DNP3

Intrusion Detection Dataset

Readme File

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

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

Publication Date: November 22, 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

In the digital era of the Industrial Internet of Things (IIoT), the conventional Critical Infrastructures (CIs) are transformed into smart environments with multiple benefits, such as pervasive control, self-monitoring and self-healing. However, this evolution is characterised by several cyberthreats due to the necessary presence of insecure technologies. DNP3 is an industrial communication protocol which is widely adopted in the CIs of the US. In particular, DNP3 allows the remote communication between Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA). It can support various topologies, such as Master-Slave, Multi-Drop, Hierarchical and Multiple-Server. Initially, the architectural model of DNP3 consists of three layers: (a) Application Layer, (b) Transport Layer and (c) Data Link Layer. However, DNP3 can be now incorporated into the Transmission Control Protocol/Internet Protocol (TCP/IP) stack as an application-layer protocol. However, similarly to other industrial protocols (e.g., Modbus and IEC 60870-5-104), DNP3 is characterised by severe security issues since it does not include any authentication or authorisation mechanisms. More information about the DNP3 security issue is provided in [1-3]. This dataset contains labelled Transmission Control Protocol (TCP) / Internet Protocol (IP) network flow statistics (Common-Separated Values - CSV format) and DNP3 flow statistics (CSV format) related to 9 DNP3 cyberattacks. These cyberattacks are focused on DNP3 unauthorised commands and Denial of Service (DoS). The network traffic data are provided through Packet Capture (PCAP) files. Consequently, this dataset can be used to implement Artificial Intelligence (AI)-powered Intrusion Detection and Prevention (IDPS) systems that rely on Machine Learning (ML) and Deep Learning (DL) techniques.

2. Instructions

This DNP3 Intrusion Detection Dataset was implemented following the methodological frameworks of A. Gharib et al. in [4] and S. Dadkhah et al in [5], 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) eight industrial entities, (b) one Human Machine Interfaces (HMI) and (c) three cyberattackers was used to implement this DNP3 Intrusion Detection Dataset. In particular, the following cyberattacks were implemented.

- On Thursday, May 14, 2020, the **DNP3 Disable Unsolicited Messages Attack** was executed for 4 hours.
- On Friday, May 15, 2020, the **DNP3 Cold Restart Message Attack** was executed for 4 hours.
- On Friday, May 15, 2020, the **DNP3 Warm Restart Message Attack** was executed for 4 hours.
- On Saturday, May 16, 2020, the **DNP3 Enumerate Attack** was executed for 4 hours.
- On Saturday, May 16, 2020, the **DNP3 Info Attack** was executed for 4 hours.
- On Monday, May 18, 2020, the **DNP3 Initialisation Attack** was executed for 4 hours.
- On Monday, May 18, 2020, the **Man In The Middle (MITM)-DoS Attack** was executed for 4 hours.
- On Monday, May 18, 2020, the **DNP3 Replay Attack** was executed for 4 hours.
- On Tuesday, May 19, 2020, the **DNP3 Stop Application Attack** was executed for 4 hours.

The aforementioned DNP3 cyberattacks were executed, utilising penetration testing tools, such as Nmap[1] and Scapy[2]. For each attack, a relevant folder is provided, including the network traffic and the network flow statistics for each entity. In particular, for each cyberattack, a folder is given, providing (a) the pcap files for each entity, (b) the Transmission Control Protocol (TCP)/ Internet Protocol (IP) network flow statistics for 120 seconds in a CSV format and (c) the DNP3 flow statistics for each entity (using different timeout values in terms of second (such as 45, 60, 75, 90, 120 and 240 seconds)). The TCP/IP network flow statistics were produced by using the CICFlowMeter[3], while the DNP3 flow statistics were generated based on a Custom DNP3 Python Parser[4], taking full advantage of Scapy.

[1] https://nmap.org/
[2] Scapy - https://scapy.net/
[3] CICFlowMeter - https://github.com/ahlashkari/CICFlowMeter
[4] This parser could be available upon request

3. Dataset Structure

The dataset consists of the following folders:

- **20200514_DNP3_Disable_Unsolicited_Messages_Attack**: It includes the pcap and CSV files related to the DNP3 Disable Unsolicited Message attack.
- **20200515_DNP3_Cold_Restart_Attack**: It includes the pcap and CSV files related to the DNP3 Cold Restart attack.
- **20200515_DNP3_Warm_Restart_Attack**: It includes the pcap and CSV files related to DNP3 Warm Restart attack.
- **20200516_DNP3_Enumerate**: It includes the pcap and CSV files related to the DNP3 Enumerate attack.
- **20200516_DNP3_Info**: It includes the pcap and CSV files related to the DNP3 Info attack.
- **20200518_DNP3_Initialize_Data_Attack**: It includes the pcap and CSV files related to the DNP3 Data Initialisation attack.
- **20200518_DNP3_MITM_DoS**: It includes the pcap and CSV files related to the DNP3 MITM-DoS attack.
- **20200518_DNP3_Replay_Attack**: It includes the pcap and CSV files related to the DNP3 replay attack.
- **20200519_DNP3_Stop_Application_Attack**: It includes the pcap and CSV files related to the DNP3 Stop Application attack.
- **Training_Testing_Balanced_CSV_Files**: It includes balanced CSV files from CICFlowMeter and the Custom DNP3 Python Parser that could be utilised for training ML and DL methods. Each folder includes different sub-folder for the corresponding flow timeout values used by the DNP3 Python Custom Parser. For CICFlowMeter, only the timeout value of 120 seconds was used.

Each folder includes respective subfolders 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 DNP3 network traffic (pcap file) related to this entity/device during each attack, (b) the TCP/IP network flow statistics (CSV file) generated by CICFlowMeter for the timeout value of 120 seconds and finally (c) the DNP3 flow statistics (CSV file) from the Custom DNP3 Python Parser. Finally, it is noteworthy that the network flows from both CICFlowMeter and Custom DNP3 Python Parser in each CSV file are **labelled** based on the DNP3 cyberattacks executed for the generation of this dataset. The description of these attacks is provided in the following section, while the various features from CICFlowMeter and Custom DNP3 Python Parser are presented in Section 5.

4. Testbed & DNP3 Attacks

The following figure shows the testbed utilised for the generation of this dataset. It is composed of eight industrial entities that play the role of the DNP3 outstations/slaves, such as Remote Terminal Units (RTUs) and Intelligent Electron Devices (IEDs). Moreover, there is another workstation which plays the role of the Master station like a Master Terminal Unit (MTU). For the communication between, the DNP3 outstations/slaves and the master station, opendnp3[5]was used.

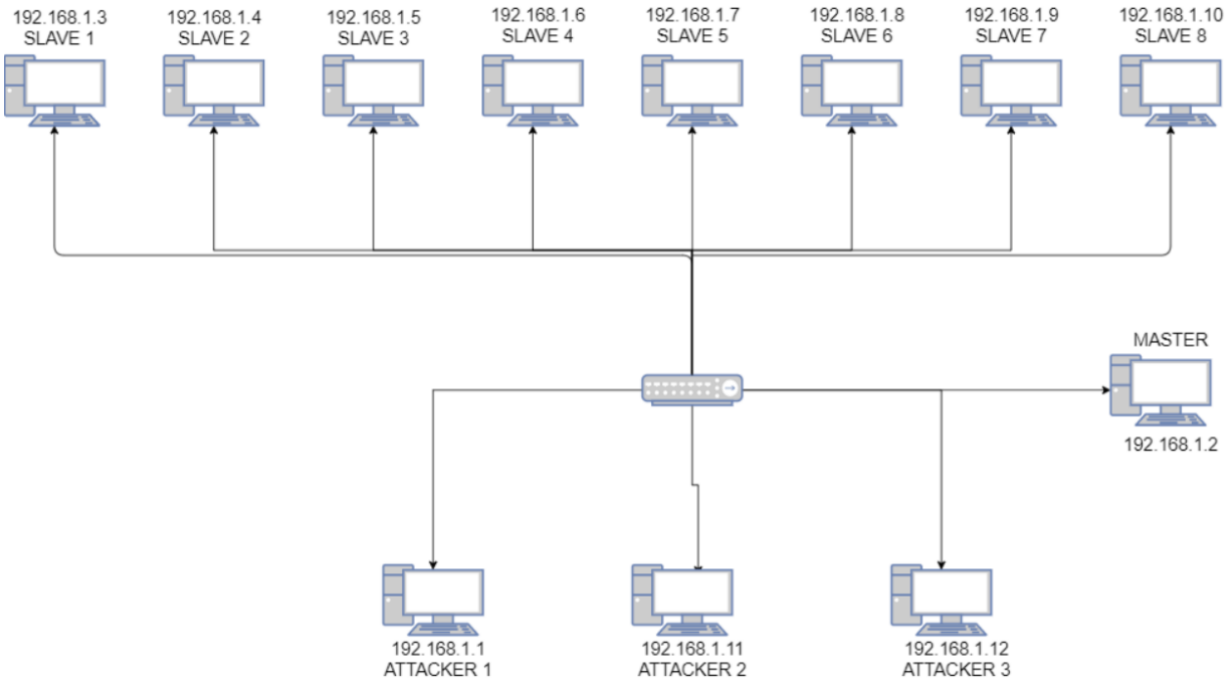

Figure 1: Testbed used for the generation of the DNP3 Intrusion Detection Dataset

[5] https://dnp3.github.io/

Table 1: DNP3 Attacks Description

DNP3 Attack	Description	Dataset Folder
DNP3 Disable Unsolicited Message Attack	This attack targets a DNP3 outstation/slave, establishing a connection with it, while acting as a master station. The false master then transmits a packet with the DNP3 Function Code 21, which requests to disable all the unsolicited messages on the target.	20200514_DNP3_Disable_Unsolicited_Messages_Attack
DNP3 Cold Restart Attack	The malicious entity acts as a master station and sends a DNP3 packet that includes the "Cold Restart" function code. When the target receives this message, it initiates a complete restart and sends back a reply with the time window before the restart process.	20200515_DNP3_Cold_Restart_Attack
DNP3 Warm Restart Attack	This attack is quite similar to the "Cold Restart Message", but aims to trigger a partial restart, re-initiating a DNP3 service on the target outstation.	20200515_DNP3_Warm_Restart_Attack
DNP3 Enumerate Attack	This reconnaissance attack aims to discover which DNP3 services and functional codes are used by the target system.	20200516_DNP3_Enumerate
DNP3 Info Attack	This attack constitutes another reconnaissance attempt, aggregating various DNP3 diagnostic information	20200516_DNP3_Info

	related the DNP3 usage.	
Data Initialisation Attack	This cyberattack is related to Function Code 15 (Initialize Data). It is an unauthorised access attack, which demands from the slave to re-initialise possible configurations to their initial values, thus changing potential values defined by legitimate masters	20200518_Initialize_Data_Attack
MITM-DoS Attack	In this cyberattack, the cyberattacker is placed between a DNP3 master and a DNP3 slave device, dropping all the messages coming from the DNP3 master or the DNP3 slave.	20200518_MITM_DoS
DNP3 Replay Attack	This cyberattack replays DNP3 packets coming from a legitimate DNP3 master or DNP3 slave.	20200518_DNP3_Replay_Attack
DNP3 Step Application Attack	This attack is related to the Function Code 18 (Stop Application) and demands from the slave to stop its function so that the slave cannot receive messages from the master.	20200519_DNP3_Stop_Application_Attack

5. Features

The TCP/IP network flow statistics generated by `CICFlowMeter` are summarised below. **The TCP/IP network flows and their statistics generated by `CICFlowMeter` are labelled based on the DNP3 attacks described above, thus allowing the training of ML/DL models. Finally, it is worth mentioning that these statistics are generated when the flow timeout value is equal with 120 seconds.**

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 DNP3 flow statistics generated by the DNP3 Python Parser are summarised below. **The DNP3 flows and their statistics generated by the DNP3 Python Parser are labelled based on the DNP3 attacks described above, thus allowing the training of ML/DL models. Finally, it is worth mentioning that these statistics are available for various flow timeout values, such as 45, 60, 75, 90, 120 and 240 seconds.**

Table 3: DNP3 Flow Statistics – Features

Feature	**Field description**
flow ID	ID of the flow
source IP	Source IP address
destination IP	Destination IP address

source port	Source TCP/UDP Port
destination port	Destination TCP/UDP port
protocol	The protocol related to the corresponding flow
date	Flow timestamp
TotalFwdPkts	The total number of the DNP3 packets in the forward direction
TotalBwdPkts	The total number of the DNP3 packets in the backyard direction
TotLenfwdDL	The total size of the DNP3 payload at the link layer in the forward direction
TotLenfwdTR	The total size of the DNP3 payload at the transport layer in the forward direction
TotLenfwdAPP	The total size of the DNP3 payload at the application layer in the forward direction
TotLenbwdDL	The total size of the DNP3 payload at the link layer in the backyard direction
TotLenbwdTR	The total size of the DNP3 payload at the transport layer in the backyard direction
TotLenbwdAPP	The total size of the DNP3 payload at the application layer in the backyard direction
DLfwdPktLenMAX	The maximum size of the DNP3 payload at the link layer in the forward direction
DLfwdPktLenMIN	The minimum size of the DNP3 payload at the link layer in the forward direction
DLfwdPktLenMEAN	The mean of the DNP3 payload at the link layer in the forward direction
DLfwdPktLenSTD	The standard deviation of the DNP3 payload at the link layer in the forward direction
TRfwdPktLenMAX	The maximum size of the DNP3 payload at the transport layer in the forward direction
TRfwdPktLenMIN	The minimum size of the DNP3 payload at the transport layer in the forward direction
TRfwdPktLenMEAN	The mean of the DNP3 payload at the transport layer in the forward direction
TRfwdPktLenSTD	The standard deviation of the DNP3 payload at the transport layer in the forward direction
APPfwdPktLenMAX	The maximum size of the DNP3 payload at the application layer in the backyard direction
APPfwdPktLenMIN	The minimum size of the DNP3 payload at the application layer in the backyard direction
APPfwdPktLenMEAN	The mean of the DNP3 payload at the application layer in the backyard direction

APPfwdPktLenSTD	The standard deviation of the DNP3 payload at the application layer in the backyard direction
DLbwdPktLenMAX	The maximum size of the DNP3 payload at the link layer in the backyard direction
DLbwdPktLenMIN	The minimum size of the DNP3 payload at the link layer in the backyard direction
DLbwdPktLenMEAN	The mean of the DNP3 payload at the link layer in the backyard direction
DLbwdPktLenSTD	The standard deviation of the DNP3 payload at the link layer in the backyard direction
TRbwdPktLenMAX	The maximum size of the DNP3 payload at the transport layer in the backyard direction
TRbwdPktLenMIN	The minimum size of the DNP3 payload at the transport layer in the backyard direction
TRbwdPktLenMEAN	The mean of the DNP3 payload at the transport layer in the backyard direction
TRbwdPktLenSTD	The standard deviation of the DNP3 payload at the transport layer in the backyard direction
APPbwdPktLenMAX	The maximum size of the DNP3 payload at the application layer in the backyard direction
APPbwdPktLenMIN	The minimum size of the DNP3 payload at the application layer in the backyard direction
APPbwdPktLenMEAN	The mean of the DNP3 payload at the application layer in the backyard direction
APPbwdPktLenSTD	The standard deviation of the DNP3 payload at the application layer in the backyard direction
DLflowBytes/sec	How many bytes of the DNP3 link-layer were transmitted per second
TRflowBytes/sec	How many bytes of the DNP3 transport layer were transmitted per second
APPflowBytes/sec	How many bytes of the DNP3 application layer were transmitted per second
FlowPkts/sec	How many DNP3 packets were transmitted per second
FlowIAT_MEAN	The mean of the DNP3 packets interarrival time
FlowIAT_STD	The standard deviation of the DNP3 packets interarrival time
FlowIAT_MAX	The maximum value of the DNP3 packets interarrival time
FlowIAT_MIN	The minimum value of the DNP3 packets interarrival time
TotalFwdIAT	The sum of the DNP3 packets interarrival time in the forward direction
fwdIAT_MEAN	The mean of the DNP3 packets interarrival time in the forward direction

fwdIAT_STD	The standard deviation of the DNP3 packets interarrival time in the forward direction
fwdIAT_MAX	The maximum value of the DNP3 packets interarrival time in the forward direction
fwdIAT_MIN	The minimum value of the DNP3 packets interarrival time in the forward direction
TotalBwdIAT	The sum of the DNP3 packets interarrival time in the backyard direction
bwdIAT_MEAN	The mean of the DNP3 packets interarrival time in the backyard direction
bwdIAT_STD	The standard deviation of the DNP3 packets interarrival time in the backyard direction
bwdIAT_MAX	The maximum value of the DNP3 packets interarrival time in the backyard direction
bwdIAT_MIN	The minimum value of the DNP3 packets interarrival time in the backyard direction
DLfwdHdrLen	The sum of the DNP3 headers at the link layer in the forward direction
TRfwdHdrLen	The sum of the DNP3 headers at the transport layer in the forward direction
APPfwdHdrLen	The sum of the DNP3 headers at the application layer in the forward direction
DLbwdHdrLen	The sum of the DNP3 headers at the link layer in the backyard direction
TRbwdHdrLen	The sum of the DNP3 headers at the transport layer in the backyard direction
APPbwdHdrLen	The sum of the DNP3 headers at the application layer in the backyard direction
fwdPkts/sec	How many DNP3 packets per second in the forward direction
bwdPkts/sec	How many DNP3 packets per second in the backyard direction
DLpktLenMEAN	The mean of the bytes at the DNP3 link layer
DLpktLenMIN	The minimum value of the bytes at the DNP3 link layer
DLpktLenMAX	The maximum value of the bytes at the DNP3 link layer
DLpktLenSTD	The standard deviation of the bytes at the DNP3 link layer
DLpktLenVAR	The variance of the bytes at the DNP3 link layer
TRpktLenMEAN	The mean of the bytes at the DNP3 transport layer
TRpktLenMIN	The minimum value of the bytes at the DNP3 transport layer
TRpktLenMAX	The maximum value of the bytes at the DNP3 transport layer
TRpktLenSTD	The standard deviation of the bytes at the DNP3 transport layer

TRpktLenVAR	The variance of the bytes at the DNP3 transport layer
APPpktLenMEAN	The mean of the bytes at the DNP3 application layer
APPpktLenMIN	The minimum value of the bytes at the DNP3 application layer
APPpktLenMAX	The maximum value of the bytes at the DNP3 application layer
APPpktLenSTD	The standard deviation of the bytes at the DNP3 application layer
APPpktLenVAR	The variance of the bytes at the DNP3 application layer
ActiveMEAN	The time-mean where the flow was active
ActiveSTD	The time standard deviation where the flow was active
ActiveMAX	The maximum value of the time where the flow is active
ActiveMIN	The maximum value of the time where the flow is idle.
IdleMEAN	The time-mean where the flow was idle before becoming active
IdleSTD	The standard deviation of the time where the flow was idle before becoming active
IdleMAX	The maximum value of the time where the flow was idle before becoming active
IdleMIN	The minimum value of the time where the flow was idle before becoming active
frameSrc	The source MAC address
frameDst	The destination MAC address
TotPktsInFlow	The total number of the DNP3 packets
firstPacketDIR	Whether the flow was initiated by a DNP3 master device or DNP3 slave device
mostCommonREQ_FUNC_CODE	The DNP3 function code which was used mostly in the DNP3 request packets
mostCommonRESP_FUNC_CODE	The DNP3 function code which was used mostly in the DNP3 response packets
corruptConfigFragments	How many responses were sent by the slave, setting the corruptConfig bit in the IIN value
deviceTroubleFragments	How many responses were sent by the slave, setting the deviceTrouble bit in the IIN value
deviceRestartFragments	How many responses were sent by the slave, setting the deviceRestart bit in the IIN value
pktsFromMASTER	How many packets that transmitted by a DNP3 master device
pktsFromSLAVE	How many packets that transmitted by a DNP3 slave device
Label	Attack label

6. Citation

The users of this dataset are kindly asked to cite the following papers as follows.

V. Kelli et al., "Attacking and Defending DNP3 ICS/SCADA Systems", 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2022, pp. 183-190, doi: 10.1109/DCOSS54816.2022.00041.

V. Kelli, P. Radoglou-Grammatikis, T. Lagkas, E. K. Markakis and P. Sarigiannidis, "Risk Analysis of DNP3 Attacks", 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022, pp. 351-356, doi: 10.1109/CSR54599.2022.9850291.

P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, P.-A.Karypidis, and A. Sarigiannidis, "Diderot: An intrusion detection and prevention system for dnp3-based scada systems", in Proceedings of the15th International Conference on Availability, Reliability and Security, ser. ARES '20.New York, NY, USA: Association for Computing Machinery, 2020, doi: 10.1145/3407023.3409314.

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] V. Kelli et al., "Attacking and Defending DNP3 ICS/SCADA Systems", 2022 18th International Conference on Distributed Computing in Sensor Systems (DCOSS), 2022, pp. 183-190, doi: 10.1109/DCOSS54816.2022.00041.

[2] V. Kelli, P. Radoglou-Grammatikis, T. Lagkas, E. K. Markakis and P. Sarigiannidis, "Risk Analysis of DNP3 Attacks", 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022, pp. 351-356, doi: 10.1109/CSR54599.2022.9850291.

[3] P. Radoglou-Grammatikis, P. Sarigiannidis, G. Efstathopoulos, P.-A.Karypidis, and A. Sarigiannidis, "Diderot: An intrusion detection and prevention system for dnp3-based scada systems", in Proceedings of the15th International Conference on Availability, Reliability and Security, ser. ARES '20.New York, NY, USA: Association for Computing Machinery, 2020, doi: 10.1145/3407023.3409314.

[4] 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.

[5] S. Dadkhah, H. Mahdikhani, P. K. Danso, A. Zohourian, K. A. Truong and A. A. Ghorbani, "Towards the Development of a Realistic Multidimensional IoT Profiling Dataset", 2022 19th Annual International Conference on Privacy, Security & Trust (PST), 2022, pp. 1-11, doi: 10.1109/PST55820.2022.9851966.