POLITECNICO DI TORINO

Master Degree
Mechatronic Engineering

Thesis

ATTACKS DETECTION IN DIRECT DATA-DRIVEN CONTROL

Supervisor

prof. Diego Regruto

Student

Gulorom Inoyatova

December 2020

Acknowledgments

I would like to address my sincere acknowledgements to all the people who have helped me and who have contributed directly or indirectly to the writing of this thesis.

I would first like to acknowledge my thesis supervisor, Professor Diego Regruto, *Associate Professor of Automatic Control, Dipartimento di Automatica e Informatica* at Politecnico di Torino. Without his trust and enthusiasm, this thesis could not have been successfully conduced. I would as well like to thank the teachers and speakers who participated in my two-year degree. They consistently shared meaningful experiences and valuable learnings, which steered me in the right direction.

This paper is also the result of my final year internship at Manganorobot Srl, an Italian automation company based in Turin and operating all over the world. I would like to thank my manager Daniele Mangano, Chief Executive Office, for his warm welcome, his availability, and giving me the great opportunity to actively participate in the growth of Manganorobot Srl; as well as my colleagues that always shared their valuable experiences and advices during my internship.

Finally, I must express my profound gratitude to my family and friends for providing me with unfailing support and continuous encouragement. This accomplishment would not have been possible without them. Thank you.

TABLE OF CONTENTS

i. Abstract

A scope of the thesis work is to detect attacks that may compromise the work of sensor and/or actuator in the direct data-driven control. Attacks which potentially may violate the work of sensors and actuators, consequently may do the same with an outcome of the controller and of the entire system.

The main concept of the direct data-driven control is to design a controller which will correspond output of the system to a given reference model, having in disposition only measured input and output data; in other words, without knowing the exact structure and mathematical model of the plant itself.

Taking into consideration the errors that may interfere with the signal during the measurement of the input and output data, the feasible controller parameter set is defined. The final controller is designed by choosing suitable parameters from the previously defined feasible set.

In order to identify false control commands to actuators and false sensor readings, in this thesis work we study a new approach of attack detection. The study is divided into two steps:

1. Detecting an attack in a closed feedback loop system.
2. Distinguishing the attacks on the sensor and on the actuator separately.

ii. Introduction. Objective of the thesis.

In this thesis work we will focus on detecting attacks that may disturb the appropriate work of the sensors and of the actuators. Using input-output data of the system we propose a method of real-time attacks detection which could be directly implemented after a feasible controller in SM-DDDC has been designed.

We consider the following control system:

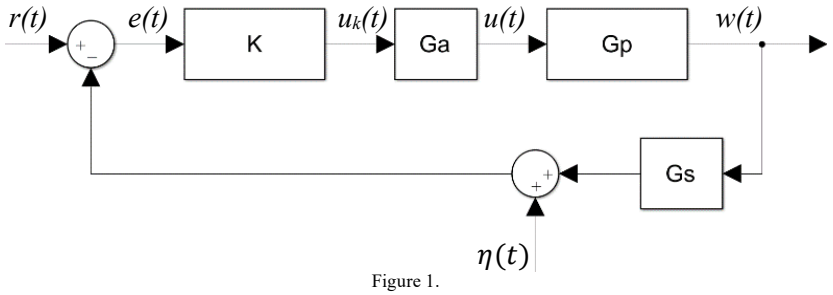

Figure 1.

where

- $G_p(q^{-1})$ is unknown plant model
- G_a is actuator model: assumed to be known constant gain
- G_s is sensor model: assumed to be known constant gain
- $K(q^{-1})$ is controller obtained through set membership in direct data-driven control approach
- $\eta(t)$ is unknown, but bounded $|\eta(t)| \leq \Delta\eta$

$K(q^{-1})$ has been already designed by using the set-membership (SM) in the direct data-driven control (DDDC) technique presented in the chapter **iv. Direct data-driven control (p.8).**
More precisely here we assume that:
The attention is focused on a specific given reference signal *r(t)*.
The feasible controller parameter set (FCPS) has been obtained assuming that $|\eta(t)| \leq \Delta\eta$.
A particular controller belonging to the feasible controller parameter set has been implemented.

The focus here is on discrete-time system (DT).

The general framework is the assumption that generically the system has a spatially distributed character - in the sense that information between controller and actuator, sensor and controller, are exchanged through communication links that are potentially subjected to external attacks, that aimed to modify or to compromise the behavior of the actuator and/or sensor.

Assumptions:

- The communication links are delay-free
- The attacks **cannot** corrupt the controller $K(q^{-1})$, but only G_a and/or G_s [Note that here G_a and G_s are constant values]

Objective of the work:

- To propose a method for detecting (on-line) the presence of an attack
- To discriminate if the attack is affecting only the sensor or also the actuator

Motivation and Novelty: Most of the work in this field rely on the exact knowledge of the mathematical model of the plant to detect and counteract the attacks. We are proposing a model free (data-driven) approach (in the framework of DDDC).

iii. Set membership. Basic overview.

In this section we will review fundamental results on SM identification theory. The interested reader can find details in the paper 'Set-Membership Error-in-Variables Identification Through Convex Relaxation Techniques' [1] and 'Improved parameters bounds for set-membership EIV problems' [2].

In many problems - such as, linear and nonlinear regressions, parameter and state estimation of dynamic systems, state space and time series prediction - using the data available, unknown variables are subject of evaluation. The data are always associated with some uncertainty and it is necessary to evaluate how this uncertainty affects the estimated variables.

Typically, the problem is approached assuming a probabilistic description of uncertainty and applying a statistical estimation theory. Set membership or unknown but bounded (UBB) error description is another way of solving the problem of uncertainty. With this approach, uncertainty is described by an additive noise which is known only to have given integral or component wise bounds.

In real life examples, when it is necessary to measure input and output data of the system, the collected information is corrupted by a noise. Since the only available information about this additive noise is its bound, the effect of the noise on parameter of the system to be calculated are taken into consideration by using set membership approach.

In our case, we consider the set-membership error-in-variables identification problem.
The main focus of this approach is the computation of parameter bounds, taking explicitly into account a priori information on system stability, in the set-membership error-in-variable (EIV) framework, that is when input and output signals are corrupted by bounded noise.

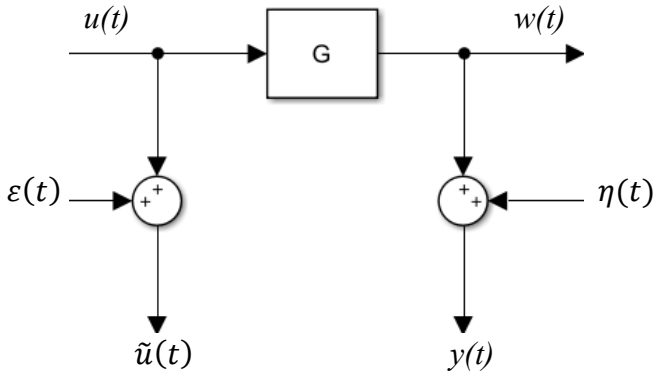

Figure 2.

All the results obtained from the calculations are considered to be in the small neighborhood, bounded by maximum and minimum values of the parameters, that is a set of all values that satisfy the given conditions.

[1] V. Cerone; D. Piga; D. Regruto Set-Membership Error-in-Variables Identification Through Convex Relaxation Techniques. IEEE TRANSACTIONS ON AUTOMATIC CONTROL, Vol.57, No. 2, pp.517-522, 2012
[2] V. Cerone; D. Piga; D. Regruto Improved parameters bounds for set-membership EIV problems. INTERNATIONAL JOURNAL OF ADAPTIVE CONTROL AND SIGNAL PROCESSING, Vol.25, No. 3, pp.208-227, 2011

iv. Direct data-driven control

DDC approach is of particular interest in real-world practical application where an exact and accurate model of the plant to be controlled is not available. Data-driven control approaches do not rely on plant model identification, since available input-output data experimentally collected from the plant can be directly used to design the controller.

More explicit detail on this topic can be found in papers 'Direct data-driven control design through set-membership errors-in-variables identification techniques' [3] and 'A set-membership approach to direct data-driven control design for SISO non-minimum phase plants' [4].

In the "classical" approach of designing robust controller, we choose a mathematical model of the plant affected by uncertainty

(Eq.1) $$G_p(q^{-1}) = \frac{\beta_0+\beta_1*q^{-1}+\cdots+\beta_m*q^{-m}}{1+\alpha_1*q^{-1}+\cdots+\alpha_n*q^{-n}}, \qquad \beta_i \in \left[\underline{\beta}_i,\ \overline{\beta}_i\right],\ \alpha_j \in \left[\underline{\alpha}_j,\ \overline{\alpha}_j\right]$$

In this case, the objective is to design a controller $K(q^{-1})$ such that the following control system

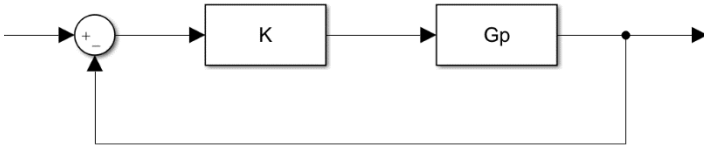

Figure 3.

is stable for all $\beta_i \in \left[\underline{\beta}_i,\ \overline{\beta}_i\right], \alpha_j \in \left[\underline{\alpha}_j,\ \overline{\alpha}_j\right]$ and fullfill assigned performance specifications for all $\beta_i \in \left[\underline{\beta}_i,\ \overline{\beta}_i\right], \alpha_j \in \left[\underline{\alpha}_j,\ \overline{\alpha}_j\right]$.

The procedure consists of two steps:

1. An unknown model of the plant G_p is obtained by means of Set memebership identification from a set of noisy data.
2. A robust controller is designed based on the identified uncertain model.

   Remarks:

   a) Initial data of the problem are just collected input-output sequences.
   b) The uncertainty in the model comes from the uncertianty (noise) affecting the collected data.

[3] V. Cerone, D. Regruto, M. Abuabiah "Direct data-driven control design through set-membership errors-in-variables identification techniques", 2017 American Control Conference (ACC), 388-393

[4] V. Cerone, D. Regruto, M. Abuabiah "A set-membership approach to direct data-driven control design for SISO non-minimum phase plants", 2017 IEEE 56th Annual Conference on Decision and Control (CDC), 1284-1290

On the other hand, in the direct data-driven control (DDDC), the scope is to design the controller starting directly from the collected input-output data.

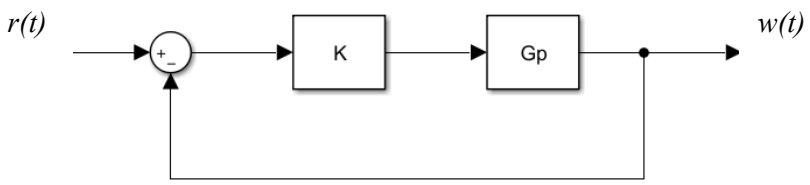

Figure 4.

We assume that a reference model $M(q^{-1})$ is given, where $M(q^{-1})$ describes the desired behavior of the controlled system, i.e. $M(q^{-1})$ is the desired closed-loop transfer function from *r* to *w*.

(Eq.2)
$$T(q^{-1}) = \frac{K(\rho,q^{-1})*G_p(q^{-1})}{1+K(\rho,q^{-1})*G_p(q^{-1})}$$

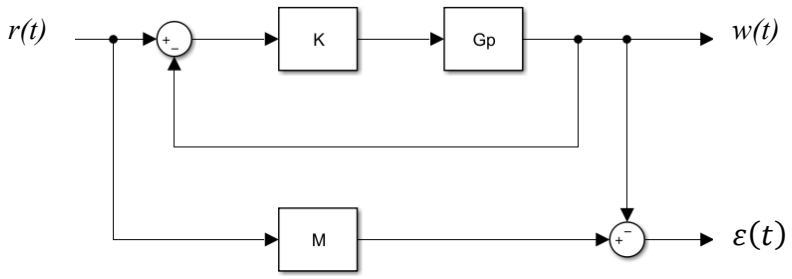

Figure 5.

Starting from a set of input-output data experimentally collected on the plant, find a controller $K(\rho, q^{-1})$ such that:

(Eq.3)
$$\varepsilon(t) = M(q^{-1}) * r(t) - T(q^{-1}) * r(t) = 0$$

The Feasible Controller Set (FCS) is defined as the set of all controllers belonging to a given class such that the Eq. 3 is satisfied for a noise sequence $\eta(t)$ satisfying the bound

$$|\eta(t)| \leq \Delta\eta, \quad \forall t = 1, \ldots, N$$

Feasible Controller Parameter Set (FCPS) is defined as the set of all the controller parameters ρ such that the Eq. 3 is satisfied.

v. Collecting data and designing of controller.

In order to design the controller, output data should be collected directly from the plant.

The measured output *w(t)* is corrupted by the noise $\eta(t)$, which is unknown, but bounded by $\Delta\eta$.

The data are measured every second during 100 seconds.

Saved input and output data is used to design feasible controller parameter set (FCPS) in set membership using direct data-driven control technique.

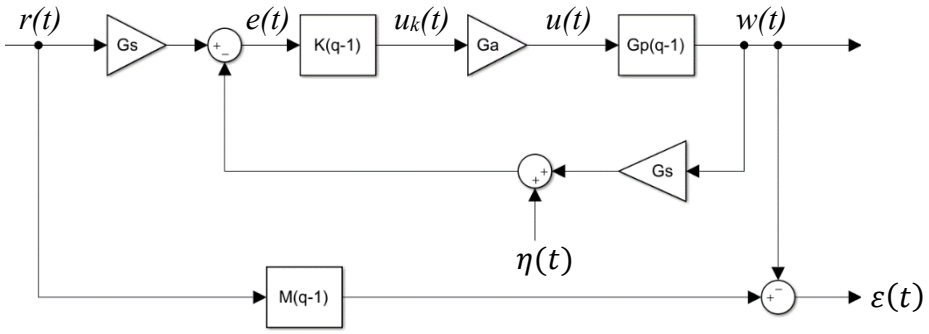

Figure 6.

We would like to design controller able to match our reference model $M(q^{-1})$ by means of DDDC. In order to characterizing a set of all controllers that are matching the reference model $M(q^{-1})$, we consider not open loop system, but directly close loop system, such that $T(q^{-1}) = M(q^{-1})$.

(Eq.4) $$M(q^{-1}) * r(t) - T(q^{-1}) * r(t) = 0$$

(Eq.5) $$T(q^{-1}) = \frac{K(q^{-1})*G_a*G_p(q^{-1})*G_s}{1+K(q^{-1})*G_a*G_p(q^{-1})*G_s}$$

$$M(q^{-1}) * r(t) - \frac{K(q^{-1}) * G_a * G_p(q^{-1}) * G_s}{1 + K(q^{-1}) * G_a * G_p(q^{-1}) * G_s} * r(t) = 0$$

$$M * r(t) = K(q^{-1}) * G_a * G_p(q^{-1}) * G_s * r(t) - K(q^{-1}) * G_a * G_p(q^{-1}) * G_s * M * r(t)$$

$$M(q^{-1}) * r(t) = K(q^{-1}) * G_a * G_p(q^{-1}) * G_s * r(t) * (1 - M(q^{-1}))$$

(Eq.6) $$K(q^{-1}) = \frac{M(q^{-1})}{(1-M(q^{-1}))*G_a*G_p(q^{-1})*G_s} * r(t)$$

The controller K (q^{-1}) is designed such that the output of the closed loop system is the same as the output of the reference model to which the reference signal r(t) is applied.

vi. Objective 1. Detecting presence of attacks on sensor or actuator.

vi.i. Attack detection.

In order to obtain condition for detecting the presence of an effective attack, we firstly review the concept of "feasible controller", derived in chapter ***v. Collecting data and designing of controller.***

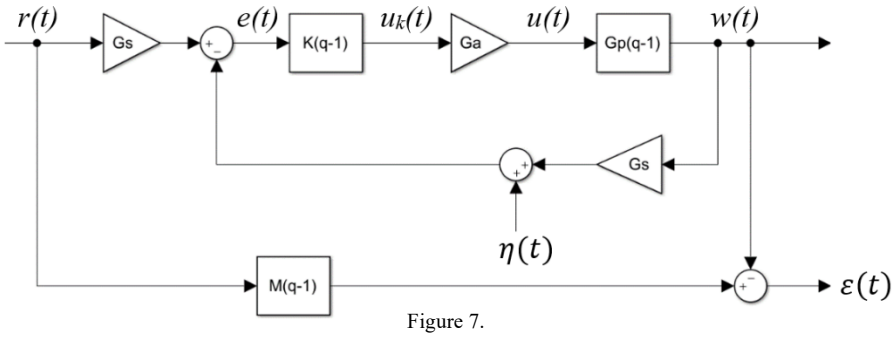

Figure 7.

The controller $K(q^{-1})$ solving the set membership direct data-driven control is, by construction, such that it solves the following model matching problem:

(Eq.7) $$M(q^{-1}) * r(t) = T(q^{-1}) * r(t)$$

Starting from this equation we want to derive a "model-free" (data-driven) condition to detect the presence of an attack.

Since $G_p(q^{-1})$ is unknown, $T(q^{-1})$ is also not known.

Let's consider the following equations from Figure 7 to derive $T(q^{-1}) * r(t)$:

- $w(t) = e(t) * K * G_a * G_p$
- $e(t) = G_s * r(t) - y(t)$
- $y(t) = G_s * w(t) + \eta(t)$

$$\Rightarrow w(t) = (G_s * r(t) - G_s * w(t) - \eta(t)) * K(q^{-1}) * G_a * G_p(q^{-1})$$

$$w(t) + w(t) * K * G_a * G_p * G_s = r(t) * K * G_a * G_p * G_s - \eta(t) * K * G_a * G_p$$

$$w(t) * (1 + K * G_a * G_p * G_s) = (r(t) * G_s - \eta(t)) * K * G_a * G_p$$

$$w(t) = \frac{T(q^{-1})}{G_s} * (G_s * r - \eta(t))$$

(Eq.8) $$T(q^{-1}) * r(t) = w(t) + \frac{T(q^{-1})}{G_s} * \eta(t)$$

By filling Eq.8 in to Eq.7, we get:

(Eq.9) $$M(q^{-1}) * r(t) = w(t) + \frac{T(q^{-1})}{G_s} * \eta(t)$$

Now, we would like to derive equation for reference signal $r(t)$:

- $e(t) = G_s * r(t) - G_s * w(t) - \eta(t)$
- $u_k(t) = K(q^{-1}) * e(t)$

$$\Rightarrow \quad K^{-1}(q^{-1}) * u_k(t) = G_s * r(t) - G_s * w(t) - \eta(t)$$

(Eq.10) $$r(t) = \frac{u_k(t)}{K(q^{-1}) * G_s} + w(t) + \frac{\eta(t)}{G_s}$$

By merging Eq.9 and Eq.10, we get:

$$\frac{M(q^{-1}) * u_k(t)}{K(q^{-1}) * G_s} + M(q^{-1}) * w(t) + \frac{M(q^{-1}) * \eta(t)}{G_s} = w(t) + \frac{T(q^{-1}) * \eta(t)}{G_s}$$

$$M * u_k(t) + M * K * G_s * w(t) + K * M * \eta(t) = w(t) * K * G_s + T * K * \eta(t)$$

$$M * u_k(t) + K * G_s * w(t) * (M - 1) = K * (T - M) * \eta(t)$$

We would like to apply some simplification, considering that, firstly, T is very close to M, since the main idea is to match one system to another and, secondly, usually noise $\eta(t)$, that is corrupting our output signal is high frequency signal. Following our simplification arguments, in a "well designed" control system we can reasonably assume that:

- $M \cong T \implies (T - M)$ is "small"
- $M \quad and \quad T$ are low pass filters
- $\eta(t)$ is a high frequency signal

$\Rightarrow K * (T - M) * \eta(t)$ can be neglected

Thanks to this reasonable simplification we obtain the following result:

Result 1

The controller $K(q^{-1})$ is such that at each time *t* the following condition is satisfied:

$$K(q^{-1}) * G_s * w(t) = \frac{M(q^{-1})}{(1 - M(q^{-1}))} * u_k(t)$$

$$y(t) = G_s * w(t) + \eta(t) \qquad \Rightarrow \qquad G_s * w(t) = y(t) - \eta(t)$$

(Eq.11) $$K(q^{-1}) * y(t) - K(q^{-1}) * \eta(t) = \frac{M(q^{-1})}{(1 - M(q^{-1}))} * u_k(t)$$

From Result 1 and Eq.11, the following condition is derived:

Result 2

At each time *t* the controller $K(q^{-1})$ is such that:

(Eq.12)
$$\left|K(q^{-1}) * y(t) - \frac{M(q^{-1})}{(1-M(q^{-1}))} * u_k(t)\right| \leq \|K(q^{-1})\|_1 * \Delta\eta$$

$$\|K(q^{-1})\|_1 * \Delta\eta = \Delta f$$

where $\|K(q^{-1})\|_1$ is the L_1-norm of the system $K(q^{-1})$ and $\Delta\eta$ is the bound on the noise.

Proof of the Result 2

From Eq.11 we can write:

$$K(q^{-1}) * y(t) - \frac{M(q^{-1})}{(1 - M(q^{-1}))} * u_k(t) = K(q^{-1}) * \eta(t)$$

$$\left|K(q^{-1}) * y(t) - \frac{M(q^{-1})}{(1 - M(q^{-1}))} * u_k(t)\right| \leq \max(K(q^{-1}) * \eta(t)) \quad \forall t$$

From result on linear system theory

$$\max(K(q^{-1}) * \eta(t)) = \|K(q^{-1})\|_1 * \|\eta(t)\|_\infty$$

and since $\|\eta(t)\|_\infty = \Delta\eta$

$$\left|K(q^{-1}) * y(t) - \frac{M(q^{-1})}{(1 - M(q^{-1}))} * u_k(t)\right| \leq \|K(q^{-1})\|_1 * \Delta\eta$$

Note:
$\|K(q^{-1})\|_1$ is calculated as following:

$$\|K(q^{-1})\|_1 = \|h_k\|_1$$

where $\|h_k\|_1$ is the L_1-norm of the vector $[h_1\ h_2\ h_3\ \ldots\ldots]$
and $h_1\ h_2\ h_3$ are the samples of the impulse response of $K(q^{-1})$

If there is an attack, then the final effect of the attack is to change $w(t)$ and then also to change $y(t)$. In this situation there may be two different cases.

Case 1: the effect of the attack is such that for the considered controller $K(q^{-1})$ Eq.12 is still satisfied. In this case the attack is **NOT effective.**

Case 2: the effect of the attack is such that for the considered controller $K(q^{-1})$ Eq.12 is NOT satisfied. In this case the attack is **effective.**

The objective is to detect the presence of an **effective** attack.

From Result 2 it is obtained:

Result 3

At time *t* the attack is effective if and only if the controller $K(q^{-1})$ is no more feasible which is equivalent to say that the collected output $y(t)$ is such that:

(Eq.13) $$\left| K(q^{-1}) * y(t) - \frac{M(q^{-1})}{(1-M(q^{-1}))} * u_k(t) \right| > \Delta f$$

If condition in Eq.13 is satisfied, it means that there is attack or attacks on sensor and/or actuator.

vi.ii. The simulation in Simulink

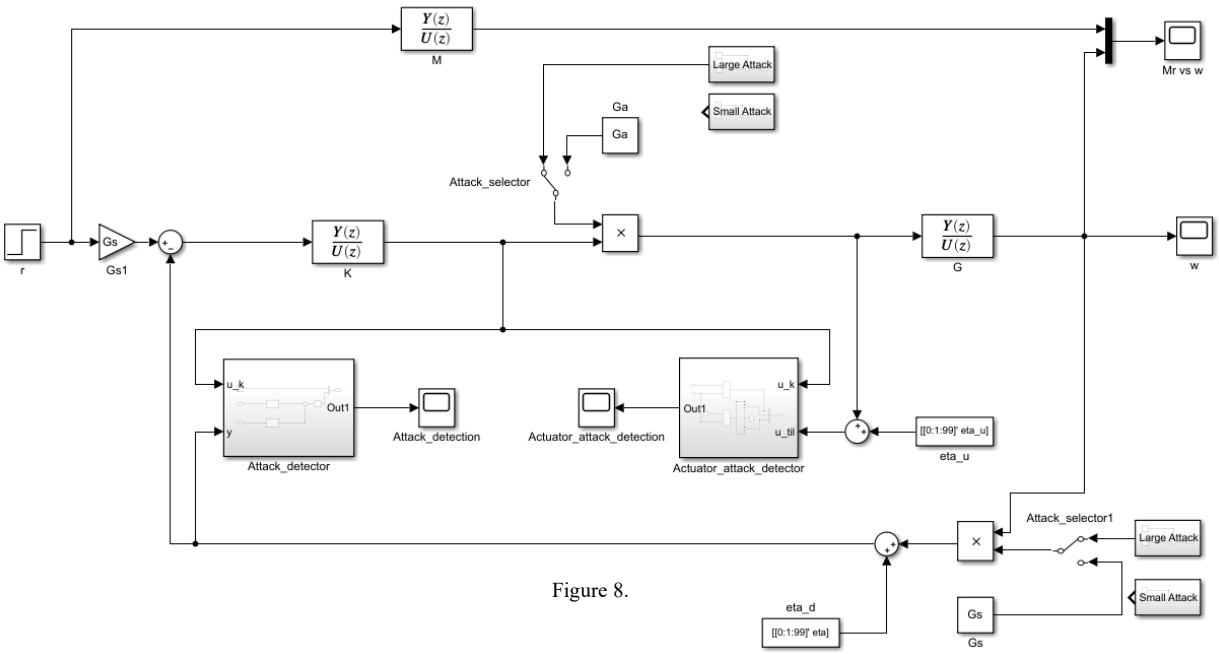

Figure 8.

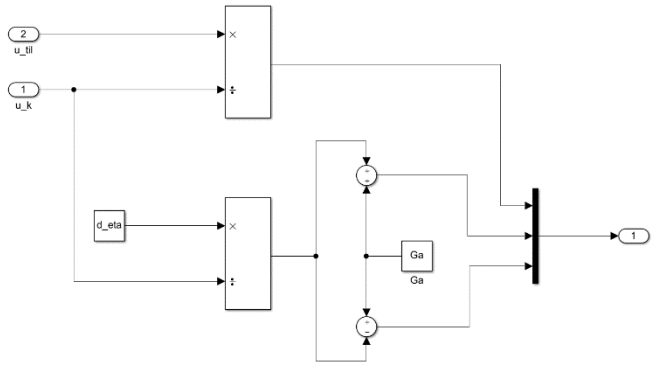

Figure 9. 'Attack detector' block

The simulation in Simulink (Figure 8) was done by changing output signal which is coming from sensor and actuator. The figures below depict different scope of results of the signal coming from block of 'Attack detector' (Figure 9) affected by small and large attacks:

1. Without any attack.
2. Small attack on sensor only.
3. Small attack on actuator only.
4. Small attack on actuator and sensor together.
5. Large attack on sensor only.
6. Large attack on actuator only.
7. Large attack on actuator and sensor together.

Studying the change of output of the 'Attack detector' block affected by the small attack on the system.

The system is corrupted by small attacks, that were acting on actuator and sensor from 10^{th} till 50^{th} second starting from the beginning of simulation. Below are the simulation graphs, output signals from actuator and sensor and the way attacks influence the matching problem:

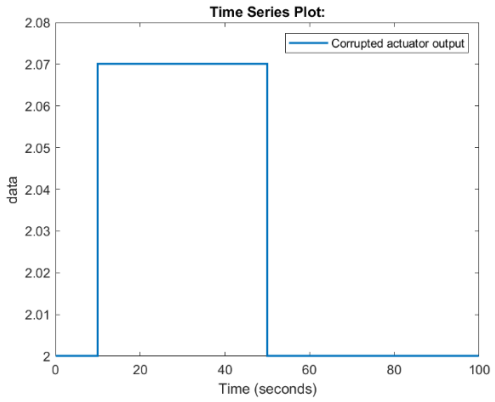

Figure 10. Small attack changes output of the actuator

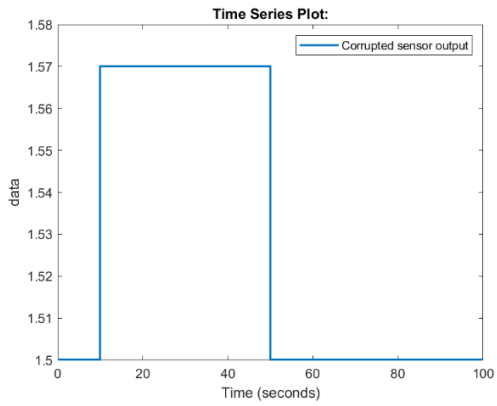

Figure 11. Small attack changes output of the sensor

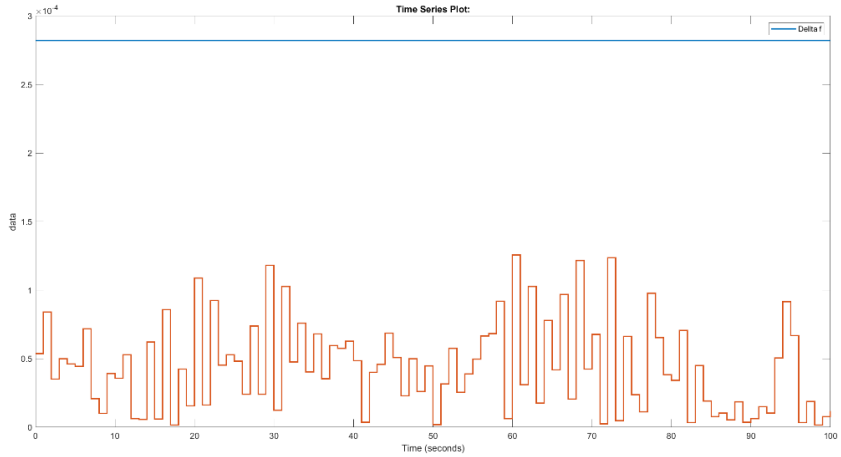

Figure 12. Attack detection without any attack. The evidence of the Result 2, Eq.12

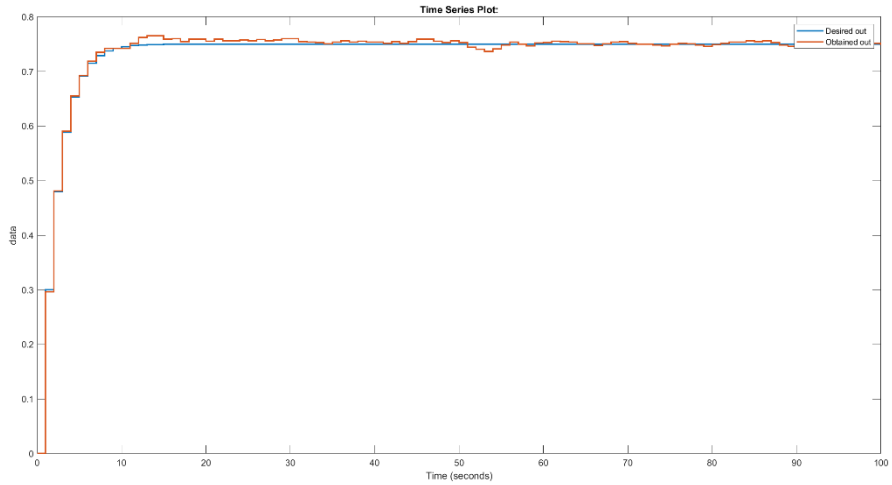

Figure 13. Comparison between outputs of the reference model and the designed control system in presence of small attack on actuator

In Figure 13, 'Desired out' is the output from Reference model M, and 'Obtained out' is output of the system. The plot of the outputs does not show clearly the presence of an attack in the system. But on the Figure 14, the attack is detected correctly.

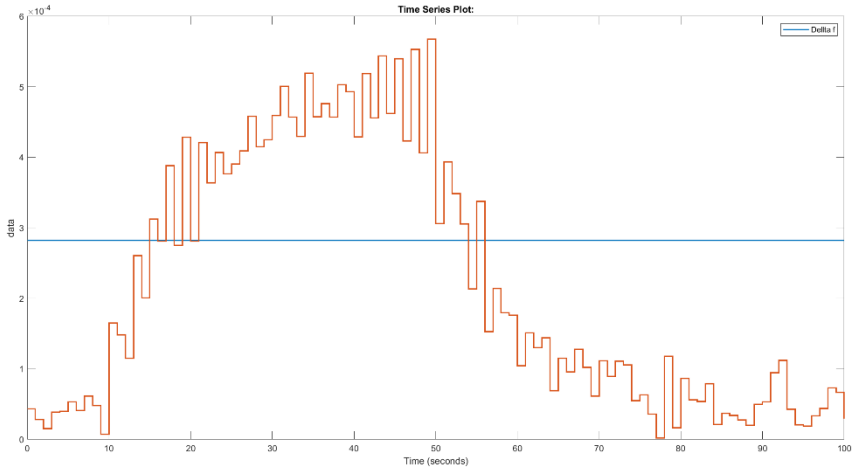

Figure 14. Attack detection with sensor being under small attack

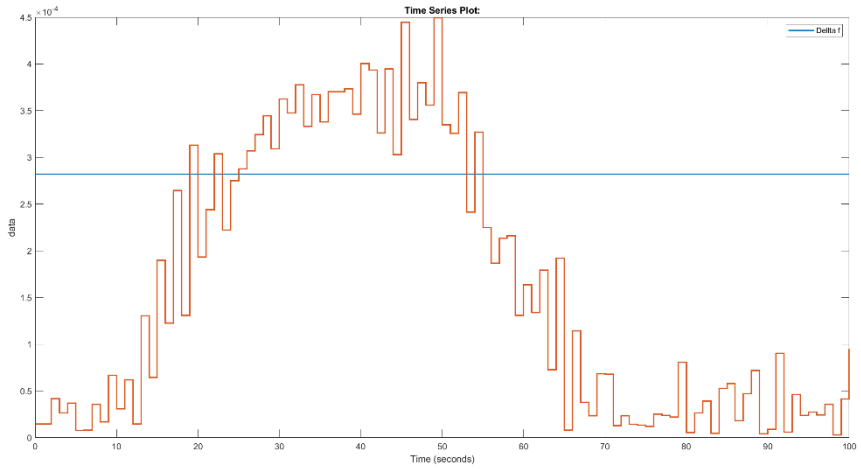

Figure 15. Attack detection with actuator being under small attack

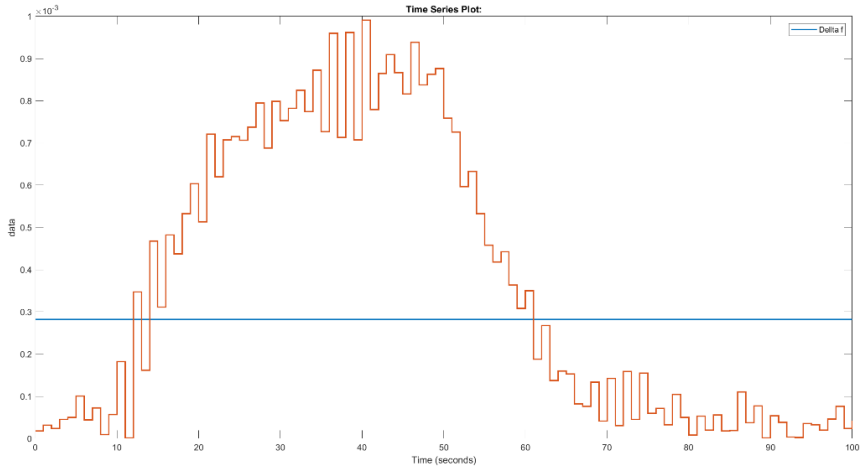

Figure 16. Attack detection with sensor and actuator being under small attack

Studying the change of output of the 'Attack detector' block affected by the large attack on the system.

The system is corrupted by large attacks, that were acting on actuator and sensor from 10^{th} till 50^{th} second starting from the beginning of simulation. Output signals from actuator and sensor have the following shapes, correspondingly:

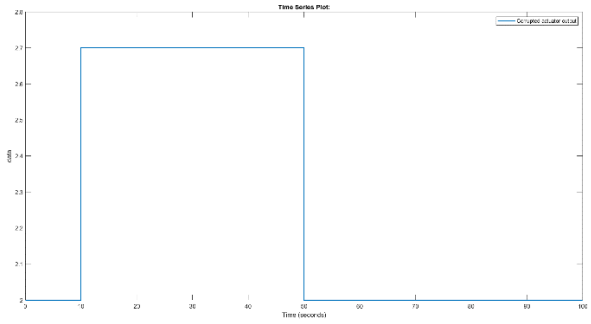

Figure 17. Large attack changes output of the actuator

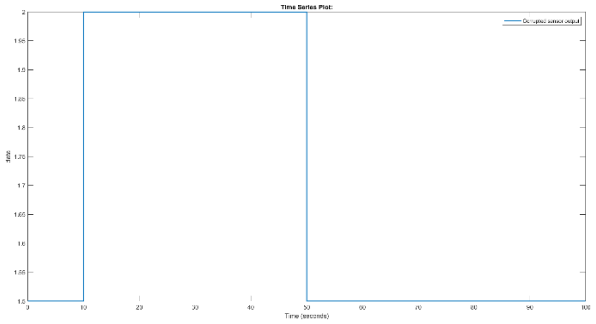

Figure 18. Large attack changes output of the sensor

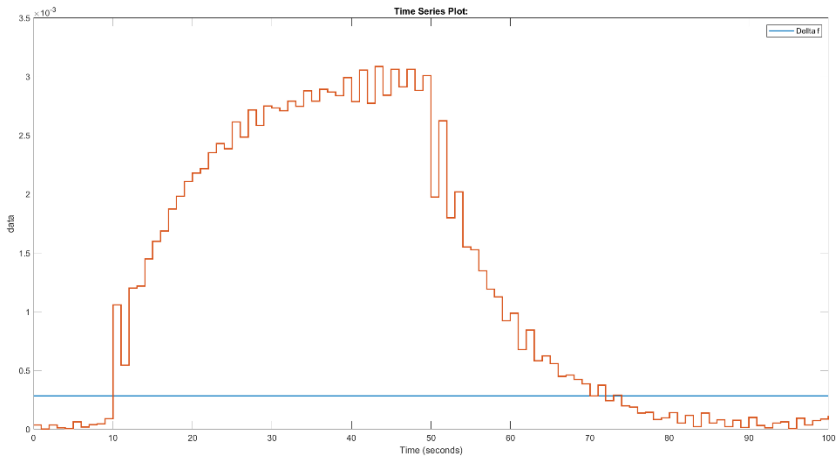

Figure 19. Attack detection with sensor being under large attack

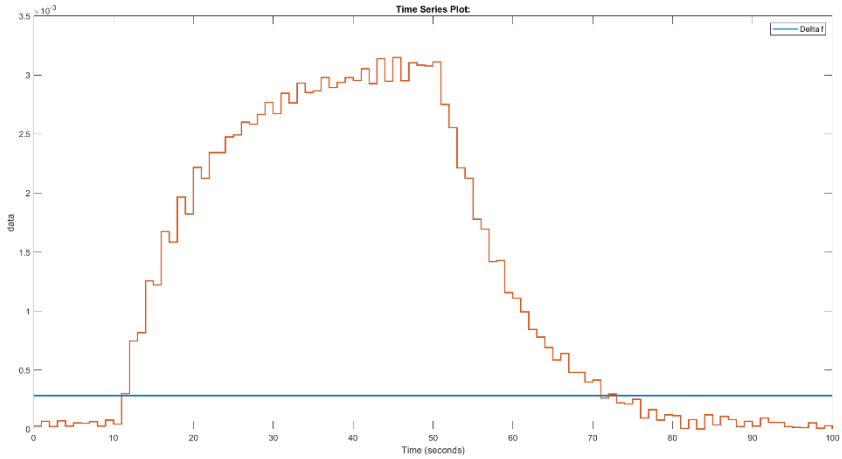

Figure 20. Attack detection with actuator being under large attack

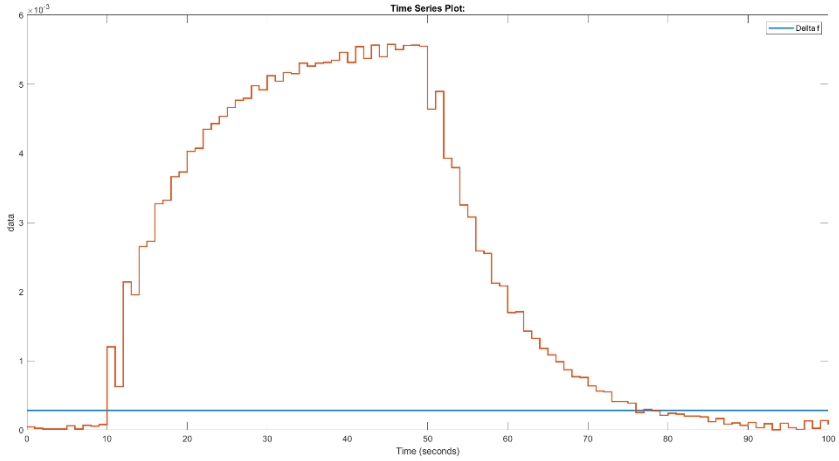

Figure 21. Attack detection with sensor and actuator being under large attack

In the next chapter we study the way to distinguish attack on actuator from the one on the sensor.

vii. Objective 2. Separate attacks on actuator from the ones on sensors.

vii.i. Attack discrimination.

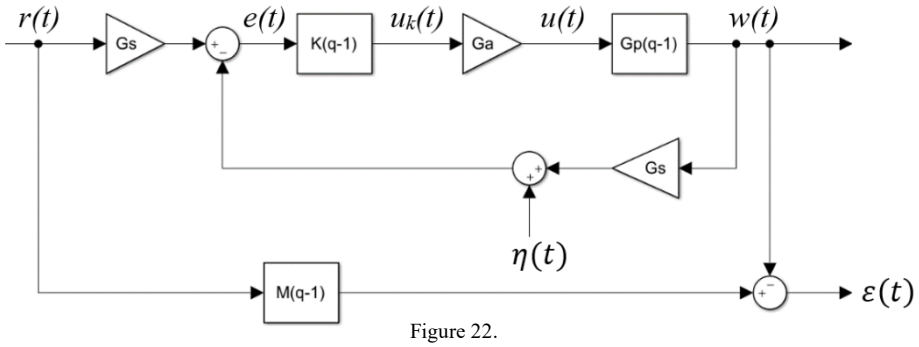

Figure 22.

Once the effective attack is detected, the next step is to understand whether the attack is focused on G_a or on G_s.

Output of the actuator, which is input of the plant, is measured physically, but the data are corrupted by the noise $\eta_u(t)$.

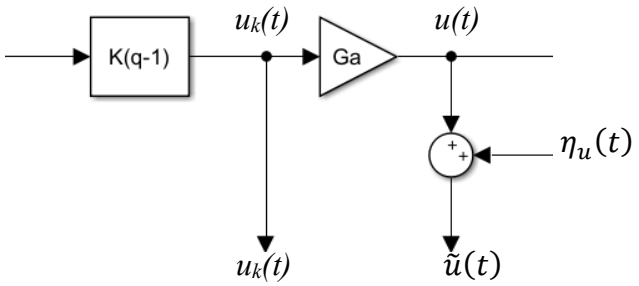

Figure 23.

Result 4

If $\left|\frac{\tilde{u}(t)}{u_k(t)}\right| \notin \left[G_a - \frac{\Delta\eta_u}{u_k(t)}, G_a + \frac{\Delta\eta_u}{u_k(t)}\right]$, then for sure the detected attack is affecting the actuator.

Proof of the Result 4

In case the attack is not affecting the actuator, we have that

$$\left.\begin{array}{l} u(t) = G_a * u_k(t) \\ \tilde{u}(t) = u(t) + \eta_u(t) \\ |\eta_u(t)| \leq \Delta\eta_u \end{array}\right\} \Rightarrow \quad \left|\frac{\tilde{u}(t)}{u_k(t)}\right| = \left|\frac{u(t)+\eta_u(t)}{u_k(t)}\right| = \left|\frac{G_a * u_k(t)+\eta_u(t)}{u_k(t)}\right| = \left|G_a + \frac{\eta_u(t)}{u_k(t)}\right|$$

(Eq.14)
$$\left|G_a + \frac{\eta_u(t)}{u_k(t)}\right| \in \left[G_a - \frac{\Delta\eta_u}{u_k(t)},\ G_a + \frac{\Delta\eta_u}{u_k(t)}\right]$$

Therefore, when the attack is acting on G_a, then condition in Eq.14 becomes $\notin$.

From Eq.14 it is evident that there are always two bounds, in between which we can define signal, that characterize presence of an attack in actuator. As soon as bounds are exceeded by a defined signal, we can be sure, that the existing attack in the system is acting or only on actuator, or on actuator as well as on the sensor.

vii.ii. The simulation in Simulink

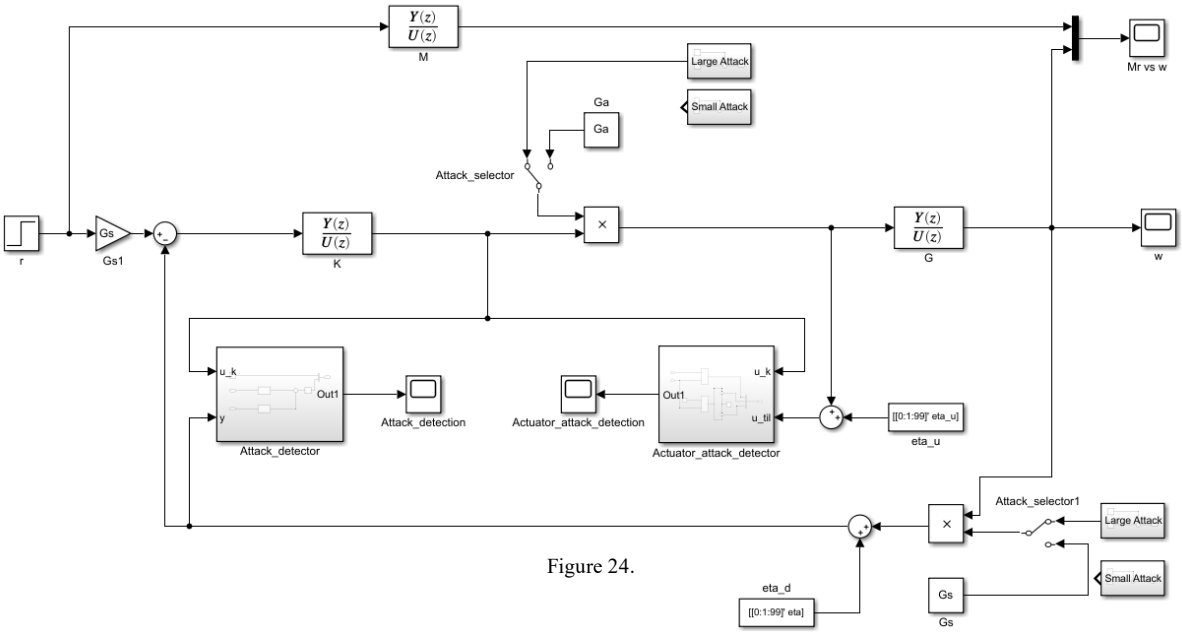

Figure 24.

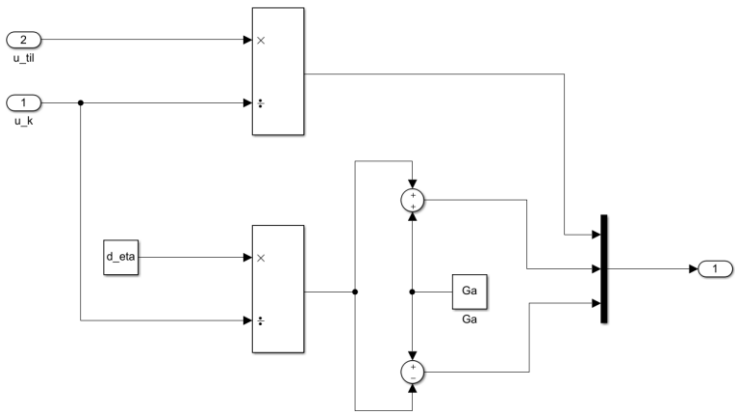

Figure 25. 'Actuator attack detector' block

Studying the change of output of the 'Actuator attack detector' block affected by the small attack on the system.

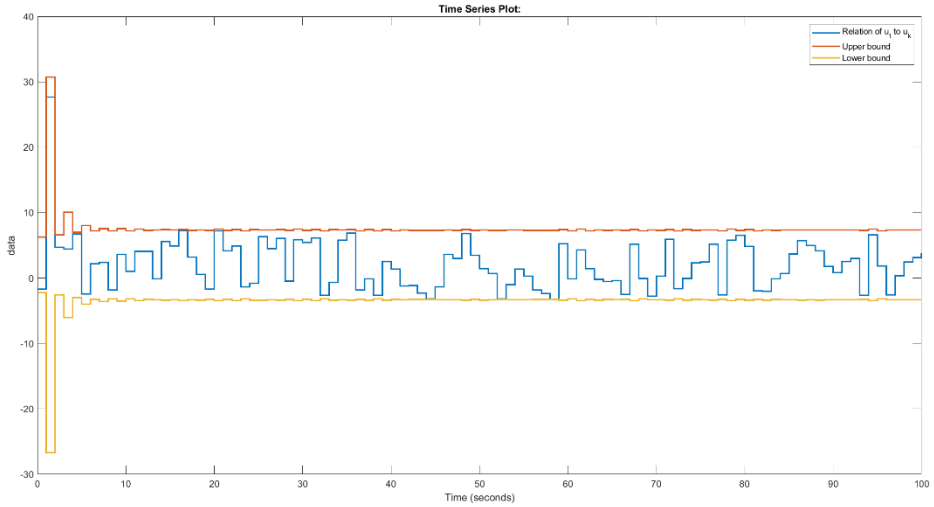

Figure 26. Attack discrimination without any attack in the system

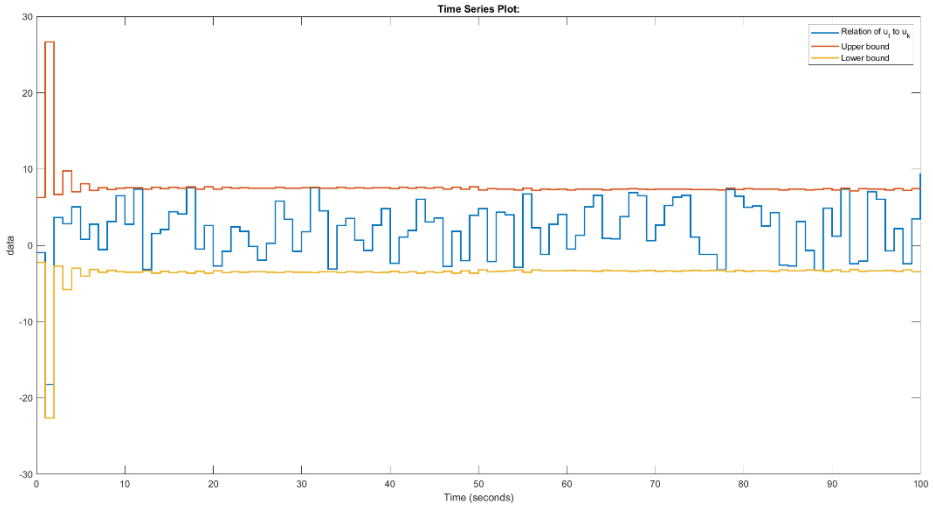

Figure 27. Attack discrimination with sensor being under small attack

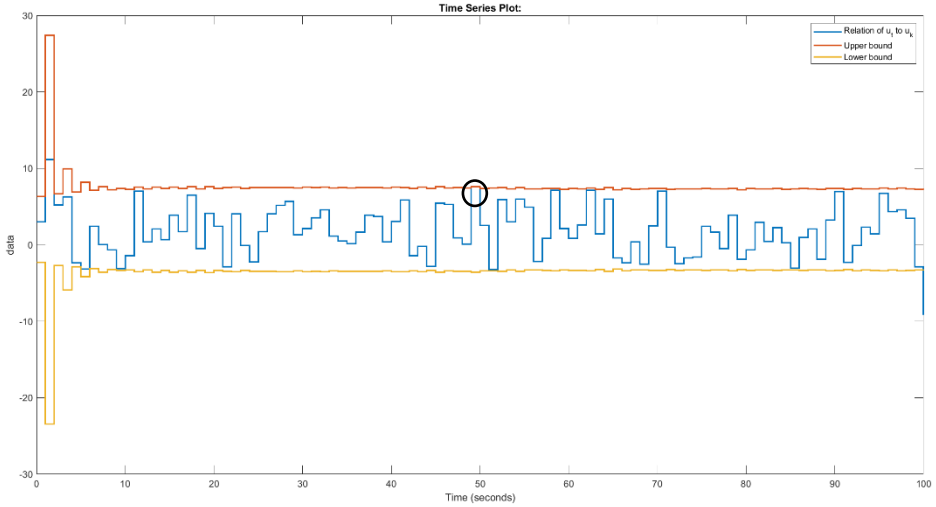

Figure 28. Attack discrimination with actuator being under small attack

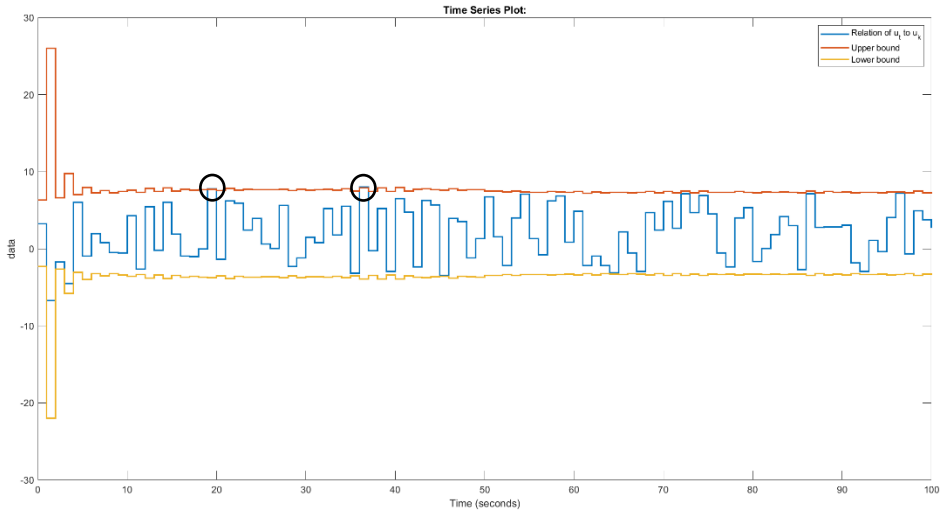

Figure 29. Attack discrimination with actuator and sensor together being under small attack

Studying the change of output of the 'Actuator attack detector' block affected by the large attack on the system.

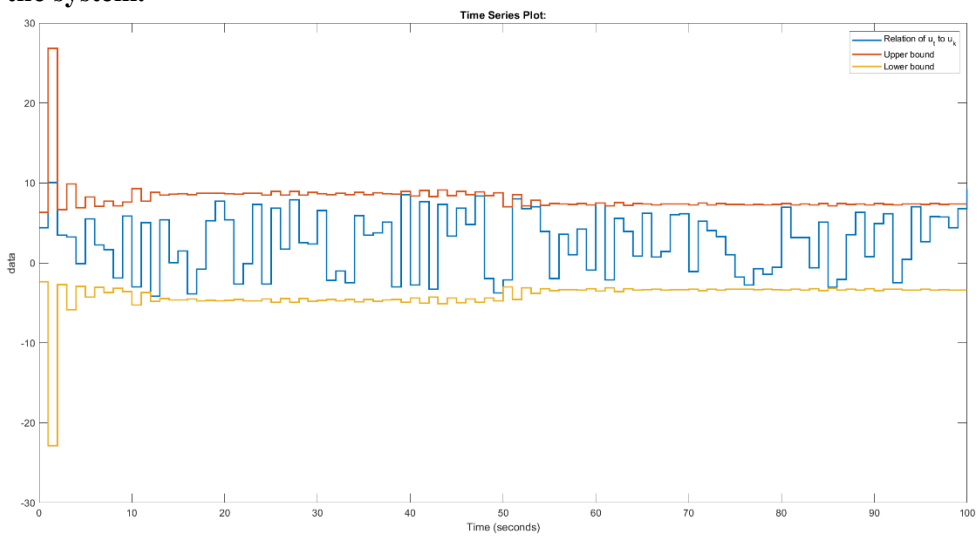

Figure 30. Attack discrimination with sensor being under large attack

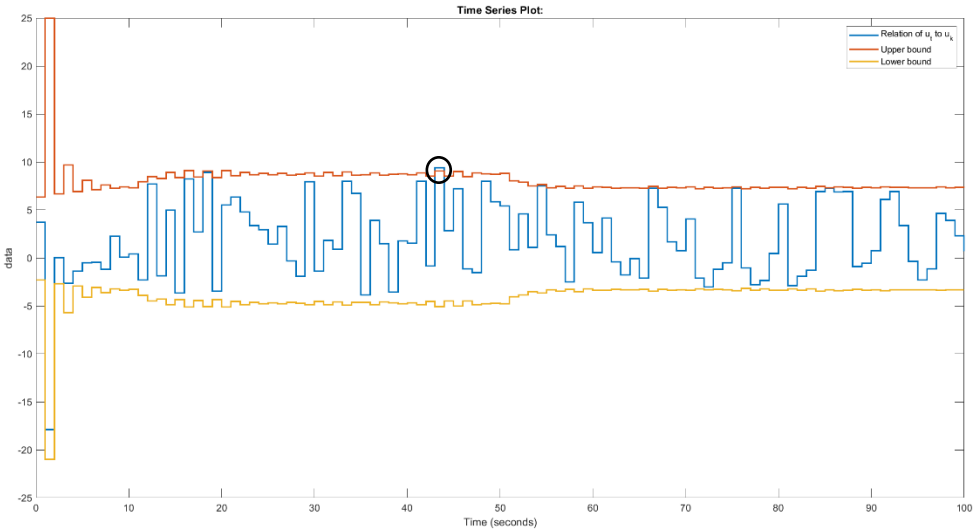

Figure 31. Attack discrimination with actuator being under large attack

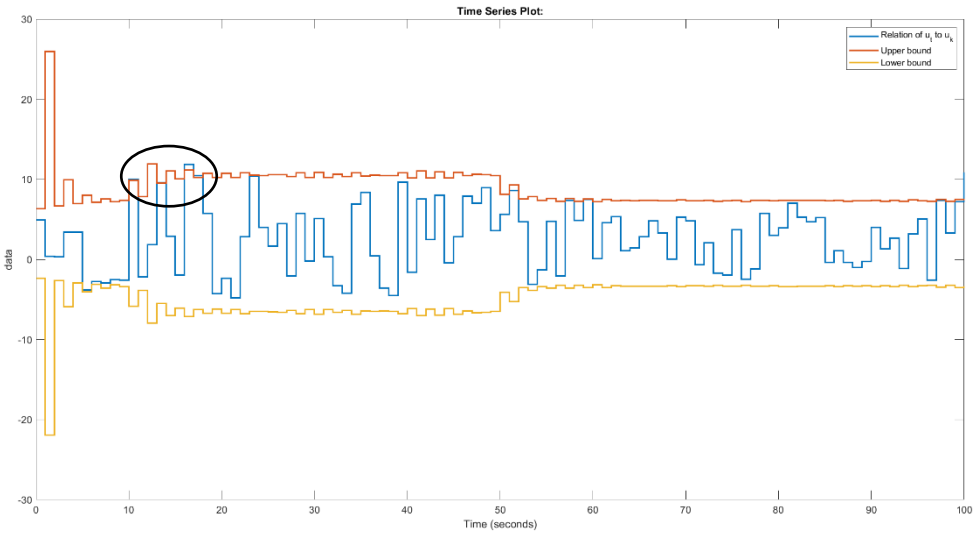

Figure 32. Attack discrimination with sensor and actuator being under large attack

viii. Conclusion.

This thesis work has proven that having feasible controller, designed in SM-DDDC in close loop feedback system directly using collected data available, we are able to detect attack presence in the system. Additionally, we are also able to detect presence of attacks on actuator, or on sensor, or on both. In order to confirm the above mentioned, we derived necessary equations and implemented calculations in MATLAB, first to collect data and then to simulate attacks and behavior of the potentially destructed system.

If condition from Eq. 13 in Result 3 is **satisfied**, it shows that the sensor and/or actuator are corrupted by an attack. It can be used as an attack detector system, which is sensible to large signals as well as to small attack signals. An important point to be declared is that attack detection works efficiently even when the attack is small enough not to influence the matching problem.

If condition from Eq.14 in Result 4 is **not satisfied**, we can identify that the existing attack in the system is acting on actuator or on actuator and sensor together. By examining the simulation plots, we compare the number of time instants, when bounds are exceeded, in two different conditions:

1. Attack is **only** on actuator.
2. Attack is acting not only on actuator, but also on sensor.

It is evident that in the first case, the number is less than the number of time instants in the former case.

Finally, to summarize, as soon as the controller is designed from the collected data, the Δf can be defined. Comparing the defined output of the system with this value, we identify the presence of the attack in the system. Only after detection of the attack, the outcome from the second objective shows where exactly in the system the attacks are coming from.

In the future this outcome can be developed to find a way to design controller, in such a way that, as soon as an attack appears it will automatically adjust itself in order to protect the output of the system from being corrupted. This in its turn keeps the overall system stable. If we were to go deeper, this idea could be developed also to design sensors and actuators.

ix. References.

[1] V. CERONE; D. PIGA; D. REGRUTO Set-Membership Error-in-Variables Identification Through Convex Relaxation Techniques IEEE TRANSACTIONS ON AUTOMATIC CONTROL, Vol.57, No. 2, pp.517-522, 2012

[2] V. CERONE; D. PIGA; D. REGRUTO Improved parameters bounds for set-membership EIV problems INTERNATIONAL JOURNAL OF ADAPTIVE CONTROL AND SIGNAL PROCESSING, Vol.25, No. 3, pp.208-227, 2011

[3] V. CERONE, D. REGRUTO, M. ABUABIAH "Direct data-driven control design through set-membership errors-in-variables identification techniques", 2017 American Control Conference (ACC), 388-393

[4] V. CERONE, D. REGRUTO, M. ABUABIAH "A set-membership approach to direct data-driven control design for SISO non-minimum phase plants", 2017 IEEE 56th Annual Conference on Decision and Control (CDC), 1284-1290