정 보 보 호 학 회 지
제29권 제2호, 2019. 4

SWaT 테스트베드 데이터 셋 및 비정상행위 탐지 동향

권 성 문*, 손 태 식**

요 약

CPS(Cyber Physical System)에 대한 사이버 공격이 다양해지고 고도화됨에 따라 시그니처에 기반한 악성행위 탐지는 한계가 있어 기계학습 기반의 정상행위 학습을 통한 비정상행위 탐지 기법이 많이 연구되고 있다. 그러나 CPS 보안 연구는 보안상의 이유로 CPS 데이터가 주로 외부에 공개되지 않으며 또한 실제 비정상행위를 가동 중인 CPS에 실험하는 것이 불가능하여 개발 기법의 검증이 어려운 문제가 있다. 이를 해결하기 위해 2015년 SUTD(Singapore University of Technology and Design)의 iTrust 연구소에서 SWaT(Secure Water Treatment) 테스트베드를 구성하고 36가지의 공격을 수행한 데이터셋을 공개하였다. 이후 국·내외에서 SWaT 테스트베드 데이터를 사용하여 다양한 보안 기법을 검증한 연구 결과가 발표되고 있으며 CPS 보안에 기여하고 있다. 따라서 본 논문에서는 SWaT 테스트베드 데이터 및 SWaT 테스트베드 데이터에 기반한 비정상행위 탐지 연구를 분석한 내용을 설명하고, 이를 통해 CPS 비정상행위 탐지 설계의 주요 요소를 분석하여 제시하고자 한다.

Ⅰ. 서 론

CPS에 대한 사이버공격은 물리적 피해로 이어질 수 있기 때문에 CPS 보안은 매우 중요하다. CPS에 대한 사이버공격은 2009년 Stuxnet 이후 끊이지 않고 있으며 최근에는 2016, 2017년 우크라이나 정전을 유발한 Crashoverride와, 2018년 사우디아라비아의 석유화학 공장을 해킹하여 시스템을 마비시키고 Schneider Electric 社의 안전 계장 시스템에 악성코드를 심어 1억 달러 규모의 피해를 입힌 Triton이 보고된바 있다. 특히 Crashoverride, Triton은 CPS에서 사용되는 고유의 프로토콜을 사용하여 네트워크 통신을 수행하는 모듈을 포함하고 있을 뿐만 아니라 매우 고도화된 악성코드로 분석되어 보고되었다. 이러한 고도화된 사이버공격은 시그니처 기반의 악성행위 탐지로는 불가능하다. 따라서 CPS 환경이 일반 IT(Information Technology) 환경에 비해 규칙적인 점에 착안하여 데이터의 분포에서 규칙을 찾아내거나, SVM(Support Vector Machine), 딥러닝과 같은 기계학습 기법을 통한 정상행위를 학습하여 비정상행위를 탐지하는 다양한 연구가 수행되고 있다. 이러한 CPS 보안 연구를 위해서는 CPS 환경의 데이터셋이 필수적으로 요구된다. 그러나 CPS 환경의 실제 데이터는 보안상의 이유로 주로 외부에 공개되지 않으며 실제 CPS 환경에 비정상행위, 즉 공격을 수행하는 것이 일반적으로 불가능하기 때문에 연구에 효과적으로 활용 가능한 데이터셋을 구하는 것이 쉽지 않다. 따라서 공개된 많은 연구 결과들에 비해 실제 CPS 환경에서 비정상행위 탐지 보안 기술이 효과적으로 적용된 성공적인 사례는 많지 않다.

이러한 문제점을 해결하기 위해 싱가포르 SUTD 대학의 iTrust 연구소에서는 수처리 시스템, 배수 시스템, 전력 제어 시스템에 대한 테스트베드를 구성하고 다양한 시나리오 기반의 공격을 수행한 데이터셋을 구성하여 이를 공개하고 있다. 이 중 수처리 시스템 테스트베드인 SWaT 테스트베드 데이터셋은 일반 도시의 수처리 시스템의 각 단계를 충분히 묘사하고 있으며 36가지의 다양하고 복잡한 공격을 포함하고 있다. 따라서 SWaT 테스트베드 데이터셋은 국·내외 수처리 시스템의 CPS 보안 연구뿐만 아니라 다른 CPS 환경의 보안 연구에서도 사전 연구 데이터로 활용되고 있으며 다양한 연구 결과가 발표되고 있다. 본 논문은 이러한 SWaT 테스트베드 데이터셋에 기반한 비정상행위 탐지 연구 분석을 통해 기존 연구에서의 주요 사항과 보완점을 도출하여 CPS 비정상행위 탐지 시스템 설계에 있어

* 아주대학교 컴퓨터공학과 (calmcombat@gmail.com)
** 아주대학교 사이버보안학과 (tsshon@ajou.ac.kr)

주요 사항에 대해 분석하고 제시하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 SWaT 테스트베드 환경과 데이터셋에 대해 설명하며, 3장에서는 SWaT 테스트베드 데이터셋을 이용한 다양한 비정상행위 탐지 연구를 설명한다. 4장에서는 3장의 다양한 비정상행위 탐지 연구를 통해 CPS 비정상행위 탐지 시스템 설계의 주요 사항을 분석하며, 마지막 5장에서 결론을 맺는다.

Ⅱ. SWaT 테스트베드 환경 및 데이터셋

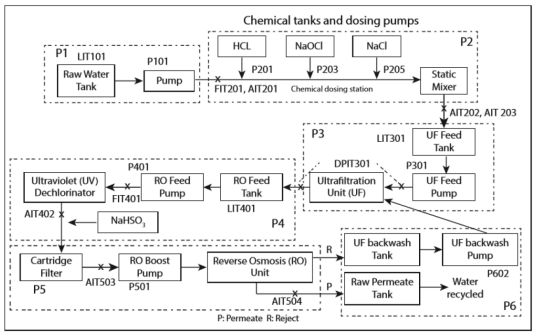
2장에서는 SWaT의 테스트베드 환경과 데이터셋에 대한 특성을 상세 설명한다.

2.1. SWaT 테스트베드 환경

SWaT 테스트베드는 SUTD의 iTrust 연구소에서 2015년 제작한 테스트베드로 일반 도시에서 사용되는 수처리 시스템을 축소하여 구축한 것이며 그림 1과 같다. 총 6단계로 구성되어 있으며, 3종류 32개의 actuator와 5종류 25개의 센서로 구성되어 있다. actuator에는 물, 화학품을 공급하는 펌프(P)와 벨브(MV), 자외선을 통해 염소를 제거하는 모듈(UV)이 있으며 센서에는 물탱크의 높이를 측정하는 센서(LIT), 단위 시간당 물 이동 량을 측정하는 센서(FIT), 전도율 및 pH 농도를 측정하는 센서(AIT), 현재 압력(PIT)과 압력의 변화량(DPIT)을 측정하는 센서가 있다.

그림 2는 SWaT 테스트베드의 전체 6단계별 구성도를 표현한 것이다. 1단계는 원수(RAW water)를 탱크

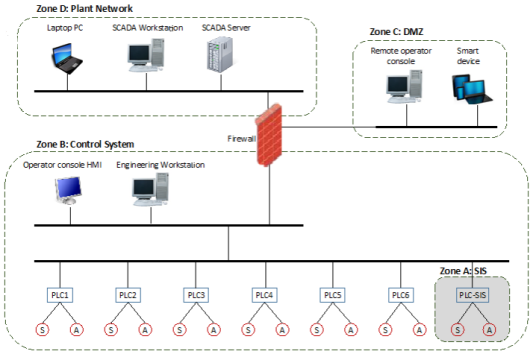
〔그림 1〕 SWaT 테스트베드〔1〕



〔그림 2〕 SWaT 테스트베드 각 단계별 구성도〔1〕

에 공급하여 저장하는 단계이다. 2단계는 원수의 질을 조정하는 단계로 원수의 질이 나쁜 경우 HCl, NaOCl, NaCl과 같은 화학약품을 통해 원수의 질을 조정한다. 3단계는 한외 여과기(ultrafilter)를 통해 불필요한 요소들을 걸러내며, 4단계에서는 자외선을 통해 잔여 염소를 제거한다. 5단계에서는 역삼투(reverse osmosis) 시스템을 통해 무기물 종류의 불순물을 걸러내며, 마지막 6단계에서는 물 공급 시스템을 모방하기 위한 시스템으로 최종적으로 생산된 물을 방류한다.

모든 계측은 1초에 한 번 씩 수행되고 있으며, 따라서 특정 사이버 공격이 1초 이내에 수행되지는 않는다고 가정하고 있다. 각 단계 별로 1대의 PLC(Programmable Logic Controller)가 센서와 actuator를 제어하고 있으며 네트워크 통신 프로토콜은 Rockwell 社의 PLC를 사용함에 따라 해당 기기가 사용 중인 Ethernet/IP에 기반한 CIP(Common Industrial Protocol)를 이용하여 통신하고 있다. 네트워크 구성도는 그림 3과 같다.



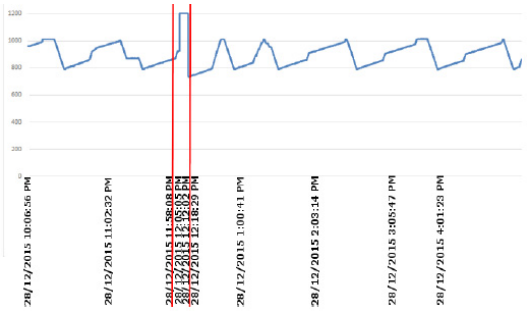
〔그림 3〕 SWaT 테스트베드 네트워크 구성도〔2〕

2.2. SWaT 테스트베드 데이터셋

SWaT 테스트베드 데이터셋은 iTrust 연구소 홈페이지에서 요청하여 다운로드 링크를 제공받을 수 있다. 데이터셋은 총 11일 동안 중지 없이 캡처한 데이터로 7일은 정상 동작 데이터이며, 나머지 4일은 공격을 수행을 포함한 데이터이다. 단, 테스트베드 가동 후 물탱크가 완전히 비어 있는 상태에서 원수를 공급하여 시스템의 정상 동작 까지 30분이 소요되었으며, 데이터셋 version 0은 해당 30분이 포함된 데이터셋이며 version 1은 해당 30분이 제거된 데이터셋이다. 데이터셋은 패킷 데이터와 CSV(Comma-separated Values) 데이터로 제공된다. 패킷 데이터는 Ethernet/IP 기반 CIP 패킷 데이터로 구성되어 있다. 반면 CSV 데이터는 57개의 센서 및 actuator 중 실제 SWaT 테스트베드 동작에 불필요하다 판단되는 6개를 제외한 51개의 센서와 actuator에 대하여 매초 기록된, 총 946,722개의 정보로 구성되어 있다.

공격은 공격자가 내부의 패킷을 가로채어 조작할 수 있다는 조건하에 수행되었으며 오직 응용 계층에서의 데이터 조작으로 총 36가지의 공격이 수행되었다. 수행된 공격의 유형은 크게 4가지로 나뉜다. SSSP(Single Stage Single Point) 공격 유형은 하나의 단계에 대하여 하나의 데이터를 조작한 공격이며 SSMP(Single Stage Multi Point) 공격 유형은 하나의 단계에 대하여 다수의 데이터를 조작한 공격이다. 반면 MSSP(Multi Stage Single Point), MSMP(Multi Stage Multi Point)는 다수의 단계에 대하여 각각 단일, 다수의 데이터를 조작한 공격이다. SSSP 26가지, SSMP 4가지, MSSP 2가지, MSMP 4가지 공격이 수행되었다. 각 공격은 목표를 달성하기 위해 단 몇 분에서 길게는 몇 시간에 이르는 공격이 있다. 또한 다른 공격이 수행되기 전에 시스템을 정상으로 다시 돌려두고 수행한 독립적인 공격과 다수의 공격을 동시에 수행한 공격이 있다. 각 공격은 물탱크 범람과 같은 바로 드러나는 물리적 공격부터 시스템의 성능을 저하시켜 겉으로 드러나지 않으며 지속적으로 피해를 줄 수 있는 공격 등 실제 물리적 피해를 초래하는 시나리오로 구성되어 있다. 그림 4는 물탱크의 수위를 실제 값 보다 낮은 값으로 조작하여 실제 물 높이가 높아졌음에도 이를 인식하지 못하게 하여 물탱크를 범람하게 하는 공격이다. 반면 그림 5는 실제 물탱크의 수위를 실제 값보다 높게 조작하여 물의 공급을 멈추고

〔그림 4〕 SSSP 공격 예시 1 - 물탱크의 수위를 실제 값 보다 낮은 값으로 조작함



〔그림 5〕 SSSP 공격 예시 2 - 물탱크의 수위를 실제 값 보다 높은 값으로 조작함

물을 방류하게 함으로써 물의 생산량을 낮추는 공격이다.

이와 같이 SWaT 테스트베드 데이터셋은 실제 물리적 피해를 초래하며, 탐지가 쉬운 공격부터 매우 어려운 공격까지 포함되어 있기 때문에 정상행위 모델의 비정상행위 탐지 검증에 활용도가 높아 다양한 연구에서 활용되고 있다.

Ⅲ. SWaT 비정상행위 탐지 연구

3장에서는 SWaT 테스트베드 데이터셋을 이용한 다양한 비정상행위 탐지 연구에 대해 설명한다. 기계학습을 이용한 연구로 SVM을 이용한 A. Agrawal *et al.*의 연구[3], 딥 러닝을 이용한 J. Goh *et al.*의 연구[4], Bayesian network를 이용한 Q. Lin *et al.*의 연구[5]를, 데이터의 특성을 이용한 C. Feng *et al*의 연구.[6]을 설명한다.

3.1. SVM - Agrawal *et al*.의 기법

SVM이 기계학습의 한 세대를 주름 잡았던 훌륭한 기법임에는 틀림없지만, CPS 환경의 비정상행위를 탐지하기 위한 일련의 데이터처리에는 적합하지 않다고 볼 수 있다. 따라서 Agrawal *et al*.은 데이터의 변화량을 SVM의 feature로 사용하였다. OCSVM(One-class Support Vector Machine)이 아닌 SVM을 사용함에 따라 정상, 비정상으로 레이블된 데이터로 지도학습을 수행하였으며, 비정상으로 분류된 공격은 수처리 시스템의 생산성을 낮추는 것을 목적으로 하여 공격자가 쉽게 드러나지 않는 공격만을 포함하였다. 실험 결과 10초 단위의 데이터 변화량을 사용하여 정상, 비정상 데이터를 지도학습을 수행하였을 때, 96.87%로 가장 좋은 정확도를 가진 것으로 보고되었다.

3.2. 딥 러닝 – J. Goh *et al*.의 기법

딥 러닝의 기법 중 RNN(Recurrent Neural Network)은 일련의 데이터 예측에 적합한 기법이다. 각 센싱 데이터 자체를 인풋으로 하여 다음 센싱 데이터를 예측하는 모델을 생성할 수 있으나 모델의 결과 값을 통한 비정상행위 판별에 있어 문제가 있다. 정상과 비정상의 판별은 RNN 모델의 예측 값과 실제 값의 차이가 특정 임계치를 초과하는 지로 수행한다. 이 임계치는 모두 동일한 값이 아닌 각 데이터의 분산과 같은 특징에 따라 다르게 설정되어야 한다. 따라서 J. Gho *et al*.은 이러한 문제를 해결하기 위해 일련의 데이터의 변화가 예측 범위인지 판별하는 고전적인 기법인 누적합(CUSUM, Cumulative Sum) 관리도 분석 기법을 각각의 센싱 데이터에 개별적으로 사용하였다. 이를 통해 RNN의 종류 중 하나인 LSTM(Long Short-Term Memory)으로 정상행위만을 학습하여 비정상행위 10 유형 중 9 유형을 탐지하는 결과가 보고되었다. 반면, 다음과 같은 한계점을 지닌다. RNN의 높은 계산량 때문에 50만개의 데이터 기준 SWaT의 1단계의 센서, actuator의 값 만을 학습하는 데만 24시간이 걸려 2~6단계는 학습이 불가능하였던 문제점이 있다. 그리고 RNN의 비정상 인풋이 들어감에 따라 다음 예측 값에도 영향을 주어 공격 데이터 이후 다음 정상 데이터 예측 또한 실패하는 경우가 관찰되어 결과 값 해석을 위한 보정이 필요하였다.

3.3. Bayesian network - Q. Lin *et al*.의 기법

J. Goh *et al*.의 기법이 RNN을 통해 센서, actuator 간의 연관성을 비교적 블랙박스 기법으로 찾는 기법이라면 Q. Lin *et al*.의 기법은 데이터를 단순하게 전처리하고 Bayesian network를 사용하여 비교적 직관적으로 센서, actuator 간의 연관성을 찾는 기법이라 할 수 있다. 우선 센싱 데이터의 변화량을 단순하게, SU(Slow Up), QU(Quick UP), SC(Staying Constant), QD(Quick Down)[1]로 표현하였다. 이후 동일 시간대의 센서, actuator의 값을 K2[7] 알고리즘을 사용하여 Bayesian network를 학습함으로써 센서, actuator 간의 연관관계를 도출하였다.[2] 학습 결과 학습 시간과 테스트 시간이 각각 214초, 33초 밖에 걸리지 않는 장점과 전체 36 유형의 공격 중 24 유형의 공격을 식별하여 타 알고리즘에 비해 비정상행위 탐지율이 높은 장점이 있다. 단, 정상행위에 대한 오탐률이 높은 단점 또한 갖고 있다.

3.4. 데이터의 특성 - C. Feng *et al*.

C. Feng *et al*.은 Siemens 社와 SUTD가 공동 수행한 연구로 CPS 데이터 특성에 기반한 규칙을 생성하여 정상과 비정상을 판별하는 알고리즘을 제안하였다. 알고리즘은 간단한 2가지의 특성에 기반하고 있다. 첫째, 센서 계측 값의 변화는 특정 actuator와 같은 다른 요소의 상태에 기인한다. 가령 1번 물탱크의 수위가 증가하고 있으면, 1번 물탱크의 펌프가 on 되어 있기 때문이다. 이후 1번 물탱크의 수위 변화가 바뀌었다면, 이는 임의적인 것이 아닌 다른 actuator의 상태 변화가 있었을 것이며 동일한 actuator의 상태 내에서는 물탱크의 수위 변화 또한 같을 것이다. 둘째, actuator를 조작하는 특정 이벤트가 발생하였을 시, 이는 임의로 조작된 것이 아닌 특정 센서 값의 결과로 actuator를 조작하는 결과가 발생한 것이다. 가령 1번 물탱크의 펌프가 off 되는 경우는 1번 물탱크의 수위가 특정 임계치를 넘은 것 때문일 수 있다. 두 가지 특성 모두 간단한 개념이나, 이를 이용하기 위해서는 다음과 같은 문제점이 있다. 첫 번째 특성의 문제점은 센서 계측 값의 변화가 어떤

1) SD(Slow Down)는 데이터 상에서 관찰되지 않았음
2) 학습/테스트 데이터셋의 구성에 대한 내용은 기술되어 있지 않음

actuator의 상태 변화에 따른 변화인지 알 수 없을뿐더러, 해당 센서에 영향을 주는 actuator 가 몇 개인지, 또한 actuator 간의 상태 변화의 조합에 따라서도 센서 계측 값이 변화할 수 있어 현재 센서 계측 값의 변화가 어떤 특정 상태인지 정의하는 것이 힘들다. 두 번째 특성의 문제점은 특정 이벤트가 발생 했을 때, 어떤 센서의 값이 해당 이벤트를 발생시켰는지를 파악해야 한다. 물론 두 가지 문제점 모두 SWaT 시스템 수준의 규모가 작은 경우 시스템 운영자가 수동으로 규칙을 생성하여 정상행위를 규정할 수도 있다. C. Feng *et al*.의 연구에서도 평가 단계에서 해당 두 가지 특성에 기반하여 시스템 관리자가 작성한 규칙이 99.5%의 높은 정상행위 판별률을 보인 바 있다. 그러나 전력제어시스템과 같이 대규모 CPS 시스템에서는 데이터의 종류가 적게는 수백 개에서 많게는 수만 개까지 되며 이 경우 사람이 직접 만드는 규칙은 한계가 있다. 우선 첫 번째 특성의 문제점을 해결하기 위해서, 각 센서 데이터의 변화량이 몇 개인지 모르는 특정 정규분포를 따른다는 가정을 하였다. 그리고 센서 데이터의 변화량을 EM (Expectation-maximization) 알고리즘을 사용하여 적합한 정규 분포의 개수를 찾아 GMM(Gaussian Mixture Model)을 생성하였다. 이를 통해 센서의 변화량이 실제 어떠한 actuator의 상태 조합에 따른 값인지는 모르지만 특정 actuator의 상태 조합에 해당하는 것으로 분류를 수행할 수 있다. 그리고 실제 각 센서 변화량의 분포와 actuator 상태 조합 간의 조건부 확률을 통해 적합한 규칙을 생성하였다. 두 번째 특성의 문제점을 해결하기 위해서는 특정 이벤트에 대한 센서 값의 선형 회귀 모델을 통해 L1 손실 값을 최소화하는 센서 종류만을 선택함으로써 특정 이벤트에 영향을 주는 센서 값을 찾아내었다. 주요 특성이 간단한 만큼 알고리즘의 원리도 직관적이고 간단하다. 학습 결과 99.9%의 정상행위 학습률을 보였으나 공격 탐지율은 79%에 그쳤다.

Ⅳ. SWaT 비정상행위 탐지 연구 분석

본 장에서는 SWaT 테스트베드 데이터셋에 대한 비정상행위 탐지 연구들을 통해 CPS 비정상행위 탐지엔진 설계시의 주요 사항에 대해 분석한다.

정상과 비정상을 판단하기 위한 모델의 구성방법은 다양하다. SVM, 딥 러닝, Bayesian Network 등 기계학습 알고리즘이 사용될 수도 있으며, 데이터 특성에 기반한 C. Feng *et al*. 알고리즘이 또한 일부 기계학습 알고리즘을 이용하고 있으며 이는 다량의 데이터 및 유형에서 사람의 한계를 극복하기 위함이다. 단, 해당 알고리즘을 CPS 환경에 효과적으로 적용하기 위해서는 각 알고리즘을 이해하고 알고리즘의 선택 뿐만 아니라 알고리즘의 정확도 개선 또는 CPS 특성을 반영하기 위한 알고리즘별 전처리 과정이 수행이 필수적일 것이다.

학습 방법에서는 크게 지도학습과 비지도학습이 있으며, SVM의 경우 알고리즘의 특성상 지도학습이 사용되었다. 그러나 동일한 데이터 전처리로 OCSVM을 통한 비지도학습을 수행하여 정상행위 학습 이후 비정상행위 탐지에 활용 될 수도 있다. 단, 지도학습은 일반적으로 CPS 환경에서 공격데이터에 대한 취득이 어려워 적용이 불가능한 경우가 많다. 해당 CPS 환경에서 SWaT 테스트베드 데이터셋과 같이 다양하고 치밀한 내부자 공격 또는 false data injection[8]과 같은 세밀한 공격을 수행하여 탐지 엔진을 검증을 수행하는 것이 바람직하나 실제 가동 중인 CPS 환경의 가용성을 해칠 수 있기 때문에 문제가 된다. 따라서 다른 CPS 환경의 비정상행위 탐지 시스템 개발 시 SWaT 테스트베드 데이터셋에 방법론을 일부 검증해보거나 SWaT 테스트베드와 같은 각 CPS 환경의 특성을 반영한 축소된 테스트베드를 구축하여 개발 시스템의 검증을 수행해야 할 것이다.

비정상행위 탐지 엔진의 정확도 면에서도 차이가 있다. Q. Lin *et al*.의 연구는 비정상행위 탐지율이 높은 대신 정상행위에서의 오탐률이 높다. 반면, C. Feng *et al*.의 연구는 정상행위 탐지율이 매우 높은 반면, 비정상행위 탐지율이 비교적 낮다. Triton 악성코드의 경우 감염 이전에 사이버해킹의 시도를 의미하는 알람이 다수 발견되었음에도 무시되어 사이버공격이 성공한 사례이다. 따라서 비정상행위 탐지율이 높더라도 다수의 데이터를 차지하는 정상행위에서 오탐률이 높다면 수 많은 오경보가 발생하여 실제 비정상행위가 탐지되더라도 무시될 가능성이 높다. 따라서 비정상탐지 시스템 개발에 있어 탐지 로그를 효과적으로 분석할 수 있는 도구나 충분한 인력 등을 고려하여 효과적으로 활용 될 수 있도록 하여야 한다.

마지막으로 SWaT 데이터는 응용 계층에서의 데이터 조작만을 포함하고 있다. 이는 네트워크상에서의 공

격은 수행되지 않음을 뜻한다. 그러나 [9]의 DNP3 패킷 재조립을 불가능하게 하는 공격과 같이 네트워크 상의 데이터 취득 중 가용성을 방해받을 수 있어 네트워크 상의 보안 또한 중요히 고려되어야 하는 보안 요소이다. 따라서 네트워크를 통한 데이터 취득에 대한 보안을 보장하고, 응용계층에 대한 보안을 수행해야 할 것이다.

Ⅴ. 결 론

본 논문에서는 SWaT 테스트베드 및 데이터셋과 이를 이용한 비정상행위 탐지 연구를 설명하고 분석하였다. SWaT 테스트베드에 기반한 연구의 방법론을 다른 CPS에 적용하는 것도 좋은 방법이나 성공적으로 바로 적용될 수는 없을 것이다. 따라서 SWaT 테스트베드와 같이 축소된 버전의 다른 CPS 환경을 구성하여 활용하거나, 해당 CPS 환경을 반영한 기법을 SWaT 테스트베드 데이터셋을 통해 유효성을 일부 사전 검증하는데 활용할 수 있을 것이다. CPS 비정상행위 탐지 시스템 개발에 설계에 있어서는 비지도학습/지도학습 또는 정상행위/비정상행위에 초점을 맞출지 고려해야 하며 이를 통해 올바른 알고리즘 또는 방법론을 선택해야 한다. 또한 이후 탐지 엔진의 결과물을 효과적으로 활용하기 위한 방안 또한 함께 고려되어야 하는 주요 요소이다. 이외 SWaT 테스트베드 데이터셋에 고려되지 않는 네트워크 특성 또한 고려되어 네트워크를 통한 정상적인 데이터 취득이 보장되어야 할 것이다.

참 고 문 헌

[1] Goh, Jonathan, et al. “A dataset to support research in the design of secure water treatment systems.” International Conference on Critical Information Infrastructures Security. Springer, Cham, 2016.

[2] SWaT testbed, by iTrust of SUTD, [Online]. Available: https://itrust.sutd.edu.sg/testbeds/secure-water-treatment-swat/

[3] Agrawal, Anand, Chuadhry Mujeeb Ahmed, and Ee-Chien Chang. “Poster: Physics-Based Attack Detection for an Insider Threat Model in a Cyber-Physical System.” Proceedings of the 2018 on Asia Conference on Computer and Communications Security. ACM, 2018.

[4] Goh, Jonathan, et al. “Anomaly detection in cyber physical systems using recurrent neural networks.” 2017 IEEE 18th International Symposium on High Assurance Systems Engineering (HASE). IEEE, 2017.

[5] Lin, Qin, et al. “TABOR: A Graphical Model-based Approach for Anomaly Detection in Industrial Control Systems.” Proceedings of the 2018 on Asia Conference on Computer and Communications Security. ACM, 2018.

[6] Feng, Cheng, et al. “A Systematic Framework to Generate Invariants for Anomaly Detection in Industrial Control Systems.” (2019).

[7] Gregory F Cooper and Edward Herskovits. 1992. A Bayesian method for the induction of probabilistic networks from data. Machine learning 9, 4 (1992), 309–347.

[8] Liu, Yao, Peng Ning, and Michael K. Reiter. “False data injection attacks against state estimation in electric power grids.” ACM Transactions on Information and System Security (TISSEC) 14.1 (2011): 13.

[9] Kwon, Sungmoon, Hyunguk Yoo, and Taeshik Shon. “Recovery Measure against Disabling Reassembly Attack to DNP3 Communication.” IEICE Transactions on Information and Systems 100.8 (2017): 1790-1797.

〈저 자 소 개〉

권 성 문 (Sungmoon Kwon)

학생회원

2013년 2월 : 아주대학교 정보컴퓨터공학부 졸업(학사)
2013년 3월~현재 : 아주대학교 컴퓨터공학과 통합과정
<관심분야> 전력제어시스템 보안, 디지털 포렌식, 비정상행위탐지

손 태 식 (Taeshik Shon)

종신회원

2000년 2월 : 아주대학교 정보및컴퓨터공학부 졸업(학사)
2002년 2월 : 아주대학교 정보통신전문대학원 졸업(석사)
2005년 8월 : 고려대학교 정보보호대학원 졸업(박사)
2004년 2월~2005년 2월 : University of Minnesota 방문연구원
2005년 8월~2011년 2월 : 삼성전자 통신· DMC 연구소 책임연구원
2017년 3월~2018년 2월 : Illinois Institute of Technology 방문교수
2011년 3월~현재 : 아주대학교 정보통신대학 사이버보안학과 교수
<관심분야> ICS/SCADA, DFIR, Anomaly Detection