Científica

vol. 30, no. 1, January-June 2026, pp. 01-14
ISSN 2594-2921, Instituto Politécnico Nacional, MÉXICO
e300108 | DOI: 10.46842/ipn.cien.v30n1a08

ARTICLE

Detección y mitigación de ataques *evil twin* en redes inalámbricas: una revisión sistemática de la literatura

Detection and Mitigation of Evil Twin Attacks in Wireless Networks: A Systematic Literature Review

Andres **Santacruz Menendez** [1]
Joel **Caguasango León** [2]
Martha **Sevilla Abarca** [3]

Universidad Técnica de Ambato,
Facultad de Ingeniería en Sistemas,
Electrónica e Industrial,
Ambato, ECUADOR

[1] ORCID: 0009-0001-0389-499X / dsantacruz9748@uta.edu.ec
[2] ORCID: 0009-0002-1080-2771 / acaguasango8805@uta.edu.ec
[3] ORCID: 0000-0002-3928-4085 / marthaesevilla@uta.edu.ec

Recibido 20/04/2026, aceptado 05/06/2026, publicado 12/06/2026.

Resumen

La expansión de dispositivos IoT y redes inalámbricas ha aumentado significativamente la susceptibilidad a los ataques de suplantación de puntos de acceso, también llamados Evil Twin (ET). Este artículo ofrece un análisis sistemático de la literatura con el propósito de evaluar el estado actual en cuanto a la detección y minimización de esta amenaza. Las arquitecturas de defensa actuales fueron clasificadas mediante un estudio detallado de 30 investigaciones primarias. Los hallazgos muestran que el 73.33% de las propuestas se centran en la alta precisión algorítmica a través de la Inteligencia Artificial, sobrepasando con frecuencia el 95% de exactitud. No obstante, se detectaron brechas tecnológicas importantes: el 36.67% de las soluciones todavía produce falsos positivos a causa de cambios en el entorno físico (RSSI) y un 33.33% está supeditado a hardware adicional. Se concluye que el desarrollo futuro exige arquitecturas híbridas, autoadaptables y enfoques del lado del cliente (Client-side) para garantizar una latencia viable en estándares emergentes.

Palabras clave: ciberseguridad, evil twin, machine learning, redes inalámbricas, revisión sistemática, WI-FI.

Abstract

The proliferation of wireless networks and IoT devices has critically increased vulnerability to access point spoofing attacks, known as Evil Twin (ET). This paper presents a systematic literature review aimed at evaluating the state-of-the-art in detecting and mitigating this threat. Through a rigorous analysis of 30 primary studies, current defense architectures were categorized. The results reveal that 73.33% of the proposals prioritize high algorithmic precision through Artificial Intelligence, frequently exceeding 95% accuracy. However, critical technological gaps were identified: 36.67% of the solutions still generate false positives due to physical environment fluctuations (RSSI), and 33.33% rely on additional hardware. It is concluded that future development demands hybrid, self-adaptive architectures and Client-side approaches to guarantee viable latency in emerging standards.

Index terms: cybersecurity, evil twin, machine learning, wireless networks, systematic review, Wi-Fi.

I. Introducción

En la actualidad, la ubicuidad de las redes de área local inalámbricas (WLAN) bajo el estándar IEEE 802.11 ha transformado la conectividad global en entornos públicos, industriales y domésticos. No obstante, esta expansión ha incrementado la superficie de ataque, posicionando a la infraestructura inalámbrica como el primer objetivo de intrusión para ciberadversarios. Entre las amenazas más críticas se encuentra el ataque de punto de acceso malicioso o *Evil Twin* (ET), el cual se fundamenta en la suplantación de un nodo legítimo mediante la clonación de su identificador de conjunto de servicios (SSID) y dirección MAC [11], [19]. A través de esta técnica, el atacante establece una posición de *Man-in-the-Middle* (MitM) que le permite interceptar tráfico sensible y ejecutar la recolección de credenciales mediante portales cautivos fraudulentos [3], [25].

Investigaciones recientes sugieren que, a pesar de la implementación del estándar *Wi-Fi Protected Access 3* (WPA3) y el uso de tramas de gestión protegidas (802.11w), el ataque *Evil Twin* (ET) sigue siendo efectivo mediante el forzado de roaming silencioso [4] y ataques de desautenticación en dispositivos legados [21]. El estado del arte actual presenta una polarización en las estrategias de defensa: por un lado, se proponen soluciones basadas en el análisis de parámetros temporales como el *Round-Trip Time* (RTT) y la carga de tráfico [1]; por otro, emerge con fuerza el uso de inteligencia artificial mediante modelos de *k-Nearest Neighbors* (KNN) y *Random Forest* para clasificar anomalías en la fuerza de la señal (RSSI) y huellas digitales de radiofrecuencia [13], [18], [22].

El problema fundamental radica en la confianza implícita de los dispositivos cliente hacia los parámetros de las capas física (PHY) y de enlace, los cuales carecen de mecanismos de autenticación mutua robustos en redes abiertas o con configuraciones WPA2 deficientes. Aunque existen propuestas de detección basadas en *software* distribuido [6] y protocolos de baja latencia como SAP [26], la implementación masiva de estas soluciones se ve limitada por la sobrecarga computacional y la heterogeneidad de los dispositivos IoT. Esto plantea la siguiente interrogante de investigación: ¿cuáles son los métodos de detección y mitigación de ataques *Evil Twin* más eficaces y escalables documentados en la literatura científica entre 2021 y 2026?

El propósito de este trabajo es realizar una revisión sistemática de la literatura (SLR) bajo la metodología PRISMA 2020 para sintetizar y evaluar críticamente las tendencias tecnológicas en la detección de puntos de acceso fraudulentos. Mediante el análisis de 30 estudios de alto impacto, esta investigación busca identificar las métricas de rendimiento más precisas y las herramientas de *hardware* libre (ej. Raspberry Pi, NodeMCU) que facilitan el despliegue de sistemas de detección de intrusiones inalámbricas (WIDS) en redes contemporáneas, considerando un periodo de estudio comprendido entre 2021 y 2026 [2], [14], [20].

II. Metodología

La investigación se define como documental y descriptiva, con un enfoque cualitativo orientado al análisis de seguridad en redes inalámbricas [13]. Se implementó una revisión sistemática de literatura (SLR) bajo los estándares de la declaración PRISMA 2020 [31], asegurando así que el estudio sea transparente y sea replicable. Las etapas jerárquicas que se describen a continuación fueron la estructura del desarrollo de la investigación.

A. Experimental test rig

Esta fase implicó la definición del área de estudio y el establecimiento de las herramientas para recuperar información técnica en bases de datos con un alto impacto. Se planteó la pregunta: ¿qué formas de detectar ataques Evil Twin son las más escalables y eficaces, según lo documentado durante el periodo 2021-2026? Para encontrar la respuesta, se eligieron los repositorios Google Scholar e IEEE Xplore.

1) Cadena de búsqueda y depuración inicial

Para optimizar la sensibilidad de los resultados, se diseñó una cadena de búsqueda compleja: ((“Evil Twin” OR “Rogue Access Point”) AND (“Detection” OR “Mitigation”) AND (“WLAN” OR “Wi-Fi security”)). Esta etapa produjo un total de 60 registros iniciales. Tras la comparación de metadatos, se suprimieron 7 artículos duplicados, resultando en 53 estudios únicos para la fase de evaluación.

B. Criterios de selección y proceso de cribado

Se llevaron a cabo filtros sucesivos basados en la relevancia temática y la calidad técnica para perfeccionar la muestra y garantizar que únicamente artículos rigurosos desde el punto de vista experimental se incluyeran en el análisis. Para ello, se establecieron criterios de inclusión específicos: 1) Estudios primarios empíricos publicados entre 2021 y 2026; 2) Investigaciones que propongan arquitecturas o métodos directos de detección/mitigación de ataques Evil Twin en redes WLAN; y 3) Disponibilidad de texto completo en inglés o español. Por otro lado, los criterios de exclusión contemplaron: 1) Estudios secundarios o teóricos sin validación experimental; 2) Entornos de red no aplicables o enfocados exclusivamente en IoT sin contexto WLAN; y 3) Propuestas con un nivel de generalidad excesivo.

Para la evaluación de calidad y riesgo de sesgo, se priorizó la inclusión de artículos revisados por pares en bases de datos de alto impacto, garantizando que todos los estudios seleccionados presentaran métricas de rendimiento comprobables.

1) Fases de exclusión y muestra técnica final

El proceso de selección operó bajo una dinámica de revisión independiente. Los metadatos de los 53 estudios únicos fueron importados a la herramienta colaborativa Rayyan para un cribado estructurado. Durante esta fase inicial, dos revisores independientes leyeron los resúmenes y títulos, tras lo cual se eliminaron cinco registros; de esos, dos eran sobre temas no relacionados con el objetivo de investigación y tres eran estudios secundarios (revisiones). Cualquier discrepancia en los criterios de inclusión fue resuelta mediante debate y consenso directo entre ambos investigadores.

Más tarde, de los 48 informes que quedaban, se eliminaron 4 porque no había acceso al archivo PDF completo. Durante la etapa de idoneidad, se revisaron 44 artículos completos y se descartaron 14 registros por razones técnicas concretas fundamentadas en los criterios de exclusión: 6 por tratarse de entornos de red no relevantes, 4 por centrarse únicamente en IoT, 2 porque no tratan el ataque directamente y 2 debido a que sus propuestas son demasiado generales. Por último, se estableció una selección técnica de 30 artículos (consulte la Fig. 1)

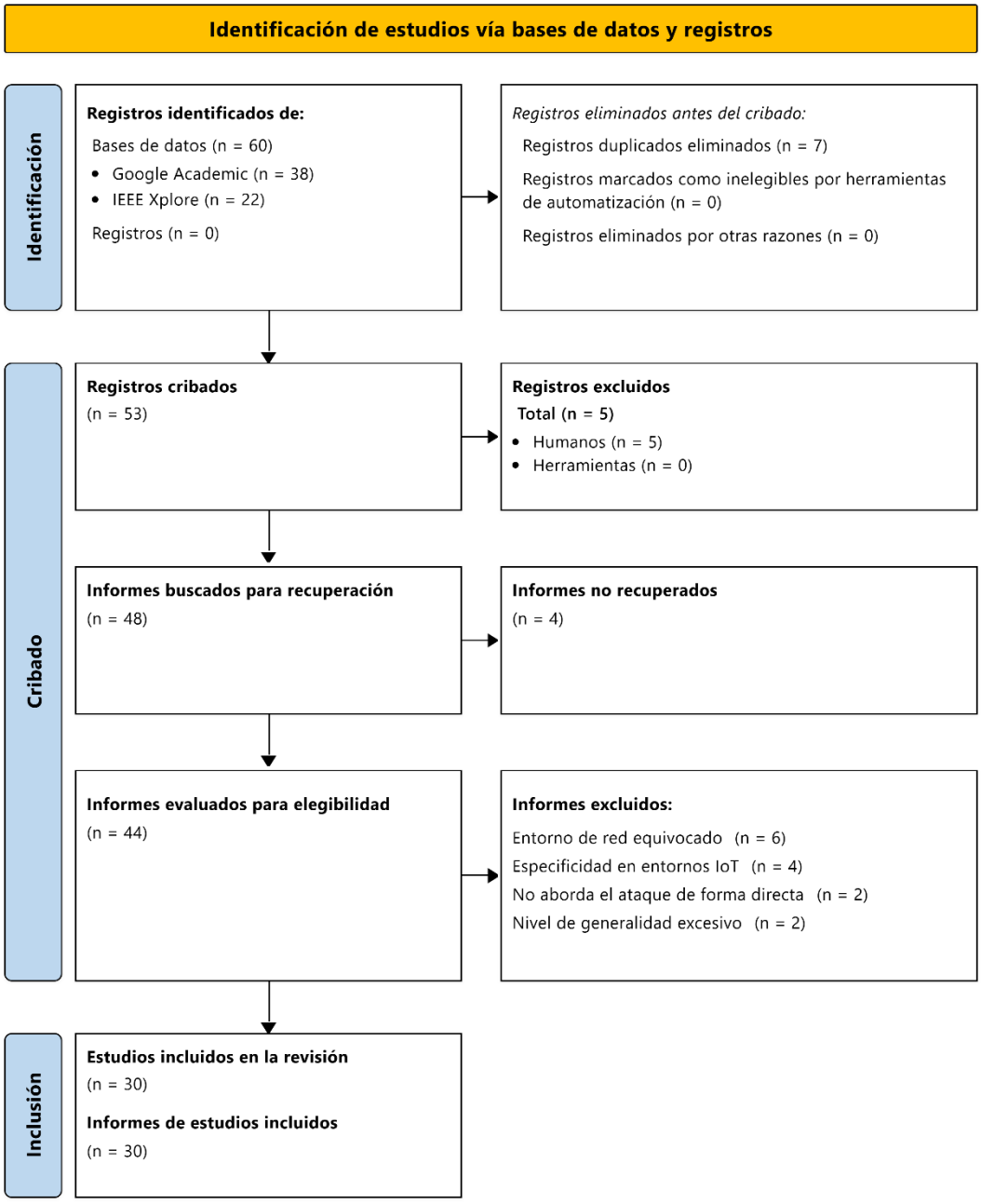

Fig. 1. Diagrama de flujo PRISMA para la selección de estudios.

Científica, vol. 30, no. 1, pp. 01-14, January-June 2026,
ISSN 2594-2921, Instituto Politécnico Nacional, México
e300108 | DOI: 10.46842/ipn.cien.v30n1a08

2) Extracción y clasificación de la información

Para sistematizar la información de la muestra técnica final, se diseñó una matriz de extracción de datos estandarizada. De cada uno de los 30 artículos se extrajeron las siguientes variables: autor(es) y año de publicación, país o región de origen de la propuesta empírica, técnica principal implementada, y los resultados o aportes clave reportados. Posteriormente, para facilitar la síntesis temática, la información extraída fue clasificada en tres categorías funcionales de defensa: 1) Detección en el Lado del Cliente (Client-side); 2) Inteligencia Artificial y Machine Learning; y 3) Monitoreo de Red, WIDS y Auditoría de Protocolos.

III. RESULTADOS

A continuación, se presentan los resultados logrados después del análisis sistemático de la bibliografía que se considera relevante para identificar y reducir ataques Evil Twin se muestran a continuación. Se percibe un aumento en las investigaciones publicadas entre 2023 y 2024 en la totalidad de la muestra seleccionada (30 publicaciones científicas), lo que se relaciona con el cambio global hacia la norma de seguridad WPA3 y el crecimiento de redes IoT. Además, la mayor parte de sugerencias experimentales viene de las zonas de Europa y Asia, resaltando el progreso de algoritmos de detección en el borde de la red. La Tabla 1 presenta la base empírica de esta revisión y muestra todos los artículos examinados, además de sus autores, el enfoque metodológico utilizada y la principal métrica de éxito reportada.

TABLA 1
PUBLICACIONES LITERARIAS SELECCIONADAS (MUESTRA TOTAL).

Núm.	Título de la investigación	Autor(es) y Año	País o Región	Técnica Principal	Resultados y Aportes Clave
1	*A Client-Side Evil-Twin Attack Detection System*, **[1]**	Ueda, T. et al. (2023)	Alemania	RTT (Tiempo de ida y vuelta) con umbral adaptativo.	Mejora de los criterios de detección asumiendo la congestión de la red.
2	*A Lightweight Frame-Based Wireless Intrusion...*, **[2]**	S. M. et al. (2026)	No especificado	Análisis a nivel de tramas MAC, variaciones de señal) sin ML.	Precisión >97% y latencia <1s; ideal para dispositivos IoT.
3	*A New Approach to Disabling SSL/TLS*, **[3]**	Kimura, K. et al. (2023)	Japón	Explotación de portal cautivo y redirección a motores falsos.	Anulación exitosa de SSL/TLS y HSTS sin alertas al usuario.
4	*Evil Twin MiTM through 802.11v protocol...*, **[4]**	Louca, C. et al. (2023)	Chipre	Explotación de tramas BSS Transition Management (802.11v).	Forzado de roaming silencioso independiente de la potencia de señal.
5	*A Robust Certificate Management System...*, **[5]**	Daldoul, Y. et al. (2020)	Túnez e Indonesia	RCMS y Autenticación 802.1X.	Protección total y rechazo de certificados de servidor no autorizados.
6	*A distributed and cooperative signature-based...*, **[6]**	Thankappan, M. et al. (2024)	España e India	DC-SWIDS, Firmas de ataque (CSA, Jamming) y MQTT.	Precisión promedio del 98% en ataques multi-canal (FragAttacks).
7	*An Active User-Side Detector for Evil Twins*, **[7]**	Hsu, F. H. et al. (2022)	Taiwán	AWPD basado en reglas de retransmisión TCP/IP.	Detección activa sin requerir hardware adicional o dispositivos asistentes.
8	*An Intelligent Rule-Based System for Detecting...*, **[8]**	Naik, D. B. et al. (2025)	No especificado	Framework basado en reglas deterministas y perfiles de señal.	Alta precisión de detección con baja demanda computacional para PYMES.

Científica, vol. 30, no. 1, pp. 01-14, January-June 2026,
ISSN 2594-2921, Instituto Politécnico Nacional, MÉXICO
e300108 | DOI: 10.46842/ipn.cien.v30n1a08

9	*Security Analysis of Evil Twin Attacks*, **[9]**	Rahman, R. et al. (2026)	Bangladesh	Penetration testing experimental con Aircrack-ng y RCMS.	Identifica interceptación de tráfico HTTP/HTTPS y valida certificados.
10	*Client-side Evil-Twin access point detection...*, **[10]**	Wakhloo, A. et al. (2023)	Irlanda	Análisis de RSSI, retardo de tramas Beacon y desviación del OUI.	Determinación efectiva mediante la inconsistencia de MAC y Timestamp.
11	*Data Mining Approach for Evil Twin Attack...*, **[11]**	Banakh, R. et al. (2024)	Ucrania y EE. UU.	KNN, Algoritmo generativo de RSSI y triangulación.	Identificación exitosa basada en huellas digitales del espectro (100%).
12	*Deauthentication Attacks, Rogue and Fake...*, **[12]**	Myrtaj, E. et al. (2024)	Bélgica	Fingerprinting de Capas MAC/PHY y Sniffing con Scapy.	Mitigación en tiempo real de deautenticación con alertas vía Telegram.
13	*Detection using autonomous sensors*, **[13]**	Banakh, R. et al. (2023)	Ucrania	Sensores autónomos (Raspberry Pi + Alfa) y clasificación KNN.	Logra 100% de precisión en entornos controlados mediante triangulación.
14	*DPETAs: Detection and Prevention of Evil Twin...*, **[14]**	Rofoo, F. F. H. et al. (2020)	Irak e India	Parámetros de configuración BSSID y cálculo de fórmula FSPL.	Localización física del atacante mediante atenuación de energía radio.
15	*Enhanced Detection of Evil Twin Attacks...*, **[15]**	Nanayakkara, J. et al. (2024)	Sri Lanka	Clasificador Random Forest con selección de rasgos AWID2.	El algoritmo Random Forest logró una precisión del 99.9186%.
16	*EvilSpot: Detection and Mitigation in Multi Channel*, **[16]**	Ahadi, S. A. A. et al. (2023)	India	Algoritmo multicanal, distribución de prefijos IP y listas blancas.	Detecta BSSID no autorizados y bloquea tramas de deautenticación.
17	*FakeAP Detector: An Android-Based Client-Side...*, **[17]**	Mwinuka, L. J. et al. (2022)	Tanzania	Análisis de Probe Responses, RSSI y seguridad en Android.	Precisión del 99.7% en redes cerradas sin requerir permisos root.
18	*Feature Selection in Wireless Intrusion...*, **[18]**	Kamble, A. et al. (2023)	India	Clasificador Random Forest con algoritmo Gini Index.	Precisión de detección del 99.99% utilizando el dataset AWID3.
19	*Implementación y evaluación de un prototipo MITM*, **[19]**	Yulán Mendoza, L. et al. (2025)	Ecuador y España	Simulación con Kali Linux, Airgeddon y estándares NIST.	92% de usuarios ingresó credenciales en 15-19 segundos; fragilidad WPA2.
20	*Mobile Proxy framework for privacy*, **[20]**	Xhemajli, A. et al. (2024)	No especificado	Proxy móvil en Raspberry Pi con túneles VPN.	Mejora la privacidad del usuario y reduce la severidad MitM (CVSS).
21	*Performing Man in the Middle Attacks Within a...*, **[21]**	Buckle, R. et al. (2023)	Reino Unido	Envenenamiento ARP, desautenticación y clonación con BeEF.	Intercepción exitosa; evalúa ineficacia frente al estándar 802.11w.

Científica, vol. 30, no. 1, pp. 01-14, January-June 2026,
ISSN 2594-2921, Instituto Politécnico Nacional, México
e300108 | DOI: 10.46842/ipn.cien.v30n1a08

22	*PHYSICAL LAYER AUTHENTICATION: MITIGATING...*, **[22]**	Tafoor, M. W. et al. (2025)	Reino Unido	RF Fingerprinting, NESDR mini 2 SDR y análisis FFT.	Autenticación basada en imperfecciones de fabricación del hardware.
23	*Public Wi-Fi security threat evil twin attack...*, **[23]**	Ahadi, S. A. A. et al. (2022)	India	Sistema 'ETDetector' basado en RSSI y recuento de saltos.	Detección efectiva mediante huellas de AP difíciles de replicar.
24	*Real-Time Detection of Rogue Wi-Fi Hotspots...*, **[24]**	Yusuf, S. L. et al. (2024)	No especificado	Association Rule Mining (ARM) integrado con análisis de comportamiento.	Identifica relaciones ocultas entre potencia de señal y tiempos de conexión.
25	*Rogue Access Points and Their Impact on Networks*, **[25]**	Belmokhtar, S. et al. (2025)	Estados Unidos	Análisis cualitativo y experimental de credential harvesting.	Analiza riesgos en infraestructura crítica y la importancia de túneles TLS.
26	*SAP: A Secure Low-Latency Protocol for Mitigating...*, **[26]**	Jain, V. et al. (2023)	Alemania, India y Francia	Protocolo SAP, Criptografía de Curva Elíptica (ECC) y AES-CCMP.	Baja sobrecarga computacional; mitiga overhead en redes industriales.
27	*Security Risks from the Modern Man-in-the-Middle...*, **[27]**	Cekerevac, Z. et al. (2025)	Serbia, Rusia e Irak	Revisión sistemática de ataques MITM y vulnerabilidades BLE.	Revela vulnerabilidades arquitectónicas en Bluetooth 5.4 (BLUFFS).
28	*Smart Cyber Defense: Machine Learning Powered...*, **[28]**	Kaya, M. et al. (2024)	Turquía	Dataset Wi-ADS con clasificadores optimizados LGBM y RF.	El clasificador LightGBM logró una precisión del 96.39%.
29	*Optimization of attack scripts for robustness*, **[29]**	Augustyniak, A. et al. (2024)	No especificado	Optimización de scripts de ataque desde perspectiva del adversario.	Propone mejoras en la robustez de los WIDS mediante sintonización.
30	*WPFD: Active User-Side Detection of Evil Twins*, **[30]**	Hsu, F. H. et al. (2022)	Taiwán y China	WPFD basado en handshake de 3 vías TCP/IP.	Tasa de verdaderos positivos del 100% incluso con señales débiles (RSSI 45%).

A. Síntesis temática y categorización técnica

Con el fin de brindar un entendimiento estructurado del estado actual del arte, se dividió la muestra documental en tres categorías funcionales que caracterizan las arquitecturas de defensa vigentes. Como se muestra en la Tabla 2, el estudio indica que la mayoría de las investigaciones se enfocan en soluciones del lado de la red y en auditoría de protocolos (Network-side), después de estas vienen las implementaciones predictivas fundamentadas en Inteligencia Artificial y los métodos reactivos dirigidos al usuario final (Client-side).

TABLA 2
SÍNTESIS TEMÁTICA DE LOS ENFOQUES DE DETECCIÓN ET.

Categoría técnica y enfoque	Referencias asociadas	Características Principales (Ventajas – Desventajas)
Detección en el Lado del Cliente (Client-side) **(Análisis de tráfico y retransmisión desde el usuario)**	[1], [7], [10], [17], [30]	**Ventaja:** Independencia total de la infraestructura de red; no requiere la instalación de hardware adicional o sensores. **Limitación:** Depende de los recursos del dispositivo final (batería, procesamiento) y puede requerir permisos específicos en sistemas operativos móviles.
Inteligencia Artificial y Machine Learning ***(Clasificación predictiva de señales y tráfico)***	[11], [13], [15], [18], [24], [28]	**Ventaja:** Tasas de precisión superiores al 95% y capacidad de adaptación dinámica frente a atacantes que cambian sus firmas de radiofrecuencia. **Limitación:** Alto costo computacional para el procesamiento en tiempo real y fuerte dependencia de *datasets* exhaustivos (como AWID) para evitar falsos positivos.
Monitoreo de Red, WIDS y Auditoría de Protocolos ***(Sistemas distribuidos y análisis de capa física/enlace)***	[2], [3], [4], [5], [6], [8], [9], [12], [14], [16], [19], [20], [21], [22], [23], [25], [26], [27], [29]	**Ventaja:** Visión global del ecosistema inalámbrico, protección centralizada y capacidad de auditar vulnerabilidades críticas en estándares vigentes (802.11v, WPA2/3, TLS). **Limitación:** Alta susceptibilidad a fluctuaciones ambientales (obstáculos que alteran el RSSI) y necesidad de hardware dedicado (sondas, Raspberry Pi) para cobertura total.

B. Beneficios y métricas de rendimiento

Con base en los estudios analizados, se determinaron y organizaron las ventajas competitivas de cada propuesta técnica. Los beneficios clave que se han encontrado en la muestra documental se resaltan en la figura 2. El estudio del corpus mostró que el 73.33% (n=22 de 30 estudios) de las investigaciones consideraron la Alta Precisión y la Tasa de Detección Exacta como su mayor beneficio, logrando frecuentemente niveles por encima del 95%, e incluso llegando al 100% en situaciones controladas de laboratorio. En segundo lugar, el 13.33% (n=4 de 30 estudios) destacó la independencia de infraestructura, lo que posibilitó la detección sin hardware adicional en la red (enfoque del lado del cliente). El resto de la muestra priorizó el bajo costo y latencia (10.00%, n=3) y la escalabilidad (3.33%, n=1). Estos hallazgos evidencian que, aunque el objetivo principal es la precisión algorítmica, se está mostrando un interés cada vez mayor en soluciones autónomas y descentralizadas.

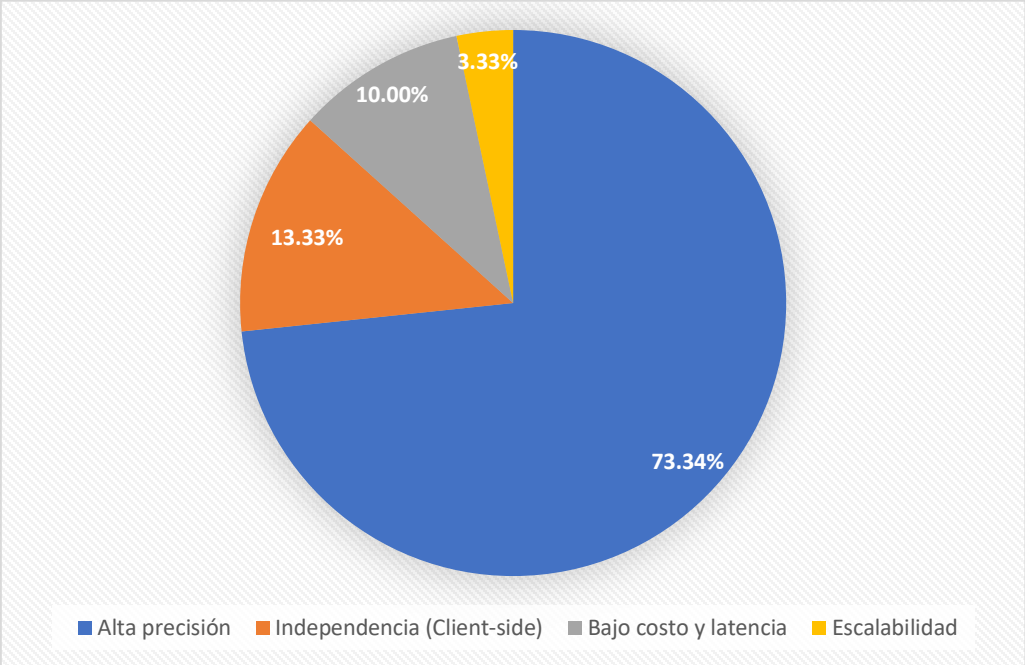

Fig. 2. Beneficios y métricas de rendimiento predominantes en la literatura.

C. Limitaciones técnicas y desafíos

Aunque se registraron índices de detección elevados, se encontraron obstáculos significativos para poner en práctica estas defensas y riesgos importantes. Como se muestra en la figura 3, el principal impedimento sigue siendo la dependencia del entorno físico y la producción de falsos positivos (debido a que los obstáculos o el movimiento provocan cambios en la señal RSSI), según lo informaron el 36.67% (n=11 de 30 estudios) de los autores. Además, el 33.33% (*n*=10 de 30 estudios) de las soluciones necesita sensores o hardware adicionales para la supervisión distribuida, lo que aumenta de manera significativa los costos de implementación a gran escala. Por último, la sobrecarga computacional (16.67%, *n*=5) tiene un impacto negativo considerable en los modelos predictivos de aprendizaje profundo que operan en tiempo real, mientras que una minoría (13.33%, n=4) reportó susceptibilidad a técnicas modernas de evasión.

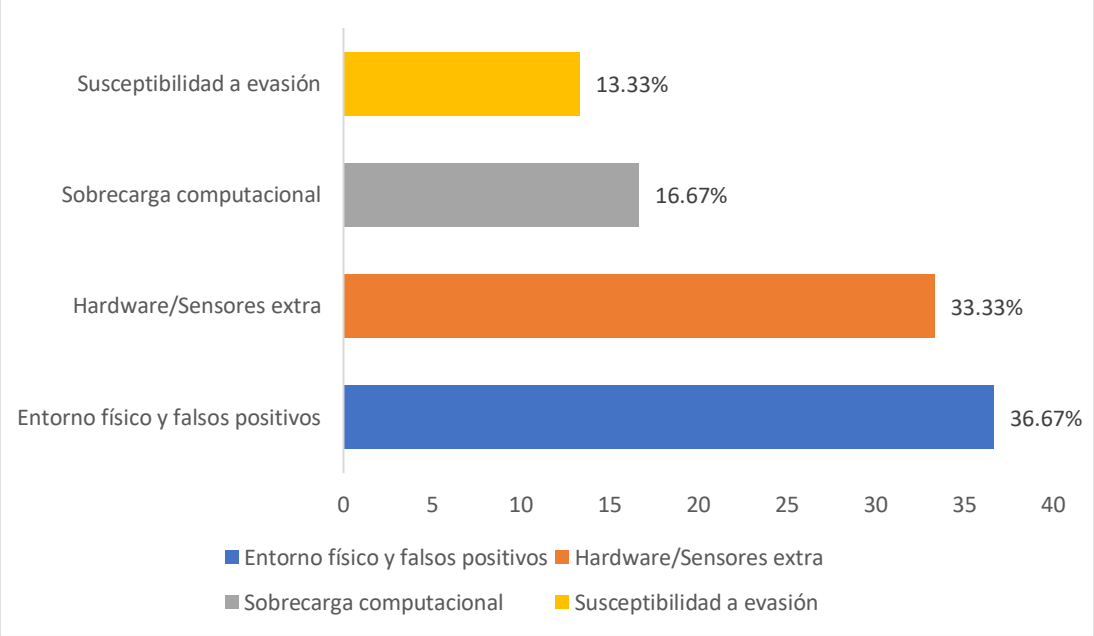

Fig. 3. Principales limitaciones técnicas identificadas en las propuestas de detección.

IV. Discusión

Una minuciosa revisión sobre la literatura actual acerca de la detección de ataques Evil Twin (ETA) muestra un panorama tecnológico disperso, en el cual los investigadores luchan entre la precisión algorítmica y la factibilidad operativa en redes reales. Se examinan a continuación las disparidades más importantes, los huecos tecnológicos no cubiertos y las proyecciones futuras en esta área.

A. El debate central: complejidad vs. ligereza

La cuestión principal en la literatura contemporánea es si usar modelos complejos de Machine Learning (ML) o soluciones ligeras (Lightweight) del lado del cliente. Por un lado, se sostiene que las metodologías tradicionales de ML exigen una carga alta en términos de infraestructura y computación, lo cual restringe su uso en ecosistemas periféricos o PYMES, por lo que los sistemas basados en reglas deterministas son más adecuados [8]. Las propuestas del lado del cliente apoyan fuertemente esta preferencia por la independencia en la infraestructura, sosteniendo que los métodos de servidor impiden que el usuario final verifique la legitimidad del punto de acceso [10]. En este contexto, las soluciones que se operan directamente desde el dispositivo del usuario resultan ideales, pues no necesitan la asistencia del operador de la WLAN ni el rastreo de IP por medio de puertas de enlace [7]. Además, una parte significativa de la investigación apoya el empleo requerido de la Inteligencia Artificial, evidenciando que, bajo condiciones experimentales y con conjuntos de datos específicos, algoritmos de clasificación multiclase como Random Forest obtienen precisiones sobresalientes que superan el 99.91% [15], y que iteraciones optimizadas como LightGBM llegan al 96.39%. Así, se justifica la carga de procesamiento a cambio de una considerable disminución en la vulnerabilidad [28].

B. Brechas de investigación y limitaciones físicas

A pesar de los avances algorítmicos, el problema crítico que la literatura admite como no resuelto es la alta tasa de falsos positivos derivados de las fluctuaciones físicas del entorno. La propagación de ondas de radio y la métrica de intensidad de señal (RSSI) dependen de factores incontrolables como la atenuación, la propagación multitrayecto, la reflexión y la dispersión, lo que dificulta que los sensores diferencien una falsificación MAC de un cambio ambiental legítimo [11]. En entornos dinámicos, estas obstrucciones físicas distorsionan las señales de radiofrecuencia, conduciendo inevitablemente a falsas alarmas [22]. Adicionalmente, emerge una brecha crítica en el rendimiento de los nuevos estándares: a medida que los protocolos aumentan su robustez criptográfica (como en WPA3), se produce un aumento significativo en la latencia computacional, degradando el rendimiento de sistemas críticos como el Internet de las Cosas Industrial (IIoT) [26]. Sumado a esto, se ha demostrado que los atacantes modernos logran evadir defensas tradicionales explotando vectores previamente considerados seguros, como la manipulación silenciosa de tramas de gestión de transición BSS en el protocolo IEEE 802.11v [4].

C. Direcciones futuras

Para mitigar estas deficiencias, la academia propone dos grandes directrices tecnológicas. En primer lugar, se recomienda la integración de Inteligencia Artificial dinámica y autoadaptable. En lugar de depender de perfiles de tráfico estáticos, los sistemas futuros deben incorporar técnicas avanzadas de ML que se adapten a topologías de red complejas [24], fusionando la identificación por radiofrecuencia (RF fingerprinting) con modelos de Deep Learning para contrarrestar métodos de ofuscación sofisticados [22]. En segundo lugar, se plantea la transición hacia arquitecturas distribuidas y nuevos estándares. Resulta imperativo que los marcos de detección evolucionen hacia módulos instalables en ecosistemas de domótica para proteger el borde del IoT [6], así como el diseño de sistemas analíticos basados en la nube que garanticen una integración nativa y retrocompatible con estándares emergentes como Wi-Fi 6 y Wi-Fi 6E [12].

D. Limitaciones del estudio

Es importante reconocer ciertas limitaciones en la presente revisión sistemática. En primer lugar, el sesgo de selección de bases de datos, dado que la búsqueda se limitó principalmente a IEEE Xplore y Google Scholar, excluyendo repositorios de pago cerrados. En segundo lugar, se excluyeron 4 estudios relevantes por restricciones de acceso al texto completo. Finalmente, aunque la revisión abarcó literatura de diversas regiones a nivel global, el corpus analizado se concentró predominantemente en publicaciones en inglés y español, lo que podría representar un sesgo idiomático parcial frente a la totalidad de la producción científica en otros idiomas nativos.

V. CONCLUSIONES

Esta revisión sistemática de la literatura muestra que se ha producido un cambio importante en la identificación y reducción de ataques Evil Twin, pasando de realizar análisis perimetrales simples a contar con ecosistemas de seguridad predictiva. El estudio de la muestra revela una dicotomía tecnológica contemporánea: la industria se encuentra en una lucha entre poner en marcha modelos de Inteligencia Artificial que, de acuerdo con los resultados reportados por los autores en los estudios analizados, proporcionan precisiones por encima del 99% en ambientes controlados, pero requieren un elevado costo computacional y generar soluciones ligeras del lado del cliente (Client-side), las cuales son ideales para contextos con recursos escasos. La alta vulnerabilidad a la generación de falsos positivos debido a las variaciones físicas de las señales de radiofrecuencia (RSSI) en contextos dinámicos continúa siendo el reto más persistente, aun con estos progresos. Por ende, se concluye que la trayectoria de la seguridad en redes inalámbricas, sobre todo frente al crecimiento del Internet de las cosas y a los nuevos estándares como WPA3 y Wi-Fi 6, no se

basará en una sola tecnología. En cambio, dependerá del progreso de arquitecturas híbridas y autoadaptables que consigan balancear la precisión algorítmica profunda con una latencia operativa factible.

CRediT (*Contributor Roles Taxonomy*)

Contribuciones de los autores: Conceptualización: DA**SM**; Metodología: DA**SM**, AJ**CL**, ME**SA**; Investigación: DA**SM**, AJ**CL**; Análisis formal: DA**SM**, AJ**CL**; Redacción y preparación del borrador original: DA**SM**; Redacción, revisión y edición: DA**SM**, AJ**CL**, ME**SA**; Supervisión: ME**SA**; Adquisición de fondos: No aplica.

Financiamiento: Los autores declaran que no se requirió de adquisición de fondos para este estudio.

Declaración de disponibilidad de datos: Los datos analizados se encuentran integrados en la muestra documental dentro del artículo.

Agradecimientos: Los autores desean expresar su agradecimiento a la profesora Martha Esperanza Sevilla Abarca por su guía académica y metodológica en este proyecto. Adicionalmente, se agradece a la plataforma de Inteligencia Artificial generativa, Gemini, por haber brindado asistencia en la etapa de pulido del formato, estructuración del lenguaje y adaptación al manual de estilo. Es importante destacar que la investigación profunda, el análisis formal y la interpretación técnica de los resultados presentados son responsabilidad exclusiva de los autores humanos.

Conflicto de interés: Los autores declaran que no existe conflicto de interés.

REFERENCIAS

[1] T. Ueda, A. Saif, S. Miyata, M. Nakahara, A. Kubota, "A client-side evil-twin attack detection system with threshold considering traffic load," in *2023 IEEE 13th International Conference on Consumer Electronics - Berlin (ICCE-Berlin)*, 2023, pp. 68–69, doi: https://doi.org/10.1109/icce-berlin58801.2023.10375616

[2] S. Sudhakaran, et al., "A lightweight frame-based wireless intrusion detection system for resource-constrained networks," in *2026 8th International Conference on Intelligent Sustainable Systems (ICISS)*, 2026, pp. 1–8, doi: https://doi.org/10.1109/iciss67859.2026.11453957

[3] K. Kimura, Y. Shiraishi, M. Morii, "A New Approach to Disabling SSL/TLS: Man-in-the-Middle Attacks are still Effective," in *2023 Eleventh International Symposium on Computing and Networking (CANDAR)*, 2023, pp. 11–19, doi: https://doi.org/10.1109/candar60563.2023.00010

[4] C. Louca, A. Peratikou, S. Stavrou, "A novel Evil Twin MiTM attack through 802.11v protocol exploitation," *Comput. Secur.*, vol. 130, p. 103261, 2023, doi: https://doi.org/10.1016/j.cose.2023.103261

[5] Y. Daldoul, M. Berrima, "A robust certificate management system to prevent evil twin attacks in IEEE 802.11 networks," *Int. J. Inf. Technol.*, vol. 17, no. 6, pp. 3589–3599, 2025, doi: https://doi.org/10.1007/s41870-024-02008-4

[6] M. Thankappan, H. Rifà-Pous, C. Garrigues, "A distributed and cooperative signature-based intrusion detection system framework for multi-channel man-in-the-middle attacks against protected Wi-Fi networks," *Int. J. Inf. Secur.*, vol. 23, no. 6, pp. 3527–3546, 2024, doi: https://doi.org/10.1007/s10207-024-00899-9

[7] F.-H. Hsu, C.-H. Lee, C.-S. Wang, "An active user-side detector for evil twins," in *Smart Innovation, Systems and Technologies, Cham: Springer International Publishing*, 2023, pp. 153–158, doi: https://doi.org/10.1007/978-3-031-05491-4_16

[8] D. S. B. Naik, V. Dondeti, "An intelligent rule-based system for detecting evil twin attacks in wireless networks," in *2025 IEEE 17th International Conference on Computational Intelligence and Communication Networks (CICN)*, 2025, pp. 750–757, doi: https://doi.org/10.1109/cicn67655.2025.11368194

[9] R. Rahman, N. Ramli, A. P. Rahmadani, "Analisis keamanan jaringan Wi-Fi publik terhadap serangan evil twin," *Journal Riset Sistem Inf.*, vol. 3, no. 2, pp. 35–38, 2026, doi: https://doi.org/10.69714/vzqtrw67

[10] A. Wakhloo, "Client-side Evil-Twin access point detection using beacon-frame delay and wireless network parameter deviation," National College of Ireland, Dublin, 2023, available: https://norma.ncirl.ie/6555/

[11] R. Banakh, E. Nyemkova, C. Justice, A. Piskozub, Y. Lakh, "Data mining approach for evil twin attack identification in Wi-Fi networks," *Data*, vol. 9, no. 10, p. 119, 2024, doi: https://doi.org/10.3390/data9100119

[12] E. Myrtaj, et al., "Deauthentication attacks, rogue and fake wireless access points detection through fingerprinting," 2024, available: https://www.researchgate.net/profile/Ernando-Myrtaj/publication/384253853_Deauthentication_Attacks_Rogue_and_Fake_Wireless_Access_Points_Detection_Through_Fingerprinting.pdf

[13] R. Banakh, A. Piskozub, I. Opirskyy, "Devising a method for detecting 'evil twin' attacks on IEEE 802.11 networks (Wi-Fi) with KNN classification model," *East.-Eur. J. Enterp. Technol.*, vol. 3, no. 9 (123), pp. 20–32, 2023, doi: https://doi.org/10.15587/1729-4061.2023.282131

[14] F. F. H. Rofoo, M. G. Galety, N. Arulkumar, R. Maaroof, "DPETAs: Detection and prevention of evil twin attacks on WI-fi networks," in Lecture Notes in Electrical Engineering, Singapore: Springer Singapore, 2022, pp. 559–568, doi: https://doi.org/10.1007/978-981-16-9012-9_45

[15] J. Nanayakkara, et al., "Enhanced detection of evil twin attacks in public WI-fi networks using machine learning algorithms," in *2024 9th International Conference on Information Technology Research (ICITR)*, 2024, pp. 1–6, doi: https://doi.org/10.1109/icitr64794.2024.10857762

[16] S. A. A. Ahadi, T. Arora, V. Abrol, K. Sharma, "EvilSpot: Detection and mitigation in multi channel," in *2023 International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS)*, 2023, pp. 121–126, doi: https://doi.org/10.1109/icaecis58353.2023.10170047

[17] L. J. Mwinuka, A. Z. Agghey, S. F. Kaijage, J. D. Ndibwile, "FakeAP detector: An android-based client-side application for detecting WI-fi hotspot spoofing," *IEEE Access*, vol. 10, pp. 13611–13623, 2022, doi: https://doi.org/10.1109/access.2022.3146802

[18] A. Kamble, D. Kshirsagar, "Feature selection in wireless intrusion detection system for evil twin attack detection," in *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, 2023, pp. 1–5, doi: https://doi.org/10.1109/cisct57197.2023.10351382

[19] L. Yulán Mendoza, et al., "Implementación y evaluación de un prototipo MITM Evil Twin Attack," *Quitensis*, 2025, available: https://quitensis.com/index.php/home/article/view/33

[20] N. Xhemajli, Z. Tafa, "Mobile proxy in public WiFi networks: A tool against MITM attacks," in *2024 13th Mediterranean Conference on Embedded Computing (MECO)*, 2024, pp. 1–5, doi: https://doi.org/10.1109/meco62516.2024.10577803

[21] R. Buckle, "Performing man in the middle attacks within a wireless local area network," 2022, doi: https://doi.org/10.36227/techrxiv.21176347.v1

[22] M. W. Tafoor, "Physical layer authentication: Mitigating MitM and eavesdropping in public wlans," *Theses Journal*, vol. 3, no. 12, pp. 869–899, 2025, available: https://thesesjournal.com/index.php/1/article/view/1743

[23] S. A. A. Ahadi, et al., "Public Wi-Fi security threat evil twin attack detection based on signal variant and hop count," 2022, available: https://pubs.aip.org/aip/acp/article-abstract/2424/1/020002/2822329/Public-Wi-Fi-security-threat-evil-twin-attack

[24] S. L. Yusuf, et al., "Real-Time detection of rogue Wi-Fi hotspots using association rule mining and behavioral analysis," 2024, available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5233478

[25] S. Belmokhtar, "Rogue access points and their impact on networks," Cybersecurity Undergraduate Research Showcase, Old Dominion University, 2025, doi: https://doi.org/10.25776/H2C7-3166

[26] V. Jain, U. Wetzker, V. Laxmi, M. S. Gaur, M. Mosbah, D. Mery, "SAP: A secure low-latency protocol for mitigating high computation overhead in WI-FI networks," *IEEE Access*, vol. 11, pp. 84620–84635, 2023, doi: https://doi.org/10.1109/access.2023.3302529

[27] Z. Čekerevac, P. Cekerevac, L. Prigoda, F. Al-Naima, "Security risks from the modern man-in-the-middle attacks," *MEST J.*, vol. 13, no. 1, pp. 34–51, 2025, doi: https://doi.org/10.12709/mest.13.13.01.04

[28] M. Kaya, H. K. Kucukates, M. Demez, I. F. Kilincer, "Smart cyber defense: Machine learning powered intrusion detection in 802.11 networks," in *2024 8th International Artificial Intelligence and Data Processing Symposium (IDAP)*, 2024, pp. 1–7, doi: https://doi.org/10.1109/idap64064.2024.10710835

[29] P. Augustyniak, O. Rogowicz, P. Zwierzykowski, "Theoretical and practical aspects of the evil twin attack," *in Communications in Computer and Information Science*, Cham: Springer Nature Switzerland, 2024, pp. 224–236, doi: https://doi.org/10.1007/978-3-031-62843-6_23

[30] F. H. Hsu, et al., "WPFD: Active user-side detection of evil twins," *Appl. Sci.*, vol. 12, no. 16, p. 8088, 2022, available: https://www.mdpi.com/2076-3417/12/16/8088

[31] M. J. Page, et al., "The PRISMA 2020 statement: an updated guideline for reporting systematic reviews," *BMJ*, vol. 372, no. n71, 2021, doi: https://doi.org/10.1136/bmj.n71

Científica, vol. 30, no. 1, pp. 01-14, January-June 2026,
ISSN 2594-2921, Instituto Politécnico Nacional, México
e300108 | DOI: 10.46842/ipn.cien.v30n1a08