

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.

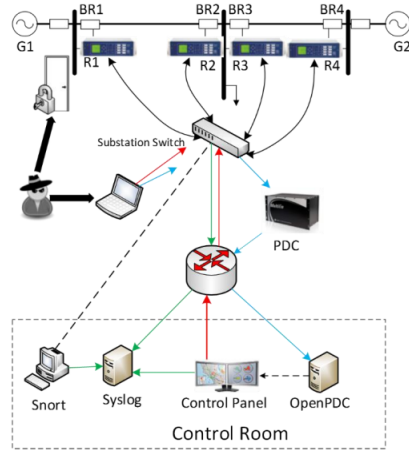


Figure 1: Power system framework configuration used in generating these scenarios

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

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 Cyberattacks 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 10-15% on L1
2	Fault from 20-70% on L1
3	Fault from 80-90% on L1
4	Fault from 10-15% on L2
5	Fault from 20-70% 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
Attack Events	
Scenario	Attack Events
7	Attack: Sub-type 0 (L1 fault type)
8	Fault from 10-15% on L1 with tripping command
9	Fault from 20-70% on L1 with tripping command
10	Fault from 80-90% on L1 with tripping command
11	Fault from 10-15% on L2 with tripping command
12	Fault from 20-70% on L2 with tripping command
13	Fault from 80-90% on L2 with tripping command
14	Attack: Sub-type 1 (L1 fault type)
15	Attack: Sub-type 2 (L2 fault type)
16	Attack: Sub-type 3 (L3 fault type)
17	Attack: Sub-type 4 (L4 fault type)
18	Attack: Sub-type 5 (L5 fault type)
19	Attack: Sub-type 6 (L6 fault type)
20	Attack: Sub-type 7 (L7 fault type)
21	Attack: Sub-type 8 (L8 fault type)
22	Attack: Sub-type 9 (L9 fault type)
23	Attack: Sub-type 10 (L10 fault type)
24	Attack: Sub-type 11 (L11 fault type)
25	Attack: Sub-type 12 (L12 fault type)
26	Attack: Sub-type 13 (L13 fault type)
27	Attack: Sub-type 14 (L14 fault type)
28	Attack: Sub-type 15 (L15 fault type)
29	Attack: Sub-type 16 (L16 fault type)
30	Attack: Sub-type 17 (L17 fault type)
31	Attack: Sub-type 18 (L18 fault type)
32	Attack: Sub-type 19 (L19 fault type)
33	Attack: Sub-type 20 (L20 fault type)
34	Attack: Sub-type 21 (L21 fault type)
35	Attack: Sub-type 22 (L22 fault type)
36	Attack: Sub-type 23 (L23 fault type)
37	Attack: Sub-type 24 (L24 fault type)
38	Attack: Sub-type 25 (L25 fault type)
39	Attack: Sub-type 26 (L26 fault type)
40	Attack: Sub-type 27 (L27 fault type)
41	Attack: Sub-type 28 (L28 fault type)
42	Attack: Sub-type 29 (L29 fault type)
43	Attack: Sub-type 30 (L30 fault type)
44	Attack: Sub-type 31 (L31 fault type)
45	Attack: Sub-type 32 (L32 fault type)
46	Attack: Sub-type 33 (L33 fault type)
47	Attack: Sub-type 34 (L34 fault type)
48	Attack: Sub-type 35 (L35 fault type)
49	Attack: Sub-type 36 (L36 fault type)
50	Attack: Sub-type 37 (L37 fault type)
51	Attack: Sub-type 38 (L38 fault type)
52	Attack: Sub-type 39 (L39 fault type)
53	Attack: Sub-type 40 (L40 fault type)
54	Attack: Sub-type 41 (L41 fault type)
55	Attack: Sub-type 42 (L42 fault type)
56	Attack: Sub-type 43 (L43 fault type)
57	Attack: Sub-type 44 (L44 fault type)
58	Attack: Sub-type 45 (L45 fault type)
59	Attack: Sub-type 46 (L46 fault type)
60	Attack: Sub-type 47 (L47 fault type)
61	Attack: Sub-type 48 (L48 fault type)
62	Attack: Sub-type 49 (L49 fault type)
63	Attack: Sub-type 50 (L50 fault type)
64	Attack: Sub-type 51 (L51 fault type)
65	Attack: Sub-type 52 (L52 fault type)
66	Attack: Sub-type 53 (L53 fault type)
67	Attack: Sub-type 54 (L54 fault type)
68	Attack: Sub-type 55 (L55 fault type)
69	Attack: Sub-type 56 (L56 fault type)
70	Attack: Sub-type 57 (L57 fault type)
71	Attack: Sub-type 58 (L58 fault type)
72	Attack: Sub-type 59 (L59 fault type)
73	Attack: Sub-type 60 (L60 fault type)
74	Attack: Sub-type 61 (L61 fault type)
75	Attack: Sub-type 62 (L62 fault type)
76	Attack: Sub-type 63 (L63 fault type)
77	Attack: Sub-type 64 (L64 fault type)
78	Attack: Sub-type 65 (L65 fault type)
79	Attack: Sub-type 66 (L66 fault type)
80	Attack: Sub-type 67 (L67 fault type)
81	Attack: Sub-type 68 (L68 fault type)
82	Attack: Sub-type 69 (L69 fault type)
83	Attack: Sub-type 70 (L70 fault type)
84	Attack: Sub-type 71 (L71 fault type)
85	Attack: Sub-type 72 (L72 fault type)
86	Attack: Sub-type 73 (L73 fault type)
87	Attack: Sub-type 74 (L74 fault type)
88	Attack: Sub-type 75 (L75 fault type)
89	Attack: Sub-type 76 (L76 fault type)
90	Attack: Sub-type 77 (L77 fault type)
91	Attack: Sub-type 78 (L78 fault type)
92	Attack: Sub-type 79 (L79 fault type)
93	Attack: Sub-type 80 (L80 fault type)
94	Attack: Sub-type 81 (L81 fault type)
95	Attack: Sub-type 82 (L82 fault type)
96	Attack: Sub-type 83 (L83 fault type)
97	Attack: Sub-type 84 (L84 fault type)
98	Attack: Sub-type 85 (L85 fault type)
99	Attack: Sub-type 86 (L86 fault type)
100	Attack: Sub-type 87 (L87 fault type)
101	Attack: Sub-type 88 (L88 fault type)
102	Attack: Sub-type 89 (L89 fault type)
103	Attack: Sub-type 90 (L90 fault type)
104	Attack: Sub-type 91 (L91 fault type)
105	Attack: Sub-type 92 (L92 fault type)
106	Attack: Sub-type 93 (L93 fault type)
107	Attack: Sub-type 94 (L94 fault type)
108	Attack: Sub-type 95 (L95 fault type)
109	Attack: Sub-type 96 (L96 fault type)
110	Attack: Sub-type 97 (L97 fault type)
111	Attack: Sub-type 98 (L98 fault type)
112	Attack: Sub-type 99 (L99 fault type)
113	Attack: Sub-type 100 (L100 fault type)
114	Attack: Sub-type 101 (L101 fault type)
115	Attack: Sub-type 102 (L102 fault type)
116	Attack: Sub-type 103 (L103 fault type)
117	Attack: Sub-type 104 (L104 fault type)
118	Attack: Sub-type 105 (L105 fault type)
119	Attack: Sub-type 106 (L106 fault type)
120	Attack: Sub-type 107 (L107 fault type)
121	Attack: Sub-type 108 (L108 fault type)
122	Attack: Sub-type 109 (L109 fault type)
123	Attack: Sub-type 110 (L110 fault type)
124	Attack: Sub-type 111 (L111 fault type)
125	Attack: Sub-type 112 (L112 fault type)
126	Attack: Sub-type 113 (L113 fault type)
127	Attack: Sub-type 114 (L114 fault type)
128	Attack: Sub-type 115 (L115 fault type)
129	Attack: Sub-type 116 (L116 fault type)
130	Attack: Sub-type 117 (L117 fault type)
131	Attack: Sub-type 118 (L118 fault type)
132	Attack: Sub-type 119 (L119 fault type)
133	Attack: Sub-type 120 (L120 fault type)
134	Attack: Sub-type 121 (L121 fault type)
135	Attack: Sub-type 122 (L122 fault type)
136	Attack: Sub-type 123 (L123 fault type)
137	Attack: Sub-type 124 (L124 fault type)
138	Attack: Sub-type 125 (L125 fault type)
139	Attack: Sub-type 126 (L126 fault type)
140	Attack: Sub-type 127 (L127 fault type)
141	Attack: Sub-type 128 (L128 fault type)
142	Attack: Sub-type 129 (L129 fault type)
143	Attack: Sub-type 130 (L130 fault type)
144	Attack: Sub-type 131 (L131 fault type)
145	Attack: Sub-type 132 (L132 fault type)
146	Attack: Sub-type 133 (L133 fault type)
147	Attack: Sub-type 134 (L134 fault type)
148	Attack: Sub-type 135 (L135 fault type)
149	Attack: Sub-type 136 (L136 fault type)
150	Attack: Sub-type 137 (L137 fault type)
151	Attack: Sub-type 138 (L138 fault type)
152	Attack: Sub-type 139 (L139 fault type)
153	Attack: Sub-type 140 (L140 fault type)
154	Attack: Sub-type 141 (L141 fault type)
155	Attack: Sub-type 142 (L142 fault type)
156	Attack: Sub-type 143 (L143 fault type)
157	Attack: Sub-type 144 (L144 fault type)
158	Attack: Sub-type 145 (L145 fault type)
159	Attack: Sub-type 146 (L146 fault type)
160	Attack: Sub-type 147 (L147 fault type)
161	Attack: Sub-type 148 (L148 fault type)
162	Attack: Sub-type 149 (L149 fault type)
163	Attack: Sub-type 150 (L150 fault type)
164	Attack: Sub-type 151 (L151 fault type)
165	Attack: Sub-type 152 (L152 fault type)
166	Attack: Sub-type 153 (L153 fault type)
167	Attack: Sub-type 154 (L154 fault type)
168	Attack: Sub-type 155 (L155 fault type)
169	Attack: Sub-type 156 (L156 fault type)
170	Attack: Sub-type 157 (L157 fault type)
171	Attack: Sub-type 158 (L158 fault type)
172	Attack: Sub-type 159 (L159 fault type)
173	Attack: Sub-type 160 (L160 fault type)
174	Attack: Sub-type 161 (L161 fault type)
175	Attack: Sub-type 162 (L162 fault type)
176	Attack: Sub-type 163 (L163 fault type)
177	Attack: Sub-type 164 (L164 fault type)
178	Attack: Sub-type 165 (L165 fault type)
179	Attack: Sub-type 166 (L166 fault type)
180	Attack: Sub-type 167 (L167 fault type)
181	Attack: Sub-type 168 (L168 fault type)
182	Attack: Sub-type 169 (L169 fault type)
183	Attack: Sub-type 170 (L170 fault type)
184	Attack: Sub-type 171 (L171 fault type)
185	Attack: Sub-type 172 (L172 fault type)
186	Attack: Sub-type 173 (L173 fault type)
187	Attack: Sub-type 174 (L174 fault type)
188	Attack: Sub-type 175 (L175 fault type)
189	Attack: Sub-type 176 (L176 fault type)
190	Attack: Sub-type 177 (L177 fault type)
191	Attack: Sub-type 178 (L178 fault type)
192	Attack: Sub-type 179 (L179 fault type)
193	Attack: Sub-type 180 (L180 fault type)
194	Attack: Sub-type 181 (L181 fault type)
195	Attack: Sub-type 182 (L182 fault type)
196	Attack: Sub-type 183 (L183 fault type)
197	Attack: Sub-type 184 (L184 fault type)
198	Attack: Sub-type 185 (L185 fault type)
199	Attack: Sub-type 186 (L186 fault type)
200	Attack: Sub-type 187 (L187 fault type)
201	Attack: Sub-type 188 (L188 fault type)
202	Attack: Sub-type 189 (L189 fault type)
203	Attack: Sub-type 190 (L190 fault type)
204	Attack: Sub-type 191 (L191 fault type)
205	Attack: Sub-type 192 (L192 fault type)
206	Attack: Sub-type 193 (L193 fault type)
207	Attack: Sub-type 194 (L194 fault type)
208	Attack: Sub-type 195 (L195 fault type)
209	Attack: Sub-type 196 (L196 fault type)
210	Attack: Sub-type 197 (L197 fault type)
211	Attack: Sub-type 198 (L198 fault type)
212	Attack: Sub-type 199 (L199 fault type)
213	Attack: Sub-type 200 (L200 fault type)
214	Attack: Sub-type 201 (L201 fault type)
215	Attack: Sub-type 202 (L202 fault type)
216	Attack: Sub-type 203 (L203 fault type)
217	Attack: Sub-type 204 (L204 fault type)
218	Attack: Sub-type 205 (L205 fault type)
219	Attack: Sub-type 206 (L206 fault type)
220	Attack: Sub-type 207 (L207 fault type)
221	Attack: Sub-type 208 (L208 fault type)
222	Attack: Sub-type 209 (L209 fault type)
223	Attack: Sub-type 210 (L210 fault type)
224	Attack: Sub-type 211 (L211 fault type)
225	Attack: Sub-type 212 (L212 fault type)
226	Attack: Sub-type 213 (L213 fault type)
227	Attack: Sub-type 214 (L214 fault type)
228	Attack: Sub-type 215 (L215 fault type)
229	Attack: Sub-type 216 (L216 fault type)
230	Attack: Sub-type 217 (L217 fault type)
231	Attack: Sub-type 218 (L218 fault type)
232	Attack: Sub-type 219 (L219 fault type)
233	Attack: Sub-type 220 (L220 fault type)
234	Attack: Sub-type 221 (L221 fault type)
235	Attack: Sub-type 222 (L222 fault type)
236	Attack: Sub-type 223 (L223 fault type)
237	Attack: Sub-type 224 (L224 fault type)
238	Attack: Sub-type 225 (L225 fault type)
239	Attack: Sub-type 226 (L226 fault type)
240	Attack: Sub-type 227 (L227 fault type)
241	Attack: Sub-type 228 (L228 fault type)
242	Attack: Sub-type 229 (L229 fault type)
243	Attack: Sub-type 230 (L230 fault type)
244	Attack: Sub-type 231 (L231 fault type)
245	Attack: Sub-type 232 (L232 fault type)
246	Attack: Sub-type 233 (L233 fault type)
247	Attack: Sub-type 234 (L234 fault type)
248	Attack: Sub-type 235 (L235 fault type)
249	Attack: Sub-type 236 (L236 fault type)
250	Attack: Sub-type 237 (L237 fault type)
251	Attack: Sub-type 238 (L238 fault type)
252	Attack: Sub-type 239 (L239 fault type)
253	Attack: Sub-type 240 (L240 fault type)
254	Attack: Sub-type 241 (L241 fault type)
255	Attack: Sub-type 242 (L242 fault type)
256	Attack: Sub-type 243 (L243 fault type)
257	Attack: Sub-type 244 (L244 fault type)
258	Attack: Sub-type 245 (L245 fault type)
259	Attack: Sub-type 246 (L246 fault type)
260	Attack: Sub-type 247 (L247 fault type)
261	Attack: Sub-type 248 (L248 fault type)
262	Attack: Sub-type 249 (L249 fault type)
263	Attack: Sub-type 250 (L250 fault type)
264	Attack: Sub-type 251 (L251 fault type)
265	Attack: Sub-type 252 (L252 fault type)
266	Attack: Sub-type 253 (L253 fault type)
267	Attack: Sub-type 254 (L254 fault type)
268	Attack: Sub-type 255 (L255 fault type)
269	Attack: Sub-type 256 (L256 fault type)
270	Attack: Sub-type 257 (L257 fault type)
271	Attack: Sub-type 258 (L258 fault type)
272	Attack: Sub-type 259 (L259 fault type)
273	Attack: Sub-type 260 (L260 fault type)
274	Attack: Sub-type 261 (L261 fault type)
275	Attack: Sub-type 262 (L262 fault type)
276	Attack: Sub-type 263 (L263 fault type)
277	Attack: Sub-type 264 (L264 fault type)
278	Attack: Sub-type 265 (L265 fault type)
279	Attack: Sub-type 266 (L266 fault type)
280	Attack: Sub-type 267 (L267 fault type)
281	Attack: Sub-type 268 (L268 fault type)
282	Attack: Sub-type 269 (L269 fault type)
283	Attack: Sub-type 270 (L270 fault type)
284	Attack: Sub-type 271 (L271 fault type)
285	Attack: Sub-type 272 (L272 fault type)
286	Attack: Sub-type 273 (L273 fault type)
287	Attack: Sub-type 274 (L274 fault type)
288	Attack: Sub-type 275 (L275 fault type)
289	Attack: Sub-type 276 (L276 fault type)
290	Attack: Sub-type 277 (L277 fault type)
291	Attack: Sub-type 278 (L278 fault type)
292	Attack: Sub-type 279 (L279 fault type)
293	Attack: Sub-type 280 (L280 fault type)
294	Attack: Sub-type 281 (L281 fault type)
295	Attack: Sub-type 282 (L282 fault type)
296	Attack: Sub-type 283 (L283 fault type)
297	Attack: Sub-type 284 (L284 fault type)
298	Attack: Sub-type 285 (L285 fault type)
299	Attack: Sub-type 286 (L286 fault type)
300	Attack: Sub-type 287 (L287 fault type)
301	Attack: Sub-type 288 (L288 fault type)
302	Attack: Sub-type 289 (L289 fault type)
303	Attack: Sub-type 290 (L290 fault type)
304	Attack: Sub-type 291 (L291 fault type)
305	Attack: Sub-type 292 (L292 fault type)
306	Attack: Sub-type 293 (L293 fault type)
307	Attack: Sub-type 294 (L294 fault type)
308	Attack: Sub-type 295 (L295 fault type)
309	Attack: Sub-type 296 (L296 fault type)
310	Attack: Sub-type 297 (L297 fault type)
311	Attack: Sub-type 298 (L298 fault type)
312	Attack: Sub-type 299 (L299 fault type)
313	Attack: Sub-type 300 (L300 fault type)
314	Attack: Sub-type 301 (L301 fault type)
315	Attack: Sub-type 302 (L302 fault type)
316	Attack: Sub-type 303 (L303 fault type)
317	Attack: Sub-type 304 (L304 fault type)
318	Attack: Sub-type 305 (L305 fault type)
319	Attack: Sub-type 306 (L306 fault type)
320	Attack: Sub-type 307 (L307 fault type)
321	Attack: Sub-type 308 (L308 fault type)
322	Attack: Sub-type 309 (L309 fault type)
323	Attack: Sub-type 310 (L310 fault type)
324	Attack: Sub-type 311 (L311 fault type)
325	Attack: Sub-type 312 (L312 fault type)
326	Attack: Sub-type 313 (L313 fault type)
327	Attack: Sub-type 314 (L314 fault type)
328	Attack: Sub-type 315 (L315 fault type)
329	Attack: Sub-type 316 (L316 fault type)
330	Attack: Sub-type 317 (L317 fault type)
331	Attack: Sub-type 318 (L318 fault type)
332	Attack: Sub-type 319 (L319 fault type)
333	Attack: Sub-type 320 (L320 fault type)
334	Attack: Sub-type 321 (L321 fault type)
335	Attack: Sub-type 322 (L322 fault type)
336	Attack: Sub-type 323 (L323 fault type)
337	Attack: Sub-type 324 (L324 fault type)
338	Attack: Sub-type 325 (L325 fault type)
339	Attack: Sub-type 326 (L326 fault type)
340	Attack: Sub-type 327 (L327 fault type)
341	Attack: Sub-type 328 (L328 fault type)
342	Attack: Sub-type 329 (L329 fault type)
343	Attack: Sub-type 330 (L330 fault type)
344	Attack: Sub-type 331 (L331 fault type)
345	Attack: Sub-type 332 (L332 fault type)
346	Attack: Sub-type 333 (L333 fault type)
347	Attack: Sub-type 334 (L334 fault type)
348	Attack: Sub-type 335 (L335 fault type)
349	Attack: Sub-type 336 (L336 fault type)

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	7,8,9,10,11,12,15,1 6,17,18,19,20,21,22, 23,24,25,26,27,28, 29,30,35,36,37,38,3 9,40	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	7,8,9,10,11,12,15,1 6,17,18,19,20,21,22, 23,24,25,26,27,28, 29,30,35,36,37,38,3 9,49	1,2,3,4,5,6,13,14,41

Figure 4: Binary classification

6.2 Data analysis

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.

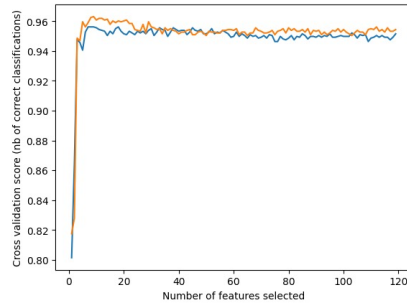


Figure 6: Finding critical features is a critical step in preprocessing data for machine learning models

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

Figure 5 visualize the data after PCA.

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.

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.

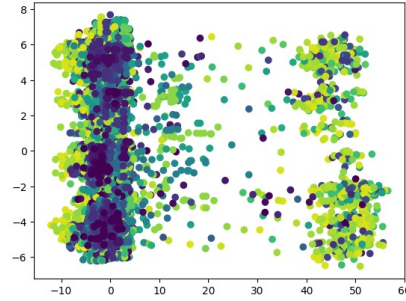


Figure 7: PCA

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.