잡한 환경에서 정확도를 유지하려면 비지도 접근 방식의 성능 향상이 필요하다고 제안하였다[12].

Wlazlo 등은 Snort 기반으로 테스트 베드에서 중간자 공격 탐지를 실험하였다. 평균 왕복 시간(RTT), 재전송 속도 등을 지표로 활용하여 탐지할 수 있음을 보였으나, 규칙 선택 기준에 따라 오탐률에 차이가 있었다. 또한 처리 시간을 줄이는 등 공격자가 완벽하게 준비한다면 공격 탐지가 어려울 수 있다는 한계가 있었다[13].

Altaha 등은 공격자가 Function Code를 악용해 시스템을 조작한다는데 착안하여 TCP 특성과 Function Code 빈도를 지표로 활용하는 Autoencoder 기반의 이상 탐지 방안을 제안하였다. 실제 변전소 데이터를 활용한 데이터 셋을 기반으로 검증한 결과 단순히 TCP 연결 특성에 의존하는 것보다 더 나은 방안임을 확인하였다[14].

Kelli 등은 DNN 기반 다중 모델 침입 탐지 시스템을 제안하였다. 시뮬레이션 환경에서 Cold Restart 등 8가지 DNP3 공격에 대해 검증하였고, DNP3 관련 프로토콜 속성이 포함된 네트워크 트래픽을 활용하는 것이 TCP/IP 기반 트래픽을 활용하는 것보다 훨씬 높은 정확도를 보임을 알 수 있었다[15].

권희용 등은 시그니처 기반 방법과 행위 기반 방법을 결합한 하이브리드 이상 탐지 방법을 제안하였다. 수처리 시스템의 SWaT 데이터 세트를 이용하여 실험을 하였으며, 하이브리드 방식이 행위 기반 단독 방식보다 정밀도가 높고 처리 시간이 단축 되었다. 하지만 이상현상이 발생했다는 사실만을 탐지할 뿐 어떤 센서나 액츄에이터가 공격 받았는지 알 수 없다는 한계가 있었다[16].

III. 배경 지식

3.1 DNP3 개요

DNP(Distributed Network Protocol)3는 해리스(Harris)의 Distributed Automation Products에서 개발된 산업용 프로토콜로 서로 다른 컴퓨터 간의 데이터 수집 정보 및 제어 명령의 전송을 최적화하기 위해 설계되었으며 주로 전력, 수도, 가스 등의 산업에서 사용되고 있다[17]. 시리얼 방식 뿐만 아니라 TCP/IP 기반의 DNP3도 사용할 수 있으며, 인터넷 기술을 활용해 멀리 떨어진 장치 간의 경제적인 데이터 수집 및 제어가 가능하다[18].

Fig. 1.은 DNP3 Exchange Samples를 참고하여 전력 제어시스템의 시각 동기화 요청 패킷을 표현한 것이다[19].

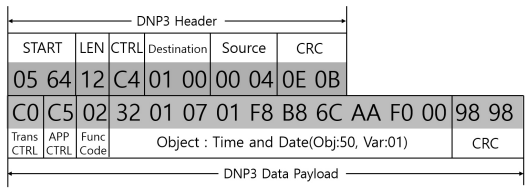

Fig. 1. DNP3 Request Packet

DNP3 요청 패킷은 헤더와 데이터 영역으로 구성되며, 헤더는 0x05 0x64로 시작하여 패킷 길이, 출발지, 목적지 주소, CRC(Cyclic Redundancy Check) 등으로 구성되어 있다. 데이터 영역은 Function Code, Object, CRC 등으로 구성되어 있으며 Object는 프로토콜에서 정한 데이터 유형을 말한다. 표현된 패킷은 전력 제어시스템(주소 : 1024, 0x0400)이 원격소 장치(주소 : 1, 0x0001)에게 시각 동기화를 위해 Time and Data를 Write(Function Code : 0x02)하라는 명령을 전송하고 있다. DNP3의 Function Code는 이외에도 Confirm, Read, Select, Operate, Restart, Enable and Disable Unsolicited Messages 등이 있다[19].

통신 방식은 전력 제어시스템에서 요청을 보내면 원격소 장치가 응답하는 구조이며 이를 폴링이라 한다. 기본적으로 전력 제어시스템에서만 요청을 보낼 수 있으며 원격소 장치 단독으로 동작할 수는 없다. 하지만 Unsolicited Response를 사용하면 전력 제어시스템의 요청 없이도 원격소 장치의 상태 변화를 알려줄 수 있다. Unsolicited Response 사용 시 고려사항으로는 메세지 발생 빈도가 많지 않아야 한다는 것이다. 그렇지 않을 경우 많은 충돌이 발생할 수 있으며, 이 경우에는 전력 제어시스템의 폴링을 통해 데이터를 요청하는 것이 더 안정적이다[18].

3.2 공개된 DNP3 취약점

Digital Bond社에서는 DNP3 프로토콜 취약점을 Snort 기반 침입 탐지 규칙과 함께 공개하였으며, 취약점의 내용은 Table 1.에 요약하였다[20].

공개된 취약점을 전력 제어시스템 공격 가능 여부를 기준으로 분석한 결과 대부분 원격소 장치의 서비스 거부 공격, 정보 탈취 및 비인가 명령 전송 취약점 등으로 구성되어 있었다. DNP3 통신의 경우 전력 제어시스템에서 원격소 장치로 요청을 해야 응답하는 구조이기 때문에 14개의 취약점 중 단 2개만이 전력 제어시스템 서버에 실제 침해시도를 할 수 있을 것으로 보였고, 해당 취약점은 Non-DNP3 Communication on a DNP3 Port와 Unsolicited Response Storm이다.

Non-DNP3 Communication on a DNP3 Port는 제시된 항목 중에 유일하게 양방향으로 탐지 정책을 수립한 취약점으로 전력 제어시스템과 원격소 장치 모두에 영향을 미칠 수 있다. 특히 TCP/IP 환경에서 하이재킹이나 스푸핑이 일어날 수 있으며, 이 경우에는 DNP3 형식을 따르지 않는 패킷을 사용할 가능성이 있다. 모든 DNP3 패킷은 0x05 0x64로 시작하기 때문에 DNP3 포트로 통신하는 패킷 중 이와 일치 하지 않는 패킷은 공격을 의심해야 한다.

DNP Technical Committee에서는 DNP3 패킷의 유효성 검증을 위해 Validation of Incoming DNP3 Data 문서를 2013년 12월 11일에 발표하였고, 현재 최신 버전은 2014년 8월 13일에 발표된 AN2013-004b 버전이다.

Unsolicited Response Storm은 DNP3 통신에서 유일하게 원격소 장치가 먼저 전력 제어시스템에 정보를 보낼 수 있는 Unsolicited Response 기능을 이용한 공격이다. 전력 제어시스템이 처리하기 힘들 정도로 대량의 Unsolicited Response를 보낼 경우 전력 제어시스템 서비스 방해 공격이 가능하다.

3.3 전력 제어시스템 구성

전력계통의 안정적 운영과 효율적인 제어를 위해서 SCADA(Supervisory Control And Data Acquisition) 기능이 탑재된 전력 제어시스템을 사용한다[21]. 우리나라에서는 계통운영시스템을 예로 들 수 있으며, 중앙급전발전기와 345kV 이상 변전소는 원격소 장치(RTU)로부터 직접 취득을 하고 154kV 변전소는 지역계통운영센터(RCC : Regional Control Center)를 통해 취득하고 있다[6]. 이렇게 취득한 데이터를 기반으로 경제적인 전력 생산과 안정적 전력 공급에 기여하고 있으며, 계통운영시스템의 데이터 취득 현황은 Fig. 2.에서 볼 수 있다.

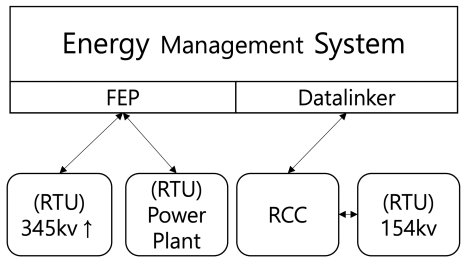

Fig. 2. Status of Data Acquisition in EMS

Table 1. Description of Digital Bond's DNP3 Vulnerabilities

Vulnerability Name	Description
Disable Unsolicited Responses	Attackers may disable the Unsolicited Response feature to disrupt reception of critical events, such as status change notifications from field control devices.
Non-DNP3 Communication on a DNP3 Port	The connection established between the control system server and field control devices can be spoofed or hijacked, serving as a means of attack.
Unsolicited Response Storm	An excessive volume of Unsolicited Response messages, beyond the capacity for processing by the control system server, can be generated to disrupt services.
Cold Restart From Authorized Client	Authorized control system servers can send restart or stop commands to field control devices, rendering them unavailable.
Cold Restart From Unauthorized Client	Attackers can send restart or stop commands to field control devices, rendering them unavailable, thus disrupting services
Unauthorized Read Request to a PLC	Attackers may attempt to retrieve information from field control devices.
Unauthorized Write Request to a PLC	Attackers may attempt to write information to field control devices.
Unauthorized Miscellaneous Request to a PLC	Attackers may attempt to request different functionalities from field control devices.
Stop Application	Sending a service stop command to field control devices can halt the application.
Warm Restart	Sending a service restart command to field control devices can initiate device reconfiguration and delete events.
Broadcast Request from Authorized Client	Authorized control system servers can send broadcast request packets to the field control device network to obtain addresses or launch denial-of-service attacks.
Broadcast Request from Unauthorized Client	Attackers can send broadcast request packets to the field control device network to obtain addresses or launch denial-of-service attacks.
Points List Scan	Attackers can send request messages with Point addresses to collect DNP3 data point information through the IIN(Internal Indications) field in response packets.
Function Code Scan	Attackers can send request messages with Function Codes to collect available Function Code information through the IIN field in response packets.

3.4 상태추정

상태추정이란 취득한 데이터와 네트워크 모델을 사용하여 전력계통의 전압, 조류 등의 현재 상태를 추정하는 방법으로 가중최소자승법 등 수학적 알고리즘을 사용한다. 가중최소자승법은 항공우주분야에도 사용되고 있으며, 전력계통의 상태 파악 및 감시 목적으로도 쓰여지고 있다[22].

전력은 인입되는 양과 인출되는 양이 같아야 하기 때문에 측정되는 MW값을 모두 더하면 0MW에 가까워야 한다. 하지만 합이 맞지 않는 경우 취득 데이터가 이상하다고 볼 수 있으며, 이를 이용하여 전력계통 내 설비들의 데이터 정상 취득 여부를 검증 할 수 있다[23].

입력값으로는 계통 구성요소의 상태와 측정값 및 발전기 데이터 등이 있으며, 취득 데이터의 오류를 제거하여 모선 전압, MW/MVAr 조류값, 발전량, 부하량 등의 상태를 추정할 수 있다[22].

Table 2. Jeju-Haenam HVDC State Estimation Results

Line	Haenam C/S		Jeju C/S	
	Values	State Estima-tion	Values	State Estima-tion
1[MW]	35.6	36.0	36.4	36.0
2[MW]	35.8	36.4	36.9	36.3

우리나라에서는 계통운영시스템을 활용하여 전력계통을 실시간으로 감시·제어하고 있으며, 현장제어장치 성능저하로 인한 오차 발생 및 시스템 또는 통신구간 장애로 인한 데이터 미취득에 대비하여 매 1분 주기로 상태추정을 시행하고 있다. 수행시간은 10~20초로 최대 허용 편차는 50MW이며 연간 일평균 수렴율은 약 99%이다[24].

Table 2.는 한국형 에너지관리시스템(K-EMS) 개발 당시 제주-해남 HVDC(High Voltage Direct Current transmission system) 상태추정 결과이며, 실제 측정값과 비교했을 때 유사함을 확인할 수 있다[25].

IV. 전력 제어시스템으로의 공격 유형

전력 제어시스템에서 원격소 장치로 통신을 요청하는 프로토콜 특성상 전력 제어시스템으로의 연결요청은 없기 때문에 원격소 장치에서 전력 제어시스템으로의 공격은 존재하지 않는다고 볼 수 있다. 비인가 접근 시도 또한 방화벽을 통한 접근제어가 가능하다. 이러한 측면에서 바라보았을 때 전력 제어시스템으로의 공격 유형은 Fig. 3.과 같이 정리할 수 있다.

4.1 패킷 조작 공격

전력 제어시스템의 요청에 대해 원격소 장치의 응답 시 메세지를 규격과 맞지 않게 만들거나 조작된 패킷을 보냄으로써 전력 제어시스템에 버퍼 오버플로우 공격이나 시스템 이상을 유발할 수 있다. 원격소 장치 1대의 비정상적인 응답으로 전력 제어시스템에 영향을 준다면 전체 데이터 취득에 문제가 생길 수 있기 때문에 주의가 요구된다.

4.2 데이터 위변조 공격

전력 제어시스템은 원격소 장치의 데이터를 실시간으로 취득하고 있다. 취득 데이터로는 선로 전압, 조류, 주파수, 차단기 상태 등이 있으며 이러한 데이터는 전력계통을 운영하는데 있어서 중요한 데이터이다. 위변조된 데이터가 취득될 경우 스카다 시스템의 역할 자체가 무의미해 질 수 있으며, 잘못된 데이터를 기반으로 설비를 조작할 경우 전체 전력망이 붕괴되는 사태가 올 수도 있다.

4.3 Unsolicited Response Storm 공격

Unsolicited Response는 원격소 장치가 전력 제어시스템의 요청 없이도 상태 변화를 전송할 수 있는 기능이다. 메세지를 보낼 때 전력 제어시스템이 처리하기 힘들 정도로 대량의 Unsolicited

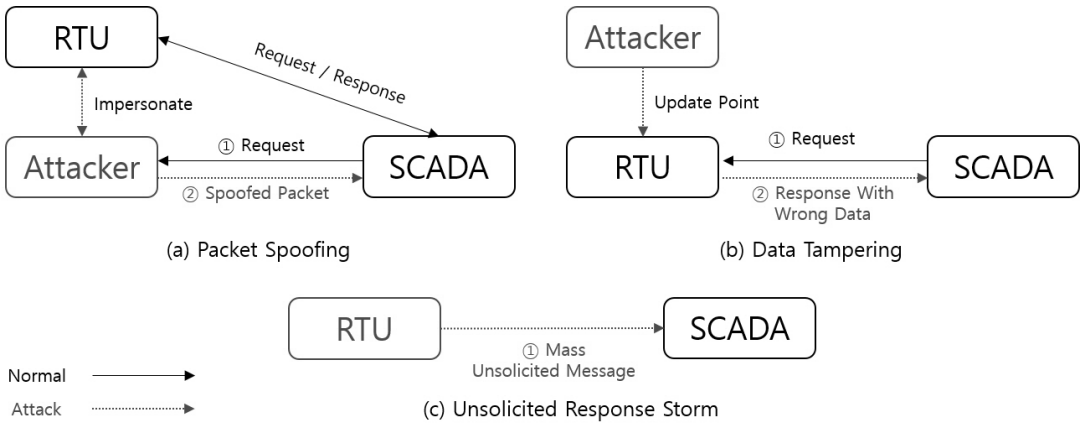

Fig. 3. Process of three attacks in DNP3 over TCP/IP

Message를 보낸다면 서비스 거부 공격이 될 수 있다.

DNP3 통신에서 Unsolicited Message가 자주 생성되는 것은 시스템에 악영향을 끼칠 수 있으며, DNP Users Group에서도 폴링 방식으로 데이터를 업데이트 하는 것이 더 적절하다고 명시하고 있다[18].

V. 제안하는 침입 탐지 모델

본 논문에서는 전력 제어시스템으로의 보안 위협에 대응하기 위해 기존 시그니처 기반 탐지에 상태추정 기반 탐지를 결합한 침입 탐지 모델을 TCP/IP 기반 DNP3 네트워크에서 활용할 것을 제안한다.

전국의 발전 및 송변전 설비는 전력계통 상황에 따라 운전 상태가 다르기 때문에 발전량 등의 데이터가 규칙적이지 않아 검증이 어렵지만, 상태추정 기반 탐지는 취득 데이터를 바탕으로 데이터의 유효성을 검증할 수 있다는 특징이 있다. 전력은 인입지점과 인출지점의 값이 같기 때문에 취득 포인트의 주변 데이터를 이용해 해당 값을 예측할 수 있다. 이를 통해 암호화 및 인증이 구현되어 있지 않은 환경에서 데이터를 보내는 원격소 장치를 특정할 수 없지만 값을 검증함으로써 유효한 데이터인지 확인할 수 있다.

본 논문에서 제안한 침입 탐지 모델은 시그니처 기반의 침입탐지시스템에서 얻은 탐지 결과에 상태추정을 활용한 데이터 검증 단계를 추가했으며 Fig. 4.에서 볼 수 있다.

패킷이 전력 제어시스템이나 원격소 장치에 도달하기 전에 시그니처 기반 탐지 규칙을 활용하여 1차적으로 탐지를 수행하고 전력 제어시스템에서 취득한 데이터를 기반으로 상태추정 기반 탐지를 2차 수행한다.

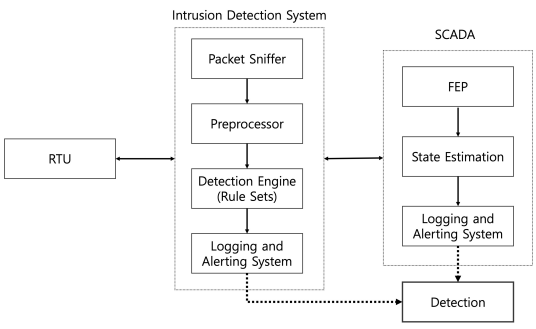

Fig. 4. Proposed Intrusion Detection Model

시그니처 기반 탐지와 상태추정 기반 탐지 결과를 종합하여 둘 중에 하나 또는 둘 다 탐지될 경우 공격으로 간주할 수 있다. IT 기반의 탐지 방법인 Snort 활용 네트워크 패킷 탐지에 OT 기반의 전력 제어시스템 데이터를 추가 검증함으로써 데이터 위변조 공격도 탐지가 가능하다.

5.1 시그니처 기반 탐지

전력 제어시스템으로의 보안위협을 탐지하기 위해 Digital Bond社에서 발표한 취약점 및 탐지 규칙[20]을 참고하여 Table 3.과 같이 Snort 기반 탐지 규칙을 작성하였다.

기존에 공개된 탐지 규칙은 대부분 원격소 장치의 위협을 방어하는 규칙이 대다수이며, 새로운 탐지 규칙 작성 시에는 전력 제어시스템으로의 공격을 탐지할 수 있는 규칙을 우선 고려하였다.

기존 공개된 규칙 중에는 Non-DNP3 Communication on a DNP3 Port와 Unsolicited Response Storm이 포함되어 있는데 각각 패킷 조작 공격과 Unsolicited Response Storm 공격과 연관되어 있다. 특히 Non-DNP3 Communication on a DNP3 Port는 하이재킹이나 스푸핑 공격을 위해 패킷을 조작하는 과정 중 탐지될 수 있으며 전력 제어시스템과 원격소 장치 모두 영향을 미칠 수 있기 때문에 양방향 탐지 룰을 설정하였다.

또한 전력 제어시스템과 원격소 장치간 DNP3 통신 시 각각 고유의 주소를 사용하는데 통신 방향에 따라 Source Address와 Destination Address를 지정하고 있다. 원격소 장치는 여러 대이기 때문에 요청, 응답 시마다 다양한 값이 오가지만 전력 제어시스템의 주소는 오직 하나이기 때문에 다른 값으로 요청을 보내거나 응답이 온다면 위변조된 패킷으로 판단 할 수 있다.

5.2 상태추정 기반 탐지

전력 제어시스템의 상태추정 기능을 활용한 탐지 방안이다. 상태추정은 전력 제어시스템으로 취득되는 데이터가 현장 기기 노후화 또는 네트워크 상태에 따라 잘못된 정보가 취득될 때 오류를 보정하기 위해 사용하는 방법이다. 상태추정을 통해 전력 제어시스템으로 취득되는 현장 제어장치 데이터의 유효성 여

Table 3. Signature-based Snort Detection Rules

Detection Name	Detection Rules
Non-DNP3 Communication on a DNP3 Port	alert tcp SCADA_IP any → RTU_IP DNP3_PORTS (flow:from_client; pcre:"/(?!\x05\x64)/iAR";)
Non-DNP3 Communication on a DNP3 Port(R)	alert tcp RTU_IP DNP3_PORTS → SCADA_IP any(flow:from_server; pcre:"/(?!\x05\x64)/iAR";)
Unsolicited Response Storm	alert tcp RTU_IP DNP3_PORTS → SCADA_IP any(flow:from_server; content:"|82|"; offset:12; depth:1; threshold: type threshold, track by_src, count 5, seconds 10;)
Wrong Source Address from SCADA	alert tcp SCADA_IP any → RTU_IP DNP3_PORTS (flow:from_client; content:"|05 64|"; depth:2; content:! "Source Address"; distance:4; within:2;)
Wrong Destination Address from RTU	alert tcp RTU_IP DNP3_PORTS → SCADA_IP any (flow:from_server; content:"|05 64|"; depth:2; content:!"Destination Address"; distance:2; within:2;)

부를 판단할 수 있다.

상태추정 결과 값으로는 모선 전압 크기 및 위상각, MW/MVAr 조류값, 발전량, 부하량 등이 있으며[22], 모선별 mismatch(모선 기준 MW 값의 합은 0), 상태체크를 통한 취득이상 개소 판단 및 차단기 상태도 판단할 수 있다[23].

전력 제어시스템에서는 취득 데이터를 기반으로 매 1분 마다 상태추정을 수행하며, 탐지 시에는 원격소 장치에 어떤 부분이 문제인지를 확인할 수 있기 때문에 빠르게 이상 포인트를 찾을 수 있다.

현장 취득 값과 상태추정 결과가 기준치 이상으로 차이 날 경우 취득 데이터에 이상이 있다고 볼 수 있으며, 차단기 정보 같은 경우에는 ON/OFF 두 종류만 존재하기 때문에 명확하게 탐지가 가능하다.

VI. 실험 방법 및 결과

본 논문에서 제안하는 침입 탐지 모델의 성능을 검증하기 위해 TCP/IP 기반 DNP3 통신을 사용하는 전력 제어시스템 환경에서 실험을 수행하였다. 패킷 조작 공격, 데이터 위변조 공격, Unsolicited Response Storm 공격에 대해 실험을 수행 후 결과를 정리하였다.

6.1 패킷 조작 공격 탐지

패킷 조작 공격은 전력 제어시스템과 원격소 장치 중간에서 패킷을 조작하는 공격이다. 전력 제어시스템에서 원격소 장치로 연결을 시도할 때 패킷을 조작 후 탐지 여부를 확인하였다.

실험은 공격자가 전력 제어시스템에서 요청 패킷을 수신 후 원격소 장치의 IP 주소를 변조하여 원격소 장치로 패킷을 보내 전력 제어시스템으로 응답하도록 구성하였다.

실험 결과 전력 제어시스템의 요청에 변조한 IP를 가진 원격소 장치는 응답을 하였고 원래 요청을 했던 원격소 장치가 아닌 다른 장치의 데이터를 수신하였다. Fig. 5.는 패킷 조작 공격 과정을 나타내고 있다.

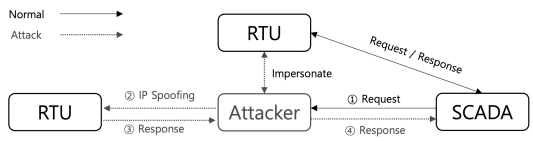

Fig. 5. Process of Packet Spoofing Attack

패킷 조작 공격 탐지 결과는 Table 4.와 같다.

Table 4. Detection Result of Packet Spoofing Attack

Type	Signature	State Estimation	Result
Packet Spoofing	None	MW, CB Status Error	Attack

전력 제어시스템의 요청 패킷 변조로 인해 다른 원격소 장치가 응답하였지만 정상적인 DNP3 패킷이었기 때문에 시그니처 기반 탐지에서는 탐지가 되

지 않았다. 하지만 전혀 다른 장치의 데이터가 수신되었기 때문에 상태추정 기반 탐지에서는 MW, 차단기 상태 등 취득되는 전체 데이터가 상태추정 결과와 전혀 다른 것을 확인할 수 있었다.

6.2 데이터 위변조 공격 탐지

데이터 위변조 공격은 원격소 장치의 데이터를 조작하는 공격이다. 전력 제어시스템에서 원격소 장치에 데이터를 요청하면 공격자에 의해 조작된 데이터를 전송하여 탐지 여부를 확인하였다.

실험은 공격자가 원격소 장치의 데이터 포인트 순서를 변경한 이후 전력 제어시스템에서 요청 패킷을 수신하고 원격소 장치가 조작된 데이터를 전력 제어시스템으로 응답하도록 구성하였다.

실험 결과 전력 제어시스템의 요청에 원격소 장치는 정상 응답을 하였지만 공격자에 의해 포인트 순서가 변경된 데이터를 수신하였다. Fig. 6.은 데이터 위변조 공격 과정을 나타내고 있다.

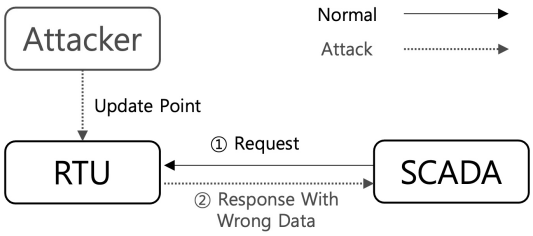

Fig. 6. Process of Data Tampering Attack

데이터 위변조 공격 탐지 결과는 Table 5.와 같다.

Table 5. Detection Result of Data Tampering Attack

Type	Signature	State Estimation	Result
Data Tampering	None	CB Status Error	Attack

공격자의 원격소 장치 데이터 포인트 순서 변경으로 인해 전력 제어시스템은 조작된 데이터를 수신하였다. 데이터 위변조 공격 또한 패킷 조작 공격과 같이 정상적인 DNP3 패킷이었기 때문에 시그니처 기반 탐지에서는 탐지가 되지 않았다. 하지만 포인트 순서가 변경되어 개방된 차단기는 투입상태로 투입된 차단기는 개방상태로 표시 되었으며, 상태추정 기반 탐지에서는 차단기 상태 이상으로 탐지되었다.

6.3 Unsolicited Response Storm 공격 탐지

Unsolicited Response Storm 공격은 원격소 장치가 Unsolicited Response 메세지를 다량으로 발생시켜 전력 제어시스템을 마비시키는 공격이다.

공격 탐지 여부 확인을 위해 전력 제어시스템으로 수신되는 원격소 장치의 Unsolicited Response 메세지를 대상으로 실험을 수행하였다.

실험 결과 다량으로 Unsolicited Response 메세지를 보내는 원격소 장치를 확인하였으며, Fig. 7.은 Unsolicited Response Storm 공격 과정을 나타내고 있다.

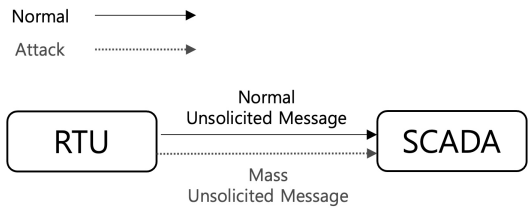

Fig. 7. Process of Unsolicited Response Storm Attack

Unsolicited Response Storm 공격 탐지 결과는 Table 6.과 같다.

Table 6. Detection Result of Unsolicited Response Storm Attack

Type	Signature	State Estimation	Result
Unsolicited Response Storm	Unsolicited Response Storm	None	Attack

탐지된 Unsolicited Message는 1초에 4번씩 수신되어 Unsolicited Response Storm 공격으로 탐지 되었으며, 분석 결과 원격소 장치에 문제가 있어 메세지를 지속적으로 보내는 것을 확인할 수 있었다. 탐지 규칙의 임계값은 10초 동안 5번이며, 본 공격은 네트워크 관련 공격으로 시그니처 기반 탐지에서 탐지가 되었으나 상태추정 기반 탐지에서는 탐지되지 않았다.

6.4 기존 침입탐지 방안과 비교

DNP3 통신 네트워크에서 침입 탐지를 위해 다양한 방안들이 이제까지 연구되었다. 초기에는 시그니처 기반 탐지가 주를 이뤘으며, 최근에는 프로토콜의 주기적, 규칙적 특성을 이용한 비정상행위 기반 탐지 방법들이 연구되고 있다.

시그니처 기반 탐지의 경우 오탐은 없었으나 새로운 공격을 탐지할 수는 없었으며, 탐지율을 높이기 위해서는 추가 규칙 개발이 필요하다[12]. 비정상행위 탐지의 경우 Function Code, DNP3 프로토콜 속성 등을 기반으로 탐지가 이루어 졌고 데이터의 변조보다는 비인가 명령 탐지가 주를 이루었다[14][15]. 또한 알려지지 않은 공격도 탐지할 수 있는 장점이 있으나, 이상현상이 발생했다는 사실만을 탐지할 뿐 어떠한 공격을 받았는지 알 수 없는 문제가 있었다[8][16].

시그니처 기반 탐지와 비정상행위 기반 탐지 방법을 함께 적용한 경우에는 비정상행위 기반 탐지 방식을 단독으로 적용한 경우 보다 정밀도가 높고 처리 시간이 단축되었다[16]. 이를 통해 시그니처 기반 탐지방식과 비정상행위 기반 탐지방식은 각각의 장·단점이 있음을 알 수 있다.

하지만 위 두 가지 방법으로는 전력 제어시스템으로의 공격을 탐지하는데는 한계가 있다. 특히 데이터 위변조 공격에 대한 대응이 어려운데, 정상적인 패킷에 데이터만 변조했을 경우 탐지해 내기가 어렵기 때문이다. 시그니처 기반의 탐지 방식은 처리 시간을 줄이는 등 정상과 가깝게 통신하게 되면 공격 탐지가 어려울 수 있으며[13], 비정상행위 탐지 방법도 주로 DNP3 속성에 의해서 탐지하기 때문에 정상과 비슷한 중간자 공격에 대한 탐지가 어렵다. 논문에서 테스트한 취약점도 Function 관련 항목들 위주였다[14][15]. DNP3 프로토콜의 사례는 아니지만 차량용 SOME/IP 통신에서의 ClientId Spoofing 공격 또한 패킷 포맷 및 전송방식은 정상 패킷과 같아 미탐이 발생하기 쉬운 유형으로 탐지율이 다소 낮았다[26].

위와 같이 기존의 연구에서는 비인가 명령 전송, 프로토콜 속성을 통한 탐지 등을 주로 연구했었으며 데이터 위변조 공격의 경우 패킷의 형태가 같고 내용만 다른 형태라 탐지해 내기가 어려웠었다.

본 논문에서 제안한 상태추정 기반 탐지는 취득 데이터를 기반으로 값을 검증하기 때문에 패킷 및 데이터 변조 공격에도 탐지가 가능하다. 또한 어떤 원격소 장치의 포인트가 문제인지도 식별이 가능해 공격이 탐지될 경우 차단 등 조치도 신속하게 이루어질 수 있을 것이라 생각된다.

VII. 결 론

본 논문에서는 TCP/IP 기반 DNP3 통신을 사용하는 전력 제어시스템으로의 공격 유형을 정의하고 탐지할 수 있는 방안을 제안하였다. 제안한 탐지 방안을 실험한 결과 시그니처 기반 탐지와 함께 상태추정 기반 탐지를 활용하여 서비스 거부 공격 뿐만 아니라 패킷 조작 및 데이터 위변조 공격도 탐지가 가능하였다. 특히 상태추정 기반 탐지 방식은 전력 제어시스템의 데이터를 사용하는 방식이기 때문에 암호화 프로토콜을 적용하더라도 지속적으로 사용가능한 방법이다.

전력 제어시스템의 경우 데이터 취득 주기가 2초로 짧기 때문에 공격이 탐지되는 즉시 문제를 파악하여 대응할 필요성이 있다. 본 논문에서 제안한 방식은 시그니처 및 상태추정 기반 탐지를 사용함으로써 문제가 있는 부분은 즉시 확인 할 수 있는 체계를 갖추고 있다. 물론 규칙이 등록되지 않으면 탐지할 수 없는 한계점도 있지만 결과를 명확히 확인할 수 있기 때문에 가용성이 우선인 제어시스템에서의 대응측면에서는 더욱 적절하다고 볼 수 있다.

하지만 상태추정에서 확인하지 못하는 오류가 발생할 경우 제안하는 방법 또한 제한적일 수 밖에 없으며, 데이터에 대한 값을 검증하는 방식이기 때문에 현장장치의 오류인지 네트워크상의 문제인지 확인하기가 어렵다. 또한 중간자 공격 등을 통해 패킷을 변조하더라도 취득 데이터가 정상 범위에 속한다면 탐지가 어렵기 때문에 인증과 암호화가 없는 환경에서 이와 같은 공격을 방어하는 것은 어려움이 있을 것이라 생각된다.

그럼에도 불구하고 인증과 암호화를 당장 도입하기 어려운 상황 속에서 제안하는 탐지 방법은 즉시 적용가능한 수단이라고 생각되며, IT와 OT의 정보를 융합해 보안관제를 수행하는 좋은 예가 될 수 있다고 생각한다.

향후에는 DNP Users Group에서 밝힌 DNP3 유효성 검증을 기반으로한 Snort 탐지 규칙 개발 및 추가 적용함으로써 조작된 패킷을 보다 정교하게 방어할 수 있는 체계를 구축하고, 취득 데이터 변조

시 원인 구간 파악을 위한 주-예비 시스템 데이터 연계 분석 등 탐지율을 높이기 위한 연구를 진행할 계획이다.

References

[1] Monthly Electrical Journal, "Cyber Threats and Security Strategies in the Intelligence of Power Grids", http://www.keaj.kr/news/articleView.html?idxno=5126, Accessed: Apr. 2024.

[2] Cybersecurity and Infrastructure Security Agency, "Cyber-Attack Against Ukrainian Critical Infrastructure", https://www.cisa. gov/news-events/ics-alerts/ir-alert-h-16-056-01, Accessed: Apr. 2024.

[3] ESET, "WIN32/INDUSTROYER: A new threat for industrial control systems", https://web-assets.esetstatic.com/wls/2017/06/Win32_Industroyer.pdf, Accessed: Apr. 2024.

[4] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A Review of Colonial Pipeline Ransomware Attack," 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW), pp. 8-15, May. 2023.

[5] Ministry of Trade, Industry and Energy, The 10th Basic Plan for Long-term Electricity Supply and Demand (2022-2036), Jan. 2023.

[6] Korea Power Exchange, Electricity Market Operation Regulations, Feb. 2024.

[7] Moon-su Jang, Gun-hee Lee, Sin-kyu Kim, Byung-gil Min, Woo-nyon Kim, and Jung-taek Seo, "Testing Vulnerabilities of DNP3," Journal of Security Engineering, 7(1), pp. 15-28, Feb. 2010.

[8] Pauline Koh, Hwa-jae Choi, Se-ryoung Kim, Hyuk-min Kwon, and Huy-kang Kim, "Intrusion Detection Methodology for SCADA system environment based on traffic self-similarity property," Journal of The Korea Institute of Information Security & Cryptology, 22(2), pp. 267-281, Apr. 2012.

[9] Jeong-han Yun, Sung-ho Jeon, Kyoung-ho Kim, and Woo-nyon Kim, "Burst-based Anomaly Detection on the DNP3 Protocol," International Journal of Control and Automation, vol. 6, no. 2, pp. 313-324, Apr. 2013.

[10] Sung-moon Kwon, Hyung-uk Yoo, Sang-ha Lee, and Tae-shik Shon, "DNP3 Protocol Security and Attack Detection Method," Journal of Advanced Navigation Technology, 18(4), pp. 353-358, Aug. 2014.

[11] Myung-jong Kim, Sung-moon Kwon, Woo-yeon Jo, and Tae-shik Shon, "WhiteList-based DNP3 Intrusion Detection System for SCADA," Proceedings of the Korea Information Processing Society Conference, pp. 228-231, Nov. 2016.

[12] E. Michael, E. Günther, and E. Dominik, "Comparison of approaches for intrusion detection in substations using the IEC 60870-5-104 protocol," Energy Informatics, vol. 3, no. S1, pp. 1-17, Oct. 2020.

[13] W. Patrick, S. Abhijeet, M. Zeyu, H. Hao, G. Ana, D. Kather-ine, and Z. Saman, "Man-in-the-middle attacks and defence in a power system cyber-physical testbed," IET Cyber-Physical Systems, vol. 6, no. 3, pp. 164-177, Apr. 2021.

[14] M. Altaha and S. Hong, "Anomaly Detection for SCADA System Security Based on Unsupervised Learning and Function Codes Analysis in the DNP3 Protocol," Electronics, vol. 11, no. 14,

July. 2022.
[15] V. Kelli, P. Radoglou-Grammatikis, A. Sesis, T. Lagkas, E. Fountoukidis, E. Kafetzakis, I. Giannoulakis, and P. Sa-rigiannidis, "Attacking and Defending DNP3 ICS/SCADA Systems," 2022 18th International Conference on Distributed Computing in Sensor Systems(DCOSS), pp. 183-190, May. 2022.
[16] Hee-yong Kwon, Tae-sic Kim, and Mun-kyu Lee, "Advanced Intrusion Detection Combining Signature-Based and Behavior-Based Detection Methods," Electronics, vol. 11, no. 6, Mar. 2022.
[17] DNP Users Group, "Overview of DNP3 Protocol", https://www.dnp.org/About/Overview-of-DNP3-Protocol, Accessed: Apr. 2024.
[18] DNP Users Group, A DNP3 Protocol Primer, Mar. 2005.
[19] DNP Users Group, DNP3 SPECIFICATION, Volume 1, Nov. 2002.
[20] Digital Bond, "Quickdraw-Snort DNP3 Rules", https://github.com/digitalbond/Quickdraw-Snort/blob/master/dnp3.rules, Accessed: Apr. 2024.
[21] Hyo-sang Lee, Wan-hong Kim, Min-ryung Park, and Yeo-jun Yoon, "A Study of SCADA Function Specific Design in Korean EMS," Proceedings of the KIEE Conference, pp. 402-403, Jul. 2007.
[22] Tae-young Song, Seuk-ha Song, Hyun-keun Riu, Hyung-ku Kang, and Bu-il Kang, "Application and Experience of State Estimation in Korea Power System," Proceedings of the KIEE Conference, pp. 89-91, Jul. 2003.
[23] Young-in Kim, Hong-ju Kim, Myung-hwan Lee, Byung-sub Kim, and Yong-hak Shin, "Data acquisition Status Check Method for Power System Analysis," Proceedings of the KIEE Conference, pp. 233-234, Jul. 2015.
[24] Hyung-koo Kang, Tae-eon Kim, Kwang-ho Kim, Young-min Choi, and Gun-woong Lee, "The Utilization Evolution of EMS Network Analysis for Optimal Power System Operation", Proceedings of the KIEE Conference, pp. 20-21, Jul. 2009.
[25] Yoon-seong Cho, Geon-soo Park, Young-in Kim, Jin Lee, Seong-ill Hur, Yeo-jun Yoon, and Hyo-sang Lee, "Validation Methodology of Network Analysis Applications in the K-EMS," Proceedings of the KIEE Conference, pp. 142-143, Jul. 2010.
[26] Yeon-jae Kang, Dae-kwon Pi, Hae-rin Kim, Sang-ho Lee, and Huy-kang Kim, "Intrusion Detection System Based on Sequential Model in SOME/IP," Journal of The Korea Institute of Information Security & Cryptology, 32(6), pp. 1171-1181, Dec. 2022.

〈저자소개〉

최 현 호 (Hyeonho Choi) 정회원
2017년 2월: 조선대학교 컴퓨터공학과 졸업
2022년 9월~현재: 고려대학교 정보보호대학원 석사과정
2016년 9월~현재: 한국전력거래소 정보보안실 근무
〈관심분야〉 제어시스템 보안, 네트워크 보안

이 중 희 (Junghee Lee) 종신회원
2000년 2월: 서울대학교 컴퓨터공학과 졸업
2003년 2월: 서울대학교 컴퓨터공학과 석사
2013년 12월: Georgia Institute of Technology 전자공학과 박사
2003년 2월~2008년 8월: 삼성전자 연구원
2014년 9월~2019년 1월: University of Texas at San Antonio 전자공학과 조교수
2019년 3월~현재: 고려대학교 정보보호대학원 조/부교수
〈관심분야〉 하드웨어 보안, 블록체인