ML based anomaly, attack detection on DHALSIM testbed

PLCs exchange sensor and actuator values using the CIP protocol. Anytime a CIP message needs to be sent, TCP and ENIP messages are exchanged to set up a CIP session. Because of this, the number of packets exchanged by TCP and ENIP protocols is higher than the number of packets exchanged by CIP and CIP CM. For TCP connections there will be SYN, SYN-ACK, ACK messages. The 'REG' commands are ENIP messages that signal a request to create an ENIP session to exchange CIP messages. Because of this, the number of REG messages is higher than the 'number of 'DATA', 'GET T42, 'GET T41', 'GET P78', and 'GET P79' messages. 'GET T42, 'GET T41', 'GET P78', and 'GET P79' are CIP CM messages requesting the values of each one of those tags.

Important thing is there is a pattern of network messages under normal circumstances. Also in normal circumstances the tanks will be full end empty in cycles. So there will be cycle of patterns in network data.

We will have all these network data captured in .pcap file using tc.

Also we will have sensor readings or SCADA data; both for normal circumstances (ground truth) and also under attack or disruption.

Bottom line is the periodic behavior shown by both process and network data denotes the bi-directional relationship between physical and cyber layers.

When there is packet loss and delay, there will be less messages. When there is a DoS attack there will be more messages. When there is an MITM attack using ARP spoofing, there will be spurt of ARP messages.

What I am arguing is that there are patterns and we should be able to train ML models to recognize these patterns. I am suggesting that we should use both .pcap data and SCADA data to train the model. I am still not sure how to represent the input for ML model. Maybe we can take data of say, 5 seconds from both and somehow convert them into a usable vector or matrix.

ML data model for anomaly/attack detection:

For each second we will count total packets of each type and take sensor values

TCP	TCP-SYN	ARP	ENIP	…. PLC1	PLC2	PLC3 ….	Classification
3	1	0	2	5.2	0.3	3.1	Normal
2	1	0	1	5.1	0.2	3.5	Normal
9	5	1	3	3.2	0.1	2.1	DoS
3	2	1	2	4.2	0.2	3.2	MITM

Then we will split the data with each split having 5 or 10 rows. Each split will have 1 classification - classified as normal if all rows are normal, otherwise classify as DoS, MITM or packet loss based on the nature of anomalies/attack.

What do we aim to achieve with the ML model:
We want to train a model that will be able to take packet count and sensor data of every 5 or 10 seconds and will be able to detect normal/attack scenario.

This will allow us near real time detection.
This will allow us to introduce an HMI node with real time monitoring. HMI node will allow us to introduce new attack scenarios.

Attack prevention:
The original paper only discusses attack detection. So new work can be done on the prevention front.

Since CIP protocols use authentication, it is not as vulnerable as other industrial protocols like modbus.

But it is still vulnerable to attacks like DoS and MITM.

I am thinking about introducing packet filtering firewalls to mitigate MITM/ARP spoofing attacks since static ARP does not seem feasible.

For DoS attack also I am thinking about firewall based solution, setting custom/appropriate rules.

I was thinking, whether SDN based solution for routing is feasible in these kinds of industrial network.

Other possible attacks:
Replay attack might be used. But it appears to be like MITM.

Stealth command modification attack. The stealth command modification attack is a combination of replay attack and man-in-the-middle attack. It is discussed in paper [3].

Paper [3] also discusses PLC worm virus. This would be a good attack if can be implemented.

Paper[4] discusses package payload alteration and ICMP flood. This paper focuses on deep packet inspection to detect attacks.

Any previous work on this?

I have read two papers [1], [2] that deal with ML and smart water grid, Both use historic SCADA data, but not the network messages. Both these papers use same C-Town data available publicly. Both of these paper rathers focus on different ML algorithms and comparisons of results achieved using those algorithms.

[1] Real-Time Identification of Cyber-Physical Attacks on Water Distribution Systems via Machine Learning–Based Anomaly Detection Techniques. URL: https://ascelibrary.org/doi/10.1061/%28ASCE%29WR.1943-5452.0001023

[2] Attack detection in water distribution systems using machine learning . URL: https://hcis-journal.springeropen.com/articles/10.1186/s13673-019-0175-8

[3] Review of PLC Security Issues in Industrial Control System. URL https://www.techscience.com/JCS/v2n2/39507/pdf

[4] Deep packet inspection for intelligent intrusion detection in software-defined industrial networks: A proof of concept. URL: https://academic.oup.com/jigpal/article-abstract/28/4/461/5691244?redirectedFrom=fulltext