International Journal of Basic and Applied Sciences, 14 (2) (2025) 470-483

International Journal of Basic and Applied Sciences

Website: www.sciencepubco.com/index.php/IJBAS
https://doi.org/10.14419/bd6zqx18
Research paper



Detection Of Methods for Enhancing Security in Cyber-PhysicalSystems Counteracting Zero Dynamic and False Information Injection Attacks

Peter Jose P. [1] *, Teena KB [2], Shruti Tyagi [3], D. Rosy Salomi Victoria [4], R. Vijayakumar [5], S. Lakshminarasimhan [6], Elangovan Bal-Asubramanian [7], P. Deepa [8]

[1] Department of Computer Science, Mount Carmel College Autonomous, Bengaluru, Karnataka 560052, India
[2] Department of Information Science and Engineering, East point College of Engineering and Technology, Bengaluru, Karnataka 560049, India
[3] Department of Problem Management, ServiceNow, 2225 Lawson Lane, Santa Clara, CA 95054, USA
[4] Department of Information Technology, Chennai Institute of Technology, Kundrathur, Chennai, Tamil Nadu 600069, India
[5] Department of Computer Science and Engineering, Sri Ramakrishna Engineering College, Coimbatore, Tamil Nadu 641022, India
[6] Department of Artificial Intelligence and Data Science, J.J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu 620009, India
[7] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh 522302, India
[8] Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, Tamil Nadu 600123, India
**Corresponding author E-mail: peterjose210@gmail.com*

Received: May 11, 2025, Accepted: June 18, 2025, Published: June 30, 2025

Abstract

This research focuses on the design and implementation of Zero-Dynamics Attacks on a Quanser coupled tank plant and proposes a detection scheme to mitigate such cyber-physical threats. Zero-Dynamics Attacks are particularly insidious because they can initially remain detected by conventional monitoring methods while causing significant disruption. The study begins by characterizing the plant through control loop design and extracting its key parameters for accurate simulation. Simulations conducted in MATLAB demonstrate that Zero-Dynamics Attacks can remain hidden for extended periods, posing a critical risk. However, when transferred to a physical environment, actuator saturation limits the effectiveness of these attacks, introducing an unexplored area in cyber-physical system security. This research highlights how multi-frequency modeling can be leveraged to alter system dynamics and eliminate unstable zeros, improving the chances of attack detection. Furthermore, the study proposes early detection algorithms tailored to identify the presence of Zero-Dynamics Attacks before irreversible damage occurs. The results underscore the potential of saturation-aware defense strategies and open new directions for securing cyber-physical systems against stealthy intrusions.

Keywords: *Zero-Dynamics Attacks; Quanser Coupled Tank Plant; Irreversible Damage; Cyber-Physical Systems; Stealthy Intrusions.*

1. Introduction

Infrastructure security has become a top priority in modern industrial environments. As technology infrastructures continue to evolve, particularly in communications networks, control systems, and work environments, enterprises face unprecedented challenges in maintaining the integrity and reliability of their systems. With this complexity comes an increase in cyber vulnerabilities as more components of industrial systems connect and interact with the internet and cloud-based services (Hu et al., 2023; Zahid et al., 2024; Amin et al., 2021; Duo et al., 2022).

One of the main reasons for the proliferation of cyberattacks in recent years is the proliferation of vulnerabilities in different layers of the system architecture. Industrial systems now include a wide range of internet-connected devices, such as programmable logic controllers (PLCs), sensors, actuators, and computing nodes (Shih et al., 2016, Wang et al., 2021, Kazemi et al., 2021). These devices in critical infrastructure, such as refineries and manufacturing plants, are typically not designed with robust cybersecurity measures in mind. Including them in broader digital environments without adequate security mechanisms exposes them to threats ranging from unauthorized access to sophisticated malware to same-day exploitation (Ma, Che, & Deng, 2022; Shalini et al., 2023; Yang et al., 2022).

As a result, the threat landscape has expanded dramatically, with attackers targeting not only enterprise IT networks but also operational technology (OT) environments. The convergence of IT and OT has increased the impact of cyber incidents, which can disrupt physical processes and cause damage worldwide (Liu et al., 2023; Albalawi & Ganeshkumar, 2024; Kumari & Mrunalini, 2022).

Copyright © Peter Jose P. et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Given these growing threats, early detection of cyberattacks is crucial to minimize damage, ensure system resilience, and ensure business continuity. Early detection mechanisms, including intrusion detection systems (IDS), anomaly-based monitoring, and machine learning techniques, can generate real-time alerts, enabling rapid incident response and system recovery (Mollapour et al., 2022). Proactive detection, combined with a secure approach and ongoing monitoring, forms the foundation of modern industrial cybersecurity strategies.

1.1. Scope and final products

Table 1: Operational and Simulation Outcomes in Water Tank Control and Security Analysis

Proposal	Result
Operation of Quanser water tanks	The coupled tanks were assembled, and PI control was implemented to manage the tank height.
Study of cyber-physical attacks	The work focused on studying zero-dynamic attacks due to the damage they can cause to a plant and the difficulty in detecting them.
Simulations of water tank models and zero-dynamic attacks	Several simulations were performed on the nonlinear and linearized models of the Quanser plant. Once the models were verified, the zero-dynamic attack was carried out.
Implementation of the attack in a physical plant	The implementation of the attack on the physical plant was not possible because the water pumps were saturated.
Operation of Quanser water tanks	The coupled tanks were assembled, and PI control was implemented to manage the tank height.

2. Literature review

Reji et al. (2023) created an intrusion detection system (IDS) specifically for Internet of Things (IoT) networks by combining the Seagull Optimization Algorithm (SOA) with an Extreme Learning Machine (ELM) classifier. Employing the CIC-IDS-2018 dataset, the hybrid model attained impressive performance measures: 94.22% accuracy, 92.95% precision, 93.45% detection rate, and 91.26% F1-score. This method highlights the capability of merging optimization algorithms with machine learning classifiers to improve IDS performance in IoT settings.

Huang and Li (2022) examined the susceptibility of machine learning-driven network attack detection models in power systems to adversarial threats. They suggested a mitigation approach based on causal theory, intending to enhance the resilience of these models to adversarial disturbances. This method lessens dependence on adversarial examples and computational power, improving the robustness of power system monitoring infrastructures.

Kavousi-Fard et al. (2020) proposed a framework that utilizes machine learning to identify cyberattacks in wireless sensor networks situated in microgrids. The approach uses prediction intervals obtained from the Lower Upper Bound Estimation (LUBE) method to detect anomalies in smart meter data. This method improves the identification of data integrity assaults, aiding in the secure functioning of microgrids.

Combastel and Zolghadri (2020) introduced a Distributed Zonotopic and Gaussian Kalman Filter (DZG-KF) aimed at reliable state estimation in CPS. By integrating symbolic zonotopes and a Unique Symbols Provider (USP), the approach efficiently manages bounded disturbances and stochastic noises within a distributed network. This improves the dependability of state estimation in CPS settings.

Chen et al. (2021) examined the difficulties of distributed fusion estimation in CPS, considering communication delays and reduced dimensions. They created a recursive Distributed Kalman Fusion Estimator (DKFE) that addresses information loss caused by delays and dimensionality reduction. The method guarantees stability and lowers computational complexity, making it appropriate for real-time applications in CPS.

Choraria et al. (2022) examined the structure of false data injection (FDI) attacks aimed at distributed process estimation within CPS. Their research underscores the risk that adversaries pose to estimation accuracy by introducing misleading data, stressing the necessity for strong detection and mitigation strategies to protect distributed estimation processes.

Wang et al. (2022) explored control methods for discrete-time nonlinear systems in the context of denial-of-service (DoS) attacks. They suggested an adaptive event-triggered control scheme based on a neural network that modifies communication thresholds according to system dynamics. This method improves system resilience against DoS attacks by maintaining stability and minimizing unnecessary communications.

Ma et al. (2024) concentrated on distributed secure estimation amidst sparse FDI attacks. They created estimation algorithms that preserve accuracy in the face of harmful data, safeguarding the integrity of CPS operations. This study aids in the advancement of robust estimation methods that can endure limited adversarial attacks.

Ma, Ya, and Fan (2024) propose a sustainable self-triggered predictive control strategy for nonlinear systems under two-channel deception attacks, focusing on both sensory and actuator pathways. By combining self-monitoring, MPC, and attack-resistant hosts, this method reduces the frequency of updates and improves security. Although effective in a variety of nonlinear settings, MPC can face limitations due to computational demands and reliance on accurate system modelling.

Eslam, Kazem, and Khorasan (2024) investigate event-driven stealth attacks on CPS exchanges, providing a design and research framework for exploiting system residuals and exchange vulnerabilities. Their work shows that hybrid dynamics mask the attack, but the detection accuracy depends on the correct model of the transformation behavior.

Ku et al. (2024) proposed a secure shell encryption method for smart grids by embedding Paillier homomorphic encryption, which allows evaluating the encryption state against cyberattacks. The approach maintains data confidentiality and integrity but introduces significant computational overhead and imposes secure key management.

Xin and Long (2024) propose a learning-based passive resilient controller that maintains system stability against stealthy deception attacks and loss of actuator control. Through adaptive learning and passive control, the system ensures the stability of BIBO without active control power. However, its effectiveness depends on the quality of training and lacks active recovery capabilities.

3. Problem description and justification of the work

The security of cyber-physical systems has taken on a highly important role in recent years. The ability of an attacker to damage processes or control plants without being detected led to the completion of this work. For example, work (Hu et al., 2023) shows that it is possible to access the power grid and change the estimated power states, all without being detected by false information injection detection methods. The latter is just one example of the wide range of attacks that can be carried out on a control system. This work proposes de-

tection methods that will prevent damage to both the product and the machines. A system with a zero is potentially vulnerable to a zero dynamics attack. Therefore, it is especially important to have detection methods to counteract possible damage.

4. Theoretical and conceptual framework

4.1. Theoretical framework

Cyber-physical systems integrate both computation and communication to control entities in the physical world. These systems are composed of sensors, actuators, controllers, and communication devices (Hu et al., 2023).

4.2. Conceptual framework

The security objectives of these systems are to maintain communication channels and ensure the availability of sensors and actuators. However, cyberattacks targeting control systems compromise the integrity of the information and the availability of the systems (Zahid et al., 2024).

Cyberattacks can be classified into three groups: deception attacks, DoS attacks, and direct attacks. A deception attack consists of sending false information from a sensor or controller. This information may include an erroneous measurement, an incorrect measurement time, or a false sender ID. A DoS attack prevents the controller from receiving sensor measurements; this is achieved by blocking communication channels or attacking the transmission protocols. Direct attacks consist of physical manipulation of the plant (Hu et al., 2023).

Technology offers solutions based on proactive and reactive mechanisms and design principles for the proposed cyberattacks. Authentication methods are proposed as proactive mechanisms that prevent unauthorized access by unwanted users. Message encryption is also essential to ensure secure communication. Reactive mechanisms allow for the detection and response to an attack, but one problem with their implementation is false alarms and failed detections, which can lead to considerable losses in a plant where production must be maintained. Finally, design principles establish that a system is secure if the model proposed for the attacker is true. Therefore, security systems must not only consider infrastructure protection but must also be kept up-to-date with the evolution of the different attacks and models that the attacker may use (Zahid et al., 2024).

5. Work definition and specification

A cyber-physical system integrates computing, communication, monitoring, and control systems. This system is composed of sensors, actuators, and control processors. For modern control applications, the components that make up the cyber-physical system are critical to its operation. A failure in one of the systems can cause irreparable damage to the physical system being controlled.

A cyber-physical system performs critical functions in infrastructure, such as the power distribution network, oil companies, natural gas extractors, and transportation systems. The failure of any of these sectors can negatively impact security, health, and the economy (Hu et al., 2023).

Studies have been conducted on prevention mechanisms, but they do not consider how a system can continue operating when under attack. And the analysis of faults caused by a malicious attack is still very superficial, so there are no tools to protect plants against attacks such as zero dynamics.

5.1. Specifications

The project is limited to studying zero dynamics attacks, specifically those of a Quanser plant. The work studies the situation where, even if a plant does not have a zero, when discretized, it is possible to introduce a zero that may even be unstable, which can lead to irreparable damage to expensive and process-critical equipment.

This work proposes attack detection through multi-sampling, which is expected to estimate plant values in order to detect an attack in time.

The failure of the physical implementation was not due to the weaknesses in the theoretical framework, but rather to the practical limitations of the cyber-physical system, especially the actuators' charging. For future work, a hybrid approach that combines theoretical models with realistic system constraints and uses physical constraints as protection mechanisms is key. With this, detection systems such as multi-sampling can be better applied to real-world industrial control systems.

6. Work methodology

6.1. Information search

Using control theory, a controller model was implemented for the plant. Thanks to system dynamics, it was possible to model the plant and perform its respective linearization. To make the appropriate plant connections and verify its modeling parameters, the Quanser guide for coupled tanks (Duo et al., 2022) was used. This work was based on the work on cyberattacks by Zahid et al. (2024). As support for the implementation of the attack and subsequent detection, we used works such as that of Mohammad (Ma, Che, & Deng, 2022), in which a Zero-Dynamics Attack was implemented on an AVR. With the help of Luis Felipe Giraldo, my work advisor, the characteristics of the Zero-Dynamics Attack were studied, and simulations of it were performed in Matlab.

6.2. Development alternatives

At the beginning of the work, various studies were considered on types of attacks other than the Zero-Dynamics Attack, such as the replay attack or integrity attack. However, ultimately, a study exclusively of the Zero-Dynamics Attack was conducted in order to implement a physical setup of the attack. A discrete model was chosen for plant modeling as these models are the closest to reality. MATLAB can approximate continuous models, but for the physical implementation, a continuous model with a discrete controller was used.

The Zero-Dynamics Attack uses the system's zeros to generate an exponential input with a zero output. The plant studied did not have any zeros, but a zero was introduced when discretizing it to allow the zero-dynamics study of the plant to be performed.

7. Implementation

7.1. Plant characterization

The Quanser coupled tanks plant (Duo et al., 2022) consists of two coupled tanks. The dynamic system was characterized. The output of tank 2 was obtained from Equation 1.

$$F_{02} = A_{02}V_{02} \tag{1}$$

Where F represents the flow and V the flow velocity, and A is the cross-sectional area. Applying Bernoulli's equation for small holes gives Equation 2

$$V_{02} = \sqrt{2GL_2} \tag{2}$$

Where L1 and L2 represent the height of the water column. Replacing Equation 2 in Equation 1 for the tank, Equation 3 becomes:

$$F_{02} = A_{02}\sqrt{2GL_2} \tag{3}$$

The inlet to the tank is given by Equation 4

$$F_{i2} = A_{01}\sqrt{2GL_1} \tag{4}$$

Using the principle of mass balance, Equation 5 is obtained

$$A_{t2}\left(\frac{d}{dt}L_2\right) = F_{i2} - F_{02} \tag{5}$$

Replacing the equations and arranging the data, Equation 6 is obtained

$$\frac{d}{dt}L_2 = \frac{-A_{02}\sqrt{2GL_2}+A_{01}\sqrt{2GL_1}}{A_{t2}} \tag{6}$$

To obtain the equilibrium water level, the system is verified in a state of equilibrium. In this state, all derivative terms become zero, and Equation 7 is obtained.

$$A_{02}\sqrt{2GL_2} = A_{01}\sqrt{2GL_1} \tag{7}$$

Rearranging the data in Equation 7 gives the equilibrium water level expressed in Equation 8.

$$L_{10} = \frac{A_{02}^2 L_{20}}{A_{01}} \tag{8}$$

Next, a Taylor series linearization is performed, yielding Equation 9.

$$\frac{d}{dt}L_2 = \frac{-A_{02}\sqrt{2gL_{20}}+A_{01}\sqrt{2gL_{10}}}{A_{t2}} - \frac{1}{2}\frac{A_{02}\sqrt{2}\,L_{21}}{\sqrt{gL_{20}}\,A_{t2}} + \frac{1}{2}\frac{A_{01}\sqrt{2}\,L_{11}}{\sqrt{gL_{10}}\,A_{t2}} \tag{9}$$

At the linearization point, the system is in a stable state, so the equality of Equation is obtained 10.

$$A_{02}\sqrt{2gL_2} = A_{01}\sqrt{2gL_1} \tag{10}$$

And the linearized equation simplifies to Equation 11.

$$\frac{d}{dt}L_2 = -\frac{1}{2}\frac{A_{02}\sqrt{2}\,gL_{21}}{\sqrt{gL_{20}}\,A_{t2}} + \frac{1}{2}\frac{A_{01}\sqrt{2}\,gL_{11}}{\sqrt{gL_{10}}\,A_{t2}} \tag{11}$$

A similar procedure is performed to obtain the linearized system of tank 1, obtaining Equation 12

$$\frac{d}{dt}L_{11} = -\frac{\frac{1}{2}A_{01}\sqrt{2}\,gL_{11}}{\sqrt{gL_{10}}\,A_{tl}} + \frac{K_p V_{pl}}{A_{tl}} \tag{12}$$

Using Equation 11 and Equation 12, the state equation representation is obtained, which is presented in Equation 13.

$$\begin{matrix} L'_{11} \\ L'_{21} \end{matrix} = \begin{bmatrix} -\frac{A_{01}\sqrt{2}\,g}{2\sqrt{gL_{10}}\,A_{tl}} & 0 \\ \frac{A_{01}\sqrt{2}\,g}{2\sqrt{gL_{10}}\,A_{t2}} & -\frac{A_{02}\sqrt{2}\,g}{2\sqrt{gL_{20}}\,A_{t2}} \end{bmatrix} \begin{bmatrix} L_{11} \\ L_{21} \end{bmatrix} + \begin{bmatrix} \frac{k_p}{A_{tl}} \\ 0 \end{bmatrix} V_{pl}$$

$$y = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} L_{11} \\ L_{22} \end{bmatrix} \quad (13)$$

7.2. Simulation

To perform the simulation, the tank values are substituted into Equation 14. The values the plant will work with are presented below (Duo et al., 2022).

$$A_{01} = 0.1781$$

$$g = 981$$

$$L_{10} = 15$$

$$L_{20} = 15$$

$$A_{t1} = 15.5179$$

$$A_{t2} = 15.5179$$

$$kp = 3.3 \quad (14)$$

Plugging the values into equation 3 gives Equation 15.

$$\begin{matrix} L'_{11} \\ L'_{21} \end{matrix} = \begin{bmatrix} -0.0635 & 0 \\ 0.0635 & -0.0635 \end{bmatrix} \begin{bmatrix} L_{11} \\ L_{21} \end{bmatrix} + \begin{bmatrix} 0.2127 \\ 0 \end{bmatrix} V_{pl} \quad (15)$$

The transfer function of system is obtained from equation 16, from which the transfer function of the system represented in equation 17 is obtained.

$$G(S) = C([SI - A]^{-1} * B) \quad (16)$$

$$\frac{3.2}{s^2+2s+1} \quad (17)$$

A proportional-integral control with feed-forward control is proposed, as shown in Figure 1. Block reduction gives Equation 18.

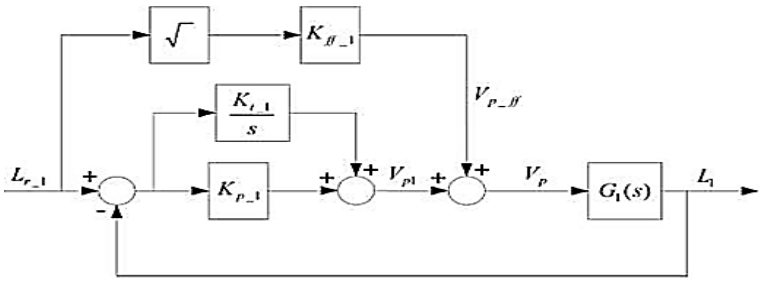


Fig. 1: Feed-Forward PD Control.

$$S^2 + \frac{(1+k_{dc}K_{p1})S}{t_1} + \frac{k_{dc1}K_{i1}}{t_1} = 0 \quad (18)$$

The desired characteristic equation for the system can be expressed by Equation 19, solving for the unknowns Kp1 and ki1 to obtain the two sets of equations expressed in Equation 20 and Equation 21.

$$\frac{w_n^2}{S^2+2\zeta\omega_n s+\omega_n^2} \quad (19)$$

$$K_{i1} = \frac{2\zeta\omega_{n1}t_1-1}{K_{dc1}} \quad (20)$$

$$K_{i1} = \frac{w_{n1}^2 t_1}{k_{dc1}} \quad (21)$$

Using Equation 22 and Equation 23, the values of Kp and Ki can be obtained; the controller calculations are performed for both tanks.

$$\zeta_1 = \frac{\ln\left(\frac{1}{100}PO_1\right)}{\sqrt{\ln\left(\frac{1}{100}PO_1\right)^2+\pi^2}} \quad (22)$$

$$\omega_{n1} = \frac{4}{\zeta_1 t_{s_1}} \quad (23)$$

7.3. Zeros and the zero output problem

A discrete system S(A,B,C,D) is considered with one input and one output, in the form of Equation 24.

$$x(k+1) = Ax(k) + Bu(k)$$

$$y(k) = Cx(k) + Du(k)$$

$$k \in N = \{0,1,2,\dots\} \tag{24}$$

A, B, C, D are real matrices with appropriate dimensions. The system is called proper if $D \neq 0$, otherwise the system is called strictly proper.
A number $\lambda \in C$ is an invariant zero of the system in Equation 24 if there exist vectors $x0 \neq 0 \in C$ (state zero direction) and g $\in C$ such that λ, $x0$ and $y\ g$ satisfy the relation in Equation 25.

$$\begin{bmatrix} \lambda I - A & -B \\ C & D \end{bmatrix} \begin{bmatrix} x^0 \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{25}$$

$\lambda \in C$ is defined as the transmission zero of a transfer function if it is a zero of the minimal realization of the state variables, and the transfer function G(z) is called degenerative if it has an infinite number of transmission zeros; otherwise, it is called non-degenerative.
For each invariant zero, it is possible to assign an input that generates a zero output. To prove the above statement, the system is considered complex, allowing complex inputs, outputs, and solutions, denoted respectively as $\tilde{u}$, $\tilde{y}$, and $y\ \tilde{x}$.
If $\lambda \in C$ is an invariant zero of the system and λ, xo, g satisfy equation 2, then the input is of equation 26,

$$\tilde{u}(k) = \begin{cases} g & \text{for } k = 0 \\ \lambda^k g & \text{for } k = 1,2,\dots \end{cases} \tag{26}$$

Will generate the solution of equation 27,

$$\tilde{x}(k) = \begin{cases} x^0 & \text{for } k = 0 \\ \lambda^k x^0 & \text{for } k = 1,2,\dots \end{cases} \tag{27}$$

And the system response will be $\tilde{y}(k) = 0$ for all k ϵN (Yang et al., 2022)

7.4. Design and simulation of zero-dynamic attack

The plant state variables are given by equation 28,

$$A = \begin{bmatrix} -0.0635 & 0 \\ 0.0635 & -0.0635 \end{bmatrix}$$

$$B = \begin{bmatrix} 0.2127 \\ 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 1 \end{bmatrix}$$

$$D = 0 \tag{28}$$

The plant is discretized using the "First Order Hold" method with a sampling rate of 0.5, where the discrete state variable equations were obtained as in equation 29,

$$A_d = \begin{bmatrix} 0.968748738993070 & 0 \\ 0.030757772463030 & 0.968748738993070 \end{bmatrix}$$

$$B_d = \begin{bmatrix} 0.103035083439317 \\ 0.003254053222734 \end{bmatrix}$$

$$C_d = \begin{bmatrix} 0 & 1 \end{bmatrix}$$

$$D_d = 5.539192949936821^{-4} \tag{29}$$

When performing the discretization, two zeros are introduced into the system $\lambda = -3.6734$ and $\lambda = -0.2637$. Any zero greater than 1 is unstable, so this is the number used to perform the attack. Given that $\lambda = -3.6734$ and applying Equation 25:

$$\begin{bmatrix} \lambda * I - A_d & -B_d \\ C_d & D_d \end{bmatrix} \begin{bmatrix} x_0 \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{30}$$

Replacing the values, the following system is obtained as in equation 31:

$$\begin{bmatrix} -4.6421 & 0 & -0.1030 \\ -0.0308 & -4.6421 & -0.0033 \\ 0 & 1.000 & 0.0006 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ g \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \tag{31}$$

A solution to the problem is as in equation 32:

$$\begin{bmatrix} x_0 \\ x_1 \\ g \end{bmatrix} = \begin{bmatrix} -0.0222 \\ -0.00060 \\ 0.9998 \end{bmatrix} \tag{32}$$

The attack will be in the form of Equation 33 where Zo is the unstable zero introduced through discretization.

$$d[i] = gz_0^i \tag{33}$$

Figure 2 shows the response of the linear plant to the attack. It can be seen that although the height of tank 1 (blue line) increases exponentially, the value of the system's output (orange line) remains at zero.

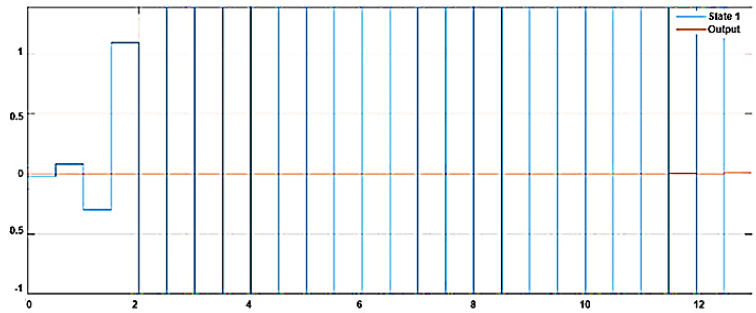


Fig. 2: Attack Simulation.

7.5. Multi-frequency sampling

Conventionally sampled systems are those in which the input and output variables are sampled every T time periods. There are synchronous and asynchronous cases, if there are delays. A multi-frequency system is one in which sampling occurs at different frequencies. Figure 3 shows a system with two sampling frequencies: a global sampling frequency, Tk, and a faster sampling frequency, kT.

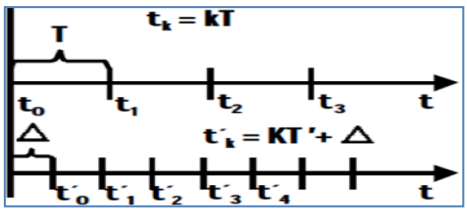


Fig. 3: Multi-Sampling.

The SISO structure, shown in Figure 4, considers two independent sampling frequencies: one at the regulator output and one at the process output. One sampling frequency is performed every T/m instants at the regulator output, and one sampling frequency is performed every T/n instants at the process output.

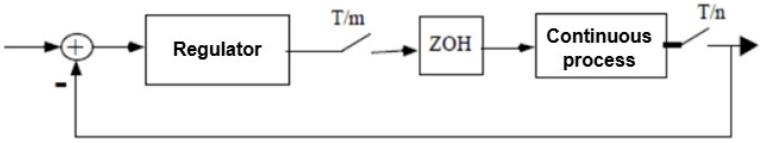


Fig. 4: Multi-Sampling Structure.

For the water tank, a variant of MRIC (multi-rate input controller) is used, which seeks to set m = 1 and n = 1/N to ensure that the control signal is generated every T time instants while the process output is generated every NT time instants.
The lifting method applied to periodic systems and multi-frequency system modeling consists of obtaining a time-invariant single-frequency model equivalent to the multi-frequency system, but with a greater number of inputs and outputs than the original system.
Kranc introduced vector connection decomposition, a method that represents multi-frequency sampling as the superposition of several conventional samples, all of them working with the longest sampling period considered in the system. This allows the use of single-frequency system analysis methods provided the ratio between frequencies is an integer (Liu et al., 2023).
Using the Velez model (Shalini et al., 2023), a new model for the tanks was obtained, presented in Figure 5. The new model has no zeros, so it is not possible to apply the zero dynamics attack.

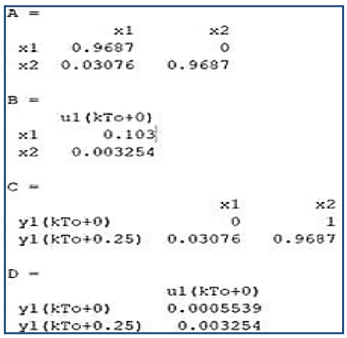


Fig. 5: "Lift" Model.

8. Description of the result

The project was structured in three stages: attack implementation and simulation, implementation of the proposed detection method, and physical implementation on a plant. The details involved in the development of each stage are presented below.

8.1. Attack design and simulation

A bibliographical survey was conducted, studying authors such as Texeira, who introduce concepts about cyber-physical attacks. To implement the attack on the water tanks, it was necessary to introduce an unstable zero through discretization using the First Order Hold method. Finally, the attack was implemented on both the linearized and nonlinear plants.

8.2. Detection method design and simulation

Based on the work (Ma, Che, & Deng, 2022), a detection model based on multi-frequency sampling was developed. The system has a global sampling rate of 0.5 seconds, but the tank outlet is sampled at 0.25 seconds, for which the crank operators proposed in the work of Vélez (Liu et al., 2023) are used.

8.3. Physical implementation

For the physical implementation, a plant characterization was performed, and real-time plant control was performed using the parameters given by Duo et al. (2022). It was not possible to implement the Zero-Dynamics Attack in the plant because the effect of saturations on the tank motors was not considered.

8.4. Computational work

The Matlab toolbox presented and studied in the works (Yang et al., 2022). The toolbox's operation is based on the crank operators, which are described below.
A continuous system G(s) is modeled in a discrete multi-frequency scheme to obtain $\mathrm{G}^{\mathrm{To}}(\mathrm{z})$ as in equation 34,

$$\mathrm{G}(\mathrm{s}) = \begin{bmatrix} \mathrm{A} & \mathrm{B} \\ \mathrm{C} & \mathrm{D} \end{bmatrix} \text{ and } \mathrm{G}^{\mathrm{To}}(\mathrm{z}) = \begin{bmatrix} \widetilde{\mathrm{A}} & \widetilde{\mathrm{B}} \\ \widetilde{\mathrm{C}} & \widetilde{\mathrm{D}} \end{bmatrix} \tag{34}$$

The multi-frequency system has the following form of equation 35:

$$\begin{cases} \mathrm{X}(\mathrm{K}+1)\mathrm{T}_0 = \widetilde{\mathrm{A}}\mathrm{x}(\mathrm{kT}_0) + \widetilde{\mathrm{B}}\mathrm{u}^{\mathrm{D}}(\mathrm{kT}_0) \\ \mathrm{y}^{\mathrm{D}}(\mathrm{kT}_0) = \tilde{\mathrm{C}}\mathrm{x}(\mathrm{kT}_0) + \widetilde{\mathrm{D}}\tilde{\mathrm{u}}(\mathrm{kT}_0) \end{cases} \quad \mathrm{k} = 0,1,2,3,\ldots$$

$$\mathrm{u}^{\mathrm{D}}(\mathrm{kT}_0) = [\mathrm{u}(\mathrm{kT}_0) \quad \mathrm{u}(\mathrm{kT}_0 + \mathrm{T}_1) \quad \ldots\ldots \quad \mathrm{u}(\mathrm{kT}_0 + (\mathrm{N}_1 - 1)\mathrm{T}_1)]^{\mathrm{T}}$$

$$\mathrm{y}^{\mathrm{D}}(\mathrm{kT}_0) = [\mathrm{y}(\mathrm{kT}_0) \quad \mathrm{y}(\mathrm{kT}_0 + \mathrm{T}_2) \quad \ldots\ldots \quad \mathrm{u}(\mathrm{kT}_0 + (\mathrm{N}_2 - 1)\mathrm{T}_2)]^{\mathrm{T}} \tag{35}$$

G(s) is the system associated with the state variables, and $GT0$ (z) is the multi-frequency digital system with a period T0. The period $T0/\mathrm{m}$ is the input period, and the period $T0/\mathrm{n}$ is the output sampling period.
The Crank operator converts N1 inputs spaced every $T0/N1$ seconds into N1 inputs at an instant $KT0$ (called the vectorization process), and converts N1 inputs at an instant $KT0$ into N2 outputs spaced every $T0/N2$ seconds (called the reduction process).
Quadruple $[\bar{A}\ \bar{B}\ ; [\bar{C}\ \bar{D}]$ of the corresponding crank operator, this is a way of internally representing a period T0 for an unconventionally sampled process. Figure 6 shows the crank system model, where [A, B, C, D] represent the internal system operating at a frequency t0, n is the number of samples at the process output, m the number of samples at the process input, and k the number of samples at frequency t0 in a meta-period to (Yang et al., 2022).

$$G^{To}(z) = \begin{bmatrix} \bar{A} & \bar{B} \\ \bar{C} & \bar{D} \end{bmatrix} = \begin{vmatrix} A^K & \ldots. & A_{11}B & \ldots. & A_{1m}B \\ \ldots. & \ldots. & \ldots. & \ldots. & D_{1m} \\ C_1 & \ldots. & D_{11} & \ldots. & \ldots. \\ C_n & \ldots. & D_{n1} & \ldots. & D_{nm} \end{vmatrix}$$

Fig. 6: Crank.

$$X = I + A + A^2 + \cdots + A^{\frac{k}{n}-1}$$

$$C_i = CA^{(i-1)\frac{k}{n}}$$

$$D_{ij} = C\left[\sum_{q=0}^{\frac{k}{m}-1} \Psi_{ij}(q)\right]B + \Omega_{ij}$$

$$\Psi_{ij} = \begin{cases} A^l, & if\ \ l = q + (i-1)\frac{k}{n} - (j-1)\frac{k}{m} - \frac{k}{m} \geq 0 \\ 0, & otherwise \end{cases}$$

$$\Omega_{ij} = \begin{cases} D, & if\ \ 0 \leq (i-1)\frac{k}{n} - (j-1)\frac{k}{m} < \frac{k}{m} \\ 0, & otherwise \end{cases}$$

Fig. 7: Crank Operators.

Figure 7 presents the equations for the implementation of the Crank operators.
The model is defined for a period T0, but internally operates with a t0 sampling rate to correctly reorder the samples taken at both the input and output levels.
All simulations were performed in Simulink, and the discrete and state variable models were obtained using MATLAB. For the real-time implementation, RT-LAB was used, a Simulink add-on.

9. Work validation

9.1. Testing methodology

To validate the attacks, the zero values were varied, along with the direction parameters, to verify that the zero dynamics effect was being applied.
The attack was implemented on the nonlinear plant, and the effect of the attack on the system was verified. This test allows us to review what happens in a real plant where linearization is not present.
A Zero-Dynamics Attack is performed on the multi-frequency plant, verifying whether the attack can be detected and whether the new model still maintains the plant's original dynamics.

9.2. Validation of simulated results

$$\begin{bmatrix} -4.6421 & 0 & -0.1030 \\ -0.0308 & -4.6421 & -0.0033 \\ 0 & 1.0000 & 0.0006 \end{bmatrix} * \begin{bmatrix} -0.0222 \\ -0.0006 \\ 0.9998 \end{bmatrix} = \begin{bmatrix} -0.0431^{-15} \\ -0.7976^{-15} \\ 0.1058^{-15} \end{bmatrix}$$

Fig. 8: Zero Dynamics Validation.

Figure 8 presents the validation of Equation 24 for the values obtained by MATLAB. As can be seen, the result is not exactly zero; it is very close to zero. However, when the zero dynamics attack is performed, this value begins to grow until it reaches a point where the approximation of this value is different from zero. This error occurs because matrix A has a determinant of 1.4222−15, which MATLAB considers to be a matrix close to singular or poorly scaled, so reaching the value of zero is impossible.
Below, an attack is presented, along with the implications of the value not being exactly equal to zero.

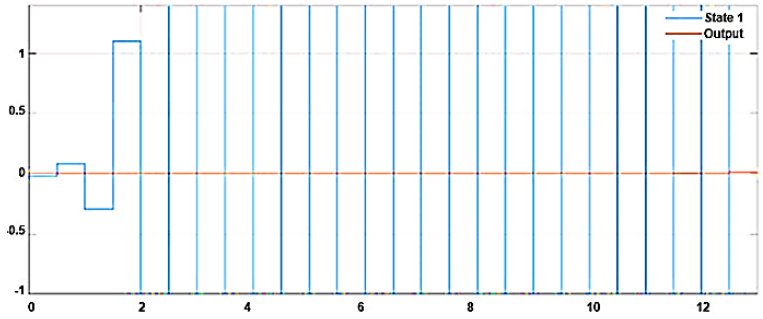


Fig. 9: Attack.

The output value, the orange line, remains relatively small, but as the attack progresses, it reaches values that are no longer negligible. If you zoom in on Figure 9 at t=14, the output value already begins to show values above one, and from this point onward, it continues to grow, as evidenced in Figure 10, where the output, represented by the orange line, moves away from zero.

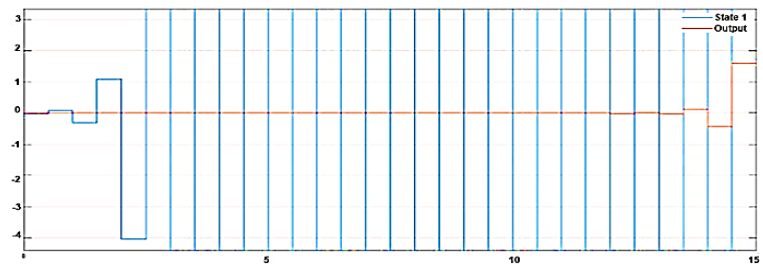


Fig. 10: Attack.

The direction of the zero states functions as a scale; changing their value only changes the moment at which the attack begins. Figure 11 shows how changing the value of g to a much smaller value causes the attack to begin at t=14, and not at t=0 as in Figure 10. However, the dynamics remain the same; the output value will continue to grow until it reaches a value that cannot be brought close to zero.

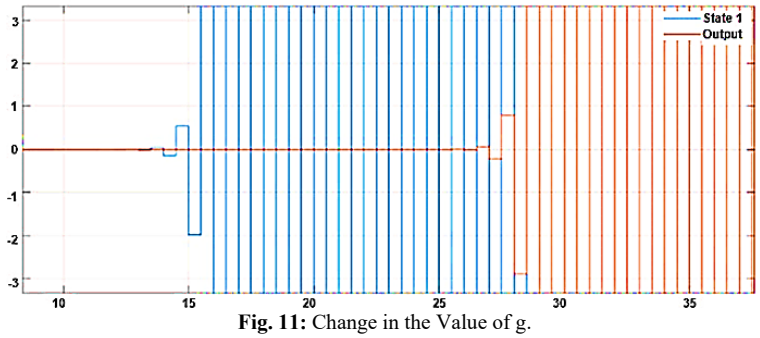


Fig. 11: Change in the Value of g.

The value of λ determines the value closest to zero for the multiplication in Equation 24.

$$\begin{bmatrix} \lambda * I - A_d & -B_d \\ C_d & D_d \end{bmatrix} \begin{bmatrix} x_0 \\ g \end{bmatrix} \tag{35}$$

Changing this value results in the attack being detected more quickly. Illustration 13 presents this situation. When performing the attack, the zero dynamics will only be met for the system zero. In the case of this work, due to numerical problems and poorly scaled matrices, implementing the attack with the system zero will be the attack that will take the longest to detect, as evidenced by the blue line in Figure 12.

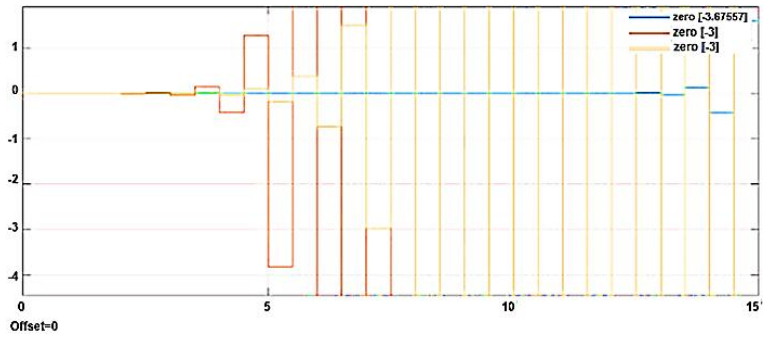


Fig. 12: Zero Change. Correct Zero Is the Blue Line, and the One That Takes the Longest to Change from Zero.

9.3. Nonlinear plant simulation

The nonlinear plant model using this system, the zero-dynamic attack was performed, resulting in Figure 13.

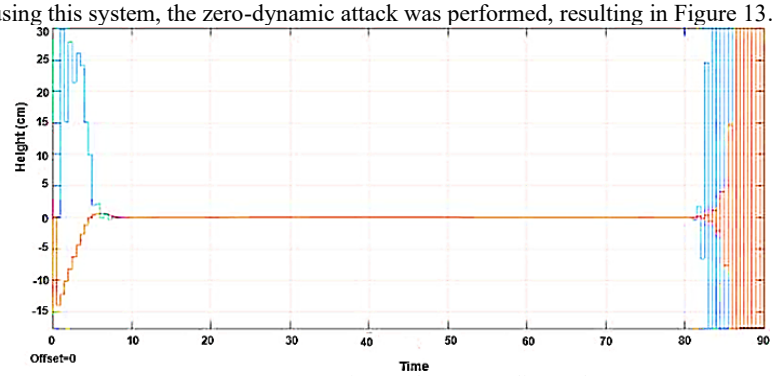


Fig. 13: Zero-Dynamic Attack on A Nonlinear Plant.

The attack begins at t=80, but the output, the orange line, remains at zero until t=83. This occurs because the attack was designed for the linearized system. Therefore, once the height state of tank one begins to exit the linearization range, the model changes, and the zero-dynamics no longer apply. However, during the period in which the zero-dynamic applies, the attack cannot be detected, and tank one begins to overflow.

9.4. Simulation of the multi-frequency model

Figure 14 shows the comparison between the multi-frequency model and the single-frequency model. As can be seen, multi-frequency estimation maintains the system dynamics and is a very close approximation to the single-frequency model.

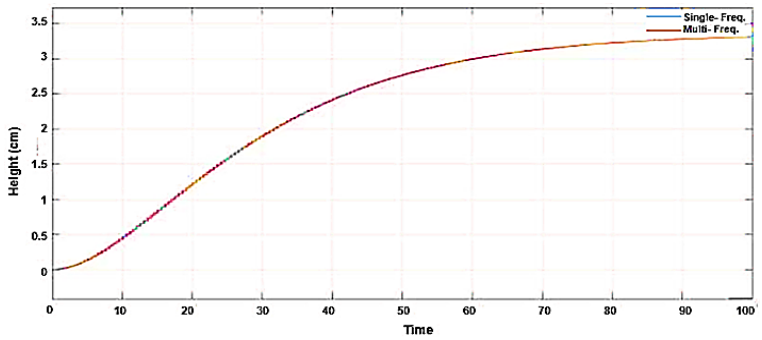


Fig. 14: Comparison of Multi-Frequency and Single-Frequency Models.

Figure 15 shows the comparison between the multi-frequency and single-frequency models under a Zero-Dynamics Attack initiated at t=100. Once the attack begins, the multi-frequency system detects the attack because the model has no zeros. Meanwhile, the single-frequency model cannot detect the attack until almost 10 seconds have passed. Figure 15 demonstrates that the Zero-Dynamics Attack can be detected through a model change using multi-frequency sampling.

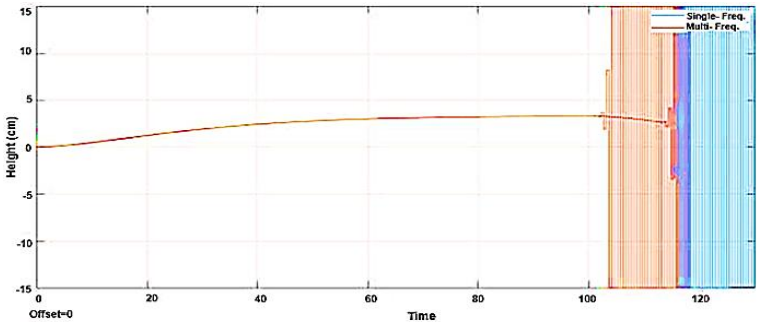


Fig. 15: Attack on a Single- and Multi-Frequency System.

Figure 15 shows the outputs of the multi-frequency and single-frequency systems. The attack begins at t=100, but the single-frequency model continues its dynamics without detecting the attack, while the multi-frequency model begins to oscillate exponentially, allowing the attack to be detected.

9.5. Plant saturation

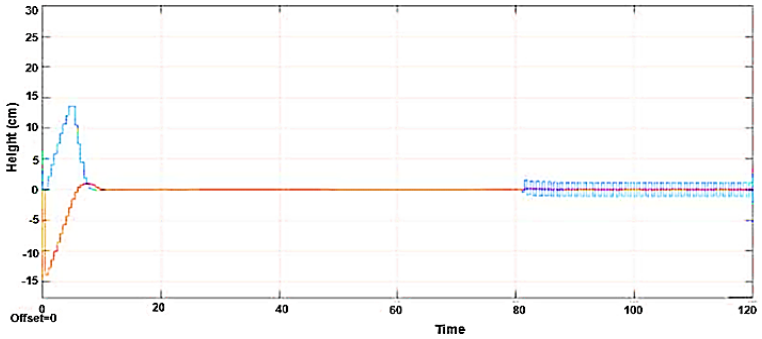


Fig. 16: Saturation.

Figure 16 shows the situation where there is saturation in the plant. Saturation does not allow the attack to grow exponentially, so the attack cannot overflow the tank. However, from this, using saturation makes it possible to counteract zero-dynamic attacks. By designing an appropriate saturation, it is possible to leave the system in a state of oscillation where the height of tank one varies constantly, but the height of tank 2 remains constant. This last situation was what occurred when the attack was physically implemented: one of the tanks oscillated constantly, while tank 2, the outgoing tank, remained constant.

9.6. Experimental setup

9.6.1. Quanser plant characterization

The plant was assembled and connected to its connections. Using the RTlab tool for real-time simulations, the plant was connected to MATLAB, and PD control was implemented. To implement the controllers and simulate the plant, the plant was linearized around the operating point, 15 cm. Once the system was linearized, the controller values were obtained, and their operation was reviewed both in simulation and in the physical operation of the plant.

Dynamic models of the plant under study were created, their operation was tested, and a control loop was implemented. Figure 17 shows the impulse response of the nonlinear system implemented in Simulink.

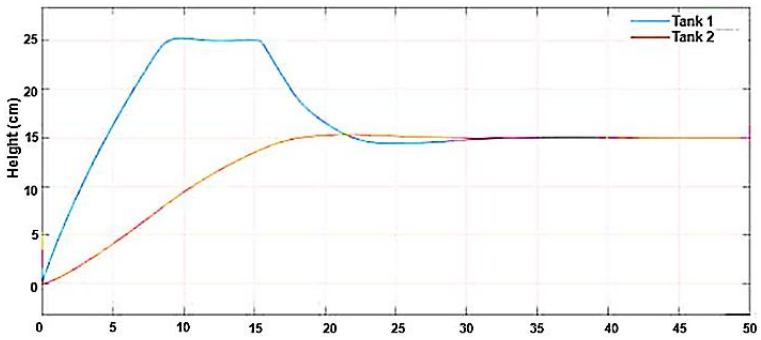


Fig. 17: Impulse Response Tank Simulation.

9.6.2. Implementation of attacks on Quanser tanks

A Zero-Dynamics Attack is implemented in Simulink; the setup is presented in Figure 18. To carry out the attack, the system was discretized, and the attack was carried out on an unstable zero of the discrete system.

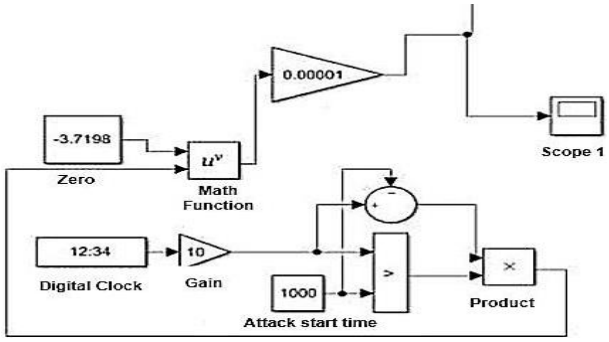


Fig. 18: Simulink Setup for Zero-Dynamics Attack.

Figure 19 shows the form of the attack. The attack grows exponentially, which can lead to plant damage if not detected quickly.

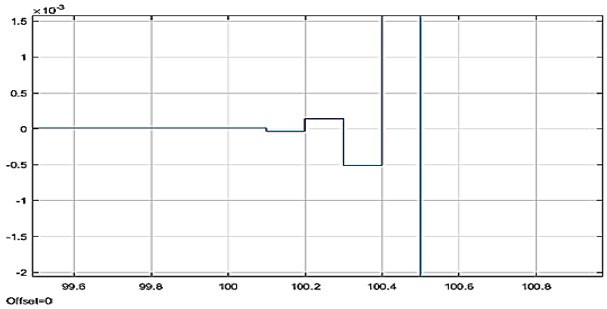


Fig. 19: Attack.

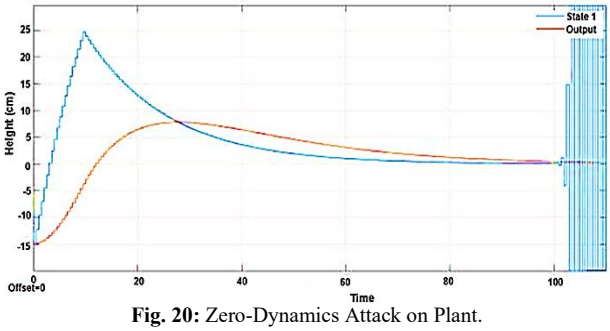


Fig. 20: Zero-Dynamics Attack on Plant.

Figure 20 shows the result obtained from carrying out the attack on the plant, once it was discretized and linearized.

9.6.3. Detection process approach

Through the results obtained in the implementation of the attacks, methodologies that allow for early detection of attacks are investigated. Through a literature review, the use of a controller with a double sampling rate was defined. This approach to the problem seeks to sample the plant at a higher rate than First Order Hold, which converts information from discrete to continuous. Using the Matlab toolbox implemented by (Shalini et al., 2023), a new multi-sampling model was generated, eliminating unstable zeros while maintaining the same system dynamics. Figure 21 shows the system used to create the multi-sampling model.

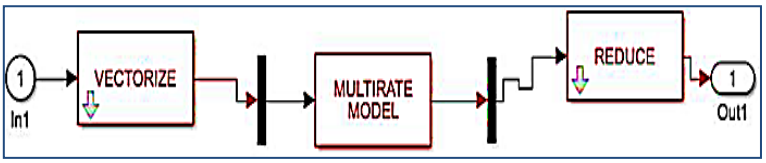


Fig. 21: Multi-Sampling Model.

9.6.4. Results analysis

A comparison of the detection and attack methods implemented was performed. Finally, the attack was implemented in the physical plant, but the expected results were not obtained because the saturation of the motors never allowed the Zero-Dynamics Attack to be fully effective.

10. Discussion

A Zero-Dynamics Attack was implemented on a nonlinear plant. To carry out the attack, it was necessary to introduce a zero through sampling. Using First Order Hold, an unstable zero was generated in the system. Using the unstable zero, it was possible to implement a Zero-Dynamics Attack, which was corroborated through simulations. Equation 24 establishes the necessary conditions to solve the zero-output problem. The system in Equation 24 should yield zero, but due to numerical problems and ill-conditioned matrices, the value is not exactly zero but very small. When implementing the attack, the value remains negligible for 10 seconds, but as the attack continues to grow, the value is no longer negligible, and the output can no longer be considered zero.

Multi-frequency sampling was proposed to change the plant model, maintaining its dynamics but removing the unstable zeros. The physical assembly of the plant was not possible due to motor saturation, which quickly saturates, preventing the Zero-Dynamics Attack from taking effect. The latter was the only objective that could not be met, and it leads to considering saturation as a possible countermeasure against cyberattacks, since these theoretically grow exponentially, but in practice, systems face physical limitations. In the case of the tank, despite sending a higher voltage signal, the water flow would not exceed a limit, so the attack could damage the motors, but it would not overflow the tank. To implement the multi-sampling detection method in physical plants, it is proposed to have an estimated model, based on the multi-frequency system, which is compared with the actual tank output. When an attack occurs, the estimated system can warn that a threat is present, since the estimate does not match the zero output shown by the physical plant.

While this study advances understanding of Zero-Dynamics Attacks and their detection in cyber-physical systems, it raises important ethical and practical considerations. Ethically, sharing knowledge about exploiting unstable zeros can risk dual-use misuse, where malicious actors may leverage this information to compromise critical systems. To mitigate this, the work avoids sharing sensitive implementation details, advocates responsible disclosure, and promotes adherence to cybersecurity research guidelines. Practically, the multi-sampling detection approach, while effective, incurs computational overhead and may strain embedded systems with limited processing capabilities. Accurate modeling is also crucial, as system nonlinearities and noise can impair detection reliability. Moreover, while physical constraints like actuator saturation may limit attack feasibility, they are not foolproof and may be circumvented through alternative stealthy strategies. Finally, generalizing the framework to other CPS domains requires addressing system-specific variations and ensuring scalable, real-time implementation. Future research should explore hardware-accelerated solutions, adaptive sampling, and model-agnostic detection strategies to address these challenges responsibly.

Although the study focuses on control engineering based on Quanser, the proposed methods—especially the multilevel search scheme and unsteady zero dynamics analysis—are widely applicable to various cyber-physical systems (CPS). Many CPS, such as autonomous vehicles, industrial robots, smart grids, and medical devices, exhibit similar discrete-time control behavior with unstable zeros due to digital implementation and sampling. The principles behind the use or detection of zero-dynamic attacks are relevant in each of these fields. However, practical application requires a search strategy focused on system-specific dynamics, sensory characteristics, and operational constraints. In addition, the robustness of uncertainty, nonlinearity, and perturbation modeling needs to be improved for real-world applications. By generalizing the modeling framework and incorporating system identification or learning-based evaluation, the proposed approach can be extended to ensure safe performance in different CAP environments.

The physical implementation of the zero-dynamic attack prevented saturation of the actuator, primarily because the control inputs required to apply the system's unstable zero exceeded the operating limits of the motor. In theory, such attacks require precise and often powerful control signals to remain stealthy during a system failure, but real-world actuators face severe constraints on torque, speed, and voltage. At the Kwanser plant, these constraints limited the loading rate and allowed deviation from the planned attack trajectory to be detected. To overcome this, several strategies can be considered: (1) adjusting the motor parameters or using higher-capacity actuators to accommodate larger input amplitudes; (2) reducing the attack trajectory or improving the stealth profile to remain within saturation limits; (3) the use of soft mesh models in simulation for attack reconstruction under more realistic input constraints; or (4) testing the method on alternative CPS platforms with more flexible or higher dynamic range actuators. This adaptation provides a better fit to theoretical attack models and physical system constraints, enabling practical validation and wider deployment.

This paper presents a comprehensive survey of zero-dynamic attacks on cyber-physical systems (CPS) by providing a practical approach for representation using different frequency samples. The study is based on rigorous modeling, simulation, and partial physics implementation, and it provides important insights into the limitations and practical considerations, particularly of actuator overlays as a passive protection mechanism. The novelty of this work is the use of crank operator theory and multi-sample search schemes to remove unstable zeros introduced during discretization. While the theoretical and simulation results are encouraging, the details—structure, clarity in technical explanations, and in-depth discussion of the generality of the approach—need to be considered to improve efficiency and impact. Overall, this paper has great potential to make a meaningful contribution to CPS security research.

11. Conclusions

Multi-frequency modeling allows for the detection of Zero-Dynamics Attacks by changing the system model and eliminating unstable zeros. The Zero-Dynamics Attack did not maintain the output at zero for all iterations due to numerical issues, but the attack can remain undetectable for a period sufficient to cause serious damage to a plant.

In simulations, the attacks work and are undetectable, but once they are implemented on a physical plant, saturations prevent the Zero-Dynamics Attack from being fully effective. The effect of saturations has not been studied in the field of cyber-physical attacks, and future work could explore their effect on preventing an attack and how to design a saturation-oriented protection against attacks.

References

[1] Hu, P.; Gao, W.; Li, Y.; Wu, M.; Hua, F.; Qiao, L. Detection of false data injection attacks in smart grids based on expectation maximization. Sensors 2023, 23, 1683. https://doi.org/10.3390/s23031683.

[2] Zahid, F.; Kuo, M.M.; Sinha, R.; Funchal, G.; Pedrosa, T.; Leitao, P. Actively Detecting Multiscale Flooding Attacks & Attack Volumes in Resource-Constrained ICPS. IEEE Trans. Ind. Inform. 2024. https://doi.org/10.1109/TII.2024.3383520.

[3] Amin, M.; El-Sousy, F.F.; Aziz, G.A.A.; Gaber, K.; Mohammed, O.A. CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: A review. IEEE Access 2021, 9, 38571–38601. https://doi.org/10.1109/ACCESS.2021.3063229.

[4] Duo, W.; Zhou, M.; Abusorrah, A. A survey of cyber attacks on cyber physical systems: Recent advances and challenges. IEEE/CAA J. Autom. Sin. 2022, 9, 784–800. https://doi.org/10.1109/JAS.2022.105548.

[5] Shih, C.S.; Chou, J.J.; Reijers, N.; Kuo, T.W. Designing CPS/IoT applications for smart buildings and cities. IET Cyber-Phys. Syst. Theory Appl. 2016, 1, 3–12. https://doi.org/10.1049/iet-cps.2016.0025.

[6] Wang, Z.; Xie, W.; Wang, B.; Tao, J.; Wang, E. A survey on recent advanced research of CPS security. Appl. Sci. 2021, 11, 3751. https://doi.org/10.3390/app11093751.

[7] Kazemi, Z.; Safavi, A.A.; Arefi, M.M.; Naseri, F. Finite-time secure dynamic state estimation for cyber–physical systems under unknown inputs and sensor attacks. IEEE Trans. Syst. Man Cybern. Syst. 2021, 52, 4950–4959. https://doi.org/10.1109/TSMC.2021.3106228.

[8] Ma, Y.S.; Che, W.W.; Deng, C. Dynamic event-triggered model-free adaptive control for nonlinear CPSs under aperiodic DoS attacks. Inf. Sci. 2022, 589, 790–801. https://doi.org/10.1016/j.ins.2022.01.009.

[9] Shalini, P.; Radha, V.; Sanjeevi, S.G. Early detection and mitigation of TCP SYN flood attacks in SDN using chi-square test. J. Supercomput. 2023, 79, 10353–10385. https://doi.org/10.1007/s11227-023-05057-x.

[10] Yang, H.; Han, H.; Yin, S.; Han, H.; Wang, P. Sliding mode-based adaptive resilient control for Markovian jump cyber–physical systems in face of simultaneous actuator and sensor attacks. Automatica 2022, 142, 110345. https://doi.org/10.1016/j.automatica.2022.110345.

[11] Liu, S.; Gao, M.; Feng, Y.; Sheng, L. Dynamic event-triggered fault detection for rotary steerable systems with unknown time-varying noise covariances. ISA Trans. 2023, 142, 478–491. https://doi.org/10.1016/j.isatra.2023.08.018.

[12] Albalawi, T.; Ganeshkumar, P. CL2ES-KDBC: A Novel Covariance Embedded Selection Based on Kernel Distributed Bayes Classifier for Detection of Cyber-Attacks in IoT Systems. Comput. Mater. Contin. 2024, 78. https://doi.org/10.32604/cmc.2024.046396.

[13] Kumari, K.; Mrunalini, M. Detecting Denial of Service attacks using machine learning algorithms. J. Big Data 2022, 9, 56. https://doi.org/10.1186/s40537-022-00616-0.

[14] Reji, M.; Joseph, C.; Nancy, P.; Lourdes Mary, A. An intrusion detection system based on hybrid machine learning classifier. J. Intell. Fuzzy Syst. 2023, 44, 4245–4255. https://doi.org/10.3233/JIFS-222427.

[15] Huang, R.; Li, Y. Adversarial attack mitigation strategy for machine learning-based network attack detection model in power system. IEEE Trans. Smart Grid 2022, 14, 2367–2376. https://doi.org/10.1109/TSG.2022.3217060.

[16] Kavousi-Fard, A.; Su, W.; Jin, T. A machine-learning-based cyber attack detection model for wireless sensor networks in microgrids. IEEE Trans. Ind. Inform. 2020, 17, 650–658. https://doi.org/10.1109/TII.2020.2964704.

[17] Combastel, C.; Zolghadri, A. A distributed Kalman filter with symbolic zonotopes and unique symbols provider for robust state estimation in CPS. Int. J. Control 2020, 93, 2596–2612. https://doi.org/10.1080/00207179.2019.1707278.

[18] Chen, B.; Ho, D.W.; Hu, G.; Yu, L. Delay-dependent distributed Kalman fusion estimation with dimensionality reduction in cyber-physical systems. IEEE Trans. Cybern. 2021, 52, 13557–13571. https://doi.org/10.1109/TCYB.2021.3119461.

[19] Choraria, M.; Chattopadhyay, A.; Mitra, U.; Ström, E.G. Design of false data injection attack on distributed process estimation. IEEE Trans. Inf. Forensics Secur. 2022, 17, 670–683. https://doi.org/10.1109/TIFS.2022.3146078.

[20] Wang, X.; Ding, D.; Ge, X.; Han, Q.L. Neural-network-based control for discrete-time nonlinear systems with denial-of-service attack: The adaptive event-triggered case. Int. J. Robust Nonlinear Control 2022, 32, 2760–2779. https://doi.org/10.1002/rnc.5831.

[21] Ma, R.; Hu, Z.; Xu, L.; Wu, L. Distributed Secure Estimation Against Sparse False Data Injection Attacks. IEEE Trans. Syst. Man Cybern. Syst. 2024, 54, 2685–2697. https://doi.org/10.1109/TSMC.2023.3344876.

[22] Ma, K.; He, N.; Fan, Z. Resilient Self-Triggered Predictive Control for Nonlinear System under Dual-Channel Deception Attacks. Nonlinear Dyn. 2024, 112, 20081–20099. https://doi.org/10.1007/s11071-024-10080-5.

[23] Eslami, A.; Kazemi, M.G.; Khorasani, K. Event-Based Covert Cyber-Attack in Switching Cyber-Physical Systems: Design and Detection Mechanisms. In Proceedings of the 2024 IEEE International Systems Conference (SysCon), Vancouver, BC, Canada, 15–18 April 2024; pp. 1–7. https://doi.org/10.1109/SysCon61195.2024.10553591.

[24] Qu, B.; Wang, Z.; Shen, B.; Dong, H.; Zhang, X. Secure Particle Filtering with Paillier Encryption-Decryption Scheme for Cyber-Physical Multi-Machine Power Grids. IEEE Trans. Smart Grid 2024, 15, 863–873. https://doi.org/10.1109/TSG.2023.3271949.

[25] Xin, L.; Long, Z.-Q. A Learning-Based Passive Resilient Controller for Cyber-Physical Systems: Countering Stealthy Deception Attacks and Complete Loss of Actuators Control Authority. IEEE/CAA J. Autom. Sin. 2024.