XX Simposio CEA de Control Inteligente
25-27 de junio de 2025, Huelva

Protección de sistemas domóticos frente a ciberataques mediante sistemas de inferencia neuroborrosos

Fernández-Píriz, L., García, R.A.*, Escaño, J.M.

Departamento de Ingeniería de Sistemas y Automática, Universidad de Sevilla,
Escuela Técnica Superior de Ingeniería, Camino de los Descubrimientos s/n, 41092, Sevilla, España.

To cite this article: Fernández-Píriz, L., García, R.A., Escaño, J.M. 2025. Protection of home automation systems against cyberattacks using neuro-fuzzy inference systems. XX Simposio CEA de Control Inteligente, Huelva (Spain), 2025.

Resumen

Este trabajo presenta una arquitectura de control resiliente para entornos domóticos inteligentes sometidos a ciberataques. La solución propuesta integra un sistema de inferencia neuroborroso adaptativo (ANFIS) directamente en un PLC, con el objetivo de estimar la temperatura real de una habitación incluso cuando los datos de los sensores han sido manipulados. El modelo ANFIS posee una estructura autoregresiva que incorpora estimaciones anteriores y temperaturas de estancias contiguas, lo que le permite detectar anomalías provocadas por ataques de tipo *Man-in-the-Middle* e inyección de datos. El sistema ha sido validado en un entorno de simulación en tiempo real que combina Home I/O, MATLAB/Simulink y un PLC M221 de Schneider Electric. Los resultados experimentales muestran que el ANFIS mantiene estimaciones precisas durante el ataque, evitando que el controlador PID actúe de forma incorrecta. Esta estrategia incrementa la ciberresiliencia del sistema y se alinea con el enfoque de defensa en profundidad propuesto por la norma IEC 62443. La arquitectura desarrollada demuestra el potencial de integrar mecanismos inteligentes de detección dentro del propio lazo de control de sistemas ciberfísicos.

Palabras clave: Métodos basados en redes neuronales y/o lógica borrosa para la FDI, Automatización de edificios, Detección y diagnóstico de fallos.

Protection of home automation systems against cyberattacks using neuro-fuzzy inference systems

Abstract

This work presents a resilient control architecture for smart home environments under cyberattack conditions. The proposed approach integrates an Adaptive Neuro-Fuzzy Inference System (ANFIS) directly into a PLC to estimate room temperature even when sensor data is falsified. The ANFIS is designed with an autoregressive structure, incorporating previous estimations and neighboring room temperatures, allowing it to detect anomalies caused by Man-in-the-Middle and data injection attacks. The system was tested using a real-time simulation environment combining Home I/O, MATLAB/Simulink, and a Schneider Electric M221 PLC. Experimental results show that the ANFIS maintains accurate temperature estimations during attacks, preventing incorrect control actions by the conventional PID controller. This enhances the cyber-resilience of the system and aligns with the IEC 62443 defense-in-depth strategy. The proposed framework demonstrates the potential of embedding intelligent detection mechanisms into the control loop of cyber-physical systems.

Keywords: Methods based on neural networks and/or fuzzy logic for FDI, Building Automation, Fault detection and diagnosis.

*Autor para correspondencia: ramongr@us.es

1. Introducción

La digitalización progresiva de las infraestructuras residenciales ha impulsado el desarrollo de los denominados edificios inteligentes, donde diversos subsistemas como la climatización, la iluminación o la seguridad son gestionados de forma automatizada mediante tecnologías conectadas. Esta automatización aporta beneficios evidentes en términos de eficiencia energética y confort. Sin embargo, también incrementa la exposición a vulnerabilidades de ciberseguridad, especialmente cuando los dispositivos se comunican a través de redes digitales abiertas o poco protegidas (Buil-Gil et al., 2023).

En particular, los sistemas domóticos que integran sensores, actuadores y controladores son susceptibles a ciberataques que pueden alterar el comportamiento normal del sistema. Entre las técnicas más relevantes se encuentran los ataques de intermediario (Man-in-the-Middle) y la inyección de datos falsos (False Data Injection Attacks), que permiten modificar las señales que recibe el sistema de control sin que existan alteraciones físicas visibles (Cash et al., 2023). En un contexto residencial, este tipo de ataques podría, por ejemplo, inducir al sistema de calefacción a operar fuera de los valores deseados, con consecuencias en el consumo energético, el confort térmico e incluso la seguridad de los ocupantes.

Los enfoques clásicos de ciberseguridad, basados en el aislamiento o la detección perimetral, resultan insuficientes en este tipo de sistemas ciberfísicos, especialmente cuando el atacante ya ha comprometido las comunicaciones internas. Por ello, es necesario incorporar mecanismos internos de detección de anomalías que permitan identificar comportamientos no esperados y mitigar su impacto en tiempo real.

La seguridad ciber-física en sistemas de automatización de edificios (BAS) presenta crecientes desafíos ante ataques que manipulan sensores y lazos de control. Li et al. (2023) ofrecen una revisión exhaustiva de los riesgos en BAS, destacando la necesidad de detección integrada en el lazo de control. Melgaard et al. (2022) revisan técnicas de detección de fallos (FDD) en sistemas HVAC, donde métodos basados en inteligencia artificial permiten detectar anomalías operativas. Sin embargo, la mayoría de estos enfoques actúan externamente al control, mientras que este trabajo propone integrar un modelo ANFIS embebido directamente en el PLC, aportando detección continua y resiliencia operativa.

La norma internacional IEC 62443 (International Electrotechnical Commission, 2009), específicamente diseñada para sistemas de automatización y control industrial (IACS), establece como principio fundamental la defensa en profundidad (defense-in-depth), una estrategia que reconoce que ningún componente individual puede ofrecer protección total frente a amenazas cibernéticas. Este enfoque promueve la implementación de múltiples capas de seguridad distribuidas en todo el sistema, de modo que si un atacante compromete una capa, aún existan mecanismos de contención y detección en niveles posteriores.

Aunque esta norma ha sido desarrollada para entornos industriales, su aplicabilidad se extiende a los sistemas domóticos residenciales modernos, que comparten con los IACS muchas características de los sistemas ciberfísicos críticos: conectividad permanente, dependencia del control automatizado y sensibilidad a fallos provocados por manipulación de datos. En este contexto, la resiliencia se convierte en un objetivo esencial: el sistema debe ser capaz no solo de resistir ataques, sino de continuar operando de forma segura, identificando y aislando los efectos del comportamiento malicioso (Escaño, 2025).

Este trabajo se enmarca en dicha filosofía de defensa en profundidad, al proponer la integración de un sistema de inferencia neuroborroso (Adaptive Neural Fuzzy Inference System, ANFIS) que actúa como capa interna de detección y mitigación de anomalías. Este mecanismo, implementado directamente en el PLC, es capaz de estimar de forma robusta el estado real del sistema térmico, incluso cuando las señales de entrada han sido manipuladas, contribuyendo así a la ciberresiliencia del entorno domótico.

El sistema se ha implementado en un entorno de simulación domótica con Home I/O, MATLAB y un PLC modelo M221 de Schneider-Electric, simulando una vivienda con control térmico distribuido. Se ha desarrollado un escenario de ataque mediante inyección de datos falsos, con el objetivo de evaluar la respuesta del sistema ANFIS ante perturbaciones simuladas.

El objetivo principal es demostrar la viabilidad de integrar un mecanismo de defensa embebido, no intrusivo y con capacidad de respuesta autónoma, que permita mantener la estabilidad del sistema de control aún bajo condiciones adversas. La propuesta tiene especial relevancia en el ámbito de la ciberseguridad residencial, donde la tolerancia a fallos y la continuidad del servicio resultan esenciales.

2. Arquitectura general del sistema propuesto

Este trabajo propone una arquitectura de control resiliente basada en la combinación de controladores PID y un sistema neuroborroso (ANFIS), capaz de estimar valores de la temperatura de una habitación en función de las otras temperaturas medidas. En la Figura 1 se puede apreciar la arquitectura propuesta.

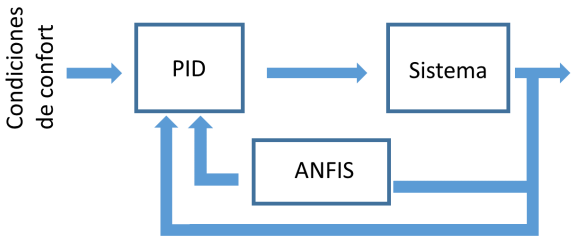

Figura 1: Arquitectura general del sistema PID ANFIS.

El estimador implementado se basa en un sistema de inferencia neuro-borroso adaptativo (ANFIS), que combina la capacidad de aprendizaje adaptativo de las redes neuronales con la representación explícita de reglas difusas de tipo Takagi-Sugeno (Jang, 1993). Esta estructura híbrida permite modelar relaciones no lineales complejas entre entradas y salidas, utilizando funciones de pertenencia parametrizadas cuya adaptación se realiza mediante un algoritmo híbrido que combina retropropagación para la actualización de parámetros no lineales

y mínimos cuadrados para los parámetros lineales. Gracias a esta capacidad de aprendizaje supervisado, el ANFIS puede capturar la dinámica térmica del sistema sin necesidad de un modelo físico detallado, resultando particularmente adecuado para entornos con incertidumbres o comportamientos no modelados, como ocurre en contextos de ciberseguridad.

El sistema ANFIS ha sido implementado directamente en el PLC con el objetivo de incorporar una capa de inteligencia que permita estimar la temperatura real de una habitación incluso en presencia de datos alterados. Este sistema de inferencia difusa recibe como entradas: la temperatura estimada en los instantes $k-1$ y $k-2$ por el propio ANFIS, $T_{a_{k-1}}$ y $T_{a_{k-2}}$ (es decir, salidas anteriores del sistema, lo que configura una arquitectura autoregresiva), la señal de control aplicada al calefactor en el instante $k-1$, $V_{a_{k-1}}$, la temperatura en el instante $k-1$ de la habitación contigua, $T_{c_{k-1}}$, y la temperatura en el instante $k-2$ de una habitación más alejada, $T_{d_{k-1}}$. La salida actual del sistema T_{a_k} representa la estimación de la temperatura de la habitación objetivo en el instante k, robusta frente a posibles manipulaciones de los sensores. Esta estructura autoregresiva mejora la capacidad del sistema para detectar inconsistencias temporales y espaciales en los datos. La estructura del sistema ANFIS, incluyendo sus entradas y salida, se muestra en la Figura 2.

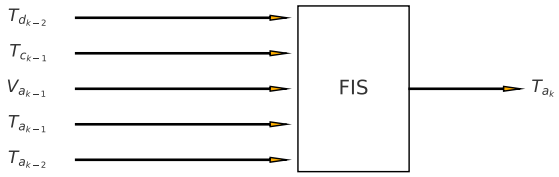

Figura 2: Entradas y salidas del FIS

El entrenamiento del sistema ANFIS se ha realizado utilizando datos históricos obtenidos mediante simulación en lazo abierto, donde se registraron las temperaturas reales y las señales de control aplicadas sin la intervención de algoritmos inteligentes. El conjunto de datos se ha dividido en dos subconjuntos: uno para entrenamiento y otro para validación (checking), con el objetivo de evitar el sobreajuste (*overfitting*) del modelo y asegurar su capacidad de generalización. El algoritmo de entrenamiento empleado fue el método híbrido estándar de retropropagación y mínimos cuadrados, disponible en la herramienta ANFIS de MATLAB.

Los resultados de la validación mostraron un ajuste adecuado entre la salida estimada por el sistema y la temperatura real de la estancia, con un error cuadrático medio (RMSE) inferior a 0,5°C en todas las habitaciones modeladas. Además, el coeficiente de determinación (R^2) superó el 0,95, lo que indica una alta capacidad predictiva del sistema entrenado. Estos resultados confirman que el modelo ANFIS puede predecir con precisión la evolución térmica de la habitación bajo condiciones nominales, proporcionando una base sólida para la detección de desviaciones anómalas en tiempo real.

Gracias a su diseño autoregresivo y a la incorporación de información contextual (de estancias adyacentes y variables de control), el sistema ANFIS resulta particularmente eficaz para identificar inconsistencias causadas por ataques de manipulación de datos, sin requerir un modelo físico detallado del comportamiento térmico del entorno.

La Figura 3 muestra un ejemplo representativo de la validación del sistema ANFIS, donde se observa la buena concordancia entre la temperatura real y la estimación generada por el modelo.

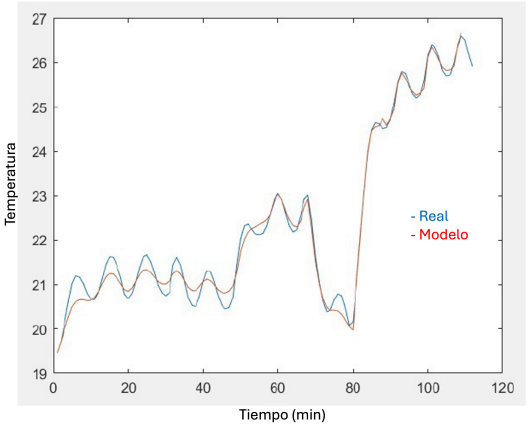

Figura 3: Validación del ANFIS entrenado con datos

Como se introdujo anteriormente, la arquitectura del sistema se basa en la integración de tres componentes principales: el entorno de simulación *Home I/O*, que emula el comportamiento físico de la vivienda; MATLAB/Simulink, utilizado para implementar los algoritmos de control y estimación; y el autómata programable M221 de Schneider Electric, que actúa como ejecutor de las señales de control. Estos elementos se describen con más detalle en las subsecciones siguientes.

En la Figura 4 se puede apreciar como es la conexión entre los distintos elementos.

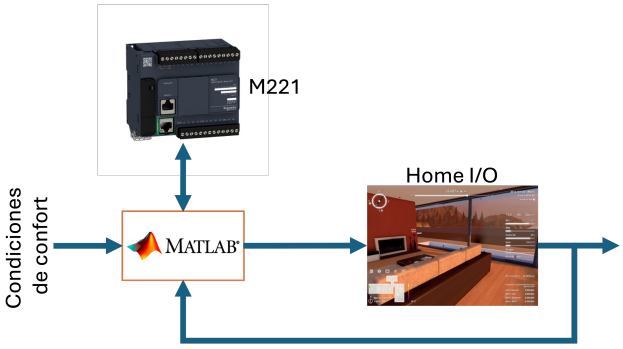

Figura 4: Arquitectura general.

El sistema ANFIS (Adaptive Neuro-Fuzzy Inference System) combina las capacidades de aprendizaje adaptativo de las redes neuronales con la representación interpretativa de los sistemas de inferencia difusa. Esta arquitectura híbrida permite modelar relaciones no lineales complejas entre entradas y salidas a partir de datos, manteniendo al mismo tiempo una estructura basada en reglas lingüísticas comprensibles. Un ANFIS típico implementa un sistema difuso de tipo Takagi-Sugeno con parámetros ajustables en sus funciones de pertenencia, entrenados mediante algoritmos de retropropagación y mínimos

cuadrados. Esta dualidad lo convierte en una herramienta especialmente útil en entornos donde la dinámica del sistema no puede modelarse con precisión a priori, o donde es necesario detectar desviaciones sutiles respecto al comportamiento esperado, como ocurre en contextos de ciberseguridad en sistemas ciberfísicos.

En el presente trabajo, se ha implementado un sistema de control térmico distribuido para tres estancias independientes, cada una equipada con su propio controlador PID y su correspondiente sistema ANFIS. El controlador PID recibe la temperatura medida por el sensor de su habitación y genera una señal de control en el rango 0–10 V, que regula la potencia aplicada al calefactor correspondiente. El sistema ANFIS asociado a cada estancia actúa como un estimador robusto de la temperatura real, proporcionando una segunda capa de supervisión basada en inteligencia difusa.

Cada ANFIS recibe como entradas la temperatura medida en instantes anteriores en las tres habitaciones y la señal de control aplicada en el instante anterior al calefactor de su propia habitación. La salida del sistema ANFIS es la estimación de la temperatura actual de la habitación correspondiente. Esta estimación se utiliza como referencia interna para verificar la coherencia de los valores sensados y detectar posibles manipulaciones o errores anómalos.

2.1. Home I/O

Para la realización del estudio se ha empleado *Home I/O*, un entorno de simulación interactivo que permite modelar, visualizar y controlar en tiempo real una vivienda inteligente. Este software ha sido diseñado específicamente para la enseñanza y experimentación en automatización de edificios, proporcionando una representación tridimensional realista de una vivienda unifamiliar equipada con sensores, actuadores, dispositivos de climatización, iluminación, seguridad, y comunicaciones.

Home I/O permite establecer una conexión en tiempo real con entornos de programación externos, como MATLAB/Simulink, CODESYS o Python, lo cual lo convierte en una plataforma idónea para desarrollar e implementar sistemas de control avanzados, como los descritos en este trabajo. En este artículo, se ha utilizado para simular un sistema domótico compuesto por tres estancias con calefacción independiente, cada una equipada con sensores de temperatura, calefactores eléctricos y controladores PID, supervisados por sistemas ANFIS para la detección de anomalías térmicas.

La elección de Home I/O permite evaluar de forma precisa el impacto de las estrategias de control inteligente propuestas, no solo desde un punto de vista técnico, sino también en términos de indicadores clave como el confort térmico, el ahorro energético y la ciberseguridad. Además, al tratarse de un entorno cerrado y controlado, resulta especialmente útil para ensayar escenarios de ciberataques, como la manipulación de señales de sensores o la alteración de las acciones de control, sin comprometer sistemas reales.

2.2. Implementación Hardware-Software

El entorno MATLAB/Simulink se ha utilizado como plataforma de desarrollo y ejecución del sistema de control, actuando como intermediario entre los algoritmos inteligentes diseñados y el entorno de simulación física proporcionado por *Home I/O*. El objetivo principal de esta integración es permitir la lectura en tiempo real de las variables de entrada del entorno domótico simulado —como sensores de temperatura, detectores de presencia o estados de actuadores—, y enviar señales de control calculadas a las salidas correspondientes, tales como la activación de calefactores o la apertura de persianas.

Para lograr una comunicación eficaz y sincronizada entre MATLAB/Simulink y Home I/O, es fundamental que ambos sistemas operen en tiempo real. Sin embargo, Simulink, por defecto, ejecuta las simulaciones a la máxima velocidad computacional disponible, lo que no garantiza una correspondencia temporal con el entorno físico simulado. Para solventar esta limitación, se ha empleado el paquete *RealTime_Pacer*, una herramienta que fuerza a Simulink a ejecutar el modelo siguiendo el tiempo del reloj del sistema operativo. De este modo, se asegura una ejecución determinista y sincronizada, condición imprescindible para mantener la coherencia temporal con la simulación en Home I/O.

Gracias a esta integración, MATLAB/Simulink no solo actúa como controlador del sistema, sino también como plataforma para la implementación de algoritmos avanzados de control adaptativo y detección de anomalías, como el sistema ANFIS desarrollado en este artículo. La posibilidad de modificar dinámicamente los modelos, registrar datos de simulación y visualizar señales en tiempo real convierte a Simulink en una herramienta clave para la validación funcional del sistema propuesto.

Para implementar el control físico de los calefactores modelados en el entorno de simulación Home I/O, se ha utilizado un autómata programable (PLC) modelo M221 de Schneider Electric. Este controlador forma parte de la familia Modicon y está diseñado específicamente para aplicaciones de automatización compactas y de complejidad moderada, como las que se encuentran habitualmente en entornos domóticos y de automatización de edificios.

El M221 ha sido programado mediante el entorno de desarrollo gratuito *EcoStruxure Machine Expert - Basic*, una herramienta proporcionada por el fabricante que permite la programación estructurada en lenguajes IEC 61131-3, incluyendo diagramas de escalera (LD) y texto estructurado (ST). Esta plataforma permite la configuración de entradas y salidas, la creación de bloques de función personalizados y la monitorización en tiempo real del sistema.

En este artículo, el PLC M221 actúa como ejecutor de las señales de control generadas por los sistemas de inferencia inteligente implementados en MATLAB/Simulink. La arquitectura resultante integra el cálculo de las acciones de control en un entorno de simulación externo (donde residen los controladores PID y ANFIS) y su ejecución física mediante el PLC, lo cual permite validar estrategias de control híbridas que combinan inteligencia artificial y lógica cableada convencional.

Esta configuración facilita la experimentación con esquemas de control distribuidos y supervisados, así como la validación de mecanismos de detección y mitigación frente a ciberataques, sin renunciar a la robustez y fiabilidad que ofrece una plataforma industrial como el M221.

Aunque el presente trabajo ha sido desarrollado y validado en el contexto específico de control térmico en entornos domóticos, la arquitectura propuesta es generalizable a otros sistemas

ciberfísicos donde existan relaciones dinámicas entre variables medidas y controladas, y donde los ataques puedan inducir inconsistencias temporales en los datos de sensores. Sistemas como control de humedad, iluminación adaptativa, o gestión energética distribuida en microrredes podrían beneficiarse de este enfoque. La selección de un horizonte autoregresivo de dos pasos ($k-1, k-2$) responde a un equilibrio entre complejidad computacional y capacidad de captura de la dinámica térmica del sistema. Extender el horizonte más allá de dos muestras proporcionaría potencialmente una mayor memoria histórica, pero incrementaría exponencialmente el número de reglas difusas y el coste computacional en su implementación embebida en el PLC.

3. Implementación del ataque

3.1. *Descripción del escenario físico*

El entorno simulado representa una vivienda unifamiliar compuesta por quince estancias diferenciadas, incluyendo un salón principal, un aseo, dos cuartos de baño, tres dormitorios, una oficina y un garaje, entre otros espacios funcionales. Una característica arquitectónica relevante para este estudio es la comunicación directa entre la oficina y el vestíbulo de entrada, los cuales se encuentran conectados sin separación estructural superior, como puede observarse en la Figura 5. Esta configuración influye en el intercambio térmico entre estancias y, por tanto, en la dinámica de control de temperatura.

El sistema de climatización de la vivienda está compuesto por calefactores eléctricos individuales instalados en todas aquellas estancias destinadas al tránsito frecuente o al uso habitual de los ocupantes. La distribución espacial de los calefactores puede visualizarse en la misma Figura 5, mientras que la Tabla 1 recoge la potencia asignada a cada uno de ellos. Esta información es clave para establecer las condiciones iniciales del sistema, dimensionar adecuadamente los controladores PID, y evaluar el impacto de perturbaciones provocadas por un ataque cibernético sobre el sistema térmico.

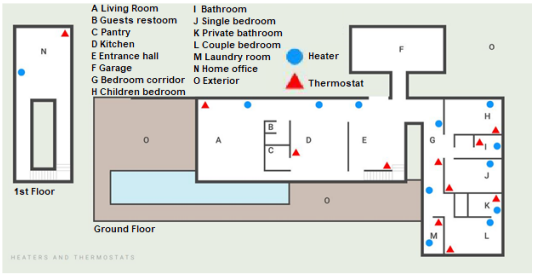

Figura 5: Mapa de la calefacción de la vivienda.

Tabla 1: Potencia eléctrica por zona de la vivienda

Zona	Potencia (kW)
A (Salón)	2.0
D (Cocina)	1.5
E (Hall)	1.75
G (Pasillo dormitorio)	0.75 + 0.75
H (Dormitorio infantil)	1.0
I (Cuarto de baño)	0.75
J (Habitación individual)	0.75
K (Baño privado)	1.0
L (Habitación doble)	0.75
M (Lavandería)	0.5
N (Oficina)	1.5

3.2. *Objetivos y modalidades del ataque*

En el escenario propuesto, se analiza la ejecución de un ataque tipo *Man-in-the-Middle* (MitM) que afecta a los sensores de temperatura de una de las habitaciones. El objetivo del atacante es manipular las lecturas de los sensores sin modificar el estado físico del sistema, induciendo así un comportamiento incorrecto en el lazo de control, que puede derivar en consumo energético innecesario o en la generación de condiciones térmicas inadecuadas para los ocupantes.

Los principales objetivos del ataque se resumen a continuación:

- **Interrupción y Bloqueo de la Comunicación Cliente-PLC:** Interrumpir la comunicación directa entre el sistema de control legítimo y el PLC, permitiendo al atacante inyectar comandos o lecturas falsas sin ser detectado inicialmente.
- **Evasión de Detección Mediante Infiltración Silenciosa:** Posicionarse entre el cliente y el PLC mediante *ARP Spoofing*, interceptando y modificando el tráfico sin generar alertas visibles.
- **Prueba de Resiliencia del Sistema de Seguridad:** Evaluar experimentalmente la capacidad del sistema ANFIS para detectar lecturas manipuladas, tanto con alteraciones progresivas como puntuales.
- **Evaluación del Impacto Funcional y Energético:** Observar el impacto de la manipulación sostenida sobre el confort térmico, el consumo energético y la estabilidad del sistema.

3.3. *Procedimiento de implementación técnica*

El ataque corresponde a una intrusión de tipo *Man-in-the-Middle* (MitM), cuyo objetivo es manipular las comunicaciones entre el sistema de control legítimo y el PLC M221. La técnica utilizada para interceptar y modificar el tráfico es el *ARP Spoofing*, permitiendo al atacante actuar como intermediario en la red local.

Para la implementación práctica del ataque, se configuró una red local entre el sistema de control, el PLC M221 y un equipo atacante. Mediante la herramienta `Ettercap`, se realizó un ataque de envenenamiento ARP, redirigiendo el tráfico entre el cliente y el PLC a través del ordenador atacante. Una vez establecida la interceptación, se utilizaron herramientas estándar de acceso a registros Modbus TCP/IP, como `ModbusPoll`, para modificar manualmente los valores de los sensores de temperatura, provocando la activación indebida de los calefactores.

3.4. *Mecanismo de detección basado en ANFIS*

Durante la ejecución del ataque, el sistema ANFIS previamente entrenado actúa como detector de anomalías. La salida estimada por el ANFIS se compara en tiempo real con la lectura recibida del sensor, permitiendo identificar desviaciones significativas que sugieren comportamientos anómalos. Este mecanismo de validación cruzada dota al sistema de resiliencia frente a ataques silenciosos, al incorporar inteligencia embebida directamente en el lazo de control, sin depender exclusivamente de mecanismos perimetrales de seguridad.

Este experimento demuestra la viabilidad de ataques MitM sobre sistemas domóticos conectados mediante protocolos estándar como Modbus TCP/IP, y la necesidad de integrar mecanismos internos de detección de intrusiones como los propuestos en la arquitectura basada en ANFIS.

4. Resultados de la simulación del ataque

La Figura 6 muestra la evolución temporal de las señales de temperatura durante una simulación en la que se inyecta un ataque de tipo *False Data Injection* en el sistema. En esta figura se representan tres variables clave: Home I/O (azul): Temperatura real de la estancia obtenida directamente del sensor del entorno simulado, FIS (rojo): Estimación de la temperatura generada por el sistema ANFIS, Ataque (verde): Valor falsificado que ha sido inyectado en el registro del PLC mediante un ataque MitM, simulando una lectura incorrecta.

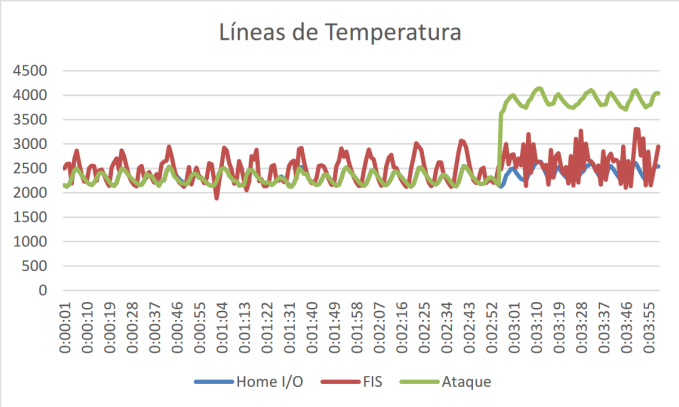

Figura 6: Resultado de simulación.

Durante el primer tramo de la simulación (hasta aproximadamente el segundo 160), el sistema opera con normalidad: la temperatura estimada por el ANFIS se mantiene en buena concordancia con la lectura del sensor, y ambas siguen un patrón coherente de oscilaciones.

A partir del instante **00:02:40**, se inicia el ataque. Se observa cómo la señal manipulada (verde) sufre un incremento abrupto y se mantiene en un rango superior al esperado, simulando un calentamiento ficticio. A pesar de ello, la estimación del sistema ANFIS (rojo) permanece próxima a la temperatura real (azul), demostrando su capacidad para filtrar datos incoherentes y mantener una estimación robusta.

Este resultado valida la funcionalidad del sistema ANFIS como mecanismo de detección y mitigación de anomalías. Al identificar una divergencia sostenida entre la estimación y el dato reportado por el sensor (manipulado), el sistema puede generar una alerta o tomar decisiones correctivas. Además, su estabilidad en presencia del ataque contribuye a la resiliencia general del sistema de control térmico.

5. Conclusiones

En este trabajo se ha propuesto y validado una arquitectura de control resiliente frente a ciberataques en sistemas domóticos, mediante la integración de un sistema ANFIS directamente en el PLC. Esta solución permite estimar la temperatura real de una estancia incluso cuando los datos del sensor han sido manipulados, gracias a una estructura autoregresiva que combina entradas temporales y espaciales. La simulación del ataque, basada en técnicas de ARP spoofing e inyección de datos, ha puesto de manifiesto la vulnerabilidad de los sistemas tradicionales y la necesidad de implementar mecanismos de detección en el propio lazo de control.

Los resultados obtenidos muestran que el sistema ANFIS mantiene una estimación coherente y cercana al valor real durante todo el ataque, lo que evita decisiones erróneas por parte del controlador PID. Esta estrategia, alineada con los principios de defensa en profundidad de la norma IEC 62443, refuerza la seguridad de los entornos ciberfísicos residenciales y abre la puerta a futuras ampliaciones con modelos adaptativos y otras variables críticas. La combinación de simulación realista con Home I/O y control en tiempo real con PLC y MATLAB proporciona un entorno flexible para validar nuevas estrategias de protección.

Agradecimientos

Este trabajo ha recibido financiación del proyecto PID2022-142069OB-I00, financiado por MCIN /AEI /10.13039 /501100011033 /FE-DER, UE y ha sido realizado en parte gracias al apoyo de la subvención RED2022-134588-T concedida por el MICIU/AEI/10.13039/501100011033.

Referencias

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., Nicholson, J., 2023. The digital harms of smart home devices: A systematic literature review. Computers in Human Behavior 145, 107770. DOI: https://doi.org/10.1016/j.chb.2023.107770

Cash, M., Morales-Gonzalez, C., Wang, S., Jin, X., Parlato, A., Zhu, J., Sun, Q. Z., Fu, X., 2023. On false data injection attack against building automation systems. In: 2023 International Conference on Computing, Networking and Communications (ICNC). pp. 35–41. DOI: 10.1109/ICNC57223.2023.10074353

Escaño, J. M., 2025. Ciberseguridad industrial, 1st Edition. Paraninfo, Madrid, España.

International Electrotechnical Commission, 2009. IEC 62443-1-1: Terminology, concepts and models. IEC, part of the IEC 62443 series on industrial communication network security.

Jang, J.-S., 1993. Anfis: adaptive-network-based fuzzy inference system. IEEE Transactions on Systems, Man, and Cybernetics 23 (3), 665–685. DOI: 10.1109/21.256541

Li, G., Ren, L., Fu, Y., Yang, Z., Adetola, V., Wen, J., Zhu, Q., Wu, T., Candan, K., O'Neill, Z., 2023. A critical review of cyber-physical security for building automation systems. Annual Reviews in Control 55, 237–254. URL: https://www.sciencedirect.com/science/article/pii/S1367578823000032 DOI: https://doi.org/10.1016/j.arcontrol.2023.02.004

Melgaard, S. P., Andersen, K. H., Marszal-Pomianowska, A., Jensen, R. L., Heiselberg, P. K., 2022. Fault detection and diagnosis encyclopedia for building systems: A systematic review. Energies 15 (12). URL: https://www.mdpi.com/1996-1073/15/12/4366 DOI: 10.3390/en15124366