Ben-Gurion University of the Negev

Faculty of Engineering Science

Department of Software and Information Systems Engineering

Project in Advanced Topics in Cyber Security

OAI Final Project - Robustness of Real Time deepfakes

Author:
Amit Kama

Author:
Ron Magen

Author:
Barak Yacouel

June 1, 2022

Contents

1 Introduction

Industrial control system (ICS) is a general term that encompasses several types of control systems and associated instrumentation used for industrial process controls. Control systems can range in size from a few modular panel-mounted controllers to large interconnected and interactive distributed control systems (DCSs) with many thousands of field connections. Larger systems are usually implemented by supervisory control and data acquisition (SCADA) systems, or DCSs, and programmable logic controllers (PLCs), though SCADA and PLC systems are scalable down to small systems with few control loops.

ICSs are extensively used in many industries, including power generation, water treatment, oil and gas processing, industrial manufacture, and telecommunications. Most systems use information obtained from Remote Terminal Units (RTUs) to generate commands automatically or manually by a human operator. The commands are passed back to the remote end units on the basis of some communication infrastructure.

As stated in [?], "cyber attacks against ICS would lead to disruption to controlling those critical infrastructures and result in harmful physical damage to plants, environment and humans. According to ICS-CERT, the ICS-targeted attacks have been continuously increasing in the past few years. There were 73 incidents reported to ICS-CERT by trusted industrial partners in 2013, then 245 reported in 2014 and 295 incidents in 2015".

According to [?], the typical architecture of modern ICS roughly consists of three networks; a corporate network which provides business to business and business to customer services, a control network, which receives and processes data from field devices and responses with proper control commands, and lastly, a field network which is the fusion of PLCs, actuators and sensors for measurement data transmission and the direct control of industrial processes. They also stated that cyber attacks against ICS often start with gaining access to the the corporate network, which is usually exposed to the internet, then propagate virus across the whole network in search of valuable targets, and finally sabotage control programs running on field devices. The first widely documented ICS cyber attack was Stuxnet, disclosed in 2011. In this case, the virus was introduced by a removal drive, and eventually managed to change the program controlling field devices.

One Promising ICS security solution is an anomaly detection system, which monitors the network traffic and field devices' data logs, and utilize this information in order to warn of a possible intrusions. Although anomaly detection is the basis of many security systems developed in recent years, only a few of them are specifically designed to secure ICS systems. Therefore, there is an urgent need of effective ICS specific anomaly detection systems.

In light of this, there is a significant need to create datasets relevant to ICS and from various fields, that will be used to train and test those systems. As stated in [?], "a number of datasets to design and study anomaly detectors have been published (e.g., BATADAL, SWaT, and WADI). Those datasets consist of multivariate time series of sensor readings that occurred in an ICS (real plant, testbed, or simulation). Datasets for ICS anomaly detection are often provided in different data captures. Usually, there are at least two data captures. The first (generally used as a Training set) contains data collected during normal operating conditions. The second (generally used as the Test set) contains data collected while attacks are occurring".

Collection and creation of datasets for security research in ICSs are not easy tasks. As stated in [?], when doing so, it is essential to construct and reproduce various attack situations. When leveraging a dataset for anomaly detection, both a normal dataset and an abnormal dataset should be provided for learning and evaluation. Without an abnormal dataset that includes attack-related data, it cannot be evaluated whether it trains properly or detects anomalies. Such a dataset is helpful for research on the following areas: development of data-driven defense technologies, such as machine learning; testing of various attack situations; and performance evaluation according to the desired purpose.

In this work, we present a survey of open and available ICS datasets from various domains, which can be used to implement anomaly detection algorithms in ICS-related studies. We provide the needed background to use each dataset, and a demonstration of how to implement machine learning algorithms to the main one. Lastly, we present a comparison table between the various datasets, which allows the selection of appropriate datasets to perform anomaly detection tasks.

2 ICS Datasets

Given the growing need for IDS and IPS for securing ICS, there is a growing need to create quality datasets for training and evaluating anomaly detection models. This includes setting up testbeds, collecting data from them, and usually simulating data to provide anomalies. In this section we present the main datasets developed for the purpose of training and evaluating such models in the ICS domain.

2.1 BATADAL

BATADAL dataset was released with 'The Battle Of The Attack Detection Algorithms', a competition to detect cyber attacks on water distribution networks [?]. The BATADAL dataset represents a water distribution network consisting of seven storage tanks with eleven pumps and five valves, controlled by nine PLCs. The network was generated with epanetCPA, a MATLAB toolbox that allows the injection of cyber attacks and simulates the network's response to the attacks. The test dataset contains 2,089 records (from 87 days of recording) with seven attacks [?]. The dataset is divided into three data chunks: the first contains the sensor readings collected during 365 days of normal operations, the second and the third contain the sensor data collected during 14 cyber attacks. BATADAL dataset features a collection of 43 sensors and actuators, i.e., water levels, the pressure at pumping stations, flow, and actuator status. There are two available versions of the dataset, the original one, which contains replay attacks aimed to conceal the true system state, and the second one, which contains sensor readings without concealment. The second version consists of two different Test sets.

2.2 HAI

HIL-based Augmented ICS (HAI) dataset was collected in 2017 from a realistic ICS testbed augmented with a simulator that emulates steam-turbine power generation and pumped-storage hydropower generation. There are three versions of HAI - HAI 1.0, HAI 20.07 and HAI 20.03. Two major versions of HAI datasets have been released so far. Each dataset consists of several CSV files, and each file satisfies time continuity. HAI 21.03 was released in 2021, and is based on a more tightly coupled HIL simulator to produce clearer attack effects with additional attacks. This provides more

quantitative information and covers a variety of operational situations and better insights into the dynamic changes of the physical system [?].

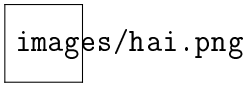

Figure 1: HAI framework [?].

2.3 SWaT

The Secure Water Treatment (SWaT) plant is a scaled-down water treatment plant which was built at the Singapore University of Technology and Design. It consists of six steps process in which the water is gradually filtrated and purified, and is able to produce five US gallons/hr of filtered water. Each step is equipped with a precise number of sensors and actuators. The dataset contains seven days of recording under normal conditions and four days during which 36 attacks were conducted [?]. There are many versions of the SWaT dataset, opening also a fragmentation problem when using it as a benchmark for the detection algorithms. We refer to the network traffic as the pcap dump of the network communications and as physical data the value of the sensors and actuators recorded [?].

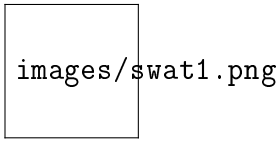

Figure 2: SWaT framework.

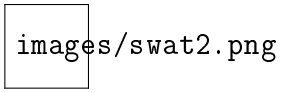

Figure 3: SWaT framework.

2.4 WADI

The WADI dataset has been collected from a scaled-down water distribution testbed and compiled by the developers of SWaT. The testbed consists of large water tanks that supply water to consumer tanks. The dataset contains 16 attacks whose goal is to stop the water supply to the consumer tanks [**?**]. More specifically, WADI is a realistic ICS testbed that reproduces a water distribution network. It comprises two elevated reservoir tanks, six consumer tanks, and a return tank (for water recycling purposes). It is controlled by 103 sensors and actuators connected to three PLCs. Each PLC controls one of the following stages: P1 (primary supply and analysis), P2 (elevated reservoir with domestic grid and leak detection), and P3 (return process). The dataset is divided into two data chunks, the first contains 14 days of normal operations, the second contains 15 attacks on the physical process that occurred over two days of operations. There are two versions of the WADI dataset available on request. As reported by the authors of the dataset, the newer version resolves some problems of the data contained in the first version. The new version refers to the same testbed run but with about 35% fewer lines [**?**]. The dataset is significantly larger than the SWaT and BATADAL datasets; there are 1,209,610 data points in the training set and 126 features [**?**].

2.5 EPIC

The EPIC dataset describes the operational Electric Power and Intelligent Control (EPIC) testbed. EPIC is an electric power testbed that mimics a real world power system in small scale smart-grid. Comprising four stages, namely Generation, Transmission, Micro-grid, and Smart Home, EPIC is capable of generating up to 72 kVA power. It is designed to enable cyber security researchers to conduct experiments and assess the effectiveness of novel cyber defense mechanisms. Physical process: EPIC has two motor-driven generators (Generator1 and Generator2), Photovoltaic (PV) panels, Battery system-with state-of-charge (SOC) based control and Load demand [**?**].

Figure 4: EPIC Control Room.

Figure 5: EPIC Generator and Battery Room.

2.6 D1 - Power System Datasets

Created by Uttam Adhikari, Shengyi Pan, and Tommy Morris in collaboration with Raymond Borges and Justin Beaver of Oak Ridge National Laboratories (ORNL). The datasets include measurements of data logs from Snort (IPS software) and are related to electric transmission system normal, disturbance, control and cyber attack behaviors [?]. There are three datasets contained in this project, which are made from one initial dataset consisting of 15 sets with 37 power system event scenarios in each. The multiclass datasets are in arff format. The 37 scenarios are divided into Natural Events (8), No Events (1) and Attack Events (28) [?]. The dataset was randomly sampled and transformed into three different datasets:

1. Binary - divides between Attack and No attack
2. Three-class - divides between Natural, No events, and Attacks
3. Multiclass datasets - divides between every possible event

As can be seen in the attached jupyter notebook [?], we implemented classification of binary classes on this dataset, which as maintained, contains power system data. First, we read the data and then applied basic pre-processing on the dataset which includes handling with missing values, and transforming the features data to a suitable format (which includes discretization if needed). Afterwards, we have done a randomized division of the dataset to train set and test set. Having train and test sets, we have done the following for three machine-learning and deep-learning algorithms: We read the data, definied parameters and hyper parameter optimization using Grid Search. We then chose the best model and used it to predict the classes on the test set. Lastly, we presented the results using various known metrics, such as precision and recall for each class. The algorithms we have chosen are:

1. Linear SVM Model
2. Bagging classifier of decision trees

3. Basic Deep-learning MLP(Multi layer perceptron) network

Below is a summary of the main results we obtained (N = Normal; A = Anomaly).

Algorithm / Metric	Precision (N, A)	Recall (N, A)	Accuracy
Linear SVM	0.75, 0.52	0.99, 0.03	75%
Bagging of DT's	0.9, 0.89	0.9, 0.89	92%
MLP	0.85, 0	0.85, 0	74%

2.7 D3 - Gas Pipeline and Water Storage Tank

Wei Gao and Tommy Morris have created a datasets of cyber attacks against two laboratory scale ICSs; a gas pipeline and water storage tank. They created a gas pipeline testbed which is used to move natural gas and other similar products to the market. The gas pipeline testbed represents a typical SCADA system embracing an MTU, RTU, and an HMI. The gas pipeline control system contains an air pump that pumps air into the pipeline, a pressure sensor that allows pressure visibility at the pipeline and remotely on the HMI, a release valve and a solenoid release valve to loose air pressure from the pipeline. The allowed pressure range in the pipeline is from 0 to 20 PSI (pound per square inch), with a margin of 10% which fixes the maximum accepted pressure to 22 PSI. The pipeline operates in three principal modes: the first mode is characterized by a very low pressure maintained around 0.1 PSI; the second mode pressure maintained around 10 PSI (the accepted range lays between 9 and 11 PSI); and the third mode should maintain the pressure around 20 PSI (the accepted range is 18 to 22 PSI). The high pressure (greater than 22 PSI) and the transitional states between different modes are considered as anomalies. They reviewed various cyber attacks by their influence on the gas system at each mode, and by that collected data into a dataset from their testbed. To create this dataset, traffic between the Master Terminal Unit (MTU) and the slave Remote Terminal Unit (RTU) was recorded in a file, that contains 28 attacks/anomalies against the gas pipeline. Each line in the new dataset represents one network transaction. the format of the final dataset file is arff [**?**].

2.8 D4 - New Gas Pipeline

Ian Turnipseed developed a new set of datasets with more randomness. These samples are originated only from the gas pipeline control system. This is an improved version of the same dataset in 3. Ian changes the previous dataset structure(one arff dataset) into a raw dataset and an arff dataset:

1. The raw dataset contains the whole MODBUS frame, which was not included in the previous dataset.

2. The arff dataset contains a deep packet inspection of the MODBUS frame.

Figure 6: New Gas Pipeline Scheme. [?]

Water Storage: This dataset comes from the daily measures of sensors in an urban waste water treatment plant. Each sample contains 38 attributes related to the measurements of several important components in the water such as input zinc, input pH, input biological demand of oxygen, input suspended solids, input conductivity, input volatile suspended solids, input sediments to secondary settler, output chemical demand of oxygen, output volatile suspended solids, and other attributes. The values of each attribute vary in a different manner, i.e., the range of input pH is between 6.9 and 8.7, input zinc between 0.1 and 33.5, input conductivity between 651 and 3230, input suspended solids between 98 and 2008, and input sediments to secondary settler between 0 and 3.5. The train set contains 513 samples related to four different normal situations, whereas the test set encloses measurements of abnormal situations such as after storms or when solids overload. The water treatment dataset contains 2.95% of missing attributes [?].

2.9 D5 - Energy Management System Data

The data is arranged in rows where each row is a unique event, except the first row which gives names of the columns. The dataset includes 30 days of events as logged by an Energy Management System (EMS) at an investor owned utility in the United States of America. The data in the dataset has been anonymized by changing the names of operators, devices, and facilities [**?**].

2.10 Cyber Security MODBUS

This dataset was generated on a small-scale process automation scenario using MODBUS/TCP equipment, for research on the application of ML techniques to cybersecurity in ICSs. The testbed emulates a CPS process controlled by a SCADA system using the MODBUS/TCP protocol. The PLC communicates horizontally with the RTU, providing insightful knowledge of how this type of communications may have an effect on the overall system. The PLC also communicates with the Human-Machine Interface (HMI) controlling the system. The testbed is depicted in Figure 7 [**?**].

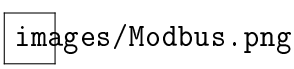

Figure 7: Cyber Security MODBUS.

The dataset contains different scenarios that control different industrial processes. For each scenario, files are provided to capture normal communication and communication with anomalies. The data is in csv format and contains a collection of network packets (pcaps) from wireshark, with 12 fields which are provided in wireshark packet inspection information.

2.11 WUSTL-IIOT-2018

This dataset was built using the SCADA system testbed in order to emulate real-world industrial systems closely. In this testbed, the focus was on reconnaissance attacks where the network is scanned for possible vulnerabilities to be used for later attacks. In order to construct it, scan tools have been used to inspect the topology of the victim network (in this case, the testbed), and identify the devices in the network as well as their vulnerabilities. There

are 5 types of attacks that have been carried out against the testbed, among them are exploit attacks, port scanning, and more [?].

All network traffic (normal and abnormal traffic) was monitored by the Audit Record Generation and Utilization System (ARGUS) tool. The monitored traffic is captured and stored in a "csv" file.

This dataset has been collected during 25 hours, and contains about 7M samples, while around 6% of them corresponds with cyber attacks and the other ones corresponds with normal traffic. The data contains 25 networking features.

2.12 Electra

Electra is an ICS dataset, which has been generated from the network traffic of an electric traction substation running in normal and under attack ways. The Electra dataset has been created in a realistic scenario with industrial devices such as Programmable-Logic Controllers (PLCs) and a SCADA system that are controlled by well-known industrial protocols such as S7Comm and MODBUS [?]. The Electra dataset models the behavior of an electric traction substation used in a real high-speed railway area. The main purpose of this testbed is to allow converting the electric power of the general network to voltage, current, and frequency conditions to supply railways or trams. This system can be used to convert the three-phase alternating current into single phase with the lower frequency needed for railway electrification systems. To accomplish its task, the electric traction substation has 5 PLCs (1 master PLC and 4 slave PLCs) and a SCADA system. Additionally, the testbed has a switch (D5) for the interconnection of the different devices and a firewall (D4) to protect the substation from attacks coming from outside. The testbed devices communicate through control protocols following a master-slave architecture, where the master initiates the communication requesting some data and a slave response with information requested. The network communication is carried out through the following protocols: MODBUS TCP, OPC and S7Comm. The SCADA system consists of a Nanobox (A1) and an HMI (A4) that communicates through the OPC protocol. The SCADA acts as a master of both MODBUS slaves A2 and A3. Similarly, regarding the S7Comm protocol, D1 PLC acts as the master of A1, D2 and D3 PLCs. The data contains features regarding the network packets received on the testbed devices.

3 Datasets Comparison

Below is a comparison table between the abovementioned ICS datasets. The purpose of the table is to be a decision support tool in selecting a suitable dataset for conducting anomalies detection studies in the ICS field. Note that only BATADAL dataset does not cointain the class labels for the test set.

4 Summary

Today, ICS are an integral part of the day-to-day operations of many industries and critical infrastructures, from power generation, through water treatment, and to oil and gas processing. Cyber attacks against ICS would lead to disruption to controlling those critical infrastructures and result in harmful physical damage to plants, environment and humans. According to ICS-CERT, the ICS-targeted attacks are continuously increasing from year to year [**?**].

One Promising ICS security solution is an anomaly detection system, which monitors the network traffic and field devices' data logs, and utilize this information in order to warn of a possible intrusions. Although anomaly detection is the basis of many security systems developed in recent years, only a few of them are specifically designed to secure ICS systems. Therefore, there is an urgent need of effective ICS specific anomaly detection systems.

In light of this, there is a significant need to create datasets relevant to ICS and from various fields, that will be used to train and test those systems. In this work, we presented a survey of open and available ICS datasets from various domains, which can be used to implement anomaly detection algorithms in ICS-related studies.

We provided the needed background to use 12 significant datasets, and a demonstration of how to implement machine learning algorithms to the main one. Finally, we summarized the topic with a table of comparison between those datasets, which we hope will serve as a decision support tool in selecting a suitable dataset for conducting anomalies detection studies in the ICS field.