**SUTD 51.508: Secure Cyber Physical Systems (2020)**

**Assignment 4 by Group 7**

Ong Yang Chen, Justin (1003988)

Loh Wei Long (1004009)

Tan Teik Guan (1004067)

**Plant Simulation**

We have written a simple simulator to mimic the physical appearance of SWaT stage 1. The main component is Tank 101 where we simulated the actual water level of the tank when pump P101, valve MV101 and level sensor LIT101 is in operation. We can also manually control the state of P101 and MV101 as if from the HMI. For purposes of simulation, we have reduced the time scale from minutes to seconds. The simulator runs at continuously with every second representing one minute of PLC operations.

In the following, we show the screenshots of the simulator under normal operation.

3 buttons on the top MV101, LIT101, P101 indicate the state and values.

Clicking on MV101 and P101 can toggle the ON/OFF the actuators. Due to PLC logic, the MV101 and P101 states will toggle back almost immediately based on the LIT101 values. To turn off the PLC logic, click on the green ‘Auto’ button to toggle the state to ‘Manual’. The actuators’ states will be permanently fixed on that state.

Level Rate (mm/min) displays the net flow rate.

*t – CUSUM threshold*

*b – CUSUM bias*

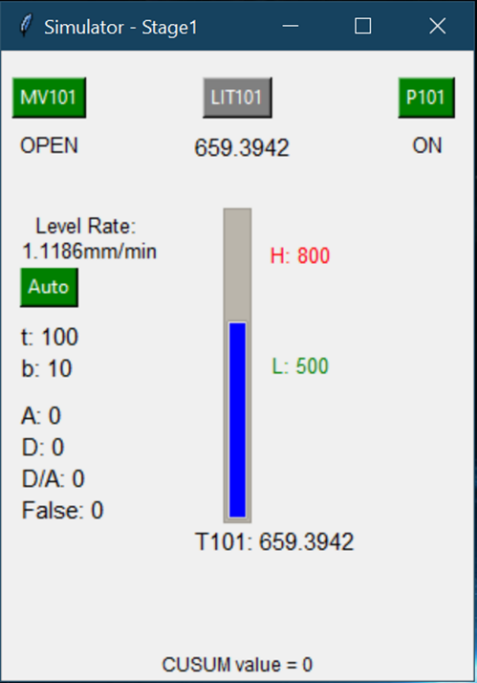
*A – Number of attacks*

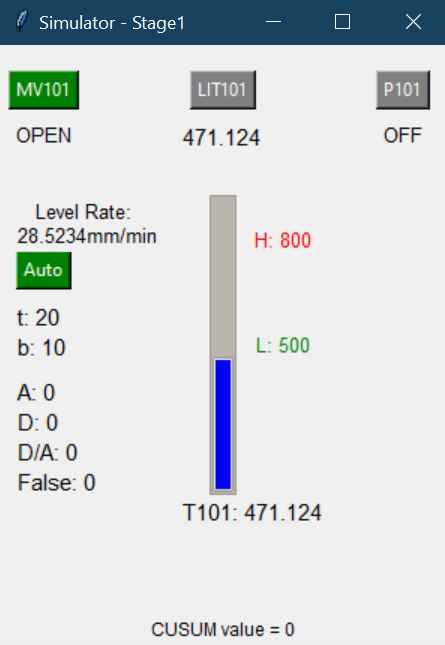
*D – Number of detections*

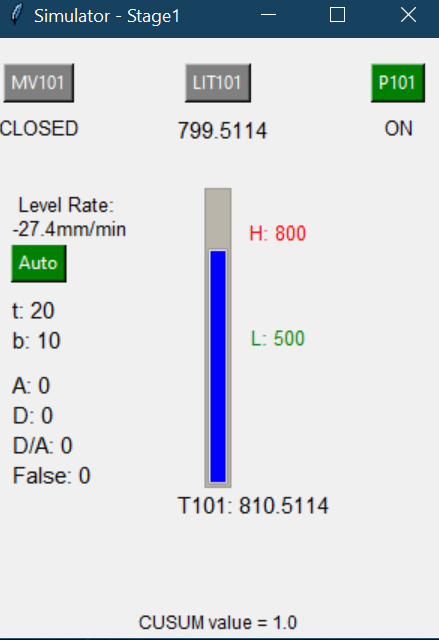
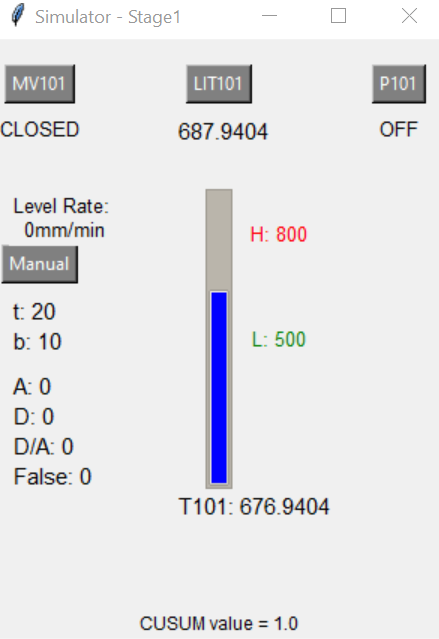
*D/A – Detection rate defined as Number of detection/Number of attacks*

*False – Number of false alarms.*

The current CUSUM value calculated is shown at the bottom.

* + MV101=OPEN, P101=ON: Rise at 1.11857mm/minute
  + MV101=OPEN, P101=OFF: Rise at 28.5234mm/minute



* + MV101=CLOSED, P101=ON: Fall at 27.40 mm/minute
  + MV101=CLOSED, P101=OFF: No change in water level

**Attack Simulation**

To trigger attack on LIT101, click on the LIT101 button. It will turn to ‘Red’ to indicate an attack is ongoing. To trigger multi-point attacks, manually toggle MV101 and P101 when LIT101 attack is ongoing.

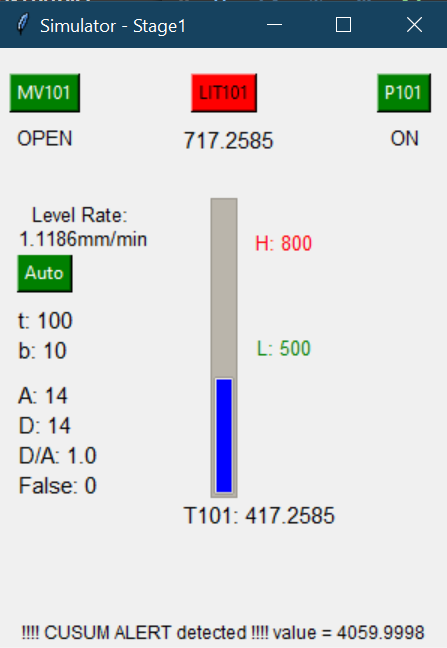
The LIT attack values are taken from ‘attack.txt’ randomly from a list of integer deltas delimited by a space.

The CUSUM bias and threshold values are set from ‘cusum.txt’ in the format <bias threshold> separated by a space.

The result readings are written in CSV format to ‘output.txt’

The attacks that can be performed on the simulator are:

**Surge Attacks** – For surge attacks, the attacker can set the value of LIT101 to be > H (800mm) to force the pump P101 to operate while MV101 to close. This will cause an underflow as soon as possible.

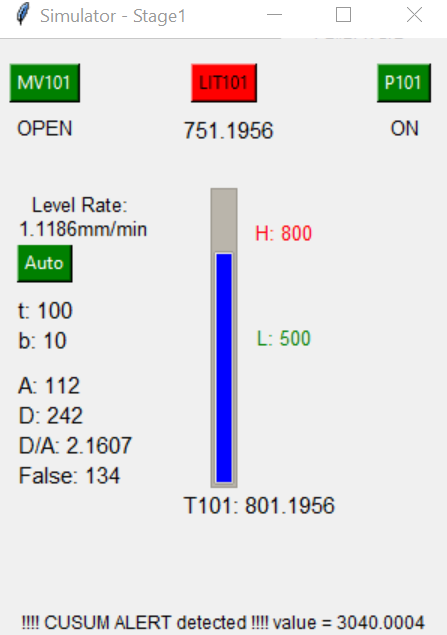


In this attack demo, we constantly attack the LIT101 by giving a delta of **+300**.

This results in an underflow situation eventually. In the screenshot on the left, the LIT101 value is 717.2585 whereas the actual T101 value is 417.1956. Based on the PLC logic, MV101 and P101 will remain OPEN and ON respectively which will damage the P101 in the long run.

CUSUM alert is triggered and we observed that the CUSUM value is increasingly higher and higher. This is due to the simulator attacking LIT101 constantly at every second.

The attacker can also set the value of LIT101 to be < L (500mm) to make MV101 open and stop P101 which will cause an overflow as soon as possible.

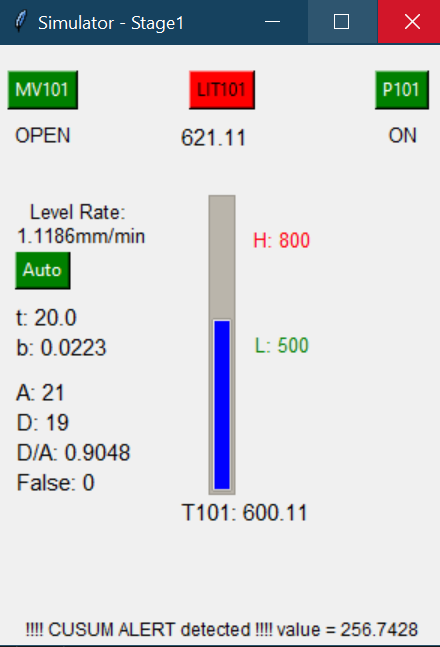
In this attack demo, we constantly attack the LIT101 by giving a delta of **-50.**

This results in an overflow situation eventually. In the screenshot on the left, the LIT101 value is 751.1956 whereas the actual T101 value is 801.1956. Going by actual PLC logic, the MV101 should be CLOSED and the P101 should be ON to drain the tank 101. However, the attack on LIT101 is preventing the PLC to reach that state.

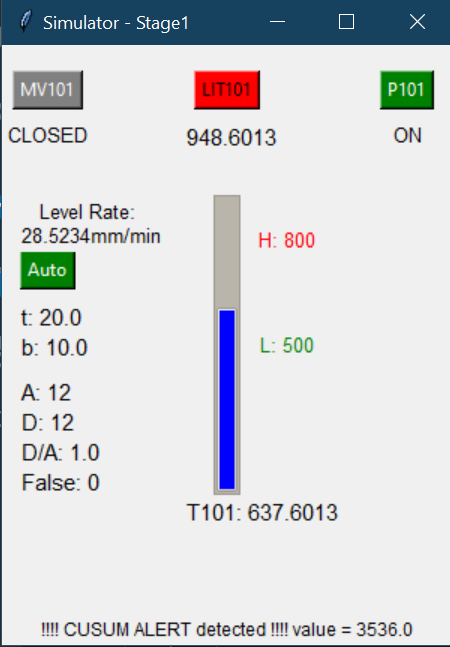
CUSUM alert is triggered and we observed that the CUSUM value is increasingly higher and higher. This is due to the simulator attacking LIT101 constantly at every second.

**Bias Attacks** – For bias attacks, the attacker can set either a positive or negative bias at each time step which will eventually lead to an underflow or overflow.

Bias attack can be set by adding the text ‘BIAS’ to the ‘attacktype.txt’ in the simulator. The small constant value will be taken from the ‘cusum.txt’ first integer.

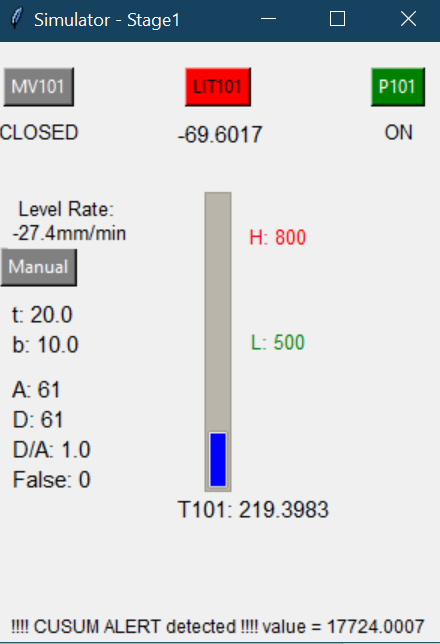
As the time steps become larger, that is, with the longer time period, the CUSUM value will increase at an extremely fast rate. For an attacker to attack a long time, a very small bias must be set. Else, the Bias attack will be detected very easily.

**Chattering** – For chattering, the attack can randomly set large positive and negative bias which will force the pump P101 and valve MV101 to switch states very quickly.

The large values caused the CUSUM value to rise very fast. And the detection rate is 100% due to the large values exceeding the threshold by a huge margin.

The simulator does not simulate actual pump or valve breakdown due to this attack.

* Multi-point attack – For multi-point attack, the attack can simultaneously set LIT101 and change the state of pump P101 and/or valve MV101

To demonstrate this attack, we can toggle the mode of the simulator to ‘Manual’ and attack LIT101 at the same time. From the screenshot on the left, we can see that even though the water level is low, the forced closure of the MV101 and turning ON of P101 is an effective attack on the pumps.

Attack Detection

CUSUM was implemented to detect the attacks where the bias b and threshold τ can be modified dynamically. We show the screen shots of the cumulation of the CUSUM value in a bias attack before and after the threshold is reached. In this simulation, b = 10 and τ = 20. The values are determined after calibration for false alarms. (see following section)

**Experiments**

False Alarms – We experimented stage 1 by putting in a small positive and negative changes to LIT101 readings to simulate randomness / noise in the sensor. The values set randomly values for the sensor is in the interval of [-11, 10].

Bias b remains at 10 while τ varies from 4 to 20.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Value of τ | 4 | 8 | 12 | 16 | 20 |
| Time to false positive | 10 seconds | 22 seconds | 50 seconds | 100 seconds | No false positive after 5 minutes |

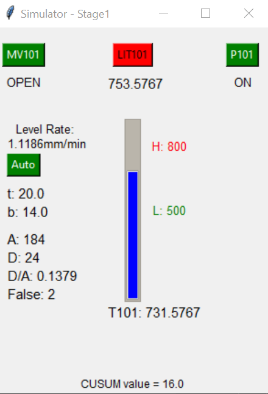
|  |  |
| --- | --- |
| Value of τ | No. of False Alarms |
| 4 | 97 |
| 8 | 42 |
| 12 | 14 |
| 16 | 1 |
| 20 | 0 |

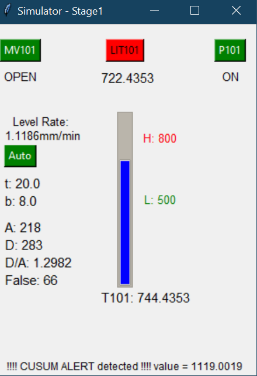
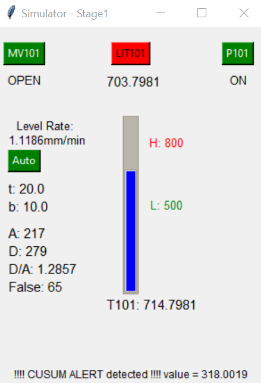
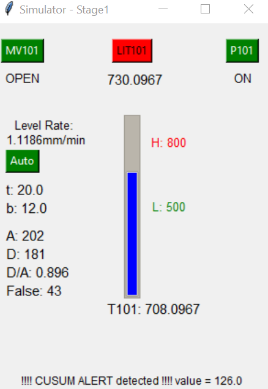
We observed that the false alarm decreased exponentially with the increase of the threshold value τ, as shown by the graph on the right. (No. of false alarms against value of τ)

To select the optimal threshold τ, we want to select as high as possible to avoid false alarm, however, increasing τ will increases the detection time.

Attack detection effectiveness – We next simulated the various attacks using different bias (ranging from 8 to 14) while τ remains at 20 for a surge attack at random with inclination to overflow.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Bias b | Attacks | Detected | False Alarms | Effectiveness  (Detected – False Alarms)/ Attacks |
| 8 | 218 | 283 | 66 | 99% |
| 10 | 217 | 279 | 65 | 98% |
| 12 | 202 | 181 | 43 | 88% |
| 14 | 184 | 24 | 2 | 13% |

Bias: 8 Bias: 10 Bias: 12 Bias: 14



We observed that the Bias value is sensitive to the surge attack values we set for the simulator. In this attack scenario, we maxed out the threshold in a short time for a bias closer to our attack values of 11. Considering the random noise, once the Bias attack exceeds the attack values, the effectiveness of the detection drops drastically. We concluded that we cannot be adjusting the bias against different kinds of possible attacks, it is easier to adjust the threshold for various attack detection.