

INSE 6630 PROJECT

Recent Development in Information System Security

Submitted To: Prof. Walter Lucia

Submitted By: Group 20

Hetvi Shah (40089272)

Jaldhi Prajapati (40107457)

Shreya Monpara (40105352)

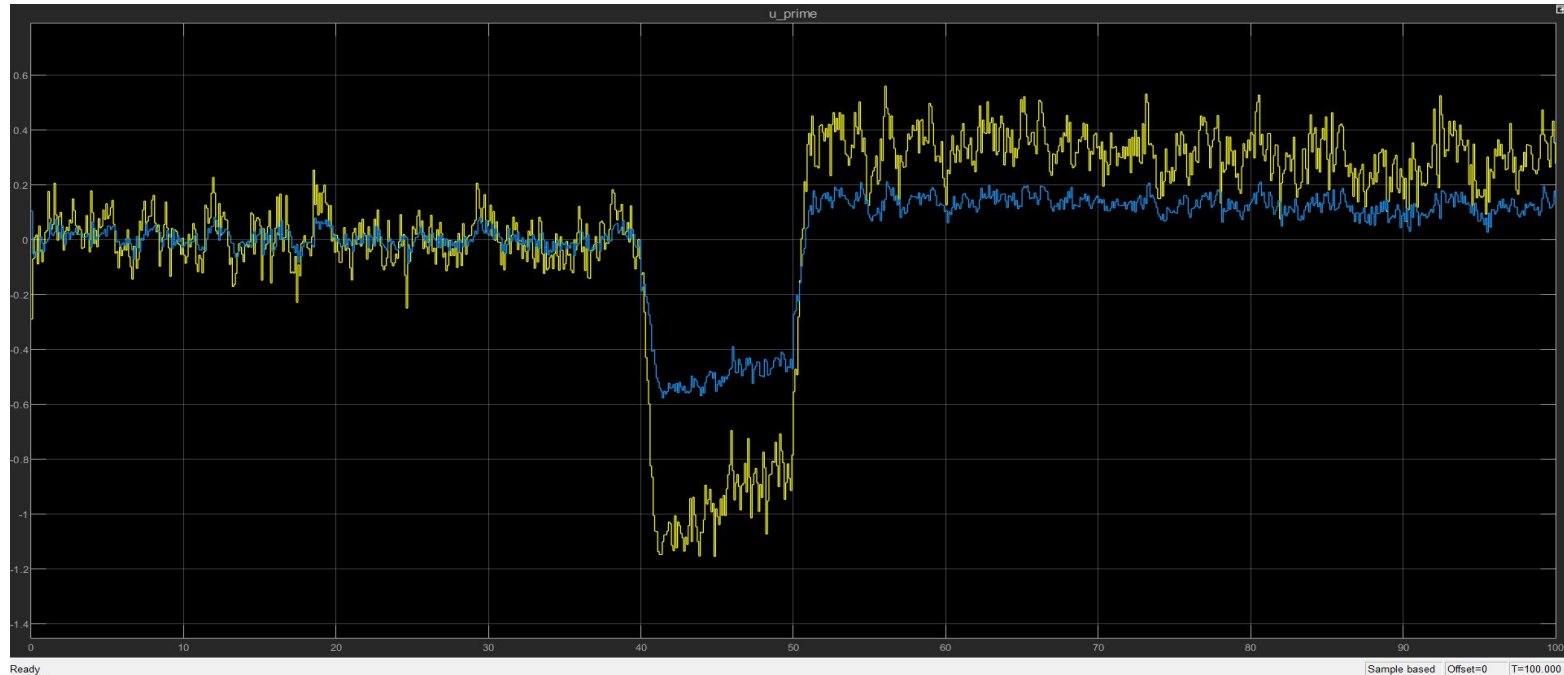


**CYBER PHYSICAL
SYSTEMS**

1. False Data Injection Attack (FDI)



It is done on the Actuation Channel of the system.



Ready

Sample based Offset=0 T=100.000

FDI Analysis

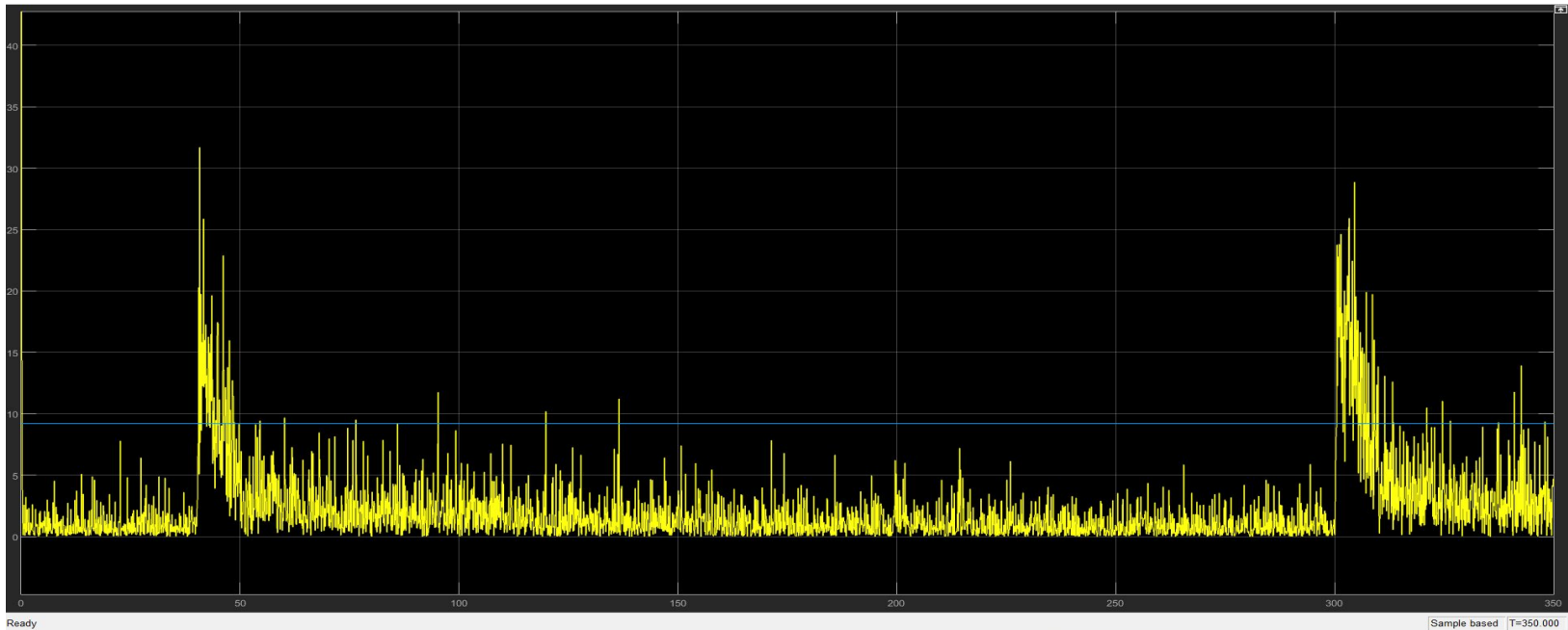


1. The plant constraints were violated during the attack.
2. From the graph, it is observed that the plant reaches the equilibrium.
3. As the system is resilient, when the attack is over, the system reaches stable equilibrium state.

2. Detection of FDI Attack

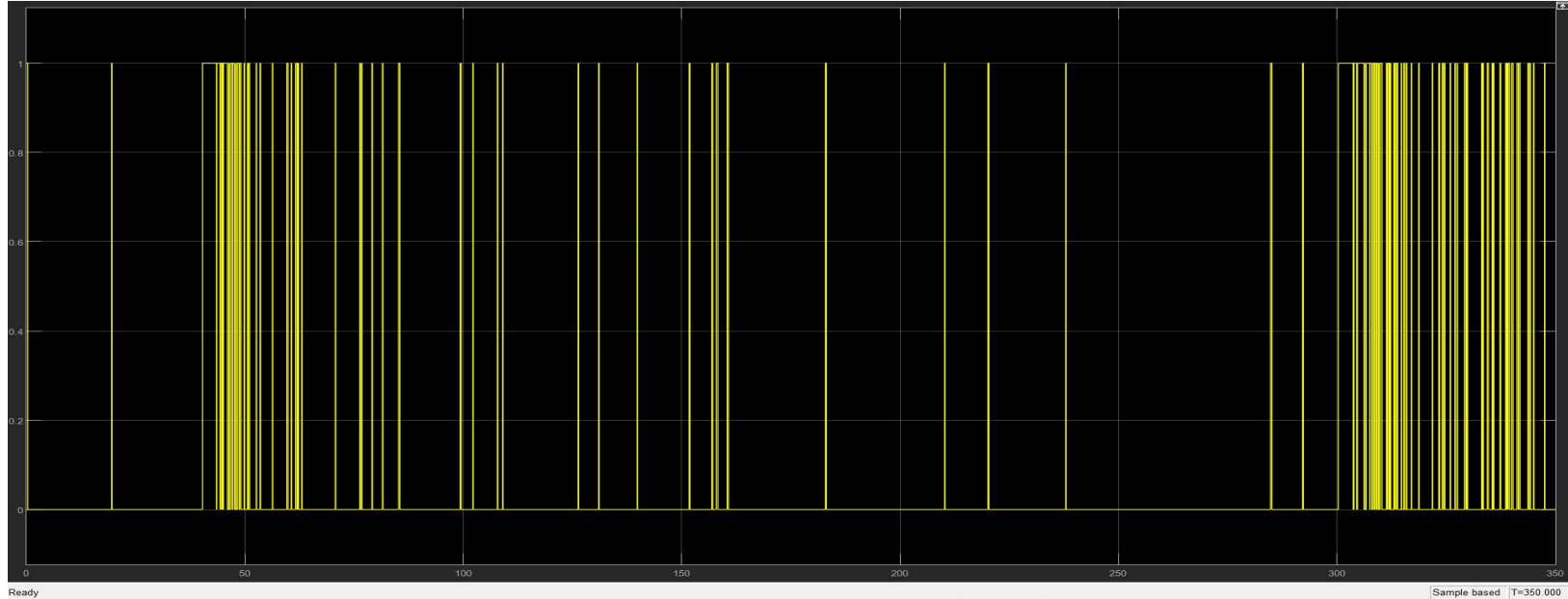


The FDI attack is detected through Chi-Square detection technique.

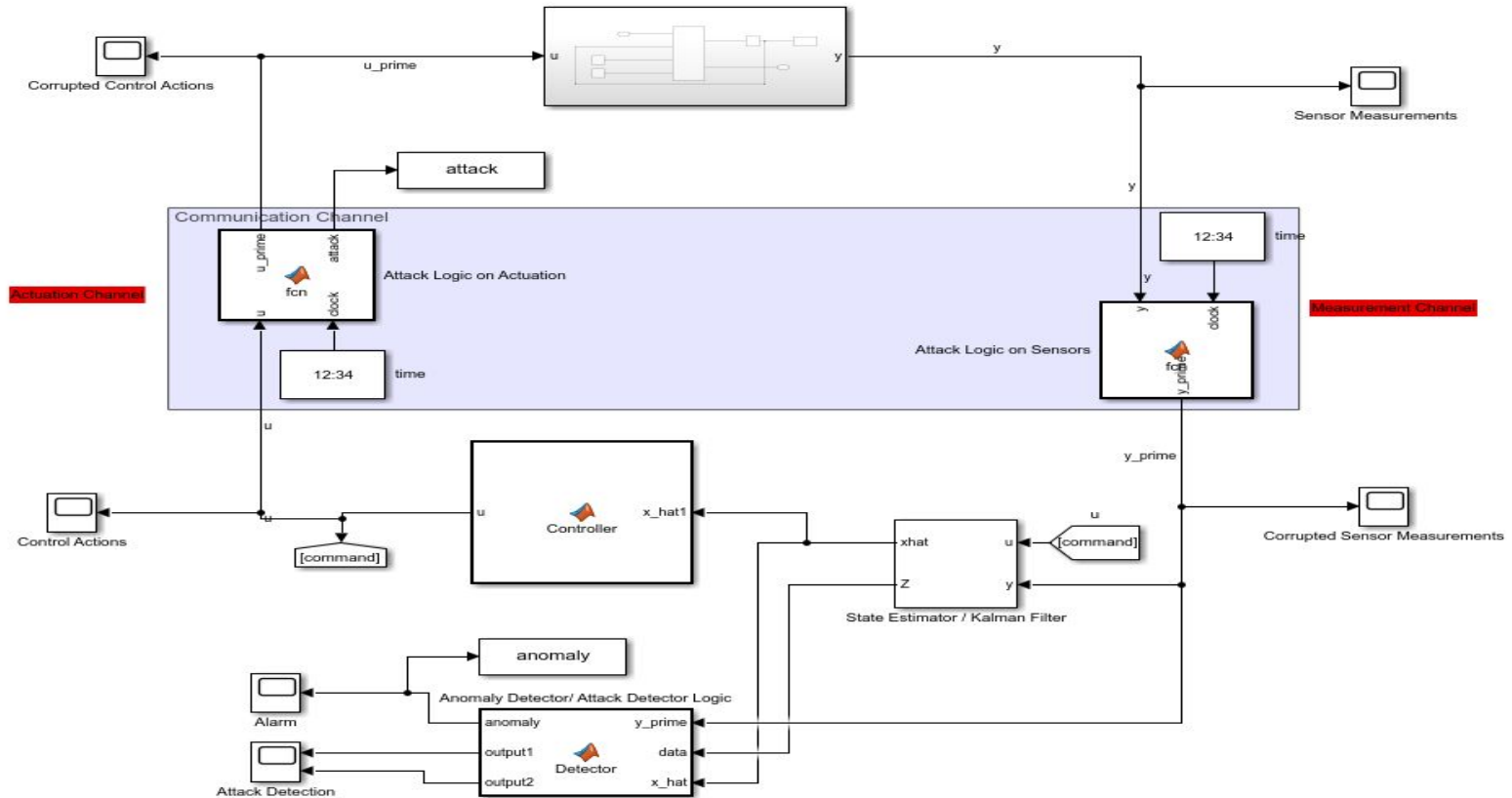


FDI Detector 1 Analysis: This simulink depicts the Chi-Square detection.

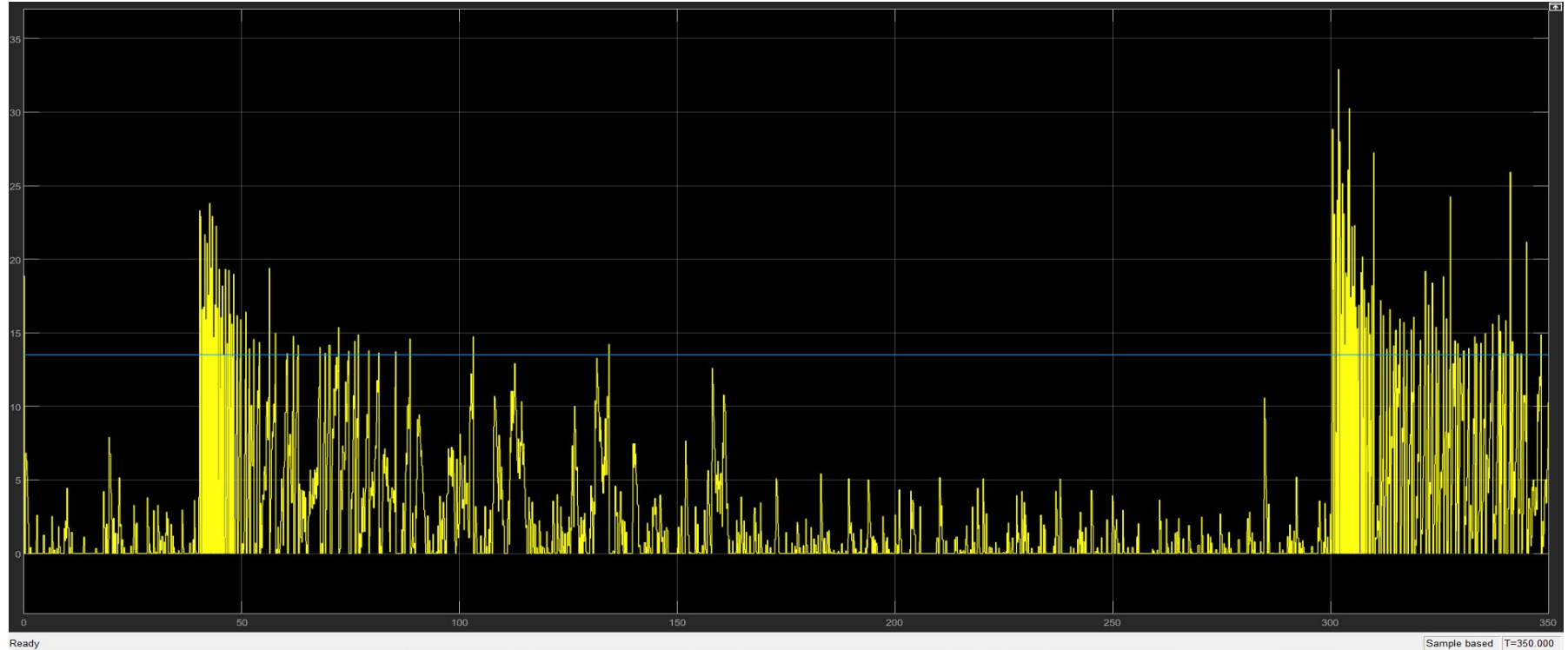
- The detection is detected between two time intervals 40 to 50 and 300 to 310.
- The attack performed was detectable.



Chi-Square Detector in System.



FDI Detector 2: Cumulative Sum (CUSUM) Detector



CUSUM Detector



- CUSUM (Cumulative Sum) is a sequential analysis technique which is used to aggregate the error over an adaptive window.
- CUSUM protects the system against small, but persistent attacks.
- CUSUM is a dynamic detector while Chi-Square detector is static detector which uses a single measurement at a time.
- Given, a chosen distance measure z_k (considered as quadratic distance measure) [1]

$$z_k = r_k^T \Sigma^{-1} r_k$$

But it is possible to drive the CUSUM with any other choice of distance measure.

For a given distance measure, Z_k

CUSUM: $S_1 = 0$,

$$S_k = \max(0, S_{k-1} + z_k - b), \quad \text{if } S_{k-1} \leq \tau,$$

$$S_k = 0 \quad \text{and} \quad \bar{k} = k - 1, \quad \text{if } S_{k-1} > \tau.$$

Design Parameters: bias $b \in \mathbf{R} > 0$ and threshold $\tau \in \mathbf{R} > 0$.

Output: alarm time(s) \bar{k} . [2]


- Since $Z_k \geq 0$, the bias parameter b prevents the inherent growth due to the sum of nonnegative number bias b must be selected properly based on the properties of the distance measure.
- For the tightest detection b is similar to $P(\text{state estimator error Covariance})$ [1].

- Once the bias is chosen, the threshold β must be selected to fulfill a required false alarm rate
- Advantages of the dynamic CUSUM detector is to
 - Maintain sensitivity to low-amplitude but long term attacks.
 - Because of CUSUM bias b is typically selected smaller than the chi-squared threshold α , the attacker capabilities are much reduced using a CUSUM detector since $b < \alpha$ which implies $\gamma_{CS} < \gamma_{\chi^2}$ [1].

However, both chi-squared and CUSUM detectors implement an attack sequence that does not vary with the time.

Therefore, to maintain an equitable comparison between the detectors, a static sequence is selected [1].

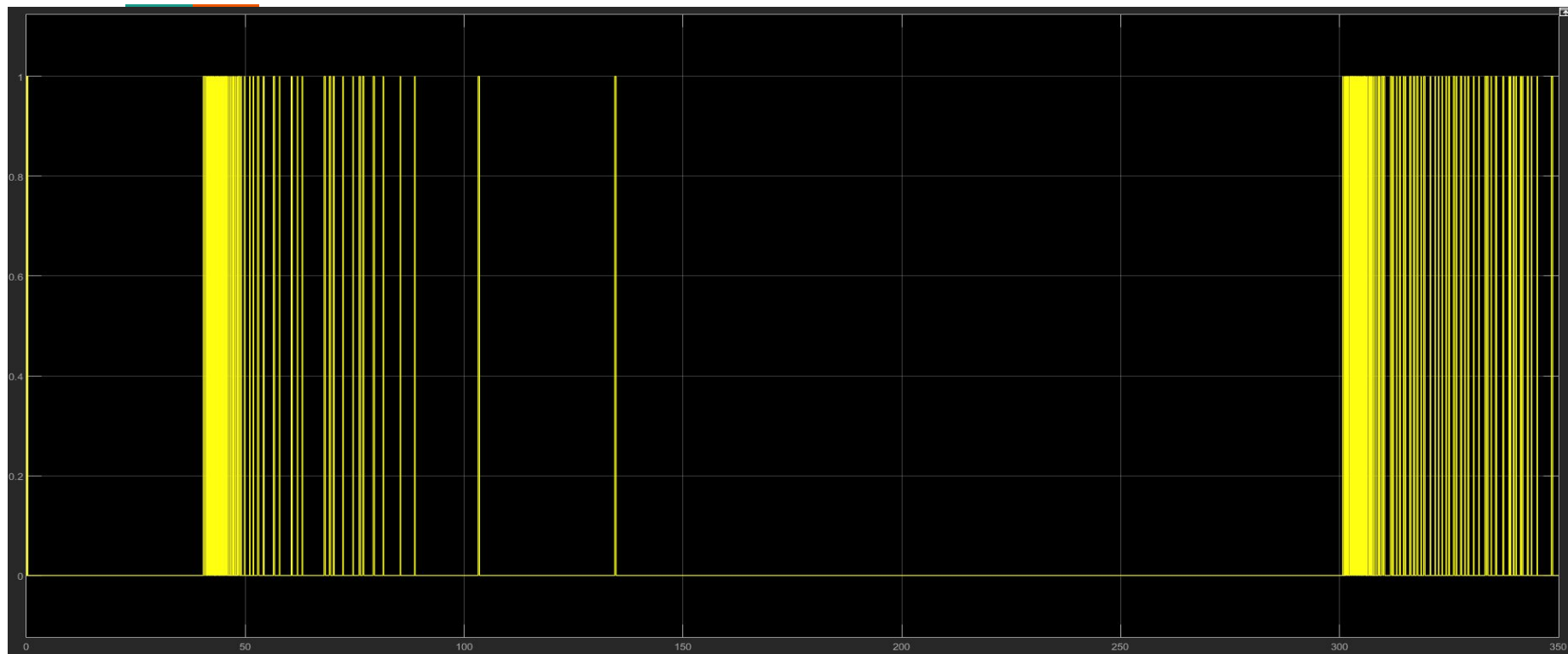
$$\bar{\delta}_k = \bar{\delta} = \frac{\beta}{\ell}$$

- 
- Even if the opponent has access to the parameters of the CUSUM (b, τ), given the stochastic nature of the residuals, the attacker would need to know the complete history of observations (from when the CUSUM was started) to be able to reconstruct S_{k^*-1} from the data.

This is an inherent security advantage in favour of the CUSUM over chi-squared detector.

- Chi-Square detector is Better than CUSUM detector because it can select large false alarm rate ($\approx 40\%$ or larger).
- Empirically, it has been seen that static attack generates the largest steady-state deviation. However, Still this is a future work.

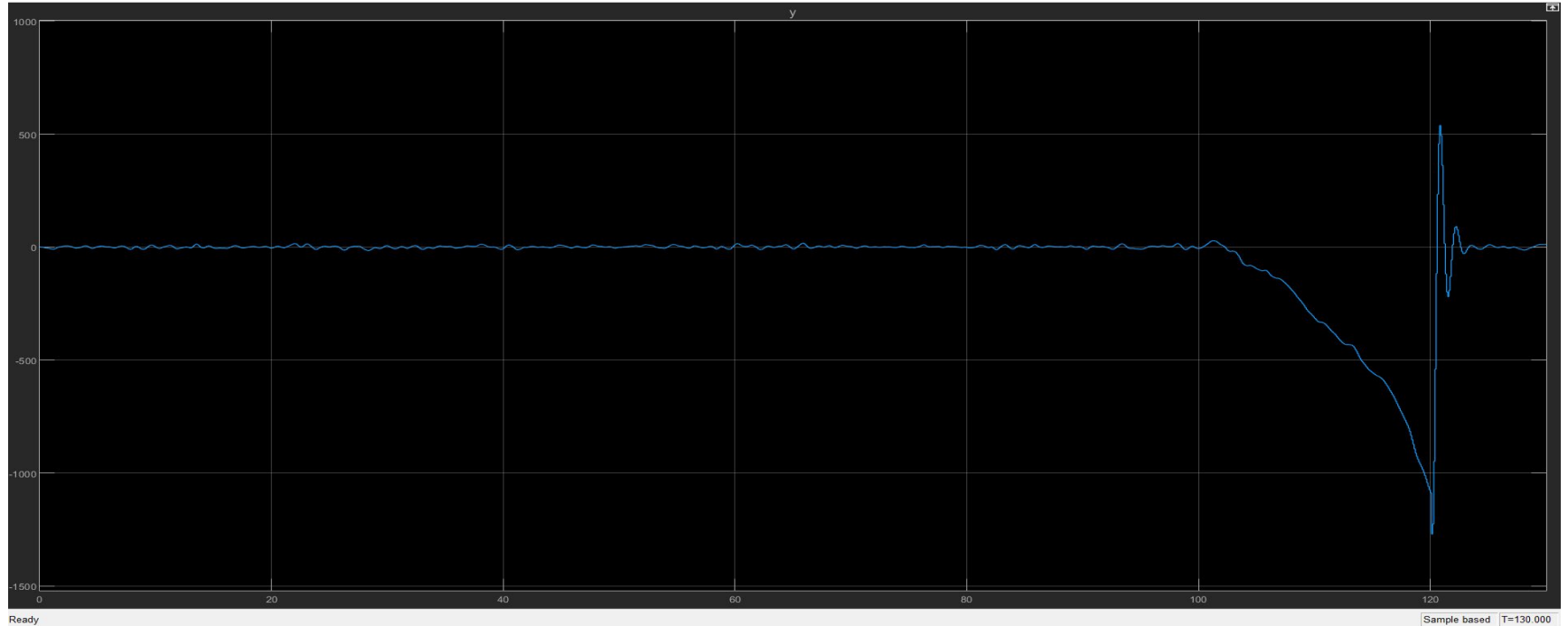
CUSUM Detection



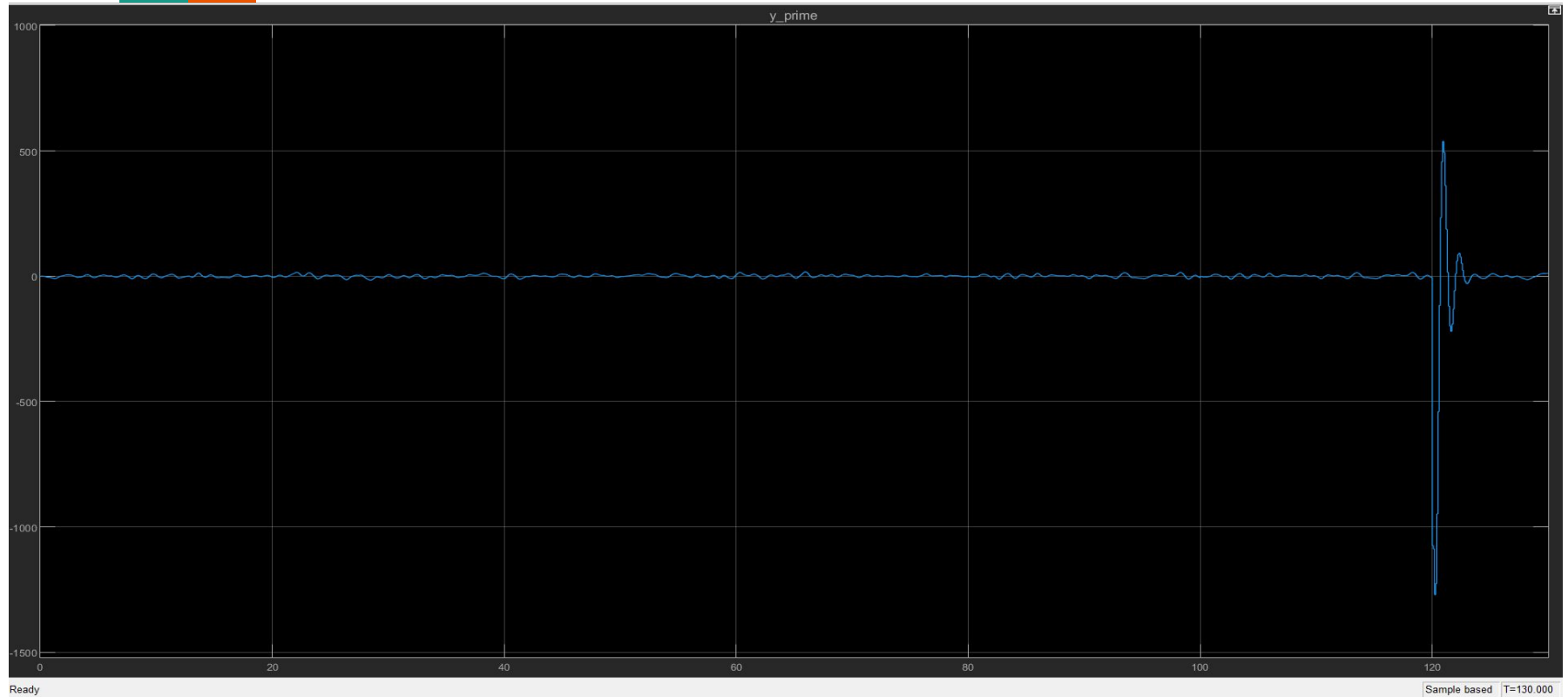
3. Replay Attack



It is done on the Sensor Channel of the system. (Result of signal y)



The below simulink result of attack depicts that it stored the data between 80 to 100 and restored between 100 to 120. (Result of y_{prime} signal)



Replay Attack Analysis

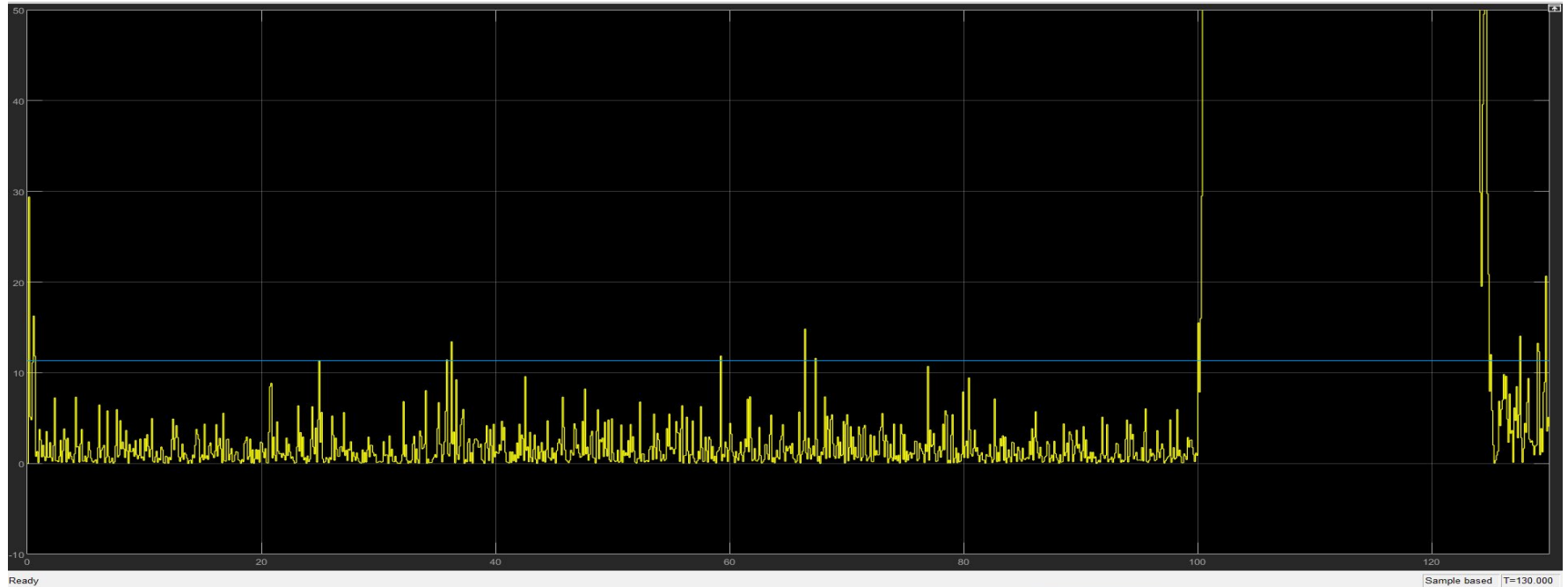


1. The replay attack is stealthy under the steady state condition which are observed from the simulink graph.
2. The attack is undetectable through Chi-Square and CUSUM technique because of steady state condition.
3. For the detection of Replay Attack, a new random noise is required.

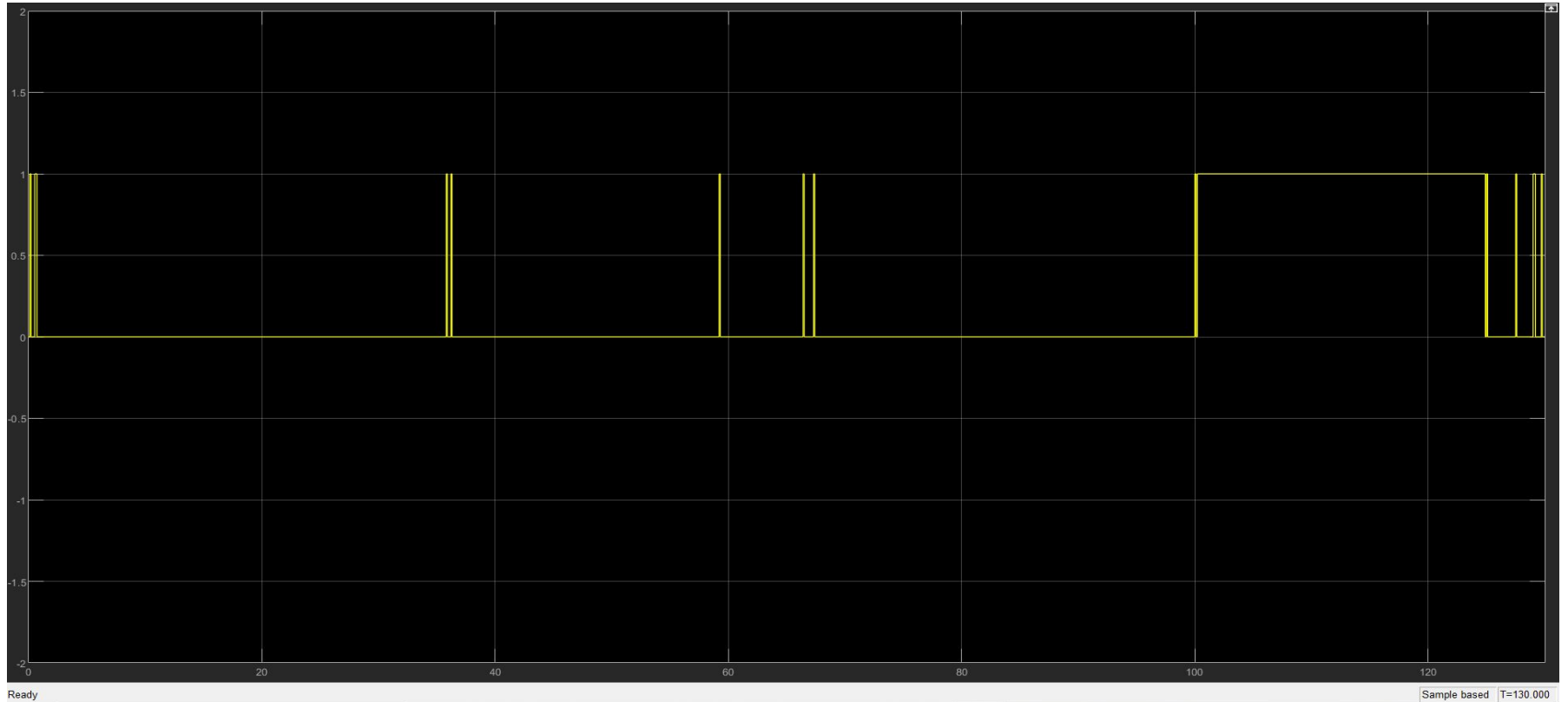
4. Detection of Replay Attack



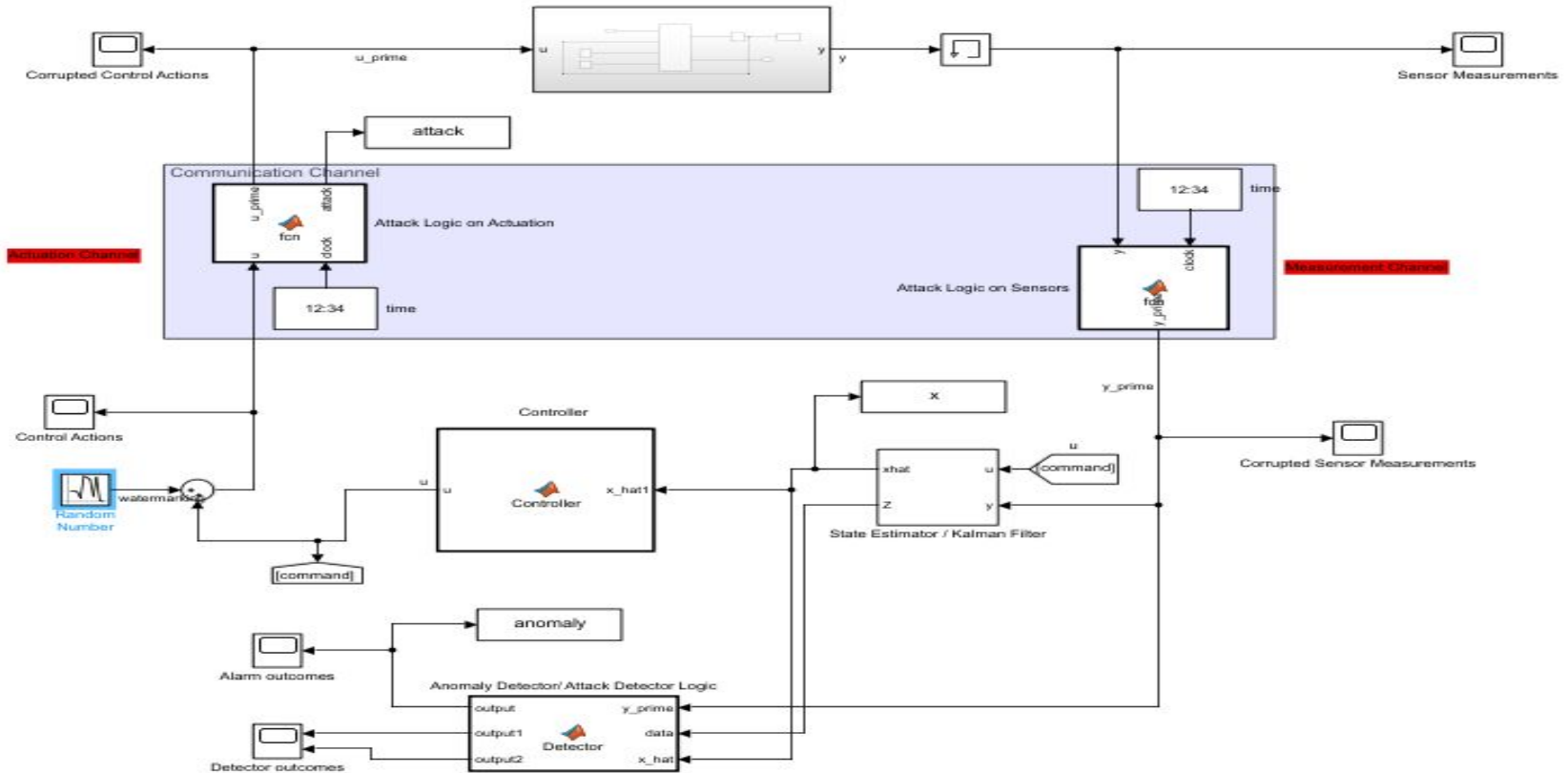
It is done through Watermarking based detection system.



Simulink of Alarm Detection between 100 to 120.



Watermarking Model



Replay Attack Detection Analysis

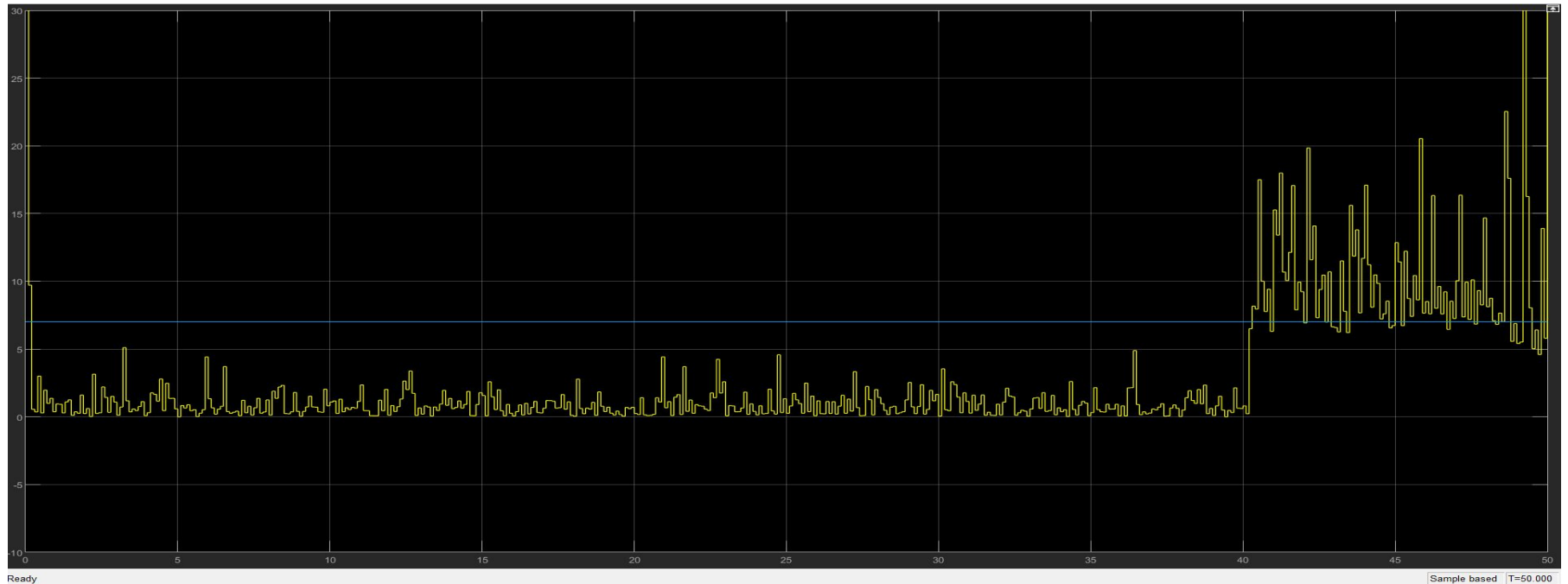


1. The Watermarking signal is incorporated into the sensor input to identify the data introduced by the intruders.
2. The detection mechanism affects the controller performance if the covariance of the detection technique is very large.
3. As per the performed simulink, the control performance is at 0.0001 covariance; where it detected the replay attack.

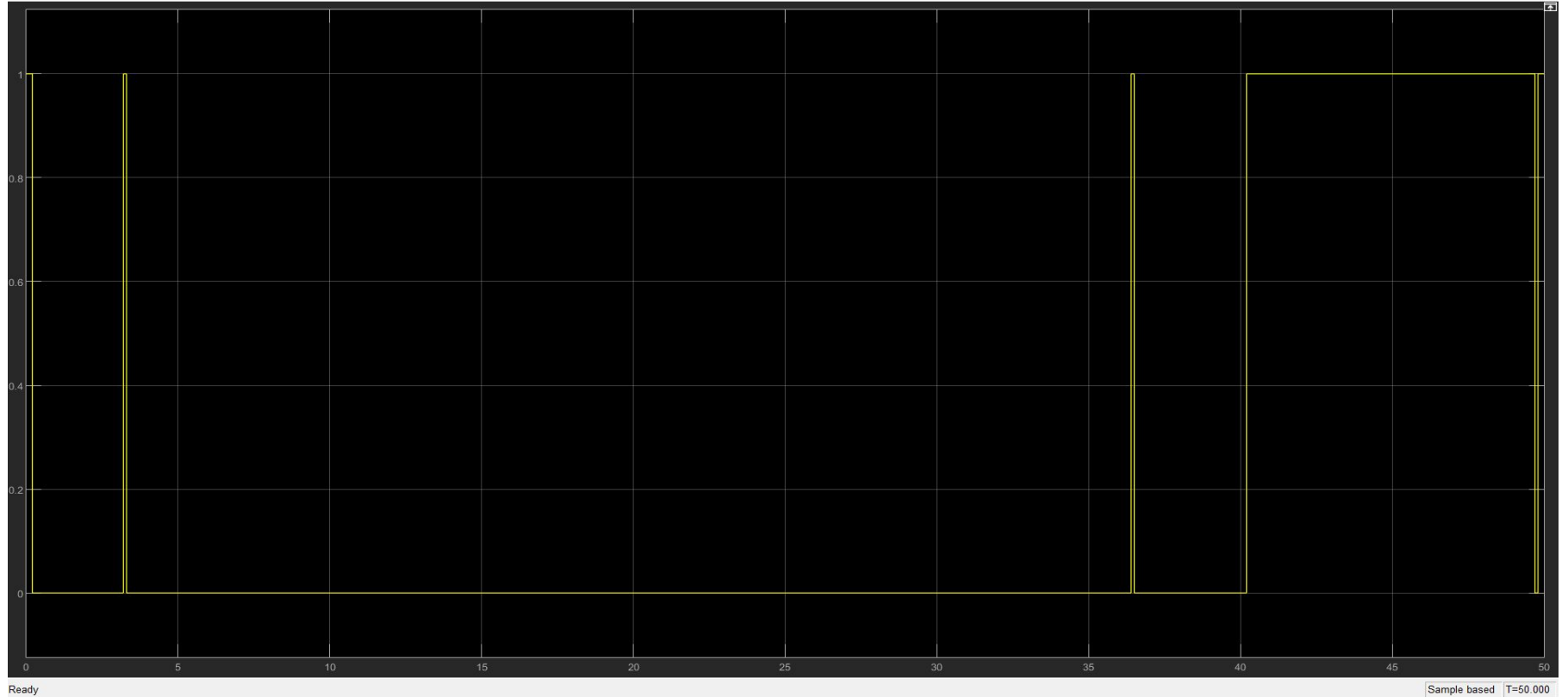
5. Covert Attack



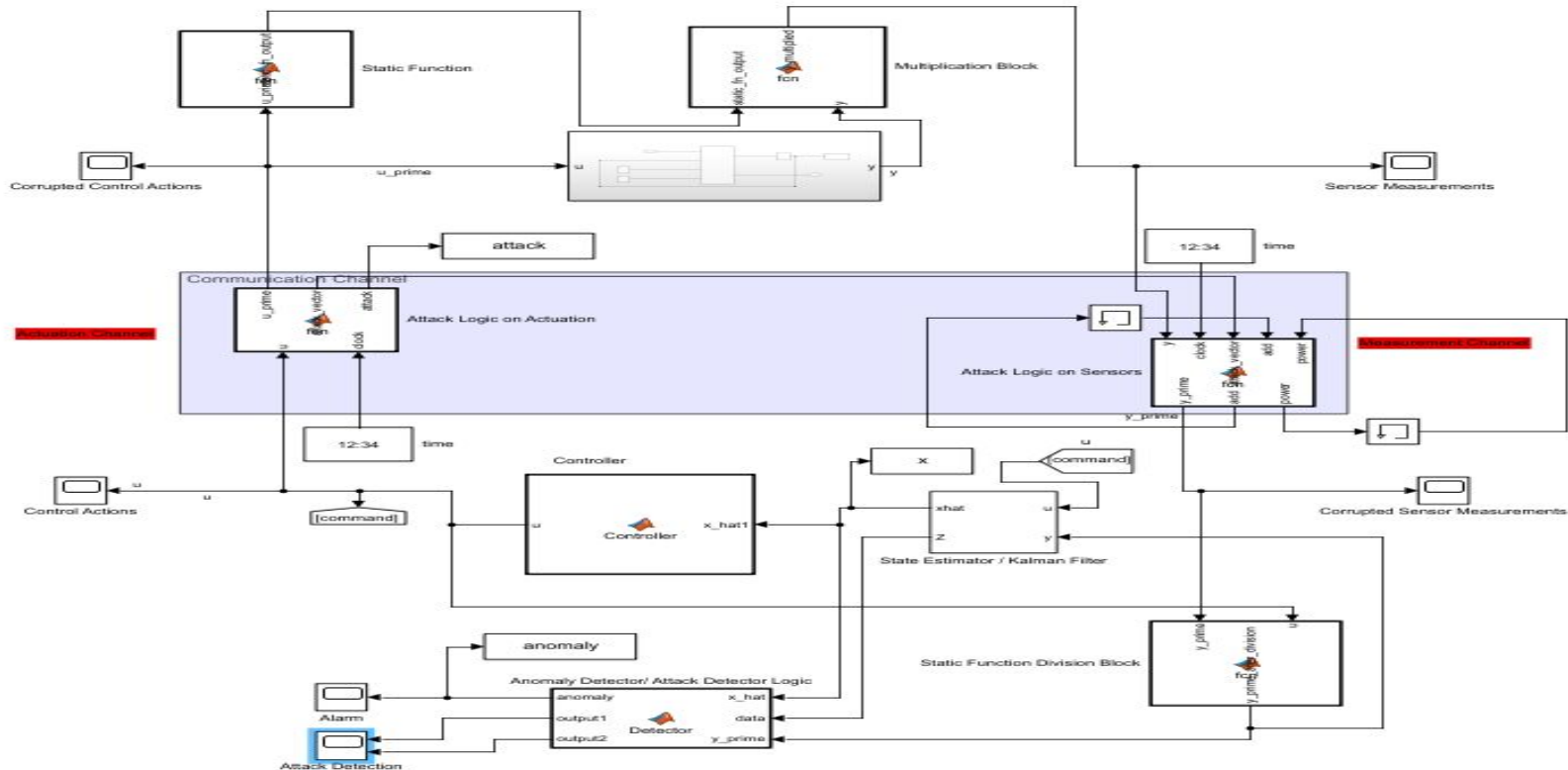
The attack is implemented in the time interval 40 to 50.



Moving Target Detector: the attack was detected between 40 to 50.



Cover Attack, Moving Target Detection Model



Covert Attack Analysis



1. In this attack, the attacker needs to know all the resources: Plant model, Disruptive and Disclosure resources.
2. Moving Target detection technique is used to detect covert attack.
3. The detection mechanism does not affect the controller performance (as it is implemented outside of the plant model).

REFERENCES



- <https://ieeexplore.ieee.org/document/8431073>
- <https://ieeexplore.ieee.org/document/7587875>
- <https://www.mathworks.com/products/statistics.html>
- <https://www.mathworks.com/matlabcentral/answers/104876-matrix-size-mismatch-in-embedded-function-simulink>
- <https://www.mathworks.com/matlabcentral/answers/95310-what-are-algebraic-loops-in-simulink-and-how-do-i-solve-them>
- <https://www.mathworks.com/matlabcentral/answers/54603-how-to-solve-algebraic-loop-error>
- <https://www.mathworks.com/matlabcentral/answers/165862-how-can-i-solve-an-algebraic-loop-error>
- <https://www.mathworks.com/help/simulink/ug/using-the-sim-command.html>
- <https://www.mathworks.com/help/simulink/slref/simulink.simulationoutput-class.html>
- <https://www.youtube.com/watch?v=mCJNuH5PdoU>

- https://www.mathworks.com/help/matlab/data_analysis/time-series-objects.html
- <https://www.mathworks.com/help/matlab/ref/persistent.html>
- <https://www.youtube.com/watch?v=TCRLMPIWwIc>
- <https://www.mathworks.com/help/simulink/slref/unitdelay.html>
- <https://www.mathworks.com/help/simulink/slref/simulationmanager.html>
- <https://blogs.mathworks.com/simulink/2017/09/27/new-in-matlab-r2017b-the-simulation-manager/>
- <https://www.mathworks.com/help/simulink/ug/analyse-results-with-simulation-manager.html>
- https://www.researchgate.net/post/How_to_run_simulink_model_from_matlab_script_for_every_time_instant_and_retain_the_updated_values_in_simulink_model_after_each_run
- <https://www.mathworks.com/matlabcentral/answers/403942-the-block-computed-at-time-is-inf-or-nan>
- https://www.researchgate.net/post/I_am_receiving_the_following_error_msg_in_my_simulink_model_what_should_i_do
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6512826/>
- https://www.researchgate.net/publication/309242563_CUSUM_and_Chi-squared_Attack_Detection_of_Compromised_Sensors
- https://www.researchgate.net/publication/281567648_The_CuSum_algorithm_-_a_small_review

