Combining Physical and Network Data for Attack Detection in Water Distribution Networks

Côme Frappé, Pierre Parrend

engineering proceedings

MDPI

Proceeding Paper

COMBINING PHYSICAL AND NETWORK DATA FOR ATTACK DETECTION IN WATER DISTRIBUTION NETWORKS†

Côme Frappé - - Vialatoux[1,2,*], Pierre Parrend[1,2]

1 ICube - Laboratoire des sciences de l'ingénieur, de l'informatique et de l'imagerie UMR 7357, Université de Strasbourg, Strasbourg 67000, France ; come.frappe-vialatoux@etu.unistra.fr, pierre.parrendl@epita.fr
2 Laboratoire de Recherche de l'EPITA, EPITA, Le Kremlin-Bicêtre 94270, France ;
* Correspondence: come.frappe-vialatoux@etu.unistra.fr
† Presented at 3rd International Joint Conference of Water Distribution Systems Analysis & Computing and Control for the Water Industry (WDSA/CCWI 2024), Ferrara (Italy), 1–4 July 2024.

Abstract: Water distribution infrastructures are increasingly incorporating IoT in the form of sensing and computing power to improve control over the system and achieve greater adaptability to the water demand. This evolution, from physical towards cyber physical systems, comes with an attack perimeter extended from physical infrastructure to the cyberspace. Being able to detect this novel kind of attacks is gaining traction in the scientific community. Machine learning detection algorithms, which are showing encouraging results in cybersecurity applications, are leveraging the increasing amount of datasets published in the water distribution community for better attack detection. These datasets also begin to reflect this novel cyberphysical aspect in two ways, first by conducting cyberattacks against the testbed infrastructures during the data acquisition, and second, by including network traffic data along with the physical data captured during the experimentations. However, current machine learning models do not fully take into account this cyberphysical component, being only trained either on the physical or on the network data. This paper addresses this problem by providing a multi-layer approach to applying machine learning to cyberphysical systems, by combining physical and network traffic data and assessing its effects on attack detection performances of machine learning algorithms as well as its cross impact with data enriched with graph metrics.

Keywords: Cyber-physical systems, security, Machine learning

Citation: To be added by editorial staff during production.

Academic Editor: Firstname Lastname

Published: date

1. Introduction

The role of water distribution infrastructures to provide access to water is crucial to society, as it is both a vital need and amongst the most used resource in the industry. This importance places these infrastructures as part of the critical system family, which implies the highest level of resilience, security and reliability. To meet these requirements, a modernization effort is being conducted on water distribution infrastructures in the vein of industry 4.0 that allows for better monitoring, adaptability and control over the system. This transformation effectively places water distribution infrastructures in the category of the Cyber-Physical Systems (CPS), in that they are composed of a physical layer dedicated to the handling of water, and a cyber layer that supports the communication of the components of the physical layer. However, this increase in connectedness is expanding the attack perimeter of water distribution infrastructures significantly and exposes it to the threat of cyber-attacks [1]. These new threats motivate the need for more accurate detection models, for which Machine Learning (ML) algorithms gained attention for their

promising results. Still, the current use of ML algorithms for attack detection has yet to be adapted to the specific architecture of a CPS by integrating the physical and cyber layers [2]. Recent work from the literature introduces a combination method based on model aggregation [3]. However, while showing promising results, its reliance on numerous models in parallel imply a custom fit for the CPS architecture as well as high computational costs.

This paper describes a general approach for combining physical and network data of a CPS, allowing ML algorithms to be trained on data that capture the interactions between the multiple layers of the systems.

The remainder of the paper presents the combination approach and the experimental setup in section 2, the results are reported in section 3 and discussion and conclusion are given in section 4.

2. Materials and Methods

2.1. Data Combination Process

The combination process requires both the physical data and the network traffic data to have the time of acquisition, and to have been acquired during the same timeframe. As observed in CPS open datasets in the water distribution field, the physical data's acquisition frequency is lower than that of the network data, usually with an acquisition each second versus acquisition at the millisecond scale for network data. To allow for a conjoint use of these data, a synchronization process is required consisting of concatenating the most recent anterior physical data to each network data entry. The complete combination pipeline for static data is shown in Figure 1. The first step for both data types accounts for cases when the data are separated into multiple files. This step results in all network data as one file, and all physical data as another file, from which we remove lines with only missing values. The next step creates a common time column with an identical granularity for both files, corresponding to the physical data's time granularity. This allows for a left join of the physical data on to the network data, based on this common time column just created. This column is then removed, and the eventual network data that do not have physical data corresponding to their acquisition time are treated via filling with the most recent anterior physical data.

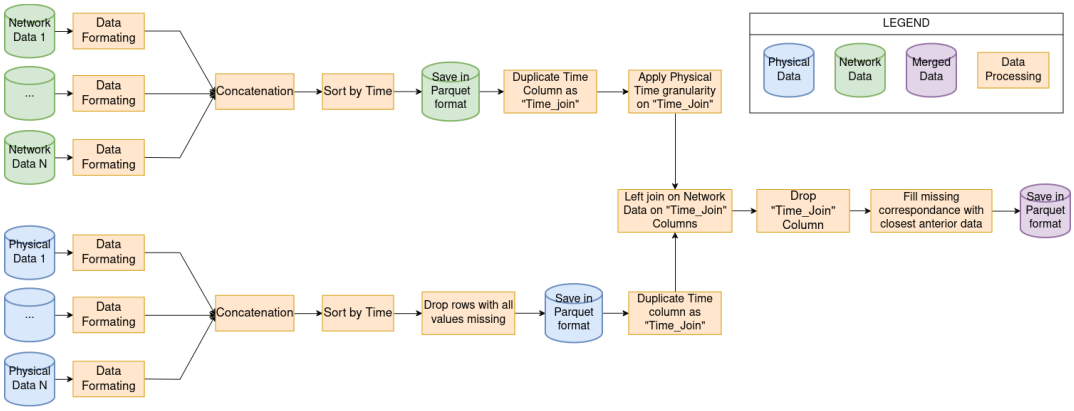

Figure 1: Complete pipeline of the combination process

2.2. Experimental Setup

To assess the performance of the proposed combination, we benchmark the proposed process on the Hardware-In-The Loop (HITL) dataset [4]. This experiment consists of training 4 different machine learning algorithms, namely Decision Tree, Random Forest, XGBoost and Multi-Layer Perceptron (MLP) respectively on physical data, network data, network data enriched with graph metrics, and on the data obtained by applying

proposed combination. The graph metrics are computed on two graphs generated from network data, with edges representing communication between nodes consisting of MAC_Source and MAC_Destination for the first graph, and consisting of the unique combinations of MAC_Source + Source_Port and MAC_Destination + Destination_Port for the second. These graphs are constructed over time windows of one and five minutes and used to compute the following metrics: number of edges, number of nodes, average degree and density.

The hardware used to run the experiment is a laptop with 32Gb of RAM, 13th Gen Intel® Core™ i7-13700H 20 cores CPU, NVIDIA RTX A500 GPU. The operating system is Ubuntu 22.04.3 LTS. Evaluations are run using Python 3.11.4 and the libraries pandas (2.0.2), numpy (1.25.1), scikit-learn (1.2.2), xgboost (1.7.6) and keras (2.13.1). As the available RAM is limited, network data are reduced in size by keeping only one instance of each unique packet at each second and adding the count of duplicates in a new column.

3. Results

The detection performance of the models shows a benefit associated with the use of the proposed data combination for all models except Random Forest.

Figure 1: Balanced Accuracy performance of models for all data configurations

The detection performance, using balanced accuracy metric for each model on the different data configurations, is shown in Figure 1. The best results are obtained with XGBoost algorithm on the combined data with 99.84% balanced accuracy. Table 1 shows that the addition of graph metrics to network data greatly improved detection performances of Physical Fault and MITM respectively from 0% to 77% and from 1% to 88% of True Positive Rate, however, it led to a decrease of 8.70% TPR in the detection of the Scan label on combined data. A possible explanation is that the addition of graph data adds less qualitative information for the detection of this specific label than the network data alone do provide, thus diluting the useful information and resulting in a harder detection task. The overall improvement of detection performances also reflects on the False Positive Rate as shown in Table 2, which is especially relevant in attack detection where false alarms have costs in terms of time and resources spent on irrelevant investigation in addition to the impact on the personnel through the effect of alarm fatigue [5].

Data	Model	TPR Normal	TPR DoS	TPR MITM	TPR Physical Fault	TPR Scan
Physical	XGB	99.21%	96.88%	88.56%	95.48%	0.00%
Network	XGB	99.90%	97.50%	1.41%	0.01%	100.00%
Network+Graph	XGB	98.04%	99.51%	88.69%	77.43%	87.50%
Combined	XGB	99.91%	99.94%	99.74%	99.62%	100.00%
Combined+Graph	XGB	99.96%	99.96%	99.77%	99.67%	91.30%

Table 1: True Positive Rates of XGBoost

Data	Model	FPR DoS	FPR MITM	FPR Physical Fault	FPR Scan
Physical	XGB	0.031%	0.505%	0.164%	0.000%
Network	XGB	0.066%	0.043%	0.000%	0.000%
Network+Graph	XGB	0.011%	0.755%	0.984%	0.000%
Combined	XGB	0.003%	0.036%	0.036%	0.000%
Combined+Graph	XGB	0.002%	0.016%	0.020%	0.000%

Table 2: Per attack False Positive Rate of XGBoost

4. Discussion and conclusion

The proposed approach for data combination improves the performances of machine learning models on attack detection task in CPS by having the training data capture the interactions between the physical and network subsystems. The addition of graph metrics to network data has a positive effect on performance compared to using network data without graph metrics, however, adding graph metrics to combined data lowered the detection performance. A possible explanation for this lowered detection performance is that graph metrics contain less qualitative information than the combined data itself, which makes the high-quality information more diluted in the data and thus harder for the models to learn. This work proves a promising approach for integrating the network and physical parts of a CPS for machine learning based detection.

Author Contributions: Conceptualization, C.FV. and P.P.; methodology, C.FV. and P.P.; software, C.FV.; validation, C.FV. and P.P.; formal analysis, C.FV.; investigation, C.FV.; resources, P.P.; data curation, C.FV.; writing—original draft preparation, C.FV.; writing—review and editing, C.FV. and P.P.; visualization, C.FV.; supervision, P.P.; project administration, P.P.; funding acquisition, P.P. All authors have read and agreed to the published version of the manuscript.

Funding: This work is funded by French ANR under grant ANR-22-CE39-0010 for Correau Project.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article

References

1. Tuptuk, N.; Hazell, P.; Watson, J.; Hailes, S. A Systematic Review of the State of Cyber-Security in Water Systems. *Water 2021*, 13, 81, doi:10.3390/w13010081.
2. Ahmed Jamal, A.; Mustafa Majid, A.-A.; Konev, A.; Kosachenko, T.; Shelupanov, A. A Review on Security Analysis of Cyber Physical Systems Using Machine Learning. *Materials Today: Proceedings 2023*, 80, 2302–2306, doi:10.1016/j.matpr.2021.06.320.
3. Faramondi, L.; Flammini, F.; Guarino, S.; Setola, R. A Hybrid Behavior- and Bayesian Network-Based Framework for Cyber–Physical Anomaly Detection. *Computers and Electrical Engineering 2023*, 112, 108988, doi:10.1016/j.compeleceng.2023.108988.
4. Faramondi, L.; Flammini, F.; Guarino, S.; Setola, R. A Hardware-in-the-Loop Water Distribution Testbed Dataset for Cyber-Physical Security Testing. *IEEE Access 2021*, 9, 122385–122396, doi:10.1109/ACCESS.2021.3109465.
5. Deb, S.; Claudio, D. Alarm Fatigue and Its Influence on Staff Performance. *IIE Transactions on Healthcare Systems Engineering 2015*, 5, 183–196, doi:10.1080/19488300.2015.1062065.