The Analytics Edge (Fall 2018) – Data competition

Detailed problem description and rules

`https://www.kaggle.com/t/fabdc31a8de24a5d85d71a76a8a09390`

Introduction

Modern water distribution systems rely on computers, sensors and actuators for both monitoring and operational purposes. This combination of physical processes and embedded systems—cyber-physical systems, in short—improves the level of service of water distribution networks but exposes them to the potential threats of cyber attacks. During the past decade, several water supply and distribution systems have been attacked, with the consequent creation of cyber-security agencies and international partnerships to defend water networks [1]. Yet, little is known about the potential effect of these attacks as well as the design and implementation of attack detection algorithms—which identify anomalous behaviors of sensors, pumps and other components of water networks.

1 Approach and Schedule

Your task is to contribute an attack detection algorithm for a given water network following a set of rules (outlined below). The algorithm development and testing will be based on three datasets. The first two datasets are characterized by the absence/presence of cyber attacks and are to be used for the development of the detection algorithms. The third dataset will be used to test the algorithms. The schedule of events for this data competition is outlined in Table 1.

Date	Event
November 29, 2018	Announcement of the Data Competition
November 29, 2018 (17.00)	Publication of problem details and competition rules + Release of the first dataset (with no attacks) + Release of the second dataset (with attacks) + Release of the test dataset (with attacks)
December 8, 2018 (23.59)	Last opportunity for submitting the results on Kaggle
December 10, 2018 (23.59)	Submission of the reports and code

Table 1: Schedule of events.

Other info about the data competition will be published on Kaggle, which will act as a portal for downloading the data and uploading the predictions for the test dataset.

2 Problem description

C-Town Public Utility (CPU) is the main water distribution system operator of C-Town (Fig. 1). For many years, CPU has operated a static distribution topology. In the last year, CPU has introduced novel smart technology to enable remote data collection from sensors in the field, and remote control of actuators. Shortly after that new technology has been introduced, anomalous levels in some water tanks were observed. Searching for the causes, CPU engineers suspect potential cyber-attacks for all these episodes. In particular, they are considering adversaries that are able to activate and deactivate the actuators in C-Town,

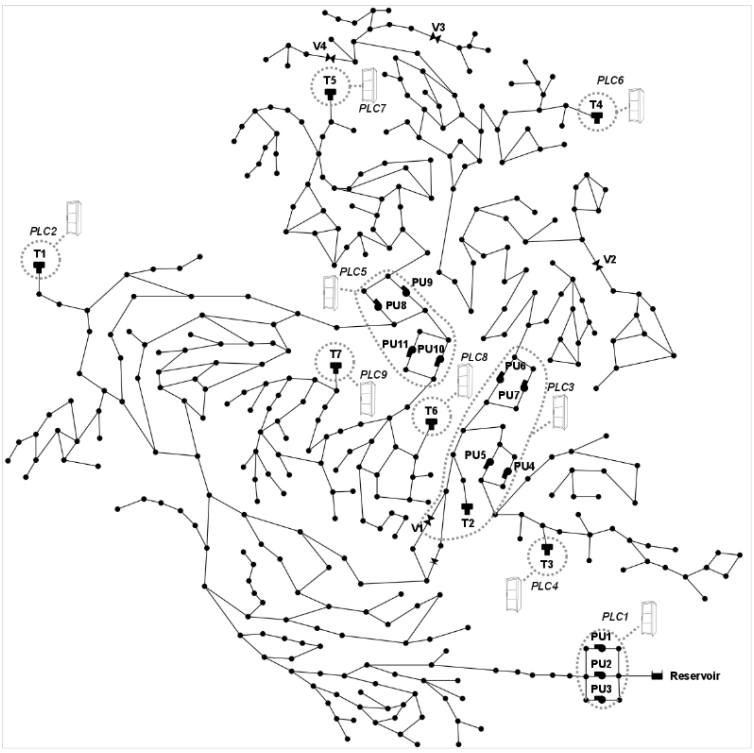

Figure 1: Graphical representation of C-Town water distribution system.

as well as altering the readings of the sensors deployed in the network and the reported status of actuators, and interfering with the connections established between networked components. The participants task is thus to develop an alert system for cyber-physical attacks.

2.1 Development data

C-Town (Figure 1) is based on a real-world medium-sized network. Water consumption is fairly regular throughout the year with no seasonal variations. Water storage and distribution across the demand nodes is guaranteed by seven tanks, whose water levels trigger the operations of one valve and eleven pumps distributed in five pumping stations (S1-S5). Pumps, valves and tank water level sensors are connected to nine PLCs (Programmable Logic Controller), which are located in proximity of the hydraulic components they monitor/control. C-Town has a Supervisory Control And Data Acquisition (SCADA) system that collects the readings from all PLCs and coordinates the operations of the entire network. Table 2 reports the water level sensors and the hydraulic actuators controlled by each PLC. Most of the PLCs controlling the pumps are not directly connected to the water level sensors employed in the control logic, but receive the necessary information via other PLCs. Each PLC controlling a given actuator also reads its status (ON/OFF or OPEN/CLOSED), the flow passing through it, and the suction and discharge pressures.

Historical SCADA data

The following data based on historical SCADA operations are provided.

- First set (*train_dataset01.csv*): Data from about 12 months preceding the installation of the smart devices (January 2015–2016). These data are guaranteed to be without attacks and can be used to study the normal system operations.
- Second set (*train_dataset02.csv*): A few months of data following the installation of the smart devices. This dataset contains attacks causing anomalous hydraulic conditions. CPU engineers were able to discover these attacks and label them properly.

- Test set (*test_dataset.csv*): This dataset contains unlabelled attack data. It will be used to quantify the performance of the algorithms (see Section 2.2).

The available SCADA readings are:

- Water level in each tank (Float);
- Status (Boolean, False for OFF/CLOSED, True for ON/OPEN) for each pump and valve in the system;
- Flow through each pump and valve (Float);
- Suction pressure and discharge pressure for each valve and pumping station (Float);
- Attack flag for first and second set (Boolean, False for SAFE, True for UNDER ATTACK) .

The variables are indicated using the term LEVEL for water level, STATUS for status, FLOW for flow, and PRESSURE for pressure.

PLC	Sensor	Actuators (controlling sensor)
PLC1	-	PU1(T1), PU2(T1)
PLC2	T1	-
PLC3	T2	V1(T2), PU4(T3), PU5(T3), PU6(T4), PU7(T4)
PLC4	T3	-
PLC5	-	PU8(T5), PU9(-), PU10(T7), PU11(T7)
PLC6	T4	-
PLC7	T5	-
PLC8	T6	-
PLC9	T7	-

Table 2: Controlling sensors and controlled actuators attached to each PLC.

2.2 Test data, solution submission, and evaluation criteria

The test dataset will contain a few months of data and attack instances that may differ from those of the development dataset. The submission should resemble the *sample_submission.csv* file available on Kaggle—i.e., two columns containing the DATETIME of all instances in the test dataset and the corresponding predictions ATT_FLAG.

The performance of the algorithms will be then evaluated based on their capability of classifying correctly the state of the water distribution system (SAFE or UNDER ATTACK). Considering the importance of classifying correctly the presence of attacks (which are rare instances), we will use the $F1$ score, which is defined as:

$$F1 = 2 \cdot \frac{p \cdot r}{p + r}, \tag{1}$$

where p (precision) and r (recall) are defined as follows:

$$p = \frac{TP}{TP + FP}, \tag{2}$$

and

$$r = \frac{TP}{TP + FN}, \tag{3}$$

where TP represents the True Positives (the state of the system is correctly classified as under attack), FP the False Positives (the state of the system is erroneously classified as under attacks), and FN the False Negatives (the state of the system is erroneously classified as safe). In other words, p is the number

of correct positive results divided by the number of all positive results returned by the detection algorithm, while r is the number of correct positive results divided by the number of all relevant samples (all samples that should have been identified as positive). A graphical illustration of TP, FP, FN, and TN is given in Figure 2. With the $F1$ score we thus simultaneously account for both precision and recall of the detection algorithms.

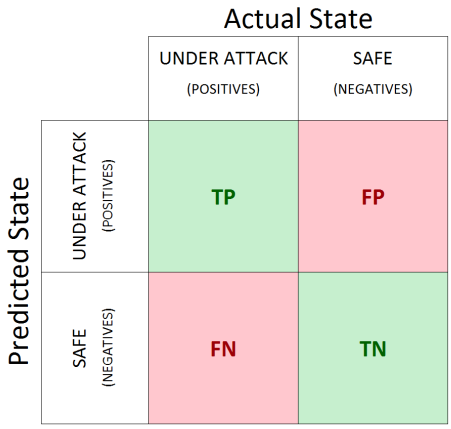

Figure 2: Confusion Matrix.

Kaggle will calculate the value of the $F1$ score on two subsets of the test dataset, named *public* and *private*. The results on the public dataset will be available during the competition (*public leaderboard*), while the results on the private one will be available at the end of the competition (*private leaderboard*).

3 Grading

The Data Competition is worth a maximum of 40 points, which will be distributed as follows:

- 10 points for the report. This is a short document (max. 4 pages) containing: a high-level description of the approach developed, a short description of the results, and a brief discussion on interpretability and limits of the approach. An executive summary is not needed. The reports must be submitted using the eDimension submission inbox. When submitting the report, please also upload a zipped file containing the code you developed. There will be a dedicated submission inbox on eDimension;
- 10 points for the public leaderboard;
- 20 points for the private leaderboard.

References

[1] R. Taormina, S. Galelli, N. O. Tippenhauer, E. Salomons, and A. Ostfeld, “Characterizing cyber-physical attacks on water distribution systems,” *Journal of Water Resources Planning and Management*, vol. 143, no. 5, p. 04017009, 2017.