정 보 보 호 학 회 지
제29권 제2호, 2019. 4

스마트 제조 환경에서의 이상징후 탐지 기술 현황

김 기 현*

요 약

4차 산업혁명이 본격화됨에 따라 스마트 제조 환경으로 변화하면서 제조 공장은 설비제어가 자동화되고 산업용 이더넷과 TCP/IP 기반으로 네트워크 연결되어 통합 운영되고 있으며 본사 비즈니스망의 MES, ERP, PLM 등과 연계되면서 랜섬웨어 등 악성코드 유입 및 외부 사이버 공격으로부터의 보안 위협이 높아지고 있다. 본 논문에서스마트 제조 공장에 대한 사이버 침입을 탐지하고 대응하기 위해 스마트 제조 환경에서의 이상징후 탐지 기술 현황을 분석한다. 먼저 ICS(Industrial Control System)에 대한 이상징후 탐지를 위해 ICS 위협 경로를 분석하고 스마트 제조 네트워크에서 사용되는 산업용 이더넷 프로토콜을 살펴본다. 다음으로 국내 제어망 이상징후 탐지 체계 구축 동향을 분석하고 제어망 이상징후 탐지 기술을 분류한다. 마지막으로 ㈜앤앤에스피에서 과학기술정보통신부 과제로 수행하고 있는 “선제적인 제조공정 이상징후 인지” 연구과제의 수행 현황을 살펴본다.

Ⅰ. 서 론

4차 산업혁명이 본격화됨에 따라 스마트 제조 환경에 범용 운영체제가 도입되고 개방형 프로토콜로 변화하고 있으며, [그림 1]과 같이 스마트 공장의 제조 시스템이 기업 비즈니스망의 시스템과 연계되면서 외부 사이버 공격으로부터의 보안 위협이 높아지고 있다.

스마트 제조 환경으로의 변화에 따라 기업정보 유출 방지를 위한 보안이 강조되었으나 최근 워너크라이 등 랜섬웨어가 스마트 제조 환경을 공격하면서 악성코드 유입 및 외부 해킹에 대한 이상징후 탐지 및 대응 체계 구축이 보안의 핵심이 되고 있다.

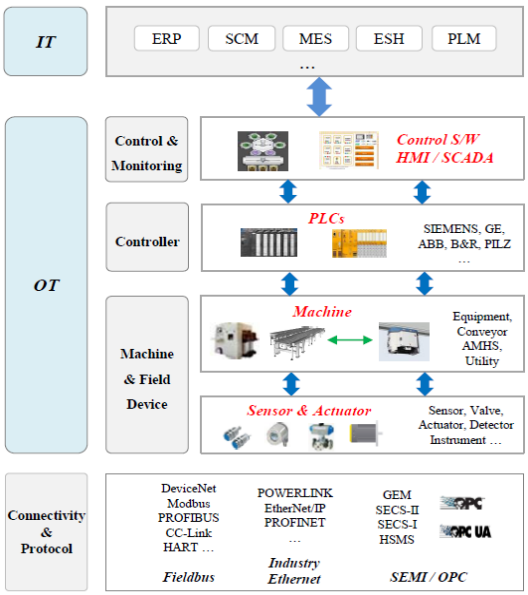
스마트 제조 공장에 대한 통합으로 산업용 이더넷(Industrial Ethernet)을 기반으로 센서와 디바이스를 PLC(Programmable Logic Controller)와 연결하고 HMI(Human Machine Interface)에서 TCP/IP 기반으로 설비를 제어하고 현장 설비의 데이터를 히스토리언(Historian)으로 수집하여 여러 공장에 대한 통합 모니터링 및 통합 운영체계가 가능하게 되었다. 또한 MES(Manufacturing Execution System), ERP(Enterprise Resource Planning), PLM (Product Lifecycle Management) 등 제조 실행 어플리케이션과 연동을 통해 공장 제조망과 본사 비즈니스망이 통합되어 생산 프로세스 관리를 위한 MES에서 생산 현장(Shop Floor)의 데이터를 수집하고 전사적 자원관리를 위한 ERP와 제품 생명주기 관리를 위한 PLM까지 유기적으로 연계되어 생산시스템 통합이 이루어지고 있다.

설비제어 자동화 및 통합 운영은 여러 제조 공장을 연결하는 구조를 가지고 있어 하나의 제조 공장에서 보안 위협이 발생할 경우 다른 제조 공장으로 전파될 위험을 가지고 있으며 MES, ERP, PLM 등 제조 실행 어플리케이션과의 연동은 인터넷과 연결되는 기업 비즈니스망과 공장 제조망을 연결하는 구조를 가지고 있어 외부 해킹, 악성코드 등 사이버 위협이 기업 비즈니스망을 통해 공장 제조망으로 전파될 위험성이 증가하고 있다.

공장 제조망과 기업 비즈니스망의 연계에 따른 보안 문제점을 해결하기 위해서는 기업 비즈니스망의 보안 관제와 마찬가지로 공장 제조망에 대한 이상징후 탐지와 통합 보안관제가 필요하다.

본 논문에서는 스마트 제조 환경에서의 이상징후 탐지 기술 현황을 살펴본다. 먼저 ICS(Industrial Control System)에 대한 이상징후 탐지를 위해 ICS 위협 경로와 랜섬웨어 공격 시나리오를 분석하고 우크라이나 정전에 대한 ICS(Industrial Control System) 사이버 킬체

본 연구는 2018년도 과학기술정보통신부 기술개발((No. 2018-0-00336, 사이버공격으로 인한 스마트공장 운영중단 문제해결을 위한 선제적인 제조공정 이상징후 인지) 지원 및 정보통신기획평가원(IITP) 관리로 수행되고 있는 연구입니다.
* ㈜앤앤에스피 부설연구소 (khkim@nnsp.co.kr)



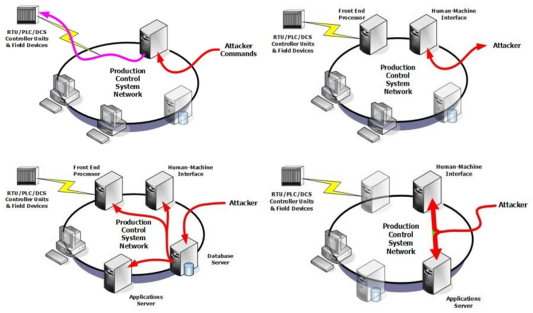
〔그림 1〕 스마트 제조 공장의 시스템 체계[6]

인(Cyber Kill Chain)을 분석한다. 다음으로 스마트공장에서 표준 프로토콜로 사용되는 산업용 이더넷 프로토콜 구조를 알아보고 IT 기반의 이상징후 탐지 기술의 한계를 살펴본다. 또한 현재 스마트공장 이상징후 탐지에 대한 산업계 동향을 알아보고 ICS 네트워크에서 비정상행위를 탐지하기 위한 방법을 4가지로 분류하고 Unknown 프로토콜에 대한 논의 한다. 마지막으로 ㈜앤앤에스피에서 과학기술정보통신부 과제로 수행하고 있는 “사이버 공격으로 인한 스마트공장 운영중단 문제 해결을 위한 선제적인 제조공정 이상징후 인지” 연구과제에 대해 수행 현황을 살펴본다.

Ⅱ. ICS 위협 경로를 고려한 이상징후 탐지

본 절에서는 ICS(Industrial Control System) 네트워크에 대한 공격 경로와 랜섬웨어 공격 시나리오를 살펴보고 이에 대응하기 위한 ICS 사이버 킬체인(Cyber Kill Chain)을 분석한다.

제어시스템 네트워크를 공격하기 위해서는 제어 프로세스가 어떻게 구현되는지 세부 사항을 발견해야 하며 공격에게 중요한 포인트는 HMI와 데이터 수집 서버 데이터(Data Acquisition Server DataBase)이며 이상징후 인지는 이 시스템들 간의 행위 규칙으로 공격자를 확인하는데 효과적으로 사용할 수 있다.

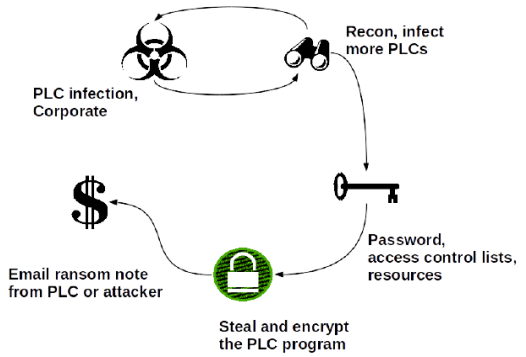


〔그림 2〕 제어 프로세스 공격 경로

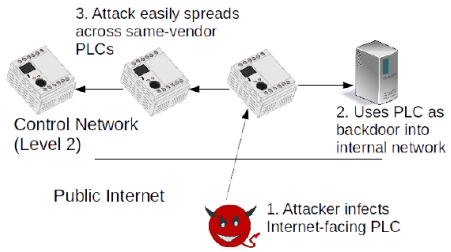
미국 ICS-CERT[1]에서는 제어 프로세스에 대한 공격 경로로 [그림 2]와 같이 데이터 수집 서버를 통한 직접적인 명령어 전달, HMI 콘솔 화면 export, 데이터베이스 변경, 중간자(Man-in-the-Middle) 공격 방법을 제시하고 있어 제어시스템에 대한 공격 특성에 일반 IT 공격의 특성이 포함되어 있음을 알 수 있다.

랜섬웨어(ransomware)는 사이버 범죄에 있어 새로운 비즈니스 모델로 되고 있으며 스마트 제조 공장은 훌륭한 타겟으로 부상하고 있다. Formby et al[2]는 쇼단(shodan)에서 발견할 수 있는 취약한 장비들을 기반으로 랜섬웨어를 수처리 시설에 감염시키는 과정을 [그림 3]과 같이 보여주고 있다.

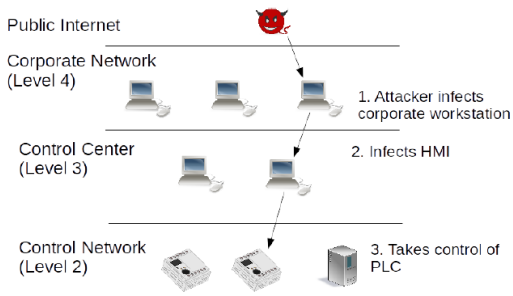
[그림 3]에서와 같이 랜섬웨어 공격은 초기 감염 → 추가 감염 → 잠금 → 암호화 → 협상 단계로 구성된다. 초기 감염 단계는 인터넷에 연결되고 쇼단에서 발견할 수 있는 PLC를 공격하여 [그림 4]와 같이 같은 PLC를 추가 감염시켜 수평이동할 수 있지만 [그림 5]와 같이 회사 네트워크를 통해 HMI를 감염시킨 후 PLC를 공격하는 수직이동도 발생할 수도 있다.



〔그림 3〕 ICS 랜섬웨어 공격의 일반적 플로우



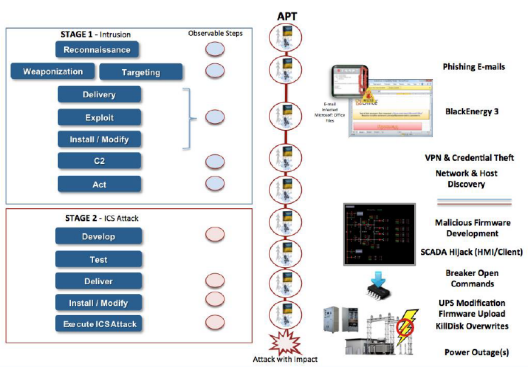
〔그림 4〕 같은 벤더 PLC로의 수평적 이동



〔그림 5〕 회사 네트워크를 통한 공격자의 수직적 이동

사이버 킬 체인(cyber kill chain)은 2010년 Lockheed Martin 애널리스트인 Eric et al[3]에 의해 침입을 보다 잘 탐지하고 대응하기 위한 의사 결정 프로세스로 만들어 졌으며 ICS 사이버 킬체인(ICS cyber kill chain)은 2015년에 SANS의 Michael et al[4]에 의해 사이버 체인을 변형하여 만들어 졌다.

ICS 사이버 킬체인은 1단계와 2단계로 구성되며 1단계는 기존 사이버 킬체인을 사용하고 있으며 2단계로 ICS 사이버 킬체인을 구성하고 있다. E-ISAC[5]의 우크라이나 파워 그리드에 대한 사이버 공격에 대해 ICS 킬체인을 적용하면 [그림 6]과 같이 분석된다.



〔그림 6〕 우크라이나 파워 그리드 공격에 대한 ICS Cyber Kill Chain

우크라이나 파워 그리드 공격은 사이버 킬체인 1단계에서 공격 대상에 대한 정찰(Reconnaissance)을 수행하고 무기화(Weaponization) 및 타겟팅(Targeting) 단계에서 BlackEnergy를 Microsoft Office 문서(Excel 및 Word)에 포함시키고 전달(Delivery) 및 취약점 공격(Exploit) 단계에서 사이버 침입 단계에서 전자 메일을 통해 악의적인 Office 문서가 전기 회사의 관리 또는 IT 네트워크에 있는 개인에게 전달되었다. 설치(Install) 단계에서 멀웨어가 Office 매크로 기능을 사용하여 BlackEnergy를 설치하고 명령 및 제어(C2, Command and Control) 및 실행(Act) 단계에서 멀웨어는 명령 및 제어 시스템에 연결되어 악성 프로그램 및 감염된 시스템과의 통신을 가능하게 하였다.

2 단계 ICS 사이버 킬체인의 개발(Develop) 및 테스트(Test) 단계에서는 공격자는 세 가지 DMS (Distribution Management Systems) 환경을 익히고 Serial- to-Ethernet 디바이스에 대한 악성 펌웨어(malicious firmware)를 개발하고 검증하였다. 전달(Deliver) 단계에서 공격자는 원격의 작업자 워크스테이션에서 VPN을 통하여 제어망에 접속하여 설치/변경(Install/Modify)단계에서 KillDisk를 설치하였다. ICS 공격 실행(Execute ICS Attack) 단계에서 SCADA 환경의 HMI를 사용하여 차단기를 열어 별전소를 오프라인으로 전환하고 동시에 악성 펌웨어를 직렬-이더넷 디바이스에 업로드하였다. 또한 영향을 받은 고객이 중단을 보고하지 못하도록 수천 건의 전화를 통해 콜센터에 대한 원격 전화 거부 서비스 공격이 이루어졌으며 일부 시스템은 KillDisk로 인해 마스터 부트 레코드를 조작되어 작동하지 못하거나 일부 시스템에서는 로그 및 시스템 이벤트가 삭제되었다.

Ⅲ. 산업용 이더넷 프로토콜과 이상징후 탐지

스마트 제조에서 사용되는 산업용 네트워크 프로토콜은 크게 필드버스(fieldbus)와 산업용 이더넷 등으로 구분된다[6]. 필드버스는 생산에 필요한 각종 장비/설비(Sensor, Actuator, 제어 Device 등)들의 운영 및 운전이 이루어지는 현장에서 데이터를 전송하는 디지털 직렬 통신망으로 [표 1]과 같다.

〔표 1〕 필드버스(Fieldbus)

프로토콜	협회 및 벤더	비고
AS-Interface	AS-INTERNATIONAL	
BACnet	ASHERE BACnet	ANSI/SHARE에서 개발
CAN Kingdom	CiA(CAN in Automation)	Bosch 차량제어용 개발
CANopen		CAN 기반
CC-Link	CLPA (CC-Link Partner Association)	미쓰비시전기에서 개발
ControlNet	ODVA(Open DeviceNet Vendor Association), Rockwell	
DeviceNet		Allen-Bradley(현 Rockwell Automation)에서 개발
Foundation Fieldbus	FILEDCOMM GROUP	
HART		
INTERBUS	Phoenix Contact	Phoenix Contact에서 개발
LonWorks	ECHELON	ECHELON에서 개발
Modbus	Modbus organization	Midicom에서 개발
PROFIBUS	PI(PROFIBUS/PROFINET International), SIEMENS	독일 국가 표준 DIN19245 지정
SERCOS I & II	VDW, ZVEI	
SECS-I, II	SEMI	반도체 통신 시리얼 프로토콜

대부분 이상징후 탐지시스템은 이더넷 환경의 TCP/IP를 기반으로 하고 있어 디지털 직렬 통신망을 사용하는 필드버스로의 확장에는 어려움이 있다.

산업용 이더넷(Industry Ethernet)은 산업 현장의 제어기(PLC)의 Master & Slave 사이 통신에 인터넷 통신 개념이 도입되면서 2006년 ISO TC 184 SC5 전문위원회에서 ISO 15745 Open Systems Application Integration Frameworks의 Part 4인 Ethernet-based control systems에서 규격 제정 시 탄생하였다. 스마트 제조 환경에서 이상징후 탐지는 대부분 산업용 이더넷을 대상으로 하고 있다.

〔표 2〕 산업용 이더넷(Industry Ethernet)

프로토콜	협회 및 벤더	비고
EtherCAT	ETG (EtherCAT Technology Group)	Beckhoff에서 개발
EtherNet/IP	ODVA, Rockwell	CIP 기반 사용
ETHERNET POWERLINK	EPSG(Ethernet POWERLINK Standardization Group),B&R	CANopen 기반
Foundation Fieldbus HSE	FILEDCOMM GROUP	
Modbus TCP	Modbus organization	
PROFINET	PI, SIEMENS	
RAPIEnet	LSIS	LS산전에서 개발
SERCOS III	VDW, ZVEI	
CC-Link/IE	CLPA	

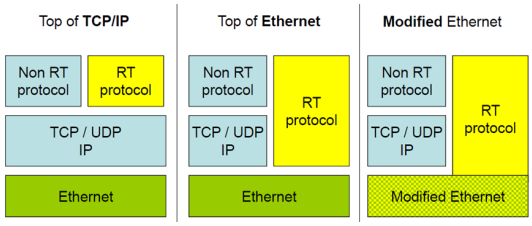
기타 스마트 제조 관련 표준 프로토콜로는 [표 3]과 같이 OPC(UA), SECS, EDA, IEC 61850 등이 있다. 4차 산업혁명과 관련하여 스마트공장의 데이터 수집 및 RTDB 연계를 위해 OPC UA가 표준화되고 있으며 GEM, SEM 등은 반도체 설비 제어분야에서 IEC 61850은 DNP3와 함께 전력 제어 분야에서 사용되며 이상징후 탐지 대상이 된다.

〔표 3〕 기타 표준 프로토콜

프로토콜	협회 및 벤더	비고
OPC DA/HDA/A&E	OPC FOUNDATION	스마트공장 시스템 및 디바이스 연계 국제산업표준
OPC UA		
HSMS,GEM,SEM	SEMI	반도체 통신 표준 프로토콜
EDA (Interface A)	SEMATECH	SECS 대체 프로토콜
DNP3	IEC (International Electro-technical Commission)	변전 자동화 통신 프로토콜
IEC 61850		

산업용 이더넷은 RT(Real-Time) 이더넷은 [그림 7]과 같은 구조를 가지고 있다[7]. EtherNet/IP, P-NET, Vnet/IP, Modbus-TCP 등은 TCP/IP 계층 상위에서 제공되며 Profinet, TCnet, Powerlink, EPA 등은 이더넷 계층 상위에서 제공되며 Profinet IRT, EtherCAT, SERCOS III 등은 변형된 이더넷 계층 상위에서 제공된다.

IT 환경에서의 이상징후 탐지 기술과 마찬가지로 스마트 제조 환경에서의 이상징후 탐지 기술 연구도 TCP/IP를 기반으로 하고 있어 적용할 수 있는 프로토콜이 제한적이다. Snort, Bro 등은 모두 TCP/IP에 기반한 공개도구들로 이를 사용하여 이상징후 탐지 시스템을 개발하는 경우 이더넷 계층에서 응용으로 연결되는 산업용 제어 프로토콜로의 확장에 어려움이 발생할 수 있다.



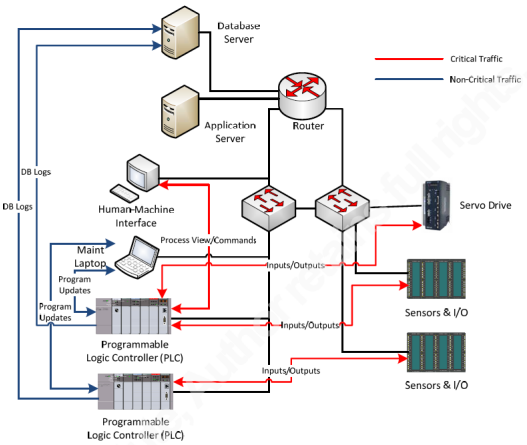
〔그림 7〕 RT(Real-Time) 이더넷 구조

Ⅳ. 국내 제어망 이상징후 탐지 체계 구축

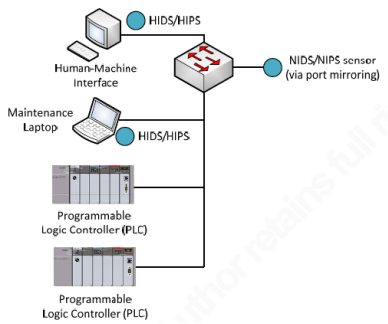
스마트 제조 네트워크에서 Critical 트래픽과 Non-Critical 트래픽은 [그림 8]과 같다[8]. 대부분 Critical 트래픽은 HMI와 PLC 사이, PLC와 Sensor/IO 사이에 존재한다.

PLC와 Sensor&I/O 사이 트래픽은 필드버스로 모니터링 대상에서 제외되는 경우가 많으므로 대부분 이상징후 탐지 네트워크 센서는 HMI와 PLC 사이의 트래픽을 대상으로 하며 호스트 센서일 경우 HMI 또는 유지보수 시스템이 대상이 되며 센서의 위치는 [그림 9]과 같이 구성된다[8].

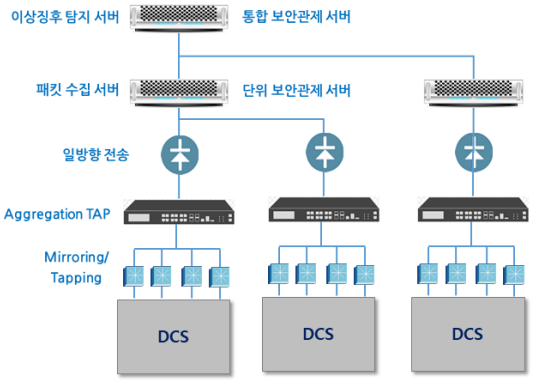
국내 스마트 제조 분야에서 제어망에 대한 이상징후 탐지 체계는 대부분 네트워크 센서 기반이며 발전사를 중심으로 구축 되고 있다. [그림 10]과 같이 발전사의 이상징후 탐지 네트워크 구성은 DCS 네트워크를 미러



〔그림 8〕 Critical vs. Non-Critical 트래픽



〔그림 9〕 제조 존에서 센서 위치



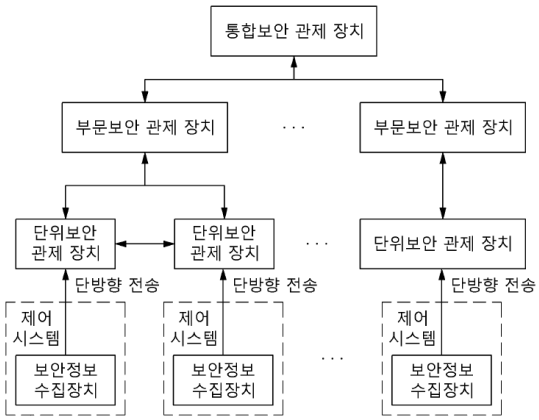
〔그림 10〕 제어망 이상징후 탐지 네트워크 구성

링/태핑을 통해 패킷을 모니터링하고 Aggregation Tap을 통해 패킷 수집 서버로 일방향으로 전달되고 이상징후 탐지 서버를 통해 침입을 탐지한다. 여기서 일방향 장비는 정보통신기반보호법에 따라 기반시설을 폐쇄망으로 유지하기 위해 사용된다.

네트워크 패킷 수집은 스위치 미러링 포트에서 일방향 장비로 직접 연결하는 경우도 있고 Aggressive Tap으로 네트워크를 태핑하고 모니터링 포트로 일방향 장비로 보내는 경우도 있다. 단순한 보안관제 체계에서는 패킷수집 서버에 대해 이상징후 탐지 서버에서 보안관제를 수행하지만 통합 보안관제 체계에서는 단위 보안관제 서버에서 화이트리스트 기반으로 이상징후를 탐지하고 통합 보안관제에서 머신러닝/딥러닝 기반으로 이상징후 탐지한다.

제어시스템에 대한 대규모 통합 보안관제 체계는 국가보안기술연구소의 특허[9]에 잘 나타나 있다. [그림 11]과 같이 대규모 제어시스템 통합보안관제 체계는 제어시스템에 포함된 적어도 하나의 보안장치를 기반으로 보안정보를 수집하고 데이터를 단방향 전송하고 단위보안관제 장치에서 화이트리스트 기반으로 보안관제를 수행하고, 부문보안관제는 단위보안관제 장치들로부터 보안정보를 획득하여 상관관계 분석을 통해 화이트리스트를 생성하고 통신정보의 일관성을 분석하며 상위 통합보안관제장치를 통해 보안관제정보를 공유한다.

제어시스템에서 수집되는 정보는 네트워크 트래픽 로그뿐만 아니라 방화벽 로그, 임베디드 제어기기 트래픽 로그, NAC(Network Access Control) 로그, USB 접속로그, 백신 탐지 로그, 시스템 로그, 네트워크 시스템 로그, 물리적 방호 시스템 로그 등을 포함하고 있다.

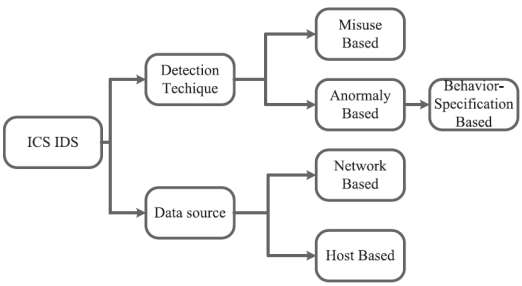


〔그림 11〕 제어시스템 통합 보안관제 체계

Ⅴ. 제어망 이상징후 탐지 기술 분류

이상징후 탐지 기술은 탐지 기술 측면으로 오용탐지 기반(Misuse Based)과 비정상행위탐지 기반(Anomaly Based)로 구분되며 데이터 소스 측면에서 네트워크 기반(Network Based)과 호스트 기반(Host Based)로 구분된다. Mitchell et al[11]은 [그림 12]와 같이 비정상탐지 기반(Anomaly Based) 하위에 행위 명세 기반(Behavior Specification Based)를 두고 있다.

본 논문에서는 Yan et al[11]이 분류한 ICS IDS 기술 분류를 기준으로 화이트리스트 기반 탐지, 머신러닝/딥러닝 탐지 등으로 표현되는 국내 기술 분류에 맞춰 다음과 같이 ICS Protocol Specification based, ICS Whitelist based, ICS Learning based, Control Process Analysis-based 등 4가지로 분류하고 추가적으로 Unknown 프로토콜에 대해 논의하고자 한다.



〔그림 12〕 ICS IDS 분류

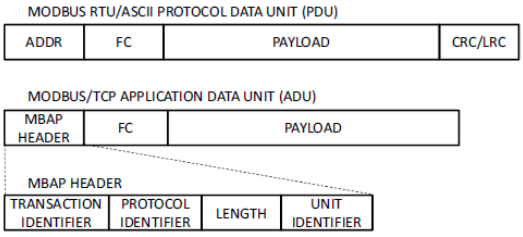
5.1. ICS Protocol Specification-based 또는 Signature-based

ICS 프로토콜 명세 기반은 ICS 프로토콜 패킷 분석을 통해 이상징후를 탐지하는 것으로 패킷 필드의 정합성 및 상태 분석, 공격 시그니처 감지, Critical 명령어 시그니처 감지 등을 포함한다.

패킷 필드의 정합성 및 상태 분석의 예로 Morris et al[12]에서는 Snort를 기반으로 Modbus ASCII에서 Modbus TCP로의 변환에 대한 이상징후 탐지를 위해 MBAP 헤더의 트랜잭션 식별자(2 바이트), 프로토콜 식별자(2 바이트), 길이(2 바이트), 유닛 식별자(1 바이트) 등을 [그림 13]과 같이 점검한다.

공격 시그니처 감지는 Snort, Bro 등이 대표적이며 ICS 시그니처 감지는 Snort에 Add-on할 수 있는 Digital Bond社의 Quickdraw를 들 수 있다. Quickdraw는 BACnet, DNP3, ENIP, FOX, Modbus, Modicon, Omron, S7 등에 대한 Snort 탐지 시그니처를 제공하지만 50~60개 정도로 현재 업데이트 되지 않고 있다. [그림 14]는 Modbus TCP에 대한 Function Code Scan 시그니처 규칙을 보여주고 있다.

정상 명령어지만 Write, Stop 등 제어시스템에 영향



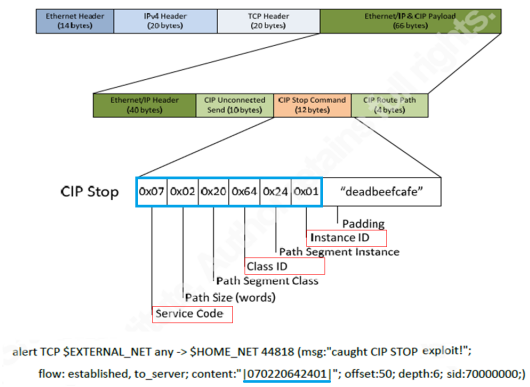
〔그림 13〕 Modbus ASCII와 Modbus TCP 구조

```
alert tcp $MODBUS_SERVER 502 -> $MODBUS_CLIENT any (flow:established; content:"|00 00|"; offset:2; depth:2; byte_test: 1, >=, 0x80, 7; content:"|01|"; offset:8; depth:1; msg:"SCADA_IDS: Modbus TCP - Function Code Scan"; threshold: type threshold, track by_src, count 3, seconds 60; reference:url,digitalbond.com/tools/quickdraw/modbus-tcp-rules; classtype:attempted-recon; sid:1111014; rev:2; priority:2;)
```

〔그림 14〕 Quickdraw의 Modbus TCP에 대한 Function Code Scan 규칙

을 줄 수 있는 Critical 명령어를 감지 예는 Hicheal et al[8]에서 찾아볼 수 있으며 Stop 명령어 취약점에 대한 Snort 시그니처 규칙을 [그림 15]와 같이 보여주고 있다.

ICS 프로토콜들은 멀티 서비스 패킷을 제공하는 경우가 많으며 Snort, Bro 등에서 이를 처리하기 위한 확장의 문제가 발생한다. [그림 16]과 같이 Multiple CIP 일 경우 여러 개의 CIP Service 필드를 제공하고 있어 Variable Offset 범위를 벗어나는 경우 시그니처로 탐지하지 못한다.



〔그림 15〕 EtherNet/IP CIP에서 Stop 명령어에 대한 Snort 규칙

〔그림 16〕 EtherNet/IP의 Multiple CIP 구조

5.2. ICS Whitelist-based

ICS 화이트리스트 기반은 호스트 화이트리스트와 네트워크 화이트리스트로 구분된다.

호스트 화이트리스트는 인가된 정상 프로세스 목록과 상태 정보를 화이트리스트로 유지하고 정상 프로세스 목록에 없거나 정상 프로세스의 변형이 발생할 경우 이를 이상징후로 인지한다. 정상 프로세스는 업데이트 되어 변경될 수 있으며 작업이 추가되거나 변경될 경우 또는 업데이트 시 프로세스가 추가될 수 있어 이에 대한 관리적 대응이 필요하다.

호스트 화이트리스트는 화이트리스트 백신 등으로 알려져 있으며 화이트리스트 기반의 EDR(Endpoint Detection & Response) 성격을 띠고 있다.

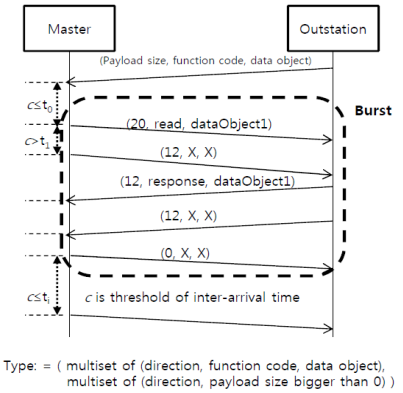
네트워크 화이트리스트는 정상 ICS 패킷을 학습하여 인가된 근원지 MAC/IP/PORT와 인가된 목적지 MAC/IP/PORT, 정상 명령어 등을 패킷 화이트리스트로 구성하고 요청-응답 상관 화이트리스트, 명령어수(주기), 트래픽량 등 플로우 화이트리스트로 확장한다.

패킷 화이트리스트 예는 한국전력공사 특허[13]에 잘 나타나 있다. 일반적으로 화이트리스트는 근원지 IP/Port, 목적지 IP/Port로 구성되는 경우가 많지만 [표 4]와 같이 화이트리스트는 네트워크 계층에서는 근원지/목적지 IP, Service 정보 등을 컨트롤 계층에서는 Opcodes (Function Code), 데이터 리스트, 시간(주기) 등을 상관관계 계층에서는 Relation Set을 화이트리스트로 구성하고 있다. ICS에서 네트워크 화이트리스트는 명령어(Opcode, Function Code) 필드를 포함하고 있는 특징을 가지고 있다.

요청-응답에 대한 상관 화이트리스트 예는 Yun et al[14]에 나타나 있으며 [그림 17]과 같이 DNP3 Master와 Outstation 간 요청-응답에 대해 Burst-based

〔표 4〕 화이트리스트 내용

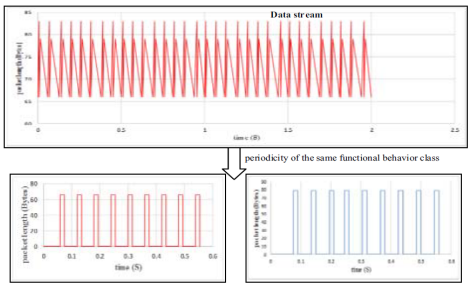
Whitelist := set of Wips	
네트워크 계층	Wips := (Sips, Dips, Wservices) Wservices := (Services, Wopcodes)
컨트롤 계층	Wopcodes := (Opcodes, Wdatalists) Wdatalists := (Datalists, Wtimes) Wtimes := (Times, Wrelations)
상관관계 계층	Wrelations := set of Relation



〔그림 17〕 Burst-based Whitelist

Whitelist 모델을 제안하고 있다.

명령어수(주기), 트래픽량 등에 대한 플로우 화이트리스트 예는 Yusheng et al[15]에서 볼 수 있으며 같은 Function 행위 클래스의 주기성을 [그림 18]과 같이 설명하고 있다.



〔그림 18〕 Function Code에 대한 주기성

5.3. ICS Learning-based

ICS 프로토콜 명세 기반 또는 ICS 화이트리스트 기반은 알 수 없는 공격에 대한 탐지 능력이 낮고 프로토콜 및 데이터 패킷 구문을 분석하는데 시간이 걸린다. 이러한 단점을 극복하기 위해 머신러닝 또는 딥러닝 기법이 적용된다.

ICS 프로토콜에 대한 학습 기반 이상징후 탐지는 최근 가장 많이 이루어지고 있는 분야이며 다양한 머신러닝(Machine Learning) 또는 딥러닝(Deep Learning)이 적용되고 있다.

머신러닝 알고리즘으로는 베이지안 네트워크(Bayesian Network), 가우시안 혼합 모델(Gaussian mixture model), 마르코프 체인(Markov Chainl), SVM(Support Vector Machine), 인공 신경망(Artificial Neural Network) 등이 사용된다.

딥러닝 알고리즘으로는 autoencoder, CNN (Convolutional Neural Network), RNN (Recurrent Neural Network), LSTM(Long short-term memory) 등이 사용된다.

Flaus et la[16]에서 리뷰한 ICS에 대한 머신러닝 기반의 이상징후 탐지에 대한 최신 연구의 일부를 정리하면 [표 5]와 같다.

머신러닝은 이전에 개발된 모델이고 딥러닝은 최신 모델로 생각할 수 있지만 스마트 제조 환경에서 당면한 문제나 새로운 해킹 문제를 처리하기 위해 적합한 알고리즘으로 머신러닝이든 딥러닝이든 그 가치가 재발견되는 경우가 많다.

〔표 5〕 Intrusion detection approaches for ICS

Input data	Learning method	References
Packets attributes State & process I-NHIDS	Hidden Markov Model Learning with Baum Welch algorithm	[17]Zhou C, Huang S, Xiong N, et al (2015)
process variables NIDS	SVM on the time window	[18]Keliris A, Salehghaffari H, CairlB (2016)
Process variables(sensors) I-HIDS	Fault detection is based neural network Link deep learning	[19] He Y, Mendis GJ, Wei J (2016)
Packets attributes &Process Variables sequences I-NIDS	Discrete Time Markov Chains (DTMCs) & statistical learning	[20]Caselli M, Zambon E, F. Kargl (2016)
Packets attributes I-NIDS	Hierarchical Neuron based Neural Network Architecture (HNA-NN)	[21]ShitharthS,D. Winston Prince(2017)
process variables I-NIDS	Neural networks trained with OPSO-BPNN	[22]Yang H, Chen T, Guo X, et al(2018)
Packet attributes and process variables I-NIDS	Tools for Weka data mining Hybrid learning approach	[23] Ullah I, Mahmoud QH (2018)
Packet processing time(by the PLC) I-HIDS(in the PLC)	K-Means Clustering	[24]Alves T, Das R. Morris T,(2018)
Packets attributes I-NIDS	Convolutional Neural Networks	[25] Moshe K., Asaf S.(2018)

ICS 학습 기반 이상징후 탐지는 침입 탐지 성능이 뛰어나지만 탐지된 침입이 무엇이지 원인을 찾기는 쉽지 않다. 침입에 대응하기 위해서는 피처(Feature)까지 학습하는 딥러닝 보다 피처(Feature) 특성을 알고 있는 머신러닝이 효율적일 수 있다. 탐지 성능이 좋다고 딥러닝에만 의존하기 보다는 다른 이상징후 탐지 방법과 하이브리드로 사용하여 원인을 규명할 수 있는 침입에 대해 대응할 수 있는 체계를 갖추어야 한다.

5.4. Control Process Data Analysis-based

스마트 제조에서 공정 데이터(압력, 온도, pH 수준 등)은 물리적 제조 프로세스의 보안 상태를 나타낸다. 제어 프로세스 데이터 분석 기반은 이러한 공정 데이터

를 분석하여 이상징후를 탐지하는 것이다.

프로세스 데이터 분석과 예측을 통한 이상징후 탐지는 Hadz˘iosmanovic´ et al[26]에서 찾아 볼 수 있으며 제어 명령어 분석을 통해 제어 명령의 결과 예측은 Lin et cal[27]에서 찾아 볼 수 있다.

Stuxnet이 원심분리기의 회전속도를 조절하면서 제어 프로세스 데이터 분석에 대한 관심도가 높아지고 있으나 통합 운영 영역인지 보안 영역인지 살펴볼 필요가 있다.

일반적으로 제조 공정 운영 정보는 지역 운영관리 또는 중앙의 통합 운영관리에서 정보를 수집하고 모니터링한다. 보안과는 차이가 있다.

IT 측면에서 보면 NMS(Network Management System) 운영과 NIDS(Network Intrusion Deetction System) 운영으로 비교할 수 있으며 서로 다른 영역에 있다.

보안 측면에서 제어 프로세스 데이터 분석이 필요할 경우 네트워크 트래픽 모니터링을 통해 제어 프로세스 정보를 획득할 수 있는지에 대한 문제를 해결해야 한다. 테크(Tag) 정보로 불리는 제어 프로세스 데이터의 분석은 소규모 사이트일 경우 가능할지 모르지만 수만에서 수십만 테크 정보가 발생하는 대규모 사이트의 경우 네트워크 패킷에서 테크 정보를 분류하고 추출하는 것을 거의 불가능에 가깝다.

현장장치의 레지스터 데이터가 산업용 이더넷 프로토콜 패킷에 [그림 19]과 같이 실려 전송될 경우 운영자는 프로토콜 패킷에서 정보를 구분할 수 없으며 제조장비를 설치한 업체와 제조사의 도움을 받더라도 쉬운 일은 아니다.

네트워크 측면에서 프로토콜 패킷으로부터 테그 정보를 추출하기는 어렵지만 시스템 측면에서는 가능하다. 일반적으로 지역 운영관리 또는 통합 운영관리에서는 시스템에 분류된 테그 정보를 대상으로 중요한 테그 정보에 대한 모니터링을 하고 있으므로 융합보안 측면에서 통합 운영관리와 통합 보안관리의 융합은 필요하다.

ICS 이상징후 탐지에서 모든 제어 프로세스 데이터를 일일이 분석할 수는 없지만 전체 제어 프로세스 데이터를 대상으로 딥러닝 분석이 가능하며 ICS 운영자가 정의한 주요 프로세스 데이터에 대한 이상징후 탐지는 가능하므로 충분한 검토를 통한 접근이 필요하다.

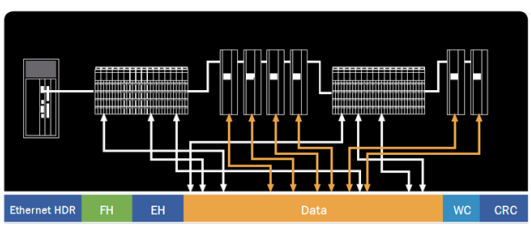
5.5. Unknown Protocol Analysis

스마트 제조 환경에서 제어 프로토콜은 개방형 프로토콜로 변화하고 있지만 자사 제어시스템 간 연동을 위한 제조사 자체 프로토콜은 여전히 존재한다. [그림 20]은 프로토콜 분석기에서 분석이 안되고 데이터로만 보이는 제조사의 자체 프로토콜의 예를 나타낸다.

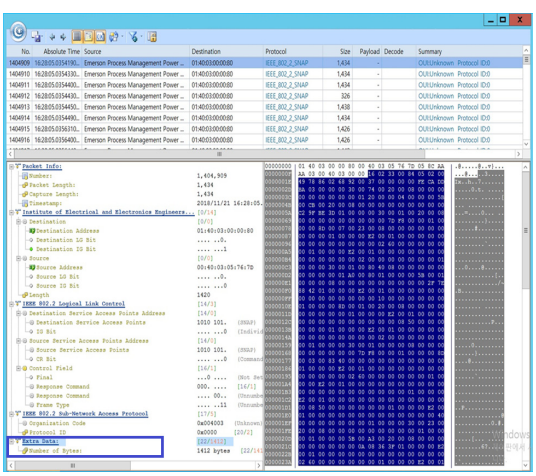
제조사 자체 제어프로토콜로 비공개로 Unknown 상태이므로 ICS 프로토콜 명세 기반, ICS 화이트리스트 기반, ICS 제어 프로세스 데이터 분석 기반의 이상징후 탐지는 어렵지만 ICS 학습 기반 이상징후 탐지는 가능하다.

그러나 ICS 학습 기반에서 이상징후를 탐지하더라도 운영자가 이상징후 원인을 찾아내 조치하기 어렵고 전문가 또한 프로토콜을 알지 못해 분석하기 힘들다.

Unknown 프로토콜도 제어 프로토콜이다. 제조사에서 자체 개발하였지만 제어 프로토콜이 가지는 기본적인 요소는 갖추고 있다. 제조사 자체 프로토콜을 완전히 분석하지는 못하겠지만 알려진 제어 프로토콜을 기반으



〔그림 19〕 산업용 이더넷 프로토콜과 제어 프로세스 데이터



〔그림 20〕 비공개 제조사 자체 제어 프로토콜

로 어느 정도의 분석은 가능하므로 분석한 범위 내에서 화이트리스트를 구성하여 이상징후 탐지에 적용함으로써 학습 기반의 이상징후 탐지에 대한 보조 역할을 할 수 있다.

Ⅵ. 결 론

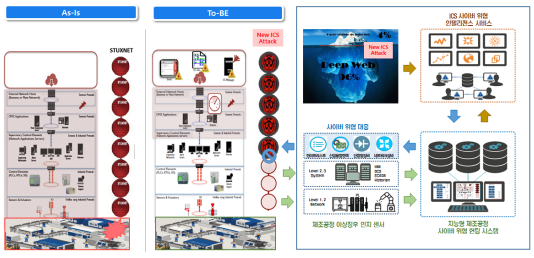
㈜앤앤에스피는 ㈜엔에스에이치씨와 아주대학교와 함께 2018년도 과학기술정보통신부 기술개발 지원 및 정보통신기획평가원(IITP) 관리로 “사이버공격으로 인한 스마트공장 운영중단 문제해결을 위한 선제적인 제조공정 이상징후 인지” 과제를 수행하고 있다.

[그림 21]과 같이 본 과제에서는 사이버 공격에 취약한 제조설비의 가동 중단을 미연에 방지하기 위해 제조공정 네트워크와 시스템에 대한 이상징후를 탐지하고 사이버 킬체인 분석과 인공지능 기법을 이용하여 ICS 보안 위협을 헌팅하고 사이버 위협에 대응함으로써 갑작스런 제조 설비의 가동중단을 예방하고자 한다. 또한 다크웹 등 오픈 정보를 이용하여 ICS 사이버 위협 정보를 수집하고 ICS에 특화된 악성코드를 분석하여 인텔리전스 서비스로 제공함으로써 최신 ICS 사이버 공격에 선제적으로 대응하고 스마트공장에 대한 보안 위협을 획기적으로 감소시키고자 한다.

1차년도에는 제조공정 네트워크에 대한 화이트리스트 기반 이상징후 인지와 제조공정 시스템에 대한 화이트리스트 기반 이상징후 인지 기술 연구를 수행하였다.

제조공정 네트워크에 대한 화이트리스트 기반 이상징후 인지에서는 EtherNet/IP와 Profinet을 대상으로 패킷을 수집하고 네트워크 침입탐지 도구와 네트워크 악성코드탐지 도구를 이용하여 악성 패킷을 필터링하고 머신러닝을 이용하여 패킷들을 클러스터링하여 화이트리스트를 구축하고 이상징후를 탐지하였다.

제조공정 시스템에 대한 화이트리스트 기반 이상징후 인지에서는 HMI에서 프로세스 정보, 네트워크 정보, 시스템 정보, 리소스 정보를 수집하고 안티바이러스와 휴리스틱 엔진을 이용하여 악성 파일을 필터링하고 머신러닝을 이용하여 프로세스들을 클러스터링하여 화이트리스트를 구축하고 이상징후 탐지하였다.



〔그림 21〕 스마트공장 운영중단 문제해결 개념도

〔그림 22〕 스마트 제조공정 이상징후 인지 테스트 환경

1차년도 결과물은 [그림 22]와 같은 스마트 제조공정 시뮬레이션 환경에서 테스트 되었다.

본 과제의 진행에 있어 ICT 리빙랩 방식을 도입하고 있으며 사이버 위협으로 인한 스마트 공장 운영 중단 문제를 실질적으로 해결할 수 있는 기술개발이 되도록 힘쓰고 있다.

참 고 문 헌

[1] ICS-CERT Homepage, Control Systems Vulnerabilities and Attack Paths, https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities

[2] D. Formby, S. Durbha, R. Beyah, "Out of Control: Ransomware for Industrial Control Systems", RSA Conference, 2017.

[3] E.M. Hutchins, M.J. Cloppert and R.M Amin "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," *Proc. 6th Int'l Conf. Information Warfare and Security* (ICIW 11), Academic Conferences Ltd., pp. 113–125, 2010.

[4] Michael J. Assante and Robert M. Lee, The Industrial Control System Cyber Kill Chain,

SANS Institute, Oct. 2015.

[5] E-ISAC, SANS, Analysis of the Cyber Attack on the Ukrainian Power Grid - Defense Use Case. March 18, 2016.

[6] 권대욱, Smart Factory 구현을 위한 Engineering Model-제어 Engineering 기반 기술, 계장기술, pp.90-85, 2018. 07.

[7] Max Felser, Hans Doran, Gunnar Prytz, “Overview of Real-Time Ethernet solutions”, 2010 IEEE International Conference, ETFA – Workshop, Sep. 2010.

[8] Micheal H., Barbara F., Challenges for IDS/IPS Deployment in Industrial Control Systems, SANS Institute InfoSec Reading Room, Jul. 2015.

[9] 김희민, 장엽, 윤정한, 최승오, 김우년, 박상우, 화이트리스트를 이용한 제어시스템의 보안관제 방법 및 이를 위한 시스템, 대한민국 등록특허 10-1871406, 2018.06.

[10] Mitchell R and Chen IR., "A survey of intrusion detection techniques for cyber-physical systems", ACM Comput Surv, 46(4), 55, 2014.

[11] Y. Hu, A. Yang, H. Li, Y. Sun, and L. Sun, "A survey of intrusion detection on industrial control systems", International Journal of Distributed Sensor Networks, vol.14, no.8, 2018.

[12] Morris T, Vaughn R and Dandass Y., "A retrofit network intrusion detection system for MODBUS RTU and ASCII industrial control systems", Proceeding of 45th Hawaii international conference on system science(HICSS), pp.2338–2345, Jan. 2012.

[13] 윤정한, 민병길, 김우년, 장문수 등, 화이트리스트를 이용한 네트워크 감시 장치 및 방법, 한국전력공사, 대한민국 특허 10-1360591, 2014. 02.

[14] J.H. Yun, S.H. Jeon, K.H. Kim, W.N. Kim, Burst-based Anomaly Detection on the DNP3 Protocol, International Journal of Control and Automation, V ol. 6, No. 2, pp.313-324, April, 2013

[15] Yusheng W, Kefeng F, Yingxu L, et al. "Intrusion detection of industrial control system based on Modbus TCP protocol", Proceeding of IEEE 13th international symposium on autonomous decentralized system(ISADS), pp.156–162. Mar. 2017.

[16] Jean-Marie Flaus, John Georgakis, "Review of machine learning based intrusion detection approaches for industrial control systems", Computer & Electronics Security Applications Rendez-vous(C&ESAR) Conference, Nov. 2018.

[17] Zhou C, Huang S, Xiong N, et al (2015) Design and Analysis of Multimodel-Based Anomaly Intrusion Detection Systems in Industrial Process Automation. IEEE Trans Syst Man, Cybern Syst 45:1345–1360 .

[18] Keliris A, Salehghaffari H, Cairl B et al (2016) Machine Learning-based Defense Against Process-Aware Attacks on Industrial Control Systems. 2016 IEEE International Test Conference (ITC)

[19] He Y, Mendis GJ, Wei J, Real-time Detection of False Data Injection Attacks in Smart Grids: A Deep Learning-Based Intelligent Mechanism. IEEE Trans Smart Grid 3053:1–12, 2016.

[20] Caselli M, Zambon E, Kargl F (2016) Sequence-aware Intrusion Detection in Industrial Control Systems Sequence-aware Intrusion Detection in Industrial Control Systems CPSS 2015 - Proceedings of the 1st ACM Workshop on Cyber-Physical System Security, Part of ASIACCS 2015. 13-24.

[21] Shitharth S, Prince Winston D, An enhanced optimization based algorithm for intrusion detection in SCADA network. Comput Secur 70:16–26, 2017.

[22] Yang H, Chen T, Guo X, et al, Research on intrusion detection of industrial control system based on OPSO-BPNN algorithm. Proc 2017 IEEE 2nd Inf Technol Networking, Electron Autom Control Conf ITNEC, Jan. 2018.

[23] Ullah I, Mahmoud QH, A hybrid model for anomaly-based intrusion detection in SCADA networks, Proc. 2017 IEEE Int Conf Big Data,

Jan. 2017.

[24] Alves T, Das R, Morris T, Embedding Encryption and Machine Learning Intrusion Prevention Systems on Programmable Logic Controllers. IEEE Embedded Systems Letters, 10:3., 2018.

[25] Moshe Kravchik and Asaf Shabtai, "Detecting cyber attacks in industrial control systems using convolutional neural networks", Proc. the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy, pages 72–83. ACM, 2018.

[26] Hadžiosmanovic´ D, Sommer R, Zambon E, et al. Through the eye of the PLC: semantic security monitoring for industrial processes. Proc. 30th annual computer security applications conference, pp.126–135. 2014.

[27] Lin H, Slagell A, Kalbarczyk Z, et al. Semantic security analysis of scada networks to detect malicious control commands in power grids. In: Proceedings of the 2013 first ACM workshop on smart energy grid security, pp. 29–34, Nov. 2013.

〈저자소개〉

김 기 현 (Ki-Hyun Kim)

정회원

1993년 2월 : 경북대학교 전자공학과 학사

1995년 2월 : 경북대학교 전자공학과 석사

2011년 8월 : 충북대학교 컴퓨터공학과 박사

1996.7～2000.4 : 한국정보보호진흥원 선임연구원

2000.5～2002.1 : ㈜정보보호기술 연구소장

2002.1～2011.9 : ㈜레드게이트 사장

2011.9～2014.4 : ㈜에스지에이 연구센터장

2013.3～현재 : 호서대학교 컴퓨터정보공학부 겸임교수

2014.4～현재 : ㈜앤앤에스피 부사장/연구소장

<관심분야> 스마트산업보안, 융합보안