

Evaluación de la seguridad del tráfico MQTT con cifrado y sin él en un entorno simulado 5G-IoT

Evaluation of MQTT Traffic Security with and without Encryption in a Simulated 5G-IoT Environment

ARMANDO LUIS CORREA MURCIA¹ - YENNIFER DAYANNA GÓMEZ RODRÍGUEZ² -
MARÍA FERNANDA MONTERO³

1. Estudiante de Maestría en Ingeniería Electrónica. Universidad Escuela Colombiana de Ingeniería Julio Garavito.

2. Estudiante de Maestría en Ingeniería Electrónica. Universidad Escuela Colombiana de Ingeniería Julio Garavito.

3. Magíster en Ingeniería Electrónica. Universidad Escuela Colombiana de Ingeniería Julio Garavito. ORCID: <https://orcid.org/0000-0003-4571-8094>

armando.correa@mail.escuelaing.edu.co - yennifer.gomez-r@mail.escuelaing.edu.co -
maria.montero-m@escuelaing.edu.co

Recibido: 06/06/2025 Aceptado: 22/08/2025

Disponible en http://www.escuelaing.edu.co/es/publicaciones_revista
<http://revistas.escuelaing.edu.co/index.php/reci>

Resumen

En este artículo se analizan vulnerabilidades en un entorno de simulación 5G para evaluar la seguridad en la comunicación de dispositivos IoT (internet de las cosas) mediante el protocolo MQTT (Message Queuing Telemetry Transport). Se diseñó un laboratorio con mensajes legítimos de un IoT y ataques simulados, empleando tráfico sin cifrado y protegido con AES-CFB (Estándar de Cifrado Avanzado en Modo de Retroalimentación de Cifrado). El analizador clasificó mensajes, verificó respuestas del broker y evaluó medidas de seguridad. Los resultados evidencian que el cifrado protege parcialmente, pero no evita ataques sin autenticación robusta, destacando la necesidad de mecanismos como autenticación mutua y firmas digitales.

Los resultados muestran que, aun cuando el cifrado aporta confidencialidad, no evita ataques sin autenticación robusta. En el escenario cifrado, el 66,20 % del tráfico correspondió a ataques, frente al 48,80 % en el escenario sin cifrado, lo que revela que el cifrado no reduce la proporción de tráfico malicioso y, de hecho, incrementó en 17,4 % la aceptación de mensajes de ataque respecto al escenario sin cifrado. Adicionalmente, la tasa de envío disminuyó de 19,02 msg/s sin cifrado a 13,98 msg/s con cifrado, lo que evidencia un impacto del proceso criptográfico en el rendimiento.

En conclusión, la protección efectiva de IoT en 5G requiere combinar cifrado con autenticación mutua, firmas digitales y mecanismos avanzados de integridad. Los resultados ofrecen una base replicable para entornos de enseñanza en ciberseguridad IoT.

Palabras claves: 5G, IoT, security, MQTT, encryption, vulnerabilities, attacks.

Abstract

This article analyzes vulnerabilities in a 5G simulation environment to assess the security of IoT device communication through the MQTT (Message Queuing Telemetry Transport) protocol. A laboratory scenario was designed with legitimate IoT messages and simulated attacks, using both unencrypted traffic and traffic protected with AES-CFB (Advanced Encryption Standard in Cipher Feedback mode). The analyzer classified messages, verified broker responses, and evaluated security measures. Results show that encryption partially protects but does not prevent attacks without strong authentication, highlighting the need for additional mechanisms such as mutual authentication and digital signatures to ensure comprehensive communication security.

It was also found that although encryption provides confidentiality, it does not prevent attacks in the absence of robust authentication. In the encrypted scenario, 66.20% of the traffic corresponded to attacks, compared to 48.80% in the unencrypted scenario, indicating that encryption does not reduce the proportion of malicious traffic and, in fact, increased the acceptance of attack messages by 17.4% compared to the non-encrypted case. Additionally, the sending rate decreased from 19.02 msg/s without encryption to 13.98 msg/s with encryption, highlighting the impact of the cryptographic process on performance. In conclusion, effective IoT protection in 5G environments requires combining encryption with mutual authentication, digital signatures, and advanced integrity mechanisms. The results provide a replicable foundation for educational and training environments focused on IoT cybersecurity.

Keywords: 5G, IoT, security, MQTT, encryption, vulnerabilities, attacks.

INTRODUCCIÓN

El crecimiento acelerado del internet de las cosas (IoT) y su integración con redes de quinta generación (5G) ha permitido el desarrollo de aplicaciones críticas que dependen de la transmisión segura y confiable de datos en tiempo real. Tecnologías como 5G, caracterizadas por su baja latencia y alta capacidad de conexión, facilitan la comunicación masiva entre dispositivos, pero también amplían la superficie de ataque y la exposición a amenazas cibernéticas en ecosistemas IoT (Zreikat et al., 2025). En este escenario altamente conectado, los desafíos de seguridad desempeñan un papel central, en especial cuando los dispositivos intercambian información sensible o realizan tareas de misión crítica.

En este contexto, el problema emerge cuando el tráfico IoT circula en texto plano o con cifrados básicos, lo que facilita ataques de inyección, repetición o suplantación, sobre todo en arquitecturas complejas como las de 5G, donde la densidad de dispositivos dificulta la detección temprana de comportamientos maliciosos (Cárdenas-Quintero et al., 2020). Esta situación demanda evaluar no solo si el cifrado protege la confidencialidad de los datos, sino también su impacto en la seguridad integral del flujo de comunicación y en el rendimiento del sistema.

Desde esta perspectiva, la justificación del presente trabajo radica en que, aunque existen estudios conceptuales sobre seguridad 5G-IoT, son escasos los análisis experimentales que contrastan el comportamiento del protocolo MQTT con cifrado y sin él en escenarios controlados. Evaluar estas condiciones permite comprender en qué medida el cifrado aporta protección real y cuáles vulnerabilidades persisten cuando no se implementan mecanismos complementarios, como autenticación mutua, integridad de mensajes o firmas digitales (Sousa and Reis, 2024).

Este artículo se estructura de la siguiente manera: primero se presenta el marco teórico sobre 5G, IoT, MQTT, cifrado y amenazas; luego se describe la metodología empleada en el entorno de simulación; posteriormente, se analizan los resultados obtenidos, y por último, se discuten los hallazgos y se exponen las conclusiones del estudio.

El objetivo de este trabajo es evaluar el impacto del cifrado en la seguridad del tráfico MQTT sobre redes 5G-IoT mediante un entorno de simulación controlado.

INTRODUCTION

The rapid growth of the Internet of Things (IoT) and its integration with fifth generation (5G) networks has enabled the development of critical applications that depend on secure and reliable real-time data transmission. Technologies such as 5G, characterized by low latency and high connection capacity, facilitate mass communication between devices, but also expand the attack surface and exposure to cyber threats in IoT ecosystems (Zreikat et al., 2025). In this highly connected scenario, security challenges play a central role, especially when devices exchange sensitive information or perform mission-critical tasks.

In this context, the problem arises when IoT traffic circulates in plain text or with basic encryption, facilitating injection, replay, or spoofing attacks, especially in complex architectures such as 5G, where device density makes early detection of malicious behavior difficult (Cárdenas-Quintero et al., 2020). This situation requires evaluating not only whether encryption protects data confidentiality, but also its impact on the overall security of the communication flow and system performance.

From this perspective, the rationale for this work lies in the fact that, although there are conceptual studies on 5G-IoT security, there are few experimental analyses that compare the behavior of the MQTT protocol with and without encryption in controlled scenarios. Evaluating these conditions allows us to understand the extent to which encryption provides real protection and what vulnerabilities persist when complementary mechanisms, such as mutual authentication, message integrity, or digital signatures, are not implemented (Sousa and Reis, 2024).

This article is structured as follows: first, the theoretical framework on 5G, IoT, MQTT, encryption, and threats is presented; then, the methodology used in the simulation environment is described; next, the results obtained are analyzed; and finally, the findings are discussed and the conclusions of the study are presented.

The objective of this work is to evaluate the impact of encryption on the security of MQTT traffic over 5G-IoT networks using a controlled simulation environment.

MARCO TEÓRICO

Tecnología 5G e internet de las cosas (IoT)

En los últimos años, el IoT ha revolucionado la comunicación al permitir que objetos cotidianos como sensores, electrodomésticos o vehículos se conecten a internet, posibilitando la recopilación y el intercambio de datos en tiempo real para optimizar procesos en sectores como salud, industria, agricultura y ciudades inteligentes (Mouapi y Hakem, 2017). La expansión del IoT exige mayor conectividad, donde 5G surge como solución clave por su alta velocidad, baja latencia y capacidad masiva, permitiendo aplicaciones críticas como vehículos autónomos, monitoreo remoto de pacientes y automatización industrial avanzada (Siles y Salas, 2020). Sin embargo, la integración 5G-IoT plantea desafíos de seguridad, con riesgos como ataques DDoS o FDIA que afectan redes ciberfísicas. Para su detección, se emplean herramientas de análisis, entre las que se destaca Wireshark como analizador de protocolos de código abierto (Zreikat et al., 2025; Tech et al., 2024; Sikos, 2020). La creciente interconexión incrementa vulnerabilidades, por lo que se requieren cifrado avanzado y autenticación robusta para proteger la información (Sousa y Reis, 2024; Hameed et al., 2019).

Protocolo MQTT

El Message Queuing Telemetry Transport (MQTT) es el protocolo estándar de comunicación en IoT debido a su ligereza. En este estudio se analiza su seguridad, considerando que su utilización en texto plano facilita la interceptación de información, acción que compromete la confidencialidad e integridad de los datos en tiempo real. MQTT opera con un modelo publicador-suscriptor, en el que los dispositivos envían mensajes a un servidor intermediario denominado *broker*, encargado de distribuirlos según los temas (*topics*) suscritos por los clientes (Hunkeler et al., 2008; Banks y Gupta, 2019).

Su eficiencia se debe a que se diseñó para redes con ancho de banda limitado, alta latencia y dispositivos con bajos recursos energéticos, motivo por el cual se emplea ampliamente en sistemas IoT industriales, agrícolas y de salud (Gupta y Shukla, 2021).

Cifrado y seguridad en la red

El cifrado permite asegurar la confidencialidad de los datos en tránsito en redes 5G-IoT.

- **Advanced Encryption Standard (AES).** Es un método simétrico valorado por su eficiencia, adoptado como estándar por el NIST debido a su seguridad y eficiencia. Su implementación en entornos 5G-IoT es clave para prevenir la interceptación y manipulación de la información (Cárdenas-Quintero et al., 2020).
- **Elliptic Curve Cryptography (ECC).** Es un algoritmo asimétrico basado en propiedades matemáticas de curvas elípticas, que además de generar claves públicas y privadas ofrece alta seguridad con claves más cortas que RSA (Rivest, Shamir y Adleman). Su eficiencia en procesamiento y bajo consumo energético lo convierten en una alternativa idónea para dispositivos IoT con recursos limitados, siendo esencial en entornos 5G-IoT (Cárdenas-Quintero et al., 2020).
- **Authentication and Key Agreement (5G-AK).** Se diseñó específicamente para redes 5G, con el fin de mejorar la seguridad frente a ataques como la suplantación e interceptación de datos. Este protocolo permite autenticación mutua y establecimiento de claves seguras en comunicaciones críticas (Cárdenas-Quintero et al., 2020). Según el 3rd Generation Partnership Project (3GPP, 2022), 5G-AKA emplea claves simétricas compartidas entre la SIM (*Subscriber Identity Module*) y el servidor AUSF (*Authentication Server Function*), reforzando la protección del sistema.

Detección de amenazas

En entornos IoT y 5G, la detección de amenazas se vuelve crucial para garantizar la confiabilidad del sistema. Herramientas como Wireshark permiten capturar y examinar paquetes de red para analizar cabeceras, protocolos y flujos de comunicación, detectando anomalías en tiempo real; este tipo de análisis se usa ampliamente en investigaciones académicas y en soluciones de seguridad aplicadas a redes IoT (Parra Camargo, 2023). Para la protección de estas redes se emplean herramientas de análisis de tráfico, como Wireshark, que permiten inspeccionar protocolos y detectar anomalías. Así mismo, la inteligencia artificial y el aprendizaje automático cum-

plen un papel creciente en la identificación de patrones sospechosos y la mitigación de ataques DDoS. Estas tecnologías permiten analizar el comportamiento del tráfico en tiempo real, detectar desviaciones respecto a patrones normales y fortalecer los sistemas de seguridad en entornos IoT y 5G, donde la densidad de dispositivos incrementa la superficie de ataque (Banaamah y Ahmad, 2022; Dahou et al., 2022).

Vulnerabilidades en redes 5G aplicadas al IoT

De acuerdo con Cárdenas-Quintero et al. (2020), IoT presenta vulnerabilidades en autenticación, cifrado y control de acceso, que se amplifican en entornos 5G; además, la falta de protocolos robustos y la diversidad de dispositivos facilitan la interceptación de información, comprometiendo confidencialidad e integridad de datos en tiempo real.

El desarrollo de la tecnología 5G ha transformado la conectividad del IoT al permitir comunicaciones más rápidas, eficientes y escalables entre dispositivos; sin embargo, esta evolución introduce desafíos significativos en materia de ciberseguridad, especialmente relacionados con vulnerabilidades de red, ataques dirigidos y una superficie de ataque ampliada debido a arquitecturas descentralizadas basadas en NFV y SDN (Wala y Kiran, 2024).

Moudoud et al. (2022) identifican amenazas como la falsificación de datos en inyección (FDIA) y los ataques DDoS, mientras que Melzer et al. (2024) evidencian su impacto directo en entornos 5G-IoT, destacando riesgos en señalización, control y comunicación masiva entre dispositivos.

Ataques de denegación de servicio distribuidos (DDoS)

Los entornos 5G-IoT son especialmente vulnerables a ataques DDoS debido a la limitada capacidad de procesamiento y seguridad de muchos dispositivos IoT, que carecen de autenticación sólida y protocolos robustos, lo cual facilita que los atacantes los comprometan y generen tráfico malicioso.

Cárdenas-Quintero et al. (2020) señalan que los DDoS afectan la disponibilidad y se pueden usar como distracción para exfiltración de datos o manipulación de configuraciones. La arquitectura descentralizada y los numerosos nodos dificultan la detección temprana.

En este contexto, se proponen soluciones basadas en inteligencia artificial y *machine learning* para mitigar el impacto de los ataques.

Prevención de ataques en el entorno 5G-IoT

La prevención de ataques en 5G-IoT exige tecnologías emergentes y medidas sólidas. La inteligencia artificial (IA) y el aprendizaje automático son claves en la detección de amenazas, puesto que con la IA, por ejemplo, se pueden analizar datos masivos en tiempo real, identificando patrones sospechosos y respondiendo proactivamente (Reis, 2025). El aprendizaje automático ayuda a entrenar modelos para reconocer anomalías en el tráfico y activar defensas. Según Cárdenas-Quintero et al. (2020), su integración en 5G-IoT es esencial contra ataques DDoS e interceptación de datos.

Desafíos y futuras tendencias de 5G-IoT

La expansión de dispositivos IoT en redes 5G incrementa riesgos como interceptación de datos y DDoS (Cárdenas-Quintero et al., 2020). Tecnologías como *blockchain* y cifrado avanzado resultan esenciales. Aun cuando 5G ofrece baja latencia, su gestión sigue siendo un reto; Network Slicing permite emplear subredes para aplicaciones críticas (Campolo et al., 2018).

ESTADO DEL ARTE

Cifrado y autenticación

Como respuesta a estas vulnerabilidades, el cifrado y la autenticación se convierten en pilares fundamentales para la protección de datos y la validación segura de dispositivos. Abie y Pirbhulal (2024) proponen un marco de seguridad adaptativo basado en inteligencia artificial para la detección en tiempo real de amenazas, mientras que Basurto y Guña (2023) resaltan la autenticación multifactor (MFA) como uno de los mecanismos más efectivos para fortalecer la seguridad en dispositivos IoT con recursos limitados. Estas estrategias buscan mitigar accesos no autorizados y reducir la exposición ante ataques avanzados.

Estrategias de prevención basadas en IA y blockchain

Además de los mecanismos tradicionales, en la bibliografía reciente se destacan enfoques emergentes como *blockchain*, segmentación de red y aprendizaje automático. Ciotirnae (2024) subraya la capacidad de *blockchain* para asegurar integridad, trazabilidad y resistencia a manipulación en redes distribuidas, en tanto que Melzer et al. (2024) sugieren la inclusión de entrenamientos tipo “Capture the Flag” (CTF) como una práctica efectiva para preparar sistemas y equipos frente a ataques sofisticados. Estas estrategias complementan los modelos de cifrado y autenticación al ofrecer capas adicionales de protección que se adaptan a la naturaleza distribuida e intensiva del ecosistema 5G-IoT.

En la mayoría de los estudios se analiza la seguridad de 5G-IoT en materia conceptual, pero pocos evalúan experimentalmente el efecto del cifrado sobre protocolos ligeros, como MQTT. Este vacío motiva la propuesta metodológica del presente artículo

METODOLOGÍA

En este artículo se presenta un análisis de seguridad en redes 5G-IoT, centrándose en la parametrización del tráfico de redes 5G en un entorno de simulación controlado. Se desarrolló una metodología estructurada en cuatro fases para garantizar un análisis de las amenazas presentes en estas redes y evaluar estrategias de mitigación.

Revisión bibliográfica

Se hizo una revisión bibliográfica centrada en la seguridad de redes 5G aplicadas a IoT. Se consultaron artículos científicos, informes técnicos y documentos académicos disponibles en bases de datos como IEEE

Xplore, ScienceDirect y Google Scholar. Esta revisión permitió identificar trabajos relevantes sobre las principales amenazas que enfrentan las redes 5G-IoT, así como enfoques recientes para su mitigación mediante técnicas como la inteligencia artificial, el análisis de tráfico y la segmentación de redes.

Parámetros técnicos de entorno 5G

El análisis se basó en un entorno de comunicación 5G simulado, configurado bajo parámetros técnicos fundamentales para esta tecnología, entre estos la latencia ultrabaja (1-10 ms), el ancho de banda promedio entre 100 y 900 Mbps y la capacidad para soportar hasta un millón de dispositivos por km² (3GPP, 2022; Zreikat et al., 2025). Estas características permitieron reproducir condiciones reales de operación para dispositivos IoT, donde la velocidad, la eficiencia espectral y la confiabilidad del canal son determinantes para el desempeño del protocolo MQTT (Cárdenas-Quintero et al., 2020; Hameed et al., 2019).

En este entorno, la comunicación se ejecutó mediante MQTT sobre TCP/IP, evaluando tráfico sin cifrar y tráfico protegido mediante **AES-CFB de 128 bits**, con pruebas complementarias bajo **TLS 1.2** para simular canales seguros en redes 5G (Sikos, 2020). La captura del tráfico, con una duración aproximada de 849 segundos por escenario, permitió identificar tasas de envío entre 13,98 y 19,02 mensajes por segundo, reflejando el impacto de la carga de cifrado en el rendimiento (Moudoud et al., 2021; Reis, 2025a).

A continuación, se presenta el flujo metodológico de la simulación, que comienza con la configuración del entorno Python y finaliza con la captura de tráfico en formato. Pcapng (figura 1).

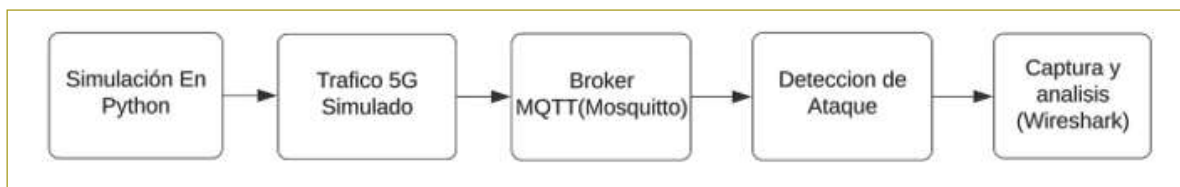


Figura 1. Diagrama de flujo de la ejecución de la simulación hecha en Python

Fuente: Elaboración propia (2025).

Diseño del entorno de simulación 5G-IoT

- Configuración de un escenario de laboratorio que emuló la comunicación de un dispositivo IoT hacia un *broker* MQTT, representando el canal de transmisión sobre una red 5G.
- Definición de tópicos MQTT para mensajes legítimos y generación de tráfico de ataque (por ejemplo, inyección de datos y repetición de mensajes).
- Establecimiento de dos escenarios de comunicación: tráfico sin cifrado (MQTT en claro) y tráfico con cifrado de *payload* (AES-CFB, con clave fija de laboratorio).

Captura y procesamiento del tráfico

- Recolección de paquetes en formato. pcapng usando Wireshark.
- Aplicación de filtros de visualización (*display filters*) para identificar tráfico MQTT.
- Registro de metadatos relevantes: tópico, dirección IP, tamaño de *payload* y presencia de cifrado.

Desarrollo del analizador de tráfico

- Implementación en Python (Anaconda) utilizando librerías como pyshark, paho-mqtt, pandas y matplotlib.
- Clasificación de mensajes en dos categorías: legítimos (IoT) y de ataque (simulados).
- Verificación de éxito en la comunicación mediante la confirmación del *broker* (Puback), lo cual permitió discriminar entre mensajes aceptados y rechazados.
- Incorporación de funciones para validar un descifrado correcto de mensajes en el escenario cifrado.

Análisis de resultados y evaluación de vulnerabilidades

- Generación de estadísticas descriptivas mediante la distribución de mensajes por tópico, proporción de tráfico cifrado/no cifrado, tasa de éxito en la entrega de mensajes y ocurrencia de ataques detectados.
- Representación gráfica de los resultados por medio de diagramas de barras y series temporales.
- Discusión de hallazgos en relación con vulnerabilidades identificadas en entornos 5G-IoT y estrategias de seguridad recomendadas en la bibliografía existente.

Definición del entorno de simulación

La simulación de tráfico 5G-IoT se orientó al análisis de seguridad mediante un entorno local para generar, transmitir y analizar datos en tiempo real. El objetivo fue recrear condiciones de red, identificar ataques, clasificar eventos y evaluar mitigaciones. Se diseñaron dos escenarios: con cifrado y sin él, contrastando vulnerabilidades y medidas de protección. El código simuló una plataforma IoT con *broker* y clientes MQTT, publicando mensajes JSON bajo MQTT v5.2. Se aplicó cifrado/descifrado, detectando excepciones y ataques. Finalmente, los intercambios quedaron registrados en *Análisis N encrip.pcapng* para evaluación posterior.

Captura y análisis del tráfico IoT con cifrado TLS y sin él

Se configuró un cliente para generar tráfico cifrado hacia un servidor TLS, capturando con Wireshark desde el *handshake* TCP hasta TLS, negociando certificados y *cipher suite*. Los datos aparecieron como Application Data, confirmando cifrado. Se usaron certificados digitales, librerías (*requests*, Paho-MQTT) y Wireshark para verificar versión TLS y parámetros. El entorno se desarrolló en macOS por estabilidad y soporte Python, gestionado con Anaconda y Jupyter (Anaconda Software Distribution, 2023). La simulación incluyó Paho-MQTT, Pyshark, Matplotlib, CSV, nest_asyncio, un *broker* Mosquitto y una red 5G simulada para análisis forense.

Entorno simulado: descripción de elementos

A renglón seguido se muestra el diagrama de bloques del análisis de tráfico en el entorno 5G-IoT. El dispositivo IoT legítimo envía mensajes cifrados con AES-CFB al *broker* MQTT, mientras un atacante simulado genera mensajes maliciosos. El analizador, desarrollado en Python con Pyshark, captura paquetes PCAPNG y verifica respuesta del *broker*: mensajes exitosos se clasifican como legítimos, y los fallidos como ataques, reforzando la detección de vulnerabilidades en IoT sobre 5G (figura 2).

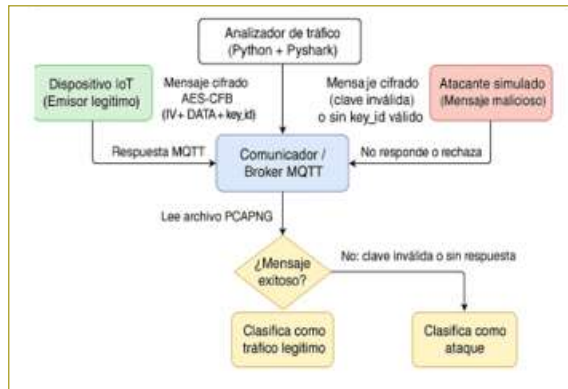


Figura 2. Diagrama en detalle de la simulación con información sobre la comunicación entre los componentes

Fuente: Elaboración propia (2025).

En la figura siguiente se puede apreciar el esquema de captura y análisis de tráfico MQTT con Wireshark. Se aplicó un filtro (mqtt) para aislar paquetes entre dispositivo IoT, *broker* y atacante en 5G. La captura en modo promiscuo registró mensajes legítimos y ataques, base para evaluar vulnerabilidades (figura 3).

Simulación de tráfico

Dispositivo IoT - Nodo IoT emisor. El dispositivo IoT actúa como emisor legítimo en 5G, enviando mensajes cifrados mediante MQTT hacia el *broker*, que gestiona respuestas.

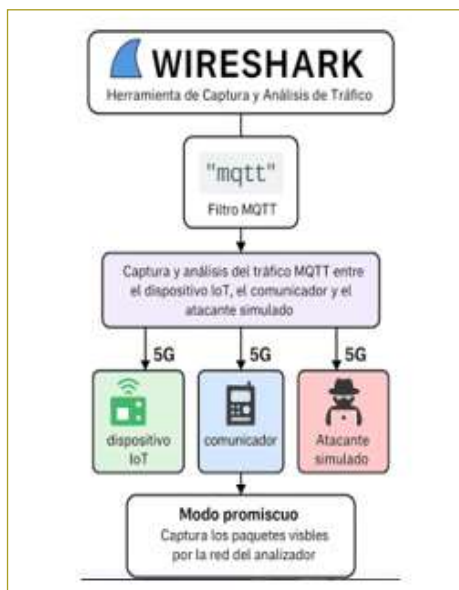
Tabla 1
Elementos y características del entorno simulado para el análisis de tráfico IoT

Elemento	Descripción	Funciones	Protocolo / Características técnicas	Ejemplo / Importancia
1. Dispositivo IoT	Nodo emisor legítimo que genera mensajes MQTT cifrados con AES en modo CFB.	Publica datos hacia el <i>broker</i> MQTT. Usa cifrado simulado para proteger la integridad y confidencialidad del mensaje.	MQTT sobre TCP/IP en una red 5G.	Sensor ambiental o dispositivo <i>wearable</i> inteligente.
2. Comunicador / Broker MQTT (Mosquitto)	Actúa como intermediario de mensajes entre los dispositivos. Verifica la recepción y reenvía los mensajes.	Recibe mensajes del dispositivo IoT. Responde (ACK) para confirmar recepción. Identifica intentos de ataque por tráfico inusual o malformado.	<i>Broker</i> Mosquitto en red local simulada 5G. Compatible con tráfico cifrado (sin descifrarlo directamente).	Asegura la comunicación y controla la integridad del tráfico.
3. Atacante simulado	Nodo que inyecta mensajes MQTT maliciosos o manipulados, cifrados o sin cifrado.	Inyecta mensajes ilegítimos. – Simula comportamiento legítimo para evadir detección. Prueba la capacidad de detección y clasificación de tráfico malicioso.	También usa MQTT, pero puede fallar al recibir respuesta del <i>broker</i> .	Evaluación de la resiliencia del sistema frente a ciberataques.
4. Red 5G simulada	Capa de comunicación que interconecta todos los elementos.	Transmisión de paquetes de baja latencia. Simula la infraestructura de una red móvil de próxima generación (5G Standalone o Non-Standalone).	Emula el entorno de comunicación 5G.	Evalúa el rendimiento en escenarios con IoT masivo.
5. Analizador de tráfico	Sistema implementado en Python que lee archivos .pcapng, descifra el tráfico (si aplica), clasifica los mensajes (legítimos o ataque) y evalúa si hubo respuesta del comunicador.	Interpretación del tráfico MQTT. Validación de éxito de mensajes mediante la respuesta del <i>broker</i> . Exportación de resultados para análisis comparativo.	Implementado en Python con librerías como pyshark , compatible con tráfico cifrado y descifrado (si aplica).	Análisis detallado del comportamiento de la red y eficacia del sistema de detección.

Fuente: Elaboración propia con base en la definición del entorno de simulación compuesto por dispositivo IoT, comunicador/*broker* MQTT, atacante simulado, red 5G simulada y analizador de tráfico.

Figura 3. Diagrama de comunicación y captación del tráfico en el entorno 5G

Fuente: Elaboración propia (2025).



Comunicador central (broker MQTT)

El comunicador, como *broker* MQTT, recibe, procesa y reenvía mensajes, validando autenticidad y éxito, y generando respuestas cuando son válidos.

Nodo atacante (simulación de amenazas IoT en entorno 5G)

Función en el entorno simulado. El atacante simulado representa un dispositivo malicioso que busca comprometer la comunicación en el entorno 5G, enviando mensajes falsos al *broker* MQTT para simular ataques como inyección, suplantación o denegación de servicio.

Mecanismo de cifrado utilizado en el payload (base 64 simulado). El cifrado del *payload* usa una simulación en base 64, lo que permite observar la gestión de transmisiones cifradas en IoT. Aunque no es un cifrado fuerte, facilita comprender la protección de datos en sistemas reales.

Analizador Python para tráfico MQTT cifrado (AES-CFB)

Objetivo. Detectar, clasificar y validar el éxito de mensajes transmitidos en un entorno simulado con dispositivos IoT y ataques maliciosos sobre una red simulada de tipo 5G, utilizando el protocolo MQTT cifrado.

Captura y análisis de tráfico de la simulación

Wireshark en el entorno de simulación de tráfico IoT sobre 5G

Wireshark es una herramienta de análisis de protocolos de red utilizada para capturar, inspeccionar y diagnosticar el tráfico que circula en una red. En este entorno experimental, Wireshark cumple un papel fundamental para:

- Capturar en tiempo real el tráfico generado por los tres actores del sistema: el dispositivo IoT, el comunicador central y el atacante simulado.
- Filtrar exclusivamente el protocolo MQTT, que es el canal principal de comunicación entre los dispositivos.
- Exportar el tráfico capturado en archivos. pcapng para su posterior análisis con herramientas automatizadas en Python.

Durante la simulación, se aplicó el siguiente filtro de visualización en Wireshark:

- Visualizar únicamente los paquetes asociados al protocolo MQTT.
- Excluir todo el tráfico irrelevante (como DNS, ARP, HTTP, etc.).
- Facilitar la identificación de patrones de comunicación entre los dispositivos, incluyendo:
 - Mensajes de publicación (Publish).
 - Mensajes de conexión (Connect).
 - Mensajes de suscripción (Subscribe).
 - Respuestas del *broker* o comunicador (Connack, Puback, Suback, etc.).

RESULTADOS

Después de la captura se elaboró un consolidado en Excel, en el que se organizaron y compararon los resultados del tráfico IoT con dos condiciones: se clasificaron los datos sin cifrado y con cifrado en función de las etiquetas de los mensajes y se representó la proporción relativa de los registros, mostrando por ejemplo el tráfico con cifrado, los intentos de ataque (ataque/dispositivo 1) y la identificación de mensajes válidos (SI).

El entorno de simulación permitió evaluar el comportamiento del protocolo MQTT en una red 5G en dos condiciones: tráfico sin cifrado y tráfico protegido mediante cifrado AES-CFB. La base de datos consoli-

dada registró los mensajes enviados por el dispositivo IoT, así como los ataques simulados inyectados en los mismos tópicos.

Los resultados muestran lo siguiente (tablas 2 y 3).

En general, los resultados demuestran que el cifrado fortalece la protección de los datos transmitidos, pero no constituye un mecanismo suficiente para evitar ataques de suplantación o repetición. Se hace evidente la necesidad de incorporar mecanismos adicionales, como autenticación mutua y validación de integridad de los mensajes, para garantizar la seguridad integral en entornos IoT sobre 5G.

A renglón seguido (figura 4), se presenta la proporción de mensajes clasificados como legítimos (**NO**) y como ataques (**SI**) en los escenarios de tráfico MQTT con cifrado y sin cifrado dentro del entorno de simulación 5G-IoT. En el caso del tráfico cifrado, los mensajes de ataque alcanzaron un 28,05 %, en tanto que los

mensajes legítimos representaron un 14,32 %. Por otra parte, en el tráfico sin cifrado los mensajes de ataque representaron un 28,13 % y los legítimos alcanzaron un 29,51 %, resultados que indican que si bien el cifrado contribuye a la protección de la información transmitida, no elimina la posibilidad de que se generen mensajes maliciosos, lo que evidencia la necesidad de mecanismos adicionales de autenticación y verificación de integridad para reforzar la seguridad en redes 5G-IoT.

A continuación, se presenta la distribución de mensajes clasificados como ataques y legítimos en el escenario de tráfico MQTT con cifrado dentro del entorno de simulación 5G-IoT. Los resultados muestran que el 66,20 % de los mensajes correspondieron a intentos de ataque (ataque/dispositivo 1), mientras que el 33,80 % se identificaron como mensajes legítimos enviados por el dispositivo IoT (iot/dispositivo 1). Esta alta proporción de tráfico malicioso evidencia que, aun

Tabla 2
Datos estadísticos descriptivos del tráfico con cifrado y sin él

Tipo de tráfico	Número de mensajes	Inicio	Fin	Duración (segundos)	Tasa de envío (msg/seg)
Tráfico con Cifrado	11868	2025-07-20 19:02:51.005	2025-07-20 19:16:59.954	848.949	13,98
Tráfico sin Cifrado	16146	2025-07-20 10:22:43.000	2025-07-20 10:36:52.000	849.000	19,02

Fuente: Elaboración propia, con base en los datos obtenidos del análisis del archivo pcapng generado por Wireshark y analizado en Python por analizador utilizado en la simulación.

Tabla 3
Resultados del análisis de tráfico IoT en escenarios cifrados y no cifrados

Resultado	
Distribución de mensajes por tópico	- Mensajes legítimos en tráfico cifrado: 33,80 % - Mensajes de ataque en tráfico cifrado: 66,20 % - Mensajes legítimos en tráfico sin cifrado: 51,20 % - Mensajes de ataque en tráfico sin cifrado: 48,80 %
Tráfico cifrado vs. no cifrado	- Tráfico sin cifrado: $\approx$ 50 % - Tráfico con cifrado AES-CFB: $\approx$ 50 %
Éxito en la comunicación	- Mensajes legítimos con Puback (éxito): Alto porcentaje en ambos escenarios (coherente con 33,80 % vs. 51,20 % legítimos). - Mensajes de ataque con Puback (éxito bajo): En cifrado, muchos ataques fueron aceptados (66,20 %), más que en no cifrado (48,80 %).
Detección de ataques	- Ataques detectados (clasificación del analizador): - Cifrado: 66,20 % - No cifrado: 48,80 % - Tipos detectados: inyección y replay
Visualización de resultados	- En tráfico cifrado (figura 4): 28,05 % ataques, 14,32 % legítimos - En tráfico no cifrado (figura 4): 28,13 % ataques, 29,51 % legítimos

Fuente: Elaboración propia, con base en los resultados del experimento de análisis de tráfico IoT.

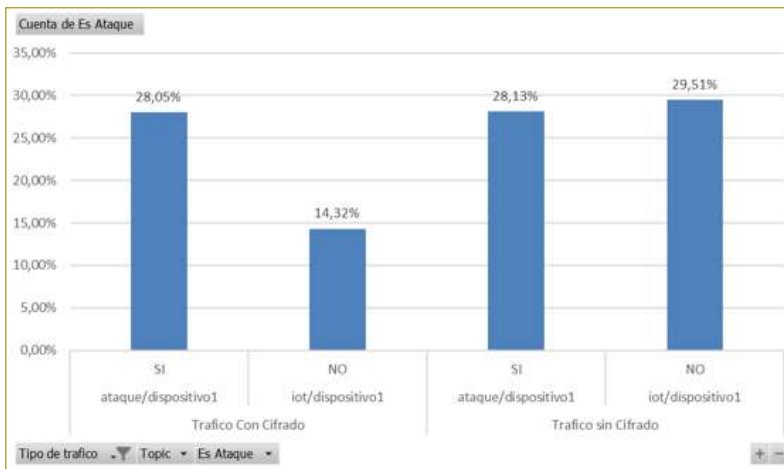


Figura 4. Distribución porcentual de mensajes legítimos y de ataque en escenarios con cifrado y sin él
Fuente: Elaboración propia (2025).

cuando el cifrado protege la confidencialidad de los datos transmitidos, no impide que un atacante intente inyectar mensajes en la red, lo que resalta la necesidad de complementar el cifrado con mecanismos robustos de autenticación y control de acceso.

En la figura que aparece a continuación (figura 6) se puede ver la distribución de mensajes clasificados como ataques y legítimos en el escenario de tráfico MQTT sin cifrado dentro del entorno de simulación 5G-IoT. Los resultados evidencian que el 48,80 % de los mensajes correspondieron a intentos de ataque (ataque/dispositivo 1), mientras que el 51,20 % de estos se identificaron como mensajes legítimos enviados por el dispositivo IoT (iot/dispositivo 1).

A diferencia del escenario con cifrado, en este caso la proporción de mensajes legítimos supera levemente a los mensajes de ataque, lo que sugiere que, aun cuando el tráfico no está protegido, los mensajes legítimos mantienen una mayor participación. Sin embargo, la exposición en texto plano aumenta la vulnerabilidad del sistema frente a la interceptación y manipulación de la información transmitida.

DISCUSIÓN

La comparación entre los dos escenarios evaluados (tráfico MQTT con cifrado y sin él) demuestra que el cifrado aporta un nivel básico de protección al ocultar el



Figura 5. Proporción de mensajes legítimos y de ataque en el escenario con tráfico cifrado
Fuente: Elaboración propia (2025).

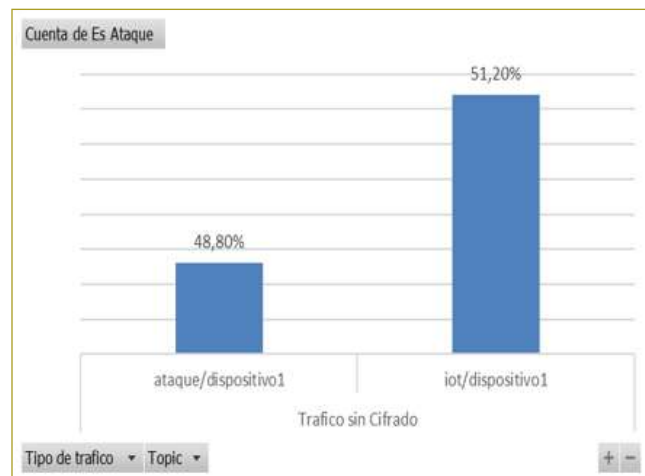


Figura 6. Proporción de mensajes legítimos y de ataque en el escenario con tráfico sin cifrado
Fuente: Elaboración propia (2025).

contenido del mensaje, pero no garantiza por sí mismo la seguridad integral en entornos 5G-IoT. Aunque el uso de AES-CFB impide la lectura directa del *payload*, los resultados evidenciaron que los ataques de repetición (*replay*) e inyección de mensajes se mantuvieron funcionales, incluso bajo tráfico cifrado, debido a la ausencia de mecanismos de autenticación y verificación de integridad. Este comportamiento coincide con lo reportado por Cárdenas-Quintero et al. (2020), quienes destacan que las vulnerabilidades en autenticación continúan siendo el principal vector de riesgo en IoT, incluso cuando se emplea cifrado.

Un hallazgo relevante es que el escenario cifrado presentó una mayor proporción de mensajes maliciosos exitosos. Esto se explica por dos factores:

- La estructura del protocolo MQTT no cambia por aplicar cifrado al *payload*, por lo que un atacante puede generar mensajes con encabezados válidos y tópicos correctos, sin necesidad de acceder al contenido.
- El uso de una clave AES fija y sin rotación en el entorno simulado facilita que un atacante que conozca el patrón del tráfico pueda replicar mensajes aparentemente legítimos, lo que incrementa la tasa de aceptación por parte del *broker*.

Estos resultados están alineados con lo planteado por Moudoud et al. (2022), quienes demuestran que ataques FDIA y de suplantación se pueden mantener efectivos incluso en entornos cifrados, cuando no existe verificación de origen ni mecanismos de integridad.

Por otra parte, la verificación mediante Puback se consolidó como un indicador clave para diferenciar tráfico legítimo de ilegítimo; sin embargo, tal validación se limita a confirmar la entrega del mensaje y no evalúa su autenticidad, lo que explica por qué algunos mensajes maliciosos también recibieron respuesta positiva del *broker*. Esto corrobora lo planteado por Reis (2025b) sobre la necesidad de complementar el cifrado con autenticación mutua y monitoreo avanzado para una detección más precisa.

Finalmente, es importante reconocer las limitaciones del entorno simulado. El uso de una clave estática, la ausencia de TLS real, la no implementación de 5G-AKA y la capacidad reducida de un entorno local simplifican la dinámica de ataque. En un entorno real, factores como

rotación de claves, certificados digitales, variabilidad de latencia y segmentación de red (*network slicing*) podrían modificar el comportamiento observado. No obstante, el experimento ofrece un marco reproducible que permite aislar variables críticas del protocolo MQTT y evaluar su comportamiento frente a ataques comunes en redes IoT.

En conjunto, los resultados refuerzan que la seguridad en 5G-IoT se debe abordar mediante un enfoque multicapa, en el que el cifrado del *payload* constituye apenas uno de los componentes necesarios. La combinación de autenticación fuerte, integridad del mensaje, control de acceso y detección temprana de anomalías es fundamental para mitigar ataques de suplantación, inyección y repetición en entornos complejos y distribuidos.

Los resultados confirman que la seguridad del IoT no depende del cifrado individual, sino de arquitecturas multicapa que integren autenticación y monitoreo inteligente.

CONCLUSIONES

En el estudio se demostró que la integración de dispositivos IoT sobre redes 5G presenta vulnerabilidades significativas cuando se emplean protocolos ligeros como MQTT, sin mecanismos adicionales de autenticación e integridad. Aun cuando el cifrado AES-CFB aplicado al *payload* aporta confidencialidad básica, los resultados confirman que este control no es suficiente para mitigar ataques de inyección, repetición o suplantación, en particular cuando un atacante puede replicar encabezados y tópicos válidos sin necesidad de acceder al contenido del mensaje.

La verificación mediante Puback se consolidó como un elemento clave para determinar la entrega exitosa de los mensajes y diferenciar parcialmente tráfico legítimo de tráfico malicioso. No obstante, esta validación no garantiza autenticidad ni integridad, lo que permitió que el *broker* aceptara ciertos ataques, incluso en el escenario cifrado. Esto resalta la necesidad de adoptar mecanismos más robustos en lo referente a la capa de aplicación o transporte, como autenticación mutua con certificados, firmas digitales o empleo de TLS (mqtts://).

El análisis comparativo entre tráfico cifrado y no cifrado evidenció que la tasa de éxito de los mensajes legítimos fue mayor cuando se verificó la respuesta del

broker, mientras que los mensajes maliciosos mantuvieron niveles significativos de aceptación en ambos escenarios. Estos resultados confirman que la seguridad en entornos 5G-IoT no puede depender únicamente del cifrado del *payload* y debe migrar hacia esquemas multi-capas que incluyan controles criptográficos, validación estricta del origen del mensaje y políticas avanzadas de control de acceso.

Desde el punto de vista metodológico, el uso conjunto de Wireshark y un analizador Python permitió identificar patrones de tráfico, detectar anomalías y registrar evidencia cuantitativa del comportamiento del protocolo MQTT en un entorno 5G simulado. Esta aproximación constituye un marco reproducible para auditorías, pruebas de laboratorio y análisis forense de tráfico IoT.

Finalmente, se identifican como líneas futuras de trabajo la integración de autenticación fuerte basada en certificados, la implementación de TLS nativo para MQTT, el empleo de rotación de claves y mecanismos de integridad como HMAC, así como la incorporación de modelos de detección de anomalías basados en inteligencia artificial para mejorar la clasificación de tráfico y anticipar comportamientos maliciosos.

En el futuro, se propone extender la simulación a escenarios de *edge computing* y comunicación TLS completa para evaluar la escalabilidad del entorno.

REFERENCIAS

- 3GPP (2022). *3rd Generation Partnership Project*. <https://portal.3gpp.org/#/>
- Abie, H., y Pirbhulal, S. (2024). *Autonomous Adaptive Security Framework for 5G-Enabled IoT*. <https://arxiv.org/abs/2406.03186v1>
- Atzori, L., Iera, A., y Morabito, G. (2010). The Internet of Things A Survey. *Computer Networks*, 54, 2787-2805. - References - Scientific Research Publishing.
- Basurto, M. O., y Gúaña, J. (2023, September). *Ciberseguridad en las redes 5G: desafíos y soluciones*. <https://portal.amelica.org/ameli/journal/572/5724522008/html/>
- Campolo, C., Fontes, R. D. R., Molinaro, A., Rothenberg, C. E., y Iera, A. (2018). Slicing on the Road: Enabling the Automotive Vertical through 5G Network Softwarization. *Sensors*, 18(12), 4435. <https://doi.org/10.3390/S18124435>
- Cárdenas-Quintero, D., Ropero-Silva, E., Puerto-López, K., Sánchez-Mojica, K., Castro-Casadiegos, S., y Ramírez-Mateus, J. (2020). Vulnerabilidad en la seguridad del internet de las cosas. *Mundo FESC*, 10(19), 161-178. <https://doi.org/10.61799/2216-0388.542>
- Ciotirnae, P. (2024). 5G Mobile Network with Blockchain, IoT and Drones Integration for Military Applications. *2024 IEEE International Workshop on Technologies for Defense and Security, TechDefense 2024 - Proceedings*, 104-109. <https://doi.org/10.1109/TECHDEFENSE63521.2024.10863401>
- Hameed, S., Khan, F. I., y Hameed, B. (2019). Understanding Security Requirements and Challenges in Internet of Things (IoT): A Review. *Journal of Computer Networks and Communications*, 2019(1), 9629381. <https://doi.org/10.1155/2019/9629381>
- Melzer, J., Shafo, A., Zhao, Z., Wang, P. P., Fenwick, W., y Almutadi, W. (2024). Developing "Capture the Flag" for 5G IoT Cyber Security Training. *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*, 816-821. <https://doi.org/10.1109/WF-IOT62078.2024.10811259>
- Mouapi, A., y Hakem, N. (2017, June). Enslavement of Wireless Sensor Network to an RF Energy Harvesting System. *Open Journal of Antennas and Propagation*, 5(2), <https://www.scirp.org/reference/referencespapers?referenceid=2064753>
- Moudoud, H., Khoukhi, L., y Cherkaoui, S. (2022). Prediction and Detection of FDIA and DDoS Attacks in 5G Enabled IoT. *IEEE Network*, 35(2), 194-201. <https://doi.org/10.1109/MNET.011.2000449>
- Reis, M. J. C. S. (2025). AI-Driven Anomaly Detection for Securing IoT Devices in 5G-Enabled Smart Cities. *Electronics* 2025, Vol. 14, Page 2492, 14(12), 2492. <https://doi.org/10.3390/ELECTRONICS14122492>
- Sikos, L. F. (2020). Packet analysis for network forensics: A comprehensive survey. *Forensic Science International: Digital Investigation*, 32, 200892. <https://doi.org/10.1016/J.FSIDI.2019.200892>
- Siles R, y Salas M. (2020). *DISPOSITIVOS Y COMUNICACIONES MÓVILES*.
- Sousa, A., y Reis, M. J. C. S. (2024). 5G Security Features, Vulnerabilities, Threats, and Data Protection in IoT and Mobile Devices: A Systematic Review. In *ESIC2024* (Vol. 8).
- Tech, M., Alawe, R., y Soni, S. (2024). A Literature Survey of Distributed Denial of Service Attack Detection using Machine Learning: A Review. In *International Journal of Scientific Research y Engineering Trends* (Vol. 10, Issue 1).
- Wala, F. B., y Kiran, M. (2024). *5G Network Security Practices: An Overview and Survey*. <https://arxiv.org/abs/2401.14350v1>
- Zreikat, A. I., AlArnaout, Z., Abadleh, A., Elbasi, E., y Mostafa, N. (2025). The Integration of the Internet of Things (IoT) Applications into 5G Networks: A Review and Analysis. *Computers* 2025, Vol. 14, Page 250, 14(7), 250. <https://doi.org/10.3390/COMPUTERS14070250>