INSE 6670

EMBEDDED SYSTEMS SECURITY

FALL 2022

Detection and Prevention of FDI attacks on the signal in Aerial (Drones) Embedded Systems

Submitted to

Prof. Mohsen Ghafouri

by

PriyaDharshan Muthu 40196410

Aravind Shankkar 40203458

Pavithran Koteeswaran 40196178

Chapter 1

Analysis

We will be summarizing two IEEE papers namely "**A Command Governor Based Approach for Detection of Setpoint Attacks in Constrained Cyber-Physical Systems"** and **"Setpoint Attack Detection in Cyber-Physical Systems"** which were presented by Concordia professors **Walter Lucia, Kian Gheitasi, Mohsen Ghaderi**.

Both papers have addressed the problems of set-point attacks on Drones in their networked control systems. They have reconstructed the architecture of the Drone System to detect and prevent cyber-attacks affecting the setpoint signal without affecting the performance of the drone.

Concerning the problem, they used the advantage of peculiar capabilities of the **Command Governor (CG)** control paradigm, which in turn enabled the system to detect reference attacks.

PAPER 1

A Command Governor-Based Approach for Detection of Setpoint Attacks in Constrained Cyber-Physical Systems

-Walter Lucia, Kian Gheitasi, Mohsen Ghaderi

***Abstract*—** In this paper, we propose a novel control architecture capable of discovering cyber-attacks affecting the setpoint signal in a networked control system. We assume that the setpoint is generated by a Control Centre remotely located concerning the closed-loop system and an insecure channel is used for communications. By taking advantage of the main features of the Command Governor (CG) control paradigm, a simple Detector module is designed to detect cyber-attacks that might affect the setpoint signal. Finally, a simulation campaign, reproducing different attack scenarios, is performed to provide tangible evidence of the control architecture capabilities.

https://drive.google.com/file/d/1XSow7KfzK2_Bw6MMXc2JVz106bI_GVch/view?usp=sharing

PAPER 2:

Setpoint Attack Detection in Cyber-Physical Systems

-Walter Lucia, Kian Gheitasi, Mohsen Ghaderi

***Abstract*—** In this paper, we face the problem of detecting setpoint attacks in networked control systems. We consider a setup where the reference signal (also known as setpoint) is generated by a control center remotely located with respect to a standard feedback controller. In this scenario, an attacker with sufficient resources can exploit the communication channel to alter the setpoint signal and ultimately affect the tracking performance of the control system. With respect to this problem, we propose a novel distributed control architecture that, taking advantage of the peculiar capabilities of the Command Governor (CG) control paradigm, enables the detection of reference attacks. We formally prove that for constrained linear systems such a detector exists. Moreover, by limiting the attacker's disclosure resources with superimposed cryptographically secure pseudo-random signals, we show that the absence of advanced stealthy attacks is also ensured. Finally, a solid numerical simulation investigating setpoint attacks on the flight control system of a single-engine fighter is presented to provide tangible evidence of the features of the presented methodology.

https://drive.google.com/file/d/17bvvoiAPmgAM8iaaMK1ilh1Ntt21N9s_/view?usp=sharing

Chapter 2

Introduction

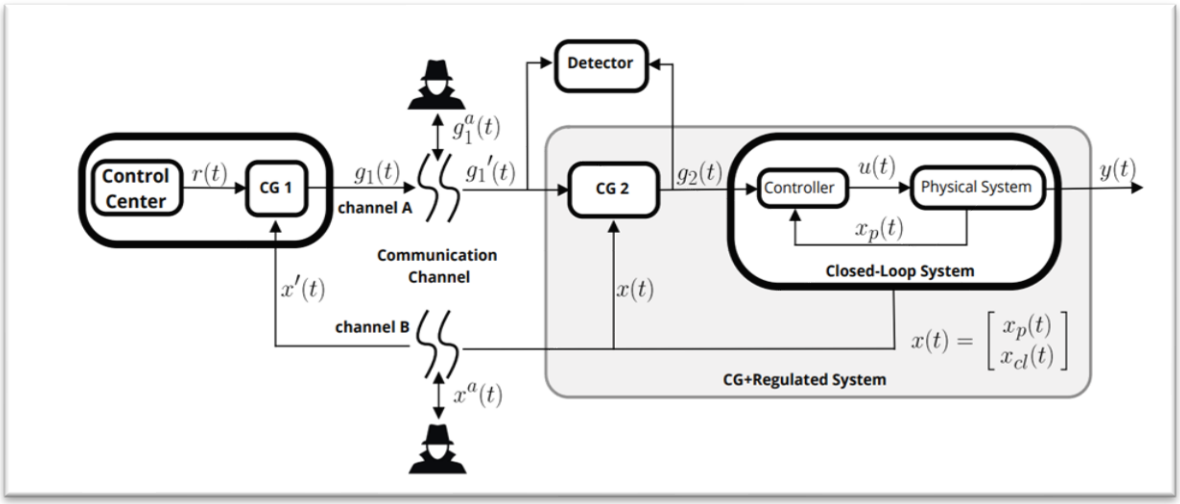
Drones are embedded systems with multiple distance sensors and are controlled by remote control ground systems (CGS) also referred to as the ground cockpit.

Drones are equipped with different state-of-the-art technology such as infrared cameras, GPS, and laser (consumer, commercial and military UAV). The latest high-tech drones are now embedded with Vision sensors, Ultrasonic, Infrared, Obstacle detection sensors, and so on.

An unmanned aerial vehicle system has two parts, the drone itself and the control system. Since the controllers are local and the only information transmitted over the network are the signals called reference signals (setpoint), the signals are vulnerable to **FDI (False data Injection) and MITM (Man in middle attacks).**

Chapter 3

Embedded Architecture Model



This was the proposed Networked control systems (NCS) architecture the in the papers. Since cyber-attacks can mainly affect communication channels. The first fundamental step towards a secure deployment of CPSs consists of developing formal methodologies capable of detecting the presence of cyber-attacks.

It has been proved that the proposed architecture model detects FDI attacks without affecting the systems tracking performance by mathematical representation with **Kalman Filter** and **LQI Controller**. Two conditions were assumed for mathematical representation

- The plant is asymptotically stable and
- The output tracks the reference ← e.g., the LQI controller

The architecture is implemented with different embedded systems to detect and prevent FDI attacks and various attacks related to it such as the Replay attack and Stealthy Replay attack. Three main embedded systems are used in the architecture to mitigate the attacks namely **Command Governor (CG1 and CG2)**, An **Anomaly detector** to make sure the signal values from CG1 and CG2 are not altered, and **Watermarking** to the signals which ensure the confidentiality of the signal values transmitted over the wireless network.

A real-world attack simulation was also addressed in the paper which ensures the mathematical analysis of the architecture model.

Chapter 4

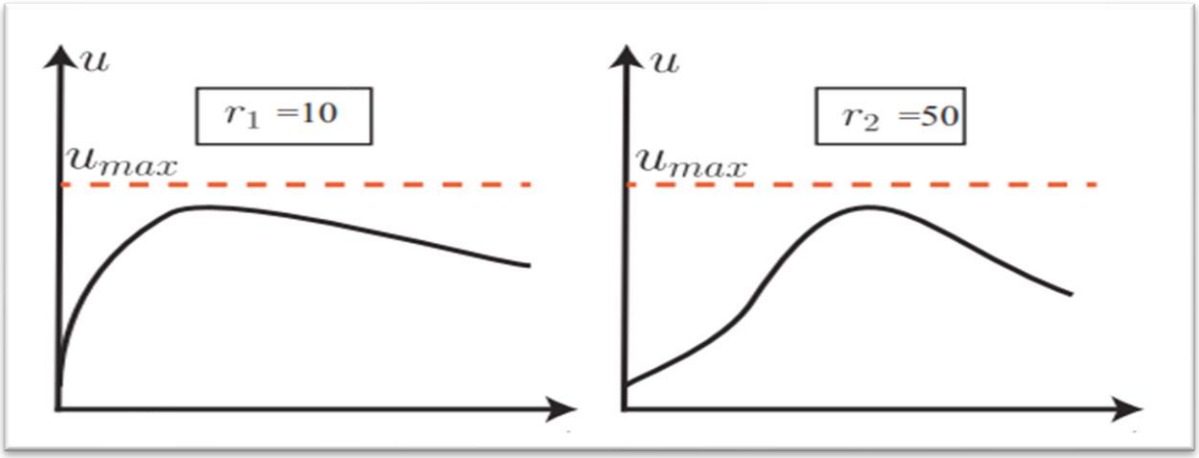
Components of NCS Architecture

4.1 Command Governor

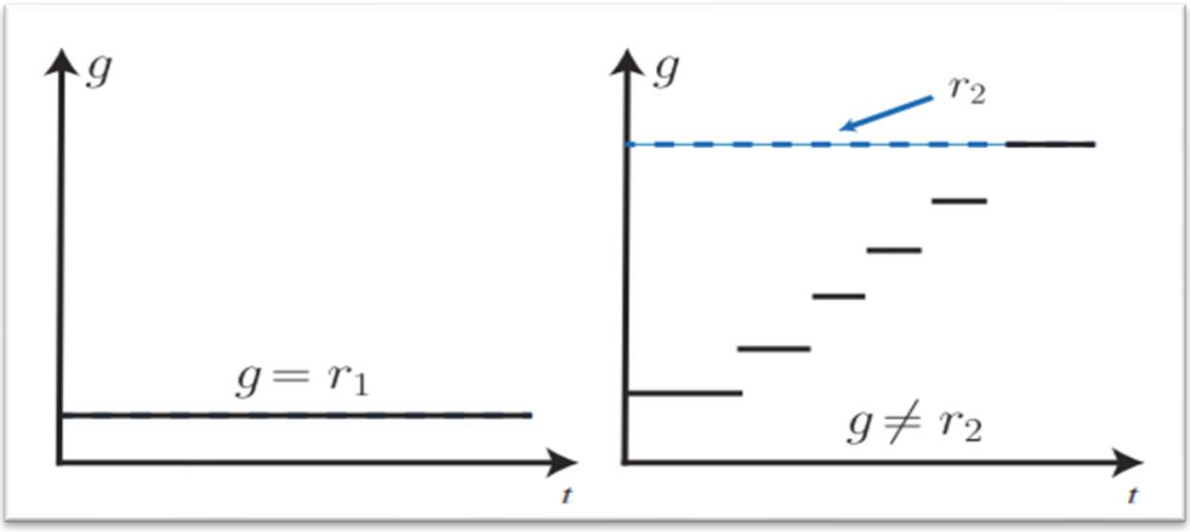
Command governors are add-on control schemes that enforce state and control constraints on pre-stabilized systems by modifying, whenever necessary.

The Command Governor (CG2) is a control device, placed between the reference signal r(k) and the closed-loop system. It takes the input x(k) from the closed-loop system also known as a Primal controller containing the state of the plant and the reference signal r(k). x(k) denotes the augmented state space vector including the plant and feedback controller components.

The CG2's objective is to understand if r(k) might lead to a constraint violation if given as input to the primal controller. g(t) is the best approximation of the reference signal r(t) complying with the prescribed constraints. If r(k) is predicted as "constraint-safe" then g(k) = r(k), otherwise, g(k) is the "best" and "constraint-safe" approximation of r(k). If there is an attack at each k, then g(k) makes sure that the maximum constraints are not violated to minimize the attack impact. If r(k) is constant, then g(k) has monotonically non-increasing or non-decreasing behaviors, and it will converge to r(k) in a finite number of steps.



The graphs show that for two different inputs r(k), the CG2 makes sure that the values do not exceed umax. This ensures that CG2 tries to mitigate the false data that has been injected r2. As we know that r2 is an altered reference value by false data injection by interrupting the wireless signal from CGS to the plant, without CG2 the curve would have exceeded the umax which would result in system-degraded tracking performance.



The above graph image represents the actual working of Command Governor 2. As explained when g(k) = r(k), the CG2 has monotonically non-increasing or non-decreasing behaviors. But when g((k)! = r(k), which represents an attack the CG2 ensures that the systems tracking value increases step by step to make sure that false data does not exceed umax.

Pros and Cons with one Command Governor

- Pros: The plant can never receive harmful references (even in presence of setpoint attacks).
- Cons: The attacker can still perform setpoint attacks to reduce tracking performance.

To overcome this drawback, another Command Governor has been added to the control center. The CG1 is fed with the inputs x(k) from the primal controller and r(k). The CG1 compares the r(k) with r(k)-1 to detect any possible attack. Both CG1 and CG2 do the same computation, hence to transmit x(k) through a wireless network for CG1 a second communication channel is added.

At the same time, an Anomaly detector has been implemented between CG1 and CG2 to check if their output estimates are the same. If the estimation from CG1 does not match with CG2, then the Detector provides an alert that we assume to be an attack.

Now we have two communication channels A and B. Through Channel A the g1(k) is transmitted through CG1 to CG2. Through channel B x(k) is transmitted to CG1 to estimate the g1(k)+1. Since there are two communication channels, we assume that there is a possibility of attacks on both channels.

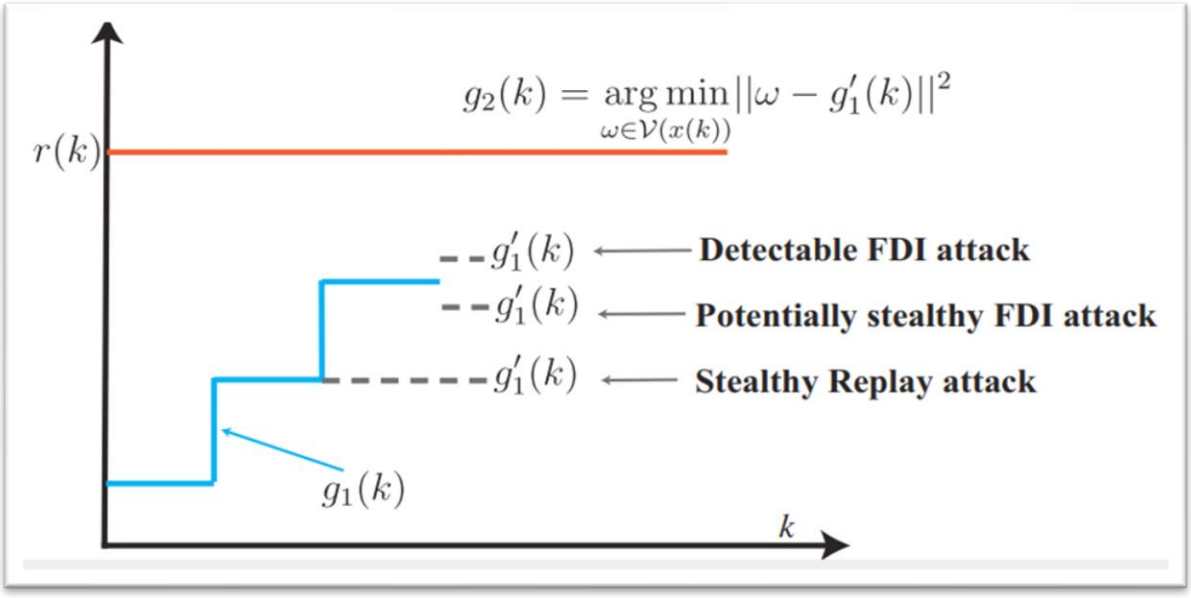
4.2 Anomaly Detector

As we know the anomaly detector is placed in between CG1 and CG2 to make sure that the estimated outputs of both CGs are the same i.e., g1(k) = g2(k).

Now we assume that the attacker is aware of the control architecture, so to perform an attack without alerting the detector, the attacker can perform a **STEALTHY REPLAY ATTACK** or a **REPLAY ATTACK** to make the drone's state unchanged or to downgrade the drone's performance respectively.

Stealthy Replay attack

A stealthy attack is an attack where the attacker injects the previous value to make the system's state unchanged. This attack is a combination of a Replay attack as the attacker uses the previous value. Both Command Governor and Anomaly detector can't detect this kind of attack as the constraints of the system are not violated but at the same time, the system remains unchanged.



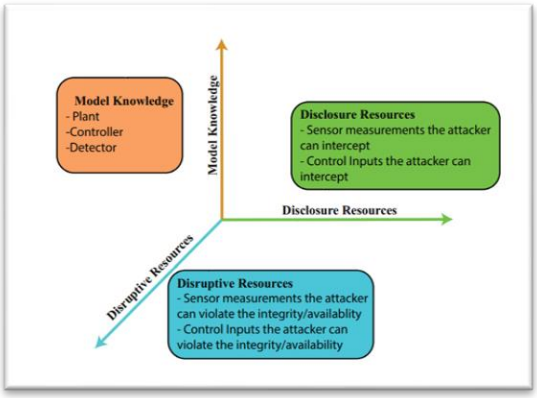
The above graph represents the performance of the system for various types of attacks.

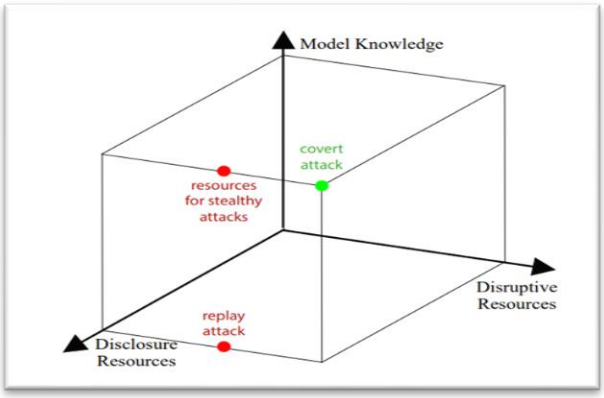
Model Knowledge

Model knowledge is a Set of knowledge of various types, facts, concepts, procedures, principles, and skills, structured by the type of links representing the relationship among them.

With the current architecture, that is with added two command Governor, Anomaly Detector we can prevent Covert attacks. But if the attacker has the

model knowledge of the NCS and its disclosure, then Stealthy Replay attacks and Replay attacks could downgrade the performance of the system.





The above figures represent the model knowledge of the remodelled Control architecture till now.

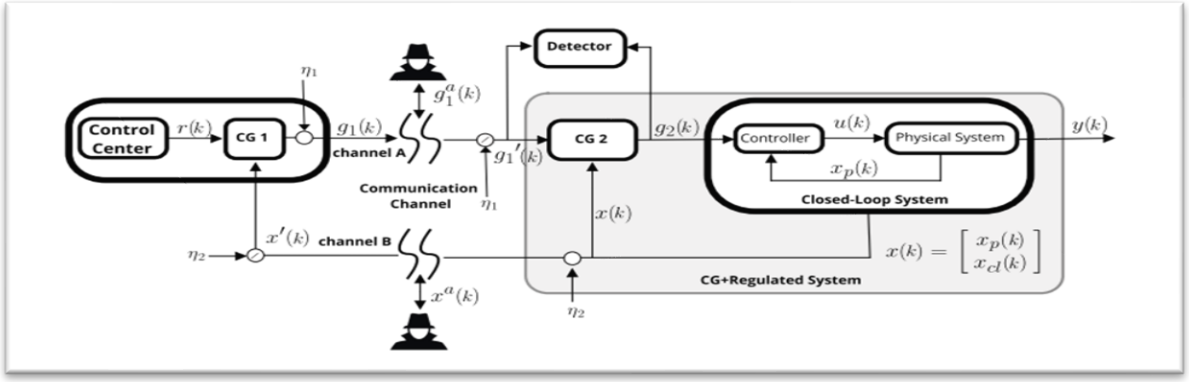
Prevention of attacks

To prevent Replay and Stealthy FDI attacks, the three possible ways are

- We prevent the attacker from having full model knowledge of the system architecture.
- We prevent the attacker from having disclosure resources in at least one of the two channels A and B.
- We prevent the attacker from having disruptive resources.

4.3 Watermarking

Another way to prevent Stealthy attacks and to recover confidentiality is to use Watermarking. Two identical and cryptographically secure pseudo-random number generators can be used on both sides of the communication channels to generate η1(k) and η2(k). η1(k) and η2(k) are used to hide g1(k) and g2(k) by performing simple Hadamard (element-wise) product and division operations.

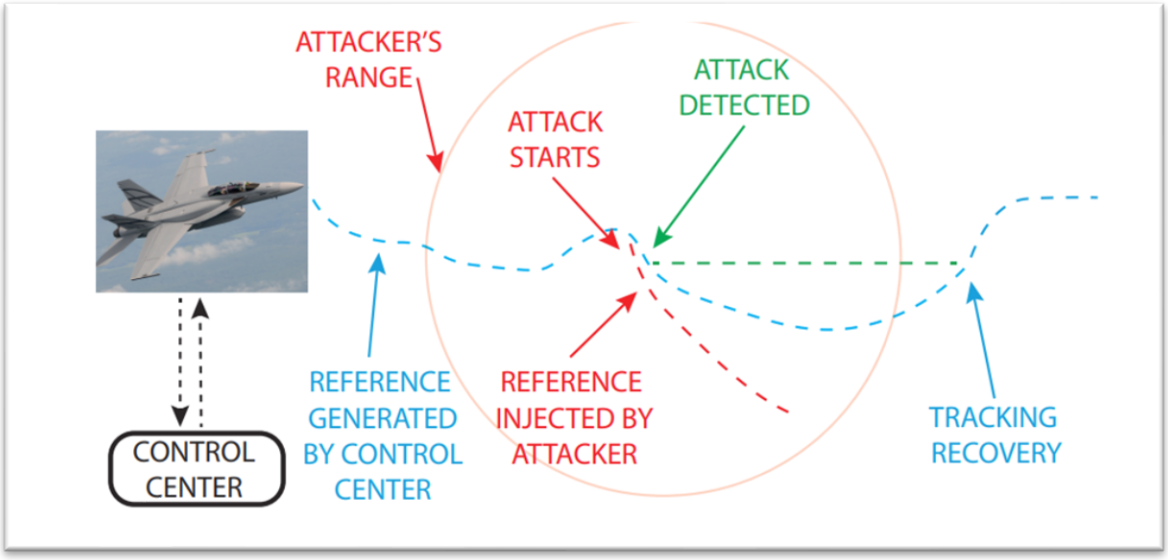


Chapter 4

Simulation

4.1 Real-Time Attack Scenario

To verify the efficiency of the reconstructed System architecture, a real-time simulation of False Data Injection was performed. The mathematical outputs provided in both papers proved that the proposed Network Control System detected the False data Injection and prevented the downgrade of the NCS while the attack was still going on.



Let's assume a scenario where the fighter pilot is exploring an area of interest. When the fighter jet was within the perimeter of the attacker, the attacker was able to intercept and corrupt the setpoint communication signals.

At first, when the attack starts according to the figure given above, the Fighter jet starts to downgrade or change directions but with the help of the Command Governor and Anomaly detector, soon the recovery tracking was performed by the embedded systems, and the Fighter Jet was on the correct lane.

To recover to the correct state, we assume that when there is an attack, the tracking controller applies a previously stored safe reference to stop downgrading the system.

4.2 Mathematical Representation

The proposed architecture was represented in Mathematical calculation with Kalman Filter and LQI controller

Two conditions were assumed for mathematical calculation:

- The plant is asymptotically stable and
- The output tracks the reference ← e.g., the LQI controller

LQI Controller:

LQI (Linear Quadratic with Integral) controllers are **static feedback controllers based**. They are used for tracking errors.

$$\begin{cases} x(t+1) &= \Phi x(t) + Gg(t) \\ y(t) &= H_y x(t) \end{cases}$$

$$g(t) = \arg \min_{\omega \in \mathcal{V}(x(t))} ||\omega - r(t)||^2$$

The state feedback controller is a linear discrete-time system with x(t) as the state space vector and g(t) as the output from the command governor.

Detector:

$$Attack\ (\forall\, t) : \begin{cases} Find\ x^a(t) \in \mathbb{R}^n\ \ and/or\ g_1^a(t) \in \mathbb{R}^p \\ \quad g_1'(t) = g_2(t)\ \ \wedge\ \ g_2(t) \neq r(t) \end{cases}$$

$$Detector(t) := \begin{cases} \text{Attack} & if\ g_1'(t) \neq g_2(t) \\ \text{No Attack} & otherwise \end{cases}$$

As said if g1(t)! = g2(t), then there is a potential attack on the communication channel. Once the attack is detected, the Anomaly Detector alerts the Control System.

Model Knowledge:

$$\mathcal{R}^a_{partial} := \begin{cases} \text{Model Knowledge: } \mathcal{I}^a_{model} \subset \mathcal{I}^{CG}_{model} \\ \text{Disclosure: } \textbf{channel A} \wedge \textbf{channel B} \\ \text{Disruptive: } \textbf{channel A} \wedge \textbf{channel B} \end{cases}$$

The above mathematical representation represents that if there is an attack, irrespective of its disruptive and disclosure resources on channel A and channel B, is not guaranteed to be complying with g2(t) and stealthy replay attack is not achieved.

Watermarking:

$$\hat{g}_1(t) = g_1(t) \circ \eta_1(t)$$
$$\hat{x}(t) = x(t) \circ \eta_2(t)$$

Adding a watermark to the output signals from the command governor (CG1).

$$g_1'(t) = \hat{g}_1'(t) \oslash \eta_1(t)$$
$$x'(t) = \hat{x}'(t) \oslash \eta_2(t)$$

Negating the watermarking signals that were added after CG1 before the signal is given input to CG2.

Chapter 5

Conclusion

Both papers proposed a new architecture for the Network Control Systems capable of detecting setpoint attacks. The detection of setpoint attacks has been achieved by using the full control use of the command governor and anomaly detector. This architecture makes the system simple and effective without downgrading the performance of the Networked Control System. Finally, the mathematical representation has proved tangible evidence of the potential of the proposed control architecture.

References

https://ieeexplore.ieee.org/document/9123676
https://ieeexplore.ieee.org/document/8618960