Homework3

ECE 631A Cyber-Security of Critical Infrastructure

Due Date: September 15, 2019 by 11:55 PM via canvas

This homework is based on the paper: "Truth Will Out: Departure-Based Process-Level Detection of Stealthy Attacks on Control Systems" by Aoudi, Iturbe, and Almgren which appeared in CCS'18.

Your job in the homework is to implement the PASAD based determination of stealthy and direct attacks SA1, SA2, SA3, DA1, and DA2 as described in Section 3.1 of the paper.

The data from Tennessee Eastman plant control sensor readings are provided in the zip file. In the zip file you will find 2 folders. You should be using the csv data files in folder called "data".

The csv files contain the sensor readings in the column major order where each column contains the time series value of one of the sensors. The sensors are named as XMEAS(1), XMEAS(2), XMEAS(3) and so on. The Column 1 in the csv file corresponds to XMEAS(1) time series, Column 2 corresponds to XMEAS(2) time series etc.

The dataset is collected for a total of 48 hours; the first 40 hours are normal measurements and the remaining 8 hours in an attacked scenario. The time duration of the length of 100 subsequences represents one hour.

Each csv files contained in the folders '1 - Scenario DA1', '2 - Scenario DA2', '3 - Scenario SA1', '4 - Scenario SA2' and '5 - Scenario SA3' contains the reading of each attack scenario mentioned in the PASAD paper (Figure 3 to figure 7).

The first 500 observations (5 hours) are used for training (determining the matrix U, and $U^{T)}$. The next 3500 observations (i.e up to 501- 4000 observations) are used for threshold determination (determining θ). The readings corresponding to attacks start from 4001^{st} observation till the end of columns.

Note that for each attack case, even when an actuator is attacked (either by directly controlling the actuator to open or close or change positions), the attack detection will happen only from sensor readings. That is why all the csv files only contain 41 columns for 41 sensors. Moreover, an attack on an actuator may not have effect on all the sensor's readings.

For example, for attack SA1: even though the manipulation is on XMV(9), the effect will be seen in XMEAS(5). For SA2: XMV(6) is manipulated but the effect is on XMEAS(10). For SA3: making XMEAS(10) readings zero will be detectable by changes in sensor XMEAS(9). For DA1: XMV(10) is manipulated but the effect will be on XMEAS(15). The DA2 is compromising the readings of XMEAS(7) but the detection will be on XMEAS(5).

So you need to apply PASAD to the right sensor variables for each of the attacks to be able to detect.

Your tasks are as follows:

1. Identify a library in the language of your code (Python/C/C++ etc) that can do efficient SVD.
2. Code the training phase, and use the first 500 observations for the sensor whose reading you want to use to detect the attack.
3. Use the training independently for the 5 sensors whose readings will detect the attacks (Note that this requires analysis of the plant and the controller but here it is already given to you).
4. Then augment your code from (2) to compute threshold. Use the next 3500 observations to compute the threshold for each sensor required for each attack.
5. Then for the next 800 observations do the detection.
6. Plot the original sensor readings against time (4800 observation points vs. sensor readings) for each case.
7. Plot the corresponding departure scores against time for all 4800 points of observations.
8. Create a report with plot of (6) and plot (7) next to each other. For Plot in (7) also show a horizonal line corresponding to the threshold.
9. Create a zip file with all code, the data files, and the report.

Scoring will be done as follows:

1. Correctness and efficiency of training code – 15
2. Correctness and efficiency of thresholding code – 15
3. Detection ability of attacks (for each attack 10 points – total 50 points)
4. Quality of graphs and clarity (20 points)

   Total: 100 points.