Revista Iberoamericana de Automática e Informática Industrial

Revista Iberoamericana de Automática e Informática industrial 21 (2024) 1–8

www.revista-riai.org

Protocolo de enmascaramiento para observador en pila de combustible

Pol Baldomà Mitjans*, Andreu Cecilia, Ramón Costa Castelló

Universitat Politécnica de Catalunya, Avinguda Diagonal, 647, 08028, Barcelona, España

To cite this article: Baldomà-Mitjans, P., Cecilia, A., Costa-Castelló, R. 2024. Masking protocol for fuel cell model based nonlinear observer. Revista Iberoamericana de Automática e Informática industrial, 1, 1-8. https://doi.org/10.4995/riai.2024.21924

Resumen

En los últimos años, las pilas de combustible de membrana electrolítica polimérica han visto incrementada su popularidad debido a su alta eficiencia energética y sus nulas emisiones en operación. Una de las aplicaciones destacadas para estos dispositivos es su inclusión en redes eléctricas inteligentes. En el marco de control de estas redes, una o varias capas de control se suelen implementar en el ciberespacio, lo que añade el riesgo de la posible recepción de ciberataques. Con esto en mente, en este trabajo se considera el problema de protección de datos, aplicado en el canal de comunicación entre una pila de combustible y un observador. En concreto, se considera un observador no lineal, basado en propiedades de pasividad, y se propone un mecanismo modular de enmascarado-desenmascarado con propósitos de protección ante ciberataques de espionaje.

Palabras clave: Diseño de observadores y filtros no lineales, Filtrado y estimación para ataques FDI, Estabilidad entrada-estado, Estabilidad de sistemas no lineales, Métodos de Lyapunov

Masking protocol for fuel cell model based nonlinear observer

Abstract

In recent years, polymer electrolyte membrane fuel cells have become increasingly popular due to their high energy efficiency and zero operating emissions. One of the prominent applications for these devices is their inclusion in smart grids. In the control framework of these grids, one or more control layers are often implemented in cyberspace, which adds the risk of potential cyber-attacks. With this in mind, this paper considers the data protection problem, applied over the communication channel between a fuel cell and an observer. Specifically, a non-linear observer, based on passivity properties, is considered and a modular masking-unmasking mechanism is proposed for the purpose of protection against cyber espionage attacks.

Keywords: Nonlinear observers and filter design, Filtering and estimation for FDI, Input-to-State Stability, Stability of nonlinear systems, Lyapunov methods

1. Introducción

La generación de energía verde es un tema candente que ha desembocado en el desarrollo de una gran variedad de tecnologías innovadoras con el propósito de eliminar la dependencia de combustibles fósiles o actuar contra el cambio climático, entre otros, teniendo un impacto significativo en los mercados energéticos mundiales (Barroso et al., 2010). Las pilas de combustible de membrana electrolítica polimérica (PEMFC) son a día de hoy un medio comúnmente usado para esta tarea debido a sus ventajas como, entre otras, la producción continua e ininterrumpida de energía (Boudghene Stambouli and Traversa, 2002), o la capacidad de usar hidrógeno como combustible, el cual puede ser obtenido a partir de procesos energéticos renovables (Hosseini and Wahid, 2016). Estos dispositivos tienen aplicación, entre otras, en redes inteligentes o *smart-grids* (Li et al., 2019; Bernstein et al., 2013). En estas se pretende mantener una cierta tensión en una linea eléctrica (DC o AC) a través de un conjunto de unidades de generación distribuidas. Este re-

*Autor para correspondencia: pol.baldoma@upc.edu

quisito, requiere del desarrollo de sistemas de control. En concreto, para que estos sistemas de control puedan cumplir los requisitos de operación en tiempo real y escalabilidad, sus diseños suelen incluir una o varias capas tanto en el plano físico como en el cibernético (Dragičević et al., 2016). En concreto, las capas cibernéticas suelen implementarse sobre redes de telecomunicaciones, las cuales están expuestas a ciberataques (Thakur et al., 2016). Estos sistemas ciberfísicos de control forman parte de las infraestructuras críticas de grandes empresas y países, las cuales están con ello expuestas a los peligros de la red. Un famoso ejemplo es el del ciberataque realizado sobre la red eléctrica en Ucrania en 2016 mediante el *malware Black Energy* (Liang et al., 2017). Debido al creciente interés sobre los peligros de este tipo de eventos, varios marcos de trabajo para la identificación, prevención, detección y mitigación de estos han sido propuestos en la literatura desde la perspectiva de la teoría de control (Sánchez et al., 2019; Teixeira et al., 2015). Asimismo, se ha desarrollado en la última década las bases teóricas sobre los llamados sistemas de control en la nube (*Cloud Control Systems*) (Ison et al., 2020), sistemas dinámicos que incluyen tanto las características físicas como las propiedades de la red de comunicaciones donde se realizan las tareas de control, como el número de agentes en la red o los tiempos de retardo en la comunicación.

En paralelo, en la actualidad, muchos algoritmos de control para PEMFCs suelen requerir del conocimiento de variables relacionadas con el nivel de humedad en la membrana (Jiao and Li, 2011) para obtener el mayor rendimiento. Las limitaciones tecnológicas para la obtención de estas variables mediante sensado hacen de imperiosa necesidad el uso de algoritmos de estimación en línea de las variables internas de la pilas, entre los que se encuentran los observadores de estado (Cecilia et al., 2021). Como se ha comentado, el control de las PEMFC en ciertas aplicaciones requiere de la implementación de algoritmos sobre redes de comunicación, por lo que, además de buscar propiedades como la estabilidad y la convergencia del error en la estimación, también se busca la privacidad de los datos comunicados entre la planta y el observador. Los métodos actuales para proporcionar seguridad y confidencialidad en las señales transmitidas desde un punto de vista informático, como la encriptación bit a bit, pueden fallar en el sentido de demostrar, garantizar y conservar propiedades como la estabilidad, la pasividad y la robustez desde un punto de vista de la teoría de control. Por ello, en la última década, en el área de estudio de los sistemas de control en la red (*Networked Control Systems* (Gupta and Chow, 2008)) ha cobrado fuerza la rama conocida como Control Seguro, la cual trata de crear un marco común entre estos dos puntos de vista.

En este trabajo se presenta un ejemplo de aplicación de un método de enmascaramiento sobre el sistema de estimación de estados de una pila de hidrógeno PEMFC. En la literatura, existen varias estrategias de control que han sido aplicadas sobre las PEMFC (Daud et al., 2017), y entre los métodos para la estimación de estados, se han propuesto observadores adaptativos, de Luenberger o de Kalman extendido, entre otros (Schultze and Horn, 2016). En este trabajo se presenta una propuesta para la modificación de un observador no lineal para la estimación del agua líquida en el cátodo de la pila de combustible (Cecilia et al., 2024), el cual será modificado para poder prevenir un ataque de espionaje o *eavesdropping* y mantener la privacidad. Primero se expone el modelo de la pila usado como base para el observador (Sección 2); seguidamente se presenta el método de prevención frente a ciberataques de espionaje de datos, junto con las condiciones que debe cumplir el sistema (Secciones 4 y 5); finalmente se muestran los resultados de este en un entorno simulado (Sección 6).

2. Modelo de la pila de combustible

El modelo sobre el que se realiza este trabajo es el presentado en (Cecilia et al., 2024; Strahl et al., 2014), en nuestro caso sólo tomando la temperatura como única variable medida. Dicho modelo viene dado en la forma de espacio de estados

$$\begin{aligned} \dot{\mathbf{x}} &= \mathbf{f}(\mathbf{x}, \mathbf{u}), \\ y &= \mathbf{c}\mathbf{x} + v, \end{aligned} \tag{1}$$

con $\mathbf{x} := \begin{bmatrix} T_{fc} & s \end{bmatrix}^T$, $\mathbf{u} := \begin{bmatrix} I & v_{air} \end{bmatrix}^T$, $y = T_{fc}$ e v el ruido en el sensor, con $\mathbf{c} = \begin{bmatrix} 1 & 0 \end{bmatrix}$. Respecto a los estados del sistema, T_{fc} representa la temperatura en grados Kelvin, en el cátodo de la pila de combustible, mientras que s es la saturación de agua líquida en el cátodo. Las entradas al sistema son la corriente I, en Amperios, y la velocidad del aire que fluye por el cátodo v_{air}, en m/s. La salida medida del sistema es la misma temperatura en el cátodo T_{fc}, y v es el ruido añadido en el sensor de la salida. Asumimos que dicho ruido v en la medida es acotado, es decir, $|v| \leq \bar{v}$ para todo $t \geq 0$. La existencia de dicho valor $\bar{v}$ es necesario para poder diseñar el algoritmo, pero no necesitamos conocer su valor. En este modelo se asume que $\mathbf{x} \in \mathcal{X}$ y $\mathbf{u} \in \mathcal{U}$. Los conjuntos $\mathcal{X} \subset \mathbb{R}^2$ y $\mathcal{U} \subset \mathbb{R}^2$ son compactos, dicho de otra manera, los estados y las variables de control se asumen acotadas por todo $t \geq 0$. El campo vectorial $\mathbf{f}$ que rige la dinámica de los estados es

$$\mathbf{f}(\mathbf{x}, \mathbf{u}) := \begin{pmatrix} K_1 P_{el}(\mathbf{x}, I) + K_2(T_{amb} - T_{fc})v_{air} - K_{11} f_p(\mathbf{x}) \\ K_3 I - K_4 f_p(\mathbf{x}) + K_5 f_d(\mathbf{x}) \end{pmatrix}.$$

El valor T_{amb} hace referencia a la temperatura ambiente en el entorno de la pila, la cual consideramos como un parámetro constante. Los términos no lineales son ecuaciones semiempíricas que vienen dadas por

$$\begin{aligned} f_p(\mathbf{x}) &= \frac{s}{T_{fc}} \left(p^0 e^{\frac{-K_6}{T_{fc}}} - K_7 \right), \\ f_d(\mathbf{x}) &= s(-0{,}96 + 3{,}32s - 3{,}78s^2), \end{aligned}$$

siendo f_p el ratio de evaporación y f_d el ratio de difusión del agua (Cecilia et al., 2024). El factor P_{el} corresponde a la potencia térmica generada que se puede calcular mediante la siguiente expresión:

$$P_{el}(\mathbf{x}, I) = n_{cell}\left(K_8 T_{fc} ln\left(\frac{I}{A_{geo} j_0(\mathbf{x})} \right) + R_{ohm} I \right) I,$$

siendo

$$j_0(\mathbf{x}) = K_9 \left(1 - \sqrt[3]{\frac{s_{opt} - s}{s_{opt}}} \right) e^{\frac{-K_{10}}{T_{fc}} \left[1 - \frac{T_{fc}}{T_{ref}} \right]},$$

la densidad de corriente nominal en la pila, n_{cell} el número de celdas, R_{ohm} la resistencia óhmica de la pila, A_{geo} el área

geométrica de la membrana, T_{ref} es la temperatura de referencia para el cálculo del efecto de la saturación del agua en la densidad de corriente j_o, p_0 es la presión de referencia para el cálculo del factor de evaporación f_d y s_{opt} el contenido de agua líquida óptimo en la membrana. Los valores de los parámetros y de las constantes K_i usadas en este trabajo se pueden ver en la Tabla 1, mostrada en la sección de resultados.

3. Formulación del problema

3.1. Observadores en PEMFCs

El modelo de PEMFC en (1) contiene un estado medible (la temperatura T_{fc}) y un estado desconocido (el agua líquida s). En la práctica, es útil conocer el valor de s, ya que puede usarse para mejorar el rendimiento y evitar la degradación de las pilas de combustible en entornos con condiciones de trabajo fluctuantes, como en la automoción (Cecilia et al., 2021). Es por ello que existe una necesidad de estimar en tiempo real el valor de esta variable. En concreto, el problema de la estimación de estados para el sistema (1) consiste en diseñar un algoritmo que, a partir del conocimiento de los valores de entrada ($\mathbf{u}$) y de salida ($\mathbf{y}$) del sistema, estime los valores $\hat{\mathbf{x}}$ de los estados internos no medibles de este, de tal manera que se cumpla

$$\lim_{t\to\infty} |\mathbf{x} - \hat{\mathbf{x}}| \leq \epsilon \tag{2}$$

con una constante $\epsilon > 0$ dependiente del ruido en la medida y la incertidumbre del sistema. En este trabajo, asumimos que la estimación, $\hat{\mathbf{x}}$, es la solución que genera un observador. En concreto, el observador (potencialmente no lineal), que recibe como señal de entrada el error entre la salida de la planta y la salida estimada a partir de $\hat{\mathbf{x}}$, tiene la dinámica

$$\begin{aligned} \dot{\hat{\mathbf{x}}} &= \mathbf{f}_o(\hat{\mathbf{x}}, \mathbf{u}, z) = \mathbf{f}(\hat{\mathbf{x}}, \mathbf{u}) + \boldsymbol{\kappa}(\hat{\mathbf{x}}, z), \\ \hat{y} &= \mathbf{c}\hat{\mathbf{x}}, \\ z &= y - \hat{y}, \end{aligned} \tag{3}$$

donde $\boldsymbol{\kappa}(\hat{\mathbf{x}}, z)$ es el término de realimentación del observador, tal que se cumple $\mathbf{f}_o(\mathbf{x}, \mathbf{u}, 0) = \mathbf{f}(\mathbf{x}, \mathbf{u})$ para todo $(\mathbf{x}, \mathbf{u}) \in \mathbb{R}^2 \times \mathcal{U}$.

3.2. Topología de comunicación y objetivos

En este trabajo, asumimos que la señal medible $\mathbf{y}$ se transmite entre la planta y el observador a través de un canal de comunicación susceptible a ciberataques. En concreto, interfiriendo en el canal de comunicación, se encuentra un potencial *eavesdropper* (Sánchez et al., 2019), refiriendo a un agente que puede obtener los datos enviados a traves de dicho canal desde la planta hasta el observador. Haciendo uso de dichos datos, el atacante puede usarlos para la realización de ataques futuros. La topología de comunicación considerada en este trabajo es la mostrada en la Figura 1. Considerando esta topología, los objetivos de este trabajo son:

- Añadir un mecanismo de protección de privacidad de los datos en el canal de comunicación entre la planta y el observador, sin modificar el observador en si. Es decir, que un potencial *eavesdropper* no pueda reconstruir los estados $\mathbf{x}$ de la PEMFC (1), a partir de la señal transmitida a través del canal de comunicación.
- Que dicho mecanismo mantenga la propiedad de convergencia (2), es decir, que se pueda estimar el estado correctamente con dicho mecanismo incorporado.
- Que dicho mecanismo no requiera de la adición de un canal de comunicación adicional.

Nótese que sólo se ha representado el canal de comunicación de la salida en el esquema de la Figura 1. Si bien es cierto que el atacante, para poder realizar una estimación del estado necesitaría tanto de los valores de $\mathbf{u}$ como de los valores de $\mathbf{y}$ para la estimación del estado, sólo se ha considerado enmascarar el canal de salidas. Al necesitar de las dos señales ($\sqcap$ e y) para realizar la estimación, con que uno solo de estos este protegido, ya se impediría la correcta estimación. Por otro lado, consideramos que el canal de salidas es más propenso a recibir ataques de espionaje ya que posteriormente se podrían usar dichos datos obtenidos para realizar ataques tipo *Replay* (Sánchez et al., 2019, Sección 3.2). Además, también cabe considerar que la ley de control que genera los valores de $\mathbf{u}$ se encuentre implementado en el mismo nodo de red que el propio observador, por lo que no sería necesario considerar el canal. El mecanismo de protección está basado en la propuesta expuesta en (Cecilia et al., 2023b). La primera parte del mecanismo se basa en *enmascarar* la señal proveniente de la planta. Con este enmascaramiento, el espía no puede estimar el valor de los estados de la planta $\mathbf{x}$ aún disponiendo del valor de las entradas de control $\mathbf{u}$ y del modelo de la planta $\mathbf{f}(\mathbf{x}, \mathbf{u})$. La segunda parte del mecanismo de protección se basa en añadir un filtro en el observador que elimina el enmascaramiento. Aun siendo similar a un proceso de encriptación-desencriptación clásico, este sistema, al poder garantizar la propiedad de convergencia (2), no añade un retardo al sistema, cosa que no puede garantizar ninguna arquitectura de control típica en criptografía.

Cabe destacar que añadir un proceso de enmascaramiento y eliminación de máscara implica modificar la dinámica global del sistema. Cuando se trabaja con sistemas no lineales, no es sencillo mantener las propiedades del sistema original, bien sea estabilidad o pasividad, entre otras. Para garantizar la convergencia de toda la arquitectura este trabajo utiliza los resultados presentados en (Cecilia et al., 2023a). Las siguientes secciones están dedicadas a dar más detalles sobre este mecanismo de protección y sus garantías de convergencia.

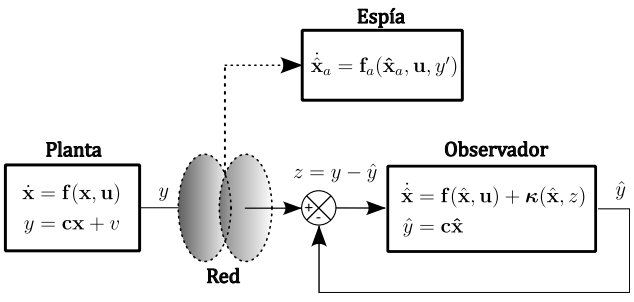

Figura 1: Esquema de comunicación entre la planta y el observador.

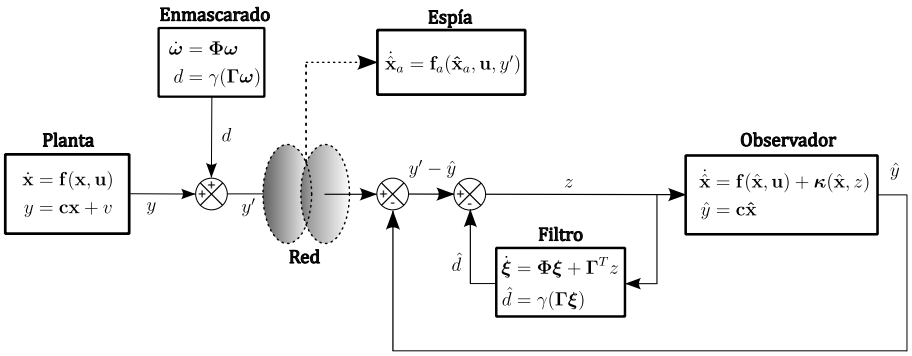

Figura 2: Esquema de comunicación entre la planta y el observador.

4. Enmascaramiento

La solución propuesta en (Cecilia et al., 2023b) comprende la adición de una señal de enmascarado $d \in \mathcal{D}$ a la señal de salida de la planta, con $\mathcal{D} \subset \mathbb{R}$ un conjunto acotado, y la incorporación de un filtro a la entrada del observador, que permite recuperar la señal original. Esta modificación, representada en la Figura 2, es independiente de la dinámica del observador y es modular, es decir, no se requiere una modificación de la dinámica original del observador. La señal de salida de la planta después de haber sido modificada es

$$y' = y + d, \tag{4}$$

donde d es la señal de enmascarado. Esta señal es generada por un sistema exógeno de la forma

$$\begin{aligned} \dot{\omega} &= \Phi\omega, \\ d &= \gamma(\Gamma\omega). \end{aligned} \tag{5}$$

Las matrices del sistema se definen

$$\begin{aligned} \Phi &= \mathbf{I}_{n_y} \otimes \mathbf{S}, \\ \mathbf{S} &= \text{diag}(\mathbf{S}_1, \mathbf{S}_2, ..., \mathbf{S}_N), \\ \mathbf{S}_i &= \begin{pmatrix} 0 & \omega_i \\ -\omega_i & 0 \end{pmatrix} \\ \omega_i &= \frac{2\pi}{T_i} \\ \Gamma &= \mathbf{I}_{n_y} \otimes \mathbf{G}, \\ \mathbf{G} &= \begin{pmatrix} \mathbf{g}_1 & \dots & \mathbf{g}_N \end{pmatrix}, \\ \mathbf{g}_i &= \begin{pmatrix} 1 & 0 \end{pmatrix}. \end{aligned}$$

con $\mathbf{I}_n$ matriz identidad de orden n, y $\otimes$ el producto de Kronecker. La señal generada se consigue mediante los estados internos $\boldsymbol{\omega} \in \mathbb{R}^{2N}$, los cuales son un conjunto de N diferentes osciladores con periodos T_i. Dichos periodos son inconmensurablemente reales entre si, es decir, para cualquier $i, j \in N$, T_i/T_j es irracional. Las N señales oscilatorias resultantes son sumadas entre si al realizar el producto matricial $\Gamma\omega$, resultando en un valor escalar. Finalmente, dicho resultado escalar es evaluado en una función (potencialmente no lineal y trascendental) $\gamma(r)$, la cual tiene una la propiedad de ser monotónica respecto a su argumento.

Suposición 4.1. *La función $\gamma(r) : \mathbb{R}^n \to \mathbb{R}^n$ es monotónica si cumple*

$$(a-b)^T(\gamma(a) - \gamma(b)) > (a-b)^T(a-b)$$

para todo a,b $\in \mathbb{R}^n$, $a \neq b$.

Nota 1. *En este protocolo se hace uso de una modificación aditiva de la señal. Dicha señal aditiva es el resultado de la suma de señales periódicas con periodos inconmensurables entre sí, resultando en una señal cuasiperiódica. Además, al pasar dicho resultado por la función γ trascendental, la señal d resultante presentaría un espectro de energía repartido, por lo que un simple filtrado de señal por un atacante no sería suficiente para eliminar el protocolo de seguridad. Sin embargo, si es cierto que, si la relación entre el espectro de la salida de la planta y el de la señal de enmascarado es muy grande, un filtro paso bajo podría servir para filtrar gran parte de este último. O también podría resultar en el uso de un filtro paso banda dadas ciertas condiciones. Para esos casos, un enmascaramiento multiplicativo si sería una mejor alternativa, pero queda fuera del marco de este trabajo.*

Con el propósito de desenmascarar la señal enviada desde la planta, se incorpora un filtro a la entrada del observador que extrae la señal de enmascarado al error de estimación que realimenta al observador (Cecilia et al., 2023a). Este filtro se realimenta con esta misma señal filtrada, y su objetivo es estimar la propia señal de enmascarado. Dicho filtro se define como

$$\begin{aligned} \dot{\boldsymbol{\xi}} &= \Phi\boldsymbol{\xi} + \Gamma^T z \\ \hat{d} &= \gamma(\Gamma\boldsymbol{\xi}) \\ z &= y' - \hat{y} - \hat{d} \end{aligned} \tag{6}$$

con las matrices Φ, Γ, y la función γ iguales que en (5). La señal z es la introducida a la entrada del observador (3) después de pasar por el filtro, tal como se muestra en la Figura 2. Dadas estas descripciones, en la siguiente sección se expondrán las condiciones necesarias para que el observador sobre el que se trabaje pueda mantener la condición (2) al agregar en el esquema de control los sistemas (5) y (6).

5. Convergencia del observador extendido

En esta sección se presenta el observador usado para el sistema formado por (1),(5), (3) y (6), y se demuestra que este

puede filtrar (rechazar) la señal d generada para el enmascaramiento. Esto es equivalente a que el sistema completo sea incrementalmente estable entrada-estado (δ-ISS) respecto a la señal v, tal como se expone en la Definición 1 de (Cecilia et al., 2023a), o en (Angeli, 2002). La propiedad de δ-ISS exponencial implica que existe una función $\rho(s)$ de clase $\mathcal{K}$ y dos constantes $\alpha, \beta > 0$ tal que, para cualquier pareja de soluciones $\boldsymbol{\eta}(t)$, $\boldsymbol{\eta}'(t)$ del sistema formado por (3) y (6), se cumpla

$$\left|\hat{\boldsymbol{\eta}}(t) - \hat{\boldsymbol{\eta}}'(t)\right| \leq \alpha e^{-\beta t}\left|\hat{\boldsymbol{\eta}}(0) - \hat{\boldsymbol{\eta}}'(0)\right| + \sup_{r\in[0,t)} \rho\left(\left|v(r) - v'(r)\right|\right) \tag{7}$$

con $\hat{\boldsymbol{\eta}}(t) = (\hat{\mathbf{x}}(t), \boldsymbol{\xi}(t))$ y $\hat{\boldsymbol{\eta}}'(t) = (\hat{\mathbf{x}}'(t), \boldsymbol{\xi}'(t))$. Basándonos en el marco propuesto en Cecilia et al. (2023a), se puede demostrar que el sistema (3), (6) es δ-ISS y, además, que los estados de (1) evolucionaran en un conjunto compacto $\mathcal{X} \subset \mathbb{R}^2$ para cualquier entrada $\mathbf{u} \in \mathcal{U}$ si se cumplen las condiciones:

- El observador (3) es incrementalmente pasivo (Pavlov and Marconi, 2008) y diferencialmente detectable (Tsinias, 1989).
- El sistema extendido formado por (1) y (5) es diferencialmente detectable.

Una condición suficiente para la propiedad 1 es la siguiente. Existen dos matrices simétricas y definidas positivas $\mathbf{P}$, $\overline{\mathbf{P}}$ y dos constantes q, $l > 0$ tal que se cumpla

$$\mathbf{P}\frac{\partial \mathbf{f}}{\partial \mathbf{x}}(\mathbf{x},\mathbf{u}) + \frac{\partial \mathbf{f}}{\partial \mathbf{x}}(\mathbf{x},\mathbf{u})^T\mathbf{P} \leq 0 \tag{8}$$

$$\overline{\mathbf{P}}\frac{\partial \mathbf{f}}{\partial \mathbf{x}}(\mathbf{x},\mathbf{u}) + \frac{\partial \mathbf{f}}{\partial \mathbf{x}}(\mathbf{x},\mathbf{u})^T\overline{\mathbf{P}} - l\mathbf{c}^T\mathbf{c} \leq -q\overline{\mathbf{P}} \tag{9}$$

para todo $(\mathbf{x},\mathbf{u}) \in \mathcal{X}\times\mathcal{U}$. Cabe remarcar que, dada la matriz $\mathbf{P}$, se puede diseñar un observador con la dinámica

$$\dot{\hat{\mathbf{x}}} = \mathbf{f}_o(\hat{\mathbf{x}},\mathbf{u},y) = \mathbf{f}(\hat{\mathbf{x}},\mathbf{u}) + \kappa\mathbf{P}^{-1}\mathbf{c}^T(y - \mathbf{c}\hat{\mathbf{x}}) \tag{10}$$

tal que

$$\lim_{t\to\infty}\left|\mathbf{x}(t) - \hat{\mathbf{x}}(t)\right| \leq \epsilon, \tag{11}$$

con $\epsilon > 0$. La condición (8) por si sola implica la propiedad de disipatividad incremental de la planta, mientras que la ganancia impuesta en el observador (10) garantiza pasividad incremental en el observador (10) (con entrada $\mathbf{c}\hat{\mathbf{x}} - y$ y salida $\hat{y}$). La condición (9) implica la detectabilidad diferencial del sistema (1). La combinación de la condición de pasividad con detectabilidad incremental es suficiente para demostrar la convergencia (11). Por otro lado, la detectabilidad diferencial del sistema extendido (1), (5), se puede demostrar a partir de la existencia de una matriz simétrica y definida positiva $\mathbf{Q}$ y de dos constantes μ, $p > 0$ tal que

$$\mathbf{Q}\frac{\partial \mathbf{f_e}}{\partial \boldsymbol{\eta}}(\boldsymbol{\eta},\mathbf{u}) + \frac{\partial \mathbf{f_e}}{\partial \boldsymbol{\eta}}(\boldsymbol{\eta},\mathbf{u})^T\mathbf{Q} - \mu\mathbf{H_e}^T\mathbf{H_e} \leq -p\mathbf{Q} \tag{12}$$

para todo $\boldsymbol{\eta} \in \mathcal{X}\times\mathbb{R}^{2N}$ y todo $\mathbf{u} \in \mathcal{U}$, siendo el sistema ampliado

$$\dot{\boldsymbol{\eta}} = \mathbf{f_e}(\boldsymbol{\eta},\mathbf{u}) = \begin{bmatrix}\mathbf{f}(\mathbf{x},\mathbf{u}) \\ \boldsymbol{\Phi}\boldsymbol{\omega}\end{bmatrix},$$

$$\boldsymbol{\zeta} = \mathbf{H_e}\boldsymbol{\eta} = \begin{bmatrix}\mathbf{C} & \boldsymbol{\Gamma}^T\end{bmatrix}\boldsymbol{\eta},$$

$$\boldsymbol{\eta} = \begin{bmatrix}\mathbf{x} \\ \boldsymbol{\omega}\end{bmatrix},$$

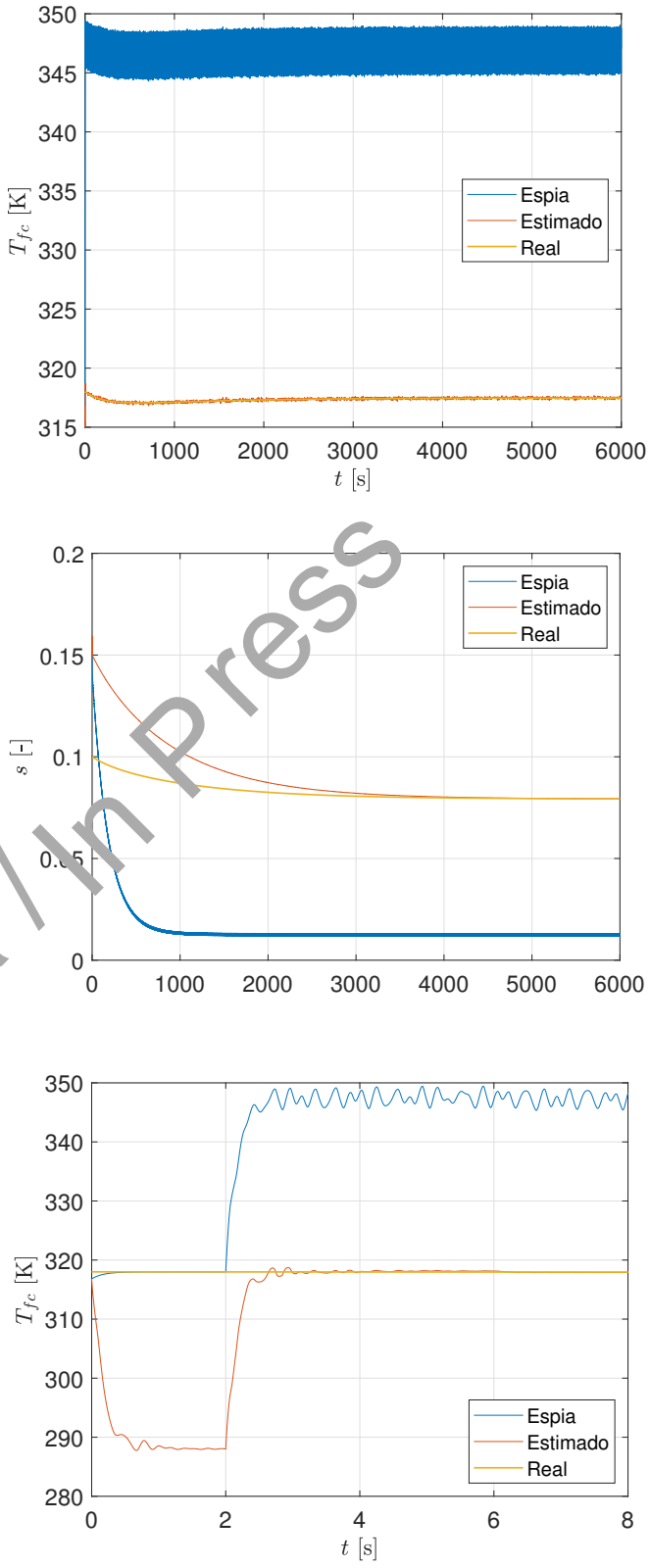

Figura 3: Estimación de la temperatura (a) y de la saturación del agua (b) , y efecto del tiempo de transmisión en la estimación.

el formado por la planta y por el generador de enmascarado. Con estas condiciones, en base al Teorema 2 de (Cecilia et al., 2023a), se garantiza la propiedad de δ-ISS para (1),(5), (3) y (6). Dicho teorema será enunciado a continuación.

Teorema 5.1. *Considerese el sistema formado por la planta* (1)*, el enmascaramiento* (5)*, y el observador ampliado* (3) , (6)*. Si existen matrices simétricas y definidas positivas* $\mathbf{P}$*,* $\overline{\mathbf{P}}$*,* $\mathbf{Q}$ *y constantes positivas l, q,* μ*, p que cumplan* (8)*,* (9) *y* (12)*, entonces, el observador ampliado es exponencialmente δ-ISS respecto a v*(*t*) *y, además, existe un conjunto* $X_0 \subset \mathbb{R}^2$ *tal que cualquier solución* $\mathbf{x}(t)$ *de* (1) *se mantendrá en dicho conjunto para cualquier* $\mathbf{u} \in \mathcal{U}$ *y para todo* $t \geq 0$*.*

En la siguiente sección se mostrará un caso de aplicación de la base teórica expuesta en un entorno simulado.

6. Resultados numéricos

En esta sección se presentan los resultados obtenidos al realizar simulaciones del algoritmo de estimación con enmascarado sobre un modelo de PEMFC. Se ha trabajado con el modelo (1) presentado en la Sección 2. Se ha considerado que, para todo $t \in [0, 6000]$, las señales de control con valores constantes $\mathbf{u} = \mathbf{u}^* = \begin{bmatrix}3{,}95 & 0{,}21\end{bmatrix}^T$, y las constantes para el sistema sistema (1) definidas en la Tabla 1. El observador diseñado para estimar los estados de (1) con la forma (3) tiene el termino de corrección de error

$$\boldsymbol{\kappa}(z, \hat{\mathbf{x}}) = \mathbf{l}(z - \mathbf{c}\hat{\mathbf{x}}),$$

con $\mathbf{l} = \begin{bmatrix}5{,}9908 & -0{,}0019\end{bmatrix}^T$. Esta ganancia del observador ha sido escogida de manera que se cumplan la condición (8). Aún que la idea de este mecanismo es que pueda ser implementado sobre observadores previamente diseñados, en este ejemplo usamos una matriz $\mathbf{l}$ precalculada de manera que podamos asegurar que nuestro observador es pasivo y se cumpla (11). El sistema de enmascaramiento se ha diseñado con $N = 3$ señales generadoras, sean $\omega_i = 20\sqrt{i}$ para $i = 1, 2, 3$. Con esto, las matrices

$$\boldsymbol{\Phi} = \begin{bmatrix} 0 & 20 & 0 & 0 & 0 & 0 \\ -20 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 20\sqrt{2} & 0 & 0 \\ 0 & 0 & -20\sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 20\sqrt{3} \\ 0 & 0 & 0 & 0 & -20\sqrt{3} & 0 \end{bmatrix},$$

$$\boldsymbol{\Gamma} = \begin{bmatrix}1 & 0 & 1 & 0 & 1 & 0\end{bmatrix}$$

componen el generador de enmascarado con forma (5) y el filtro de entrada del observador con forma (6). La función monotónica usada para la generación de $\mathbf{d}$ es

$$\gamma(r) = a + b \arctan\left(\frac{r^3}{3} - \frac{r^2}{2} + r\right)$$

con $a = 30$ y $b = 5$. Con el objetivo de comprobar el cumplimiento de las condiciones de este sistema planta-observador, se pueden plantear una serie de problemas de desigualdades matriciales lineales (LMIs). Al ser la matriz $\frac{\partial \mathbf{f}}{\partial \mathbf{x}}$ dependiente de $\mathbf{x}$, se nos plantean un conjunto de infinitas LMI. El método usado para resolver estas restricciones LMI es el planteado en Boyd et al. (1994), y se puede ver un uso práctico en Cecilia et al. (2023a). Este se basa en analizar las LMIs para un cierto conjunto de matrices $A_n = \frac{\partial \mathbf{f}}{\partial \mathbf{x}}(\mathbf{x}_n)$, es decir, la Jacobiana de $\mathbf{f}$ evaluada en un cierto conjunto de puntos. Concretamente, tomando como valores $\mathbf{x}_n$ los que forman los vértices mínimo y máximo de los valores de $\mathbf{x}$ sobre los que se estudia el cumplimiento de la condición. En nuestro caso, teniendo nuestro estado definido como

$$\mathbf{x} = \begin{bmatrix} T_{fc} \\ s \end{bmatrix}$$

y queriendo resolver la primera desigualdad de (8) para todo $\mathbf{x}$ en $\mathcal{X} = \{\mathbf{x} \mid T_{fc} \in [T_{min}, T_{max}], s \in [s_{min}, s_{opt})\}$, resolveremos el conjunto de desigualdades

$$\mathbf{P}\frac{\partial \mathbf{f}}{\partial \mathbf{x}}(T_{min}, s_{min}, \mathbf{u}^*) + \frac{\partial \mathbf{f}}{\partial \mathbf{x}}^T(T_{min}, s_{min}, \mathbf{u}^*)\mathbf{P} \leq 0,$$
$$\mathbf{P}\frac{\partial \mathbf{f}}{\partial \mathbf{x}}(T_{max}, s_{min}, \mathbf{u}^*) + \frac{\partial \mathbf{f}}{\partial \mathbf{x}}^T(T_{max}, s_{min}, \mathbf{u}^*)\mathbf{P} \leq 0,$$
$$\mathbf{P}\frac{\partial \mathbf{f}}{\partial \mathbf{x}}(T_{min}, s_{opt}, \mathbf{u}^*) + \frac{\partial \mathbf{f}}{\partial \mathbf{x}}^T(T_{min}, s_{opt}, \mathbf{u}^*)\mathbf{P} \leq 0,$$
$$\mathbf{P}\frac{\partial \mathbf{f}}{\partial \mathbf{x}}(T_{max}, s_{opt}, \mathbf{u}^*) + \frac{\partial \mathbf{f}}{\partial \mathbf{x}}^T(T_{max}, s_{opt}, \mathbf{u}^*)\mathbf{P} \leq 0.$$

Si se cumplen todas las desigualdades, entonces se cumple la primera LMI de (8). El mismo método es aplicado para las demás LMIs. Para comprobar las condición de pasividad, podemos imponer la desigualdad (8) junto con la condición de igualdad

$$\mathbf{Pl} = \kappa \mathbf{c}^T \tag{13}$$

con lo que obtenemos una matriz

$$\mathbf{P} = 10^3 \cdot \begin{bmatrix}0{,}0002 & 0{,}0005 \\ 0{,}0005 & 1{,}6189\end{bmatrix}$$

y una constante $\kappa = 1$ que es solución del problema. Por otro lado, planteando un problema con (9), e imponiendo un valor a $q = 0{,}01$, obtenemos una matriz

$$\overline{\mathbf{P}} = \begin{bmatrix}0{,}1389 & 0{,}2683 \\ 0{,}2683 & 1{,}3599\end{bmatrix}$$

y la constante

$$l = 1{,}3178,$$

de tal manera que se cumple la condición de detectabilidad de (1). Finalmente, la matriz $\mathbf{Q}$ y las constantes μ y p que demuestran (12) para el sistema completo (1), (5), se puede calcular

usando el mismo método, dando las soluciones

$$\mathbf{Q} = \begin{bmatrix} \mathbf{Q_1} & 0 \\ 0 & \mathbf{Q_2} \end{bmatrix},$$
$$\mu = 0{,}9134,$$
$$p = 0{,}0255,$$
$$\mathbf{Q_1} = \begin{bmatrix} 0{,}3105 & 0{,}3715 \\ 0{,}3715 & 1{,}4942 \end{bmatrix},$$
$$\mathbf{Q_2} = \begin{bmatrix} \mathbf{Q_{21}} & \mathbf{Q_{22}} \end{bmatrix},$$
$$\mathbf{Q_{21}} = \begin{bmatrix} 1{,}0165 & -0{,}0228 & 0 \\ -0{,}0228 & 1{,}0165 & 0{,}0910 \\ 0 & 0{,}0910 & 1{,}0320 \\ -0{,}1288 & 0 & -0{,}0161 \\ 0 & 0{,}0456 & 0 \\ -0{,}0790 & 0 & -0{,}1575 \end{bmatrix},$$
$$\mathbf{Q_{22}} = \begin{bmatrix} -0{,}1288 & 0 & -0{,}0790 \\ 0 & 0{,}0456 & 0 \\ -0{,}0161 & 0 & -0{,}1575 \\ 1{,}0320 & 0{,}1285 & 0 \\ 0{,}1285 & 1{,}0239 & -0{,}0132 \\ 0 & -0{,}0132 & 1{,}0239 \end{bmatrix}.$$

Se ha considerado un ruido blanco añadido a la salida de la planta, con el proposito de recrear el ruido en el sensado de la temperatura. Según (Cecilia et al., 2023b), el error en la estimación será sólo dependiente de manera monotónica del ruido no modelado, tal y como se puede ver en los resultados en la Figura 3. También se ha añadido un retardo de 2s en el canal de comunicación de las medidas de salida entre planta y observador, representando un posible retraso inducido por la transmisión de la señal por la red de comunicación, aunque en este caso se consideraria un caso muy particular siendo dicho retardo muy grande. El espía, suponiendo que tiene una política de ataque en la que dispone del valor de las entradas, las salidas, y un modelo exacto del observador, no puede realizar una buena estimación debido al desconocimiento del modelo de enmascarado, mientras que la arquitectura propuesta es capaz de estimar todos los estados del sistema. Este resultado valida la eficacia del mecanismo incluso en frente de ruido en el sensor y retardos en la comunicación.

7. Conclusiones

La señal de enmascarado cumple la función de incapacitar al espía de obtener el valor de los estados aún disponiendo de los valores de control y de salida y del modelo de la planta. Hay que tener en cuenta que en este caso el observador ha sido diseñado de base para cumplir las condiciones necesarias para agregar el enmascarado y su respectivo filtro al sistema. En caso de tener un observador ya dado, sería necesario demostrar, la pasividad de este y disipatividad diferencial del modelo de la planta, pues las demás condiciones no dependerán en si de como haya sido diseñado el observador. Se remarca también que el error en la estimación está acotado por la perturbación agregada en el momento del sensado.

El mecanismo de protección utilizado en el canal observador se basa en la pasividad de los diferentes bloques del lazo de control, independientemente de las características de la señal enviada, por lo que sería posible utilizar el mismo método en el canal de la señal de control. La señal de error del filtro situado a la entrada del observador puede ser usada para la detección de posibles ataques de inyección de datos falsos por parte de un ciber-atacante, ya que dicho filtro comparte el mismo esquema de varios detectores de fallos o de ciberataques mostrados en la literatura reciente. Sin embargo, se ha considerado que para llevar a cabo un análisis de la efectividad de dicho mecanismo de detección, se requeriría antes de el trabajo previo de caracterizar qué tipos de ataques sería capaz de detectar y en qué condiciones, trabajo que está fuera de los objetivos principales del trabajo. También es de remarcar que este trabajo, el cual pretende aplicarse sobre sistemas de control en la red, no ha tomado en cuenta efectos como la cuantización de la señal transmitida, el retardo temporal inducido por la red ni los efectos causados del protocolo de comunicación en esta, pues aquí solo se aborda el problema del control seguro.

En trabajos futuros se estudiarán los efectos del canal de comunicación (retardo, cuantificación, etc.) sobre la estabilidad y convergencia que pretende mantener el enmascaramiento, así como la actuación de este en un canal de comunicación de una señal de control en lazo cerrado. Asimismo, también el poder corroborar estos resultados en simulación con pruebas experimentales con modelos de pilas de combustible reales, con el uso del enmascaramiento y realizando un ataque de interceptación de datos.

Tabla 1: Valores de los parámetros del sistema (1).

Constante	Valor	Unidades
K_1	0.0025	$K \cdot J^{-1}$
K_2	0.0153	m^{-1}
K_3	2.37e-5	C^{-1}
K_4	5.33e-5	$K \cdot m^3 \cdot s^{-1} \cdot J^{-1}$
K_5	1.218e-4	$m^3 \cdot s^{-1}$
K_6	5210	K
K_7	2380	atm
K_8	3.59e-5	$J \cdot C \cdot mol^{-1}$
K_9	0.001	$A \cdot m^{-2}$
K_{10}	8419	K
K_{11}	0.0059	$Pa^{-1} \cdot s^{-1}$
p_0	1.196e11	Pa
A_{geo}	0.00225	m^2
s_{opt}	0.196	–
R_{ohm}	0.05	Ω
T_{amb}	298	K
T_{ref}	298	K
n_{cell}	20	–

Agradecimientos

Esta iniciativa se realiza en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (*Next Generation*). Este trabajo forma parte del proyecto MAFALDA (PID2021-126001OB-C31) financiado por MCIN/ AEI /10.13039/501100011033 y por «*ERDF A way of making Europe*». Este trabajo forma parte del proyecto MASHED (TED2021-129927B-I00), financiado por MCIN/ AEI/10.13039/501100011033 y por la Unión Europea *Next GenerationEU/PRTR*.

Referencias

Angeli, D., 2002. A lyapunov approach to incremental stability properties. IEEE Transactions on Automatic Control 47 (3), 410–421.

Barroso, L. A., Rudnick, H., Sensfuss, F., Linares, P., 2010. The green effect. IEEE Power and Energy Magazine 8 (5), 22–35.

Bernstein, P. A., Heuer, M., Wenske, M., 2013. Fuel cell system as a part of the smart grid. In: 2013 IEEE Grenoble Conference. pp. 1–4.

Boudghene Stambouli, A., Traversa, E., 2002. Fuel cells, an alternative to standard sources of energy. Renewable and Sustainable Energy Reviews 6 (3), 295–304.

Boyd, S., El Ghaoui, L., Feron, E., Balakrishnan, V., 1994. Linear matrix inequalities in system and control theory. SIAM.

Cecilia, A., Astolfi, D., Bin, M., Costa-Castelló, R., 2023a. Cancelling output disturbances in observer design through internal model filters. Automatica.

Cecilia, A., Astolfi, D., Casadei, G., Costa-Castelló, R., Nešić, D., 2023b. A masking protocol for private communication and attack detection in nonlinear observers. 62nd IEEE Conference on Decision and Control.

Cecilia, A., Astolfi, D., Costa-Castelló, R., 2024. A new nonlinear observer for liquid water estimation in fuel cells. IEEE Transactions on Control Systems Technology 32 (3), 990–1001.

Cecilia, A., Serra, M., Costa-Castelló, R., 2021. Nonlinear adaptive observation of the liquid water saturation in polymer electrolyte membrane fuel cells. Journal of Power Sources 492, 229641.

Daud, W., Rosli, R., Majlan, E., Hamid, S., Mohamed, R., Husaini, T., 2017. Pem fuel cell system control: A review. Renewable Energy 113, 620–638.

Dragičević, T., Lu, X., Vasquez, J. C., Guerrero, J. M., 2016. Dc microgrids—part i: A review of control strategies and stabilization techniques. IEEE Transactions on Power Electronics 31 (7), 4876–4891.

Gupta, R. A., Chow, M.-Y., 2008. Networked control systems: Theory and Applications. Springer-Verlag London.

Hosseini, S. E., Wahid, M. A., 2016. Hydrogen production from renewable and sustainable energy resources: Promising green energy carrier for clean development. Renewable and Sustainable Energy Reviews 57, 850–866.

Ison, S., Budd, L., Mahmoud, M. S., Xia, Y., 2020. Cloud Control Systems: Analysis, Design and Estimation. Emerging Methodologies and Applications in Modelling. Academic Press.

Jiao, K., Li, X., 2011. Water transport in polymer electrolyte membrane fuel cells. Progress in Energy and Combustion Science 37 (3), 221–291.

Li, Z., Zheng, Z., Xu, L., Lu, X., 10 2019. A review of the applications of fuel cells in microgrids: opportunities and challenges. BMC Energy 1 (1), 8.

Liang, G., Weller, S. R., Zhao, J., Luo, F., Dong, Z. Y., 2017. The 2015 ukraine blackout: Implications for false data injection attacks. IEEE Transactions on Power Systems 32 (4), 3317–3318.

Pavlov, A., Marconi, L., 2008. Incremental passivity and output regulation. Systems & Control Letters 57 (5), 400–409.

Schultze, M., Horn, J., 2016. Modeling, state estimation and nonlinear model predictive control of cathode exhaust gas mass flow for pem fuel cells. Control Engineering Practice 49, 76–86.

Strahl, S., Husar, A., Puleston, P., Riera, J., 2014. Performance improvement by temperature control of an open-cathode pem fuel cell system. Fuel Cells 14 (3), 466–478.

Sánchez, H. S., Rotondo, D., Escobet, T., Puig, V., Quevedo, J., 2019. Bibliographical review on cyber attacks from a control oriented perspective. Annual Reviews in Control 48, 103–128.

Teixeira, A., Shames, I., Sandberg, H., Johansson, K. H., 2015. A secure control framework for resource-limited adversaries. Automatica 51, 135–148.

Thakur, K., Ali, M. L., Jiang, N., Qiu, M., 2016. Impact of cyber-attacks on critical infrastructure. In: 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS). pp. 183–186.

Tsinias, J., 1989. Observer design for nonlinear systems. Systems & Control Letters 13 (2), 135–142.