IEC 60870-5-104

Intrusion Detection Dataset

Readme File

ITHACA – University of Western Macedonia - https://ithaca.ece.uowm.gr/

Authors: Panagiotis Radoglou-Grammatikis, Thomas Lagkas, Vasileios Argyriou, Panagiotis Sarigiannidis

Publication Date: September 23, 2022

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements No 101021936 (ELECTRON) and No 833955 (SDN-microSENSE).

1. Introduction

The evolution of the Industrial Internet of Things (IIoT) introduces several benefits, such as real-time monitoring, pervasive control and self-healing. However, despite the valuable services, security and privacy issues still remain given the presence of legacy and insecure communication protocols like IEC 60870-5-104. IEC 60870-5-104 is an industrial protocol widely applied in critical infrastructures, such as the smart electrical grid and industrial healthcare systems. The IEC 60870-5-104 Intrusion Detection Dataset was implemented in the context of the research paper entitled "Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach" [1], in the context of two H2020 projects: ELECTRON: rEsilient and seLf-healed EleCTRical pOwer Nanogrid (101021936) and SDN-microSENSE: SDN - microgrid reSilient Electrical eNergy SystEm (833955). This dataset includes labelled Transmission Control Protocol (TCP)/Internet Protocol (IP) network flow statistics (Common-Separated Values (CSV) format) and IEC 60870-5-104 flow statistics (CSV format) related to twelve IEC 60870-5-104 cyberattacks. In particular, the cyberattacks are related to unauthorised commands and Denial of Service (DoS) activities against IEC 60870-5-104. Moreover, the relevant Packet Capture (PCAP) files are available. The dataset can be utilised for Artificial Intelligence (AI)-based Intrusion Detection Systems (IDS), taking full advantage of Machine Learning (ML) and Deep Learning (DL).

2. Instructions

The IEC 60870-5-104 dataset was implemented following the methodology of A. Gharib et al. in [2], including eleven features: (a) Complete Network Configuration, (b) Complete Traffic, (c) Labelled Dataset, (d) Complete Interaction, (e) Complete Capture, (f) Available Protocols, (g) Attack Diversity, (h) Heterogeneity, (i) Feature Set and (j) Metadata.

A network topology consisting of (a) seven industrial entities, (b) one Human Machine Interfaces (HMI) and (c) three cyberattackers was used to construct the IEC 60870-5-104 Intrusion Detection Dataset. The industrial entities use `IEC TestServer`[1], while the HMI uses `Qtester104`[2]. On the other hand, the cyberattackers use `Kali Linux`[3] equipped with `Metasploit`[4], `OpenMUC j60870`[5] and `Ettercap`[6]. The cyberattacks were performed during the following days.

- On Saturday, April 25, 2020, a DoS cyberattack (`M_SP_NA_1_DoS`) was executed for 2 hours, using the `M_SP_NA_1` command.
- On Sunday, April 26, 2020, two cyberattacks were executed, namely (a) DoS (`C_CI_NA_1_DoS`) and (b) unauthorised injection (`C_CI_NA_1`), using the `C_CI_NA_1` command for 2 hours.
- On Monday, April 27, 2020, one unauthorised injection attack (`C_SE_NA_1`) was executed for 4 hours, using the `C_SE_NA_1` command.
- Tuesday, April 28, 2020 two cyberattacks were executed, namely (a) unauthorised injection (`C_SC_NA_1`) and (b) DoS (`C_SE_NA_1_DoS`), using the `C_SC_NA_1` and `C_SE_NA_1` commands for 2 hours and 4 hours, respectively.
- Wednesday, April 29, 2020, one DoS (`C_SC_NA_1`) cyberattack was performed for 2 hours, using the `C_SC_NA_1` command.
- Friday, June 05, 2020, two cyberattacks were executed, namely (a) DoS (`C_RD_NA_1_DoS`) and (b) unauthorised injection (`C_RD_NA_1`), using the `C_RD_NA_1` command for 2 and 4 hours, respectively.

[1] IEC TestServer - https://sourceforge.net/projects/iecserver/
[2] QTester104 - https://sourceforge.net/projects/qtester104/
[3] Kali Linux - https://www.kali.org/
[4] Metasploit - https://www.metasploit.com/
[5] OpenMUC j60870 - https://www.openmuc.org/iec-60870-5-104/
[6] Ettercap - https://www.ettercap-project.org/

- Saturday, June 06, 2020, two cyberattacks were executed, namely (a) DoS (`C_RP_NA_1_DoS`) and (b) unauthorised injection (`C_RP_NA_1`), using the `C_RP_NA_1` command for 2 and 4 hours, respectively.
- Monday, June 08, 2020, a `Man In The Middle (MITM)` cyberattack was executed for 2 hours, filtering and dropping the IEC 60870-5-104 packets.

For each attack, a 7zip file is provided, including the network traffic and the network flow statistics for each entity. Moreover, a relevant diagram is provided, illustrating the corresponding cyberattack. In particular, for each entity, a folder is given, including (a) the relevant pcap file, (b) Transmission Control Protocol (TCP) / Internet Protocol (IP) network flow statistics in a Common Separated Value (CSV) format and (c) IEC 60870-5-104 flow statistics in a CSV format. The TCP/IP network flow statistics were generated by `CICFlowMeter`[7], while the IEC 60870-5-104 flow statistics were generated based on a `Custom IEC 60870-5-104 Python Parser`[8], taking full advantage of `Scapy`[9].

[7] CICFlowMeter - https://github.com/ahlashkari/CICFlowMeter
[8] This parser is provided after a communication with the authors.
[9] Scapy - https://scapy.net/

3. Dataset Structure

The dataset consists of the following files:

- **20200425_UOWM_IEC104_Dataset_m_sp_na_1_DoS.7z**: A 7zip file including the pcap and CSV files related to the `M_SP_NA_1` attack.
- **20200426_UOWM_IEC104_Dataset_c_ci_na_1_DoS.7z**: A 7zip file including the pcap and CSV files related to the `C_CI_NA_1_DoS` attack.
- **20200426_UOWM_IEC104_Dataset_c_ci_na_1.7z**: A 7zip file including the pcap and CSV files related to `C_CI_NA_1` attack.
- **20200427_UOWM_IEC104_Dataset_c_se_na_1.7z**: A 7zip file including the pcap and CSV files related to the `C_SE_NA_1` attack.
- **20200428_UOWM_IEC104_Dataset_c_sc_na_1.7z**: A 7zip file including the pcap and CSV files related to the `C_SC_NA_1` attack.
- **20200428_UOWM_IEC104_Dataset_c_se_na_1_DoS.7z**: A 7zip file including the pcap and CSV files related to the `C_SE_NA_1_DoS` attack.
- **20200429_UOWM_IEC104_Dataset_c_sc_na_1_DoS.7z**: A 7zip file including the pcap and CSV files related to the `C_SC_NA_1_DoS` attack.
- **20200605_UOWM_IEC104_Dataset_c_rd_na_1_DoS.7z**: A 7zip file including the pcap and CSV files related to the `C_RD_NA_1_DoS` attack.
- **20200605_UOWM_IEC104_Dataset_c_rd_na_1.7z**: A 7zip file including the pcap and CSV files related to the `C_RD_NA_1` attack.
- **20200606_UOWM_IEC104_Dataset_c_rp_na_1_DoS.7z**: A 7zip file including the pcap and CSV files related to the `C_RP_NA_1_DoS` attack.
- **20200606_UOWM_IEC104_Dataset_c_rp_na_1.7z**: A 7zip file including the pcap and CSV files related to the `C_RP_NA_1` attack.
- **20200608_UOWM_IEC104_Dataset_mitm_drop.7z**: A 7zip file including the pcap and CSV files related to the `MITM` attack.
- **Balanced_IEC104_Train_Test_CSV_Files.zip**: This zip file includes balanced CSV files from `CICFlowMeter` and the `Custom IEC 60870-5-104 Python Parser` that could be utilised for training ML and DL methods. The zip file includes different folders for the corresponding flow timeout values used for `CICFlowMeter` and `IEC 60870-5-104 Python Parser`, respectively.

Each 7zip file includes respective folders related to the entities/devices (described in the following section) participating in each attack. In particular, for each entity/device, there is a folder including (a) the overall network traffic (pcap file) related to this entity/device during each attack, (b) the TCP/IP network flow statistics (CSV file) from `CICFlowMeter` for the overall network traffic, (c) the IEC 60870-5-104 network traffic (pcap file) related to this entity/device during each attack, (d) the TCP/IP network flow statistics

(CSV file) from `CICFlowMeter` for the IEC 608770-5-104 network traffic, (e) the IEC 60870-5-104 flow statistics (CSV file) from the `Custom IEC 60870-5-104 Python Parser` for the IEC 608770-5-104 network traffic and finally, (f) an image showing how the attack was executed. Finally, it is noteworthy that the network flow from both `CICFlowMeter` and `Custom IEC 60870-5-104 Python Parser` in each CSV file are **labelled** based on the IEC 60870-5-104 cyberattacks executed for the generation of this dataset. The description of these attacks is given in the following section, while the various features from `CICFlowMeter` and `Custom IEC 60870-5-104 Python Parser` are presented in Section 5.

4. Testbed & IEC 60870-5-104 Attacks

Fig. 1. shows the testbed created for generating this dataset. It is composed of five virtual RTU devices emulated by IEC TestServer and two real RTU devices. Moreover, there is another workstation which plays the role of Master Terminal Unit (MTU) and HMI, sending legitimate IEC 60870-5-104 commands to the corresponding RTUs. For this purpose, the workstation uses QTester104. In addition, there are three attackers that act as malicious insiders executing the following cyberattacks against the aforementioned RTUs. Finally, the network traffic data of each entity/device was captured through tshark.

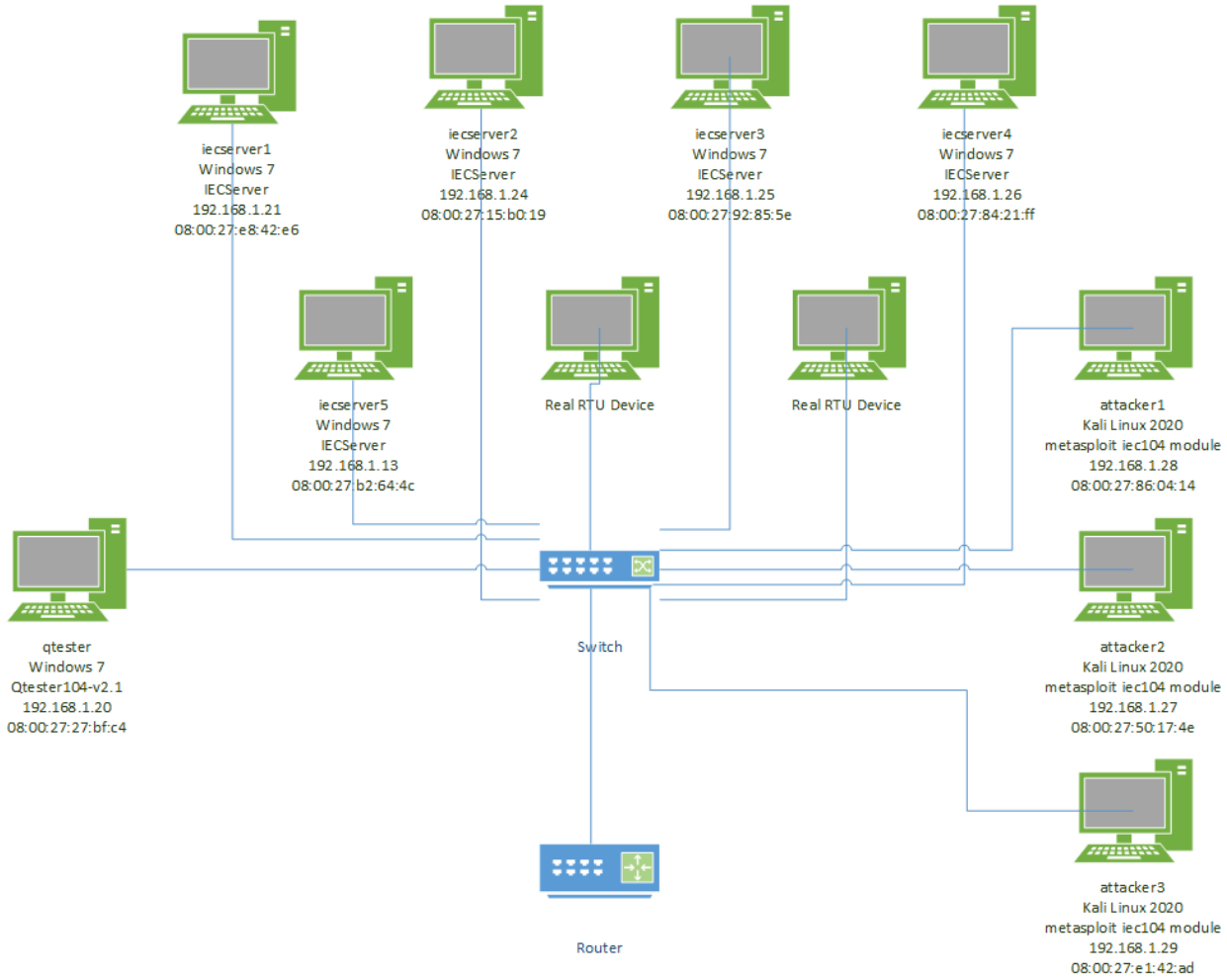

Fig. 1: Testbed used for the generation of the IEC 69870-5-104 Intrusion Detection Dataset

Table 1: IEC 60870-5-104 Cyberattacks Description

IEC 60870-5-104 Cyberattack Description	Description	Dataset Files
MITM Drop	During this attack, the cyberattacker is placed between two endpoints, thus monitoring and dropping the network traffic exchanged.	20200608_UOWM_IEC104_Dataset_mitm_drop.7z
C_CI_NA_1	The C_CI_NA_1 is a Counter Interrogation command in the control direction. This cyberattack sends unauthorised IEC 60870-5-104 C_CI_NA_1 packets to the target system.	20200426_UOWM_IEC104_Dataset_c_ci_na_1.7z
C_SC_NA_1	The C_SC_NA_1 command is a single command. This cyberattack sends unauthorised C_SC_NA_1 60870-5-104 packets to the target system	20200428_UOWM_IEC104_Dataset_c_sc_na_1.7z
C_SE_NA_1	The C_SE_NA_1 command is a set-point command with normalised values. This cyberattack sends unauthorised IEC 60870-5-104 C_SE_NA_1 packets to the target system.	20200427_UOWM_IEC104_Dataset_c_se_na_1.7z
C_RD_NA_1	The C_RD_NA_1 command is a read command. This cyberattack sends unauthorised IEC 60870-5-104 C_RD_NA_1 packets to the target system.	20200605_UOWM_IEC104_Dataset_c_rd_na_1.7z
C_RP_NA_1	The C_RP_NA_1 command is a reset command. This cyberattack sends	20200606_UOWM_IEC104_Dataset_c_rp_na_1.7z

	unauthorised IEC 60870-5-104 C_RP_NA_1 packets to the target system.	
M_SP_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 M_SP_NA_1 packets.	20200425_UOWM_IEC104_Dataset_m_sp_na_1_DoS.7z
C_CI_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_CI_NA_1 packets.	20200426_UOWM_IEC104_Dataset_c_ci_na_1_DoS.7z
C_SE_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_SE_NA_1 packets.	20200428_UOWM_IEC104_Dataset_c_se_na_1_DoS.7z
C_SC_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_SC_NA_1 packets.	20200429_UOWM_IEC104_Dataset_c_sc_na_1_DoS.7z
C_RD_NA_1_DoS	This attack floods the target system with IEC 60870-5-104 C_RD_NA_1 packets.	20200605_UOWM_IEC104_Dataset_c_rd_na_1_DoS.7z
C RP NA 1 DoS	This attack floods the target system with IEC 60870-5-104 C_RP_NA_1 packets.	20200606_UOWM_IEC104_Dataset_c_rp_na_1_DoS.7z

5. Features

The TCP/IP network flow statistics generated by `CICFlowMeter` are summarised below. **It is worth mentioning that the TCP/IP network flows and their statistics generated by `CICFlowMeter` are labelled based on the IEC 60870-5-104 attacks described above, thus allowing the training of ML/DL models.**

Table 2: CICFlowMeter TCP/IP Network Flow Statistics - Features

Feature	Description
Flow ID	ID of the flow
Src IP	Source IP address
Src Port	Source TCP/UDP port
Dst IP	Destination IP address
Dst Port	Destination TCP/UDP port
Protocol	The protocol related to the corresponding flow
Timestamp	Flow timestamp
Flow Duration	Duration of the flow in Microsecond
Tot Fwd Pkts	Total packets in the forward direction
Tot Bwd Pkts	Total packets in the backward direction
TotLen Fwd Pkts	Total size of packets in forward direction
TotLen Bwd Pkts	Total size of packets in backward direction
Fwd Pkt Len Max	Maximum size of packet in forward direction
Fwd Pkt Len Min	Minimum size of packet in forward direction
Fwd Pkt Len Mean	Mean size of packet in forward direction
Fwd Pkt Len Std	Standard deviation size of packet in forward direction
Bwd Pkt Len Max	Maximum size of packet in backward direction
Bwd Pkt Len Min	Minimum size of packet in backward direction
Bwd Pkt Len Mean	Mean size of packet in backward direction
Bwd Pkt Len Std	Standard deviation size of packet in backward direction
Flow Byts/s	Number of flow bytes per second
Flow Pkts/s	Number of flow packets per second
Flow IAT Mean	Mean time between two packets sent in the flow
Flow IAT Std	Standard deviation time between two packets sent in the flow
Flow IAT Max	Maximum time between two packets sent in the flow
Flow IAT Min	Minimum time between two packets sent in the flow
Fwd IAT Tot	Total time between two packets sent in the forward direction

Fwd IAT Mean	Mean time between two packets sent in the forward direction
Fwd IAT Std	Standard deviation time between two packets sent in the forward direction
Fwd IAT Max	Maximum time between two packets sent in the forward direction
Fwd IAT Min	Minimum time between two packets sent in the forward direction
Bwd IAT Tot	Total time between two packets sent in the backward direction
Bwd IAT Mean	Mean time between two packets sent in the backward direction
Bwd IAT Std	Standard deviation time between two packets sent in the backward direction
Bwd IAT Max	Maximum time between two packets sent in the backward direction
Bwd IAT Min	Minimum time between two packets sent in the backward direction
Fwd PSH Flags	Number of times the PSH flag was set in packets travelling in the forward direction (0 for UDP)
Bwd PSH Flags	Number of times the PSH flag was set in packets travelling in the backward direction (0 for UDP)
Fwd URG Flags	Number of times the URG flag was set in packets travelling in the forward direction (0 for UDP)
Bwd URG Flags	Number of times the URG flag was set in packets travelling in the backward direction (0 for UDP)
Fwd Header Len	Total bytes used for headers in the forward direction
Bwd Header Len	Total bytes used for headers in the backward direction
Fwd Pkts/s	Number of forward packets per second
Bwd Pkts/s	Number of backward packets per second
Pkt Len Min	Minimum length of a packet
Pkt Len Max	Maximum length of a packet
Pkt Len Mean	Mean length of a packet
Pkt Len Std	Standard deviation length of a packet
Pkt Len Var	Variance length of a packet
FIN Flag Cnt	Number of packets with FIN
SYN Flag Cnt	Number of packets with SYN
RST Flag Cnt	Number of packets with RST
PSH Flag Cnt	Number of packets with PUSH
ACK Flag Cnt	Number of packets with ACK
URG Flag Cnt	Number of packets with URG
CWE Flag Count	Number of packets with CWE
ECE Flag Cnt	Number of packets with ECE
Down/Up Ratio	Download and upload ratio

Pkt Size Avg	Average size of packet
Fwd Seg Size Avg	Average size observed in the forward direction
Bwd Seg Size Avg	Average size observed in the backward direction
Fwd Byts/b Avg	Average number of bytes bulk rate in the forward direction
Fwd Pkts/b Avg	Average number of packets bulk rate in the forward direction
Fwd Blk Rate Avg	Average number of bulk rate in the forward direction
Bwd Byts/b Avg	Average number of bytes bulk rate in the backward direction
Bwd Pkts/b Avg	Average number of packets bulk rate in the backward direction
Bwd Blk Rate Avg	Average number of bulk rate in the backward direction
Subflow Fwd Pkts	The average number of packets in a sub flow in the forward direction
Subflow Fwd Byts	The average number of bytes in a sub flow in the forward direction
Subflow Bwd Pkts	The average number of packets in a sub flow in the backward direction
Subflow Bwd Byts	The average number of bytes in a sub flow in the backward direction
Init Fwd Win Byts	The total number of bytes sent in initial window in the forward direction
Init Bwd Win Byts	The total number of bytes sent in initial window in the backward direction
Fwd Act Data Pkts	Count of packets with at least 1 byte of TCP data payload in the forward direction
Fwd Seg Size Min	Minimum segment size observed in the forward direction
Active Mean	Mean time a flow was active before becoming idle
Active Std	Standard deviation time a flow was active before becoming idle
Active Max	Maximum time a flow was active before becoming idle
Active Min	Minimum time a flow was active before becoming idle
Idle Mean	Mean time a flow was idle before becoming active
Idle Std	Standard deviation time a flow was idle before becoming active
Idle Max	Maximum time a flow was idle before becoming active
Idle Min	Minimum time a flow was idle before becoming active
Label	Attack label

The IEC 60870-5-104 flow statistics generated by `IEC 60870-5-104 Python Parser` are summarised below. **It is worth mentioning that the IEC 60870-5-104 flows and their statistics generated by `IEC 60870-5-104 Python Parser` are labelled based on the IEC 60870-5-104 attacks described above, thus allowing the training of ML/DL models.**

Table 3: IEC 60870-5-104 Flow Statistics – Features

Feature	Field description
flow id	ID of the flow
protocol	The relevant protocol of the flow. It equals IEC 60870-5-104

src ip	The source IP address of the flow. It is defined with the first relevant packet.
dst ip	The destination IP address of the flow.
src port	The source TCP/UDP port.
dst port	The destination TCP/UDP port.
flow idle time max	The maximum time where the flow was idle
flow idle time min	The minimum time where the flow was idle
flow idle time mean	The time mean where the flow was idle
flow idle time std	The time standard deviation where the flow was idle
flow idle time variance	The time variance where the flow was idle
flow active time max	The maximum time where the flow was active
flow active time min	The minimum time where the flow was active
flow active time mean	The time mean where the flow was active
flow active time std	The time standard deviation where the flow was active
flow active time variance	The time variance where the flow was active
flow IAT max	The maximum interarrival time
fw IAT max	The maximum interarrival time in the forward direction
bw IAT max	The maximum interarrival time in the backyard direction
flow IAT min	The minimum interarrival time
fw IAT min	The minimum interarrival time in the forward direction
bw IAT min	The minimum interarrival time in the backyard direction
flow IAT mean	The mean of the interarrival time
fw IAT mean	The mean of the interarrival time in the forward direction
bw IAT mean	The mean of the interarrival time in the backyard direction
flow IAT std	The standard deviation of the inter arrival time
fw IAT std	The standard deviation of the inter arrival time in the forward direction
bw IAT std	The standard deviation of the inter arrival time in the backyard direction
flow IAT tot	The total number of the interarrival times
fw iAT tot	The total number of the interarrival times in the forward direction
bw IAT tot	The total number of the interarrival times in the backyard direction
flow iec104 packts/s	The number of IEC 60870-51-04 packets per second
fw iec104 packts/s	The number of IEC 60870-51-04 packets per second in the forward direction

bw iec104 packts/s	The number of IEC 60870-51-04 packets per second in the backyard direction
flow iec104 bytes/s	The sum of APDU lengths per second
fw iec104 bytes/s	The sum of APDU lengths per second in the forward direction
bw iec104 bytes/s	The sum of APDU lengths per second in the backyard direction
flow packet APDU length max	The maximum value of the APDU lengths
flow packet APDU length min	The minimum value of the APDU lengths
flow packet APDU length mean	Mean of the APDU lengths
flow packet APDU length std	The standard deviation of the APDU lengths
flow packet APDU length var	Variance of the APDU lengths
fw packet APDU length max	The maximum value of the APDU lengths in the forward direction
fw packet APDU length min	The minimum value of the APDU lengths in the forward direction
fw packet APDU length mean	Mean of the APDU lengths in the forward direction
fw packet APDU length std	The standard deviation of the APDU lengths in the forward direction
fw packet APDU length var	The variance of the APDU lengths in the forward direction
bw packet APDU length max	The maximum value of the APDU lengths in the backyard direction
bw packet APDU length min	The minimum value of the APDU lengths in the backyard direction
bw packet APDU length mean	Mean of the APDU lengths in the backyard direction
bw packet APDU length std	The standard deviation of the APDU lengths in the backyard direction
bw packet APDU length var	The variance of the APDU lengths in the backyard direction
total flow packets	Total flow packets
total fw packets	Total flow packets in the forward direction
total bw packets	Total flow packets in the backyard direction
flow packets APDU total length	The sum of all APDU lengths
fw packets APDU total length	The sum of all APDU lengths in the forward direction
bw packets APDU total length	The sum of all APDU lengths in the backyard direction
flow duration	Flow duration in seconds
flow down/up ratio	The fraction between the IEC 60870-5-104 packets in the backyard direction and the IEC 60870-5-104 packets in the forward direction
flow total IEC104_I_Message_SeqIOA packets	The total number of the I-format APCI packets that have more than one information objects
fw total IEC104_I_Message_SeqIOA packets	The total number of the I-format APCI packets that have more than one information objects in the forward direction
bw total IEC104_I_Message_SeqIOA packets	The total number of the I-format APCI packets that have more than one information objects in the backyard direction

flow total IEC104_I_Message_SingleIOA packets	The total number of the I-format APCI packets that have one information object in ASDU
fw total IEC104_I_Message_SingleIOA packets	The total number of the I-format APCI packets that have one information object in ASDU in the forward direction
bw total IEC104_I_Message_SingleIOA packets	The total number of the I-format APCI packets that have one information object in ASDU in the backyard direction
flow total IEC104_S_Message packets	The total number of the S-format APCI packets
fw total IEC104_S_Message packets	The total number of the S-format APCI packets in the forward direction
bw total IEC104_S_Message packets	The total number of the S-format APCI packets in the backyard direction
flow total IEC104_U_Message packets	The total number of the U-format APCI packets
fw total IEC104_U_Message packets	The total number of the U-format APCI packets in the forward direction
bw total IEC104_U_Message packets	The total number of the U-format APCI packets in the backyard direction
fw URG flag amount	The number of the URG flags in the forward direction
fw PSH flag amount	The number of the PSH flags in the forward direction
bw URG flag amount	The number of the URG flags in the backyard direction
bw PSH flag amount	The number of the PSH flags in the backyard direction
flow SYN flag count	The number of the TCP SYN packets
flow RST flag count	The number of the TCP RST packets
flow PSH flag count	The number of the TCP PSH packets
flow ACK flag count	The number of the TCP ACK packets
flow URG flag count	The number of the TCP URG packets
flow CWE flag count	The number of the TCP CWE packets
flow ECE flag count	The number of the TCP ECE packets
fw_subflow_packets	The average number of packets in a sub flow in the forward direction
bw_subflow_packets	The average number of packets in a sub flow in the backward direction
fw_subflow_bytes	The average number of bytes in a sub flow in the forward direction
bw_subflow_bytes	The average number of bytes in a sub flow in the backward direction
flow start timestamp	The timestamp of the flow. It is defined with the first relevant packet.
fw avg bytes/bulk	Average number of bytes bulk rate in the forward direction
bw avg bytes/bulk	Average number of bytes bulk rate in the backyard direction
fw avg bulk rate	Average number of bulk rate in the forward direction

bw avg bulk rate	Average number of bulk rate in the backyard direction
fw avg packets/bulk	Average number of packets bulk rate in the forward direction
bw avg packets/bulk	Average number of packets bulk rate in the backyard direction
init fw window bytes	The window size of the first packet in the forward direction
init bw window bytes	The window size of the first packet in the backyard direction
fw TCP total header length	The length of the TCP headers in the forward direction
bw TCP total header length	The length of the TCP headers in the backyard direction
cot=1	The total number of the IEC 60870-5-104 packets where COT = 1 (periodic,cyclic)
cot=2	The total number of the IEC 60870-5-104 packets where COT = 2 (background interrogation)
cot=3	The total number of the IEC 60870-5-104 packets where COT = 3 (spontaneous)
cot=4	The total number of the IEC 60870-5-104 packets where COT = 4 (initialized)
cot=5	The total number of the IEC 60870-5-104 packets where COT = 5 (interrogation)
cot=6	The total number of the IEC 60870-5-104 packets where COT = 6 (activation)
cot=7	The total number of the IEC 60870-5-104 packets where COT = 7 (confirmation activation)
cot=8	The total number of the IEC 60870-5-104 packets where COT = 8 (deactivation)
cot=9	The total number of the IEC 60870-5-104 packets where COT = 9 (confirmation deactivation)
cot=10	The total number of the IEC 60870-5-104 packets where COT = 10 (termination activation)
cot=11	The total number of the IEC 60870-5-104 packets where COT = 11 (feedback, caused by distant command)
cot=12	The total number of the IEC 60870-5-104 packets where COT = 12 (feedback, caused by local command)
cot=13	The total number of the IEC 60870-5-104 packets where COT = 13 (COT data transmission)
cot=20	The total number of the IEC 60870-5-104 packets where COT = 20 (interrogated by general interrogation)
type_id_process_information_in_monitor_direction	The total number of the IEC 60870-5-104 packets where TypeID is in the range 1-40
type_id_process_information_in_control_direction	The total number of the IEC 60870-5-104 packets where TypeID is in the range 45-51

type_id_system_information_in_monitor_direction	The total number of the IEC 60870-5-104 packets where TypeID is in the range 70
type_id_system_information_in_control_direction	The total number of the IEC 60870-5-104 packets where TypeID is in the range 100-106
type_id_parameter_in_control_direction	The total number of the IEC 60870-5-104 packets where TypeID is in the range 110-113
type_id_file_transfer	The total number of the IEC 60870-5-104 packets where TypeID is in the range 120-126
Label	Attack label

6. Citation

Please cite the following paper when using this dataset:

P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos and S. Wan, "Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach", in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 2041-2052, March 2022, doi: 10.1109/TII.2021.3093905.

https://ieeexplore.ieee.org/document/9470933

7. Acknowledgment

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreements No 101021936 (ELECTRON) and No 833955 (SDN-microSENSE).

References

[1] P. Radoglou-Grammatikis, K. Rompolos, P. Sarigiannidis, V. Argyriou, T. Lagkas, A. Sarigiannidis, S. Goudos and S. Wan, "Modeling, Detecting, and Mitigating Threats Against Industrial Healthcare Systems: A Combined Software Defined Networking and Reinforcement Learning Approach", in IEEE Transactions on Industrial Informatics, vol. 18, no. 3, pp. 2041-2052, March 2022, doi: 10.1109/TII.2021.3093905.

[2] A. Gharib, I. Sharafaldin, A. H. Lashkari and A. A. Ghorbani, "An Evaluation Framework for Intrusion Detection Dataset," 2016 International Conference on Information Science and Security (ICISS), 2016, pp. 1-6, doi: 10.1109/ICISSEC.2016.7885840.