INSE 6710 PROJECT
FOUNDATION OF CYBER PHYSICAL SYSTEM

Submitted To: Walter Lucia

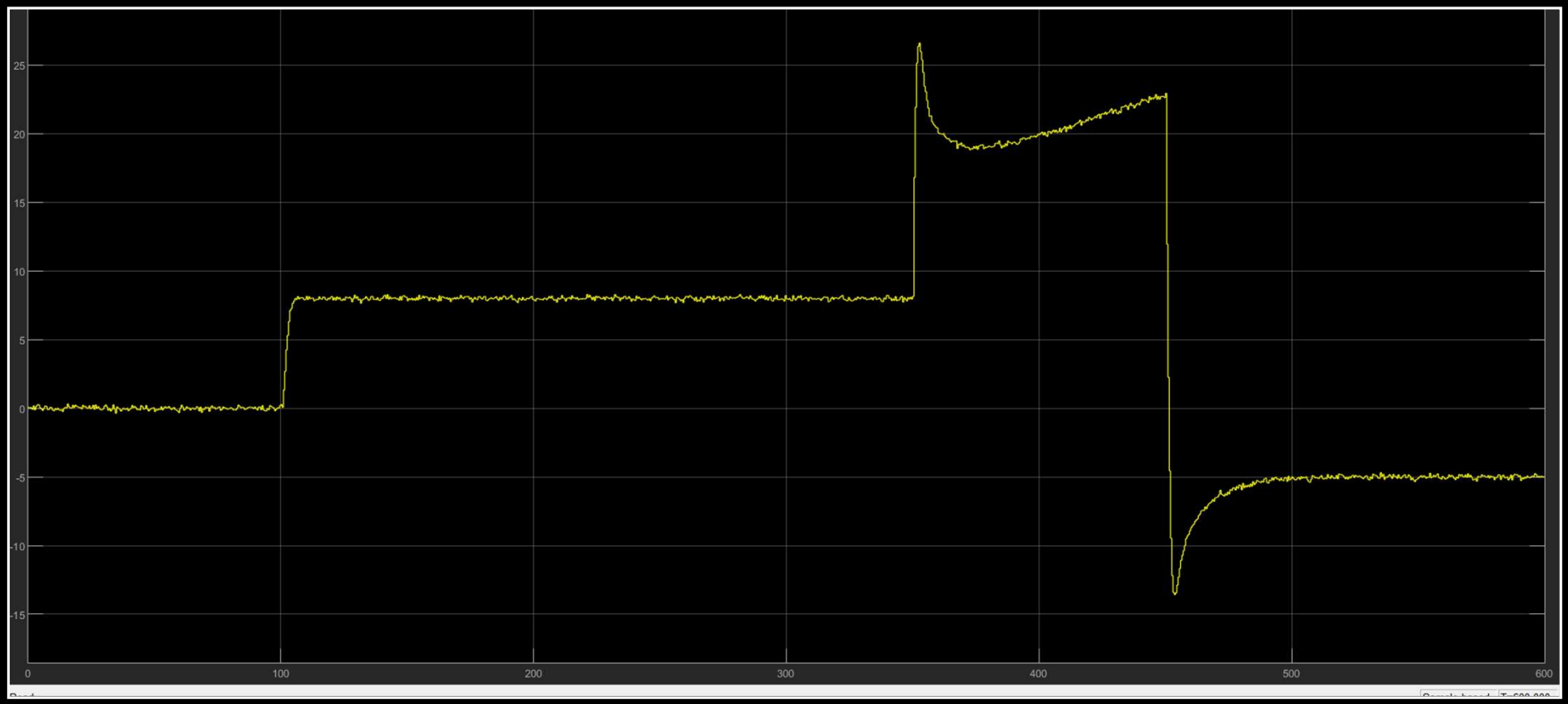
Submitted By: Group No. 26

1. Bhavsar Shivani(**40166126**)
2. Singh Amarvir(**40188944)**

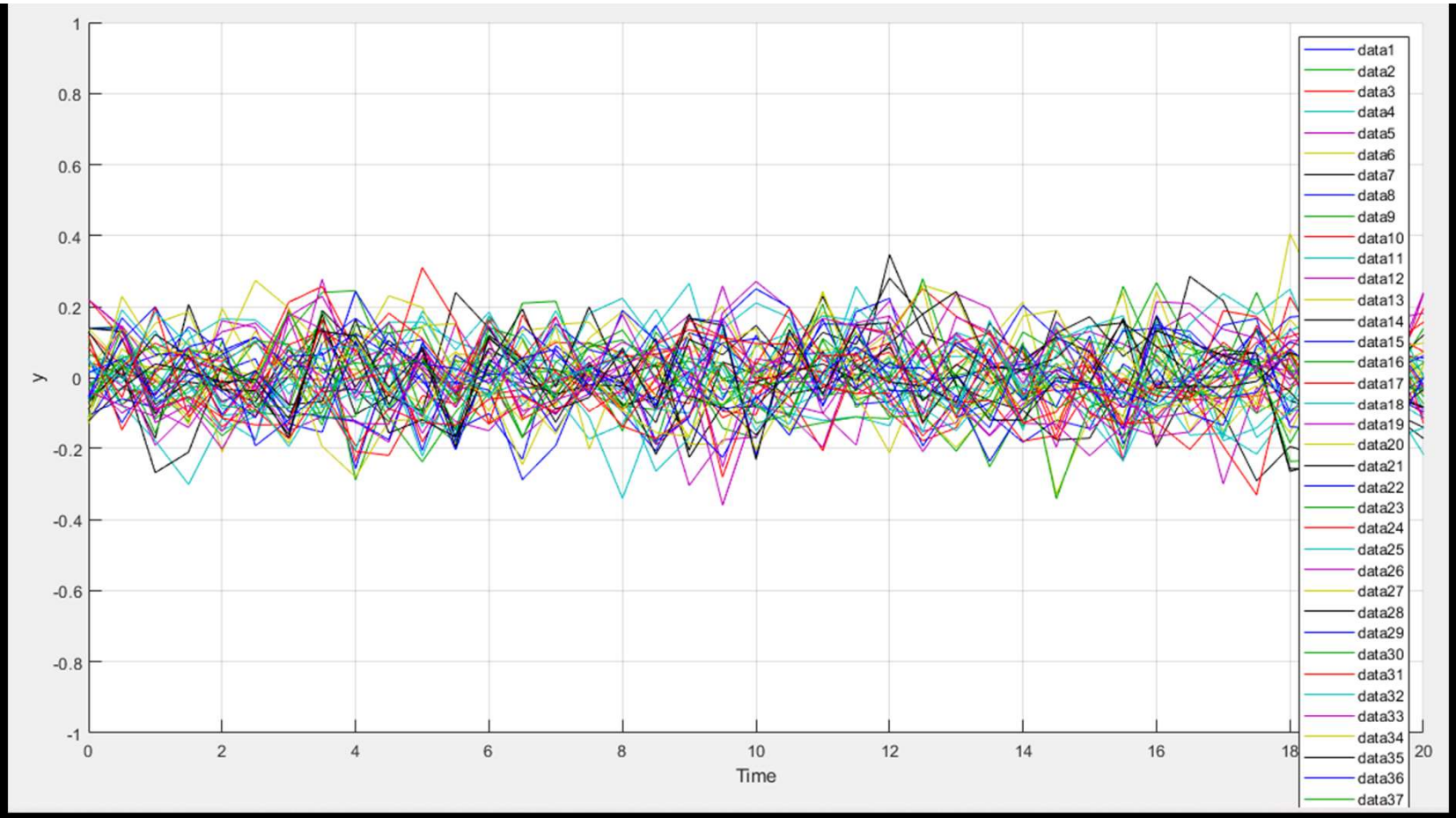
Part 1.

False Data Injection(FDI)

- It is performed on the Actuation channel of the system.



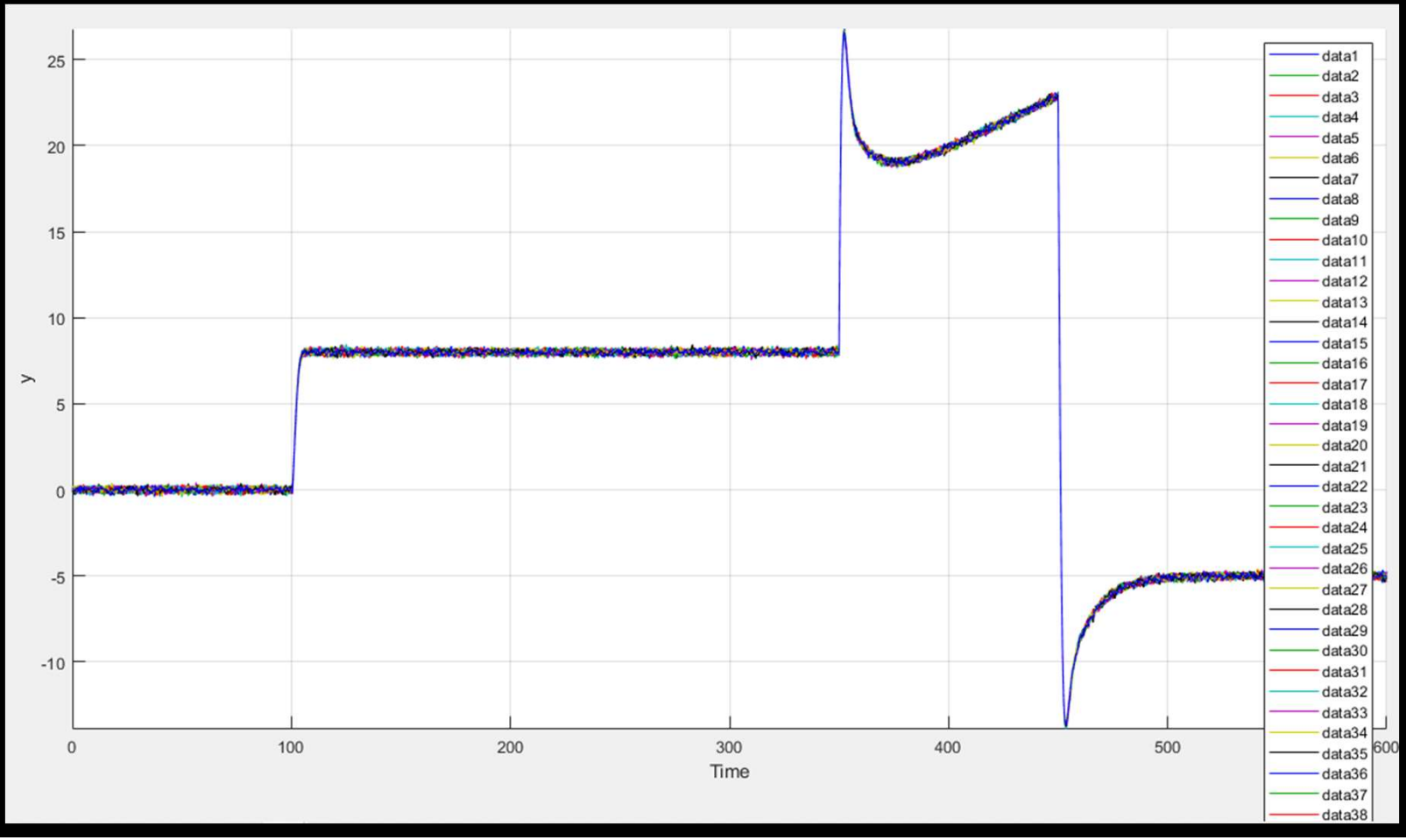
- Sensor Measurement Graph for 1 Trail Result of (y) sensor measurement



Sensor Measurement Graph 50 Trail Result of (y) sensor measurement

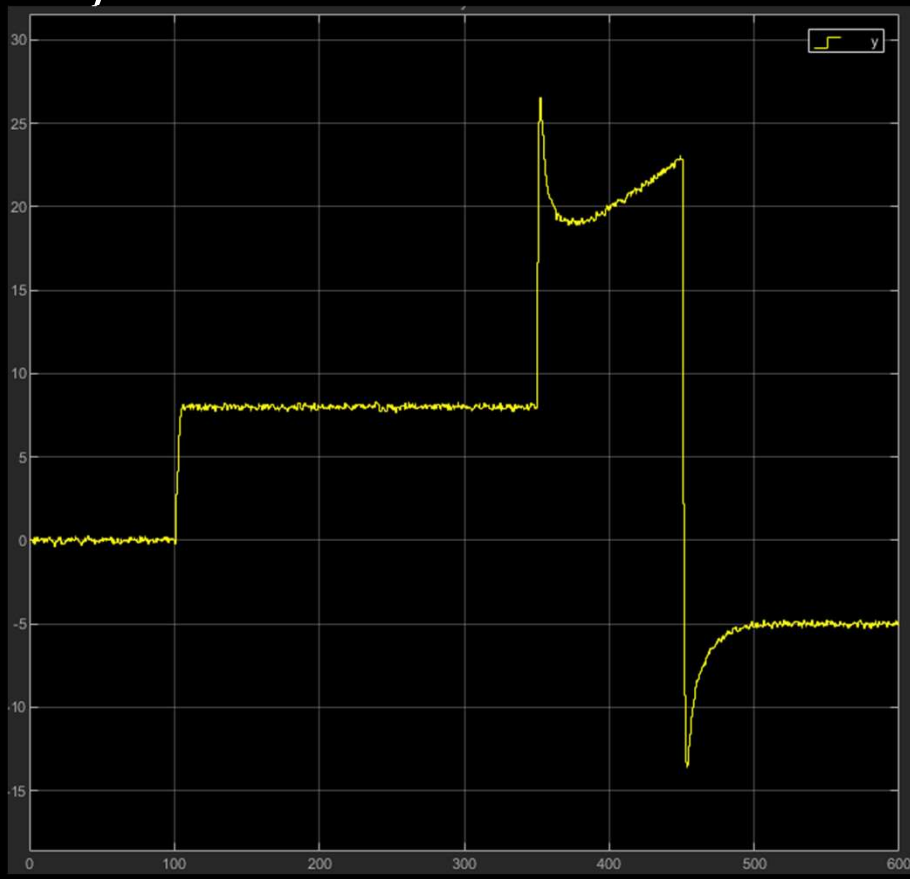
- Sensor Measurement Graph 50 Trail Result of (y) sensor measurement. As in this graph y remain with in constraints of -30<=y<=30 ,So it does not violate in 50 trails.

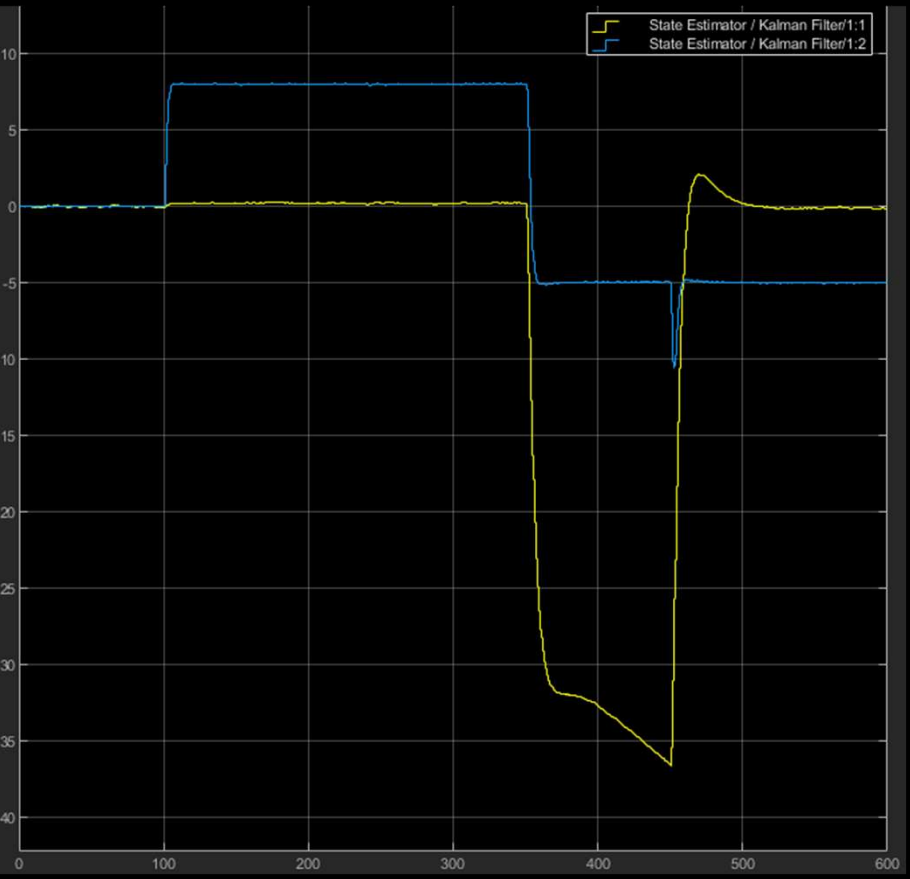
PART 1 (A)



As the y is not violating but in X_hat graph (state estimator/Kalman filter) 1 constraint Ca is violating from its range -10<=Ca<=10 reached below -35.
As if only one constraint is violating than plant also violates due to which x(real state) also violate.

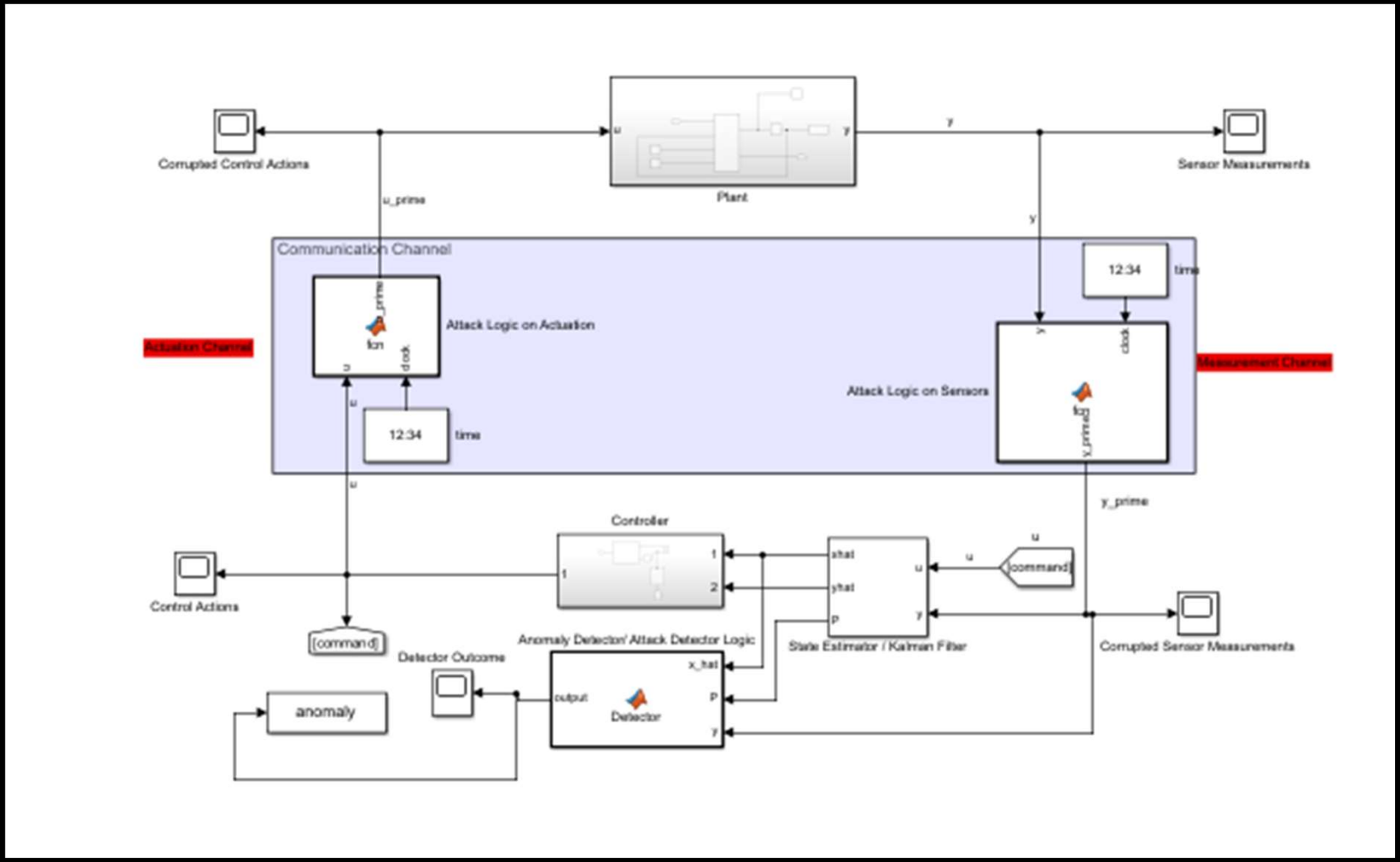
PART 1
(B)





Part2 : False Data Detection Attack

- FDI detect through chi square technique.
- Maximum tolerable false alarm rate in this is 8%



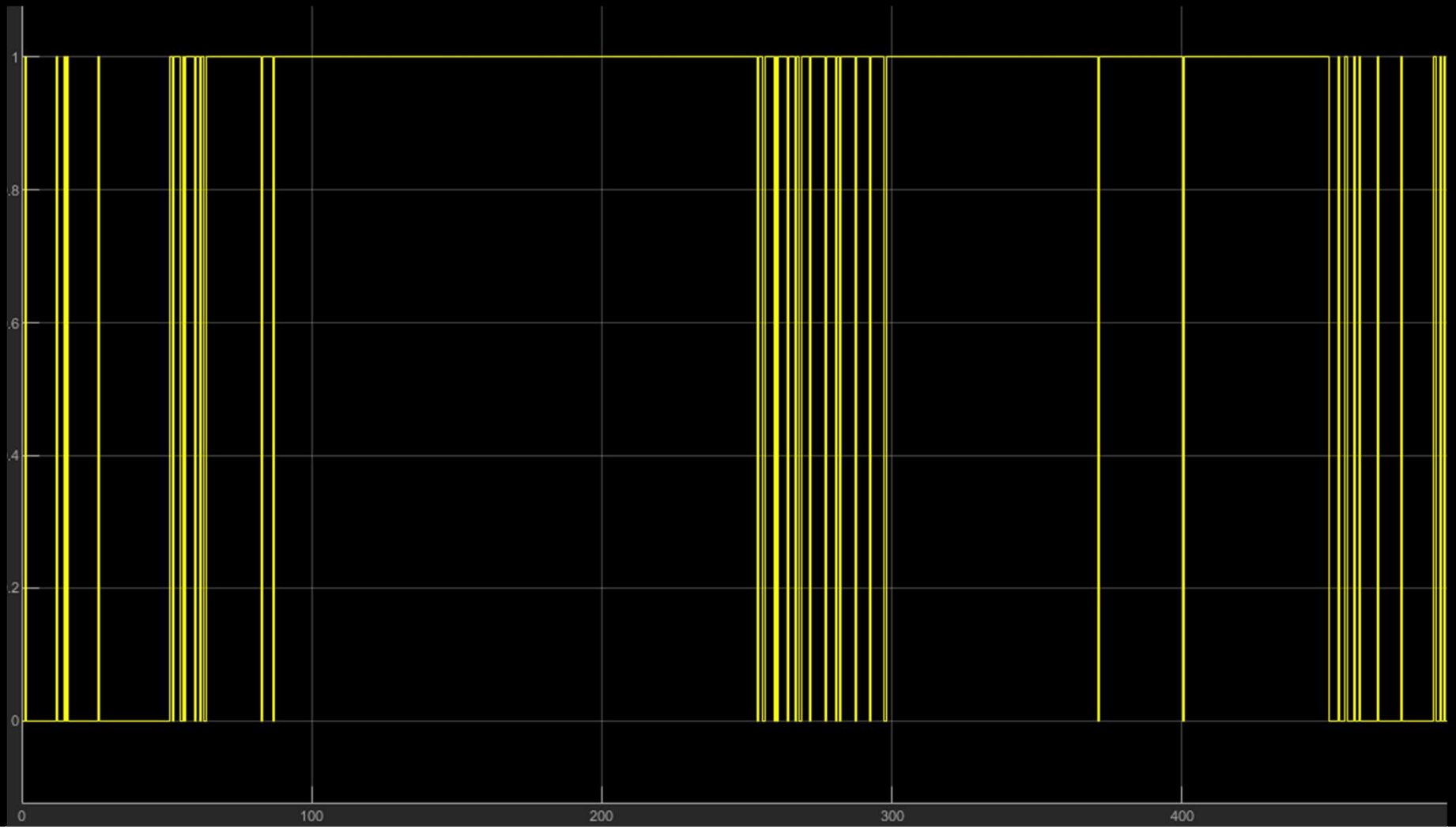
Chi-Square Detector in system

Chi-Square Detector Results

- As from the result the False alarm rate is falling under the condition of 8%
- Attack detection rate is around 96%

```
>> trails2017
Average Result of different values over 50 trails for(0,450)

falarm_average_50trails =

    7.4400


drate_average_50trails =

   96.8250


jd_average_50trails =

  189.3850
```

Attack detection by chi-square for (0,450)



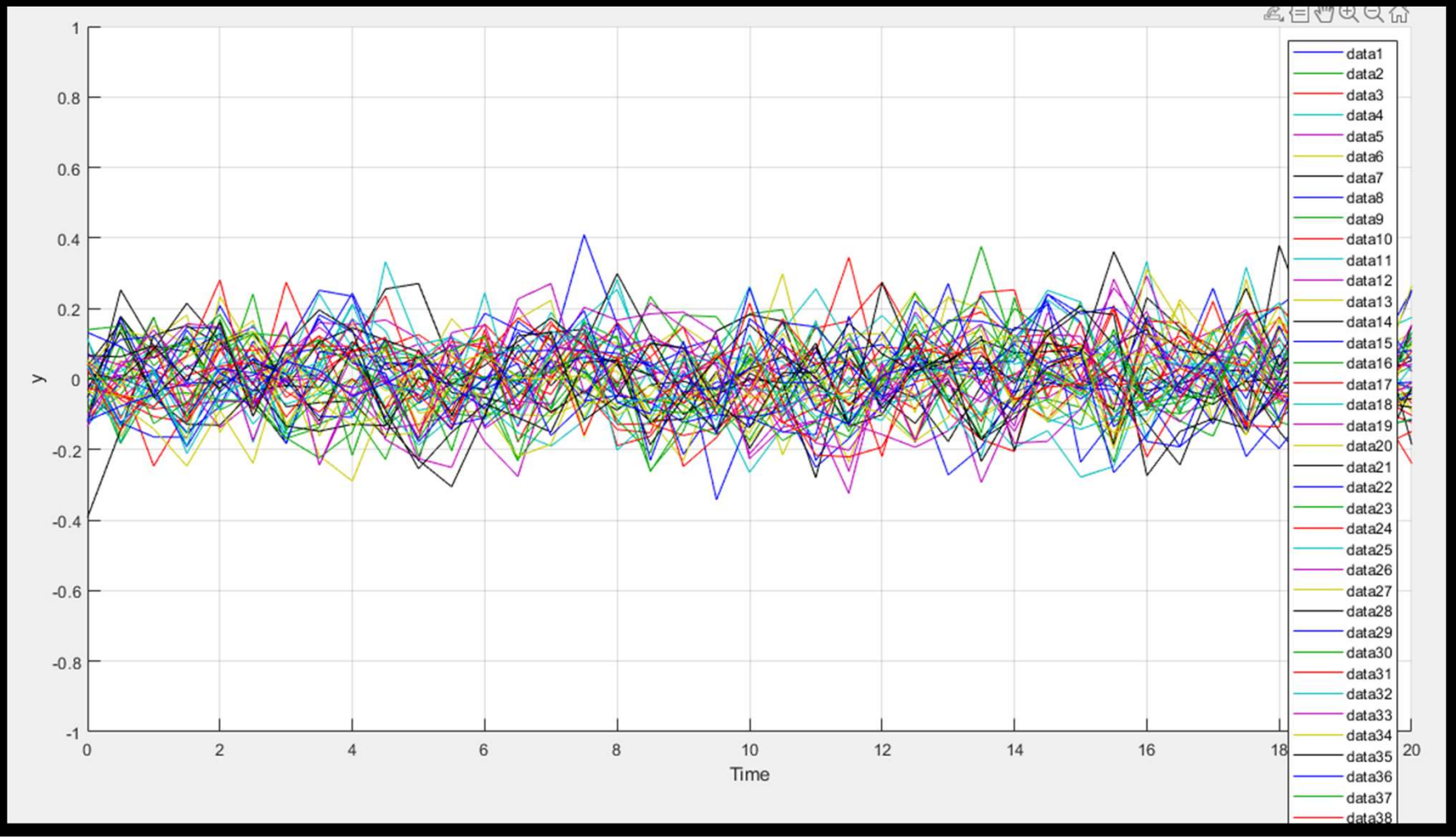
Part 3

Replay Attack

- Replay attack is taking place on the sensor measurement channel of the system.
- In this attacker replace the current sensor out with the previously recorded sensor output.

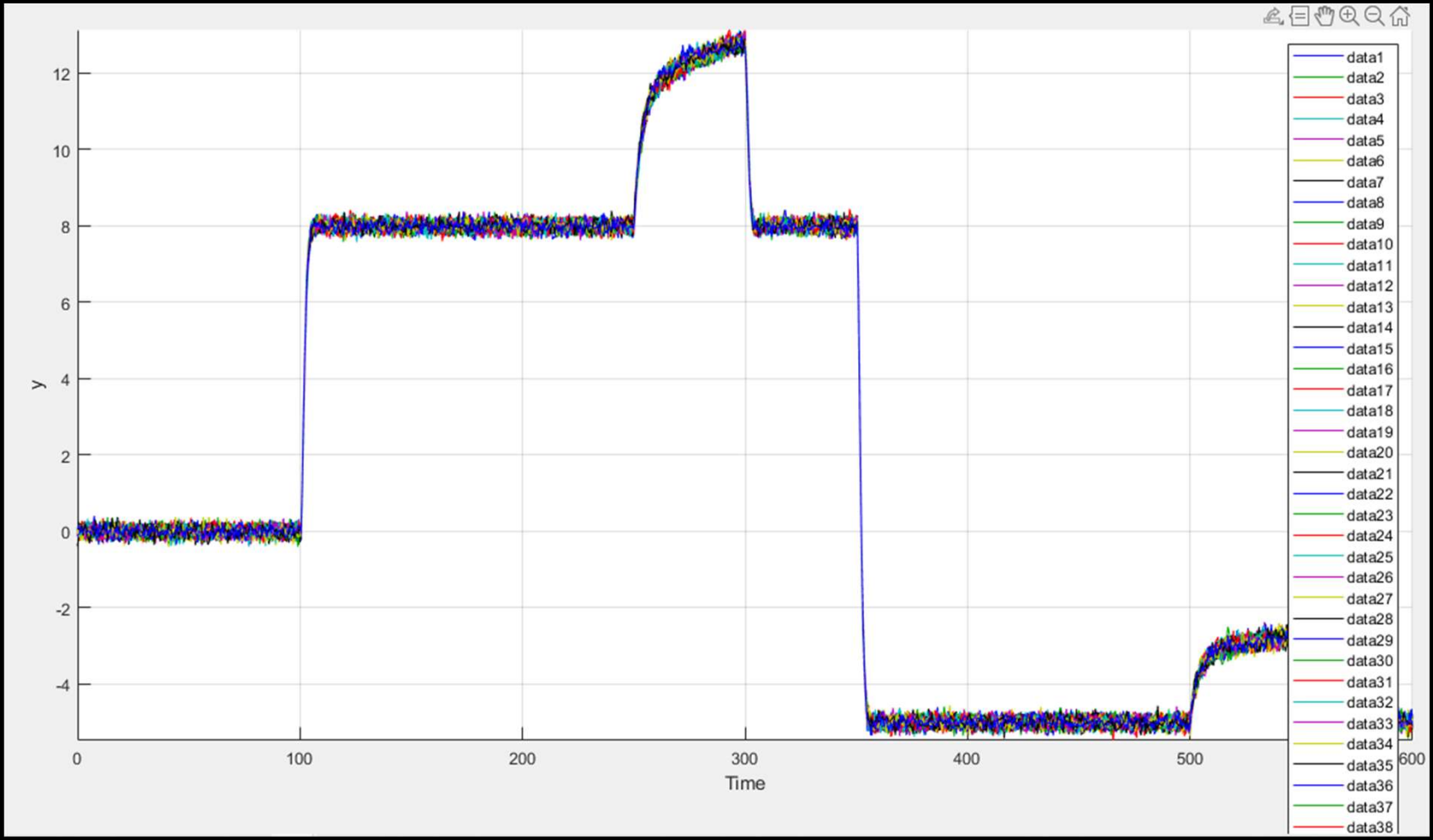
Sensor Measurement Graph 50 Trail Result of (y) **sensor** Measurement

PART 3
(A)

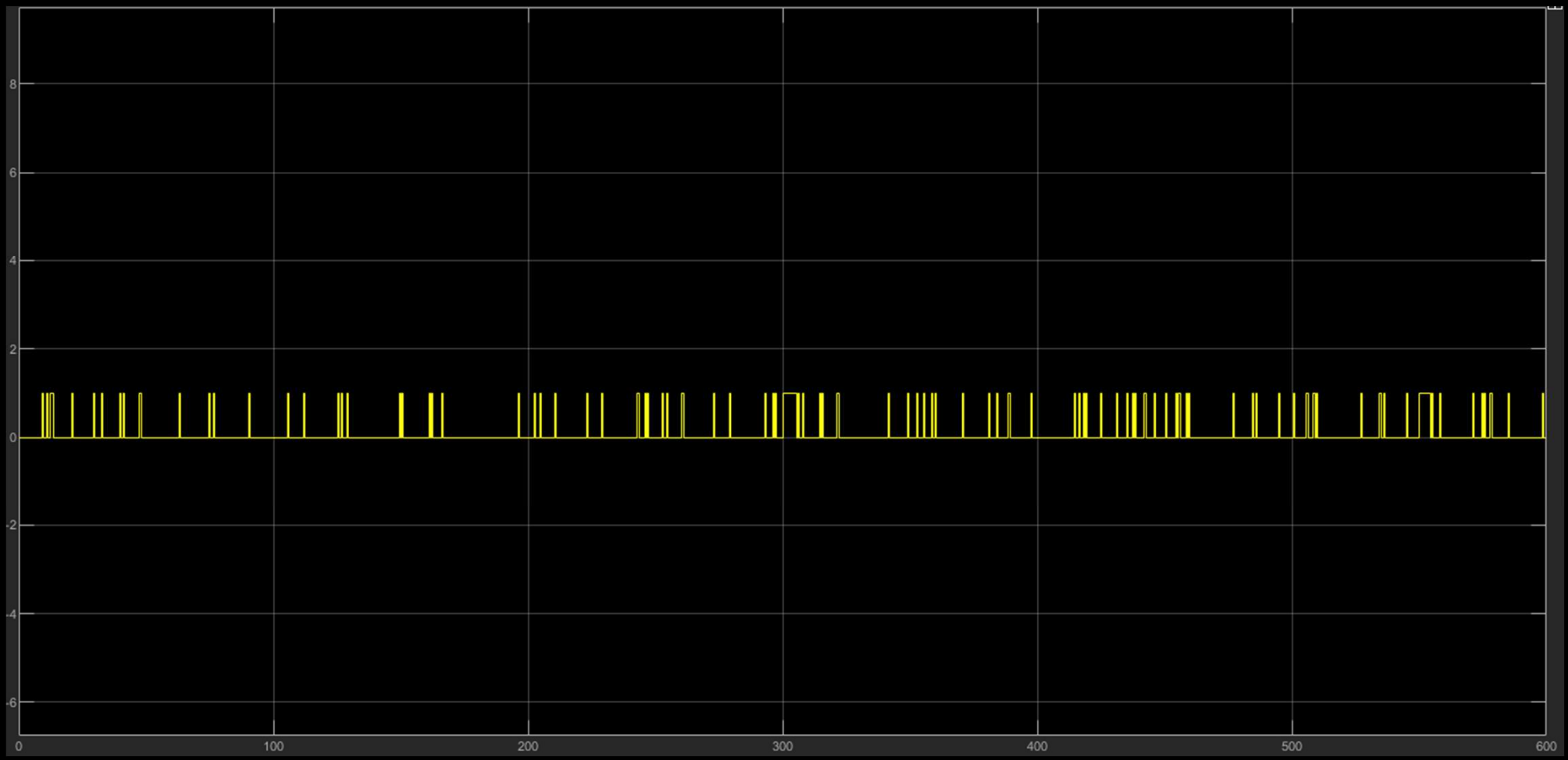


Sensor Measurement Graph 50 Trail Result of (y) sensor measurement

PART 3 (A)

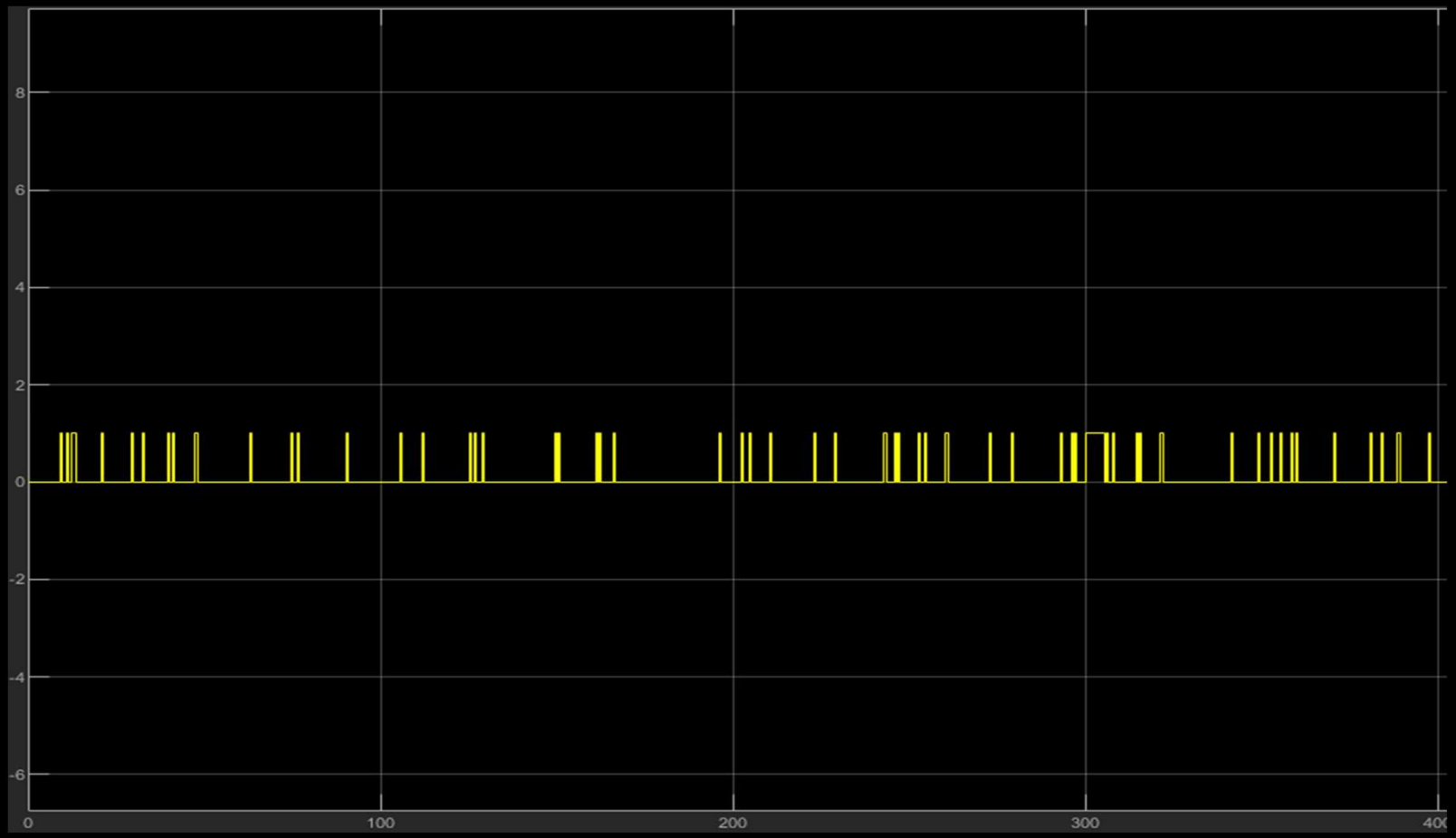


Part 3 over all output at detector for (0,600)



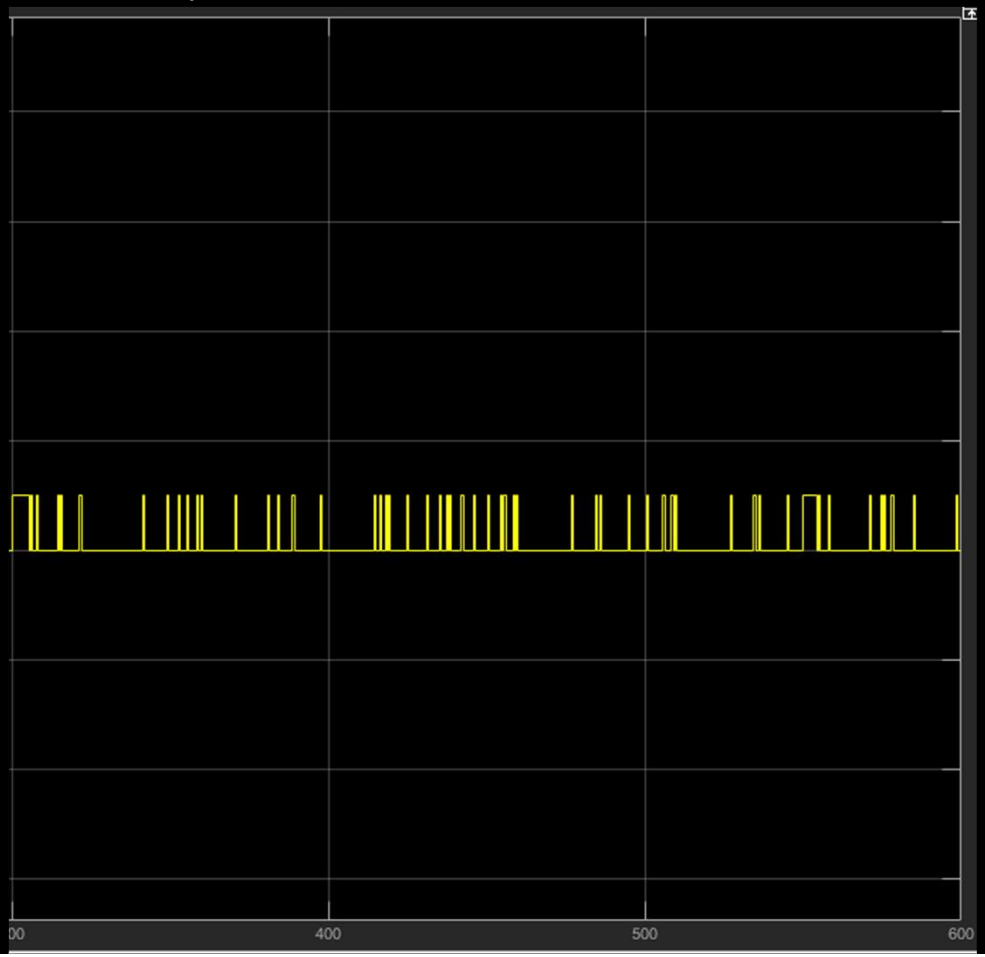
Due success of replay attack ,no attack is detected for (0,300) and (0,350) . Also when alpha = Beta (as in passive detector detection rate become equal to false alarm)

PART 3
(B)



Due Success Of Replay Attack ,No Attack Is Detected For (400,550) And (400,600) .Also when alpha = Beta (as in passive detector detection rate become equal to false alarm)

PART 3
(C)



Average Results Over 50 Trials

PART 3
(D)

```
>> trails2018
Average Result of different values over 50 trails for(0,450)

falarm_average_50trails =

    7.9681


drate_average_50trails =

    7.6200


jd_average_50trails =

   99.6519
```

Part 4. Detection of the Replay Attack

It is done by watermarking system
Also control performance is measured

Average Results Control Performance

Part 4 (A)

With Water Marking

```
>> trails2019
Average Result of different values over 50 trails

falarm_average_50trails =

    6.0594


drate_average_50trails_0to300 =

   91.8000


jd_detector_performance_average_50trails_ =

  185.7406


jw_average_50trails_200to300 =

    0.7009


jee_control_performance_average_50trails_200to300 =

    0.6189
```

Without Water Marking

```
>> trails2019
Average Result of different values over 50 trails

falarm_average_50trails =

    6.2574


drate_average_50trails_0to300 =

    5.4000


jd_detector_performance_average_50trails_ =

   99.1426


jw_average_50trails_200to300 =

    1.0152


jee_control_performance_average_50trails_200to300 =

    0.0692
```

Average Results Over 50 Trails

Part 4 (B)

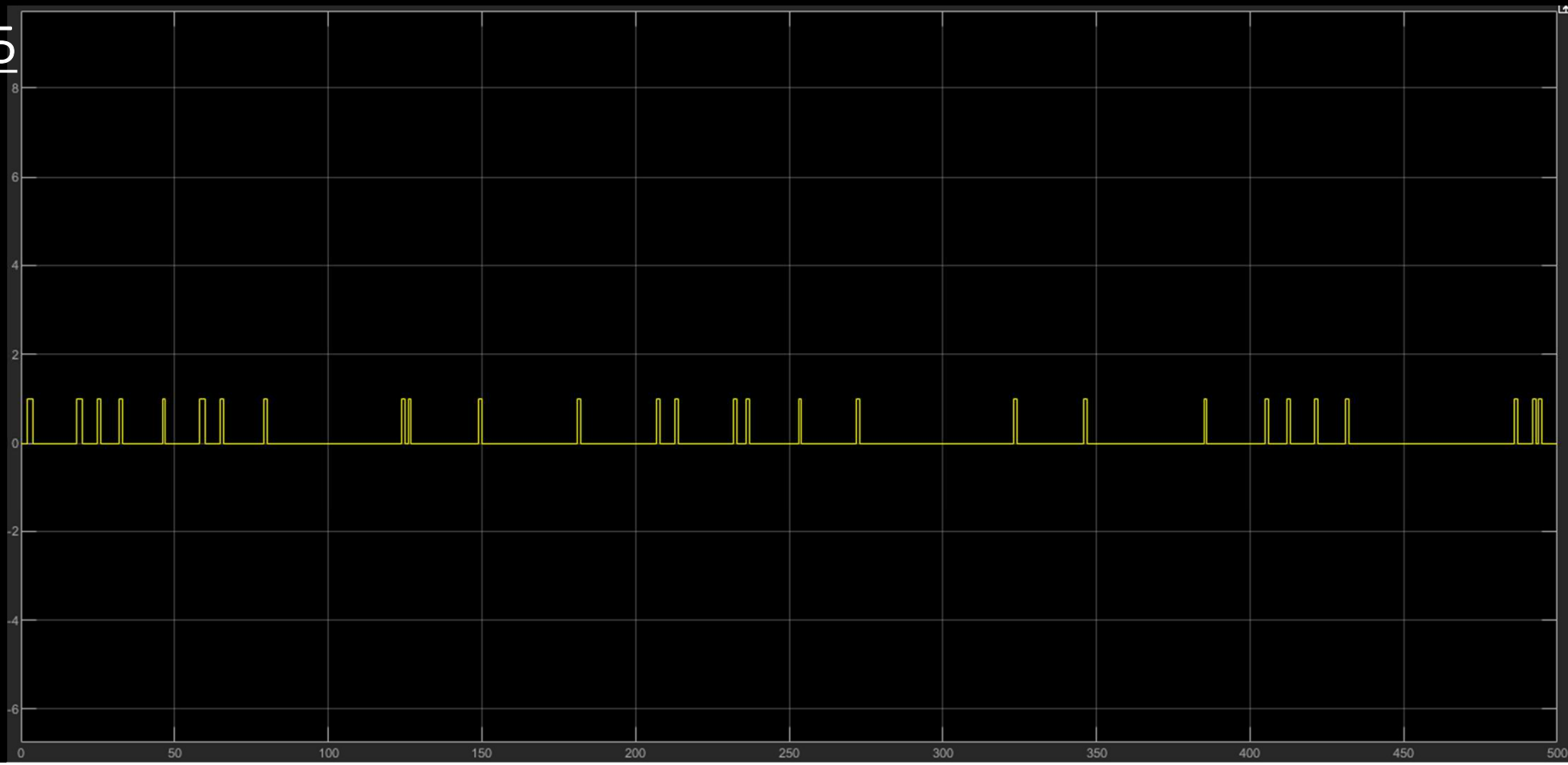
```
>> trails2019
Average Result of different values over 50 trails

falarm_average_50trails =

    6.0594


drate_average_50trails_0to300 =

   91.8000


jd_detector_performance_average_50trails_ =

  185.7406


jw_average_50trails_200to300 =

    0.7009


jee_control_performance_average_50trails_200to300 =

    0.6189
```

Part 5. Detection Of The Covert Attack

- it is done by moving target or blended target scheme.
- also control performance is measured.

Chi-square failed to detect covert attack for (0,500)

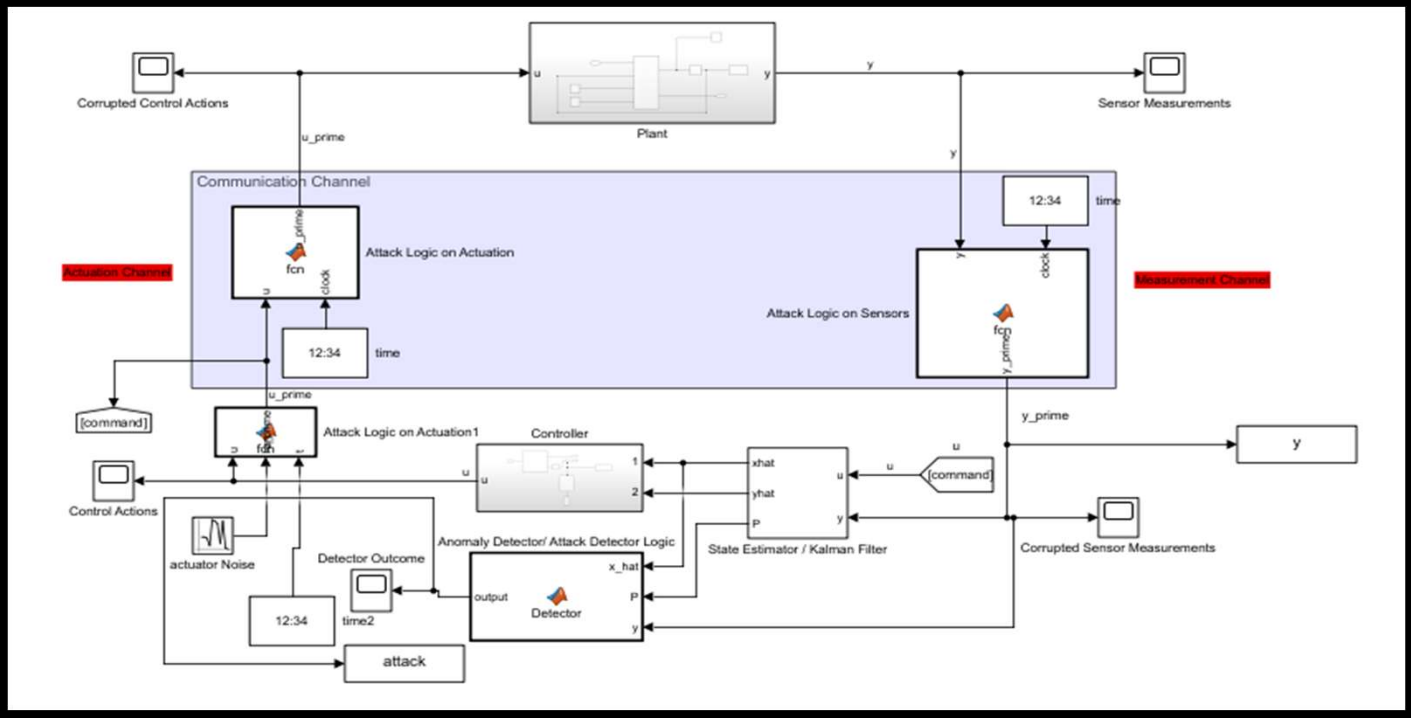
PART 5



N0 previously designed detector, detect a covert attack for (0,500)

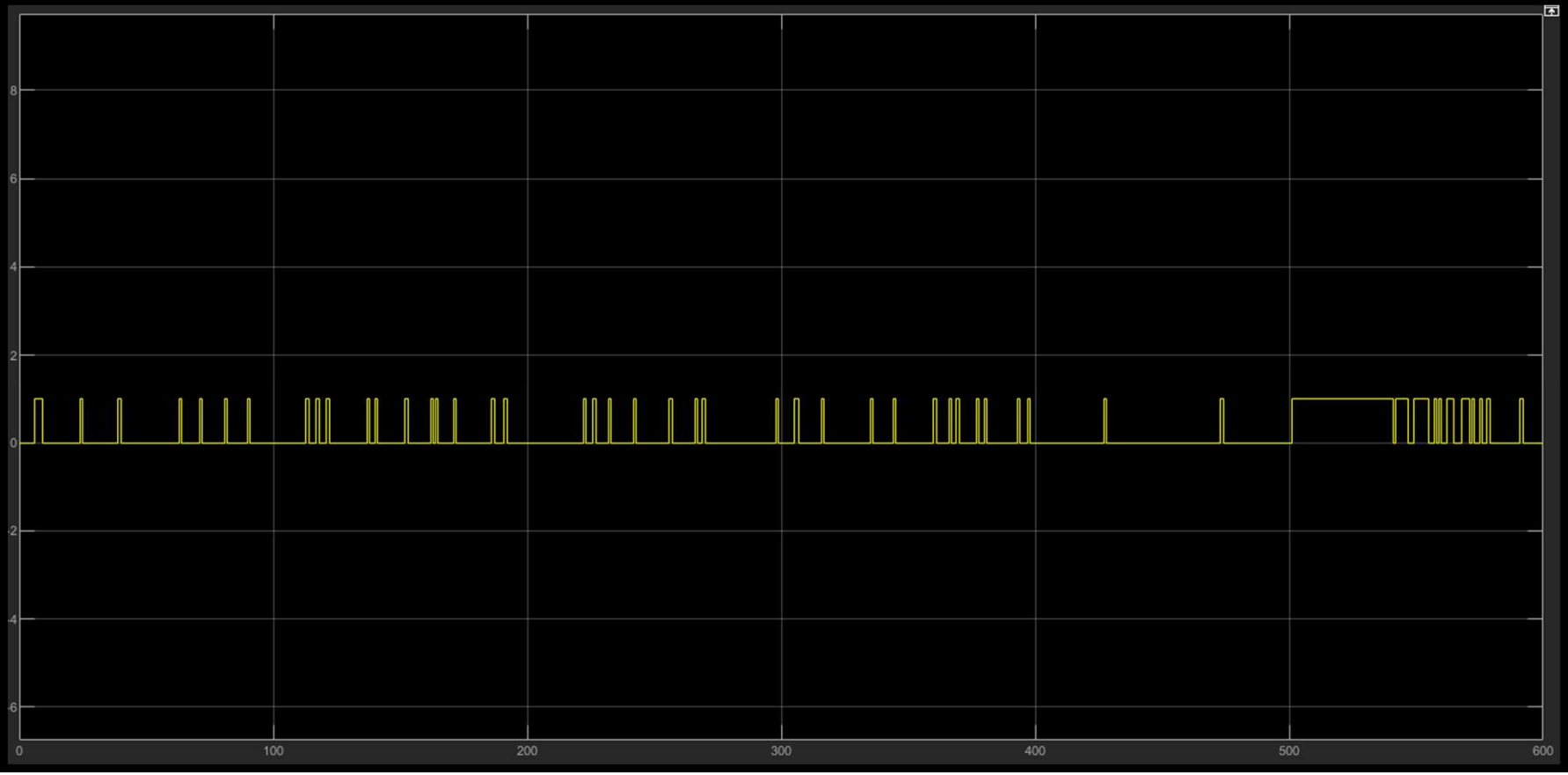
- As previously we designed chi square detector and water marking which are present on the controller side due to which covert attack become completely stealthy.

PART 5 (A)



But as in this graph after for the time frame(0,600) its detecting the attack by chi-square.

PART 5 (B)



Detection strategy used to detect this attack

PART 5 (C)

- Blended Control Architecture
- In this the water making is used on both plant and controller side
- Auxiliary system is also used.

No , detector does not effect the control performance

PART 5 (E)

- As water marking signals are removed as they are received either on plant side or controller side
- Due to this there is no loss of control performance

REFERENCES

- Class notes
- Class lectures
- http://mathworks.com/ (Math works .com)
- MATLAB – YouTube
- Joseph Delgadillo – YouTube

THANKS