한국컴퓨터정보학회 동계학술대회 논문집 제27권 제1호 (2019. 1)

이상행위 분석을 위한 제어명령 수집 시스템 구현

이진흥O, 안바울*
O*다운정보통신(주)
e-mail: jhlee@daun.co.krO, paulan@daun.co.kr*

An Implementation of Control Command Acquisition System for Analysis of Abnormal Behavior

Jin-Heung LeeO, Pa-Ul An*
O*Daun Information & Communication Co.

● 요 약 ●

본 논문에서는 자동 제어 시스템의 이상행위를 분석하기 위하여 MODBUS 프로토콜 기반의 제어 명령을 수집·분류하여 등록된 화이트리스트 기반으로 이를 탐지하는 시스템을 구현하였다. 구현 시스템은 자동 제어 시스템 기반으로 다양한 생산설비를 동작시키는 스마트팩토리 시스템을 비롯하여 국가기간 산업에 활용 가능하며, 생산설비의 이상 작동을 확인하기 위하여 생산설비의 동작 신호를 주기적으로 수집·분석하여 정상적인 작업형태에서 벗어나는 이상 작업을 판단할 수 있도록 구성하였다. 또한, 소형화된 공장 자동화 설비를 구성하여 실제 스마트팩토리 환경에서 제어명령을 수집하고, 수집된 신호로부터 이상 작동을 검출하는 제안 시스템의 구현 결과를 설명한다.

키워드: 이상행위(abnormal behavior), 탐지(detection), 자동제어(automatic control), 보안(security)

I. Introduction

산업 제어 시스템은 전력, 교통, 금융 설비 시스템 등 다양한 자동화 설비를 제어하는 시스템으로서 주로 인터넷과 분리된 폐쇄망으로 기간 산업에서 활용되고 있다. 최근 융합 ICT 기술의 활용과 4차 산업혁명에 따른 스마트팩토리 보급이 늘어나면서 점차적으로 다양한 산업 현장에서 적용되고 있다.

과거 제어 시스템은 외부 네트워크와 분리된 폐쇄망에서 소수의 운영자만이 접근할 수 있는 환경에 설치되고 운영되었기 때문에 주요 보안 위협으로부터 비교적 안전하다고 믿어졌다. 그러나, 2010년 스턱스넷(Stuxnet)이 등장하면서 보안강화의 필요성이 인식되기 시작했다. 또한 최근에는 네트워크 연결 없이 USB 연결만으로 쉽게 설치되고, 공격되는 다양한 위협들이 나타나고 있다.

2008년 경제 불황 이후, 제조업계는 인건비 절감과 함께 전기전자, 정보통신 기술 발전으로 산업자동화 시대에 도래하였으며, 특히 국내에서 제조업과 IT 융합을 통한 생산방식의 패러다임을 변화시켜 제조업의 재도약을 위한 핵심 요소로 인식하고 개발하고 있다. 즉, 스마트팩토리를 통하여 공장의 인적·물적 자원을 최적화하여 제품의 기획, 제조, 유통 등 전 과정을 통합하고 실시간으로 관리하여 생산성 향상, 에너지 절감, 안전한 생산환경 구축, 다품종 복합생산이 가능한 유연한 생산체계를 구축하려고 한다.

스마트팩토리는 생산설비에 다양한 형태의 제어 시스템을 적용하여 자동화를 이루고, 공장을 비롯한 교통, 전력생산, 자원 관리 등 국가 기반 시설 전반에 걸쳐 적용되고 있다. 제어 시스템의 기술 고도화와 시스템 간 커뮤니케이션 채널 생성을 통한 데이터 공유가 이루어지면서 제어 시스템 보안에 대한 중요성은 점점더 증가되고 있다.

본 논문에서는 지능화·고도화된 제어 시스템 공격으로부터 해당 시스템을 보호하기 위하여 화이트리스트 기반으로 사용자의 운영행위를 탐지하고, 설치된 기기의 동작 상태를 분석하여 이상행위를 판단하기 위하여 제어 명령을 수집하는 시스템을 구현하였다.

II. Related works

2.1 산업 제어 시스템의 보안 동향

제어 시스템의 발전으로 생산설비의 효율적인 사용을 실현하였으나 과거에 비해 다양한 보안 취약점을 내포하게 되었다. 오늘날 사용되고 있는 수많은 자동제어 시스템에 인증 또는 암호화 기능이 고려되지 않은채 통신이 이루어지고 있으며, 급증하고 있는 SCADA 관련 취약점에 대한 대응체계가 구비되지 않거나 이를 인식하고 있지 않은채 이용되고 있다. 이에 따라 제어 시스템을 대상으로 하는 보안 기술 분야를 연계구간 보안, 네트워크 침입탐지, 인증, 취약점 탐지 기술 등으로 개발되고 있다.

미국과 EU에서는 제어시스템에 특화된 침입탐지 및 차단 기술에

대하여 연구가 진행되고 있으며, NexDefense의 Sophia는 네트워크 트래픽을 시각화하여 침입을 감시하는 시스템을 출시하고, Queens 대학은 IEC61850 프로토콜 DPI(Deep Packet Inspection) 기술을 이용한 침입탐지 기술을 연구하고 있다.

국내에서는 한전이 전력 제어 시스템 보호를 위하여 화이트리스트 기반 이상징후 감시 시스템과 DNP3(Distributed Network Protocol 3) 보안 인증 기술을 개발하였다. 또한 독립된 산업 제어 시스템 망에 대하여 특화된 탐지 기능을 제공하고 SCADA 프로토콜을 이용하여 산업 네트워크를 분석하고 오작동을 탐지하는 SCADA Shield 제품이 출시하는 등 산·학·연 각계에서 산업용 네트워크 트래픽 분석 및 제어 시스템의 상태 분석과 관련한 연구가 진행되고 있다. 그러나, 제어 시스템 보안에 대한 국가별 출원 동향을 보면 미국이 172건으로 59%를 차지하고 있으며 그 뒤를 74건으로 한국이 25%, 일본이 26건으로 9%를 차지하고 있어, 미국과 한국에서 활발하게 연구되고 있는 것으로 나타났다.

2.2 이상행위 탐지 기술 연구

규칙기반 이상행위 탐지 기술은 네트워크 관리자에 의해 네트워크 사용자들의 행동을 규칙화 하고 어떤 행위에 규칙을 위반하고 데이터가 유출되었는지를 탐지할 수 있는 시스템이다. 규칙기반 탐지 시스템의 문제는 내부자 이상행위 탐지 시스템은 정해진 규칙을 벗어나는 내부자의 공격에 대해 능동적이지 못한 반응을 보였으며, 이를 통해 내부자의 공격도 많이 이루어졌으며 시스템 환경에 변화가 생기면 기존규칙이 제대로 탐지하지 못하였다. 최근에는 뉴스 기사와 법원 판결문을 분석하여 내부 침입자의 특성을 추출하여 유형을 미리 정하지 않고 텍스트 마이닝 기법을 활용하여 내부 침입자의 특성을 추출 하였으나, 기존의 범죄자가 조금 다르게 공격을 하여도 탐지를 못하는 단점이 있었다.

최근 이상행위 탐지연구의 동향은 규칙기반의 이상탐지 기술에서 기계학습을 통한 방법으로 연구가 변화하고 있다. 갈수록 내부자 위협이 복잡해지고 다양해지기 때문에 인간의 노동력으로 매번 규칙을 발견하는 것은 힘들어져서 기계학습을 통해 좀 더 많은 데이터를 수집하고 내부자 위협에 대해 빠른 대처를 위하여 최근 기계 학습을 통해 사람의 힘을 빌리지 않고 자동으로 추출하는 비지도 학습으로 연구하고자 하는 시도가 계속되고 있는 추세이다.

2.3 머신러닝 기반 이상행위 탐지 시스템 개발 동향

CERT Dataset을 이용한 이상행위 탐지 연구 논문 중 Haedong Kim외 5인의 논문[1]에서 이상치 탐지 알고리즘을 이용하여 각 내부 구성원의 행위의 위협 정도를 예측하는 모델을 제시하였다. 연구 과정은 과거 연구된 내부 침입 탐지에서 사용된 변수를 CERT Dataset에서 사용가능한 변수들로 생성하고, 시간단위를 하루로 하여 근무시간 과 근무 외 시간으로 나누는 방식으로 60개의 변수를 생성하였다. 비정상 범주의 관측치가 약 90% 정도 집중되어 세 가지 테이블만으로 내부 침입탐지 실험을 진행하였다. 사용된 알고리즘은 Gauss(Gaussian density estimation), Parzen(Parzen window density estimation), PCA(Principal component analysis), and KMC(K-Means clustering) 네 가지 일 범주 분류 모형이 사용되었다.

연구의 결과는 KMC알고리즘의 K=3,5,7값 그리고 Parzen과 PCA를 앙상블한 방법을 더해 총 일곱 가지 알고리즘으로 결과를 도출하였으며, 결과로 보았을 때 각 알고리즘 모두 각 테이블마다 탐지비율이 달랐으나, Parzen과 PCA를 앙상블한 방법이 일반적으로 우수한 성능을 나타낸다는 것을 연구 결과를 통해 확인하였다.

Name	특징
Gauss	주어진 데이터를 정규 분포로 가정하고 평균화 분산을 추정하여 확률밀도 함수를 구한 뒤 새로운 데이터가 추정된 확률밀도에서 생성될 확률을 이용하여 이상 치 스코어를 산출하는 방식이다. (BamnettandLewis,1994)
Parzen	커널 기능을 사용하여 비 파라메트릭 밀도의 추정 방법 중 하나로 밀도를 추정하는 방법이다. (Duda et al., 2012)
PCA	주어진 데이터의 분산을 최대한 보존하는 새로운 기저(주성분)를 찾는 기법이다. (Alpaydin, 2014)
KMC	각 관측치를 자신과 가장 가까운 중심 (Centroid)을 가지는 군집에 할당해 주는 군집화 알고리즘이다. (Alpaydin, 2014)

Dong-wook Ha외 2인의 논문[2]에서는 RNN(Recurrent Neural Network)을 이용하여 구현한 Autoencode를 이용하여 이상행위 탐지 기술을 연구하였다. 사용된 RNN(Recurrent Neural Network)은 다른 신경망 모델과 다르게 현재 값과 이전의 입력 값을 같이 고려하기 때문에 최근 자연어 처리문제와 같이 입력 순서를 생각해야 하는 문제에 많이 이용되며, 좋은 성능을 보이고 있는 모델이다. Autoencode은 기계학습 알고리즘이며, 스스로 학습을 할 수 있다. 실험에서는 정상행위 학습을 마친 Autoencode데이터를 이용하였으며, 정상패턴과 하루단위의 패턴을 비교하여 이상행위를 탐지하였다. 결과 값은 95%이상의 민감도를 보였으며 정상데이터와 일 단위 데이터를 비교하여 이상행위를 탐지할 수 있었다.

또 다른 연구 결과에서는 아래 표와 같이 6가지로 이상치 검출 방법을 나타내었다.

이름	특징
Matrix Decomposition-based outlier analysis	매트릭스 분해에 기초한 특이치 검출 방법은 주 구성 요소 분석을 사용하여 주요 대량 데이터의 상관 구조를 위반하는 사례를 찾는다.(Shyu et al. [2003]).
RNN (Replicator Neural Networks)	데이터를 압축하고 재구성하여 대용량 데이터를 정확하게 재구성하는 네트워크이다. 이상치가 아닌 데이터를 정확하게 재구성한다.
Density-based outlier analysis	분포도가 낮은 지역에 속하는 시험사례는 이상치로 간주된다.
Outlier score interpretation	다른 방법의 점수를 결합하는 것은 쉽지 않습니다. 멀티 알고리즘 아웃 라이어 검출 앙상블의 견고성을 이용하기가 어렵다.
Transforming outlier scores into probabilities	Weibull 분포를 가진 매트릭스 분해 기반의 이상치 점수는 유연하고 다양한 형태의 모델을 만들 수 있다.
Outlier detection ensembles	다중 알고리즘 앙상블은 서로 다른 기계 학습 모델의 예측 조합이다.

특이성의 검출 방법의 다중 알고리즘 앙상블은 36 억 개 로그라인 이루어지는 실제 데이터 세트로 연구 되었다. 이 논문의 결과는 시스템이 보이지 않는 공격으로부터 시스템을 보호하는 것으로 확인되

었으며, 피드백이 시간에 걸쳐 수집됨으로 수집된 데이터를 통해 이상행위 탐지의 검출 속도, 검출 속도가 증가했다.

III. The System Implementation

제안된 시스템은 제어 시스템을 실시간 관리하는 HMI 시스템, 제어 명령을 수집하는 패킷 캡쳐 시스템, 제어명령을 분석하고, 이상행위를 검출하는 분석시스템으로 구성되며, 스마트그리드 사이버 보안 가이드라인 및 표준을 반영하여 설계하고 구현하였다.

3.1 시스템 구성

그림1은 제안된 시스템의 구성을 보여주고 있다. 자동제어 관리 시스템(PMS)은 운용자 PC를 통하여 전달된 Modbus 기반의 제어 명령 패킷을 수신하고, 수신된 패킷으로부터 제어 데이터를 추출하여 분석엔진(Analysis Engine)과 검출엔진(DAD Filter) 포맷에 맞게 제어 명령 패킷을 가공한다. 이때, 검출엔진의 성능을 높이기 위하여 PMS 내의 Job Queue를 이용하여 검출 엔진을 병렬 구조로 구성하였다.

분석 엔진은 수신된 제어 명령 패킷 데이터를 각각의 제어신호 속성별로 구분되고 내부 스키마 정의에 따라 데이터베이스에 저장하고, 제어 신호별로 시각화 기능을 통하여 관리자 인터페이스로 재구성된다. 또한 분석 엔진은 자동화 설비와 연결된 PLC 시스템의 설비 상태 정보 수집기(DAD Collector)로부터 설비의 상태 정보를 수집한다. 수집된 기계 상태 정보는 미리 정의된 규격에 맞게 분석되고 내부 데이터베이스에 저장된다.

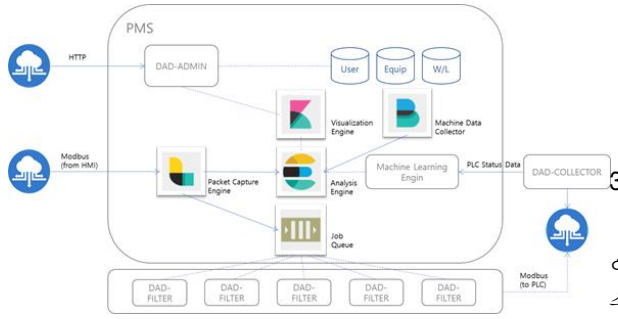

Fig. 1. System Architecture

3.2 제어 명령 수집 시스템 구현

제안 시스템은 MODBUS 프로토콜을 이용하여 공장 내 여러 기기를 작동시키는 시스템을 대상으로 기기를 작동하거나 기기로부터 특정 정보를 수집하는 시스템을 대상으로 제어 신호를 수집하는 시스템을 구현하였다.

제어 신호 수집을 위하여 대상 프로토콜인 MODBUS 패킷을 분석하여 아래와 같이 패킷 데이터 구조를 정의하고 각각의 동작을 위한 Function code를 정규화 하였다.

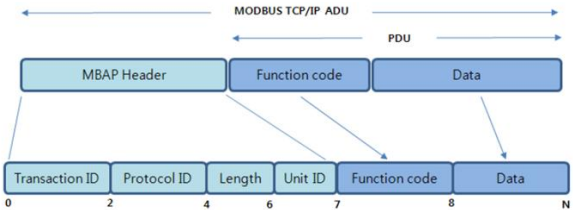

Fig. 2. MODBUS Packet

Modbus-TCP 패킷은 TCP-Header와 Modbus/ADU로 구성되며 Modbus/ADU는 7byte 고정길이의 헤더 정보와 예약된 명령어 코드의 집합으로 구성된다. 또한 7byte의 고정길이 헤더 내에는 트랜잭션 회수, 프로토콜 아이디, 페이로드 길이, PLC 아이디를 포함한다.

Function code는 Modbus 프로토콜에서 제공하는 명령어 코드 집합으로, Function code를 이용하여 메모리로부터 값을 읽어오거나 쓸 수 있다. 이러한 Function code에는 표준 규격상 1~127 사이의 값이 올 수 있지만, 일반적으로 1,2,4,5,6,15,16 값을 주로 사용한다. 각 Function code에 따라 어떤 메모리에 접근해서 작업(Read, Write)을 수행할 것인지 결정하게 된다.

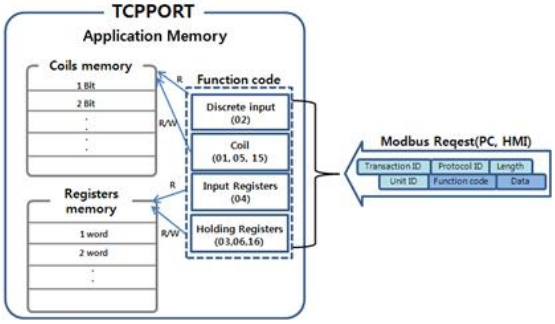

Fig. 3. Function code of Modbus/PDU

3.3 테스트베드 구축

제안 시스템 구현을 위하여 아래 그림과 같이 테스트베드를 구성하여 PLC에 연결된 모형 설비를 동작하였다. 이로부터 제어 데이터를 수집하고, 등록된 화이트리스트 기반의 사용자 행위를 탐지하였다.

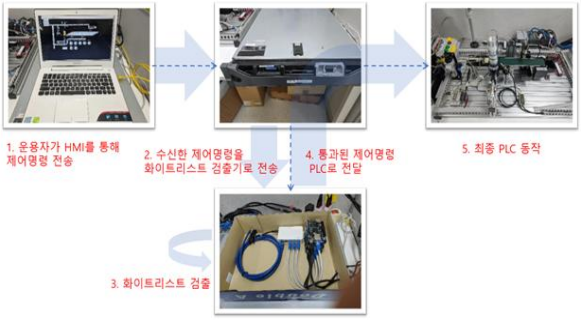

Fig. 4. Procedure for performing normal control commands

운용자가 HMI를 통하여 허가된 제어 명령을 전송하면 수신된 제어 명령을 화이트리스트 검출기로부터 1차적으로 등록된 명령인지

판단하고 최종 PLC 기기로 명령을 전달한다.

Fig. 5. Procedure for performing unregistered control commands

만일 미등록된 제어 명령을 수신한 경우, 미등록된 제어 명령의 수신을 알람 신호로 해당 운용자에게 알리고 수신된 제어 명령을 해당 PLC 시스템으로 전달하지 않는다.

이상징후 분석을 위하여 그림6과 같이 작동 중인 PLC 시스템으로부터 주기적으로 작동 상태 신호를 전달받고, 전달받은 상태 신호의 이전 동작 패턴과 비교, 분석하여 이상 행위 패턴을 검출하였다. 기존의 테스트베드 동작 범위가 벗어나는 작동 명령을 전달하는 시험을 시행하고, 이를 성공적으로 구현 시스템이 검출하는 것을 확인하였다.

Fig. 6. Procedure for analyzing abnormal behavior

IV. Conclusions

본 논문에서는 제조 ICT 융합기술과 더불어 제어 시스템을 대상으로 한 취약성 증가에 따른 안전한 산업 제어 시스템 구축을 위하여 제어 신호를 수집하는 시스템을 구축하고, 수집된 제어 신호를 분석하여 이상행위를 판단하고 알려주는 시스템을 구성하였다. 시스템 구성을 위하여 Modbus 기반의 제어 프로토콜을 대상으로 제어 신호를 분류하고, 이를 화이트리스트 기반으로 이상행위를 탐지함으로써 국내외 산업 제어 시스템에 적용 가능한 보안 탐지 시스템을 제시하였다.

ACKNOWLEDGEMENT

본 연구는 중소벤처기업부의 기술혁신개발사업의 일환으로 수행하였음.(S2457495, 운용자 행위 기반의 산업제어시스템 부정조작 및 오작동 탐지 시스템 개발)

REFERENCES

[1] Headong Kin, et al "Insider Threat Detection based on User behavior Model and Novelty Detection Algorithms" Journal of the Korean Institute of Industrial Engineers, Vol. 43, No. 4, pp. 276-287, 2017.

[2] Dong-wook HA, Ki-tae Kang, and Yeonseung Ryu, "Detecting Insider Threat Based on Machine Learning: Anomaly Detection Using RNN Autoencoder“, Journal of The Korea Institute of Information Security and Cryptology, Vol. 27, No. 4, pp. 763-774, 2017.