ISSN 1390-6712

MASKAY

Vol. 16, No.1

Revista MASKAY
Departamento de Eléctrica, Electrónica y Telecomunicaciones
Universidad de las Fuerzas Armadas ESPE

INFORMACIÓN DE CONTACTO

Revista MASKAY
Departamento de Eléctrica, Electrónica y Telecomunicaciones
Universidad de las Fuerzas Armadas ESPE

Av. Gral. Rumiñahui (S/N)
P. O. Box 17-15-243B
Sangolquí, Pichincha, Ecuador
e-mail: maskay@espe.edu.ec
Telf. +593 2 3989400 ext 1867

Presentación

El Departamento de Eléctrica, Electrónica y Telecomunicaciones de la Universidad de las Fuerzas Armadas ESPE, consciente de su gran responsabilidad con la sociedad, busca proponer e impulsar iniciativas orientadas a fomentar el desarrollo integral de la ingeniería eléctrica y electrónica en el Ecuador. Como resultado de este compromiso, nació en 2011 la revista Maskay. Esta revista sintetiza de forma documentada los esfuerzos de investigación y desarrollo que realizan los docentes, investigadores y estudiantes de la región.

En la actualidad, la revista MASKAY se encuentra indexada en diversas bases de datos: **SciELO-Ecuador**, **Latindex catálogo v2.0**, **LatAm-Studies** Estudios Latinoamericanos, **RootIndexing**, **MIAR** (Matriz de Información para el análisis de Revistas), **DOAJ** (Directory of Open Access Journals), **DRJI** Directory of Research Journals Indexing), **Dialnet** y **REDIB** (Red Iberoamericana de Innovación y Conocimiento Científico), con el objetivo de difundir a nivel internacional las publicaciones realizadas en esta revista. Además, para que exista una mejor divulgación de sus contenidos, la revista MASKAY cuenta con número **DOI (Digital Object Identifier)** legítimamente registrado y validado por **Crossref**, lo que permite una fácil localización de sus contenidos en la web.

Diego Arcos Avilés
Editor General

Presentation

The Department of Electrical, Electronics, and Telecommunications Engineering of the Universidad de las Fuerzas Armadas ESPE, aware of its great responsibility to society, seeks to propose and promote initiatives to foster the comprehensive development of electrical and electronic engineering in Ecuador. As a result of this commitment, the Maskay Journal was born in 2011. This journal presents the research and development efforts of the region's teachers/researchers and students.

Currently, the MASKAY Journal is indexed in several databases: **SciELO-Ecuador**, **Latindex catalog v2.0**, **LatAm-Studies** Estudios Latinoamericanos, **RootIndexing**, **MIAR** (Information Matrix for the Analysis of Journals), **DOAJ** (Directory of Open Access Journals), **DRJI** Directory of Research Journals Indexing), **Dialnet** and **REDIB** (Ibero-American Network of Innovation and Scientific Knowledge), to disseminate the publications in this journal internationally. In addition, to better disseminate its contents, the MASKAY Journal has a **DOI (Digital Object Identifier)** number, registered and validated by **Crossref**, which allows easy access to its contents on the web.

Diego Arcos Avilés
Editor-in-Chief

Contenido / Table of Contents

MASKAY 16(1), May 2026
ISSN 1390-6712

Recibido (Received): 2025/05/19
Aceptado (Accepted): 2025/08/19

Aplicación de la inteligencia artificial en el Internet de las Cosas: un estudio documental

Application of artificial intelligence in the Internet of Things: a documentary study

Gilma Mieles, Marlon Navia

***Abstract*— The convergence of the Internet of Things (IoT) and Artificial Intelligence (AI) has catalyzed substantial advancements across multiple sectors, including agriculture, security, healthcare, home automation, and resource management. This paper presents a systematic literature review aimed at identifying key applications, AI techniques, and benefits resulting from the integration of these technologies. The review process was conducted in accordance with the PRISMA methodology, encompassing publication selection, data extraction, and analysis. Out of 725 initially retrieved records, 53 studies were selected for detailed examination. The results indicate that multisensor systems represent 28.85% of the reported applications, followed by IoT security (21.15%) and smart cities (15.38%). In terms of AI techniques, multisensor data fusion was the most frequently employed (40.38%), followed by deep neural networks (19.23%) and support vector machines (15.38%). Most of the reviewed studies report accuracy levels of 90% or higher. These findings highlight the critical role of AI in enhancing IoT systems and identify the domains with the highest potential for future development.**

***Index Terms*—IoT, AI, machine learning, prediction algorithms.**

***Resumen*— La convergencia entre el Internet de las Cosas (IoT por sus siglas en inglés) y la Inteligencia Artificial (IA) ha impulsado avances significativos en diversas industrias, como la agricultura, la seguridad, la salud, la automatización del hogar y la gestión de recursos. Este artículo presenta una revisión sistemática de la literatura con el objetivo de identificar aplicaciones, técnicas y beneficios derivados de la integración de ambas áreas tecnológicas. Para ello se aplicó un proceso basado en la metodología PRISMA, que incluyó la selección de publicaciones, así como la extracción y el análisis de datos. Se seleccionaron 53 publicaciones de 725 encontradas en la búsqueda. Se identificó que los sistemas multisensoriales representan el 28.85% de las aplicaciones reportadas, seguidos por la seguridad en IoT con un 21.15% y las ciudades inteligentes con un 15.38%. En cuanto a técnicas de IA, la fusión de datos multisensoriales fue la más empleada (40.38%), seguida por redes neuronales profundas (19.23%) y máquinas de soporte vectorial (15.38%). La mayoría de los estudios analizados reportan precisiones iguales o superiores al 90%. Estos hallazgos evidencian el papel clave de la IA en la mejora de sistemas IoT y destacan las áreas con mayor potencial de desarrollo.**

Gilma Mieles and Marlon Navia are with the Facultad de Ciencias Informáticas, Universidad Técnica de Manabí, Portoviejo, Ecuador (e-mail: {gmieles1082, marlon.navia}@utm.edu.ec).

***Palabras Claves*—IoT, IA, aprendizaje automático, algoritmos de predicción.**

I. Introducción

El Internet de las Cosas se ha convertido en una tecnología indispensable en nuestras actividades cotidianas, y se ha posicionado como una herramienta fundamental para empresas, gobiernos y usuarios finales en sectores como los servicios, la agricultura y la salud [1], [2].

IoT se define como un paradigma que permite la conexión entre objetos, dispositivos, personas y sistemas mediante protocolos de comunicación y sensores inteligentes, posibilitando la interacción y el intercambio de datos en tiempo real entre todos ellos [3]. Su implementación, basada en sensores y dispositivos inteligentes interconectados, permite recopilar datos en tiempo real para optimizar procesos y mejorar la calidad de vida de los usuarios [4]. A pesar de su potencial, el IoT enfrenta desafíos relevantes en materia de seguridad, privacidad y escalabilidad [5].

Por otro lado, la IA se apoya en modelos computacionales que replican funciones cognitivas humanas, lo que facilita su integración en una amplia variedad de aplicaciones [6]. Una de las áreas emergentes más importantes es precisamente la convergencia entre IA e IoT. En este contexto, la IA proporciona la capacidad de análisis y aprendizaje que potencia la utilidad del IoT, mientras que el IoT proporciona los datos necesarios para el entrenamiento y operación de modelos inteligentes. Esta sinergia tecnológica ha demostrado ser especialmente útil en campos como la agricultura de precisión, la seguridad en redes de bajo consumo, el diagnóstico asistido por computadora en salud, y la automatización de procesos en hogares y ciudades inteligentes [7].

La integración de la IA y IoT está transformando numerosos sectores al proporcionar soluciones inteligentes, automatizadas y escalables. A medida que el IoT conecta dispositivos y recopila datos en tiempo real, la IA interpreta esta información para tomar decisiones más precisas, optimizar recursos y mejorar la experiencia del usuario. Los avances tecnológicos han permitido que estas innovaciones se apliquen en diversas áreas como la agricultura de precisión, la seguridad, la salud, las ciudades inteligentes y la gestión de economías colaborativas.

Este artículo presenta una revisión sistemática de literatura

DOI: 10.24133/maskay.v16i1.4161

basada en la metodología PRISMA, con el fin de identificar tendencias, aplicaciones y técnicas utilizadas en la implementación de IA dentro de sistemas IoT. Asimismo, se busca establecer una panorámica del estado del arte que permita visualizar las oportunidades de innovación y las brechas de investigación que aún persisten en la actualidad.

El resto del artículo está estructurado de la siguiente manera: la Sección 2 presenta un análisis de trabajos relacionados. En la Sección 3 se detalla la metodología aplicada en la investigación. La Sección 4 muestra tanto los resultados como el análisis de los mismos, y en la última sección se dan a conocer las conclusiones del artículo.

II. Trabajos Relacionados

Existen varios trabajos que combinan la IA con otras tecnologías. En esta sección se analizan algunos de estos trabajos y propuestas, especialmente en áreas donde es común la aplicación de IoT.

A. Agricultura y medio ambiente

El uso de IA y Vehículos Aéreos No Tripulados (UAV) en la gestión de incendios forestales, aplicando técnicas de aprendizaje automático, permite realizar un monitoreo avanzado, modelado predictivo y gestión eficiente de las estrategias antes, durante y después del incendio, mejorando la respuesta ante emergencias en este ámbito [8].

En sectores como medio ambiente, defensa e industria, se requiere la optimización de redes IoT para alertas eficientes, mejoradas mediante algoritmos heurísticos y variaciones de k-means sobre redes geodésicas [9].

El preprocesamiento de Big Data en excavaciones con TBM (Tunnel Boring Machine) es fundamental para mejorar la eficiencia de la construcción subterránea. Se han propuesto métodos para tratar datos erróneos y se ha desarrollado un programa para clasificar y limpiar los datos [10].

En la industria FoodBev (comida y bebida) se usa IA para promover sostenibilidad a través del análisis de datos y procesamiento de lenguaje natural [11].

En agricultura, modelos como IndoorPlant utilizan el historial contextual para predecir productividad y prevenir problemas [12]. Finalmente, en agricultura de precisión, el IoT y el aprendizaje automático ofrecen soluciones para mejorar rendimientos y reducir el uso de productos químicos [13].

Por otro lado, en gasoductos, se usa aprendizaje profundo con codificadores automáticos para detectar anomalías en datos de telemetría [14]. No obstante, el aprendizaje federado aún enfrenta desafíos como dispositivos maliciosos o diversidad de datos que dificultan su eficacia [15].

B. Seguridad y ciberseguridad

Ante la preocupación por la seguridad, se propone implementar marcos seguros con protocolos TLS/SSL y almacenamiento en la nube, como en hogares inteligentes con sensores programados en Arduino [4].

En este sentido, se ha propuesto el método SCDAM (Session Critical Distributed Authentication Method), una autenticación distribuida para redes de sensores IoT, basada en ECC (Elliptic Curve Cryptography), que mejora la seguridad ante ataques internos mediante sesiones breves, claves únicas y autenticación de extremo a extremo [16].

La ciberseguridad en IoT requiere soluciones inteligentes y de bajo consumo, como el uso de redes neuronales recurrentes (RNN, del inglés Recurrent Neural Networks) y detección de accesos a memoria fuera de rango [17]. En este sentido, se ha propuesto un mecanismo de detección y prevención de intrusiones en sistemas IoT mediante una arquitectura de seguridad inteligente basada en Redes Neuronales Aleatorias. Este sistema utiliza etiquetas de memoria y verificaciones en tiempo de compilación para detectar accesos a memoria fuera de límites, mejorando la protección ante ataques internos [18].

En este contexto, la integración de Blockchain (cadena de bloques) con IA descentralizada puede fortalecer la ciberseguridad, destacando sus beneficios en seguridad, privacidad y confianza, además de identificar retos, aplicaciones reales y futuras direcciones de investigación [19]. En el área de seguridad, se han implementado arquitecturas de detección de intrusiones basadas en GAN (Generative Adversarial Network) [20] y sistemas como AutoTag, que estima la frecuencia respiratoria mediante etiquetas RFID (Radio Frequency ID) y codificadores variacionales [21].

C. Salud y diagnóstico asistido

La salud digital en oftalmología ha avanzado notablemente, especialmente en el uso de inteligencia artificial para el diagnóstico del segmento ocular posterior, aunque todavía existe un escaso desarrollo en la atención visual primaria [18]. Los programas de salud digital son urgentes para acelerar la adopción de IA [22], lo cual fortalece la resiliencia en las cadenas de suministro [23].

En el área cardíaca, abundan aplicaciones que miden parámetros como fracción de eyección o gasto cardíaco [24].

Modelos como LSTM (Long Short-Term Memory) han demostrado mayor precisión que regresiones logísticas para predecir riesgos de asma, al considerar efectos acumulativos de PM (Particulate Matter) [25].

D. Ciudades inteligentes, hogares y visualización

El crecimiento del IoT implica más dispositivos conectados y más información generada. Esto permite sistemas de monitoreo y control en edificios inteligentes.

En este contexto, se ha desarrollado un modelo de control adaptativo para sistemas de iluminación inteligente basados en IoT, que ajusta la iluminancia según las preferencias del usuario, minimizando el consumo de energía a pesar de la incertidumbre en la ubicación de sensores y bombillas [26]. Así, por ejemplo, la IA aplicada al IoT genera decisiones automatizadas, como en los sistemas de iluminación adaptativa basados en sensores móviles y bombillas inteligentes [27], [28].

El diseño centrado en lo humano se ve fortalecido por herramientas como ThingCV, que visualiza redes sociales de objetos para contextos creativos como museos y hogares inteligentes [29]. El uso de memorias Magnetic Random Access Memory (MRAM) basadas en Magnetic Tunnel

Junction (MTJ) es ideal en IoT por su bajo consumo, alta velocidad y no volatilidad [30].

Se espera que estos dispositivos realicen interacciones humanas como reconocimiento de voz, visión y gestos, lo cual habilita la autenticación de usuarios y el control por gestos [31]. Esto ha impulsado aplicaciones en la construcción y conservación del patrimonio mediante gemelos digitales [32], en un contexto de transformación por la digitalización [33].

Asimismo, se ha desarrollado un marco basado en gemelos digitales (DT) y aprendizaje automático (ML) para predecir parámetros críticos en tiempo real en la industria de procesos, demostrando su eficacia en un caso práctico y destacando tanto su potencial como los desafíos de implementación [34].

E. Educación, rendimiento académico y aplicaciones sociales.

Se han desarrollado sistemas de gestión de asistencia con Raspberry Pi 3 y tecnología RFID, automatizando el registro escolar [35]. También se han explorado enfoques teóricos y prácticos para enseñar Tecnología Creativa en IoT, evaluando su impacto en la motivación y el aprendizaje de los estudiantes, y proponiendo mejoras educativas en este campo [36].

Además, se ha comprobado que factores como fracasos previos y la educación materna influyen significativamente en el rendimiento estudiantil, siendo el modelo MLP (Multilayer Perceptron) de 12 neuronas el más preciso para predecir dicho rendimiento [37], [38], con alta valoración en efectividad y aplicabilidad [39].

III. METODOLOGÍA

La metodología empleada en este estudio se basó en las directrices de PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses), lo cual permitió estructurar el proceso de revisión en tres fases principales: planificación, ejecución y redacción (Fig. 1). Como apoyo para la gestión de referencias y evaluación de artículos, se utilizó la herramienta Parsifal (https://parsif.al/).

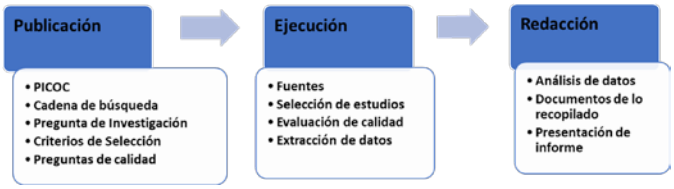


Fig. 1. Esquema del proceso de revisión.

A. Planificación

En primer lugar, se plantearon las preguntas de investigación (PI) que guiaron la investigación. Estas preguntas fueron las siguientes:

1) PI1 ¿En qué tipo de sistemas de Internet de las Cosas se ha aplicado la inteligencia artificial en los últimos años?
2) PI2 ¿Qué técnicas o estrategias de IA se han aplicado en estos sistemas?
3) PI3 ¿Qué beneficios se reportan en el Internet de las Cosas al aplicar la inteligencia artificial?

Posteriormente, se usó el método PICOC (Population, Intervention, Comparison, Outcome, Context) para definir nuestras palabras clave, tal como se muestra en la Tabla I.

TABLA I
PALABRAS CLAVE PARA LA BÚSQUEDA

Término	Palabras
Población	Internet of Things, IoT,
Intervención	Artificial Intelligence, machine learning, computational intelligence
Comparación	
Resultado	Artificial Intelligence, machine learning, computational intelligence
Contexto	

Con estos términos se elaboró la cadena de búsqueda: (“artificial intelligence” OR AI OR “intelligent machines”) AND (“internet of things” OR IoT) AND (“improvement” OR “system”).

Con base en la cadena de búsqueda se realizó una exhaustiva búsqueda en bases de datos académicas con términos clave. Concretamente se realizó la búsqueda en las bibliotecas de IEEEXplore, ACM Digital Library y Science@Direct por tener mayor cantidad de publicaciones relacionadas con el área de Tecnologías de la Información y Comunicación.

Los criterios de inclusión y exclusión mostrados en la Tabla II. Se procuró incluir artículos de calidad relacionados a la temática de estudio, por lo que se excluyeron publicaciones que no aportaban resultados originales. Se tomaron como periodo de investigación las publicaciones desde el año 2019 hasta el año 2024, para ver la evolución de la relación entre ambas áreas antes y después de la pandemia, así como la evolución de tecnologías como edge computing, aprendizaje federado y redes neuronales profundas, que han transformado el panorama de investigación en este dominio.

TABLA II
CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

Criterios de inclusión	Criterios de exclusión
Artículos publicados entre 2019 a 2024	Resúmenes, revisiones de literatura, capítulos de libros, editoriales
Artículos indexados en base de datos globales	Publicaciones en idiomas diferentes al inglés o español
	Otros tópicos diferentes al del estudio

En complemento, y con afán de determinar la suficiencia de los artículos elegidos, se plantearon las siguientes preguntas de evaluación de la calidad (PEC) de los trabajos:

- PEC1 ¿La investigación incluye una descripción técnica suficiente de la aplicación de IA?
- PEC2 ¿Se realizó una implementación (no solo simulación)?
- PEC3 ¿Se describe la mejora o beneficio al aplicar IA?

La Tabla III muestra las opciones de respuesta de las preguntas, y la puntuación asignada a cada respuesta. El

puntaje mínimo para que una publicación fuera considerada en el estudio fue de 1.5, con base en la puntuación de la Tabla III. Se consideró este valor para poder obtener información relevante de los estudios seleccionados.

TABLA III
PUNTUACIÓN DE LAS PEC

Respuesta	Puntuación
Si	1.0
Parcialmente	0.5
No	0.0

De los artículos seleccionados, se planteó extraer datos que permitan realizar los análisis planteados. Los datos que plantea extraer de cada documento son:

- Titulo
- Año
- Tipo de aplicación de IoT (PI1)
- Técnica o algoritmo de IA (PI2)
- Precisión/Exactitud de IA (PI3)
- Beneficio declarado del uso de IA (PI3)

Con base en los datos extraídos de las publicaciones seleccionadas, se realizó primero un análisis descriptivo, y posteriormente un análisis un poco más profundo de los hallazgos del estudio.

B. *Ejecución de la búsqueda*

La búsqueda se realizó de acuerdo con lo establecido en la etapa de planificación. En la Fig. 2, se detalla el proceso de selección de acuerdo con el método PRISMA, categorizado en tres fases: la identificación, el cribado y la inclusión final.

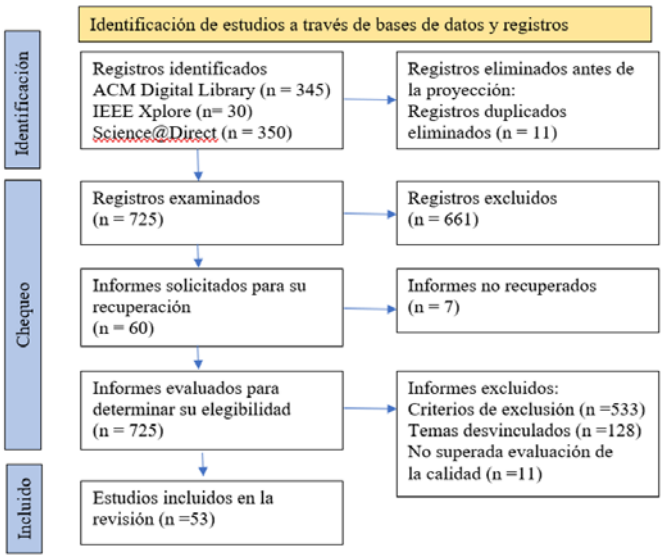


Fig. 2. Aplicación del flujo de proceso de selección PRISMA 2020.

En el apartado de identificación, se detallaron los registros iniciales y se realizó la revisión de duplicados; en el cribado, se examinaron y recuperaron los trabajos potenciales, que posteriormente son descartados de acuerdo con los parámetros pertinentes (criterios de exclusión, temas desvinculados y poca calidad de acuerdo con la evaluación de la misma). Finalmente, se obtuvo el número de registros o trabajos elegidos para la presente investigación.

C. *Redacción de resultados*

En la Fig. 3 se expone la relación entre los trabajos arrojados por la búsqueda inicial en las tres fuentes escogidas y la cantidad de publicaciones seleccionadas de cada fuente.

De manera similar, de acuerdo con el año de la publicación (Fig. 4), se nota un apogeo entre los años 2021 y 2022.

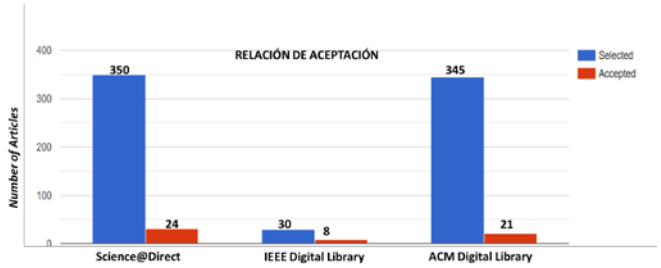


Fig. 3. Relación entre publicaciones encontradas y aceptadas en cada fuente.

Fig. 4. Publicaciones seleccionadas por año.

Inicialmente se identificaron 725 artículos. Tras eliminar duplicados, se procedió al cribado de acuerdo a los criterios de exclusión, y después por título y resumen. Luego, mediante lectura completa y aplicación del cuestionario de calidad (PEC), se seleccionaron finalmente 53 artículos relevantes para el análisis.

IV. RESULTADOS

Se identificó un total de 53 publicaciones que cumplían con los criterios de inclusión. A partir de estas, se analizaron las aplicaciones, técnicas y beneficios de la integración IA–IoT. A continuación, se presentan los resultados organizados en función de las tres preguntas de investigación:

A. *Tipo de Aplicación de IoT*

En la Tabla IV se muestran los tipos de aplicaciones encontradas en los estudios revisados. Se destacan los sistemas multisensoriales (28.85%) y la seguridad en IoT (21.15%) como los dominios más frecuentes, seguidos por hogares y ciudades inteligentes (15.38%) y la visualización de ecosistemas IoT (15.38%), mientras que las aplicaciones en economías de intercambio significaron un 9.62%, agricultura de precisión un 7.69%, y entrega de video optimizada un 3.85%.

TABLA IV
TIPOS DE APLICACIÓN DE IOT IDENTIFICADAS EN LOS ESTUDIOS

ID	Aplicaciones	Descripción	Referencias
A1	Agricultura de precisión	Uso de sensores para monitorear variables ambientales como temperatura, humedad y pH del suelo, optimizando riego y fertilización.	[38][11][12][13]
A2	Seguridad en IoT	Sistemas de detección de intrusiones (IDS) para proteger redes IoT de bajo consumo.	[5][6][40][41][17][19][30][39][20][14][15]
A3	Hogares y ciudades inteligentes	Automatización de hogares para optimizar energía, seguridad y confort.	[4][42][16][43][44][18][45][46]
A4	Sistemas multisensoriales	Simulación de sentidos humanos (vista, oído, tacto, etc.) mediante sensores IoT	[33][47][32][34][10][35][48][49][21][25][50][22][26][27][51]
A5	Economías de Intercambio	Uso de IoT para mejorar la logística y la interacción entre usuarios en modelos de economía compartida.	[2][52][53][54][28]
A6	Visualización de ecosistemas IoT	Representación de relaciones emergentes entre objetos cotidianos en redes IoT, facilitando el diseño y la integración.	[1][55][31][29][9][36][37]
A7	Entrega de video optimizada	Ajuste dinámico de resolución de video en tiempo real para garantizar calidad de servicio (QoS) en redes IoT.	[8][56]

La amplia representación de sistemas multisensoriales puede atribuirse a su aplicabilidad transversal, desde salud hasta manufactura, así como al desarrollo de tecnologías de sensores de bajo costo. La prominencia del área de seguridad refleja la preocupación creciente por la protección de redes distribuidas y dispositivos conectados.

B. Técnicas de IA aplicadas a sistemas IoT

En la Tabla V se exponen las principales técnicas de IA identificadas. La fusión de datos multisensoriales fue la más común (40.38%), seguida por redes neuronales profundas (DNN, del inglés Deep Neural Networks) (19.23%) y máquinas de soporte vectorial (SVM, del inglés Support Vector Machines) (15.38%).

El uso predominante de fusión de datos se explica por la capacidad de poder colocar varios sensores en los dispositivos que se conectan a una infraestructura IoT, pero también por la necesidad de combinar múltiples fuentes de entrada en sistemas IoT heterogéneos, como salud o ciudades inteligentes. Las DNN y SVM destacan por su capacidad de modelar patrones complejos, especialmente en seguridad y agricultura de precisión.

TABLA V
TÉCNICAS DE IA APLICADAS EN SISTEMA IOT

ID	Aplicaciones	Descripción	Referencia
B1	Máquinas de Soporte Vectorial	Clasificación de datos no lineales en sensores IoT. Análisis predictivo para enfermedades o anomalías en cultivos (agricultura de precisión). Detección de ataques o anomalías en entornos de red (seguridad en IoT).	[17][37][49][25][14][15][13][45]
B2	Redes Neuronales Profundas	Utilizadas para detectar patrones complejos en seguridad IoT y análisis de video.	[1][41][55][8][34][36][18][22][26][56]
B3	Aprendizaje por refuerzo	Implementado en economías de intercambio para optimizar decisiones en entornos dinámicos.	[2][4][53][31]
B4	Aprendizaje federado	Colaboración de dispositivos IoT para entrenar modelos globales sin compartir datos sensibles.	[54][19][20]
B5	Fusión de datos multisensoriales	Combinación de información de diferentes sensores IoT para mejorar la precisión en la toma de decisiones.	[40][33][52][42][29][30][47][32][9][10][35][38][48][11][12][21][50][23][27][46][51]
B6	Lógica difusa	Ayudan a modelar relaciones complejas entre variables	[5][6][16][39][43][44]

C. Precisión de IA aplicados en los sistemas IoT

La Tabla VI presenta los niveles de precisión informados por los estudios. En aquellas publicaciones que aplicaron DNN, se reportan valores de precisión de hasta 96,7%; mientras que las aplicaciones que emplearon SVM alcanzan un 96%. Otros enfoques, como aprendizaje federado y lógica difusa, obtuvieron alrededor del 95% en contextos específicos.

TABLA VI
PRECISIÓN DE LOS MODELOS APLICADOS

ID	Aplicaciones	Precisión	Referencia
B1	Redes Neuronales Profundas	96.7%	[41][55][17][8][34][36][49][22][13][56]
B2	Máquinas de Soporte Vectorial	96%	[37][25][14][15]
B3	Aprendizaje por Refuerzo	N/D	N/D
B4	Aprendizaje Federado	95%	[4][54][20]
B5	Fusión de Datos Multisensoriales	90%	[33][10][11]
B6	Lógica difusa	95.10%	[6][16][39]

Estos resultados evidencian que, si bien técnicas como DNN y SVM son robustas en cuanto a rendimiento, su uso está condicionado por el alto requerimiento computacional, lo que puede limitar su implementación en dispositivos IoT de bajo consumo. Por ello, otras técnicas como la lógica difusa o la fusión de datos se emplean cuando se privilegia la eficiencia energética o la interpretabilidad. Por otro lado, llama la atención que la técnica más aplicada en los estudios analizados, la fusión de datos multisensoriales, es la que menos precisión tiene entre las analizadas en la Tabla VI.

D. Matriz de aplicación cruzada

La Tabla VII muestra una matriz de cruce entre tipos de aplicación y técnicas de IA. Se observa que la técnica de fusión multisensorial está presente en casi todos los tipos de aplicaciones, lo que evidencia su versatilidad, resaltando que

es una técnica apropiada para los sistemas multisensoriales.

Por otro lado, técnicas como aprendizaje federado y refuerzo aparecen con menor frecuencia, lo que puede deberse a su complejidad y a la falta de implementaciones reales. Este análisis permite identificar convergencias frecuentes, como la coincidencia entre seguridad IoT y SVM/DNN, y también divergencias, por ejemplo, entre visualización de ecosistemas y lógicas difusas, donde se aplican enfoques más cualitativos o simbólicos.

TABLA VII
MATRIZ CRUZADA DE TÉCNICAS DE IA Y CAMPO DE APLICACIÓN DE IOT

Campo de Aplicación	Técnicas					
	B1	B2	B3	B4	B5	B6
A1	1	-	-	-	3	-
A2	3	1	-	2	1	2
A3	1	1	1	-	1	3
A4	2	3	-	-	9	-
A5	1	-	2	1	1	-
A6	1	2	1	-	2	-
A7	-	2	-	-	-	-

E. Limitaciones de los estudios revisados

Durante la revisión se detectaron varias limitaciones comunes en los estudios analizados:

- Simulaciones sin validación en entornos reales: varios trabajos validan modelos mediante simuladores o datasets artificiales, sin pruebas en condiciones reales.
- Escasa discusión sobre eficiencia energética: solo una minoría de estudios considera explícitamente el impacto de los algoritmos sobre el consumo energético del sistema.
- Falta de replicabilidad: en varios casos no se detallan las arquitecturas o configuraciones usadas, lo que dificulta la comparación entre enfoques, como el caso de modelos basados en agentes (agent-based modeling) [52].
- Desbalance regional: gran parte de las publicaciones proviene de contextos tecnológicos avanzados, lo que limita la generalización de sus conclusiones.

Estas observaciones permiten entender no solo qué se está haciendo, sino también qué falta por hacer en la aplicación efectiva y sostenible de IA en IoT.

F. Discusión

Los resultados muestran que las áreas con mayor presencia de integración IA–IoT son los sistemas multisensoriales (28.85%) y la seguridad en IoT (21.15%). En cuanto a técnicas, predominan la fusión de datos multisensoriales (40.38%), las DNN (19.23%) y las SVM (15.38%). En términos de desempeño, la mayoría de los estudios reportan niveles de precisión superiores al 90%, con valores máximos de 96.7% para DNN y 96% para SVM.

El predominio de las DNN y las SVM coincide con la precisión reportada en los estudios. Estas dos técnicas son ampliamente utilizadas en trabajos que incluyen IA, lo que explicaría la preferencia de los investigadores en su uso.

Por otro lado, a pesar de ser la técnica más encontrada, la fusión de datos multisensoriales presentó la menor precisión reportada en los estudios, aunque sigue estando en el 90%. Esto implica que aún puede mejorarse la precisión de esta técnica en aplicaciones de IoT, más aún considerando que se emplea en sistemas multisensoriales, frecuentemente utilizados en aplicaciones de salud.

Mientras que en áreas como los hogares inteligentes o a la seguridad en IoT, se han aplicado casi todos los tipos de técnicas encontradas en los estudios, en otras áreas no hay mucha diversidad de técnicas, como por ejemplo en el caso de los sistemas multisensoriales, a pesar de la cantidad de trabajos en esta área.

A pesar de la solidez metodológica planteada, este trabajo presenta algunas limitaciones:

- Se basa exclusivamente en fuentes indexadas en tres bases de datos, lo que puede dejar fuera literatura relevante publicada en otras plataformas.
- No se realizó una evaluación de calidad externa entre revisores, por lo que la selección y clasificación de estudios dependió de un único protocolo interno.
- La comparación de la precisión de las técnicas de IA aplicadas se ha hecho de acuerdo con lo reportado en las publicaciones seleccionadas, que se están enfocando en diferentes contextos, lo que podría implicar un sesgo en la comparación.

V. CONCLUSIONES

Este estudio llevó a cabo una revisión sistemática de literatura sobre la aplicación de la inteligencia artificial (IA) en sistemas de Internet de las Cosas, considerando 53 publicaciones entre 2019 y 2024. Se identificaron las principales técnicas utilizadas, los dominios de aplicación más frecuentes y los beneficios reportados en diversos contextos.

Los sistemas multisensoriales y la seguridad en IoT son las áreas donde más se ha encontrado la aplicación de técnicas de IA. La fusión de datos multisensoriales, DNN y SVM son las técnicas que más se aplican, siendo estas dos últimas las que mejor desempeño han reportado.

A pesar de la diversidad de áreas y técnicas analizadas en la literatura, en futuras investigaciones o desarrollo hace falta tomar en cuenta aspectos como:

- El impacto energético y computacional de los algoritmos aplicados en IoT, especialmente en entornos con restricciones de hardware.
- Evaluación en condiciones reales.
- Mayor detalle de las arquitecturas y parámetros utilizados, para facilitar la replicabilidad.

Como trabajos futuros que integren IoT e IA, se pueden comparar la eficiencia de los modelos relacionando la precisión con el consumo de recursos (tiempo de cómputo, energía, memoria, entre otros). También se puede evaluar la aplicación de IA en entornos Edge (computación en el borde) para reducir la latencia y la dependencia de la nube. Además, es necesario investigar aspectos éticos y regulatorios relacionados con la privacidad, la toma de decisiones

autónoma y la explicabilidad de los modelos.

De igual forma, deben consideraciones algunos aspectos prácticos de acuerdo a cada sector, por ejemplo:

- En agricultura, la combinación de IoT e IA permite mejorar el rendimiento de cultivos y optimizar el uso de recursos, pero se requiere adaptar estas soluciones a pequeños productores con baja conectividad.
- En salud, los sistemas de monitoreo inteligente deben ser evaluados clínicamente antes de su implementación masiva, considerando criterios de interoperabilidad y seguridad de datos.
- En hogares inteligentes, la privacidad es un factor que debe tomarse muy en cuenta, en especial cuando se toman datos biométricos para mejorar los modelos de IA.
- En ciudades inteligentes, la eficiencia de los sistemas depende de la escalabilidad y estandarización; se recomienda adoptar arquitecturas modulares y abiertas para facilitar su integración.

En conjunto, la integración de IA en sistemas IoT representa una oportunidad clave para transformar digitalmente sectores estratégicos. Sin embargo, su adopción debe ir acompañada de criterios técnicos, éticos y prácticos que garanticen su sostenibilidad y aplicabilidad a largo plazo.

Reconocimientos

Los autores agradecen a la Universidad Técnica de Manabí y a la Facultad de Ciencias Informáticas, por brindar las facilidades para llevar a cabo esta investigación.

Referencias

[1] C. Kim and J. Lee, “Discovering patterns and trends in customer service technologies patents using large language model,” Heliyon, vol. 10, no. 14, Jul. 2024, doi: 10.1016/j.heliyon.2024.e34701.

[2] C. Li, S. He, Y. Tian, S. Sun, and L. Ning, “Does the bank’s FinTech innovation reduce its risk-taking? Evidence from China’s banking industry,” Journal of Innovation and Knowledge, vol. 7, no. 3, Jul. 2022, doi: 10.1016/j.jik.2022.100219.

[3] M. García Munguía, H. D. Molina Ruíz, M. Cornejo Velázquez, S. S. Moreno Gutiérrez, and J. L. Alvarado Reséndiz, “Internet de las cosas,” TEPEXI Boletín Científico de la Escuela Superior Tepeji del Río, vol. 7, no. 14, 2020, doi: 10.29057/estr.v7i14.5698.

[4] J. M. Ibrahim, A. Karami, and F. Jafari, “A secure smart home using Internet-of-Things,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Oct. 2017, pp. 69–74. doi: 10.1145/3149572.3149577.

[5] V. D. Ganda, R. Ritika, P. S. Mehra, and D. Chawla, “A Systematic Review on Internet of Things (IoT) Security: Applications, Architecture, Challenges and Solutions,” in 2024 1st International Conference on Advanced Computing and Emerging Technologies, ACET 2024, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ACET61898.2024.10729954.

[6] N. Hasteer, R. Sindhwani, R. Sharma, and P. L. Singh, “A fuzzy Interpretive Structural Modeling approach for implementing IoT and achieving the United Nations Sustainable Development Goals,” Decision Analytics Journal, vol. 8, Sep. 2023, doi: 10.1016/j.dajour.2023.100313.

[7] I. Francisco Javier Flores Zermeño, E. Gonzalo Cossio Franco, and F. Javier Flores, “Aplicaciones, Enfoques y Tendencias del Internet de las Cosas (IoT): Revisión Sistemática de la Literatura,” Congreso Internacional de Investigación Academia Journals Hidalgo, vol. 13, no. 9, p. 568, 2021.

[8] S. P. H. Boroujeni et al., “A comprehensive survey of research towards AI-enabled unmanned aerial systems in pre-, active-, and post-wildfire management,” Information Fusion, vol. 108, Aug. 2024, doi: 10.1016/j.inffus.2024.102369.

[9] M. Simon, D. L. Iveta, L. Huraj, and J. Pospichal, “Multi-Hub Location Heuristic for Alert Routing,” IEEE Access, vol. 7, pp. 40369–40379, 2019, doi: 10.1109/ACCESS.2019.2907161.

[10] H. H. Xiao, W. K. Yang, J. Hu, Y. P. Zhang, L. J. Jing, and Z. Y. Chen, “Significance and methodology: Preprocessing the big data for machine learning on TBM performance,” Underground Space (China), vol. 7, no. 4, pp. 680–701, Aug. 2022, doi: 10.1016/j.undsp.2021.12.003.

[11] A. Telukdarie, M. Munsamy, T. Katsumbe, and X. Maphisa, “Smart value chain tool advancing sustainability in the FoodBev manufacturing industry,” J Clean Prod, vol. 441, Feb. 2024, doi: 10.1016/j.jclepro.2024.140871.

[12] B. G. Martini et al., “A computational model for ubiquitous intelligent services in indoor agriculture,” in Proceedings of the 25th Brazillian Symposium on Multimedia and the Web, WebMedia 2019, Association for Computing Machinery, Inc, Oct. 2019, pp. 497–500. doi: 10.1145/3323503.3360641.

[13] Y. R. Julio et al., “Cloud Framework for Precision Agriculture: Applying ‘Kernel Trick’ Techniques in Support Vector Machines via MQTT and IoT,” in 2024 IEEE Colombian Conference on Communications and Computing, COLCOM 2024 - Proceedings, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/COLCOM62950.2024.10720254.

[14] M. AL-Hawawreh, E. Sitnikova, and F. Den Hartog, “An efficient intrusion detection model for edge system in brownfield industrial internet of things,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Aug. 2019, pp. 83–87. doi: 10.1145/3361758.3361762.

[15] H. Xiong et al., “Efficient and Privacy-Enhanced Asynchronous Federated Learning for Multimedia Data in Edge-based IoT,” ACM Transactions on Multimedia Computing, Communications, and Applications, Aug. 2024, doi: 10.1145/3688002.

[16] A. Bhavani and V. Nithya, “Cryptographic Algorithm for Enhancing Data Security in Wireless IoT Sensor Networks,” Intelligent Automation and Soft Computing, vol. 36, no. 2, pp. 1381–1393, 2023, doi: 10.32604/iasc.2023.029397.

[17] A. Saeed, A. Ahmadinia, A. Javed, and H. Larijani, “Intelligent intrusion detection in low-power IoTs,” ACM Trans Internet Technol, vol. 16, no. 4, Dec. 2016, doi: 10.1145/2990499.

[18] L. Stuermer and R. Martin, “Characterization of technologies in digital health applied in vision care,” J Optom, vol. 15, pp. S70–S81, Jan. 2022, doi: 10.1016/j.optom.2022.09.005.

[19] A. M. Shamsan Saleh, “Blockchain for secure and decentralized artificial intelligence in cybersecurity: A comprehensive review,” Sep. 01, 2024, Zhejiang University. doi: 10.1016/j.bcra.2024.100193.

[20] L. Nie et al., “Intrusion Detection for Secure Social Internet of Things Based on Collaborative Edge Computing: A Generative Adversarial Network-Based Approach,” IEEE Trans Comput Soc Syst, vol. 9, no. 1, pp. 134–145, Feb. 2022, doi: 10.1109/TCSS.2021.3063538.

[21] C. Yang, X. Wang, and S. Mao, “Unsupervised Detection of Apnea Using Commodity RFID Tags with a Recurrent Variational Autoencoder,” IEEE Access, vol. 7, pp. 67526–67538, 2019, doi: 10.1109/ACCESS.2019.2918292.

[22] R. Tsopra et al., “Putting undergraduate medical students in AI-CDSS designers’ shoes: An innovative teaching method to develop digital health critical thinking,” Int J Med Inform, vol. 171, Mar. 2023, doi: 10.1016/j.ijmedinf.2022.104980.

[23] A. Kumar et al., “Digging DEEP: Futuristic building blocks of omni-channel healthcare supply chains resiliency using machine learning approach,” J Bus Res, vol. 162, Jul. 2023, doi: 10.1016/j.jbusres.2023.113903.

[24] M. Blaivas, “Artificial Intelligence and Ultrasonography,” Medicina digital, no. Vol. 31 No. 1, May 2024, doi: 10.24950/rspmi.2585.

[25] D. Kim, S. Cho, L. Tamil, D. J. Song, and S. Seo, “Predicting asthma attacks: Effects of indoor PM concentrations on peak expiratory flow rates of asthmatic children,” IEEE Access, vol. 8, pp. 8791–8797, 2020, doi: 10.1109/ACCESS.2019.2960551.

[26] D. Meana-Llorian, C. G. Garcia, B. C. P. G-Bustelo, J. M. C. Lovelle, and V. H. M. Garcia, “IntelliSenses: Sintiendo Internet de las Cosas,” in Iberian Conference on Information Systems and Technologies, CISTI, IEEE Computer Society, Jul. 2016. doi: 10.1109/CISTI.2016.7521551.

[27] A. Karapetyan, S. Chi-Kin Chau, K. Elbassioni, S. K. Azman, and M. Khonji, “Multisensor adaptive control system for IoT-empowered smart lighting with oblivious mobile sensors,” ACM Trans Sens Netw, vol. 16, no. 1, Dec. 2019, doi: 10.1145/3369392.

[28] S. Akter, Y. K. Dwivedi, S. Sajib, K. Biswas, R. J. Bandara, and K. Michael, “Algorithmic bias in machine learning-based marketing models,” J Bus Res, vol. 144, pp. 201–216, May 2022, doi: 10.1016/j.jbusres.2022.01.083.

[29] Y. C. Huang, Y. T. Cheng, R. H. Liang, J. Y. J. Hsu, and L. L. Chen, “Thing Constellation Visualizer: Exploring Emergent Relationships of Everyday Objects,” Proc ACM Hum Comput Interact, vol. 5, no. CSCW2, Oct. 2021, doi: 10.1145/3479866.

[30] A. G. Qoutb and E. G. Friedman, “MTJ magnetization switching mechanisms for IoT applications,” in Proceedings of the ACM Great Lakes Symposium on VLSI, GLSVLSI, Association for Computing Machinery, May 2018, pp. 347–352. doi: 10.1145/3194554.3194624.

[31] X. Zuo, X. Yang, Z. Dou, and J. R. Wen, “RUCIR at TREC 2019: Conversational Assistance Track,” in 28th Text REtrieval Conference, TREC 2019 - Proceedings, National Institute of Standards and Technology (NIST), 2019. doi: 10.1145/1122445.1122456.

[32] F. Ferreira, V. Amaral, and F. Brito e Abreu, “Digital twinning for smart restoration of classic cars,” in Procedia Computer Science, Elsevier B.V., 2024, pp. 2521–2530. doi: 10.1016/j.procs.2024.02.070.

[33] M. Q. Huang, J. Ninić, and Q. B. Zhang, “BIM, machine learning and computer vision techniques in underground construction: current status and future perspectives.” doi: 10.1016/j.tust.2020.103677.

[34] M. Perno, L. Hvam, and A. Haug, “A machine learning digital twin approach for critical process parameter prediction in a catalyst manufacturing line,” Comput Ind, vol. 151, Oct. 2023, doi: 10.1016/j.compind.2023.103987.

[35] B. M. Sri Madhu, K. Kanagotagi, and Devansh, “IoT based Automatic Attendance Management System,” in International Conference on Current Trends in Computer, Electrical, Electronics and Communication, CTCEEC 2017, Institute of Electrical and Electronics Engineers Inc., Sep. 2018, pp. 83–86. doi: 10.1109/CTCEEC.2017.8455099.

[36] G. De Haan, “Educating Creative Technology for the Internet of Things-Research and Practice-oriented Approaches Compared,” in MIDI 15: Actas del Congreso Multimedia, Interacción, Diseño e Innovación, pp. 1–7. doi: 10.1145/2814464.2814469.

[37] N. R. Beckham, L. J. Akeh, G. N. P. Mitaart, and J. V. Moniaga, “Determining factors that affect student performance using various machine learning methods,” in Procedia Computer Science, Elsevier B.V., 2022, pp. 597–603. doi: 10.1016/j.procs.2022.12.174.

[38] E. Anastasiou et al., “Precision farming technologies for crop protection: A meta-analysis,” Smart Agricultural Technology, vol. 5, Oct. 2023, doi: 10.1016/j.atech.2023.100323.

[39] R. Jolak et al., “CONSERVE: A framework for the selection of techniques for monitoring containers security,” Journal of Systems and Software, vol. 186, Apr. 2022, doi: 10.1016/j.jss.2021.111158.

[40] I. Latin and A. Transactions, “IoT Best Practices and their Components: A Systematic Literature Review,” IEEE Latin America Transactions, vol. 20, no. 10, pp. 2217–2228, 2022, doi: 10.1109/TLA.2022.9885169.

[41] S. Akkermans, B. Crispo, W. Joosen, and D. Hughes, “Polyglot cerberOS: Resource security, interoperability and multi-tenancy for IoT services on a multilingual platform,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Nov. 2018, pp. 59–68. doi: 10.1145/3286978.3286997.

[42] A. Kumar, “A novel framework for waste management in smart city transformation with industry 4.0 technologies,” Research in Globalization, vol. 9, Dec. 2024, doi: 10.1016/j.resglo.2024.100234.

[43] P. Arcaini et al., “Smart home platform supporting decentralized adaptive automation control,” in Proceedings of the ACM Symposium on Applied Computing, Association for Computing Machinery, Mar. 2020, pp. 1893–1900. doi: 10.1145/3341105.3373925.

[44] A. Bhardwaj, K. Kaushik, M. Alshehri, A. A.-B. Mohamed, and I. Keshta, “ISF: Security Analysis and Assessment of Smart Home IoT-based Firmware,” ACM Trans Sens Netw, Jan. 2023, doi: 10.1145/3578363.

[45] F. Li, H. Yang, X. Gao, and H. Han, “Towards IoT-based sustainable digital communities,” Intelligent and Converged Networks, vol. 3, no. 2, pp. 190–203, Jun. 2022, doi: 10.23919/ICN.2022.0015.

[46] Y. Wang et al., “IoT-based green-smart photovoltaic system under extreme climatic conditions for sustainable energy development,” Global Energy Interconnection, vol. 7, pp. 836–856, 2024, doi: 10.1016/j.gloei.2024.1.

[47] M. Woschank, D. Steinwiedder, A. Kaiblinger, P. Miklautsch, C. Pacher, and H. Zsifkovits, “The Integration of Smart Systems in the Context of Industrial Logistics in Manufacturing Enterprises,” in Procedia Computer Science, Elsevier B.V., 2022, pp. 727–737. doi: 10.1016/j.procs.2022.01.271.

[48] S. Subramaniam, L. J. Chew, S. C. Haw, and M. T. Bin Ziauddin, “WQMS: A Water Quality Monitoring System using IoT,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Nov. 2019, pp. 177–182. doi: 10.1145/3372422.3372429.

[49] S. Cairone et al., “Integrating artificial intelligence modeling and membrane technologies for advanced wastewater treatment: Research progress and future perspectives,” Science of the Total Environment, vol. 944, Sep. 2024, doi: 10.1016/j.scitotenv.2024.173999.

[50] R. Mahmud, F. L. Koch, and R. Buyya, “Cloud-fog interoperability in IoT-enabled healthcare solutions,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Jan. 2018. doi: 10.1145/3154273.3154347.

[51] J. Enes, R. R. Expósito, J. Fuentes, J. L. Cacheiro, and J. Touriño, “A pipeline architecture for feature-based unsupervised clustering using multivariate time series from HPC jobs,” Information Fusion, vol. 93, pp. 1–20, May 2023, doi: 10.1016/j.inffus.2022.12.017.

[52] K. Zia, S. Al Maskari, D. K. Saini, A. Muhammad, and U. Farooq, “A simulation model demonstrating the impact of social aspects on social internet of things,” in ACM International Conference Proceeding Series, Association for Computing Machinery, Dec. 2019. doi: 10.1145/3366030.3366076.

[53] E. Badakhshan, N. Mustafee, and R. Bahadori, “Application of simulation and machine learning in supply chain management: A synthesis of the literature using the Sim-ML literature classification framework,” Comput Ind Eng, vol. 198, Dec. 2024, doi: 10.1016/j.cie.2024.110649.

[54] E. Pournaras, P. Pilgerstorfer, and T. Asikis, “Decentralized collective learning for self-managed sharing economies,” ACM Transactions on Autonomous and Adaptive Systems, vol. 13, no. 2, Nov. 2018, doi: 10.1145/3277668.

[55] M. Caporuscio, F. Flammini, N. Khakpour, P. Singh, and J. Thornadtsson, “Smart-troubleshooting connected devices: Concept, challenges and opportunities,” Future Generation Computer Systems, vol. 111, pp. 681–697, Oct. 2020, doi: 10.1016/j.future.2019.09.004.

[56] Y. Bandung, M. A. Wicaksono, S. Pribadi, A. Z. R. Langi, and D. Tanjung, “IoT Video Delivery Optimization Through Machine Learning-Based Frame Resolution Adjustment,” ACM Transactions on Multimedia Computing, Communications, and Applications, Sep. 2024, doi: 10.1145/3665929.

Sección especial en Telecomunicaciones

Es un honor dirigirme a ustedes en el marco de **Telecom 2025**, un encuentro concebido para reflexionar sobre las tendencias emergentes, los avances tecnológicos y los desafíos que definen el presente y el futuro de las telecomunicaciones. Este congreso, de carácter intensivo y colaborativo, ha reunido a investigadores, especialistas y profesionales de diversas áreas con un propósito común: impulsar el conocimiento y promover la innovación responsable en nuestro sector.

En esta ocasión, y en estrecha colaboración con la revista científica Maskay de la Universidad de las Fuerzas Armadas ESPE, hemos llevado a cabo un llamado especial a artículos para una edición temática titulada «Tendencias y Aplicaciones Emergentes en Telecomunicaciones: De la Innovación a la Sostenibilidad». Maskay, reconocida por su compromiso con la rigurosidad académica y su presencia en índices como Latindex, constituye un espacio idóneo para visibilizar investigaciones originales de alto impacto en el campo de la ingeniería.

Los artículos aceptados y publicados en esta edición son el resultado de un proceso de revisión exigente y de la dedicación de autores que han asumido el reto de contribuir con trabajos que no solo reflejan excelencia investigativa, sino también una visión clara del papel que las telecomunicaciones desempeñan en el desarrollo sostenible, la transformación digital y la inclusión tecnológica.

Los temas abordados en este llamado —que abarcan desde **tecnologías de acceso avanzadas como 5G, 6G y Wi-Fi 6/7, hasta sostenibilidad energética, inteligencia artificial aplicada a redes, seguridad y privacidad, IoT, modelos híbridos satelitales-terrestres, y nuevas arquitecturas de transmisión**— evidencian la diversidad y profundidad de las líneas de investigación que hoy impulsan nuestra disciplina. Cada artículo incluido en esta publicación aporta una mirada valiosa, ya sea conceptual, experimental o aplicada, y contribuye a fortalecer el ecosistema de innovación tecnológica en Ecuador y la región.

Agradezco sinceramente a los autores por su confianza y por compartir sus contribuciones; al comité científico por su compromiso con la calidad y la transparencia del proceso de evaluación; y a Maskay por abrir sus páginas a esta edición especial que marca un hito en la articulación entre academia, industria y comunidad técnica.

Con entusiasmo, presento esta colección de artículos que, estoy seguro, inspirará nuevas colaboraciones, motivará investigaciones futuras y continuará posicionando a las telecomunicaciones como un eje fundamental del progreso sostenible.

Dr. Román Lara
IEEE ComSoc Ecuador Chair

Special section on Telecommunications

It is an honor to address you on the occasion of **Telecom 2025**, a one-day congress that explores the latest trends, innovations, and challenges shaping the present and future of telecommunications. This event brings together researchers, experts, and professionals from diverse fields with a shared purpose: advancing knowledge and promoting responsible innovation in our field.

In collaboration with Maskay, the scientific journal of the Universidad de las Fuerzas Armadas ESPE, we have launched a special call for papers for a thematic edition titled "Emerging Trends and Applications in Telecommunications: From Innovation to Sustainability." Maskay, recognized for its academic rigor and indexed in Latindex, provides an ideal platform for disseminating original, high-impact engineering research.

The articles accepted and published in this special issue result from a thorough review process and the dedication of authors who have risen to the challenge of contributing work that reflects not only academic excellence but also a clear understanding of the role telecommunications play in sustainable development, digital transformation, and technological inclusion.

The themes addressed in this call—ranging from **advanced access technologies such as 5G, 6G, and Wi-Fi 6/7, to energy-efficient and green communications, artificial intelligence applied to networks, security and privacy, IoT systems, hybrid satellite-terrestrial architectures, and advanced transmission techniques**—demonstrate the breadth and depth of the research areas driving our discipline today. Each article included in this publication offers a valuable perspective, whether conceptual, experimental, or applied, and contributes to strengthening the technological innovation ecosystem in Ecuador and across the region.

I would like to extend my sincere appreciation to the authors for their trust and valuable contributions; to the scientific committee for their commitment to quality and transparency in the evaluation process; and to Maskay for opening its pages to this special edition, which represents an important step in strengthening collaboration between academia, industry, and the technical community.

It is with great enthusiasm that I present this collection of articles, which I am confident will inspire new collaborations, stimulate future research, and continue to position telecommunications as a cornerstone of sustainable progress.

Dr. Román Lara
IEEE ComSoc Ecuador Chair

MASKAY 16(1), May 2026
ISSN 1390-6712

Recibido (Received): 2025/04/17
Aceptado (Accepted): 2025/07/19

Evaluación del rendimiento de redes inalámbricas de conformidad con IEEE 802.11g/n- en diferentes escenarios de interferencia: Downlink

Performance evaluation of IEEE 802.11g/n compliant wireless networks under different interference scenarios: Downlink

Sayri Alta, Belén Altamirano, Álex Arévalo, Leonel Cando, Doménica Salazar, Ivanna Sotomayor

***Abstract*—In this study, the performance of IEEE 802.11g and IEEE 802.11n wireless networks was investigated under different interference scenarios. Quality of service metrics include throughput, delay, delay variability, and packet loss rate. Experiments conducted in intra-apartment environments began with co-channel interference, with all devices connected on the same channel. Each device then broadcasts on a different channel, thereby minimizing interference. Intrusive traffic in the protocol was used for precise metrics measurements. Results indicate that performance varies depending on the standard and channel configuration. Overall, IEEE 802.11n offers superior performance, although it is more susceptible to interference compared to IEEE 802.11g. Transmission efficiency suffers significantly in the presence of co-channel interference, with throughput losses reaching up to 35% in specific scenarios. This study underscores the importance of proper channel planning to maximize throughput and mitigate the adverse effects of interference.**

***Index Terms*—quality of service metrics, co-channel interference, IEEE 802.11g, IEEE 802.11n.**

***Resumen*—En este estudio, se investigó el rendimiento de las redes inalámbricas IEEE 802.11g e IEEE 802.11n en diferentes escenarios de interferencia. Las métricas de calidad de servicio incluyen el rendimiento, el retraso o la variabilidad del retraso y la tasa de paquetes perdidos. Los experimentos realizados en entornos de intraapartamento comenzaron con interferencia cocanal, con todos los dispositivos conectados en el mismo canal. A continuación, cada uno emitido en un canal diferente, minimizando así la interferencia. El tráfico intrusivo en el protocolo se utilizó para mediciones precisas de las métricas. Los resultados indican que el rendimiento varía según el estándar y la configuración del canal. En términos generales, IEEE 802.11n ofrece un rendimiento superior, aunque es más susceptible a las interferencias en comparación con IEEE 802.11g. La eficiencia de la transmisión se ve afectada de manera significativa en presencia de interferencia cocanal, con pérdidas de rendimiento que pueden alcanzar hasta un 35 % en ciertos escenarios. Este estudio subraya la importancia de una planificación adecuada de los canales para maximizar el rendimiento y mitigar los efectos negativos de la interferencia.**

***Palabras Claves*—métricas de calidad de servicio, interferencia cocanal, IEEE 802.11g, IEEE 802.11n.**

Sayri Alta, Belén Altamirano, Álex Arévalo, Leonel Cando, Doménica Salazar, Ivanna Sotomayor. Carrera en Telecomunicaciones, Unviersidad de las Fuerzas Armadas ESPE, Sangolquí, Ecuador, (e-mail: {smalta, tbaltamirano, flcando, aparevalo2, ipsotomayor, dasalazar14}@espe.edu.ec).

I. Introducción

Las redes inalámbricas que se basan en los estándares IEEE 802.11g e IEEE 802.11n se han vuelto muy comunes en una variedad de entornos, desde hogares hasta aplicaciones industriales y comerciales. Sin embargo, el aumento en su uso ha traído consigo problemas de saturación de canales, lo que genera interferencias que impactan directamente en el rendimiento de las redes. Una de las principales razones de este deterioro es la interferencia cocanal (CCI), donde varios dispositivos operan en el mismo canal, lo que disminuye la calidad del servicio (QoS) y el rendimiento general. [1].

El estándar IEEE 802.11g, que es una mejora del IEEE 802.11b, funciona en la banda de 2,4 GHz y puede alcanzar velocidades de hasta 54 Mbps gracias a la modulación OFDM (multiplexión por división de frecuencia ortogonal) [2]. Por otro lado, el IEEE 802.11n introduce tecnologías más avanzadas como MIMO (Multiple-Input Multiple-Output), que permiten utilizar varias antenas y logran velocidades de hasta 600 Mbps en las bandas de 2,4 GHz o 5 GHz, dependiendo de la configuración del canal y el número de flujos espaciales que se utilicen [3].

A pesar de los avances logrados, ambos estándares todavía son vulnerables a la interferencia en entornos donde hay una alta concentración de dispositivos. Varios estudios han demostrado que aspectos como la selección del canal y la tecnología utilizada tienen un impacto considerable en el rendimiento de la red [4], [5]. Sin embargo, aún hay pocos estudios que se centren específicamente en cómo la interferencia cocanal afecta a los estándares IEEE 802.11g e

DOI: 10.24133/maskay.v16i1.4146

IEEE 802.11n.

Este estudio tiene como finalidad analizar cómo se comportan los estándares IEEE 802.11g y 802.11n en diferentes escenarios de interferencia. Para ello, se inyectará tráfico intrusivo en un entorno de laboratorio controlado. Se evaluarán indicadores clave de rendimiento, como la latencia (δ), el jitter, la pérdida de paquetes (PL) y el rendimiento general. Además, se comparará el desempeño de las redes en canales compartidos frente a canales separados, con el objetivo de entender mejor el impacto real de la interferencia cocanal.

Este trabajo está organizado de la siguiente manera, en la sección 2 se pueden ver trabajos relacionados con el tema de investigación. En la sección 3 se describe la metodología experimental utilizada, incluyendo la configuración del entorno de pruebas y los parámetros de evaluación. En la sección 4 se presentan y analizan los resultados obtenidos. La sección 5 discute los hallazgos más relevantes y sus implicaciones. Finalmente, en la sección 5 se exponen las conclusiones del estudio.

II. Trabajos Relacionados

La interferencia cocanal es un reto importante en las redes IEEE 802.11g e IEEE 802.11n, ya que impacta tanto en la transmisión de datos como en la estabilidad general de la red. Varios estudios han explorado este tema, subrayando cómo la interferencia afecta a entornos con alta densidad de dispositivos y sugiriendo estrategias para mitigar sus efectos. Por ejemplo, un estudio [6] encontró que las redes IEEE 802.11n son más vulnerables a la interferencia en comparación con las basadas en IEEE 802.11g, especialmente en situaciones donde hay una gran cantidad de dispositivos conectados. Otro análisis [8] mostró que una buena planificación del espectro y la selección dinámica de canales son esenciales para mejorar la estabilidad y el rendimiento de la red. Además, el estudio [9] indicó que, aunque IEEE 802.11n ofrece un mejor rendimiento, su eficiencia disminuye notablemente en condiciones de fuerte interferencia cocanal, mientras que IEEE 802.11b tiende a ser más tolerante. En el ámbito de VoWLAN, el estudio [10] destacó la necesidad de evitar la asignación de canales idénticos en celdas adyacentes para reducir la interferencia. En resumen, estos trabajos enfatizan la importancia de una planificación adecuada de los canales, una gestión eficiente del espectro y la implementación de medidas para mitigar interferencias, todo con el fin de optimizar el rendimiento de las redes IEEE 802.11g e IEEE 802.11n en áreas densamente pobladas. También se identificaron diversas métricas de rendimiento en los estudios revisados, como el throughput (η), el retardo (δ), la fluctuación (jitter) y la pérdida de paquetes (packet loss, PL). Estas métricas han sido clave para evaluar el impacto de la CCI en las redes IEEE 802.11g/n y para realizar comparaciones de rendimiento en diferentes escenarios experimentales y simulados.

III. Metodología

A. Escenarios de prueba

Las mediciones se realizaron en un área cerrada de 35 m^2, cuyos muros son de diferente espesor y cuyo material es de hormigón. La Figura 1 muestra la distribución de los dispositivos utilizados en cada red para el primer escenario de prueba, donde el canal 1 se configuró para la red 1, el canal 6 para la red 2 y el canal 11 para la red 3 con el fin de evitar CCI. La Figura 1b muestra el segundo escenario de prueba, donde las tres redes inalámbricas están configuradas para el mismo canal, lo que fuerza la presencia de CCI. Este escenario se repite tres veces: el primer lugar con el canal 1, en segundo lugar con el canal 6 y, finalmente, con el canal 11, generando tres subescenarios que serán analizados.

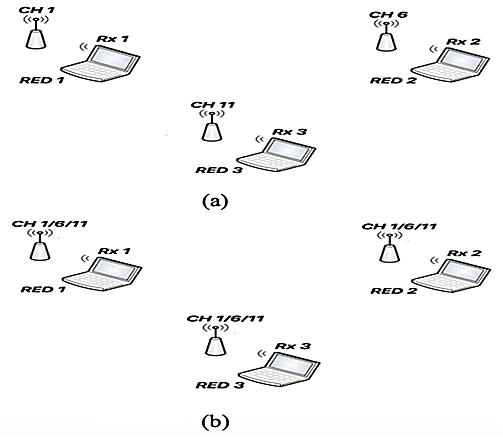


Fig. 1. Escenarios de prueba (a) Sin CCI. b) Con CCI.

B. Materiales

Para el desarrollo del experimento se utilizaron varios routers D-Link compatibles con los estándares 802.11b/g/n, configurados como AP. Este modelo de equipo permitió establecer la red inalámbrica sobre la cual se midieron los parámetros de rendimiento del enlace descendente. La versatilidad y compatibilidad del modelo con múltiples estándares facilitó la evaluación comparativa del comportamiento de cada protocolo bajo las condiciones planteadas en el escenario de prueba.

Para la toma de medidas, se utiliza el método intrusivo de inyección de tráfico utilizando el software D-ITG (Distributed Internet Traffic Generator), que genera tráfico a nivel de paquetes y permite obtener las principales métricas de QoS [10].

Las redes configuradas en cada escenario están compuestas por un Access Point (AP) y dos laptops. El AP tiene capacidad para trabajar en los estándares IEEE 802.11 b/g/n, doble frecuencia: 2.4 GHz y 5 GHz, MIMO 3x3, velocidad de transmisión 300 Mbps (2.4 GHz) y 450 Mbps (5 GHz), mientras que las laptops tienen tarjeta inalámbrica compatible con el estándar IEEE 802.11n, velocidad de procesador de 2.4 GHz, 4 Gb de RAM y sistema operativo Linux. El análisis de los datos adquiridos se realiza mediante la herramienta matemática MATLAB.

TABLA I
CONFIGURACIÓN DEL ROUTER

Parámetros de configuración	Router D-Link
Banda de frecuencia	2.5 Ghz
Modo ROJO	Solo Wireless-N
Anchura del canal	20 MHz
SSID	Grupo 1, Grupo 2, Grupo 3 respectivamente
Canal inalámbrico	1/6/11, dependiendo del escenario

Para obtener las métricas que posteriormente serán analizadas, configuramos la interfaz gráfica del D-ITG en el transmisor con el fin de determinar la velocidad máxima de transmisión que cada red puede soportar en diferentes escenarios de prueba. La inyección de tráfico comenzó con la velocidad teórica del estándar IEEE 802.11n (300 Mbps sobre un canal de 20 MHz), ajustando la velocidad para mantener la pérdida de paquetes por debajo del 5%, un nivel adecuado para aplicaciones en tiempo real. Utilizamos el protocolo UDP y medimos el tiempo de "One-Way Delay" desde el transmisor hasta el receptor. El retardo inicial se fijó en 0 segundos, y las transmisiones duraron 30 segundos en un entorno de laboratorio sin obstrucciones y con redes pequeñas, manteniendo una separación máxima de 1 metro entre los dispositivos. El tamaño del paquete fue de 512 bytes, y esta configuración se replicó en todos los escenarios.

Finalmente, se ajustó la configuración del AP según la capacidad del canal y el número de paquetes enviados en cada prueba.

TABLA II
VELOCIDADES MÁXIMAS DE TRANSMISIÓN Y NÚMERO DE PAQUETES INYECTADOS EN EL ESCENARIO SIN CCI EN EL ENLACE DESCENDENTE

Parámetros	Grupo1	Grupo 2	Grupo 3
	IEE 802.g		
Velocidades de transmisión (Mbps)	3,5546	3,0751	2,9992
Paquetes inyectados (pkt/s)	900	900	900
	IEE 802.n		
Velocidades de transmisión (Mbps)	3,3918	3,3757	3,3765
Paquetes inyectados (pkt/s)	900	900	900

Para verificar que las pruebas se realizaron en un escenario con CCI en cada uno de los canales, se utiliza la aplicación Wi-Fi Analyzer como se muestra en la Fig. 2.

La Fig. 2 muestra el escenario de prueba con canales independientes para evitar la interferencia entre los canales. De igual forma, la Fig. 3 muestra un escenario independiente en el que cada grupo se encuentra en un canal diferente sin CCI.

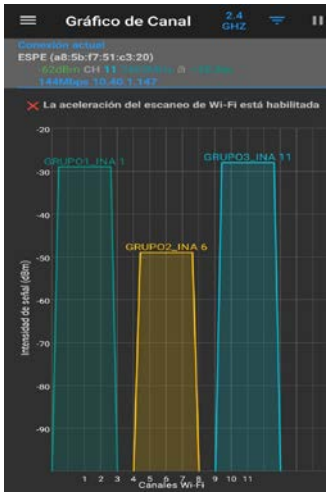
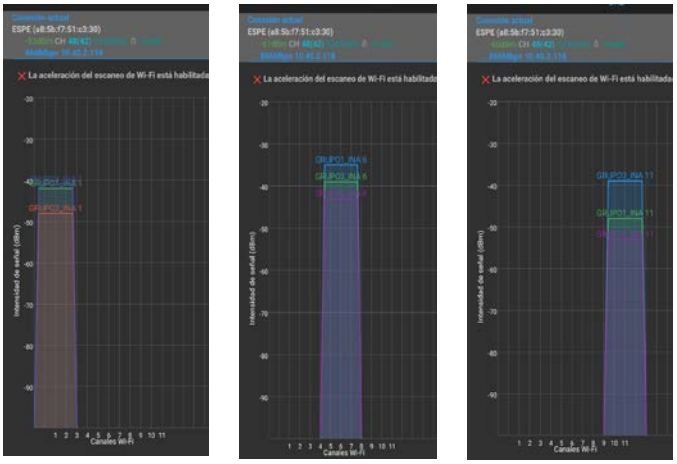


Fig. 2. Escenario de prueba no CCI.



(a) (b) (c)

Fig. 3. Escenario de prueba con CCI (a) Canal 1, (b) Canal 6, (c) Canal 11.

TABLA III
VELOCIDADES MÁXIMAS DE TRANSMISIÓN Y NÚMERO DE PAQUETES INYECTADOS EN EL ESCENARIO CON CCI EN ENLACE DESCENDENTE

Parámetros	Grupo1	Grupo 2	Grupo 3
IEEE 802.11g			
	Canal 1		
Velocidades de transmisión (Mbps)	2,9551	2,9575	2,9230
Paquetes inyectados (pkt/s)	900	900	900
	Canal 6		
Velocidades de transmisión (Mbps)	2,9616	2,9744	2,9872
Paquetes inyectados (pkt/s)	900	900	900
	Canal 11		
Velocidades de transmisión (Mbps)	2,9963	2,9702	3,0304
Paquetes inyectados (pkt/s)	900	900	900
IEEE 802.n			
	Canal 1		
Velocidades de transmisión (Mbps)	3,3787	3,3776	3,3889
Paquetes inyectados (pkt/s)	900	900	900
	Canal 6		
Velocidades de transmisión (Mbps)	3,3868	3,3866	3,3775
Paquetes inyectados (pkt/s)	900	900	900

	Canal 11		
Velocidades de transmisión (Mbps)	3,3892	3,3992	3,3770
Paquetes inyectados (pkt/s)	900	900	900

IV. Resultados

En esta sección se presentan los resultados entregados por el D-ITG, una vez realizadas las 6 inyecciones de tráfico en cada escenario de prueba para cada métrica de rendimiento.

A. *Throughput normalizado (η)*

Para calcular el throughput normalizado, es necesario aplicar la fórmula correspondiente al estándar, teniendo en cuenta las seis mediciones realizadas en cada uno de los canales independientes. Esto significa que hay diferentes mediciones tanto para el escenario con interferencia como para el escenario individual. Por ejemplo, en el canal uno, donde dos equipos operan al mismo tiempo, se obtuvo un promedio de 2.5457 Mbps, mientras que en el otro AP el promedio fue de 3.2214 Mbps. Utilizando el método de inyección de tráfico intrusivo, se determinó el flujo máximo de datos que se puede procesar en escenarios con y sin interferencia cocanal, empleando la métrica η como el principal parámetro de comparación. Esto es importante porque las demás métricas de rendimiento siguen la metodología propuesta, que asegura que la pérdida de paquetes se mantenga por debajo del 5%. Las mediciones tienen en cuenta cada uno de los estándares utilizados (IEEE 802.11 g/b/n) en los diferentes escenarios. Se observó que el estándar 802.11n ofrece un mejor rendimiento que el protocolo 802.11g en un escenario sin interferencia, alcanzando un throughput normalizado de 3.0313 Mbps, como se ilustra en la figura.

B. *Retardo (δ)*

Para obtener los retrasos en todos los escenarios, de igual manera se cuenta con la ayuda de inyecciones de tráfico a través de DITG, por lo que tenemos las medidas en el estándar IEEE 802.11 b/g/n, por lo que los mayores retos que se podrían obtener están en los escenarios no interferidos, siendo el mejor en el IEEE 802.11 g con un promedio de 3.99 ms, en los escenarios interferidos que ocupan los mismos canales, tenemos retrasos muy grandes, por lo que tenemos CCI.

C. *Fluctuación*

A partir de estos valores, se puede concluir que la fluctuación generada en ambos escenarios mantiene una consistencia significativa, ya que los valores registrados se encuentran dentro del mismo rango de medición. Esto indica que la interferencia cocanal no genera variaciones significativas en la estabilidad del tiempo de entrega de paquetes, lo que sugiere que la red mantiene un rendimiento estable en términos de fluctuación de retardo.

Sin embargo, es importante tener en cuenta que, incluso si la fluctuación es baja, otros factores, como la latencia y la pérdida de paquetes, pueden influir en la calidad general del servicio.

D. *Paquetes perdidos (PL)*

Para garantizar la validez del experimento, se mantuvo la pérdida de paquetes por debajo del 5% en todos los escenarios, incluso con interferencia cocanal. Esto se logró ajustando la velocidad de transmisión, lo que permitió reducir la congestión de la red y evitar la saturación del canal, limitando el número de paquetes enviados a un máximo de 900.

Este control contribuyó a la estabilidad del sistema y a una transmisión más eficiente. Al comparar las tasas de transmisión en escenarios con y sin CCI, se observó una disminución notable en ambos estándares (802.11n y 802.11g), siendo más severa en 802.11g, lo que evidencia su mayor susceptibilidad a la interferencia.

Curiosamente, en ausencia de CCI, 802.11g mostró mejores tasas de transmisión que 802.11n, lo cual podría atribuirse a factores externos no controlados o particularidades de su configuración en este entorno de prueba.

E. *Análisis de resultados*

- *Diferentes canales de enlace descendente estándar 802.11b*

En la Fig. 4, se muestra el gráfico perteneciente a la tasa de bits de los diferentes canales en downlink en el estándar 802.11b. La Fig. 5 muestra el gráfico del retardo de los diferentes canales en downlink en el estándar 802.11b. La Fig. 6 muestra el gráfico de la fluctuación de fase de los diferentes canales en downlink en el estándar 802.11b. La Fig. 7 muestra el gráfico de los paquetes perdidos de los diferentes canales en downlink en el estándar 802.11b.

En los gráficos que se muestran en las figuras mencionadas del estándar 802.11b en modo de enlace descendente, con diferentes canales asignados a cada punto de acceso (AP), se observa que AP1 tiene el mejor rendimiento, con un rendimiento medio más alto, mayor estabilidad y menos valores atípicos. En cambio, AP3 muestra el peor rendimiento, con mayor dispersión en los datos y un retraso más alto. Esto sugiere que AP1 experimenta un retraso menor que los otros AP. En cuanto a fluctuación, los valores son similares en todos los AP, lo que indica un tiempo de entrega de paquetes estable, y la pérdida de paquetes es baja, lo que coincide con la baja fluctuación y una transmisión sin retrasos.

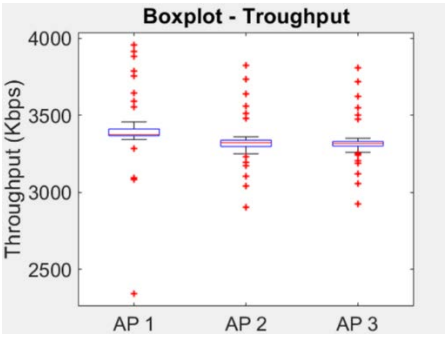


Fig. 4. Gráfico de tasa de bits de los diferentes canales en el enlace descendente en el estándar 802.11b.

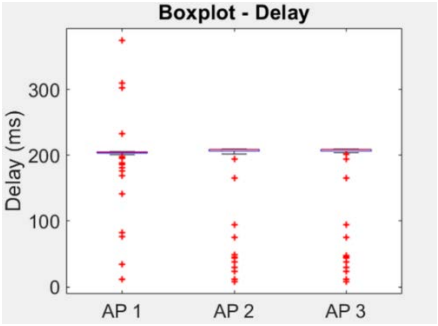


Fig. 5. Gráfico del retardo de los diferentes canales en el enlace descendente en el estándar 802.11b.

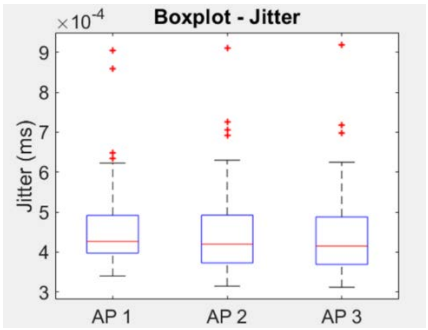


Fig. 6. Gráfico de fluctuación de fase de los diferentes canales en el enlace descendente en el estándar 802.11b.

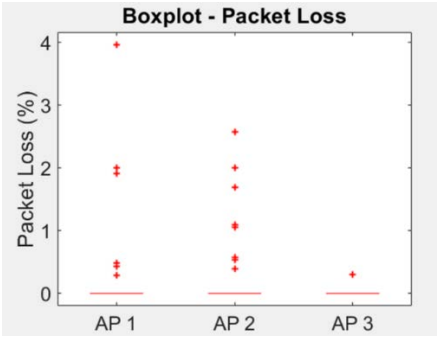


Fig. 7. Gráfico del porcentaje de paquetes perdidos de los diferentes canales en el enlace descendente en el estándar 802.11b.

- *Diferentes canales estándar 802.11g*

La Fig. 8 muestra el gráfico perteneciente a la tasa de bits de los diferentes canales en el downlink en el estándar 802.11g. La Fig. 9 muestra el gráfico del retardo de los diferentes canales en downlink en el estándar 802.11g. La Fig. 10 muestra el gráfico de la fluctuación de fase de los diferentes canales en downlink en el estándar 802.11g. La Fig. 11 muestra el gráfico de los paquetes perdidos de los diferentes canales en downlink en el estándar 802.11g.

En los gráficos del estándar 802.11g en modo de enlace descendente, con diferentes canales para cada punto de acceso (AP), se observa que el rendimiento de los AP es generalmente similar, aunque AP2 destaca con un rendimiento promedio más alto y mayor estabilidad, a pesar de tener más valores atípicos. En contraste, AP3 muestra un rendimiento promedio más bajo y menos estabilidad, reflejado en un mayor retardo y menor fluctuación. AP2 tiene el retardo más alto y AP3 el más bajo. En términos de fluctuación, todos los AP presentan valores similares, pero AP2 tiene más valores atípicos, lo que indica mayor variabilidad en el tiempo de entrega de paquetes, lo que puede contribuir a una mayor pérdida de paquetes.

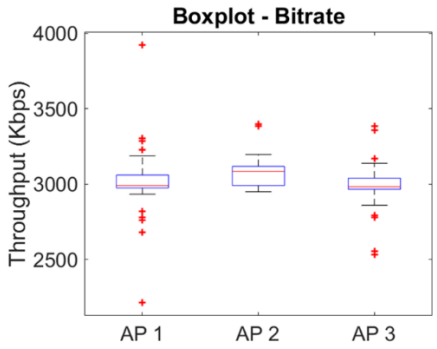


Fig. 8. Gráfico de tasa de bits de los diferentes canales en el enlace descendente en el estándar 802.11g.

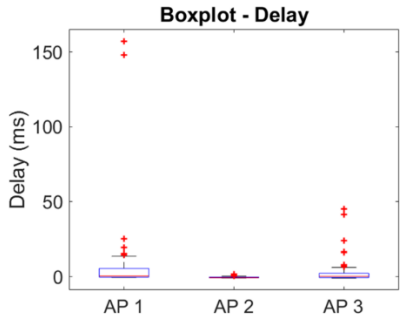


Fig. 9. Gráfico del retardo de los diferentes canales en el enlace descendente en el estándar 802.11g.

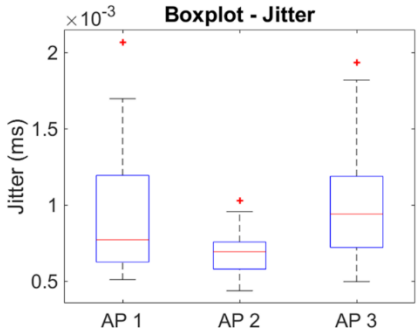


Fig. 10. Gráfico de fluctuación de fase de los diferentes canales en el enlace descendente en el estándar 802.11g.

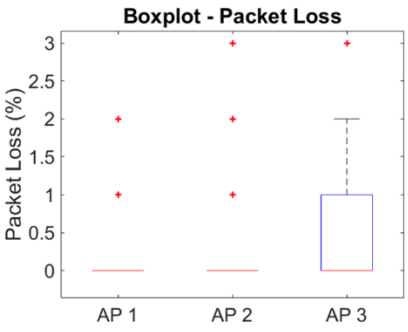


Fig. 11. Gráfico del porcentaje de paquetes perdidos de los diferentes canales en el enlace descendente en el estándar 802.11g.

- *Diferentes canales estándar 802.11n*

La Fig. 12 muestra el gráfico perteneciente a la tasa de bits de los diferentes canales en downlink en el estándar 802.11n. La Fig. 13 muestra el gráfico de la fluctuación de la fase de los diferentes canales en downlink en el estándar 802.11n. La Fig. 14 muestra el gráfico del retardo de los diferentes canales en downlink en el estándar 802.11n. La Fig. 15 muestra el gráfico de los paquetes perdidos de los diferentes canales en downlink en el estándar 802.11n.

Al emplear el estándar 802.11n con canales diferenciados para cada punto de acceso en modo de enlace descendente, AP3 obtuvo el mejor rendimiento general. Aunque su mediana fue ligeramente inferior a la de AP2, mostró mayor estabilidad al no presentar valores atípicos altos. AP1, en cambio, evidenció mayor variabilidad. La tasa de bits de AP3 y su bajo retraso lo posicionaron como el más eficiente. La fluctuación y la pérdida de paquetes fueron similares en todos los AP, reflejando una entrega de datos estable y una calidad de servicio aceptable en todos los casos.

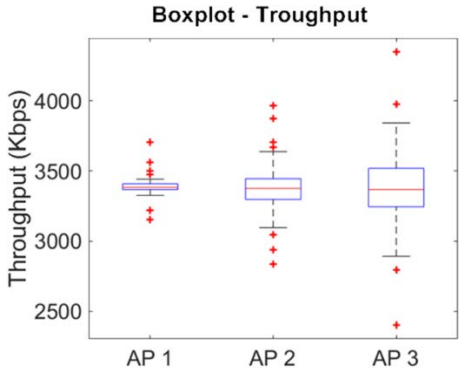


Fig. 12. Gráfico de tasa de bits de los diferentes canales en el enlace descendente en el estándar 802.11n

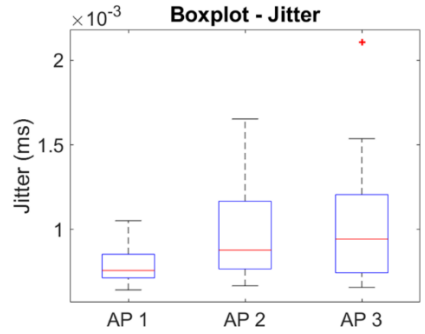


Fig. 13. Gráfico de fluctuación de fase de los diferentes canales en el enlace descendente en el estándar 802.11n

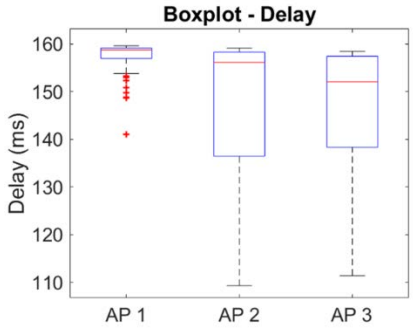


Fig. 14. Gráfico del retardo de los diferentes canales en el enlace descendente en el estándar 802.11n

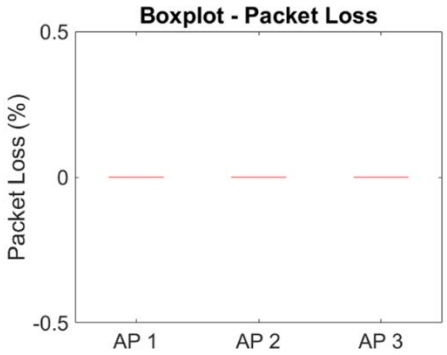


Fig. 15. Gráfico del porcentaje de paquetes perdidos de los diferentes canales en el enlace descendente en el estándar 802.11 n

- *Mismo canal / canal 1 / 802.11b*

La Fig. 16 muestra el gráfico perteneciente a la tasa de bits del canal 1 en downlink en el estándar 802.11b. La Fig. 17 muestra el gráfico de la fluctuación de fase en el canal 1 en downlink en el estándar 802.11b. La Fig. 18 muestra el gráfico del retardo del canal 1 en downlink en el estándar 802.11b. La Fig. 19 muestra el gráfico de los paquetes perdidos del canal 1 en downlink en el estándar 802.11b.

En los gráficos correspondientes al estándar 802.11b en modo de enlace descendente, utilizando el mismo canal 1 para todos los puntos de acceso (APs), se observa que AP2 y AP3 se comportan mejor que AP1, especialmente en términos de tasa de bits. El rendimiento medio es similar entre los AP, pero AP1 presenta un rendimiento más bajo, lo que también se refleja en un mayor retraso de los paquetes. En cuanto a la fluctuación, AP1 exhibe más variabilidad en los tiempos de entrega de paquetes, con valores atípicos notables, aunque esto no conduce a un aumento en la pérdida de paquetes. Esto sugiere que, si bien AP1 se ve más afectado por la interferencia del canal, el sistema aún logra mantener la integridad de la transmisión.

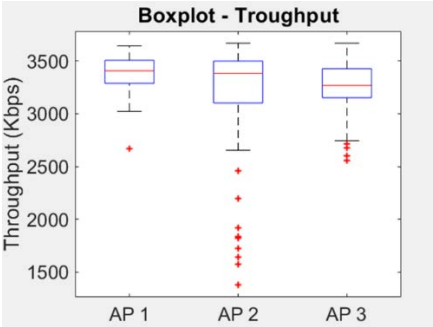


Fig. 16. Gráfico de la tasa de bits perdida del canal 1 en el enlace descendente en el estándar 802.11b

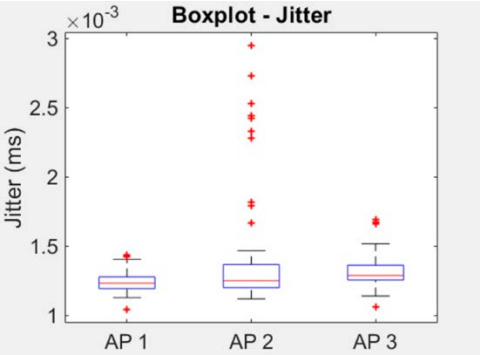


Fig. 17. Gráfico de la fluctuación de fase perdida del canal 1 en el enlace descendente en el estándar 802.11b

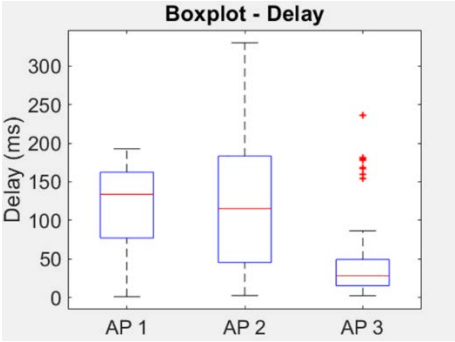


Fig. 18. Gráfico de retardo del canal perdido 1 en el enlace descendente en el estándar 802.11b

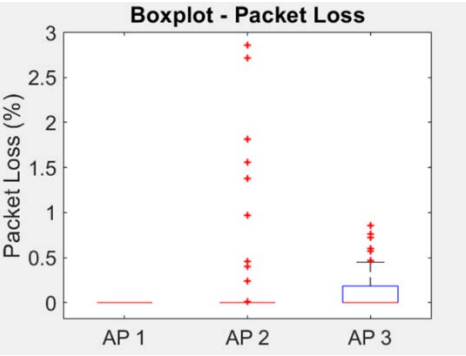


Fig. 19. Gráfico del porcentaje de paquetes perdidos del canal 1 en el enlace descendente en el estándar 802.11b

- *Mismo canal / Canal 1 / Estándar 802.11g*

La Fig. 20 muestra el gráfico perteneciente a la tasa de bits del canal 1 en downlink en el estándar 802.11g. La Fig. 21 muestra el gráfico de la fluctuación de fase en el canal 1 en downlink en el estándar 802.11g. La Fig. 22 muestra el gráfico del retardo del canal 1 en downlink en el estándar 802.11g. La Fig. 23 muestra el gráfico de los paquetes perdidos del canal 1 en downlink en el estándar 802.11g. En el escenario con el estándar 802.11g y el canal 1 en modo de enlace descendente, AP3 presentó el mejor rendimiento general, con mayor tasa de bits y menor retraso, además de un comportamiento más estable sin valores atípicos relevantes. En contraste, AP1 y AP2 mostraron mayor variabilidad en su desempeño. La fluctuación fue similar en todos los AP, aunque se detectaron algunos valores atípicos y pérdidas de paquetes, lo cual es coherente, ya que una mayor variabilidad en la entrega puede provocar pérdida de datos, incluso en condiciones de canal compartido.

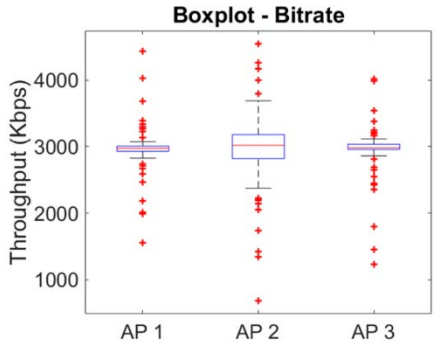


Fig. 20. Gráfico de la tasa de bits del canal 1 en el enlace descendente en el estándar 802.11g

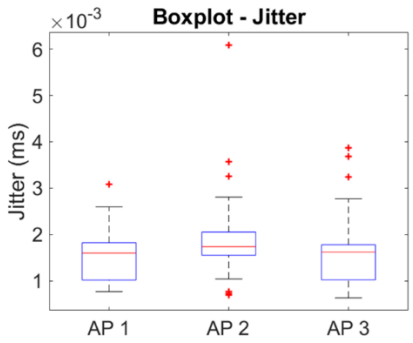


Fig. 21. Gráfico de la fluctuación de fase del canal 1 en el enlace descendente en el estándar 802.11g

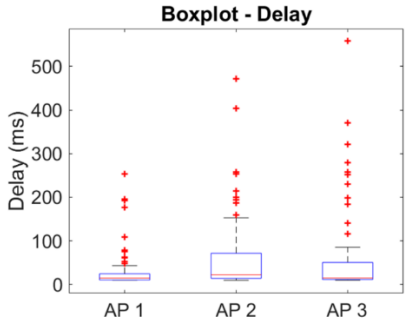


Fig. 22. Gráfico del retardo del canal 1 en el enlace descendente en el estándar 802.11g

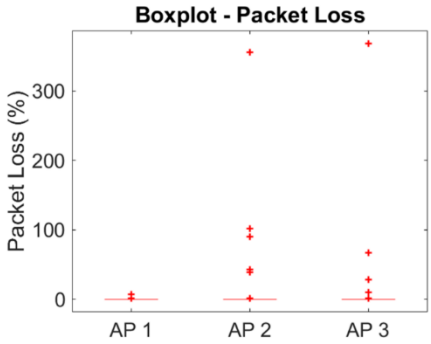


Fig. 23. Gráfico del porcentaje de paquetes perdidos del canal 1 en el enlace descendente en el estándar 802.11g

- *Mismo canal / Canal 1 / 802.11n*

La Fig. 24 muestra el gráfico perteneciente a la tasa de bits del canal 1 en downlink en el estándar 802.11n. La Fig. 25 muestra el gráfico de la fluctuación de fase en el canal 1 en downlink en el estándar 802.11n. La Fig. 26 muestra el gráfico del retardo del canal 1 en downlink en el estándar 802.11n. La Fig. 27 muestra el gráfico de los paquetes perdidos del canal 1 en downlink en el estándar 802.11n.

Al utilizar el canal 1 con el estándar 802.11n en modo de enlace descendente, AP3 mostró un rendimiento ligeramente superior al de los otros puntos de acceso, destacando por una mayor tasa de bits y menor retraso, aunque las diferencias no fueron significativas debido al entorno controlado. Se observaron valores atípicos en otros AP, lo que refleja cierta variabilidad en la transmisión. La fluctuación fue similar entre APs, aunque AP1 presentó algunos picos, y la pérdida de paquetes estuvo presente en todos, siendo levemente mayor en AP3, posiblemente por la interferencia del canal compartido.

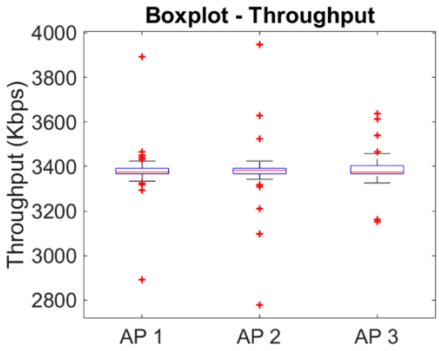


Fig. 24. Gráfico de la tasa de bits del canal 1 en el enlace descendente en el estándar 802.11n

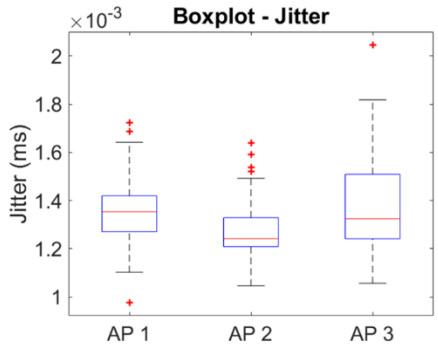


Fig. 25. Gráfico de la fluctuación de fase del canal 1 en el enlace descendente en el estándar 802.11n

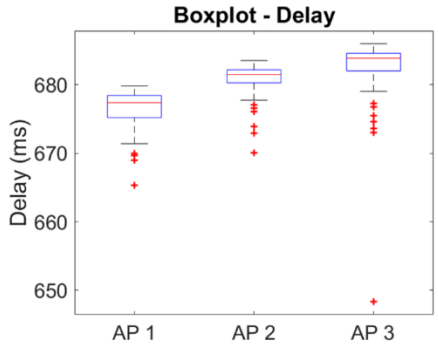


Fig. 26. Gráfico del retardo del canal 1 en el enlace descendente en el estándar 802.11n

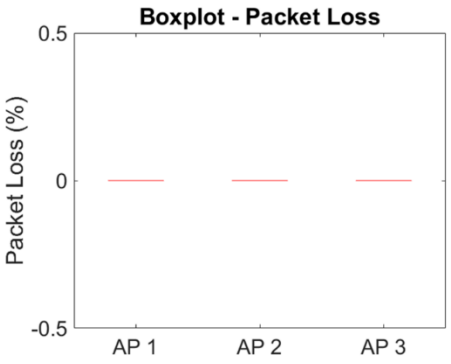


Fig. 27. Gráfico del porcentaje de paquetes perdidos del canal 1 en el enlace descendente en el estándar 802.11 n

- *Mismo canal / Canal 6 / 802.11b*

La Fig. 28 muestra el gráfico perteneciente a la tasa de bits del canal 6 en downlink en el estándar 802.11b. La Fig. 29 muestra el gráfico de la fluctuación de fase en el canal 6 en downlink en el estándar 802.11b. La Fig. 30 muestra el gráfico del retardo del canal 6 en downlink en el estándar 802.11b. La Fig. 31 muestra el gráfico de los paquetes perdidos del canal 6 en downlink en el estándar 802.11b. En el escenario con canal 6 y el estándar 802.11b en modo de enlace descendente, el rendimiento fue bajo en general, evidenciando las limitaciones de este estándar ante múltiples dispositivos operando en el mismo canal. AP1 mostró una ligera mejora en estabilidad, pero con muchas fluctuaciones, mientras que AP2 y especialmente AP3 fueron más inestables. El retraso fue elevado y constante, con grandes variaciones en la temporización (jitter) que afectaron la calidad de transmisión. Además, se registró una pérdida considerable de paquetes, lo que confirma la baja eficiencia del estándar 802.11b en condiciones de interferencia por canal compartido.

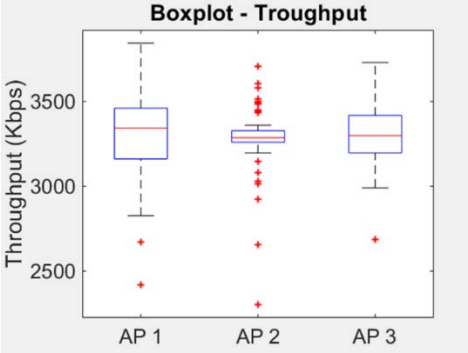


Fig. 28. Gráfico de la tasa de bits del canal 6 en el enlace descendente en el estándar 802.11b

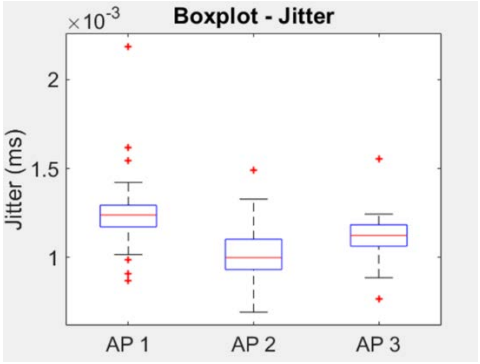


Fig. 29. Gráfico de la fluctuación de fase del canal 6 en el enlace descendente en el estándar 802.11b

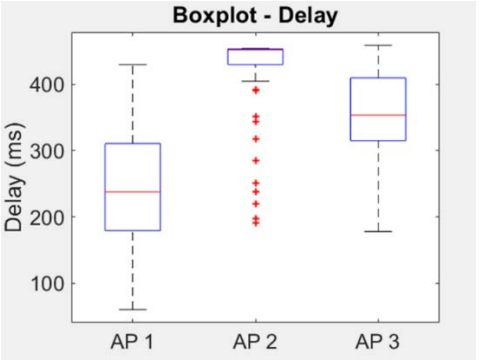


Fig. 30. Gráfico del retardo de 6 canales en el enlace descendente en el estándar 802.11b

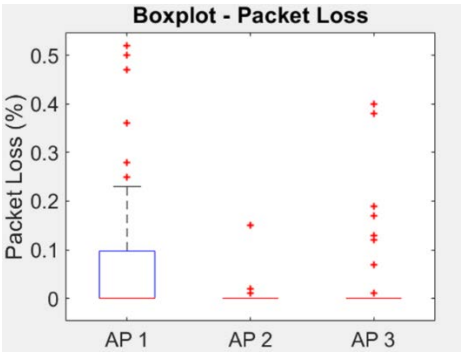


Fig. 31. Gráfico del porcentaje de paquetes perdidos del canal 6 en el enlace descendente en el estándar 802.11b

- *Mismo canal / Canal 6 / 802.11g*

La Fig. 32 muestra el gráfico perteneciente a la tasa de bits del canal 6 en downlink en el estándar 802.11g. La Fig. 33 muestra el gráfico de la fluctuación de fase en el canal 6 en downlink en el estándar 802.11g. La Fig. 34 muestra el gráfico del retardo del canal 6 en downlink en el estándar 802.11g. La Fig. 35 muestra el gráfico de los paquetes perdidos del canal 6 en downlink en el estándar 802.11g. Al utilizar el canal 6 con el estándar 802.11g en modo de enlace descendente, se observó una mejora considerable respecto al 802.11b. Todos los puntos de acceso presentaron un aumento significativo en el rendimiento, especialmente AP2, que mostró los valores más altos y estables. AP1 también obtuvo buenos resultados, mientras que AP3 mejoró, aunque aún registró algunas variaciones. La fluctuación fue menor que con 802.11b, aunque AP3 mostró algunos picos. La pérdida de paquetes se redujo, pero persistió, lo que indica que, aunque 802.11g maneja mejor la interferencia, aún puede verse afectado por el uso compartido del canal.

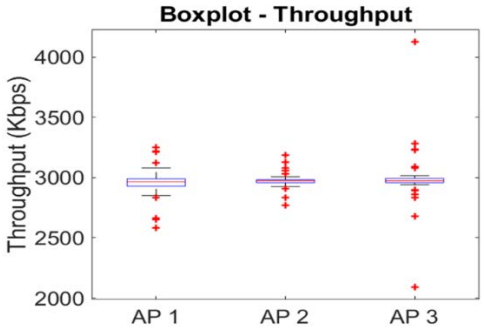


Fig. 32. Gráfico de la tasa de bits del canal 6 en el enlace descendente en el estándar 802.11g

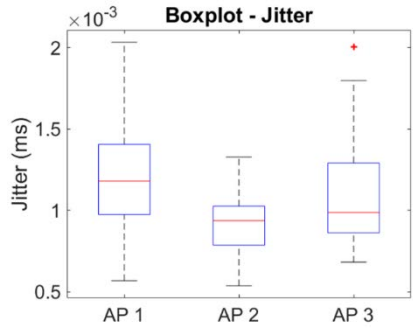


Fig. 33. Gráfico de la fluctuación de fase del canal 6 en el enlace descendente en el estándar 802.11g

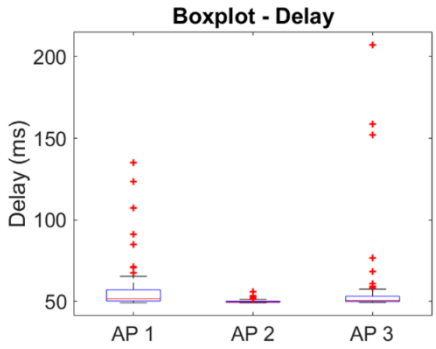


Fig. 34. Gráfico del retardo del canal 6 en el enlace descendente en el estándar 802.11g

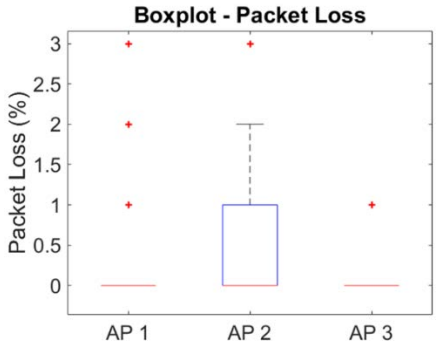


Fig. 35. Gráfico del porcentaje de paquetes perdidos del canal 6 en el enlace descendente en el estándar 802.11g

- *Mismo canal / Canal 6 / 802.11n*

La Fig. 36 muestra el gráfico perteneciente a la tasa de bits del canal 6 en downlink en el estándar 802.11n. La Fig. 37 muestra el gráfico de la fluctuación de fase en el canal 6 en downlink en el estándar 802.11n. La Fig. 38 muestra el gráfico del retardo del canal 6 en downlink en el estándar 802.11n. La Fig. 39 muestra el gráfico de los paquetes perdidos del canal 6 en downlink en el estándar 802.11n. El uso del estándar 802.11n en el canal 6 mejoró notablemente el rendimiento en enlace descendente respecto a los estándares anteriores. Todos los AP mostraron un rendimiento elevado, destacando AP2 por su estabilidad y eficiencia. El retraso fue bajo en general, con AP2 nuevamente como el más rápido. La fluctuación se mantuvo reducida, con leves picos en AP3, y la pérdida de paquetes fue mínima o inexistente. Estos resultados confirman la alta resistencia del estándar 802.11n frente a la interferencia cuando varios AP comparten canal.

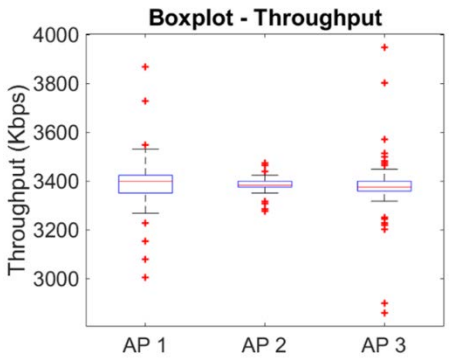


Fig. 36. Gráfico de la tasa de bits del canal 6 en el enlace descendente en el estándar 802.11n

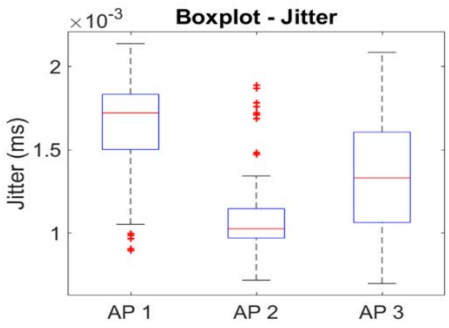


Fig. 37. Gráfico de la fluctuación de fase del canal 6 en el enlace descendente en el estándar 802.11n

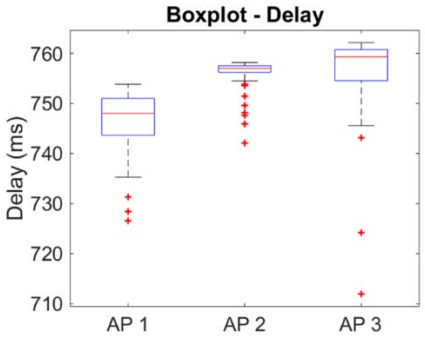


Fig. 38. Gráfico del retardo del canal 6 en el enlace descendente en el estándar 802.11n

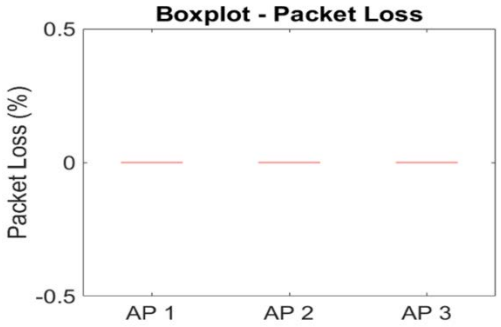


Fig. 39. Gráfico del porcentaje de paquetes perdidos del canal 6 en el enlace descendente en el estándar 802.11n

- *Mismo canal / canal 11 / 802.11b*

La Fig. 40 muestra el gráfico perteneciente a la tasa de bits del canal 11 en downlink en el estándar 802.11b. La Fig. 41 muestra el gráfico de la fluctuación de fase en el canal 11 en downlink en el estándar 802.11b. La Fig. 42 muestra el gráfico del retardo del canal 11 en downlink en el estándar 802.11b. La Fig. 43 muestra el gráfico de los paquetes perdidos del canal 11 en downlink en el estándar 802.11b. Con el estándar 802.11b en el canal 11, el rendimiento fue bajo y comparable al obtenido en el canal 6. AP1 mostró un leve mejor desempeño, pero sin destacarse, mientras que AP3 fue el más inestable. El retraso se mantuvo elevado, especialmente en AP3, y la fluctuación fue muy variable en todos los puntos de acceso. La pérdida de paquetes fue significativa, lo que evidencia que 802.11b no responde bien ante interferencias por uso compartido del canal.

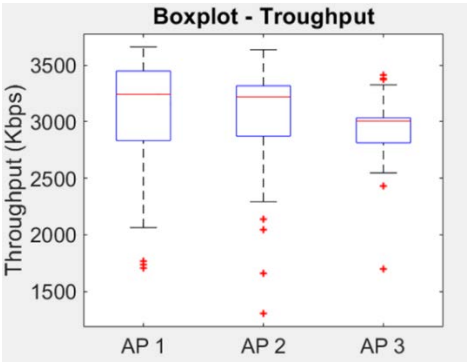


Fig. 40. Gráfico de la tasa de bits del canal 11 en el enlace descendente en el estándar 802.11b

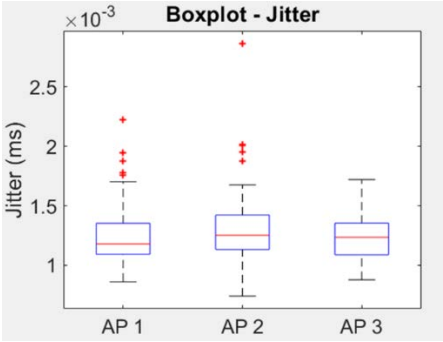


Fig. 41. Gráfico de la fluctuación de fase del canal 11 en el enlace descendente en el estándar 802.11b

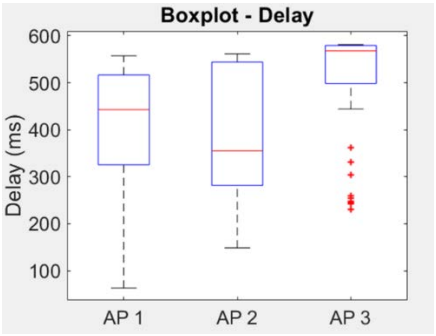


Fig. 42. Gráfico de la tasa de bits del canal 11 en el enlace descendente en el estándar 802.11b

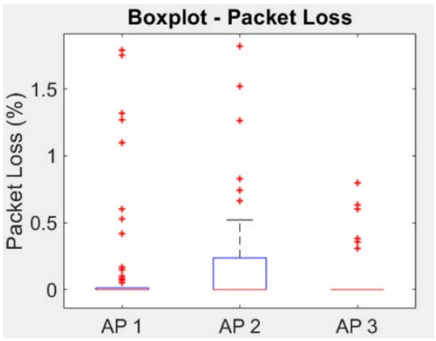


Fig. 43. Gráfico del porcentaje de paquetes perdidos del canal 11 en el enlace descendente en el estándar 802.11b

- *Mismo canal / Canal 11 / 802.11g*

La Fig. 44 muestra el gráfico perteneciente a la tasa de bits del canal 11 en downlink en el estándar 802.11g. La Fig. 45 muestra el gráfico de la fluctuación de fase en el canal 11 en downlink en el estándar 802.11g. La Fig. 46 muestra el gráfico del retardo del canal 11 en downlink en el estándar 802.11g. La Fig. 47 muestra el gráfico de los paquetes perdidos del canal 11 en downlink en el estándar 802.11g. El uso del estándar 802.11g en el canal 11 mejoró el rendimiento general en enlace descendente, mostrando resultados similares a los obtenidos con otros canales del mismo estándar. AP2 fue el que alcanzó los valores más altos y estables, seguido de AP1 con un buen desempeño y AP3 con algunas variaciones. El retraso fue bajo en todos los puntos de acceso y la fluctuación se mantuvo controlada, aunque AP3 presentó cierta inestabilidad. La pérdida de paquetes se redujo respecto al estándar 802.11b, pero aún se evidenciaron efectos de

interferencia debido al uso compartido del canal entre los AP.

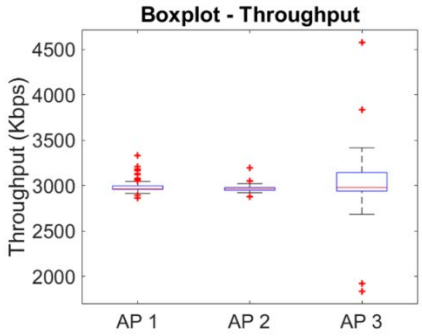


Fig. 44. Gráfico de la tasa de bits del canal 11 en el enlace descendente en el estándar 802.11g

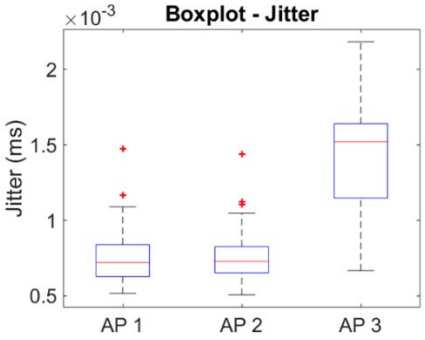


Fig. 45. Gráfico de la fluctuación de fase del canal 11 en el enlace descendente en el estándar 802.11g

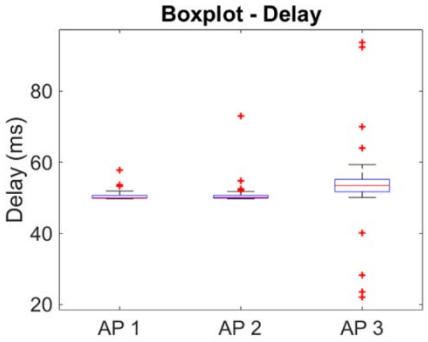


Fig. 46. Gráfico del retardo del 11º canal en el enlace descendente en el estándar 802.11g

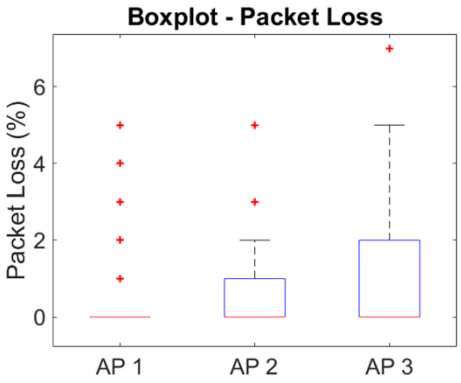


Fig. 47. Gráfico del porcentaje de paquetes perdidos del canal 11 en el enlace descendente en el estándar 802.11g

- *Mismo canal / Canal 11 / 802.11n*

La Fig. 48 muestra el gráfico perteneciente a la tasa de bits del canal 11 en downlink en el estándar 802.11n. La Fig. 49 muestra el gráfico de la fluctuación de fase en el canal 11 en downlink en el estándar 802.11n. La Fig. 50 muestra el gráfico del retardo del canal 11 en downlink en el estándar 802.11n. La Fig. 51 muestra el gráfico de los paquetes perdidos del canal 11 en downlink en el estándar 802.11n.

El uso del estándar 802.11n en el canal 11 ofreció el mejor desempeño global en modo de enlace descendente. AP2 destacó con el mayor rendimiento y menor retraso, seguido de AP1 con buenos resultados, y AP3 con ligera inestabilidad, pero aún superior a escenarios previos. La fluctuación fue mínima y bien controlada, y la pérdida de paquetes casi inexistente, lo que confirma la alta eficiencia del estándar 802.11n frente a la interferencia y congestión del canal.

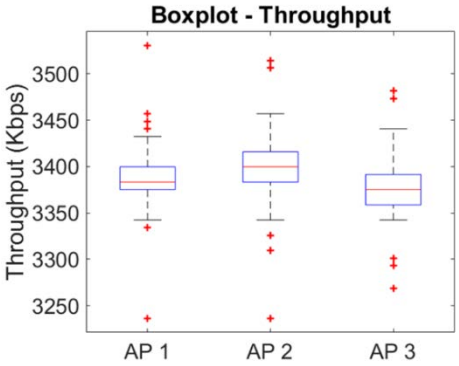


Fig. 48. Gráfico de la tasa de bits del canal 11 en el enlace descendente en el estándar 802.11n

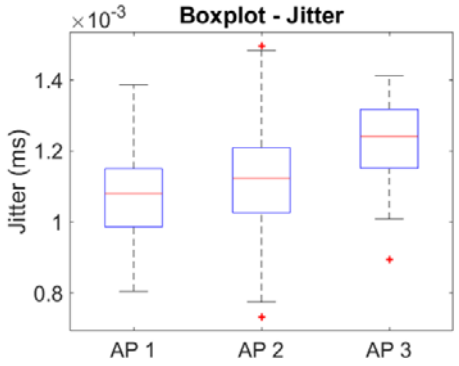


Fig. 49. Gráfico de la fluctuación de fase del canal 11 en el enlace descendente en el estándar 802.11n

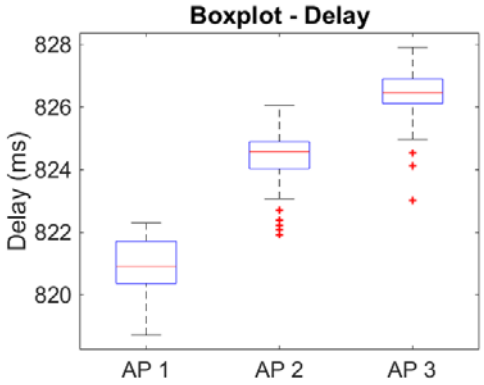


Fig. 50. Gráfico del retardo del canal 11 en el enlace descendente en el estándar 802.11n

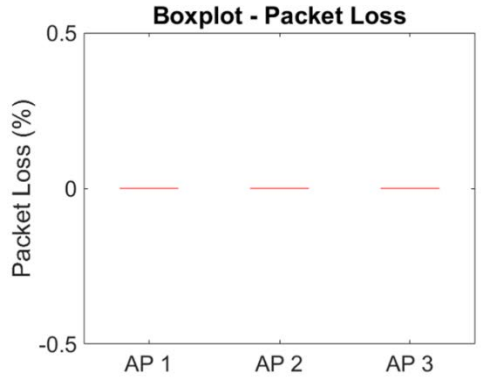


Fig. 51. Gráfico del porcentaje de paquetes perdidos del canal 11 en el enlace descendente en el estándar 802.11n

V. Discusión

Los experimentos llevaron a cabo una evaluación del comportamiento de redes inalámbricas bajo diversas configuraciones de inyección de tráfico, centrándose en la transmisión de enlace descendente en los estándares IEEE 802.11g e IEEE 802.11n. Durante las pruebas, se utilizaron diferentes puntos de acceso (AP) y estaciones, distribuidos en tres canales operativos (CH1, CH6 y CH11), con el objetivo de reducir la interferencia y analizar el rendimiento en cada escenario. Los resultados mostraron que el estándar IEEE 802.11n superó al IEEE 802.11g, especialmente en cuanto a velocidad y estabilidad de la conexión. Este hallazgo era predecible, ya que el estándar IEEE 802.11n incluye mejoras en la eficiencia espectral y utiliza tecnologías como MIMO (Multiple-Input Multiple-Output). Sin embargo, se encontraron limitaciones en ciertos dispositivos, que no permitían una conmutación flexible entre los modos G y N, lo que limitó la adaptabilidad de los experimentos en algunos casos.

Además, el uso simultáneo de los canales CH1, CH6 y CH11 ayudó a disminuir la interferencia, lo que subraya lo crucial que es planificar adecuadamente los canales en entornos con múltiples puntos de acceso (multi-AP) para maximizar el rendimiento de la red. Por otro lado, cuando todos los dispositivos funcionaron en el mismo canal, los niveles de interferencia aumentaron considerablemente, lo que resultó en una degradación de la conexión y un incremento en la latencia. Este estudio reafirma la importancia de elegir correctamente el estándar y de planificar de manera eficiente el uso de canales en redes inalámbricas, ya que son mecanismos clave para mejorar el rendimiento y reducir los efectos de la interferencia. Los resultados obtenidos son una referencia valiosa para futuras investigaciones en entornos multi-AP y diversas configuraciones de tráfico descendente.

Tal como se muestra en la Tabla I, la configuración del router impacta directamente en la calidad del enlace, especialmente al operar bajo diferentes bandas y anchos de canal.

Según los datos presentados en la Tabla II, las velocidades de transmisión en escenarios sin interferencia muestran una leve ventaja del estándar 802.11n sobre 802.11g.

De acuerdo con la Tabla III, la interferencia cocanal provoca una reducción significativa en el rendimiento, particularmente en el estándar 802.11g, mientras que 802.11n se mantiene más estable.

Además, al comparar con estándares más recientes como IEEE 802.11ac, se observa que este ofrece mejoras significativas frente a IEEE 802.11n, principalmente en la banda de 5 GHz. El estándar 802.11ac implementa canales más anchos (hasta 160 MHz), modulación 256-QAM y soporte para MU-MIMO, lo que le permite alcanzar velocidades superiores a 1 Gbps y manejar múltiples dispositivos de manera más eficiente. En contraste, IEEE 802.11n está limitado a 600 Mbps y tecnologías MIMO tradicionales, lo que reduce su desempeño en entornos con alta densidad de tráfico. Esta comparación técnica destaca la evolución de las redes Wi-Fi hacia un mayor rendimiento y eficiencia espectral.

VI. Conclusiones

El estándar IEEE 802.11n ofrece un rendimiento mucho mejor que el 802.11g, gracias a tecnologías como MIMO y un mayor ancho de banda. Sin embargo, su eficiencia se ve afectada por la interferencia cocanal, especialmente en áreas con alta densidad de dispositivos. Por eso, la planificación de canales es clave: al distribuir los puntos de acceso (AP) en canales no superpuestos (1, 6 y 11), se logra una notable mejora en la calidad del servicio, reduciendo la latencia y la pérdida de paquetes. En cambio, si todos los dispositivos operan en un solo canal, el rendimiento puede caer drásticamente, con pérdidas de hasta el 35%.

A pesar de estas pérdidas, la fluctuación (jitter) se mantuvo generalmente por debajo de 2 ms, lo cual es aceptable para aplicaciones sensibles como VoIP. La pérdida de paquetes también se mantuvo bajo control (<5%) al ajustar cuidadosamente la velocidad de transmisión usando el protocolo UDP. El software D-ITG demostró ser muy útil para evaluar el tráfico, permitiendo obtener métricas precisas de calidad de servicio (QoS) en escenarios de prueba controlados.

VII. Recomendaciones

Es recomendable considerar estándares más avanzados, como IEEE 802.11ac y 802.11ax (Wi-Fi 5 y Wi-Fi 6), para

futuros proyectos, ya que ofrecen mejoras notables en eficiencia espectral, capacidad para múltiples usuarios y rendimiento en entornos con alta densidad de dispositivos. Además, es crucial establecer sistemas de monitoreo y análisis continuo del espectro radioeléctrico, especialmente en redes densas, para poder detectar y abordar de manera proactiva cualquier interferencia que pueda afectar la calidad del servicio. También es importante llevar a cabo pruebas adicionales en entornos operativos reales con tráfico mixto y usuarios concurrentes, para validar la escalabilidad de los resultados observados en laboratorio y evaluar cómo las condiciones dinámicas, como la movilidad de los usuarios, la variabilidad en el uso de aplicaciones y la coexistencia con otras redes, impactan el rendimiento. Finalmente, se recomienda utilizar herramientas de monitoreo en tiempo real durante las pruebas, como analizadores de espectro o sistemas de gestión de redes, que permitan correlacionar eventos específicos (como picos de interferencia o pérdida de señal) con las métricas obtenidas, lo que mejorará la capacidad de diagnóstico y optimización.

REFERENCIAS

[1] Norma IEEE para Tecnología de la Información—Redes de área local y metropolitana—Requisitos específicos—Parte 11: Especificaciones de control de acceso al medio (MAC) y capa física (PHY) de LAN inalámbrica, Enmienda 5: Mejoras para un mayor rendimiento.

[2] D. Crespo Sen, "Mecanismos de asignación de canales en redes IEEE 802.11", Universidad de Alcalá, 2019. [En línea]. Disponible: https://ebuah.uah.es/dspace/bitstream/handle/10017/38651/TFG_Crespo_Sen_2019.pdf

[3] C. Muñoz Morales, "Análisis de Desempeño de un Sistema MIMO-OFDM con Predicción de Canales", Tesis Doctoral, Universidad Nacional de Colombia, Bogotá DC., 2013.

[4] S. H. Masood, "Comparación del rendimiento de IEEE 802.11g e IEEE 802.11n en presencia de interferencia de red 802.15.4", preimpresión de arXiv arXiv:1308.0678, 2013. [En línea]. Disponible: https://arxiv.org/abs/1308.0678.

[5] R. A. Lara Cueva, C. B. Fernández Jiménez y C. A. Morales Maldonado, "Análisis de rendimiento en un enlace descendente de redes basadas en los estándares IEEE 802.11b, IEEE 802.11n y WDS", Reci, vol. 5, núm. 10, 2016.

[6] S. H. Masood, "Comparación del rendimiento de IEEE 802.11g e IEEE 802.11n en presencia de interferencia de red 802.15.4", preimpresión de arXiv arXiv:1308.0678, 2013. [En línea]. Disponible: https://arxiv.org/abs/1308.0678

[7] S. M. Kala, M. P. K. Reddy, R. Musham, B. R. Tamma, "Asignaciones de canales conscientes de la coubicación de radio para la mitigación de interferencias en redes de malla inalámbricas", preimpresión de arXiv arXiv:1503.04533, 2015. [En línea]. Disponible: https://arxiv.org/abs/1503.04533

[8] J. L. Muñoz, "Análisis de Desempeño en Redes WLAN: Estudio de Caso", Universidad Católica de Colombia, 2014. [En línea]. Disponible: https://repository.ucatolica.edu.co/bitstream/10983/1300/3/Articulo_trabajo%20de%20grado.pdf

[9] R. A. Lara Cueva, C. B. Fernández Jiménez, C. A. Morales Maldonado, "Análisis de rendimiento en un enlace descendente de redes basado en los estándares IEEE 802.11b, IEEE 802.11n y WDS", Reci, vol. 5, núm. 10, 2016. [En línea]. Disponible: https://www.reci.org.mx/index.php/reci/article/view/92/404

[10] L. F. Pedraza, "Consideraciones para la implementación de la voz sobre WLAN", Universidad Industrial de Santander, 2006. [En línea]. Disponible: https://noesis.uis.edu.co/bitstreams/33e56af9-f5b4-44d7-8572-ffc4339b29b8/download

MASKAY 16(1), May 2026
ISSN 1390-6712

Recibido (Received): 2025/04/21
Aceptado (Accepted): 2025/07/19

Análisis sistemático de protocolos de seguridad de datos en el cloud computing: Revisión de la literatura

Systematic analysis of data security protocols in cloud computing: Literature review

Kevin Zambrano and Denise Vera

***Abstract*—This paper presents a systematic review of relevant studies published between 2019 and 2024, focusing on data security protocols in cloud computing environments. The selection process was based on rigorous criteria to identify the most relevant features of these protocols and their current applications. The review examines their advantages as well as the cryptographic mechanisms used to protect sensitive data, including Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC). Additionally, the increasing use of Kubernetes as a container orchestration tool is analyzed, acknowledging its significance in modern cloud infrastructures. Within this context, several studies are reviewed that highlight implementation limitations such as inadequate privilege management and the reliance on third-party solutions. This research aims to provide a comprehensive understanding of current trends and challenges in cloud data security and to support the identification of potential strategies to address these issues and enhance the robustness of cloud-based security architectures.**

***Index Terms*—Cloud security, security protocols, data encryption, Cloud Computing, Kubernetes.**

***Resumen*—Este trabajo presenta una revisión sistemática de estudios relevantes publicados entre los años 2019 y 2024, centrados en los protocolos de seguridad de datos en entornos de computación en la nube. La selección de artículos se realizó mediante criterios rigurosos, con el objetivo de identificar las características más destacadas de estos protocolos y sus aplicaciones actuales. Se analizan tanto sus ventajas como los mecanismos criptográficos utilizados para proteger la información sensible, entre los que se encuentran AES, RSA y ECC. Adicionalmente, se considera el creciente uso de Kubernetes como herramienta de orquestación de contenedores, reconociendo su importancia dentro de las infraestructuras modernas en la nube. En este contexto, se examinan diversas publicaciones que evidencian limitaciones en su implementación, tales como la gestión inadecuada de privilegios y la dependencia de soluciones de terceros. El estudio ofrece una visión integral que facilite la comprensión de los desafíos actuales y oriente la búsqueda de soluciones que fortalezcan la seguridad en entornos cloud.**

***Palabras Claves*—Seguridad en la nube, protocolos de seguridad, cifrado de datos, computación en la nube, Kubernetes.**

Kevin Zambrano and Denise Vera are with the Facultad de Ciencias Informática, Universidad Tecnica de Manabí, Manabí, Ecuador (e-mail: {kzambrano0732 , denise.vera}@utm.edu.ec).

I. Introducción

El cloud computing es una forma de trabajo que ha transformado los métodos mediante los cuales las empresas procesan, administran y almacenan datos, aprovechando su flexibilidad, escalabilidad y reducción de costos. Este entorno ha permitido la reducción de costos operativos y ha facilitado el acceso a recursos computacionales avanzados sin la necesidad de costear una infraestructura física propia.

Sin embargo, estas compañías enfrentan preocupaciones importantes relacionadas con la seguridad de los datos, debido a la rápida adopción de esta tecnología, la creciente amenaza de ataques informáticos más sofisticados y la posible exposición de datos sensibles en entornos compartidos.

Las amenazas en la seguridad de la nube son diversas, incluyendo el acceso no autorizado, la filtración de datos, ataques de denegación de servicio y la manipulación de información. Estas vulnerabilidades crean brechas en la confidencialidad, integridad y disponibilidad de los datos, lo que crea un gran desafío para las organizaciones que manejan información crítica.

En este contexto, los protocolos de seguridad fueron diseñados para mitigar estos riesgos proporcionando diversas técnicas de autenticación, cifrado y control de acceso que buscan garantizar la protección de los datos en el entorno cloud. A medida que un mayor número de empresas adopta la tecnología en la nube, enfrentan desafíos relacionados con su implementación. Esto genera incertidumbre en las organizaciones sobre la delegación de datos sensibles al entorno cloud, ya que existen muchos riesgos asociados a la privacidad y seguridad [1].

Para reducir esta incertidumbre, se realizó una revisión sistemática de los protocolos de seguridad de datos en el entorno de cloud computing, utilizando la literatura disponible en los últimos años. La gran cantidad de protocolos de seguridad existentes, la variabilidad de su efectividad y los requisitos para su aplicación complican la tarea de seleccionar e implementar la solución más adecuada. Considerando esto, la criptografía es un método ampliamente usado para solidificar la seguridad de la información [2] y suele ser

DOI: 10.24133/maskay.v16i1.4150

incluida como parte integral de varios protocolos.

Este trabajo tuvo como objetivo ofrecer un panorama más amplio sobre los protocolos de seguridad de datos existentes y ofrecer recomendaciones para la mejora de las estrategias actuales y orientar futuras investigaciones en el área. La correcta implementación de medidas de seguridad en la nube es fundamental para garantizar la confianza de las organizaciones y sus usuarios en los servicios cloud, ofreciendo un entorno más seguro y eficiente para el manejo de la información.

Considerando lo mencionado, el estudio analizó de manera sistemática los protocolos de seguridad de datos en el cloud computing, evaluando sus características y técnicas de encriptación utilizadas. Se buscó identificar las estrategias de cifrado más usadas, las principales características de dichos protocolos, así como las limitaciones que presenta la infraestructura basada en Kubernetes dentro del cloud computing. Para ello, se realizó una revisión de la literatura académica reciente, seleccionando estudios relevantes publicados en los últimos cinco años.

II. Trabajos Relacionados

Las amenazas a la seguridad de los datos han impulsado investigaciones en torno a métodos de protección, identificación de vulnerabilidades y aplicación de normativas internacionales como las normas ISO/IEC 27001. Sin embargo, la mayoría de los estudios se han centrado en la seguridad general de la información en la nube, sin profundizar en los protocolos específicos de seguridad de datos. A continuación, se presenta un análisis de investigaciones recientes relacionadas.

En 2020, Kumar y Bhatia, de la Netaji Subhas University of Technology, llevaron a cabo un análisis de diversos métodos para reducir riesgos como la filtración o alteración de datos [3]. Su estudio concluyó que la mejora en la seguridad requiere la incorporación de estrategias innovadoras en la transferencia y almacenamiento de datos, más allá de los métodos tradicionales.

En paralelo, el mismo año, en la Charotar University of Science and Technology, Patel, Shah, Ramoliya y Nayak llevaron a cabo una revisión sobre amenazas, ataques y problemas de seguridad en cloud computing [1]. Identificaron ocho problemas de seguridad, veinte amenazas y once formas de ataque. Señalaron que la rápida adopción del entorno de la nube sin un análisis de riesgos adecuado puede generar vulnerabilidades significativas para las organizaciones.

En 2021, Pérez Reyes llevó a cabo una evaluación sobre seguridad informática en la adopción del cloud computing en la industria alimentaria [4]. Aplicando las normas ISO 2009 y 2013, determinó que existe una relación directa entre la integridad de los datos y los controles de acceso, además de identificar debilidades en la implementación de medidas de seguridad.

En 2020, Torres González realizó un estudio en Bogotá, Colombia, enfocado en los componentes de seguridad implementados por pequeñas y medianas empresas (pymes) que adoptan soluciones de cloud computing [5]. Su estudio encontró que los proveedores de servicios en la nube cuentan con medidas de protección contra alteraciones de datos, suplantación de identidad y ataques de denegación de servicio. Además, subrayó la importancia de que tanto proveedores como clientes implementen planes de recuperación ante desastres y mecanismos de control de acceso.

III. Metodología

Para la presente revisión sistemática de la literatura, se estableció dividir la metodología en tres fases secuenciales: planificación, realización y resultados.

Dicha división facilitó estructurar el proceso de búsqueda, filtrado y análisis de estudios relevantes de manera sistemática y coherente con los objetivos del trabajo.

A. Planificación

Durante esta fase se formularon las preguntas de investigación que guiarían todo el proceso:

- Q1: ¿Cuál es la ventaja del protocolo en específico para asegurar los datos en el cloud computing?
- Q2: ¿Cuáles son las medidas de seguridad con técnicas de cifrado más utilizadas en la protección de datos en cloud computing, según los estudios revisados en los últimos cinco años?
- Q3: ¿Cuáles son las limitaciones que presenta la seguridad de datos en cloud computing en la infraestructura Kubernetes?

A partir de estas preguntas, se establecieron las palabras clave en inglés: “Cloud Computing", "security data”, "data security", "Protocol", "encrypted", "Kubernetes", "K8s", "security", "cloud", "Container". Estas palabras se combinaron para crear dos cadenas de búsqueda que se aplicaron en las bases de datos Scopus y IEEE Xplore. Las combinaciones se diseñaron para maximizar la cobertura temática, empleando operadores booleanos adecuados. Los detalles de las cadenas de búsqueda ejecutadas se presentan en la Tabla I.

Tabla I
Cadenas de búsqueda utilizadas en las bases de datos Scopus e IEEE Xplore para la recopilación de literatura relacionada

Fuente	Primera cadena de búsqueda	Segunda cadena de búsqueda
Scopus	("Cloud Computing" AND ("security data" OR "data security") AND ("Protocol" OR "encrypted"))	("Kubernetes" OR "K8s") AND "security" AND ("cloud" OR "Container")
IEEE Xplore	("Cloud Computing" AND ("security data" OR "data security") AND ("Protocol" OR "encrypted"))	("Kubernetes" OR "K8s") AND "security" AND ("cloud" OR "Container")

Solo se consideraron exclusivamente publicaciones entre 2019 y 2024 y se priorizaron las publicaciones en revistas científicas y actas de conferencias. Los criterios de inclusión y exclusión se detallan a continuación en la Tabla II.

Tabla II

CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN UTILIZADOS PARA FILTRAR LOS ARTÍCULOS RELEVANTES

# Inclusión	# Exclusión
Publicaciones de los últimos 5 años	Análisis o revisión
Ponencias o publicaciones en revistas científicas	Enfoque no relevante al almacenamiento o transferencia de datos
Enfoque en implementación y mejoramiento	Artículo restringido.
elación con el uso de Kubernetes	No relacionado con cloud computing.

B. Realización

Los resultados obtenidos fueron sometidos a filtros conforme a los criterios de inclusión y exclusión definidos en la Tabla II. El proceso se divide en dos etapas, una automatizada basada en criterios del idioma, disponibilidad del artículo y tipo de documento. La segunda etapa fue manual, donde se incluyó una lectura preliminar de título, resumen y palabras clave para evaluar la relación temática de los estudios.

Los estudios preseleccionados fueron analizados en mayor profundidad en la introducción, metodología y conclusiones. Este procedimiento permitió una depuración progresiva, lo que redujo el total inicial de 4132 artículos a una muestra final de 43 estudios relevantes. Este proceso se detalla en la Tabla III y en la Fig. 1.

TABLA III
PROCESO DE FILTRADO DE ARTÍCULOS DESDE LA BÚSQUEDA INICIAL HASTA LA SELECCIÓN FINAL

Scopus	IEEE Xplore	Descripción
1354	2778	Ejecución de las cadenas de búsqueda
961	1694	Filtros (año, idioma, tipo de documento)
151	310	Filtro resumen, título, palabras clave y criterios de inclusión y duplicados.
22	21	Filtro introducción, metodología y conclusiones.

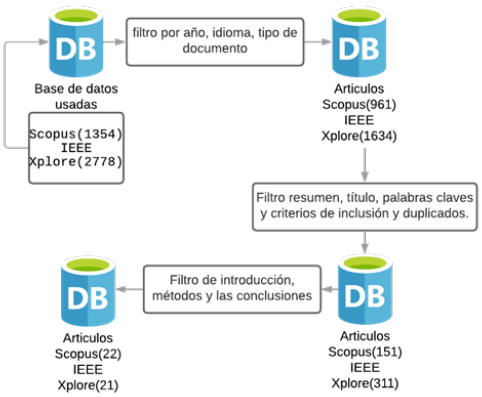


Fig. 1. Proceso de selección de artículos desde la búsqueda inicial hasta la muestra final de estudios relevantes. Visualización basada en los datos de la Tabla III.

En la Fig. 2 se muestra el total de artículos recuperados en la búsqueda. Se observa que en IEEE se encontraron mayor cantidad de artículos, esto debido a la especialización de la base de datos en la tecnología, mientras que en Scopus el total de resultados es más de la mitad de los encontrados en IEEE Xplore.

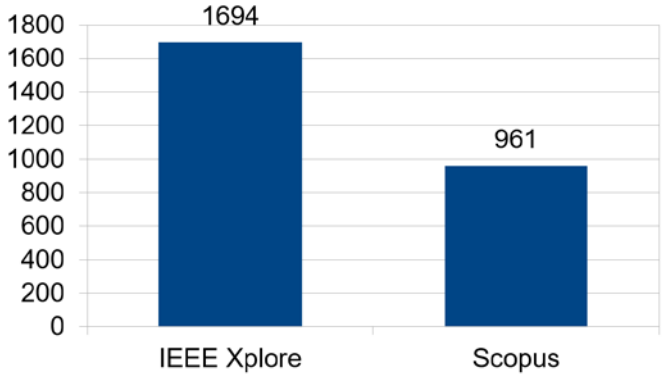


Fig. 2. Comparativa del total de artículos encontrados por base de datos.

La Fig. 3 muestra la tendencia de publicación por año de los artículos encontrados. Se puede observar cómo las publicaciones desde 2020 tienden a subir hasta 2024, donde se presenta una bajada en las publicaciones, lo cual puede atribuirse a la fecha en la que se realizó la búsqueda, que fue antes de la finalización del año 2024.

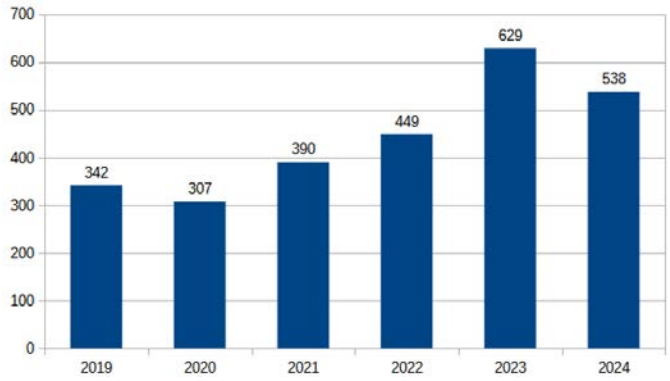


Fig. 3. Tendencia anual de publicaciones encontradas. Se evidencia un aumento progresivo hasta 2023, con una caída parcial en 2024 atribuible al momento de cierre de la búsqueda.

En la Tabla IV se aprecia el cambio de los potenciales estudios del período de tiempo de 2019 a 2024, a los que se usaron para el trabajo.

TABLA IV
NÚMERO DE ARTÍCULOS POTENCIALES Y SELECCIONADOS POR BASE DE DATOS. REFLEJA EL RESULTADO DEL PROCESO DE FILTRADO APLICADO A SCOPUS E IEEE XPLORE

Fuente	Estudios potencialmente elegibles	Estudios seleccionados
Scopus	961	22
IEEE Xplore	1634	21

La Fig. 4 muestra cómo la cantidad de artículos seleccionados después de aplicar los filtros, criterios de

exclusión y revisión de los artículos, lo cual resultó en una selección final de 22 artículos de Scopus y 21 de IEEE Xplore.

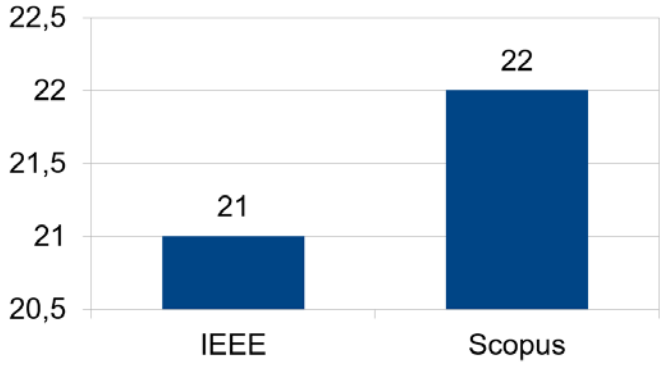


Fig. 4. Distribución final de los 43 artículos seleccionados por base de datos. Scopus e IEEE aportaron proporciones similares.

La Fig. 5 presenta cómo los artículos seleccionados tendieron a disminuir con el paso de los años desde su publicación original, lo que no implica que los artículos recientes sean menos relevantes, sino que no se ajustaban a los objetivos del estudio.

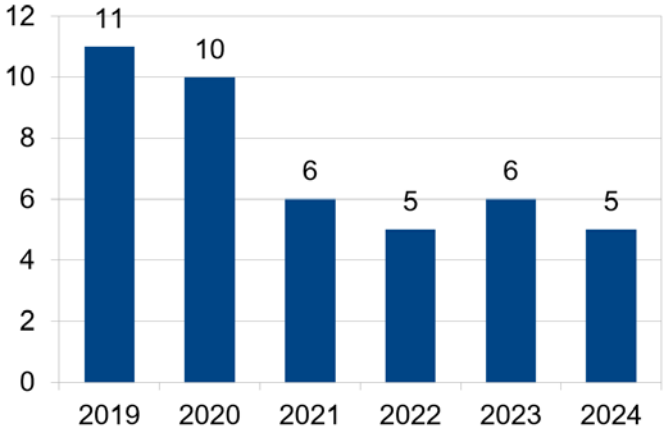


Fig. 5. Evolución anual de los artículos seleccionados. Se observa menor presencia de estudios recientes, sin que ello implique una menor relevancia científica.

C. Resultados

La muestra final de los 43 artículos se utilizó para responder las tres preguntas de investigación. Para Q1 se identificaron y clasificaron protocolos de seguridad en cloud computing según sus características. En Q2, se extrajeron las técnicas de cifrado empleadas y su frecuencia de uso. Finalmente, para Q3, se revisaron estudios que abordaron limitaciones en Kubernetes, permitiendo consolidar un conjunto de vulnerabilidades comunes. Este proceso está desarrollado de forma más clara en la Sección IV.

IV. Resultados

Q1. ¿Cuál es la ventaja del protocolo en específico para asegurar los datos en el cloud computing?

Tabla V

Protocolos de seguridad analizados y sus características, organizadas según: detección de seguridad, control de acceso, privacidad, integridad, resistencia a ataques y descentralización

Protocolo	c1	c2	c3	c4	c5	c6
[6]		✓		✓	✓	
[7]		✓	✓	✓	✓	
[8]		✓	✓		✓	
[9]		✓	✓	✓	✓	✓
[10]		✓	✓	✓	✓	
[11]				✓	✓	
[12]	✓			✓	✓	
[13]		✓	✓		✓	
[14]		✓		✓	✓	
[15]		✓	✓		✓	✓
[16]		✓	✓			
[17]		✓	✓		✓	
[18]		✓	✓			

c1=Detección de seguridad, c2=Control de acceso, c3=Anonimato y Privacidad, c4=Integridad de datos, c5=Resistencia a ataque, c6=Descentralizado

Como se puede observar en la TABLA V en el análisis de 13 protocolos identificados [6]-[18].

Siguiendo el orden de la TABLA V los protocolos incluidos son protocolo de intercambio seguro de datos médicos en el entorno de WBAN asistido por la nube, protocolo de seguridad de datos para terceros de confianza semiautorizados (ADSS), protocolo de autenticación robusta para infraestructura de salud en la nube basada en iomt (RAPCHI), protocolo de ias basado en blockchain, autenticación de servicios inteligentes (SSA), protocolo eficiente de intersección privada de conjuntos para entornos en la nube, Sec-Manage, protocolo ligero y seguro para sistemas de salud electrónica (LSP–eHS), protocolo de preservación de privacidad en nube con EDAC-MAC, agrupamiento y gestión multiagencia, construcción de un protocolo de acuerdo de claves para infraestructura médica en la nube utilizando blockchain (CKMIB), protocolo de gestión de claves de grupo de intercambio de secretos (SSGK), protocolo de clasificación SVM privado en la nube, Control de Acceso Distribuido anónimo finamente granular con decifrado verificable en la nube pública (VOD-ADAC),

Se puede destacar que el protocolo llamado Sec-Manage [12] incorpora una técnica para implementar detección de seguridad; el protocolo emplea un modelo de interacción basado en políticas, el cual establece cómo deben interactuar las entidades en el entorno cloud. Esto permite supervisar las interacciones en tiempo real y detectar comportamientos anómalos. Además, esta capacidad permite mantener la integridad de los datos y proporciona resistencia a ciertos ataques maliciosos.

Once de los protocolos: [6], [7], [8], [9], [10], [13], [14], [15], [16], [17], [18], ofrecen mecanismos de control de acceso. Nueve protocolos analizados [7], [8], [9], [10], [13], [15], [16], [17], [18] implementan o proponen técnicas o procesos para asegurar el anonimato y la privacidad de los usuarios. Siete [6], [7], [9], [10], [11], [12], [14] incluyen métodos para mantener la integridad de los datos.

Este aspecto es clave, junto con el control de acceso y la

privacidad, para entornos de salud, donde solo el paciente y el médico tratante deben tener acceso.

De los protocolos analizados, once [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [17] proporcionan resistencia a uno o varios tipos de ataques maliciosos externos o internos como se puede ver en la Tabla VI a continuación.

TABLA VI
PROTOCOLOS DE SEGURIDAD Y SU RESISTENCIA A DIVERSOS ATAQUES ORGANIZADOS POR EXTERNOS E INTERNOS

Protocolo	Ataques de seguridad							
	Externos					Internos		
	a1	a2	a3	a4	a5	a6	a7	a8
[6]	✓	✓	✓	✓	✓		✓	✓
[7]	✓	✓	✓	✓	✓			
[8]	✓	✓	✓	✓	✓	✓	✓	✓
[9]	✓	✓	✓		✓		✓	✓
[10]	✓	✓	✓	✓	✓			
[11]	✓	✓						
[12]	✓	✓			✓			✓
[13]	✓	✓	✓		✓	✓		✓
[14]	✓	✓	✓	✓	✓			
[15]	✓	✓	✓	✓	✓	✓	✓	✓
[17]					✓			

a1 =Intercepción, a2 =Repetición de mensajes, a3 = Man-in-the-middle, a4 = Divulgación de clave de sesión, a5 =Frescura de clave y secreto perfecto hacia adelante, a6 = Ataque interno, a7 =Fuga de seguridad efímera a8 =Ataques relacionados con secretos compartidos y parámetros del protocolo

Dos de los protocolos [9], [15] tienen aspectos descentralizados mediante tecnología blockchain.

En situaciones específicas, los protocolos otorgan sólo un marco general, lo que permite la implementación o personalización. Por ejemplo, el protocolo de intercambio seguro de datos médicos en el entorno de WBAN asistido por la nube [6], el cual recomienda el uso de una clave simétrica para el cifrado y descifrado.

Se observa que los principales aspectos que un protocolo de seguridad de datos en el cloud computing priorizan mantener un control de acceso a los datos, la privacidad mediante anonimato de los datos, la integridad frente a cambios no autorizados y la resistencia a los ataques tanto externos como internos.

Q2. ¿Cuáles son las medidas de seguridad con técnicas de cifrado más utilizadas en la protección de datos en cloud computing, según los estudios revisados en los últimos cinco años?

En los estudios analizados se reporta el uso de diversas técnicas de cifrado, tanto simétricas como asimétricas, empleadas para garantizar la seguridad de los datos en entornos de computación en la nube.

A continuación, se describe cada técnica, considerando su funcionamiento general, aplicación y frecuencia de uso en los artículos revisados.

TABLA VII
TÉCNICAS DE ENCRIPTADO IDENTIFICADAS EN LOS ESTUDIOS REVISADOS. SE DETALLAN EL TIPO DE CIFRADO, NÚMERO DE ESTUDIOS EN LOS QUE SE UTILIZAN Y LAS FUENTES CORRESPONDIENTES

#	Encriptación	Número de usos	Fuentes
1	Asimétricos no especificados	2	[8],[19]
2	Simétricos no especificados	4	[18],[6], [8], [9]
3	Hash	3	[8], [13], [18]
4	AES (Advanced Encryption Standard)	1	[16]
5	Cifrado homomórfico	2	[11],[17]
6	RSA	2	[10],[16]
7	3DES	1	[14]
8	Elliptic Curve Cryptography (ECC)	3	[13],[15],[10]
9	Hyper Elliptic Curve Cryptography (HECC)	1	[9]
10	Identity-based encryption	1	[17]
11	proxy re-encryption	1	[6]
12	Attribute-Based Encryption (ABE)	2	[18],[20]
13	Simétricos totales	6	[18],[6], [8], [19],[14],[16]
14	Asimétricos totales	11	[8],[19],[13],[15],[10],[9],[18],[20],[10],[16],[17]

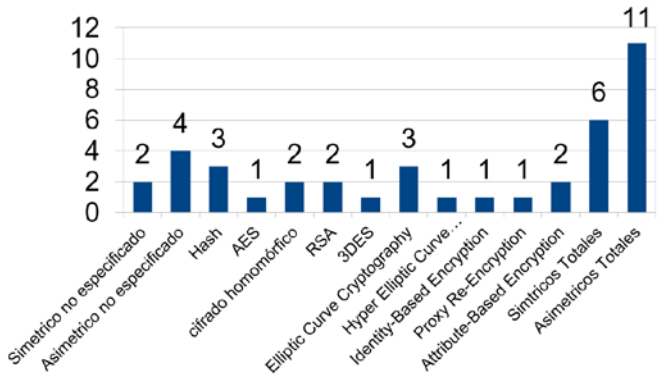


Fig. 6. Técnicas de encriptación representadas en barras según el total de veces implementadas en los estudios analizados.

AES (Advanced Encryption Standard) es un algoritmo de cifrado simétrico ampliamente adoptado por su eficiencia, velocidad y nivel de seguridad. Resulta especialmente adecuado para el cifrado de grandes volúmenes de datos. Fue reportado en el estudio [16], donde se empleó para proteger la información almacenada en entornos cloud.

RSA (Rivest-Shamir-Adleman) constituye uno de los algoritmos de cifrado asimétrico más ampliamente utilizados en entornos de seguridad digital. Se basa en la dificultad computacional de factorizar grandes números primos y se emplea con frecuencia para el intercambio seguro de claves en arquitecturas distribuidas. Su uso fue identificado en dos de los estudios revisados [10], [16].

ECC (Elliptic Curve Cryptography) es un método de cifrado asimétrico que ofrece altos niveles de seguridad utilizando claves de menor longitud, lo que lo convierte en una opción eficiente en términos de rendimiento. Esta técnica fue empleada en tres de los estudios revisados [10], [13], [15].

HECC (Hyper Elliptic Curve Cryptography) es una variante de ECC que utiliza curvas hiperelípticas para ofrecer una

mayor complejidad matemática y, potencialmente, una mayor seguridad. Se identificó en un único estudio [9].

3DES (Triple Data Encryption Standard) representa una evolución del algoritmo DES, en la cual el proceso de cifrado se aplica tres veces consecutivas sobre cada bloque de datos, lo que incrementa la robustez frente a ataques de fuerza bruta. Aunque ofrece un nivel de seguridad superior al de su predecesor, presenta desventajas significativas en términos de eficiencia y rendimiento frente a algoritmos más modernos, como AES. Esta técnica fue reportada en un estudio [14].

El cifrado homomórfico permite realizar operaciones matemáticas directamente sobre datos cifrados sin necesidad de desencriptarlos previamente, lo cual resulta especialmente útil en contextos donde se requiere preservar la confidencialidad durante el procesamiento de datos. Esta técnica fue mencionada en dos estudios [11], [17].

Las funciones hash se utilizaron de manera complementaria a otros esquemas de cifrado con el fin de asegurar la integridad de los datos. Su implementación fue identificada en tres estudios [8], [13], [18].

Attribute-Based Encryption (ABE) es una técnica de cifrado asimétrico que permite establecer políticas de acceso detalladas basadas en atributos específicos del usuario. De esta forma, se ofrece un mayor control sobre quién puede acceder a determinados datos. Se identificó en dos estudios [18], [20].

Identity-Based Encryption (IBE) permite generar claves públicas a partir de la identidad del usuario, lo cual simplifica la gestión de certificados y facilita la distribución de claves. Esta técnica fue mencionada en un estudio [17].

Proxy Re-Encryption es un mecanismo mediante el cual un tercero autorizado puede transformar un mensaje cifrado para que sea accesible por un nuevo destinatario, sin necesidad de revelar el contenido original. Fue identificada en un estudio [6].

También se identificaron varios estudios [6], [8], [9], [18], [19] en los que se alude al uso de técnicas de cifrado simétrico o asimétrico sin especificar. En estos casos, los autores se limitaron a señalar el uso de cifrado de forma general, lo que indica flexibilidad en la elección de la técnica, determinada por los requisitos específicos del entorno de aplicación.

En conjunto, las técnicas identificadas reflejan una diversidad de enfoques y soluciones tecnológicas orientadas a fortalecer la seguridad de los datos en el contexto de la computación en la nube, especialmente en lo que respecta a la confidencialidad, integridad y control de acceso. El uso recurrente de algoritmos como ECC, RSA y ABE indica una tendencia hacia mecanismos criptográficos robustos, eficientes y adaptables a distintos escenarios de implementación.

Para concluir las dos primeras preguntas, a continuación, se presenta una tabla sintetizada con los estudios analizados correspondientes a las dos primeras preguntas de investigación, Q1 y Q2, donde se resumen las técnicas de cifrado usadas y las características reforzadas o agregadas en el estudio.

TABLA VIII

ESTUDIOS ANALIZADOS, TÉCNICAS DE CIFRADO IMPLEMENTADAS Y ASPECTOS REFORZADOS

Fuente	Técnicas de cifrado implementadas
[6]	Cifrado simétrico no especificado, Proxy re-encryption
[7]	No aplica.
[8]	Hash, Asimétrico no especificado, Simétrico no especificado
[9]	Simétrico no especificado, Hyper Elliptic Curve Cryptography (HECC)
[10]	Elliptic Curve Cryptography (ECC), RSA
[11]	Cifrado homomórfico
[12]	No aplica
[13]	Elliptic Curve Cryptography (ECC), Hash.
[14]	3DES
[15]	Elliptic Curve Cryptography (ECC)
[16]	AES (Advanced Encryption Standard), RSA
[17]	Cifrado homomórfico, Identity-based encryption
[18]	Simétricos no especificado, Attribute-Based Encryption (ABE)
[19]	Asimétricos no especificado,
[20]	Attribute-Based Encryption (ABE)

Q3. ¿Cuáles son las limitaciones que presenta la seguridad de datos en cloud computing en la infraestructura Kubernetes?

TABLA IX

COMPILACIÓN DE DEBILIDADES TÉCNICAS IDENTIFICADAS EN ESTUDIOS RECIENTES SOBRE KUBERNETES

Fuente	Limitación encontrada
[19]	Falta de soporte para cifrado
[21]	Seguridad de la Infraestructura Compartida
[22]	Sustitución de imágenes de contenedor
[23]	Abuso de privilegios
[24]	Dependencia de Soluciones de Terceros
[25]	Dependencia de Soluciones de Terceros
[26]	Abuso de privilegios
[27]	Complejidad en la Gestión Global
[28]	Limitaciones en la monitorización
[29]	Dependencia de Soluciones de Terceros
[30]	Limitaciones en la monitorización
[31]	Contención de Memoria de Enclave
[32]	Seguridad de la Infraestructura Compartida
[33]	Seguridad de la Infraestructura Compartida, Contención de Memoria de Enclave
[34]	Inconsistencias en la Configuración de Seguridad
[35]	Distribución desigual de carga
[36]	Asignación estática de recursos
[37]	Asignación estática de recursos
[38]	Abuso de privilegios
[39]	Limitaciones en la monitorización
[40]	Dependencia de Soluciones de Terceros
[41]	Configuraciones Inseguras por Defecto
[20]	Abuso de privilegios
[42]	Configuraciones Inseguras por Defecto
[43]	Enfoque Reactivo en Seguridad
[44]	Dependencia de Soluciones de Terceros, Seguridad de la Infraestructura Compartida
[45]	Inconsistencias en la Configuración de Seguridad
[46]	Sustitución de imágenes de contenedor, Gestión de contenedores infectados
[47]	Configuraciones Inseguras por Defecto
[48]	Configuraciones Inseguras por Defecto, Abuso de privilegios
[49]	Configuraciones Inseguras por Defecto

En el análisis basado en los problemas que las propuestas de los artículos buscaron resolver, se identificaron múltiples

limitaciones, desafíos o problemas que afectan la seguridad de datos en Kubernetes los cuales se en listan a continuación:

Falta de soporte para cifrado, infraestructura compartida, abuso de privilegios, dependencia de soluciones de terceros, complejidad en la gestión global, limitaciones en la monitorización, contención de memoria de enclave, seguridad de la infraestructura compartida, asignación estática de recursos, inconsistencias en la configuración de seguridad.

Los más mencionados son la dependencia de soluciones de terceros y la configuración insegura por defecto, abuso de privilegios, infraestructura compartida.

El estudio realizado por Stoyanov et al. [19] señala cómo los checkpoints generados por defecto en Kubernetes no están encriptados y para esto se usa una herramienta de CRIU (Checkpoint/Restore In Userspace) para congelar el estado del contenedor y cifrarlo de forma que se aseguran los datos.

En el estudio donde se aborda los riesgos de la seguridad en las nubes basadas en contenedores, específicamente cómo las llamadas a un sistema vulnerable pueden ser explotadas por contenedores maliciosos, se identifica el problema del vecino ruidoso (noisy neighbor) [21], en el que múltiples usuarios comparten el mismo cluster y generan llamadas al sistema vulnerable que pueden interferir entre sí, abriendo vectores de ataques a nivel de sistema.

Los estudios realizados por Pecka et al. [23] y Santos et al. [48] expresan una preocupación por un posible abuso de privilegios en un entorno de Kubernetes ya sea mediante el despliegue de programas maliciosos o la acumulación de cargas de trabajo privilegiado que deja expuestos los datos con los que se trabaja. Estas situaciones se relacionan con un pobre aislamiento entre contenedores, que se puede mitigar poniendo políticas de comunicación más estrictas entre los elementos orquestados por Kubernetes.

Por su parte, Bringhenti et al. [27] menciona que en los entornos que ejecutan programas en paralelo, dificulta la gestión global y que, si no se hace de forma adecuada, crea brechas de seguridad. Esto evidencia cómo la escalabilidad, aunque ventajosa, también introduce retos en cuanto a coordinación y aislamiento.

El estudio de Lim et al. [25] destaca que Kubernetes no dispone de un mecanismo nativo para gestionar el ciclo de vida de las máquinas virtuales. Lo que obliga a recurrir a soluciones externas, como las que ofrece la plataforma OpenStack para la creación y gestión de entornos en la nube.

El estudio donde Karn et al. [49] documenta configuraciones predeterminadas inseguras que otorgan privilegios elevados a los contenedores, lo cual amplifica el riesgo de escalamiento de privilegios si no se controlan con políticas de acceso estrictas.

También se mencionan limitaciones como la falta de migración de procesos en vivo, gestión de versiones y problemas en la asignación de recursos. Estas limitaciones son incluidas como parte de la dependencia de soluciones de terceros.

Cabe destacar que una buena parte de las limitaciones existentes pueden mitigarse con herramientas externas y un cuidado adecuado de las políticas de aislamiento, pero esto refuerza el problema original, ya que la seguridad de Kubernetes depende en gran medida de soluciones de terceros, lo que puede convertirse en una fuente adicional de riesgo si dichas herramientas no están correctamente integradas ni validadas.

Finalmente, la Tabla IX muestra la recurrencia en la que se encontraron las limitaciones de Kubernetes

TABLA X
RECURRENCIA DE LIMITACIONES ENCONTRADAS EN LA INFRAESTRUCTURA KUBERNETES SEGÚN LOS ESTUDIOS REVISADOS

Limitación encontrada	Veces encontrada	Fuente
Falta de soporte para cifrado	1	[19]
Seguridad de la Infraestructura Compartida	4	[21], [32], [33], [44]
Sustitución de imágenes de contenedor	2	[22], [46]
Abuso de privilegios	5	[20], [23], [26], [38], [48]
Dependencia de Soluciones de Terceros	5	[24], [25], [29], [40], [44]
Complejidad en la Gestión Global	1	[27]
Limitaciones en la monitorización	3	[28], [30], [39]
Contención de Memoria de Enclave	2	[31], [33],
Inconsistencias en la Configuración de Seguridad	2	[34], [45]
Distribución desigual de carga	1	[35]
Asignación estática de recursos	2	[36], [37]
Configuraciones Inseguras por Defecto	5	[41], [42], [47], [48], [49]
Enfoque Reactivo en Seguridad	1	[43]
Gestión de contenedores infectados	1	[46]

V. DISCUSIÓN

El análisis de los protocolos de seguridad de datos en cloud computing evidencia avances significativos en aspectos como el control de acceso y la integridad de los datos, logrados mediante el uso de tecnologías emergentes como la blockchain.

Aun así, se presentan oportunidades de mejora, particularmente en el monitoreo preventivo de anomalías, como se señala en el trabajo de Farahmandian et al. [12], previniendo ataques externos o comprometer la integridad de los datos. El uso de blockchain como herramienta para evitar el acceso no autorizado o la modificación de los datos es prometedor; sin embargo, la dificultad que presenta su implementación y sus altos costos asociados desalienta la normalización de su uso.

Respecto a la segunda pregunta de investigación, entre las técnicas criptográficas analizadas, ECC destaca por ofrecer un alto nivel de seguridad con claves más cortas, lo que mejora la eficiencia. A pesar de esto, su implementación enfrenta obstáculos relacionados con la compatibilidad con sistemas, lo que restringe su adopción en infraestructuras existentes.

En contraste, ABE permite definir políticas de acceso detalladas basadas en atributos, lo que proporciona

flexibilidad en la gestión de datos confidenciales, aunque presenta mayor complejidad operativa y coste computacional.

Por su parte, RSA, a pesar de su amplia adopción, presenta desventajas en términos de rendimiento, especialmente en entornos que requieren alta escalabilidad, como los entornos cloud. Estas diferencias reflejan que no existe una solución universal, y que la elección del protocolo debe estar alineada con las necesidades técnicas y operativas de cada caso.

Además, se identificó el uso de cifrado homomórfico y proxy re-encryption como mecanismos avanzados, que permiten preservar la confidencialidad sin sacrificar flexibilidad. No obstante, estos enfoques suelen implicar una carga computacional elevada, lo que limita su adopción en entornos productivos. Asimismo, varios artículos no especifican la técnica de cifrado utilizada, lo que refleja una flexibilidad intencionada en la integración de algoritmos criptográficos.

En el caso de Kubernetes, si bien proporciona ventajas en la escalabilidad y gestión de recursos, existen vulnerabilidades que lo acompañan. Las configuraciones por defecto inseguras facilitan el abuso de privilegios y una exposición de los datos sensibles.

Cabe mencionar que otra limitación frecuente es la dependencia de herramientas externas para la monitorización, dado que la supervisión nativa de Kubernetes se considera insuficiente por varios autores. Esta dependencia aumenta los posibles puntos de fallo. No obstante, se destaca que muchos de los problemas encontrados se pueden atribuir a la dependencia de soluciones de terceros. Existen herramientas que solucionan y facilitan lidiar con las limitaciones presentadas por Kubernetes, pero esto genera vulnerabilidades si no se seleccionan herramientas confiables.

En consecuencia, resulta fundamental avanzar en el desarrollo de mecanismos de seguridad nativos para Kubernetes, así como en la estandarización de configuración segura que reduzcan la necesidad de herramientas externas.

También se observó la ausencia de pruebas comparativas de rendimiento de las técnicas de cifrado en entornos orquestados con Kubernetes. Realizar evaluaciones en este tipo de entornos sería clave, proporcionando resultados relevantes que podrían orientar el desarrollo de futuros protocolos de seguridad adaptados a plataformas distribuidas.

En conjunto, los hallazgos indican que la seguridad en el cloud computing requiere un enfoque integral que combine múltiples estrategias y tecnologías para hacer frente a los riesgos actuales.

En este sentido, futuras investigaciones podrían centrarse en la adaptación de algoritmos de cifrado en entornos cloud orquestados, en análisis comparativo o en el desarrollo de soluciones integradas que refuercen el aislamiento entre contenedores, y optimicen el monitoreo sin comprometer el rendimiento del sistema.

VI. Conclusiones

El presente análisis sistemático de los protocolos de seguridad de datos en cloud computing permitió identificar las principales estrategias utilizadas para garantizar la protección de la información. Se evidenció la existencia de múltiples protocolos con características específicas, cuyo grado de efectividad depende del contexto de implementación y del nivel de riesgo asumido.

Uno de los hallazgos más relevantes encontrados es el uso creciente de los algoritmos de encriptado asimétricos y, en menor medida, simétricos, para asegurar los datos en su transferencia y almacenamiento, como el encriptado ECC, RSA y ABE. También se identificó el uso de características y técnicas como el cifrado homomórfico o el empleo de proxy de re-encriptado, que proporcionan una capa adicional de seguridad y flexibilidad en la gestión de acceso, lo cual contribuye a un control más seguro de los datos.

Se le identificaron en Kubernetes limitaciones relacionadas con el abuso de privilegios, configuraciones inseguras por defecto y la dependencia de soluciones de terceros. Esto demuestra la necesidad de fortalecer la personalización de la seguridad en los entornos de orquestación de contenedores, así como de seleccionar cuidadosamente las herramientas empleadas y contar con personal técnico capacitado.

Según los hallazgos, las organizaciones deben adoptar protocolos de seguridad adecuados según su contexto específico, nivel de riesgo y su capacidad operativa. Tecnologías como blockchain pueden ser útiles para garantizar trazabilidad y resistencia frente a ataques, pero se requiere avanzar en soluciones más accesibles y menos costosas para su adopción generalizada.

Entre las recomendaciones clave que surgen de este estudio, se destacan:

- Diseñar protocolos de seguridad ligeros pero robustos, adaptables a entornos distribuidos y orquestados.
- Validar empíricamente los protocolos en plataformas reales como Kubernetes.
- Mejorar la integración nativa de herramientas de monitoreo y control dentro del ecosistema Kubernetes.
- Desarrollar estándares para la evaluación comparativa de técnicas criptográficas bajo métricas comunes de rendimiento, consumo de recursos y resistencia a ataques.
- Fomentar el uso combinado de tecnologías como mecanismos complementarios y no excluyentes.

En conclusión, la seguridad en cloud computing continúa representando un desafío que exige un enfoque dinámico. La constante evolución de amenazas e innovación tecnológica requiere la adopción de soluciones contextualmente adecuadas. En este contexto, la adopción de protocolos robustos y adaptativos es clave para mitigar los riesgos y fortalecer la protección de los datos en la nube.

Referencias

[1] A. Patel, N. Shah, D. Ramoliya and A. Nayak, "A detailed review of Cloud Security: Issues, Threats & Attacks," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, India, pp. 758-764, 2020, doi: 10.1109/ICECA49313.2020.9297572.

[2] Sinchana, M.K., Savithramma, R.M, " Survey on Cloud Computing Security" Innovations in Computer Science and Engineering. Lecture Notes in Networks and Systems, Springer, Singapore, vol 103, pp 1-6, https://doi.org/10.1007/978-981-15-2043-3_1

[3] R. Kumar and M. P. S. Bhatia, "A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability," 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON), Greater Noida, India, pp. 334-337, 2020, doi: 10.1109/GUCON48875.2020.9231255.

[4] P. R. Tomás Gabriel, "Seguridad Informática en la Adopción de Cloud Computing en la Industria Alimentaria", Rev. Boaciencia. Negocios Tecnol., vol. 1, n.º 2, p. 93, 2021.

[5] A. M. Torres González, "Análisis de los componentes de seguridad informática en la implementación de cloud computing en pequeñas y medianas empresas colombianas", Monografía, UNIVIERSIDAD. NACIONAL ABIERTA Y A DISTANCIA - UNAD ESCUELA DE CIENCIAS BÁSICAS, TECNOLGÍA E INGENIERÍA., Bogotá, 2020.

[6] J. Liu, Q. Zhong, R. Sun, X. Du and M. Guizani, "A Secure and Efficient Medical Data Sharing Protocol for Cloud-Assisted WBAN" in 2019 IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 2019, pp. 1-6, doi: 10.1109/GLOBECOM38437.2019.9014307.

[7] P. Zhang, H. Chi, J. Wang, and Y. Shang, "Data security protocol with blind factor in cloud environment" in Information, vol. 12, no. 9, art. no. 340, 2021, doi: 10.3390/info12090340.

[8] V. Kumar, M. S. Mahmoud, A. Alkhayyat, J. Srinivas, M. Ahmad, and A. Kumari, "RAPCHI: Robust authentication protocol for IoMT-based cloud-healthcare infrastructure" in The Journal of Supercomputing, vol. 78, no. 14, pp. 16167–16196, 2022, doi: 10.1007/s11227-022-04513-4.

[9] S. N. Prasad and C. Rekha, "Blockchain-based IAS protocol to enhance security and privacy in cloud computing," in Measurement: Sensors, vol. 28, art. no. 100813, 2023, doi: 10.1016/j.measen.2023.100813.

[10] B. D. Deebak and F. Al-Turjman, "Smart mutual authentication protocol for cloud-based medical healthcare systems using internet of medical things," in IEEE Journal on Selected Areas in Communications, vol. 39, no. 2, pp. 346–360, 2021, doi: 10.1109/jsac.2020.3020599.

[11] O. Ruan, X. Huang and H. Mao, "An efficient private set intersection protocol for the cloud computing environments," in 2020 IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2020, doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00053.

[12] S. Farahmandian and D. B. Hoang, "A policy-based interaction protocol between software defined security controller and virtual security functions," in 2020 4th Cyber Security in Networking Conference (CSNet), 2020,doi: 10.1109/CSNet50428.2020.9265460.

[13] A. Delham Algarni, F. Algarni, S. Ullah Jan and N. Innab, "LSP–eHS: A lightweight and secure protocol for e-healthcare system," IEEE Access: Practical Innovations, Open Solutions, vol. 12, pp. 156849–156866, 2024, doi: 10.1109/access.2024.3477922.

[14] S. S. Manivannan, P. Shashidhar, C. Vanmathi and P. M. D. R. Vincent, "Multi authority privacy preserving protocol in cloud computing authentication using grouping algorithm and EDAC-MAC" in 2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT), 2019 doi: 10.1109/ICICICT46008.2019.8993380.

[15] S. Itoo, A. A. Khan, V. Kumar, A. Alkhayyat, M. Ahmad and J. Srinivas, "CKMIB: Construction of key agreement protocol for cloud medical infrastructure using blockchain" IEEE Access: Practical Innovations, Open Solutions, vol. 10, pp. 67787–67801, 2022, doi: 10.1109/access.2022.3185016.

[16] S. Han, K. Han and S. Zhang, "A data sharing protocol to minimize security and privacy risks of cloud storage in big data era" in IEEE Access: Practical Innovations, Open Solutions, vol. 7, pp. 60290–60298, 2019, doi: 10.1109/access.2019.2914862.

[17] J. Liang, Z. Qin, J. Ni, X. Lin and X. Shen, "Efficient and Privacy-Preserving Outsourced SVM Classification in Public Cloud," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), Shanghai, China, 2019, pp. 1-6, doi: 10.1109/ICC.2019.8761610.

[18] H. Wang, D. He and J. Han, "VOD-ADAC: Anonymous distributed fine-grained access control protocol with verifiable outsourced decryption in public cloud" in IEEE Transactions on Services Computing, vol. 13, no. 3, pp. 572–583, 2020, doi: 10.1109/tsc.2017.2687459.

[19] R. Stoyanov, A. Reber, D. Ueno, M. Clapiński, A. Vagin and R. Bruno, "Towards efficient end-to-end encryption for container checkpointing systems." in Proceedings of the 15th ACM SIGOPS Asia-Pacific Workshop on Systems, pp. 60–66. 2024. DOI: 10.1145/3678015.3680477.

[20] M. Femminella, M. Palmucci, G. Reali, and M. Rengo, "Attribute-based management of secure Kubernetes cloud bursting." un IEEE Open Journal of the Communications Society, vol. 5, pp. 1276–1298, 2024, doi: 10.1109/ojcoms.2024.3367461.

[21] M. V. Le, S. Ahmed, D, Williams and H. Jamjoom, "Securing container-based clouds with syscall-aware scheduling." in Proceedings of the ACM Asia Conference on Computer and Communications Security, pp. 812–826. 2023 . DOI: 10.1145/3579856.3582835.

[22] A. Sadiq, H. J. Syed, A. A. Ansari, A. O. Ibrahim, M. Alohaly and M. Elsadig, "Detection of Denial of service attack in cloud based Kubernetes using eBPF." in Applied Sciences (Basel, Switzerland), 13(8), p 4700. 2023. DOI: 10.3390/app13084700.

[23] N. Pecka, L. Ben Othmane and A. Valani, "Privilege escalation attack scenarios on the DevOps pipeline within a Kubernetes environment." in Proceedings of the International Conference on Software and System Processes and International Conference on Global Software Engineering, pp 45–49.2022 .DOI: 10.1145/3529320.3529325.

[24] J. Mahboob, and J. Coffman, "A Kubernetes CI/CD pipeline with asylo as a trusted execution environment abstraction framework." in 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC). 2021. DOI: 10.1109/CCWC51732.2021.9376148.

[25] H. Lim, Y. Kim and K. Sun, "Service management in virtual machine and container mixed environment using service mesh." in 2021 International Conference on Information Networking (ICOIN). 2021. DOI: 10.1109/ICOIN50884.2021.9333888.

[26] S. Shringarputale, P. McDaniel, K. Butler and T. La Porta, "Co-residency Attacks on Containers are Real." in Proceedings of the 2020 ACM SIGSAC Conference on Cloud Computing Security Workshop. 2020. DOI: 10.1145/3411495.3421357.

[27] D. Bringhenti, G, Marchetto, R. Sisto, F. Valenza and J. Yusupov, "Introducing programmability and automation in the synthesis of virtual firewall rules." in 2020 6th IEEE Conference on Network Softwarization (NetSoft), 2020, DOI: 10.1109/NetSoft48620.2020.9165434.

[28] A. F. Baarzi, G. Kesidis, D. Fleck and A. Stavrou, "Microservices made attack-resilient using unsupervised service fissioning." Proceedings of the 13th European Workshop on Systems Security, 2020, DOI: 10.1145/3380786.3391395.

[29] A. Borisova, V. Shvetcova, and O. Borisenko, "Adaptation of the TOSCA standard model for the Kubernetes container environment," in 2020 Ivannikov Memorial Workshop (IVMEM), 2020. DOI: 10.1109/IVMEM51402.2020.00008.

[30] T. Heo, J. H. An, and Y. Kim, "Design and implementation of migration manager between cloud edge platforms," in Proceedings of the International Conference on Research in Adaptive and Convergent Systems, 2020. DOI: 10.1145/3400286.3418279.

[31] D. Y. Yuan, and T. Wildish, "Bioinformatics application with Kubeflow for batch processing in clouds," in Lecture Notes in Computer Science, Springer International Publishing, 2020, pp. 355–367. DOI: 10.1007/978-3-030-59851-8_24.

[32] A. Brito, C. Fetzer, S. Köpsell, P. Pietzuch, M. Pasin, P. Felber, K. Fonseca, M. Rosa, L. Gomes Jr, R. Riella, C. Prado, L. F. Rust, D. E. Lucani, M. Sipos, L. Nagy and M. Fehér, "Secure end-to-end processing of smart metering data," in Journal of Cloud Computing: Advances, Systems and Applications, vol. 8, no. 1, 2019. DOI: 10.1186/s13677-019-0141-z.

[33] N. Surantha and F. Ivan, "Secure Kubernetes networking design based on zero trust model: A case study of financial service enterprise in Indonesia," in Innovative Mobile and Internet Services in Ubiquitous Computing, Springer International Publishing, pp. 348–361. 2020. DOI: 10.1007/978-3-030-22263-5_34.

[34] G. P. Fernandez and A. Brito, "Secure container orchestration in the cloud: Policies and implementation," in Proceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 1635–1642. 2019. DOI: 10.1145/3297280.3297296.

[35] B. Thurgood and R. G. Lennon, "Cloud computing with Kubernetes cluster elastic scaling," in Proceedings of the 3rd International

Conference on Future Networks and Distributed Systems, pp. 1–6. 2019. DOI: 10.1145/3341325.3341995.

[36] C. W. Tien, T. Y. Huang, C. W. Tien, T. C. Huang and S. Y. Kuo, "KubAnomaly: Anomaly detection for the Docker orchestration platform with neural network approaches," in Engineering Reports: Open Access, vol. 1, no. 5, 2019. DOI: 10.1002/eng2.12080.

[37] H. Hamzeh, S. Meacham and K. Khan, "A new approach to calculate resource limits with fairness in Kubernetes," in 2019 First International Conference on Digital Data Processing (DDP), 2019. Doi: 10.1145/3366615.3368356

[38] S. Suneja, A. Kanso and C. Isci, "Can container fusion be securely achieved?" in Proceedings of the 5th International Workshop on Container Technologies and Container Clouds, 2019, doi: 10.1145/3366615.3368356.

[39] B. Chun, J. Ha, S. Oh, H. Cho and M. Jeong, "Kubernetes Enhancement for 5G NFV Infrastructure" in 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, doi: 10.1109/ICTC46691.2019.8939817.

[40] A. Yeboah-Ofori, A. Jafar, T. Abisogun, I. Hilton, W. Oseni and A. Musa, "Data security and governance in multi-cloud computing environment" in 2024 11th International Conference on Future Internet of Things and Cloud (FiCloud),pp. 215–222, 2024. doi: 10.1109/FiCloud62933.2024.00040.

[41] D. Soldani, P. Nahi, H. Bour, S. Jafarizadeh, M. F. Soliman, L. Di Giovanna, F. Monaco, G. Ognibene and F. Risso, "EBPF: A new approach to cloud-native observability, networking and security for current (5G) and future mobile networks (6G and beyond) " in IEEE Access: Practical Innovations, Open Solutions, vol. 11, pp. 57174–57202, 2023, doi: 10.1109/access.2023.3281480.

[42] A. Blaise and F. Rebecchi, "Stay at the Helm: secure Kubernetes deployments via graph generation and attack reconstruction," un 2022 IEEE 15th International Conference on Cloud Computing (CLOUD), 2022, doi: 10.1109/CLOUD55607.2022.00022.

[43] G. Budigiri, C. Baumann, J. T. Muhlberg, E. Truyen and W. Joosen, "Network policies in Kubernetes: Performance evaluation and security analysis," un 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), 2021, doi: 10.1109/EuCNC/6GSummit51104.2021.9482526.

[44] M. Ul Haque, M. M. Kholoosi and M. A. Babar, "KGSecConfig: A knowledge graph based approach for secured container orchestrator configuration," in 2022 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER), 2022, doi: 10.1109/SANER53432.2022.00057.

[45] S. Lee and J. Nam, "Kunerva: Automated network policy discovery framework for containers" in IEEE Access: Practical Innovations, Open Solutions, vol. 11, pp. 95616–95631, 2023, doi: 10.1109/ACCESS.2023.3310281..

[46] J. M. Parra-Ullauri, L. F. Gonzalez, A. Bravalheri, R. Hussain, X. Vasilakos, I. Vidal, F. Valera, R. Nejabati, and D. Simeonidou, "Privacy preservation in Kubernetes-based federated learning: A networking approach," in IEEE INFOCOM 2023 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), pp. 1–7, 2023, doi: 10.1109/INFOCOMWKSHPS57453.2023.10225925.

[47] F. Hussain, W. Li, B. Noye, S. Sharieh and A. Ferworn, "Intelligent Service Mesh Framework for API Security and Management," in 2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2019, doi: 10.1109/IEMCON.2019.8936216.

[48] J. Santos, E. Truyen, C. Baumann, F. De Turck, G. Budigiri and W. Joosen, "Towards intent-based scheduling for performance and security in edge-to-cloud networks," in 2024 27th Conference on Innovation in Clouds, Internet and Networks (ICIN), pp. 222–227, 2024, doi: 10.1109/ICIN60470.2024.10494432.

[49] R. R. Karn, P. Kudva, H. Huang, S. Suneja and I. M. Elfadel, "Cryptomining detection in container clouds using system calls and explainable machine learning," in IEEE Transactions on Parallel and Distributed Systems: A Publication of the IEEE Computer Society, vol. 32, no. 3, pp. 674–691, 2021, doi: 10.1109/tpds.2020.3029088.

MASKAY 16(1), May 2026
ISSN 1390-6712

Recibido (Received): 2025/04/29
Aceptado (Accepted): 2025/07/28

Comparison of interior propagation models of the Wi-Fi network at the 5785 MHz band through RSSI measurements

Comparación de modelos de propagación interior de la red Wi-Fi en la banda de 5785 MHz mediante medidas RSSI

Dayana Pilco, María Díaz

***Abstract*—This study presents a comparative analysis of the Cost231-Multi-Wall Model, the Motley-Keenan Model, the Modified Free Space Model, and the Log-Normal Shadowing Path Loss Model, applied to a 5G Wi-Fi network in an indoor analysis. The research seeks to recommend the most appropriate small-scale propagation model based on empirical measurements of signal strength. Initially, the router is located within the analysis area. Then, a detailed sketch is made in SketchUp, locating 133 points around the primary router, covering the entire indoor area of the analysis, ensuring an accurate assessment of the cellular network coverage. Subsequently, with the data collected over three campaigns, propagation losses were calculated to determine the theoretical power of each model and compare the measured power values with the theoretical power values to obtain a specific model. The four propagation models analyzed in the evaluator are based on data obtained in the range [-20 to-91] dBm. It was concluded that the Keenan-Motley propagation model offered a better fit to the measurements, presenting a value of 12.59 dB. In contrast, the Cost 231 model showed a value of 17.18 dB, the Modified Free Space model showed a value of 26.47 dB, and the Log-Normal Shadowing Path Loss model showed a value of 27.57 dB, indicating a greater discrepancy concerning the measured data. This model demonstrated greater accuracy in predicting the reception power compared to the other analysis models, adapting better to the specific characteristics of the environment. These results highlight the importance of strategically locating the router; therefore, it is recommended to locate it in a central location.**

***Index Terms*—Propagation Models, indoor 5G Wi-Fi, signal strength measurement, model comparison, router placement.**

***Resumen*—Este estudio presenta un análisis comparativo del Modelo Cost231-Multi-Wall, el Modelo Motley-Keenan, el Modelo de Espacio Libre Modificado y el Modelo de Pérdida de Trayectoria por Sombreado Log-Normal, aplicado a una red Wi-Fi 5G en un análisis en interiores. La investigación busca recomendar el modelo de propagación a pequeña escala más apropiado con base en mediciones empíricas de la intensidad de la señal. Inicialmente, el enrutador se ubica dentro del área de análisis. Luego, se crea un boceto detallado en SketchUp, ubicando 133 puntos alrededor del enrutador principal, cubriendo toda el área interior del análisis, lo que garantiza una evaluación precisa de la cobertura de la red celular. Posteriormente, con los datos recopilados durante tres campañas, se calcularon las pérdidas de propagación para determinar la potencia teórica de cada modelo y comparar los valores de potencia medidos con los valores de potencia teóricos para obtener un modelo específico. Los cuatro modelos de propagación analizados en el evaluador se basan en datos obtenidos en el rango de [-20 a -91] dBm. Se concluyó que el modelo de propagación Keenan-Motley ofreció un mejor ajuste a las mediciones, presentando un valor de 12,59 dB. En contraste, el modelo Cost 231 mostró un valor de 17,18 dB, el modelo de Espacio Libre Modificado mostró un valor de 26,47 dB y el modelo Log-Normal Shadowing Path Loss mostró un valor de 27,57 dB, lo que indica una mayor discrepancia con respecto a los datos medidos. Este modelo demostró mayor precisión en la predicción de la potencia de recepción en comparación con los otros modelos de análisis, adaptándose mejor a las características específicas del entorno. Estos resultados resaltan la importancia de ubicar estratégicamente el enrutador; por lo tanto, se recomienda ubicarlo en una ubicación central.**

***Palabras Claves*—Modelos de propagación, Wi-Fi 5G en interiores, medición de la intensidad de la señal, comparación de modelos, ubicación del enrutador.**

I. Introduction

The technological advances experienced daily have radically changed people's lives, especially in the field of mobile telecommunications [1]. These advances are reflected in the study of interference, particularly when implementing new network infrastructures. For the analysis of signal power in different environments (urban, suburban, rural, and indoor), the use of propagation models is crucial; these adopt the laws of physics, where they determine how radio waves are dispersed, refracted, and reflected [2].

Wi-Fi networks, which operate on the 2.4 GHz and 5 GHz frequencies, also play a fundamental role in everyday connectivity. The 2.4 GHz network, although more susceptible to interference due to device congestion on this frequency, offers greater range, making it ideal for covering vast areas. However, its performance is often compromised by the presence of other electronic devices, such as microwaves or

Dayana Pilco and María Díaz are with the Carrera en Telecomunicaciones, Escuela Politécnica del Chimborazo, (e-mail: {dayana.pilco, mariac.diaz}@espoch.edu.ec).

DOI: 10.24133/maskay.v16i1.4152

cordless phones, using the same band. On the other hand, the 5 GHz network provides faster connection speeds due to fewer devices on this frequency. Although its range is shorter compared to 2.4 GHz, the 5 GHz network is better suited for environments with high bandwidth demands, such as streaming high-definition video or online gaming [3].

Small-scale propagation models in mobile telephony are designed to study the variation in the received power of an emitted signal. The Motley-Keenan model analyzes signal loss by considering several factors, such as the distance between the transmitter and receiver and physical obstacles (walls, floors, doors, or ceilings). This model is beneficial because it allows the loss estimate to be customized for each specific environment, using empirical values for each type of obstacle, making it ideal for designing Wi-Fi, Bluetooth, or indoor communication systems [4]. The Cost 231 model is an extension of the Okumura Hata model, which was initially designed for urban environments but is also often used indoors. This model considers path loss as a function of frequency, distance, and certain correction factors, including the type of environment (such as office buildings or factories) [5].

A comparative analysis of the two models shows that the Motley-Keenan model is specifically designed for indoor environments because it offers a better representation of the actual attenuation within specific locations, especially in locations with multiple subdivisions. Therefore, this paper presents a comparative analysis of the propagation models to select the most appropriate model that achieves good quality of service while ensuring efficient connectivity in a variety of contexts, facilitating the development of emerging technologies such as the Internet of Things (IoT) deployed in 4G and 5G networks [6].

II. Indoor Propagation Models

A. Keenan-Motley

The modified-free-space model analyzes the distances between the building walls and the penetration losses of the walls. The model, according to Motley and Keenan, computes the path loss based on the direct ray between transmitter and receiver. In contrast to the modified free space model, this model considers the exact locations of the walls, floors, and ceilings. Additional factors for absorption of the direct ray path by walls are considered [7], [8].

Designed exclusively for propagation in indoor environments, this empirical model considers both free space loss and the additional loss that occurs when the direct signal between the transmitter and receiver passes through different walls and floors. [9] Its application requires a large volume of data, and the signal attenuation is determined through:

$$L(dB) = L_0 + 10\log(d) + \sum_{i=1}^{N_f} L_{f,i} + \sum_{j=1}^{N_w} L_{w,j} \qquad (1)$$

where L_0 is the propagation losses at one (1) meter from the transmitting antenna, in dB, $L_{f,i}$ is the propagation losses of the signal through floors, in dB, $N_{f,I}$ is the number of floors with the same characteristics, $L_{w,j}$ is the propagation losses of the signal through walls, in dB, $N_{w,j}$ is the number of walls with the same characteristics, i is the number of types of floors crossed by the signal, and j is the number of types of walls crossed by the signal.

As shown in Fig. 1, the parameter kw describes the number of walls intersected by the direct path between transmitter and receiver. A uniform transmission (penetration) loss L_w for all walls is used for the computation; that is, the material properties of the individual walls are not considered. This uniform transmission loss can be specified by using the Settings button [10].

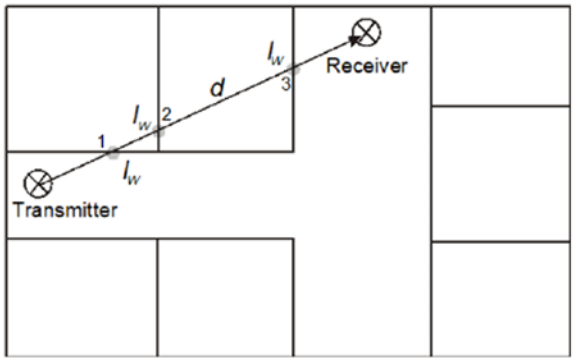


Fig. 1. Principle of the Motley-Keenan model.

The Keenan-Motley model is used to analyze signal loss, considering factors such as distance and physical obstacles. Total attenuation is calculated by adding the free-space loss and the additional losses caused by walls and floors. The equation used is:

$$L(dB) = 37 + 20\log(d) + N_f \cdot L_f + \sum_{j=1}^{N_w} L_{w,j} \qquad (2)$$

where L is the total loss of signal in decibels (dB), d is the distance between the transmitter and the receiver, N_f is the number of floors crossed by the signal, L_f is the propagation losses through floors, in dB, L_{w1} are the losses in lightweight walls such as wood or doors, and L_{w2} are the losses in thick walls such as brick or concrete

In Table I, the typical values of the mentioned losses are shown:

TABLE I
LOSS FACTORS ACCORDING TO WALL TYPE

Type of loss	Attenuation range (dB)
L_f	13-27
L_{w1}	2-4
L_{w2}	8-12

B. Cost 231-multi-wall

The COST 231 Multi-wall (MWM) model, an extension of the COST 231 Keenan and Motley propagation model, introduces a linear loss component that is proportional to the number of walls traversed by the signal. In addition, it includes a more complex term related to the number of floors

crossed. This additional term takes into account that signal loss increases at a slower rate after the first floor traversed, reflecting a decrease in incremental attenuation as the signal traverses more floors [9], [14].

Overall, the total attenuation in the COST 231 Multi-wall model is calculated by adding the free space loss, the loss due to the number of walls, and the loss due to the number of floors. [15] This approach allows for a more accurate representation of signal propagation in complex indoor environments, where multiple obstacles can significantly impact signal quality. According to Saunders (2007), this model is beneficial for designing and optimizing wireless networks in buildings, providing an effective tool to predict coverage and improve network planning [16], [17].

$$L(dB) = L_0 + 10\gamma \log(d) + L_f N_f^{\left(\frac{L_f - 2}{L_f + 1} \cdot b\right)} + \sum_{j=1}^{J} N_{w,j} L_{w,j} \quad (3)$$

where γ is the path loss exponent and *b* is an attenuation factor associated with the floors that the signal must pass through.

In any case, the propagation model in free space is represented by the previous equation.

$$L_{el}(dB) = 92.44 + 20\log f + 20\log d \quad (4)$$

where *f* is the operating frequency in GHz.

This model accounts for losses due to walls and floors, as shown in Tables II and III. Therefore, the following parameters are used for each scenario:

TABLE II
MATERIAL LOSSES FOR THE COST 231-MULTI-WALL MODEL

Description	Material	Factor (dB)
L_f	Floors (typical structure) Tiles or concrete covering, thickness ¡ 30 cm	18.3
L_{wi}	Thin internal walls, Plaster or wall with openings (windows and/or doors), width ¡ 10 cm	3.4
L_{wi}	Thick internal walls, Concrete or Brick width ¿ 10 cm	6.9

TABLE III
MATERIAL LOSSES FOR THE COST 231-MULTI-WALL MODEL

Wall material	Thickness (cm)	Attenuation (dB)
Wood	0.4	Lw11=0.9
Plasterboard	13.5	Lw21=3.0
Glass	1.5	Lw41=2.5
Double-glazed window (12 mm air gap)	2.0	Lw51=12
Reinforced concrete block	30.2	Lw61 = 10

III. METHODOLOGY

To better understand the focus of this research, Fig. 2 presents a representative diagram of the router's (Access Point) location and how the signal propagates in different directions within an indoor environment. In this specific case, the analysis was carried out inside a home, where it was identified that the signal must cross various physical obstacles such as walls, windows, desks, floors, and ceilings, among others. These conditions directly influence the quality and range of the wireless signal. For this reason, it is essential to correctly locate the access point to ensure better signal diffusion between the transmitter (the Access Point itself) and the receiver, which in this context corresponds to the end user, who accesses the service through a technological device with an Internet connection.

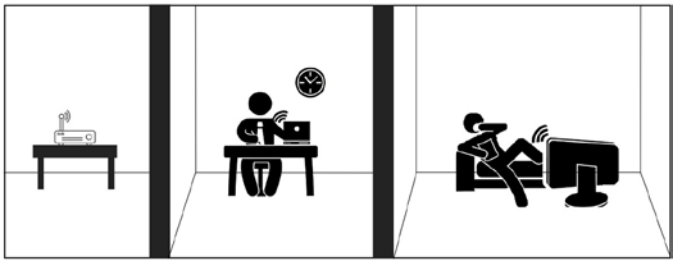


Fig. 2. Diagram of an access point transmission in a house.

For indoor propagation measurements, a Huawei EchoLife HS8546V5 Gigabit smart home solution intelligent gateway device, shown in Fig. 3, was used. It offers a POTS voice interface, 4 GE/FE adaptive Ethernet ports, and dual-band WiFi (2.4 GHz and 5 GHz). It offers application flexibility, plug-and-play support, remote diagnosis, green power saving, and other functions [18].

Fig. 3. Router Huawei EchoLife HS8546V5.

The HS8546V5 features a transmission power of up to 20 dBm for 802.11n WLAN networks in the 2.4 GHz band, and up to 26 dBm for 802.11ac networks in the 5 GHz band. It operates over a GPON interface and features compact dimensions of 173 mm long, 120 mm wide, and 30 mm high. It is equipped with two fixed external antennas, each with a 5 dBi gain, enabling more exhaustive and optimized signal coverage. These specifications make it an ideal device for efficient data transmission and reliable coverage, especially in indoor environments during measurement processes [19].

Measurements were taken in the city of Riobamba, Ecuador, at an altitude of 2,754 meters above sea level, with an average temperature of approximately 13°C. The house is a single-story country house, spanning approximately 150 square meters. The walls are made of kiln-fired clay brick, rectangular with dimensions of 24 cm long, 12 cm wide, and 7 cm high. Inside, each wall is plastered (a thin layer of mortar

to smooth, protect, and prepare the surface for the final finish), plastered, and painted with water-based paint. Outside, the exposed brick finish is preserved. The roof is composed of fiber cement sheets with additives, silica, and cellulose fiber, supported by a metal frame. Beneath this is a “ceiling” structure, which acts as a false ceiling to conceal the roof structure.

A network of measuring points was established within the home, with a total of 133 points distributed as follows: 25 points in the main room (Room II), where the access point is located; 15 points in Room I; 29 points in Room III; 38 points in the kitchen (including the kitchen itself); 6 points in the bathroom; 12 points in the hallway; and 10 points in the basement. These measuring points were distributed proportionally to each square meter of the different interior spaces of the home, and a 1.25 m over the floor, as shown in Fig. 4.

To capture the signal data, the ”WIFI Heatmap” application was used, which allowed analyzing the bandwidth provided by the WiFi network, as detailed in Fig. 5. In addition, the SketchUp and Epic Games Launcher tools were used in Unreal Engine, specifically in version 3.5.2, to create both the 2D and 3D scenery and model the environment in detail.

The 5 GHz network, being less congested, experiences less interference, resulting in a faster connection. Additionally, it offers a greater number of available channels, providing additional space for device distribution in Fig. 6. Due to these advantages, it was decided to use the 5 GHz network for the measurements, thus ensuring greater quality and precision in the data obtained.

Several parameters are needed to calculate the propagation losses for each model. To determine the receiving power, it is necessary to implement equation (5), where P_r is the receiving power, P_t is the transmitting power, G_t is the gain of the transmitting antenna, G_r is the gain of the antenna of the mobile system, which is usually 1.5 dB, and L are the losses obtained according to each model.

Fig. 4. WiFi network measurement points: implementation in SketchUp.

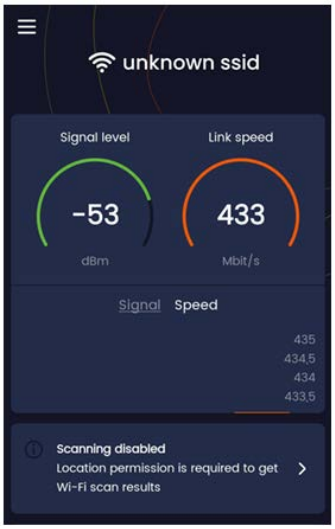


Fig. 5. Wifi Heatmap application to determine the bandwidth of the WiFi network.

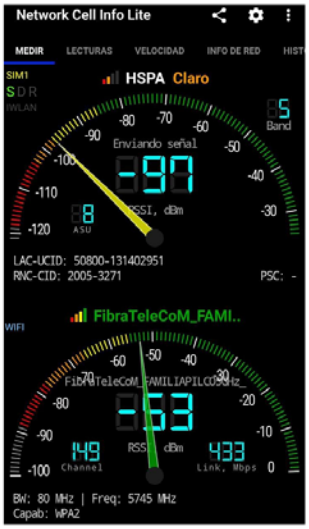


Fig. 6. Network Cell Info Lite application for operating band determination.

$$P_r = P_t + G_t + G_r - L \tag{5}$$

Fig. 7 presents the results of signal strength measurements carried out inside a house with brick walls and tile floors, with the router located on the second floor. Measurements show a progressive decrease in received signal power as the distance from the router increases. This attenuation can be attributed to several factors, such as signal reflection from tile flooring, diffraction caused by obstacles such as furniture and walls, and inherent free space losses. These variations highlight the complexity of signal propagation in a home environment and the importance of strategic router placement to maximize coverage.

Furthermore, the structure of the building, especially the thickness of the brick walls, plays a crucial role in signal degradation. RF signals are significantly attenuated when passing through dense materials, which explains notable decreases in signal strength in different rooms and floors. These results underscore the need for careful planning of access point placement and network configuration to ensure

optimal wireless connectivity in complex home environments.

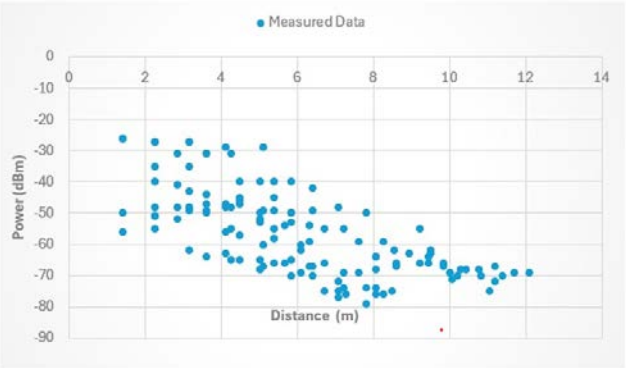


Fig. 7. Measured power.

A. *Transmission Power Analysis*

Calculating the actual transmit power of the Huawei HS8546V5 access point is crucial, as it may differ from the power specified in the device's data sheet. In practice, the adequate power tends to decrease when multiple users are connected at the same time. This occurs because the router must distribute its capacity among all connected devices, which can reduce the transmission power available for each one. Therefore, estimating the real power allows a better understanding of the router's performance in real conditions and facilitates network optimization to ensure more efficient and balanced connectivity for all users.

The following equation is used to calculate the actual adequate isotropic radiated power (EIRP) emitted by the router. The EIRP considers not only the transmit power of the router, but also the gain of the antennas and the losses in the cables and connectors. This calculation is essential to understand the actual range and coverage of the router, allowing more precise network planning and the implementation of measures to improve signal quality in different areas of the home environment.

$$\begin{aligned} EIRP &= P_r - G_r + L_{bf} \\ EIRP &= -24 - 1.5 + 52.44 \\ EIRP &= 26.94 \end{aligned} \tag{6}$$

The received power measured directly at 2 meters from the access point was -29 dBm, as shown in Fig. 8. This measurement resulted in an adequate isotropic radiated power (EIRP) of 26.94 dBm. The measurement was performed in an anechoic chamber, ensuring a controlled environment free from external interference. The obtained value of 26.94 dBm is consistent with the value specified in the access point's data sheet, which indicates an EIRP of 26 dBm.

Fig. 8. Power measured at 2 meters from the router.

IV. Results

This section compares the propagation losses obtained using different applied models, allowing their accuracy and applicability to be evaluated in real conditions. Cost231Multi-Wall, the Motley-Keenan, Modified Free Space, and LogNormal Shadowing Path Loss, taking into account factors such as diffraction and reflection from obstacles. Comparing these models with real measurements is essential to optimizing the design and planning of communication networks, as well as to determining the optimal placement of routers. This ensures greater efficiency and adequate coverage in various environments.

A. *Keenan-Motley model*

Theoretical data for the Motley-Keenan model were calculated using (2) as it is more appropriate for the measurement environment. This is because not all the data necessary to apply the general equation of the Motley-Keenan model was available. Table IV presents the parameters used in this model, based on the information provided in Table II.

TABLE IV
MOTLEY-KEEMAN PARAMETERS

L_f	14
L_{w1}	3
L_{w2}	9

Fig. 9 shows the measured data points (blue dots) and the theoretical predictions of the Keenan-Motley model (green dots). It is noted that there is a concentration of blue dots near the model's prediction curve, suggesting a good approximation. The Keenan-Motley model had an error of 12.59 dB, indicating that it best fits the measurements taken in the brickwalled house. This figure demonstrates the model's accuracy in estimating receiving power in an indoor environment with multiple obstacles and subdivisions.

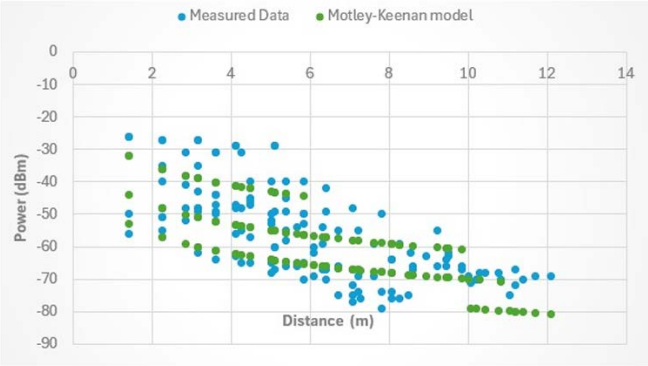


Fig. 9. Keenan-Motley model.

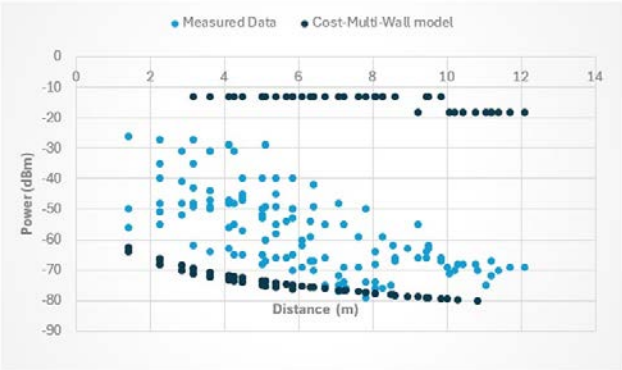


Fig. 11. Cost 231-Multi-Wall model.

B. *Log-Normal Shadowing Path Loss model*

In Fig. 10, the measured data (light blue dots) are compared with the prediction curve of the Log-Normal Shadowing Path Loss model (red dots). It can be seen that most of the measured points do not align with the model curve. The high error value (27.57 dB) confirms that this model is not suitable for the measurement environment. It can be inferred that this model, although it incorporates a log-normal distribution term for fading, does not effectively capture the specific characteristics of the analyzed residential environment.

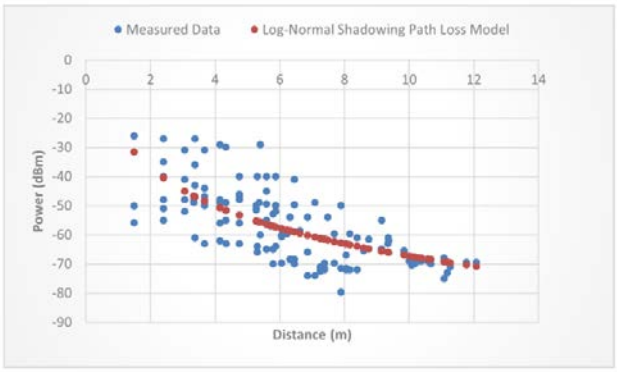


Fig. 10. Log-normal shadowing path loss model.

C. *Cost 231-Multi-Wall model*

Theoretical data for the Cost-Multi-Wall model were calculated using Equation 3. Data were taken from Tables II and III and adjusted according to the measurement environment and the number of walls or floors present in each scenario. Furthermore, the values of γ and b were set to 2 and 0.46, respectively.

Fig. 11 compares the measured data (light blue dots) with the prediction curve of the Cost 231-Multi-Wall model (blue dots). At first glance, it is noticeable that the measured and predicted points are clustered together, but in different locations on the graph. Although this model accounts for loss through walls and floors, its error of 17.18 dB is significantly higher than that of the Keenan-Motley model. The figure indicates that the model is not well-suited to this type of building, with brick walls and fiber cement roofs, which limits its ability to predict reception power in this particular scenario.

D. *Modified Free Space model*

The model uses parameters such as the horizontal distance between the transmitter and receiver. This distance is determined using the right triangle formula to calculate the hypotenuse, which represents the horizontal distance. The equations were applied because all the necessary data were available for the measurement environment. Since the measurements were taken in a home, a setting similar to an office building, parameters appropriate for that type of environment were used.

Finally, Figure 12 shows the measured data (light blue dots) and the predictions of the Modified Free Space model (purple dots). The prediction curve is considerably far from the measured points, suggesting that this model, by assuming ideal conditions with minimal obstructions, is not appropriate for an indoor environment with walls, furniture, and other barriers. The error of 26.47 dB confirms this, placing it as one of the least accurate models for this study.

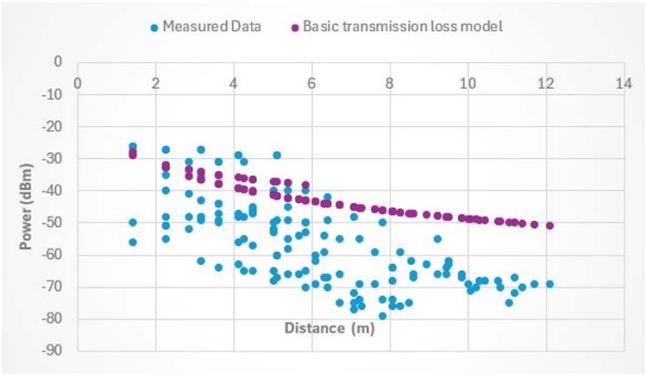


Fig. 12. Modified free-space model.

E. *Mean square error*

Table V presents the results of the mean square errors (MSE) obtained for different propagation models evaluated in the study environment. It is observed that the Keenan-Motley model presents the lowest root mean square error, indicating that it is the model that best fits the measured data, showing greater accuracy in estimating the reception power. This behavior suggests that, in the specific context of this study, the Keenan-Motley model is the most suitable for predicting signal distribution in indoor environments with multiple walls

and obstacles. In contrast, other models show higher MSE (mean square error), indicating lower accuracy in their predictions.

TABLE V
COMPARISON OF PROPAGATION MODELS IN THE EVALUATED ENVIRONMENT

Propagation model	MSE (dB^2)	RMSE (dB)
Motley-Keenan	158.56	12.59
Log-Normal Shadowing Path Loss	760.15	27.57
Cost-Multi-Wall	295.25	17.18
Modified Free Space	700.78	26.47

F. Mapping of Received Powers.

To evaluate the reception strength of a 5G Wi-Fi network, measurements were taken inside a home located in the rural area of Riobamba. One hundred thirty-three sampling points were recorded, spaced one square meter apart, providing a detailed view of the signal distribution within the property.

Initially, SketchUp was used to create 2D and 3D models of the study area, ensuring an accurate representation of the physical environment. The collected data was then integrated into Unreal Engine (version 3.5.2 by Epic Games), where the reception strength was modeled and visualized in a three-dimensional and dynamic manner, facilitating a more realistic and understandable analysis.

Fig. 13 shows the visualization generated in Unreal Engine, using a color palette ranging from green (good reception) to white and red (poor reception). This clear representation makes it easy to identify areas with good coverage, as well as those that might require adjustments to the router's location or network settings to improve performance.

Fig. 13. Mapping of Received Powers.

V. CONCLUSIONS

The received power measured directly at 2 meters from the access point in the anechoic chamber, with a value of -29 dBm, yielded an adequate isotropically radiated power (EIRP) of 26.94 dBm. This value matches the value provided in the access point's data sheet, which specifies an EIRP of 26 dBm, confirming that the access point operates according to the manufacturer's specifications and that the measurement in the anechoic chamber was accurate, as it was performed in an interference-free environment.

For the propagation analysis, two propagation models were applied to data obtained from a total of 133 measurement points distributed throughout key spaces in the home, including the kitchen, hallway, bedrooms, and basement, to assess coverage under various environmental conditions. The data obtained were compared with the results of the Keenan-Motley and Cost 231 propagation models. The Keenan-Motley model showed an error of only 12.59 dB, providing a better fit to the home environment. In contrast, the Cost 231 model had an error of 17.18 dB, the Log-Normal Shadowing Path Loss model had an error of 27.57 dB, and the Modified Free Space model had an error of 26.47 dB, indicating a greater discrepancy with current measurements. This model is less suitable for these types of environments, characterized by brick, plaster, and metal-framed fiber cement roofs. These structural characteristics affect signal propagation, making the Keenan-Motley model more appropriate for this type of building.

Using the measurement data, an electromagnetic map was generated that visualizes signal distribution in the evaluated environment. This mapping facilitates understanding how the signal propagates in different spaces, providing an educational tool to explain signal processing and power distribution based on the structural characteristics of the environment. Therefore, the mapping serves as a visual resource to practically illustrate how environmental variables affect electromagnetic coverage and propagation.

Beyond root mean square errors (RMSE), each model's implementation presents its limitations. The Keenan-Motley model, while the most accurate in this study, requires a significant amount of empirical data and a detailed description of obstacles for calibration. Its adaptability to different materials is high, as it allows for customized losses by wall and floor. On the other hand, the Cost 231-Multi-Wall model, although it also considers obstacles, proved less adaptable to the specific environment of this study, possibly due to the construction characteristics of the home.

The Log-Normal Shadowing Path Loss and Modified Free Space models are more straightforward to implement. Still, their accuracy decreases considerably in complex environments, limiting their usefulness for detailed indoor network planning.

As future work, we plan to implement machine learning and deep learning models to improve accuracy and adapt to more complex scenarios. Incorporating these techniques would allow for more robust analysis and more accurate results.

REFERENCES

[1] J. Pérez, "Impacto de las nuevas tecnologías móviles en la sociedad," Revista UNESUM Ciencias, vol. 7, no. 1, pp. 4560, 2025. [Online]. Available: https://revistas.unesum.edu.ec/index.php/unesumciencias/article/view/474/591

[2] Naciones Unidas, "Influencia de las tecnologías digitales," https://www.un.org/es/un75/impact-digital-technologies, 2020, accedido: 16 de abril de 2025.

[3] S. M. Cordero, "Análisis de la calidad de señal en una red wi-fi con la herramienta netstumbler," Umbral Científico, vol. 7, pp. 61–71, 2005. [Online]. Available: https://www.redalyc.org/pdf/304/30400708.pdf

[4] J. L. Camargo Olivares. (2009) Modelos de propagación en interiores. [Online]. Available: https://biblus.us.es/bibing/proyectos/abreproy/11761/fichero/Volumen2%252F11-Cap%C3%ADtulo6+-+Modelos+de+propagaci%C3%B3n+en+interiores.pdf

[5] Xirio Online, “COST 231,” 2025, accedido: 16 de abril de 2025. [Online]. Available: https://www.xirio-online.com/web/help/es/cost231.htm

[6] S. P. R. Torres, and A. J. G. Meza, “Fundamentos de las comunicaciones móviles,” Universidad Tecnológica de Bolívar, Cartagena, Colombia, 2008, disponible en: https://biblioteca.utb.edu.co/notas/tesis/0043125.pdf.

[7] S. Sadowski and P. Spachos, “RSSI-based indoor localization with the internet of things,” IEEE Access, vol. 6, pp. 30149–30161, 2018.

[8] A. M. Al-Samman, T. Abd. Rahman, T. Al-Hadhrami, A. Daho, M. N. Hindia, M. H. Azmi, K. Dimyati, and M. Alazab, “Comparative study of indoor propagation model below and above 6 GHz for 5 G wireless networks,” Electronics, vol. 8, no. 1, p. 44, 2019. [Online]. Available: https://doi.org/10.3390/electronics8010044

[9] C. Maldonado, N. Pérez García, J. Uzcátegui, and E. Malaver, “Nuevo modelo de propagación para redes wlan operando en 2.4 ghz, en ambientes interiores,” Télématique, vol. 9, pp. 1–22, 01 2010.

[10] O. A. Guzm´an Obreg´on, S. Fern´andez, Y. Arbella, and W. Calzadilla, “Indoor propagation models in mobile communications,” 11 2010.

[11] G. Keenan and F. Motley, “A new propagation model for urban environments,” IEEE Transactions on Communications, vol. 45, no. 3, pp. 201–213, 1997.

[12] G. Molina and J. Keenan, Propagation Models and Predictions for Wireless Communications, 1st ed. New York: Springer, 2000.

[13] I. Altair Engineering, Motley-Keenan Model (MK), 2022. [Online]. Available: https://2022.help.altair.com/2022.1/winprop/topics/winprop/user guide/propagation methods/propagation models indoor mk.htm

[14] E. C. in the Field of Scientific and T. R. (COST), “Urban transmission loss models for mobile radio in the 900 and 1800 MHz bands,” COST 231 Final Report, 1999, available online at the COST 231 project website.

[15] M. Hata, Empirical Formula for Propagation Loss in Land Mobile Radio Services. IEEE, 1980, vol. 29, no. 3.

[16] R. Ogilvie. (2024) Modelo cost. [Online]. Available: https://www.studocu.com/latam/document/universidad-tecnologica-de-panama/comunicaciones-i/modelo-cost/85013323

[17] E. C. in the Field of Scientific and T. R. (COST), Final Report of COST 231: Digital Mobile Communications. Brussels: COST, 1999.

[18] Huawei, “Echolife hg8546m5,” 2024, accessed: 2024-07-24. [Online]. Available: https://support.huawei.com/enterprise/es/spanish-documents/echolife-hg8546m5-pid-23033074

[19] Huawei Technologies Co., Ltd., “Huawei HS8546V5 Smart Gateway,” https://szfibersystem.com/producto/huawei-hs8456v5/, 2020, accedido: 22 de abril de 2025

MASKAY 16(1), May 2026
ISSN 1390-6712

Recibido (Received): 2025/04/24
Aceptado (Accepted): 2025/07/19

Diseño y simulación de antenas de microcinta, casi cuadrada, circularmente polarizada para microsatélites: Guía práctica para la simulación con el software HFSS™

Design and simulation of circularly polarized, quasi-square microstrip antennas for microsatellites: A practical guide to simulation with HFSS™ software

Clara S. Franco, Willian Fontella, Marco V.T. Heckler, Edson R. Schlosser, Marco Fernando Lara, Rubén D. León V, Hector Moya, José J. Freire, and Alexis F. Tinoco-S

***Abstract*—This paper presents a practical guide for the design of a Right-Hand Circular Polarization (RHCP) microstrip antenna using HFSS software. The design considers an antenna to acquire information transmitted by the Global Positioning System (GPS) in the L1 band. This signal is used by the Attitude Control Unit (ACU) to improve the positioning control of a microsatellite traveling in a Low Earth Orbit (LEO). Following the proposed procedure, values of an Axial Ratio (AR) of 1.22 dB, a directivity of 5.14 dB in the broadside direction, and an AR bandwidth of 15 MHz were obtained.**

***Index Terms*—Microsatellites, Microstrip antenna, Circular polarization antenna, Attitude determination, LEO satellites, Global Positioning System (GPS).**

***Resumen*—En este trabajo se presenta una guía práctica para el diseño de una antena de microcinta, circularmente polarizada a derecha (RHCP), usando el software HFSS. Este procedimiento se aplica al diseño de una antena para adquirir la información transmitida por el sistema de posicionamiento global (GPS), en la banda L1, que se utiliza en la unidad de control de actitud (ACU) para el mejoramiento del control de la actitud de un microsatélite viajando en una órbita baja (LEO). Valores para la razón axial (AR) de 1,22 dB, una directividad de 5,14 dB en la dirección Broadside, y un ancho de banda para la RA de 15 MHz fueron obtenidos siguiendo el procedimiento propuesto.**

C.S. Franco, W. Fontella, M.V.T. Hekler, and E.R.Schlosser are with "Laboratório de Electromagnetismo, Micro-ondas e Antenas - LEMA" laboratory at "Universidad Federal do Pampa - UNIPAMPA", Alegrete, RS-Brazil ({clarafranco.aluno, willianfontella.aluno, marcosheckler, edsonschlosser}@unipampa.edu.br).

F.Lara M. is with "Departamento de Electrónica, Telecomunicaciones y Redes de Información (DETRI)" at "Escuela Politécnica Nacional – EPN", Quito, Ecuador (marco.lara@epn.edu.ec).

R.D. León V. and H. Moya. are with Repairing Upgrading Global Radar Advanced – RUGRA, Quito, Ecuador (rleon@rugra-rdr.com)

J.J. Freire and A.F. Tinoco-S. are with Faculty of Engineering and Applied Sciences, Networking and Telecommunications Engineering, Universidad de Las Américas (UDLA), Quito 170503, Ecuador ({jose.freire, alexis.tinoco}@udla.edu.ec).

***Palabras Claves*—Microsatélites, Antena de microcinta, Antena circularmente polarizada, Determinación de la actitud, satélites LEO, Sistema de posicionamiento Global - GPS.**

I. Introducción

Iniciativas destinadas al progreso de la industria aeroespacial y por ende al desarrollo de todas las ramas de la Ingeniería han sido impulsadas en los últimos años por varios gobiernos y agencias internacionales. En la actualidad, proyectos multidisciplinares en el ámbito académico destinados al desarrollo de Nanosatélites, microsatélites o también conocidos como Satélites Universitarios son encontradas a nivel global [1]-[3]. Agencias como la Administración Nacional de Aeronáutica y el Espacio - NASA (National Aeronautics and Space Administration) a través de su iniciativa ELaNa (Educational Launch of Nanosatellites), la Agencia Espacial Brasilera - AEB (Agência Espacial Brasileira) a través de su programa de nanosatélites educacionales o la Agencia Espacial Europea – ESA (European Space Agency) con la ESA Academy y su programa "Fly Your Satellite" son ejemplos de estos programas [2].

De por sí, un microsatélite es un sistema complejo, que requiere la integración de varios subsistemas y de su correcta interoperabilidad [1], [4]. En este sentido, podemos decir que los principales subsistemas integrantes de un microsatélite, según el modelo estándar para microsatélite propuesta por el California Polytechnic State University (Cal Poly) y por el Stanford University's Space Systems Development Lab en 1999 [4], son: a) computadora de vuelo, b) unidad controladora de carga útil, c) sistema de energía eléctrica, d) subsistema de adquisición de actitud y control de trayectoria, e) unidad de comando / control y telemetría, por ejemplo [1], [3], [5]-[7].

Cada una de las unidades antes mencionadas cumple tareas especializadas para garantizar el correcto funcionamiento del

DOI: 10.24133/maskay.v16i1.4151

microsatélite. A saber, el control de la órbita del microsatélite es una tarea que se desarrolla en el subsistema de adquisición de actitud y control de trayectoria. Este subsistema depende, básicamente, del sensor de actitud de vuelo y de sus actuadores. Podemos mencionar que de los varios dispositivos comúnmente usados para orientar el viaje del microsatélite, los más usados son dos: el sensor detector de estrellas o un subsistema que usa las señales transmitidas por alguno de los sistemas de posicionamiento global (Global Navigation Satellite System - GNSS), entre los cuales el más popular es el GPS. En relación con los actuadores disponibles en la actualidad, los más usados son: microsistema de propulsión o magneto par (Magnetorquer) [1], [5]-[8].

Este artículo presenta el diseño y simulación de una antena de microcinta, casi cuadrada, circularmente polarizada para recepción de la señal de GPS en la banda L1 y se enfoca en una guía práctica para la simulación usando el software HFSS™ [9]. La antena diseñada será integrada al subsistema ACU. Para esta finalidad, la antena debe trabajar a la frecuencia de 1,575 GHz - banda L_1 de GPS, tener un ancho de banda de 15 MHz, una razón axial (RA) menor a 3 dB dentro de la banda de pasaje y debe presentar polarización circular a derecha (Right Hand Circularly Polarized – RHCP).

Para estimar la geometría inicial de la antena de microcinta circularmente polarizada, el modelo de la cavidad equivalente será usado. En la sección II se presenta, de forma resumida, el modelo de la cavidad equivalente, las condiciones que deben cumplir los modos TM_{01} y TM_{10} para generar la polarización circular y a partir de esta teoría se estima la geometría para la antena GPS. En la sección III se presenta una guía para la optimización de la geometría inicial, con auxilio del software HFSS, en términos de su diagrama de la función directividad ($D(\theta,\phi)$), la RA e impedancia de entrada del irradiador (Zin). En la sección IV se muestran la geometría final y los resultados optimizados de la razón axial (RA), los diagramas de $D(\theta,\phi)$ y Zin de la antena. Adicionalmente, se relacionan los temas que serán tratados en trabajos futuros. Finalmente, las conclusiones son presentadas en la sección V de este artículo.

II. Uso Del Modelo De La Cavidad Equivalente Para Diseñar La Geometría Inicial De La Antena

El objetivo de este trabajo es mostrar el diseño, simulación y optimización de una antena de microcinta, circularmente polarizada, que será integrada al sistema de adquisición y control de actitud de un microsatélite. El paso inicial es la selección del material (laminado de microondas) que será usado. De entre los posibles laminados de microondas se decidió usar el TMM10i de la empresa Roger [10]. Sus principales características son presentadas en la Tabla I.

La selección del tipo de material se debió, principalmente, a ser un material cerámico, presentar un elevado ε_r - que permite miniaturizar el irradiador, su baja tangente de perdida y porque el ε_r presenta una estabilidad de -43 ppm/oK entre -55ºC a 125ºC, que es el rango de temperatura requerida para el sector de aeroespacial.

Tabla I
Características eléctricas del laminado TMM10i [10]

	Constante dieléctrica ε_r	Tolerancia	Tangente de pérdida tgδ	Espesura *h* [mm]
TMM10i	9.80	± 0.245	0.0020	3.81

Definido el laminado de microondas, la etapa siguiente es definir las características básicas que son necesarias para que la antena de recepción capte la señal de GPS en la banda L1. Como ya fue mencionado, estas son: frecuencia de operación igual a 1,575 GHz, polarización RHCP a derecha, ancho de banda de 15 MHz y razón axial inferior a 3 dB en la banda de operación. Seguidamente, hay que definir el tipo de geometría que será usada para este irradiador. De todas las posibles geometrías disponibles en la literatura especializada [11] se usará la casi cuadrada con un único punto de alimentación en su esquina. La razón para la selección de este tipo de irradiador es por facilidad de construcción. La ilustración de la geometría y de sus parámetros de diseño se presenta en la Fig. 1.

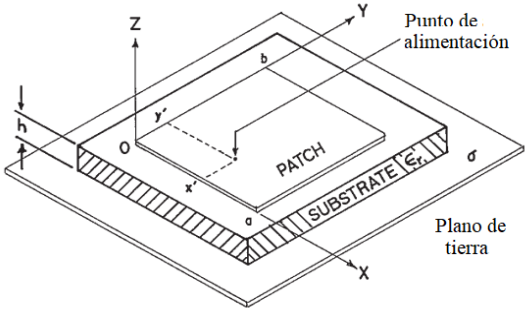


Fig. 1. Geometría y parámetros de la antena de microcinta rectangular. Las dimensiones del patch irradiador son a x b, el punto de alimentación está en la coordenada (*x*', *y*') y la espesura del dieléctrico es igual a *h*.

Observando el gráfico de la Fig. 1 se puede intuir que la antena puede ser aproximada a una cavidad formada por dos paredes eléctricas perfectas – constituidas por el patch de dimensiones $a \times b$ y su proyección sobre el plano de tierra – y cuatro paredes magnéticas perfectas posicionadas sobre el perímetro del patch con altura *h*. En esta cavidad, internamente, tenemos el dieléctrico que forma parte del laminado TMM10i y cuyas características fueron presentadas en la Tabla I. El punto de alimentación, en este gráfico, está posicionado en las coordenadas (*x*', *y*') y para este análisis se considerará una punta de prueba coaxial.

Los profesores Lo y Richards son considerados como los primeros investigadores en proponer la analogía con la cavidad equivalente para estudiar antenas de microcinta (Microstrip anntenas) [12]. A partir de esa propuesta, expresiones para los modos de propagación, impedancia de entrada y eficiencia de irradiación fueron propuestas para varias geometrías canónicas básicas, como la rectangular, triangular, circular, entre otras. Con el objetivo de tornar el texto autcontenido se presentan, a continuación, las expresiones usadas para caracterizar el campo eléctrico de los modos de propagación TM_{mn}, la impedancia de entrada y los

campos eléctricos distantes en los planos principales [13]. Iniciemos con las expresiones del campo $E_z(x, y)$ para los modos TM_{mn}.

$$E_z(x,y) = \sum_{m=0}^{M}\sum_{n=0}^{N} A_{mn}\Phi_{mn}(x,y) \quad (1)$$

donde:

$$A_{mn} = j\omega\mu \frac{\langle J_z, \Phi_{mn}\rangle}{\langle \Phi_{mn}, \Phi_{mn}\rangle}\left(\frac{1}{k_c^2 - k_{mn}^2}\right) \quad (2)$$

$$\Phi_{mn}(x,y) = \cos\left(\frac{m\pi x}{a_{eff}}\right)\cos\left(\frac{n\pi y}{b_{eff}}\right) \quad (3)$$

$$k_c^2 = \varepsilon_r(1 - j\tan\delta_{eff})k_0^2 \quad (4)$$

$$k_{mn}^2 = \left(m\pi/a_{eff}\right)^2 + \left(n\pi/b_{eff}\right)^2 \quad (5)$$

Se resalta que, el operador producto interno es representado por la notación <, >. El parámetro a_{eff} es igual a $a + \Delta a$, b_{eff} es igual a $b + \Delta b$, Δa y Δb son pequeños incrementos en las dimensiones físicas del patch para compensar los efectos de borde, k_0 es el número de onda en el espacio libre ($k_0 = c_0/f_{op}$), f_{op} es igual a la frecuencia de operación de 1.575 GHz y c_0 es la velocidad de la luz en el vacío; i.e., ≈ 3x108 m/s.

Para el cálculo de la impedancia de entrada, en el punto de coordenadas (x', y'), se tiene la expresión:

$$Z_{prova} = \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{j\omega\alpha_{mn}}{\omega_{mn}^2 - k_c^2\omega^2/(\varepsilon_r k_0^2)} \quad (6)$$

donde:

$$\alpha_{mn} = \frac{h\delta_m\delta_n}{a_{eff}b_{eff}\varepsilon_0\varepsilon_r}\cos^2\left(\frac{m\pi x'}{a_{eff}}\right)\cos^2\left(\frac{n\pi y'}{b_{eff}}\right)\mathrm{sinc}^2\left(\frac{m\pi\omega_p}{2a_{eff}}\right) \quad (7)$$

δ_m y δ_n son coeficientes que deben cumplir con la condición de que $\delta_i = 1$ si $i = 0$ y $\delta_i = 2$ si $i \neq 0$. Además, ω_p es el ancho de la punta de prueba coaxial.

Las componentes de campo eléctrico distante E_θ (θ, ϕ) y $E\phi$ (θ,ϕ), en coordenadas esféricas y generadas por el modo TM*01*, son:

$$E_\phi = -j2V_0 bk_0 \frac{e^{-jk_0 r}}{4\pi r} F(\theta,\phi) \quad (8)$$

$$E_\theta = 0 \quad (9)$$

donde V_0 es la tensión sobre la abertura equivalente que se establece alrededor de la patch rectangular, $F(\theta,\phi)$ es una función angular que depende del modo de propagación y de los planos principales de irradiación considerados. Para el modo TM_{01} la función $F(\theta,\phi)$ es expresa a través de la relación $F(\theta,\phi) = F_E(\phi)F_H(\theta)$. Además, $F_E(\phi)$ es el diagrama de irradiación en el plano-E y $F_H(\theta)$ es el diagrama de irradiación en el plano-H. Esto es:

$$F_E(\phi) = \frac{\sin\left(k_0(h/2)\cos\phi\right)}{k_0(h/2)\cos\phi}\cos\left(k_0(b/2)\cos\phi\right) \quad (10)$$

$$F_H(\theta) = \frac{\sin\left(k_0 b\cos\theta\right)}{k_0 b\cos\theta}\sin(\theta) \quad (11)$$

Expresiones análogas a las presentadas en (8) y (9) se pueden obtener para los planos-E y plano-H, ahora para el modo de propagación TM10, mas, en este caso la componente nula se intercambia entre E_θ y E_ϕ.

Para obtener la polarización circular, el punto de alimentación y la geometría del patch deben ser tales que se garantice la excitación simultánea de los modos TM_{01} y TM_{10}. Adicionalmente, estos modos deben estar temporalmente y geométricamente desplazados de 90º. Estas condiciones se logran, en la geometría casi cuadrada, cuando las dimensiones de los lados a_{eff} y b_{eff} son similares (condición para excitar simultáneamente de los modos TM_{01} y TM_{10}) y posicionando la prueba coaxial alrededor de la diagonal del patch [11]-[15].

Analizando el comportamiento del desempeño de la impedancia de entrada (6), para el modo TM_{01} o TM_{10}, se puede concluir que el valor de impedancia que se obtienen cuando la punta de prueba se posiciona en cualquiera de las esquinas de la diagonal del patch (denominada de impedancia de borde) son sumamente altas y del orden de centenas de ohms. Esto hace que el descasamiento entre la prueba coaxial (típicamente 50Ω o 75Ω) y la impedancia de borde sea una dificultad a más en el diseño. En este punto se debe resaltar que una de las características intrínsecas de las antenas de microcinta es la posibilidad de integrar circuitería de microondas. Por lo tanto, se puede usar esta característica e integrar un circuito de acoplamiento de impedancia al patch. Este acoplador podría estar constituido por una sección de línea de transmisión que funciona como un desfaje adicional y un transformador λ/4, por ejemplo. Esto permite minimizar el valor de |S11| y garantizar el acoplamiento de impedancia necesario. En este trabajo solo se consideran los efectos producidos por la adición de la línea de transmisión, ya que el acoplamiento con un conector SMA será presentado futuramente.

Para garantizar la coexistencia simultánea de los modos TM_{10} y TM_{01}, observe (1), las dimensiones de a y b deben ser muy próximas a $\lambda_g/2$ – donde λ_g se puede calcular, en una primera aproximación, como $\lambda_0/(\varepsilon_r)^{1/2}$. Para la frecuencia de operación de 1.575 GHz y con el ε_r igual a 9.8 la dimensión de $a \cong b$ = 30.41 mm. Para completar las dimensiones de la geometría inicial se considera que $x' = y' =$ 30.41 mm. Las dimensiones del sustrato fueron fijadas a 60 mm x 60 mm y la esquina inferior del pach se desplazó del borde del sustrato de 8 mm. Las dimensiones de la geometría inicial son mostradas en la Fig. 2.

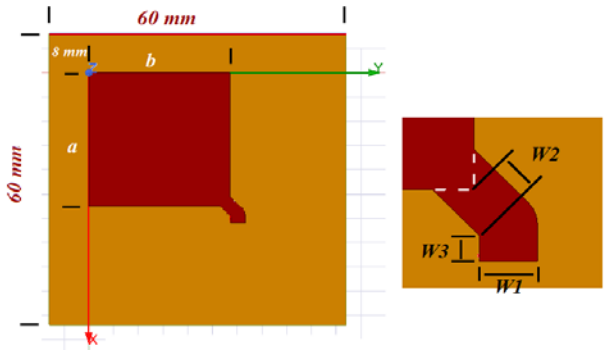


Fig. 2. Geometría inicial diseñada a través del método de la cavidad resonante equivalente.

Las dimensiones calculadas para la geometría inicial, presentadas en la Fig. 2 y que fueron estimadas en el párrafo anterior, serán optimizadas con el auxilio del software HFSS. La guía paso a paso para garantizar la optimización, en términos de, RA, $D(\theta,\phi)$ y Zin se presenta en la próxima sección.

III. Optimización De La Geometría Inicial Con Auxilio Del Software HFSS

Antes de iniciar con el proceso de optimización, debemos resaltar, de lo expuesto anteriormente, que el modo TM_{10} es controlado por la dimensión *a*, el modo TM_{01} es controlado por la dimensión *b*, que la polarización circular requiere que los dos modos coexistan simultáneamente y que la impedancia de borde es del orden de centenas de ohms.

Paso uno: construcción, dentro del entorno de diseño mecánico de HFSS, de la geometría inicial y, adicionalmente, parametrizar todas sus dimensiones para poder realizar una sintonía fina de sus dimensiones y mejorar el desempeño de RA, $D(\theta,\phi)$ y Zin. El modelo virtual de la antena construida dentro del entorno del HFSS se muestra en la Fig. 3.

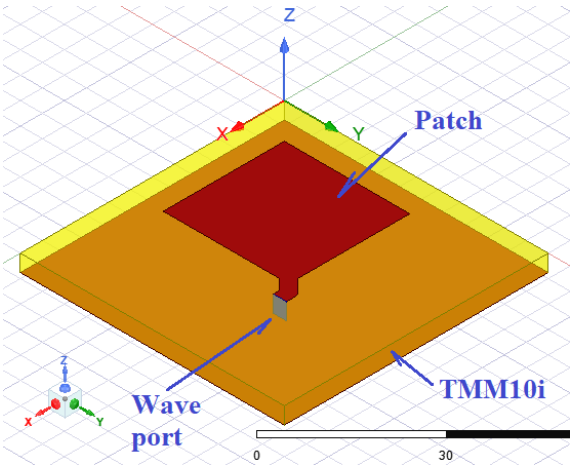
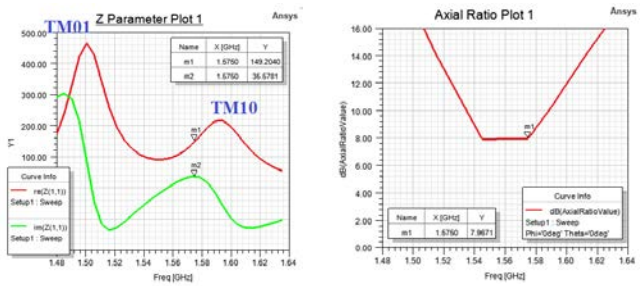


Fig. 3. Modelo virtual de la geometría inicial construida en HFSS.

Los materiales que fueron definidos para los elementos destacados en la Fig. 3 son: i) cobre para el patch y para el plano de tierra con conductividad eléctrica igual a 58 MS, ii) para el wave port se optó por un puerto concentrado interno o Lumped Port y iii) para las condiciones de frontera se usó paredes del tipo PML (Perfectly Matched Layer) de acuerdo con lo recomendado en los manuales de HFSS [9].

Con el objetivo de que los dos modos de propagación sean excitados, en una primera simulación, se modificó la dimensión del lado b, que controla el modo inferior (TM_{01}), a 29.41mm (1 mm menor al valor estimado de 30.41 mm en la sección II), la reducción en el parámetro *a*, que controla el modo superior (TM10), dio una dimensión de 27.41 mm y el puerto Lumped Port se posicionado en punto (*a*, *b*). Para esta simulación, las dimensiones W_2 y W_3 fueron configuradas a 0 mm. La reducción en las dimensiones de los valores de *a*, *b* y el posicionamiento del punto de alimentación garantizaron, en principio, que la antena presente polarización RHCP [11]. Los resultados simulados para Zin y RA son presentados en la Fig. 4.

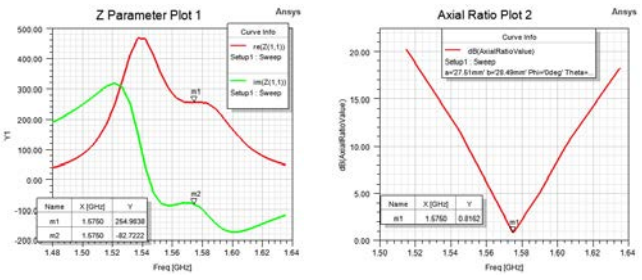
Observando los gráficos de la Fig. 4 se verifica que: i) los dos modos TM_{01} y TM_{10} están presentes, pero fueron excitados de forma desbalanceada, ii) la RA es mayor que 3 dB en toda la banda y por tanto la antena no está circularmente polarizada. iii) La frecuencia de 1.575 GHz no es ni la frecuencia de mejor RA, ni la de mejor Zin y que, principalmente, la antena está trabajando fuera de la frecuencia de operación necesaria para GPS.



(a) (b)

Fig. 4. Resultados de la primera simulación en HFSS para: a) impedancia en el puerto Zin, b) razón axial en la dirección $\theta = 0°$ y $\phi = 0°$.

Paso dos: Para poder corregir los problemas mencionados, se debe modificar la geometría del patch (las dimensiones a y b) y así propiciar que los modos superior e inferior se posicionen alrededor de la frecuencia central de 1.575 GHz. Adicionalmente, los modos serán excitados de forma desbalanceada para corregir la característica capacitiva de la impedancia de entrada producida por la espesura del substrato. Después de pocas iteraciones más, se llegó a definir los nuevos valores de $a = 27.51$ mm y $b = 28.49$ mm que optimizan la RA. Los resultados obtenidos se presentan en la Fig. 5.



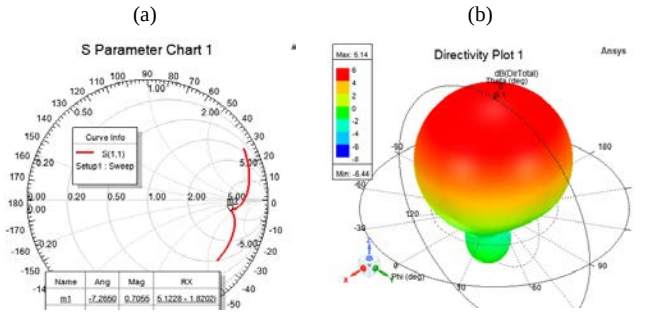


Fig. 5. Resultados de la simulación con a = 27.51 mm y b = 28.49 mm. En a) la impedancia en el puerto – Zin, en b) la razón axial en la dirección broadside, en c) el comportamiento del parámetro S11 en la carta de Smith y en d) la representación 3D de la función directividad – $D(\theta, \phi)$.

Claramente se observa que los modos superior e inferior, Fig. 5a, están fuertemente desbalanceados. Esto permitió ajustar la RA a 0.82 dB en la frecuencia de 1.575 GHz, más, incrementa el descasamiento de la Zin. En la frecuencia de proyecto la Zin presenta un comportamiento capacitivo, Zin ≅ 255-j83 Ω, que se puede apreciar en las Fig. 5a y Fig. 5b. El valor del parámetro S11 graficado en la carta de Smith (Fig. 5c) es de 5.12-j1.65. Este valor dificultará el acoplamiento de la impedancia de entrada. Ahora, el valor obtenido para la directividad, directamente sobre la dirección broadside $D(0,0)$, fue igual a 5.14 dB (Fig. 5d). Este resultado y el comportamiento del diagrama 3D concuerdan con los datos que diversos autores han presentado en la literatura técnica disponible.

Paso tres: Con el objetivo de facilitar el casamiento de Zin, se adicionó una línea de transmisión (desfasaje) entre el irradiador y el puerto lumped port. El objetivo de esta línea es mover, sobre un círculo de Γ constante, el punto de operación desde el valor de S_{11} = 5.12-j1.65 hasta aproximadamente la posición 1-jX. Las dimensiones finales para las líneas de transmisión adicionadas (ver Fig. 2) fueron: ancho W_1 = 3 mm, las longitudes W_2 y W_3 fueron 2.5 mm y 1.97 mm, respectivamente. Los resultados de esta simulación se observan en la Fig. 6.

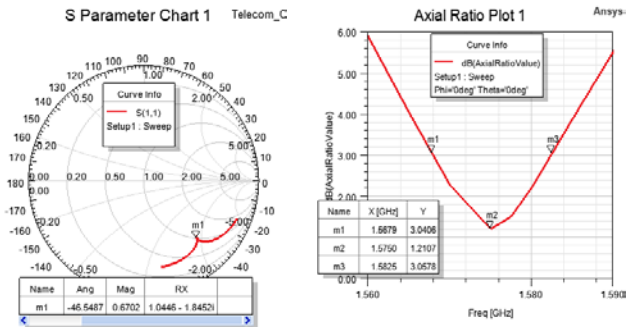


Fig. 6. Resultados de la simulación cuando una línea de transmisión se adicionó al irradiador. Se observa en a) el comportamiento, sobre la carta de Smith, del parámetro S_{11}, b) la razón axial en la dirección broadside.

Comparando el comportamiento de $|S_{11}|$ de las figuras Fig. 5c y Fig. 6a se observa que realmente el punto de trabajo se desplazó para 1.04-j1.85 en la frecuencia de 1.575 GHz. Además, el incremento de 0,4 dB en la RA (i.e., de 0.82 para 1.22) es producido por la perturbación que la línea de transmisión causa sobre los campos irradiados por el patch. Adicionalmente, se puede observar en la Fig. 6b que el ancho de banda de la RA es de aproximadamente 15 MHz como fue definido en las especificaciones.

Finalmente, las dimensiones optimizadas para la geometría de la antena y las simulaciones para los parámetros de desempeño son presentadas en la sección IV.

IV. Geometría Optimizada De La Antena Y Su Desempeño Simulado Con HFSS

En este punto se debe recordar que la geometría y las dimensiones del laminado TMM10i usado para construir la antena es un cuadrado de 60mm x 60mm y 3,81mm de espesura. Adicionalmente, el patch irradiador está alejado de la borda del laminado de 8 mm (ver Fig. 2). En la Tabla II se presenta la comparación entre las dimensiones de la geometría inicial y la geometría optimizada.

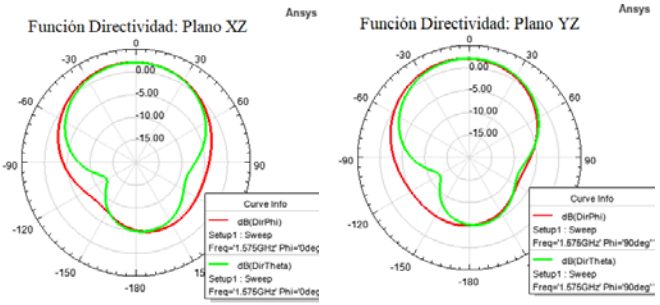
Al comparar las dimensiones a y b (ver Tabla II), se observa que la reducción en sus dimensiones no supera el 9,5%, aproximadamente. Si no se realiza esta reducción en las dimensiones de la geometría inicial, la antena simplemente no opera dentro de las especificaciones necesarias. Al contrario, la antena optimizada cumple totalmente con las especificaciones del proyecto y esto se verifica observando las Fig. 6, Fig. 7 y Fig. 8.

Tabla II
Comparación entre las dimensiones de la geometría inicial y optimizada para la antena casi cuadrada

Geometría	a mm	b mm	W_1 mm	W_2 mm	W_3 mm
Inicial	30.41	30.41	0.00	0.00	0.00
Optimizada	27.52	28.51	3.00	2.50	1.97

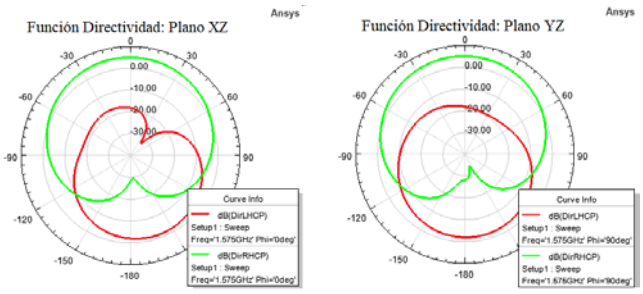
En relación con el casamiento de impedancia se debe mencionar que en este trabajo solamente se adicionó la línea de transmisión para desplazar el valor de S_{11} a una posición que facilite el casamiento con el conector SMA (ver Fig.6a) y que en trabajos futuros se presentará el casamiento de la antena.

El valor de 1,22 dB para la RA (Fig. 6b) garantiza que la antena esté circularmente polarizada en la frecuencia L1 de GPS, i.e., 1,575 GHz. Adicionalmente, los diagramas de irradiación para la función directividad (Fig. 7) confirman esta característica. Además, comparando los componentes $D_\theta(\theta, \phi)$ y $D_\phi(\theta, \phi)$ se observa que la mejor RA está sobre la dirección broadside y con un ancho de lóbulo de ±30º. Se debe resaltar que, hasta este punto, no se ha dicho nada con relación a la dirección de la polarización, i.e., si es derecha o izquierda. Esta duda se verificó graficando los diagramas RHCP y LHCP en la Fig. 8.



(a) (b)

Fig. 7. Diagramas de la función directividad en la frecuencia de 1.575 GHz. Las características en los planos *xz* y *yz* se muestran en los gráficos (a) y (b), respectivamente. La línea roja describe el comportamiento de la componente D_ϕ y la línea verde la componente D_θ.



(a) (b)

Fig. 8. Diagramas de la función directividad asociadas la polarización circular a la derecha RHCP, en verde, y a la polarización circular a izquierda LHCP, en rojo, en la frecuencia de 1.575 GHz. Los gráficos (a) y (b) presentan el comportamiento en los planos *xz* y *yz*, respectivamente.

Los gráficos en verde de la Fig. 8 representa la función directividad $D(\theta, \phi)$ obtenida solamente para la polarización RHCP, en cuanto que los gráficos en rojo corresponden a la polarización LHCP. Por lo tanto, la antena diseñada presenta una polarización RHCP en la dirección broadside, cumpliendo con las especificaciones iniciales del proyecto.

V. Conclusiones

El diseño, simulación y la guía de optimización de antenas de microcinta, circularmente polarizadas RHCP, que trabajan en la banda L_1 del sistema GPS, con el auxilio del software HFSS, se mostraron eficaces para alcanzar las especificaciones iniciales del proyecto propuesto. La razón axial RA de 1.22 dB en la dirección broadside, su ancho de banda de la RA de 15 MHz y los diagramas de irradiación que muestran una directividad de 5.14 dB en esta misma dirección permiten deslumbrar un adecuado funcionamiento para esta aplicación. Como mencionado en la Sección IV, futuramente se presentará el procedimiento para el casamiento de impedancia y, adicionalmente, las medidas de los diagramas de irradiación, las pérdidas de retorno, así como, la comparación con sus correspondientes valores simulados con el HFSS.

Referencias

[1] A. Cratere, L. Gagliardi, G. A. Sanca, F. Golmar, y F. Dell'Olio, "On-Board Computer for CubeSats: State-of-the-Art and Future Trends", IEEE Access, vol. 12, pp. 99537–99569, 2024, doi: 10.1109/ACCESS.2024.3428388.

[2] J. P. Tovar Soto, C. F. Pareja Figueredo, J. S. Vargas Cañón, y L. C. Gutiérrez Martínez, "A review of the current state of Pico and Nanosatellites: some applications in Latin America and other regions of the world", GRAINE. Boletín de Investigaciones., vol. 2, no 1, pp. 13–30, sep. 2020, doi: 10.52408/gbdivol2iss1pp13-30.

[3] A. Zeedan y T. Khattab, "CubeSat Communication Subsystems: A Review of On-Board Transceiver Architectures, Protocols, and Performance", IEEE Access, vol. 11, pp. 88161–88183, 2023, doi: 10.1109/ACCESS.2023.3304419.

[4] S. Malisuwan y B. Kanchanarat, "Small Satellites for Low-Cost Space Access: Launch, Deployment, Integration, and In-Space Logistics", American Journal of Industrial and Business Management, vol. 12, no 10, pp. 1480–1497, 2022, doi: 10.4236/ajibm.2022.1210082.

[5] K. S. Low, M. S. C. Tissera, y J. W. Chia, "In-orbit results of VELOX-II nanosatellite", en 2016 IEEE Region 10 Conference (TENCON), IEEE, nov. 2016, pp. 3658–3663. doi: 10.1109/TENCON.2016.7848740.

[6] S. A. Ali Shah y U. Arshad, "General system design of Cubesat in LEO for IR imaging", en 2013 International Conference on Aerospace Science & Engineering (ICASE), IEEE, ago. 2013, pp. 1–5. doi: 10.1109/ICASE.2013.6785552.

[7] J. Li, M. Post, T. Wright, y R. Lee, "Design of Attitude Control Systems for CubeSat-Class Nanosatellite", Journal of Control Science and Engineering, vol. 2013, pp. 1–15, 2013, doi: 10.1155/2013/657182.

[8] N. Nadarajah, P. J. G. Teunissen, y P. J. Buist, "Attitude determination of LEO satellites using an array of GNSS sensors", en 2012 15th International Conference on Information Fusion, Singapore: IEEE, jul. 2012, pp. 1066–1072.

[9] Ansoft Corporation, User's guide – High Frequency Structure Simulator. Pittsburgh, PA: Ansoft Corporation, 2005.

[10] Rogers Corporation, "TMM® 10i Laminates", https://www.rogerscorp.com/advanced-electronics-solutions/ tmm-laminates/tmm-10i-laminates.

[11] J. R. James y P. S. Hall, Handbook of Microstrip Antennas, 2a ed. London - UK: Peter Peregrinus Ltd., 1989.

[12] W. Richards, Yuen Lo, y D. Harrison, "An improved theory for microstrip antennas and applications", IEEE Trans Antennas Propag, vol. 29, no 1, pp. 38–46, ene. 1981, doi: 10.1109/TAP.1981.1142524.

[13] R. Bancroft, Microstrip and printed antenna design, 2th ed. Raleigh, NC: SciTech publishing Inc., 2009.

[14] D. Chagas y J. C. da S. Lacav, "Design of Low-Cost Probe-Fed Microstrip Antennas", en Microstrip Antennas, InTech, 2011. doi: 10.5772/14523.

[15] A. F. Tinoco S, D. C. Nascimento, y J. C. da S. Lacava, "Rectangular microstrip antenna design suitable for undergraduate courses", en 2008 IEEE Antennas and Propagation Society International Symposium, IEEE, jul. 2008, pp. 1–4. doi: 10.1109/APS.2008.4619275.

MASKAY 16(1), May 2026
ISSN 1390-6712

Recibido (Received): 2025/04/18
Aceptado (Accepted): 2025/07/19

Evaluación del rendimiento Uplink de redes inalámbricas en conformidad con IEEE 802.11g e IEEE 802.11n bajo un escenario de interferencia cocanal

Uplink performance evaluation of wireless networks based on IEEE 802.11g and IEEE 802.11n under co-channel interference

Darling Cruz, Kevin Méndez, David Morán, Ángelo Tupiza, Carlos Veloz, Alina Villavicencio

***Abstract*—Due to their widespread use, wireless networks conforming to IEEE 802.11g/n standards can experience channel saturation, leading to interference that affects their performance. This study analyzes the performance of these networks under various interference scenarios, evaluating their behavior in terms of Quality of Service (QoS) metrics, including throughput, delay, jitter, and packet loss. Experiments were conducted in indoor environments using two standards, IEEE 802.11g/n, and different channel configurations. Initially, networks were evaluated in scenarios where all devices operated on the same channel (1, 6, or 11), creating co-channel interference. Subsequently, scenarios were analyzed where each access point operated on a different channel to minimize interference. The intrusive traffic injection technique was employed for data collection, enabling precise measurements of the analyzed metrics. The results indicate that network performance varies significantly depending on the standard used and the channel configuration. Overall, networks operating under the IEEE 802.11n standard exhibited better throughput performance but were more susceptible to interference compared to those operating under the IEEE 802.11g standard. Additionally, transmission efficiency decreased significantly in the presence of co-channel interference, with performance losses of up to 35% in some scenarios. These findings underscore the significance of effective channel planning in wireless networks, enabling optimal performance and mitigating the adverse effects of interference.**

***Index Terms*— Normalized throughput, delay, jitter, packet loss, co-channel interference, IEEE 802.11g, IEEE 802.11n.**

***Resumen*— Debido a su amplio uso, las redes inalámbricas en concordancia con los estándares IEEE 802.11g/n pueden experimentar saturación de canal, lo que genera interferencias que afectan su rendimiento. Este estudio analiza el rendimiento de estas redes en diferentes escenarios de interferencia, evaluando su comportamiento en términos de métricas de Calidad de Servicio, como rendimiento, retardo, jitter y pérdida de paquetes. Se realizaron experimentos en interiores utilizando dos estándares, IEEE 802.11g/n, y diferentes configuraciones de canal. Inicialmente, las redes se evaluaron en escenarios donde todos los dispositivos operaban en el mismo canal (1, 6 u 11), lo que generaba interferencia cocanal. Posteriormente, se analizaron escenarios donde cada punto de acceso operaba en un canal diferente para minimizar la interferencia. Se empleó la técnica de inyección de tráfico intrusivo para la recopilación de datos, lo que permitió mediciones precisas de las métricas analizadas. Los resultados indican que el rendimiento de la red varía significativamente según el estándar utilizado y la configuración del canal. En general, las redes que operan bajo el estándar IEEE 802.11n mostraron un mejor rendimiento, pero fueron más susceptibles a las interferencias en comparación con IEEE 802.11g. Además, la eficiencia de transmisión disminuyó significativamente en presencia de interferencia con pérdidas de rendimiento de hasta un 35 % en algunos escenarios. Estos hallazgos resaltan la importancia de una planificación adecuada de canales en las redes inalámbricas para optimizar el rendimiento y minimizar los efectos adversos de las interferencias.**

***Palabras Claves*— Rendimiento normalizado, retardo, jitter, pérdida de paquetes, interferencia IEEE 802.11g, IEEE 802.11n.**

D. Cruz, K. Méndez, D. Morán, A. Tupiza, C. Veloz, and A. Villavicencio pertenecen a la Carrera en Telecomunicaciones del Departamento de Eléctrica, Electrónica y Telecomunicaciones de la Universidad de las Fuerzas Armadas ESPE ({dmcruz3, ksmendez, cymoran, ajtupiza, csveloz, apvillavicencio1}@espe.edu.ec).

I. Introducción

Las redes inalámbricas en concordancia con los estándares IEEE 802.11g/n han experimentado una adopción masiva en diversos entornos, desde el hogar hasta aplicaciones industriales y comerciales. Sin embargo, su creciente uso ha provocado problemas de saturación de canales, lo que genera interferencias y afecta el rendimiento de la red. La interferencia es uno de los principales factores que deterioran el desempeño de las redes Wi-Fi, ya que múltiples dispositivos que operan en el mismo canal pueden interferir entre sí, reduciendo la calidad del servicio (QoS, del inglés Quality of Service) y el throughput [1].

El estándar IEEE 802.11g, desarrollado como una mejora sobre IEEE 802.11b, opera en la banda de 2.4 GHz y permite velocidades de transmisión de hasta 54 Mbps mediante el uso de la multiplexación por división de frecuencia ortogonal

DOI: 10.24133/maskay.v16i1.4149

(OFDM, del inglés *Orthogonal Frequency Division Multiplexing*) [2]. Por otro lado, IEEE 802.11n introdujo mejoras significativas en el rendimiento de las redes inalámbricas al implementar tecnologías de múltiples entradas y múltiples salidas (MIMO Multiple-Input Multiple-Output), que permiten el uso de varias antenas para aumentar la capacidad de transmisión. Este estándar ofrece velocidades de hasta 600 Mbps en la banda de 2.4 GHz o 5 GHz, dependiendo de la configuración del canal y el número de flujos espaciales utilizados [3].

Aunque estos estándares ofrecen ventajas notables, las redes basadas en IEEE 802.11g/n continúan presentando desafíos en entornos con alta densidad de dispositivos, particularmente por la interferencia se han comparado el rendimiento de diferentes variantes del estándar IEEE 802.11 en términos de potencia de señal, cobertura y sensibilidad a la interferencia, encontrando que la elección del canal y la tecnología utilizada pueden influir significativamente en el rendimiento de la red [4], [5]. No obstante, los estudios que abordan específicamente el impacto de la interferencia en redes IEEE 802.11g/n son aún limitados.

En este contexto, el objetivo de este artículo es evaluar el desempeño de redes inalámbricas en concordancia con IEEE 802.11g/n bajo diferentes escenarios de interferencia. Se analizarán métricas clave de QoS como throughput, retardo (δ), jitter y pérdida de paquetes (PL), mediante la técnica de inyección intrusiva de tráfico en un entorno de laboratorio. Se compara el rendimiento de las redes cuando operan en los mismos canales y en canales independientes, con el fin de determinar el impacto de la interferencia cocanal (ICC, del inglés *Interference Co-Channel*) en ambos estándares.

El resto del artículo está organizado de la siguiente manera: la Sección II presenta los estudios relacionados con la interferencia en redes IEEE 802.11. La Sección III describe la metodología utilizada en los experimentos, incluyendo los escenarios de prueba, materiales y métodos. En la Sección IV se presentan los resultados obtenidos, y en la Sección V se realiza el análisis y la discusión de los mismos. Finalmente, la Sección VI concluye el estudio y sugiere futuras líneas de investigación.

II. Trabajos Relacionados

La ICC representa un desafío significativo en redes inalámbricas basadas en los estándares IEEE 802.11g y IEEE 802.11n, ya que puede afectar el rendimiento de la transmisión de datos y la estabilidad de la red. En los últimos años, diversas investigaciones han abordado este problema desde distintas perspectivas, evaluando su impacto en redes de alta densidad y proponiendo soluciones para mitigar sus efectos. En [6], se llevó a cabo un estudio sobre el impacto de la interferencia generada por redes IEEE 802.15.4 en dispositivos IEEE 802.11g/n, analizando cómo la coexistencia de ambas tecnologías afecta el rendimiento en términos de throughput, retardo y tasa de errores. Los resultados demostraron que las redes basadas en IEEE 802.11n presentan una mayor susceptibilidad a la interferencia en comparación con IEEE 802.11g, especialmente en entornos donde la densidad de dispositivos es alta.

Otros estudios han explorado estrategias de asignación de canales para reducir los efectos de la ICC en redes inalámbricas malladas [7]. Este enfoque permite optimizar la utilización del espectro disponible mediante algoritmos de asignación dinámica, lo que puede mejorar significativamente el rendimiento de redes IEEE 802.11n en entornos urbanos con múltiples puntos de acceso (AP, del inglés *Access Point*) y alta demanda de tráfico.

Por otra parte, en [8] se realizó un análisis comparativo del rendimiento de redes IEEE 802.11 bajo diferentes condiciones de interferencia y planificación de canales, destacando la importancia de una adecuada configuración de la red para minimizar la ICC. Este estudio concluyó que la elección del estándar y la correcta distribución de los canales juegan un papel fundamental en la estabilidad de la conexión, recomendando la combinación de mecanismos de control de potencia y selección dinámica de canales para mejorar el rendimiento de redes IEEE 802.11g/n en entornos con interferencia.

El trabajo presentado en [9] evaluó específicamente el impacto de la ICC en redes IEEE 802.11b/n, analizando su desempeño a distintas distancias y bajo diferentes niveles de interferencia. Los resultados sugieren que, aunque IEEE 802.11n ofrece un mejor rendimiento en términos de throughput, su eficiencia disminuye drásticamente mientras que IEEE 802.11b muestra una mayor tolerancia a la degradación del canal.

Adicionalmente, en [10] se estudiaron las condiciones óptimas para la implementación de voz sobre redes inalámbricas de área local (VoWLAN, del inglés *Voice over Wireless LAN*), destacando la necesidad de evitar la asignación de canales iguales en celdas adyacentes para minimizar la ICC. Este estudio enfatiza que QoS en aplicaciones de voz y video en redes IEEE 802.11g/n depende en gran medida de la planificación de frecuencias y de la capacidad de mitigación de interferencias mediante la selección dinámica de canales.

En general, estos estudios destacan la importancia de la planificación adecuada del uso de canales en redes IEEE 802.11g/n, especialmente en entornos con alta densidad de dispositivos. La correcta gestión del espectro, el uso de algoritmos de asignación dinámica y la implementación de mecanismos de mitigación de interferencia son estrategias clave para garantizar un rendimiento óptimo en redes inalámbricas que operan bajo estos estándares.

III. Metodología

La presente sección describe la metodología aplicada para evaluar el rendimiento de las redes inalámbricas IEEE 802.11g/n. En primer lugar, se detallan los escenarios de prueba diseñados para representar situaciones con y sin interferencia, lo que permite observar el impacto real de la coexistencia de múltiples APs en un mismo entorno. A continuación, se presentan los materiales y equipos utilizados, cuya selección responde a la necesidad de garantizar que las pruebas se ejecuten con dispositivos representativos y compatibles con los estándares analizados. Finalmente, se

explican los procedimientos experimentales empleados, que integran los escenarios y materiales como parte esencial del enfoque metodológico, asegurando la validez y precisión de los resultados obtenidos.

A. Escenarios de prueba

El experimento se realizó en un cuarto cerrado con dimensiones internas de 7 m de largo, 5 m de ancho y 2,5 m de alto. Esto corresponde a un área de 35 m² y un volumen interior de 87.5 m³. Las paredes son de concreto y tienen diferentes espesores.

La Fig. 1 muestra la distribución de los dispositivos usados en cada red para el primer escenario de prueba, donde se configuró el canal 1 para la red 1, el canal 6 para la red 2 y el canal 11 para la red 3 con el fin de evitar ICC. El segundo escenario de prueba, donde las tres redes inalámbricas se configuran para el mismo canal, forzando la presencia de ICC. Este escenario se repite por tres ocasiones, el primer lugar con el canal 1, en segundo lugar, con el canal 6 y por último con el canal 11, generándose tres subescenarios que serán analizados.

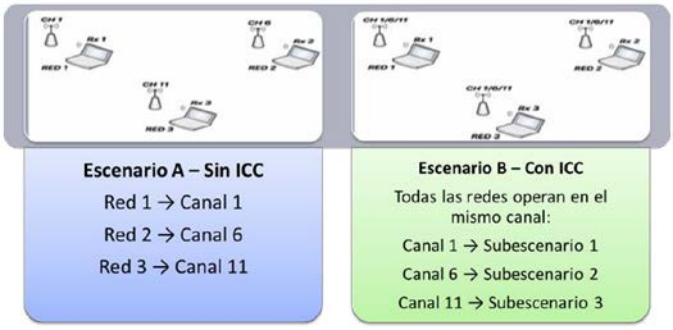
La distancia entre los nodos fue de aproximadamente 1 metro en todos los escenarios, dado que se trata de un entorno controlado de laboratorio.

B. Materiales

Para la toma de mediciones se emplea el método intrusivo de inyección de tráfico mediante el software D-ITG (*Distributed Internet Traffic Generator*), el cual genera tráfico a nivel de paquetes y permite obtener las principales métricas de QoS, tales como: throughput (η), retardo (δ), jitter y pérdida de paquetes (PL). El análisis de los datos adquiridos se realizó mediante la herramienta matemática MATLAB®, mientras que la verificación visual del uso de canales y la presencia de interferencia se efectuó con la aplicación WiFi Analyzer. Las redes configuradas en cada escenario se componen de un AP y dos computadoras portátiles. El AP utilizado, con capacidad para trabajar en los estándares IEEE 802.11 b/g/n, doble frecuencia: 2.4 GHz y 5 GHz, tecnología MIMO 3x3 y velocidades de transmisión de hasta 300 Mbps (2.4 GHz) y 450 Mbps (5 GHz). En la Tabla I se presenta la configuración de los APs. Las computadoras portátiles poseen tarjeta inalámbrica compatible con el estándar IEEE 802.11n, procesador de 2.4 GHz, memoria RAM de 4 GB y sistema operativo Linux.

Para todos nuestros escenarios de prueba se garantiza la sincronización de los relojes internos de los equipos de transmisión y recepción. Esta sincronización se estableció mediante el protocolo NTP (*Network Time Protocol*), el cual se usa generalmente para sincronizar relojes en la Internet.

En este caso las redes implementadas no están conectadas a Internet, por lo que se sincronizan los relojes creando un servidor propio, como se explica en [4], garantizando el valor del retardo entregado por D-ITG. Se utilizó la misma configuración para el estándar IEEE 802.11n e IEEE 802.11g, ajustando únicamente el modo del router según el estándar requerido. Las pruebas se realizaron en los escenarios descritos, utilizando la misma metodología de inyección de tráfico.



(a) (b)

Fig. 1. Escenarios de prueba: (a) Sin interferencia cocanal. (b) Con interferencia cocanal.

TABLA I
CONFIGURACIÓN DEL ROUTER

Parámetros	Valor
Banda de frecuencia	2.5 GHz
Modo de RED	Wireless-N Only
Ancho de canal	20 MHz
SSID	Grupo 1, Grupo 2, Grupo 3
Canal inalámbrico	1/6/11

Con el fin de determinar el valor de la tasa de transmisión máxima que soporta cada red en los diferentes escenarios de prueba. Para esto se realizaron diferentes inyecciones de tráfico, considerando como punto de partida la tasa de transmisión teórica del estándar IEEE 802.11n, de 300 Mbps sobre un ancho de canal de 20 MHz.

Esta tasa de transmisión se varía hasta conseguir una pérdida de paquetes menor al 5%, aconsejable en aplicaciones en tiempo real, para lo cual se utilizó el protocolo UDP (*User Datagram Protocol*) y se consideró solo el tiempo que tarda un paquete en viajar desde el transmisor al receptor, usando el parámetro "*One Way Delay*" recomendado para trabajar en entornos de laboratorio en el que la información de los eventos está disponible al usuario.

El inicio del retardo se fijó en 0s, y la duración de las transmisiones se limitó a 30s, tiempo suficiente para capturar las métricas del rendimiento de la red, haciendo que sea una medición rápida y repetible en los escenarios, por estar en un ambiente de laboratorio, el cual no presenta obstrucciones, además, se trabajó con redes relativamente pequeñas, máximo 1 m de separación entre dispositivos.

Finalmente, el tamaño del paquete escogido fue de 512 bytes. Se replica la misma configuración en todos los escenarios.

Una vez determinada la tasa de transmisión máxima, luego de considerar la capacidad máxima del canal y el número de paquetes a ser enviados en cada prueba, se configura nuevamente el AP para cada escenario en *uplink*. Las configuraciones de los enlaces se indican en la Tabla II y Tabla III.

TABLA II
TASAS DE TRANSMISIÓN MÁXIMAS Y NÚMERO DE PAQUETES INYECTADOS EN EL ESCENARIO SIN ICC EN UP LINK

Parámetros	Grupo 1	Grupo 2	Grupo 3
	IEEE 802.g		
Tasas de transmisión (Mbps)	3.3919	3.3173	3.3783
Paquetes inyectados (pkt/s)	900	900	900
	IEEE 802.n		
Tasas de transmisión (Mbps)	3.3959	3.3784	3.3034
Paquetes inyectados (pkt/s)	900	900	900

TABLA III
TASAS DE TRANSMISIÓN MÁXIMAS Y NÚMERO DE PAQUETES INYECTADOS EN EL ESCENARIO SIN ICC EN UP LINK

Parámetros	Grupo 1	Grupo 2	Grupo 3
	IEEE 802.g		
	Canal 1		
Tasas de transmisión (Mbps)	3.1776	3.3952	3.3994
Paquetes inyectados (pkt/s)	900	900	900
	Canal 6		
Tasas de transmisión (Mbps)	1.9104	3.3737	3.4002
Paquetes inyectados (pkt/s)	900	900	900
	Canal 11		
Tasas de transmisión (Mbps)	3.4537	3.4310	3.4551
Paquetes inyectados (pkt/s)	900	900	900
	IEEE 802.n		
	Canal 1		
Tasas de transmisión (Mbps)	3.1971	3.3874	3.4163
Paquetes inyectados (pkt/s)	900	900	900
	Canal 6		
Tasas de transmisión (Mbps)	3.4702	3.4508	3.3881
Paquetes inyectados (pkt/s)	900	900	900
	Canal 11		
Tasas de transmisión (Mbps)	3.4553	3.4578	3.5738
Paquetes inyectados (pkt/s)	900	900	900

Para verificar que se realizaron las pruebas en un escenario con ICC en cada uno de los canales, se utiliza la aplicación WiFi Analyzer como se muestra en la Fig. 2. Así como en la Fig. 3 se verifica un escenario independiente donde cada grupo se encuentra en un canal diferente sin ICC.

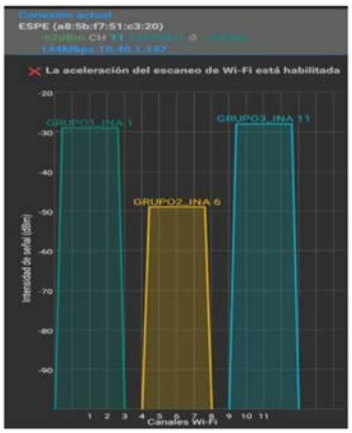
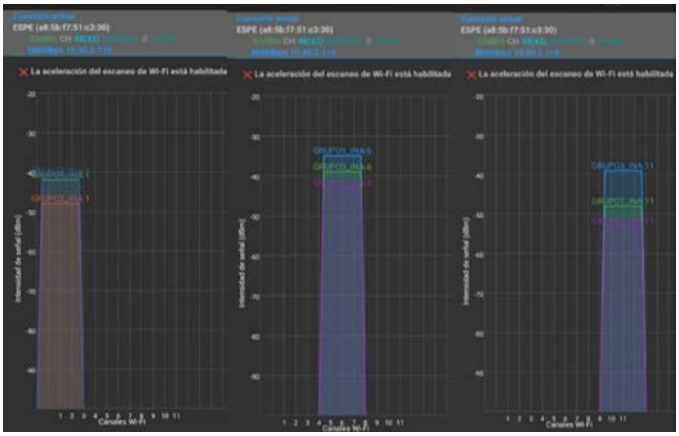


Fig. 2. Escenario de prueba sin ICC.



(a) (b) (c)

Fig. 3. Escenario de prueba con ICC (a) Canal 1 (b) Canal 6 (c) Canal 11.

IV. RESULTADOS

En esta sección se presentan los resultados obtenidos mediante la herramienta D-ITG, considerando los escenarios con y sin ICC. Para cada configuración se evaluaron las métricas de desempeño definidas: η, δ, jitter y PL.

A. *Throughput (η)*

El η se calculó a partir del promedio de seis inyecciones de tráfico en cada escenario. En condiciones sin ICC, los valores obtenidos oscilaron entre 2.54 y 3.22 Mbps, destacándose el mejor desempeño en IEEE 802.11g, con un promedio de 3.03 Mbps.

En presencia de ICC, el η disminuyó de forma significativa en ambos estándares. En 802.11g, las variaciones fueron más pronunciadas, evidenciando una mayor susceptibilidad a la interferencia. Por su parte, 802.11n mostró un η más alto en la mayoría de los escenarios, aunque también presentó caídas cuando todos los AP operaron en un mismo canal.

B. *Retardo (δ)*

El δ se mantuvo bajo en escenarios sin ICC, con promedios cercanos a 3.99 ms en 802.11g. Sin embargo, al operar varios AP en el mismo canal, el δ aumentó de forma considerable, reflejando la degradación generada por la ICC. En contraste, 802.11n evidenció menores valores de δ en la mayoría de los escenarios, confirmando su mayor eficiencia en la transmisión.

C. *Jitter*

Los valores de jitter fueron consistentes en todos los escenarios, con promedios generales inferiores a 2 ms. Esto demuestra que la ICC no generó variaciones significativas en la estabilidad temporal de entrega de paquetes. No obstante, algunos AP presentaron valores atípicos, especialmente en configuraciones con canales solapados, lo que indica posibles colisiones puntuales en la transmisión.

D. *Paquetes Perdidos (PL)*

Para garantizar la validez del experimento se estableció como criterio que la PL no superara el 5 %, límite aceptado en aplicaciones de transmisión en tiempo real. En todos los escenarios evaluados, tanto en condiciones sin interferencia

como bajo la presencia de ICC, este requisito se cumplió de manera consistente. El cumplimiento de este parámetro fue posible gracias al ajuste en la tasa de transmisión configurada en el software de pruebas, lo que permitió reducir la congestión en el canal y evitar la sobresaturación de la red. De este modo, el número de paquetes transmitidos se fijó en un máximo de 900, valor que aseguró estabilidad en el sistema y una entrega confiable de datos. Esta estrategia de control posibilitó mantener un entorno experimental más robusto, minimizando el impacto de factores como la interferencia y la variabilidad en la latencia.

El análisis comparativo de los resultados evidencia que, en presencia de ICC, el η experimenta una reducción significativa en ambos estándares. Sin embargo, la disminución resulta más marcada en IEEE 802.11g, donde la caída en la tasa de transmisión es más pronunciada, lo que confirma una mayor vulnerabilidad de este estándar frente a la interferencia. Por el contrario, aunque IEEE 802.11n también sufre degradaciones en estas condiciones, los valores obtenidos se mantienen en niveles más altos, lo que refleja una mayor capacidad de adaptación al entorno congestionado.

Al examinar el escenario sin ICC se observa un comportamiento particular: los valores de η registrados en IEEE 802.11g superan los alcanzados por IEEE 802.11n. Esta diferencia puede atribuirse a factores externos no controlados durante la ejecución de las pruebas o a características propias del estándar IEEE 802.11g, cuya configuración pudo haber favorecido momentáneamente una mayor estabilidad en la transmisión. No obstante, este resultado puntual no contradice la tendencia general, que señala al estándar IEEE 802.11n como el que ofrece un desempeño superior en la mayoría de escenarios analizados.

1) Diferentes Canales Uplink estándar 802.11g

En la Fig. 4 se aprecia que los AP mantienen un comportamiento de rendimiento similar. El AP2 registra una mediana de η superior respecto a los demás dispositivos, lo que refleja un desempeño más consistente. Sin embargo, presenta una mayor cantidad de valores atípicos, lo que indica variabilidad en la transmisión. En contraste, el AP3, ubicado en el canal 11, muestra menos valores atípicos, aunque con una media de η más baja, lo que compromete la estabilidad general de su desempeño.

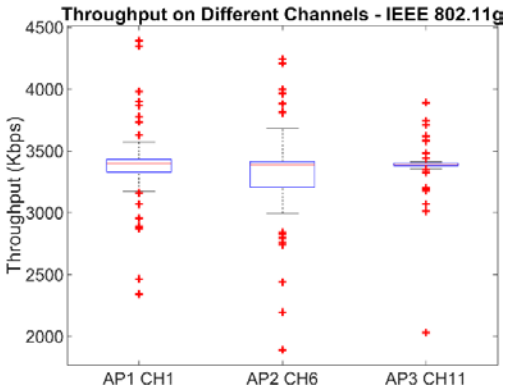


Fig. 4. Gráfica del throughput de los diferentes canales en uplink con el estándar IEEE 802.11g.

En la Fig. 5 se observa que el jitter se mantiene en rangos similares para todos los AP, aunque el AP2 presenta un mayor número de valores atípicos, lo que evidencia fluctuaciones más frecuentes en la estabilidad temporal de la transmisión. Este comportamiento es crítico en aplicaciones sensibles al tiempo, como voz o video en tiempo real.

En la Fig. 6, el AP3 destaca al registrar el menor valor de δ en comparación con los demás dispositivos, lo que indica una transmisión más ágil y eficiente. Por su parte, el AP2, pese a alcanzar un η elevado, presenta el δ más alto, lo que sugiere congestión interna o un mayor procesamiento necesario para sostener dicho caudal de datos.

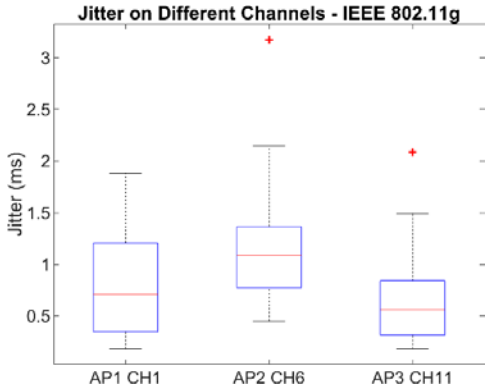


Fig. 5. Gráfica del jitter de los diferentes canales en uplink con el estándar IEEE 802.11g.

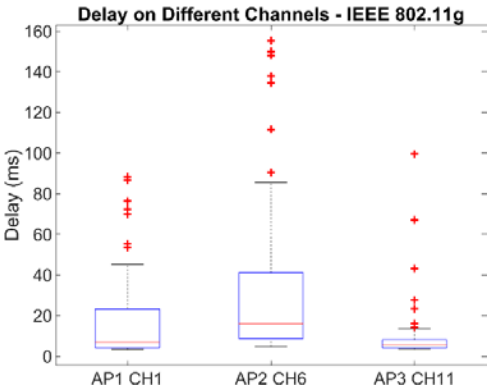


Fig. 6. Gráfica del delay de los diferentes canales en uplink con el estándar IEEE 802.11g.

En la Fig. 7 se aprecia que el PL es similar en el AP1 y el AP3, manteniéndose dentro de los márgenes aceptables. En el AP2, en cambio, se observa un PL más alto, coherente con el jitter elevado registrado en este dispositivo. Este comportamiento confirma la relación entre variabilidad en los tiempos de entrega y mayor probabilidad de descarte de paquetes, lo que repercute en la estabilidad de la transmisión.

2) Diferentes Canales Uplink estándar 802.11n

En la Fig. 8, correspondiente al uplink bajo IEEE 802.11n con diferentes canales, el AP3 alcanza valores superiores de η respecto a los demás dispositivos. Sin embargo, su mediana es más baja que la del AP2, lo que refleja menor estabilidad en la transmisión. A diferencia del AP1, el AP3 no presenta valores atípicos significativos, por lo que, en conjunto, puede considerarse el dispositivo con mejor desempeño al lograr un mayor bitrate aunque con menor consistencia.

En la Fig. 9 se muestra que el jitter mantiene un comportamiento prácticamente uniforme entre los tres AP. La variación en los retardos de los paquetes es mínima, lo que indica una transmisión estable en este escenario y sin diferencias significativas entre los dispositivos.

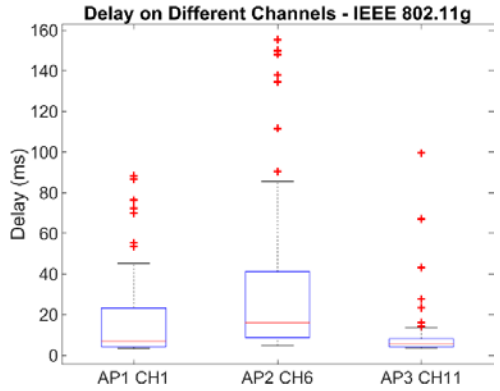


Fig. 7. Gráfica del packet loss de los diferentes canales en uplink con el estándar IEEE 802.11g.

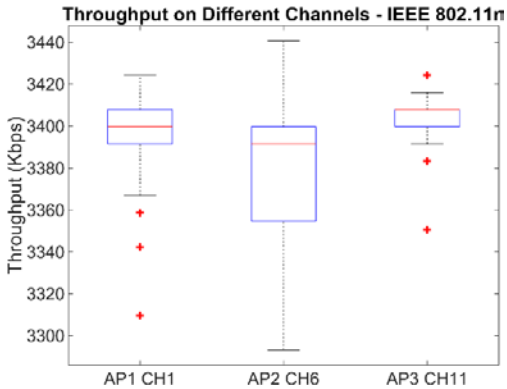


Fig. 8. Gráfica del throughput de los diferentes canales en uplink con el estándar IEEE 802.11n.

En la Fig. 10 se observa que el AP3 registra el menor valor de δ, lo que confirma una transmisión más eficiente y con menor latencia, característica fundamental para aplicaciones en tiempo real. Este resultado evidencia que el AP3 logra optimizar mejor la entrega de datos en comparación con los demás AP.

La Fig. 11 refleja que el PL presenta valores similares en todos los AP, lo que concuerda con los resultados de jitter. La llegada ordenada de los paquetes y la baja variabilidad en δ reducen la probabilidad de descarte, manteniendo la tasa de pérdida en niveles aceptables para servicios que requieren continuidad y estabilidad.

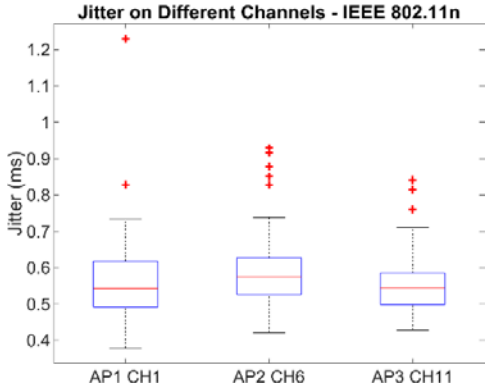


Fig. 9. Gráfica del jitter de los diferentes canales en uplink con el estándar IEEE 802.11n.

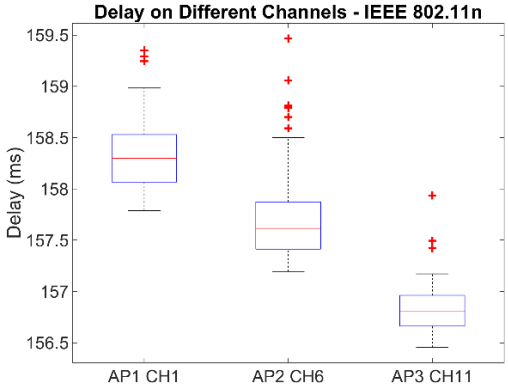


Fig. 10. Gráfica del delay de los diferentes canales en uplink con el estándar IEEE 802.11n.

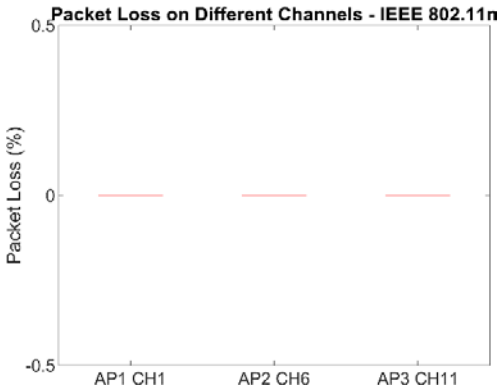


Fig. 11. Gráfica del packet loss de los diferentes canales en uplink con el estándar IEEE 802.11n.

3) Mismo canal / Canal 1/ Estándar 802.11g

En las Fig. 12, Fig. 13, Fig. 14 y Fig. 15, se observa que el

AP3 alcanza un η superior respecto a los demás dispositivos. Aunque la mediana de η en el AP3 resulta menor que la del AP1, este dispositivo mantiene una mayor estabilidad al no presentar valores atípicos significativos, a diferencia del AP1 y el AP2. Este comportamiento indica que el AP3 logra un desempeño más eficiente y consistente, lo que se refleja también en el valor de δ, claramente inferior en comparación con los otros puntos de acceso y, por lo tanto, asociado a un enlace más fluido y con menor latencia.

Con relación al jitter, los tres dispositivos muestran tendencias similares, aunque con la presencia de algunos valores atípicos. A pesar de estas variaciones, los valores globales de jitter permanecen dentro de márgenes aceptables, lo que evidencia que la estabilidad temporal de la red se conserva en este escenario. Mientras que el PL confirma un comportamiento semejante entre los tres AP, aunque el uso compartido del canal pudo haber provocado colisiones ocasionales, coherentes con las fluctuaciones detectadas en el jitter. No obstante, la llegada ordenada de los paquetes en el AP3 parece haber reducido la probabilidad de descarte, lo que explica que este dispositivo presente un manejo más eficiente del tráfico en comparación con los demás.

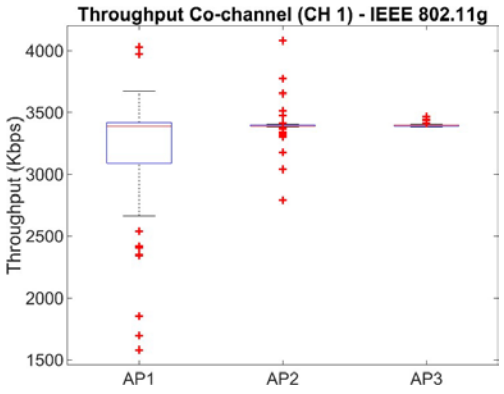


Fig. 12. Throughput del canal 1 en uplink con el estándar IEEE 802.11g.

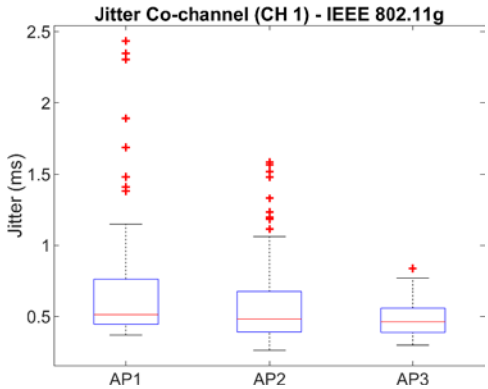


Fig. 13. Jitter del canal 1 en uplink con el estándar IEEE 802.11g.

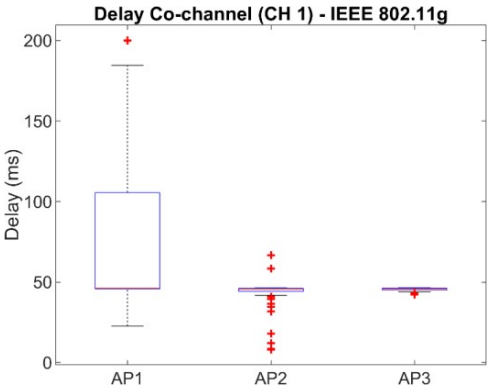


Fig. 14. Delay del canal 1 en uplink con el estándar IEEE 802.11g.

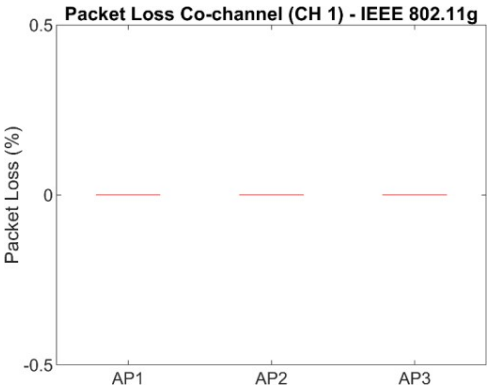


Fig. 15. Packet loss del canal 1 en uplink con el estándar IEEE 802.11g.

4) Mismo canal / Canal 1/ Estándar 802.11n

En las Fig. 16, Fig. 17, Fig. 18 y Fig. 19, se observa que el AP3 alcanza un η ligeramente superior al de los demás dispositivos. La diferencia no resulta significativa debido a que las pruebas se desarrollaron en un entorno controlado y homogéneo; sin embargo, el AP3 puede considerarse el de mejor desempeño al mantener un bitrate más alto en promedio. Este comportamiento se refleja también en el valor de δ, que es menor en el AP3 en comparación con los otros puntos de acceso. En contraste, tanto el AP1 como el AP2 presentan valores atípicos en sus retardos, lo que sugiere una mayor variabilidad en la transmisión.

El análisis del jitter muestra un comportamiento similar entre los tres dispositivos, aunque en el AP1 se evidencian valores atípicos que indican fluctuaciones ocasionales en la estabilidad temporal. Finalmente, el PL se mantiene presente en todos los AP, con un valor más alto en el AP3 a pesar de haber alcanzado un η superior. Esta condición sugiere que, aunque el AP3 logra mayor eficiencia en la transmisión, el efecto de la interferencia generada por la operación simultánea de los tres AP en el mismo canal contribuye a un incremento en la tasa de pérdida.

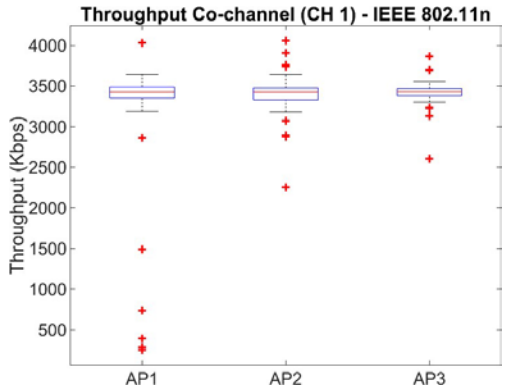


Fig. 16. Throughput del canal 1 en uplink con el estándar IEEE 802.11n.

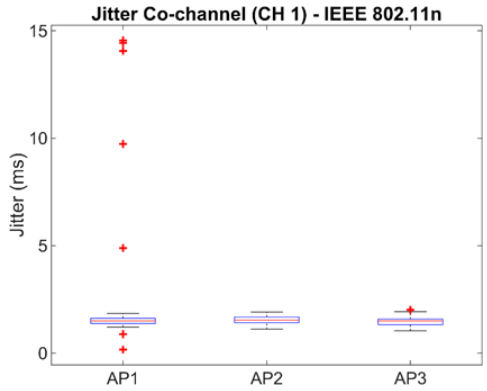


Fig. 17. Jitter del canal 1 en uplink con el estándar IEEE 802.11n.

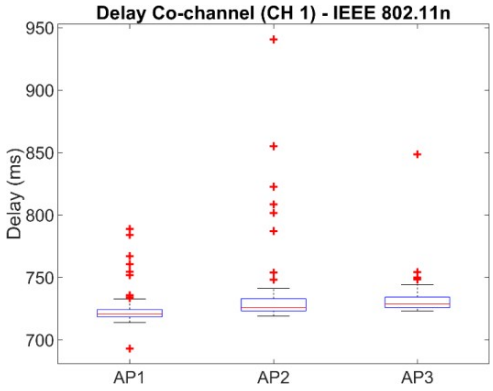


Fig. 18. Delay del canal 1 en uplink con el estándar IEEE 802.11n.

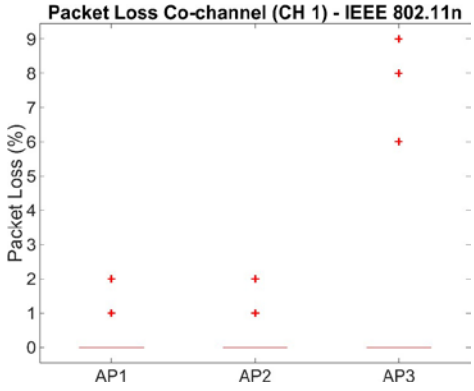


Fig. 19. Packet loss del canal 1 en uplink con el estándar IEEE 802.11n.

5) Mismo canal / Canal 6/ Estándar 802.11g

En las Fig. 20, Fig. 21, Fig. 22 y Fig. 23, se observa una mejora notable en comparación con los resultados obtenidos en el canal 1. En este escenario, el η aumentó de manera significativa en los tres puntos de acceso, con el AP2 alcanzando los valores más altos y mostrando mayor estabilidad en la transmisión. El AP1 también presentó un desempeño aceptable, aunque con una variación ligeramente superior, mientras que el AP3 evidenció una mejora respecto al canal anterior, aunque con episodios de inestabilidad que afectaron la consistencia de su rendimiento.

Por otro lado, el δ refleja una disminución generalizada en todos los dispositivos, con el AP2 nuevamente destacando como el más eficiente, al mantener un retardo menor y más estable en comparación con los otros puntos de acceso. En cuanto al jitter, se aprecia una reducción en términos generales, aunque el AP3 continuó registrando picos de variación que repercuten directamente en su desempeño.

Respecto al PL se muestra una tendencia a la baja en los tres dispositivos, lo que confirma una transmisión más robusta en este escenario. No obstante, la presencia de pérdidas, aunque reducida, indica que la coexistencia de los tres AP en el mismo canal sigue generando colisiones y descartes de paquetes. En conjunto, los resultados demuestran que el uso de 802.11g en el canal 6 permite un mejor manejo de la interferencia respecto al canal 1, aunque todavía persisten limitaciones que impiden alcanzar una estabilidad plena.

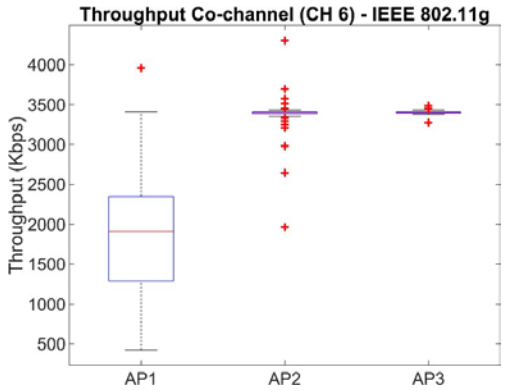


Fig. 20. Throughput del canal 6 en uplink con el estándar IEEE 802.11g.

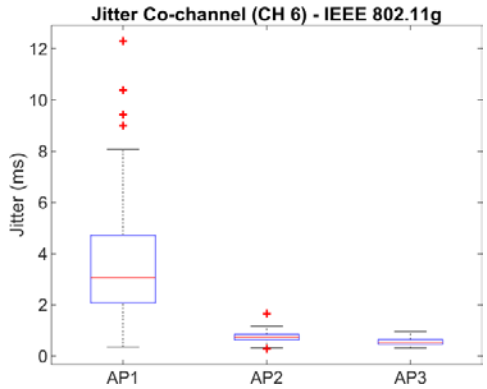


Fig. 21. Jitter del canal 6 en uplink con el estándar IEEE 802.11g.

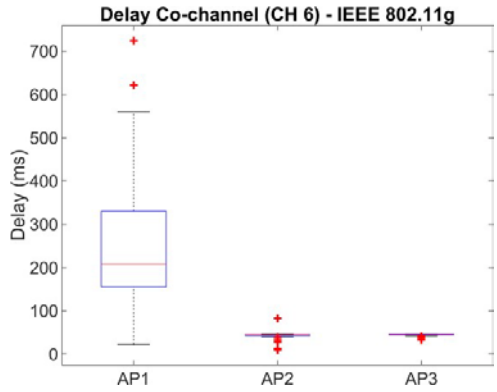


Fig. 22. Delay del canal 6 en uplink con el estándar IEEE 802.11g.

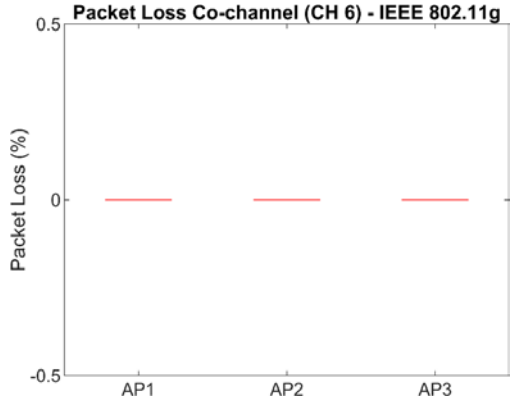


Fig. 23. Packet loss del canal 6 en uplink con el estándar IEEE 802.11g.

6) Mismo canal / Canal 6/ Estándar 802.11n

En la Fig. 24, Fig. 25, Fig. 26 y Fig. 27, se aprecia un incremento considerable de η en los tres puntos de acceso en comparación con los escenarios anteriores. El AP2 alcanzó el mejor desempeño, caracterizado por valores más altos y estables, mientras que el AP1 mantuvo un rendimiento estable con un η notable. El AP3 mostró una mejora respecto a otros escenarios, aunque sus resultados no fueron tan consistentes como los registrados por el AP2. Sus δ evidencian una disminución significativa en este escenario, lo que confirma una transmisión más ágil y con menor latencia. El AP2 se consolidó como el dispositivo más eficiente en esta métrica, presentando valores de retardo inferiores a los de los demás AP.

En cuanto al jitter, los resultados muestran valores bajos y estables en general, aunque en el AP3 se identificaron algunos picos de variación que, si bien no fueron tan pronunciados como en escenarios anteriores, reflejan cierta inestabilidad temporal en la entrega de paquetes. Similar a casos anteriores, el PL se mantuvo en niveles mínimos, prácticamente inexistentes en los tres AP. Esta condición confirma que el estándar 802.11n presenta una mayor capacidad de adaptación a entornos con varios dispositivos operando en el mismo canal, logrando sostener la calidad del servicio aun en condiciones de interferencia cocanal.

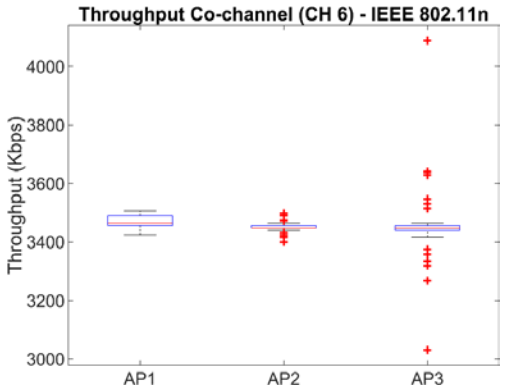


Fig. 24. Throughput del canal 6 en uplink con el estándar IEEE 802.11n.

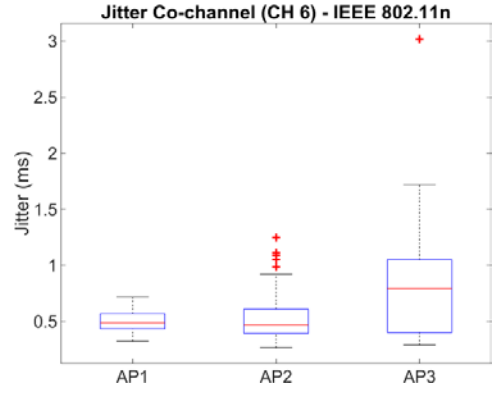


Fig. 25. Jitter del canal 6 en uplink con el estándar IEEE 802.11n.

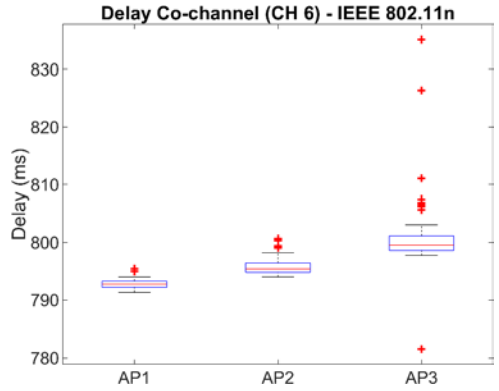


Fig. 26. Delay del canal 6 en uplink con el estándar IEEE 802.11n.

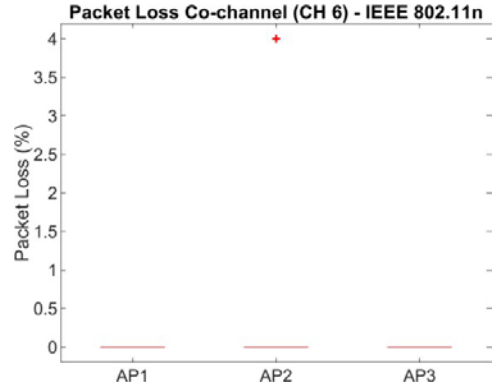


Fig. 27. Packet loss del canal 6 en uplink con el estándar IEEE 802.11n.

7) Mismo canal / Canal 11/ Estándar 802.11g

En la Fig. 28, Fig. 29, Fig. 30 y Fig. 31, se observa una mejora en el desempeño general respecto a escenarios anteriores. El η aumentó de manera significativa en los tres puntos de acceso, con el AP2 destacándose nuevamente como el de mayor rendimiento al registrar valores más altos y estables. El AP1 mantuvo un comportamiento adecuado, mientras que el AP3 presentó ciertas variaciones que afectaron su consistencia, aunque logró un δ inferior al de los otros dispositivos, lo que indica una transmisión más ágil en este punto de acceso.

El jitter se aprecia un comportamiento más controlado en comparación con canales previos, aunque el AP3 mostró episodios de inestabilidad que generaron ligeras fluctuaciones en la entrega de los paquetes. Finalmente, el análisis del PL evidencia una reducción en todos los dispositivos frente a escenarios anteriores, aunque sin llegar a eliminarse por completo. Estos resultados confirman que el uso de 802.11g en el canal 11 permite un mejor aprovechamiento del espectro y una transmisión más eficiente, aunque la presencia de interferencia cocanal continúa afectando el rendimiento cuando los tres AP comparten el mismo canal.

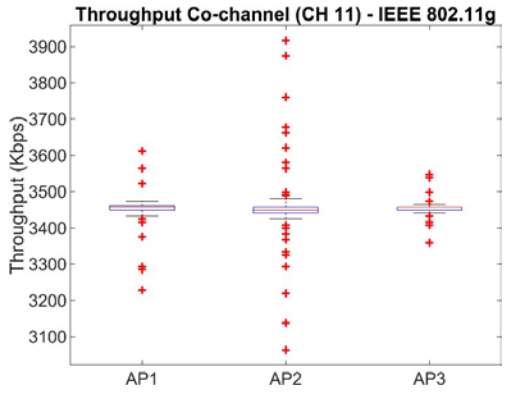


Fig. 28. Throughput del canal 11 en uplink con el estándar IEEE 802.11g.

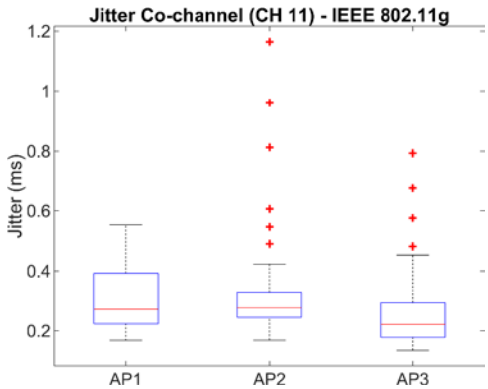


Fig. 29. Jitter del canal 11 en uplink con el estándar IEEE 802.11g.

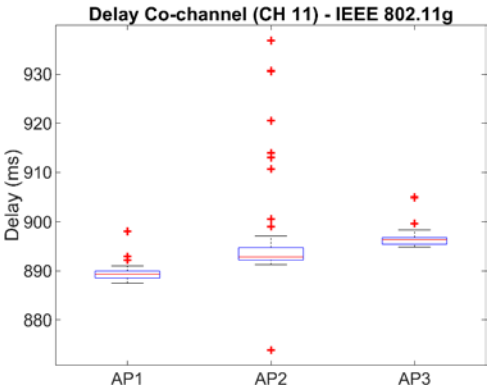


Fig. 30. Delay del canal 11 en uplink con el estándar IEEE 802.11g.

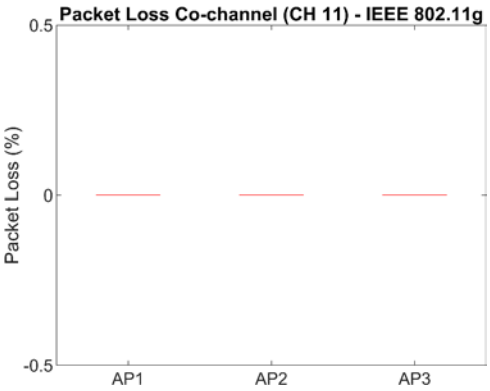


Fig. 31. Packet loss del canal 11 en uplink con el estándar IEEE 802.11g.

8) Mismo canal / Canal 11/ Estándar 802.11n

En la Fig. 32, Fig. 33, Fig. 34 y Fig. 35, se alcanzaron los mejores resultados en todas las métricas evaluadas. El η fue el más alto de todos los escenarios, destacándose el AP2 por su desempeño superior y estable, mientras que el AP1 también registró valores elevados y consistentes. El AP3 presentó un comportamiento ligeramente menos estable, aunque aun así superó los resultados obtenidos en escenarios previos, consolidándose como un dispositivo con rendimiento satisfactorio.

El análisis de δ muestra valores reducidos en todos los AP, con el AP2 nuevamente como el más eficiente al mantener el retardo más bajo, lo que confirma la solidez de este dispositivo en condiciones de alta demanda. En cuanto al jitter, los resultados se mantuvieron controlados, con la excepción de algunos picos menores en el AP3 que no comprometieron la estabilidad general de la transmisión. Finalmente, el PL fue prácticamente nulo en todos los dispositivos, lo que evidencia que el estándar 802.11n es capaz de manejar de forma eficiente la interferencia y la congestión en escenarios donde varios AP comparten el mismo canal, asegurando la calidad del servicio incluso en condiciones de coexistencia crítica.

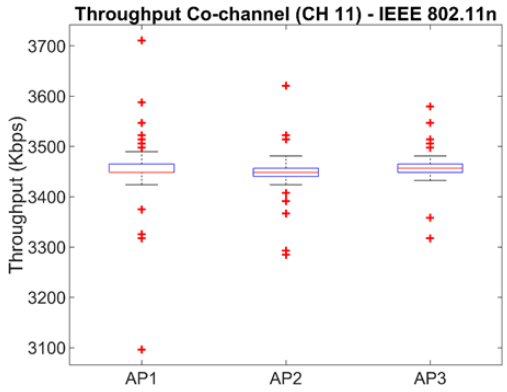


Fig. 32. Throughput del canal 11 en uplink con el estándar IEEE 802.11n.

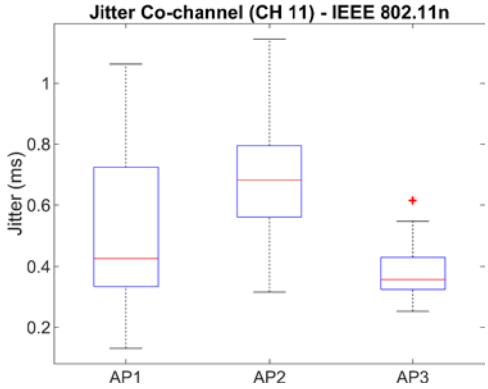


Fig. 33. Jitter del canal 11 en uplink con el estándar IEEE 802.11n.

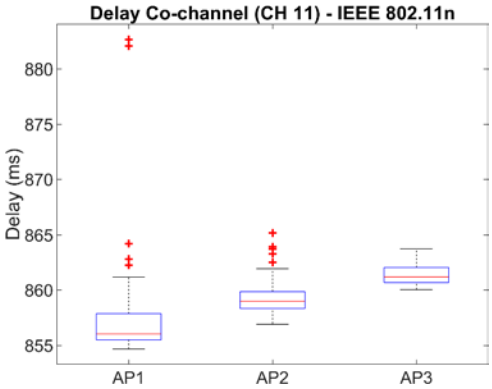


Fig. 34. Delay del canal 11 en uplink con el estándar IEEE 802.11n.

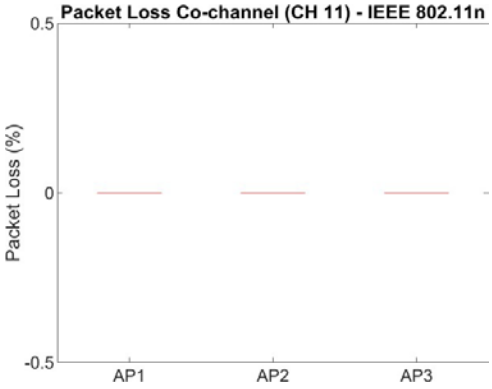


Fig. 35. Packet loss del canal 11 en uplink con el estándar IEEE 802.11n.

9) Análisis entre IEEE 802.11g y IEEE 802.11n

- Throughput: La diferencia es clara ya que el estándar 802.11n tiene un rendimiento significativamente mayor que el 802.11g por lo que sí es coherente con lo que se espera, ya que el estándar n fue diseñado para ofrecer mayores velocidades gracias al uso de MIMO y mejoras en la eficiencia del espectro.
- Delay: Se observa una disminución notable en el retardo cuando se usa 802.11n, que quiere decir que los paquetes viajan más rápido en esa red, lo cual es bueno para aplicaciones sensibles al tiempo como videollamadas o juegos en línea.
- Jitter: Aunque ambos estándares muestran cierta variabilidad, el jitter en 802.11n es menor, lo que implica una transmisión más constante de los paquetes y significa que la experiencia del usuario será más fluida.

Pérdida de Paquetes: Aquí también se ve que con 802.11n hay menos paquetes perdidos, pues esto tiene mucho sentido porque al mejorar la eficiencia y reducir el retardo y el jitter, también se reduce la probabilidad de que los paquetes sean descartados.

V. Discusión

Los experimentos realizados permitieron evaluar el comportamiento de las redes inalámbricas bajo diferentes configuraciones de inyección de tráfico, considerando el uplink en los estándares IEEE 802.11g e IEEE 802.11n. Durante la ejecución de las pruebas, se analizaron distintos puntos de acceso (AP) y estaciones, distribuyéndolos en tres canales de operación (CH1, CH6 y CH11) para mitigar interferencias y evaluar el rendimiento en cada caso.

Los resultados mostraron que el estándar IEEE 802.11n presentó un mejor desempeño en comparación con el IEEE 802.11g, especialmente en términos de velocidad y estabilidad de la conexión. Esto era de esperarse, dado que el estándar n ofrece mejoras en la eficiencia del espectro y el uso de múltiples antenas (MIMO).Sin embargo, se observó que ciertos dispositivos no permitían cambiar libremente entre los modos g y n, lo que limitó la flexibilidad del experimento en algunos casos.

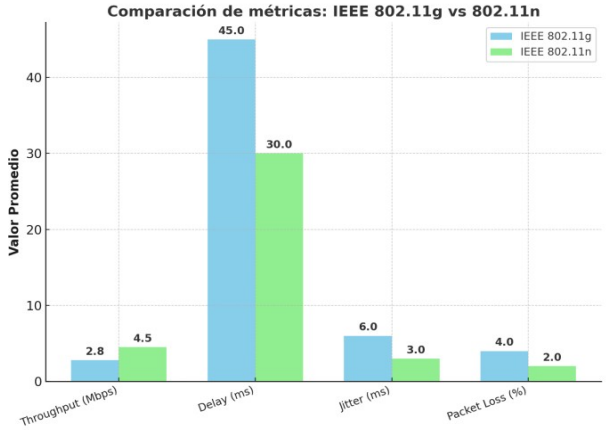


Fig. 36. Comparación entre IEEE 802.11g y IEEE 802.11n.

La Fig. 36 muestra un resumen comparativo entre los estándares IEEE 802.11g y IEEE 802.11n en función de las métricas promediadas durante las pruebas. Se aprecia que 802.11n presenta un throughput más alto (4.5 Mbps frente a 2.8 Mbps en 802.11g), además de un delay y un jitter menores, lo que confirma que este estándar aprovecha mejor el espectro gracias al uso de MIMO y a las mejoras de capa física. En cuanto a la pérdida de paquetes, ambos mantienen valores similares, alrededor del 2 %, coherentes con la metodología de limitar la tasa de transmisión para evitar sobrecarga en el canal.

Estos resultados también concuerdan con lo observado en los distintos escenarios de canales. Cuando los AP se distribuyeron en CH1, CH6 y CH11 de manera simultánea, la interferencia se redujo y el rendimiento general mejoró, mientras que al concentrar todos los dispositivos en un mismo canal, el desempeño cayó significativamente, incrementando la latencia y afectando la estabilidad del enlace. En ese sentido, la figura no solo compara los dos estándares, sino que también refleja cómo la correcta planificación de canales puede marcar la diferencia en la experiencia final de los usuarios.

Finalmente, el propósito del gráfico comparativo que se muestra en la Fig. 36 sintetiza que, aunque 802.11n ofrece claras ventajas sobre 802.11g, estas se ven condicionadas por la presencia de interferencia cocanal, reafirmando la importancia de una adecuada planificación de la red.

VI. Conclusiones

El estándar IEEE 802.11n supera al 802.11g en rendimiento general, gracias a sus características avanzadas como MIMO y mayor ancho de banda. Sin embargo, esta mejora se ve afectada notablemente en escenarios con interferencia cocanal, lo que evidencia su mayor susceptibilidad frente a entornos densamente poblados de dispositivos.

La planificación del canal es crítica. Los resultados demuestran que la distribución de los AP en canales no solapados (1, 6 y 11) mejora sustancialmente la calidad del servicio, minimizando el retardo y la pérdida de paquetes. En contraste, el uso de un solo canal para todos los dispositivos degrada severamente el rendimiento.

El throughput normalizado se reduce hasta un 35% en escenarios con ICC, evidenciando la necesidad de una gestión activa del espectro. Esta pérdida es más pronunciada en el estándar 802.11g, lo que indica una menor robustez frente a interferencias comparado con 802.11n.

El jitter se mantuvo dentro de parámetros aceptables (menores a 2 ms) en la mayoría de los escenarios, lo cual es positivo para aplicaciones sensibles a la fluctuación temporal como VoIP. Sin embargo, se identificaron valores atípicos que deben ser considerados en entornos productivos.

La pérdida de paquetes se mantuvo por debajo del 5%, cumpliendo con los requisitos para aplicaciones en tiempo real, gracias al control sobre la tasa de transmisión durante las pruebas. Esto valida la eficacia del uso del software D-ITG y una configuración adecuada de UDP.

El software D-ITG demostró ser una herramienta eficiente para la evaluación de tráfico en redes inalámbricas, permitiendo medir con precisión parámetros críticos como jitter, retardo y pérdida de paquetes; esto valida su utilidad en pruebas de rendimiento para escenarios controlados o entornos de prueba.

La presencia de interferencia cocanal impacta negativamente en los parámetros de calidad de servicio, como el throughput y la pérdida de paquetes, lo que evidencia la necesidad de realizar estudios previos de espectro en entornos reales antes del despliegue de redes inalámbricas.

Referencias

[1] IEEE Standard for Information Technology—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, Amendment 5: Enhancements for Higher Throughput.

[2] D. Crespo Sen, “Mecanismos de Asignación de Canales en Redes IEEE 802.11,” Universidad de Alcalá,2019. [Online]. Available: https://ebuah.uah.es/dspace/bitstream/handle/10017/38651/TFG_Crespo_Sen_2019.pdf

[3] C. Muñoz Morales, "Análisis de Desempeño de un Sistema MIMO-OFDM con Predicción de Canal," Doctoral Dissertation, Universidad Nacional de Colombia, Bogotá DC., 2013.

[4] S. H. Masood, “Comparación del rendimiento de IEEE 802.11g e IEEE 802.11n en presencia de interferencia de redes 802.15.4,” arXiv preprint arXiv:1308.0678, 2013. [Online]. Available: https://arxiv.org/abs/1308.0678.

[5] R. A. Lara Cueva, C. B. Fernández Jimenez, and C. A. Morales Maldonado, "Análisis del desempeño en un enlace descendente de redes basadas en los estándares IEEE 802.11b, IEEE 802.11n y WDS," Reci, vol. 5, no. 10, 2016.

[6] S. H. Masood, “Comparación del rendimiento de IEEE 802.11g e IEEE 802.11n en presencia de interferencia de redes 802.15.4,” arXiv preprint arXiv:1308.0678, 2013. [Online]. Available: https://arxiv.org/abs/1308.0678

[7] S. M. Kala, M. P. K. Reddy, R. Musham, B. R. Tamma, “Radio Co-location Aware Channel Assignments for Interference Mitigation in Wireless Mesh Networks,” arXiv preprint arXiv:1503.04533, 2015. [Online]. Available: https://arxiv.org/abs/1503.04533

[8] J. L. Muñoz, “Análisis del rendimiento en redes WLAN: caso de estudio,” Universidad Católica de Colombia,2014. [Online]. Available: https://repository.ucatolica.edu.co/bitstream/10983/1300/3/Articulo_trabajo%20de%20grado.pdf

[9] L. F. Pedraza, “Consideraciones para la implementación de voz sobre WLAN,” Universidad Industrial de Santander, 2006. [Online]. Available: https://noesis.uis.edu.co/bitstreams/33e56af9-f5b4- 44d7-8572-ffc4339b29b8/download

DEPARTAMENTO DE ELÉCTRICA, ELECTRÓNICA Y TELECOMUNICACIONES

Universidad de las Fuerzas Armadas – ESPE

El Departamento de Eléctrica, Electrónica y Telecomunicaciones (antigua Facultad de Ingeniería Electrónica) fue creado el 25 de abril de 1977 e inició sus labores en octubre del mismo año en la modalidad presencial, con sus planes y programas de estudio encaminados a la formación del Ingeniero Electrónico. A partir de octubre de 1990, ofrece dos carreras con perfiles profesionales definidos: Ingeniería Electrónica en Telecomunicaciones e Ingeniería Electrónica en Computación.

En la propuesta actual del Departamento se integran en un solo perfil estas aspiraciones, ofreciendo las carreras de Ingeniería en Telecomunicaciones e Ingeniería en Electrónica y Automatización.

Además oferta los siguientes programas de posgrado: **Maestría de Investigación en Electrónica menciones en Automática y Telecomunicaciones**, Maestría en Redes de Información y Conectividad, y Maestría en Gerencia de Redes y Telecomunicaciones.

The Department of Electrical, Electronics, and Telecommunications (formerly the Faculty of Electronic Engineering) was created on April 25, 1977, and began its work in October of the same year in the face-to-face modality, with its study plans and programs aimed at the training of the Electronic Engineer. Since October 1990, it has offered two careers with defined professional profiles: Electronic Engineering in Telecommunications and Electronic Engineering in Computing.

The Department's current proposal integrates these aspirations into a single profile, offering the careers of Telecommunications Engineering, and Electronics and Automation Engineering.

It also offers the following graduate programs: **Research Master's in Electronics with mentions in Automation and Telecommunications**, Master's in Information Networks and Connectivity, and Master's in Network and Telecommunications Management.

Mayor información en `http://deee.espe.edu.ec/`
Further information `http://deee.espe.edu.ec/`

Departamento de Eléctrica, Electrónica y Telecomunicaciones
Universidad de las Fuerzas Armadas ESPE