2nd International Joint Conference on Water Distribution Systems Analysis & Computing and Control in the Water Industry
Valencia (Spain), 18-22 July 2022
doi: https://doi.org/10.4995/WDSA-CCWI2022.2022.14793

A THOROUGH CYBERSECURITY DATASET FOR INTRUSION DETECTION IN SMART WATER NETWORKS

Andrés F. Murillo[1], Riccardo Taormina[2], Nils Ole Tippenhauer[3] and Stefano Galelli[4]

[1]Singapore University of Technology and Design, Singapore
[2]Delft University of Technology, Delft, Netherlands
[3]CISPA Helmholtz Center for Information Security, Saarbrücken, Germany
[4]Singapore University of Technology and Design, Singapore

[1]andres_murillo@sutd.edu.sg, [2]r.taormina@tudelft.nl, [3]tippenhauer@cispa.de, [4] stefano_galelli@sutd.edu.sg

Abstract

The increase in the number and complexity of cyber-physical attacks on water distribution systems requires better intrusion detection systems. So far, the design and validation of such systems has relied on datasets, such as the EWRI 2017 BATtle of the Attack Detection ALgorithms (BATADAL), that provide a detailed representation of hydraulic processes in response to cyber-physical attacks. However, the BATADAL, generated with epanetCPA, does not include an equivalent and detailed representation of the processes occurring within the industrial communication system. Here, we fill in this gap by presenting the BATADAL 2.0 dataset, generated with the DHALSIM simulator, a novel co-simulation environment that can represent the hydraulic processes, digital control, and network communication of smart water networks. The dataset includes a broad variety of attacks and network anomalies. Most importantly, the availability of both process and network data is expected to pave the way to more advanced and accurate detection algorithms.

Keywords
Cyber-security, cyber-physical security, cyber-attacks, DHALSIM, water distribution systems, smart water networks, BATADAL, dataset, SCADA.

1 INTRODUCTION

With the widespread digitalization of the water sector, the world is witnessing an increasing trend in the number and complexity of cyber-physical attacks against critical water infrastructures [1]. This trend requires extra measures to harden smart water networks so that they can operate in a hostile cyber-security environment. Such hardening includes the integration of intrusion detection and protection mechanisms into the infrastructure management systems. Designing such mechanisms usually requires vast amounts of data that represent the behaviour of both physical and cyber layers during normal and under attack conditions.

In recent years, researchers and practitioners used the EWRI 2017 BATtle of the Attack Detection ALgorithms (BATADAL) dataset generated with epanetCPA to develop intrusion detection techniques for water distribution systems [2]. While tools like epanetCPA [3] or RISKNOUGHT [4] can simulate the response of physical processes to cyber-physical attacks, they are not able to replicate traffic data in the cyber layer of smart water networks. Yet, complementing process data with features extracted from network traffic would enable the development of advanced attack detection and localization techniques discovering anomalies across the entire cyber-physical system [5].

In this work, we fill this gap by presenting an open dataset generated by the Digital HydrAuLic SIMulator (DHALSIM) simulator [5]. DHALSIM is a novel co-simulation environment that can represent the hydraulic processes, digital control, and network communication of smart water

networks by interfacing EPANET with miniCPS, an industrial control network emulator. DHALSIM thus outputs both process variables (e.g., pressures, water levels, flows) as well as records of packet data pulled from network scans (e.g., PCAP files). The proposed dataset "extends" the BATADAL dataset by implementing similar attacks on the C-Town benchmark system, with data on both normal operating conditions and anomalous conditions. The normal operating conditions were generated using multiple demand patterns, tank initial water levels, sensor noise, as well as small network events (e.g., loss of packets in the communication networks) that better resemble the real operation of water distribution networks. The anomalous conditions include not only malicious cyber-physical attacks, but also benign anomalies, such as disruptive network events.

In the remainder of the manuscript, we first introduce DHALSIM (Section 2) and describe the experimental setup for the generation of the dataset (Section 3). We then illustrate key aspects of the dataset (Section 4) and briefly outline the way forward (Section 5).

2 THE DIGITAL HYDRAULICSIMULATOR (DHALSIM)

DHALSIM is a simulation environment that combines the hydraulic simulation capabilities of EPANET with the network emulation capabilities provided by MiniCPS [6] and Mininet [7]. Mininet is a virtualization platform that allows users to easily create virtual networks to connect virtualized guests (or Mininet nodes). These virtual nodes have their own virtual network interfaces and can run any software installed in the host machine. MiniCPS is built on top of Mininet and provides an implementation of popular ICS communication protocols. DHALSIM uses MiniCPS and Mininet to create virtual industrial control networks. These virtual networks are composed of Mininet nodes and virtual network links. The Mininet nodes represent PLCs or SCADA and communicate using industrial communication protocols. As for the physical system, DHALSIM launches a process running an EPANET process simulation. Finally, DHALSIM experiments can simulate cyber-physical attacks or network events that impact the behaviour of the industrial communication layer, and, as a consequence, also impact the underlying physical processes.

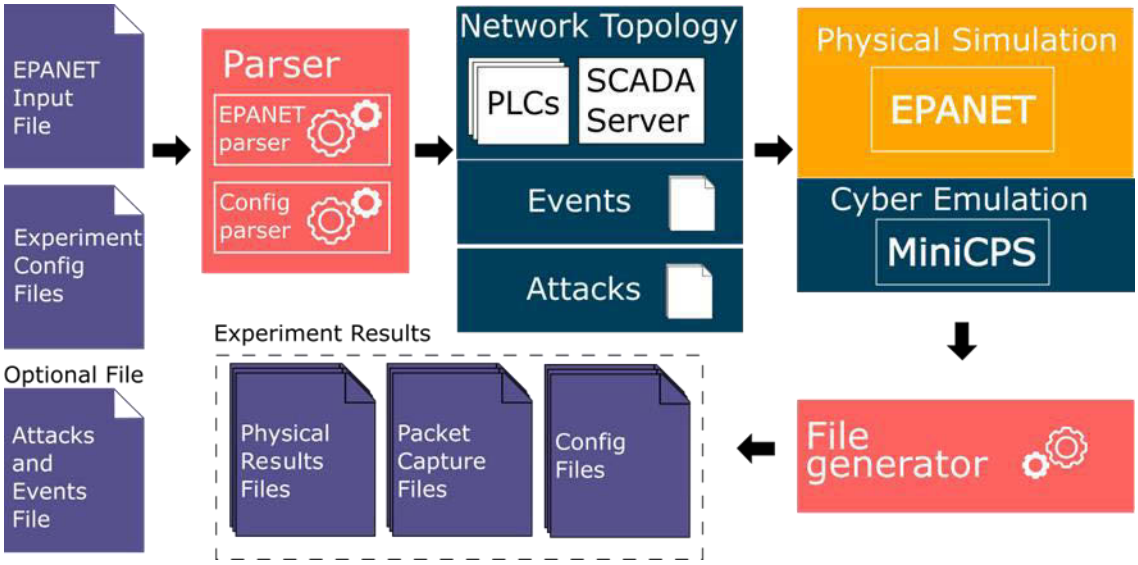

Figure 1. DHALSIM architecture. DHALSIM uses EPANET to simulate hydraulic processes and MiniCPS to emulate the cyber physical system.

The main components of DHALSIM include a parser, a physical simulator, a cyber emulator, and a file generator (Figure 1). Experiments in DHALSIM run in the following way: first, the configuration files are created for the experiment. Second, the Parser reads these configuration files and creates a Mininet network and concurrently launches a process to run the physical

simulation. The Mininet network consists of Mininet nodes, running scripts with the behaviour of PLCs, or SCADA, and network links connecting these nodes. On the other hand, the physical simulation is an EPANET instance running in a step-by-step fashion. Third, during the simulation, different events or attacks can be launched. The experiment ends when the end of the physical simulation is reached, and the resulting output files are stored.

Three types of input files are used to launch an experiment:

- EPANET Input file: this is the EPANET input file of the water distribution used in the simulation.
- Experiment configuration files: two files constitute the configuration files. The first one is the general config file, which defines global parameters such as the path to the EPANET input file, the number of hydraulic time step iterations the experiment will run for, the type of simulation used (demand-driven or pressure-driven), and the paths to additional configuration files.
- Optional attacks and events files: DHALSIM can process these optional files in order to launch cyber physical attacks or network anomalies during an experiment. Network anomalies are network events that affect the way a network link behaves. For example, users could launch anomalies that cause a percentage of packets to be lost at a network link, or a network delay between each packet being sent. Cyber-physical attacks can be of two types: PLC attacks or network attacks. The former force a PLC to operate hydraulic actuators (such as pump) in a way that ignores the system control rules, while the latter launch an additional network node that executes a script running the network attack.

3 EXPERIMENTAL SETUP

The objective of DHALSIM is to provide a co-simulation environment for water distribution systems that combines physical simulation with network emulation capabilities. Providing network emulation is important, because the network behaviour might affect the physical response of a water distribution system. Using DHALSIM, we generated a dataset with 52 weeks of simulation of the C-Town water distribution system under normal operating conditions. In addition, the dataset contains 8 more weeks of network anomalies and cyber physical attacks. Here, we first describe the benchmark water distribution system and then illustrate the cyber-physical attacks included in the dataset.

3.1 CASE STUDY: C-TOWN AND BATADAL

To create the dataset, we began by extending the traditional C-Town topology to include 9 PLCs controlling the system behaviour, as illustrated in [2,5]. Figure 2 shows the resulting C-Town cyber physical system. The left panel illustrates the topology of the water distribution system along with the location of the PLCs controlling the system. The right panel illustrates the corresponding network topology deployed in MiniCPS. In the network topology, each PLC is located in a local area network, and all local networks are connected through a central router. In addition, a SCADA server is located at another substation. This SCADA server polls all the PLCs for information regarding the physical state of the system.

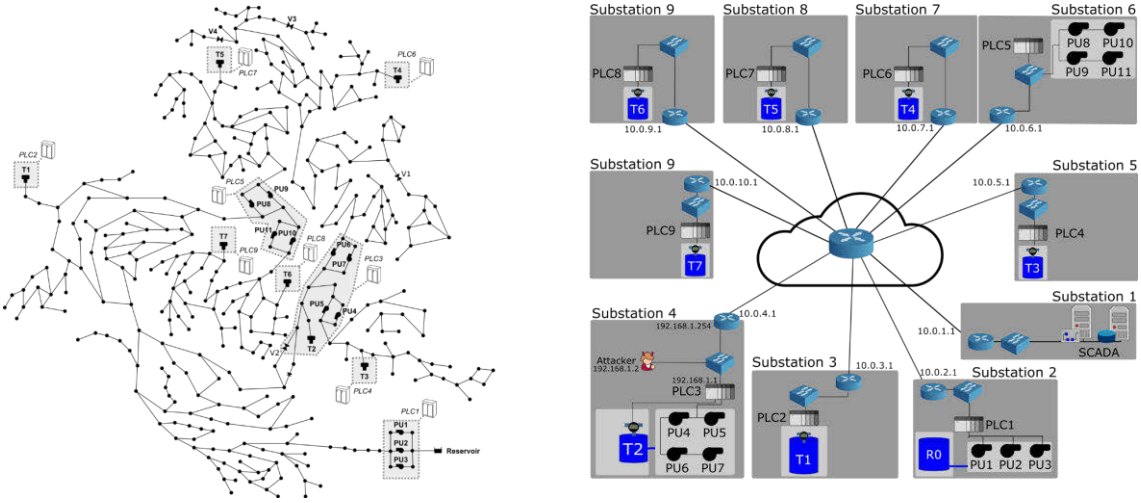

Figure 2. C-Town Cyber-physical system. The left panel shows the topology of the water distribution system. The right panel shows the network topology and the local area networks with PLCs, sensors, and actuators

As mentioned above, the dataset presented in this paper is inspired by the BATADAL [2], which we aim to extend by providing a thorough representation of both physical and cyber processes. The no attack conditions were generated using 52 different weekly demand patterns, with a pattern timestep of 15 minutes. In addition, for each week, different initial tank level conditions were configured. Finally, for each week, we introduced small network benign anomalies in the links connecting all PLCs and SCADA. These included a percentage of packet loss lower than 1% and a network delay of less than 30ms in all links (thus representing typical operating conditions of the cyber layer). We run all simulations using a hydraulic timestep of five minutes, and by resorting to pressure-driven hydraulic simulations [8] with EPANET 2.2 and epynet, a Python wrapper developed by Vitens[1].

3.2 CYBER-PHYSICAL ATTACKS AND NETWORK ANOMALIES

In addition to the 52 normal operating conditions, we ran 8 weeks of simulation under cyber-physical attacks and network anomalies. All simulations were run using the hydraulic boundary conditions of Week 6, to compare the physical and network impact of the anomalies under the same physical and network conditions (i.e., tank levels, demand patterns, percentage of packet loss, and network delay). Table 1 shows the details of the simulated attacks and benign anomalies, collectively named anomalies for simplicity. We grouped the four types of anomalies reported in Table 1 with respect to two different effects (or objectives). All the anomalies with an odd ID number may cause Tank T3 to run empty, while all anomalies with an even ID number may cause Tank T3 to overflow.

Attack ID	Duration (hours)	Anomaly Description	Anomaly Type	Objective/Effect
1	31	MiTM on PLC4 to manipulate T3	MiTM Attack	Empty T3
2	31	MiTM on PLC4 to manipulate T3	MiTM Attack	Overflow T3

[1] https://github.com/Vitens/epynet

3	31	Malicious activation Pump PU4	PLC Attack	Empty T3
4	31	Malicious activation Pump PU4	PLC Attack	Overflow T3
5	31	DoS on PLC3	Dos Attack	Empty T3
6	31	DoS on PLC3	Dos Attack	Overflow T3
7	31	Network anomaly on PLC3	Network Anomaly	Empty T3
8	31	Network anomaly on PLC3	Network Anomaly	Overflow T3

Table 1. Attack details. The attacks have two objectives, that is, to empty or to overflow Tank 3. The acronyms MiTM and DoS refer to Man-in-The-Middle and Denial-of-Service respectively.

Figure 3 shows an overview of the events run during these experiments. The first anomaly (top left panel) is a Man-in-the-Middle attack (MiTM). In this case, an attacker manipulates the sensor readings reaching a PLC. Specifically, the attacker manipulates Tank T3 readings sent by PLC4 and received by PLC3. Since PLC3 activates Pumps PU3 and PU4 (according to the T3 reading), this manipulation can cause PLC3 to make the wrong control decision, emptying or overflowing the tank. The second anomaly (top right panel) is a PLC attack. An attacker gains control of PLC3 and causes a malicious activation of Pump PU4. This manipulation can lead PU4 to being closed or open during the entire anomaly duration, causing Tank T3 to empty or overflow. The third anomaly (bottom left) is a Denial-of-Service Attack (DoS). In this attack, the attacker intercepts Tank T3 readings destined to PLC3, causing these messages not to be received by PLC3. This causes PLC3 to operate the pumps with outdated information. That is, Pumps PU3 and PU4 are activated with the last value before the attack was launched. Depending on the state of the system (T3 emptying or filling), this might cause T3 to empty or overflow. Finally, the fourth anomaly (bottom right) is a Network Anomaly. In this case, there is no attacker present, and the anomaly causes PLC3 to be disconnected from the network and to stop receiving updates on Tank T3 water level. This causes a similar physical response to the previously describe DoS attack.

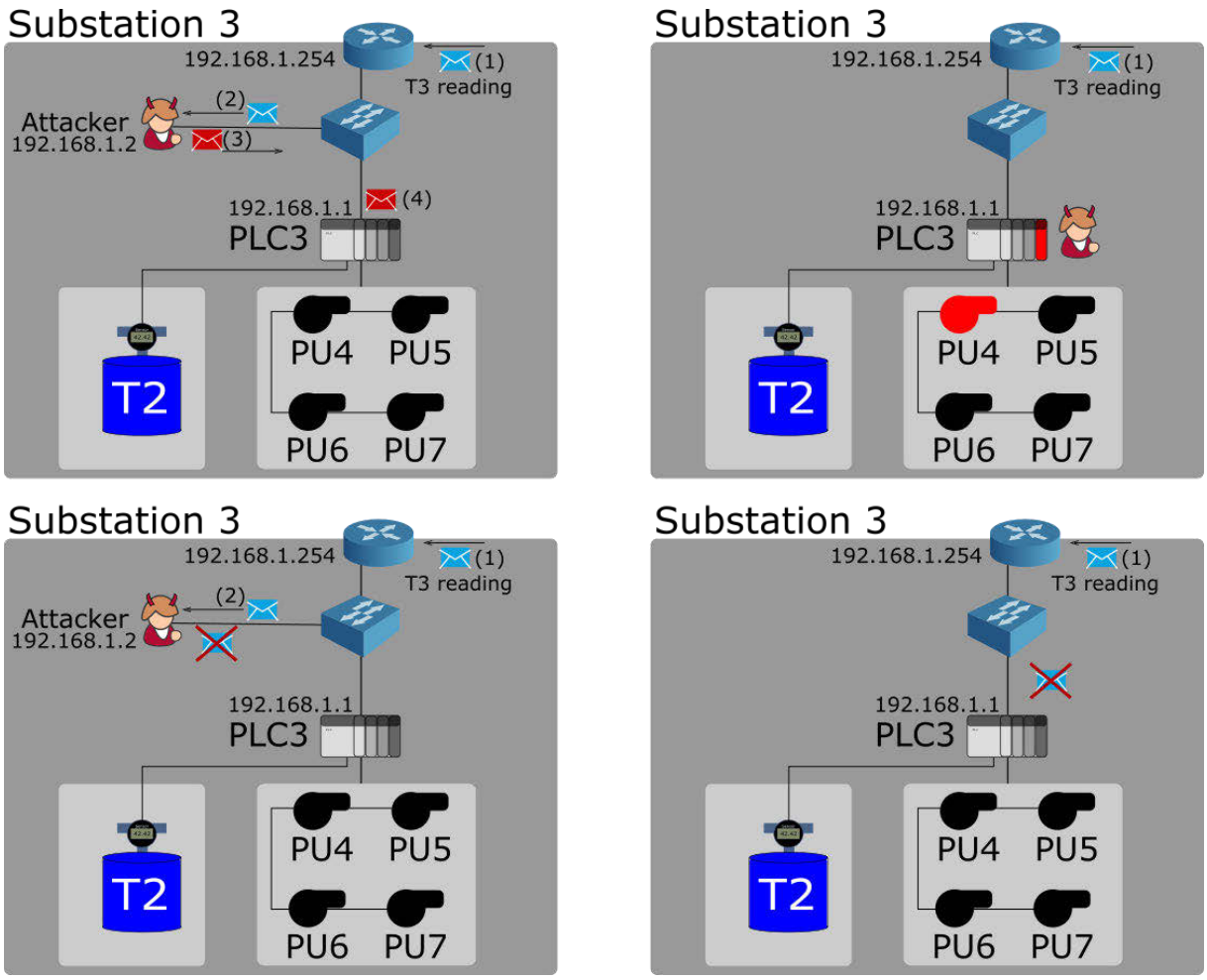

Figure 3. Cyber-physical attacks and network anomalies used in the experiments. All anomalies have PLC3 as the target. The top left panel shows a Man-in-the-Middle Attack. The top right panel shows a PLC attack. The bottom left panel shows a Denial of Service attack. Finally, the bottom right panel shows a network anomaly.

4 KEY FEATURES

4.1 ANALYSIS OF NETWORK DATA

In addition to the physical results, DHALSIM generates network captures of all the messages exchanged between PLCs and SCADA during the simulation. DHALSIM has the capability to generate these files, because MiniCPS and Mininet offer a full implementation of common industrial protocols used in cyber-physical systems, including water distribution systems. Figure 4 shows a screenshot of a CIP2 packet dissection carried out with the network analyzer Wireshark. The dissected message was received by PLC3 and sent by PLC4 (PLC4 has an outbound IP of 10.0.5.1). This particular message carries the value of Tank T3 level. The general information of this message is highlighted in the black box in the figure. In addition, the blue box highlights the stack of protocols supporting the CIP protocol. These are: Ethernet, IIP, TCP, and ENIP. Finally, the dissection shows additional details of the CIP message, including the hexadecimal reading of the tank level (highlighted in red). This value is decoded by the MiniCPS library into the float value reported by sensor T3. Accurately generating this network information is important because the

[2] The Common Industrial Protocol (CIP) is a common industrial protocol for industrial automation applications.

network behaviour can have impacts on the physical system. In a similar way, network information can help identify the root cause of physical anomalies or cyber-physical attacks.

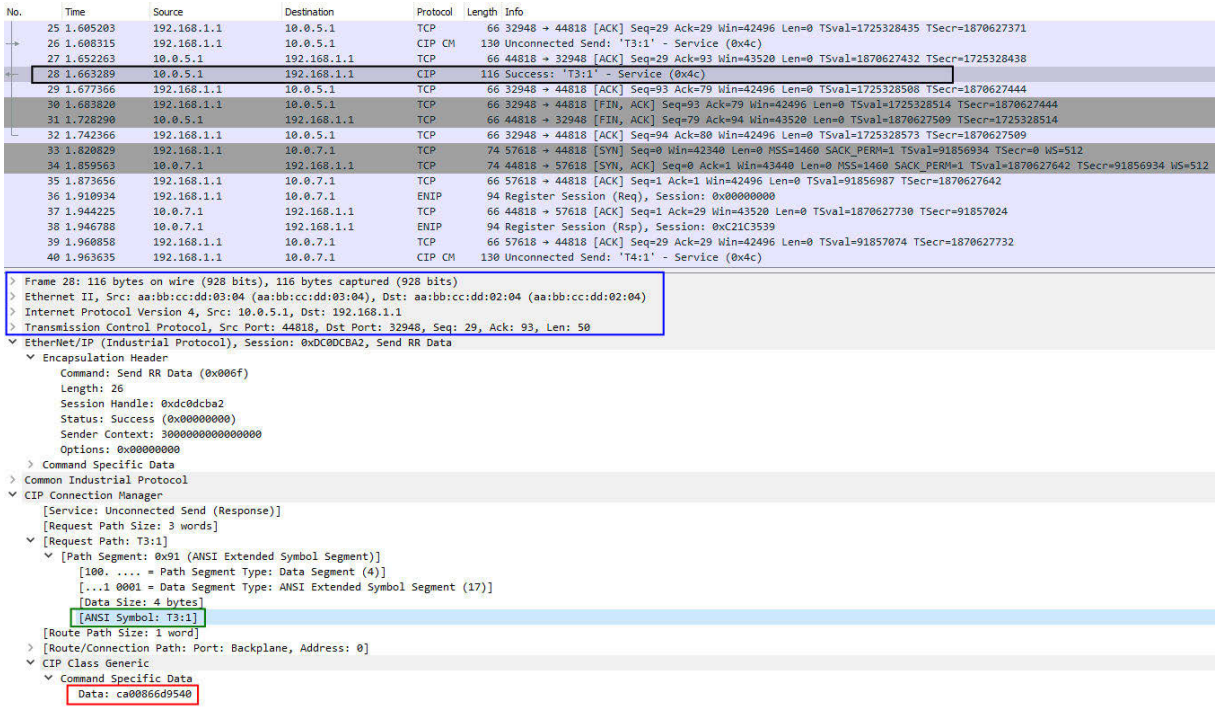

Figure 4. Wireshark packet retrieved for one of the routers in C-Town. The dissected packet shows a CIP packet and its payload (i.e., the value of Tank 3 level, black/green boxes). The message also shows the stack of protocols supporting CIP (blue box) and the hexadecimal reading of the tank level (red box).

Recall that DHALSIM generates both physical and network data. For the physical data, the model creates one file with ground truth values and one file with SCADA values. The former contains the values of variables handled by the EPANET simulator, namely, tank level, pressure at junctions, status and flow of valves and pumps, time-stamp, and a variable indicating the status of the water system (i.e., normal operating conditions or under attack / anomaly). The latter stores the values of the variables received by the SCADA server (as specified in the PLCs configuration files). Both files have a *.csv* format. For a single one-week simulation they have a size of about 20 MB. As for the network data, DHALSIM creates one network capture file for each PLC and SCADA server. Such file stores all network messages sent and received by that node in *.pcap* format, which allows software libraries to retrieve and process the network packets. In our case, the *.pcap* files processing is carried out with a software library named *scapy*. In addition to *scapy*, we used two specific parsers for ENIP and CIP messages [9]. For a single one-week simulation, a PLC *.pcap* file has a size of 30MB.

4.2 NO ATTACK CONDITIONS

Figure 5 shows the envelope of variability of the 52 weeks of normal operating conditions for the water levels of Tanks T1. The envelope of variability was calculated by obtaining the minimum and maximum value at each iteration (or hydraulic timestep). The behaviour of the envelope is explained by the different initial conditions (tank levels) and by the different demand patterns, as those are the ones driving the system behaviour. The blue line highlights the trajectory of the water level in T1 for Week 6.

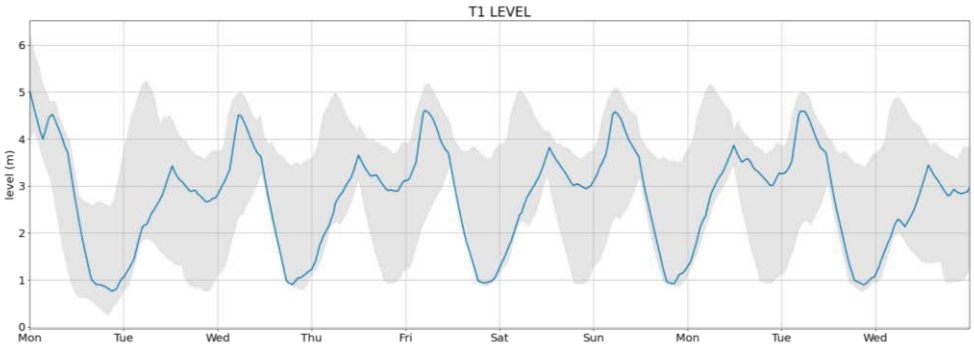

Figure 5. Envelop of variability for Tank T1 for all normal conditions. For the 52 weeks of normal operating conditions, different initial tank levels and demand patterns were used. The blue line shows the trajectory of the water level in T1 for Week 6.

4.3 PHYSICAL AND NETWORK RESULTS OF THE ANOMALIES

The main objective of all the anomalies presented in this dataset is to show how DHALSIM extends the type of data included in the BATADAL dataset. Since DHALSIM has network emulation capabilities, similar anomalies in the physical processes may derive not only from different cyber-physical attacks, but also from benign network anomalies.

The results of the anomalies are shown in Figures 6 and 7. In particular, Figure 6 shows the physical and network results of all the anomalies resulting in an empty T3, while Figure 7 shows the physical and network results of all the anomalies leading to an overflow in T3. Beginning with Figure 6, the left panels show the water level of Tanks T1 and T3 during the weeks featuring different anomalies. The anomalies occur during the grey highlighted area in the plots. The figure shows that the physical responses are similar for almost all the anomalies, except for the PLC3 Attack. The process followed by the victim PLC in all anomalies can be summarized as follows: for Anomaly 1 (MiTM Attack), PLC3 receives a modified value of T3. This modified value (7.0m), causes PLC3 to turn off both pumps (PU3 and PU4) and as a consequence, empties T3. For Anomaly 3 (PLC Attack), the PLC3 operates maliciously on PU4, causing its shut down. Note that PU3 keeps working normally and, consequently, Tank T3 does not run empty, although water levels are lower than expected. Anomalies 5 and 7 have a similar physical effect—PLC3 stops receiving updated information regarding T3 and does not activate the pumps properly. By timing the beginning of these anomalies, we can control whether the tank will be emptied or overflown.

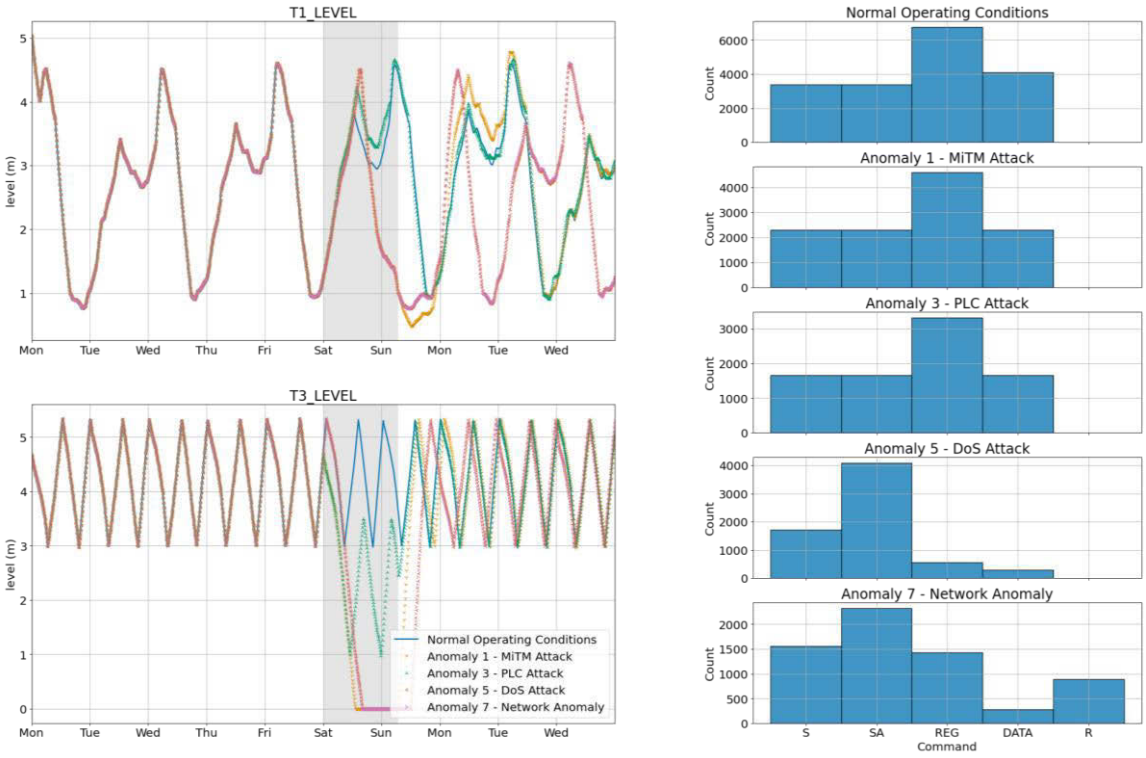

Figure 6. The panels on the left show the water tank levels of Tank T1 and T3. All physical responses are similar, but the anomalies used to obtain them have different vectors. The panels on the right show a histogram of the number of messages received by PLC3 during the anomalies.

The right panels of Figure 6 show a histogram of the different types of Command messages received by PLC3 during the anomalies. A "Command" is a network feature extracted using the libraries specified in Section 4.1. This feature indicates the objective or type of network message. For example, a TCP-SYN message (a special type of message used by the TCP protocol to establish a network connection), would receive the "Command" value of "S". An "SA" is the acknowledgement of an "S" message. "REG" messages are messages requesting for a sensor or actuator reading. "DATA" messages are the messages carrying the sensor or actuator readings, and "R" messages are messages sent when a connection is abruptly closed or cannot be established. The network behaviour depends on the type of anomaly generated, as the panels show. For example, for Normal operating conditions and anomalies 1 and 3 there are no changes in the patterns of the packets received by PLC3. This is because the PLC attack does not generate changes in the network patterns. Instead, PLC3 operates Pump PU4 ignoring the configured control rules. In a similar way, Anomaly 1 (MiTM Attack) simply manipulates the payload of the messages with the T3 readings—all other messages and communication behaviour are unaffected.

The more significant network differences happen with anomalies 5 and 7. The DoS attack causing anomaly 5 stops PLC3 from receiving all "REG" and "DATA" commands. This happens because the DoS stops all messages arriving at PLC3; the attacker drops even the messages that are sent back by the switch connected to PLC3. In anomaly 7, the network issue happens between the router and the PLC3, which allows for some messages to reach PLC3. Nevertheless, PLC3 has a significant drop in the "DATA" messages received and "R" messages are sent by the PLC3, because none of the TCP connections are established successfully. We can draw similar conclusions by analysing the remaining four anomalies in Figure 7.

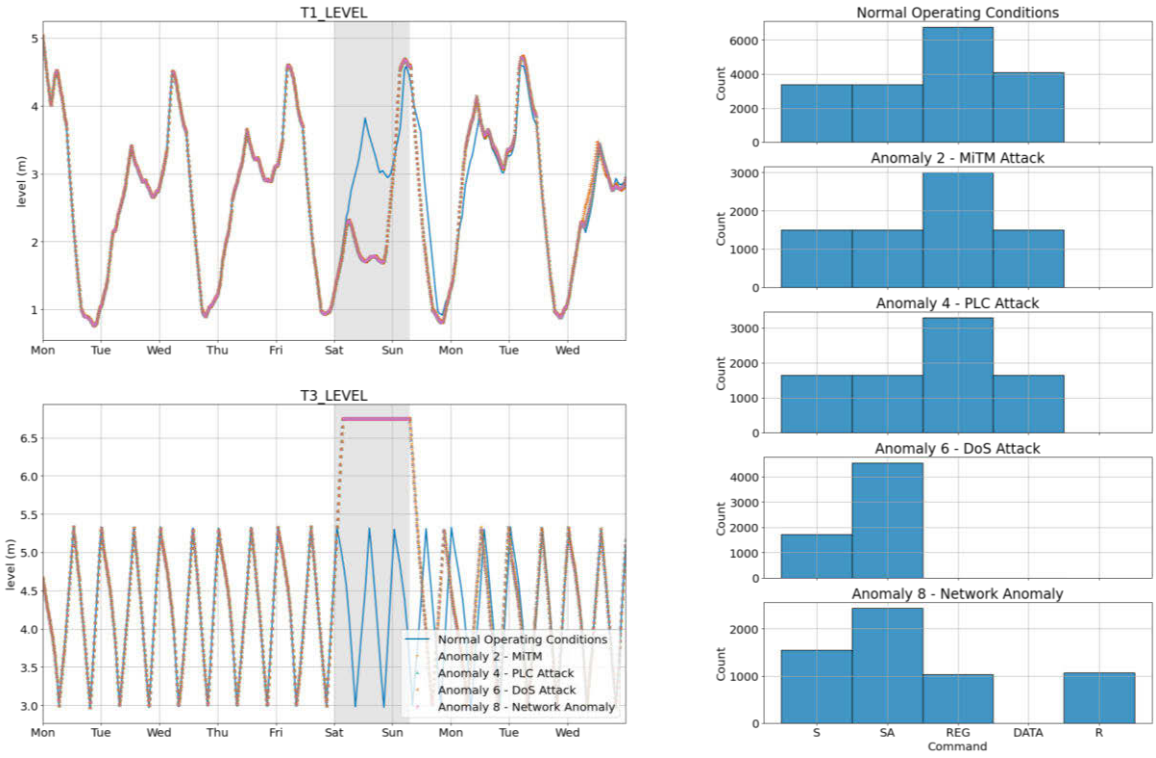

Figure 7. The panels on the left show the water levels of Tanks T1 and T3. All physical responses are similar, but the anomalies used to obtain them have different vectors. The panels on the right show a histogram of the number of messages received by PLC3 during the anomalies.

5 OUTLOOK

This paper presents the first version of the BATADAL 2.0 dataset generated with the DHALSIM simulator. As explained above, our ultimate goal is to provide a thorough dataset that can support the development of a new generation of intrusion detection systems. The next step of our research will therefore focus on such systems. Another important step would be to extend DHALSIM with attack concealment capabilities, to fully replicate the attacks generated in BATADAL and to extend those attacks with more attack vectors, as enabled by DHALSIM. We finally note that the dataset presented in this paper is available online at https://zenodo.org/record/6545035.

6 ACKNOWLEDGMENTS

This research is supported by Singapore's NATIONAL SATELLITE OF EXCELLENCE, DESIGN SCIENCE AND TECHNOLOGY FOR SECURE CRITICAL INFRASTRUCTURE (NSoE DeST-SCI) through the project "LEarning from Network and Process data to secure Water Distribution Systems (LENP-WDS)" (Award No. NSoE_DeST-SCI2019-0003). Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not reflect the views of National Research Foundation, Singapore.

7 REFERENCES

[1] Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., and Banks, K. (2020). "A Review of Cybersecurity Incidents in the Water Sector". Journal of Environmental Engineering 146, 5, 03120003.

[2] Taormina, R., Galelli, S., Tippenhauer, N.O., Salomons, E., Ostfeld, A., Eliades, D., et al. (2018). "Battle of the Attack Detection Algorithms: Disclosing Cyber Attacks on Water Distribution Networks." Journal of Water Resources Planning and Management 144, 8, 04018048.

[3] Taormina, R., Galelli, S., Douglas, H.C., Tippenhauer, N.O, Salomons, E., and Ostfeld, A. (2019). "A Toolbox for Assessing the Impacts of Cyber-physical Attacks on Water Distribution Systems". Environmental Modelling & Software 112 (2019), 46-51.

[4] Nikolopoulos, D., Moraitis, G., Bouziotas, D., Lykou, A., Karavokiros, G., and Makropoulos, C. (2020). "Cyber-Physical Stress-Testing Platform for Water Distribution Networks." Journal of Environmental Engineering, 146(7), 04020061.

[5] Murillo, A., Taormina, R., Tippenhauer, N., and Galelli, S. (2020). "Co-Simulating Physical Processes and Network Data for High-Fidelity Cyber-Security Experiments." Sixth Annual Industrial Control System Security (ICSS) Workshop, 13–20.

[6] Antonioli, D. and Tippenhauer, N. O. (2015). "MiniCPS: A Toolkit for Security Research on CPS Networks." Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or PrivaCy, CPS-SPC '15, New York, NY, USA, Association for Computing Machinery, 91–100.

[7] Lantz, B., Heller, B., and McKeown, N. (2010). "A Network in a Laptop: Rapid Prototyping for Software-Defined Networks." Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics

[8] Douglas, H.C., Taormina, R., and Galelli, S. (2019). "Pressure-driven modeling of cyber-physical attacks on water distribution systems." Journal of Water Resources Planning and Management 145, 3, 06019001.

[9] Urbina, D. I., Giraldo, J. A., Tippenhauer, N. O., and Cárdenas, A. A. (2016). "Attacking Fieldbus Communications in ICS: Applications to the SWaT Testbed." SG-CRC.