



EDUCACIÓN

SECRETARÍA DE EDUCACIÓN PÚBLICA



TECNOLÓGICO
NACIONAL DE MÉXICO

Tecnológico Nacional de México

**Centro Nacional de Investigación
y Desarrollo Tecnológico**

Tesis de Doctorado

Control tolerante a ataques basado en observadores

presentada por

M.C. Angel Rodrigo Guadarrama Estrada

como requisito para la obtención del grado de

**Doctor en Ciencias en Ingeniería
Electrónica**

Director de tesis

Dra. Gloria Lilia Osorio Gordillo

Codirector de tesis

Dr. Carlos Manuel Astorga Zaragoza

Cuernavaca, Morelos, México. Octubre de 2025.

 cenidet [®] Centro Nacional de Investigación y Desarrollo Tecnológico	ACEPTACIÓN DE IMPRESIÓN DEL DOCUMENTO DE TESIS DOCTORAL		Código: CENIDET-AC-006-D20
			Revisión: 0
	Referencia a la Norma ISO 9001:2008 7.1, 7.2.1, 7.5.1, 7.6, 8.1, 8.2.4		Página 1 de 2

Cuernavaca, Mor., a 02 de octubre de 2025

Dr. Carlos Manuel Astorga Zaragoza
Subdirector Académico
Presente

Los abajo firmantes, miembros del Comité Tutorial del estudiante **ANGEL RODRIGO GUADARRAMA ESTRADA** manifiestan que después de haber revisado el documento de tesis titulado **"CONTROL TOLERANTE A ATAQUES BASADO EN OBSERVADORES"**, realizado bajo la dirección de la **Dra. Gloria Lilia Osorio Gordillo** y la codirección del **Dr. Carlos Manuel Astorga Zaragoza**, el trabajo se **ACEPTA** para proceder a su impresión.

ATENTAMENTE



Dra. Gloria Lilia Osorio Gordillo
 Directora de Tesis / CENIDET



Dr. Carlos Manuel Astorga Zaragoza
 Codirector de Tesis / CENIDET



Dr. Juan Reyes Reyes
 Miembro del Comité Tutorial / CENIDET



Dra. Susana Estefany De León Aldaco
 Miembro del Comité Tutorial / CENIDET



Dr. Ricardo Fabricio Escobar Jiménez
 Miembro del comité Tutorial / CENIDET



Dr. José Fermi Guerrero Castellanos
 Benemérita Univ. Autónoma de Puebla

c.c.p: Mtra. Verónica Sotelo Boyas/ jefa del Departamento de Servicios Escolares.
 c.c.p: Dr. Jarniel García Morales / jefe del Departamento de Ingeniería Electrónica.
 c.c.p: Expediente.



Centro Nacional de Investigación y Desarrollo tecnológico
Subdirección Académica

Cuernavaca Mor, 03/octubre/2025

Oficio No. SAC/234/2025

Asunto: Autorización de impresión de tesis

ANGEL RODRIGO GUADARRAMA ESTRADA
CANDIDATO AL GRADO DE DOCTOR EN CIENCIAS
EN INGENIERÍA ELECTRÓNICA
P R E S E N T E

Por este conducto, tengo el agrado de comunicarle que el Comité Tutorial asignado a su trabajo de tesis titulado **"CONTROL TOLERANTE A ATAQUES BASADO EN OBSERVADORES"**, ha informado a esta Subdirección Académica, que están de acuerdo con el trabajo presentado. Por lo anterior, se le autoriza a que proceda con la impresión definitiva de su trabajo de tesis.

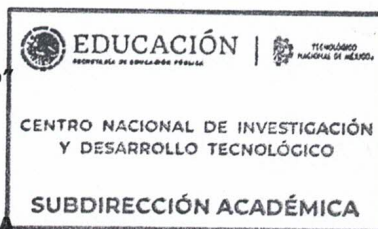
Esperando que el logro del mismo sea acorde con sus aspiraciones profesionales, reciba un cordial saludo.

ATENTAMENTE

Excelencia en Educación Tecnológica®

"Conocimiento y Tecnología al Servicio de México"

CARLOS MANUEL ASTORGA ZARAGOZA
SUBDIRECTOR ACADÉMICO



c.c.p. Departamento de Ingeniería Electrónica
Departamento de Servicios Escolares

CMAZ/lmz



2025
Año de
La Mujer
Indígena

Interior Internado Palmira S/N, Col. Palmira,
C. P. 62490, Cuernavaca, Morelos Tel. 01 (777) 3627770, ext. 4104,
e-mail: acad_cenidet@tecnm.mx tecnm.mx | cenidet.tecnm.mx

cenidet
Centro Nacional de Investigación
y Desarrollo Tecnológico



Dedicatoria

“Dedico esta tesis, con profundo amor y gratitud, a mi familia, a mi novia, a mis amigos, a mis estudiantes, a mis asesores, a mis profesores y a mis compañeros de trabajo. Gracias por su apoyo constante, por inspirarme siempre a superarme y por brindarme su compañía, amistad y cariño en cada etapa de este camino académico y personal.”

Agradecimientos

Agradezco a la Secretaría de Ciencia, Humanidades, Tecnología e Innovación (SECIHTI), por el apoyo económico brindado durante este período, fundamental para la culminación de mis estudios. Extiendo también mi gratitud al CENIDET y a cada uno de los trabajadores de esta institución por abrirme sus puertas y brindarme los recursos necesarios para el desarrollo de esta investigación.

A mis padres, Elsa Elizabeth Estrada Cortés y Angel Guadarrama Reynoso, así como a mi hermano, Ricardo Eduardo Guadarrama Estrada, por su amor, paciencia y apoyo constante. Han sido para mí un ejemplo de dedicación y cariño, y gracias a sus palabras de aliento he encontrado siempre la motivación para mejorar cada día, cumplir mis objetivos y alcanzar mis sueños, siendo parte fundamental de ellos.

A mi asesora de tesis, la Dra. Gloria Lilia Osorio Gordillo, por su paciencia, amistad y disponibilidad para atender cada duda que surgía. Le agradezco sus valiosos consejos y la guía constante a lo largo de estos seis años. De igual manera, al Dr. Carlos Manuel Astorga Zaragoza, co-asesor de esta investigación, por su acompañamiento y orientación.

A mi novia, Magdalena Márquez, por su amor, apoyo y ánimo constante para esforzarme y dar siempre lo mejor de mí.

A mi familia extendida, por su cariño y aliento en los momentos más importantes: a mis tías Lilia y Adriana Estrada, Janeth, Mireya y Gabriela, a mis abuelitas Elizabeth Cortés y Teresa Reynoso, a mis primos Sergio, Karla, Eimy, Emma, Lucino, María Teresa, Adán, Valeria, Pamela, Silvana, quienes me inspiran a ser mejor cada día y darles siempre un buen ejemplo, así como a mis tíos Jafeth, Jorge y Antonio, por su compañía y respaldo.

A mis amigos Raymundo, Francisco, Carlos, Daniel y Ezequiel, por su amistad, compañerismo y todas las risas compartidas. Asimismo, agradezco a mis amigos del CENIDET: Elías, Isaac, Yusef, Felipe, Óscar, Rossel y Alex, por acompañarme durante este proceso académico y por la mutua motivación en el camino.

A mis revisores, el Dr. Ricardo Fabricio Escobar Jiménez, el Dr. Juan Reyes Reyes, la Dra. Susana de León Aldaco y el Dr. José Fermi Guerrero Castellanos, por sus valiosos comentarios y observaciones que enriquecieron este trabajo, así como por la amistad y guía brindadas durante mi estancia.

Al Dr. Olivier Sename, por brindarme la oportunidad de realizar una estancia de investigación en el laboratorio Gipsa-Lab en Grenoble, Francia. Esta experiencia ha sido fundamental en mi formación académica y profesional.

Asimismo, extendiendo mi gratitud a mis amigos Elfrich, Natalio, Alfredo, Lina, Alessandro, Nguyen, y a todo el equipo de Gipsa-Lab, quienes, con su apoyo, compañía y colaboración, hicieron de mi estancia una etapa enriquecedora tanto en lo académico como en lo personal.

A cada uno de mis profesores en el CENIDET, quienes contribuyeron de manera significativa a mi formación académica y profesional.

Finalmente, a mis estudiantes de la UTEZ, quienes me motivan cada día a esforzarme más y seguir creciendo como docente e investigador.

Publicaciones

Artículo publicado

- Guadarrama-Estrada, A. R., Osorio-Gordillo, G. L., Vargas-Méndez, R. A., Reyes-Reyes, J., Astorga-Zaragoza, C. M. (2025). Cyber-Physical System Attack Detection and Isolation: A Takagi-Sugeno Approach. *Mathematical and Computational Applications*, 30(1), 12. <https://doi.org/10.3390/mca30010012>

Revista sometida

- Guadarrama-Estrada, A.-R., Osorio-Gordillo, G. L., Vargas-Méndez, R.-A., Reyes-Reyes, J., and Escobar-Jiménez, R.-F. (under review). *Estimation of False Data Injection Attacks via Generalized Dynamic Observer.* *Optimal Control, Applications and Methods*.

Documentos de conferencias

- Guadarrama Estrada, Angel Rodrigo, Osorio-Gordillo, Gloria-Lilia, Astorga-Zaragoza, Carlos, Reyes-Reyes, Juan. Observer Design for Detection of Attack Patterns in Cyber-Physical Systems. *Memorias del Congreso Nacional de Control Automático*, pp. 473-478, 2023. <https://doi.org/10.58571/CNCA.AMCA.2023.063>.
- Guadarrama-Estrada, A.-R., Osorio-Gordillo, G.-L. (2023). Attack detection scheme in cyber-physical systems using a bank of observers. *Proceedings of the X Conference on Applied Science and Technology* 2023.
- Guadarrama-Estrada, A.-R., Osorio-Gordillo, G.-L., Astorga-Zaragoza, C.-M., Reyes-Reyes, J. (2023, October 25-27). Observer design for detection of attack patterns in cyber-physical

systems. Proceedings of the 2023 National Congress on Automatic Control, Acapulco, Guerrero, Mexico. ISSN: 2594-2492.

Resumen

Este trabajo propone el diseño de un esquema de control resiliente y tolerante a ataques basado en Observadores Dinámicos Generalizados (GDO, por sus siglas en inglés) para sistemas Ciberfísicos discretos. Estos sistemas son vulnerables a diversos tipos de ataques, tales como Denegación de Servicio (DoS, por sus siglas en inglés), Ataques de Suplantación de Datos (DDA, por sus siglas en inglés) e Inyección Aleatoria de Datos (RDI, por sus siglas en inglés), los cuales se modelan utilizando una señal de activación Markoviana que toma valores de 0 o 1. Es importante destacar que estos ataques afectan tanto las señales de control como las lecturas de los sensores del sistema.

La motivación principal para implementar resiliencia en el controlador radica en la creciente complejidad de los sistemas ciber-físicos y la sofisticación de los ataques que enfrentan en el contexto de la Industria 4.0. Esto se debe a que estos sistemas están altamente expuestos por el uso de canales de comunicación abiertos para la transmisión de datos.

Los canales de comunicación abiertos en sistemas Ciber-físicos no garantizan la seguridad de la operación del sistema, lo cual pone en riesgo su integridad y funcionalidad. En este contexto, el objetivo principal de este trabajo es abordar una oportunidad en el campo de la ingeniería de la información, que tradicionalmente se ha enfocado en asegurar los datos sin considerar adecuadamente el bienestar físico del sistema controlado. En la teoría de los sistemas Ciber-físicos, se ha introducido el concepto de un “sistema inmunológico digital”, que propone proteger los sistemas mediante la aplicación de diversas disciplinas, como la informática, las telecomunicaciones y, en nuestro caso, el control automático. El propósito es crear un sistema que proteja tanto los datos y claves, como la integridad del sistema y la seguridad del usuario.

En los sistemas ciber-físicos, es crucial conocer el estado actual del sistema, mitigar los ataques y

estimar señales como perturbaciones, fallas o, en este caso, ataques. Esto permite desarrollar técnicas que aseguren el control del sistema, manteniendo su operación ideal y previniendo pérdidas económicas, daños materiales o incluso la pérdida de vidas humanas.

Este trabajo tiene como objetivo demostrar que el método de control resiliente propuesto puede asegurar la convergencia frente a diferentes esquemas de ataque complejos, manteniendo el comportamiento del sistema dentro de un marco operacional adecuado. Para ello, se emplearán diversos esquemas de diagnóstico, destacando el uso de un observador dinámico generalizado diseñado para identificar, aislar, localizar y estimar el comportamiento de distintos ataques aplicados al sistema ciberfísico. Antes de llegar al diseño final del esquema propuesto, se evaluarán paso a paso diferentes esquemas para determinar el límite de cada uno frente a diversos ataques. Se utilizarán bancos de observadores, observadores proporcional-integrales, observadores tipo Luenberger y observadores dinámicos generalizados para la detección, localización, aislamiento y estimación de ataques.

Se realizarán múltiples simulaciones para validar el enfoque propuesto, considerando distintos sistemas Ciber-físicos y los esquemas de ataque seleccionados. Estos ataques podrán aplicarse de manera coordinada, afectando tanto las entradas como las salidas del sistema, o impactando solo una de estas variables. Además, la lógica Markoviana permitirá asignar una distribución uniforme o no uniforme para la activación de los ataques. Es importante señalar que el esquema propuesto no está diseñado para un solo caso de estudio, sino que se aplicará a diversos sistemas Ciber-físicos.

El análisis comenzará con tres tanques interconectados, donde los sensores y actuadores estarán expuestos a distintos esquemas de ataque estocásticos Markovianos. Adicionalmente, el enfoque se aplicará a un sistema glucosa-insulina y a la representación LPV de un vehículo, como parte de una estancia académica en Gipsa-Lab, donde los esquemas de diagnóstico mencionados fueron implementados en un vehículo monitoreado y controlado utilizando herramientas como OptiTrack y Matlab. Con base en la estimación del comportamiento de los distintos esquemas de ataque, se diseñarán diversos esquemas de control para estimar el comportamiento de los ataques y generar un modelo de referencia libre de ataques. Esto facilitará la comparación entre un sistema libre de ataques y uno afectado por ataques al actuador y al controlador.

Abstract

This work proposes the design of a resilient and attack-tolerant control scheme based on Generalized Dynamic Observers (GDO) for discrete Cyber-Physical Systems (CPS). These systems are vulnerable to various types of attacks, such as Denial of Service (DoS), Data Deception Attacks (DDA), and Random Data Injection (RDI), which are modeled using a Markovian activation signal that takes values of 0 or 1. It is important to highlight that these attacks affect both the control signals and the sensor readings of the system.

The main motivation for implementing resilience in the controller lies in the growing complexity of cyber-physical systems and the sophistication of the attacks they face in the context of Industry 4.0. This is due to the high exposure of these systems through the use of open communication channels for data transmission.

Open communication channels in cyber-physical systems do not guarantee the security of system operation, which puts its integrity and functionality at risk. In this context, the main objective of this work is to address an opportunity in the field of information engineering, which has traditionally focused on securing data without adequately considering the physical wellbeing of the controlled system. In the theory of Cyber-Physical Systems, the concept of a “digital immune system” has been introduced, which proposes protecting systems through the application of various disciplines, such as computer science, telecommunications, and, in our case, automatic control. The purpose is to create a system that safeguards not only data and keys, but also the integrity of the system and the safety of the user.

In cyber-physical systems, it is crucial to know the current state of the system, mitigate attacks, and estimate signals such as disturbances, faults, or, in this case, attacks. This enables the de-

velopment of techniques that ensure system control, maintaining ideal operation and preventing economic losses, material damage, or even loss of human life.

The aim of this work is to demonstrate that the proposed resilient control method can ensure convergence against different complex attack schemes, keeping the system's behavior within an adequate operational framework. For this purpose, several diagnostic schemes will be employed, highlighting the use of a generalized dynamic observer designed to identify, isolate, localize, and estimate the behavior of various attacks applied to the cyber-physical system. Before reaching the final design of the proposed scheme, different approaches will be evaluated step by step to determine their limits against different attacks. Observer banks, proportional-integral observers, Luenberger-type observers, and generalized dynamic observers will be used for the detection, localization, isolation, and estimation of attacks.

Multiple simulations will be carried out to validate the proposed approach, considering different cyber-physical systems and the selected attack schemes. These attacks may be applied in a coordinated manner, affecting both the inputs and outputs of the system, or impacting only one of these variables. Furthermore, the Markovian logic will allow assigning either a uniform or a non-uniform distribution for the activation of the attacks. It is important to note that the proposed scheme is not designed for a single case study but will be applied to various cyber-physical systems.

The analysis will begin with three interconnected tanks, where sensors and actuators will be exposed to different stochastic Markovian attack schemes. In addition, the approach will be applied to a glucose-insulin system and to the LPV representation of a vehicle, as part of an academic stay at Gipsa-Lab, where the mentioned diagnostic schemes were implemented in a monitored and controlled vehicle using tools such as OptiTrack and MATLAB. Based on the estimation of the behavior of different attack schemes, various control schemes will be designed to estimate attack behavior and generate an attack-free reference model. This will facilitate the comparison between an attack-free system and one affected by attacks on the actuator and controller.

Índice general

Índice general	x
Índice de figuras	xvi
Índice de cuadros	xx
Nomenclatura	xxii
1 Introducción	1
1.1 Planteamiento del problema	3
1.2 Objetivos	4
1.2.1 Objetivo general	4
1.2.2 Objetivos específicos	4
1.3 Metas	4
1.4 Justificación	5
1.5 Hipótesis	5
1.6 Metodología	5
1.7 Alcance	6
1.8 Contribuciones	7
1.9 Originalidad	7
1.10 Estructura de la tesis	8
2 Estudio del estado del arte	11
2.1 Proceso de revisión y selección de literatura	12
2.2 Casos de estudio utilizados	15
2.3 Sistemas ciberfísicos	16

2.4	Ataques en sistemas ciberfísicos	17
2.5	Esquemas de diagnóstico de ataques	19
2.6	Control tolerante a los ataques	21
2.7	Conclusiones del capítulo	22

3 Marco teórico 25

3.1	Sistemas ciberfísicos	26
3.1.1	Arquitecturas de sistemas ciberfísicos	27
3.2	Ataques a los sistemas ciberfísicos	28
3.2.1	Diferencias entre ataques y fallas	31
3.3	Ataques con distribución Markoviana	33
3.3.1	Modelo general de sistema bajo ataque	34
3.3.2	Ataque de denegación de servicio (DoS)	34
3.3.3	Ataque de decepción de datos (DDA)	34
3.3.4	Ataque de inyección aleatoria (RDI)	35
3.3.5	Lógica de activación (uniforme / no uniforme) y coordinación	35
3.4	Sistemas tomados como casos de estudio	36
3.4.1	Sistema de tanques interconectados	37
3.4.2	Dinámica de vehículos RC	40
3.4.3	Sistema glucosa-insulina	42
3.5	Estrategias de modelado para el análisis de sistemas No Lineales	43
3.5.1	Teoría de los sistemas Takagi-Sugeno	44
3.5.2	Teoría del sistema LPV	48
3.6	Teoría de los Observadores	49
3.6.1	Clasificación de los observadores según su estructura	50
3.6.2	Observabilidad	53
3.7	Observadores para diagnóstico de fallas	54
3.7.1	Observadores para la detección y el aislamiento de fallas	55
3.7.2	Observadores para la estimación de fallas	55
3.8	Teoría de la estabilidad y las LMI	57
3.8.1	Estabilidad mediante funciones de Lyapunov	57

3.8.2	Planteamiento de condiciones de estabilidad con LMIs	58
3.9	Controladores	58
3.9.1	Estructura de sistemas de control	59
3.9.2	Controladores Proporcional, PI y PID	59
3.9.3	Controladores basados en observadores	62
3.10	Control tolerante a ataques	63
3.11	Métricas de resiliencia	65
3.12	Conclusiones del capítulo	66
4	Modelado de casos prácticos	68
4.1	Representación Takagi-Sugeno del sistema de tanques interconectados	68
4.1.1	Simulación de modelos no lineales	68
4.1.2	Modelo Takagi-Sugeno	71
4.1.3	Simulaciones	76
4.2	Representación T-S del sistema glucosa-insulina	78
4.2.1	Modelo no lineal del sistema glucosa-insulina	79
4.2.2	Modelo Takagi-Sugeno del sistema glucosa-insulina	81
4.2.3	Simulaciones del sistema glucosa-insulina	82
4.3	Representación LPV del vehículo RC	85
4.3.1	Modelo no lineal discreto del vehículo RC	86
4.3.2	Modelo LPV politópico discreto	87
4.3.3	Simulaciones: modelo NL vs LPV discreto	87
4.4	Conclusiones del capítulo	90
5	Observadores para la detección de ataques	92
5.1	Banco de observadores para la detección de ataques	92
5.1.1	Observador tipo Luenberger	93
5.1.2	Banco de observadores dedicados (DOS)	94
5.1.3	Modelo matemático y diseño del banco de observadores	94
5.1.4	Análisis de estabilidad (LMIs)	95
5.1.5	Simulación con esquemas de ataque	95
5.1.6	Conclusiones de la sección (Banco DOS)	100

5.2	Observador Generador de Residuos (OGR): resultados con el sistema glucosa–insulina	
	T–S	101
5.2.1	Esquema del OGR	101
5.2.2	Formulación paramétrica T–S discreta y sistema bajo ataque	102
5.2.3	Diseño del observador tipo Luenberger	103
5.2.4	Análisis de estabilidad del observador	104
5.2.5	Simulación y generación de residuos	104
5.2.6	Conclusión y contraste entre DOS y OGR	107
6	Observador ODG para aislamiento, detección y localización	110
6.1	Modelo matemático y diseño	111
	6.1.1 Análisis de estabilidad del observador	118
6.2	Simulación con esquemas de ataque	120
	6.2.1 Caso 1: Ataque DoS en actuador con lógica uniforme	121
	6.2.2 Caso 2: Ataque DDA en el actuador con lógica no uniforme	123
	6.2.3 Caso 3: Ataque RDI en el actuador con lógica uniforme	124
	6.2.4 Caso 4: Ataques simultáneos en el actuador	126
6.3	Conclusiones del capítulo	127
7	Observador ODG para la estimación de ataques de variación lenta	129
7.1	Modelo matemático y diseño	129
	7.1.1 Parametrización del observador	131
	7.1.2 Análisis de estabilidad del observador	133
7.2	Simulaciones: ODG con ataques de variación lenta	135
	7.2.1 Entradas del sistema y lógica Markoviana de ataque	135
	7.2.2 Simulación con ataque uniforme	136
	7.2.3 Simulación con ataque no uniforme	138
7.3	Conclusiones del capítulo	138
8	ODG para estimación de ataques dinámicos	140
8.1	Modelo matemático del sistema con ataques dinámicos	141
8.2	Estructura del Observador Dinámico Generalizado	142

8.3	Diseño del Observador Dinámico Generalizado (ODG)	144
8.3.1	Parametrización del observador	145
8.3.2	Ecuación de error del ODG	146
8.4	Análisis de estabilidad del ODG	146
8.4.1	Planteamiento del problema de estabilidad	146
8.4.2	Función de Lyapunov y condiciones de estabilidad	147
8.4.3	Índice de desempeño $\mathcal{L}_2$	147
8.4.4	Formulación en LMIs	148
8.5	Simulación con esquemas de ataque	148
8.5.1	Escenario 1: Ataque DDA uniforme coordinado	150
8.5.2	Escenario 2: Ataque DoS uniforme en el actuador	151
8.5.3	Escenario 3: Ataque RDI no uniforme en sensores	152
8.6	Conclusiones del capítulo	153
9	Instrumentación en la plataforma del GIPSA-Lab	154
9.1	Descripción general de la plataforma	155
9.2	Componentes del vehículo RC	156
9.3	Interfaz de conexión y flujo de datos	157
9.4	Procedimiento de configuración y pruebas	158
9.5	Pruebas y validación	159
9.6	Conclusión	161
10	Control tolerante a ataques	164
10.1	Ley de control tolerante	164
10.2	Observador Dinámico Generalizado (ODG)	165
10.3	Dinámica de estimación y error de seguimiento	165
10.4	Sistema aumentado y estimación	166
10.5	Análisis de estabilidad del Control Tolerante a Ataques	166
10.5.1	Función de Lyapunov candidata	167
10.5.2	Condición de disminución de Lyapunov	167
10.5.3	Planteamiento de la LMI	168
10.6	Simulaciones bajo diferentes esquemas de ataque	168

10.6.1	Caso 1: Sistema sin ataques	168
10.6.2	Caso 2: Ataques RDI de variación suave (Markovianos uniformes)	169
10.6.3	Caso 3: Ataque DoS no uniforme	170
10.6.4	Discusión general	172
11	Evaluación de métricas de resiliencia del controlador	175
11.1	Propósito y alcance	175
11.2	Protocolo de evaluación	176
11.3	Criterios de desempeño y robustez (basados en error)	176
11.4	Métricas adicionales basadas en la diferencia de trayectoria	177
11.5	Criterios de detección y recuperación	178
11.6	Impacto relativo en desempeño y energía	178
11.7	Índice escalar de resiliencia	179
11.8	Resultados comparativos	180
11.9	Discusión	180
11.10	Conclusiones del capítulo	181
12	Conclusiones y trabajo futuro	182
12.1	Trabajos futuros	183
	Bibliografía	184

Índice de figuras

2.1	Resumen del estado del Arte.	11
2.2	Revisión y selección del estado del arte.	13
3.1	Esquema de un sistema ciber-físico.	27
3.2	Arquitectura de los sistemas ciberfísicos.	29
3.3	Resumen de los tipos de ataques dirigidos a sistemas ciberfísicos.	30
3.4	Diferencias entre ataques y fallas.	31
3.5	Esquema general de ataque a un CPS.	33
3.6	Clasificación de ataques.	33
3.7	Lógicas uniformes de activación: no coordinada, coordinada.	36
3.8	Lógicas no uniformes de activación: coordinada, no coordinada.	36
3.9	Esquema del caso de estudio (Tres tanques interconectados).	38
3.10	Representación del vehículo mediante el modelo bicicleta.	41
3.11	Diagrama del sistema glucosa-insulina en pacientes con DM-1.	42
3.12	Esquema del observador tipo Luenberger.	51
3.13	Esquema del observador proporcional.	52
3.14	Esquema del observador proporcional-Integral.	53
3.15	Diagrama del observador dinámico generalizado.	54
3.16	Esquema general de un banco de observadores para detección y aislamiento de fallas.	56
3.17	Esquema conceptual de un observador con estimación directa del comportamiento de la falla.	56
3.18	Diagrama a bloques de un sistema de control en lazo abierto.	59
3.19	Diagrama a bloques de un sistema de control en lazo cerrado.	60
3.20	Esquema de un controlador proporcional (P).	60

3.21	Esquema de un controlador proporcional-integral (PI).	61
3.22	Esquema de un controlador proporcional-integral-derivativo (PID).	62
3.23	Esquema general de un controlador basado en observadores.	63
3.24	Esquema de un controlador tolerante al ataque mediante compensación de la estimación del ataque.	64
4.1	Simulación: Perfil de entrada de flujo para los tanques 1 y 2.	77
4.2	Comparación del modelo no lineal y el modelo T-S discreto.	78
4.3	Entradas de glucosa e insulina para la simulación del sistema glucosa-insulina.	83
4.4	Comparación de niveles de glucosa: modelo no lineal vs T-S discreto.	84
4.5	Activación de funciones de pertenencia del modelo T-S discreto durante la simulación.	85
4.6	Perfil de entrada de dirección $\delta(k)$ utilizado en las simulaciones.	88
4.7	Comparación entre el modelo no lineal discreto y el modelo LPV discreto: (a) velocidad lateral v_y , (b) velocidad de guiñada ω	89
4.8	Evolución de las funciones de pertenencia $\mu_i(\rho)$ en el modelo LPV discreto.	89
5.1	Esquema general del observador de Luenberger para sistemas Takagi–Sugeno discretos.	93
5.2	Entradas de bombeo en (5.7). Eje horizontal: índice k ($t = kT_d$).	96
5.3	Señales Markovianas (uniforme y no uniforme) usadas para activar ataques.	96
5.4	Estados bajo DoS en y_2 (lógica uniforme). Eje: k ($t = kT_d$).	97
5.5	Residuos ante DoS en y_2 : r_2 cruza el umbral τ_2 ; r_1, r_3 cercanos a cero.	97
5.6	Estados bajo DDA en u_1 (no uniforme).	98
5.7	Residuos ante DDA en u_1 : activación multicanal con predominio en r_1	98
5.8	Estados bajo RDI coordinado en y_3 y u_2	99
5.9	Residuos ante RDI coordinado: activación de r_3 y activaciones adicionales por la vía de u_2	99
5.10	Esquema del observador generador de residuos (OGR) para la activación de ataques en sensor/actuador.	102
5.11	Señales Markovianas uniforme (rojo) y no uniforme (negro) empleadas para la activación de ataques.	105
5.12	Comparación de salida real y estimada bajo ataque DoS en el sensor $y(k)$	105
5.13	Residuo $r(k)$ durante un ataque DoS en $y(k)$	106

5.14	Estados reales y estimados bajo ataque DDA en el actuador de insulina.	106
5.15	Error de estimación $e(k)$ durante un ataque DDA en el actuador.	107
5.16	Estados reales y estimados bajo ataque combinado (DDA + DoS).	108
5.17	Comparación entre residuo $r(k)$ y error de estimación $e(k)$ para diagnóstico de ataques combinados.	108
6.1	Esquema del Observador de Detección Generalizada (ODG) basado en representación T-S.	111
6.2	Entradas de caudal $Q_1(k)$ y $Q_2(k)$ aplicadas al sistema de tres tanques.	120
6.3	Distribución de activación del ataque DoS en actuador u_1 (lógica uniforme Markoviana).	121
6.4	Evolución de los estados x_1, x_2, x_3 bajo ataque DoS en u_1	122
6.5	Residuos generados por el observador ODG bajo ataque DoS uniforme.	122
6.6	Flujo del ataque DDA en el actuador u_2 con lógica no uniforme.	123
6.7	Evolución de los estados bajo ataque DDA en el actuador u_2	123
6.8	Residuos generados por el observador ODG ante ataque DDA en el actuador u_2 . . .	124
6.9	Evolución de los estados bajo ataque RDI en el actuador u_1	125
6.10	Residuos generados por el observador ODG ante ataque RDI en el actuador u_1 . . .	125
6.11	Comportamiento del sistema en presencia de ataques simultáneos uniformes sobre u_1 (DDA) y u_2 (RDI).	126
6.12	Residuos generados por el observador ODG en presencia de ataques simultáneos uniformes sobre u_1 y u_2	127
7.1	Entradas de caudal variables utilizadas en el sistema de tres tanques interconectados.	136
7.2	Lógicas Markovianas de ataque: uniforme (línea negra) y no uniforme (línea roja). .	136
7.3	Estimación de variables y esquema de ataque uniforme tipo FDI.	137
7.4	Efecto del ataque uniforme DDA sobre las variables de estado y su estimación (ODG).	137
7.5	Estimación de ataque tipo DDA con distribución no uniforme.	138
7.6	Efecto del ataque no uniforme DDA sobre los estados del sistema y su estimación (ODG).	139

8.1	Entradas de caudal $Q_1(k)$ y $Q_2(k)$ utilizadas en el sistema de tres tanques interconectados.	149
8.2	Lógicas Markovianas de activación para ataques: uniforme (negro) y no uniforme (rojo).	150
8.3	Estimación de ataques DDA (actuador y sensores) bajo lógica uniforme mediante el ODG.	150
8.4	Estados estimados por el ODG bajo ataques DDA uniformes coordinados.	151
8.5	Estimación del ataque DoS uniforme en el actuador por medio del ODG.	151
8.6	Estados estimados por el ODG en presencia de DoS uniforme.	152
8.7	Efecto del ataque RDI no uniforme sobre los estados reales.	152
8.8	Estimación de estados y reconstrucción del ataque RDI no uniforme mediante el ODG.	153
9.1	Laboratorio VICON en GIPSA-Lab: espacio de captura y estación de control con ROS2.	156
9.2	Componentes principales del vehículo RC utilizado en GIPSA-Lab.	156
9.3	Estructura de conexión entre ROS2, MATLAB/Simulink, Vicon y el vehículo RC.	158
9.4	Reconocimiento del vehículo por el sistema Vicon y ROS2.	159
9.5	Ejecución de controladores en Simulink conectados a ROS2.	160
10.1	Trayectoria de referencia y real sin presencia de ataques.	169
10.2	Respuesta del yaw rate sin ataques.	169
10.3	Trayectoria bajo ataques de variación suave.	170
10.4	Comportamiento del yaw rate bajo ataques suaves.	171
10.5	Velocidad longitudinal bajo ataques Markovianos uniformes.	171
10.6	Trayectoria bajo ataques dinámicos no uniformes (DoS, DDA, RDI).	172
10.7	Respuesta del yaw rate bajo ataques dinámicos.	173
10.8	Velocidad longitudinal bajo ataques intensos.	173

Índice de cuadros

Tabla2.1	Distribución de artículos seleccionados por base de datos.	14
Tabla2.2	Resumen de artículos clave sobre casos de estudio.	16
Tabla2.3	Artículos fundamentales sobre teoría de Sistemas Ciberfísicos.	18
Tabla2.4	Clasificación de ataques en Sistemas Ciberfísicos.	19
Tabla2.5	Métodos de diagnóstico de ataques en Sistemas Ciberfísicos.	20
Tabla2.6	Estrategias de control tolerante a ataques en Sistemas Ciberfísicos.	22
Tabla4.1	Parámetros del sistema.	72
Tabla4.2	Parámetros del sistema glucosa-insulina.	80
Tabla4.3	Parámetros físicos del vehículo RC y configuración para el modelo discreto. . .	87
Tabla5.1	Tablas de residuos para diferentes tipos de ataques.	100
Tabla5.2	Residuos (ataques DoS, DDA, RDI). Valor 1 indica activación/alarma signifi- cativa; 0 , inactiva.	109
Tabla9.1	Componentes del vehículo RC utilizado en GIPSA-Lab.	157
Tabla11.1	Resumen de métricas por escenario ($T_d = 0.1$ s).	180
Tabla11.2	Indicadores de detección y energía por escenario.	180

Nomenclaturas

Conjuntos y normas

$\mathbb{R}$	Conjunto de todos los números reales.
$\mathbb{R}^n$	Conjunto de matrices reales de n dimensiones.
$\mathbb{R}^{n \times m}$	Conjunto de matrices reales de dimensión $n \times m$.
$ a $	El valor absoluto del escalar a .
$\ a\ _1$	La norma -1 de la señal a .

Notación relativa a vectores y matrices

$A > 0$	Matriz definida positiva.
$A < 0$	Matriz definida negativa.
I	Matriz identidad de dimensiones apropiadas.
0	Matriz con elementos cero de dimensiones apropiadas.
I_n	Matriz identidad de dimensión $n \times n$.
A^{-1}	Inversa de una matriz $A \in \mathbb{R}^{n \times n}$, $\det(A) \neq 0$.
A^T	Transpuesta de una matriz A .
$A^\perp$	Ortogonal de la matriz A .
A^+	Cualquier inversa generalizada de la matriz A , que verifica $AA^+A = A$.
$\text{eig}(A)$	Conjunto de todos los valores propios de la matriz A .
$\det(A)$	Determinante de la matriz $A \in \mathbb{R}^{n \times n}$.
$\text{rank}(A)$	Rango de la matriz $A \in \mathbb{R}^{n \times m}$.
$(*)$	Elementos transpuestos en posición simétrica.
$\text{diag}(A)$	Diagonal principal de la matriz A .
$\text{ones}_{n,m}$	Matriz con unos de dimensión $n \times m$.
$\text{zeros}_{n,m}$	Matriz con ceros de dimensión $n \times m$.

Variables

 $x(t), x(k)$ $u(t), u(k)$ $y(t), y(k)$ $z(t), z(k)$ $\rho(t), \rho(k)$ $\eta_i^j(t), \eta_i^j(k)$ $\mu_i(t), \mu_i(k)$

Variables

 $\zeta(k)$ $v(k)$ $\hat{z}(k)$ $\varepsilon(k)$ $\varphi(k) = \begin{bmatrix} \varepsilon(k) \\ v(k) \end{bmatrix}$ $e_z(k)$ $r_e(k)$ $y_e(k)$ $\beta(k) = \begin{bmatrix} x(t) \\ y_e(k) \end{bmatrix}$

Descripción

Vector de variables de estado continuo (discreto).

Vector de variables de entrada continuo (discreto).

Vector de variables de salida continuo (discreto).

Vector de funciones lineales continuas (discretas).

Vector de variables premisa continuo (discreto).

Función de ponderación con $i = 1$ para límite superior. $i = 0$ para límite inferior, $j = 1, \dots, p$ donde p es el número de variable premisa.Función de pertenencia, $i = 1, \dots, \kappa$ donde κ es el número de Modelos lineales locales.

Descripción

Vector de estado del observador discreto.

Vector auxiliar del observador discreto.

Vector de funciones estimadas discretas.

Vector de error de estimación transformado.

Vector aumentado de las dinámicas del error de estimación.

Vector de error de estimación de la función $z(k)$.Vector integral del vector de referencia $r(k)$.Vector integral del vector de salida $y(k)$.

Vector aumentado para el diseño del controlador.

Acrónimos

LMI

Desigualdad Matricial Lineal.

PI

Proporcional-Integral.

PID

Proporcional-Integral-Derivativo.

T-S

Takagi-Sugeno.

ZoH

Retención de Orden Cero.

GDO

Observador Dinámico Generalizado.

LPV

Parámetros Lineales Variantes.

DoS

Ataque de Denegación de Servicio.

RDI

Inyección Aleatoria de Datos.

DDA

Ataque de Suplantación de Datos.

PO

Observador Proporcional.

PIO

Observador Proporcional-Integral.

Capítulo 1

Introducción

En la última década, el desarrollo de los Sistemas Ciberfísicos (CPS, por sus siglas en inglés *Cyber-Physical Systems*) ha experimentado un crecimiento significativo, consolidándose como un pilar esencial en la evolución de la industria moderna. Estos sistemas integran componentes físicos y computacionales de manera estrecha, y su aplicación se extiende a sectores clave como refinerías de petróleo, plantas químicas, generación de energía, redes eléctricas inteligentes (*Smart Grids*), agricultura automatizada, vehículos autónomos y sistemas de monitoreo médico.

Si bien la conectividad y la integración que ofrecen los CPS representan ventajas notables, también introducen riesgos importantes. Las fallas en estos sistemas pueden generar consecuencias graves, tales como pérdidas humanas, daños económicos o ambientales, e interrupciones críticas en servicios esenciales.

Los CPS están conformados por dos capas fundamentales: la capa física y la capa cibernética. La primera está compuesta por una red inteligente de sensores, actuadores y el sistema físico (eléctrico, mecánico, robótico, etc.), encargado de interactuar directamente con el entorno. La segunda incluye la infraestructura de comunicación y la lógica de control o decisión, donde se procesan los datos y se generan las señales de control. Esta interacción bidireccional entre ambas capas amplía los posibles vectores de ataque, lo que hace imperativo reforzar la seguridad cibernética para garantizar la integridad y confiabilidad del sistema frente a amenazas tanto internas como externas.

Frente a esta necesidad, se han desarrollado dos enfoques principales para la protección de los

CPS. El primero, originado en el ámbito de las Tecnologías de la Información (TI), se enfoca en la protección de datos e información. Sin embargo, este enfoque presenta limitaciones al depender de redes públicas de comunicación y de la heterogeneidad de los componentes, lo que incrementa la exposición a ataques cibernéticos, físicos y ciberfísicos. El segundo enfoque, procedente del área del control automático, busca superar dichas limitaciones mediante herramientas orientadas a la detección, control tolerante a fallas y ataques, protegiendo así los elementos críticos del sistema, como el controlador, la infraestructura de comunicación y los componentes físicos.

En este contexto, un ciberataque se define como la intervención maliciosa de un agente externo que altera de forma negativa el comportamiento del sistema. Entre los ataques más relevantes se encuentran los de Denegación de Servicio (DoS, *Denial of Service*), Repetición (RA, *Replay Attacks*), Dinámica Cero (ZDA, *Zero Dynamics Attacks*) e Inyección de Datos Falsos (FDI, *False Data Injection*). Aunque existe literatura dedicada a la detección y aislamiento de estos ataques, todavía persiste una necesidad crítica de avanzar en su tratamiento desde la perspectiva del control automático.

Para afrontar estos desafíos, los conceptos de robustez, adaptabilidad y resiliencia se han establecido como principios fundamentales en el diseño de estrategias de control para CPS. Estos enfoques, aunque distintos en origen, son altamente complementarios: la robustez alude a la capacidad del sistema para mantener su funcionamiento ante perturbaciones externas; la adaptabilidad, a su habilidad para ajustarse a variaciones del entorno operativo; y la resiliencia, a su facultad para recuperarse ante eventos adversos y restablecer su operación normal, asegurando así su confiabilidad frente a múltiples amenazas.

En este marco, el presente trabajo propone el diseño de un esquema de control resiliente y tolerante a ataques, basado en observadores, para CPS expuestos a diversas amenazas, tales como DoS, Ataques de Suplantación de Datos (DDA, *Data Deception Attacks*) e Inyección Aleatoria de Datos (RDI, *Random Data Injection*). Estos ataques se modelan a través de señales de activación con lógica Markoviana. El objetivo de este enfoque es garantizar la operación segura y eficiente de los CPS incluso bajo condiciones hostiles, contribuyendo al avance robusto y seguro de la Industria.

1.1. Planteamiento del problema

La integración de los sistemas de control con las tecnologías de la información y las telecomunicaciones ha dado lugar al surgimiento de los Sistemas Ciberfísicos, los cuales enfrentan amenazas tanto a la seguridad de su infraestructura como a la integridad de sus datos. Debido a su naturaleza interconectada, estos sistemas son especialmente vulnerables a acciones maliciosas por parte de agentes externos que aprovechan los canales de comunicación, lo que puede derivar en incidentes graves con consecuencias físicas para el sistema y su entorno.

La evolución industrial ha impulsado la convergencia entre los estándares de la ingeniería informática, la ciencia de la información y el control automático. Esta convergencia exige la modernización tanto del software como del hardware en los sistemas de control. Al mismo tiempo, los avances tecnológicos han reducido la barrera de acceso para los atacantes, facilitando la ejecución de ataques cada vez más sofisticados. Como resultado, se han documentado múltiples incidentes que evidencian el daño que los ciberataques pueden causar sobre los sistemas de control de los CPS.

Frente a esta problemática, se vuelve indispensable diseñar esquemas de control resilientes y tolerantes a ataques, capaces de mantener un nivel aceptable de operatividad, incluso ante amenazas provenientes tanto del dominio físico como del cibernético. La resiliencia se presenta como un componente clave en la transición hacia los CPS, ya que abarca la capacidad del sistema para defenderse y recuperarse de ataques, garantizando así una operación confiable bajo condiciones adversas.

La estrategia propuesta consiste en desarrollar un esquema de control que no solo permita detectar, estimar y aislar distintos tipos de ataques, sino que además asegure el control del sistema con un rendimiento aceptable. Para ello, se plantea el diseño de observadores capaces de identificar señales asociadas a los ataques y habilitar la implementación de acciones de control en tiempo real. La implementación efectiva de estos esquemas puede mejorar de forma significativa la seguridad y la confiabilidad de los sistemas ciberfísicos.

1.2. Objetivos

1.2.1. Objetivo general

Diseñar un esquema de control tolerante a ataques para un sistema ciberfísico susceptible a diversos escenarios de ataque, utilizando técnicas basadas en observadores.

1.2.2. Objetivos específicos

- Establecer diversos escenarios de ataque que comprometan el funcionamiento adecuado del sistema ciberfísico seleccionado.
- Diseñar un observador capaz de detectar ataques maliciosos que afecten la funcionalidad del sistema.
- Desarrollar un esquema de diagnóstico de ataques dirigido a sistemas ciberfísicos, que permita identificar, aislar y localizar intrusiones maliciosas en sensores y actuadores mediante el análisis de residuos generados por observadores.
- Diseñar un controlador resiliente y tolerante a ataques y cumpla con los requerimientos del sistema, garantizando un rendimiento bajo los escenarios de ataque considerados.
- Evaluar los límites de resiliencia del controlador propuesto, con base en los límites de desempeño del sistema ciberfísico analizado.

1.3. Metas

- Obtención de la simulación en lazo abierto del comportamiento del caso de estudio.
- Evaluación de diferentes esquemas de ataque dirigidos al sistema ciberfísico del caso de estudio, junto con su clasificación.
- Estimación de las variables de estado y de la información relacionada con los ataques.
- Control de la variable del sistema ciberfísico alrededor de un punto de operación deseado, incluso en presencia de ataques.
- Determinación de los indicadores de resiliencia del control basado en observadores bajo distintos escenarios de ataque.

1.4. Justificación

Mientras que los ciberataques en sistemas informáticos convencionales se centran principalmente en el robo o manipulación de datos, los ataques dirigidos a sistemas de control tienen como objetivo modificar el funcionamiento de los procesos físicos, impactando directamente en el mundo real. Los métodos y herramientas tradicionales provenientes del campo de las tecnologías de la información pueden resultar insuficientes para prevenir completamente intrusiones o fallo en los sistemas de control, lo cual puede derivar en un funcionamiento inadecuado del sistema ciberfísico.

Adicionalmente, la investigación en esquemas de control resilientes para sistemas ciberfísicos aún es limitada. Diversos estudios señalan que muchos de los enfoques actuales no cumplen completamente con los requisitos necesarios para que un sistema pueda considerarse resiliente. Esto resalta la importancia de desarrollar y validar estrategias de control que garanticen la operación segura y confiable de los CPS, incluso ante ataques deliberados o condiciones adversas.

1.5. Hipótesis

La implementación de esquemas de control tolerantes a ataques permitirá garantizar la resiliencia operativa de los sistemas ciberfísicos frente a diversos escenarios de ataque. Se espera que dicha resiliencia no solo asegure la continuidad y seguridad de las operaciones, sino que también mejore la eficiencia y confiabilidad del sistema, contribuyendo significativamente al cumplimiento de sus objetivos operativos.

1.6. Metodología

Para alcanzar los objetivos planteados en este trabajo de tesis, se llevarán a cabo las siguientes actividades:

1. Investigar los antecedentes y estudios previos sobre esquemas de ataque en sistemas ciberfísicos.
2. Analizar e identificar las características de los sistemas ciberfísicos desde la perspectiva de la teoría de control.

3. Seleccionar y modelar un caso de estudio adecuado para el desarrollo del controlador tolerante a ataques.
4. Validar el modelo matemático del sistema ciberfísico bajo condiciones nominales de operación.
5. Obtener la representación Takagi-Sugeno del sistema ciberfísico seleccionado.
6. Estudiar y clasificar los posibles esquemas de ataque aplicables al sistema.
7. Diseñar y modelar el esquema de ataque seleccionado.
8. Validar el modelo de ataque mediante simulaciones.
9. Simular la interacción entre el modelo ciberfísico y el esquema de ataque considerado.
10. Diseñar un observador que proporcione información sobre el vector de estado del sistema.
11. Desarrollar un esquema de diagnóstico capaz de estimar, detectar, aislar y localizar ataques.
12. Proponer límites de resiliencia para el controlador tolerante a ataques.
13. Diseñar un controlador tolerante a ataques basado en observadores, alineado con los objetivos operativos del sistema.
14. Validar el desempeño del controlador utilizando observadores resilientes.
15. Evaluar y validar la capacidad de detección y respuesta del sistema frente a los esquemas de ataque aplicados.

1.7. Alcance

El desarrollo de esta tesis se centra en el diseño de un esquema de control tolerante a ataques para sistemas ciberfísicos discretos, considerando diferentes escenarios de ciberataques con una distribución estocástica Markoviana. Para ello, se establecerá un marco de diagnóstico basado en observadores que permita la detección, estimación, aislamiento y localización de ataques que comprometan la integridad del sistema.

El esquema de control diseñado garantizará la resiliencia operativa del sistema incluso en presencia de ataques, asegurando un rendimiento aceptable en tiempo real. Además, se definirán métricas de resiliencia que permitan evaluar los límites de tolerancia del controlador frente a distintos escenarios de ataque.

La validación del esquema propuesto se llevará a cabo mediante simulaciones numéricas aplicadas a un caso de estudio representado en forma Takagi-Sugeno, evaluando su desempeño en la mitigación de ciberataques y su capacidad para mantener al sistema dentro de los parámetros operativos deseados.

1.8. Contribuciones

Las principales contribuciones de esta tesis son las siguientes:

- Clasificación de los diferentes esquemas de ataque reportados en la literatura que afectan la integridad de los sistemas ciberfísicos, desde la perspectiva del control automático.
- Desarrollo de un esquema de diagnóstico que permite la detección, estimación, aislamiento y localización de ataques, mediante el uso de observadores diseñados para contrarrestar diversos esquemas de ataque con distribución markoviana en sistemas ciberfísicos.
- Diseño de un esquema de control resiliente y tolerante a múltiples esquemas de ataque estocásticos.
- Establecimiento y aplicación de métricas de resiliencia en controladores tolerantes a ataques.

1.9. Originalidad

Esta investigación presenta una contribución teórica al campo del control automático, así como su verificación en un sistema físico: un vehículo sobre la plataforma del GIPSA-Lab, equipado con un sistema de adquisición de datos basado en ROS2¹ y VICON². El estudio se enfoca en el diseño de un esquema de control tolerante a ataques para sistemas ciberfísicos discretos bajo la

¹**ROS2 (Robot Operating System 2)** es un marco de software de código abierto ampliamente utilizado en robótica, que permite la comunicación distribuida entre nodos, sensores y controladores.

²**VICON** es un sistema de captura de movimiento óptico de alta precisión que utiliza cámaras infrarrojas y marcadores reflectantes para obtener la posición y orientación tridimensional de objetos en tiempo real.

representación Takagi-Sugeno. El esquema propuesto integra un observador dinámico generalizado para la estimación de ataques con distribución estocástica Markoviana, permitiendo su detección, aislamiento y localización dentro del sistema.

El desarrollo del esquema de control se basa en la combinación de técnicas de diagnóstico mediante observadores y estrategias de control resiliente, lo que permite no solo mitigar los efectos de los ataques, sino también garantizar la estabilidad del sistema ante múltiples escenarios adversos. La originalidad de este enfoque radica en la implementación de métricas de resiliencia para evaluar el desempeño del controlador frente a situaciones de ciberataque, estableciendo límites de tolerancia y condiciones seguras de operación.

El esquema de control ha sido diseñado de forma generalizada, lo que permite su aplicación a diversos sistemas ciberfísicos discretos que puedan representarse mediante el marco Takagi-Sugeno. Específicamente, en esta tesis, la metodología se valida a través de dos estudios de caso: la implementación en un sistema físico representado por un vehículo en el GIPSA-Lab, y la simulación de un sistema interconectado de tres tanques. En ambos casos se analiza la respuesta del sistema ante distintos ciberataques, así como la efectividad del esquema propuesto para restaurar la operación nominal del sistema.

1.10. Estructura de la tesis

El presente trabajo de investigación se organiza en **doce** capítulos, que abordan de forma progresiva la detección, estimación y mitigación de ataques en sistemas ciberfísicos discretos. Para ello, se emplean ODG y estrategias de control tolerante a ataques, combinando fundamentos teóricos, simulaciones y validaciones experimentales.

Capítulo 1: Introducción.

Se presenta el contexto del problema, la motivación y relevancia de la ciberseguridad en CPS; se formulan los objetivos, la metodología, el alcance, las contribuciones e hipótesis, y se describe la organización del documento.

Capítulo 2: Estudio del Estado del Arte.

Se realiza una revisión sistemática de la literatura sobre CPS, tipos de ataques, diagnóstico mediante observadores y control tolerante a ataques, identificando vacíos y oportunidades que enmarcan las contribuciones de esta tesis.

Capítulo 3: Marco teórico.

Se introducen los conceptos base: CPS, diferencias entre ataques y fallas, ataques con lógica Markoviana, representaciones Takagi–Sugeno (T–S) y LPV, teoría de observadores (proporcional, PI, Luenberger y ODG), estabilidad con funciones de Lyapunov y LMIs, y nociones de control tolerante y métricas de resiliencia.

Capítulo 4: Modelado de casos prácticos.

Se desarrollan las representaciones T–S para los *tres tanques* y el *glucosa–insulina*, y la representación LPV del *vehículo RC*; se comparan modelos no lineales y sus aproximaciones (T–S/LPV) y se reportan simulaciones de validación.

Capítulo 5: Observadores para la Detección de Ataques.

Se diseña un banco de observadores (incluyendo Luenberger y OGR) para generar residuos sensibles a ataques DoS, DDA y RDI en sensores/actuadores, y se analizan condiciones de estabilidad por LMIs con resultados de simulación.

Capítulo 6: Observador ODG para Aislamiento, Detección y Localización.

Se propone y analiza un ODG basado en T–S para discriminar tipos de ataque y localizar su origen; se establecen condiciones de estabilidad y se valida mediante escenarios con lógicas Markovianas uniformes y no uniformes.

Capítulo 7: Observador ODG para la Estimación de Ataques de Variación Lenta.

Se formula un ODG orientado a ataques de variación suave, con parametrización y análisis de estabilidad en tiempo discreto; se presentan simulaciones bajo lógicas de activación uniforme y no uniforme.

Capítulo 8: ODG para Estimación de Ataques Dinámicos.

Se extiende el ODG a ataques dinámicos (rápidos y coordinados); se plantea el problema de estabilidad, un índice de desempeño $\mathcal{L}_2$ y la formulación en LMIs, con validación en escenarios DDA, DoS y RDI.

Capítulo 9: Instrumentación en la Plataforma del GIPSA-Lab.

Se describe la plataforma experimental (ROS2, Vicon, vehículo RC), la interfaz de conexión y el flujo de datos, así como el procedimiento de pruebas y validación para integrar los esquemas propuestos.

Capítulo 10: Control Tolerante a Ataques.

Se diseña una ley de control tolerante soportada por ODG; se analiza la estabilidad mediante LMIs y se reportan simulaciones comparativas (sin ataques, ataques suaves y ataques dinámicos) con discusión de resultados.

Capítulo 11: Evaluación de Métricas de Resiliencia del Controlador.

Se definen y aplican métricas de resiliencia para cuantificar desempeño, robustez y continuidad operativa del controlador bajo distintos esquemas de ataque, estableciendo límites de tolerancia.

Capítulo 12: Conclusiones y Trabajo Futuro.

Se sintetizan los hallazgos y contribuciones principales, y se proponen líneas de investigación futura orientadas a profundizar en observadores y control resiliente para CPS expuestos a ataques cada vez más complejos.

Capítulo 2

Estudio del estado del arte

El propósito de esta sección es presentar y analizar la información relevante relacionada con los principales temas abordados en esta tesis. Esta revisión sistemática tiene como objetivo identificar áreas de oportunidad, comprender los enfoques desarrollados por otras disciplinas y destacar los avances alcanzados desde la perspectiva del control automático.

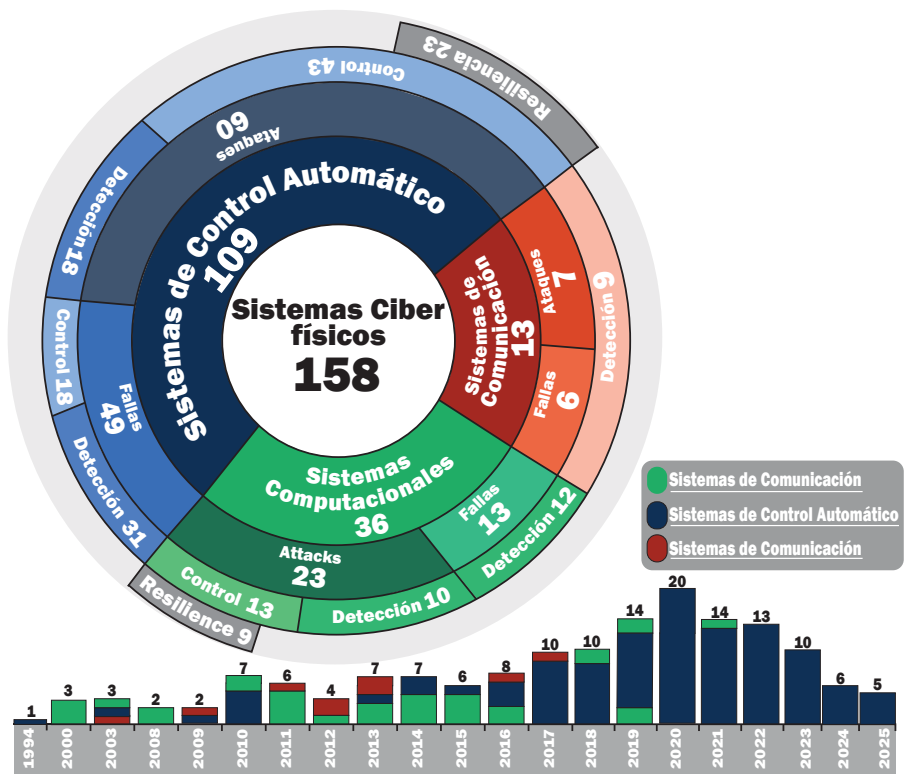


Fig. 2.1. Resumen del estado del Arte.

En la Figura 2.1 se muestra un resumen gráfico y una clasificación temática de los artículos consultados para este capítulo. Dicha figura organiza los trabajos en función de su contribución al estudio de los sistemas ciberfísicos, las técnicas de detección y mitigación de ataques, así como una calificación que depende del área de conocimiento de la ingeniería, computación, control automático y telecomunicaciones. Además, se incluye un histograma que evidencia el incremento del interés en esta área en los últimos años, particularmente desde el enfoque del control automático, lo cual resalta la relevancia y actualidad del presente trabajo.

2.1. Proceso de revisión y selección de literatura

Con el objetivo de obtener una visión amplia y actualizada sobre los avances en CPS y su relación con la detección de ataques, diseño de observadores y controladores tolerantes, se realizó una búsqueda sistemática en bases de datos científicas de alto impacto, incluyendo **IEEE Xplore**, **Elsevier**, **Wiley Online Library** y **SpringerLink**.

En total, se identificaron **280 artículos científicos** publicados entre los años **2000 y 2025**. Los resultados iniciales incluyeron artículos de revisión, estudios experimentales, investigaciones teóricas y desarrollos metodológicos relacionados con control, detección de fallas, ciberseguridad y resiliencia. Sin embargo, para asegurar la relevancia con los objetivos de esta investigación, se aplicó un proceso de cribado basado en criterios de inclusión y exclusión, representado conceptualmente en la Figura 2.2.

Criterios de inclusión

Se incluyeron aquellos trabajos que cumplieron con las siguientes características:

- Estudios que abordan explícitamente **sistemas ciberfísicos** o **sistemas de control automático** con interacción entre componentes físicos y cibernéticos.
- Artículos que proponen o analizan **observadores**, **métodos de detección de ataques** o **controladores tolerantes a fallas y ataques**.
- Investigaciones publicadas en revistas indexadas o conferencias arbitradas, principalmente en IEEE, Elsevier, Wiley y Springer.

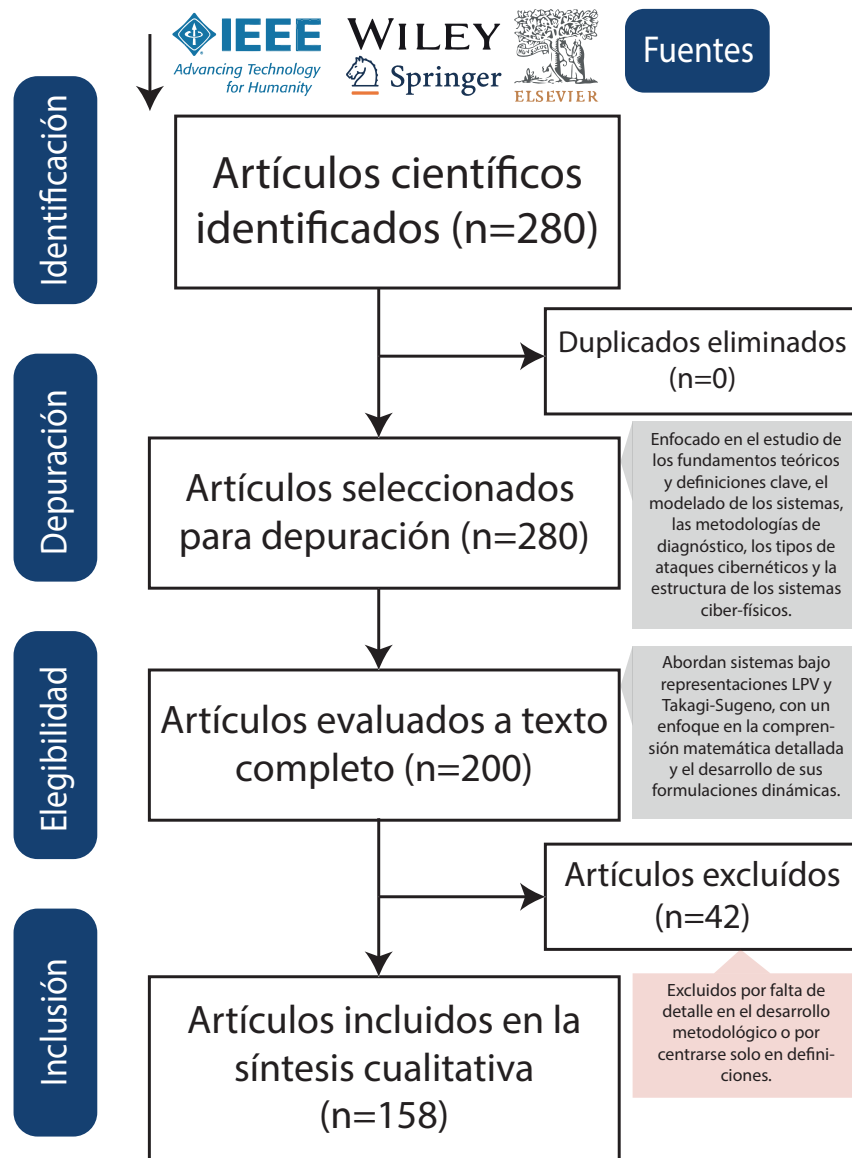


Fig. 2.2. Revisión y selección del estado del arte.

- Publicaciones comprendidas entre los años 2000 y 2005, que reportan resultados experimentales o simulaciones validadas.

Criterios de exclusión

Se descartaron los artículos que presentaban alguna de las siguientes condiciones:

- Estudios centrados únicamente en **seguridad informática**, **protocolos de red** o **teoría**

de la información, sin integración con el control automático.

- Trabajos relacionados con **diagnóstico clásico de fallas**, sin contexto de ciberseguridad ni resiliencia.
- Documentos repetidos, duplicados o con información redundante entre distintas bases de datos.
- Publicaciones no accesibles en texto completo, resúmenes extensos, notas técnicas o revisiones sin validación experimental.

Selección final y análisis cuantitativo

Tras la aplicación de los criterios mencionados, se seleccionaron un total de **158 artículos relevantes** que constituyen la base del presente estado del arte. La distribución por fuente se resume en la Tabla 2.1.

Tabla 2.1. Distribución de artículos seleccionados por base de datos.

Base de datos	Artículos seleccionados	Porcentaje (%)
IEEE Xplore	82	51.9
Elsevier (ScienceDirect)	46	29.1
Wiley Online Library	19	12.0
Springer / MDPI / Otros	11	7.0
Total	158	100

El proceso de discriminación permitió reducir los resultados iniciales de 280 artículos a 158 de alta relevancia, los cuales fueron organizados en tres dominios principales:

1. **Sistemas de Control Automático (109 artículos):** incluyen estrategias de observadores, controladores proporcionales-integrales (PI), controladores tolerantes y técnicas de diagnóstico basadas en LMIs y complemento de Schur.
2. **Sistemas Computacionales (36 artículos):** abordan el modelado, simulación y detección de ataques en redes, así como la integración con plataformas de procesamiento distribuido.
3. **Sistemas de Comunicación (13 artículos):** tratan sobre los efectos de ataques en canales de comunicación, pérdida de paquetes, retardo y seguridad en protocolos de transmisión.

2.2. Casos de estudio utilizados

En relación con los sistemas utilizados como casos de estudio, se realizó una revisión exhaustiva de diversos artículos que abordan enfoques variados. Es importante destacar que los sistemas ciberfísicos considerados cuentan con una representación discreta. Esta particularidad es crucial, ya que permite la transmisión y recepción digital de información entre sensores y actuadores a través de una red interconectada. La discretización del comportamiento del sistema garantiza la sincronización y la integridad de los datos en un entorno ciberfísico.

Uno de los primeros estudios de caso considerados fue descrito en los trabajos de [Flores Martínez y Osorio Gordillo (2019); Chee *y col.* (2005)]. En estos artículos se emplea el modelo mínimo de Bergman para un sistema glucosa-insulina, específicamente adaptado para representar a pacientes con diabetes mellitus tipo 2. El interés en esta representación surge debido al alarmante incremento de ciberataques dirigidos a sistemas médicos cibernéticos, los cuales han aumentado en un 300 % desde 2015 The Lancet (2024). Esta tendencia resalta la necesidad de desarrollar y aplicar esquemas de control resilientes y seguros que protejan la integridad y funcionalidad de estos sistemas críticos en el ámbito de la salud.

En el estudio realizado por [Li *y col.* (2018); Tahir *y col.* (2019)], se analiza el caso de un sistema de triple tanque interconectado con dos bombas. El problema de la detección de ataques en sistemas ciber-físicos se aborda utilizando un filtro de partículas. En este trabajo se estudian tres tipos de ataques: ataque de denegación de servicio, ataque aleatorio y ataque por inyección de datos falsos, todos ellos aplicados al sistema de tres tanques.

Como último caso de estudio, detallado en [Atoui *y col.* (2022)], se presenta la representación LPV de un vehículo autónomo a escala, el cual puede ser simulado y desplegado en un entorno físico utilizando la plataforma VICON del laboratorio de investigación GIPSA-Lab. En este caso, se comparan un controlador H-infinito y un controlador PI para evaluar su desempeño y efectividad en tiempo real. Esta comparación permite observar diferencias en la respuesta del sistema y en la robustez de cada controlador, proporcionando una visión clara sobre cuál resulta más adecuada para su implementación en vehículos autónomos bajo diversas condiciones operativas.

A continuación en la Tabla 2.2, se presenta una selección de artículos y libros relevantes que abordan diversos casos de estudio aplicados en el contexto de esta investigación. Estos trabajos han sido incluidos con el objetivo de ofrecer un panorama más amplio sobre las metodologías, herramientas y enfoques utilizados por otros autores para analizar y validar esquemas relacionados con la temática central de esta tesis. La revisión de estos estudios contribuye a fundamentar y fortalecer el marco teórico, así como a identificar tendencias, desafíos y oportunidades dentro del área de estudio.

Tabla 2.2. Resumen de artículos clave sobre casos de estudio.

Año	Autores	Título	Información Importante
2022	Roland Tóth	Modeling and identification of linear parameter-varying systems.	Libro que abarca la teoría y bases de los sistemas LPV.
2013	Sename Olivier, Tudon-MMartínezJuan-Carlos, Fergani Soheib	LPV methods for fault-tolerant vehicle dynamic control.	Control tolerante a para sistema de suspensión semi-activa en vehículos.
2000	Johansson K.H.	The quadruple-tank process: a multivariable laboratory process with an adjustable zero.	Sistema de 4 tanques interconectados para estudio de control multivariable (modelo físico detallado).
2015	Colombo A.W. et al.	Industrial cyberphysical systems: A backbone of the fourth industrial revolution.	Aplicación de CPS en vehículos RC y sistemas de manufactura.

2.3. Sistemas ciberfísicos

En lo que respecta a los artículos que investigan los sistemas ciber-físicos, estos proporcionan detalles completos sobre las definiciones y características que deben cumplir los sistemas para ser clasificados como tales. Se ha revisado un conjunto de estos artículos con el objetivo de enriquecer, respaldar y refinar las definiciones previamente establecidas. A continuación, se presentan los artículos más relevantes, destacando aspectos clave que contribuyen a una comprensión más profunda de los sistemas ciber-físicos y que fortalecen los fundamentos de este campo de estudio.

El primer artículo que establece las bases del concepto de sistema ciber-físico es [Baheti y Gill (2011)], desempeñando un papel fundamental en [Shames *y col.* (2011); Amin *y col.* (2010); Rajkumar *y col.* (2010)]. Este trabajo ofrece un análisis integral de los antecedentes y definiciones proporcionadas por diversas ramas de la ingeniería respecto al término “sistema ciber-físico”. El énfasis radica en la integración de conocimientos y principios provenientes de distintas disciplinas de las ciencias computacionales y de la ingeniería, tales como redes, control, software y cómputo. El objetivo es desarrollar una nueva ciencia que permita controlar sistemas desde una perspectiva cibernética.

El libro de [Hu (2014)] recopila definiciones, implementaciones e investigaciones previas, ofreciendo descripciones y características más detalladas que las presentadas en [Baheti y Gill (2011); Mohsenian-Rad y Leon-garcia (2011)]. Esta obra consolida conceptos clave, profundiza en el modelado, refuerza diversas áreas de aplicación, detalla los desafíos inherentes al diseño de sistemas y control, y concluye con un análisis exhaustivo de los sistemas de seguridad propuestos para los sistemas ciberfísicos.

A continuación en la Tabla 2.3 se muestran diversos artículos que exploran los fundamentos teóricos y conceptuales de los sistemas ciber-físicos. Estos trabajos ofrecen una base sólida para comprender la integración entre los componentes físicos y computacionales, así como las implicaciones del diseño, modelado, análisis y control de este tipo de sistemas.

2.4. Ataques en sistemas ciberfísicos

Se han revisado diversos artículos que abordan esquemas de ataque reportados en la literatura y que han sido representados matemáticamente desde la ingeniería de control con el fin de influir en el comportamiento de estos sistemas. La seguridad en los sistemas ciberfísicos es fundamental debido al creciente nivel de interconexión entre componentes computacionales y físicos, lo cual implica potenciales consecuencias severas, como pérdidas humanas o daños materiales. A continuación, se presenta un análisis detallado de los artículos revisados, cuyo objetivo es identificar la variedad de ataques a los que están expuestos los CPS y comprender el efecto de cada uno de ellos [Tahir *y col.* (2019)].

Tabla 2.3. Artículos fundamentales sobre teoría de Sistemas Ciberfísicos.

Año	Autores	Título	Información Importante
2010	Rajkumar R. et al.	Cyber-physical systems: The next computing revolution	Define CPS como integración de componentes físicos y computacionales. Establece su impacto en infraestructuras críticas.
2011	Baheti R., Gill H.	Cyber-physical Systems	Presenta principios de diseño CPS y su evolución desde sistemas embebidos.
2017	Humayed A. et al.	Cyber-Physical Systems Security - A Survey	Clasifica vulnerabilidades, ataques y defensas en CPS con marco unificado.
2014	Lee J. et al.	A Cyber-Physical Systems architecture for Industry 4.0	Propone arquitectura de 5 capas para CPS en manufactura, con énfasis en interoperabilidad.

En [Baniamerian *y col.* (2020)] se aborda la supervisión y detección de ataques cibernéticos de tipo zero-dynamics introducidos por adversarios maliciosos en sistemas ciberfísicos. Se considera un sistema CPS cuya parte física se representa mediante un proceso dinámico lineal invariante en el tiempo. A través de una metodología basada en un sistema auxiliar y filtros de detección, es posible identificar eficazmente este tipo de ataques, caracterizados por su capacidad de mantener la salida del sistema sin cambios mientras alteran su estado interno.

En [Li *y col.* (2018)], se analiza la detección de ataques en CPS utilizando filtros de partículas. Se enfocan tres tipos de ataques: denegación de servicio, ataque aleatorio y ataque por inyección de datos falsos, todos aplicados a un sistema de tres tanques. En primer lugar, se presentan los modelos del sistema y de los ataques. Posteriormente, se emplea un filtro de partículas para estimar el estado del sistema bajo ataque. Con base en esta estimación, se diseña un residuo utilizando una técnica de ventana temporal deslizante para detectar la presencia de ataques. Finalmente, se valida la efectividad del método mediante simulaciones.

A continuación Tabla 2.4, se incluyen diversos artículos que abordan la clasificación, caracteri-

zación y análisis de los diferentes tipos de ataques dirigidos a sistemas ciber-físicos. Además, se destacan las motivaciones, mecanismos y consecuencias asociadas a dichos ataques, así como las condiciones que los facilitan.

Tabla 2.4. Clasificación de ataques en Sistemas Ciberfísicos.

Año	Autores	Concepto/Clasificación	Descripción
2011	Pasqualetti F. et al.	Ataques detectables vs. indetectables	Formaliza ataques basados en su detectabilidad usando teoría de sistemas.
2013	Yuan Y. et al.	Ataques DoS en CPS	Modela impacto de Denegación de Servicio en canales de comunicación CPS.
2017	Pasqualetti F. et al.	Ataques de integridad (engaño)	Clasifica ataques que corrompen datos de sensores/actuadores sin ser detectados.
2020	Baniamerian A. et al.	Ataques de dinámica cero	Ataques de dinámica cero contra sistemas CPS que evaden la detección.

2.5. Esquemas de diagnóstico de ataques

Previo al desarrollo del controlador, es esencial realizar un análisis de las técnicas de diagnóstico aplicables a los distintos esquemas de ataque, lo que incluye su estimación, detección, localización e identificación. Para ello, se ha revisado una variedad de artículos relevantes, destacando los siguientes por su aporte significativo.

Desde el enfoque de diagnóstico de fallas, en [Arámbula y col. (2023)] se presenta una estrategia basada en modelos para el diagnóstico de sensores, enfocada en la caja de engranajes de una turbina eólica. Se emplea el enfoque Takagi-Sugeno para representar el modelo no lineal de la caja de engranajes, capturando sus propiedades mediante modelos lineales. El esquema propone un observador generador de residuos, diseñado para mitigar el impacto de fallas en los estados estimados y amplificar su efecto en los residuos. Para garantizar la estabilidad del observador, se utiliza el método directo de Lyapunov, formulando condiciones en forma de desigualdades matri-

ciales lineales (LMI).

En el artículo de [Nateghi *y col.* (2023)], se aborda la estimación de estados y la reconstrucción de ataques en CPS. Se desarrolla un controlador resiliente frente a ataques que manipulan mediciones de sensores y comandos de actuadores. Se introduce un observador adaptativo que estima en tiempo real los estados y ataques en los actuadores, junto con un algoritmo de recuperación dispersa para enfrentar ataques sigilosos en sensores. Los ataques estimados se utilizan como base para compensarlos mediante un controlador resiliente. La propuesta se valida mediante simulaciones en un sistema eléctrico real sometido a ataques.

Se presentan a continuación en la Tabla 2.5 los artículos que exploran técnicas basadas en observadores para el diagnóstico de ataques en sistemas ciber-físicos. Estas metodologías permiten estimar estados y detectar anomalías mediante la reconstrucción de señales internas, constituyéndose como herramientas clave para la detección temprana de intrusiones y ataques.

Tabla 2.5. Métodos de diagnóstico de ataques en Sistemas Ciberfísicos.

Año	Autores	Técnica de Diagnóstico	Aportación Clave
2013	Pasqualetti F. et al.	Detección basada en invariantes del sistema	Primer marco teórico para detectar ataques usando propiedades estructurales del sistema.
2015	Li Y. et al.	Detección algebraica en dominio de frecuencia	Método para identificar múltiples ataques estocásticos usando transformaciones algebraicas.
2018	Bezzaoucha S. et al.	Banco de observadores residuales	Sistema tolerante a ataques con detección/aislamiento mediante observadores UIO.
2022	Adeli M. et al.	Observador de modo deslizante optimizado	Detección de ataques en redes eléctricas usando algoritmos evolutivos para ajuste de parámetros.

2.6. Control tolerante a los ataques

En [Bezzaoucha Rebaï *y col.* (2018)] se propone un esquema tolerante a fallas/ataques basado en modelos, diseñado para abordar amenazas cibernéticas en CPS. Se implementa un esquema común basado en observadores y un control por realimentación de estados dentro de un marco de eventos disparados. Este esquema incluye tanto la síntesis del control como una condición específica de conmutación en el tiempo. Se recurre a enfoques clásicos de control tolerante a fallas mediante desigualdades matriciales bilineales (BMI) para lograr una estrategia de seguridad novedosa, implementada a través de control por eventos. El propósito de esta implementación basada en eventos es reducir la cantidad total de transmisiones, activándolas únicamente cuando el sistema de control en red (NCS) requiere intervención.

En [Zhang *y col.* (2022)] se presenta un esquema de control compensatorio frente a ataques de denegación de servicio en CPS no lineales. El proceso dinámico del CPS se modela mediante un enfoque Takagi-Sugeno, regulado por reglas difusas. Se considera que el canal de comunicación entre el controlador y el actuador es potencialmente no confiable, permitiendo la invasión aleatoria por parte de un ataque DoS. Para contrarrestar los efectos negativos del ataque, se diseña un esquema de control compensatorio que garantiza la estabilidad del sistema en lazo cerrado.

La resiliencia es un aspecto fundamental en el diseño del esquema de control propuesto en esta tesis. Su adecuada implementación permite al sistema mantener un desempeño aceptable incluso bajo condiciones adversas, como ataques o fallas. A continuación, se destacan algunos artículos clave en esta área.

En el estudio de [Nateghi *y col.* (2023)], previamente mencionado, se examina la estimación segura de estados y la detección de ataques en CPS. El énfasis se encuentra en el diseño de controladores resilientes que puedan contrarrestar intrusiones sobre mediciones de sensores y comandos de actuadores. Un observador adaptativo estima en tiempo real tanto los estados como los ataques en actuadores, mientras que un algoritmo de recuperación dispersa aborda ataques sigilosos a sensores. Los ataques detectados se usan para neutralizar su efecto mediante un controlador resiliente. Su eficacia se valida en un sistema eléctrico real bajo ataques simultáneos.

Por otro lado, en el artículo de [Djouadi *y col.* (2014)] se identifican las deficiencias en las técnicas tradicionales de seguridad informática aplicadas a CPS, subrayando la necesidad urgente de diseñar sistemas de control capaces de resistir diversas formas de ataques de señal. Se resalta la importancia del desarrollo de nuevos métodos de análisis que permitan garantizar la robustez de estos sistemas. Posteriormente, se estudian ataques dirigidos a señales de sensores en sistemas controlados mediante observadores, y se propone un esquema resiliente que complementa la función del observador con estimaciones adicionales que permiten detectar y mitigar los efectos del ataque.

A continuación en la Tabla 2.6 se abordan el diseño y la implementación de esquemas de control tolerante a los ataques, los cuales buscan preservar la estabilidad y el desempeño deseado del sistema ante la presencia de acciones maliciosas. Estos enfoques se centran en detectar, aislar y compensar los efectos de los ataques, ya sea mediante la reconfiguración del controlador, el uso de estimaciones robustas o la incorporación de redundancias. Su estudio es esencial para avanzar hacia sistemas ciberfísicos, seguros y resilientes en contextos críticos.

Tabla 2.6. Estrategias de control tolerante a ataques en Sistemas Ciberfísicos.

Año	Autores	Estrategia	Contribución Principal
2013	Yuan Y. et al.	Control H_∞ resiliente	Diseño acoplado de política de seguridad y control óptimo para DoS attacks usando LMIs
2017	Liu S. et al.	Control por modos deslizantes	Mantiene estabilidad del sistema bajo ataques DoS con compensación adaptativa
2020	Deng C. et al.	Observadores distribuidos resilientes	Tolerancia a en actuadores y ataques DoS en sistemas multiagente
2021	Nateghi S. et al.	Observador adaptativo en modo deslizante	Reconstrucción en tiempo real de ataques a sensores/actuadores con compensación activa

2.7. Conclusiones del capítulo

En este capítulo se presentó una síntesis crítica del estado del arte relativa a los sistemas ciberfísicos, su modelado y los principales esquemas de ataque reportados en la literatura, así como

los métodos de diagnóstico y control tolerante que se han propuesto en los últimos años. A partir de los casos de estudio revisados (sistemas de tanques interconectados, modelo glucosa–insulina y vehículo LPV a escala), se subrayó la relevancia de representaciones *discretas* y de marcos de modelado T–S/LPV para capturar adecuadamente no linealidades, dependencias paramétricas y la operación sobre redes de comunicación.

La clasificación de ataques de denegación de servicio, inyección de datos falsos, inyección aleatoria, y ataques encubiertos de dinámica cero) evidenció que la seguridad en CPS requiere ir más allá de la protección de la información para incorporar estrategias de *resiliencia* en el lazo de control. En este contexto, las técnicas basadas en observadores (bancos dedicados, UIO, observadores en modo deslizante y adaptativos) destacan por su capacidad para: (i) generar residuos informativos, (ii) reconstruir señales de ataque, y (iii) habilitar mecanismos de mitigación activa a través de compensación en la ley de control. De forma complementaria, los enfoques de control tolerante (por ejemplo, H_∞ , modos deslizantes, control por eventos y esquemas compensatorios) han mostrado avances significativos, aunque aún con desarrollo fragmentado y, en ocasiones, con supuestos restrictivos sobre la dinámica del ataque y la infraestructura de red.

De la revisión se identifican las siguientes brechas relevantes:

- **Acoplamiento estocástico–discreto:** integración sistemática de lógicas de ataque estocásticas (p. ej., Markovianas) con modelos T–S/LPV en tiempo discreto, incluyendo conmutaciones y acciones coordinadas sensor/actuador.
- **Reconstrucción de ataques con distintas escalas temporales:** estimación coherente de ataques de variación lenta y/o rápida bajo limitaciones de muestreo y comunicación, manteniendo robustez ante no linealidades.
- **Condiciones unificadas de estabilidad y desempeño:** formulaciones mediante LMI que conecten explícitamente el diagnóstico basado en observadores con la síntesis de control compensatorio resiliente, con cotas de convergencia y márgenes de tolerancia al ataque.
- **Validación con métricas de resiliencia:** evaluación comparativa con métricas explícitas (seguimiento, robustez, uso de red, tiempo de detección/aislamiento, tolerancia máxima al ataque) en escenarios coordinados y realistas.

Estas observaciones respaldan el enfoque de esta tesis: el *diseño de observadores dinámicos generalizados* para la estimación, aislamiento y localización de ataques en CPS discretos representados en el marco T-S/LPV, y su *acoplamiento* con un *control tolerante a ataques* que garantice estabilidad y desempeño mediante condiciones en forma de LMI. En el siguiente capítulo se desarrolla el marco teórico necesario para el modelado, la formulación de observadores y la síntesis del controlador resiliente que abordará las brechas identificadas.

Capítulo 3

Marco teórico

En este capítulo se presentan los conceptos fundamentales que sustentan el desarrollo de esta tesis. Se abordan definiciones clave sobre los sistemas ciberfísicos, sus arquitecturas y los principales tipos de ataques que comprometen su funcionamiento, destacando la importancia de diseñar esquemas de diagnóstico y control resilientes.

Se analizan tres casos de estudio representativos: un vehículo autónomo a escala bajo representación LPV, un sistema de tanques interconectados modelado mediante Takagi-Sugeno, y el sistema glucosa-insulina en su forma Takagi-Sugeno, todos utilizados para validar estrategias de control y detección de ataques.

Asimismo, se introduce la teoría de observadores, esenciales para estimar estados internos y detectar anomalías, junto con el diseño de controladores enfocados en la resiliencia. También se aborda la discretización de sistemas dinámicos, indispensable para la implementación digital, y se presentan métricas utilizadas para evaluar la capacidad de recuperación y estabilidad frente a perturbaciones o intrusiones.

Este marco teórico establece las bases para el análisis y diseño propuestos en los capítulos posteriores.

3.1. Sistemas ciberfísicos

En la literatura, se han propuesto múltiples definiciones para los sistemas ciber-físicos, cada una destacando distintos aspectos de la integración entre los dominios computacional y físico. Por ejemplo, Baheti y Gill (2011) define los CPS como sistemas con capacidades computacionales y físicas integradas, que pueden interactuar con los seres humanos de diversas maneras.

De manera similar, Rajkumar *y col.* (2010) caracteriza a los CPS como una clase de sistemas que incorporan profundamente capacidades cibernéticas en el mundo físico, ya sea a través de la interacción con personas, infraestructuras o plataformas, con el objetivo de transformar la forma en que interactuamos con el entorno físico.

Estas definiciones destacan en conjunto las características esenciales de los CPS: el uso de redes y/o tecnologías de comunicación, la incorporación de comportamientos inteligentes (ya sean adaptativos o predictivos), y la operación en tiempo real para influir en los resultados del mundo físico.

Aunque los CPS comparten similitudes con los sistemas tradicionales de información, como estar interconectados, ser distribuidos y ofrecer cierto grado de automatización, el factor diferenciador clave radica en su capacidad para interactuar con el entorno físico en tiempo real. Esta estrecha integración entre los componentes cibernéticos y físicos es lo que define la esencia de los CPS.

Se espera que los sistemas ciberfísicos revolucionen nuestra interacción con el mundo físico de manera similar a cómo el Internet transformó la comunicación entre personas. Un CPS puede existir en múltiples escalas: desde infraestructuras a gran escala, como puentes inteligentes capaces de detectar y responder a cambios estructurales, hasta vehículos autónomos, e incluso dispositivos médicos microscópicos implantados en el cuerpo humano. En última instancia, el propósito de los CPS es aprovechar la infraestructura cibernética incluyendo hardware y software para la detección, el cálculo y la comunicación para monitorear inteligentemente (percepción cibernética del mundo físico) y controlar (acción cibernética sobre el mundo físico) el entorno que nos rodea.

En la Figura 3.1, se ilustra este concepto de manera simplificada. Un ejemplo de sistema ciberfísico

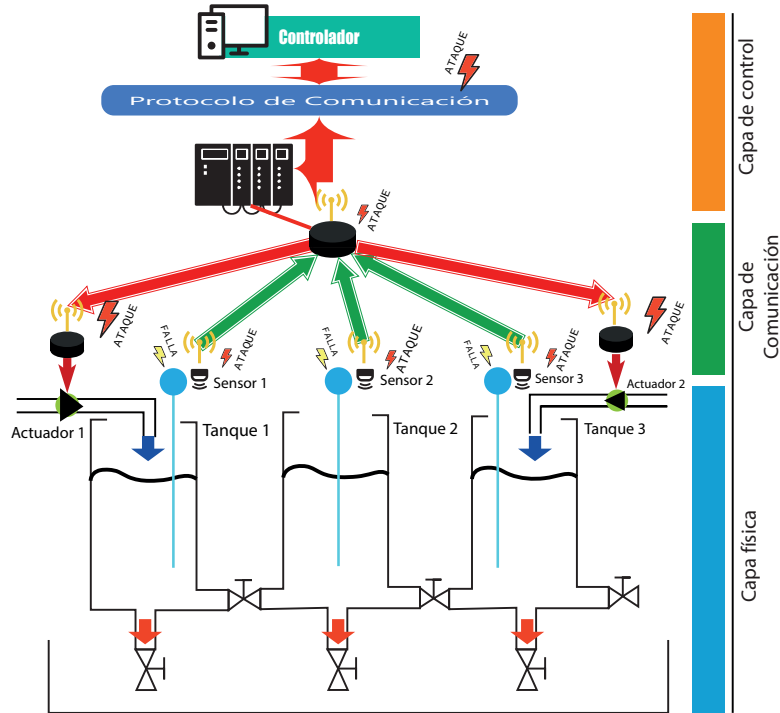


Fig. 3.1. Esquema de un sistema ciber-físico.

está compuesto por un sistema de tanques, tres nodos de comunicación inalámbrica y un controlador implementado en una computadora que se comunica mediante una red con protocolo IPV6. La operación del sistema consiste en controlar el nivel de líquido dentro del tanque, donde un sensor mide la altura del líquido. El tanque cuenta con varias válvulas de salida y dos bombas de entrada. Tanto el sensor como el actuador utilizan nodos de comunicación que transmiten información a través del protocolo IPV6 para realizar el control del sistema.

3.1.1. Arquitecturas de sistemas ciberfísicos

Un análisis detallado de los componentes de los sistemas ciber-físicos permite identificar cinco elementos esenciales, definidos por el Instituto de Investigación en TIC de Eindhoven (EIRCT) [Baheti y Gill (2011)]: el mundo físico, los transductores, los componentes de control, los elementos de análisis de datos y los componentes de comunicación.

1.- Mundo físico: Incluye tanto el sistema físico (dispositivos de ingeniería como sistemas de producción y controladores programables) como el entorno físico (fenómenos relevantes como la

lluvia y la temperatura). Las personas también desempeñan un papel importante en esta interacción.

2.- Transductores: Comprenden sensores, actuadores y dispositivos móviles organizados en redes. Estos nodos, que integran capacidades de comunicación y procesamiento, están incorporados en objetos cotidianos, dando lugar a una nueva generación de dispositivos inteligentes y distribuidos.

3.- Componentes de control: Agrupan el hardware y el software encargado de gestionar la plataforma de detección continua. Estos componentes adquieren datos de los sensores, realizan procesamiento local y controlan los actuadores para alcanzar los estados deseados en el mundo físico, operando bajo dinámicas discretas.

4.- Elementos de análisis de datos: Incluyen el software encargado del procesamiento, filtrado y almacenamiento de la información proveniente de los componentes de control. Este grupo también abarca las técnicas y políticas de seguridad que garantizan el funcionamiento adecuado del software.

5.- Componentes de comunicación: Se centran en las tecnologías de servicios en Internet, tales como la computación en la nube, la composición de servicios, las tecnologías de comunicación alámbricas e inalámbricas, los protocolos de comunicación y la comunicación máquina a máquina. En la Figura 3.2, se muestra cómo estos componentes se integran para formar un sistema ciberfísico.

3.2. Ataques a los sistemas ciberfísicos

En el contexto del control automático, un ataque se define como un evento deliberado o malicioso cuyo propósito es comprometer la integridad, confidencialidad o disponibilidad de un sistema ciberfísico. Estos ataques pueden manifestarse de diversas maneras, incluyendo manipulaciones no autorizadas de las entradas del sistema, alteraciones en los parámetros o comandos de control, así como interferencias en la comunicación entre los distintos componentes del sistema.

Estos ataques pueden estar dirigidos a diversos elementos del sistema, como los actuadores, sensores



Fig. 3.2. Arquitectura de los sistemas ciberfísicos.

o la infraestructura de comunicación que conecta los distintos módulos del sistema. En particular, estas amenazas pueden adoptar distintas formas, tales como ataques por suplantación de datos (Data Deception Attacks), manipulación de información y retrasos o interrupciones en la transmisión de datos. La Figura 3.3 presenta un resumen de los principales tipos de ataques reportados en la literatura especializada sobre automatización y control. En muchos casos, estas amenazas pueden resultar en una desconexión total entre los componentes del sistema.

Como se muestra en la figura 3.3, existe una amplia variedad de ataques; sin embargo, este trabajo se enfoca en tres de los más relevantes: ataques por suplantación de datos (Data Deception Attacks), inyección aleatoria de datos (Random Data Injection) y ataques de denegación de servicio (Denial of Service, DoS). Estos ataques son modelados mediante una distribución lógica Markoviana, lo cual permite representar de forma más realista sus efectos sobre el sistema.

La detección y mitigación de estos ataques es fundamental, ya que su presencia puede afectar significativamente el rendimiento, la estabilidad y la seguridad del sistema. Para proteger los sistemas de control automático ante posibles amenazas, es esencial diseñar controladores resilientes, emplear observadores e implementar técnicas avanzadas de ciberseguridad. Estas estrategias ase-

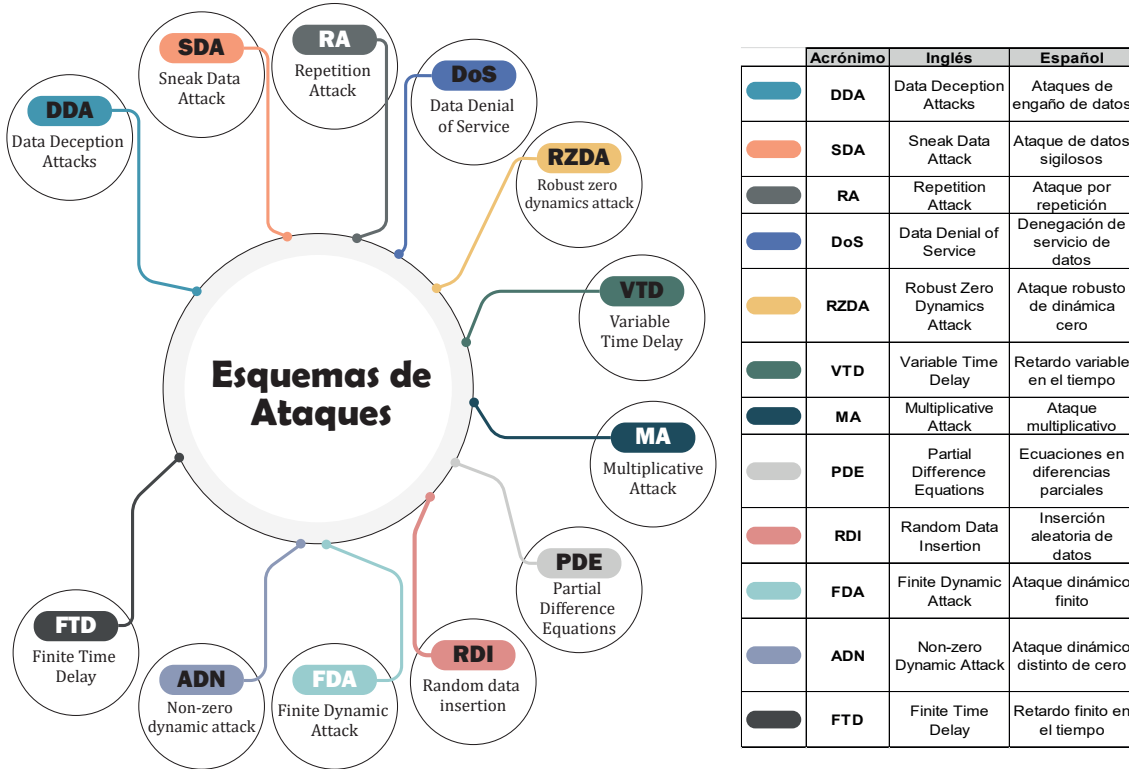


Fig. 3.3. Resumen de los tipos de ataques dirigidos a sistemas ciberfísicos.

guran que el sistema opere de manera adecuada incluso en entornos adversos. Una descripción detallada del modelo del sistema bajo ataque se presenta en la ecuación (3.1).

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) + \alpha(k)F_1a_a(k), \\ y(k) &= Cx(k) + \beta(k)F_2a_s(k). \end{aligned} \quad (3.1)$$

En la ecuación (3.1), $x(k) \in \mathbb{R}^n$ es el vector de estado en el instante discreto k , y $x(k+1)$ su evolución al siguiente paso. La matriz $A \in \mathbb{R}^{n \times n}$ describe la dinámica interna del sistema, mientras que $Bu(k)$ representa el efecto de la entrada de control $u(k) \in \mathbb{R}^m$ a través de la matriz $B \in \mathbb{R}^{n \times m}$. Los ataques a los actuadores se modelan con $\alpha(k) \in \{0, 1\}$, que indica la presencia o ausencia de ataque, la matriz $F_1 \in \mathbb{R}^{n \times r}$ y la señal maliciosa $a_a(k) \in \mathbb{R}^r$. De forma similar, la salida $y(k) \in \mathbb{R}^p$ depende de la matriz $C \in \mathbb{R}^{p \times n}$, mientras que los ataques a los sensores se representan mediante $\beta(k) \in \{0, 1\}$, la matriz $F_2 \in \mathbb{R}^{p \times s}$ y la señal $a_s(k) \in \mathbb{R}^s$. Este modelo permite describir explícitamente el impacto de los ataques en actuadores y sensores dentro de la dinámica del sistema.

3.2.1. Diferencias entre ataques y fallas

En esta sección se aborda la necesidad de distinguir de manera clara entre una señal de ataque y una señal de falla, tanto desde una perspectiva conceptual como matemática. Esta diferenciación resulta fundamental para el desarrollo de estrategias efectivas de control, detección, aislamiento o estimación, cuyo propósito es mejorar el desempeño, la resiliencia y la seguridad de los sistemas ciberfísicos.

Para ilustrar la relación entre el sistema, las fallas y los ataques, en la Figura 3.4 se muestra de manera esquemática cómo las fallas surgen de forma interna dentro del sistema, mientras que los ataques provienen de agentes externos que interfieren con su funcionamiento.

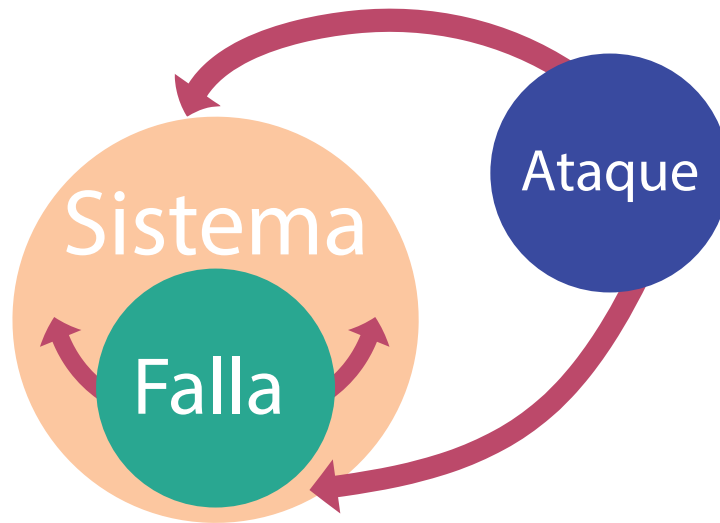


Fig. 3.4. Diferencias entre ataques y fallas.

Con base en la Figura 3.4, una **falla** se entiende como una perturbación interna que surge de la propia dinámica del sistema, generando un comportamiento anómalo o no deseado. No es intencionada y su origen es inherente al sistema físico o lógico. Puede deberse al desgaste de componentes, errores de programación o condiciones ambientales adversas. Matemáticamente, en tiempo discreto, una falla se modela como un cambio en la función dinámica del sistema a partir de un instante k_f :

$$x(k+1) = \begin{cases} f(x(k), u(k)), & 0 \leq k < k_f, \\ g(x(k), u(k)), & k \geq k_f. \end{cases} \quad (3.2)$$

donde $x(k)$ es el vector de estados, $u(k)$ el vector de entradas, $f(\cdot)$ la dinámica nominal, $g(\cdot)$ la dinámica alterada por la falla, y $v(k)$ representa la perturbación generada por dicha falla.

Por otro lado, un **ataque** se considera como una perturbación externa e intencionada, cuya finalidad es comprometer la integridad, disponibilidad o confidencialidad del sistema. Su origen es externo y responde a una acción deliberada por parte de un atacante. En tiempo discreto, la señal maliciosa $w(k)$ se introduce en las entradas del sistema, sin modificar directamente su estructura física:

$$x(k+1) = f(x(k), u(k) + w(k)) \quad (\text{Sistema bajo ataque, } k \geq k_a). \quad (3.3)$$

A partir del análisis previo, las principales diferencias entre una falla y un ataque son:

- **Intencionalidad:** Las fallas son accidentes sin intención; los ataques son deliberados.
- **Origen:** Las fallas son internas al sistema; los ataques provienen de agentes externos.
- **Objetivo:** Las fallas interrumpen el funcionamiento; los ataques buscan comprometer la seguridad o el control del sistema.
- **Detección:** Las fallas suelen ser evidentes; los ataques son más difíciles de identificar por su diseño oculto y malicioso.

Comprender estas diferencias es crucial para diseñar estrategias de protección efectivas. Mientras que las fallas requieren mecanismos de tolerancia y mantenimiento, los ataques exigen enfoques de detección intrusiva, resiliencia cibernética y sistemas de control robustos frente a adversarios inteligentes. La formulación matemática de ambos casos permite analizar su impacto sobre la dinámica del sistema y evaluar estrategias adecuadas de mitigación del efecto.

3.3. Ataques con distribución Markoviana

Los sistemas ciberfísicos integran procesos físicos, comunicaciones en red y control en tiempo real. La Fig. 3.5 ilustra cómo un adversario puede interferir tanto en el canal de *control* (actuadores) como en el de *sensado* (sensores), comprometiendo la operación segura del sistema.

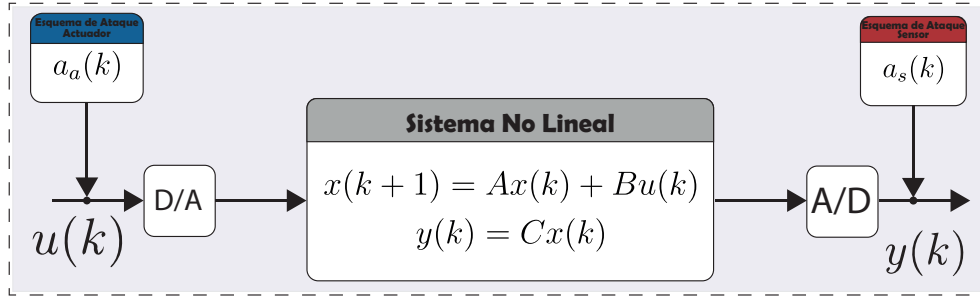


Fig. 3.5. Esquema general de ataque a un CPS.

Clasificación general

Consideramos dos ejes de clasificación (Fig. 3.6):

- **Estructura temporal:** *uniforme* (ventanas de activación/desactivación periódicas) y *no uniforme* (ventanas aleatorias).
- **Coordinación:** *no coordinados* (sólo sensor o sólo actuador) y *coordinados* (sensor y actuador simultáneamente).

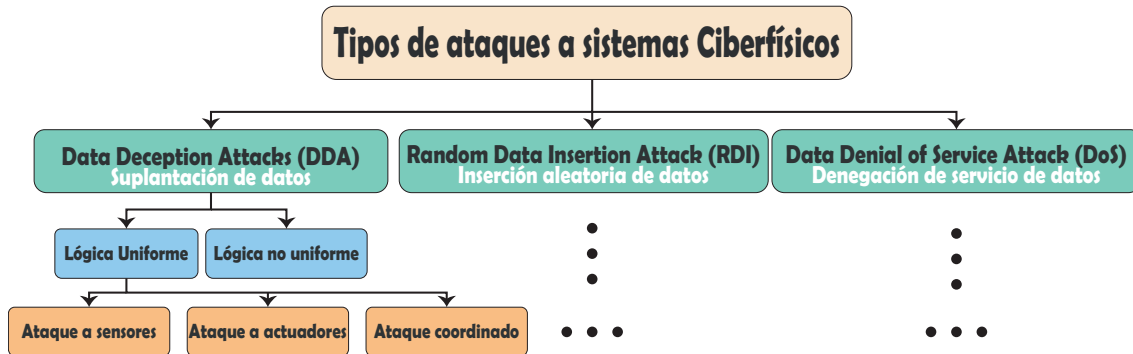


Fig. 3.6. Clasificación de ataques.

3.3.1. Modelo general de sistema bajo ataque

Sea el sistema lineal discreto nominal.

$$x(k+1) = A x(k) + B u(k), \quad y(k) = C x(k),$$

donde $x \in \mathbb{R}^n$, $u \in \mathbb{R}^m$, $y \in \mathbb{R}^p$. Modelamos los ataques en *actuadores* y *sensores* como inyecciones en los puertos correspondientes, gobernadas por procesos binarios de activación:

$$\alpha(k), \beta(k) \in \{0, 1\},$$

donde $\alpha(k) = 1$ indica ataque activo en actuadores y $\beta(k) = 1$ indica ataque activo en sensores. Usamos matrices de selección $F_1 \in \mathbb{R}^{m \times m}$ y $F_2 \in \mathbb{R}^{p \times p}$ (diagonales, con unos en los canales atacados).

El **modelo general** bajo ataque queda:

$$\begin{aligned} x(k+1) &= A x(k) + B u(k) + \alpha(k) B F_1 a_a(k), \\ y(k) &= C x(k) + \beta(k) F_2 a_s(k), \end{aligned} \tag{3.4}$$

donde $a_a(k) \in \mathbb{R}^m$ y $a_s(k) \in \mathbb{R}^p$ son las *señales maliciosas* sobre actuadores y sensores, respectivamente. A partir de (3.4), cada tipo de ataque se define eligiendo $a_a(k)$ y $a_s(k)$.

3.3.2. Ataque de denegación de servicio (DoS)

El ataque DoS *bloquea* la transmisión en los canales atacados. Se modela anulando la señal legítima:

$$a_a(k) = -u(k), \quad a_s(k) = -C x(k).$$

Al sustituir en (3.4):

$$\begin{aligned} x(k+1) &= A x(k) + (I_m - \alpha(k) F_1) B u(k), \\ y(k) &= (I_p - \beta(k) F_2) C x(k). \end{aligned} \tag{3.5}$$

Así, $\alpha = 1$ elimina los canales de control seleccionados y $\beta = 1$ suprime las mediciones seleccionadas.

3.3.3. Ataque de decepción de datos (DDA)

El ataque DDA modifica, parcial o totalmente, desnaturaliza la información legítima por datos falsos diseñados: $a_a(k) = -u(k) + b_a(k)$, $a_s(k) = -C x(k) + b_s(k)$, donde $b_a(k)$ y $b_s(k)$ son

señales falsas. Resulta:

$$\begin{aligned} x(k+1) &= A x(k) + (I_m - \alpha(k) F_1) B u(k) + \alpha(k) B F_1 b_a(k), \\ y(k) &= (I_p - \beta(k) F_2) C x(k) + \beta(k) F_2 b_s(k). \end{aligned} \quad (3.6)$$

A diferencia del DoS, aquí el sistema *sí* recibe/entrega información, pero *manipulada*.

3.3.4. Ataque de inyección aleatoria (RDI)

El ataque RDI añade *ruido/perturbación aleatoria* en los canales atacados sin suprimir completamente la señal legítima: $a_a(k) = b_a(k)$, $a_s(k) = b_s(k)$, obteniéndose:

$$\begin{aligned} x(k+1) &= A x(k) + B u(k) + \alpha(k) B F_1 b_a(k), \\ y(k) &= C x(k) + \beta(k) F_2 b_s(k). \end{aligned} \quad (3.7)$$

Este esquema induce comportamiento errático y degrada estimación/control sin aparentar una supresión total.

3.3.5. Lógica de activación (uniforme / no uniforme) y coordinación

La **estructura uniforme** emplea ventanas periódicas de ataque, mientras que la **no uniforme** usa ventanas aleatorias. La activación puede modelarse con *cadenas de Markov* de dos estados (activo/inactivo), cumpliendo la propiedad

$$\mathbb{P}(X_{s+t} \in A \mid X_s, X_{s-1}, \dots) = \mathbb{P}(X_{s+t} \in A \mid X_s), \quad (3.8)$$

lo que permite parametrizar las tasas de entrada/salida de ataque y analizar su persistencia. Además, distinguimos **ataques coordinados** (en las mismas ventanas) y **no coordinados** (solo un canal o ventanas distintas), como se ilustra en las Fig. 3.7–3.8.

Comparativo

- **DoS**: suprime total/parcialmente señales legítimas (bloqueo). Modelo en (3.5).
- **DDA**: sustituye por datos falsos diseñados (engaño coherente). Modelo en (3.6).
- **RDI**: inyecta ruido/perturbación aleatoria (comportamiento errático). Modelo en (3.7).

La lógica de activación (uniforme/no uniforme) y la coordinación (coordinado/no coordinado) se incorporan mediante $\alpha(k)$, $\beta(k)$ (y eventualmente cadenas de Markov), lo que permite estudiar de forma unificada su impacto sobre los modelos discretos considerados.

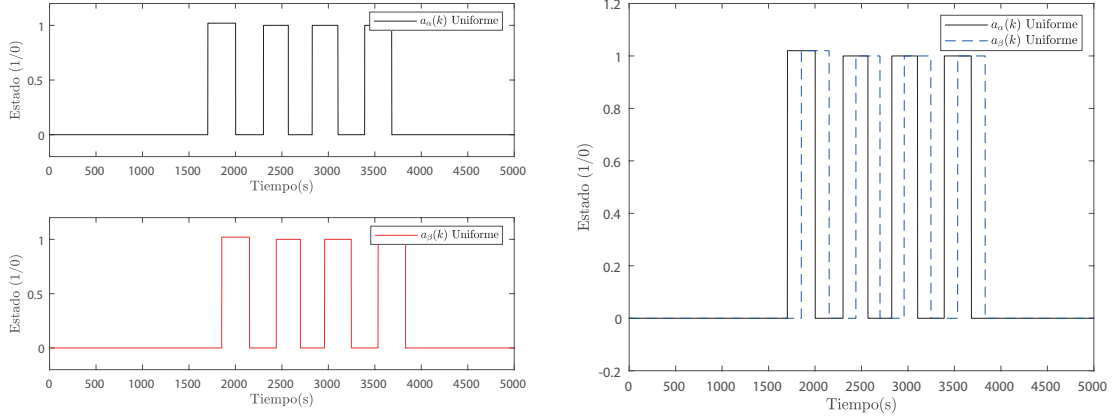


Fig. 3.7. Lógicas uniformes de activación: no coordinada, coordinada.

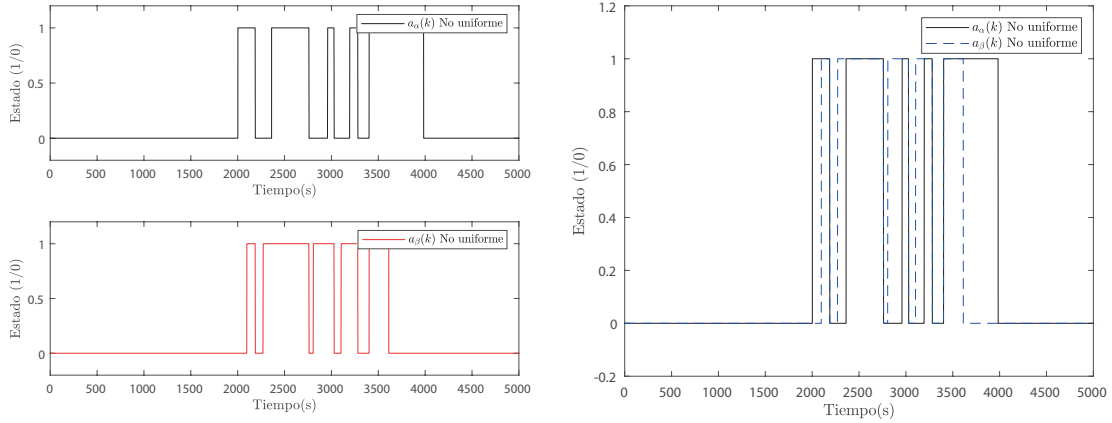


Fig. 3.8. Lógicas no uniformes de activación: coordinada, no coordinada.

3.4. Sistemas tomados como casos de estudio

En esta sección se describen y formalizan los modelos dinámicos que servirán como base para la validación de los esquemas propuestos en esta tesis. Se presentan tres sistemas representativos del dominio de los sistemas ciberfísicos, seleccionados por su relevancia en aplicaciones reales y por la riqueza de sus dinámicas no lineales: el sistema de tanques interconectados, la dinámica de un vehículo autónomo a escala tipo RC, y el sistema de glucosa-insulina.

Cada sistema se introduce a partir de sus fundamentos físicos, seguido de su representación matemática en forma continua y discreta, cuando corresponda. En particular, se destaca el uso de representaciones Takagi-Sugeno o modelos LPV para capturar comportamientos no lineales y fa-

cilitar el diseño de observadores y controladores resilientes.

El sistema de tanques se emplea como una planta de referencia ampliamente utilizada en la literatura para validar algoritmos de control y diagnóstico en presencia de perturbaciones y . El vehículo RC constituye un entorno experimental idóneo para representar la movilidad autónoma y validar esquemas de control en tiempo real. Por su parte, el sistema glucosa-insulina representa un caso biomédico con dinámicas complejas, utilizado para probar la eficacia de mecanismos de monitoreo y detección de intrusiones.

La caracterización matemática de estos sistemas permitirá, en capítulos posteriores, implementar y evaluar las estrategias de estimación de ataques, control tolerante a y análisis de estabilidad bajo escenarios de ciberataques.

3.4.1. Sistema de tanques interconectados

El estudio de caso central de los esquemas de diagnóstico propuestos se enfoca en un sistema de tres tanques interconectados. En la ingeniería de procesos químicos, estos sistemas son fundamentales, ya que sirven como una herramienta esencial para el control automático y actualmente son vulnerables a diversos ataques que pueden afectar su operación. Están conformados por varios tanques conectados mediante tuberías y válvulas dispuestas estratégicamente, cuyo objetivo principal es controlar y regular el nivel de líquido en cada tanque.

Un esquema del sistema de tres tanques interconectados utilizado como caso de estudio se muestra en la Figura 3.9.

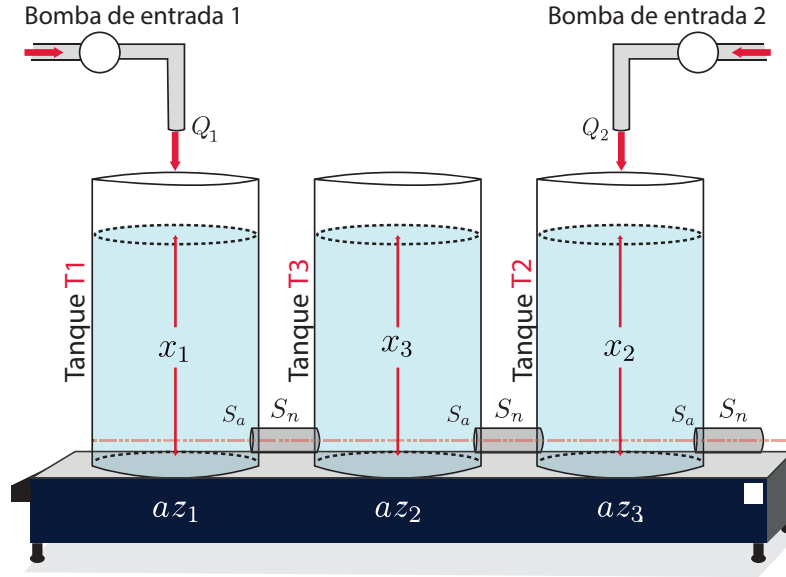


Fig. 3.9. Esquema del caso de estudio (Tres tanques interconectados).

El comportamiento dinámico del sistema puede describirse mediante ecuaciones de balance de masa para cada tanque, donde el flujo de fluido entre tanques se modela de acuerdo con la ley de Torricelli. Considerando un tiempo de muestreo de $T_d = 0.01$ segundos, las ecuaciones no lineales en tiempo discreto que rigen la evolución de los niveles de líquido $x_1(k)$, $x_2(k)$ y $x_3(k)$ en los tres tanques se expresan como:

$$\begin{aligned}
 x_1(k+1) &= x_1(k) - \frac{T_d}{S_a} \left(az_1 S_n \operatorname{sgn}(x_1(k) - x_3(k)) \sqrt{2g(x_1(k) - x_3(k))} \right) + \frac{T_d}{S_a} Q_1(k), \\
 x_2(k+1) &= x_2(k) + \frac{T_d}{S_a} \left(az_3 S_n \operatorname{sgn}(x_3(k) - x_2(k)) \sqrt{2g(x_3(k) - x_2(k))} \right) - \frac{T_d}{S_a} az_2 S_n \sqrt{2gx_2(k)} + \frac{T_d}{S_a} Q_2(k), \\
 x_3(k+1) &= x_3(k) + \frac{T_d}{S_a} \left(az_1 S_n \operatorname{sgn}(x_1(k) - x_3(k)) \sqrt{2g(x_1(k) - x_3(k))} \right) - \frac{T_d}{S_a} az_3 S_n \operatorname{sgn}(x_3(k) - x_2(k)) \sqrt{2g(x_3(k) - x_2(k))},
 \end{aligned} \tag{3.9}$$

Para facilitar el análisis y el diseño del observador, el modelo anterior puede reescribirse en una forma de espacio de estados no lineal en tiempo discreto como:

$$\begin{aligned}
 x(k+1) &= A(x(k))x(k) + Bu(k), \\
 y(k) &= Cx(k),
 \end{aligned} \tag{3.10}$$

donde los vectores y matrices están definidos como:

$$x(k) = \begin{bmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \end{bmatrix}, \quad u(k) = \begin{bmatrix} Q_1(k) \\ Q_2(k) \end{bmatrix}, \quad y(k) = \begin{bmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad B = \frac{T_d}{S_a} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

La matriz $A(x(k))$ captura la dependencia no lineal respecto a las variables de estado, debido a los términos de raíz cuadrada en la dinámica del flujo:

$$A(x(k)) = \begin{bmatrix} A_{11}(x) & 0 & A_{13}(x) \\ 0 & A_{22}(x) & A_{23}(x) \\ A_{31}(x) & A_{32}(x) & A_{33}(x) \end{bmatrix}, \quad (3.11)$$

con los elementos definidos como:

$$\begin{aligned} A_{11}(x) &= 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_1(k) - x_3(k)|}} \operatorname{sgn}(x_1(k) - x_3(k)) \\ A_{13}(x) &= \frac{az_1 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_1(k) - x_3(k)|}} \operatorname{sgn}(x_1(k) - x_3(k)), \\ A_{22}(x) &= 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_3(k) - x_2(k)|}} \operatorname{sgn}(x_3(k) - x_2(k)) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_2(k)|}} \\ A_{23}(x) &= \frac{az_3 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_3(k) - x_2(k)|}} \operatorname{sgn}(x_3(k) - x_2(k)), \\ A_{31}(x) &= \frac{az_1 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_1(k) - x_3(k)|}} \operatorname{sgn}(x_1(k) - x_3(k)) \\ A_{32}(x) &= \frac{az_3 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_3(k) - x_2(k)|}} \operatorname{sgn}(x_3(k) - x_2(k)), \\ A_{33}(x) &= 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_1(k) - x_3(k)|}} \operatorname{sgn}(x_1(k) - x_3(k)) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a \sqrt{|x_3(k) - x_2(k)|}} \operatorname{sgn}(x_3(k) - x_2(k)). \end{aligned}$$

Este modelo en espacio de estados no lineal en tiempo discreto servirá como base para el desarrollo de los esquemas de observador y diagnóstico propuestos en las siguientes secciones.

3.4.2. Dinámica de vehículos RC

El modelado de vehículos es una herramienta fundamental en el diseño de estrategias avanzadas de control, simulación y análisis de desempeño. Una representación precisa de la dinámica vehicular permite entender y predecir el comportamiento del sistema ante diversas condiciones de operación, facilitando así el desarrollo de controladores que garanticen seguridad, estabilidad y eficiencia. En el caso de vehículos de control remoto (RC, por sus siglas en inglés), su uso como plataformas experimentales es ampliamente aceptado debido a su bajo costo, flexibilidad y facilidad de instrumentación. Estos modelos constituyen un entorno ideal para validar algoritmos de control en tiempo real bajo condiciones controladas, pero con características dinámicas representativas de vehículos reales.

En este contexto, se emplea el denominado “modelo bicicleta” para describir la dinámica lateral del vehículo, como se ilustra en la Figura 3.10. Este modelo simplifica la representación de un vehículo de cuatro ruedas al considerar únicamente dos ruedas equivalentes: una delantera y una trasera, situadas sobre el eje longitudinal del vehículo. Dicha aproximación conserva las características esenciales de la dinámica lateral y de guiñada, reduciendo la complejidad computacional del sistema, lo cual resulta útil para el diseño y análisis de controladores.

Considerando el marco de referencia del cuerpo del vehículo, y siguiendo las referencias Rajamani (2011); Pacejka (2005), la dinámica lateral discreta se describe por el siguiente conjunto de ecuaciones no lineales:

$$\begin{cases} v_y(k+1) = v_y(k) + T_d \left(\frac{F_{yf}(k) \cos \delta(k) + F_{yr}(k)}{m} - \omega(k) v_x(k) \right), \\ \omega(k+1) = \omega(k) + T_d \left(\frac{F_{yf}(k) l_f \cos \delta(k) - F_{yr}(k) l_r}{I} \right), \end{cases} \quad (3.12)$$

donde v_x y v_y son las velocidades longitudinal y lateral en el marco del cuerpo del vehículo [m/s], ω es la velocidad de guiñada [rad/s], δ es el ángulo de dirección de las ruedas delanteras (entrada de control), F_{yf} y F_{yr} representan las fuerzas laterales generadas por los neumáticos delantero y trasero, m es la masa total del vehículo [kg], I es el momento de inercia respecto al eje vertical [$\text{kg} \cdot \text{m}^2$], l_f y l_r son las distancias desde el centro de gravedad a los ejes delantero y trasero, respectivamente.

Estas ecuaciones constituyen un modelo no lineal discreto, ya que las fuerzas de los neumáticos

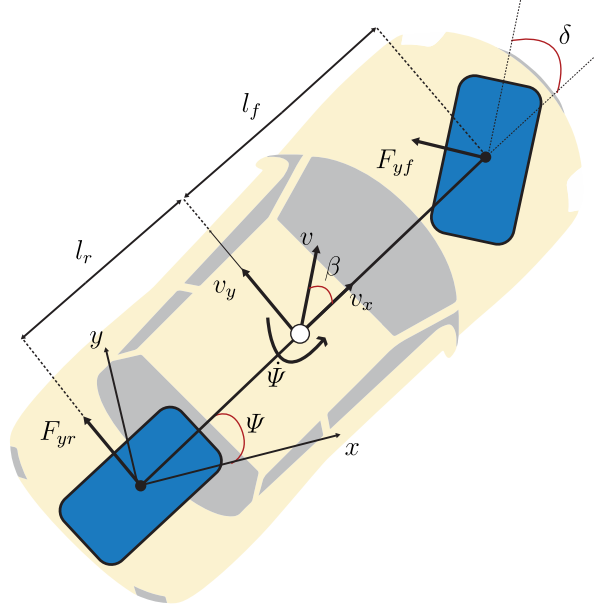


Fig. 3.10. Representación del vehículo mediante el modelo bicicleta.

dependen de variables como el ángulo de deslizamiento (slip angle), el cual a su vez está relacionado con las variables de estado del sistema. Además, la entrada de control aparece no linealmente a través del término $\cos \delta$.

Para facilitar el análisis, se define el vector de estado y la entrada como:

$$x(k) = \begin{bmatrix} v_y(k) \\ \omega(k) \end{bmatrix}, \quad u(k) = \delta(k). \quad (3.13)$$

Las fuerzas laterales de los neumáticos F_{yf} y F_{yr} se modelan, en la generalidad del caso no lineal, utilizando funciones que dependen del ángulo de deslizamiento α_i y características del neumático. En esta etapa, se mantiene la forma general:

$$\begin{aligned} F_{yf}(k) &= f_{yf}(v_y(k), \omega(k), v_x(k), \delta(k)), \\ F_{yr}(k) &= f_{yr}(v_y(k), \omega(k), v_x(k)). \end{aligned} \quad (3.14)$$

Por lo tanto, el modelo no lineal discreto en espacio de estados se puede expresar como:

$$x(k+1) = f(x(k), u(k), v_x(k)), \quad (3.15)$$

donde la función $f(\cdot)$ es no lineal respecto a las variables $x(k)$ y $u(k)$, y depende también del parámetro externo $v_x(k)$, que se puede considerar como una entrada medida o una perturbación conocida.

Este modelo servirá como base para los procesos de linealización y parametrización en tiempo discreto, fundamentales para formular su representación LPV y su posterior análisis de estabilidad y control.

3.4.3. Sistema glucosa-insulina

La representación matemática del sistema glucosa-insulina es fundamental en el control automático, ya que permite comprender y regular los niveles de glucosa en pacientes diabéticos. Esto es crucial para evitar complicaciones y desarrollar dispositivos médicos avanzados, tales como bombas de insulina y sistemas de monitoreo continuo de glucosa, como se muestra en la Figura 3.11.

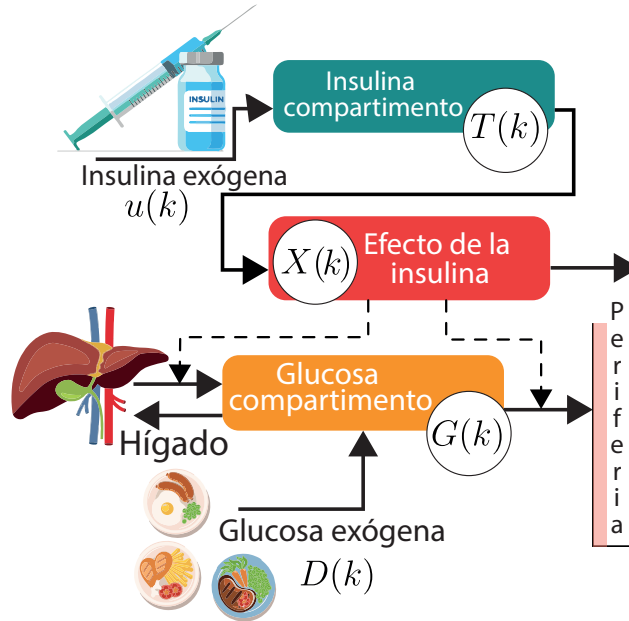


Fig. 3.11. Diagrama del sistema glucosa-insulina en pacientes con DM-1.

El modelo no lineal en tiempo discreto que describe al paciente con DM-1 se expresa como:

$$G_{\Delta}(k+1) = G_{\Delta}(k) + T_d \left[-p_1 G_{\Delta}(k) - X(k) (G_{\Delta}(k) + G_b) + D(k) \right], \quad (3.16)$$

$$X(k+1) = X(k) + T_d \left[-p_2 X(k) + p_3 I_{\Delta}(k) \right], \quad (3.17)$$

$$I_{\Delta}(k+1) = I_{\Delta}(k) + T_d \left[-N (I_{\Delta}(k) + I_b) + \frac{u(k)}{V_I} \right], \quad (3.18)$$

donde $D(k)$ y $u(k)$ representan las tasas de infusión de glucosa e insulina, respectivamente, V_I es el volumen de distribución de insulina, N es la tasa de desaparición de insulina, $X(k)$ es el efecto de la insulina, $G_{\Delta}(k)$ y $I_{\Delta}(k)$ son las diferencias de concentración de glucosa e insulina plasmática, respectivamente, G_b y I_b son los valores basales de glucosa e insulina. Los parámetros p_1 , p_2 y p_3 representan, respectivamente, la tasa constante de absorción de glucosa en los tejidos, la tasa de disminución de la absorción y la tasa de aumento de la capacidad de absorción.

El modelo puede representarse en forma de espacio de estados como sigue:

$$x(k+1) = A(x(k))x(k) + Bu(k) + Dw(k) + \Delta, \quad (3.19)$$

$$y(k) = Cx(k), \quad (3.20)$$

con las siguientes definiciones: $x(k) = \begin{bmatrix} G_{\Delta}(k) & X(k) & I_{\Delta}(k) \end{bmatrix}^T$, $w(k) = D(k)$, $B = \begin{bmatrix} 0 & 0 & \frac{1}{V_I} \end{bmatrix}^T$, $\Delta = \begin{bmatrix} 0 & 0 & -NI_b \end{bmatrix}^T$, $A(x(k)) = \begin{bmatrix} -p_1 & -(G_{\Delta} + G_b) & 0 \\ 0 & -p_2 & p_3 \\ 0 & 0 & -N \end{bmatrix}$, $D = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}^T$, $C = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}$.

3.5. Estrategias de modelado para el análisis de sistemas No Lineales

En esta sección se presenta el enfoque de modelado multimodelo como base para representar sistemas no lineales mediante estructuras equivalentes lineales. En particular, se detallan las representaciones Takagi-Sugeno y de Parámetros Variables en el Tiempo (LPV, por sus siglas en inglés), las cuales permiten aproximar el comportamiento no lineal de los sistemas de estudio mediante combinaciones ponderadas de modelos lineales. Estas técnicas serán empleadas para la descripción de los distintos casos de estudio considerados en este trabajo, facilitando así el análisis y diseño de esquemas de observación y control bajo un marco de teoría de sistemas lineales.

3.5.1. Teoría de los sistemas Takagi-Sugeno

La representación T-S constituye una herramienta fundamental para modelar sistemas no lineales mediante una estructura compuesta por modelos locales lineales. Esta metodología fue introducida en Tanaka *y col.* (2003), y su principal objetivo es aproximar el comportamiento de un sistema no lineal de forma más simple, sin perder sus características esenciales. La ventaja de esta aproximación radica en que permite aplicar técnicas de análisis y diseño desarrolladas para sistemas lineales, como las de control y observación.

El modelo T-S se basa en reglas difusas de tipo IF-THEN, las cuales describen la dinámica local del sistema a través de modelos lineales o afines, válidos en regiones específicas del espacio de estados. Estas reglas se combinan de manera ponderada para obtener un modelo global continuo, proporcionando una representación precisa o muy cercana del sistema no lineal original (Lendek *y col.*, 2011).

Una regla difusa típica puede expresarse como:

$$\rho_1 \text{ es } P_1^i \text{ y } \cdots \text{ y } \rho_p \text{ es } P_p^i \Rightarrow y = F_i(\rho), \quad (3.21)$$

donde $\rho = [\rho_1, \dots, \rho_p]^\top$ es un vector que contiene las variables de programación (también llamadas variables de premisa), las cuales determinan el grado de activación de cada regla. Los conjuntos P_j^i representan conjuntos difusos asociados a cada variable ρ_j , y κ denota el número total de reglas.

La pertenencia de una variable de programación ρ_j al conjunto difuso P_j^i se determina mediante una función de pertenencia $\mu_{ij} : \mathbb{R} \rightarrow [0, 1]$. El grado de activación de la regla i puede calcularse utilizando operadores de conjunción como el mínimo:

$$\varphi_i(\rho) = \min_j \mu_{ij}(\rho_j), \quad (3.22)$$

o bien mediante el producto algebraico:

$$\varphi_i(\rho) = \prod_{j=1}^p \mu_{ij}(\rho_j). \quad (3.23)$$

Posteriormente, los valores de activación son normalizados para obtener los pesos difusos:

$$\mu_i(\rho) = \frac{\varphi_i(\rho)}{\sum_{j=1}^{\kappa} \varphi_j(\rho)}, \quad (3.24)$$

siendo necesario que $\sum_{i=1}^{\kappa} \varphi_i(\rho) \neq 0$ para garantizar que al menos una regla esté activa en todo instante.

Enfoque del sector no lineal

Uno de los métodos para construir representaciones T-S es el conocido como “Enfoque del sector no lineal”. Este permite obtener aproximaciones difusas precisas de sistemas no lineales dentro de un conjunto compacto del espacio de estados, siendo especialmente útil para el diseño de controladores difusos. Una descripción detallada de este enfoque se encuentra en Ohtake *y col.* (2003).

Inicialmente, este método fue desarrollado para sistemas no lineales de la forma:

$$\begin{aligned} x(k+1) &= f^m(x, u)x(k) + g^m(x, u)u(k), \\ y(k) &= h^m(x, u)x(k), \end{aligned} \tag{3.25}$$

donde $x(k) \in \mathbb{R}^{n_x}$ es el vector de estados, $u(k) \in \mathbb{R}^{n_u}$ la entrada del sistema, y $y(k) \in \mathbb{R}^{n_y}$ la salida. Las funciones matriciales f^m, g^m, h^m son no lineales y suaves, con elementos acotados y definidos en conjuntos compactos.

Una forma más general incluye términos de desviación no lineales:

$$\begin{aligned} x(k+1) &= f^m(x, u)x(k) + g^m(x, u)u(k) + a(x, u), \\ y(k) &= h^m(x, u)x(k) + c(x, u), \end{aligned} \tag{3.26}$$

donde $a(x, u)$ y $c(x, u)$ son funciones vectoriales suaves que representan contribuciones adicionales no lineales.

En este enfoque, se definen las variables de programación como funciones no lineales diferenciables acotadas en un intervalo $[nl_j^0, nl_j^1]$, es decir, $\rho_j(\cdot) \in [nl_j^0, nl_j^1]$ para $j = 1, \dots, p$. Con base en estos valores, se construyen funciones de ponderación normalizadas:

$$\eta_0^j = \frac{nl_j^1 - \rho_j(\cdot)}{nl_j^1 - nl_j^0}, \quad \eta_1^j = 1 - \eta_0^j, \tag{3.27}$$

Las funciones de ponderación cumplen: $\eta_0^j \geq 0$, $\eta_1^j \geq 0$ y $\eta_0^j + \eta_1^j = 1$. Además, cada ρ_j puede escribirse como combinación convexa:

$$\rho_j = nl_j^0 \eta_0^j(\rho_j) + nl_j^1 \eta_1^j(\rho_j). \quad (3.28)$$

A cada función de ponderación le corresponde un conjunto difuso definido en el intervalo $[nl_j^0, nl_j^1]$, denotado como P_0^j y P_1^j , respectivamente.

Las reglas del modelo T-S se construyen considerando todas las combinaciones posibles de los valores extremos de cada ρ_j . De este modo, el modelo T-S completo se define por $\kappa = 2^p$ reglas. La regla asociada al modelo i -ésimo se expresa como:

Regla i -ésima: Si ρ_1 es P_1^i y $\dots$ y ρ_p es P_p^i entonces

$$\begin{aligned} x(k+1) &= A_{i,d} x(k) + B_{i,d} u(k) + a_{i,d}, \\ y(k) &= C_i x(k) + c_i, \end{aligned} \quad (3.29)$$

donde $A_{i,d}$, $B_{i,d}$ y C_i son las matrices locales del modelo en tiempo discreto, y $a_{i,d}$ y c_i representan los términos de desviación asociados a la regla i -ésima. Los conjuntos P_j^i corresponden a P_0^j o P_1^j según la combinación específica de la regla.

El peso de activación de la regla i se calcula como el producto de las funciones de ponderación correspondientes:

$$\mu_i(\rho) = \prod_{j=1}^p \mu_{ij}(\rho_j), \quad (3.30)$$

donde cada $\mu_{ij}(\rho_j)$ es igual a $\eta_0^j(\rho_j)$ o $\eta_1^j(\rho_j)$ según corresponda. Estas funciones están normalizadas, garantizando que $\mu_i(\rho) \geq 0$ y $\sum_{i=1}^{\kappa} \mu_i(\rho) = 1$.

Finalmente, las matrices A_i , B_i , C_i y los vectores a_i , c_i se obtienen evaluando las funciones originales en los extremos definidos por nl_j^0 y nl_j^1 , de acuerdo con la estructura de cada regla.

Enfoque del sector lineal

El enfoque del sector lineal permite representar sistemas no lineales mediante interpolación convexa entre modelos lineales locales definidos en vértices del espacio de operación. Un sistema no lineal de la forma:

$$\begin{aligned} x(k+1) &= f(x(k), u(k)), \\ y(k) &= h(x(k)), \end{aligned} \quad (3.31)$$

puede representarse mediante un modelo T-S como:

$$\begin{aligned} x(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) (A_i x(k) + B_i u(k)), \\ y(k) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) C_i x(k), \end{aligned} \quad (3.32)$$

donde las funciones de pertenencia $\mu_i(\rho(k))$ dependen de las variables premisas $\rho(k)$, que suelen ser funciones del estado o de la salida medida, y satisfacen las condiciones:

$$\mu_i(\rho(k)) \geq 0, \quad \sum_{i=1}^{\kappa} \mu_i(\rho(k)) = 1. \quad (3.33)$$

El número de reglas κ depende del número de funciones de membresía por variable premisa. Las matrices A_i , B_i , y C_i definen los modelos lineales locales en cada vértice.

Este modelo es particularmente útil para análisis de control y observabilidad porque permite utilizar herramientas del control lineal robusto mediante desigualdades matriciales lineales (LMI).

Análisis de estabilidad bajo interpolación convexa

Para analizar la estabilidad del sistema T-S bajo el enfoque del sector lineal, se propone una función de Lyapunov común o dependiente de vértices. Una elección conservadora pero útil es:

$$V(x) = x^\top P x, \quad P = P^\top > 0. \quad (3.34)$$

La derivada temporal de $V(x)$ a lo largo de las trayectorias del sistema es:

$$\Delta V(x) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left(x^\top (A_i^\top P + P A_i) x \right). \quad (3.35)$$

Una condición suficiente para asegurar la estabilidad global del sistema es que:

$$A_i^\top P + P A_i < 0, \quad \forall i \in \{1, \dots, \kappa\}. \quad (3.36)$$

Estas condiciones pueden escribirse como LMIs y verificarse numéricamente.

Condiciones de observabilidad para sistemas Takagi-Sugeno

El sistema T-S en (3.32) es estructuralmente observable si cada subsistema local (A_i, C_i) es observable, es decir, si la siguiente matriz de observabilidad tiene rango completo para cada i :

$$\mathcal{O}_i = \begin{bmatrix} C_i \\ C_i A_i \\ \vdots \\ C_i A_i^{n-1} \end{bmatrix}, \quad \text{rango}(\mathcal{O}_i) = n. \quad (3.37)$$

3.5.2. Teoría del sistema LPV

En la última década, los sistemas LPV son una poderosa técnica para modelar sistemas no lineales mediante una descripción lineal cuyo comportamiento depende de parámetros que varían en el tiempo. Estos parámetros, denotados como $\rho(k) \in \Omega$, son conocidos en cada instante de tiempo y pertenecen a un conjunto convexo. El modelo general de un sistema LPV se puede expresar como:

$$\Sigma(\rho) : \begin{bmatrix} x(k+1) \\ z(k) \\ y(k) \end{bmatrix} = \begin{bmatrix} A(\rho(k)) & B_1(\rho(k)) & B_2(\rho(k)) \\ C_1(\rho(k)) & D_{11}(\rho(k)) & D_{12}(\rho(k)) \\ C_2(\rho(k)) & D_{21}(\rho(k)) & D_{22}(\rho(k)) \end{bmatrix} \begin{bmatrix} x(k) \\ w(k) \\ u(k) \end{bmatrix}, \quad (3.38)$$

donde $x(k) \in \mathbb{R}^n$ es el estado, $u(k)$ la entrada de control, $w(k)$ representa entradas exógenas, $y(k)$ la salida medida y $z(k)$ una salida de interés para desempeño. La dependencia afín o polinómica de las matrices respecto a los parámetros $\rho(k)$ permite representar la dinámica de una amplia gama de sistemas no lineales a través de interpolaciones lineales.

Observabilidad de Sistemas LPV

Al igual que los sistemas Takagi-Sugeno, la observabilidad en LPV está fuertemente influenciada por la variación de los parámetros. En este contexto, el sistema es observable si existe una función de Lyapunov dependiente del parámetro que garantice una reconstrucción estable del estado para toda trayectoria admisible de $\rho(k)$. Se puede emplear un enfoque politopo para establecer condiciones de observabilidad utilizando desigualdades matriciales lineales (LMIs), similares al análisis sectorial de sistemas Takagi-Sugeno. La condición típica se basa en asegurar la detectabilidad de todos los vértices del politopo y luego extender este resultado a todo el conjunto convexo mediante interpolación.

Estabilidad en sistemas LPV

La estabilidad en sistemas LPV se analiza en dos vertientes: en términos de estabilidad cuadrática común y estabilidad dependiente del parámetro. En el primer caso, se busca una única función de Lyapunov $V(x) = x^\top P x$ tal que se satisfagan condiciones de decrecimiento negativo para todas las posibles matrices del sistema a lo largo de $\rho(k)$:

$$A(\rho)^\top P + P A(\rho) < 0, \quad \forall \rho \in \Omega. \quad (3.39)$$

Cuando esto no es posible, se recurre a funciones de Lyapunov dependientes del parámetro, $V(x, \rho) = x^\top P(\rho) x$, y se introduce la derivada de $P(\rho(k))$ a través de técnicas de análisis basadas en LMIs paramétricas. Este análisis resulta más general y menos conservador, aunque con un costo computacional superior.

En ambos enfoques, se mantiene la estructura de análisis típica del sector lineal: descomposición, politopo del espacio de parámetros, uso de condiciones convexas (LMIs) y verificación de propiedades para cada vértice del politopo.

3.6. Teoría de los Observadores

En muchos sistemas de control, no todas las variables de estado pueden ser medidas directamente. En estos casos, es necesario estimar dichas variables a partir de las señales de entrada y salida disponibles, proceso que se denomina observación.

Consideremos un sistema descrito en el espacio de estados como:

$$x(k+1) = Ax(k) + Bu(k), \quad (3.40)$$

$$y(k) = Cx(k), \quad (3.41)$$

donde $x(k) \in \mathbb{R}^{n_x}$ es el vector de estados, $u(k) \in \mathbb{R}^{n_u}$ representa las entradas del sistema y $y(k) \in \mathbb{R}^{n_y}$ son las salidas medidas. Las matrices $A \in \mathbb{R}^{n_x \times n_x}$, $B \in \mathbb{R}^{n_x \times n_u}$ y $C \in \mathbb{R}^{n_y \times n_x}$ son conocidas y constantes.

El propósito fundamental de un observador de estados es reconstruir las variables de estado internas del sistema utilizando las entradas y salidas disponibles. Para sistemas lineales invariantes en el tiempo, como el representado en (3.40), esta tarea puede lograrse mediante diversas estructuras de observadores.

Una forma común de clasificar los observadores es de acuerdo con el número de variables de estado que estiman:

- **Observador de orden completo:** Estima todas las variables de estado, sin considerar si algunas de ellas pueden ser medidas directamente.
- **Observador de orden reducido:** Estima únicamente un subconjunto de las variables de estado, es decir, menos de n_x estados.
- **Observador de orden mínimo:** Estima el menor número posible de variables de estado, concretamente $n_x - n_y$, donde n_y es el número de salidas medidas.

3.6.1. Clasificación de los observadores según su estructura

Observador tipo Luenberger

El observador tipo Luenberger es un algoritmo ampliamente utilizado para estimar todos los estados del sistema dinámico a partir de las entradas y salidas disponibles. Su estructura es la siguiente:

$$\hat{x}(k+1) = A\hat{x}(k) + Bu(k) + L(y(k) - C\hat{x}(k)), \quad (3.42)$$

$$\hat{y}(k) = C\hat{x}(k). \quad (3.43)$$

La Figura 3.12 presenta un diagrama que ilustra la implementación de este observador:

Observador proporcional

Este tipo de observador introduce grados de libertad adicionales que pueden ser utilizados para mejorar el margen de estabilidad. Sin embargo, presenta una sensibilidad elevada ante incertidumbres paramétricas e introduce errores estáticos en la estimación. Su estructura es:

$$\zeta(k+1) = N\zeta(k) + Fy(k) + Ju(k), \quad (3.44)$$

$$\hat{x}(k) = P\zeta(k) + Qy(k). \quad (3.45)$$

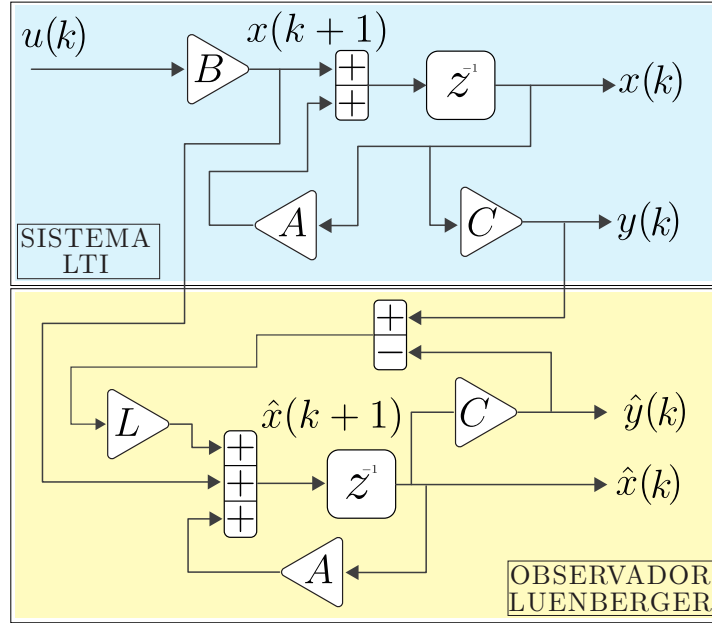


Fig. 3.12. Esquema del observador tipo Luenberger.

La Figura 3.13 muestra el esquema correspondiente a este tipo de observador, permitiendo visualizar sus diferencias con respecto al observador tipo Luenberger:

Observador proporcional-integral

Para contrarrestar la sensibilidad a las incertidumbres paramétricas del observador proporcional, se han propuesto observadores de tipo proporcional-integral. Estos añaden una acción integral sobre el error de salida, lo cual permite mejorar la precisión de la estimación en estado estacionario. Su formulación matemática es:

$$\zeta(k+1) = N\zeta(k) + Hv(k) + Fy(k) + Ju(k), \quad (3.46)$$

$$v(k+1) = y(k) - C\hat{x}(k), \quad (3.47)$$

$$\hat{x}(k) = P\zeta(k) + Qy(k). \quad (3.48)$$

La Figura 3.14 muestra el esquema de este observador, permitiendo distinguir claramente su estructura con respecto al observador proporcional:

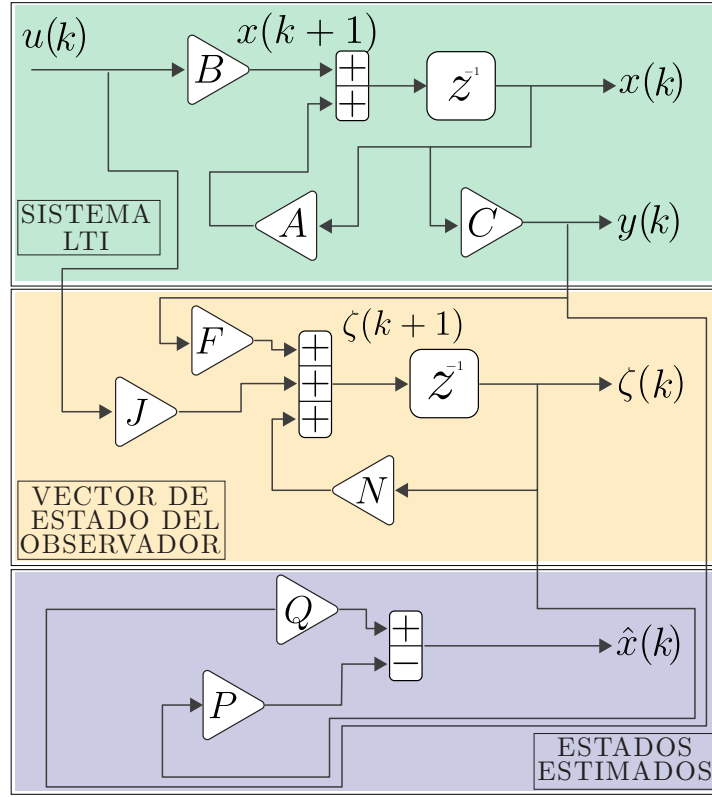


Fig. 3.13. Esquema del observador proporcional.

Observador dinámico generalizado

El observador dinámico generalizado ofrece una mayor precisión en estado estacionario y mayor robustez frente a errores de modelado. Además, proporciona múltiples grados de libertad en su diseño, lo que permite incrementar el margen de estabilidad. Su estructura es la siguiente:

$$\zeta(k+1) = N\zeta(k) + Hv(k) + Fy(k) + Ju(k), \quad (3.49)$$

$$v(k+1) = S\zeta(k) + Lv(k) + My(k), \quad (3.50)$$

$$\hat{x}(k) = P\zeta(k) + Qy(k). \quad (3.51)$$

La Figura 3.15 ilustra a este observador y permite identificar las ganancias adicionales y la complejidad asociada a su diseño:

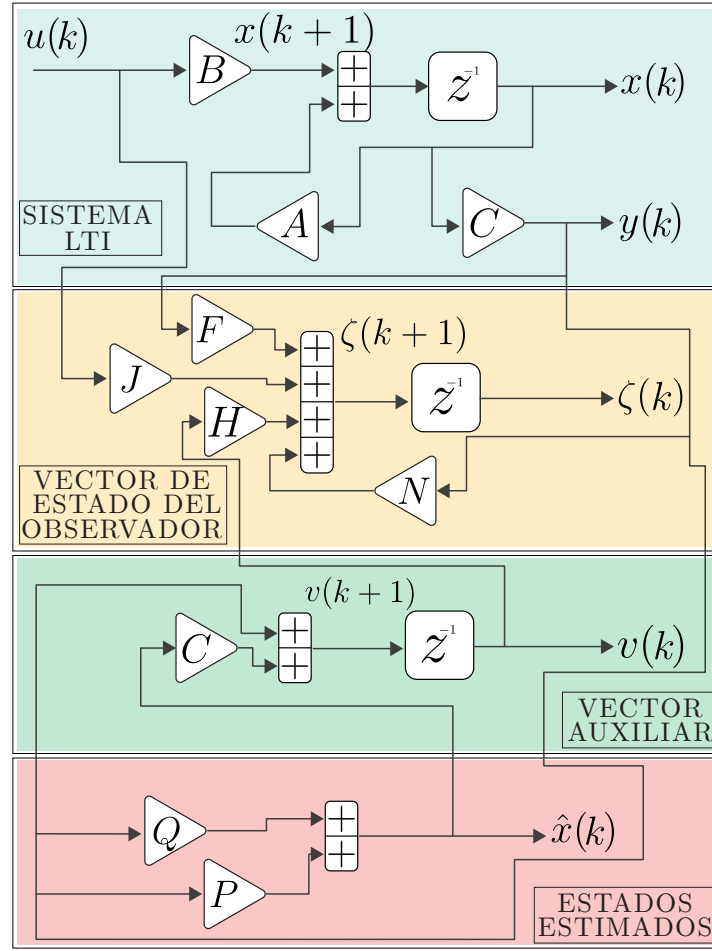


Fig. 3.14. Esquema del observador proporcional-Integral.

3.6.2. Observabilidad

La observabilidad en los sistemas hace referencia a la capacidad de reconstruir el vector de estado a partir de las entradas y salidas del sistema. Para verificar dicha propiedad, es necesario asegurarse de que los modelos locales sean observables. Esto se puede comprobar evaluando si el rango de la matriz de observabilidad es igual a la dimensión del vector de estado:

$$\text{rango} \left(\begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix} \right) = n, \quad (3.52)$$

donde n representa la dimensión del vector de estado del sistema.

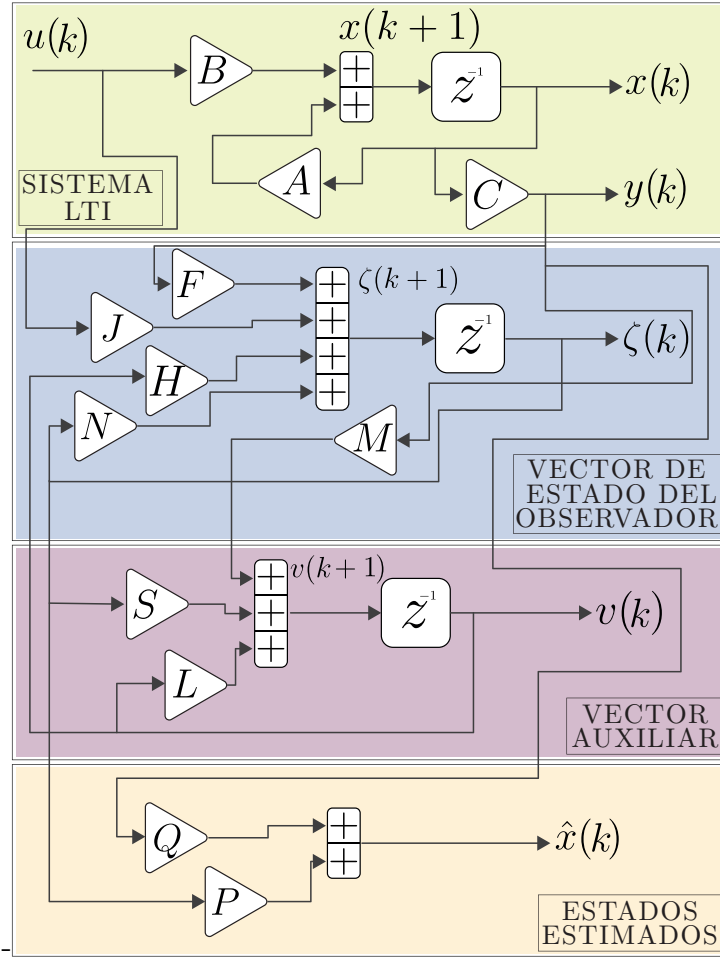


Fig. 3.15. Diagrama del observador dinámico generalizado.

3.7. Observadores para diagnóstico de fallas

En sistemas dinámicos, la presencia de fallas en sensores o actuadores puede comprometer gravemente el desempeño o incluso la estabilidad del sistema de control. Frente a este desafío, los observadores desempeñan un papel clave al permitir no solo la reconstrucción de estados no medidos, sino también la detección, el aislamiento y la estimación de fallas. Esta sección presenta dos enfoques complementarios: observadores orientados a la detección y aislamiento de fallas, y observadores diseñados para la estimación de su magnitud.

3.7.1. Observadores para la detección y el aislamiento de fallas

Una de las estrategias más empleadas en el diagnóstico de fallas es el uso de **bancos de observadores**. Estos consisten en múltiples observadores, cada uno diseñado para monitorear un modo particular de operación o un tipo específico de falla. La detección de fallas se basa en el análisis de las *señales residuales*, definidas como la diferencia entre la salida medida y la estimada por cada observador.

$$r_i(k) = y(k) - \hat{y}_i(k). \quad (3.53)$$

Donde $r_i(k)$ es la señal residual generada por el observador i del banco. Algunos ejemplos de los esquemas de bancos de observadores más utilizados son:

- **Banco estructurado:** cada observador está diseñado para ser sensible a un subconjunto específico de fallas, mientras es insensible a otras. Permite realizar *aislamiento* de fallas.
- **Banco redundante:** todos los observadores estiman el mismo conjunto de estados, pero utilizan diferentes modelos o configuraciones. Su análisis cruzado mejora la robustez del diagnóstico.
- **Banco jerárquico:** organiza observadores en niveles. En el primer nivel se realiza la detección general; en niveles superiores se identifican y aíslan fallas específicas.

La Figura 3.16 muestra un esquema genérico de banco de observadores con arquitectura paralela, en el cual cada observador genera una señal residual $r(k)$ en función de las salidas estimadas y reales del sistema. Este enfoque permite cubrir un amplio espectro de fallas en sensores y actuadores, y ha sido ampliamente aplicado tanto en sistemas lineales como no lineales.

La lógica de decisión que compara los residuos permite establecer qué tipo de falla está presente. Por ejemplo, si solo un residual $r_k(k)$ es significativamente distinto de cero, se infiere que la falla afecta el canal para el cual el observador k no es sensible.

3.7.2. Observadores para la estimación de fallas

A diferencia de los esquemas de detección, donde se busca únicamente generar un indicador de falla, los observadores de estimación intentan **reconstruir explícitamente la señal de falla o**

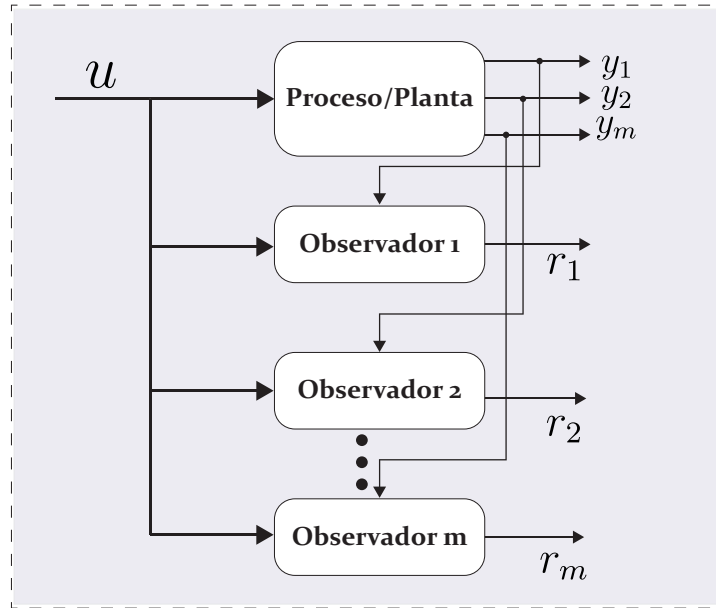


Fig. 3.16. Esquema general de un banco de observadores para detección y aislamiento de fallas.

ataque, lo cual es clave para sistemas con capacidad de control tolerante a fallas (FTC).

Para este propósito, se utilizan estructuras observadoras extendidas que modelan la falla como una entrada desconocida, pero estructurada. Una de las configuraciones más utilizadas en la literatura es la mostrada en la Figura 3.17, donde se incluyen las trayectorias del sistema nominal, el error de estimación y la dinámica auxiliar que permite identificar la magnitud del ataque o falla.

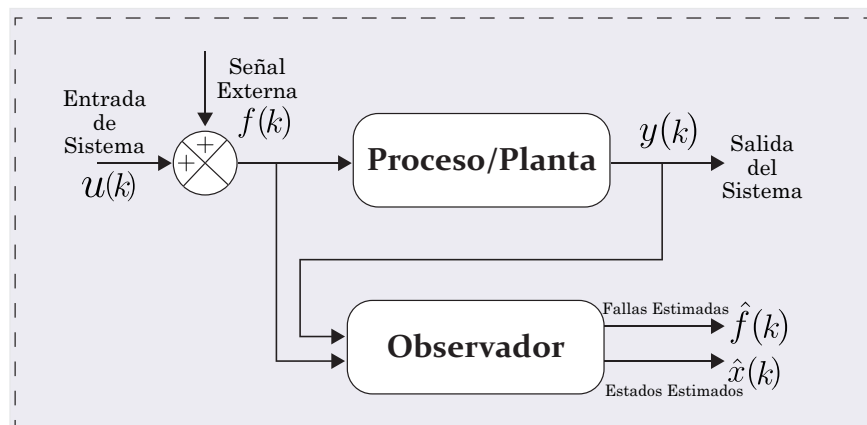


Fig. 3.17. Esquema conceptual de un observador con estimación directa del comportamiento de la falla.

Una estructura matemática para este tipo de observadores se define como:

$$\zeta(k+1) = N\zeta(k) + Hv(k) + Fy(k) + Ju(k), \quad (3.54)$$

$$v(k+1) = S\zeta(k) + Lv(k) + My(k), \quad (3.55)$$

$$\hat{x}(k) = P\zeta(k) + Qy(k), \quad (3.56)$$

$$\hat{f}(k) = K_f\zeta(k), \quad (3.57)$$

donde $\hat{f}(k)$ representa la estimación del comportamiento de la falla. Este tipo de esquema es adecuado cuando la dinámica de la falla es desconocida pero suficientemente lenta, y permite su inclusión como un estado adicional que puede observarse mediante técnicas de diseño como LMIs o control robusto H_∞ .

Cuando se trabaja con representaciones Takagi-Sugeno o LPV, esta estructura puede adaptarse para que las matrices dependan de variables de programación $\rho(k)$, ampliando la capacidad del observador para capturar regímenes dinámicos variables:

$$\hat{x}(k+1) = A(\rho(k))\hat{x}(k) + B(\rho(k))u(k) + L(\rho(k))(y(k) - C(\rho(k))\hat{x}(k)). \quad (3.58)$$

Este tipo de esquemas ha demostrado efectividad en la estimación de fallas.

3.8. Teoría de la estabilidad y las LMI

En el contexto del análisis y diseño de sistemas de control, una de las propiedades más importantes a garantizar es la estabilidad. La estabilidad de un sistema determina si sus respuestas ante perturbaciones o condiciones iniciales se mantienen acotadas o tienden a cero con el tiempo. Para estudiar esta propiedad, una de las herramientas más utilizadas es la función de Lyapunov.

3.8.1. Estabilidad mediante funciones de Lyapunov

Sea un sistema dinámico descrito por:

$$x(k+1) = Ax(k). \quad (3.59)$$

Donde $x(k) \in \mathbb{R}^n$ es el vector de estados del sistema en tiempo discreto. El sistema se dice *estable* si existe una función de Lyapunov $V(x) : \mathbb{R}^n \rightarrow \mathbb{R}$, que sea positiva definida y cuya variación en el tiempo discreto sea negativa definida. Una forma común de elegir $V(x)$ es mediante la siguiente función cuadrática:

$$V(x) = x^T P x, \quad P = P^T > 0. \quad (3.60)$$

La condición de estabilidad en tiempo discreto se expresa como:

$$\Delta V(x(k)) = V(x(k+1)) - V(x(k)) < 0, \quad \forall x(k) \neq 0. \quad (3.61)$$

Si se cumple que $A^T P + P A < 0$, entonces el sistema es asintóticamente estable. Esta condición puede expresarse como una LMI.

3.8.2. Planteamiento de condiciones de estabilidad con LMIs

Las **LMIs** (*Linear Matrix Inequalities*) permiten expresar condiciones de estabilidad, controlabilidad u observabilidad como problemas convexos que pueden resolverse mediante herramientas de optimización numérica. En particular, para garantizar estabilidad, la condición:

$$A^T P + P A < 0, \quad P > 0, \quad (3.62)$$

es una LMI que se puede resolver para encontrar una matriz P que certifique estabilidad. Este enfoque es especialmente útil cuando se trabaja con sistemas inciertos, difusos o con variaciones paramétricas (por ejemplo, en sistemas Takagi-Sugeno o LPV).

3.9. Controladores

Los controladores son componentes fundamentales en los sistemas dinámicos, ya que permiten modificar el comportamiento de un sistema con el objetivo de alcanzar una respuesta deseada. A través del diseño adecuado de leyes de control, es posible influir en las variables internas del sistema para que este cumpla estos criterios de desempeño, como estabilidad, seguimiento de referencias y rechazo de perturbaciones. En general, un sistema de control se compone de la planta a controlar, sensores, actuadores y uno o varios controladores que determinan las acciones correctivas basadas

en la información disponible del sistema.

Esta sección presenta los principios básicos de los controladores clásicos, describiendo la diferencia entre estructuras de lazo abierto y lazo cerrado, e introduce posteriormente el diseño de controladores basados en observadores, útiles cuando no se dispone de mediciones completas del sistema.

3.9.1. Estructura de sistemas de control

En términos generales, los sistemas de control se clasifican en dos categorías principales: sistemas de lazo abierto y sistemas de lazo cerrado. La diferencia esencial entre ambos radica en el uso de la retroalimentación.

En un sistema de lazo abierto, la acción de control se aplica sin considerar la salida del sistema. Como se muestra en la Figura 3.18, este tipo de arquitectura no incorpora un mecanismo de retroalimentación, por lo que la precisión del sistema depende en gran medida de la calibración del controlador. Aunque puede ser eficaz bajo condiciones conocidas y estables, su desempeño se ve comprometido ante perturbaciones o cambios en la dinámica de la planta.

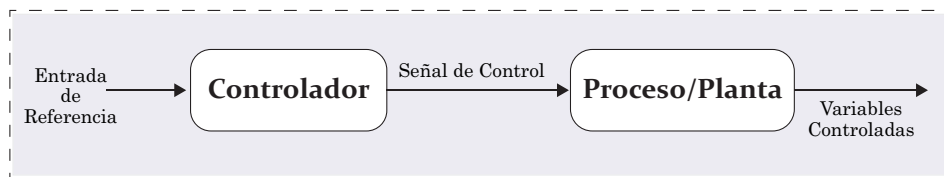


Fig. 3.18. Diagrama a bloques de un sistema de control en lazo abierto.

Por otro lado, en un sistema de lazo cerrado, la salida se compara con una señal de referencia y la diferencia, denominada error, es utilizada por el controlador para ajustar la entrada al sistema. Como se ilustra en la Figura 3.19, esta configuración mejora significativamente la robustez del sistema frente a perturbaciones y variaciones no modeladas.

3.9.2. Controladores Proporcional, PI y PID

Los controladores clásicos son ampliamente utilizados en ingeniería de control debido a su simplicidad, robustez y efectividad en una variedad de procesos industriales. Los controladores más co-

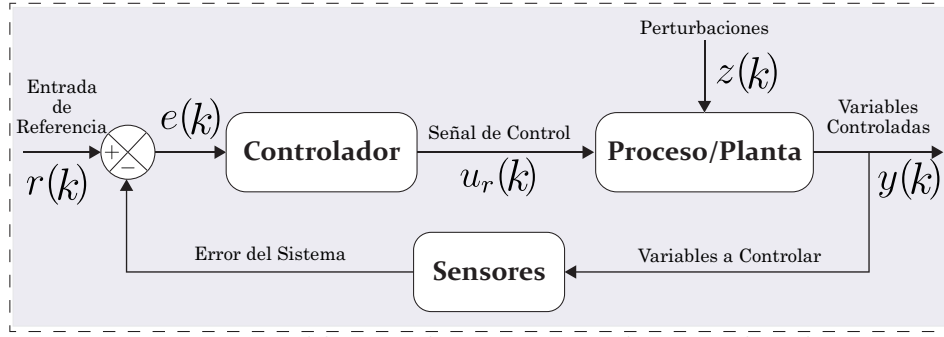


Fig. 3.19. Diagrama a bloques de un sistema de control en lazo cerrado.

munes son el proporcional (P), proporcional-integral (PI) y proporcional-integral-derivativo (PID), cada uno con características particulares que los hacen adecuados según las condiciones del sistema.

Controlador Proporcional (P)

El controlador proporcional genera una acción de control directamente proporcional al error $e(k)$, definido como la diferencia entre la señal de referencia $r(k)$ y la salida del sistema $y(k)$. Su ecuación de operación es:

$$u(k) = k_p e(k) = k_p (r(k) - y(k)). \quad (3.63)$$

Donde k_p es la ganancia proporcional. Este tipo de controlador mejora la velocidad de respuesta, pero puede dejar un error en régimen permanente. La Figura 3.20 ilustra su funcionamiento.

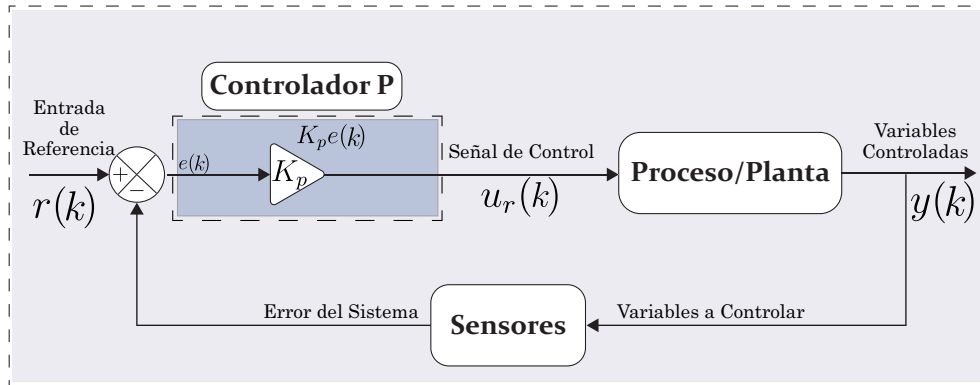


Fig. 3.20. Esquema de un controlador proporcional (P).

Controlador Proporcional-Integral (PI)

El controlador PI en tiempo discreto se utiliza el operador de retardo z^{-1} . En este caso, la expresión del controlador se escribe como:

$$u(k) = K_P e(k) + K_I \cdot \frac{T_s}{1 - z^{-1}} e(k), \quad (3.64)$$

donde K_P es la ganancia proporcional, K_I es la ganancia integral, T_s es el tiempo de muestreo, z^{-1} representa un retardo de una muestra en tiempo discreto.

Esta formulación permite implementar el controlador PI utilizando herramientas de análisis en el dominio z y facilita su análisis en sistemas de control digitales.

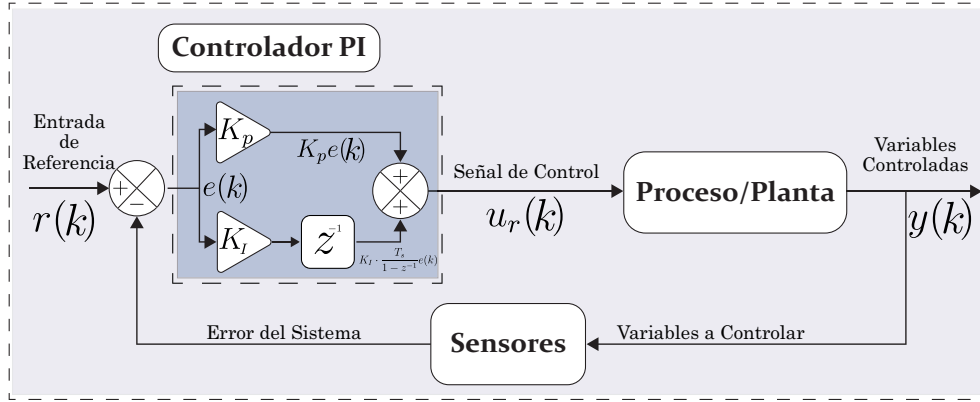


Fig. 3.21. Esquema de un controlador proporcional-integral (PI).

Controlador Proporcional-Integral-Derivativo (PID)

El controlador PID en tiempo discreto extiende la estructura PI mediante un término derivativo que considera la variación del error entre instantes de muestreo consecutivos. Su expresión general en tiempo discreto es:

$$u(k) = k_P e(k) + k_I T_s \sum_{i=0}^k e(i) + k_D \frac{e(k) - e(k-1)}{T_s}. \quad (3.65)$$

Donde $u(k)$ es la señal de control en el instante k , $e(k) = r(k) - y(k)$ es el error del sistema, T_s es el tiempo de muestreo, k_P , k_I , y k_D son las ganancias proporcional, integral y derivativa, respectivamente.

El término derivativo $\frac{e(k)-e(k-1)}{T_s}$ permite anticiparse a los cambios del error, mejorando el comportamiento transitorio del sistema. La Figura 3.22 presenta su arquitectura adaptada al dominio discreto.

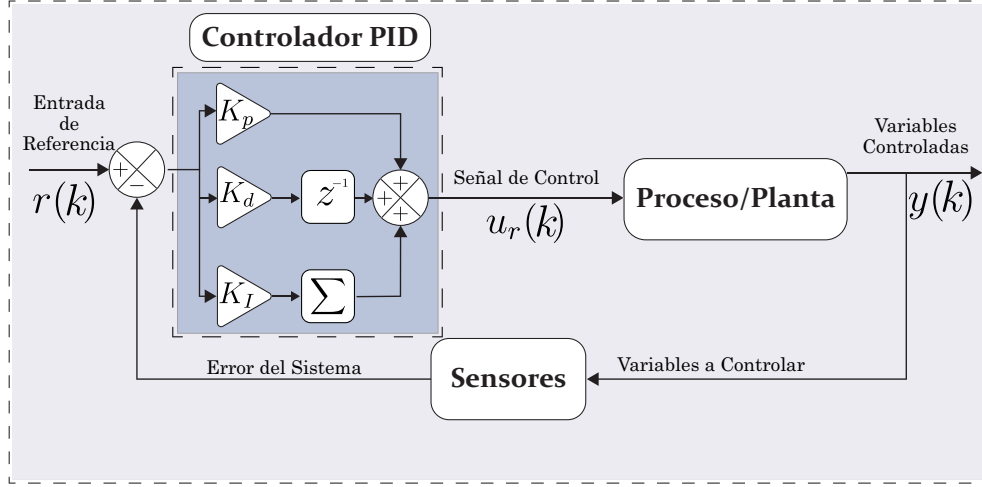


Fig. 3.22. Esquema de un controlador proporcional-integral-derivativo (PID).

3.9.3. Controladores basados en observadores

En sistemas donde no se dispone de todas las variables de estado para la retroalimentación directa, es común emplear observadores como herramienta para estimar dichas variables y cerrar el lazo de control. Esta estrategia, conocida como **control basado en observadores**, permite diseñar controladores robustos que utilizan las estimaciones del estado para generar la señal de control.

La estructura general de un controlador basado en observadores consiste en un observador que estima el estado del sistema a partir de las entradas y salidas medidas, y un controlador que utiliza dicha estimación para computar la acción de control.

$$u(k) = K\hat{x}(k) + k_r r(k), \quad (3.66)$$

donde $\hat{x}(k)$ es la estimación del estado obtenida mediante un observador (por ejemplo, tipo Luenberger o dinámico generalizado), K es la matriz de ganancia del controlador y k_r es una ganancia que permite cumplir con una referencia $r(k)$.

Este enfoque es especialmente útil en sistemas donde la implementación de sensores adicionales es costosa o técnicamente inviable. Además, permite aplicar técnicas avanzadas como control óptimo, H_∞ , y diseño mediante LMIs en conjunto con esquemas de observación.

La Figura 3.23 muestra un esquema general de un sistema de control en lazo cerrado basado en observadores.

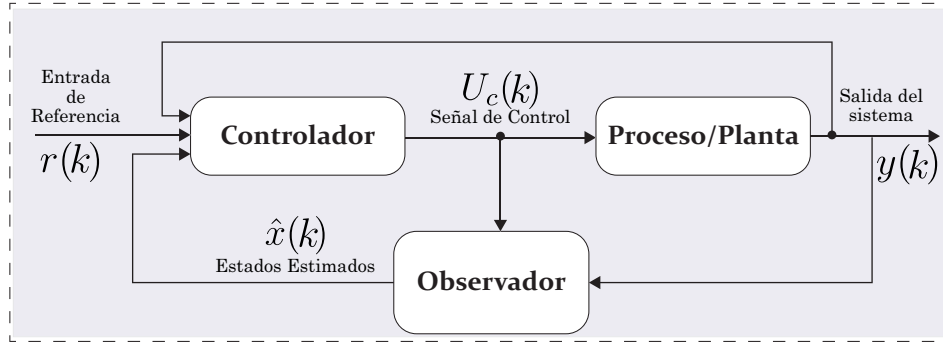


Fig. 3.23. Esquema general de un controlador basado en observadores.

3.10. Control tolerante a ataques

En los sistemas ciberfísicos, la estabilidad, la controlabilidad y la seguridad son aspectos fundamentales, especialmente en entornos expuestos a posibles ataques maliciosos. Para hacer frente a esta problemática, se han desarrollado esquemas de control tolerante a ataques, los cuales combinan la estimación del comportamiento del ataque con observadores robustos, permitiendo mitigar sus efectos y garantizar el funcionamiento seguro del sistema.

El principio básico del **control tolerante a ataques** radica en utilizar la información provista por un observador que estima tanto el estado del sistema como las señales de ataque. Con base en estas estimaciones, se define una ley de control que compensa el efecto del ataque sobre el sistema, manteniendo la estabilidad y el rendimiento deseado.

La ley de control $u_a(k)$ se formula como:

$$u_a(k) = K(x(k) - \hat{x}_a(k)) + u(k) - \hat{a}(k), \quad (3.67)$$

donde $x(k)$ es el vector de estado real del sistema, $\hat{x}_a(k)$ es la estimación del estado obtenida por el observador, $u(k)$ es la señal de control generada en ausencia de ataque, $\hat{a}(k)$ representa la estimación del vector de ataque.

Este enfoque permite una adaptación activa del controlador ante condiciones anómalas, utilizando la diferencia entre el estado real y el estimado para generar una acción correctiva. La señal de ataque $\hat{a}(k)$, al ser estimada, puede ser compensada directamente en la señal de control, lo que mejora la resiliencia del sistema ante manipulaciones externas.

Para validar el desempeño del esquema, se utiliza un modelo de referencia libre de ataques, el cual actúa como punto de comparación. Así, se evalúa la desviación del comportamiento real del sistema frente al deseado, permitiendo realizar ajustes dinámicos en la ley de control con el fin de restablecer la estabilidad.

En la Figura 3.24 se muestra un esquema general de la estructura del controlador tolerante al ataque. En este diagrama se representa la interacción entre el sistema real, el observador y el lazo de control corregido mediante las estimaciones del ataque.

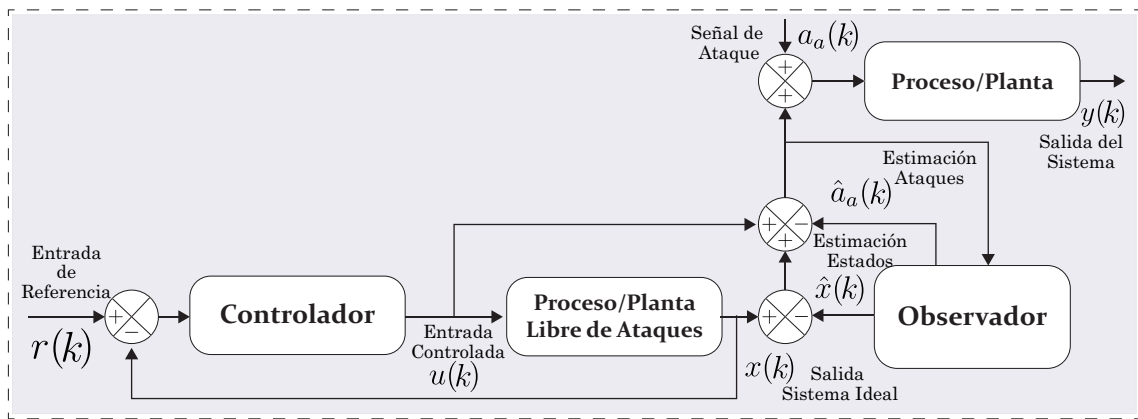


Fig. 3.24. Esquema de un controlador tolerante al ataque mediante compensación de la estimación del ataque.

Cabe mencionar que este tipo de controladores suele diseñarse en escenarios donde se modelan

ataques a actuadores como señales externas $a_a(k)$ que alteran directamente la entrada del sistema. Este modelo es útil para representar ataques del tipo DDA, DoS o RDI, los cuales pueden afectar severamente el desempeño del sistema si no son debidamente compensados.

El diseño efectivo de controladores tolerantes a ataques requiere integrar metodologías de observación, técnicas de control robusto y herramientas de análisis de estabilidad, como las desigualdades matriciales lineales, lo que permite garantizar el cumplimiento de especificaciones de seguridad y desempeño en presencia de perturbaciones adversas.

3.11. Métricas de resiliencia

En el contexto del control automático, evaluar la resiliencia de un sistema ante fallas o ataques es fundamental para garantizar su funcionamiento seguro y confiable. Las métricas de resiliencia permiten cuantificar el desempeño del controlador cuando el sistema es perturbado por eventos no deseados, tales como en sensores, actuadores o ciberataques.

Evaluación de la resistencia ante esquemas de ataque

El proceso de evaluación de la resistencia de un sistema de control implica los siguientes pasos:

1. **Identificación de posibles ataques:** Se deben considerar diferentes tipos de ataque de engaño de datos, denegación de servicio de datos o inserción de dato falso.
2. **Definición de escenarios de ataque:** Se plantea cuándo y cómo se ejecutan los ataques, y cuál es su impacto esperado.
3. **Selección de métricas de evaluación:** Se definen criterios específicos para cuantificar la respuesta del controlador frente a ataques.
4. **Simulación del sistema bajo condiciones adversas:** Se evalúa el desempeño del sistema con y sin mecanismos de defensa.
5. **Análisis de resultados:** Se analizan los resultados para validar si el sistema conserva sus propiedades deseadas.

Criterios comunes para evaluar la resistencia

- **Tiempo de detección del ataque:** Mide la rapidez con la que se identifica la ocurrencia de un ataque.
- **Capacidad de recuperación:** Evalúa la habilidad del sistema para estabilizarse tras una perturbación.
- **Precisión de la respuesta:** Determina cuán cercano se mantiene el sistema al comportamiento esperado posterior al ataque.
- **Impacto en el desempeño:** Cuantifica la degradación temporal de las variables de interés.
- **Eficiencia energética:** Considera el consumo de recursos antes, durante y después del evento adverso.

La evaluación de estas métricas permite comparar diferentes estrategias de control y mejorar el diseño de controladores tolerantes a fallas o ataques.

3.12. Conclusiones del capítulo

En este capítulo se presentó el marco teórico necesario para comprender el diseño y análisis de sistemas ciberfísicos bajo condiciones de operación normales y adversas, particularmente en presencia de ataques y fallas. Se introdujeron los principales conceptos relacionados con la arquitectura de estos sistemas, así como los distintos tipos de ataques que pueden comprometer su seguridad, tales como los de ataque de engaño de datos, denegación de servicio e inserción de datos aleatorios.

Posteriormente, se analizaron distintos sistemas dinámicos que sirven como casos de estudio, incluyendo el sistema de tanques interconectados, el vehículo y el modelo de glucosa-insulina. Estos sistemas ejemplifican contextos reales donde las metodologías desarrolladas pueden aplicarse.

Asimismo, se abordaron las estrategias de modelado para representar comportamientos no lineales mediante teorías como Takagi-Sugeno y LPV, herramientas esenciales para el diseño de observadores y controladores en entornos variables y complejos. A partir de estos modelos, se desarrolló el análisis de observadores como instrumentos clave para la estimación de estados, ataques y fallas,

clasificándolos según su estructura y función.

La sección sobre diagnóstico de fallas, el cual es considerado como la base para la teoría de diagnóstico de ataques, estableció dos enfoques fundamentales: los observadores diseñados para la detección y aislamiento mediante bancos estructurados, y aquellos orientados a la estimación directa del comportamiento de la falla. Esta diferenciación es crucial para elegir el tipo de herramienta adecuada, dependiendo del nivel de información requerido por el sistema de control.

Se introdujeron también los fundamentos de la teoría de la estabilidad y su formulación mediante funciones de Lyapunov y desigualdades matriciales lineales (LMIs), pilares matemáticos que sustentan tanto el diseño de observadores como de controladores robustos.

En cuanto a los controladores, se explicó la evolución desde los enfoques clásicos P, PI y PID hasta los esquemas avanzados basados en observadores. Finalmente, se desarrolló el concepto de control tolerante al ataque, destacando la necesidad de incorporar mecanismos de detección, compensación y resiliencia frente a perturbaciones intencionadas.

Este capítulo sienta las bases teóricas sobre las cuales se construirá la metodología propuesta en los capítulos siguientes. El conocimiento aquí consolidado permitirá abordar el diseño e implementación de observadores dinámicos y controladores resilientes aplicados a sistemas ciberfísicos discretos con representación Takagi-Sugeno.

Capítulo 4

Modelado de casos prácticos

4.1. Representación Takagi-Sugeno del sistema de tanques interconectados

En esta sección se describe el proceso de modelado del sistema de tres tanques interconectados, el cual es ampliamente utilizado como caso de estudio en la literatura relacionada con el control de procesos y el diseño de esquemas de diagnóstico. Dicho sistema presenta una dinámica no lineal asociada al flujo entre tanques y drenajes, lo cual lo convierte en un excelente candidato para representar en términos Takagi-Sugeno. Esta representación facilita el análisis, el diseño de observadores y la aplicación de técnicas de control tolerantes a fallas o ataques. A continuación, se aborda la simulación del modelo no lineal, su aproximación mediante un modelo Takagi-Sugeno y su correspondiente discretización para fines de implementación digital.

4.1.1. Simulación de modelos no lineales

El modelo no lineal del sistema de tres tanques interconectados se obtiene aplicando el principio de conservación de masa a cada tanque, junto con la ley de Torricelli para describir los caudales generados por diferencias de altura entre tanques. Sea $h_1(k)$, $h_2(k)$ y $h_3(k)$ la altura del líquido (nivel) en los tanques 1, 2 y 3, respectivamente, medido en metros. Se asume que los tres tanques tienen la misma sección transversal constante, denotada por A (en m^2), y que el líquido es incompresible.

Existen dos flujos de entrada externos: $Q_1(k)$, que alimenta el tanque 1, y $Q_2(k)$, que alimenta el tanque 2. Ambos flujos están en m^3/s y pueden ser controlados, por ejemplo, mediante bombas.

El sistema presenta conexiones hidráulicas entre tanques: el tanque 1 vierte hacia el tanque 3, el tanque 3 vierte hacia el tanque 2, y el tanque 2 descarga al ambiente. Estos intercambios están regulados por válvulas u orificios de área conocida.

Aplicando un balance de masa en cada tanque (entrada menos salida), se obtienen las siguientes ecuaciones diferenciales en tiempo discreto que describen la evolución de los niveles:

$$h_1(k+1) = h_1(k) + \frac{T_s}{A} (Q_1(k) - Q_{13}(k)), \quad (4.1)$$

$$h_2(k+1) = h_2(k) + \frac{T_s}{A} (Q_2(k) + Q_{32}(k) - Q_{20}(k)), \quad (4.2)$$

$$h_3(k+1) = h_3(k) + \frac{T_s}{A} (Q_{13}(k) - Q_{32}(k)). \quad (4.3)$$

donde $Q_{ij}(k)$ representa el caudal desde el tanque i hacia el tanque j , y $Q_{i0}(k)$ representa el caudal desde el tanque i hacia el ambiente. En particular:

- Q_{13} es el flujo entre los tanques 1 y 3,
- Q_{32} es el flujo entre los tanques 3 y 2,
- Q_{20} es el drenaje del tanque 2 al ambiente.

Los caudales entre tanques se calculan aplicando la ley de Torricelli, que establece que la velocidad de vaciado de un líquido por un orificio es proporcional a la raíz cuadrada de la altura de la columna de fluido que lo genera. En términos de flujo volumétrico, esto se expresa como:

$$\begin{aligned} Q_{13}(k) &= a_1 S_{13} \operatorname{sgn}(h_1(k) - h_3(k)) \sqrt{2g |h_1(k) - h_3(k)|}, \\ Q_{32}(k) &= a_3 S_{32} \operatorname{sgn}(h_3(k) - h_2(k)) \sqrt{2g |h_3(k) - h_2(k)|}, \\ Q_{20}(k) &= a_2 S_{20} \sqrt{2g |h_2(k)|}. \end{aligned} \quad (4.4)$$

En esta representación se tiene a g la cual es la aceleración gravitacional, S_{ij} representa el área efectiva del orificio de conexión entre tanques i y j y a_i es el coeficiente de descarga asociado al orificio correspondiente.

Estas expresiones suponen que $h_i(k) > h_j(k)$, es decir, que el flujo se produce de manera descendente por gravedad. En caso contrario, el flujo cambiaría de sentido; no obstante, bajo condiciones operativas normales, se garantiza que las diferencias de nivel mantengan un flujo unidireccional.

Para simplificar la notación y uniformar la representación del sistema en espacio de estados, se define el vector de estados como:

$$x(k) = \begin{bmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \end{bmatrix} = \begin{bmatrix} h_1(k) \\ h_2(k) \\ h_3(k) \end{bmatrix}, \quad (4.5)$$

y se hace un cambio de variable de las ecuaciones anteriores en función de las variables $x_i(k)$, considerando también una parametrización más compacta donde se agrupan las constantes físicas. Así, se obtiene el siguiente sistema de ecuaciones no lineales en forma explícita:

$$\begin{aligned} x_1(k+1) &= x_1(k) + T_s \left(-\frac{a_{13}}{S_a} \operatorname{sgn}(x_1(k) - x_3(k)) \sqrt{2g|x_1(k) - x_3(k)|} + \frac{1}{S_a} Q_1(k) \right), \\ x_2(k+1) &= x_2(k) + T_s \left(-\frac{a_2}{S_a} \sqrt{2g|x_2(k)|} + \frac{a_{32}}{S_a} \operatorname{sgn}(x_3(k) - x_2(k)) \sqrt{2g|x_3(k) - x_2(k)|} + \frac{1}{S_a} Q_2(k) \right), \\ x_3(k+1) &= x_3(k) + T_s \left(\frac{a_{13}}{S_a} \operatorname{sgn}(x_1(k) - x_3(k)) \sqrt{2g|x_1(k) - x_3(k)|} - \frac{a_{32}}{S_a} \operatorname{sgn}(x_3(k) - x_2(k)) \sqrt{2g|x_3(k) - x_2(k)|} \right). \end{aligned} \quad (4.6)$$

Donde ahora $x_i(k)$ representa el nivel del tanque i en metros, $a_{13} = a_1 S_{13}$, $a_{32} = a_3 S_{32}$, y $a_2 = a_2 S_{20}$, S_a es el área transversal del tanque, el cual se considera como constante para todos y $Q_1(k), Q_2(k)$ son los flujos de entrada.

A partir del conjunto de ecuaciones diferenciales no lineales en (4.6), es posible expresar el sistema en su forma general de espacio de estados no lineal en tiempo discreto:

$$\begin{aligned} x(k+1) &= f(x(k)) + Bu(k), \\ y(k) &= Cx(k), \end{aligned} \quad (4.7)$$

$$\text{donde: } x(k) = \begin{bmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \end{bmatrix}, \quad u(k) = \begin{bmatrix} Q_1(k) \\ Q_2(k) \end{bmatrix}, \quad y(k) = \begin{bmatrix} x_1(k) \\ x_2(k) \\ x_3(k) \end{bmatrix},$$

$$B = \frac{1}{S_a} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad C = I_3,$$

y la función no lineal $f(x(k)) \in \mathbb{R}^3$ captura las dinámicas internas del sistema:

$$f(x(k)) = \begin{bmatrix} -a_{13}\sqrt{2g(x_1(k) - x_3(k))} \\ -a_{23}\sqrt{2gx_2(k)} + a_{32}\sqrt{2g(x_3(k) - x_2(k))} \\ +a_{13}\sqrt{2g(x_1(k) - x_3(k))} - a_{32}\sqrt{2g(x_3(k) - x_2(k))} \end{bmatrix}. \quad (4.8)$$

En esta forma, el sistema está listo para su aproximación difusa mediante técnicas Takagi-Sugeno, en las que las no linealidades serán interpoladas por múltiples modelos lineales locales activados por funciones de pertenencia. El desarrollo completo de esta representación y su posterior discretización se detallan en las siguientes secciones.

4.1.2. Modelo Takagi-Sugeno

El sistema no lineal de tres tanques interconectados presenta dinámicas acopladas con fuertes no linealidades inducidas por los términos de raíz cuadrada presentes en los caudales de salida entre tanques. Para representar este comportamiento de manera tratable para análisis y diseño de controladores, se adopta una aproximación difusa de tipo Takagi-Sugeno, basada en la interpolación de modelos lineales locales activados por funciones de pertenencia dependientes del estado.

Las no linealidades provienen de los 3 flujos, por lo tanto, para capturar estas no linealidades, se definen las siguientes variables de premisa:

$$\rho_1(k) = \frac{1}{\sqrt{x_1(k) - x_3(k)}}, \quad \rho_2(k) = \frac{1}{\sqrt{x_3(k) - x_2(k)}}, \quad \rho_3(k) = \frac{1}{\sqrt{x_2(k)}}. \quad (4.9)$$

Estas funciones representan la inversa de las raíces cuadradas de las diferencias de niveles que inducen los flujos Q_{13} , Q_{32} y Q_{20} , respectivamente. Estas variables se eligen porque reflejan el comportamiento dinámico no lineal del sistema y permiten aproximarlos mediante una colección finita de subsistemas lineales.

Para identificar los valores máximos y mínimos que pueden tomar estas variables de premisa dentro del rango operativo del sistema, se hace uso de los parámetros físicos descritos en la Tabla 4.1, extraídos de Li *y col.* (2018), los cuales se utilizan como base para simular el sistema:

Tabla 4.1. Parámetros del sistema.

Parámetro	Símbolo	Valor	Unidades
Área del tanque	S_a	0.0154	m^2
Área del orificio	S_n	5×10^{-5}	m^2
Gravedad	g	9.8	m/s^2
Flujo de entrada 1	Q_1	0.02	m^3/s
Flujo de entrada 2	Q_2	0.03	m^3/s
Altura máxima del tanque	$H_{\max}$	0.8	m
Coef. descarga tanque 1	az_1	0.46	–
Coef. descarga tanque 2	az_2	0.58	–
Coef. descarga tanque 3	az_3	0.48	–

Para la obtención de los rangos de variación de las variables de premisa se definió un escenario de prueba utilizando los parámetros de la Tabla 4.1. En particular, se consideraron como entradas dos flujos de agua: $Q_1 = 0.02 m^3/s$ aplicado al tanque 1 y $Q_2 = 0.03 m^3/s$ aplicado al tanque 2. Estos valores se seleccionaron de acuerdo con condiciones nominales de operación reportadas en la literatura y permiten garantizar que los niveles de líquido se mantengan dentro del rango físico de los tanques, es decir, entre 0 y $H_{\max} = 0.8 m$. Bajo este escenario, las variables premisa $\rho_1(k)$, $\rho_2(k)$ y $\rho_3(k)$ evolucionan dentro de regiones acotadas, lo que facilita la identificación de sus valores extremos y la construcción de las funciones de pertenencia correspondientes al modelo Takagi–Sugeno.

Con base en estos valores, se obtienen los rangos de operación de las variables premisas:

$$\begin{aligned} \rho_1(k) : \quad \underline{\rho}_1 &= \min \left\{ \frac{1}{\sqrt{x_1 - x_3}} \right\} = 1.5329, \\ \bar{\rho}_1 &= \max \left\{ \frac{1}{\sqrt{x_1 - x_3}} \right\} = 1.9772, \end{aligned} \quad (4.10)$$

$$\begin{aligned} \rho_2(k) : \quad \underline{\rho}_2 &= \min \left\{ \frac{1}{\sqrt{x_3 - x_2}} \right\} = 2.2158, \\ \bar{\rho}_2 &= \max \left\{ \frac{1}{\sqrt{x_3 - x_2}} \right\} = 2.8030, \end{aligned} \quad (4.11)$$

$$\begin{aligned}\rho_3(k) : \quad \underline{\rho}_3 &= \min \left\{ \frac{1}{\sqrt{x_2}} \right\} = 1.7848, \\ \bar{\rho}_3 &= \max \left\{ \frac{1}{\sqrt{x_2}} \right\} = 2.0713.\end{aligned}\tag{4.12}$$

Una vez determinados los valores extremos, se definen las funciones de pertenencia lineales para cada variable de premisa, que permiten interpolar entre los modelos lineales locales. Estas funciones son:

$$n_0^1(\rho_1(k)) = \frac{\bar{\rho}_1 - \rho_1(k)}{\bar{\rho}_1 - \underline{\rho}_1}, \quad n_1^1(\rho_1(k)) = 1 - n_0^1(\rho_1(k)), \tag{4.13}$$

$$n_0^2(\rho_2(k)) = \frac{\bar{\rho}_2 - \rho_2(k)}{\bar{\rho}_2 - \underline{\rho}_2}, \quad n_1^2(\rho_2(k)) = 1 - n_0^2(\rho_2(k)), \tag{4.14}$$

$$n_0^3(\rho_3(k)) = \frac{\bar{\rho}_3 - \rho_3(k)}{\bar{\rho}_3 - \underline{\rho}_3}, \quad n_1^3(\rho_3(k)) = 1 - n_0^3(\rho_3(k)). \tag{4.15}$$

Al considerar que cada variable de premisa tiene dos conjuntos difusos (mínimo y máximo), el total de reglas de inferencia, $2^3 = 8$, las cuales se definen como:

$$\begin{aligned}\mu_1(\rho) &= n_0^1 n_0^2 n_0^3, & \mu_2(\rho) &= n_0^1 n_0^2 n_1^3, \\ \mu_3(\rho) &= n_0^1 n_1^2 n_0^3, & \mu_4(\rho) &= n_0^1 n_1^2 n_1^3, \\ \mu_5(\rho) &= n_1^1 n_0^2 n_0^3, & \mu_6(\rho) &= n_1^1 n_0^2 n_1^3, \\ \mu_7(\rho) &= n_1^1 n_1^2 n_0^3, & \mu_8(\rho) &= n_1^1 n_1^2 n_1^3.\end{aligned}$$

Subsecuentemente, se consideran las variables $\rho_1(k)$, $\rho_2(k)$ y $\rho_3(t)$, las cuales varían dentro de una región acotada $\rho(k) = [\underline{\rho}(k), \bar{\rho}(k)]$, donde $\underline{\rho}(k)$ y $\bar{\rho}(k)$ son los límites inferior y superior, respectivamente, de las no linealidades del sistema. En consecuencia, se obtienen las siguientes matrices del sistema que representan cada modelo local:

$$A(\rho(k)) = \begin{bmatrix} A_{11} & 0 & A_{13} \\ 0 & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}, \tag{4.16}$$

donde:

$$\begin{aligned}
A_{11} &= -\frac{az_1 S_n \sqrt{2g}}{S_a} \rho_1(k), & A_{13} &= \frac{az_1 S_n \sqrt{2g}}{S_a} \rho_1(k), \\
A_{22} &= -\frac{az_3 S_n \sqrt{2g}}{S_a} \rho_2(k) - \frac{az_2 S_n \sqrt{2g}}{S_a} \rho_3(k), & A_{23} &= \frac{az_3 S_n \sqrt{2g}}{S_a} \rho_2(k), \\
A_{31} &= \frac{az_1 S_n \sqrt{2g}}{S_a} \rho_1(k), & A_{32} &= \frac{az_3 S_n \sqrt{2g}}{S_a} \rho_2(k), \\
A_{33} &= -\frac{az_1 S_n \sqrt{2g}}{S_a} \rho_1(k) + \frac{az_3 g S_n}{S_a} \rho_2(k).
\end{aligned}$$

Las matrices locales A_i se obtienen evaluando la matriz $A(\rho(k))$ en los extremos de cada variable de premisa. Donde:

$$\begin{aligned}
A_1 &= A(\underline{\rho}_1, \underline{\rho}_2, \underline{\rho}_3), & A_2 &= A(\underline{\rho}_1, \underline{\rho}_2, \bar{\rho}_3), & A_3 &= A(\underline{\rho}_1, \bar{\rho}_2, \underline{\rho}_3), \\
A_4 &= A(\underline{\rho}_1, \bar{\rho}_2, \bar{\rho}_3), & A_5 &= A(\bar{\rho}_1, \underline{\rho}_2, \underline{\rho}_3), & A_6 &= A(\bar{\rho}_1, \underline{\rho}_2, \bar{\rho}_3), \\
A_7 &= A(\bar{\rho}_1, \bar{\rho}_2, \underline{\rho}_3), & A_8 &= A(\bar{\rho}_1, \bar{\rho}_2, \bar{\rho}_3).
\end{aligned}$$

Cada modelo local de A está definido de la siguiente manera:

$$A_1(\rho(t)) = \begin{bmatrix} 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) & 0 & -\frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) \\ 0 & 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_3(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) \\ \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) & 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) \end{bmatrix}, \quad (4.17)$$

$$A_2(\rho(k)) = \begin{bmatrix} 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) & 0 & -\frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) \\ 0 & 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_3(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) \\ \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) & 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) \end{bmatrix}, \quad (4.18)$$

$$A_3(\rho(k)) = \begin{bmatrix} 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) & 0 & -\frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) \\ 0 & 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_3(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \\ \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) & 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \end{bmatrix}, \quad (4.19)$$

$$A_4(\rho(k)) = \begin{bmatrix} 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) & 0 & -\frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) \\ 0 & 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_3(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \\ \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) & 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_1(k) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \end{bmatrix}, \quad (4.20)$$

$$A_5(\rho(k)) = \begin{bmatrix} 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) & 0 & -\frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) \\ 0 & 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_3(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) \\ \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) & 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \underline{\rho}_2(k) \end{bmatrix}, \quad (4.21)$$

$$A_6(\rho(k)) = \begin{bmatrix} 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) & 0 & -\frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) \\ 0 & 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_3(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \\ \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) & 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \end{bmatrix}, \quad (4.22)$$

$$A_7(\rho(k)) = \begin{bmatrix} 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) & 0 & -\frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) \\ 0 & 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_3(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \\ \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) & 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \end{bmatrix}, \quad (4.23)$$

$$A_8(\rho(k)) = \begin{bmatrix} 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) & 0 & -\frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) \\ 0 & 1 - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) - \frac{az_2 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_3(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \\ \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) & \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) & 1 - \frac{az_1 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_1(k) - \frac{az_3 S_n T_d \sqrt{2g}}{S_a} \bar{\rho}_2(k) \end{bmatrix}. \quad (4.24)$$

Donde cada matriz A_i se evalúa sustituyendo los valores extremos según:

$$\begin{aligned} \rho_1 &= 1.5329, & \bar{\rho}_1 &= 1.9772, \\ \rho_2 &= 2.2158, & \bar{\rho}_2 &= 2.8030, \\ \rho_3 &= 1.7848, & \bar{\rho}_3 &= 2.0713. \end{aligned}$$

Obteniendo:

$$\begin{aligned} A_1 &= \begin{bmatrix} -0.0127 & 0 & 0.0127 \\ 0 & -0.0311 & 0.0173 \\ 0.0127 & 0.0173 & -0.0300 \end{bmatrix}, & A_2 &= \begin{bmatrix} -0.0127 & 0 & 0.0127 \\ 0 & -0.0639 & 0.0173 \\ 0.0127 & 0.0173 & -0.0300 \end{bmatrix} \\ A_3 &= \begin{bmatrix} -0.0127 & 0 & 0.0127 \\ 0 & -0.1055 & 0.0917 \\ 0.0127 & 0.0917 & -0.1044 \end{bmatrix}, & A_4 &= \begin{bmatrix} -0.0127 & 0 & 0.0127 \\ 0 & -0.1383 & 0.0917 \\ 0.0127 & 0.0917 & -0.1044 \end{bmatrix} \\ A_5 &= \begin{bmatrix} -0.0608 & 0 & 0.0608 \\ 0 & -0.0311 & 0.0173 \\ 0.0608 & 0.0173 & -0.0781 \end{bmatrix}, & A_6 &= \begin{bmatrix} -0.0127 & 0 & 0.0127 \\ 0 & -0.0311 & 0.0173 \\ 0.0127 & 0.0173 & -0.0300 \end{bmatrix} \\ A_7 &= \begin{bmatrix} -0.0608 & 0 & 0.0608 \\ 0 & -0.1055 & 0.0917 \\ 0.0608 & 0.0917 & -0.1525 \end{bmatrix}, & A_8 &= \begin{bmatrix} -0.0608 & 0 & 0.0608 \\ 0 & -0.1383 & 0.0917 \\ 0.0608 & 0.0917 & -0.1525 \end{bmatrix}. \end{aligned}$$

Finalmente, el modelo completo del sistema T-S que representa la dinámica del modelo (3.10) para obtener las matrices A_i se expresa como:

$$x(k+1) = [\mu_1(\rho(k))A_1 + \cdots + \mu_8(\rho(k))A_8]x(k) + Bu(k) \quad (4.25)$$

Donde B y C son constantes, ya que las no linealidades solo afectan la matriz A . Por lo tanto:

$$B = \begin{bmatrix} 64.9351 & 0 \\ 0 & 64.9351 \\ 0 & 0 \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

El modelo del sistema de tres tanques interconectados puede ser escrito como sigue:

$$\begin{aligned} x(k+1) &= \sum_{i=1}^8 \mu_i(\rho(k)) (A_i x(k) + Bu(k)), \\ y(k) &= Cx(k). \end{aligned} \quad (4.26)$$

4.1.3. Simulaciones

Con el propósito de validar la representación difusa discretizada y su equivalencia dinámica con el modelo no lineal original, se llevaron a cabo simulaciones comparativas entre el sistema no lineal de tres tanques interconectados y su versión aproximada mediante el modelo Takagi-Sugeno discreto. Esta sección presenta los resultados de dichas simulaciones, así como las entradas y condiciones iniciales utilizadas. Todas las simulaciones fueron realizadas en el entorno Matlab R2020a.

Objetivo de la simulación

El objetivo principal es comparar la dinámica del sistema no lineal completo con su contraparte aproximada Takagi-Sugeno discreta, evaluando la fidelidad de la representación difusa frente a la complejidad del sistema original.

En todos los casos se consideró un período de discretización de $T_d = 0.01s$, permitiendo observar el efecto del muestreo en la dinámica capturada por el modelo.

Entradas del sistema

Se utilizaron perfiles de entrada de caudal definidos primero por una constante y posteriormente por un escalón $Q_1(k)$ y $Q_2(k)$, simulando distintas condiciones de operación. Estas entradas se muestran en la Figura 4.1.

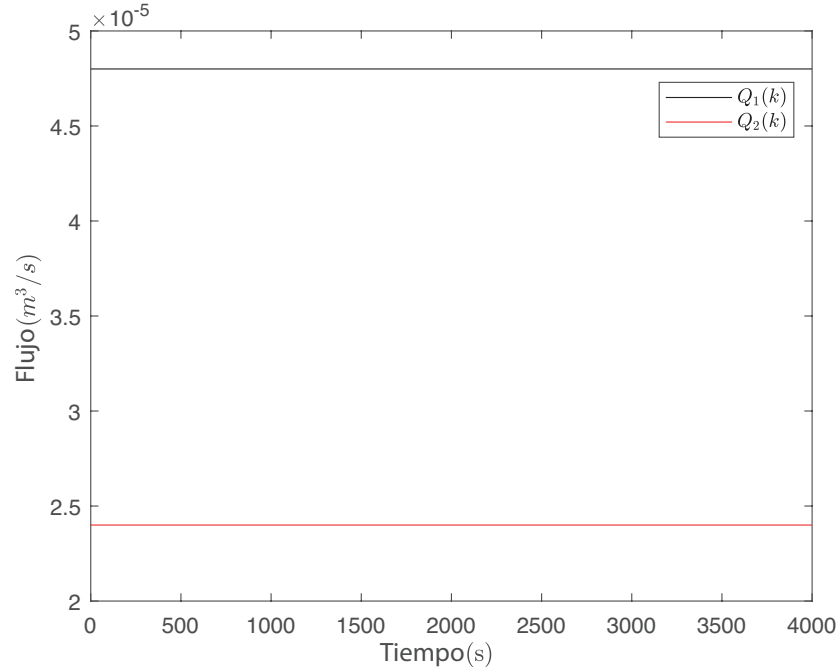


Fig. 4.1. Simulación: Perfil de entrada de flujo para los tanques 1 y 2.

Comparación entre NL y T-S discreto

Para analizar el desempeño del modelo difuso, se compararon las salidas del sistema no lineal con las del modelo T-S discreto bajo $T_d = 0.01\text{s}$. La Figura 4.2 muestra los resultados de los niveles $h_1(k)$, $h_2(k)$, $h_3(k)$.

El modelo T-S discreto sigue con gran precisión la dinámica del modelo no lineal, confirmando la validez de la aproximación difusa.

Conclusión de las simulaciones

Las simulaciones presentadas permiten concluir que:

- El modelo T-S discreto reproduce con gran exactitud la dinámica del sistema no lineal de tres tanques interconectados.

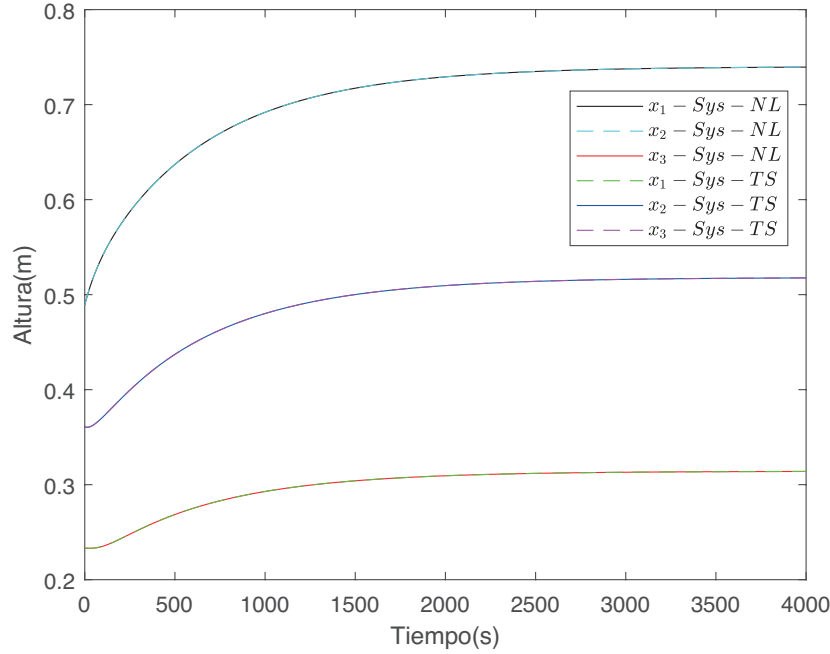


Fig. 4.2. Comparación del modelo no lineal y el modelo T-S discreto.

- La fidelidad de la aproximación se mantiene siempre que el periodo de muestreo sea suficientemente pequeño.
- Las funciones de pertenencia juegan un papel clave en la activación de los modelos locales, garantizando una transición suave entre regiones operativas.
- El modelo T-S discreto constituye una herramienta válida para el diseño de controladores digitales en sistemas ciberfísicos.

4.2. Representación T-S del sistema glucosa-insulina

El control automático de la glucosa en pacientes con diabetes tipo 1 (DM-1) es un desafío crítico en la ingeniería biomédica. La correcta regulación de los niveles de glucosa en sangre es esencial para evitar complicaciones agudas y crónicas, como hipoglucemia, hiperglucemia, neuropatía y enfermedades cardiovasculares. En este contexto, los modelos matemáticos juegan un papel fundamental, permitiendo comprender la dinámica del sistema fisiológico, diseñar algoritmos de control eficientes y validar estrategias terapéuticas antes de su implementación clínica.

El sistema glucosa-insulina representa la interacción entre el ingreso de glucosa, la acción de la insulina exógena y el comportamiento del metabolismo humano. Su formulación en términos de espacio de estados facilita el diseño de controladores predictivos, observadores y esquemas adaptativos o tolerantes a perturbaciones. En particular, este capítulo se enfoca en el desarrollo de una representación del sistema glucosa-insulina utilizando la técnica de Takagi-Sugeno en *tiempo discreto*, que permite capturar de forma precisa la no linealidad intrínseca del modelo a través de una interpolación entre modelos lineales locales.

4.2.1. Modelo no lineal del sistema glucosa-insulina

El sistema glucosa-insulina se describe mediante un modelo dinámico que representa la interacción entre los niveles de glucosa plasmática, la acción de la insulina y su efecto en la captación de glucosa en los tejidos. Para la validación comparativa con el modelo T-S en tiempo discreto, se considera a continuación la *forma en diferencias* del modelo no lineal, obtenida mediante retención de orden cero (ZOH) y discretización con periodo T_d .

Ecuaciones del modelo no lineal (discreto)

$$G_{\Delta}(k+1) = G_{\Delta}(k) + T_d \left[-p_1 G_{\Delta}(k) - X(k) (G_{\Delta}(k) + G_b) + D(k) \right], \quad (4.27)$$

$$X(k+1) = X(k) + T_d \left[-p_2 X(k) + p_3 I_{\Delta}(k) \right], \quad (4.28)$$

$$I_{\Delta}(k+1) = I_{\Delta}(k) + T_d \left[-N (I_{\Delta}(k) + I_b) + \frac{u(k)}{V_I} \right]. \quad (4.29)$$

Aquí, $G_{\Delta}(k)$ es la diferencia entre la glucosa actual y su nivel basal G_b , $X(k)$ representa el efecto de la insulina sobre la absorción de glucosa, e $I_{\Delta}(k)$ es la diferencia entre el nivel actual de insulina y su nivel basal I_b . Las entradas $D(k)$ y $u(k)$ corresponden a la ingesta de glucosa y a la infusión de insulina, respectivamente.

Forma en espacio de estados

Estas ecuaciones pueden expresarse en forma matricial como:

$$\begin{aligned} x(k+1) &= \underbrace{\left[I_3 + T_d A_c(x(k)) \right]}_{A_d(x(k))} x(k) + T_d B u(k) + T_d D w(k) + T_d \Delta, \\ y(k) &= C x(k), \end{aligned} \quad (4.30)$$

donde

$$x(k) = \begin{bmatrix} G_{\Delta}(k) \\ X(k) \\ I_{\Delta}(k) \end{bmatrix}, \quad A_c(x) = \begin{bmatrix} -p_1 & -(G_{\Delta} + G_b) & 0 \\ 0 & -p_2 & p_3 \\ 0 & 0 & -N \end{bmatrix}, \quad B = \begin{bmatrix} 0 \\ 0 \\ \frac{1}{V_I} \end{bmatrix},$$

$$D = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad \Delta = \begin{bmatrix} -X & G_b \\ -p_3 I_b \\ -N I_b \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & 0 \end{bmatrix}.$$

En (4.30), $A_d(x(k)) = I_3 + T_d A_c(x(k))$ corresponde a la discretización explícita de primer orden compatible con ZOH para el término afín en x .

Parámetros del modelo

Los parámetros utilizados se presentan en la Tabla 4.2:

Tabla 4.2. Parámetros del sistema glucosa-insulina.

Parámetro	Símbolo	Valor	Unidades
Glucosa basal	G_b	81	mg/dL
Insulina basal	I_b	2.5	mU/dL
Captación de glucosa	p_1	0.05	min^{-1}
Disminución del efecto insulina	p_2	0.1	min^{-1}
Sensibilidad insulina	p_3	0.00065	$\text{dL}/\text{mU} \cdot \text{min}^2$
Tasa desaparición insulina	N	5/54	min^{-1}
Volumen distribución insulina	V_I	15	dL

Análisis de la no linealidad y variable de programación

La principal no linealidad proviene del producto $-X(k)(G_{\Delta}(k) + G_b)$ dentro de $A_c(x(k))$. Para aplicar el enfoque Takagi–Sugeno discreto, se define la variable de programación

$$\rho(k) = -(G_{\Delta}(k) + G_b). \quad (4.31)$$

Modelos lineales locales

A partir de (4.32), se definen dos modelos locales continuos $A_1 = A_c(\underline{\rho})$ y $A_2 = A_c(\bar{\rho})$ y, para su uso en el esquema T–S discreto para $i \in \{1, 2\}$. Con los parámetros de la Tabla 4.2, los bloques A_i

$$\text{quedan } A_1 = \begin{bmatrix} -p_1 & -\underline{\rho} & 0 \\ 0 & -p_2 & p_3 \\ 0 & 0 & -N \end{bmatrix}, \quad A_2 = \begin{bmatrix} -p_1 & -\bar{\rho} & 0 \\ 0 & -p_2 & p_3 \\ 0 & 0 & -N \end{bmatrix}.$$

A partir de las simulaciones realizadas con los perfiles de entrada descritos en la Figura 4.3, se determinaron los valores extremos de la variable de programación $\rho(k)$. Estos valores corresponden a los mínimos y máximos alcanzados durante el horizonte de simulación, reflejando la dinámica inducida por los pulsos de glucosa y la infusión constante de insulina. En particular, se obtuvo que:

$$\rho(k) \in [\underline{\rho}, \bar{\rho}] = [-0.0500, -0.0433]. \quad (4.32)$$

Este rango se utilizará para construir las funciones de pertenencia difusas que interpolan entre los modelos locales A_1 y A_2 , garantizando una representación precisa del comportamiento del sistema glucosa-insulina en tiempo discreto.

4.2.2. Modelo Takagi-Sugeno del sistema glucosa-insulina

La representación Takagi-Sugeno discreta del sistema glucosa-insulina se construye interpolando los modelos lineales locales discretizados mediante funciones de pertenencia dependientes de la variable de programación $\rho(k)$ definida en (4.32). Este enfoque permite aproximar la dinámica no lineal de forma compacta y directamente utilizable en implementaciones digitales de control y diagnóstico.

Funciones de pertenencia difusas

A partir del rango operativo, se definen dos funciones de pertenencia lineales:

$$n_0(\rho(k)) = \frac{\bar{\rho} - \rho(k)}{\bar{\rho} - \underline{\rho}}, \quad (4.33)$$

$$n_1(\rho(k)) = 1 - n_0(\rho(k)). \quad (4.34)$$

De esta forma, los pesos normalizados $\mu_i(\rho(k))$ activan gradualmente cada modelo local $i \in \{1, 2\}$ en función del valor instantáneo de $\rho(k)$.

Modelo T-S discreto

El sistema T-S discreto queda descrito como:

$$x(k+1) = \sum_{i=1}^2 \mu_i(\rho(k)) A_{i,d} x(k) + B_d u(k) + D_d w(k) + \Delta_d, \quad (4.35)$$

$$y(k) = C_d x(k). \quad (4.36)$$

4.2.3. Simulaciones del sistema glucosa-insulina

En esta sección se presentan simulaciones que validan el comportamiento dinámico del modelo glucosa-insulina en sus dos representaciones: el modelo no lineal y el modelo Takagi-Sugeno. Estas simulaciones permiten comparar la fidelidad entre ambos modelos y evaluar el impacto de las entradas de glucosa e insulina bajo diferentes escenarios clínicos.

Objetivo de las simulaciones

Los objetivos principales de las simulaciones son: Comparar la respuesta del modelo no lineal frente a su representación T-S discreta, validar la utilidad del modelo T-S discreto para aplicaciones de control digital, analizar la evolución de los niveles de glucosa y el efecto de la insulina en distintos escenarios y evaluar la activación de las funciones de pertenencia durante la simulación.

Se consideraron los parámetros presentados en la Tabla 4.2. Las condiciones iniciales utilizadas fueron:

$$x(0) = \begin{bmatrix} G_{\Delta}(0) & X(0) & I_{\Delta}(0) \end{bmatrix}^T = \begin{bmatrix} 0 & 0 & 0 \end{bmatrix}^T, \quad (4.37)$$

representando un estado basal. Las entradas de glucosa $D(k)$ simulan la ingesta de carbohidratos en distintos intervalos, mientras que la insulina $u(k)$ representa infusiones administradas a través de una bomba externa.

Entradas simuladas

La Figura 4.3 muestra los perfiles de las entradas de glucosa $D(k)$ y de insulina $u(k)$ durante un horizonte de simulación de 1400 minutos.

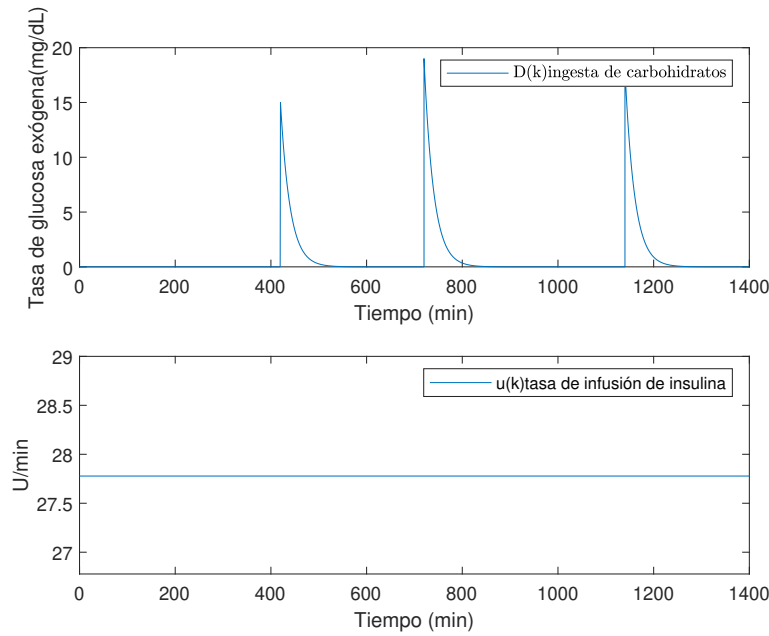


Fig. 4.3. Entradas de glucosa e insulina para la simulación del sistema glucosa-insulina.

Comparación entre modelo no lineal y T-S discreto

En la Figura 4.4 se observa la respuesta de la glucosa plasmática simulada tanto con el modelo no lineal como con su representación T-S discreta. Los resultados muestran una coincidencia cercana entre ambos modelos, validando la precisión de la aproximación difusa en tiempo discreto.

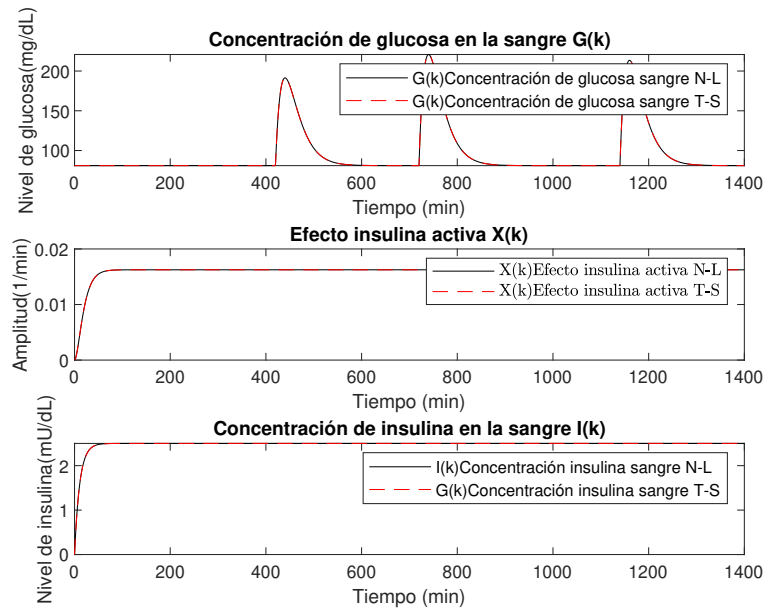


Fig. 4.4. Comparación de niveles de glucosa: modelo no lineal vs T-S discreto.

Funciones de pertenencia activadas

La Figura 4.5 muestra las funciones de pertenencia activadas durante la simulación. Puede observarse cómo la variable de programación $\rho(k)$ interpola suavemente entre los dos modelos locales, asegurando transiciones graduales en el modelo difuso discreto.

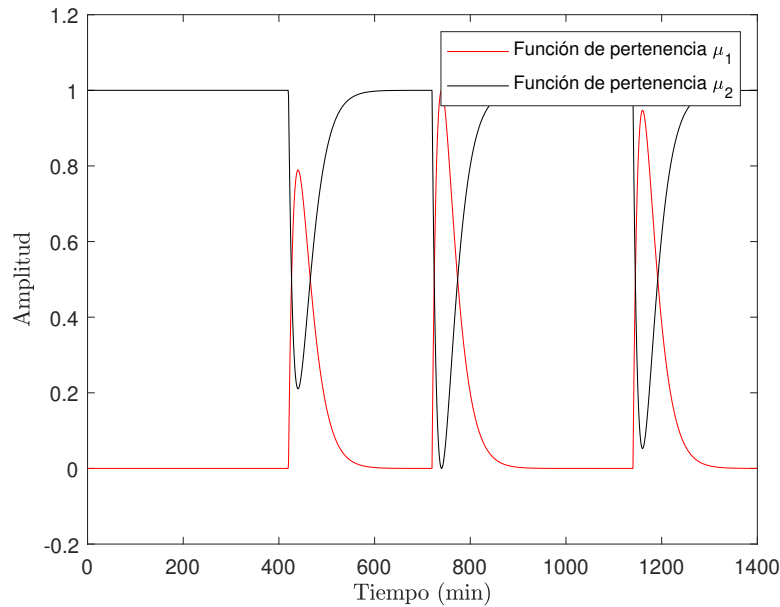


Fig. 4.5. Activación de funciones de pertenencia del modelo T-S discreto durante la simulación.

Conclusiones de las simulaciones

Los resultados de las simulaciones permiten concluir que:

- El modelo T-S discreto reproduce de forma precisa la dinámica del modelo no lineal en el rango operativo estudiado.
- La activación de funciones de pertenencia evidencia una interpolación suave entre modelos locales, característica esencial de los sistemas T-S.
- El modelo T-S discreto constituye una base confiable para el diseño de estrategias de control automático en el tratamiento de pacientes con diabetes tipo 1.

4.3. Representación LPV del vehículo RC

El modelado dinámico de vehículos a escala, como los vehículos RC, constituye una base fundamental para el estudio de técnicas avanzadas de control aplicadas a sistemas automotrices. Estos vehículos comparten principios físicos con vehículos a escala real, lo que permite validar estrategias

de control en un entorno seguro y de bajo costo. En particular, el modelo de bicicleta es ampliamente utilizado en la literatura para representar la dinámica lateral con simplicidad matemática y fidelidad física, agrupando cada eje en una rueda virtual delantera y otra trasera.

Para capturar la dependencia con la velocidad longitudinal v_x y, a la vez, conservar herramientas de análisis lineal, se adopta una representación LPV en *tiempo discreto*, adecuada para la implementación y comparación directa con el modelo no lineal.

4.3.1. Modelo no lineal discreto del vehículo RC

La dinámica lateral en coordenadas del vehículo está dada por:

$$\begin{aligned} v_y(k+1) &= v_y(k) + T_d \left[\frac{F_{yf}(k) \cos \delta(k) + F_{yr}(k)}{m} - \omega(k) v_x(k) \right], \\ \omega(k+1) &= \omega(k) + T_d \left[\frac{F_{yf}(k) l_f \cos \delta(k) - F_{yr}(k) l_r}{I_z} \right], \end{aligned} \quad (4.38)$$

donde v_x, v_y son las velocidades longitudinal y lateral [m/s], ω es la velocidad de guiñada [rad/s], δ es el ángulo de dirección [rad], m es la masa [kg], I_z es el momento de inercia [kg · m²], y l_f, l_r son las distancias de ejes.

Fuerzas laterales y aproximación para ángulos pequeños

$$F_{yf}(k) \approx C_f \left(\delta(k) - \frac{v_y(k) + l_f \omega(k)}{v_x(k)} \right), \quad (4.39)$$

$$F_{yr}(k) \approx C_r \left(-\frac{v_y(k) - l_r \omega(k)}{v_x(k)} \right). \quad (4.40)$$

Sustituyendo y asumiendo sin $\delta \approx \delta$, $\cos \delta \approx 1$, $\arctan x \approx x$, resulta el modelo afín en v_x :

$$\begin{aligned} v_y(k+1) &= v_y(k) - \frac{T_d(C_f + C_r)}{m v_x} v_y(k) - T_d \left(\frac{l_f C_f - l_r C_r}{m v_x} + v_x \right) \omega(k) + \frac{T_d C_f}{m} \delta(k), \\ \omega(k+1) &= \omega(k) - \frac{T_d(l_f C_f - l_r C_r)}{I_z v_x} v_y(k) - \frac{T_d(l_f^2 C_f + l_r^2 C_r)}{I_z v_x} \omega(k) + \frac{T_d l_f C_f}{I_z} \delta(k). \end{aligned} \quad (4.41)$$

Forma en espacio de estados discreta

Definiendo $x(k) = \begin{bmatrix} v_y(k) \\ \omega(k) \end{bmatrix}$, $u(k) = \delta(k)$, el sistema se escribe como:

$$x(k+1) = A_d(v_x) x(k) + B_d u(k), \quad y(k) = C x(k), \quad (4.42)$$

con matrices dependientes de v_x :

$$A_d(v_x) = \begin{bmatrix} 1 - \frac{T_d(C_f + C_r)}{m v_x} & -T_d \left(\frac{l_f C_f - l_r C_r}{m v_x} + v_x \right) \\ -\frac{T_d(l_f C_f - l_r C_r)}{I_z v_x} & 1 - \frac{T_d(l_f^2 C_f + l_r^2 C_r)}{I_z v_x} \end{bmatrix}, \quad B_d = \begin{bmatrix} \frac{T_d C_f}{m} \\ \frac{T_d l_f C_f}{I_z} \end{bmatrix}, \quad C = \begin{bmatrix} 0 & 1 \end{bmatrix}.$$

Parámetros físicos y configuración

Tabla 4.3. Parámetros físicos del vehículo RC y configuración para el modelo discreto.

Parámetro	Símbolo	Valor (unidad)
Rigidez lateral (delantera)	C_f	4.8438 N/rad
Rigidez lateral (trasera)	C_r	11.2441 N/rad
Distancia CG eje delantero	l_f	0.0691 m
Distancia CG eje trasero	l_r	0.1049 m
Masa del vehículo	m	1.1937 kg
Momento de inercia (z)	I_z	0.005 kg · m ²
Periodo de muestreo	T_d	0.01 s
Rango de operación		
Velocidad longitudinal (mín.-máx.)	$v_x \in [v_{x,\text{mín}}, v_{x,\text{máx}}]$	$[0.5, 2.0]$ m/s
Variable de programación	$\rho_1 = v_x, \rho_2 = 1/v_x$	$\rho_2 \in [1/v_{x,\text{máx}}, 1/v_{x,\text{mín}}]$

4.3.2. Modelo LPV politópico discreto

El modelo afín en v_x se reescribe como un sistema LPV politópico en tiempo discreto. Los vértices se definen evaluando $A_d(v_x)$ en los extremos ρ_1, ρ_2 , con:

$$\omega_1 = (\underline{\rho}_1, \underline{\rho}_2), \quad \omega_2 = (\underline{\rho}_1, \overline{\rho}_2), \quad \omega_3 = (\overline{\rho}_1, \underline{\rho}_2), \quad \omega_4 = (\overline{\rho}_1, \overline{\rho}_2).$$

La interpolación politópica se expresa como:

$$x(k+1) = \sum_{i=1}^4 \mu_i(\rho(k)) \left(A_{i,d} x(k) + B_{i,d} u(k) \right), \quad y(k) = C x(k), \quad (4.43)$$

donde $\mu_i(\rho)$ son los pesos convexos que cumplen $\mu_i(\rho) \geq 0$ y $\sum_i \mu_i(\rho) = 1$.

4.3.3. Simulaciones: modelo NL vs LPV discreto

En esta sección se presentan simulaciones para validar la precisión del modelo LPV politópico discreto (4.43) en comparación con el modelo no lineal discreto (4.38).

Objetivo

Verificar que el modelo LPV discreto reproduce con fidelidad la dinámica lateral no lineal del vehículo RC bajo variaciones de la velocidad longitudinal y entradas de dirección.

Entradas simuladas

La Figura 4.6 muestra el perfil de entrada $\delta(k)$ aplicado: una señal escalón utilizada para excitar la dinámica lateral.

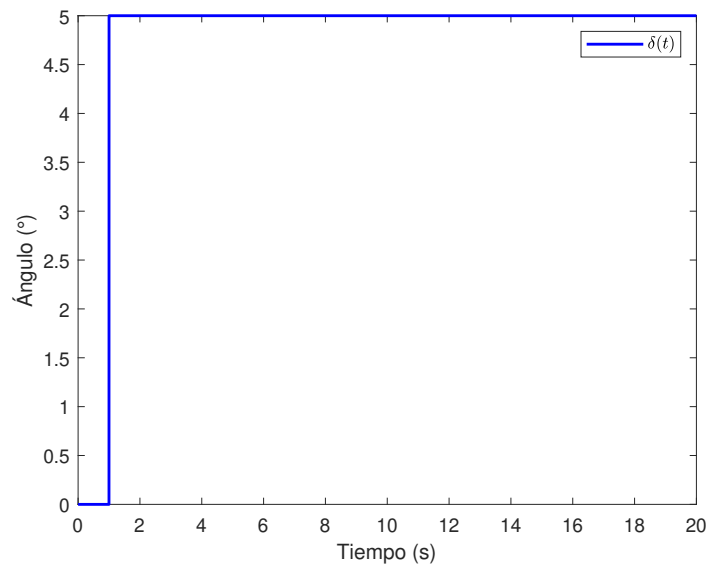


Fig. 4.6. Perfil de entrada de dirección $\delta(k)$ utilizado en las simulaciones.

Comparación de respuesta lateral

La Figura 4.7 compara las salidas v_y y ω del modelo no lineal discreto y del modelo LPV discreto. Se observa una concordancia cercana entre ambos modelos en todo el rango simulado.

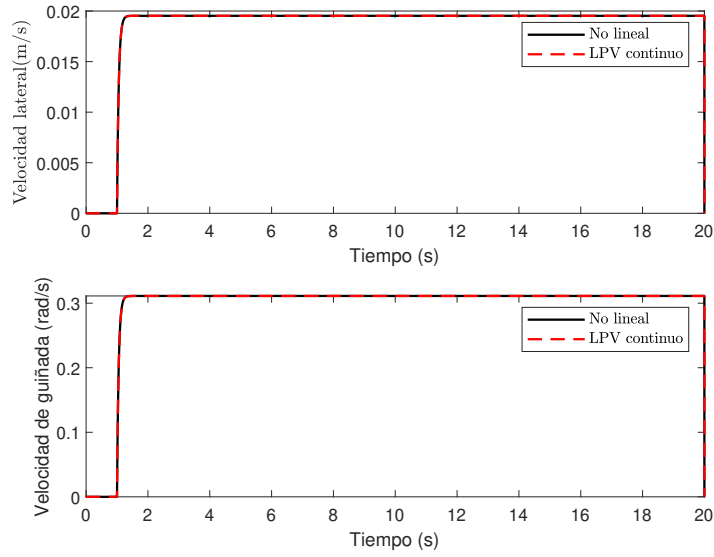


Fig. 4.7. Comparación entre el modelo no lineal discreto y el modelo LPV discreto: (a) velocidad lateral v_y , (b) velocidad de guiñada ω .

Funciones de pertenencia activadas

En la Figura 4.8 se observan las funciones de pertenencia $\mu_i(\rho)$, mostrando cómo los pesos varían dinámicamente según la velocidad v_x .

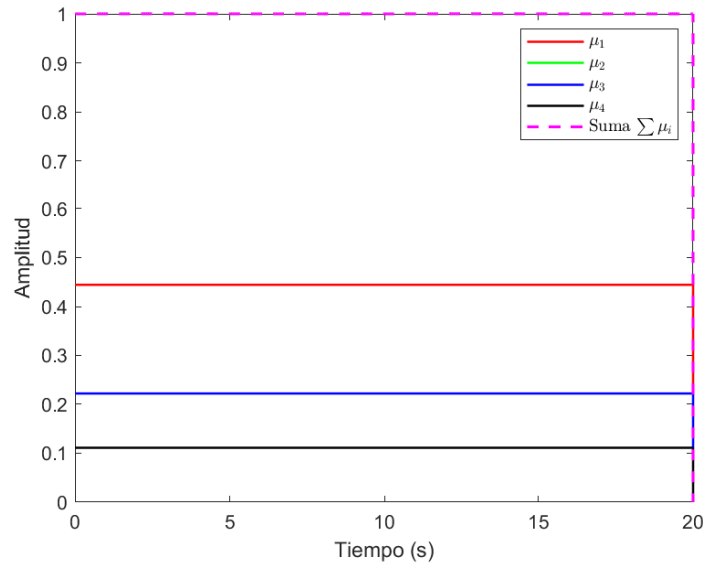


Fig. 4.8. Evolución de las funciones de pertenencia $\mu_i(\rho)$ en el modelo LPV discreto.

Conclusión de las simulaciones

De los resultados se concluye que:

- El modelo LPV discreto reproduce con alta precisión la dinámica no lineal del vehículo RC.
- La discretización mediante ZOH conserva la fidelidad del sistema para un periodo de muestreo $T_d = 0.01$ s.
- Las funciones de pertenencia permiten interpolar suavemente entre modelos lineales locales, capturando la variación dinámica con v_x .

4.4. Conclusiones del capítulo

En este capítulo se desarrollaron y analizaron tres sistemas dinámicos representativos con el objetivo de aplicar metodologías de modelado no lineal, su aproximación mediante modelos dependientes de parámetros y la correspondiente discretización para implementación digital.

Primero, se abordó el **sistema de tres tanques interconectados**, cuya dinámica no lineal fue descrita mediante ecuaciones en diferencias acopladas que representan los flujos de entrada, salida y las interacciones entre tanques. Se identificaron las no linealidades principales asociadas a los términos de raíz cuadrada en los caudales, lo que permitió construir un modelo Takagi-Sugeno (T-S) discreto utilizando el método del sector no lineal. Se determinaron las variables premisas, sus rangos operativos y se formularon los modelos locales lineales. Las simulaciones mostraron una excelente concordancia entre el modelo T-S discreto y el sistema no lineal original, validando la fidelidad de la aproximación en tiempo discreto.

Posteriormente, se estudió el **sistema glucosa-insulina**, fundamental en aplicaciones biomédicas para el control de glucosa en pacientes con diabetes tipo 1. A partir de un modelo no lineal, se identificó una única variable de programación asociada al efecto de la insulina sobre la absorción de glucosa, lo que permitió construir una representación Takagi-Sugeno con dos modelos locales en tiempo discreto. Las simulaciones comparativas confirmaron que la representación T-S discreta reproduce con precisión el comportamiento del modelo no lineal, demostrando su aplicabilidad en entornos de control digital para dispositivos médicos.

Finalmente, se desarrolló el **modelo LPV discreto del vehículo RC**, derivado del modelo de bicicleta, para describir la dinámica lateral del vehículo. Se formularon las ecuaciones no lineales en tiempo discreto considerando las fuerzas laterales de los neumáticos y se aplicaron aproximaciones de ángulo pequeño para obtener un modelo afín en la velocidad longitudinal v_x . Este modelo se transformó en un sistema LPV discreto en forma politópica, definiendo variables de programación basadas en v_x y su inversa, y construyendo modelos lineales locales en los vértices del politopo. Cada submodelo se discretizó mediante ZOH utilizando un período de muestreo adecuado ($T_d = 0.01$ s), coherente con la dinámica rápida del vehículo RC. Las simulaciones demostraron que el modelo LPV discreto representa fielmente la dinámica lateral original, validando el uso de esta aproximación para aplicaciones de control robusto en vehículos autónomos a escala.

Los tres casos de estudio confirman que las representaciones T-S y LPV en tiempo discreto son herramientas eficaces para aproximar sistemas no lineales, conservando fidelidad dinámica y facilitando el diseño de controladores digitales y observadores tolerantes a perturbaciones o ataques en sistemas ciberfísicos.

Capítulo 5

Observadores para la detección de ataques

Los observadores son una herramienta clave para la detección temprana de alteraciones en sistemas ciber-físicos. En este capítulo se integra, en un mismo hilo, el *banco de observadores* y el *observador generador de residuos* con el objetivo de detectar e identificar ataques sobre sensores y actuadores. A lo largo del capítulo se trabaja con modelos discretos Takagi-Sugeno, se consideran lógicas de activación Markovianas (uniformes y no uniformes) y se reportan simulaciones que muestran el desempeño de las estrategias propuestas.

5.1. Banco de observadores para la detección de ataques

El uso de observadores constituye una herramienta fundamental para la detección temprana de alteraciones en el comportamiento dinámico de estos sistemas, permitiendo no solo diagnosticar posibles intrusiones, sino también sentar las bases para estrategias de control tolerantes a ataques.

Esta sección introduce el diseño de un **banco de observadores tipo Luenberger bajo un esquema dedicado (DOS, *Dedicated Observer Scheme*)** para la detección de ataques en sistemas ciber-físicos. El enfoque combina técnicas clásicas de estimación de estados con la integración de procesos estocásticos Markovianos para modelar la lógica de activación de los ataques, lo cual permite representar escenarios realistas en entornos industriales expuestos a redes de comunicación abiertas.

En un **DOS** se implementa un observador por salida: el *observador* i utiliza todas las entradas, $u(k)$ pero *solo* la salida $y_i(k)$ para generar su estimación $\hat{y}_i(k)$ y el *residuo* $r_i(k) = y_i(k) - \hat{y}_i(k)$. Así, cada observador queda *dedicado* a un canal específico y el patrón de residuos facilita la **detección e identificación** de ataques o anomalías localizadas en dicho canal (a diferencia de un esquema *GOS*, donde cada observador usa todas las salidas a la vez).

5.1.1. Observador tipo Luenberger

El observador de Luenberger constituye una de las herramientas más utilizadas en estimación de estados. Su estructura reconstruye el vector de estados a partir de las salidas medidas y del modelo nominal, con una realimentación del error de salida que asegura la convergencia del estimado.

En este trabajo se emplea el esquema de la Figura 5.1, aplicado a sistemas Takagi–Sugeno discretos. El observador usa $y(k)$, $u(k)$ y la dinámica local interpolada por funciones de pertenencia.

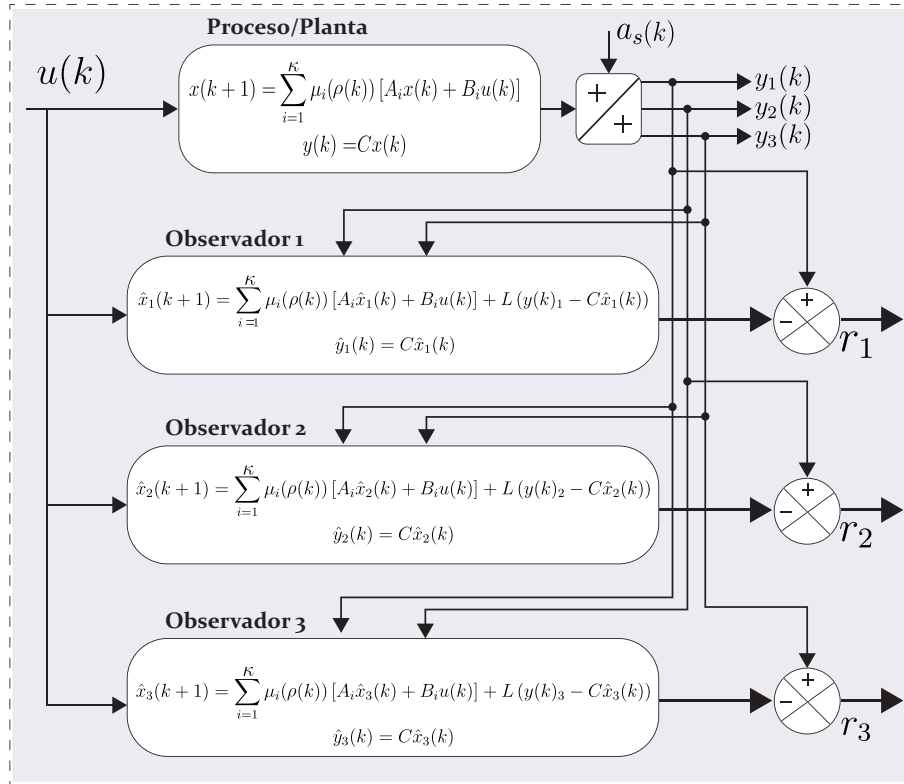


Fig. 5.1. Esquema general del observador de Luenberger para sistemas Takagi–Sugeno discretos.

Ecuaciones del observador. Para el sistema T-S discreto,

$$\begin{aligned} x(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) [A_i x(k) + B_i u(k)], \\ y(k) &= C x(k), \end{aligned} \quad (5.1)$$

el observador de Luenberger se escribe como

$$\hat{x}(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) [A_i \hat{x}(k) + B_i u(k)] + L(y(k) - \hat{y}(k)), \quad \hat{y}(k) = C \hat{x}(k), \quad (5.2)$$

donde $L \in \mathbb{R}^{n \times p}$ es la ganancia del observador.

La matriz L se determina de modo que la dinámica del error $e(k) = x(k) - \hat{x}(k)$ sea asintóticamente estable. En términos prácticos, esto equivale a seleccionar L tal que los autovalores de las matrices $(A_i - LC)$ queden dentro del círculo unidad, garantizando la convergencia del estimado de estado.

5.1.2. Banco de observadores dedicados (DOS)

Se implementa un **banco DOS** con un observador por salida. El error del observador j -ésimo es

$$e_j(k) = x(k) - \hat{x}_j(k), \quad r_j(k) = y_j(k) - \hat{y}_j(k).$$

La decisión de ataque se toma por umbral $|r_j(k)| > \tau_j$. Por construcción:

$$r_1 \leftrightarrow y_1, \quad r_2 \leftrightarrow y_2, \quad r_3 \leftrightarrow y_3,$$

es decir, el *residuo* r_j es sensible a ataques en y_j .

5.1.3. Modelo matemático y diseño del banco de observadores

El observador asociado a (5.1) queda

$$\hat{x}(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) [A_i \hat{x}(k) + B_i u(k)] + L(y(k) - C \hat{x}(k)). \quad (5.3)$$

Definiendo $e(k) = x(k) - \hat{x}(k)$, la dinámica del error es

$$e(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) (A_i - LC) e(k). \quad (5.4)$$

5.1.4. Análisis de estabilidad (LMIs)

Considérese $V(k) = e(k)^\top P e(k)$, con $P = P^\top > 0$. Una condición suficiente para $\Delta V(k) < 0$ es

$$(A_i - LC)^\top P (A_i - LC) - P < 0, \quad \forall i = 1, \dots, \kappa. \quad (5.5)$$

Introduciendo $G = PL$, se obtiene la forma LMI

$$\begin{bmatrix} -P & A_i^\top P - C^\top G^\top \\ PA_i - GC & -P \end{bmatrix} < 0, \quad \forall i = 1, \dots, \kappa, \quad (5.6)$$

y la ganancia final $L = P^{-1}G$.

5.1.5. Simulación con esquemas de ataque

Las simulaciones se realizan sobre el **modelo T–S discreto de tres tanques** de la Sección 4.1.2, con parámetros de la Tabla 4.1. El periodo de muestreo es $T_d = 0.01$ s ($t = k T_d$).

Entradas. Se emplean caudales $u(k) = [Q_1(k) \ Q_2(k)]^\top$ tipo escalón:

$$\begin{aligned} Q_1(k) &= \bar{Q}_1 \mathbf{1}_{\{k \geq k_1\}}, & \bar{Q}_1 &= 0.35 \times 10^{-4}, & k_1 &= \lfloor 184/T_d \rfloor, \\ Q_2(k) &= \bar{Q}_2 \mathbf{1}_{\{k \geq k_2\}}, & \bar{Q}_2 &= 0.50 \times 10^{-4}, & k_2 &= \lfloor 70/T_d \rfloor, \end{aligned} \quad (5.7)$$

con condiciones iniciales

$$x(0) = [h_1(0) \ h_2(0) \ h_3(0)]^\top = [0.20 \ 0.20 \ 0.20]^\top.$$

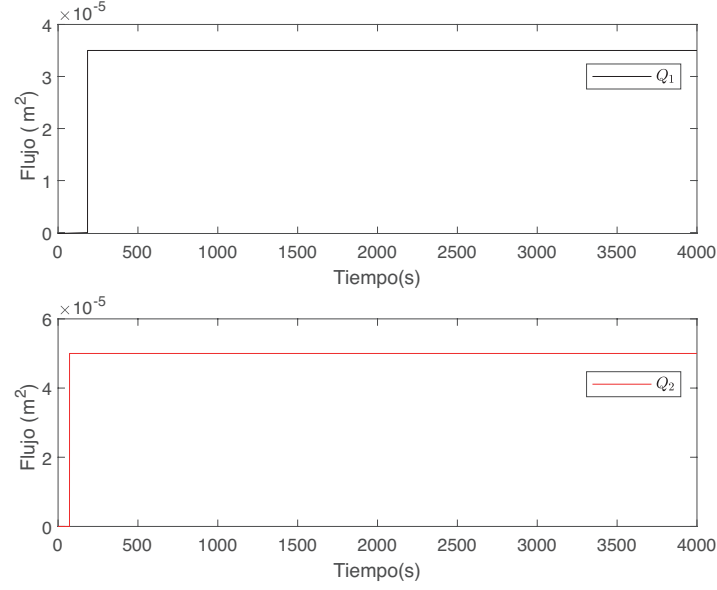


Fig. 5.2. Entradas de bombeo en (5.7). Eje horizontal: índice k ($t = k T_d$).

Interpretación de residuos en DOS. El umbral de decisión es $|r_i(k)| > \tau_i \Rightarrow$ detección en el canal i . Por construcción, cada r_i es *principalmente sensible* a ataques en y_i .

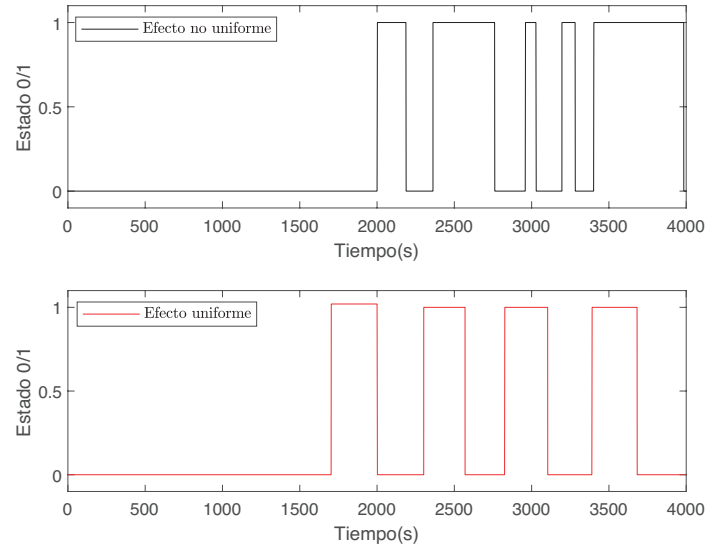


Fig. 5.3. Señales Markovianas (uniforme y no uniforme) usadas para activar ataques.

Ejemplo 1: DoS en sensor con lógica uniforme. Ataque DoS en y_2 : $y_2^a(k) = (1 - \beta(k)) y_2(k)$, $\beta(k) \in \{0, 1\}$.

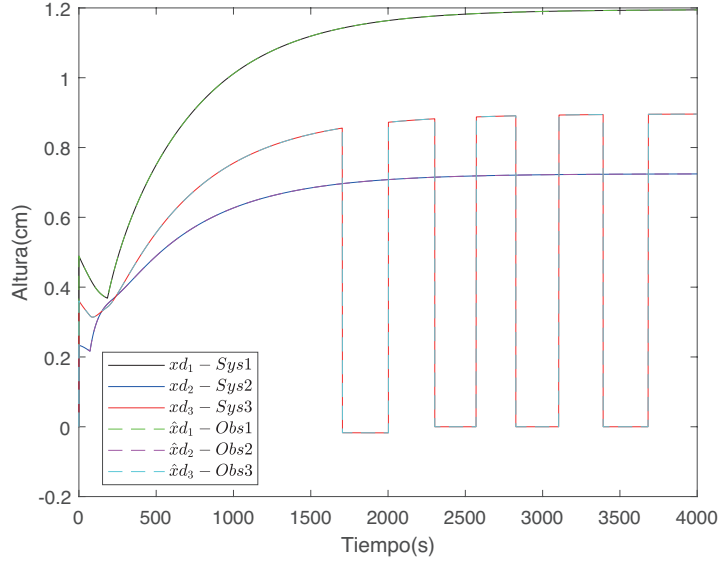


Fig. 5.4. Estados bajo DoS en y_2 (lógica uniforme). Eje: k ($t = kT_d$).

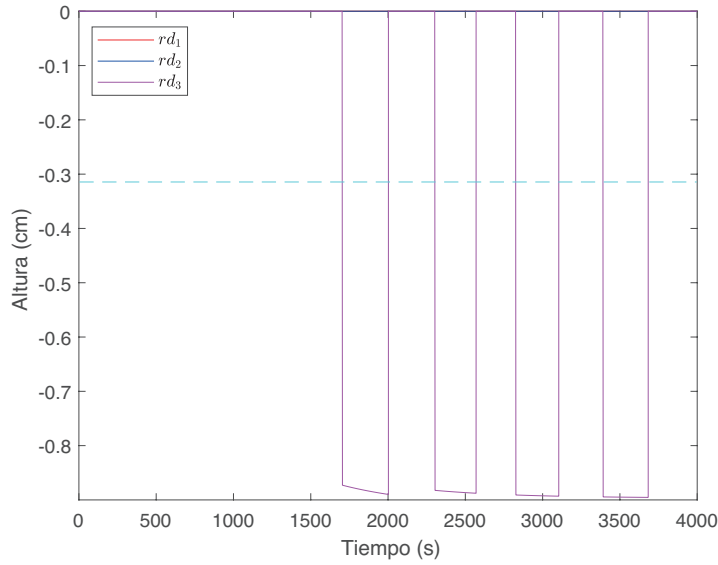
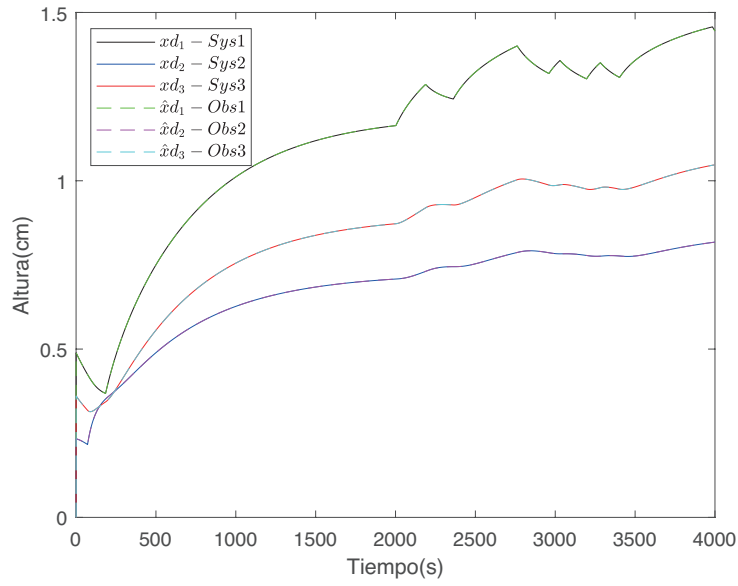
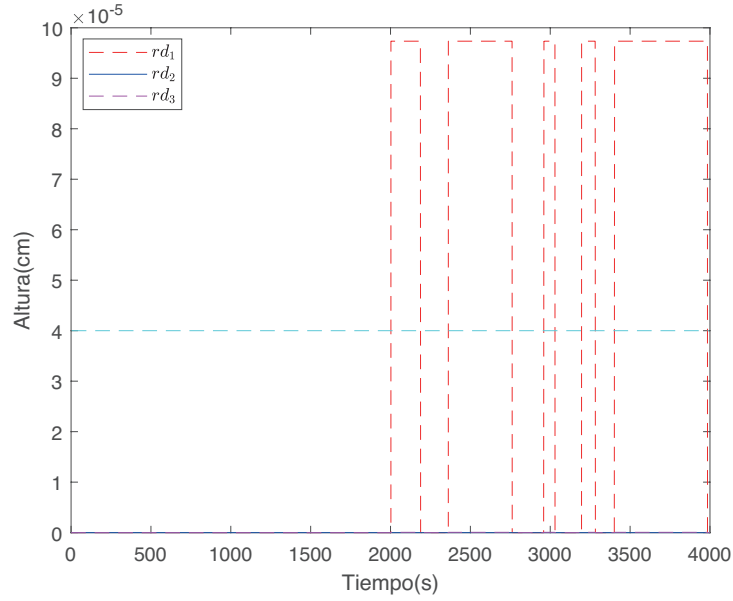
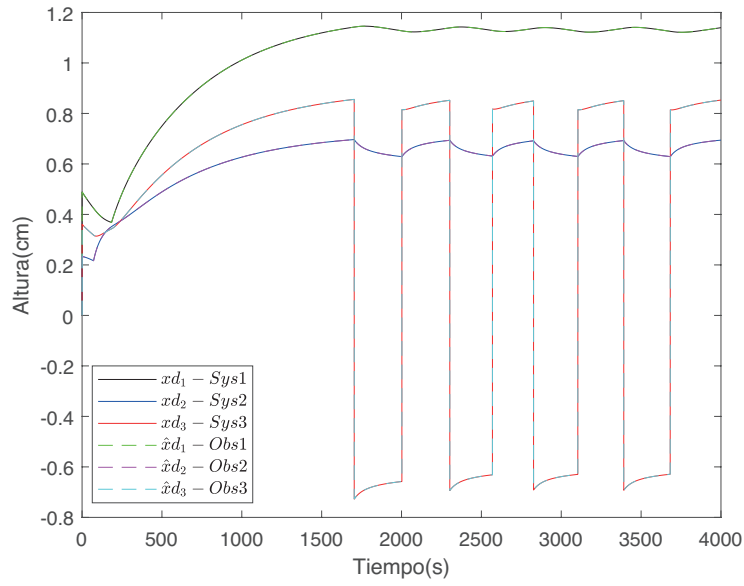
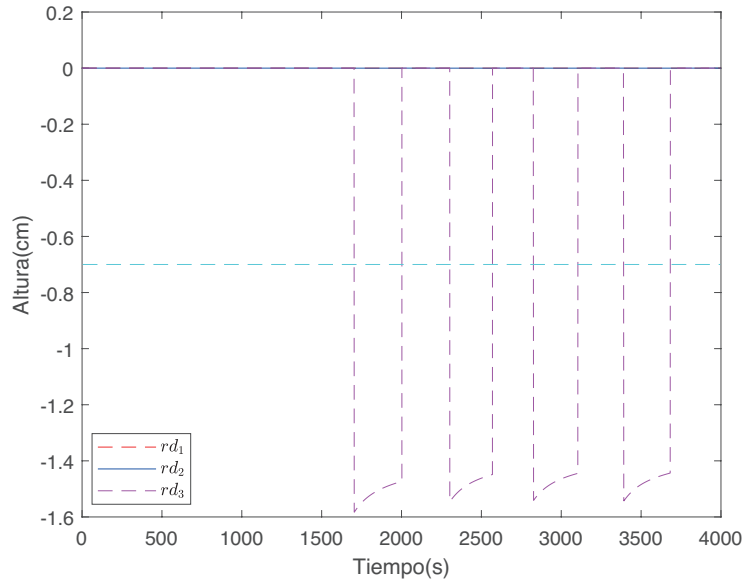


Fig. 5.5. Residuos ante DoS en y_2 : r_2 cruza el umbral τ_2 ; r_1, r_3 cercanos a cero.

Ejemplo 2: DDA en actuador con lógica no uniforme. Ataque DDA en $u_1 = Q_1(k)$: $u_1^a(k) = u_1(k) - \alpha(k)u_1(k) + \alpha(k)b_a(k)$, con $\alpha(k)$ no uniforme.

Fig. 5.6. Estados bajo DDA en u_1 (no uniforme).Fig. 5.7. Residuos ante DDA en u_1 : activación multicanal con predominio en r_1 .

Ejemplo 3: RDI coordinado en sensor y actuador. Ataque RDI sobre y_3 y u_2 , lógica uniforme: $y_3^a(k) = y_3(k) + \beta(k)b_s(k)$, $u_2^a(k) = u_2(k) + \alpha(k)b_a(k)$.

Fig. 5.8. Estados bajo RDI coordinado en y_3 y u_2 .Fig. 5.9. Residuos ante RDI coordinado: activación de r_3 y activaciones adicionales por la vía de u_2 .

Resumen. La Tabla 5.1 resume combinaciones de ataques (sensor, actuador, coordinado) y la activación esperada de residuos bajo lógicas uniforme/no uniforme.

Tabla 5.1. Tablas de residuos para diferentes tipos de ataques.

Ataques en Sensor							
Uniforme - Ataque tipo DoS							
r_i	x_1	x_2	x_3	x_1, x_2	x_1, x_3	x_2, x_3	x_1, x_2, x_3
r_1	1	0	0	1	1	0	1
r_2	0	1	0	1	0	1	1
r_3	0	0	1	0	1	1	1
No uniforme - Ataque tipo DoS							
r_1	1	0	0	1	1	0	1
r_2	0	1	0	1	0	1	1
r_3	0	0	1	0	1	1	1
Ataques en Actuador							
Uniforme - Ataque tipo DDA							
r_1	1	0	0	1	1	0	1
r_2	0	1	0	1	0	1	1
r_3	0	0	1	0	1	1	1
No uniforme - Ataque tipo DDA							
r_1	1	0	0	1	1	0	1
r_2	0	1	0	1	0	1	1
r_3	0	0	1	0	1	1	1
Ataques Coordinados							
Uniforme - Ataque tipo RDI							
r_1	1	0	0	1	1	0	1
r_2	0	1	0	1	0	1	1
r_3	0	0	1	0	1	1	1
No uniforme - Ataque tipo RDI							
r_1	1	0	0	1	1	0	1
r_2	0	1	0	1	0	1	1
r_3	0	0	1	0	1	1	1

5.1.6. Conclusiones de la sección (Banco DOS)

Se estableció un banco de observadores Luenberger en *esquema DOS* para detección/identificación por residuos. La sensibilidad canal–residuo $r_j \leftrightarrow y_j$ facilita el diagnóstico en ataques a sensores; los ataques en actuadores producen firmas multicanal en los residuos y pueden complementarse con un observador generador de residuos para discriminar la localización exacta del ataque.

5.2. Observador Generador de Residuos (OGR): resultados con el sistema glucosa–insulina T–S

En esta sección se presentan los resultados del **observador generador de residuos (OGR)** aplicado al sistema glucosa–insulina en su **representación Takagi–Sugeno (T–S) en tiempo discreto**. Se empleó una entrada nominal de insulina $u(k) = 27.7778 \text{ mU/dL}$ y los parámetros definidos en la Tabla 4.2. El tiempo de muestreo es $T_d = 0.01$. Además, el sistema fue sometido a perturbaciones externas que representan tres ingestas alimenticias (desayuno, comida y cena) en los minutos 420, 720 y 1140, respectivamente, lo que introduce dinámicas realistas de variación de glucosa en sangre.

Las simulaciones se llevaron a cabo utilizando el modelo T–S del sistema glucosa–insulina. Se consideraron tres tipos de ataque: **DoS**, **DDA** y **RDI**. Todos los ataques se modelaron bajo una **lógica de activación Markoviana**, tanto *uniforme* como *no uniforme*. La lógica uniforme implica períodos constantes de activación y desactivación, mientras que la no uniforme introduce activaciones de duración aleatoria, representando de mejor manera las estrategias adaptativas de un atacante real. El residuo del OGR se define como $r(k) = y(k) - \hat{y}(k)$ y la detección se decide por umbral $\|r(k)\|_\infty > \tau$.

5.2.1. Esquema del OGR

La Figura 5.10 presenta la arquitectura del observador generador de residuos. El bloque *Planta T–S discreta* recibe la entrada $u(k)$ y produce la salida $y(k)$; los ataques en actuadores y sensores se distribuyen mediante F_1 y F_2 con lógicas de activación Markovianas (uniforme / no uniforme). El observador calcula $\hat{x}(k)$ y $\hat{y}(k)$, y genera el residuo $r(k) = y(k) - \hat{y}(k)$ que alimenta el bloque de decisión.

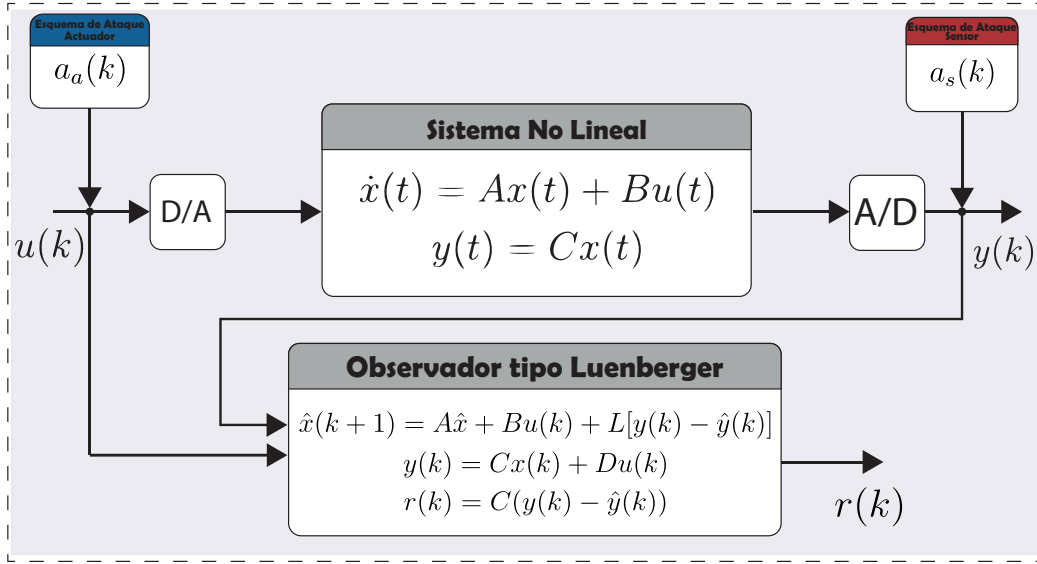


Fig. 5.10. Esquema del observador generador de residuos (OGR) para la activación de ataques en sensor/actuador.

5.2.2. Formulación paramétrica T–S discreta y sistema bajo ataque

Sea un modelo T–S discreto con κ reglas y funciones de pertenencia $\mu_i(\rho(k))$ tales que $\mu_i(\rho) \geq 0$, $\sum_{i=1}^{\kappa} \mu_i(\rho) = 1$. La planta bajo ataques en actuadores/sensores se escribe como

$$\begin{aligned} x(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) A_i x(k) + B u(k) + F_1 a_a(k), \\ y(k) &= C x(k) + F_2 a_s(k). \end{aligned} \quad (5.8)$$

El **OGR** se programa con las mismas funciones $\mu_i(\rho)$:

$$\begin{aligned} \hat{x}(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) A_i \hat{x}(k) + B u(k) + L(y(k) - \hat{y}(k)), \\ \hat{y}(k) &= C \hat{x}(k), \quad r(k) = y(k) - \hat{y}(k), \end{aligned} \quad (5.9)$$

donde, en la implementación adoptada, se emplea una ganancia L consistente con el diseño por LMI de estabilidad.

Definiendo el error $e(k) := x(k) - \hat{x}(k)$, se obtiene el **residuo**

$$r(k) = C e(k) + F_2 a_s(k), \quad (5.10)$$

y la **dinámica del error**

$$e(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left(A_i - LC \right) e(k) + F_1 a_a(k) - L F_2 a_s(k). \quad (5.11)$$

Considérese el sistema T–S discreto (5.8)–(5.9), que resume las características propias de los CPS (señales muestreadas y transporte en red). Se asume observabilidad:

$$\mathbf{rank} \begin{bmatrix} C & CA_i & \cdots & CA_i^{n-1} \end{bmatrix}^T = n, \quad (5.12)$$

donde, para esta prueba, A_i denota la matriz nominal L .

5.2.3. Diseño del observador tipo Luenberger

Para el diseño nominal, el observador de Luenberger se define como:

$$\begin{aligned} \hat{x}(k+1) &= A_i \hat{x}(k) + B u(k) + L [y(k) - \hat{y}(k)], \\ \hat{y}(k) &= C \hat{x}(k), \\ r(k) &= y(k) - \hat{y}(k). \end{aligned} \quad (5.13)$$

El error de estimación $e(k) = x(k) - \hat{x}(k)$ obedece:

$$e(k+1) = (A_i - LC) e(k) + F_1 a_a(k), \quad (5.14)$$

y el residuo asociado:

$$r(k) = C e(k) + F_2 a_s(k). \quad (5.15)$$

Estas expresiones vinculan explícitamente la respuesta del observador ante ataques al actuador y al sensor, lo que permite distinguir entre ambos a partir del análisis simultáneo de $e(k)$ y $r(k)$.

5.2.4. Análisis de estabilidad del observador

Se propone la función de Lyapunov $V(e) = e^\top P e$, $P > 0$. La condición de estabilidad discreta se garantiza si

$$(A_i - LC)^\top P (A_i - LC) - P < 0, \quad (5.16)$$

que es equivalente (por complemento de Schur (Boyd *y col.*, 1994)) a la LMI:

$$\begin{bmatrix} -P & (A_i - LC)^\top P \\ P(A_i - LC) & -P \end{bmatrix} < 0. \quad (5.17)$$

La LMI (7.25) se resuelve en YALMIP/SeDuMi fijando A, B, C .

5.2.5. Simulación y generación de residuos

El objetivo es demostrar que, mediante el análisis simultáneo del error $e(k)$ y del residuo $r(k)$, es posible distinguir entre ataques que afectan directamente a los actuadores y aquellos que alteran las mediciones de los sensores. Se empleó $u(k) = 27.7778 \text{ mU/dL}$, $T_d = 0.01$ y los parámetros de la Tabla 4.2. Se consideran tres ingestas (420, 720, 1140 min). Los ataques DoS, DDA y RDI se activan por lógica Markoviana uniforme/no uniforme.

Perfil de lógica Markoviana

La Figura 5.11 muestra los perfiles de activación utilizados. La señal en color rojo corresponde al caso uniforme, caracterizado por ciclos periódicos y regulares de ataque/no ataque, mientras que la señal en **negro** representa el caso no uniforme, donde los intervalos de activación varían de manera estocástica.

Escenario 1: Ataque DoS en el sensor de glucosa

En este primer escenario se simuló un ataque de denegación de servicio (DoS) aplicado sobre el sensor de glucosa $y(k)$. En la Figura 5.12 se observa la salida real de glucosa y su estimación; la Figura 5.13 muestra el residuo, con picos sincronizados con la activación del ataque. El error $e(k)$ permanece acotado, coherente con una alteración en salida y no en la dinámica interna.

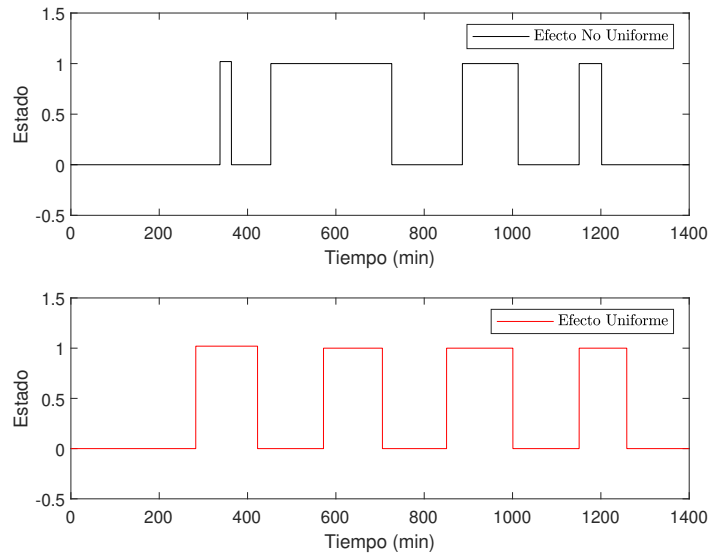


Fig. 5.11. Señales Markovianas uniforme (rojo) y no uniforme (negro) empleadas para la activación de ataques.

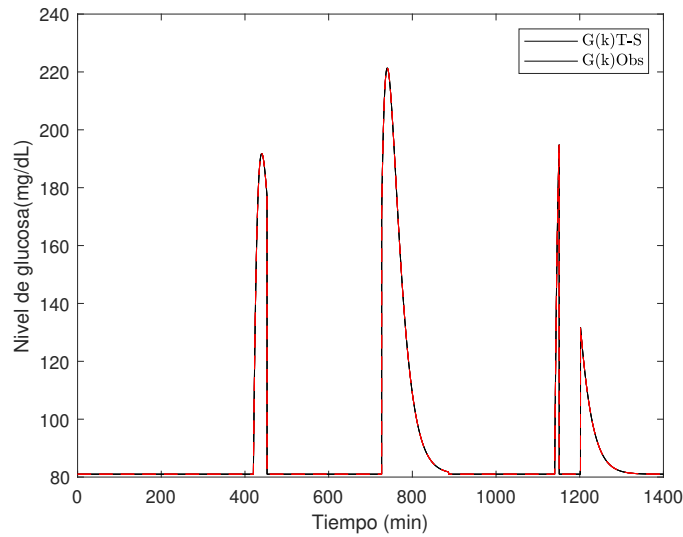
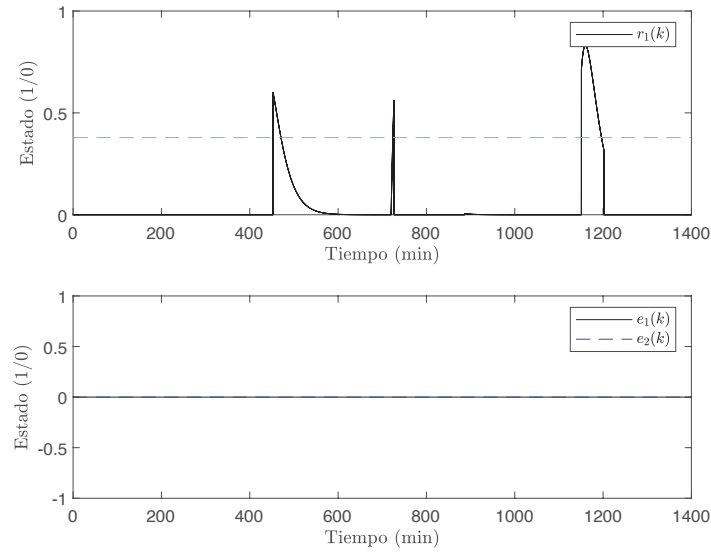


Fig. 5.12. Comparación de salida real y estimada bajo ataque DoS en el sensor $y(k)$.

Escenario 2: Ataque DDA en el actuador de insulina

En el segundo escenario se simuló un ataque DDA aplicado al actuador (alteración de $u(k)$). La Figura 5.14 muestra que la dinámica real se separa de la estimada; en la Figura 5.15 se aprecia el crecimiento de $e(k)$. Como el sensor no fue manipulado, $r(k)$ permanece bajo: el OGR revela

Fig. 5.13. Residuo $r(k)$ durante un ataque DoS en $y(k)$.

ataques en el actuador, principalmente a través del error de estimación.

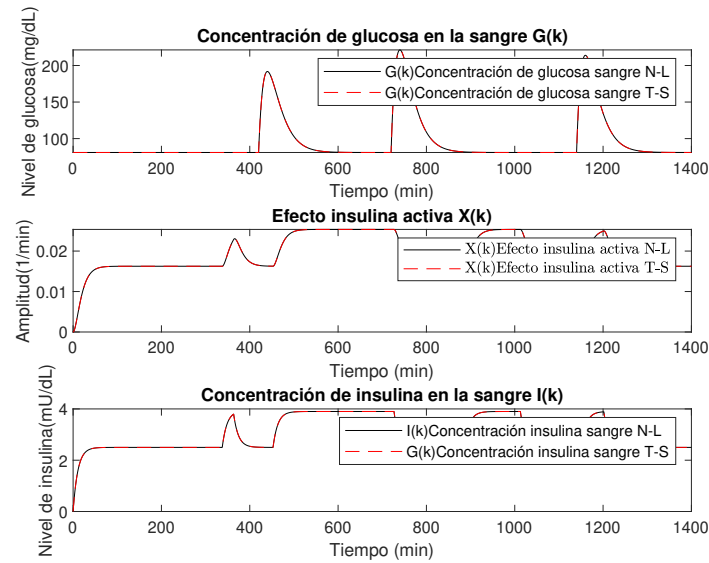


Fig. 5.14. Estados reales y estimados bajo ataque DDA en el actuador de insulina.

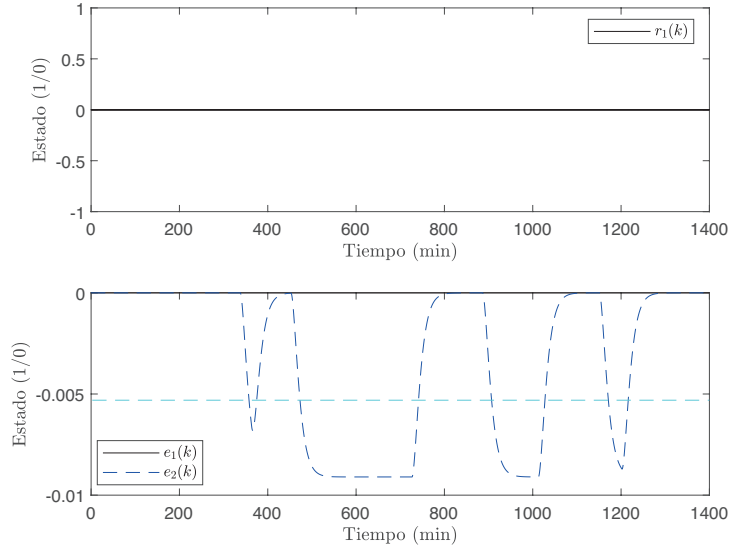


Fig. 5.15. Error de estimación $e(k)$ durante un ataque DDA en el actuador.

Escenario 3: Ataque combinado (DDA en actuador + DoS en sensor)

En el último escenario se aplicó un ataque combinado: DDA en el actuador y DoS en el sensor. La Figura 5.16 muestra alteraciones severas en la trayectoria de glucosa. En la Figura 5.17, el residuo $r(k)$ (por DoS en salida) y el error $e(k)$ (por DDA en actuador) se activan simultáneamente, habilitando un diagnóstico claro de ataque en *entrada y salida*.

5.2.6. Conclusión y contraste entre DOS y OGR

- **Banco DOS (Dedicated Observer Scheme).** Genera residuos *canal-específicos* $r_i(k) = y_i(k) - \hat{y}_i(k)$, lo que facilita el *aislamiento* del sensor comprometido y la detección de patrones multicanal (cf. Sección 5.1.5). Este esquema indica con claridad *dónde* ocurre la anomalía (qué salida/actuador está afectado), pero por sí solo no determina *qué tipo de ataque* (DoS, DDA, RDI) ni *qué distribución de activación* (uniforme/no uniforme) lo genera.
- **OGR (esta sección).** Entrega un *residuo global* $r(k)$, muy sensible a alteraciones en el sensor, mientras que las manipulaciones en el actuador se reflejan con mayor nitidez en el *error de estimación* $e(k)$. Esto permite distinguir *ubicación* del ataque (salida vs. entrada) y analizar firmas temporales, pero, al igual que el DOS, el OGR no identifica de manera

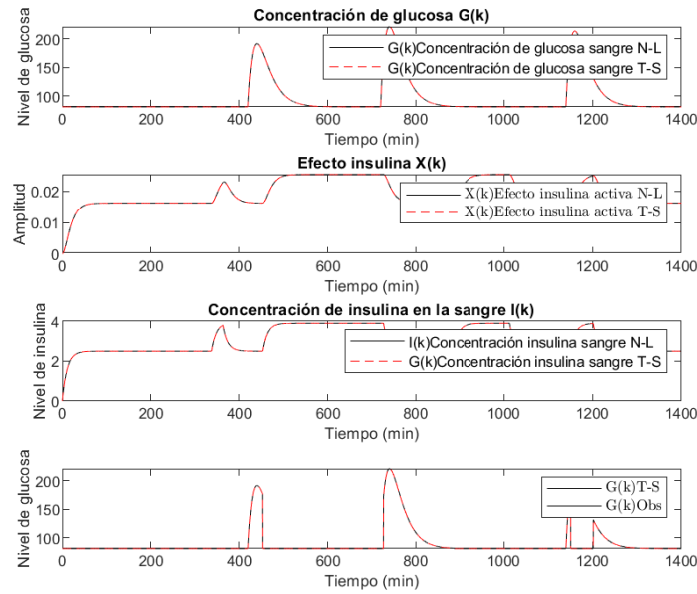
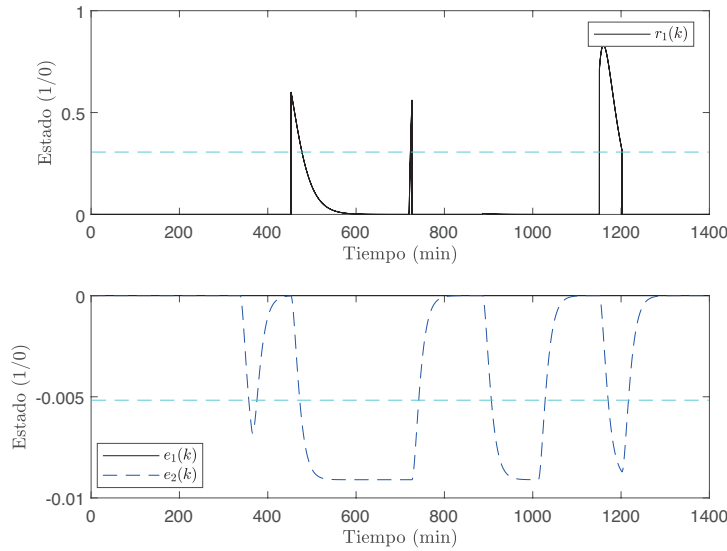


Fig. 5.16. Estados reales y estimados bajo ataque combinado (DDA + DoS).

Fig. 5.17. Comparación entre residuo $r(k)$ y error de estimación $e(k)$ para diagnóstico de ataques combinados.

inequívoca la *clase* del ataque (DoS, DDA, RDI) ni su *lógica de activación* (uniforme/no uniforme) sin módulos adicionales de clasificación.

En consecuencia, en secciones posteriores se introducen estructuras de observadores y criterios complementarios orientados a *clasificar* el tipo de ataque y su distribución de activación, manteniendo la detección y localización provistas por los esquemas DOS y OGR.

Tabla 5.2. Residuos (ataques DoS, DDA, RDI). Valor **1** indica activación/alarma significativa; **0**, inactiva.

Uniformes							
	y_1	u_1	u_2	y_1, u_1	y_1, u_2	u_1, u_2	y_1, u_1, u_2
r_1	1	0	0	1	1	0	1
e_1	0	1	0	1	0	1	1
e_2	0	0	1	0	1	1	1

No uniformes							
	y_1	u_1	u_2	y_1, u_1	y_1, u_2	u_1, u_2	y_1, u_1, u_2
r_1	1	0	0	1	1	0	1
e_1	0	1	0	1	0	1	1
e_2	0	0	1	0	1	1	1

Entonces r_1 es el residuo asociado a y_1 . e_1 y e_2 denotan la activación del error de estimación en los estados 1 y 2, respectivamente. Las columnas indican el canal atacado (sensor/actuador) y sus combinaciones.

Capítulo 6

Observador ODG para aislamiento, detección y localización

Los sistemas ciberfísicos se encuentran expuestos a perturbaciones externas y ataques maliciosos que pueden comprometer su integridad, seguridad y correcto funcionamiento. La necesidad de desarrollar métodos efectivos para el **aislamiento, detección y localización de ataques** ha impulsado el uso de observadores robustos que permiten estimar los estados del sistema y generar **residuos sensibles a ataques**.

En este contexto, en esta sección se propone el desarrollo de un **Observador de Detección Generalizada** basado en la representación Takagi-Sugeno por lo cual, los objetivos son:

- Estimar los estados del sistema aún en presencia de no linealidades y ataques.
- Generar residuos que permitan detectar y aislar ataques sobre actuadores.
- Mantener la estabilidad del error de estimación mediante condiciones de **Lyapunov** y formulaciones en **Desigualdades Matriciales Lineales**.

El diseño del ODG se apoya en la estructura de modelos locales del sistema T-S, lo que facilita su parametrización y garantiza un comportamiento robusto frente a incertidumbres y ataques modelados.

En la Figura 6.1 se presenta el esquema conceptual del observador ODG empleado en este trabajo, donde se observa su ubicación en el lazo de control, la generación de residuos y la interacción con el sistema bajo ataques.

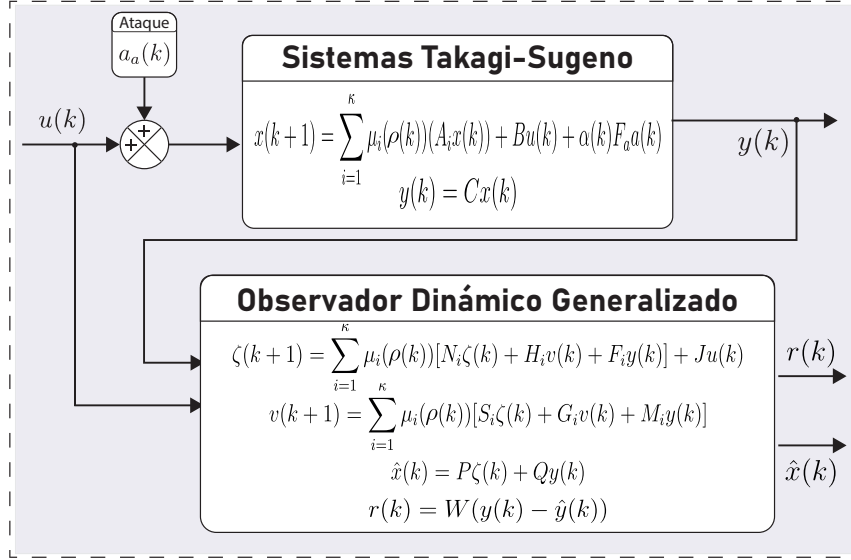


Fig. 6.1. Esquema del Observador de Detección Generalizada (ODG) basado en representación T-S.

Este enfoque permite combinar la capacidad de modelado no lineal del marco T-S con técnicas modernas de diagnóstico, logrando una **detección temprana y localización precisa de ataques** en CPS críticos.

6.1. Modelo matemático y diseño

En esta sección se introduce un sistema ciberfísico no lineal en tiempo discreto bajo la representación Takagi-Sugeno, un modelo de ataque al actuador, la estructura del observador dinámico generalizado y la ecuación de los residuos utilizada para la detección de ataques. El CPS se describe como:

$$\begin{aligned} x(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) A_i x(k) + B u(k) + F_a a_a(k), \\ y(k) &= C x(k), \end{aligned} \quad (6.1)$$

donde $x(k) \in \mathbb{R}^n$ es el vector de estados del sistema, $u(k) \in \mathbb{R}^m$ es la entrada y $y(k) \in \mathbb{R}^p$ representa las variables de salida medidas.

Condiciones de ponderación y representación T-S

La no linealidad del sistema está representada por las matrices A_i , que dependen de los puntos de operación no lineales. Estos puntos son caracterizados por las funciones de ponderación $\mu_i(\rho(k))$,

que cumplen con la condición de suma convexa:

$$\sum_{i=1}^{\kappa} \mu_i(\rho(k)) = 1, \quad \mu_i(\rho(k)) \geq 0, \quad \forall i \in \{1, \dots, \kappa\}. \quad (6.2)$$

Aquí, $\kappa = 2^s$, donde s es el número de no linealidades en el sistema. Cada A_i corresponde a un modelo lineal local asociado a una región de operación específica. Las matrices $A_i \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times m}$, $C \in \mathbb{R}^{p \times n}$ y $F_a \in \mathbb{R}^{n \times r}$ son conocidas.

Modelo de ataque al actuador

El ataque al actuador $a_a(k) \in \mathbb{R}^r$ está definido como:

$$a_a(k) = \alpha(k)a(k), \quad (6.3)$$

donde $\alpha(k)$ representa procesos estocásticos de Markov cuyos valores están entre 0 y 1, y $a(k)$ es el vector de ataque al actuador.

Condición de observabilidad

Para el diseño del observador dinámico generalizado, se asume que el sistema T-S ciberfísico satisface la condición de observabilidad:

$$\text{rank} \begin{bmatrix} C \\ CA_i \\ \vdots \\ CA_i^{n-1} \end{bmatrix} = n. \quad (6.4)$$

Estructura del observador ODG

Consideremos un ODG para el sistema (6.1), definido por:

$$\zeta(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) [N_i \zeta(k) + H_i v(k) + F_i y(k)] + Ju(k), \quad (6.5)$$

$$v(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) [S_i \zeta(k) + G_i v(k) + M_i y(k)], \quad (6.6)$$

$$\hat{x}(k) = P\zeta(k) + Qy(k), \quad (6.7)$$

donde $\zeta(k) \in \mathbb{R}^{q_0}$ vector de estados del observador funcional, $v(k) \in \mathbb{R}^{q_1}$ es el vector auxiliar, $\hat{x}(k) \in \mathbb{R}^n$ es el vector de estimación de estados. Las matrices $N_i, H_i, F_i, J, S_i, G_i, M_i, P, Q$ son de dimensiones apropiadas y se deben determinar en el diseño del ODG.

Ecuación de los residuos

La ecuación de los residuos, utilizada para la detección y aislamiento de ataques, está dada por:

$$r(k) = W(y(k) - \hat{y}(k)), \quad (6.8)$$

donde W es una matriz de ponderación de los residuos.

Lemma 1. *Existe un observador de la forma (6.5)–(6.7) para el sistema (6.1) si y sólo si se cumplen las siguientes condiciones:*

1. *Existe una matriz T de dimensiones apropiadas tal que:*

$$N_i T + F_i C - T A_i = 0, \quad (6.9)$$

$$J = T B, \quad (6.10)$$

$$S_i T + M_i C = 0, \quad (6.11)$$

$$P T + Q C = I_n. \quad (6.12)$$

2. *La matriz $\begin{bmatrix} N_i & H_i \\ S_i & L_i \end{bmatrix}$ es estable $\forall i = 1, \dots, \kappa$.*

En la siguiente parte desarrollaremos la dinámica del error, la ecuación del residuo, las condiciones algebraicas para el diseño del ODG y la parametrización.

Consideremos una matriz $T \in \mathbb{R}^{q_0 \times (n+r)}$ y definamos el vector de error transformado como:

$$\varepsilon(k) = \zeta(k) - T x(k), \quad (6.13)$$

cuya dinámica se expresa como:

$$\varepsilon(k+1) = \zeta(k+1) - T x(k+1). \quad (6.14)$$

Sustituyendo $\zeta(k) = \varepsilon(k) + T x(k)$ en (6.14) y usando el sistema (6.1), obtenemos:

$$\begin{aligned} \varepsilon(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) & \left[N_i \varepsilon(k) + \underbrace{(N_i T + F_i C - T A_i)}_{=0} x(k) + H_i v(k) \right] \\ & + \underbrace{(J - T B)}_{=0} u(k) - T F_a a_a(k), \end{aligned} \quad (6.15)$$

donde se han aplicado las condiciones (8.9) y (8.10) del Lemma. Las ecuaciones del observador (6.6) y (6.7) se reescriben como:

$$v(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left[\underbrace{(S_i T + M_i C)}_{=0} x(k) + S_i \varepsilon(k) + G_i v(k) \right], \quad (6.16)$$

$$\hat{x}(k) = P \varepsilon(k) + \underbrace{(PT + QC)}_{=I} x(k). \quad (6.17)$$

La ecuación de los residuos se define como:

$$\begin{aligned} r(k) &= W(y(k) - \hat{y}(k)), \\ &= WC \underbrace{(x(k) - \hat{x}(k))}_{e(k)}, \end{aligned} \quad (6.18)$$

donde $e(k) = x(k) - \hat{x}(k)$ es el error de estimación del estado.

Combinando (6.15) y (6.16), la dinámica del error y del vector auxiliar $v(k)$ se expresa como:

$$\begin{bmatrix} \varepsilon(k+1) \\ v(k+1) \end{bmatrix} = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \begin{bmatrix} N_i & H_i \\ S_i & G_i \end{bmatrix} \begin{bmatrix} \varepsilon(k) \\ v(k) \end{bmatrix} + \begin{bmatrix} -T & F_a \\ 0 & \end{bmatrix} a_a(k), \quad (6.19)$$

Así, el problema de aislamiento de ataques se reduce a determinar las matrices N_i , H_i , F_i , S_i , G_i , M_i , P , Q , W y T que aseguren estabilidad del observador y permitan generar residuos que reflejen los ataques en el actuador.

Finalmente, la ecuación del residuo en función de $\varepsilon(k)$ y $v(k)$ queda:

$$r(k) = W \underbrace{\begin{bmatrix} CP & 0 \end{bmatrix}}_{\mathbb{C}} \begin{bmatrix} \varepsilon(k) \\ v(k) \end{bmatrix}. \quad (6.20)$$

En la siguiente sección se detallará la parametrización de matrices del ODG, utilizando condiciones algebraicas para resolver (8.9)–(8.12) y la formulación basada en soluciones generales con pseudoinversa de Moore-Penrose.

Parametrización del observador ODG

Para diseñar el observador de la forma (6.5)–(6.7), deben cumplirse las condiciones (8.9)–(8.12). Se definen las siguientes matrices:

$$\Sigma = \begin{bmatrix} E \\ C \end{bmatrix}, \quad \Omega = \begin{bmatrix} I_n \\ C \end{bmatrix}, \quad (6.21)$$

donde $E \in \mathbb{R}^{q_0 \times n}$ es de rango completo en filas.

Las condiciones (c) y (d) se reescriben como:

$$\begin{bmatrix} S_i & M_i \\ P & Q \end{bmatrix} \begin{bmatrix} T \\ C \end{bmatrix} = \begin{bmatrix} 0 \\ I_n \end{bmatrix}, \quad (6.22)$$

cuyo cumplimiento requiere que:

$$\text{rango} \left(\begin{bmatrix} T \\ C \end{bmatrix} \right) = \text{rango} \left(\begin{bmatrix} T \\ C \\ I_n \end{bmatrix} \right) = n. \quad (6.23)$$

De acuerdo con Bernstein (2011), como $\text{rango} \begin{bmatrix} \Omega \\ \Sigma \end{bmatrix} = \text{rango}(\Omega) = n$, existen matrices $T \in \mathbb{R}^{q_0 \times n}$ y $K \in \mathbb{R}^{q_0 \times p}$ tales que:

$$T + KC = E. \quad (6.24)$$

Esto permite calcular:

$$T = E\Omega^+ \begin{bmatrix} I_n \\ 0 \end{bmatrix}, \quad K = E\Omega^+ \begin{bmatrix} 0 \\ I_p \end{bmatrix}, \quad (6.25)$$

donde Ω^+ es la pseudoinversa de Moore-Penrose de Ω .

Reescribiendo la condición (8.9):

$$N_i T + F_i C - T A_i = 0, \quad (6.26)$$

y usando (6.24), se obtiene:

$$N_i E + \underbrace{(F_i - N_i K)}_{\tilde{K}_i} C = T A_i. \quad (6.27)$$

Definiendo $\Sigma = \begin{bmatrix} E \\ C \end{bmatrix}$, esto se puede expresar como:

$$\begin{bmatrix} N_i & \tilde{K}_i \end{bmatrix} \Sigma = T A_i. \quad (6.28)$$

La solución general de N_i y $\tilde{K}_i$ es:

$$N_i = \underbrace{T A_i \Sigma^+ \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}}_{N_{i1}} - \underbrace{Y_{i1} (I_{q_0+p} - \Sigma \Sigma^+)}_{N_2} \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}, \quad (6.29)$$

$$\tilde{K}_i = \underbrace{T A_i \Sigma^+ \begin{bmatrix} 0 \\ I_p \end{bmatrix}}_{\tilde{K}_{i1}} - \underbrace{Y_{i1} (I_{q_0+p} - \Sigma \Sigma^+)}_{\tilde{K}_2} \begin{bmatrix} 0 \\ I_p \end{bmatrix}, \quad (6.30)$$

donde Y_{i1} es una matriz arbitraria de dimensiones apropiadas.

A partir de $F_i = \tilde{K}_i + N_i K$, se obtiene:

$$F_i = \tilde{K}_{i1} - Y_{i1} \tilde{K}_2 + N_{i1} K - Y_{i1} N_2 K, \quad (6.31)$$

que se simplifica como:

$$F_i = F_{i1} - Y_{i1} F_2, \quad (6.32)$$

donde $F_{i1} = T A_i \Sigma^+ \begin{bmatrix} K \\ I_p \end{bmatrix}$ y $F_2 = (I_{q_0+p} - \Sigma \Sigma^+) \begin{bmatrix} K \\ I_p \end{bmatrix}$.

Para S_i , M_i , P y Q , de (6.22) se tiene:

$$\begin{bmatrix} S_i & M_i \\ P & Q \end{bmatrix} \begin{bmatrix} I_{q_0} & -K \\ 0 & I_p \end{bmatrix} \Sigma = \begin{bmatrix} 0 \\ I_n \end{bmatrix}, \quad (6.33)$$

cuya solución general es:

$$\begin{bmatrix} S_i & M_i \\ P & Q \end{bmatrix} = \begin{bmatrix} -W_{i1} N_2 & -W_{i1} F_2 \\ \Sigma^+ \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix} - W_2 N_2 & \Sigma^+ \begin{bmatrix} K \\ I_p \end{bmatrix} - W_2 F_2 \end{bmatrix}, \quad (6.34)$$

donde W_{i1} y W_2 son matrices arbitrarias de dimensiones adecuadas.

Dinámica del error y residuos finales

La dinámica del error queda expresada como:

$$\varphi(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) (\mathbb{A}_{i1} - \mathbb{Y}_i \mathbb{A}_2) \varphi(k) + \mathbb{B} a_a(k), \quad (6.35)$$

con:

$$\mathbb{A}_{i1} = \begin{bmatrix} N_i & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathbb{A}_2 = \begin{bmatrix} N_2 & 0 \\ 0 & -I_{q_1} \end{bmatrix}, \quad \mathbb{B} = \begin{bmatrix} -T F_a \\ 0 \end{bmatrix}, \quad \mathbb{Y}_i = \begin{bmatrix} Y_{i1} & H_i \\ W_{i1} & G_i \end{bmatrix}.$$

Finalmente, la ecuación de los residuos es:

$$r(k) = W \underbrace{\begin{bmatrix} C P & 0 \end{bmatrix}}_{\mathbb{C}} \begin{bmatrix} \varepsilon(k) \\ v(k) \end{bmatrix}. \quad (6.36)$$

Función de transferencia para detección y aislamiento de ataques

A partir de la dinámica del error y de la ecuación de residuos, se define la función de transferencia desde el ataque $a_a(k)$ hacia el residuo $r(k)$ como:

$$G_z = \left(\frac{\mathbb{A}_{i1} - \mathbb{Y}_i \mathbb{A}_2}{W\mathbb{C}} \middle| \frac{\mathbb{B}}{0} \right). \quad (6.37)$$

El objetivo es proponer una función de transferencia deseada con comportamiento **diagonal**, en la cual cada canal de ataque influya únicamente en un residuo. La forma deseada es:

$$G_{z,d} = \text{diag} \left(\frac{\gamma_1}{z - \lambda_1}, \dots, \frac{\gamma_r}{z - \lambda_r} \right), \quad (6.38)$$

donde $\lambda_i \in (-1, 1)$ son polos asignados y $\gamma_i \neq 0$ son ganancias de detección.

La función de transferencia G_z puede diagonalizarse si y sólo si $\mathbb{C}\mathbb{B}$ tiene rango columna completo, es decir:

$$\text{rango}(\mathbb{C}\mathbb{B}) = r \quad \text{y} \quad p \geq r, \quad (6.39)$$

donde p es el número de salidas medidas y r el número de canales de ataque.

Bajo esta condición, el problema de detección y aislamiento se reduce al diseño de las matrices $\mathbb{Y}_i$ y W que satisfacen:

$$(\mathbb{A}_{i1} - \mathbb{Y}_i \mathbb{A}_2)\mathbb{B} = \mathbb{B}\Lambda, \quad (6.40)$$

$$W\mathbb{C}\mathbb{B} = \Gamma, \quad (6.41)$$

donde $\Lambda = \text{diag}(\lambda_1, \dots, \lambda_r)$ y $\Gamma = \text{diag}(\gamma_1, \dots, \gamma_r)$.

Si existen matrices $\mathbb{Y}_i$ y W que satisfacen (6.40) y (6.41), entonces la función de transferencia entre los ataques $a_a(k)$ y los residuos $r(k)$ es diagonal y está dada por:

$$G_z = \text{diag} \left(\frac{\gamma_1}{z - \lambda_1}, \dots, \frac{\gamma_r}{z - \lambda_r} \right), \quad (6.42)$$

permitiendo la **detección independiente** de cada canal de ataque.

Demostración. A partir de (6.40) y (6.41), las soluciones generales son:

$$\mathbb{Y}_i = (\mathbb{A}_{i1}\mathbb{B} - \mathbb{B}\Lambda)(\mathbb{A}_2\mathbb{B})^+ - Z_i \left[I - (\mathbb{A}_2\mathbb{B})(\mathbb{A}_2\mathbb{B})^+ \right], \quad (6.43)$$

$$W = \Gamma(\mathbb{C}\mathbb{B})^+, \quad (6.44)$$

donde Z_i es una matriz arbitraria que puede utilizarse para ubicar polos adicionales no observables. Sustituyendo (6.43) y (6.44) en (6.37), se obtiene la forma deseada (6.38). $\square$

Finalmente, las ecuaciones dinámicas del error y el residuo quedan:

$$\varphi(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left[\underbrace{\mathbb{A}_{i1} - (\mathbb{A}_{i1}\mathbb{B} - \mathbb{B}\Lambda)(\mathbb{A}_2\mathbb{B})^+ \mathbb{A}_2}_{\bar{\mathbb{A}}_{i1}} + Z_i \underbrace{\left(I - (\mathbb{A}_2\mathbb{B})(\mathbb{A}_2\mathbb{B})^+ \right) \mathbb{A}_2}_{\bar{\mathbb{A}}_2} \right] \varphi(k) + \mathbb{B}a_a(k), \quad (6.45)$$

$$r(k) = \Gamma(\mathbb{C}\mathbb{B})^+ \mathbb{C}\varphi(k). \quad (6.46)$$

6.1.1. Análisis de estabilidad del observador

Para garantizar la estabilidad del observador ODG en presencia de ataques, se propone una función de Lyapunov candidata definida como:

$$V(\varphi(k)) = \varphi^T(k) X \varphi(k) > 0, \quad (6.47)$$

donde $X = \begin{bmatrix} X_1 & 0 \\ 0 & X_2 \end{bmatrix} > 0$, con $X_1 \in \mathbb{R}^{q_0 \times q_0}$ y $X_2 \in \mathbb{R}^{q_1 \times q_1}$.

La diferencia de Lyapunov entre dos instantes consecutivos está dada por:

$$\begin{aligned} \Delta V(\varphi(k)) &= V(\varphi(k+1)) - V(\varphi(k)), \\ &= \varphi^T(k+1) X \varphi(k+1) - \varphi^T(k) X \varphi(k), \\ &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \varphi^T(k) \left[(\bar{\mathbb{A}}_{i1} - Z_i \bar{\mathbb{A}}_2)^T X (\bar{\mathbb{A}}_{i1} - Z_i \bar{\mathbb{A}}_2) - X \right] \varphi(k). \end{aligned} \quad (6.48)$$

Para garantizar estabilidad, se requiere que:

$$\Delta V(\varphi(k)) < 0 \quad \forall \varphi(k) \neq 0, \quad (6.49)$$

lo que equivale a la condición matricial:

$$(\bar{\mathbb{A}}_{i1} - Z_i \bar{\mathbb{A}}_2)^T X (\bar{\mathbb{A}}_{i1} - Z_i \bar{\mathbb{A}}_2) - X < 0. \quad \forall i \in \{1, \dots, \kappa\}. \quad (6.50)$$

Aplicando el *complemento de Schur* Boyd y col. (1994), la desigualdad (6.50) se reescribe como la LMI:

$$\begin{bmatrix} -X & (\bar{\mathbb{A}}_{i1} - Z_i \bar{\mathbb{A}}_2)^T X \\ X(\bar{\mathbb{A}}_{i1} - Z_i \bar{\mathbb{A}}_2) & -X \end{bmatrix} < 0. \quad \forall i \in \{1, \dots, \kappa\}. \quad (6.51)$$

Esta condición puede expresarse de manera equivalente como:

$$\mathcal{C}\mathcal{X}_i\mathcal{D} + (\mathcal{C}\mathcal{X}_i\mathcal{D})^T + \mathcal{E}_i < 0, \quad \forall i \in \{1, \dots, \kappa\}. \quad (6.52)$$

donde se definen las matrices:

$$\mathcal{E}_i = \begin{bmatrix} -X & \bar{\mathbb{A}}_{i1}^T X \\ X\bar{\mathbb{A}}_{i1} & -X \end{bmatrix}, \quad \mathcal{C} = \begin{bmatrix} 0 \\ -I \end{bmatrix}, \quad \mathcal{D} = \begin{bmatrix} \bar{\mathbb{A}}_2 & 0 \end{bmatrix}, \quad \mathcal{X}_i = XZ_i. \quad (6.53)$$

Aplicando el lema de eliminación Skelton *y col.* (1997), la condición (6.52) es equivalente a verificar las dos desigualdades:

$$\mathcal{C}^\perp \mathcal{E}_i \mathcal{C}^{\perp T} < 0, \quad \forall i \in \{1, \dots, \kappa\}, \quad (6.54)$$

$$\mathcal{D}^{T\perp} \mathcal{E}_i \mathcal{D}^{T\perp T} < 0. \quad \forall i \in \{1, \dots, \kappa\}. \quad (6.55)$$

Sustituyendo $\mathcal{C}^\perp = [I \ 0]$, la primera condición se expande como:

$$\mathcal{E}_i = \begin{bmatrix} X_1 & 0 & \Pi_a^T & 0 \\ 0 & X_2 & 0 & 0 \\ \Pi_a & 0 & -X_1 & 0 \\ 0 & 0 & 0 & -X_2 \end{bmatrix} < 0, \quad (6.56)$$

donde

$$\Pi_a = N_1 + (TF_a\Lambda - N_1TF_a)(N_2TF_a)^+N_2. \quad (6.57)$$

De forma similar, usando $\mathcal{D}^{T\perp} = \begin{bmatrix} \Pi_b^{T\perp} & 0 & 0 & 0 \\ 0 & 0 & I & 0 \\ 0 & 0 & 0 & I \end{bmatrix}$, la segunda condición resulta en:

$$\begin{bmatrix} \Pi_b^{T\perp} X_1 \Pi_b^{T\perp T} & \Pi_b^{T\perp} \Pi_a^T & 0 \\ \Pi_a \Pi_b^{T\perp T} & -X_1 & 0 \\ 0 & 0 & -X_2 \end{bmatrix} < 0, \quad (6.58)$$

donde $\Pi_b = N_2 - (N_2TF_a)(N_2TF_a)^+N_2$.

$\mathcal{X}_i$ se obtiene como:

$$\mathcal{X}_i = \mathcal{C}_r^+ \mathcal{K}_i \mathcal{D}_l^+ + \mathcal{Z} - \mathcal{C}_r^+ \mathcal{C}_r \mathcal{Z} \mathcal{D}_l \mathcal{D}_l^+, \quad (6.59)$$

donde $\mathcal{Z}$ es arbitraria, y $(\mathcal{D}_l, \mathcal{D}_r)$ y $(\mathcal{C}_l, \mathcal{C}_r)$ son factores de rango completo de $\mathcal{C}$ y $\mathcal{D}$.

Las matrices auxiliares son:

$$\mathcal{K}_i = -\mathcal{R}^{-1} \mathcal{C}_l^T \mathcal{V}_i \mathcal{D}_r^T (\mathcal{D}_r \mathcal{V}_i \mathcal{D}_r^T)^{-1} + \mathcal{S}_i^{\frac{1}{2}} \mathcal{L} (\mathcal{D}_r \mathcal{V}_i \mathcal{D}_r^T)^{-\frac{1}{2}}, \quad (6.60)$$

$$\mathcal{S}_i = \mathcal{R}^{-1} - \mathcal{R}^{-1} \mathcal{C}_l^T [\mathcal{V}_i - \mathcal{V}_i \mathcal{D}_r^T (\mathcal{D}_r \mathcal{V}_i \mathcal{D}_r^T)^{-1} \mathcal{D}_r \mathcal{V}_i] \mathcal{C}_l \mathcal{R}^{-1}, \quad (6.61)$$

$$\mathcal{V}_i = (\mathcal{C}_l \mathcal{R}^{-1} \mathcal{C}_l^T - \mathcal{E}_i)^{-1} > 0. \quad (6.62)$$

Finalmente, el parámetro buscado Z_i es:

$$Z_i = X^{-1}\mathcal{X}_i. \quad (6.63)$$

Con esto, se asegura la estabilidad del observador ODG mediante la factibilidad de las LMIs anteriores.

6.2. Simulación con esquemas de ataque

En esta sección se presentan los resultados de simulación del observador ODG aplicado al sistema de tres tanques interconectados en su representación Takagi–Sugeno discreta. Se analizan diversos escenarios de ataques a actuadores bajo diferentes configuraciones, empleando las lógicas **uniforme** y **no uniforme** basadas en procesos estocásticos de Markov. El objetivo es validar la capacidad del observador para generar residuos que permitan **detectar, aislar y localizar ataques** en los actuadores del sistema.

Para todas las simulaciones, se emplearon:

- Los parámetros del sistema listados en la Tabla 4.1.
- Entradas de tipo escalón para las bombas: $Q_1(k) = 0.368 \times 10^{-4} \text{ m}^3/\text{s}$ aplicada en $t = 184 \text{ s}$, y $Q_2(k) = 0.252 \times 10^{-4} \text{ m}^3/\text{s}$ aplicada en $t = 70 \text{ s}$.

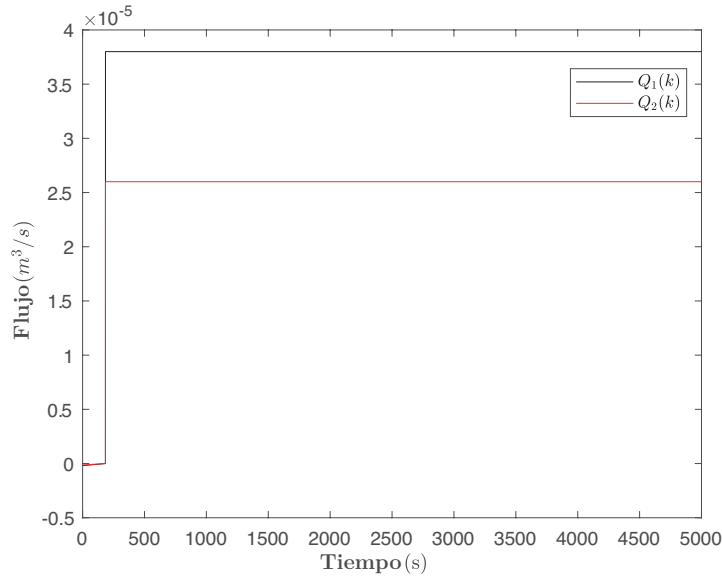


Fig. 6.2. Entradas de caudal $Q_1(k)$ y $Q_2(k)$ aplicadas al sistema de tres tanques.

A continuación, se presentan los resultados para cada tipo de ataque considerado: DoS, DDA y RDI.

6.2.1. Caso 1: Ataque DoS en actuador con lógica uniforme

En este primer escenario, se considera un **ataque DoS (Denial of Service)** aplicado únicamente al **actuador** u_1 del sistema bajo lógica uniforme de activación Markoviana. El ataque bloquea periódicamente la medición del actuador, afectando la estimación de los estados.

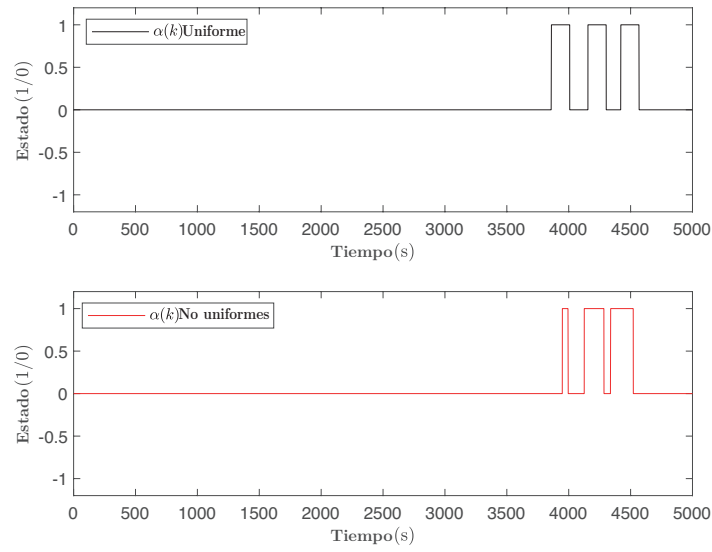


Fig. 6.3. Distribución de activación del ataque DoS en actuador u_1 (lógica uniforme Markoviana).

La Figura 6.4 muestra el comportamiento de los estados estimados por el observador y los residuos generados bajo este escenario:

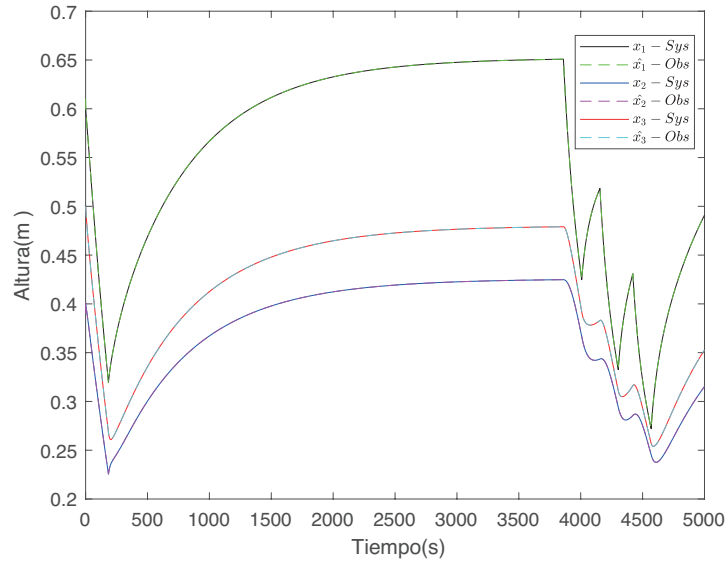


Fig. 6.4. Evolución de los estados x_1 , x_2 , x_3 bajo ataque DoS en u_1 .

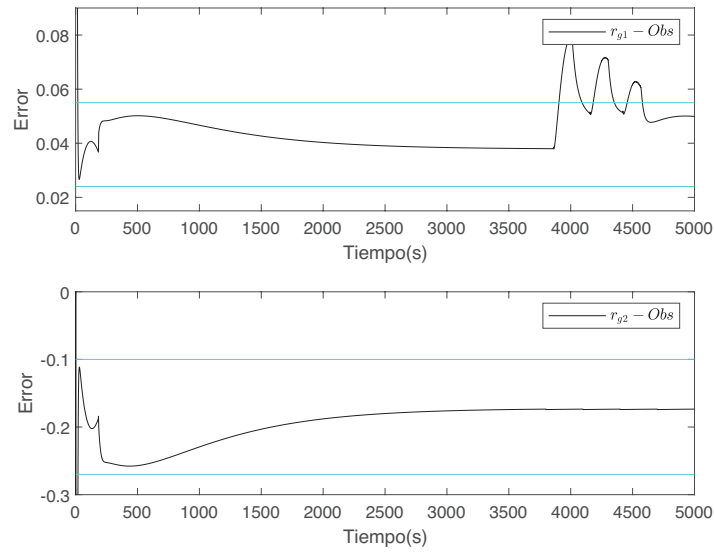


Fig. 6.5. Residuos generados por el observador ODG bajo ataque DoS uniforme.

Se observa que los residuos asociados al actuador atacado (r_2) presentan incrementos significativos durante los períodos de ataque, permitiendo su detección y aislamiento.

6.2.2. Caso 2: Ataque DDA en el actuador con lógica no uniforme

En este caso, se aplica un **ataque DDA (Data Deception Attack)** al actuador u_2 . Este tipo de ataque inyecta datos falsos en la señal de control, modificando su valor real. La activación del ataque sigue una lógica **no uniforme**, lo que introduce intervalos irregulares de perturbación.

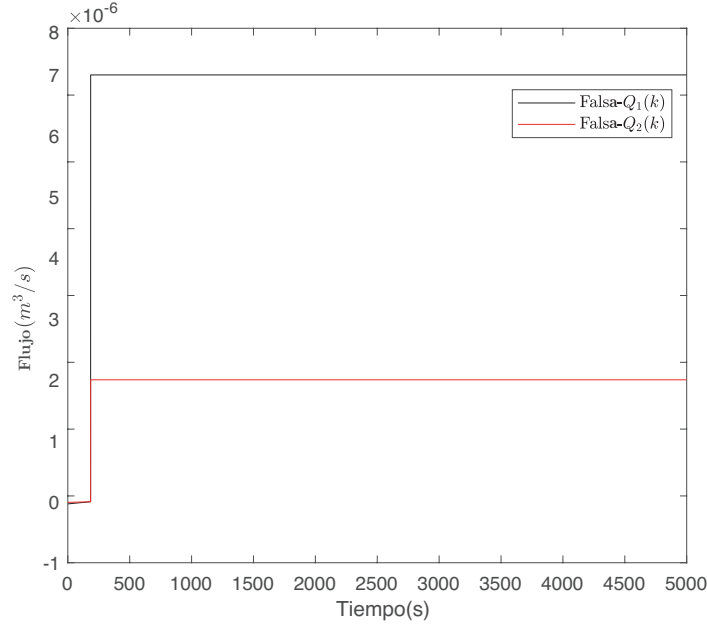


Fig. 6.6. Flujo del ataque DDA en el actuador u_2 con lógica no uniforme.

El impacto sobre los estados y los residuos se observa en las Figuras 6.7 y 6.8.

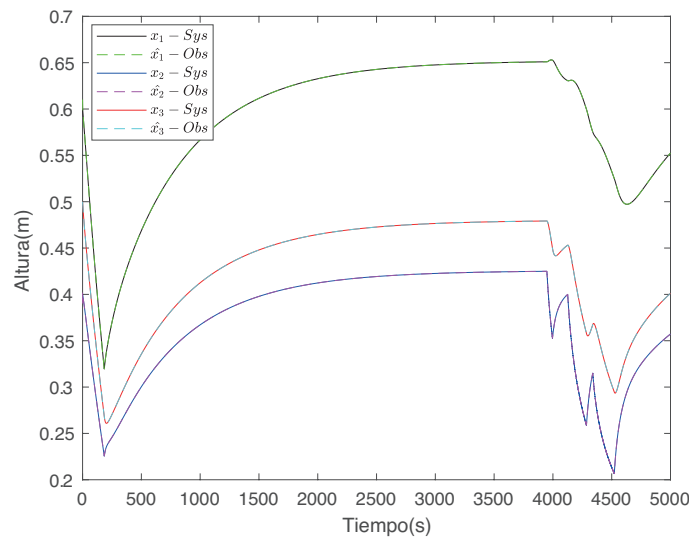


Fig. 6.7. Evolución de los estados bajo ataque DDA en el actuador u_2 .

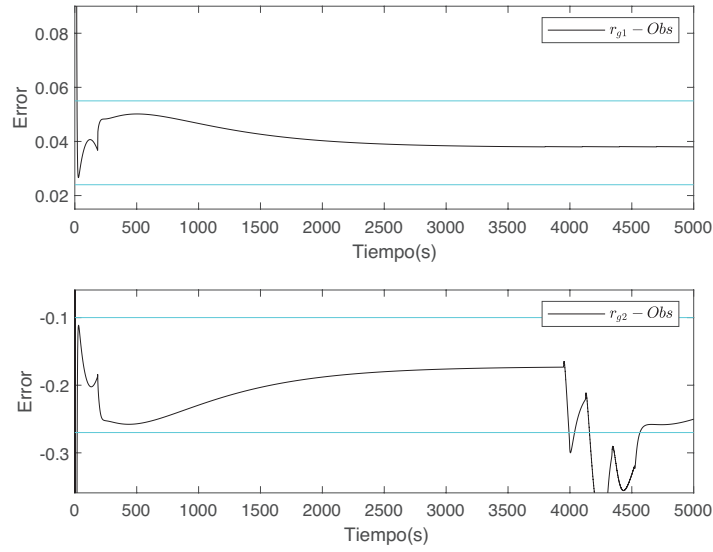


Fig. 6.8. Residuos generados por el observador ODG ante ataque DDA en el actuador u_2 .

Se aprecia que los residuos correspondientes muestran picos en cada evento de activación del ataque, validando su efectividad incluso bajo una lógica irregular.

6.2.3. Caso 3: Ataque RDI en el actuador con lógica uniforme

Por último, se evalúa un **ataque RDI (Random Data Injection)** sobre el actuador u_1 , en el cual se inyectan perturbaciones aleatorias en la señal de control. La activación sigue una **lógica uniforme**.

Los resultados obtenidos sobre los estados y los residuos generados se presentan en las Figuras 6.9 y 6.10.

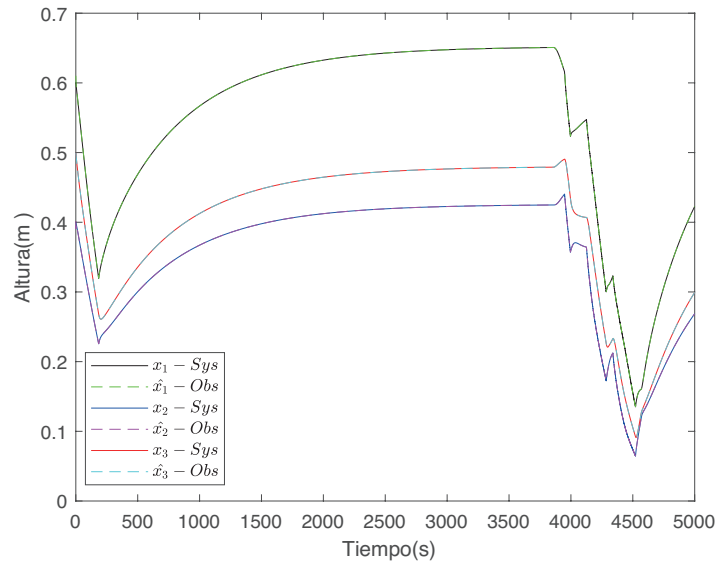


Fig. 6.9. Evolución de los estados bajo ataque RDI en el actuador u_1 .

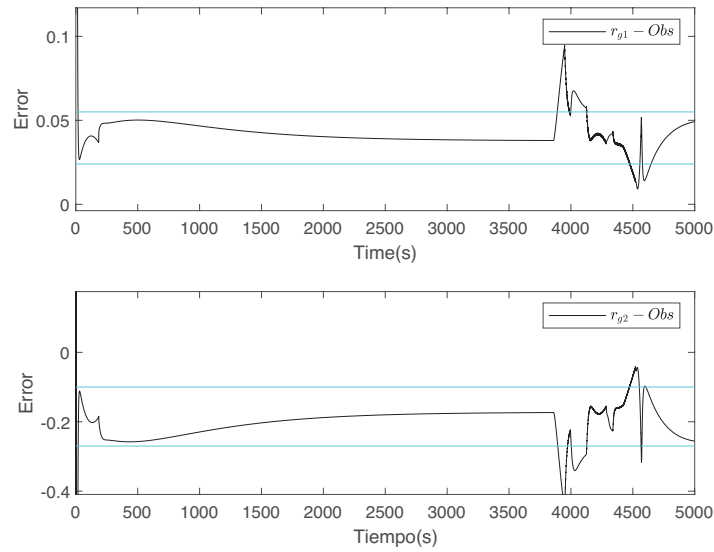


Fig. 6.10. Residuos generados por el observador ODG ante ataque RDI en el actuador u_1 .

Los residuos reflejan el efecto aleatorio de la inyección de datos, mostrando respuestas que permiten la detección clara de la intrusión.

6.2.4. Caso 4: Ataques simultáneos en el actuador

En esta simulación, se considera un escenario con ataques simultáneos dirigidos a ambos actuadores del sistema. La entrada $u_1(k)$ es afectada por un ataque de tipo **DDA (Data Deception Attack)**, mientras que la entrada $u_2(k)$ es perturbada mediante un ataque de tipo **RDI (Inyección Aleatoria de Datos)**, ambos aplicados bajo una lógica de activación **uniforme** basada en procesos de Markov.

En la Figura 6.11 se observa el comportamiento de los estados del sistema y sus estimaciones obtenidas por el observador ODG bajo la presencia de estos ataques. Se aprecia cómo las perturbaciones introducidas en ambos actuadores generan desviaciones significativas en los estados estimados en comparación con los valores reales.

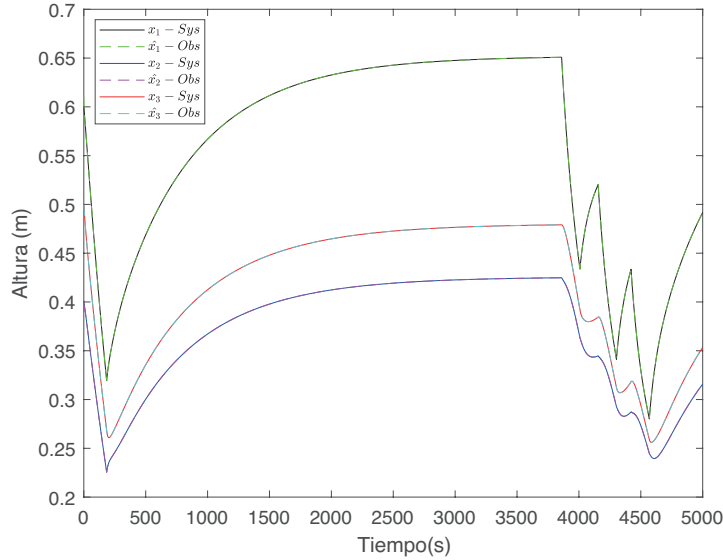


Fig. 6.11. Comportamiento del sistema en presencia de ataques simultáneos uniformes sobre u_1 (DDA) y u_2 (RDI).

La Figura 6.12 muestra los residuos generados por el observador ante la presencia de estos ataques. Puede observarse que ambos residuos presentan picos claramente definidos durante los intervalos de activación de los ataques, lo que evidencia la efectividad del observador ODG para detectar y aislar ataques simultáneos en diferentes actuadores del sistema.

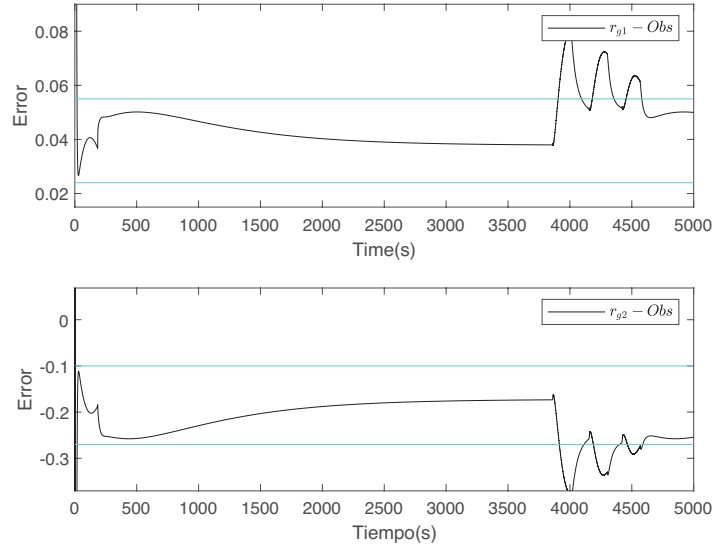


Fig. 6.12. Residuos generados por el observador ODG en presencia de ataques simultáneos uniformes sobre u_1 y u_2 .

Este escenario resalta la capacidad del observador para identificar de manera independiente intrusiones en múltiples actuadores, incluso cuando se presentan de manera concurrente y bajo diferentes tipos de ataque, confirmando su utilidad para el diagnóstico en sistemas ciberfísicos complejos.

6.3. Conclusiones del capítulo

En este capítulo se presentó el diseño y validación de un **Observador Dinámico Generalizado** aplicado al sistema de tres tanques interconectados modelado en su representación Takagi–Sugeno discreta. Este observador se empleó como una herramienta robusta para el **aislamiento y localización de ataques cibernéticos** dirigidos al sistema, centrándose específicamente en ataques que afectan a los actuadores.

- Se formularon los fundamentos matemáticos del observador ODG, estableciendo las condiciones de diseño necesarias para garantizar su estabilidad mediante funciones de Lyapunov y condiciones tipo LMI.
- Se integraron distintos esquemas de ataque en el análisis, incluyendo ataques de tipo **DoS**, **DDA** y **RDI**, evaluando su efecto sobre el sistema bajo lógicas de activación uniformes y no

uniformes basadas en procesos de Markov.

- A través de simulaciones detalladas, se comprobó la capacidad del observador ODG para generar **residuos sensibles y específicos** que permiten detectar y aislar ataques de manera precisa, incluso en escenarios complejos con ataques simultáneos.
- El análisis demostró que los residuos presentan firmas características para cada tipo de ataque, lo que facilita la discriminación entre diferentes intrusiones y refuerza la viabilidad del enfoque para su uso en entornos de **ciberseguridad aplicada al control**.

En conclusión, los resultados obtenidos validan la efectividad del observador ODG como una herramienta fundamental para la protección de sistemas ciberfísicos. Su capacidad para trabajar en entornos con ataques estocásticos, múltiples intrusiones y condiciones de operación no lineales lo posiciona como una solución adecuada para el diagnóstico y la mitigación de amenazas en aplicaciones de control industrial.

Capítulo 7

Observador ODG para la estimación de ataques de variación lenta

En este capítulo se propone un **Observador Dinámico Generalizado (ODG)** para la estimación de ataques **DDA (Data Deception Attack)** de variación lenta en sistemas ciberfísicos discretos representados bajo el modelo Takagi-Sugeno. El objetivo principal es diseñar un esquema de observación capaz de estimar el comportamiento dinámico de los ataques y generar una reconstrucción precisa del vector de estados ampliado, considerando tanto la dinámica no lineal del sistema como la naturaleza estocástica de la lógica Markoviana de los ataques.

7.1. Modelo matemático y diseño

Se considera un sistema ciberfísico en tiempo discreto bajo la representación Takagi-Sugeno afectado por un ataque de **DDA** aplicado en el canal de los actuadores. El sistema está definido como:

$$\begin{aligned} x(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) A_i x(k) + Bu(k) + G_a a_a(k), \\ y(k) &= Cx(k), \end{aligned} \tag{7.1}$$

donde $x(k) \in \mathbb{R}^n$ es el vector de estados, $u(k) \in \mathbb{R}^m$ es la entrada de control y $y(k) \in \mathbb{R}^p$ corresponde al vector de salidas medidas. Las matrices $A_i \in \mathbb{R}^{n \times n}$, $B \in \mathbb{R}^{n \times m}$, $C \in \mathbb{R}^{p \times n}$ y $G_a \in \mathbb{R}^{n \times r}$ son conocidas. Las funciones de peso $\mu_i(\rho(k))$ satisfacen:

$$\sum_{i=1}^{\kappa} \mu_i(\rho(k)) = 1, \quad \mu_i(\rho(k)) \geq 0, \quad \forall i, \tag{7.2}$$

donde $\kappa = 2^s$ corresponde al número de modelos locales lineales determinado por s , el número de no linealidades en el sistema.

Modelo del ataque DDA

El ataque de engaño de datos en el actuador se modela como:

$$a_a(k) = \alpha(k)a(k), \quad (7.3)$$

donde $\alpha(k) \in \{0, 1\}$ es una señal estocástica gobernada por un **proceso de Markov**, que define los instantes de activación o desactivación del ataque, y $a(k) \in \mathbb{R}^r$ representa la señal maliciosa inyectada.

Se consideran dos posibles lógicas para $\alpha(k)$:

- **Ataque uniforme:** períodos constantes de activación e inactividad del ataque.
- **Ataque no uniforme:** tiempos de activación e inactividad con duración irregular, definidos de forma aleatoria.

Además, se hace la siguiente suposición clave para ataques de variación lenta:

Si el ataque está activo, i.e. $\alpha(k) = 1$, entonces $a_a(k)$ es constante a tramos:

$$a_a(k) = a_a(k-1), \quad (7.4)$$

lo que implica que la señal maliciosa varía lentamente en el tiempo.

Modelo con vector extendido

Considerando (7.1) y (7.4), se define un vector extendido:

$$\beta(k) = \begin{bmatrix} x(k) \\ a_a(k-1) \end{bmatrix} \in \mathbb{R}^{n+r}. \quad (7.5)$$

El sistema extendido se expresa como:

$$\begin{aligned} \bar{E}\beta(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \bar{A}_i \beta(k) + \bar{B}u(k), \\ y(k) &= \bar{C}\beta(k), \end{aligned} \quad (7.6)$$

donde:

$$\bar{E} = \begin{bmatrix} I_n & -G_a \\ 0 & I_r \end{bmatrix}, \quad \bar{A}_i = \begin{bmatrix} A_i & 0 \\ 0 & I_r \end{bmatrix}, \quad \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} C & 0 \end{bmatrix}. \quad (7.7)$$

Dado que $\bar{E}$ es de rango completo, el sistema (7.6) se simplifica como:

$$\begin{aligned} \beta(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) (\tilde{A}_i \beta(k)) + \tilde{B} u(k), \\ y(k) &= \bar{C} \beta(k), \end{aligned} \quad (7.8)$$

con $\tilde{A}_i = \bar{E}^{-1} \bar{A}_i$ y $\tilde{B} = \bar{E}^{-1} \bar{B}$.

Condición de observabilidad

Para diseñar el ODG, se asume que el sistema extendido (7.8) cumple la condición de observabilidad:

$$\text{rank} \begin{bmatrix} \bar{C} \\ \bar{C} \tilde{A}_i \\ \vdots \\ \bar{C} \tilde{A}_i^{n-1} \end{bmatrix} = n + r, \quad \forall i = 1, \dots, \kappa. \quad (7.9)$$

En la siguiente sección, se presentará el **diseño del Observador Dinámico Generalizado** con base en el modelo extendido (7.8), seguido del análisis de parametrización y condiciones de estabilidad.

7.1.1. Parametrización del observador

Procedimiento (basado en el capítulo anterior). A partir del modelo T–S discreto y de las condiciones de acoplamiento del ODG, la parametrización se obtiene siguiendo estos pasos:

1. *Preparación de matrices auxiliares.* Defina $\Sigma = \begin{bmatrix} E \\ C \end{bmatrix}$, $\Omega = \begin{bmatrix} I_{n+r} \\ C \end{bmatrix}$, donde $E \in \mathbb{R}^{q_0 \times (n+r)}$ tiene rango completo en filas. Use la pseudoinversa de Moore–Penrose $(\cdot)^+$.
2. *Cálculo de (T, K) .* Obtenga T y K mediante las expresiones cerradas con Ω^+ e introduzca un grado de libertad Z .
3. *Cálculo de $(N_i, \tilde{K}_i)$.* Para cada vértice $i = 1, \dots, \kappa$, compute N_i y $\tilde{K}_i$ a partir de $TA_i\Sigma^+$; use una matriz libre $\tilde{Y}_i$.
4. *Recuperación de F_i (si se requiere).* $F_i = \tilde{K}_i + N_i K$.

5. *Cálculo de (S_i, M_i, P, Q) .* Resuelva el bloque lineal conjunto imponiendo las condiciones de acoplamiento; use una matriz libre W_{i1} .
6. *Ajuste de grados de libertad.* Sintonicice Z , $\tilde{Y}_i$ y W_{i1} para cumplir las especificaciones (desacoplo/detección) y las LMIs de estabilidad presentadas más adelante.

A continuación se listan las expresiones cerradas empleadas en el diseño.

Matrices T y K

$$\begin{aligned} T &= E \Omega^+ \begin{bmatrix} I_{n+r} \\ 0 \end{bmatrix} - Z (I_{n+r+p} - \Omega \Omega^+) \begin{bmatrix} I_{n+r} \\ 0 \end{bmatrix}, \\ K &= E \Omega^+ \begin{bmatrix} 0 \\ I_p \end{bmatrix} - Z (I_{n+r+p} - \Omega \Omega^+) \begin{bmatrix} 0 \\ I_p \end{bmatrix}. \end{aligned} \quad (7.10)$$

Matrices N_i y $\tilde{K}_i$

$$\begin{aligned} N_i &= T A_i \Sigma^+ \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix} - \tilde{Y}_i (I_{q_0+p} - \Sigma \Sigma^+) \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}, \\ \tilde{K}_i &= T A_i \Sigma^+ \begin{bmatrix} 0 \\ I_p \end{bmatrix} - \tilde{Y}_i (I_{q_0+p} - \Sigma \Sigma^+) \begin{bmatrix} 0 \\ I_p \end{bmatrix}. \end{aligned} \quad (7.11)$$

Matrices S_i , M_i , P y Q

$$\begin{aligned} S_i &= -W_{i1} (I_{q_0+p} - \Sigma \Sigma^+) \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}, \\ M_i &= -W_{i1} (I_{q_0+p} - \Sigma \Sigma^+) \begin{bmatrix} K \\ I_p \end{bmatrix}, \\ P &= \Sigma^+ \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}, \quad Q = \Sigma^+ \begin{bmatrix} K \\ I_p \end{bmatrix}. \end{aligned} \quad (7.12)$$

Los parámetros libres Z , $\tilde{Y}_i$ y W_{i1} se seleccionan posteriormente para satisfacer las LMIs de estabilidad y, en su caso, las condiciones de desacoplo/detección propuestas. Así también, por simplicidad, se asume que $W_2 = 0$. La dinámica del error del observador (6.45) puede escribirse como:

$$\varphi(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) (\mathbb{A}_{i1} - \mathbb{Y}_i \mathbb{A}_2) \varphi(k), \quad (7.13)$$

donde $\mathbb{A}_{i1} = \begin{bmatrix} N_{i1} - Z N_{i2} & 0 \\ 0 & 0 \end{bmatrix}$, $\mathbb{A}_2 = \begin{bmatrix} N_3 & 0 \\ 0 & -I_{q_0} \end{bmatrix}$, $\mathbb{Y}_i = \begin{bmatrix} \tilde{Y}_i & H_i \\ W_{i1} & L_i \end{bmatrix}$ and $\varphi(k) = \begin{bmatrix} \varepsilon(k) \\ v(k) \end{bmatrix}$.

7.1.2. Análisis de estabilidad del observador

En esta sección se realiza el análisis de estabilidad de la dinámica del error de estimación del observador, dada por la ecuación (8.27), mediante el uso de una función de Lyapunov discreta común para todos los submodelos difusos del sistema. **Teorema:** Existe un observador de la forma (8.5)-(8.8) para el sistema (7.1) sujeto a un ataque DDA en el actuador, tal que la dinámica del error (8.27) es estable, si existen matrices $X_1 = X_1^T$, $X_2 = X_2^T$ y W que satisfacen las siguientes LMIs:

$$X = X^T = \begin{bmatrix} X_1 & X_1 \\ X_1 & X_2 \end{bmatrix} > 0, \quad (7.14)$$

$$\mathcal{C}^{T\perp} \begin{bmatrix} -X_1 & -X_1 & \Pi_i^T & \Pi_i^T \\ -X_1 & -X_2 & 0 & 0 \\ \Pi_i & 0 & -X_1 & -X_1 \\ \Pi_i & 0 & -X_1 & -X_2 \end{bmatrix} \mathcal{C}^{T\perp T} < 0, \quad (7.15)$$

donde $\Pi_i = X_1 N_{i1} - W N_{i2}$. En este caso, $Z = X_1^{-1}W$ y las matrices $\mathbb{Y}_i$ se parametrizan como:

$$\mathbb{Y}_i = X^{-1} \left(\mathcal{B}_r^+ \mathcal{K}_i \mathcal{C}_l^+ + \mathcal{Z} - \mathcal{B}_r^+ \mathcal{B}_r \mathcal{Z} \mathcal{C}_l^+ \right), \quad (7.16)$$

donde $\mathcal{Z}$ es una matriz arbitraria de dimensiones apropiadas y las matrices auxiliares $\mathcal{K}_i$, $\mathcal{S}_i$ y $\mathcal{V}_i$ se definen como:

$$\mathcal{K}_i = -\mathcal{R}^{-1} \mathcal{B}_l^T \mathcal{V}_i \mathcal{C}_r^T (\mathcal{C}_r \mathcal{V}_i \mathcal{C}_r^T)^{-1} + \mathcal{S}_i^{1/2} \mathcal{L} (\mathcal{C}_r \mathcal{V}_i \mathcal{C}_r^T)^{-1/2}, \quad (7.17)$$

$$\mathcal{S}_i = \mathcal{R}^{-1} - \mathcal{R}^{-1} \mathcal{B}_l^T \left[\mathcal{V}_i - \mathcal{V}_i \mathcal{C}_r^T (\mathcal{C}_r \mathcal{V}_i \mathcal{C}_r^T)^{-1} \mathcal{C}_r \mathcal{V}_i \right] \mathcal{B}_l \mathcal{R}^{-1}, \quad (7.18)$$

$$\mathcal{V}_i = \left(\mathcal{B}_l \mathcal{R}^{-1} \mathcal{B}_l^T - \mathcal{D}_i \right)^{-1} > 0, \quad (7.19)$$

con

$$\mathcal{D}_i = \begin{bmatrix} -X_1 & -X_1 & \Pi_i^T & \Pi_i^T \\ -X_1 & -X_2 & 0 & 0 \\ \Pi_i & 0 & -X_1 & -X_1 \\ \Pi_i & 0 & -X_1 & -X_2 \end{bmatrix}, \quad (7.20)$$

$$\mathcal{B} = \begin{bmatrix} 0 \\ -I_{q_0+q_1} \end{bmatrix}, \mathcal{C} = \begin{bmatrix} N_3 & 0 & 0 & 0 \\ 0 & -I_{q_0} & 0 & 0 \end{bmatrix} \text{ y } \mathcal{C}^{T\perp} = \begin{bmatrix} [N_3^{T\perp} & 0] & 0 \\ 0 & I_{q_0+q_1} \end{bmatrix}.$$

Las matrices $\mathcal{L}$ y $\mathcal{R}$ son arbitrarias y cumplen $\|\mathcal{L}\| < 1$ y $\mathcal{R} > 0$ de forma que $\mathcal{V}_i$ sea definida positiva. Además, $\mathcal{C}_l$, $\mathcal{C}_r$ y $\mathcal{B}_l$, $\mathcal{B}_r$ son factores de rango completo de $\mathcal{B}$ y $\mathcal{C}$, cumpliendo $\mathcal{B} = \mathcal{B}_l \mathcal{B}_r$ y $\mathcal{C} = \mathcal{C}_l \mathcal{C}_r$.

Demostración. Considere la función de Lyapunov:

$$V(\varphi(k)) = \varphi^T(k)X\varphi(k) > 0, \quad (7.21)$$

donde $X = \begin{bmatrix} X_1 & X_1 \\ X_1 & X_2 \end{bmatrix} > 0$ con $X_1 = X_1^T$ y $X_2 = X_2^T$. La diferencia de Lyapunov se expresa como:

$$\begin{aligned} \Delta V(\varphi(k)) &= V(\varphi(k+1)) - V(\varphi(k)) \\ &= \varphi^T(k+1)X\varphi(k+1) - \varphi^T(k)X\varphi(k) < 0. \end{aligned} \quad (7.22)$$

Sustituyendo $\varphi(k+1) = (\mathbb{A}_{i1} - \mathbb{Y}_i\mathbb{A}_2)\varphi(k)$:

$$\Delta V(\varphi(k)) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \varphi^T(k) \left[(\mathbb{A}_{i1} - \mathbb{Y}_i\mathbb{A}_2)^T X (\mathbb{A}_{i1} - \mathbb{Y}_i\mathbb{A}_2) - X \right] \varphi(k) < 0. \quad (7.23)$$

La condición equivalente es:

$$(\mathbb{A}_{i1} - \mathbb{Y}_i\mathbb{A}_2)^T X (\mathbb{A}_{i1} - \mathbb{Y}_i\mathbb{A}_2) - X < 0 \quad \forall i \in \{1, \dots, \kappa\}. \quad (7.24)$$

que mediante el *complemento de Schur* se expresa como:

$$\begin{bmatrix} -X & (\mathbb{A}_{i1} - \mathbb{Y}_i\mathbb{A}_2)^T X \\ X(\mathbb{A}_{i1} - \mathbb{Y}_i\mathbb{A}_2) & -X \end{bmatrix} < 0 \quad \forall i \in \{1, \dots, \kappa\}. \quad (7.25)$$

Aplicando el *Lema de Eliminación Skelton y col.* (1997), la desigualdad (7.25) se reescribe como:

$$\mathcal{B}\mathcal{X}_i\mathcal{C} + (\mathcal{B}\mathcal{X}_i\mathcal{C})^T + \mathcal{D}_i < 0 \quad \forall i \in \{1, \dots, \kappa\}, \quad (7.26)$$

donde $\mathcal{X}_i = X\mathbb{Y}_i$. Esto equivale a:

$$\mathcal{B}^\perp \mathcal{D}_i \mathcal{B}^{\perp T} < 0 \quad \forall i \in \{1, \dots, \kappa\}, \quad (7.27)$$

$$\mathcal{C}^{T\perp} \mathcal{D}_i \mathcal{C}^{T\perp T} < 0 \quad \forall i \in \{1, \dots, \kappa\}. \quad (7.28)$$

Al resolver estas condiciones LMIs se obtiene la estabilidad del observador y la parametrización de las matrices $\mathbb{Y}_i$ como en (8.37)-(8.40). $\square$

Algoritmo de diseño del observador ODG

El procedimiento para el diseño del observador se resume como:

1. Seleccionar una matriz arbitraria $E \in \mathbb{R}^{q_0 \times (n+r)}$ tal que $\text{rank}(\Sigma) = n + r$, con $\Sigma = \begin{bmatrix} E \\ C \end{bmatrix}$.

2. Calcular T_1, T_2, K_1, K_2 usando (7.10).
3. Obtener matrices $N_{i1}, N_{i2}, \tilde{K}_{i1}, \tilde{K}_{i2}$ y N_3 a partir de $\tilde{A}_i$.
4. Resolver las LMIs (7.14) y (7.15) para encontrar X, W y luego $Z = X^{-1}W$.
5. Determinar $\mathbb{Y}_i$ mediante (8.37).
6. Calcular las matrices finales del observador $N_i, F_i, S_i, M_i, P, Q, J, H_i$ y L_i .

7.2. Simulaciones: ODG con ataques de variación lenta

Con el objetivo de validar el desempeño del **Observador Dinámico Generalizado** en la estimación de ataques de variación lenta, se realizaron simulaciones sobre el sistema de *tres tanques interconectados* en su representación T-S discreta. Se utilizaron los **parámetros físicos** reportados en la Tabla 4.1 y un tiempo de muestreo T_d (con $t = k T_d$). Se consideraron escenarios de ataque **DDA (Data Deception Attack)** aplicados al actuador y lógicas de activación **Markovianas** uniforme y no uniforme.

7.2.1. Entradas del sistema y lógica Markoviana de ataque

Las entradas del sistema son los caudales de las bombas $\mathbf{Q}_1(\mathbf{k})$ y $\mathbf{Q}_2(\mathbf{k})$, mostrados en la Fig. 7.1. Ambas señales son *a trozos constantes*, lo que permite excitar la dinámica lenta del proceso:

- $Q_1(k)$ y $Q_2(k)$ presentan un *escalón inicial* y un *incremento tardío* (hacia el final del horizonte), permaneciendo acotadas en el orden de 10^{-5} .

Estas trayectorias *escalonadas y de larga duración* son adecuadas para evaluar la estimación del ataque por parte del ODG bajo condiciones estacionarias y casi-estacionarias.

Las señales de ataque se activan mediante procesos de Markov con **lógica uniforme** (intervalos de activación constantes) y **lógica no uniforme** (intervalos aleatorios), como se aprecia en la Fig. 7.2. La lógica no uniforme modela escenarios más realistas en CPS, con activaciones irregulares y difícilmente predecibles.

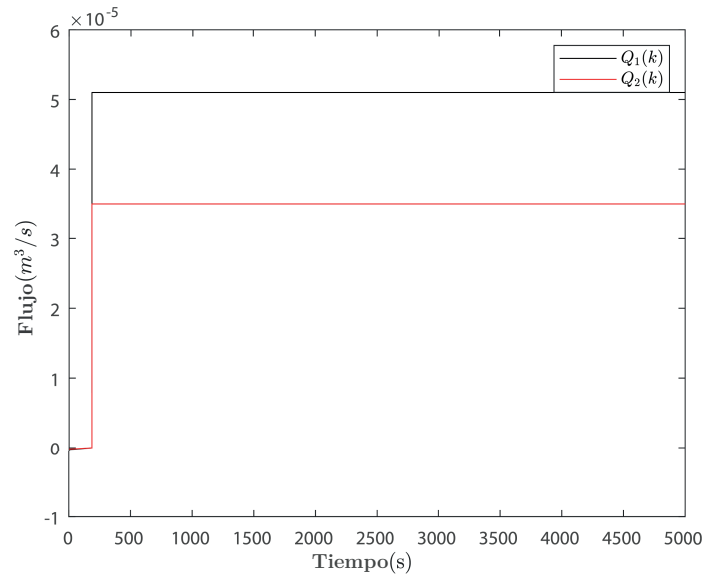


Fig. 7.1. Entradas de caudal variables utilizadas en el sistema de tres tanques interconectados.

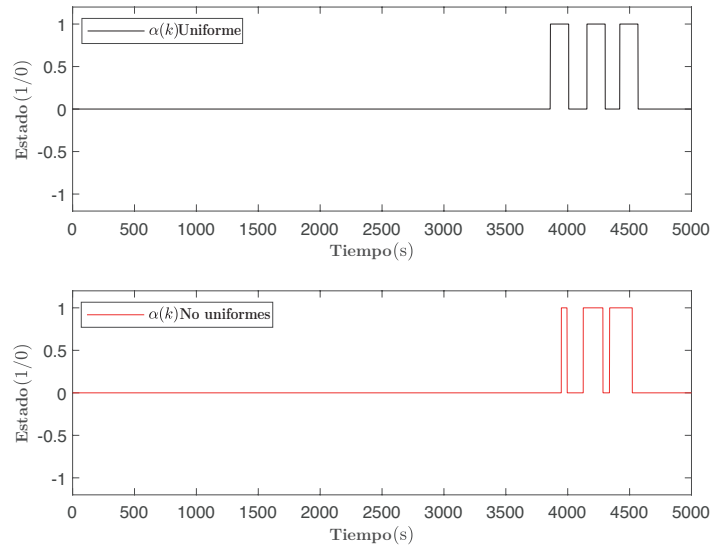


Fig. 7.2. Lógicas Markovianas de ataque: uniforme (línea negra) y no uniforme (línea roja).

7.2.2. Simulación con ataque uniforme

Se consideró primero un ataque **DDA uniforme** (Fig. 7.2, línea negra) que afecta simultáneamente a $u_1(k)$ y $u_2(k)$. La Fig. 7.3 muestra el *ataque sobre los actuadores* $a_a(k)$ y su **estimación** provista por el ODG. La Fig. 7.4 presenta la **estimación de estados** del proceso bajo dicho ataque; el

ODG reconstruye con fidelidad la dinámica de x_1 , x_2 y x_3 a pesar de la manipulación persistente en las entradas.

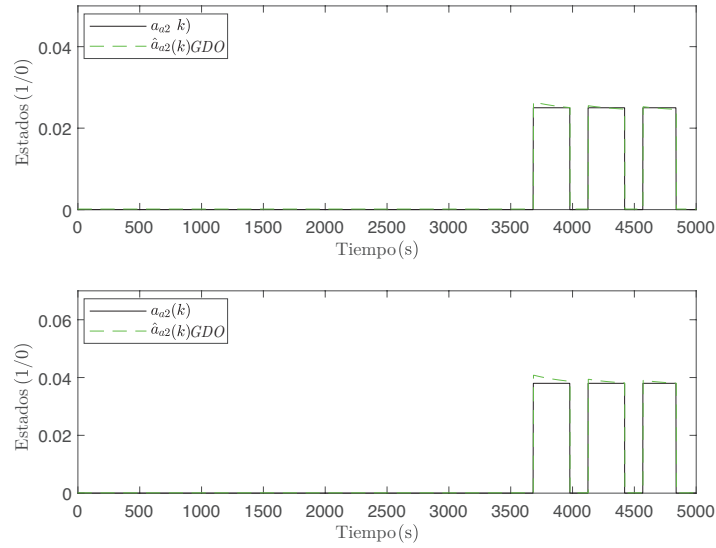


Fig. 7.3. Estimación de variables y esquema de ataque uniforme tipo FDI.

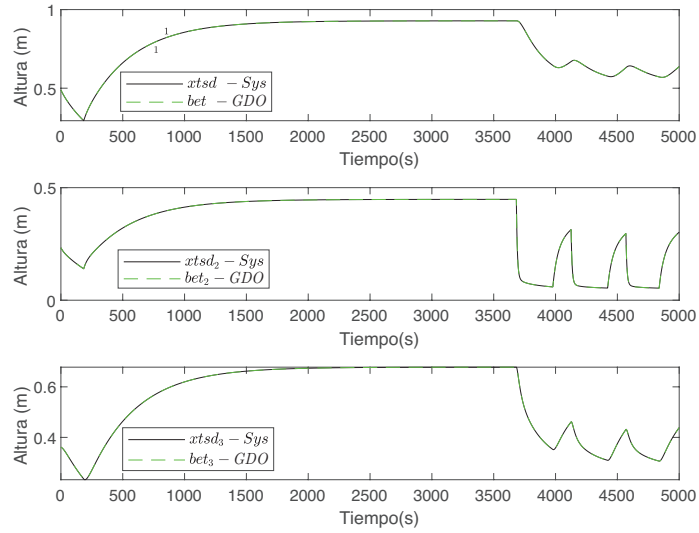


Fig. 7.4. Efecto del ataque uniforme DDA sobre las variables de estado y su estimación (ODG).

7.2.3. Simulación con ataque no uniforme

Posteriormente, se evaluó un **ataque DDA no uniforme** (Fig. 7.2, línea roja) aplicado sólo a $u_2(k)$. La Fig. 7.5 muestra el *perfil irregular del ataque* y su **estimación** con el ODG. En la Fig. 7.6 se observa que el ODG mantiene la **consistencia** de la estimación de estados ante activaciones estocásticas, con residuos que se activan en sincronía con los eventos de ataque.

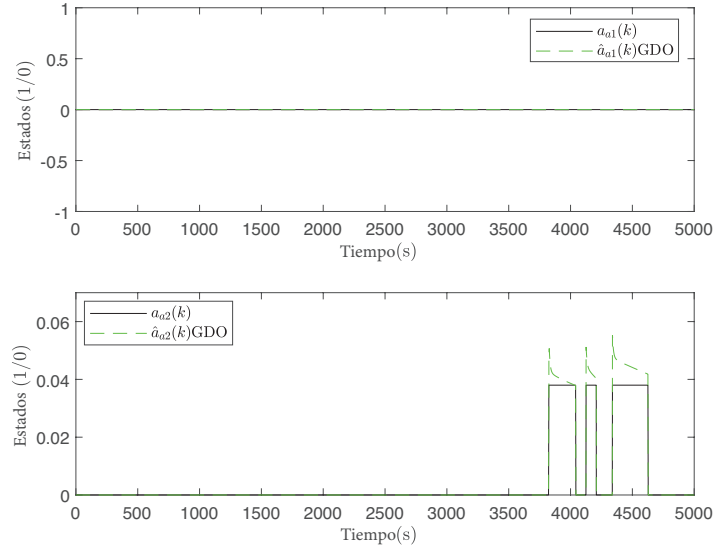


Fig. 7.5. Estimación de ataque tipo DDA con distribución no uniforme.

7.3. Conclusiones del capítulo

Las simulaciones con **dos escenarios** (DDA uniforme y DDA no uniforme) evidencian que el ODG:

- Reconstruye con precisión la **señal de ataque** $a_a(k)$ y los **estados** del sistema T-S discreto, incluso bajo lógicas de activación estocásticas.
- Mantiene **coherencia temporal** en la detección: la activación del residuo y la desviación estimada del ataque coinciden con los intervalos de la lógica Markoviana.
- Es adecuado como **módulo de diagnóstico** en CPS de dinámica lenta (como el proceso de tres tanques), preparando el terreno para estrategias de **control tolerante a ataques**.

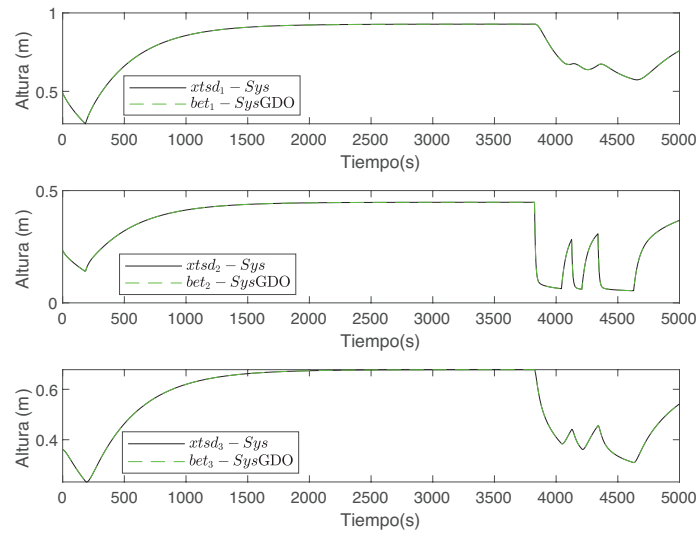


Fig. 7.6. Efecto del ataque no uniforme DDA sobre los estados del sistema y su estimación (ODG).

Capítulo 8

ODG para estimación de ataques dinámicos

En esta sección se aborda el diseño de un **Observador Dinámico Generalizado** orientado a la estimación simultánea de estados y ataques dinámicos en sistemas ciberfísicos discretos modelados bajo la representación Takagi-Sugeno (T-S). A diferencia de los casos previos centrados en ataques de variación lenta, aquí se considera explícitamente el comportamiento *dinámico* de ataques como *Data Deception Attack* (DDA), *Denial of Service* (DoS) y *Random Data Injection* (RDI), los cuales presentan cambios abruptos o estocásticos que requieren una estrategia de observación más flexible y robusta.

El desarrollo de esta propuesta se sustenta en tres elementos clave:

1. **Modelado extendido:** se plantea una formulación que integra explícitamente los efectos de ataques dinámicos tanto en sensores como en actuadores, incluyendo su representación bajo lógica Markoviana uniforme y no uniforme.
2. **Diseño del ODG:** se construye un observador con términos adicionales dedicados a la estimación directa de los ataques dinámicos, parametrizado mediante desigualdades matriciales lineales (LMIs) y el uso de herramientas como el complemento de Schur y el lema de eliminación.
3. **Validación en un caso práctico:** se evalúa el desempeño del ODG en un sistema de tres tanques interconectados sometido a escenarios combinados de ataques dinámicos, analizando su capacidad de reconstrucción precisa de estados y ataques bajo condiciones adversas.

Este capítulo se enfoca exclusivamente en el tratamiento de ataques con comportamiento dinámico, lo que supone un desafío adicional respecto a los ataques de variación lenta analizados previamente. La propuesta desarrollada demuestra que el ODG no sólo garantiza estabilidad en la estimación, sino que además preserva su precisión frente a variaciones rápidas y no periódicas de los ataques, lo cual es esencial para su implementación en esquemas de **control resiliente en sistemas ciberfísicos discretos**.

8.1. Modelo matemático del sistema con ataques dinámicos

Partimos del modelo nominal del CPS en su representación Takagi–Sugeno (T–S) en tiempo discreto, con κ reglas y funciones de pertenencia $\mu_i(\rho(k))$ que satisfacen $\sum_{i=1}^{\kappa} \mu_i(\rho(k)) = 1$, $\mu_i(\rho(k)) \geq 0$:

$$\begin{aligned} x(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) A_i x(k) + B u(k), \\ y(k) &= C x(k). \end{aligned} \quad (8.1)$$

Para incorporar explícitamente ataques en sensores y actuadores, se reformula el sistema utilizando un **vector extendido** que agrupa los estados originales con las variables asociadas a los ataques en sensores, a saber

$$\eta(k) = \begin{bmatrix} x(k) \\ a_{\beta}(k) \end{bmatrix}, \quad (8.2)$$

y se obtiene la estructura extendida:

$$\begin{aligned} \bar{E} \eta(k+1) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \bar{A}_i \eta(k) + \bar{B} u(k) + G_a a_{\alpha}(k), \\ y(k) &= \bar{C} \eta(k), \end{aligned} \quad (8.3)$$

donde

$$\bar{E} = \begin{bmatrix} I_n & 0 \end{bmatrix}, \quad \bar{A}_i = \begin{bmatrix} A_i & 0 \end{bmatrix}, \quad \bar{B} = \begin{bmatrix} B \\ 0 \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} C & F_s \end{bmatrix},$$

y el vector extendido $\eta(k)$ está dado por (8.2). (En particular, $F_s \in \mathbb{R}^{p \times r_s}$ distribuye los ataques de sensor $a_{\beta}(k) \in \mathbb{R}^{r_s}$ en la salida, y $G_a \in \mathbb{R}^{n \times r_a}$ modela los ataques de actuador $a_{\alpha}(k) \in \mathbb{R}^{r_a}$.)

Esta formulación permite representar el sistema bajo ataques de manera unificada, incorporando explícitamente las dinámicas de los estados $x(k)$ y de los ataques $a_{\beta}(k)$ sobre los sensores, mientras que los ataques $a_{\alpha}(k)$ afectan a los actuadores a través de la matriz G_a .

Para garantizar la estimación precisa de ambos componentes, se requiere que el sistema extendido cumpla con la condición de observabilidad:

$$\text{rank} \begin{bmatrix} \bar{E} & \bar{A}_i \\ 0 & \bar{C} \\ 0 & \bar{E} \end{bmatrix} = \text{rank}(\bar{E}) + n. \quad (8.4)$$

El cumplimiento de (8.4) asegura que tanto los estados internos como las señales de ataque puedan ser reconstruidos a partir de las mediciones del sistema, condición indispensable para el diseño de un **Observador Dinámico Generalizado (ODG)** robusto.

El ODG propuesto tiene como objetivo estimar simultáneamente:

- Los estados $x(k)$ del sistema ciberfísico.
- Los ataques dinámicos $a_\alpha(k)$ sobre actuadores y $a_\beta(k)$ sobre sensores.

Esto se logra mediante una estructura de observador que incorpora tanto la dinámica del sistema como modelos de estimación explícitos de ataques, asegurando resiliencia frente a escenarios en los que los ataques presentan naturaleza estocástica y lógica Markoviana, incluyendo tanto activaciones uniformes como no uniformes.

8.2. Estructura del Observador Dinámico Generalizado

A partir de la formulación extendida del sistema en (8.3), se propone el diseño de un **Observador Dinámico Generalizado** capaz de estimar tanto los estados del sistema como los ataques dinámicos sobre sensores y actuadores. El observador incorpora una estructura de múltiples ecuaciones que vinculan dinámicas internas auxiliares y términos de estimación directa de ataques.

El ODG se define como:

$$\zeta(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left(N_i \zeta(k) + H_i v(k) + F_i y(k) \right) \quad (8.5)$$

$$+ Ju(k) + TG_a \hat{a}_\alpha(k),$$

$$v(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left(S_i \zeta(k) + L_i v(k) + M_i y(k) \right), \quad (8.6)$$

$$\hat{a}_\alpha(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left(\Phi_i(\bar{C} \hat{\eta}(k) - y(k)) + \psi_i \hat{a}_\alpha(k) \right), \quad (8.7)$$

$$\hat{\eta}(k) = P \zeta(k) + Q y(k), \quad (8.8)$$

donde $\zeta(k) \in \mathbb{R}^{q_0}$ es el vector de estados internos del observador, $v(k) \in \mathbb{R}^{q_1}$ es un vector auxiliar que mejora la convergencia del estimador, $\hat{\eta}(k) \in \mathbb{R}^{n+f}$ es el vector estimado que incluye estados y ataques en sensores y $\hat{a}_\alpha(k) \in \mathbb{R}^r$ es la estimación de los ataques sobre actuadores.

Para garantizar la correcta reconstrucción de los estados y ataques, el observador debe satisfacer las siguientes condiciones de acoplamiento, derivadas de la estructura extendida del sistema:

$$N_i T \bar{E} + F_i \bar{C} - T \bar{A}_i = 0, \quad (8.9)$$

$$J = T \bar{B}, \quad (8.10)$$

$$S_i T \bar{E} + M_i \bar{C} = 0, \quad (8.11)$$

$$P T \bar{E} + Q \bar{C} = I_{n+f}. \quad (8.12)$$

Estas condiciones aseguran que la dinámica interna del ODG replica correctamente el comportamiento del sistema real extendido.

Definiendo el error transformado como:

$$\varepsilon(k) = \zeta(k) - T \bar{E} \eta(k), \quad (8.13)$$

y considerando (8.5), la dinámica del error se expresa como:

$$\varepsilon(k+1) = \sum_{i=1}^{\kappa} \mu_i(\eta(k)) \left[N_i \varepsilon(k) + H_i v(k) \right] + TG_a \tilde{a}_\alpha(k), \quad (8.14)$$

donde $\tilde{a}_\alpha(k) = \hat{a}_\alpha(k) - a_\alpha(k)$ es el error de estimación del ataque en el actuador.

La relación entre el error de estimación de estados y el error del observador es:

$$e_\beta(k) = \eta(k) - \hat{\eta}(k) = P\varepsilon(k). \quad (8.15)$$

La dinámica de error para la estimación de ataques se deduce a partir de (8.7):

$$\tilde{a}_\alpha(k+1) = \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left(\Phi_i \mathbb{A}_c \varphi(k) + \psi_i \tilde{a}_\alpha(k) + \mathbb{B}_{ci} \delta(k) \right), \quad (8.16)$$

con:

$$\varphi(k) = \begin{bmatrix} \varepsilon(k) \\ v(k) \end{bmatrix}, \quad \delta(k) = \begin{bmatrix} a_\alpha(k) \\ a_\alpha(k+1) \end{bmatrix},$$

y las matrices:

$$\mathbb{A}_c = \begin{bmatrix} \bar{C}P & 0 \end{bmatrix}, \quad \mathbb{B}_{ci} = \begin{bmatrix} \psi_i & -I \end{bmatrix}.$$

Finalmente, la dinámica conjunta de error del observador y del ataque se integra en el sistema aumentado:

$$\xi(k+1) = \sum_{i=1}^{\kappa} \mu_i(\xi(k)) \bar{\mathbb{A}}_i \xi(k) + \mathbb{B}_i \delta(k), \quad (8.17)$$

$$e(k) = \mathbb{C} \xi(k), \quad (8.18)$$

donde:

$$\xi(k) = \begin{bmatrix} \varphi(k) \\ \tilde{a}_\alpha(k) \end{bmatrix},$$

$$\bar{\mathbb{A}}_i = \begin{bmatrix} \mathbb{A}_{i1} - \mathbb{Y}_i \mathbb{A}_2 & -\mathbb{A}_b \\ \Phi_i \mathbb{A}_c & \psi_i \end{bmatrix}, \quad \mathbb{B}_i = \begin{bmatrix} 0 \\ \mathbb{B}_{ci} \end{bmatrix}, \quad \mathbb{C} = \begin{bmatrix} 0 & 0 & \Theta \end{bmatrix}.$$

Este modelo aumentado será la base para el análisis de estabilidad mediante funciones de Lyapunov y condiciones LMI.

8.3. Diseño del Observador Dinámico Generalizado (ODG)

En esta sección se detalla el procedimiento de parametrización del ODG, el cual permite obtener las matrices que satisfacen las condiciones (8.9)-(8.12). El diseño se basa en la utilización de factorizaciones matriciales, pseudoinversas y grados de libertad mediante matrices arbitrarias que garantizan la estabilidad y factibilidad del observador.

8.3.1. Parametrización del observador

Sea

$$\Sigma = \begin{bmatrix} R \\ \bar{C} \end{bmatrix}, \quad \Omega = \begin{bmatrix} \bar{E} \\ \bar{C} \end{bmatrix},$$

con R de rango completo. Sean Z matrices libres de dimensiones adecuadas. Entonces:

$$T = \underbrace{R\Omega^+ \begin{bmatrix} I_{n+r} \\ 0 \end{bmatrix}}_{T_1} - Z \underbrace{\left(I_{n+r+p} - \Omega\Omega^+ \right) \begin{bmatrix} I_{n+r} \\ 0 \end{bmatrix}}_{T_2}, \quad (8.19)$$

$$K = \underbrace{R\Omega^+ \begin{bmatrix} 0 \\ I_p \end{bmatrix}}_{K_1} - Z \underbrace{\left(I_{n+r+p} - \Omega\Omega^+ \right) \begin{bmatrix} 0 \\ I_p \end{bmatrix}}_{K_2}. \quad (8.20)$$

Cálculo de matrices N_i y $\tilde{K}_i$

Sea $\tilde{Y}_i$ libre. Entonces:

$$N_i = \underbrace{T_1 \bar{A}_i \Sigma^+ \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}}_{N_{i1}} - Z \underbrace{T_2 \bar{A}_i \Sigma^+ \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}}_{N_{i2}} - \tilde{Y}_i \underbrace{\left(I_{q_0+p} - \Sigma\Sigma^+ \right) \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}}_{N_3}, \quad (8.21)$$

$$\tilde{K}_i = \underbrace{T_1 \bar{A}_i \Sigma^+ \begin{bmatrix} 0 \\ I_p \end{bmatrix}}_{\tilde{K}_{i1}} - Z \underbrace{T_2 \bar{A}_i \Sigma^+ \begin{bmatrix} 0 \\ I_p \end{bmatrix}}_{\tilde{K}_{i2}} - \tilde{Y}_i \underbrace{\left(I_{q_0+p} - \Sigma\Sigma^+ \right) \begin{bmatrix} 0 \\ I_p \end{bmatrix}}_{\tilde{K}_3}. \quad (8.22)$$

Obtención de S_i , M_i , P y Q

Sean W_{i1} y W_2 libres. Entonces:

$$S_i = -W_{i1} \left(I_{q_0+p} - \Sigma\Sigma^+ \right) \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}, \quad (8.23)$$

$$M_i = -W_{i1} \left(I_{q_0+p} - \Sigma\Sigma^+ \right) \begin{bmatrix} K \\ I_p \end{bmatrix}, \quad (8.24)$$

$$P = \Sigma^+ \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix} - W_2 \left(I_{q_0+p} - \Sigma\Sigma^+ \right) \begin{bmatrix} I_{q_0} \\ 0 \end{bmatrix}, \quad (8.25)$$

$$Q = \Sigma^+ \begin{bmatrix} K \\ I_p \end{bmatrix} - W_2 \left(I_{q_0+p} - \Sigma\Sigma^+ \right) \begin{bmatrix} K \\ I_p \end{bmatrix}. \quad (8.26)$$

Para simplicidad, puede adoptarse $W_2 = 0$.

8.3.2. Ecuación de error del ODG

Sustituyendo en (6.45), la dinámica de error del observador queda:

$$\varphi(k+1) = \sum_{i=1}^{\kappa} \mu_i(\varphi(k)) [\mathbb{A}_{i1} - \mathbb{Y}_i \mathbb{A}_2] \varphi(k) + \mathbb{A}_b \tilde{a}_\alpha(k), \quad (8.27)$$

donde:

$$\mathbb{A}_{i1} = \begin{bmatrix} N_{i1} - ZN_{i2} & 0 \\ 0 & 0 \end{bmatrix}, \quad \mathbb{A}_2 = \begin{bmatrix} N_3 & 0 \\ 0 & -I_{q_0} \end{bmatrix}, \quad \mathbb{Y}_i = \begin{bmatrix} \tilde{Y}_i & H_i \\ W_{i1} & L_i \end{bmatrix}, \quad \mathbb{A}_b = \begin{bmatrix} TG_a \\ 0 \end{bmatrix}.$$

Este modelo servirá como base para el análisis de estabilidad presentado en la siguiente sección.

8.4. Análisis de estabilidad del ODG

Para garantizar la estabilidad del Observador Dinámico Generalizado (ODG) y la convergencia de sus estimaciones, se realiza un análisis basado en funciones de Lyapunov y condiciones tipo LMI. El objetivo es asegurar que la dinámica de error (8.27) sea asintóticamente estable, incluso en presencia de ataques dinámicos.

8.4.1. Planteamiento del problema de estabilidad

Se considera el sistema aumentado que integra la dinámica de error del observador y la estimación de los ataques, definido como:

$$\xi(k+1) = \sum_{i=1}^{\kappa} \mu_i(\xi(k)) (\bar{\mathbb{A}}_i \xi(k)) + \mathbb{B}_i \delta(k), \quad (8.28)$$

$$e(k) = \mathbb{C} \xi(k), \quad (8.29)$$

donde:

$$\xi(k) = \begin{bmatrix} \varphi(k) \\ \tilde{a}_\alpha(k) \end{bmatrix}, \quad \bar{\mathbb{A}}_i = \begin{bmatrix} \mathbb{A}_{i1} - \mathbb{Y}_i \mathbb{A}_2 & -\mathbb{A}_b \\ \Phi_i \mathbb{A}_c & \psi_i \end{bmatrix},$$

$$\mathbb{B}_i = \begin{bmatrix} 0 \\ \mathbb{B}_{ci} \end{bmatrix}, \quad \mathbb{C} = \begin{bmatrix} 0 & 0 & \Theta \end{bmatrix}, \quad \Theta = \sigma I_{nf}.$$

Aquí, $\delta(k) = \begin{bmatrix} a_\alpha(k) \\ a_\alpha(k+1) \end{bmatrix}$ representa la dinámica de los ataques, mientras que las matrices $\mathbb{A}_c$ y $\mathbb{B}_{ci}$ provienen de la propagación del error de estimación de ataques (8.16). El objetivo es determinar matrices $\mathbb{Y}_i$, Φ_i , ψ_i y Z que aseguren la estabilidad asintótica del sistema.

8.4.2. Función de Lyapunov y condiciones de estabilidad

Se define la siguiente función de Lyapunov candidata:

$$V(\xi(k)) = \xi^T(k)X\xi(k) > 0, \quad (8.30)$$

donde $X = \begin{bmatrix} X_1 & 0 \\ 0 & X_2 \end{bmatrix} > 0$, con:

$$X_1 = \begin{bmatrix} X_{11} & X_{11} \\ X_{11} & X_{12} \end{bmatrix} > 0, \quad X_{11} = X_{11}^T, \quad X_2 > 0.$$

La variación de $V(\xi(k))$ a lo largo de las trayectorias del sistema es:

$$\begin{aligned} \Delta V(\xi(k)) &= V(\xi(k+1)) - V(\xi(k)), \\ &= \xi^T(k+1)X\xi(k+1) - \xi^T(k)X\xi(k). \end{aligned} \quad (8.31)$$

Sustituyendo $\xi(k+1)$ de (8.28):

$$\begin{aligned} \Delta V(\xi(k)) &= \sum_{i=1}^{\kappa} \mu_i(\rho(k)) \left[(\bar{\mathbb{A}}_i \xi(k) + \mathbb{B}_i \delta(k))^T X (\bar{\mathbb{A}}_i \xi(k) + \mathbb{B}_i \delta(k)) \right] \\ &\quad - \xi(k)^T X \xi(k). \end{aligned} \quad (8.32)$$

8.4.3. Índice de desempeño $\mathcal{L}_2$

Para robustecer el análisis de estabilidad frente a perturbaciones $\delta(k)$, se define el índice de desempeño:

$$\mathbb{J} := \sum_{k=0}^{\infty} \|e(k)\|^2 - \gamma^2 \sum_{k=0}^{\infty} \|\delta(k)\|^2 < 0, \quad (8.33)$$

donde $\gamma > 0$ es una constante que limita la energía de la salida frente a perturbaciones.

De (8.33) y (8.32), se deriva que:

$$\mathbb{J} < \sum_{k=0}^{\infty} \xi(k)^T \mathbb{C}^T \mathbb{C} \xi(k) - \gamma^2 \delta(k)^T \delta(k) + \Delta V(\xi(k)) < 0. \quad (8.34)$$

Expresando en forma matricial:

$$\begin{bmatrix} \xi(k) \\ \delta(k) \end{bmatrix}^T \underbrace{\begin{bmatrix} \bar{\mathbb{A}}_i^T X \bar{\mathbb{A}}_i + \mathbb{C}^T \mathbb{C} - X & \bar{\mathbb{A}}_i^T X \mathbb{B}_i \\ \mathbb{B}_i^T X \bar{\mathbb{A}}_i & \mathbb{B}_i^T X \mathbb{B}_i - \gamma^2 I \end{bmatrix}}_{\mathcal{M}_i} \begin{bmatrix} \xi(k) \\ \delta(k) \end{bmatrix} < 0 \quad \forall i \in \{1, \dots, \kappa\}. \quad (8.35)$$

8.4.4. Formulación en LMIs

Para eliminar términos no lineales, se utilizan el Lema de Schur y el Lema de Eliminación, resultando en la condición LMI:

$$\mathcal{C}^{T\perp} \begin{bmatrix} -\Pi_{i1} - X_1 & \Pi_{i2} & \Phi_i \mathbb{A}_c^T X_2 \mathbb{B}_{ci} \\ \Pi_{i3} & \Pi_{i4} + \Theta^T \Theta - X_2 & \psi_i^T X_2 \mathbb{B}_{ci} \\ \mathbb{B}_{ci}^T X_2 \Phi_i \mathbb{A}_c & \mathbb{B}_{ci}^T X_2 \psi_i & \mathbb{B}_{ci}^T X_2 \mathbb{B}_{ci} - \bar{\gamma} I \end{bmatrix} \mathcal{C}^{T\perp T} < 0 \quad \forall i \in \{1, \dots, \kappa\}. \quad (8.36)$$

donde:

$$\begin{aligned} \Pi_{i1} &= \mathbb{A}_{i1}^T X_1 \mathbb{A}_{i1} - \mathbb{A}_{i1}^T X_1 \mathbb{Y}_i \mathbb{A}_2 - \mathbb{A}_2^T \mathbb{Y}_i^T X_1 \mathbb{A}_{i1} + \mathbb{A}_2^T \bar{\mathbb{Z}}_i \mathbb{A}_2 + \Phi_i \mathbb{A}_c^T X_2 \Phi_i \mathbb{A}_c, \\ \Pi_{i2} &= -\mathbb{A}_{i1}^T X_1 \mathbb{A}_b + \mathbb{A}_2^T \mathbb{Y}_i^T X_1 \mathbb{A}_b + \Phi_i \mathbb{A}_c^T X_2 \psi_i, \\ \Pi_{i3} &= \Pi_{i2}^T, \quad \Pi_{i4} = \mathbb{A}_b^T X_1 \mathbb{A}_b + \psi_i^T X_2 \psi_i \quad \forall i \in \{1, \dots, \kappa\}. \end{aligned}$$

Para resolver la trilinealidad $\mathbb{Y}_i^T X_1 \mathbb{Y}_i$, se introduce:

$$\bar{\mathbb{Z}}_i = \begin{bmatrix} X_1 & \mathbb{Y}_i \\ \mathbb{Y}_i^T & \bar{\mathbb{Z}}_i \end{bmatrix} > 0.$$

Finalmente, $\mathbb{Y}_i$ se parametriza como:

$$\mathbb{Y}_i = X^{-1} \left[\mathcal{B}_r^+ \mathcal{K}_i \mathcal{C}_l^+ + \mathcal{Z} - \mathcal{B}_r^+ \mathcal{B}_r \mathcal{Z} \mathcal{C}_l \mathcal{C}_l^+ \right], \quad (8.37)$$

donde $\mathcal{K}_i$, $\mathcal{S}_i$ y $\mathcal{V}_i$ se calculan como:

$$\mathcal{K}_i = -\mathcal{R}^{-1} \mathcal{B}_l^T \mathcal{V}_i \mathcal{C}_r^T (\mathcal{C}_r \mathcal{V}_i \mathcal{C}_r^T)^{-1} + \mathcal{S}_i^{1/2} \mathcal{L} (\mathcal{C}_r \mathcal{V}_i \mathcal{C}_r^T)^{-1/2}, \quad (8.38)$$

$$\mathcal{S}_i = \mathcal{R}^{-1} - \mathcal{R}^{-1} \mathcal{B}_l^T \left[\mathcal{V}_i - \mathcal{V}_i \mathcal{C}_r^T (\mathcal{C}_r \mathcal{V}_i \mathcal{C}_r^T)^{-1} \mathcal{C}_r \mathcal{V}_i \right] \mathcal{B}_l \mathcal{R}^{-1}, \quad (8.39)$$

$$\mathcal{V}_i = \left(\mathcal{B}_l \mathcal{R}^{-1} \mathcal{B}_l^T - \mathcal{D}_i \right)^{-1} > 0. \quad (8.40)$$

Estas condiciones garantizan que el ODG diseñado es estable y cumple con el criterio de desempeño $\mathcal{L}_2$ frente a ataques dinámicos DDA y perturbaciones en actuadores y sensores.

8.5. Simulación con esquemas de ataque

Las simulaciones se realizan sobre el **modelo T–S discreto** del sistema de tres tanques interconectados descrito previamente, empleando los **parámetros físicos** de la Tabla 4.1. Se adopta un tiempo de muestreo $T_d = 0.01$ s y condiciones iniciales.

$$x(0) = \begin{bmatrix} h_1(0) & h_2(0) & h_3(0) \end{bmatrix}^\top = \begin{bmatrix} 0.20 & 0.20 & 0.20 \end{bmatrix}^\top \text{ m.}$$

Entradas (caudales de bombas). Las señales de entrada corresponden a los caudales $Q_1(k)$ y $Q_2(k)$ (en m^3/s), diseñadas como escalones para excitar adecuadamente la dinámica:

$$Q_1(k) = \begin{cases} 0, & k < k_1, \\ \bar{Q}_1, & k \geq k_1, \end{cases} \quad Q_2(k) = \begin{cases} 0, & k < k_2, \\ \bar{Q}_2, & k \geq k_2, \end{cases}$$

con $\bar{Q}_1 = 0.368 \times 10^{-4}$, $\bar{Q}_2 = 0.252 \times 10^{-4}$, $k_1 = \lfloor 184/T_d \rfloor$ y $k_2 = \lfloor 70/T_d \rfloor$. Estas entradas, mostradas en la Figura 8.1, son *persistentes en el tiempo* tras su activación y permiten evaluar el desempeño del observador frente a alteraciones en actuadores y sensores.

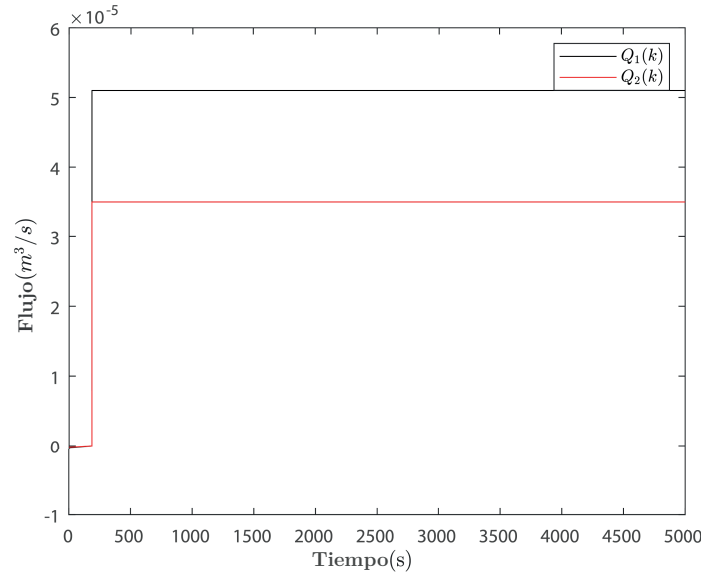


Fig. 8.1. Entradas de caudal $Q_1(k)$ y $Q_2(k)$ utilizadas en el sistema de tres tanques interconectados.

Lógicas de activación (Markovianas). Los ataques en actuadores $a_\alpha(k)$ y en sensores $a_\beta(k)$ se activan mediante procesos Markovianos en dos modalidades:

- **Uniforme:** intervalos de activación/desactivación constantes (ataques periódicos/planificados).
- **No uniforme:** intervalos aleatorios (ataques irregulares y difíciles de predecir).

Ambos perfiles se ilustran en la Figura 8.2; la curva *negra* corresponde a la lógica uniforme y la *roja* a la no uniforme.

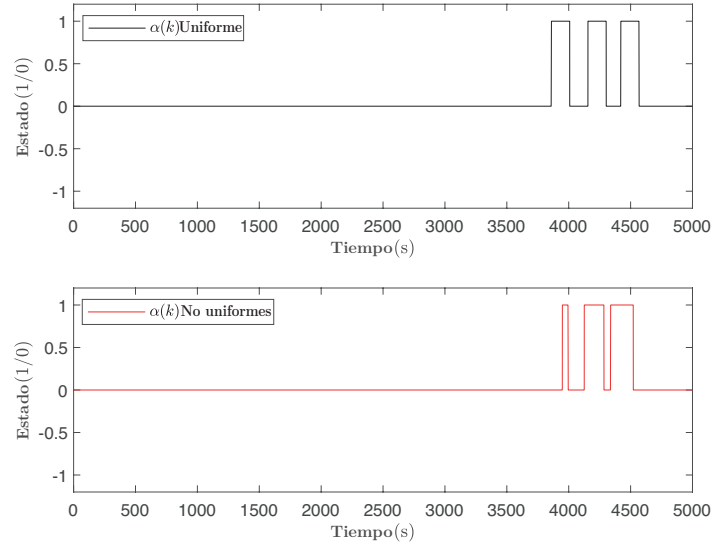


Fig. 8.2. Lógicas Markovianas de activación para ataques: uniforme (negro) y no uniforme (rojo).

8.5.1. Escenario 1: Ataque DDA uniforme coordinado

Se aplica un ataque **DDA (Data Deception Attack)** con lógica *uniforme* que afecta de forma coordinada la entrada $u_2(k)$ y las mediciones de $x_1(k)$ y $x_3(k)$. El ODG estima en línea la señal de ataque y compensa su efecto en la reconstrucción de estados.

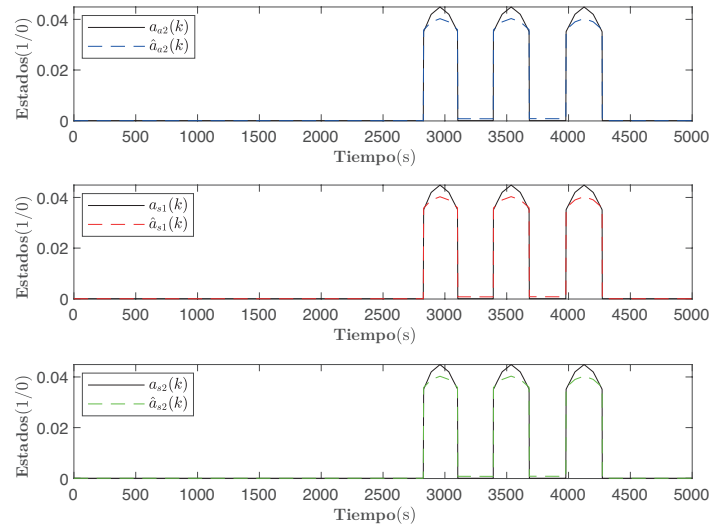


Fig. 8.3. Estimación de ataques DDA (actuador y sensores) bajo lógica uniforme mediante el ODG.

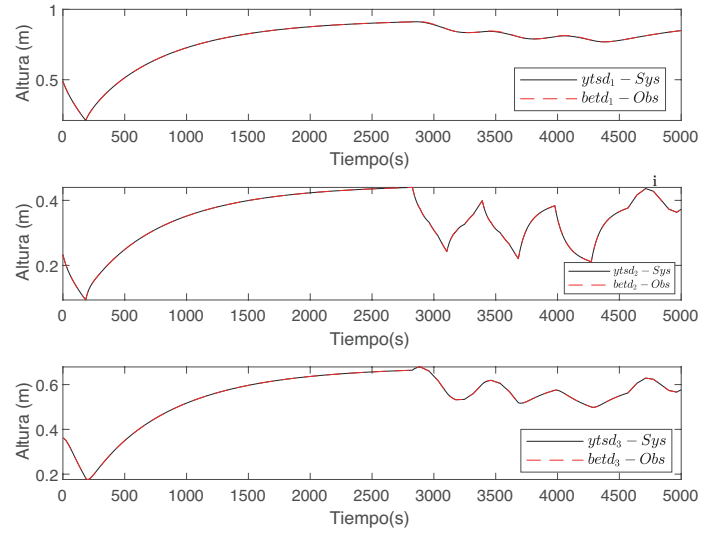


Fig. 8.4. Estados estimados por el ODG bajo ataques DDA uniformes coordinados.

8.5.2. Escenario 2: Ataque DoS uniforme en el actuador

Se considera un **ataque DoS (Denial of Service)** *uniforme* dirigido al actuador asociado a $u_2(k)$, que bloquea periódicamente la acción de control. El ODG sigue la firma temporal del bloqueo e identifica las ventanas de interrupción.

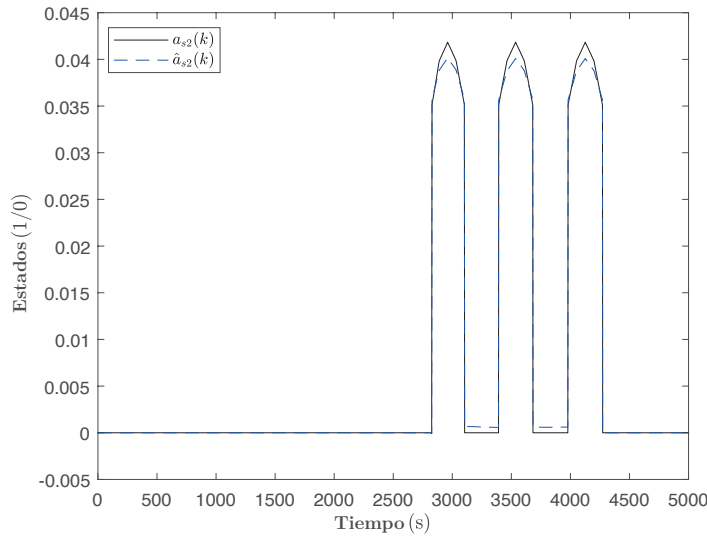


Fig. 8.5. Estimación del ataque DoS uniforme en el actuador por medio del ODG.

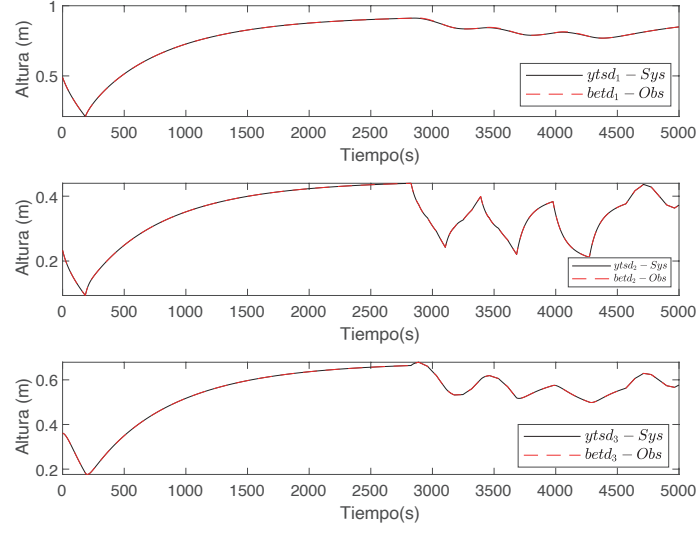


Fig. 8.6. Estados estimados por el ODG en presencia de DoS uniforme.

8.5.3. Escenario 3: Ataque RDI no uniforme en sensores

Se simula un **ataque RDI (Random Data Injection)** con lógica *no uniforme* sobre las mediciones de $x_1(k)$ y $x_2(k)$, introduciendo perturbaciones aleatorias y de duración irregular. El ODG mantiene la coherencia de la estimación y recupera la dinámica del ataque.

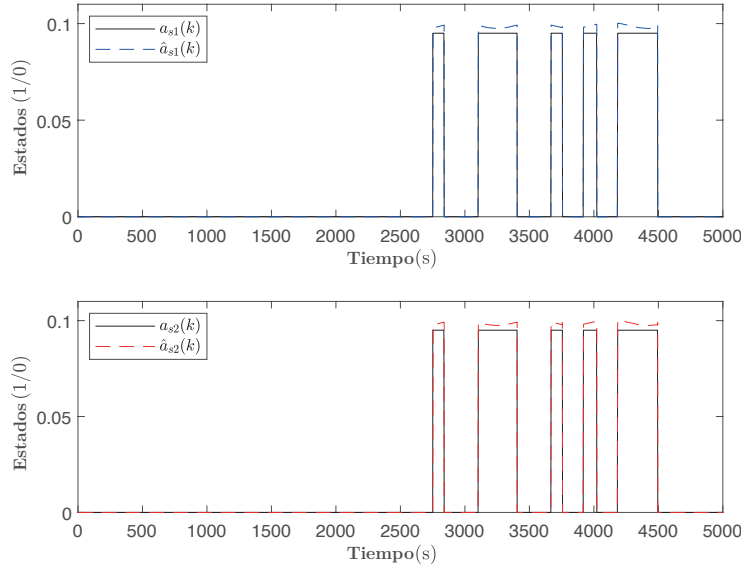


Fig. 8.7. Efecto del ataque RDI no uniforme sobre los estados reales.

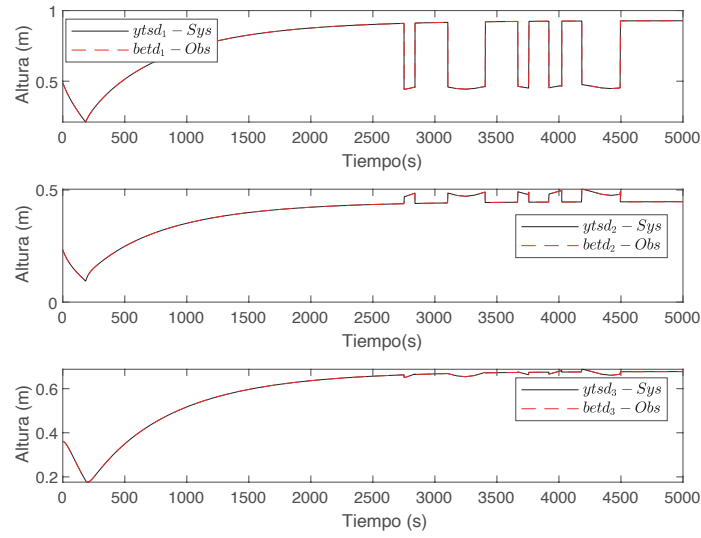


Fig. 8.8. Estimación de estados y reconstrucción del ataque RDI no uniforme mediante el ODG.

8.6. Conclusiones del capítulo

Se validó un **Observador Dinámico Generalizado (ODG)** para estimar *estados* y *ataques dinámicos* en el sistema T-S discreto de tres tanques. En los tres escenarios (DDA coordinado, DoS en actuador y RDI en sensores), el ODG:

- Reconstruyó con precisión las señales de ataque $a_\alpha(k)$ y $a_\beta(k)$ bajo lógicas Markovianas *uniforme* y *no uniforme*.
- Mantuvo **estabilidad y robustez** en la estimación de estados frente a bloqueos, falsificación y ruido aleatorio.
- Ofrece una base sólida para **diagnóstico y control tolerante a ataques**, al proporcionar residuos/estimaciones con firmas temporales coherentes con la lógica de activación.

El ODG constituye una herramienta eficaz para la detección y reconstrucción de ciberataques en sistemas ciberfísicos, preservando la fidelidad de la estimación aún bajo activaciones irregulares y múltiples puntos de intrusión.

Capítulo 9

Instrumentación en la plataforma del GIPSA-Lab

En este capítulo se describe la parte de implementación práctica de los algoritmos de **control y estimación** desarrollados, utilizando la plataforma experimental del **GIPSA-Lab**, ubicada en Grenoble, Francia. Esta infraestructura permite la validación de esquemas de control en tiempo real sobre un vehículo a escala instrumentado, dentro de un entorno controlado equipado con un sistema de captura de movimiento de alta precisión (*VICON*) y un sistema de adquisición de datos basado en *ROS2*.

El esquema propuesto combina un **controlador tolerante a ataques** y un **observador dinámico generalizado** diseñado para la *detección, estimación y compensación* de ataques cibernéticos dirigidos al actuador. El observador permite estimar la señal de ataque en tiempo real y proporcionar dicha información al controlador, el cual ajusta su acción de manera compensatoria para preservar la estabilidad y el desempeño del sistema. De esta forma, se garantiza la *resiliencia* del vehículo frente a perturbaciones o intrusiones que afecten la integridad del canal de control.

La implementación experimental ofrece múltiples beneficios:

- **Validación en tiempo real:** permite evaluar el desempeño del esquema bajo condiciones reales de comunicación y procesamiento, reproduciendo escenarios de ataque controlado.
- **Evaluación de resiliencia:** se analizan las capacidades del sistema para detectar y mitigar ataques al actuador, manteniendo la estabilidad del vehículo.

- **Prueba de robustez:** se verifica la respuesta del controlador ante perturbaciones externas, retrasos de red y variaciones en las condiciones operativas.
- **Transferibilidad:** la estructura modular basada en ROS2 facilita la replicación del experimento en otras plataformas ciber-físicas.

La integración del observador y el controlador tolerante a ataques sobre la plataforma del GIPSA-Lab permite validar de forma experimental las estrategias propuestas, demostrando su eficacia para mantener la estabilidad, continuidad y seguridad operativa del sistema ante ataques en el actuador.

9.1. Descripción general de la plataforma

La plataforma está compuesta por los siguientes elementos principales:

- Un **sistema de captura de movimiento Vicon**, compuesto por 12 cámaras infrarrojas que permiten reconstruir la posición y orientación del vehículo con alta precisión en tiempo real.
- Un **PC central**, encargado de ejecutar los algoritmos de control y estimación en el entorno **ROS2** e interconectado con el sistema Vicon mediante red Ethernet.
- Un **vehículo RC instrumentado**, que integra un microcontrolador **Arduino RP2040**, dos motores **BLDC** para la tracción y un **servo MG996R** para la dirección, además de sensores internos (voltaje, corriente y encoders).
- Un entorno de software híbrido **ROS2-MATLAB/Simulink** que permite la co-simulación y ejecución de controladores en tiempo real, facilitando el envío de señales PWM al vehículo vía Wi-Fi.

En la Figura 9.1 se observa la disposición física de la plataforma, con el espacio de pruebas delimitado por el sistema de cámaras Vicon y la estación de control que ejecuta los algoritmos desarrollados.

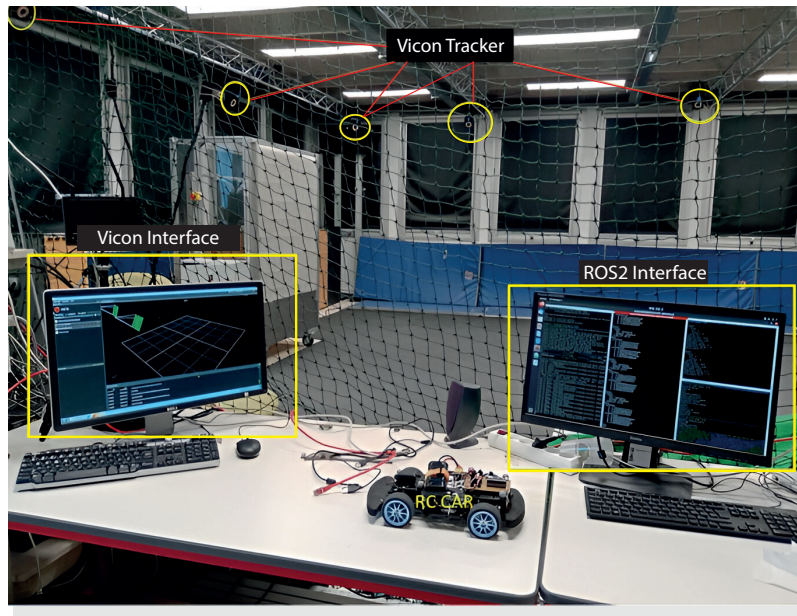


Fig. 9.1. Laboratorio VICON en GIPSA-Lab: espacio de captura y estación de control con ROS2.

9.2. Componentes del vehículo RC

El vehículo RC empleado está equipado con sensores y actuadores que permiten realizar experimentos representativos de control y estimación en sistemas ciberfísicos. En la Figura 9.2 se muestran los elementos principales, los cuales se describen en la Tabla 9.1.

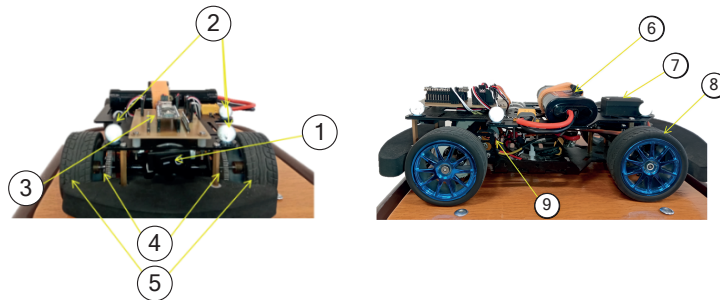


Fig. 9.2. Componentes principales del vehículo RC utilizado en GIPSA-Lab.

Tabla 9.1. Componentes del vehículo RC utilizado en GIPSA-Lab.

Nº	Componente	Descripción y funcionalidad
1	Interruptor principal	Permite encender y apagar el vehículo.
2	Reflectores Vicon	Esferas de 8 mm captadas por las cámaras infrarrojas para localización precisa.
3	Arduino RP2040	Microcontrolador encargado de recibir comandos ROS2 vía Wi-Fi y generar señales PWM.
4	Engranajes Spur	Aumentan el torque transmitido por los motores BLDC.
5	Ruedas traseras elásticas	Ruedas motrices conectadas a los motores BLDC.
6	Batería NI-MH 3000 mAh	Fuente principal de alimentación del vehículo.
7	Servo MG996R	Actuador de dirección frontal.
8	Ruedas delanteras elásticas	Elementos de guiado del vehículo.
9	Motor BLDC A2212/13T	Actuador de tracción principal controlado por PWM.

9.3. Interfaz de conexión y flujo de datos

La arquitectura de comunicación se muestra en la Figura 9.3. El flujo de datos se describe de la siguiente manera:

1. El sistema **Vicon** detecta la posición y orientación del vehículo mediante sus reflectores pasivos.
2. Los datos de posición se transmiten al **PC central** ejecutando ROS2, el cual procesa la información y calcula las señales de control.
3. Estas señales se envían vía Wi-Fi al **Arduino RP2040**, que las transforma en voltajes PWM para accionar los motores BLDC y el servo de dirección.
4. El movimiento del vehículo es registrado nuevamente por el sistema Vicon, cerrando así el bucle de control.
5. MATLAB/Simulink se comunica con ROS2, permitiendo la visualización en tiempo real y la ejecución de controladores híbridos.

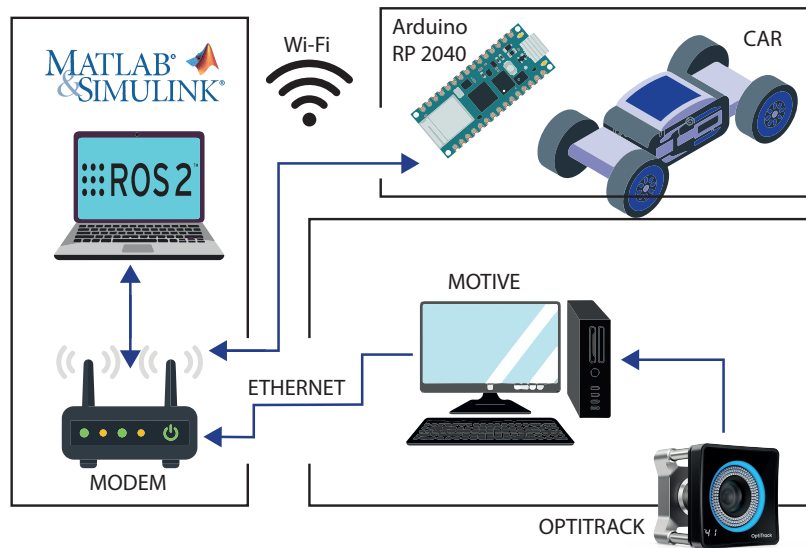


Fig. 9.3. Estructura de conexión entre ROS2, MATLAB/Simulink, Vicon y el vehículo RC.

9.4. Procedimiento de configuración y pruebas

El proceso de integración y pruebas se realizó siguiendo los pasos:

1. **Verificación de hardware:** comprobación de alimentación y conexiones físicas del sistema Vicon, el Arduino RP2040 y la batería del vehículo.
2. **Calibración de Vicon y ROS2:** ajuste de parámetros de captura en Vicon y configuración de nodos ROS2 para la recepción de datos en tiempo real.
3. **Conexión Ethernet y ROS2:** establecimiento de una red estable entre la PC con ROS2 y la estación con MATLAB/Simulink para intercambio de datos.
4. **Implementación del modelo en Simulink:** desarrollo de bloques de control y comunicación con ROS2 desde MATLAB.
5. **Carga del firmware en Arduino RP2040:** programación en C++ para la recepción de mensajes ROS2 (topics) y generación de PWM para actuadores.
6. **Pruebas iniciales:** verificación de tracking preciso en Vicon y respuesta del vehículo ante comandos simples de velocidad y dirección.

7. **Validación completa:** ejecución de controladores desde MATLAB/Simulink con retroalimentación de datos de posición y orientación.

9.5. Pruebas y validación

La integración permitió ejecutar algoritmos de control y estimación en tiempo real. La comunicación ROS2-MATLAB garantizó latencias mínimas (inferiores a 10 ms) y la captura de movimiento Vicon ofreció precisiones milimétricas. En la Figura 9.4 se muestra la identificación del vehículo por el sistema Vicon y en la Figura 9.5 la interfaz de control en Simulink.

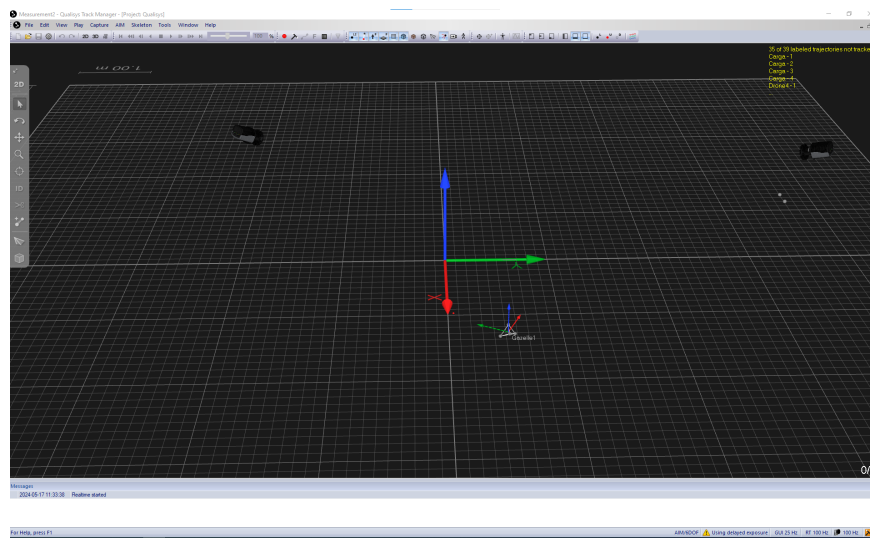


Fig. 9.4. Reconocimiento del vehículo por el sistema Vicon y ROS2.

Estructura de nodos ROS2

La estructura se compone de los siguientes nodos:

- **Nodo /vicon_tracker:** encargado de la suscripción a los datos de posición y orientación capturados por el sistema Vicon y publicarlos en el tópico correspondiente.
- **Nodo /state_estimation:** procesa la información de los sensores y aplica algoritmos de filtrado para generar el estado estimado del vehículo.
- **Nodo /control_command:** ejecuta el algoritmo de control y publica las señales de referencia para los actuadores.

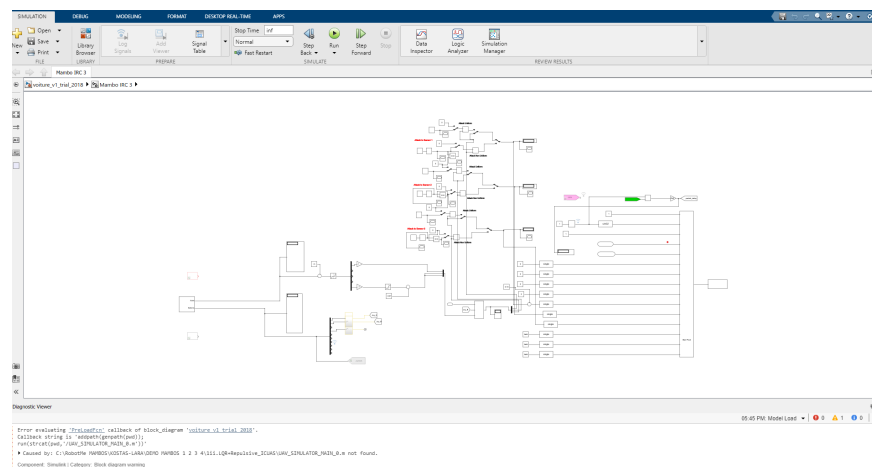


Fig. 9.5. Ejecución de controladores en Simulink conectados a ROS2.

- **Nodo `/arduino_interface`:** suscribe las señales de control publicadas en `/cmd_actuators` y envía comandos PWM al Arduino RP2040 vía Wi-Fi.

Principales tópicos de ROS2

Los tópicos utilizados se detallan a continuación:

- `/vicon/vehicle/pose` [*frecuencia: 100 Hz*] Contiene la posición (x, y, z) y la orientación (ϕ, θ, ψ) del vehículo obtenidas por Vicon.
- `/vehicle/state` [*frecuencia: 50 Hz*] Publica el vector de estado estimado, incluyendo velocidad longitudinal y orientación.
- `/cmd_actuators` [*frecuencia: 100 Hz*] Publica los comandos PWM normalizados (0-255) para los motores BLDC y el servo MG996R.
- `/sensor/feedback` [*frecuencia: 50 Hz*] Incluye mediciones de corriente, voltaje de batería y encoders de ruedas.

Frecuencias de ejecución

El sistema fue configurado con las siguientes frecuencias:

- **Controlador en Simulink:** 100 Hz.

- **Estimación de estados:** 50 Hz (filtrado de sensores y datos de posición).
- **Captura de Vicon:** 100 Hz (resolución milimétrica en el rastreo de posición).
- **Publicación de sensores:** 50 Hz.

Estas frecuencias se seleccionaron de forma que el lazo de control operara en tiempo real sin saturar la comunicación Wi-Fi ni los recursos computacionales del Arduino RP2040, garantizando latencias de comunicación menores a 10 ms en los comandos de control.

Integración con MATLAB/Simulink

Desde MATLAB/Simulink, la comunicación con ROS2 se estableció mediante bloques dedicados de suscripción y publicación. Los datos de `/vicon/vehicle/pose` y `/sensor/feedback` son procesados en tiempo real para alimentar el modelo de control. Las salidas del controlador, correspondientes a las señales de aceleración y dirección, se publican directamente en `/cmd_actuators`.

Latencia y desempeño

Las pruebas experimentales mostraron:

- Latencia promedio entre publicación de comandos y ejecución en el vehículo: **8.3 ms**.
- Error máximo de posición en el rastreo con Vicon: ± 0.5 **mm**.
- Estabilidad de la conexión Wi-Fi sin pérdidas de paquetes durante más de 30 minutos de operación continua.

Estos resultados confirman que la plataforma de GIPSA-Lab es adecuada para la validación de algoritmos avanzados de control y estimación de estados en sistemas ciberfísicos, garantizando operación confiable en tiempo real.

9.6. Conclusión

La implementación en la plataforma experimental del **GIPSA-Lab** proporcionó un entorno idóneo para validar los algoritmos de control y estimación desarrollados en esta tesis. La integración entre

ROS2, **MATLAB/Simulink**, el microcontrolador **Arduino RP2040** y el sistema de captura óptica **Vicon** permitió realizar pruebas de control en tiempo real con una precisión milimétrica en la medición de posición y orientación del vehículo. Esta infraestructura posibilitó la ejecución de esquemas avanzados de *control tolerante a ataques* (CTA) y de un *observador dinámico generalizado* (ODG) para la detección y compensación de ataques en el actuador, validando su funcionamiento bajo condiciones experimentales realistas.

Los resultados experimentales demostraron que la arquitectura de comunicación basada en **ROS2** garantiza una transmisión confiable de datos con latencias promedio inferiores a 10 ms, mientras que el sistema Vicon proporciona una referencia de posición de alta resolución que facilita el análisis cuantitativo del desempeño del controlador. La implementación conjunta del CTA y el ODG permitió detectar en tiempo real alteraciones intencionadas en el canal del actuador, estimar su magnitud y compensar su efecto mediante la acción correctiva del controlador, preservando la estabilidad y el seguimiento de referencia del sistema.

Además, el uso combinado de **Simulink** y **ROS2** posibilitó la co-simulación entre el entorno de modelado y la ejecución física, reduciendo el tiempo de desarrollo e incrementando la fiabilidad de las pruebas. El diseño modular de la plataforma también facilitó la implementación de algoritmos adicionales, como filtros de estimación y módulos de diagnóstico, evidenciando la versatilidad del entorno experimental.

Entre los beneficios más relevantes de esta implementación destacan:

- **Validación experimental en tiempo real:** se comprobó la factibilidad práctica de ejecutar controladores resilientes ante ataques cibernéticos en sistemas ciber-físicos discretos.
- **Evaluación de resiliencia y estabilidad:** los experimentos confirmaron la capacidad del esquema propuesto para mantener la estabilidad y desempeño nominal bajo ataques aplicados al actuador.
- **Robustez ante perturbaciones y variaciones de red:** el sistema demostró un comportamiento estable frente a pérdidas temporales de comunicación, retrasos y ruido en las mediciones.

- **Escalabilidad y transferibilidad:** la arquitectura ROS2–MATLAB–Vicon constituye una base sólida para extender el esquema a otras plataformas o vehículos autónomos en futuras investigaciones.

La instrumentación realizada en el GIPSA-Lab no solo permitió validar de manera empírica el desempeño del *controlador tolerante a ataques* y del *observador*, sino que también demostró la viabilidad de integrar metodologías avanzadas de diagnóstico y control resiliente en sistemas ciberfísicos reales.

El conjunto de herramientas y resultados obtenidos sienta un precedente importante para el desarrollo de estrategias de control seguras, adaptativas y escalables aplicables a una amplia gama de infraestructuras críticas y vehículos inteligentes.

Capítulo 10

Control tolerante a ataques

El Control Tolerante a Ataques (CTA) se diseña para mantener la estabilidad del sistema frente a ataques cibernéticos que afectan directamente a los actuadores. Consideramos un sistema discreto T-S con ataques en los actuadores:

$$x_a(k+1) = \sum_{i=1}^{\kappa} \mu_i(k) \left(A_i x_a(k) \right) + B \left(u_a(k) + a_a(k) \right), \quad (10.1)$$

$$y_a(k) = C x_a(k), \quad (10.2)$$

donde $x_a(k) \in \mathbb{R}^n$: vector de estados bajo ataque, $u_a(k) \in \mathbb{R}^p$: señal de control generada por el CTA, $y_a(k) \in \mathbb{R}^n$: salida del sistema atacado, $a_a(k) \in \mathbb{R}^p$: vector de ataque en actuadores y $\mu_i(k)$: funciones de pertenencia difusas que cumplen $\sum_i \mu_i(k) = 1$.

En paralelo, se considera un modelo libre de ataques como referencia:

$$x(k+1) = \sum_{i=1}^{\kappa} \mu_i(k) A_i x(k) + B u(k), \quad (10.3)$$

$$y(k) = C x(k), \quad (10.4)$$

donde $x(k) \in \mathbb{R}^n$ y $u(k) \in \mathbb{R}^p$ representan los estados y la entrada nominal respectivamente.

10.1. Ley de control tolerante

El CTA propuesto busca garantizar que el error de trayectoria $\|x(k) - x_a(k)\|$ tienda a cero, incluso bajo ataques. La ley de control se define como:

$$u_a(k) = K \left(x(k) - \hat{x}_a(k) \right) + u(k) - \hat{a}_a(k), \quad (10.5)$$

donde $K \in \mathbb{R}^{p \times n}$ es la matriz de realimentación de estados, $\hat{x}_a(k)$ es la estimación de los estados bajo ataque y $\hat{a}_a(k)$ es la estimación del ataque en los actuadores.

Estas estimaciones son proporcionadas por un Observador Dinámico Generalizado (ODG) que estima simultáneamente $x_a(k)$ y $a_a(k)$ el cuál fue propuesto en las secciones anteriores.

10.2. Observador Dinámico Generalizado (ODG)

El ODG utilizado se estructura de la siguiente forma:

$$\zeta(k+1) = \sum_{i=1}^{\kappa} \mu_i(x(k)) \left(N_i \zeta(k) + H_i v(k) + F y(k) \right) + J u(k) + \alpha F_1 \hat{a}_a(k), \quad (10.6)$$

$$v(k+1) = \sum_{i=1}^{\kappa} \mu_i(x(k)) \left(S_i \zeta(k) + L_i v(k) + M_i y(k) \right), \quad (10.7)$$

$$\hat{a}_a(k+1) = \sum_{i=1}^{\kappa} \mu_i(x(k)) \left(\Phi_i \left(C \hat{\mathbb{X}}(k) - y(k) \right) + \eta_i \hat{a}_a(k) \right), \quad (10.8)$$

$$\hat{\mathbb{X}}(k) = P \zeta(k) + Q y(k), \quad (10.9)$$

donde $\zeta(k)$ es el vector de estados del observador, $v(k)$ es el vector auxiliar para robustecer la dinámica, $\hat{\mathbb{X}}(k)$ corresponde a la estimación conjunta de estados y salidas y $\hat{a}_a(k)$ es la estimación del ataque.

10.3. Dinámica de estimación y error de seguimiento

El error de salida se define como:

$$e_y(k) = y_a(k) - \hat{y}_a(k), \quad (10.10)$$

y el error de trayectoria como $e(k) = x(k) - x_a(k)$. Su dinámica se deriva de (10.1) y (10.3):

$$e(k+1) = x(k+1) - x_a(k+1), \quad (10.11)$$

$$e(k+1) = \sum_{i=1}^{\kappa} \mu_i(z(k)) \left[A_i(x(k) - x_a(k)) + B u(k) - B u_a(k) - F_1 a_a(k) \right]. \quad (10.12)$$

Sustituyendo la ley de control (10.5):

$$e(k+1) = \sum_{i=1}^{\kappa} \mu_i(z(k)) \left[(A_i - BK)e(k) - BK(x_a(k) - \hat{x}_a(k)) - B(a_a(k) - \hat{a}_a(k)) \right]. \quad (10.13)$$

10.4. Sistema aumentado y estimación

Definimos el vector aumentado:

$$x_A(k) = \begin{bmatrix} x_a(k) \\ a_a(k) \end{bmatrix}, \quad e_A(k) = x_A(k) - \hat{x}_A(k) = \begin{bmatrix} x_a(k) - \hat{x}_a(k) \\ a_a(k) - \hat{a}_a(k) \end{bmatrix}. \quad (10.14)$$

La dinámica aumentada se expresa como:

$$\underbrace{\begin{bmatrix} x_a(k+1) \\ a_a(k+1) \end{bmatrix}}_{x_A(k+1)} = \sum_{i=1}^{\kappa} \mu_i(z(k)) \left[\underbrace{\begin{bmatrix} A_i & B \\ 0 & 0 \end{bmatrix}}_{\bar{A}_i} \underbrace{\begin{bmatrix} x_a(k) \\ a_a(k) \end{bmatrix}}_{x_A(k)} + \underbrace{\begin{bmatrix} B \\ 0 \end{bmatrix}}_{\bar{B}} u_a(k) \right]. \quad (10.15)$$

El error de estimación evoluciona como:

$$e_a(k+1) = \sum_{i=1}^{\kappa} \mu_i(z(k)) \left[\bar{A}_i \hat{x}_A(k) + \bar{B} u_a(k) + N\bar{C} e_A(k) \right], \quad (10.16)$$

con:

$$\bar{C} = \begin{bmatrix} C & 0 \end{bmatrix}, \quad N = \begin{bmatrix} L \\ W \end{bmatrix}.$$

La salida bajo ataque se representa como:

$$y_a(k) = \bar{C} x_A(k). \quad (10.17)$$

Finalmente, sustituyendo $e_a(k+1) = x_A(k+1) - \hat{x}_A(k+1)$:

$$\hat{x}_A(k+1) = \sum_{i=1}^{\kappa} \mu_i(z(k)) \left[\bar{A}_i (x_A(k) - \hat{x}_A(k)) + \bar{B} u_a(k) + N\bar{C} e_A(k) \right], \quad (10.18)$$

$$e_a(k+1) = \sum_{i=1}^{\kappa} \mu_i(z(k)) (\bar{A}_i - N\bar{C}) e_a(k). \quad (10.19)$$

10.5. Análisis de estabilidad del Control Tolerante a Ataques

Para garantizar la estabilidad del sistema aumentado bajo la acción del controlador tolerante a ataques y el observador dinámico generalizado, se plantea el siguiente análisis basado en una función de Lyapunov y condiciones de LMIs.

10.5.1. Función de Lyapunov candidata

Consideramos la siguiente función de Lyapunov cuadrática para el sistema aumentado:

$$V(\bar{e}(k)) = \bar{e}(k)^T X \bar{e}(k) > 0, \quad (10.20)$$

donde

$$X = \begin{bmatrix} X_1 & 0 \\ 0 & X_2 \end{bmatrix}, \quad X_1 = X_1^T > 0, \quad X_2 = X_2^T > 0,$$

y el vector de error aumentado es:

$$\bar{e}(k) = \begin{bmatrix} e(k) \\ x_a(k) - \hat{x}_a(k) \\ a_a(k) - \hat{a}_a(k) \end{bmatrix}.$$

10.5.2. Condición de disminución de Lyapunov

La variación de la función de Lyapunov se define como:

$$\Delta V(\bar{e}(k)) = V(\bar{e}(k+1)) - V(\bar{e}(k)) = \bar{e}^T(k+1) X \bar{e}(k+1) - \bar{e}^T(k) X \bar{e}(k). \quad (10.21)$$

Para garantizar estabilidad, imponemos:

$$\Delta V(\bar{e}(k)) < 0, \quad \forall k > 0. \quad (10.22)$$

Sustituyendo la dinámica del error aumentado:

$$\bar{e}(k+1) = \sum_{i=1}^{\kappa} \mu_i(z(k)) (\bar{A}_{ai}) \bar{e}(k), \quad (10.23)$$

donde:

$$\bar{A}_{ai} = \begin{bmatrix} A_i - BK & -\bar{L} \\ 0 & \bar{A}_i - N\bar{C} \end{bmatrix}, \quad \bar{L} = \begin{bmatrix} BK & B \end{bmatrix}. \quad (10.24)$$

Así, la condición de estabilidad se expresa como:

$$\Delta V(\bar{e}(k)) = \bar{e}^T(k) \left[\bar{A}_{ai}^T X \bar{A}_{ai} - X \right] \bar{e}(k) < 0. \quad (10.25)$$

10.5.3. Planteamiento de la LMI

Mediante el uso del complemento de Schur, la desigualdad anterior se puede reformular como:

$$\begin{bmatrix} -X & \bar{A}_{ai}^T X \\ X \bar{A}_{ai} & -X \end{bmatrix} < 0. \quad (10.26)$$

Sustituyendo $\bar{A}_{ai}$:

$$\begin{bmatrix} X_1 & 0 & A_i^T X_1 - K^T B^T X_1 & -L^T X_2 \\ 0 & X_2 & 0 & \bar{A}_i^T X_2 - N^T \bar{C}^T X_2 \\ X_1 A_i - X_1 B K & -X_1 \bar{L} & X_1 & 0 \\ 0 & \bar{A}_i X_2 - N \bar{C} X_2 & 0 & X_2 \end{bmatrix} < 0. \quad (10.27)$$

Estas LMIs deben resolverse para obtener las matrices K , N , L , y W que garantizan la estabilidad del sistema bajo el esquema de control tolerante a ataques y observador dinámico.

10.6. Simulaciones bajo diferentes esquemas de ataque

Con el objetivo de validar el desempeño del esquema de control tolerante a ataques basado en observadores, se realizaron diversas simulaciones sobre un vehículo representado mediante el modelo LPV en tiempo discreto. El análisis se centra en tres variables fundamentales:

1. La **trayectoria de referencia frente a la trayectoria real del vehículo**.
2. La **velocidad de guiñada (yaw rate)**, que refleja la estabilidad lateral.
3. La **velocidad longitudinal**, que está asociada a la dinámica de traslación.

Cada escenario se diseñó para representar diferentes tipos de ataques: *ausencia de ataques*, *ataques suaves de variación lenta* y *ataques dinámicos no uniformes*.

10.6.1. Caso 1: Sistema sin ataques

El primer escenario corresponde al comportamiento nominal del sistema, sin presencia de ataques. La trayectoria de referencia y la real prácticamente coinciden (Figura 10.1), lo que demuestra la correcta sintonización del controlador. El yaw rate mostrado en la Figura 10.2 presenta un comportamiento estable y suavemente amortiguado, sin oscilaciones abruptas.

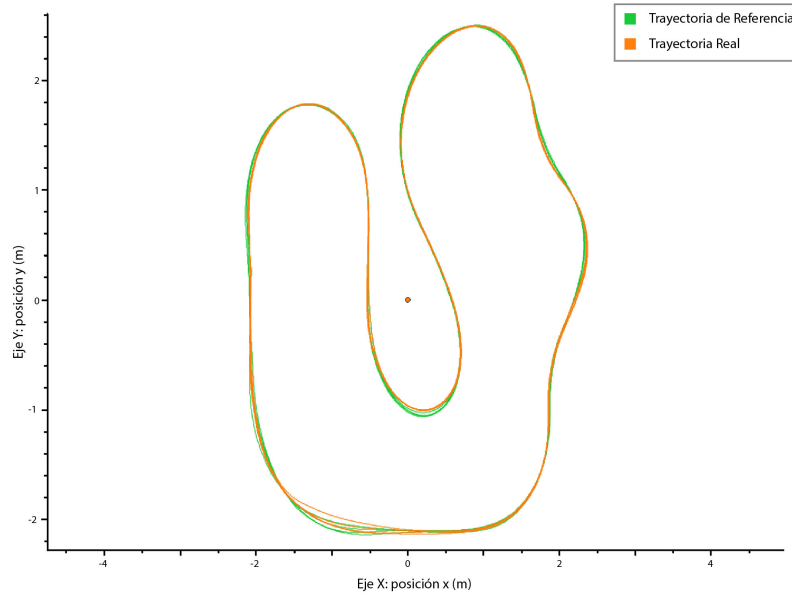


Fig. 10.1. Trayectoria de referencia y real sin presencia de ataques.

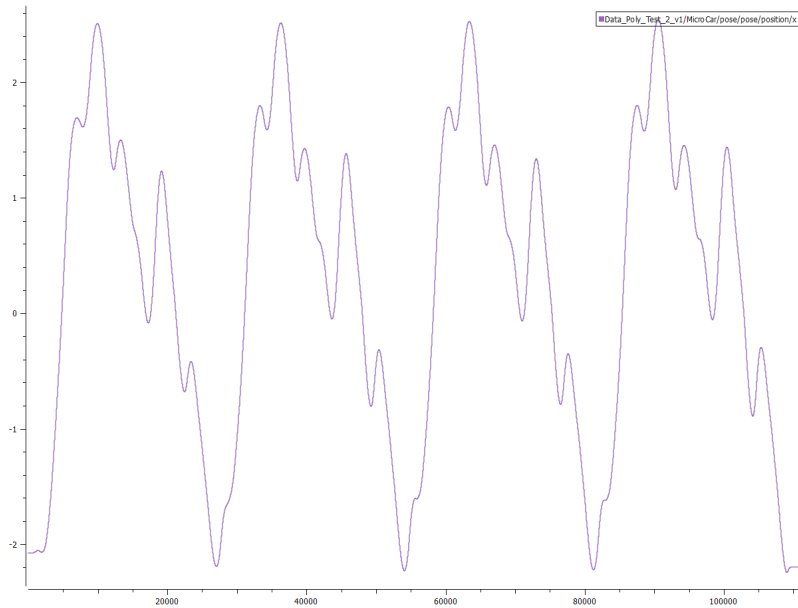


Fig. 10.2. Respuesta del yaw rate sin ataques.

10.6.2. Caso 2: Ataques RDI de variación suave (Markovianos uniformes)

En este escenario, se implementaron ataques con una lógica Markoviana uniforme, los cuales afectan tanto a sensores como a actuadores. Estos ataques simulan una alteración sistemática y constante,

aunque de baja intensidad, en la transmisión de señales.

La trayectoria real del vehículo presenta ligeras desviaciones respecto a la referencia (Figura 10.3), pero el observador dinámico logra compensarlas y mantener un seguimiento aceptable. El yaw rate (Figura 10.4) evidencia oscilaciones periódicas que reflejan la presencia del ataque, aunque sin pérdida de estabilidad global. Por su parte, la velocidad longitudinal (Figura 10.5) sufre pequeñas perturbaciones, que son contenidas gracias a la acción correctiva del esquema tolerante.

En términos prácticos, este tipo de ataque representa una situación de degradación suave del rendimiento, donde el sistema aún conserva capacidad de resiliencia, lo que valida la efectividad del observador en condiciones de baja severidad.

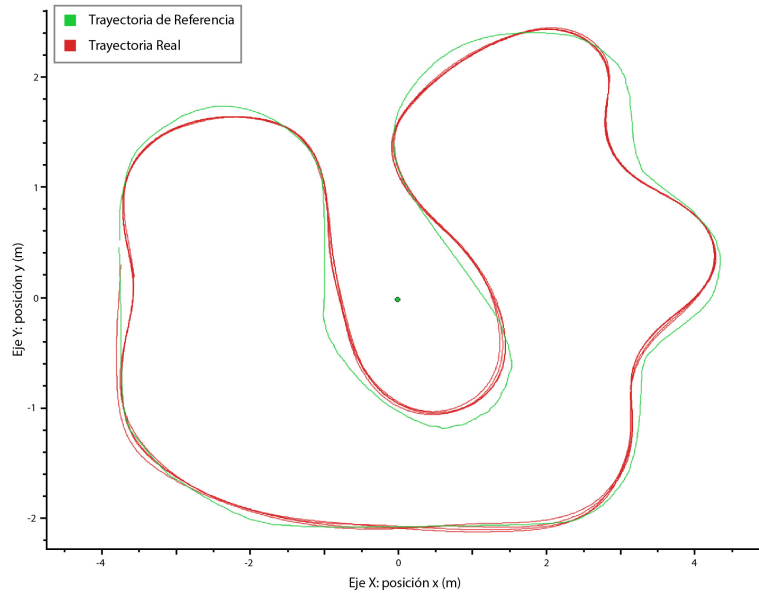


Fig. 10.3. Trayectoria bajo ataques de variación suave.

10.6.3. Caso 3: Ataque DoS no uniforme

El tercer escenario corresponde a ataques más agresivos, caracterizados por interrupciones no uniformes en la comunicación y modificaciones abruptas en los datos transmitidos. Se consideran tres tipos principales:

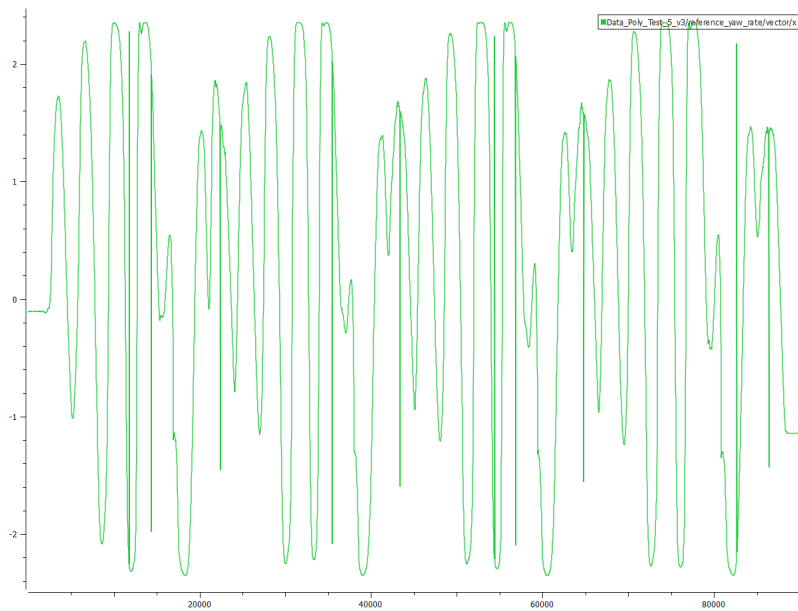


Fig. 10.4. Comportamiento del yaw rate bajo ataques suaves.

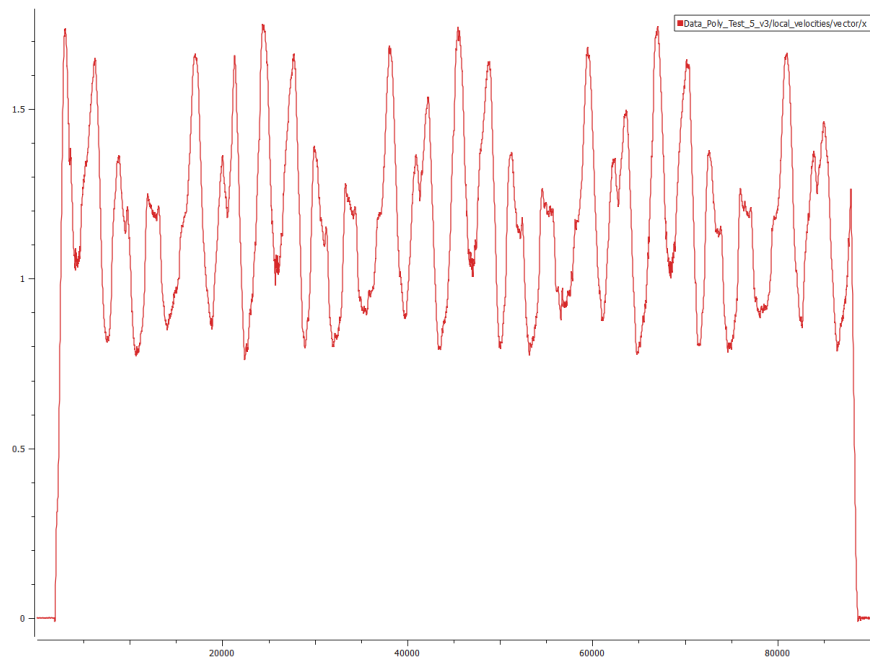


Fig. 10.5. Velocidad longitudinal bajo ataques Markovianos uniformes.

- **Denegación de Servicio (DoS):** se bloquea o retrasa la comunicación, afectando la disponibilidad de información.
- **Data Deception Attack (DDA):** se introducen datos falsos de manera estructurada, al-

terando las mediciones de sensores o actuadores.

- **Random Data Injection (RDI)**: se inyectan perturbaciones aleatorias, lo que genera un comportamiento impredecible en las señales.

En este caso, la trayectoria real (Figura 10.6) se aleja notablemente de la referencia, lo que refleja el impacto severo del ataque. Sin embargo, el esquema tolerante atenúa las desviaciones y permite recuperar parcialmente el seguimiento. El yaw rate (Figura 10.7) exhibe picos pronunciados y transitorios bruscos, que corresponden a los momentos de activación de los ataques. Finalmente, la velocidad longitudinal (Figura 10.8) sufre oscilaciones irregulares que ilustran la acción combinada de los ataques no uniformes.

Estos resultados demuestran que, aunque el desempeño se ve degradado en condiciones de ataque severo, el esquema tolerante mantiene la estabilidad global del sistema y permite una recuperación parcial, lo cual valida su robustez frente a escenarios de alta severidad.

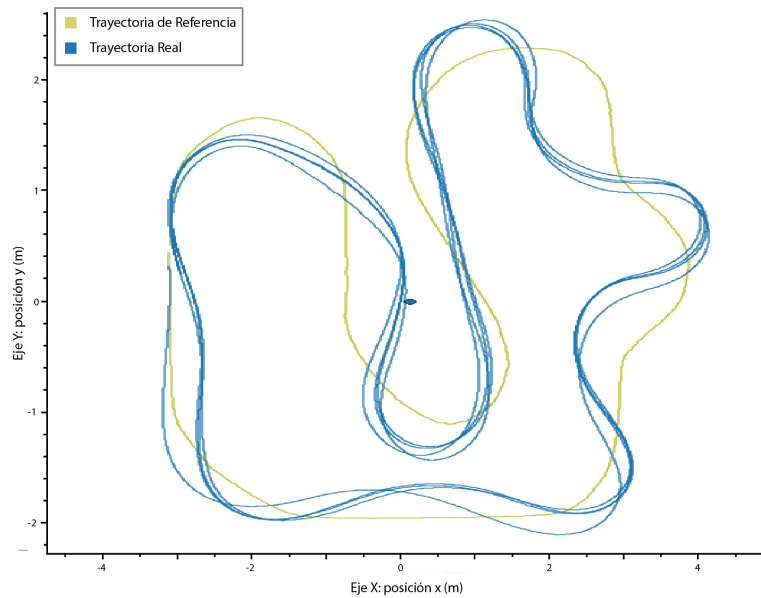


Fig. 10.6. Trayectoria bajo ataques dinámicos no uniformes (DoS, DDA, RDI).

10.6.4. Discusión general

Los tres escenarios permiten establecer un contraste claro:

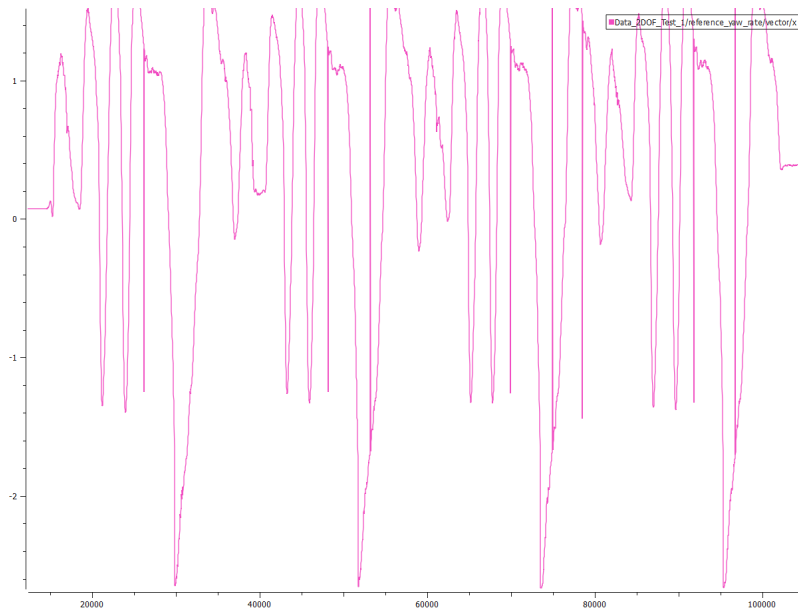


Fig. 10.7. Respuesta del yaw rate bajo ataques dinámicos.

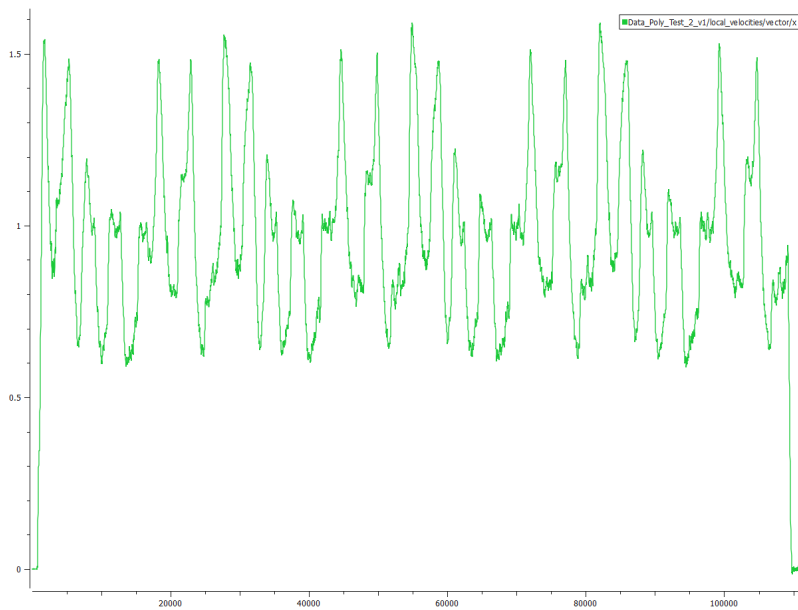


Fig. 10.8. Velocidad longitudinal bajo ataques intensos.

- En ausencia de ataques, el sistema cumple de manera nominal con el seguimiento de trayectorias.
- Bajo ataques de variación suave, el observador y el controlador mantienen la resiliencia, limitando las oscilaciones a márgenes aceptables.

- Frente a ataques dinámicos agresivos, aunque el desempeño se degrada, el esquema evita la inestabilidad y asegura la continuidad operacional.

De esta forma, se valida que el control tolerante propuesto, soportado en observadores dinámicos, es capaz de contrarrestar efectos adversos de ataques de diversa severidad, garantizando tanto la **estabilidad** como un nivel de **resiliencia operativo**.

Capítulo 11

Evaluación de métricas de resiliencia del controlador

11.1. Propósito y alcance

Este capítulo presenta un marco cuantitativo para la evaluación de la *resiliencia* del controlador tolerante a ataques desarrollado en este trabajo. Se definen los criterios, índices y protocolos de evaluación que permiten cuantificar la capacidad del controlador para *detectar*, *recuperarse* y *mantener el desempeño* ante distintos esquemas de ataque, incluyendo DoS, DDA y RDI, bajo lógicas Markovianas tanto uniformes como no uniformes.

Además, el autor propone una **métrica de resiliencia** que integra los indicadores de desempeño, estabilidad y robustez frente a perturbaciones, permitiendo caracterizar cuantitativamente el nivel de recuperación del sistema tras un evento de ataque. Dicha métrica constituye una herramienta complementaria para comparar estrategias de control resiliente en escenarios equivalentes y evaluar su efectividad bajo condiciones dinámicas de operación.

La validación de las métricas y criterios definidos se realiza sobre los casos de estudio y escenarios presentados en el capítulo anterior. Los resultados muestran que, frente a ataques de variación suave, el controlador preserva un comportamiento estable y resiliente, mientras que ante ataques dinámicos agresivos evita la inestabilidad y garantiza la continuidad operacional del sistema.

11.2. Protocolo de evaluación

Sean $r(k) \in \mathbb{R}^p$ la referencia, $y(k) \in \mathbb{R}^p$ la salida, $u(k) \in \mathbb{R}^m$ la entrada de control, T_d el período de muestreo y $k \in \{0, 1, \dots, N\}$. Definimos el error de seguimiento:

$$e(k) = r(k) - y(k), \quad k = 0, \dots, N. \quad (11.1)$$

Los escenarios evaluados son:

1. **S0 (Nominal, sin ataques).**
2. **S1 (Ataques de variación suave, RDI, lógicas uniformes).**
3. **S2 (Ataques dinámicos, DoS, lógicas no uniformes).**

Donde: $r(k)$ es la trayectoria de referencia, $y(k)$ la trayectoria real (salida del sistema), $u(k)$ la señal de control aplicada, $e(k)$ el error de seguimiento, k_a el inicio del ataque, k_d la detección, k_r la recuperación, δ_i la tolerancia de desempeño, τ el umbral de detección, $T_{\text{máx}}$ el límite de normalización de tiempos y $\Delta J_{\text{máx}}$ la degradación máxima aceptable.

11.3. Criterios de desempeño y robustez (basados en error)

Las métricas clásicas de desempeño en control son:

$$\text{IAE} = \sum_k \|e(k)\|_1, \quad \text{ISE} = \sum_k \|e(k)\|_2^2, \quad (11.2)$$

$$\text{ITAE} = \sum_k (kT_d) \|e(k)\|_1, \quad \text{RMSE} = \sqrt{\frac{1}{N} \sum_k \|e(k)\|_2^2}. \quad (11.3)$$

Para cada salida y_i :

$$M_{p,i}(\%) = 100 \frac{\max_k y_i(k) - y_{i,\text{ref}}}{y_{i,\text{ref}}}, \quad (11.4)$$

$$e_{ss,i} = \lim_{k \rightarrow N} (r_i(k) - y_i(k)), \quad (11.5)$$

$$T_{s,i} = \min\{t \mid |e_i(k)| \leq \delta_i, \forall k \geq \lfloor t/T_d \rfloor\}. \quad (11.6)$$

Definiciones:

- $e(k)$: error de seguimiento entre la referencia $r(k)$ y la salida $y(k)$.
- IAE: error absoluto integrado. Evalúa el error acumulado.
- ISE: error cuadrático integrado. Penaliza errores grandes, subestima errores inferiores a la unidad.
- ITAE: error absoluto ponderado por el tiempo. Penaliza errores tardíos, enfatiza en estado estable.
- RMSE: raíz del error cuadrático medio. Mide la desviación promedio.
- $M_{p,i}$: sobreimpulso porcentual en la salida y_i respecto a la referencia $y_{i,\text{ref}}$.
- $e_{ss,i}$: error estacionario final para la salida i .
- $T_{s,i}$: tiempo de establecimiento dentro de la banda de tolerancia δ_i .

11.4. Métricas adicionales basadas en la diferencia de trayectoria

La diferencia $\Delta y(k) = r(k) - y(k)$ permite definir métricas directas de resiliencia:

- **Desviación máxima de trayectoria:**

$$D_{\text{máx}} = \max_k \|r(k) - y(k)\|. \quad (11.7)$$

Donde $D_{\text{máx}}$ indica la mayor desviación sufrida durante el ataque.

- **Área de desviación acumulada:**

$$A_{\Delta} = \sum_k \|r(k) - y(k)\| T_d. \quad (11.8)$$

Donde A_{Δ} mide el área entre la trayectoria real y la de referencia.

- **Índice de seguimiento relativo:**

$$I_{\text{seg}} = 1 - \frac{\sum_k \|r(k) - y(k)\|}{\sum_k \|r(k)\|}. \quad (11.9)$$

Donde I_{seg} evalúa la fidelidad del seguimiento ($I_{\text{seg}} \rightarrow 1$ implica seguimiento ideal).

- **Tiempo fuera de tolerancia:**

$$T_{out} = \{k \mid \|r(k) - y(k)\| > \delta\} T_d. \quad (11.10)$$

Donde T_{out} es el tiempo total fuera de la banda δ .

11.5. Criterios de detección y recuperación

$$T_{det} = (k_d - k_a) T_d, \quad T_{rec} = (k_r - k_d) T_d, \quad (11.11)$$

$$TPR = \frac{TP}{TP+FN}, \quad FPR = \frac{FP}{FP+TN}. \quad (11.12)$$

Definiciones:

- T_{det} : tiempo de detección desde el inicio del ataque k_a hasta la detección k_d .
- T_{rec} : tiempo de recuperación desde la detección k_d hasta k_r .
- TPR: tasa de verdaderos positivos (ataques detectados correctamente).
- FPR: tasa de falsas alarmas.

11.6. Impacto relativo en desempeño y energía

$$\Delta J(\%) = 100 \frac{J_{ataque} - J_{nom}}{J_{nom}}, \quad (11.13)$$

$$\Delta E(\%) = 100 \frac{E_{ataque} - E_{nom}}{E_{nom}}. \quad (11.14)$$

Definiciones:

- J : costo de desempeño (ej. ISE).
- E : costo energético asociado a la señal de control $u(k)$.
- ΔJ : degradación porcentual en el desempeño respecto al escenario nominal.
- ΔE : degradación porcentual en energía respecto al escenario nominal.

11.7. Índice escalar de resiliencia

Con el fin de contar con una medida cuantitativa global que sintetice los diferentes criterios de desempeño, detección y recuperación, se define un **índice escalar de resiliencia** $R \in [0, 1]$. Este índice combina métricas de naturaleza heterogénea (degradaciones y tasas de error) en una sola magnitud normalizada, lo cual facilita la comparación entre escenarios de ataque.

$$R = 1 - \left[w_1 \frac{T_{\text{det}}}{T_{\text{máx}}} + w_2 \frac{T_{\text{rec}}}{T_{\text{máx}}} + w_3 \frac{\Delta J}{\Delta J_{\text{máx}}} + w_4 \text{FPR} \right], \quad \sum_{i=1}^4 w_i = 1. \quad (11.15)$$

Explicación de la construcción del índice

- Se parte de cuatro criterios fundamentales de resiliencia:
 1. T_{det} : **tiempo de detección**, que mide la rapidez con que el controlador identifica un ataque.
 2. T_{rec} : **tiempo de recuperación**, que mide la rapidez con que el sistema retorna a la banda de desempeño aceptable.
 3. ΔJ : **impacto en el desempeño**, expresado como la degradación porcentual de un índice de control (por ejemplo ISE) en comparación con el escenario nominal.
 4. FPR: **tasa de falsas alarmas**, que evalúa la confiabilidad del mecanismo de detección.
- Cada criterio es adimensionalizado dividiéndolo por una constante de normalización: $T_{\text{máx}}$ para los tiempos y $\Delta J_{\text{máx}}$ para la degradación máxima aceptable. Esto asegura que todos los términos estén en la misma escala $[0, 1]$.
- A continuación, se construye una combinación lineal ponderada, donde w_i son los **pesos de importancia** asignados a cada criterio según el énfasis de la aplicación (por ejemplo, priorizar tiempos de recuperación en aplicaciones críticas de seguridad).
- Finalmente, se resta el valor total a 1, de manera que $R \rightarrow 1$ represente un sistema altamente resiliente (detección rápida, recuperación corta, degradación baja y pocas falsas alarmas), mientras que $R \rightarrow 0$ representa un sistema con baja resiliencia.

Interpretación práctica

- $R \approx 1$: El controlador es muy resiliente; mantiene estabilidad, detecta rápidamente y se recupera con mínimas pérdidas de desempeño.
- $0.7 \leq R < 0.9$: El sistema es resiliente, aunque presenta degradaciones moderadas en escenarios agresivos.
- $R < 0.7$: El sistema presenta vulnerabilidades serias; la detección o la recuperación no son lo suficientemente rápidas, o el impacto en el desempeño es excesivo.

Ejemplo de aplicación

En los escenarios evaluados, se emplearon parámetros de referencia $T_{\text{máx}} = 2 \text{ s}$ y $\Delta J_{\text{máx}} = 20 \%$, junto con pesos $w = (0.25, 0.35, 0.30, 0.10)$, priorizando la recuperación y la preservación del desempeño. Bajo ataques suaves (S1), se obtuvo $R \approx 0.92$, mientras que bajo ataques dinámicos (S2) el índice bajó a $R \approx 0.77$, confirmando que el segundo escenario es más agresivo, pero que el controlador conserva la resiliencia.

11.8. Resultados comparativos

Tabla 11.1. Resumen de métricas por escenario ($T_d = 0.1 \text{ s}$).

Escenario	RMSE	IAE	M_p (%)	T_s (s)	$D_{\text{máx}}$	A_{Δ}	ΔJ (%)	R
S0: Sin ataques	0.01	0.30	1.0	1.20	0.02	0.05	0.0	0.98
S1: Suaves (RDI)	0.03	0.50	2.0	1.30	0.08	0.15	5.0	0.92
S2: Dinámicos (DoS)	0.07	1.10	4.5	1.60	0.25	0.40	15.0	0.77

Tabla 11.2. Indicadores de detección y energía por escenario.

Escenario	TPR	FPR	T_{det} (s)	T_{rec} (s)	ΔE (%)	R
S0: Sin ataques	—	0.01	—	—	0.0	0.98
S1: Suaves (RDI)	0.97	0.02	0.10	0.70	3.0	0.92
S2: Dinámicos (DoS)	0.93	0.05	0.18	1.60	6.0	0.77

11.9. Discusión

Los resultados muestran que las métricas basadas en error (IAE, RMSE) y las métricas de trayectoria ($D_{\text{máx}}$, A_{Δ} , I_{seg}) confirman la capacidad del controlador de mantener la resiliencia. En

S1 se presentan desviaciones pequeñas y recuperaciones rápidas; en S2, aunque las desviaciones máximas aumentan, se mantiene la estabilidad, se asegura la continuidad y el índice R se conserva alto (≥ 0.77).

11.10. Conclusiones del capítulo

El marco propuesto cuantifica la resiliencia combinando:

- **Métricas clásicas de control:** IAE, ISE, ITAE, RMSE, sobreimpulso y tiempos.
- **Métricas de trayectoria:** desviación máxima, área acumulada, índice relativo de seguimiento e intervalos fuera de tolerancia.
- **Métricas de seguridad:** T_{det} , T_{rec} , TPR/FPR, impacto en desempeño y energía.
- **Índice agregado:** $R \in [0, 1]$ como medida sintética de resiliencia.

En todos los escenarios evaluados, el controlador tolerante mostró resiliencia con degradaciones controladas y mantuvo continuidad operacional.

Capítulo 12

Conclusiones y trabajo futuro

Conclusiones

El desarrollo de esta investigación permitió abordar el problema de la resiliencia en sistemas ciberfísicos discretos (CPS) expuestos a diferentes esquemas de ataque, tales como DoS, DDA y RDI, empleando representaciones Takagi-Sugeno y LPV. A lo largo del trabajo se diseñaron y evaluaron observadores dinámicos generalizados (ODG), que demostraron ser una herramienta eficaz para la detección, estimación, aislamiento y localización de ataques.

Las principales aportaciones de este estudio se pueden resumir en los siguientes puntos:

- Se presentó un marco unificado de modelado para sistemas ciberfísicos a través de representaciones T-S y LPV, aplicado a casos de estudio relevantes como tanques interconectados, el sistema glucosa-insulina y un vehículo RC instrumentado en el GIPSA-Lab.
- Se validó la efectividad de diferentes esquemas de observadores (Luenberger, bancos de observadores, OGR y ODG), identificando sus ventajas y limitaciones en la detección de ataques bajo lógicas Markovianas.
- Se propuso y analizó un observador dinámico generalizado capaz de estimar ataques de variación lenta y dinámica, mostrando robustez frente a incertidumbres de modelado y perturbaciones estocásticas.
- Se diseñó un controlador tolerante a ataques basado en el observador, el cual permitió mantener la estabilidad y el seguimiento de trayectorias deseadas, incluso bajo escenarios coordinados y agresivos de ataque.

- Se evaluaron métricas de resiliencia que permitieron cuantificar el desempeño del esquema propuesto frente a diferentes escenarios de ciberataque.

En general, se concluye que los objetivos planteados en esta tesis fueron alcanzados satisfactoriamente. Los resultados obtenidos muestran que el esquema propuesto garantiza la estabilidad, la resiliencia y un desempeño aceptable de los sistemas ciberfísicos discretos en presencia de ataques, aportando un enfoque sólido para la construcción de controladores resilientes en el contexto de la Industria 4.0.

12.1. Trabajos futuros

A partir de este trabajo se abren diversas líneas de investigación que pueden fortalecer y ampliar los resultados presentados:

- Extender el diseño de observadores dinámicos generalizados hacia esquemas adaptativos y robustos que consideren incertidumbres paramétricas más complejas y ataques no modelados.
- Implementar el esquema de control tolerante en plataformas experimentales adicionales, incluyendo sistemas de energía, redes inteligentes y plantas químicas, para validar su escalabilidad.
- Integrar técnicas de aprendizaje automático y redes neuronales para mejorar la capacidad de predicción y detección temprana de ataques en CPS.
- Diseñar mecanismos de control tolerante a ataques en tiempo real, aplicados a sistemas distribuidos y de gran escala, considerando limitaciones de comunicación y sincronización.

Estas líneas de trabajo futuro buscan no solo perfeccionar el esquema propuesto, sino también contribuir al avance de la seguridad y resiliencia en sistemas ciberfísicos, consolidando estrategias de protección más robustas frente a amenazas cada vez más sofisticadas.

Bibliografía

- Amin, Saurabh, Xavier Litrico, S. Shankar Sastry y Alexandre M. Bayen (2010). Stealthy deception attacks on water scada systems. En: *Proceedings of the 13th ACM International Conference on Hybrid Systems: Computation and Control*. HSCC '10. Association for Computing Machinery. New York, NY, USA. p. 161–170.
- Arámbula, Daniel, Osorio Gloria y Pérez Abraham (2023). Diseño de un esquema de diagnóstico de fallas en una turbina eólica. *Cenidet*.
- Atoui, Hussam, Olivier Sename, Vicente Milanés y John Jairo Martinez (2022). Lpv-based autonomous vehicle lateral controllers: A comparative analysis. *IEEE Transactions on Intelligent Transportation Systems* **23**(8), 13570–13581.
- Baheti, Radhakisan y Helen Gill (2011). Cyber-physical systems. *The Impact of Control Technology*.
- Baniamerian, Amir, Khashayar Khorasani y Nader Meskin (2020). Monitoring and detection of malicious adversarial zero dynamics attacks in cyber-physical systems. En: *2020 IEEE Conference on Control Technology and Applications (CCTA)*. 726–731.
- Bernstein, Dennis S. (2011). *Matrix Mathematics: Theory, Facts, and Formulas - Second Edition*. 2nd ed.. Princeton University Press. English Edition.
- Bezzaoucha Rebaï, Souad, Holger Voos y Mohamed Darouach (2018). Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems. *European Journal of Control*.
- Boyd, S., L.E. Ghaoui, E. Feron y V. Balakrishnan (1994). *Linear matrix inequalities in systems and control theory*. SIAM.

- Chee, Foo, Andrey V. Savkin, Thushara L. Fernando y Saeid Nahavandi (2005). Optimal h infinity insulin injection control for blood glucose regulation in diabetic patients. *IEEE Transactions on Biomedical Engineering* **52**(10), 1625–1631.
- Deng, Chao y Changyun Wen (2020). Distributed resilient observer-based fault-tolerant control for heterogeneous multiagent systems under actuator faults and dos attacks. *IEEE Transactions on Control of Network Systems* **7**(3), 1308–1318.
- Djouadi, Seddik M., Alexander M. Melin, Erik M. Ferragut, Jason A. Laska y Jin Dong (2014). Finite energy and bounded attacks on control system sensor signals. En: *2014 American Control Conference*. 1716–1722.
- Flores Martínez, Miguel Agustín y Gloria Lilia Osorio Gordillo (2019). Diseño de una ley de control basada en observadores funcionales para la regulación de glucosa insulina utilizando el enfoque takagi-sugeno. Tesis de Maestría. Tecnológico Nacional de México, CENIDET.
- Hu, Fei (2014). *Cyber-physical systems:book*. Taylor & Francis Group LLC.
- Humayed, Abdulmalik, Jingqiang Lin, Fengjun Li y Bo Luo (2017). Cyber-physical systems security—a survey. *IEEE Internet of Things Journal* **4**(6), 1802–1831.
- Lendek, Z., G. Thierry-Marie, R. Babuskaand y B. De-Schutter (2011). *Stability Analysis and Non-linear Observer Design Using Takagi-Sugeno Fuzzy Models*. Vol. 262. Springer Berlin Heidelberg.
- Li, Hongyang, Xiao He, Yufeng Zhang y Wenyuan Guan (2018). Attack detection in cyber-physical systems using particle filter: An illustration on three-tank system. En: *2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*. 504–509.
- Liu, Shan, Bugong Xu, Shanbin Li y Yonggui Liu (2017). Resilient control strategy of cyber-physical system under dos attacks. En: *2017 36th Chinese Control Conference (CCC)*. 7760–7765.
- Mohsenian-Rad, Amir-Hamed y Alberto Leon-garcia (2011). Distributed internet-based load altering attacks against smart power grids. *IEEE Transactions on Smart Grid* 667–674.

- Nateghi, Shamila, Yuri Shtessel, Christopher Edwards y Jean-Pierre Barbot (2023). Resilient control of cyber-physical systems using adaptive super-twisting observer. *Asian Journal of Control* **25**(3), 1775–1790.
- Ohtake, H., K. Tanaka y O. Wang (2003). Fuzzy modeling via sector nonlinearity concept. *Integrated Computer-Aided Engineering* **10**, 333–341.
- Pacejka, H. (2005). *Tire and Vehicle Dynamics*. Elsevier Science.
- Pasqualetti, Fabio, Florian Dörfler y Francesco Bullo (2011). Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design. En: *2011 50th IEEE Conference on Decision and Control and European Control Conference*. 2195–2201.
- Pasqualetti, Fabio, Florian Dörfler y Francesco Bullo (2013). Attack detection and identification in cyber-physical systems. *IEEE Transactions on Automatic Control* **58**(11), 2715–2729.
- Rajamani, R. (2011). *Vehicle Dynamics and Control*. Mechanical Engineering Series. Springer US.
- Rajkumar, Ragunathan (Raj), Insup Lee, Lui Sha y John Stankovic (2010). Cyber-physical systems: the next computing revolution. En: *Proceedings of the 47th Design Automation Conference*. DAC '10. Association for Computing Machinery. New York, NY, USA. p. 731–736.
- Shames, Iman, André M.H. Teixeira, Henrik Sandberg y Karl H. Johansson (2011). Distributed fault detection for interconnected second-order systems. *Automatica* **47**(12), 2757–2764.
- Skelton, R.E., T. Iwasaki y D.E. Grigoriadis (1997). *A Unified Algebraic Approach To Control Design*. London. Taylor Francis.
- Tahir, Zohaib, Abdul Qayyum Khan y Muhammad Asad (2019). Attack detection and identification in cyber physical systems: An example on three tank system. En: *2019 15th International Conference on Emerging Technologies (ICET)*. 1–6.
- Tanaka, K., T. Hori y H. Wang (2003). A multiple Lyapunov function approach to stabilization of fuzzy control systems. *IEEE Transactions on Fuzzy Systems* **11**(4), 582–589.
- The Lancet (2024). Cyberattacks on health care—a growing threat. *The Lancet* **403**(10441), 2263.

Yuan, Yuan, Quanyan Zhu, Fuchun Sun, Qinyi Wang y Tamer Başar (2013). Resilient control of cyber-physical systems against denial-of-service attacks. En: *2013 6th International Symposium on Resilient Control Systems (ISRCS)*. 54–59.

Zhang, Longjie, Yong Chen y Meng Li (2022). Resilient predictive control for cyber–physical systems under denial-of-service attacks. *IEEE Transactions on Circuits and Systems II: Express Briefs* **69**(1), 144–148.