CEA Comité Español de Automática
XLVII JORNADAS DE AUTOMÁTICA CÓRDOBA 2026
UNIVERSIDADE DA CORUÑA

Jornadas de Automática

Mitigación de ciberataques de descarte de paquetes en sistemas de control en red con muestreo por cruce de umbrales

Julio-Ariel Romero-Pérez[1,*], Oscar Miguel-Escrig[1]

[1]*Departamento de Ingeniería de Sistemas Industriales y Diseño, Universitat Jaume I, Av. Vicent Sos Baynat, s/n 12071 Castelló de la Plana, España.*

To cite this article: Romero-Pérez, J-A, Miguel-Escrig, O. 2026. Mitigation of Packet-Dropping Cyberattacks in Networked Control Systems with Threshold-Crossing Sampling. Jornadas de Automática, 47. https://doi.org/10.17979/ja-cea.2026.47.13832

Resumen

Este artículo presenta un método de mitigación contra ciberataques de descarte de paquetes en sistemas de control en red que emplean el envío de medidas mediante cruce de umbrales. La propuesta se basa en el ajuste de la amplitud de dichos umbrales para preservar las prestaciones del lazo de control en cuanto al error en estado estable, manteniendo este dentro de las especificaciones de diseño, conservando al mismo tiempo los márgenes de robustez ante la aparición de ciclos límite inducidos por esta estrategia de envío de datos.

Palabras clave: Sistemas de control en red, Control basado en eventos, Sistemas de control en red seguros, Diseño de sistemas tolerantes a fallos/fiables, FDI y FTC para sistemas en red.

Mitigation of Packet-Dropping Cyberattacks in Networked Control Systems with Threshold-Crossing Sampling

Abstract

This article presents a mitigation method against packet-dropping cyberattacks in networked control systems that employ the transmission of measurements via threshold crossing. The proposal is based on adjusting the amplitude of said thresholds to preserve control loop performance in terms of steady-state error, keeping it within design specifications, while simultaneously conserving robustness margins against the appearance of limit cycles induced by this data transmission strategy.

Keywords: Control over networks, Event-based control, Secure networked control systems, Design of fault tolerant/reliable systems, FDI and FTC for networked systems.

1. Introducción

La creciente digitalización de los entornos industriales ha impulsado el despliegue de sistemas de control distribuidos (DCS), sistemas ciberfísicos (CPS) y sistemas de control en red (NCS), donde sensores, actuadores y controladores intercambian información mediante redes de comunicaciones. Aunque estas arquitecturas aportan ventajas en términos de flexibilidad, supervisión y eficiencia, también introducen nuevas vulnerabilidades de ciberseguridad que pueden comprometer directamente el comportamiento físico del proceso controlado.

A diferencia de los sistemas informáticos tradicionales, los ciberataques sobre sistemas industriales pueden afectar no solo a la información intercambiada, sino también a la estabilidad, seguridad y funcionamiento de la planta. Entre las amenazas más relevantes destacan los ataques de denegación de servicio (DoS), la inyección de datos falsos, los ataques de repetición, los ataques Man-in-the-Middle y los ataques stealthy, todos ellos capaces de comprometer la disponibilidad, integridad o consistencia temporal de las señales intercambiadas entre sensores y controladores.

Tradicionalmente, estos sistemas utilizan esquemas de transmisión periódica, en los que los sensores envían información a intervalos temporales fijos independientemente de

*Autor para correspondencia: romeroj@uji.es

la evolución real del proceso. Sin embargo, este enfoque genera tráfico redundante y patrones de comunicación altamente predecibles, lo que puede facilitar ataques de interceptación, saturación de red o manipulación sistemática de datos.

En este contexto, las estrategias de transmisión basadas en eventos han surgido como alternativas prometedoras al envío periódico convencional. En estos esquemas, los sensores transmiten información únicamente cuando el estado del sistema cambia de forma significativa desde el punto de vista del control, lo que reduce el volumen de comunicaciones y rompe la predictibilidad temporal del tráfico de red (Tabuada, 2007). Además de mejorar la eficiencia en el uso de recursos, esta menor predictibilidad aporta ventajas desde la perspectiva de la ciberseguridad, al reducir la superficie de ataque y reforzar la relación entre los datos transmitidos y la dinámica física del sistema.

Motivado por estas consideraciones, este trabajo analiza, desde una perspectiva de ciberseguridad, las ventajas e inconvenientes del esquema de muestreo y transmisión de datos basado en el cruce de umbrales en comparación con el muestreo periódico convencional utilizado en los sistemas de control en red. En la estrategia por cruce de niveles, los datos se transmiten únicamente cuando la variable medida atraviesa ciertos límites predefinidos. En particular, se estudia el comportamiento de este enfoque frente a ataques de denegación de servicio (DoS) y de descarte de paquetes (packet-dropping). Para este último escenario, se propone un mecanismo de mitigación con el objetivo de mantener el error en estado estable dentro de los requerimientos de diseño, garantizando asimismo la robustez ante los ciclos límite inducidos por dicho esquema de muestreo.

2. Control en red con envío por SSOD

La Figura 1 muestra el esquema de un sistema de control en red con una unidad de control físicamente próxima al actuador y una unidad sensora remota, cuyas mediciones se envían a través de una red de comunicaciones digitales según la estrategia Symmetric-Send-on-Delta (SSOD). El retardo variable propio de la red de comunicaciones se modela mediante el término $e^{-T_n s}$, que modela el peor caso de este retardo variable.

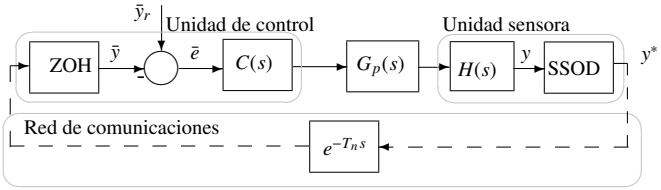


Figura 1: Sistema de control en red con muestreo SSOD.

La característica de entrada/salida del bloque SSOD se muestra en la Figura 2, donde se puede ver que el envío de un nuevo dato se realiza cada vez que se cruza un umbral definido por $n\delta$, $n \in \mathbf{Z}$ y $\delta \in \mathbf{R}^+$, con una histéresis δ. El bloque ZOH en la unidad de control mantiene el valor del último dato hasta que un nuevo dato es recibido.

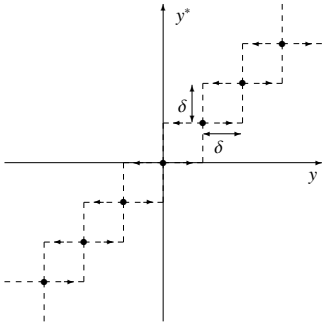


Figura 2: Estrategia de envío SSOD.

Dado que $\bar{y} = n\delta$, los valores de la referencia $\bar{y}_r$ también se fijan como múltiplos enteros de δ, de modo que, en estado estacionario, el error $\bar{e}$ pueda anularse. De lo contrario, siempre existiría un error distinto de cero que, a la postre, provocaría oscilaciones si el controlador $C(s)$ contiene algún término integral. Bajo esta consideración, este sistema de control en red de la Figura 1 es equivalente al mostrado en la Figura 3, siendo $G(s) = G_p(s)H(s)$.

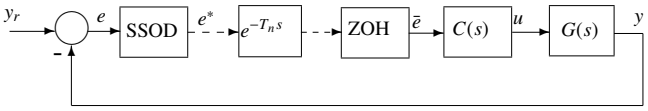


Figura 3: Sistema equivalente al de la Figura 1.

El ajuste de controladores $C(s)$ de tipo PID para el sistema con muestreo basado en SSOD mostrado en la Figura 3 ha sido ampliamente estudiado en la literatura; véanse, por ejemplo, (Beschi et al., 2012; Romero Pérez and Sanchis Llopis, 2016; Romero-Pérez and Miguel-Escrig, 2024). En estos estudios se ha demostrado que la incorporación del muestreo SSOD puede inducir oscilaciones de ciclo límite. Aunque estas pueden resultar útiles desde el punto de vista de la identificación, no son deseables desde la perspectiva del control, ya que pueden producir desgaste y deterioro en el actuador y oscilaciones innecesarias en la variable controlada.

Observación 1. *La existencia de ciclos límite inducidos por SSOD está determinada por el ajuste del controlador $C(s)$, que puede diseñarse para garantizar determinados márgenes de robustez y evitar así dichas oscilaciones. Asimismo, el muestreador SSOD y, más concretamente, su parámetro δ no influye en dichos márgenes, que quedan completamente definidos por el ajuste de $C(s)$. La influencia de δ se manifiesta, en cambio, en el error en estado estacionario, en los incrementos de la acción de control y en el número de eventos generados.*

3. Robustez de control por cruce de umbrales ante ciberataques

El paradigma de transmisión basado en umbrales presenta un comportamiento desigual ante diferentes tipos de ataques: proporciona tolerancia ante ataques de Denegación de Servicio (DoS) por saturación, pero manifiesta vulnerabilidad a ataques de descarte de paquetes (*packet dropping*) (Dolk et al., 2016; Zhao et al., 2021; Dolk and Heemels, 2017).

Frente a ataques DoS por saturación de canal, cuyo objetivo es la inyección masiva de tráfico espurio para inducir retardos por saturación de la red, el esquema por umbrales optimiza el uso de esta. Al restringir las transmisiones a los instantes en que la variable de proceso cruza los umbrales predefinidos por δ, se reduce la tasa media de utilización del canal. Esta naturaleza esporádica preserva un ancho de banda remanente que absorbe la congestión parcial, requiriendo que el atacante inyecte un volumen de tráfico significativamente superior para causar la misma degradación que en un esquema periódico.

Asimismo, la ausencia de mensajes posee un valor semántico en este esquema; mientras que en el muestreo periódico la pérdida de un paquete rompe la secuencia temporal síncrona y desactualiza inmediatamente la señal de control, en el esquema por umbrales el silencio indica que la variable medida permanece acotada dentro del espacio definido por el umbral. Esto permite al controlador retener y operar con el último valor recibido durante intervalos de indisponibilidad temporal, sin requerir actualizaciones recurrentes para mantener la estabilidad a corto plazo. Adicionalmente, la baja densidad del tráfico útil facilita la caracterización del perfil de operación normal de la red, facilitando la detección estadística de anomalías mediante sistemas de detección de intrusos (IDS).

Por el contrario, el esquema por umbrales presenta una debilidad estructural ante ataques de descarte de paquetes (*packet dropping*). En el muestreo periódico, la redundancia temporal intrínseca mitiga el impacto de las pérdidas, puesto que la información omitida es reemplazada por una nueva medición en el siguiente periodo de muestreo, acotando el error en la acción de control. En la transmisión basada en umbrales, la redundancia temporal se elimina a cambio de un uso más eficiente de la red, por lo que cada paquete posee una alta densidad informativa al encapsular un cambio significativo en la salida del sistema.

Si un atacante intercepta y descarta un evento de cruce de umbral, el controlador no recibe la actualización de la variable medida y continúa aplicando la ley de control basada en un valor desactualizado. Esta incoherencia entre la información del sensor y el controlador rompe la premisa de que la ausencia de transmisión equivale a estabilidad, induciendo un error estacionario creciente y el riesgo de inestabilidad global del sistema, aspecto estudiado en trabajos como (De Persis and Tesi, 2015; Dolk and Heemels, 2017). Aunque el envío por cruce de umbrales reduce la probabilidad de interceptación en escenarios de descarte aleatorio debido al menor volumen de tráfico expuesto, resulta vulnerable ante un atacante selectivo capaz de identificar y descartar eventos emitidos.

El análisis comparativo evidencia que la reducción del tráfico en el control basado en umbrales actúa como mecanismo de defensa pasivo contra la saturación por DoS, pero acentúa la relevancia de cada unidad de datos transmitida por el sensor, transformando el *packet dropping* en una amenaza significativa. Por consiguiente, es necesario formular estrategias de mitigación específicas que doten a este esquema de robustez. Trabajos como (Peng and Sun, 2020) exploran esta misma idea.

Con el objetivo de preservar los beneficios del cruce de umbrales frente a la saturación y neutralizar la falta de información inducida por el descarte de paquetes, en este trabajo se propone un mecanismo de mitigación fundamentado en una adaptación del parámetro δ del SSOD para contrarrestar la pérdida de datos ante un ataque de descarte de paquetes teniendo en cuenta el Número Máximo Admisible de Descartes Sucesivos (MANSD).

4. Mitigación de efectos de ataques de descarte de paquetes

Conforme a lo expuesto en la Sección 2, el valor de δ se determina fundamentalmente en función del error en estado estacionario admisible para el sistema de control ilustrado en la Figura 1. A este valor de diseño base lo denominaremos en adelante como δ original (δ_o). Sin embargo, ante un escenario de ataque por descarte de paquetes (*packet dropping*), este requerimiento de desempeño puede verse comprometido. La estrategia de mitigación planteada en esta sección tiene como objetivo principal atenuar el impacto de la pérdida de datos para evitar la violación del límite establecido para dicho error en estado estacionario. Para lograrlo, la estrategia planteada consistirá en modificar la cuantización, adoptando un nuevo valor que se definirá como δ de mitigación (δ_m). Esta estrategia de mitigación mediante variación de δ se fundamenta en el hecho de que su valor no influye en la posible aparición de oscilaciones de ciclo límite según se destacó en la Observación 1.

Este tipo de ataques se caracteriza, en general, mediante la probabilidad de descarte de paquetes; cuanto mayor es dicha probabilidad, más severo es el ataque, pero más fácil será su detección. En este artículo se asume que esta probabilidad está completamente definida por el atacante, el cual fija su valor en función del nivel de intensidad del ataque que pretende desplegar. Asimismo, se asume que el descarte de paquetes se comporta como un proceso de Bernoulli, es decir, que el atacante intercepta cada paquete y lo elimina de forma independiente con una probabilidad constante $p \in [0, 1]$. Adicionalmente, para el desarrollo de la estrategia propuesta, se asume que dicha probabilidad p de descarte de paquete es conocida mediante una estimación en-línea.

Dado el carácter estocástico del ataque, resulta inviable garantizar el cumplimiento del error admisible de forma determinista. Por consiguiente, el diseño de δ_m se aborda desde un enfoque probabilístico. El objetivo consiste en determinar un valor para δ_m tal que, ante una probabilidad de descarte p, el riesgo de que la desviación del sistema exceda el límite estipulado por δ_o sea inferior a la probabilidad q definida por el defensor ante el ataque.

Para materializar matemáticamente esta estrategia, se considera que, bajo el modelo de Bernoulli antes descrito, la probabilidad de que el adversario logre ejecutar con éxito n ataques sucesivos es p^n. Durante este intervalo de incomunicación, el desvío entre la última señal correctamente recibida y_{k-n} y el valor de la muestra actual y_k, expresado como $\epsilon = |y_k - y_{k-n}|$, se incrementa de forma acotada, alcanzando un valor máximo de $\epsilon \leq n\delta$. Este análisis se encuentra estrechamente ligado al concepto de Número Máximo Admisible de Descartes Sucesivos (MANSD), el cual define el límite de pérdidas consecutivas que el lazo de control puede tolerar bajo criterios de estabilidad o rendimiento. Con base en este vínculo, se sugiere como técnica de rediseño configurar la relación

$\delta_o = n\delta_m$, seleccionando para ello el número entero n más pequeño que cumpla con la condición $p^n \leq q$. De esta manera, se asegura que la probabilidad de experimentar un desvío mayor al diseño base δ_o quede confinada por debajo del nivel de tolerancia q especificado.

No obstante, dado que esta estrategia de mitigación se basa en reducir el umbral de transmisión en comparación con el diseño original ($\delta_m < \delta_o$), se corre el riesgo de inducir el denominado efecto Zeno. Este fenómeno consiste en la generación de un número excesivo, teóricamente infinito, de eventos dentro de un intervalo de tiempo finito, lo que se traduce en una frecuencia de conmutación extremadamente alta (*chattering*) que compromete la viabilidad del sistema.

Para evitar este comportamiento, se pueden establecer cotas inferiores para el valor de δ_m atendiendo a dos criterios de diseño distintos. En primer lugar, con el objetivo de prevenir la transmisión de eventos debida al ruido de medida, se debe seleccionar siempre una δ_m que sea mayor que la amplitud pico a pico del ruido inherente al sensor n_{p-p}. Seleccionando, por tanto, $\delta_m > n_{p-p}$, se logra establecer una cota mínima para δ_m a la vez que la información transmitida sigue siendo significativa para el control.

En segundo lugar, se pueden considerar las restricciones asociadas al ancho de banda disponible. Dado que la frecuencia de transmisión de eventos depende de la dinámica del proceso, ante cambios de tipo escalón es posible acotar superiormente esta tasa de envío. Para ello, se aproxima el transitorio de respuesta mediante una línea recta con la pendiente máxima durante todo el tiempo de subida (t_r). Esta pendiente máxima se determina como el producto entre el valor pico de la respuesta impulsional del sistema, $h_{max} = \max_{t\geq 0}\{h(t)\}$, y la magnitud del escalón, A. Bajo esta aproximación conservadora, el número total de eventos generados durante el transitorio viene dado por:

$$n_{ev} = \left\lfloor \frac{h_{max} \cdot A \cdot t_r}{\delta_m} \right\rfloor,$$

lo que se traduce en una tasa de envío de eventos aproximada:

$$rate_{rise} \approx \frac{h_{max} \cdot A}{\delta_m}.$$

Por tanto, si el ancho de banda disponible para este lazo de control está limitado por una tasa máxima de generación de eventos admisible ($rate_{BW}$), se puede garantizar el cumplimiento de esta restricción seleccionando el umbral de mitigación de modo que:

$$\delta_m > \frac{h_{max} \cdot A}{rate_{BW}}.$$

Condicionar el umbral inferior de mitigación bajo estos criterios asegura que, durante este tipo de transitorios o en presencia de ruido, la densidad de tráfico generada no sature la capacidad del canal, previniendo eficazmente el *flooding* de la red.

4.1. Detección del ataque y estimación de la probabilidad p

En el muestreo periódico es fácil detectar el ataque por descarte de paquetes y calcular la tasa de descarte (p.ej. si se esperan 100 paquetes por segundo y llegan 80, se han descartado el 20 %). Sin embargo, en el muestreo por umbrales, dado que el tráfico es esporádico e impredecible, la única forma fiable de detectar el *packet dropping* en tiempo real es combinando contadores de secuencia y mecanismos de temporización de envío, tal como se describe a continuación:

- Contadores de Secuencia: El sensor encapsula un número entero incremental en cada paquete de dato transmitido (1, 2, 3...). Si el controlador recibe el paquete 4 y el siguiente es el 7, registra inmediatamente la pérdida de dos paquetes. Los sistemas que implementan contadores de secuencia deben implementar, a su vez, mecanismos para gestionar la posible pérdida de secuencialidad en la recepción de paquetes, sea esta derivada de ciberataques o del propio retardo variable que representa la red de comunicaciones.
- Mecanismos de Temporización (*Timeouts* o *Heartbeats*): Se programa un tiempo máximo entre envíos (T_{max}) para el sensor. Si el controlador supera este umbral sin recibir ningún paquete, entonces se están perdiendo paquetes.

Utilizando estas dos técnicas de forma combinada, es posible detectar la pérdida de paquetes y hacer una estimación de la probabilidad de descarte p usada por el atacante.

5. Estudio de simulación

Con el objetivo de evaluar el desempeño de la estrategia de mitigación propuesta y validar su viabilidad, en esta sección se desarrolla un estudio de simulación numérico. Para este análisis, se considera el lazo de control estructurado según el esquema presentado en la Figura 3.

En dicho modelo, el proceso continuo a controlar viene descrito por la función de transferencia:

$$G(s) = \frac{e^{-s}}{(s+1)^3}$$

Asimismo, la acción de control se ejecuta mediante un controlador PID, el cual ha sido sintonizado empleando el método presentado en (Miguel-Escrig et al., 2020), el cual asegura márgenes de robustez frente a oscilaciones de ciclo límite inducidas por la cuantización SSOD. Los parámetros de diseño resultantes son $K_p = 0{,}864$, $T_i = 2{,}59$, $T_d = 0{,}65$ y $N = 3$. Para la cuantización SSOD se considera un valor $\delta_o = 0{,}066$, que produce 15 muestras en la duración del tiempo de subida para un cambio de referencia unitario. A partir de estas condiciones de operación, se evalúa a continuación la respuesta del sistema bajo diferentes intensidades de agresión.

Se consideran tres casos según la intensidad del ataque de descarte de paquetes, caracterizados por la probabilidad p. Se define un ataque leve con $p = 0{,}1$, un ataque moderado con $p = 0{,}5$ y un ataque severo con $p = 0{,}9$. Como parámetro de diseño para la mitigación, se selecciona un nivel de riesgo $q = 0{,}05$, el cual establece el límite admisible para la probabilidad de que la desviación de la señal, ϵ, llegue a superar el umbral δ_o a causa de n pérdidas sucesivas de información.

A partir de la condición de diseño establecida de forma teórica ($p^n \leq q$), se determina de manera exacta el menor número entero n de pérdidas consecutivas tolerables para cada escenario de agresión. Para el caso de un ataque leve ($p = 0{,}1$), la condición se satisface con $n = 2$, requiriendo un umbral de

mitigación $\delta_m = \delta_o/2$. En el escenario moderado ($p = 0{,}5$), el valor crítico aumenta a $n = 5$, lo que reduce la cuantización a $\delta_m = \delta_o/5$. Finalmente, ante un ataque severo ($p = 0{,}9$), el sistema exige un diseño considerablemente más conservador con $n = 29$, resultando en un umbral de mitigación significativamente menor, $\delta_m = \delta_o/29$.

Para evaluar el impacto de esta estrategia y contrastar el desempeño del lazo de control, en la Figura 4 se presentan de forma comparativa los resultados temporales de las simulaciones de los casos descritos anteriormente. Las figuras de cada columna muestran la respuesta del sistema bajo cada intensidad de ataque considerada. En la fila superior se muestra la evolución temporal utilizando el umbral original δ_o sin ningún mecanismo de mitigación del ataque, mientras que en la fila inferior se muestran las respuestas utilizando el umbral de mitigación δ_m para cada nivel de intensidad de ataque considerado. En cada figura, la evolución de la señal controlada y se representa en azul, la señal muestreada por la unidad sensora y^* en gris, la señal recibida por el controlador $\bar{y}$ en rojo, y cada ataque exitoso se ha indicado con una línea vertical negra en la parte inferior.

Como se puede apreciar en los gráficos de la Figura 4, la adopción de la δ_m adecuada para cada escenario da lugar a una respuesta del sistema significativamente más suave y cercana a la nominal, logrando mantener la regulación del lazo de control a pesar de la severidad en la pérdida de información.

No obstante, el resultado obtenido de forma directa para el escenario de ataque severo ($\delta_m = 0{,}066/29 \approx 0{,}0023$) puede representar un planteamiento más académico que realista en la práctica. Un umbral tan reducido puede ser inviable tanto por las condiciones de operación del entorno, como el ruido o las restricciones de ancho de banda, como por la propia resolución del sensor. Por tanto, como resultado de considerar conjuntamente el impacto del ruido y la capacidad del canal, como se detalla en la sección anterior, consideramos que se establece para este escenario una cota mínima de $\delta_m = 0{,}005$.

Los resultados de la simulación bajo esta restricción práctica se presentan en la Figura 5. Como se puede observar, el comportamiento del lazo de control experimenta un deterioro evidente en comparación con el caso ideal presentado anteriormente, traduciéndose en una respuesta con un carácter más errático y con un aumento en la variación total de la respuesta (un mayor *travel value* o recorrido acumulado de la señal). Visualmente, se aprecian extensas franjas temporales en las que la evolución de la variable controlada es muy lenta y, debido a la interrupción en el flujo de datos, el sistema es incapaz de corregir la desviación, lo que genera un efecto dinámico muy marcado.

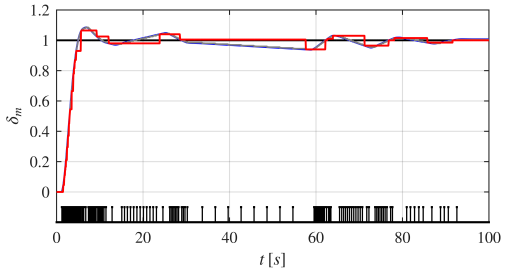


Figura 5: Respuesta del sistema frente a un ataque severo ($p = 0{,}9$) y considerando $\delta_m = 0{,}005$.

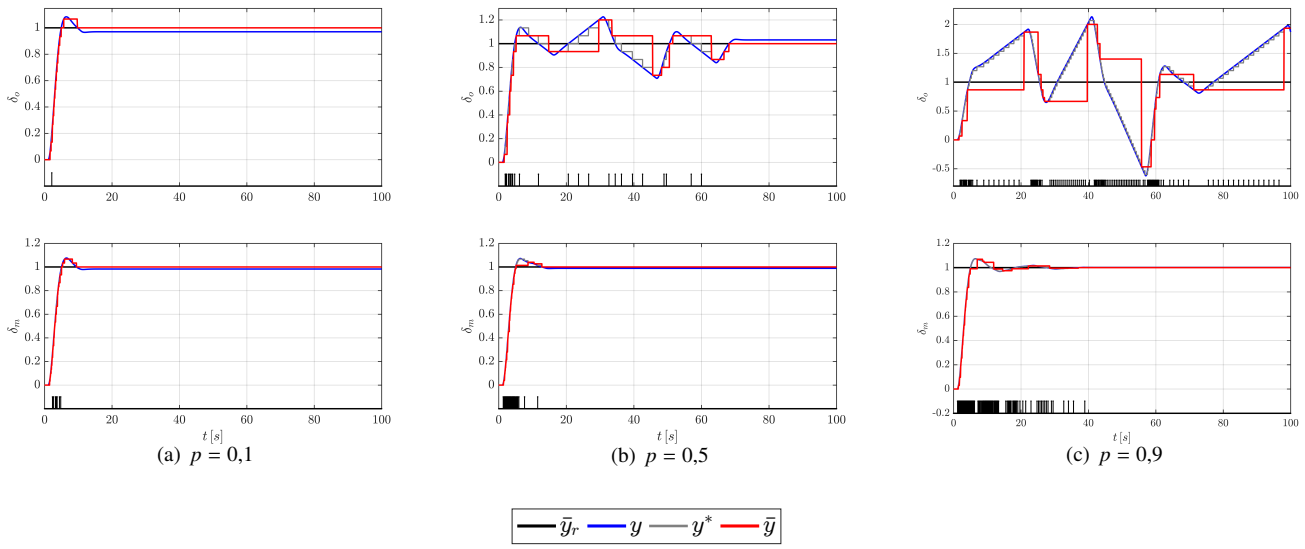
No obstante, la pérdida de información no es absoluta debido a la naturaleza probabilística del ataque, por lo que eventualmente algún paquete logra llegar con éxito al controlador. Al restablecerse la comunicación tras un periodo de silencio prolongado, el error acumulado en el sistema es ya muy elevado, lo que provoca que el algoritmo genere una acción de control de gran magnitud. Esta fuerte respuesta propicia una evolución rápida en la variable controlada. Al cambiar la salida más rápidamente, el mecanismo SSOD incrementa la densidad de eventos generados en una franja de tiempo menor.

A pesar de que en este caso la probabilidad de interceptación sigue siendo alta, la adopción de esta cota para δ_m comportaría una q equivalente de aproximadamente un 25,4 %. Si bien esto resulta en un comportamiento alejado del ideal óptimo, esta estrategia logra reducir significativamente el recorrido y la degradación de la señal de salida en comparación con el escenario sin mitigación, contribuyendo a la estabilidad global del lazo.

6. Conclusiones

Desde el punto de vista de la ciberseguridad, el envío de datos basado en cruce de niveles presenta algunas ventajas frente al muestreo periódico convencional. Al transmitir únicamente cuando la variable medida cruza determinados umbrales, se reduce el tráfico medio de la red y, con ello, la superficie de exposición frente a interceptación, congestión y manipulación de paquetes. Además, la ausencia de una cadencia estrictamente periódica dificulta la predicción de los instantes de transmisión por parte del atacante, complicando ataques de tipo Man-in-the-Middle, replay o inyección sistemática de datos falsos. En general, el envío por cruce de niveles puede mejorar la resiliencia frente a ataques de denegación de servicio parciales, ya que la menor carga de comunicaciones deja mayor margen operativo ante congestiones o pérdidas ocasionales de paquetes. También reduce la información disponible para atacantes pasivos, dificultando la reconstrucción completa de la evolución temporal del proceso.

Esta técnica de muestreo y envío de datos, sin embargo, no elimina por sí sola las vulnerabilidades de la red ni de los protocolos industriales. En este sentido, el enfoque por umbrales es especialmente sensible a los ataques de descarte de paquetes, debido a la relevancia de cada dato transmitido y a la falta de redundancia de información en comparación con el esquema periódico convencional. Para abordar este problema, en este trabajo se propone un método de mitigación basado en el ajuste dinámico de los umbrales, evitando así el impacto de la



(a) $p = 0{,}1$ (b) $p = 0{,}5$ (c) $p = 0{,}9$

Figura 4: Respuestas del sistema para diferentes valores de p y $q = 0{,}05$. Comparación entre δ_o (arriba) y δ_m (abajo).

pérdida consecutiva de paquetes de datos. Dicha propuesta se ha evaluado en varios escenarios con ataques de distinta intensidad, demostrando un desempeño satisfactorio en todos ellos. Como trabajo futuro, se plantea combinar la estrategia desarrollada con mecanismos de estimación en línea de la probabilidad de descarte, así como su validación en entornos reales de ciberataque.

Finalmente, es importante destacar que el envío basado en cruce de niveles debe entenderse como una estrategia complementaria de resiliencia y reducción de superficie de ataque, no como una solución autónoma de ciberseguridad. Su eficacia aumenta cuando se combina con autenticación, cifrado, marcas temporales, números de secuencia, señales periódicas de supervisión y mecanismos de detección basados en modelos dinámicos. En particular, una arquitectura híbrida que combine transmisión por eventos con mensajes periódicos de baja frecuencia puede conservar las ventajas de la reducción de tráfico sin perder capacidad de diagnóstico ante la ausencia prolongada de comunicaciones.

Agradecimientos

Este trabajo es parte de los proyectos de investigación PID2021-125634OB-I00 y PID2024-160455OB-I00 financiados por MCIN/AEI/10.13039/501100011033 y por ERDF/EU. También es parte del proyecto de investigación CIAICO/2024/74 financiado por la Conselleria d'Educació, Cultura, Universitats i Ocupació de la Generalitat Valenciana y la Universitat Jaume I bajo las subvenciones UJI-2024-22 y GACUJIMA/2025/08.

Referencias

Beschi, M., Dormido, S., Sanchez, J., Visioli, A., Dec. 2012. Characterization of symmetric send-on-delta PI controllers. Journal of Process Control 22 (10), 1930–1945.
DOI: 10.1016/j.jprocont.2012.09.005

De Persis, C., Tesi, P., 2015. Input-to-state stabilizing control under denial-of-service. IEEE Transactions on Automatic Control 60 (11), 2930–2944.

Dolk, V., Heemels, M., 2017. Event-triggered control systems under packet losses. Automatica 80, 143–155.

Dolk, V. S., Tesi, P., De Persis, C., Heemels, W., 2016. Event-triggered control systems under denial-of-service attacks. IEEE Transactions on Control of Network Systems 4 (1), 93–105.

Miguel-Escrig, O., Romero-Pérez, J.-A., Sanchis-Llopis, R., 2020. Tuning pid controllers with symmetric send-on-delta sampling strategy. Journal of the Franklin Institute 357 (2), 832–862.

Peng, C., Sun, H., 2020. Switching-like event-triggered control for networked control systems under malicious denial of service attacks. IEEE Transactions on Automatic Control 65 (9), 3943–3949.

Romero-Pérez, J.-A., Miguel-Escrig, O., 2024. Auto-tuning method for pi controllers under symmetric-send-on-delta sampling strategy. Journal of the Franklin Institute 361 (13), 106971.
URL: https://www.sciencedirect.com/science/article/pii/S0016003224003922
DOI: https://doi.org/10.1016/j.jfranklin.2024.106971

Romero Pérez, J. A., Sanchis Llopis, R., 2016. A new method for tuning pi controllers with symmetric send-on-delta sampling strategy. ISA Transactions 64, 161–173.
URL: https://www.sciencedirect.com/science/article/pii/S0019057816301033
DOI: https://doi.org/10.1016/j.isatra.2016.05.011

Tabuada, P., 2007. Event-triggered real-time scheduling of stabilizing control tasks. IEEE Transactions on Automatic control 52 (9), 1680–1685.

Zhao, N., Shi, P., Xing, W., Lim, C. P., 2021. Event-triggered control for networked systems under denial of service attacks and applications. IEEE Transactions on Circuits and Systems I: Regular Papers 69 (2), 811–820.