Industrial Power Control System Cyber Attacks Detection

February 25, 2023

Author:
Moriya Bitton
Victor Kushnir

1 Abstract

In both industry and society, industrial control systems (ICSs) are widely used. Failures of these systems can have severe economic and human consequences. Thus, they have become attractive targets for attacks, both physical and cyber.

As a result, power operators are heavily relied upon to determine the cause of disturbances and how to resolve them. As cyberattacks target power systems, human judgment is less reliable, since they are disguised overtly and operators are deceived as to what the attack really is.

Using machine learning, we investigate the viability of detecting cyberattacks involving deception in order to enable humans to make informed decisions.

Our goal is to develop an ML model for detecting industrial power control cyberattacks.

2 Introduction

The industrial control system (ICS), also known as the supervisory control and data acquisition (SCADA) system, combines distributed computing with physical process monitoring and control. Besides providing feedback from the real world (sensors), they also influence it (actuators).

Computers and controller networks process feedback data and send commands to actuators. There are many ICSs that are safety-critical, and disrupting their functionality can have serious financial and environmental consequences, as well as putting people's lives at risk. Cyberattacks, in particular, are highly appealing targets for ICSs because of their importance. Several high-impact incidents have occurred recently, including the attack on Ukraine's power grid, the Stuxnet malware used to target Iranian nuclear centrifuges, and an attack on Saudi Arabia's oil company. More recently, ICSs have deployed a common information technology stack and remote connectivity instead of running proprietary hardware and software. Due to this trend, ICSs are increasingly exposed to cyber threats that exploit common vulnerabilities in technology stacks. Additionally, ICS defenders' toolboxes are limited by legacy protocols without modern security features and underpowered endpoints. To address this problem, network-based intrusion detection systems (IDS) can be used to identify malicious activity without relying on endpoint computing resources. However, the rare number of known attacks on ICSs renders this approach ineffective.

2.1 Synchrophasor-based Smart Grid

The smart grid consists of two layers, cyber and physical systems. The two layers are coupled with each other and form the cyber-physical environment. The Synchrophasor or Phasor Measurement Unit (PMU) technology is built upon the cyber layer and provides real-time data to the energy management system (EMS) for the purpose of controlling the physical system. Such processes are presented as a sequence of execution events in the cyber-physical environment. The synchrophasor data includes not only the measurements such as voltage and current phasors but also the status of system devices including relays, breakers, switches, and transformers. The extremely low latency offered by time-synchronized data provides a huge volume of data with extra information and enables various real-time power system control algorithms in order to increase smart grid reliability and stability. The deployment of synchrophasor technology accelerates the use of communication networks within utilities and between neighboring utilities. The latest synchrophasor devices are vulnerable to cyber-attacks. there are still large numbers of legacy devices in service with little or no protection against the attacks.

Contemporary attacks against a power system can be launched from a compromised personal computer (PC) through a network to control a breaker. For example, the Aurora event highlights the potential for an attacker to open and close a breaker at high speed from a remote connection to damage an electric generator. Vulnerabilities can also be exploited against Intelligent Electronic Devices (IED) by uploading malicious settings. The Stuxnet worm is an example of settings changes on a control device causing a physical system to malfunction. Moreover, most network protocols used in power systems are open standard protocols without any security features. Such protocols include IEEE C37.118 protocol, used for synchrophasor data streaming, MODBUS, used to remotely monitor and control IED, and DNP3, which is also used to remotely monitor and control IED. The penetration tests conducted before have shown that cyber-attacks targeted against substation computers and devices can lead to Denial of Service (DoS) by making communication with a device impossible or causing devices to crash or reset and therefore prevent real-time monitoring and controlling of the power system.

2.2 Wide Area Monitoring Systems

Originally, intrusion detection systems were introduced to IT systems to detect activities that violate security policies. Intrusion detection systems (IDS) can be misuse-based or anomaly-based. Misuse and signature-based IDS identify well-defined patterns of known attacks and ignore undefined attacks. An anomaly-based IDS must consider a system's normal behavior in order to detect anomalies. Therefore, any deviation from normal behavior will be considered an intrusion.

2.3 Specification-based Intrusion Detection System

A probabilistic network can provide a clear semantic structure for extracting knowledge relevant to a particular domain. As they are capable of showing dependencies and interdependencies between variables, they can be used for diagnosis, learning, explanation, and a variety of other inference-related tasks. Bayesian networks are widespread among probabilistic networks because they provide explicit graphical representations of cause-and-effect reasoning. It can also represent causality, depending on how it is interpreted. Bayesian networks can be used for developing attack graphs that are used for assessing network vulnerability. An attack graph represents the causal relation between two nodes where the compromise of one will lead to the compromise of the other.

3 ICS Power Systems

Figure 5 shows the power system framework configuration used in generating these scenarios. In the network diagram, we have several components. Firstly, G1 and G2 are power generators. R1 through R4 are Intelligent Electronic Devices (IEDs) that can switch the breakers on or off. These breakers are labeled BR1 through BR4. We also have two lines. Line One spans from breaker one (BR1) to breaker two (BR2) and Line Two spans from breaker three (BR3) to breaker four (BR4). Each IED controls a single breaker. BR1 is controlled by R1, BR2 is controlled by R2, and so on. The IEDs use a distance protection scheme that trips the breaker on detected faults whether actually valid or faked since they have no internal validation to detect the difference. Operators can also manually issue commands to the IEDs

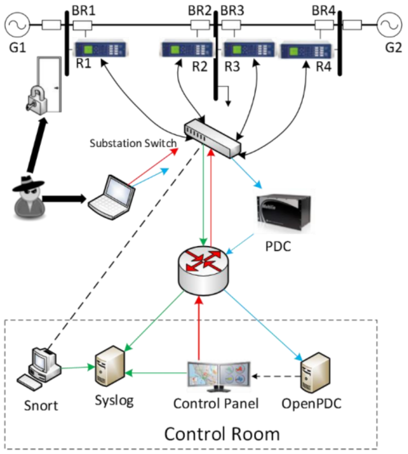


Figure 1: Power system framework configuration used in generating these scenarios

R1 through R4 to manually trip the breakers BR1 through BR4. Manual override is used when performing maintenance on the lines or other system components.

4 Types of Scenarios

1. Short-circuit fault – this is a short in a power line and can occur in various locations along the line, the location is indicated by the percentage range.

2. Line maintenance –one or more relays are disabled on a specific line to do maintenance for that line.

3. Remote tripping command injection (Attack) – this is an attack that sends a command to a relay which causes a breaker to open. It can only be done once an attacker has penetrated outside defenses.

4. Relay setting change (Attack) – relays are configured with a distance protection scheme and the attacker changes the setting to disable the relay function such that the relay will not trip for a valid fault or a valid command.

5. Data Injection (Attack) – here we imitate a valid fault by changing values to parameters such as current, voltage, sequence components, etc. This attack aims to blind the operator and cause a blackout.

5 Related works

5.1 Power system datasets

As we learn more about the vulnerability of industrial control systems (ICSs) to cyberattacks, we will be able to define the need for better methods of detecting attacks.

Due to the use of various data sets by researchers, it is difficult to compare the effectiveness of different intrusion detection solutions for SCADA systems [4].

To solve this problem, the authors have created four freely available data sets that can be used to compare intrusion detection solutions:

1. Pan, S., Morris, T., Adhikari, U., Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems, IEEE Transactions on Smart Grid. doi: 10.1109/TSG.2015.2409775.

2. Pan, S., Morris, T., Adhikari, U., Classification of Disturbances and Cyber-attacks in Power Systems Using Heterogeneous Time-synchronized Data, IEEE Transactions on Industrial Informatics. doi: 10.1109/TII.2015.2420951.

3. Pan, S., Morris, T., Adhikari, U., A Specification-based Intrusion Detection Framework for Cyber-physical Environment in Electric Power System, International Journal of Network Security (IJNS), Vol.17, No.2, PP.174-188, March 2015.

4. Beaver, J., Borges, R., Buckner, M., Morris, T., Adhikari, U., Pan, S., Machine Learning for Power System Disturbance and Cyber-attack Discrimination, Proceedings of the 7th International Symposium on Resilient Control Systems, August 19-21,2014, Denver, CO, USA.

5.2 Possible solutions

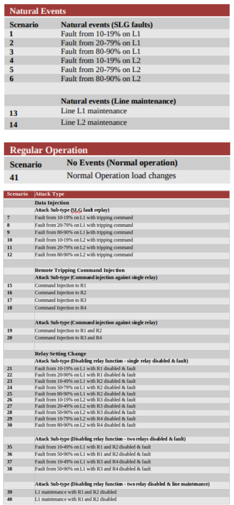
One possible solution uses neural networks based on 1D convolutions and autoencoders to detect attacks while being lightweight and generalizable [5].

In addition, Support Vector Machines (SVM) can be used to detect cyber-attacks based on the predicted attack rate [3].

Another possibility is to use neural networks that are capable of detecting attacks. Using this method, we demonstrate how effective principal component analysis can be at detecting adversarial attacks [1].

As ICS cyber security risks become more complex, decision science and data from established safety processes can assist with assessing them [2]. ICS needs better attack detection methods than the challenge itself.

6 Data exploration



Natural Events	
Scenario	**Natural events (SLG faults)**
1	Fault from 10-19% on L1
2	Fault from 20-79% on L1
3	Fault from 80-90% on L1
4	Fault from 10-19% on L2
5	Fault from 20-79% on L2
6	Fault from 80-90% on L2
	Natural events (Line maintenance)
13	Line L1 maintenance
14	Line L2 maintenance

Regular Operation	
Scenario	**No Events (Normal operation)**
41	Normal Operation load changes

Scenario	Attack Type
	Data Injection
	Attack Sub-type (SLG fault replay)
7	Fault from 10-19% on L1 with tripping command
8	Fault from 20-79% on L1 with tripping command
9	Fault from 80-90% on L1 with tripping command
10	Fault from 10-19% on L2 with tripping command
11	Fault from 20-79% on L2 with tripping command
12	Fault from 80-90% on L2 with tripping command
	Remote Tripping Command Injection
	Attack Sub-type (Command injection against single relay)
15	Command Injection to R1
16	Command Injection to R2
17	Command Injection to R3
18	Command Injection to R4
	Attack Sub-type (Command injection against single relay)
19	Command Injection to R1 and R2
20	Command Injection to R3 and R4
	Relay Setting Change
	Attack Sub-type (Disabling relay function - single relay disabled & fault)
21	Fault from 10-19% on L1 with R1 disabled & fault
22	Fault from 20-90% on L1 with R1 disabled & fault
23	Fault from 10-49% on L1 with R2 disabled & fault
24	Fault from 50-79% on L1 with R2 disabled & fault
25	Fault from 80-90% on L1 with R2 disabled & fault
26	Fault from 10-19% on L2 with R3 disabled & fault
27	Fault from 20-49% on L2 with R3 disabled & fault
28	Fault from 50-90% on L2 with R3 disabled & fault
29	Fault from 10-79% on L2 with R4 disabled & fault
30	Fault from 80-90% on L2 with R4 disabled & fault
	Attack Sub-type (Disabling relay function - two relays disabled & fault)
35	Fault from 10-49% on L1 with R1 and R2 disabled & fault
36	Fault from 50-90% on L1 with R1 and R2 disabled & fault
37	Fault from 10-49% on L1 with R3 and R4 disabled & fault
38	Fault from 50-90% on L1 with R3 and R4 disabled & fault
	Attack Sub-type (Disabling relay function - two relay disabled & line maintenance)
39	L1 maintenance with R1 and R2 disabled
40	L1 maintenance with R1 and R2 disabled

Figure 2: Multi-class

The Power System Attack Datasets were created by Mississippi State University and Oak Ridge National Laboratory in April 2014. The dataset contains information on 37 different power system event scenarios, which were randomly sampled at 1% and grouped into binary, three-class, and multi-class datasets. The scenarios are categorized into Natural Events, No Events, and Attack Events.

The dataset includes a power system framework configuration consisting of power generators (G1 and G2), Intelligent Electronic Devices (IEDs) that can switch breakers on or off (R1 through R4), breakers (BR1 through BR4), and two lines (Line One and Line Two). Each IED automatically controls one breaker, and the IEDs use a distance protection scheme that trips the breaker on detected faults whether actually valid or faked since they have no internal validation to detect the difference.

There are five types of scenarios:

1. Short-circuit fault: A short in a power line, which can occur in various locations along the line.

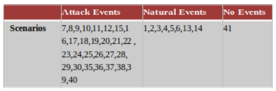
2. Line maintenance: One or more relays are disabled on a specific line to do maintenance for that line.

3. Remote tripping command injection (Attack): An attack that sends a command to a relay that causes a breaker to open.

4. Relay setting change (Attack): Relays are configured with a distance protection scheme, and the attacker changes the setting to disable the relay function such that the relay will not trip for a valid fault or a valid command.

5. Data Injection (Attack): We imitate a valid fault by changing values to parameters such as current, voltage, sequence components, etc. This attack aims to blind the operator and causes a blackout.

The dataset includes 128 features. There are 29 types of measurements from each phasor measurement unit (PMU), and in this system, there are 4 PMUs that measure 29 features for 116 PMU measurement columns in total.

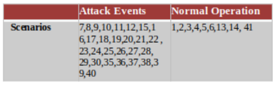


	Attack Events	Natural Events	No Events
Scenarios	7,8,9,10,11,12,15,16,17,18,19,20,21,22 , 23,24,25,26,27,28, 29,30,35,36,37,38,39,40	1,2,3,4,5,6,13,14	41

Figure 3: Three-class

6.1 PMU

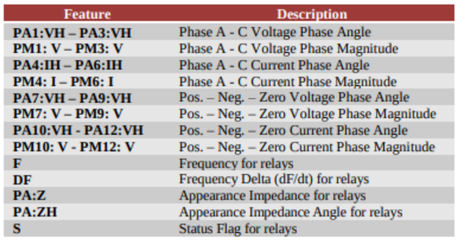
The 128 features are explained in the table below.
There are 29 types of measurements from each phasor measurement unit (PMU). A phasor measurement unit (PMU) or synchrophasor is a device that measures the electrical waves on an electricity grid, using a common time source for synchronization. In our system, there are 4 PMUs that measure 29 features for 116 PMU measurement columns total. The index of each column is in the form of "R#-Signal Reference" that indicates a type of measurement from a PMU specified by "R#". The signal references and corresponding descriptions are listed below. For example, R1-PA1:VH means Phase A voltage phase angle measured by PMU R1. After the PMU measurement columns, there are 12 columns for control panel logs, Snort alerts, and relay logs of the 4 PMU/relay (relay and PMU are integrated together). The last column is the marker. The first three digits on the right are the load condition (in Megawatts). Another three digits to their left are fault locations, for example, "085" means fault at 85% of the transmission line specified by the scenario description. However, for those that do not involve fault, e.g. "line maintenance", these digits will be set to 000. The most left one digit or two digits indicate(s) the scenario number.



	Attack Events	Normal Operation
Scenarios	7,8,9,10,11,12,15,16,17,18,19,20,21,22 , 23,24,25,26,27,28, 29,30,35,36,37,38,39,40	1,2,3,4,5,6,13,14, 41

Figure 4: Binary classification

6.2 Data analysis



Feature	Description
PA1:VH – PA3:VH	Phase A - C Voltage Phase Angle
PM1: V – PM3: V	Phase A - C Voltage Phase Magnitude
PA4:IH – PA6:IH	Phase A - C Current Phase Angle
PM4: I – PM6: I	Phase A - C Current Phase Magnitude
PA7:VH – PA9:VH	Pos. – Neg. – Zero Voltage Phase Angle
PM7: V – PM9: V	Pos. – Neg. – Zero Voltage Phase Magnitude
PA10:VH - PA12:VH	Pos. – Neg. – Zero Current Phase Angle
PM10: V - PM12: V	Pos. – Neg. – Zero Current Phase Magnitude
F	Frequency for relays
DF	Frequency Delta (dF/dt) for relays
PA:Z	Appearance Impedance for relays
PA:ZH	Appearance Impedance Angle for relays
S	Status Flag for relays

Figure 5: Power system framework configuration used in generating these scenarios

Finding critical features is a critical step in preprocessing data for machine learning models, [Figure 5]. Identifying the relevant features in a dataset can help to reduce dimensionality and remove irrelevant information, improving the accuracy and efficiency of the models. It can also help in identifying the most significant factors that contribute to the outcome being predicted, providing valuable insights into the problem being addressed. Furthermore, by reducing the number of features in the dataset, finding significant features can contribute to reducing overfitting and improving the generalizability of the models. Thus, finding critical features can be an essential step in building effective and accurate machine-learning models.

Figure 5 visualize the data after PCA.

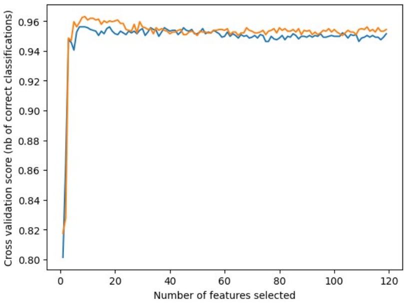


Figure 6: Finding critical features is a critical step in preprocessing data for machine learning models

7 Summary

In terms of data analysis and machine learning, we see a series of steps.

As a first step, feature engineering involves determining apparent impedance, voltage and current phases, and phase magnitudes. Next, remove infinities and nulls. In the third step, we will preprocess the dataset using various techniques, such as label encoding and scaling. In the fourth step, we select features using Recursive Feature Elimination with Cross Validation (RFECV) and Random Forest Classifiers. The last step involves training several models, including

Random Forest Classifier, Random Forest Classifier with AdaBoost, K Nearest Neighbors, and Stacking Classifier.

The steps are all part of a data analysis and machine learning process to gain insight and predict the future.

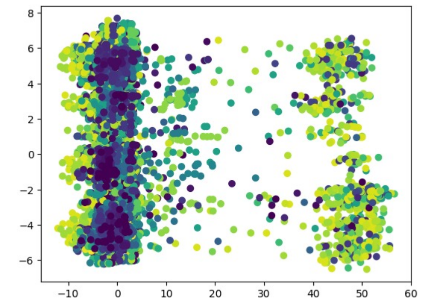


Figure 7: PCA

8 Conclusion

This project focuses on analyzing and processing data to develop machine learning models to identify cyberattacks on industrial control systems (ICSs).

Previous experience described specific methods for identifying attacks, including neural networks based on 1D convolutions and autoencoders, support vector machines, and principal component analysis. By analyzing different aspects, including predicted attack rates, adversarial attacks, and lightweight and generalizable characteristics, these methods attempt to detect cyberattacks. Additionally, decision science and established safety processes can be used to assess cybersecurity threats' risks. These changes demonstrate a more targeted approach to detecting cyber-attacks in ICS, focusing on specific machine-learning techniques and data analysis methods.

The complexity of cybersecurity risks in ICS highlights the need for better attack detection methods.

References

[1] Abdulrahman Al-Abassi, Hadis Karimipour, Ali Dehghantanha, and Reza M Parizi. An ensemble deep learning-based cyber-attack detection in industrial control system. *IEEE Access*, 8:83965–83973, 2020.

[2] Allan Cook, Richard Smith, Leandros Maglaras, and Helge Janicke. Measuring the risk of cyber attack in industrial control systems. BCS eWiC, 2016.

[3] Moshe Kravchik and Asaf Shabtai. Efficient cyber attack detection in industrial control systems using lightweight neural networks and pca. *IEEE Transactions on Dependable and Secure Computing*, 19(4):2179–2197, 2021.

[4] Thomas Morris and Wei Gao. Industrial control system traffic data sets for intrusion detection research. In *Critical Infrastructure Protection VIII: 8th IFIP WG 11.10 International Conference, ICCIP 2014, Arlington, VA,*

USA, March 17-19, 2014, Revised Selected Papers 8, pages 65–78. Springer, 2014.

[5] Asuka Terai, Shingo Abe, Shoya Kojima, Yuta Takano, and Ichiro Koshijima. Cyber-attack detection for industrial control system monitoring with support vector machine based on communication profile. In *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 132–138. IEEE, 2017.