Memorias del 2023 Congreso Nacional de Control Automático
25-27 de Octubre, 2023. Acapulco, Guerrero, México.

Observer design for detection of attack patterns in cyber-physical systems

A.-R. Guadarrama-Estrada * **G.-L. Osorio-Gordillo** *
C.M. Astorga-Zaragoza * **J. Reyes-Reyes** *

* *Tecnológico Nacional de México/CENIDET, Interior Internado Palmira S/N, Col. Palmira, Cuernavaca, Mor. México.*
e-mail: d19ce018@cenidet.tecnm.mx

Abstract. This article focuses on the design of a Luenberger structure observer with residual generation for the detection of different attack schemes (Denial of Service (DoS) and False Data Injection (FDI)) targeting the sensors and actuators of a discrete cyber-physical system. To simulate a more realistic attack signal, Markovian distribution logic is used to simulate the behavior of the signals. To demonstrate the effectiveness of the proposed scheme, a system of three interconnected tanks is used.

Keywords: Luenberger observer, Denial of Service attack, False Data Injection attack, Markovian Stochastic Processes, Cyber-Physical System.

1. INTRODUCCIÓN

En los últimos años, en el área de ingeniería han surgido una serie de sistemas que incorporan la parte cibernética y la física, conocidos como sistemas ciber-físicos(CPS, por sus siglas en inglés) Rajkumar et al. (2010); Baheti and Gill (2011); Yuan et al. (2013). Estos sistemas han revolucionado la industria debido a que incorporan conocimientos de la ingeniería informática, comunicaciones y control automático de los procesos físicos.

Dichos sistemas tienen la capacidad de poder monitorear y controlar procesos en tiempo real. Además, facilitan la recopilación y análisis de grandes volúmenes de datos generados por los sistemas para su posterior análisis, para la implementación de estrategias de control, seguridad o detección óptimas para garantizar el funcionamiento del proceso físico utilizado.

Sin embargo, junto con los beneficios, también surgen nuevos desafíos debido a la complejidad y el envío de datos por estructuras de comunicación no seguras. Por lo tanto, los sistemas ciber-físicos están expuestos a riesgos de seguridad, ya que la conectividad que se utiliza y la dependencia de la tecnología digital pueden ser aprovechadas por distintos atacantes para perjudicar el funcionamiento para alcanzar algún interés, causar daños o robar información Orojloo and Azgomi (2015); Bordel Sánchez et al. (2017). Por lo tanto, es crucial desarrollar estrategias de protección y detección de ataques en estos sistemas, garantizando así su integridad y confiabilidad.

Entre los ataques más comunes abordados por los investigadores del área de control automático se encuentran la denegación de servicio (DoS) y la inserción de datos falsos (IDF). Dichos esquemas de ataque han sido estudiados y abordados debido a su impacto potencialmente perjudicial en el funcionamiento de los sistemas ciber-físicos Li et al. (2016); Bezzaoucha Rebaï et al. (2018). Para comprender y contrarrestar la dinámica de estos ataques, los investigadores han recurrido a la técnica de distribución estocástica Markoviana. La cual nos permite modelar el comportamiento de los ataques de forma más real.

Para contrarrestar dichos esquemas de ataques, la implementación de distintas técnicas de detección eficientes se ha convertido en una prioridad. Entre las técnicas utilizadas, los bancos de observadores y observadores generadores de residuos desempeñan un papel fundamental al proporcionar información sobre el comportamiento del sistema, para identificar cambios inesperados en las variables de interés y alertar sobre posibles ataques o intrusiones Shames et al. (2010); Bezzaoucha Rebaï et al. (2018); Joo et al. (2021).

Finalmente, la principal contribución de este artículo es proponer una estructura de detección basada en un observador tipo Luenberger. Aunque esta estructura de observador puede parecer básica, su implementación inicial es solo el comienzo de una investigación más amplia sobre diversas técnicas y enfoques para lograr la implementación de controladores resilientes. La información generada por el observador servirá como punto de partida para futuras investigaciones en el desarrollo de estrategias de control resilientes y robustas. Finalmente para validar el esquema de detección propuesto, se realizaran varias simulaciones

utilizando un sistema de tres tanques interconectados Tahir et al. (2019); Januário et al. (2019).

2. FORMULACIÓN DEL PROBLEMA

Considere un sistema lineal (1) con la característica de los sistemas ciber-físicos, la cual consiste en que la entrada y salida del sistema se muestrean en momentos discretos de tiempo debido a que se considera que la entrada y salida son enviadas de forma remota:

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) + F_1 a_a(k) \\ y(k) &= Cx(k) + F_2 a_s(k) \end{aligned} \tag{1}$$

donde $x(k) \in \mathbb{R}^n$ es el vector de estados del sistema, $u(k) \in \mathbb{R}^m$ es la entrada del sistema, $y(k) \in \mathbb{R}^p$ representa las variables de salida medidas. Las matrices $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $C \in \mathbb{R}^{p\times n}$, son matrices conocidas. $F_1 \in \mathbb{R}^{n\times m}$ $F_2 \in \mathbb{R}^{p\times n}$ son las matrices de acoplamiento de los ataques $a_a(k)$ y $a_s(k)$ representan la señal de ataque al actuador y sensor, respectivamente.

Se asume que el sistema (1) cumple con la propiedad de observabilidad:

$$\mathbf{rank}\left[\, C \;\; CA \;\; \ldots \;\; CA^{n-1} \,\right]^T = n \tag{2}$$

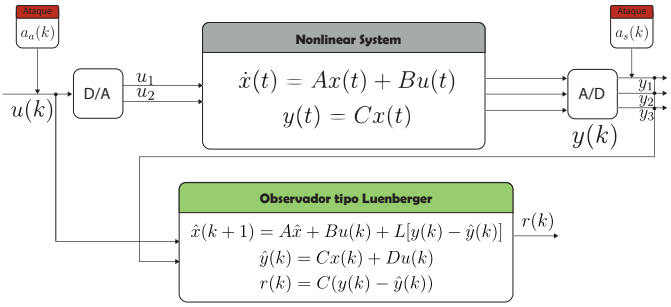

Figure 1. Esquema de detección

La Figura 1 muestra el esquema de generación residual, cabe mencionar que dicho esquema permite detectar ataques en sensores y actuadores.

Considere el observador con estructura tipo Luenberger para el sistema lineal discreto (1)

$$\begin{aligned} \hat{x}(k+1) &= A\hat{x}(k) + Bu(k) + L[y(k) - \hat{y}(k)] \\ \hat{y}(k) &= C\hat{x}(k) \\ r(k) &= y(k) - \hat{y}(k) \end{aligned} \tag{3}$$

donde $\hat{x}(k) \in \mathbb{R}^n$ que representa los estados estimados por el observador, $r(k) \in \mathbb{R}^p$ representa los residuos generados por el observador, $\hat{y}(k) \in \mathbb{R}^p$ es el vector de estimación de la salida y $L \in \mathbb{R}^{n\times p}$ es la ganancia del observador.

Por simplicidad podemos reescribir las ecuaciones de (3) de la siguiente manera, lo cual nos ayudara posteriormente en la sustitución:

$$\hat{x}(k+1) = A\hat{x}(k) + Bu(k) + LC(x(k) - \hat{x}(k)) \tag{4}$$

$$\hat{y}(k) = C\hat{x}(k) \tag{5}$$

El error de estimación está dado por $e(k) = x(k) - \hat{x}(k)$, de modo que la dinámica del error de estimación es:

$$e(k+1) = x(k+1) - \hat{x}(k+1) \tag{6}$$

Sustituyendo las ecuaciones (1) y (5), en (6) se obtiene:

$$e(k+1) = Ax(k) + Bu(k) - \overbrace{(A - LC)}^{\overline{A}}\hat{x}(k) - Ly(k) \tag{7}$$

Al simplificar y sustituir $\hat{x} = x(k)+e(k)$ en (7) obtenemos:

$$e(k+1) = Ax(k) + Bu(k) - \overline{A}(x(k) - e(k)) - LCx(k) \tag{8}$$

donde

$$e(k+1) = \overline{A}e(k) + (A - LC - \overline{A})x(k) + Bu(k) \tag{9}$$

Obtenieindo:

$$e(k+1) = (A - LC)e(k) \tag{10}$$

Posteriormente, establecemos el residuo $r(k)$ el cual es la diferencia entre la salida y la salida estimada tal que:

$$\begin{aligned} r(k) &= y(k) - \hat{y}(k) \\ r(k) &= C\underbrace{(x(k) - \hat{x}(k))}_{e(k)} \end{aligned} \tag{11}$$

Por lo tanto, tenemos las expresiones para $e(k+1)$ y $r(k)$, las cuales nos proporciona información del esquema de ataque al actuador y sensor respectivamente,

$$\begin{aligned} e(k+1) &= (A - LC)e(k) + F_1 a_a(k) \\ r(k) &= Ce(k) + F_2 a_s(k) \end{aligned} \tag{12}$$

3. FORMULACIÓN DE ESQUEMAS DE ATAQUE

En esta sección, se definirán los distintos esquemas de ataque que serán considerados para comprometer el buen funcionamiento del sistema ciber-físico seleccionado.

3.1 Ataques de denegación de servicio (DoS)

El objetivo de este tipo de esquema de ataque busca impedir la transmisión de datos de control y lectura de datos del controlador, por lo regular esta intromisión de señal puede ser lanzado mediante la interferencia de los canales de comunicación, saturación de paquetes de datos en la red o cancelación de las señales.

Los esquemas de ciber-ataques a sensor y actuador tienen la siguiente forma:

$$\begin{aligned} a^s(k) &= -x(k) \\ a^a(k) &= -u(k) \end{aligned} \tag{13}$$

Utilizamos la ecuación del sistema (1) en conjunto con la ecuación del ataque tipo DoS dirigido al sensor y actuador (13) obteniendo:

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) - \alpha(k)F_1 a_a(k) \\ y(k) &= Cx(k) - \beta(k)F_2 a_s(k) \end{aligned} \tag{14}$$

donde $a_a(k) \in \mathbb{R}^r$ representa ataque dirigido al actuador y $a_s(k) \in \mathbb{R}^m$ representa el ataque del sensor. A, B, C, F_1 y F_2 son matrices constantes conocidas. $\alpha(k)$ y $\beta(k)$ se refiere a los procesos estocásticos Markovianos que toman valores de 0 y 1.

3.2 Ataque de inserción de dato falso

El objetivo de este tipo de esquema es afectar, remplazando la lectura del sensor y del controlador, haciendo sea diferente de la señal real de lectura o control de datos. Cuando el sistema (1) se ve afectado por el ataque de inyección de datos falsos (IDF), las ecuaciones tiene la siguiente forma:

$$\begin{aligned} a_s(k) &= -x(k) + b_s(k) \\ a_a(k) &= -u(k) + b_a(k) \end{aligned} \tag{15}$$

donde $b_a(k)$ y $b_s(k)$ son datos engañosos que el adversario intenta lanzar sobre el actuador y el sensor, respectivamente. Sustituyendo la ecuación (15) en (16) obtenemos:

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) - \alpha(k)F_1u(k) + \alpha(k)F_1b_a(k) \\ y(k) &= Cx(k) - \alpha(k)F_2x(k) + \alpha(k)F_2b_s(k) \end{aligned} \tag{16}$$

4. ANÁLISIS DE ESTABILIDAD DEL OBSERVADOR

En esta sección se lleva a cabo análisis de estabilidad de la dinámica del error de estimación de la Ecuación (10) proponiendo una función de Lyapunov.

Consideramos la siguiente función de Lyapunov para realizar el análisis de estabilidad:

$$V(e(k)) = e^T(k)Pe(k) > 0 \tag{17}$$

donde $P > 0$. La variación de $V(e(k))$ a lo largo de la solución de (12) es

$$\begin{aligned} \Delta V(e(k)) &= V(e(k+1)) - V(e(k)) \\ &= e^T(k+1)Pe(k+1) - e^T(k)Pe(k) \end{aligned} \tag{18}$$

reemplazado $e(k+1)$ de la ecuación (1), se obtiene

$$\begin{aligned} \Delta V(e(k)) =& e^T(k) \\ & [(A-LC)^TP(A-LC) - P]\varphi(k) \end{aligned} \tag{19}$$

La desigualdad $\Delta V(\varphi(k)) < 0$ se cumple si

$$(A-LC)^TP(A-LC) - P < 0, \tag{20}$$

Aplicando el complemento de Schur (Boyd et al., 1994) en la desigualdad (20) se tiene

$$\begin{bmatrix} -P & (A-LC)^TP \\ P(A-LC) & -P \end{bmatrix} < 0 \tag{21}$$

Resolviendo la desigualdad matricial lineal (LMI) dada por la ecuación (21) utilizando la herramienta Yalmip en Matlab se pueden obtener los valores para la matriz L.

5. CASO DE ESTUDIO

5.1 Modelo de un sistema de tres tanques interconectados

En el campo de la ingeniería de procesos químicos, los sistemas de tanques interconectados desempeñan un papel crucial. Constituyen una herramienta esencial para el control automático. Estos sistemas están compuestos por múltiples tanques que se encuentran interconectados mediante tuberías y válvulas estratégicamente ubicadas. La

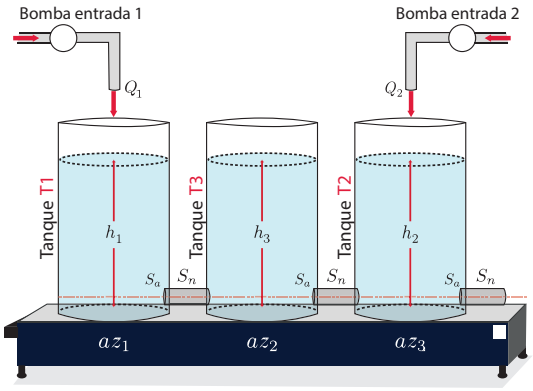

Figure 2. Esquema caso de estudio (Tres tanques interconectados)

finalidad principal de estos sistemas radica en el control y regulación del nivel de líquido presente en cada tanque, como se muestra en la Figura 2.

El modelo lineal en tiempo discreto es el siguiente Li et al. (2018):

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) \\ y(k) &= Cx(k) \end{aligned} \tag{22}$$

Definimos las variables: $x(k) = \begin{bmatrix} h_1(k) \\ h_2(k) \\ h_3(k) \end{bmatrix}$, $u(k) = \begin{bmatrix} Q_1(k) \\ Q_2(k) \end{bmatrix}$,

$y(k) = \begin{bmatrix} h_1(k) \\ h_2(k) \\ h_3(k) \end{bmatrix}$, $C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} \frac{1}{S_a} & 0 \\ 0 & \frac{1}{S_a} \\ 0 & 0 \end{bmatrix}$,

$A = \begin{bmatrix} A_{11} & 0 & A_{13} \\ 0 & A_{21} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{bmatrix}$

$A_{11} = -\dfrac{az_1S_ng}{S_a\sqrt{2g(h_1(t)-h_3(t))}}$ $\quad A_{13} = -\dfrac{az_1S_ng}{S_a\sqrt{2g(h_1(t)-h_3(t))}}$

$A_{21} = -\dfrac{az_3gS_n}{S_a\sqrt{2g(h_3(t)-h_2(t))}} - \dfrac{az_2gS_n}{S_a\sqrt{2gh_3(t)}}$

$A_{23} = \dfrac{az_3gS_n}{S_a\sqrt{2g(h_3(t)-h_2(t))}}$ $\quad A_{31} = \dfrac{az_1S_ng}{S_a\sqrt{2g(h_1(t)-h_3(t))}}$

$A_{32} = \dfrac{az_3gS_n}{S_a\sqrt{2g(h_3(t)-h_2(t))}}$

$A_{33} = -\dfrac{az_1gS_n}{S_a\sqrt{2g(h_1(t)-h_3(t))}} - \dfrac{az_3gS_n}{S_a\sqrt{2g(h_3(t)-h_2(t))}}$

donde az_1, az_2 y az_3 son coeficientes de salida que toman valores de 0 a 1; $Q_1(k)$ y $Q_2(k)$ son los caudales de la bomba 1 y la bomba 2, respectivamente.

6. PARAMETRIZACIÓN DEL CASO DE ESTUDIO

En esta sección se presenta la simulación del sistema de tres tanques interconectados. Para ello, se han establecido los valores de los parámetros del sistema, los cuales se muestran en la Tabla.1 Li et al. (2018).

Table 1. Parámetros primera simulación

Parámetro	Valor	Unidades	Definición
S_a	0.0154	m^2	Sección transversal del Tanque
S_n	5×10^{-5}	m^2	Sección transversal del Tubo
g	9.8	m^2/s	Gravedad
Q_1	0.02	m^3/s	Flujo de entrada 1
Q_2	0.03	m^3/s	Flujo de entrada 2
H_{max}	0.8	m	Altura máxima de los tanques
az_1	0.46		Coeficiente de salida tanque 1
az_2	0.58		Coeficiente de salida tanque 2
az_3	0.48		Coeficiente de salida tanque 3

Una vez establecida la parametrización, el siguiente paso consiste en proponer las señales de entrada para simular el sistema de tres tanques interconectados. En esta etapa, se utilizaron dos señales variables diseñadas a través de la herramienta Signal Builder en el programa Matlab. Utilizar señales variables proporciona un comportamiento dinámico que facilita la comprensión del funcionamiento del caso de estudio seleccionado. La Figura 3 muestra las señales de entrada resultantes.

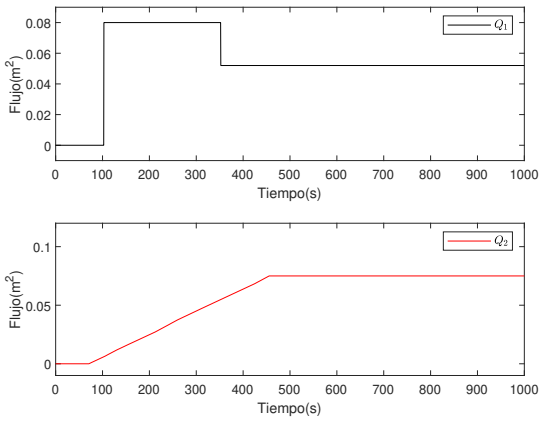

Figure 3. Entradas de flujo variable

A continuación, se lleva a cabo la generación de las señales de lógica Markoviana para simular los esquemas de ataque. En primer lugar, en el lado izquierdo se encuentran las señales generadas para representar la acción no uniforme en el sensor (línea azul) y en el actuador (línea roja). Por otro lado, en el lado derecho se encuentra la acción Markoviana uniforme, la cual se caracteriza por tener un período de activación constante. Estas señales se pueden visualizar en la Figura 4.

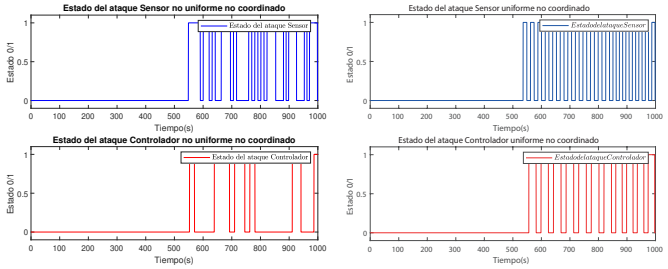

Figure 4. Lógicas Markovianas ataque al sensor

En la siguiente sección, se mostrarán diversas combinaciones de esquemas de ataque dirigidas al caso de estudio de tres tanques interconectados, tanto con lógica uniforme como no uniforme, aplicados en la entrada o salida del sistema. Asimismo, se proporcionará una tabla que muestra los residuos obtenidos en cada una de las simulaciones realizadas.

7. RESULTADOS

En esta sección, se presentan los resultados de la simulación del sistema de tres tanques interconectados bajo diferentes esquemas de ataque. Comenzaremos examinando el ataque tipo dos con lógica uniforme, centrándonos específicamente en el efecto del ataque en el sensor 1 del sistema. Los parámetros utilizados se encuentran detallados en la Tabla 1, mientras que la señal de entrada se muestra en la Figura 3. Se utilizó un paso de integración de $T_e = 0.01$, un tiempo de discretización de $T = 0.001$ y una lógica Markoviana uniforme.

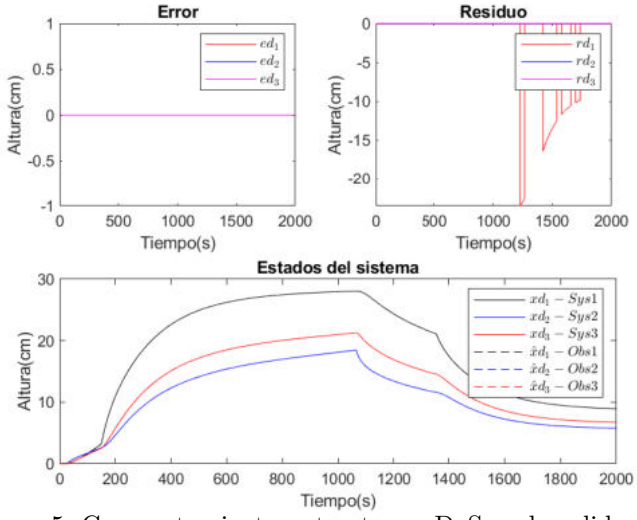

Figure 5. Comportamiento ante ataque DoS en la salida y_1

En la Figura.5 del lado izquierdo se puede observar el efecto en la ecuación del error de ataque de denegación de servicio (DoS) en la salida y_1 del sistema. Además, en la figura de lado derecho se presentan los residuos generados por el observador ante dicho esquema de ataque.

En la siguiente simulación, se considera un esquema de ataques tipo IDF dirigido a la entrada u_2 del sistema. Este tipo de ataque consiste en la inyección de datos falsos con el objetivo de alterar el comportamiento del sistema ciber-físico. El esquema de ataque utiliza una lógica no uniforme. En la Figura del lado izquierdo, se muestra el efecto del ataque IDF en la ecuación del error. Por otro lado, en la parte derecha de la figura, se pueden observar los residuos generados por parte del observador.

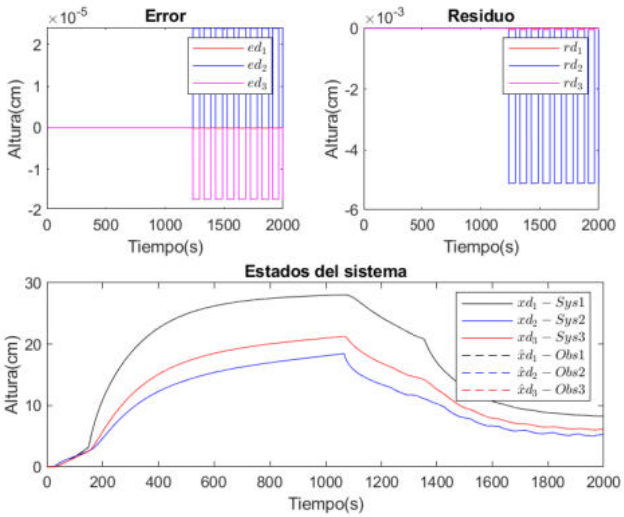

Figure 6. Comportamiento ante ataque IDF en la entrada u_2

En la Figura 7, se presenta el efecto en los estados del sistema y los residuos generados por el observador tipo Luenberger debido al ataque de denegación de servicio (DoS) con lógica no uniforme aplicado a la entrada u_1 y la salida y_3.

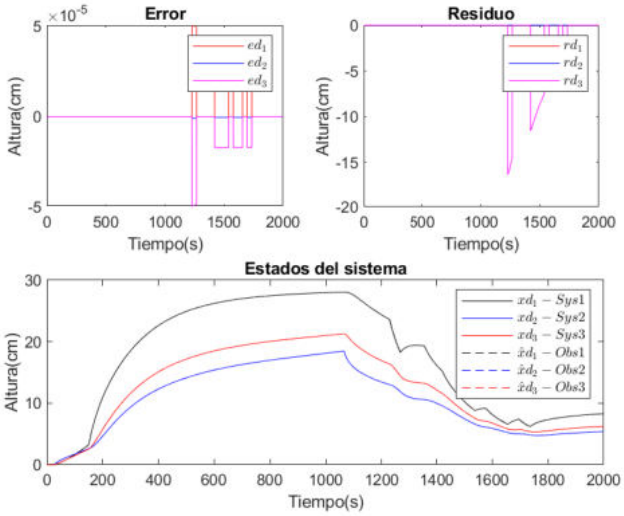

Figure 7. Comportamiento ante ataque DoS entrada y salida

A continuación, se presentan las tablas de residuos generadas para las diferentes combinaciones de esquemas de ataque con distintas lógicas de aplicación. Estas tablas proporcionan una comprensión detallada del efecto provocado por cada esquema de ataque en el sistema.

Las tablas 2, 3 muestran los resultados de simulaciones con diferentes esquemas y lógicas de ataque dirigidos a los sensores del sistema. Indica el impacto de cada combinación de ataques en los residuos, representados como valores cero, negativos o positivos. Cabe mencionar que a primera vista solo conociendo los valores positivo, negativo o cero de las distintas combinaciones de los residuos y valores de error, es imposible diferenciar el efecto de la lógica de distribución o en el caso de ataques en la entrada, identificar si es un caso DoS o IDF, sin embargo, analizando más a detalle cada valor de residuo dado por el observador es más sencillo llevar a cabo una identificación de los distintos esquemas de ataque y su lógica de distribución. Por lo tanto, se concluye que, este observador funciona bien para detectar fácilmente la diferencia de ataques a la entrada o salida o en el caso de ataques en el sensor, el sensor afectado, sin embargo,

Table 2. Tabla de residuos DoS

			Uniforme / No uniforme						
	Enfoque		r_1	r_2	r_3	e_1	e_2	e_3	
Sensor	x_1	-	-	0	0	0	0	0	**Esquema tipo DoS**
	x_2		0	-	0	0	0	0	
	x_3		0	0	-	0	0	0	
	x_1, x_2		-	-	0	0	0	0	
	x_1, x_3		-	0	-	0	0	0	
	x_2, x_3		0	-	-	0	0	0	
	x_1, x_2, x_3		-	-	-	0	0	0	
Actuador	u_1	-	-	0	0	+	-	-	
	u_2		0	-	-	-	+	-	
	u_1, u_2		-	-	-	+	+	-	
Coordinado	x_1	u_1	-	0	0	+	-	-	
	x_2		0	-	0	+	-	-	
	x_3		0	0	-	+	-	-	
	x_1, x_2		-	-	0	+	-	-	
	x_1, x_3		-	0	-	+	-	-	
	x_2, x_3		0	-	-	+	-	-	
	x_1, x_2, x_3		-	-	-	+	-	-	
	x_1	u_2	-	0	0	-	+	-	
	x_2		0	-	0	-	+	-	
	x_3		0	0	-	-	+	-	
	x_1, x_2		-	-	0	-	+	-	
	x_1, x_3		-	0	-	-	+	-	
	x_2, x_3		0	-	-	-	+	-	
	x_1, x_2, x_3		-	-	-	-	+	-	
	x_1	u_1, u_2	-	0	0	+	+	-	
	x_2		0	-	0	+	+	-	
	x_3		0	0	-	+	+	-	
	x_1, x_2		-	-	0	+	+	-	
	x_1, x_3		-	0	-	+	+	-	
	x_2, x_3		0	-	-	+	+	-	
	x_1, x_2, x_3		-	-	-	+	+	-	

se necesita un análisis más minucioso para identificar la lógica de distribución o el caso de ataques conjuntos.

Table 3. Tabla residuos IDF

	Enfoque		Uniforme / No uniforme r_1	r_2	r_3	e_1	e_2	e_3	
Sensor	x_1		-	0	0	0	0	0	
	x_2			-	0	0	0	0	
	x_3		0	0	-	0	0	0	
	x_1, x_2	,	-	-	0	0	0	0	
	x_1, x_3		-	0	-	0	0	0	
	x_2, x_3		0	-	-	0	0	0	
	x_1, x_2, x_3		-	-	-	0	0	0	
Actuador	u_1		-	0	-	+	-	-	
	u_2	,	0	+	-	0	-	-	
	u_1, u_2		+	+	-	-	-	-	
Coordinado	x_1		-	0	0	+	-	-	
	x_2		0	-	0	+	-	-	
	x_3		0	0	-	+	-	-	
	x_1, x_2	u_1	-	-	0	+	-	-	
	x_1, x_3		-	0	-	+	-	-	
	x_2, x_3		0	-	-	+	-	-	
	x_1, x_2, x_3		-	-	-	+	-	-	
	x_1		-	0	0	-	+	-	
	x_2		0	-	0	-	+	-	
	x_3		0	0	-	-	+	-	
	$x1, x_2$	u_2	-	-	0	-	+	-	
	x_1, x_3		-	0	-	-	+	-	
	x_2, x_3		0	-	-	-	+	-	
	x_1, x_2, x_3		-	-	-	-	+	-	
	x_1		-	0	0	+	+	-	
	x_2		0	-	0	+	+	-	
	x_3		0	0	-	+	+	-	
	x_1, x_2	u_1, u_2	-	-	0	+	+	-	
	x_1, x_3		-	0	-	+	+	-	
	x_2, x_3		0	-	-	+	+	-	
	x_1, x_2, x_3		-	-	-	+	+	-	

Esquema tipo IDF

8. CONCLUSIONES

En este artículo se propuso un observador de tipo Luenberger para la detección de esquemas de ataque en la entrada y salida del sistema. Se utilizó como caso de estudio un sistema de tres tanques interconectados desarrollado en tiempo discreto, ya que se trata de un sistema ciber-físico. Sin embargo, se concluyó que este tipo de observador si proporciona parte de información para llevar a cabo una identificación de los distintos esquemas de ataque pero, tienen que analizarse los residuos de forma más minuciosa para entender las características y combinaciones de los distintos esquemas de ataque. Esto plantea la necesidad de buscar técnicas más sofisticadas, como esquemas de localización, aislamiento y detección utilizando observadores robustos o adaptativos, para encontrar una solución adecuada.

REFERENCES

Baheti, R. and Gill, H. (2011). Cyber-physical systems. *null*. doi: null.

Bezzaoucha Rebaï, S., Voos, H., and Darouach, M. (2018). Attack-tolerant control and observer-based trajectory tracking for cyber-physical systems. *European Journal of Control*, 47. doi: 10.1016/j.ejcon.2018.09.005.

Bordel Sánchez, B., Alcarria, R., Robles, T., and Martín, D. (2017). Cyber-physical systems: Extending pervasive sensing from control theory to the internet of things. *Pervasive and Mobile Computing*, 40. doi:10.1016/j.pmcj.2017.06.011.

Boyd, S., Ghaoui, L., Feron, E., and Balakrishnan, V. (1994). *Linear matrix inequalities in systems and control theory*. SIAM.

Januário, F., Cardoso, A., and Gil, P. (2019). A distributed multi-agent framework for resilience enhancement in cyber-physical systems. *IEEE Access*, 7, 31342–31357. doi: 10.1109/ACCESS.2019.2903629.

Joo, Y., Qu, Z., and Namerikawa, T. (2021). Resilient control of cyber-physical system using nonlinear encoding signal against system integrity attacks. *IEEE Transactions on Automatic Control*, 66(9), 4334–4341. doi:10.1109/TAC.2020.3034195.

Li, H., He, X., Zhang, Y., and Guan, W. (2018). Attack detection in cyber-physical systems using particle filter: An illustration on three-tank system. In *2018 IEEE 8th Annual International Conference on CYBER Technology in Automation, Control, and Intelligent Systems (CYBER)*, 504–509. doi: 10.1109/CYBER.2018.8688281.

Li, Y., Voos, H., Darouach, M., and Hua, C. (2016). An application of linear algebra theory in networked control systems: stochastic cyber-attacks detection approach. *IMA Journal of Mathematical Control and Information*, 33(4), 1081–1102. doi: 10.1093/imamci/dnv026.

Orojloo, H. and Azgomi, M.A. (2015). Evaluating the complexity and impacts of attacks on cyber-physical systems. In *2015 CSI Symposium on Real-Time and Embedded Systems and Technologies (RTEST)*, 1–8. doi:10.1109/RTEST.2015.7369840.

Rajkumar, R., Lee, I., Sha, L., and Stankovic, J. (2010). Cyber-physical systems: The next computing revolution. 731–736. doi: 10.1145/1837274.1837461.

Shames, I., Teixeira, A., Sandberg, H., and Johansson, K. (2010). Distributed fault detection for interconnected second-order systems with applications to power networks.

Tahir, Z., Khan, A.Q., and Asad, M. (2019). Attack detection and identification in cyber physical systems: An example on three tank system. In *2019 15th International Conference on Emerging Technologies (ICET)*, 1–6. doi: 10.1109/ICET48972.2019.8994635.

Yuan, Y., Zhu, Q., Sun, F., Wang, Q., and Başar, T. (2013). Resilient control of cyber-physical systems against denial-of-service attacks. In *2013 6th International Symposium on Resilient Control Systems (ISRCS)*, 54–59. doi:10.1109/ISRCS.2013.6623750.