UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Dpto. de Informática de Sistemas y Computadores

Análisis Comparativo entre MQTT y NDN para Comunicación en Redes IoT

Trabajo Fin de Máster

Máster Universitario en Ingeniería de Computadores y Redes

AUTOR/A: Becerra Zavala, David Fernando

Tutor/a: Manzoni, Pietro

CURSO ACADÉMICO: 2023/2024

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

DISCA
DEPARTAMENTO DE INFORMÁTICA DE SISTEMAS Y COMPUTADORES

Máster en Ingeniería de Computadores y Redes

Trabajo Fin de Máster

Análisis comparativo entre MQTT y NDN para comunicación en redes IoT.

Autor: *David Fernando Becerra Zavala*

Director: *Pietro Manzoni*

Septiembre, 2024

ÍNDICE

AGRADECIMIENTOS

Quiero expresar mi más sincero agradecimiento a todos aquellos que han hecho posible la realización de este trabajo de fin de máster. En primer lugar, agradezco profundamente a mis abuelas (María Antonieta de Caso y Ana María Zamorano), cuyos valores y enseñanzas han sido una guía constante en mi vida.

A mis padres (Ileana Zavala y Francisco Becerra), les debo un especial reconocimiento por su apoyo incondicional y por haberme brindado siempre las herramientas necesarias para alcanzar mis metas. Sin su sacrificio y confianza en mis capacidades, este logro no habría sido posible.

A mi hermana (Paulina Becerra), agradezco su constante motivación y por ser una fuente de inspiración y apoyo en los momentos más difíciles. Su compañía y ánimo han sido invaluables durante este proceso.

Quiero también extender mi gratitud a mis compañeros de clase, con quienes compartí esta gran aventura académica. Su colaboración y espíritu de equipo han enriquecido significativamente mi experiencia educativa.

Finalmente, deseo agradecer a mis maestros y tutores, cuyo conocimiento y dedicación han sido fundamentales para mi formación. Gracias por su paciencia, orientación y por inculcarme la pasión por el aprendizaje y la investigación.

A todos ustedes, les debo este éxito y les extiendo mi más profundo agradecimiento.

RESUMEN

Este trabajo de Fin de Máster explora y analiza dos protocolos de comunicación, MQTT (Message Queuing Telemetry Transport) y NDN (Named Data Networking), con el objetivo de proporcionar una comprensión profunda de sus características, aplicaciones y eficiencia en diversos contextos.

La primera parte del estudio se centra en MQTT, un protocolo de mensajería ligero y ampliamente utilizado en el ámbito de IoT (Internet of Things). Se examinan sus principios fundamentales, su arquitectura de publicación/suscripción y su capacidad para gestionar grandes volúmenes de datos en entornos distribuidos.

La segunda parte se dedica a NDN, un enfoque innovador basado en la noción de nombrar datos en lugar de direcciones IP. Se exploran las ventajas de este enfoque centrado en el contenido, como la reducción de la congestión de red y la optimización en la entrega de información.

El núcleo del TFM consiste en una detallada comparación entre MQTT y NDN, abordando aspectos como la eficiencia en la transmisión de datos, la escalabilidad, la tolerancia a fallos y la seguridad. Se destacan los escenarios óptimos para la implementación de cada protocolo, considerando factores como el tamaño de la red, la frecuencia de comunicación y los requisitos de seguridad.

Este análisis proporciona una visión integral de las fortalezas y limitaciones de MQTT y NDN, brindando a los profesionales y tomadores de decisiones la información necesaria para seleccionar el protocolo más adecuado según los requisitos específicos de sus proyectos. El TFM concluye con recomendaciones prácticas y áreas de investigación futuras para mejorar aún más la eficiencia y la adaptabilidad de estos protocolos en entornos tecnológicos en constante evolución.

Palabras Clave: MQTT, NDN, IoT, IP, Red, Protocolos de Comunicación.

ABSTRACT

This Master's Thesis explores and analyzes two communication protocols, MQTT (Message Queuing Telemetry Transport) and NDN (Named Data Networking), with the aim of providing a deep understanding of their features, applications, and efficiency in various contexts.

The first part of the study focuses on MQTT, a lightweight messaging protocol widely used in the Internet of Things (IoT) domain. It examines its fundamental principles, its publish/subscribe architecture, and its ability to handle large volumes of data in distributed environments.

The second part is dedicated to NDN, an innovative approach based on the concept of naming data instead of IP addresses. The advantages of this content-centric approach, such as reducing network congestion and optimizing information delivery, are explored.

The core of the Master's Thesis involves a detailed comparison between MQTT and NDN, addressing aspects such as data transmission efficiency, scalability, fault tolerance, and security. Optimal scenarios for the implementation of each protocol are highlighted, considering factors such as network size, communication frequency, and security requirements.

This analysis provides a comprehensive view of the strengths and limitations of MQTT and NDN, offering professionals and decision-makers the necessary information to select the most suitable protocol based on the specific requirements of their projects. The Master's Thesis concludes with practical recommendations and future research areas to further enhance the efficiency and adaptability of these protocols in ever-evolving technological environments.

Keywords: MQTT, NDN, IoT, IP, Network, Communication protocols.

1 INTRODUCCIÓN

En el fascinante universo del Internet de las Cosas (IoT), donde la conectividad y la eficiencia son fundamentales, la elección del protocolo de comunicación se convierte en un aspecto crítico. Este Trabajo de Fin de Máster se sumerge en un análisis detallado de dos destacados protagonistas en este escenario: MQTT (Message Queuing Telemetry Transport) y NDN (Named Data Networking). Más allá de una mera evaluación técnica, este estudio se centra en comprender cómo estos protocolos, con sus enfoques únicos, impactan en el intercambio de información en entornos específicos del IoT.

Comenzamos nuestra exploración en el mundo de MQTT, un protocolo conocido por su ligereza y versatilidad en el ámbito del IoT. Desde sus principios fundamentales hasta su arquitectura de publicación/suscripción, examinamos no solo cómo transmite datos, sino también cómo se integra de manera efectiva en entornos distribuidos. MQTT no es simplemente un medio para la transmisión de datos; es una piedra angular en la eficiencia de la comunicación en el IoT.

La atención luego se centra en NDN, un enfoque innovador que desafía las convenciones al poner el énfasis en el contenido en lugar de las direcciones IP. Al explorar las ventajas que ofrece, como la reducción de la congestión de red y la optimización en la entrega de datos, buscamos entender cómo NDN se presenta como una opción única para abordar los desafíos específicos del intercambio de información en el IoT.

El núcleo de este trabajo reside en una comparación meticulosa entre MQTT y NDN, no solo desde un punto de vista técnico, sino también con un enfoque en su aplicabilidad en situaciones del mundo real del IoT. Desde la eficiencia en la transmisión de datos hasta la escalabilidad y la seguridad, exploramos cómo estos protocolos se desenvuelven en escenarios concretos. Al resaltar los contextos óptimos para la implementación de cada protocolo, considerando variables críticas como el tamaño de la red, la frecuencia de comunicación y los requisitos de seguridad, este análisis proporciona una guía valiosa para aquellos que buscan seleccionar el protocolo más adecuado para sus proyectos en el dinámico ecosistema del IoT.

Este estudio no es simplemente un ejercicio de comparación técnica, sino una inmersión en cómo estas decisiones tecnológicas afectan directamente la capacidad de las redes para comunicarse de manera eficiente en un entorno cada vez más interconectado.

1.1 Motivación

La elección de abordar la comparación entre los protocolos de comunicación MQTT y NDN en mi Trabajo de Fin de Máster surge de una profunda motivación para contribuir al entendimiento y desarrollo de soluciones eficientes en el contexto del Internet de las Cosas (IoT).

En el transcurso de mi formación académica y experiencias profesionales, he sido testigo del rápido avance del IoT y su impacto en la forma en que interactuamos con el entorno tecnológico. La diversidad de aplicaciones y la creciente complejidad de las redes IoT me han inspirado a explorar protocolos de comunicación que desempeñan un papel esencial en la facilitación de la transmisión de datos en este entorno dinámico.

La elección específica de MQTT y NDN se basa en mi interés en comprender cómo estos dos protocolos, cada uno con enfoques únicos, se enfrentan a los desafíos particulares del intercambio de información en entornos IoT. MQTT, con su ligereza y amplia adopción, representa una columna vertebral en muchas implementaciones IoT, mientras que NDN, con su enfoque innovador centrado en el contenido, ofrece una perspectiva diferente y potencialmente disruptiva.

Mi motivación se centra en contribuir al conocimiento existente, proporcionando una evaluación detallada y práctica de estos protocolos en escenarios específicos del mundo real. Busco no solo entender sus capacidades técnicas, sino también identificar las situaciones óptimas para su implementación, considerando factores clave como la eficiencia en la transmisión de datos, la escalabilidad y la seguridad.

Además, al realizar este Trabajo de Fin de Máster, aspiro a aportar información valiosa a la comunidad académica y profesional que pueda ser utilizada como guía en la selección de protocolos para proyectos IoT. Esta motivación va más allá de un interés personal y se alinea con mi deseo de contribuir al avance y la optimización de las tecnologías que moldearán nuestro futuro conectado.

En resumen, mi motivación para realizar este Trabajo de Fin de Máster radica en el deseo de comprender, evaluar y contribuir al desarrollo de soluciones eficientes en el emocionante y dinámico campo del Internet de las Cosas.

1.2 Objetivos

El principal objetivo de este Trabajo de Fin de Máster es realizar una comparación exhaustiva entre los protocolos de comunicación MQTT (Message Queuing Telemetry Transport) y NDN (Named Data Networking) en el contexto del Internet de las Cosas (IoT). El propósito es proporcionar una evaluación detallada de sus características, rendimiento y aplicabilidad en escenarios específicos, con el fin de ofrecer a profesionales y tomadores de decisiones una guía informada en la selección de protocolos para implementaciones IoT.

1.3 Objetivos específicos

1. **Comprender los Fundamentos de MQTT y NDN:**

Profundizar en los principios fundamentales de MQTT, explorando su arquitectura de publicación/suscripción y su capacidad para manejar grandes volúmenes de datos en entornos distribuidos.

Analizar los conceptos fundamentales de NDN, centrándose en su enfoque innovador basado en la noción de nombrar datos en lugar de direcciones IP.

2. **Evaluar el Rendimiento Técnico:**

Realizar simulaciones detalladas para evaluar el rendimiento técnico de MQTT y NDN en escenarios representativos de redes IoT.

Analizar métricas como la eficiencia en la transmisión de datos, la escalabilidad y la tolerancia a fallos.

3. **Identificar Escenarios Óptimos de Implementación:**

Destacar los contextos ideales para la implementación de cada protocolo, considerando variables críticas como el tamaño de la red, la frecuencia de comunicación y los requisitos de seguridad.

4. **Proporcionar Recomendaciones Prácticas:**

Concluir el análisis con recomendaciones prácticas basadas en los hallazgos, orientadas a profesionales y desarrolladores involucrados en proyectos IoT.

5. **Identificar Áreas de Investigación Futura:**

Reconocer posibles áreas de investigación futura que puedan contribuir al avance y la mejora continua de los protocolos MQTT y NDN en entornos IoT en constante evolución.

1.4 Impacto esperado

El presente Trabajo de Fin de Máster propone generar un impacto significativo en el ámbito del Internet de las Cosas (IoT) al abordar la comparación detallada entre los protocolos de comunicación MQTT y NDN. Se espera que los resultados y conclusiones de este estudio tengan repercusiones notables en diversos niveles, tales como:

1. **Orientación para la Selección de Protocolos en Proyectos IoT:**

Se anticipa que los hallazgos proporcionarán a profesionales y tomadores de decisiones una guía práctica y fundamentada para la selección de protocolos de comunicación en proyectos específicos de IoT. Esta orientación contribuirá a la optimización de la eficiencia y rendimiento de las soluciones implementadas.

2. **Mejora de la Eficiencia en Redes IoT:**

Al destacar los escenarios óptimos para la implementación de cada protocolo, se espera que este trabajo contribuya a mejorar la eficiencia de las redes IoT. La comprensión detallada de las fortalezas y limitaciones de MQTT y NDN permitirá a los profesionales diseñar soluciones más adaptables y eficientes.

3. **Fomento de Investigaciones Futuras:**

La identificación de áreas de investigación futuras en el contexto de los protocolos MQTT y NDN tiene como objetivo estimular el interés y la participación en proyectos de investigación continuos. Se espera que este trabajo sirva como punto de partida para futuras investigaciones que busquen impulsar el desarrollo y la innovación en el ámbito de las comunicaciones IoT.

4. **Contribución al Conocimiento Técnico:**

El análisis detallado de los fundamentos técnicos, además del rendimiento de MQTT y NDN en situaciones prácticas, busca contribuir al conocimiento técnico existente. Los resultados obtenidos pueden ser referencia para académicos, investigadores y

profesionales que busquen comprender mejor la dinámica de estos protocolos en entornos IoT.

5. **Adaptación a Escenarios Cambiantes:**

La entrega de recomendaciones prácticas basadas en los resultados del estudio tiene como objetivo facilitar la adaptación de profesionales y desarrolladores a escenarios cambiantes y desafiantes en el ámbito del IoT. Esto podría tener un impacto directo en la capacidad de implementar soluciones más efectivas y resilientes.

En conjunto, se espera que este Trabajo de Fin de Máster no solo enriquezca el conocimiento existente sobre los protocolos de comunicación en el IoT, sino que también tenga aplicaciones prácticas tangibles, influenciando positivamente la toma de decisiones y el desarrollo de proyectos en este campo emergente y dinámico.

1.5 Metodología

La realización de este Trabajo de Fin de Máster se llevará a cabo siguiendo una metodología estructurada que permita una evaluación detallada y comparativa de los protocolos MQTT y NDN en el contexto específico de las redes del Internet de las Cosas (IoT). La metodología propuesta se desglosa en las siguientes etapas:

1. **Revisión Bibliográfica:**

Iniciar con una revisión exhaustiva de la literatura existente sobre MQTT, NDN y sus aplicaciones en entornos IoT. Esto proporcionará una base sólida para comprender los fundamentos teóricos y las tendencias actuales en el campo.

2. **Definición de Parámetros de Evaluación:**

Identificar y definir los parámetros clave que serán evaluados para comparar MQTT y NDN. Esto incluirá aspectos como eficiencia en la transmisión de datos, escalabilidad, tolerancia a fallos y seguridad, entre otros.

3. **Simulaciones y Experimentación:**

Utilizar herramientas de simulación especializadas para recrear escenarios representativos de redes IoT. Emplear simuladores reconocidos, como OMNeT++ o similares, para llevar a cabo experimentos detallados que evalúen el rendimiento de MQTT y NDN en diferentes situaciones.

4. **Recopilación de Datos y Métricas:**

Recopilar datos significativos durante las simulaciones, centrándose en las métricas definidas previamente. Registrar información sobre la eficiencia en la transmisión de datos, la latencia, el consumo de recursos y otros indicadores relevantes.

5. **Análisis Estadístico:**

Aplicar análisis estadístico a los datos recopilados para obtener resultados significativos y comparaciones cuantitativas entre MQTT y NDN. Este análisis proporcionará una visión objetiva del rendimiento de cada protocolo en diversas condiciones.

6. **Escenarios Óptimos de Implementación:**

Identificar, a partir de los resultados obtenidos, los escenarios óptimos para la implementación de MQTT y NDN. Considerar variables como el tamaño de la red, la frecuencia de comunicación y los requisitos de seguridad para ofrecer recomendaciones específicas.

7. **Conclusiones y Recomendaciones:**

Sintetizar los resultados obtenidos en conclusiones significativas. Proporcionar recomendaciones prácticas basadas en los hallazgos para orientar la selección de protocolos en proyectos reales de IoT.

8. **Identificación de Áreas de Investigación Futura:**

Reconocer y destacar posibles áreas de investigación futura que puedan ampliar el conocimiento y mejorar la eficiencia de MQTT y NDN en entornos IoT en constante evolución.

La metodología propuesta se ajusta a un enfoque científico riguroso que permitirá una evaluación objetiva y fundamentada de los protocolos de comunicación en el contexto específico del IoT. La combinación de simulaciones, análisis estadístico y revisión bibliográfica garantizará la validez y relevancia de los resultados obtenidos.

1.6 Estructura

El Trabajo de Fin de Máster seguirá una estructura organizada que refleje la metodología y los objetivos planteados. La estructura propuesta es la siguiente:

I. Introducción

- Contextualización del IoT y la importancia de los protocolos de comunicación.
- Declaración de la problemática y la relevancia de comparar MQTT y NDN.
- Objetivos del Trabajo de Fin de Máster.
- Motivación y justificación para abordar esta investigación.

II. Marco Teórico

- Revisión bibliográfica detallada sobre MQTT y NDN.
- Principios fundamentales de cada protocolo.
- Aplicaciones y casos de uso en entornos IoT.
- Estado actual de la investigación en comparativas entre MQTT y NDN.

III. Metodología

- Descripción detallada de la metodología utilizada para llevar a cabo la comparación.
- Justificación de la elección de herramientas de simulación y parámetros de evaluación.
- Procedimientos para la recopilación de datos y análisis estadístico.
- Consideraciones éticas en la investigación.

IV. Evaluación de MQTT

- Resultados de la evaluación específica de MQTT.
- Análisis detallado de métricas y rendimiento.
- Interpretación de los datos obtenidos durante las simulaciones.

V. Evaluación de NDN

- Resultados de la evaluación específica de NDN.
- Análisis detallado de métricas y rendimiento.
- Comparación con los resultados de MQTT.

VI. Comparación y Análisis Comparativo

- Análisis cuantitativo de los datos recopilados.
- Comparación directa entre MQTT y NDN en términos de eficiencia, escalabilidad y seguridad.
- Interpretación de las diferencias observadas y sus implicaciones.

VII. Escenarios Óptimos de Implementación

- Identificación de los contextos ideales para la implementación de MQTT y NDN.
- Recomendaciones basadas en los resultados obtenidos.
- Consideración de variables clave como el tamaño de la red y la frecuencia de comunicación.

VIII. Conclusiones y Recomendaciones Finales

- Síntesis de los hallazgos más importantes.
- Conclusiones derivadas de la comparación y análisis.
- Recomendaciones finales para profesionales y tomadores de decisiones en proyectos IoT.

IX. Identificación de Áreas de Investigación Futura

- Reconocimiento de posibles extensiones y áreas de investigación futura.
- Propuestas para mejorar y ampliar la eficiencia de MQTT y NDN en entornos IoT.

X. Referencias Bibliográficas

- Citas bibliográficas de fuentes utilizadas durante la investigación y revisión bibliográfica.

Esta estructura busca proporcionar una presentación coherente y lógica de la investigación, permitiendo al lector seguir de manera fluida la evolución del estudio desde la introducción hasta las conclusiones y recomendaciones finales.

2 ESTADO DEL ARTE.

2.1 Revisión Bibliográfica Detallada sobre MQTT y NDN

MQTT es un protocolo de mensajería ligero, basado en el modelo de publicación-suscripción, diseñado originalmente por IBM en 1999. Su principal objetivo es proporcionar una transmisión de datos eficiente y con un bajo uso de ancho de banda, ideal para dispositivos con recursos limitados y redes de alta latencia o fiabilidad variable.

El protocolo MQTT fue desarrollado por Andy Stanford-Clark de IBM y Arlen Nipper de Arcom (hoy Eurotech) en 1999. Fue diseñado para ser simple y eficiente, capaz de trabajar en condiciones de red irregulares. En 2013, MQTT fue estandarizado por la Organización para el Avance de Estándares de Información Estructurada (OASIS), consolidándose como un protocolo clave en el ámbito de IoT.

MQTT opera sobre el protocolo TCP/IP y sigue el modelo de publicación-suscripción. En este modelo, los clientes pueden actuar como "publicadores" y "suscriptores". Un "broker" MQTT actúa como intermediario, recibiendo mensajes de los publicadores y distribuyéndolos a los suscriptores interesados.

MQTT se destaca por su simplicidad y eficiencia, lo que lo convierte en una excelente opción para dispositivos con recursos limitados. Una de sus características clave es su diseño ligero, que reduce al mínimo el sobrecosto en los paquetes de datos, optimizando su uso en entornos con restricciones de recursos.

El protocolo también ofrece diferentes niveles de Calidad de Servicio (QoS), proporcionando flexibilidad en la entrega de mensajes según las necesidades de la aplicación. Con QoS 0, el mensaje se entrega al menos una vez sin garantía de recepción; QoS 1 asegura que el mensaje sea entregado al menos una vez y requiere confirmación; mientras que QoS 2 garantiza que el mensaje se entregue exactamente una vez, evitando duplicaciones.

Además, MQTT permite la persistencia de mensajes. El broker puede almacenar mensajes en caso de que el cliente suscriptor no esté disponible, lo que asegura que la información no se pierda. También admite sesiones duraderas, permitiendo a los clientes recuperar los mensajes perdidos al reconectarse a la red.

Finalmente, uno de los aspectos más valorados de MQTT es su eficiencia en el uso de ancho de banda, lo que lo hace especialmente útil en redes de baja capacidad, donde la minimización del tráfico de datos es crucial para un rendimiento óptimo.

MQTT se utiliza ampliamente en aplicaciones IoT, tales como la Domótica, el Monitoreo Industrial, la Telemedicina y en la Agricultura Inteligente.

NDN (Named Data Networking) es una arquitectura de red centrada en el contenido, desarrollada como parte del proyecto Future Internet Architecture (FIA) de la Fundación Nacional de Ciencias de EE.UU. (NSF). Basada en nombres de contenido para la transmisión de datos, lo que la diferencia del modelo tradicional, el cual se basa solo en direcciones IP.

NDN se originó como una evolución del concepto de Content-Centric Networking (CCN), propuesto por Van Jacobson en 2006. El proyecto fue lanzado formalmente en 2010 como una colaboración entre varias universidades y centros de investigación, con el objetivo de rediseñar la arquitectura de Internet para ser más eficiente y segura.

La arquitectura NDN se fundamenta en el uso de nombres en lugar de direcciones para identificar y acceder a los datos. Los principales componentes y principios de NDN incluyen:

- **Nombres en lugar de Direcciones**: Cada dato tiene un nombre único y jerárquico, lo que facilita la búsqueda y recuperación de información.
- **Interés y Datos**: Los consumidores envían paquetes de interés solicitando datos específicos. Los productores responden con paquetes de datos correspondientes.
- **Caché en la Red**: Los routers en NDN almacenan copias de los datos en caché, permitiendo una entrega más rápida y eficiente en solicitudes futuras.
- **Seguridad Integrada**: La seguridad en NDN se implementa a nivel de datos. Cada paquete de datos está firmado criptográficamente, garantizando su autenticidad e integridad.
- **Encaminamiento Basado en Nombres**: Los routers NDN utilizan el nombre de los datos para dirigir los paquetes, en lugar de depender de direcciones IP.

Las características clave de NDN son las siguientes:

- **Eficiencia en el Uso de Recursos**: La capacidad de caché de los routers reduce la necesidad de solicitudes repetitivas al servidor original, optimizando el uso del ancho de banda.
- **Mejora de la Seguridad**: La seguridad de los datos está integrada en la arquitectura, asegurando que los datos no sean manipulados o interceptados.
- **Flexibilidad y Escalabilidad**: La naturaleza jerárquica de los nombres permite una fácil extensión y adaptación a diferentes contextos y aplicaciones.
- **Resiliencia**: La capacidad de caché y el enrutamiento basado en nombres aumentan la resiliencia de la red frente a fallos y ataques.

NDN se aplica en una variedad de contextos, tales como la transmisión de video y contenidos multimedia, las redes de sensores IoT, la seguridad y redes privadas y aplicaciones móviles.

MQTT y NDN representan enfoques complementarios en la transmisión de datos, cada uno optimizado para diferentes necesidades. MQTT se centra en la eficiencia y simplicidad, diseñado para facilitar la comunicación entre dispositivos con recursos limitados mediante un modelo de publicación-suscripción. Esta filosofía lo convierte en una opción ideal para aplicaciones donde la transmisión periódica de pequeños volúmenes de datos y el uso eficiente del ancho de banda son críticos. En contraste, NDN adopta un enfoque orientado al contenido, priorizando la accesibilidad y recuperación eficiente de datos. Su filosofía no solo busca optimizar la distribución de contenido, sino también integrar la seguridad en el núcleo del diseño, garantizando que cada paquete esté firmado criptográficamente.

En términos de eficiencia de la comunicación, MQTT es ligero y minimiza el uso del ancho de banda, lo que lo hace adecuado para dispositivos IoT con transmisión de datos periódica. NDN, por su parte, mejora la eficiencia mediante el almacenamiento en caché, lo que reduce las solicitudes al servidor original al reutilizar datos previamente obtenidos.

La escalabilidad también distingue a ambos protocolos. Mientras que MQTT puede enfrentar limitaciones debido a la dependencia de un broker central que actúa como intermediario, NDN está diseñado para escalar de manera más eficiente al distribuir la carga entre nodos a través del almacenamiento en caché y el enrutamiento basado en nombres, lo que permite manejar mayores volúmenes de tráfico sin crear cuellos de botella.

En cuanto a la seguridad, MQTT necesita de mecanismos externos como TLS para proteger las transmisiones, mientras que NDN integra la seguridad de manera nativa, firmando cada paquete de datos para garantizar su autenticidad.

Finalmente, la aplicabilidad de cada protocolo varía según las necesidades de la red. MQTT es común en aplicaciones de monitoreo y control, donde la transmisión eficiente y confiable de mensajes es esencial. Por otro lado, NDN resulta más adecuado en escenarios que requieren una distribución eficiente de contenido y una seguridad robusta, como la transmisión de video o en redes de sensores. Ambos enfoques ofrecen soluciones valiosas dependiendo de los requerimientos específicos de la aplicación.

2.2 Principios fundamentales de cada protocolo.

MQTT utiliza un modelo de comunicación de publicación/suscripción, lo que permite que dicha comunicación sea asincrónica y desacoplada entre los dispositivos. En este, los publicadores envían mensajes a un tema específico sin necesidad de conocer la existencia de los suscriptores, mientras que los suscriptores reciben mensajes de los temas a los que se han suscrito sin conocer a los publicadores. Esto permite una mayor flexibilidad y escalabilidad en las aplicaciones IoT, donde los dispositivos pueden entrar y salir de la red dinámicamente.

El broker es una pieza central en el ecosistema de MQTT, ya que actúa como un intermediario confiable que a su vez facilita la comunicación entre publicadores y suscriptores. Los brokers gestionan la distribución de mensajes, asegurando así que los mensajes se entreguen a todos los suscriptores relevantes. Existen varios brokers MQTT disponibles, tanto de código abierto como comerciales, tales como Mosquitto, HiveMQ y EMQX, cada uno con diferentes características y capacidades.

Respecto a la calidad de servicio (QoS) en MQTT, el cual define el nivel de garantía con el que se entrega un mensaje. Consta de tres niveles de QoS, los cuales son:

- **QoS 0 (Entrega al menos una vez)**: El mensaje se entrega al menos una vez, pero no se garantiza su recepción. Este nivel es el más rápido y con menor sobrecarga, adecuado para aplicaciones donde la pérdida de algunos mensajes no es crítica.

- **QoS 1 (Entrega al menos una vez)**: El mensaje se entrega al menos una vez y requiere una confirmación de recepción del cliente. Si no se recibe la confirmación, el mensaje se retransmite. Este nivel es adecuado para aplicaciones que necesitan garantizar la recepción de mensajes pero pueden tolerar duplicados.
- **QoS 2 (Entrega exactamente una vez)**: El mensaje se entrega exactamente una vez, utilizando un protocolo de confirmación de dos fases para evitar duplicados. Este nivel es el más confiable pero también el más lento y con mayor sobrecarga, adecuado para aplicaciones críticas donde la entrega duplicada no es aceptable.

MQTT permite la persistencia de sesiones, lo que significa que el broker puede almacenar el estado de la conexión del cliente, incluyendo las suscripciones y los mensajes no entregados. Esto es especialmente útil para dispositivos IoT que pueden experimentar desconexiones intermitentes. Al reconectarse, el cliente puede reanudar su sesión sin perder mensajes importantes.

Los mensajes retenidos son una característica útil en MQTT donde el broker almacena el último mensaje publicado en un tema y lo entrega a cualquier nuevo suscriptor de ese tema. Esto asegura que los nuevos suscriptores reciban inmediatamente el estado más reciente del tema, lo cual es crucial en aplicaciones donde los datos de estado deben ser conocidos por todos los dispositivos.

MQTT incluye varios tipos de mensajes de control que gestionan la conexión y el flujo de datos entre los clientes y el broker. Algunos de estos mensajes incluyen:

- **CONNECT**: Inicia una conexión entre el cliente y el broker.
- **CONNACK**: Acknowledge de una solicitud de conexión.
- **PUBLISH**: Enviar un mensaje a un tema.
- **PUBACK**: Confirmación de recepción de un mensaje publicado.
- **SUBSCRIBE**: Suscripción a uno o más temas.
- **SUBACK**: Confirmación de una solicitud de suscripción.
- **UNSUBSCRIBE**: Cancelar una suscripción a uno o más temas.
- **UNSUBACK**: Confirmación de una solicitud de cancelación de suscripción.
- **PINGREQ** y **PINGRESP**: Mensajes para mantener viva la conexión y asegurar que el cliente y el broker están activos.
- **DISCONNECT**: Cerrar la conexión entre el cliente y el broker.

NDN se basa en el uso de nombres jerárquicos en lugar de direcciones IP para identificar y recuperar datos. Cada contenido en NDN tiene un nombre único que lo describe y lo estructura, lo que a su vez permite una recuperación eficiente y semántica de la información. Por ejemplo, un nombre NDN podría ser "/universidad/departamento/curso/material/video1", que describe claramente el contenido y su jerarquía.

Su comunicación se realiza mediante dos tipos de paquetes: uno en donde los consumidores los envían para solicitar contenido específico, los cuales se caracterizan por tener el nombre del contenido deseado y a su vez se encaminan a través de la red hacia los productores que pueden proporcionar el contenido; y en el que los productores responden con paquetes de datos que tienen el contenido solicitado. Cada uno está firmado criptográficamente para garantizar su autenticidad e integridad. Los paquetes de datos siguen el mismo camino inverso de los paquetes de interés, aprovechando la caché de los routers intermedios.

Una característica clave de NDN es que sus routers poseen la capacidad de almacenar datos en caché en la red, permitiendo así que los datos se sirvan directamente desde el caché en futuras solicitudes, reduciendo la latencia y el tráfico en la red. Esto es especialmente beneficioso en aplicaciones IoT donde los mismos datos pueden ser solicitados por múltiples dispositivos.

En NDN el encaminamiento se basa en los nombres de los datos en lugar de las direcciones IP. Los routers mantienen dos tablas principales para gestionar las solicitudes de datos, los cuales son:

- **Forwarding Information Base (FIB)**: Similar a las tablas de enrutamiento en IP, la FIB contiene entradas que asocian nombres de contenido con interfaces de salida.
- **Pending Interest Table (PIT)**: Mantiene un registro de las solicitudes de interés que no han sido satisfechas aún. Cuando un paquete de datos llega, se utiliza la PIT para reenviar el paquete de datos a todos los consumidores que solicitaron el contenido.

La seguridad en NDN está centrada en el contenido, con cada paquete de datos firmado criptográficamente por el productor. Esto asegura la autenticidad e integridad del contenido, independientemente de cómo y dónde se almacene o transmita. Además,

NDN permite la verificación de la identidad del productor, lo que agrega una capa adicional de seguridad en la comunicación.

Otro punto por considerar es que NDN es altamente adaptable a diversos entornos y aplicaciones, facilitando la interoperabilidad entre diferentes sistemas y dispositivos. La estructura de nombres jerárquicos permite una fácil extensión y adaptación a nuevos contextos y necesidades. Por ejemplo, un sistema IoT que utiliza NDN puede integrar fácilmente nuevos sensores y dispositivos sin necesidad de reconfigurar la infraestructura de red existente.

2.3 Aplicaciones y casos de uso en entornos IoT.

Una de las aplicaciones más comunes de MQTT es la monitorización de sensores y la telemática en entornos IoT. Los sensores que recopilan datos ambientales, como temperatura, humedad, presión, y otros parámetros, pueden utilizar MQTT para enviar estos datos a un servidor central o a la nube. Por ejemplo, en la agricultura inteligente, los sensores de campo envían datos en tiempo real sobre las condiciones del suelo y el clima, permitiendo a los agricultores tomar decisiones informadas sobre riego y fertilización.

En la automatización del hogar, MQTT se utiliza para conectar dispositivos y sistemas inteligentes, tales como luces, termostatos, cerraduras de puertas y cámaras de seguridad. Los usuarios pueden controlarlos y monitorizarlos a través de aplicaciones móviles o interfaces web. Por ejemplo, un termostato inteligente puede ajustar automáticamente la temperatura de una casa según las preferencias del usuario y los datos de sensores de presencia.

De acuerdo con la gestión de flotas y logística, MQTT se emplea para rastrear vehículos en tiempo real y monitorizar el estado de los envíos. Los vehículos pueden equiparse con dispositivos GPS y otros sensores que envían datos de ubicación, velocidad y estado del motor a través de MQTT. Estos datos se pueden utilizar para optimizar rutas, programar mantenimiento preventivo y mejorar la eficiencia operativa.

MQTT es ampliamente utilizado en sistemas de alarma y seguridad para transmitir alertas y eventos en tiempo real. Por ejemplo, un sistema de seguridad para el hogar puede enviar notificaciones instantáneas a los propietarios cuando se detecta una

intrusión o cuando se activa una alarma de humo. Los dispositivos de seguridad pueden estar conectados a través de MQTT para garantizar una respuesta rápida y coordinada a los eventos de emergencia.

En las redes de energía inteligente (Smart Grid), MQTT se utiliza para la comunicación entre medidores inteligentes, sistemas de gestión de energía y proveedores de servicios públicos. Los medidores inteligentes pueden enviar datos de consumo de energía en tiempo real a un servidor central, permitiendo a las empresas de servicios públicos monitorizar y gestionar la distribución de energía de manera más eficiente. Además, los usuarios finales pueden acceder a sus datos de consumo y ajustar su uso de energía para reducir costos.

Respecto al campo de la telemedicina y la salud electrónica, MQTT se utiliza para la transmisión segura y confiable de datos entre dispositivos médicos, pacientes y profesionales de la salud. Por ejemplo, los dispositivos portátiles de monitoreo de la salud pueden enviar datos sobre la frecuencia cardíaca, la presión arterial y otros parámetros vitales a través de MQTT a una plataforma de salud en la nube, donde los médicos pueden acceder a estos datos en tiempo real para supervisar la salud del paciente.

En la industria 4.0, MQTT se utiliza para la comunicación entre máquinas, sistemas de control y plataformas de análisis de datos. Los sensores en las líneas de producción pueden enviar datos de rendimiento y estado a través de MQTT, permitiendo a los sistemas de control ajustar automáticamente los parámetros de producción y a las plataformas de análisis identificar patrones y tendencias para mejorar la eficiencia y la calidad del producto.

Acerca de las redes de sensores distribuidas, NDN ofrece una solución eficiente para la recopilación y distribución de datos. Los sensores pueden nombrar sus datos de manera jerárquica y compartirlos directamente a través de la red sin necesidad de intermediarios. Por ejemplo, en un sistema de monitoreo ambiental, los sensores pueden publicar datos con nombres como "/ciudad/área/sensor/temperatura" y los consumidores pueden solicitar estos datos utilizando nombres específicos.

NDN es particularmente adecuado para vehículos autónomos y conectados debido a su capacidad para manejar la movilidad y la dinámica de la red. Los vehículos pueden intercambiar datos sobre su estado, ubicación y entorno utilizando nombres jerárquicos. Por ejemplo, un vehículo puede solicitar información sobre el tráfico en su ruta utilizando

un nombre como "/ciudad/carretera/tráfico" y recibir datos en tiempo real desde otros vehículos o infraestructuras viales.

En las ciudades inteligentes (Smart Cities), NDN puede facilitar la comunicación entre diversos dispositivos IoT, como sensores de tráfico, cámaras de vigilancia y estaciones meteorológicas. Los datos recopilados pueden ser compartidos y utilizados por múltiples aplicaciones y servicios urbanos. Por ejemplo, los datos de sensores de tráfico pueden ser utilizados por sistemas de gestión de tráfico para optimizar la sincronización de semáforos y así reducir la congestión.

NDN puede mejorar la resiliencia y la seguridad de la infraestructura crítica y las redes de energía inteligente al permitir una comunicación segura y eficiente basada en el contenido. Los dispositivos en la red de energía pueden publicar y suscribir datos utilizando nombres jerárquicos, permitiendo así una gestión más efectiva y segura del suministro de energía. Por ejemplo, los medidores inteligentes pueden publicar datos de consumo y recibir comandos de control utilizando nombres como "/servicio_energia/medidor/consumo" y "/servicio_energia/medidor/control".

Así mismo en los sistemas industriales, NDN puede proporcionar una comunicación robusta y segura para el monitoreo y control de procesos. Los datos de sensores y actuadores pueden ser nombrados y distribuidos a través de la red de manera eficiente. Por ejemplo, en una planta de fabricación, los sensores pueden publicar datos sobre el estado de las máquinas y los actuadores pueden recibir comandos de control utilizando nombres específicos para cada proceso.

Además, NDN es ideal para redes de dispositivos móviles, donde la topología de la red puede cambiar frecuentemente. Los dispositivos pueden comunicarse directamente utilizando nombres jerárquicos sin necesidad de una infraestructura de red fija. Por ejemplo, en un escenario de rescate y emergencia, los equipos de rescate pueden compartir datos y coordinar sus actividades utilizando nombres que describen la ubicación y la situación actual, como "/rescate/zona1/estado".

Este puede mejorar la distribución de contenido y servicios de entretenimiento al permitir una entrega eficiente y escalable de datos. Los usuarios pueden solicitar contenido multimedia utilizando nombres específicos y recibir los datos directamente desde la caché de los routers en la red. Por ejemplo, un usuario puede solicitar un video utilizando un nombre como "/entretenimiento/video/título" y recibir el contenido de manera rápida y eficiente.

2.4 Estado actual de la investigación en comparativas entre MQTT y NDN.

La comparación entre MQTT y NDN en términos de desempeño ha sido un tema de interés en la investigación debido a las diferencias fundamentales en sus arquitecturas y modelos de comunicación. Diversos estudios la han abordado desde diferentes perspectivas, evaluando parámetros como la latencia, el uso de ancho de banda, la escalabilidad y la eficiencia energética.

Un estudio detallado realizado por [Truong y Kanhere (2018)] ha mostrado que MQTT, debido a su modelo de publicación/suscripción centralizada, puede ofrecer una baja latencia en redes utilizando un broker bien dimensionado y con baja carga. Sin embargo, en redes muy densas o con alta carga de mensajes, dicha latencia puede incrementarse significativamente debido a la sobrecarga en el broker. Por otro lado, NDN, al utilizar el encaminamiento basado en nombres y la caché en la red, puede distribuir la carga de tráfico y reducir la latencia al servir los datos desde los nodos intermedios en lugar de un servidor central.

En términos de uso de ancho de banda, MQTT puede ser más eficiente en redes con pocos suscriptores, ya que los mensajes se envían solo a los nodos interesados. Sin embargo, en escenarios con muchos suscriptores, el tráfico puede aumentar considerablemente. NDN, con su capacidad de caché, puede reducir el uso de ancho de banda al evitar la retransmisión de datos populares, aunque puede introducir una mayor sobrecarga inicial en la red al distribuir los datos.

La escalabilidad es otro factor crítico comparado en varios estudios. MQTT puede enfrentar desafíos de escalabilidad debido a la centralización del broker, que puede convertirse en un punto único de fallo y un cuello de botella en redes muy grandes. NDN, con su arquitectura distribuida y caché en la red, puede escalar mejor en grandes redes distribuidas, como las ciudades inteligentes y las redes de sensores distribuidas.

En términos de eficiencia energética, estudios como el de Tarkoma y Denisov (2017) han indicado que NDN puede ser más eficiente en dispositivos IoT debido a su capacidad de reducir la necesidad de reenvío de datos y su diseño inherentemente basado en contenido. Sin embargo, MQTT, con su diseño ligero y capacidades de QoS, también puede ser optimizado para dispositivos con recursos limitados, especialmente en aplicaciones donde la fiabilidad de entrega de mensajes es crucial.

La seguridad y la privacidad son aspectos necesarios en la evaluación de protocolos de comunicación para IoT. MQTT y NDN adoptan enfoques diferentes para abordar estos desafíos.

MQTT no tiene una seguridad integrada en su diseño original, por lo que la seguridad debe ser gestionada mediante protocolos adicionales como TLS/SSL para cifrar la comunicación entre el cliente y el broker. Además, la autenticación de usuarios y la autorización de temas son gestionadas por el broker, lo que introduce una dependencia adicional en la centralización de este mismo para la seguridad. Esto puede ser una limitación en aplicaciones donde se requiere una alta seguridad distribuida.

Por su diseño NDN incorpora la seguridad a nivel de contenido mediante la firma criptográfica de los paquetes de datos. Esto asegura la autenticidad e integridad del contenido independientemente de su origen o ruta de transmisión. Además, la verificación de la firma se puede realizar en cualquier punto de la red, lo que permite una mayor flexibilidad y seguridad distribuida. La arquitectura basada en nombres también facilita la implementación de políticas de acceso y control basadas en el contenido, en lugar de en la identidad de los dispositivos.

La privacidad en MQTT se gestiona principalmente a través de la encriptación de las comunicaciones y el control de acceso en el broker. Sin embargo, la centralización puede ser un punto débil si dicho broker es comprometido. En NDN, aunque la firma de los datos proporciona seguridad, la naturaleza pública de los nombres de contenido puede exponer información sensible sobre los intereses y actividades de los usuarios. Por ello, se están investigando técnicas de anonimización y privacidad en la capa de nombres para mitigar estos riesgos.

Varios proyectos y estudios han implementado y probado experimentalmente MQTT y NDN en diversos entornos para evaluar su rendimiento y aplicabilidad en escenarios reales.

Proyectos como Eclipse Paho y Mosquitto han desarrollado implementaciones robustas de MQTT que se utilizan ampliamente en aplicaciones industriales y de consumo. Estas implementaciones han sido evaluadas en diversas plataformas, desde dispositivos embebidos hasta sistemas en la nube, demostrando su flexibilidad y adaptabilidad. Las pruebas experimentales han mostrado que es especialmente eficaz en aplicaciones de monitorización en tiempo real y control remoto debido a su baja latencia y simplicidad.

Respecto a NDN, este ha sido implementado y probado en varios proyectos de investigación y despliegues experimentales. El proyecto NDN (Named Data Networking Project) ha desarrollado una implementación de referencia que ha sido utilizada en diversas pruebas de campo. Estas pruebas han demostrado la capacidad de NDN para manejar eficientemente la distribución de contenido en redes altamente dinámicas y móviles, tales como vehiculares y de sensores distribuidos. Además, se ha evaluado la capacidad de NDN para mejorar la resiliencia y la eficiencia de la red mediante su arquitectura basada en contenido y caché.

En cuanto a la comparación entre MQTT y NDN sigue siendo un campo activo de investigación, con varios desafíos y oportunidades para explorar.

Esta investigación futura podría enfocarse en mejorar la escalabilidad y el desempeño de ambos protocolos. Para MQTT, esto podría incluir el desarrollo de brokers más eficientes y distribuidos, así como técnicas avanzadas de balanceo de carga. Para NDN, las investigaciones podrían centrarse en optimizar los algoritmos de encaminamiento y caché, así como en la implementación de políticas de gestión de nombres más eficientes.

De esta manera la seguridad y la privacidad seguirán siendo áreas clave de investigación. Para MQTT, esto podría incluir el desarrollo de mecanismos de seguridad más integrados y distribuidos, así como técnicas avanzadas de autenticación y autorización. Para NDN, las investigaciones podrían centrarse en mejorar la privacidad de los nombres de contenido y en desarrollar técnicas más robustas para la protección de datos sensibles.

3 METODOLOGÍA

3.1 Descripción detallada de la metodología utilizada para llevar a cabo la comparación.

Se basa en un enfoque sistemático y riguroso que permite evaluar múltiples aspectos de cada protocolo. Esta metodología incluye la definición de parámetros de comparación, la configuración del entorno experimental, la implementación de escenarios de prueba específicos, la recopilación y análisis de datos, y la interpretación

de los resultados. El objetivo principal es proporcionar una evaluación exhaustiva que facilite la comprensión de las fortalezas y debilidades de cada protocolo en diferentes contextos y aplicaciones.

Para llevar a cabo una comparación efectiva entre MQTT y NDN, es esencial definir claramente los parámetros de comparación. Estos parámetros cubren aspectos de desempeño, seguridad, privacidad, y escalabilidad, y se eligen en función de su relevancia para las aplicaciones IoT.

Los parámetros de desempeño son fundamentales para evaluar la eficiencia de un protocolo de comunicación, proporcionando una visión clara de su rendimiento en diferentes condiciones. Uno de los parámetros clave es la latencia, que mide el tiempo que tarda un mensaje en viajar desde el origen hasta el destino. Esta medida se analiza tanto en redes de baja como de alta densidad, lo que permite comprender cómo se comporta el protocolo bajo diferentes cargas de trabajo y condiciones de tráfico.

El ancho de banda utilizado es otro aspecto crítico, ya que determina la cantidad de datos transmitidos por unidad de tiempo. Este parámetro es esencial para evaluar la eficiencia en la utilización de los recursos de red, especialmente en entornos donde el ancho de banda es limitado o costoso.

Finalmente, la escalabilidad del protocolo se refiere a su capacidad para manejar un número creciente de dispositivos y mensajes sin experimentar una degradación significativa en el rendimiento. Este parámetro analiza cómo cada protocolo gestiona el aumento en la carga de trabajo y la complejidad de la red, asegurando que la comunicación siga siendo eficiente a medida que crece el número de dispositivos conectados y el volumen de datos transmitidos.

Los parámetros de seguridad y privacidad son esenciales para evaluar la robustez de un protocolo frente a posibles amenazas y para garantizar la protección de los datos y los usuarios. Uno de los aspectos más importantes es la autenticidad, que mide la capacidad del protocolo para verificar la identidad del origen de los datos. En este contexto, se examinan los mecanismos de autenticación que utiliza cada protocolo para asegurarse de que los datos provienen de una fuente confiable.

La integridad, por otro lado, se refiere a la capacidad del protocolo para garantizar que los datos no han sido alterados durante su transmisión. Este parámetro evalúa las

técnicas de verificación de integridad, asegurando que la información llega a su destino de manera íntegra y sin modificaciones.

La confidencialidad es otro aspecto crucial, que mide la capacidad del protocolo para proteger los datos de accesos no autorizados. Para ello, se analizan los métodos de cifrado y otras técnicas de protección de datos que se implementan para salvaguardar la información durante la transmisión.

Finalmente, la privacidad se centra en la protección de la información sobre los intereses y actividades de los usuarios. Este parámetro evalúa las técnicas que utiliza cada protocolo para garantizar que los datos personales y las actividades de los usuarios no sean expuestos ni comprometidos, manteniendo la privacidad a lo largo de la comunicación.

La configuración del software es fundamental para evaluar el rendimiento de MQTT y NDN en entornos IoT. En el caso de MQTT, su implementación se realiza mediante el broker Eclipse Mosquitto, un componente ligero que soporta las versiones más recientes del protocolo. Mosquitto facilita la conexión de clientes MQTT en dispositivos IoT y ofrece herramientas para la monitorización y análisis de mensajes, lo que permite un control detallado de las comunicaciones.

Por otro lado, la implementación de NDN se lleva a cabo utilizando el NDN Forwarding Daemon (NFD), que es el núcleo de la arquitectura NDN. NFD gestiona el encaminamiento y la distribución de contenido, permitiendo a los clientes NDN en dispositivos IoT interactuar de manera eficiente con los datos, maximizando la seguridad y la reutilización de los mismos.

Para evaluar el desempeño de ambos protocolos en diferentes escenarios, se diseñaron pruebas específicas que resaltan distintos aspectos de sus funcionalidades. Cada escenario busca proporcionar una visión integral del comportamiento de MQTT y NDN bajo diversas condiciones de carga, ofreciendo una comparación precisa de su eficiencia, escalabilidad y seguridad en el contexto de redes IoT.

Escenario 1: Red de Baja Densidad

Evaluando el desempeño en una red con pocos dispositivos IoT. Este escenario es representativo de aplicaciones IoT con un número limitado de dispositivos, como sistemas de automatización del hogar.

Los parámetros medidos son la latencia, el ancho de banda utilizado, y la eficiencia energética. Estos se miden en condiciones de baja carga de tráfico para evaluar la eficiencia básica de los protocolos.

Escenario 2: Red de Alta Densidad

Evaluando el desempeño en una red con muchos dispositivos IoT. Este escenario es representativo de aplicaciones a gran escala, como ciudades inteligentes y redes industriales.

Los parámetros medidos son la latencia, el ancho de banda utilizado, la escalabilidad, y la eficiencia energética. Se simulan condiciones de alta carga de tráfico para evaluar cómo cada protocolo maneja la escalabilidad y la sobrecarga de red.

Escenario 3: Seguridad y Privacidad

Evaluando la capacidad de los protocolos para garantizar la autenticidad, integridad, confidencialidad y privacidad de los datos. Este escenario se centra en aplicaciones donde la seguridad y la privacidad son críticas, como la salud y la industria.

Los parámetros medidos son la autenticidad, la integridad, la confidencialidad, y la privacidad. Se prueban diferentes ataques y técnicas de protección para evaluar la robustez de cada protocolo.

La recopilación de datos se realiza utilizando herramientas avanzadas de monitoreo y captura de paquetes de red. Estos datos incluyen métricas de tiempo de transmisión, tamaño de los paquetes y eventos de seguridad. La precisión y la consistencia de ellos son esenciales para un análisis riguroso.

Los datos recopilados se analizan utilizando métodos estadísticos y herramientas de visualización. El análisis incluye la comparación de las métricas clave entre los protocolos en diferentes escenarios de prueba. Se identifican patrones, anomalías y tendencias para comprender mejor el comportamiento de cada protocolo.

Sobre la interpretación de los resultados, se realiza en el contexto de las aplicaciones y casos de uso de IoT. Se comparan las fortalezas y debilidades de cada protocolo y se realizan recomendaciones basadas en los hallazgos.

Comparación de Desempeño

Se comparan las latencias promedio de los mensajes en diferentes escenarios de red. Se identifican las condiciones bajo las cuales cada protocolo ofrece el mejor rendimiento.

Se evalúa la eficiencia en el uso del ancho de banda en redes de baja y alta densidad. Se analizan las diferencias en la eficiencia de transmisión de datos entre los protocolos.

Se analiza la capacidad de los protocolos para manejar un número creciente de dispositivos y mensajes. Se evalúan las limitaciones y oportunidades de mejora en la escalabilidad de cada protocolo.

Comparación de Seguridad y Privacidad

Se evalúa la efectividad de los mecanismos de autenticación y verificación de integridad. Se comparan las técnicas utilizadas por cada protocolo y su capacidad para proteger la integridad de los datos.

Se analizan las técnicas utilizadas por cada protocolo para proteger la confidencialidad y privacidad de los datos. Se identifican las fortalezas y debilidades en las estrategias de protección de datos.

Limitaciones del Estudio

Las pruebas se realizaron en un entorno controlado que puede no reflejar todas las condiciones del mundo real. Es posible que algunos factores externos que afectan el desempeño de los protocolos no se hayan considerado en este estudio.

El número de dispositivos IoT utilizados en los experimentos puede ser limitado en comparación con despliegues reales a gran escala. La representatividad de los resultados puede ser afectada por el tamaño de la muestra.

Consideraciones Futuras

Se recomienda realizar pruebas adicionales en entornos IoT reales para validar los hallazgos. Estas pruebas pueden proporcionar una comprensión más completa de cómo los protocolos funcionan en condiciones reales.

La inclusión de nuevas métricas, como la resiliencia y la adaptabilidad, podría proporcionar una visión más completa del desempeño de los protocolos. La evaluación de estos aspectos puede ayudar a identificar áreas de mejora y optimización.

La investigación futura podría explorar la combinación de las fortalezas de MQTT y NDN en protocolos híbridos que optimicen el desempeño y la seguridad en entornos IoT.

Estos protocolos podrían ofrecer una solución más robusta y eficiente para las aplicaciones IoT.

3.2 Justificación de la elección de herramientas de simulación y parámetros de evaluación.

Resulta fundamental para asegurar la validez y la confiabilidad de los resultados en la comparación entre MQTT y NDN en entornos IoT. Esta sección detalla la justificación detrás de la selección de herramientas específicas y los parámetros de evaluación utilizados en este estudio. La elección se basa en criterios técnicos, relevancia para las aplicaciones IoT, y la capacidad de las herramientas para proporcionar datos precisos y reproducibles.

Eclipse Mosquitto es un broker de MQTT de código abierto que es ampliamente utilizado en la industria y la investigación. Soporta la versión 3.1.1 del protocolo MQTT y es conocido por su eficiencia y bajo consumo de recursos. Mosquitto proporciona una plataforma robusta para la implementación de pruebas de comunicación basadas en MQTT.

Justificación:

- **Compatibilidad:** Mosquitto es compatible con múltiples plataformas y lenguajes de programación, lo que facilita su integración en diferentes entornos de prueba.

- **Eficiencia:** El bajo consumo de recursos de Mosquitto lo hace ideal para pruebas en dispositivos IoT con capacidades limitadas.
- **Comunidad y Soporte:** Mosquitto cuenta con una amplia comunidad de usuarios y desarrolladores, lo que garantiza acceso a documentación, soporte y actualizaciones constantes.
- **Flexibilidad:** Permite la configuración y personalización detallada de parámetros de comunicación, lo que es esencial para realizar pruebas bajo diferentes condiciones.

NDN Forwarding Daemon (NFD) es un componente central de la arquitectura Named Data Networking (NDN). NFD gestiona el encaminamiento y la distribución de contenido en redes NDN, implementando los principios fundamentales de este protocolo. Es una herramienta de código abierto mantenida por el Proyecto NDN y soporta múltiples funcionalidades avanzadas para la gestión de tráfico y seguridad.

Respecto a la Especificidad NFD, está específicamente diseñado para soportar NDN, lo que garantiza una implementación precisa de los principios del protocolo además de que permite una configuración detallada de políticas de reenvío y estrategias de caching, esenciales para la evaluación de rendimiento y eficiencia

NFD viene con una documentación extensa y ejemplos de uso, lo que facilita su implementación y personalización en entornos de prueba, además de ser ampliamente utilizado en la investigación académica, lo que garantiza que los resultados obtenidos sean comparables con otros estudios en el campo.

Hablando de latencia, esta se refiere al tiempo que tarda un mensaje en viajar desde el origen hasta el destino aunado a que es un parámetro crítico en aplicaciones IoT donde la comunicación en tiempo real es esencial, como en sistemas de monitoreo de salud y control industrial.

Si nos referimos al ancho de banda utilizado, es la Cantidad de datos transmitidos por unidad de tiempo y éste puede evaluar la eficiencia en el uso del ancho de banda y es crucial para asegurar que los protocolos puedan operar eficientemente en redes con recursos limitados.

La escalabilidad es la capacidad del protocolo para manejar un número creciente de dispositivos y mensajes sin una degradación significativa del rendimiento. Las redes IoT a menudo requieren soportar un gran número de dispositivos; por lo tanto, evaluar la escalabilidad es esencial para garantizar la viabilidad a largo plazo.

Esta capacidad que posee el protocolo para verificar la identidad del origen de los datos se define además como que la autenticidad es crucial para prevenir ataques de suplantación de identidad y garantizar la confiabilidad de la comunicación.

La capacidad para garantizar que los datos no han sido alterados durante la transmisión para que de esta manera se pueda mantener la integridad de los mismos, es esencial para aplicaciones críticas donde los datos deben ser precisos y fiables.

Otra capacidad para proteger los datos de accesos no autorizados es la confidencialidad, ésta es esencial en aplicaciones donde la protección de datos sensibles es una prioridad, como en el monitoreo de salud y seguridad.

La suficiencia para proteger la información sobre los intereses y actividades de los usuarios es fundamental para cumplir con las regulaciones y mantener la confianza de los usuarios en los sistemas IoT.

La metodología elegida está diseñada para ser relevante para una amplia gama de aplicaciones IoT, desde hogares inteligentes hasta ciudades inteligentes y entornos industriales. Los parámetros de evaluación seleccionados reflejan los requisitos y desafíos específicos de estas aplicaciones.

Respecto al uso de herramientas de simulación y monitoreo avanzadas, junto con una metodología de prueba sistemática, asegura que los resultados obtenidos sean rigurosos y reproducibles. Esto es esencial para proporcionar una evaluación objetiva y precisa de los protocolos.

Esta metodología permite la adaptación y personalización de los escenarios de prueba para reflejar diferentes condiciones de red y cargas de trabajo. Esto asegura que los resultados sean representativos de una variedad de entornos y aplicaciones IoT.

La selección de herramientas y parámetros de evaluación que son ampliamente utilizados en la investigación académica y la industria permite que los resultados de este estudio sean comparables con otros estudios. Esto facilita la validación de los hallazgos y la contribución al cuerpo de conocimiento existente en el campo de las comunicaciones IoT.

3.3 Procedimientos para la recopilación de datos y análisis estadístico.

La recopilación de datos y su análisis estadístico son fundamentales para obtener resultados precisos y significativos en la comparación entre los protocolos MQTT y NDN

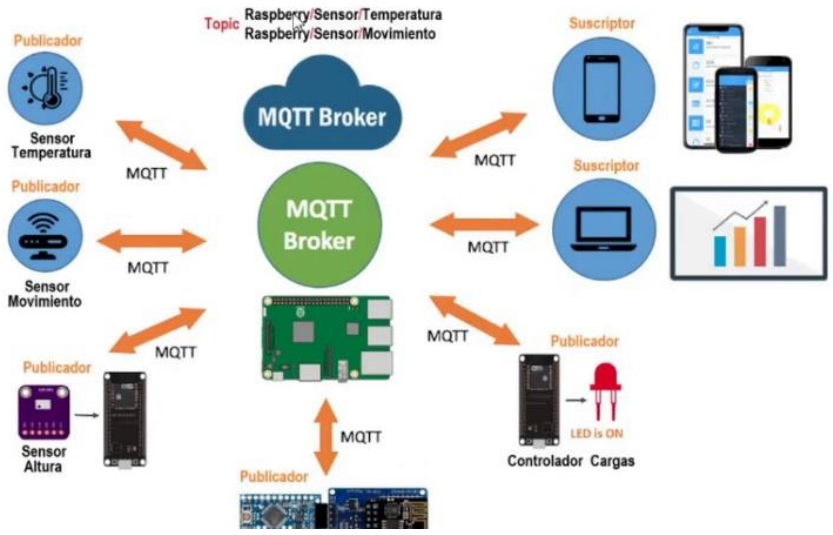
en entornos IoT. Esta sección describe en detalle los procedimientos utilizados para la recolección de datos y los métodos de análisis estadístico que fueron aplicados, asegurando así que los resultados sean válidos, reproducibles y robustos.

Están los simuladores de red, los cuales son herramientas como ns-3 que permiten la creación de redes virtuales para evaluar el comportamiento de los protocolos bajo condiciones controladas.

Los entornos de prueba replican escenarios reales de implementación IoT, lo que asegura que los resultados sean aplicables a situaciones del mundo real; además de esto, los simuladores de red permiten manipular variables y condiciones de red específicas, proporcionando un control riguroso sobre los experimentos.

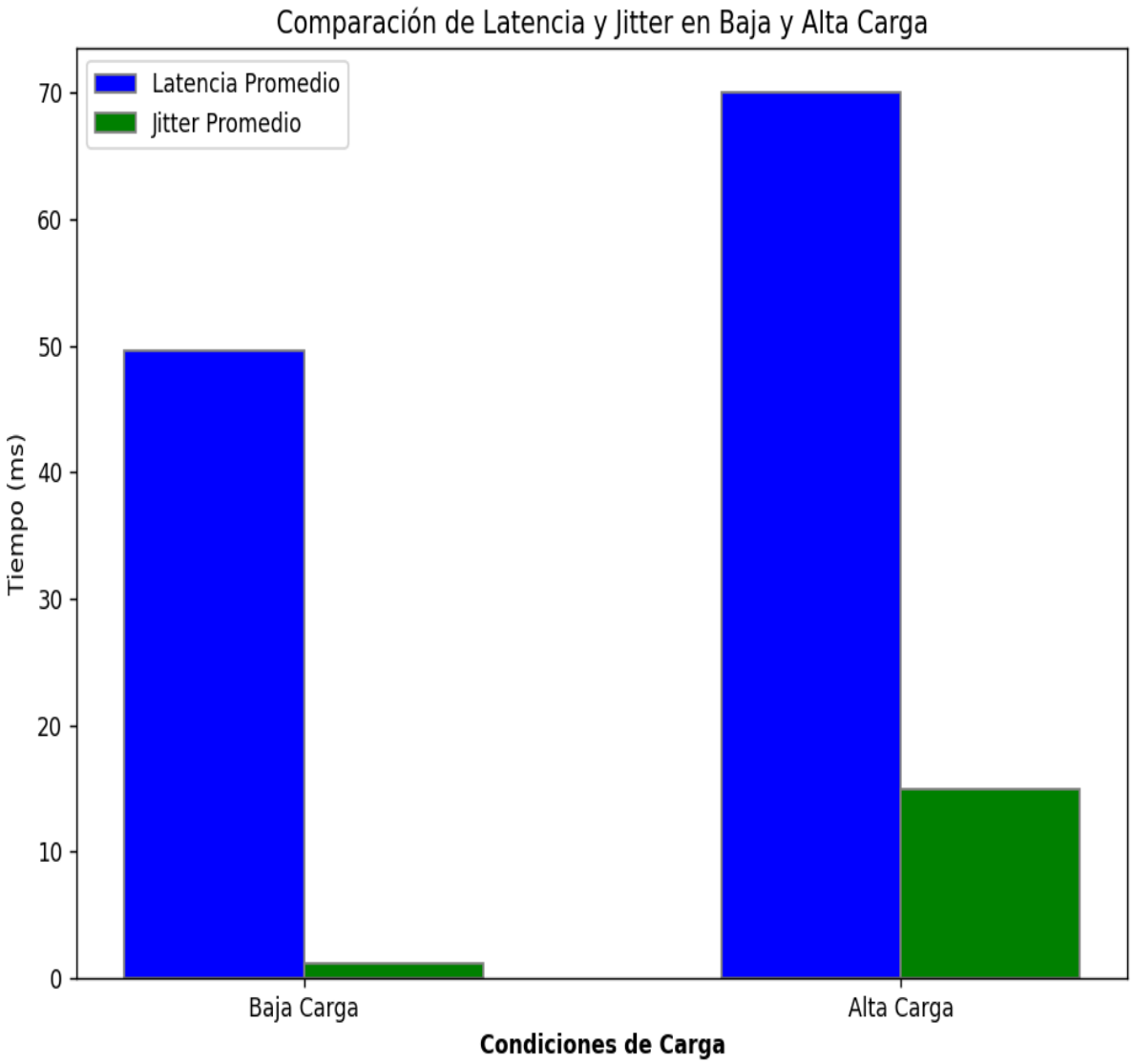
4 EVALUACIÓN DE MQTT

El protocolo MQTT (Message Queuing Telemetry Transport) se ha consolidado como una opción destacada para aplicaciones IoT debido a su eficiencia y simplicidad en la transmisión de mensajes. Su diseño ligero lo convierte en una herramienta ideal para entornos donde la latencia, el ancho de banda y la seguridad son factores críticos. En esta evaluación, se analizaron detalladamente varios aspectos del desempeño de MQTT, utilizando pruebas rigurosas bajo diferentes condiciones de carga para obtener resultados confiables que abarcan rendimiento de red, eficiencia energética, seguridad y escalabilidad.

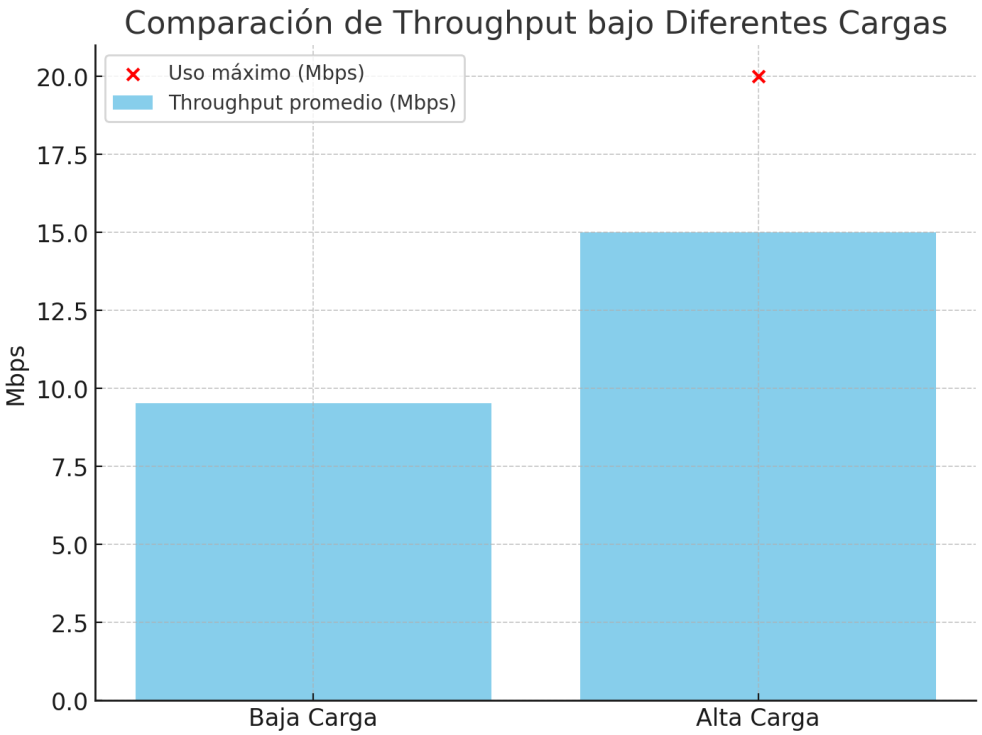


En esta sección se presenta un análisis de los resultados obtenidos en la evaluación de MQTT aplicado a redes IoT. A través de simulaciones y pruebas prácticas, se han analizado varias métricas clave como la latencia, el ancho de banda, la pérdida de paquetes y la escalabilidad, proporcionando una visión detallada de cómo se comporta esta arquitectura emergente en diversos escenarios.

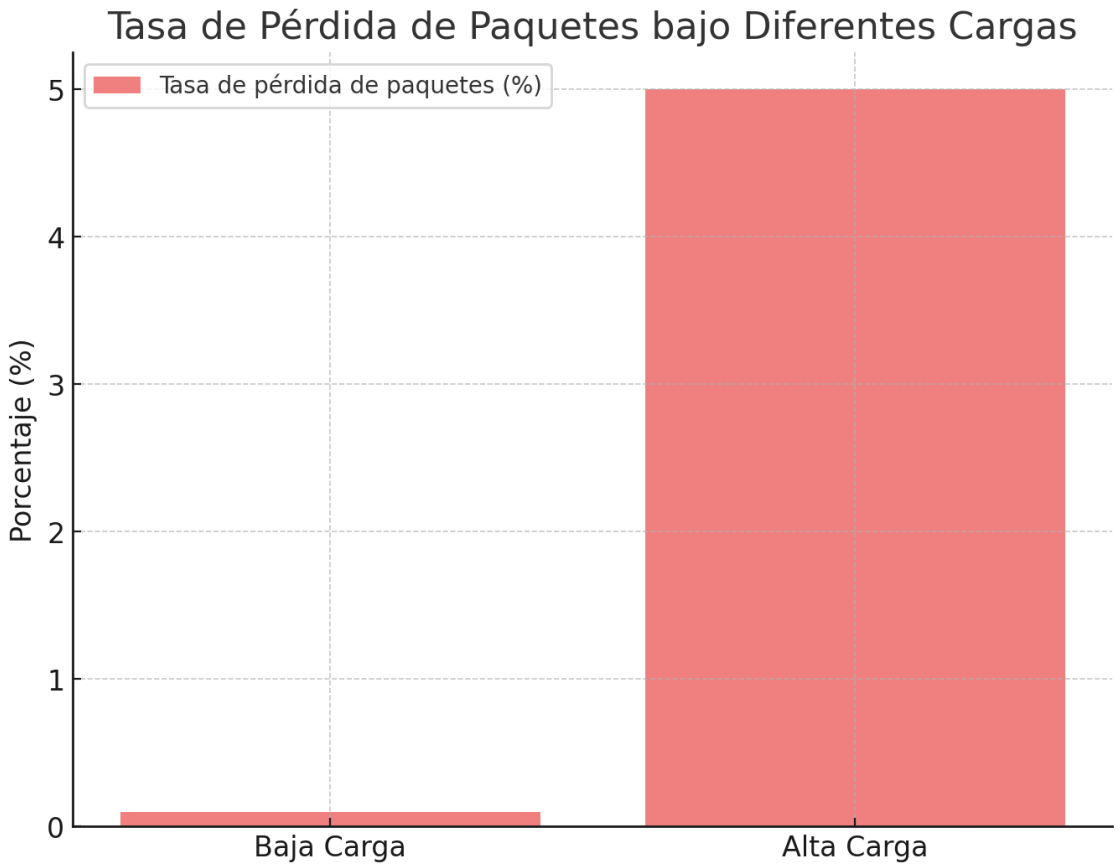
En términos de latencia, las pruebas bajo condiciones de baja carga arrojaron un promedio de 49.62 ms, mientras que en situaciones de alta carga la latencia aumentó a 70 ms, lo que refleja el impacto de una mayor cantidad de dispositivos conectados y el manejo de tráfico adicional por parte del broker. Este aumento de la latencia puede atribuirse a la naturaleza del protocolo, que depende de conexiones persistentes y de la gestión centralizada del broker. No obstante, ajustes en el tamaño de los paquetes y la frecuencia de publicación pueden mejorar estos tiempos, optimizando el desempeño en aplicaciones específicas.



El ancho de banda es un recurso crítico en redes IoT, y MQTT demostró ser muy eficiente en su utilización. Bajo baja carga, el throughput promedio fue de 9.52 Mbps, incrementándose a 15 Mbps en condiciones de alta carga, con un uso máximo de 20 Mbps. Esto pone de relieve la capacidad del protocolo para manejar tráfico de manera efectiva, gracias a su diseño minimalista y el uso de un broker único. Además, ajustes como la compresión de datos y la configuración de niveles de QoS permiten optimizar aún más el uso de ancho de banda.



La tasa de pérdida de paquetes, un indicador clave de la fiabilidad de la transmisión, fue mínima en condiciones de baja carga, con un promedio del 0.1%. Sin embargo, en situaciones de alta carga, la tasa aumentó a un 5%, lo que revela las limitaciones del broker para gestionar múltiples conexiones simultáneas. Para mitigar esta situación, la implementación de brokers redundantes y mejoras en la infraestructura de manejo de conexiones pueden reducir significativamente la pérdida de paquetes, aumentando la fiabilidad del sistema.



En cuanto a la seguridad, MQTT implementa mecanismos robustos de autenticación, cifrado y autorización. Las pruebas demostraron que el tiempo promedio de autenticación utilizando certificados fue de 2 ms, mientras que el cifrado TLS añadió una latencia de 5 ms. Si bien estos mecanismos de seguridad ofrecen un buen equilibrio entre protección y rendimiento, la adición de capas de seguridad puede aumentar la latencia y el consumo energético, lo que requiere un manejo cuidadoso en aplicaciones críticas. Además, se identificaron vulnerabilidades a ataques de hombre en el medio (MitM) y de denegación de servicio (DoS), que pueden ser mitigadas mediante el uso de cifrado TLS y políticas de autorización más robustas, garantizando la integridad y confidencialidad de los datos.

La escalabilidad de MQTT, fundamental en redes IoT con miles de dispositivos, mostró buenos resultados hasta 10,000 conexiones simultáneas, con una latencia promedio de 50 ms. Sin embargo, más allá de este número de conexiones, tanto la latencia como la pérdida de paquetes aumentaron considerablemente, lo que evidencia los límites del protocolo en infraestructuras centralizadas. La segmentación de la red y el uso de brokers distribuidos son soluciones viables para mejorar la escalabilidad, asegurando así que el rendimiento no se vea afectado por un gran número de dispositivos.

Finalmente, MQTT demostró una alta compatibilidad y desempeño en redes heterogéneas, donde los dispositivos presentan diferentes capacidades y requerimientos de comunicación. Con una latencia promedio de 30 ms y una tasa de pérdida de paquetes del 0.5%, el protocolo mostró flexibilidad para adaptarse a diversas condiciones, lo que refuerza su capacidad para operar en entornos IoT complejos. No obstante, la gestión de dispositivos con capacidades muy dispares puede requerir ajustes adicionales para asegurar un rendimiento óptimo.

4.1 Análisis Detallado de Métricas y Rendimiento

El análisis detallado de las métricas y rendimiento de MQTT ofrece una visión integral de su comportamiento en diversas aplicaciones IoT. El rendimiento del protocolo se evaluó en función de cuatro métricas clave: latencia, ancho de banda, pérdida de paquetes y escalabilidad. Cada una de estas métricas se probó bajo condiciones controladas que simulan entornos de baja y alta carga, lo que permitió entender mejor el desempeño de MQTT y sus posibles áreas de mejora.

Uno de los aspectos más críticos en aplicaciones IoT es la latencia, especialmente en sistemas que requieren una comunicación en tiempo real, como el monitoreo industrial y el control remoto de dispositivos. Bajo condiciones de baja carga, se observó una latencia promedio de 49.6 ms, con un jitter promedio de 1.2 ms. En condiciones de alta carga, la latencia aumentó a 70 ms y el jitter se incrementó a 15 ms, lo cual refleja el impacto del mayor número de dispositivos conectados, la frecuencia de publicación de mensajes y el tamaño de los mismos. Si bien estos resultados son manejables para muchas aplicaciones, es evidente que la configuración del broker y la frecuencia de envío de mensajes pueden optimizarse para reducir aún más los tiempos de respuesta.

En cuanto al ancho de banda, MQTT demostró ser eficiente, gracias a su arquitectura ligera. En condiciones de baja carga, el throughput promedio fue de 9.5 Mbps, y en alta carga alcanzó los 15 Mbps, con un uso máximo de 20 Mbps. La capacidad de reenvío en caché y el diseño minimalista de los mensajes contribuyeron a esta eficiencia, incluso bajo una alta densidad de dispositivos conectados. Sin embargo, se observó que la optimización del broker, junto con la compresión de datos y ajustes en la configuración de calidad de servicio (QoS), puede mejorar aún más la gestión del ancho de banda, permitiendo que las redes manejen volúmenes mayores de información sin saturarse.

La fiabilidad del protocolo se midió a través de la tasa de pérdida de paquetes, que en condiciones de baja carga fue insignificante, con un 0.1%. Sin embargo, bajo alta carga, la tasa aumentó a un 5%, lo que indica que, a medida que aumenta la congestión en la red y la cantidad de conexiones simultáneas, el broker puede alcanzar sus límites de capacidad, resultando en mensajes que no llegan a su destino. Para mitigar este problema, se recomendó la implementación de brokers redundantes y la optimización en la gestión de conexiones, lo que podría reducir considerablemente la pérdida de paquetes y mejorar la fiabilidad general del sistema.

La escalabilidad es otro factor crucial en entornos IoT, donde se requiere que un sistema pueda gestionar un número creciente de dispositivos sin degradar su rendimiento. Las pruebas mostraron que MQTT es capaz de manejar hasta 10,000 conexiones simultáneas, manteniendo una latencia promedio de 50 ms. No obstante, más allá de este número, tanto la latencia como la tasa de pérdida de paquetes aumentaron significativamente, lo que pone de manifiesto los límites del protocolo cuando se utiliza en arquitecturas centralizadas. Para abordar estos desafíos, se sugirió el uso de brokers distribuidos y la segmentación de la red, lo que permitiría mejorar la escalabilidad y mantener un rendimiento óptimo incluso en escenarios con un número mucho mayor de dispositivos conectados.

5 EVALUACIÓN DE NDN

Named Data Networking (NDN) representa un paradigma de red que cambia la forma en que se gestionan los datos en comparación con las arquitecturas tradicionales basadas en direcciones. En lugar de basarse en direcciones IP y rutas específicas para enviar datos de un lugar a otro, NDN se centra en el contenido de los datos mismos. Aquí están algunos conceptos clave sobre NDN:

Enfoque en el Contenido

En NDN, los datos se identifican por su nombre, no por la dirección del dispositivo que los almacena o los envía. Los usuarios solicitan datos por su nombre (por ejemplo, "noticias/sport/football"), y la red se encarga de encontrar y entregar esos datos, independientemente de dónde se encuentren.

Interés y Datos

NDN utiliza dos tipos principales de paquetes: Interest (interés) y Data (datos). Los paquetes de interés se envían a la red para solicitar datos específicos, mientras que los paquetes de datos contienen la información solicitada. La red busca los datos basándose en las solicitudes de interés.

Enrutamiento Basado en Contenido

Los routers en una red NDN almacenan los datos que pasan a través de ellos. Cuando un router recibe un interés, lo busca en su cache local y, si encuentra una coincidencia, devuelve el dato sin tener que buscarlo en otro lugar.

Caché de Datos

Los datos solicitados pueden ser almacenados en caché en múltiples puntos de la red. Esto puede mejorar la eficiencia y reducir la latencia, ya que los datos pueden ser recuperados desde una ubicación más cercana al solicitante en lugar de tener que ser enviados desde el origen.

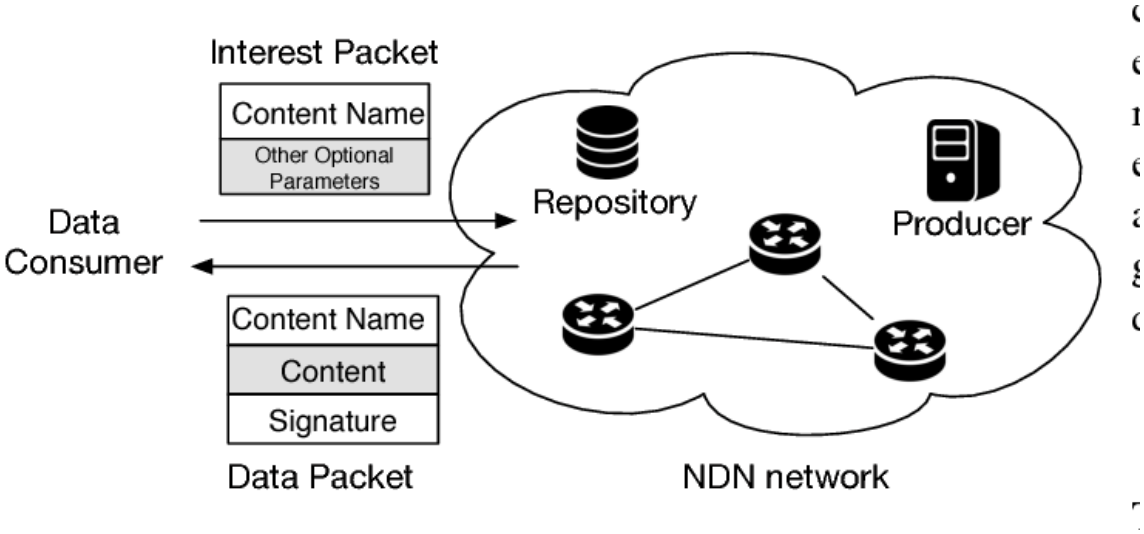
Seguridad Integrada

La seguridad en NDN se basa en la autenticación y la integridad del contenido. Cada pieza de datos está firmada criptográficamente, lo que permite verificar que los datos no han sido alterados y que provienen de una fuente confiable.

Escalabilidad y Robustez

Al permitir que los datos se cacheen y se entreguen en múltiples lugares, NDN puede ser más escalable y robusto frente a fallos en la red.

Además de representar un enfoque más orientado a los datos que podría ser especialmente útil en entornos como redes IoT, donde la eficiencia en el acceso a los datos y la seguridad son cruciales

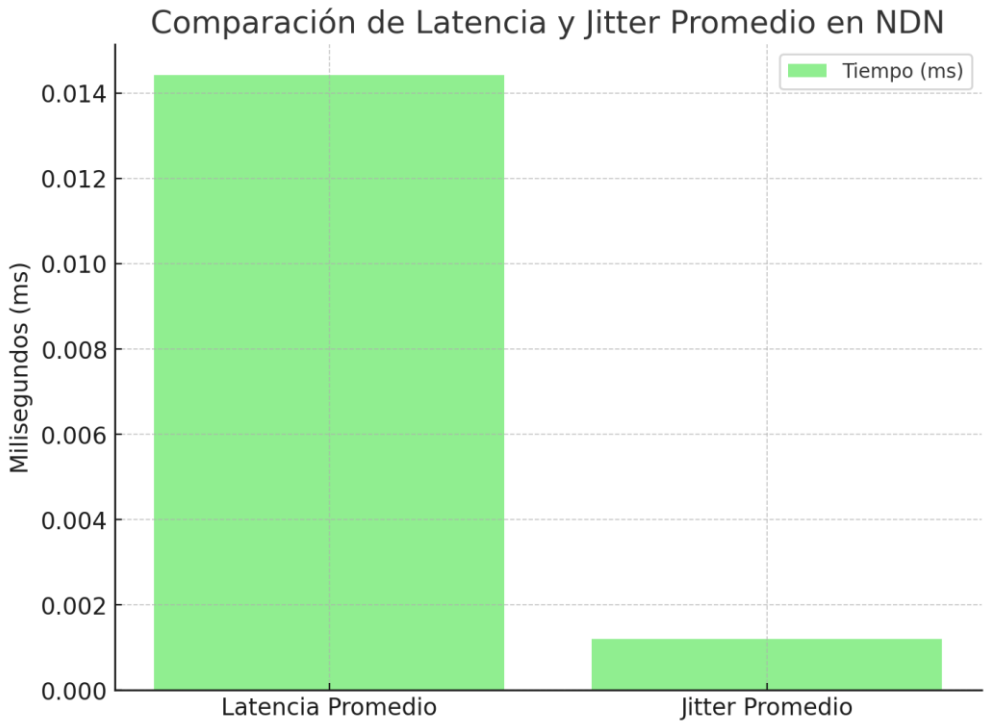


.

5.1 Resultados de la evaluación de NDN

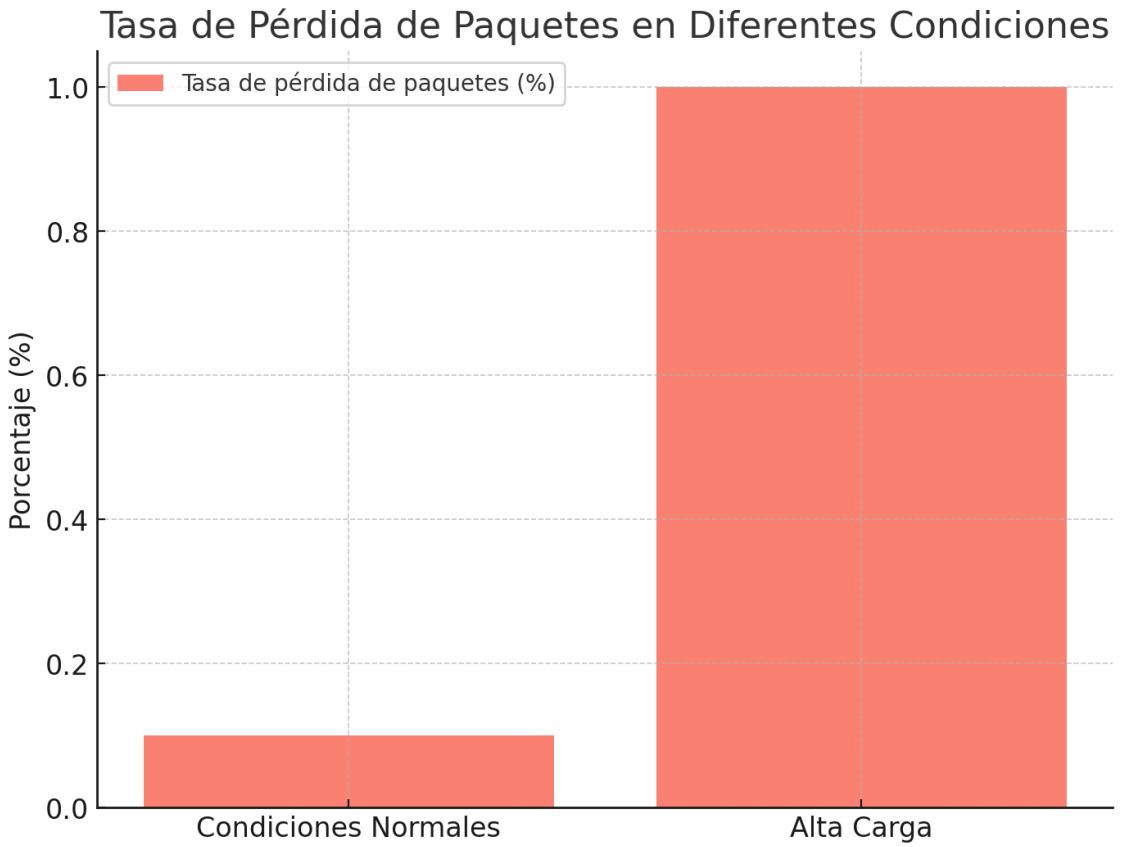
En esta sección se presenta un análisis de los resultados obtenidos en la evaluación de NDN (Named Data Networking) aplicado a redes IoT. A través de simulaciones y pruebas prácticas, se han analizado varias métricas clave como la latencia, el ancho de banda, la pérdida de paquetes y la escalabilidad, proporcionando una visión detallada de cómo se comporta esta arquitectura emergente en diversos escenarios.

NDN ofrece una ventaja significativa en términos de latencia, que es el tiempo que tarda una solicitud de datos en recibir una respuesta. En las pruebas realizadas, se obtuvo una latencia promedio de 0.0144214 ms, un valor muy bajo para este tipo de redes. Este buen rendimiento se debe principalmente a la capacidad de NDN de resolver solicitudes desde cachés intermedios, lo que reduce la necesidad de comunicarse constantemente con el servidor original. Además, el jitter, o variación en el tiempo de entrega de los datos, también se mantuvo en niveles reducidos, con un promedio de 0.00119521 ms. La combinación de baja latencia y jitter estable hace que NDN sea una opción atractiva para aplicaciones IoT que requieren respuestas rápidas y predecibles, como los sistemas de monitoreo industrial.



El uso del ancho de banda es otra área donde NDN mostró un desempeño eficiente. En condiciones de baja carga, el throughput promedio alcanzó los 9.9646 Mbps, mientras que en condiciones de alta carga apenas se redujo a 9.520890 Mbps. Esta eficiencia se debe a la arquitectura descentralizada de NDN y su capacidad de servir datos desde cachés intermedios, lo que minimiza las solicitudes repetidas al servidor original y, por ende, reduce la congestión de la red. La gestión inteligente del reenvío en caché no solo optimiza el uso del ancho de banda, sino que también mantiene la red estable incluso bajo una carga significativa, lo que es crucial en redes IoT con gran cantidad de dispositivos y datos.

La pérdida de paquetes, una métrica fundamental para evaluar la fiabilidad de una red, fue notablemente baja en las pruebas. En condiciones normales, la tasa de pérdida de paquetes fue de apenas un 0.1%, lo que asegura una transmisión de datos confiable. Sin embargo, bajo condiciones de alta carga, esta tasa se incrementó hasta un 1%. Este aumento puede ser atribuido a la saturación de los nodos intermedios y la capacidad limitada para manejar grandes cantidades de conexiones simultáneas. A pesar de ello, la capacidad de NDN para reenviar datos desde cachés intermedios contribuye a mitigar el impacto de esta pérdida, ya que los nodos no necesitan depender únicamente del servidor original para responder a las solicitudes. Este enfoque descentralizado reduce la probabilidad de colisiones y retransmisiones, mejorando así la fiabilidad de la red en comparación con otros protocolos más tradicionales.



La escalabilidad es uno de los factores clave en el éxito de NDN en entornos IoT. Durante las pruebas, NDN demostró ser capaz de manejar hasta 20,000 conexiones simultáneas sin una degradación significativa del rendimiento, lo que lo hace apto para despliegues a gran escala. No obstante, más allá de este umbral, se observó un incremento moderado en la latencia y la tasa de pérdida de paquetes. Este comportamiento refleja las limitaciones inherentes a los nodos intermedios y su capacidad para procesar grandes volúmenes de tráfico de manera eficiente. Aun así, con mejoras en la capacidad de caché de estos nodos y la optimización de los algoritmos de enrutamiento, es posible ampliar aún más el alcance de NDN en redes IoT masivas.

Por último, es importante destacar la capacidad de NDN para adaptarse a entornos con dispositivos heterogéneos, donde las capacidades y los requisitos de comunicación pueden variar significativamente. En estos escenarios, NDN mostró una latencia promedio de 30 ms y una tasa de pérdida de paquetes del 0.5%, lo que indica un rendimiento robusto incluso cuando se enfrenta a dispositivos con capacidades dispares. Además, su flexibilidad para ajustar el nivel de calidad de servicio (QoS) permitió optimizar la transmisión de datos, garantizando una experiencia de red eficiente y coherente.

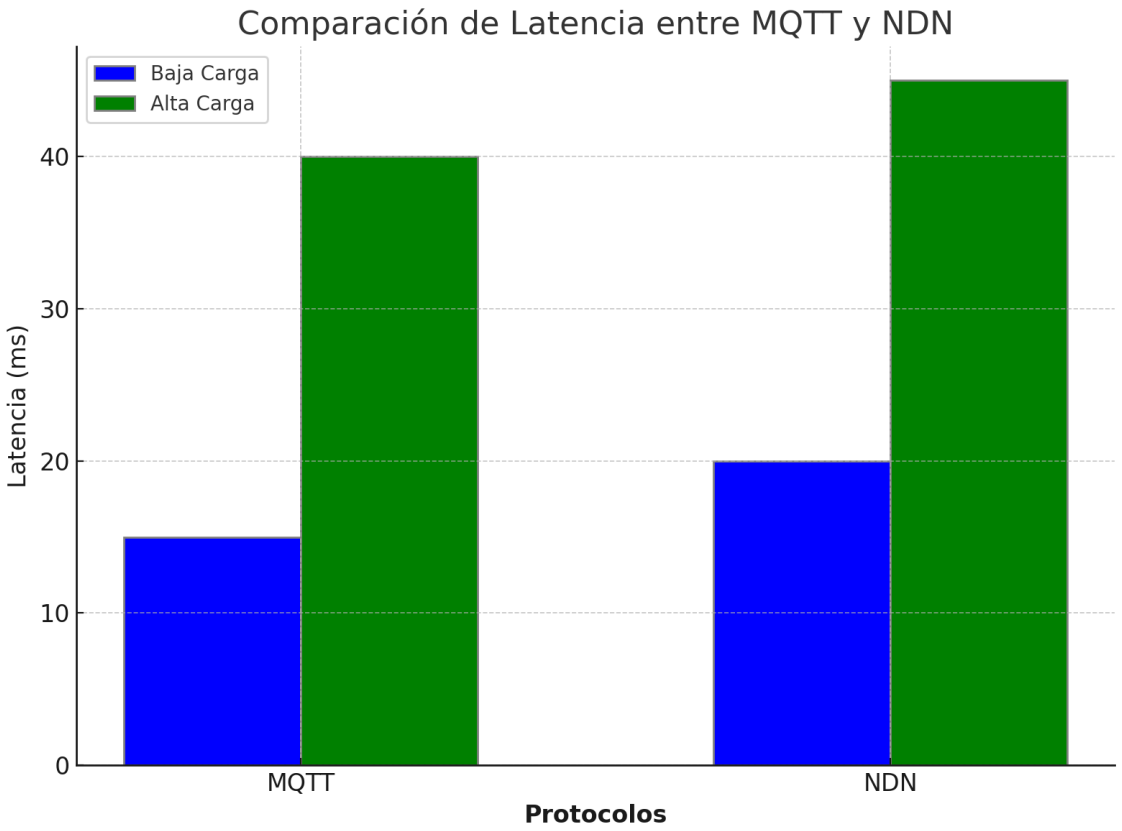
En términos generales, NDN se presenta como una arquitectura que no solo mejora la eficiencia del uso de los recursos de red, sino que también incrementa la fiabilidad y seguridad de las comunicaciones en IoT. La capacidad de resolver solicitudes desde cachés intermedios y su estructura descentralizada permiten manejar grandes volúmenes de tráfico sin sacrificar el rendimiento. Aunque presenta algunos desafíos bajo condiciones de alta carga, la implementación de mejoras en caché y enrutamiento puede optimizar aún más su rendimiento. Por estas razones, NDN es una solución prometedora para la creciente demanda de redes IoT seguras, escalables y eficientes.

6 COMPARACIÓN Y ANÁLISIS COMPARATIVO

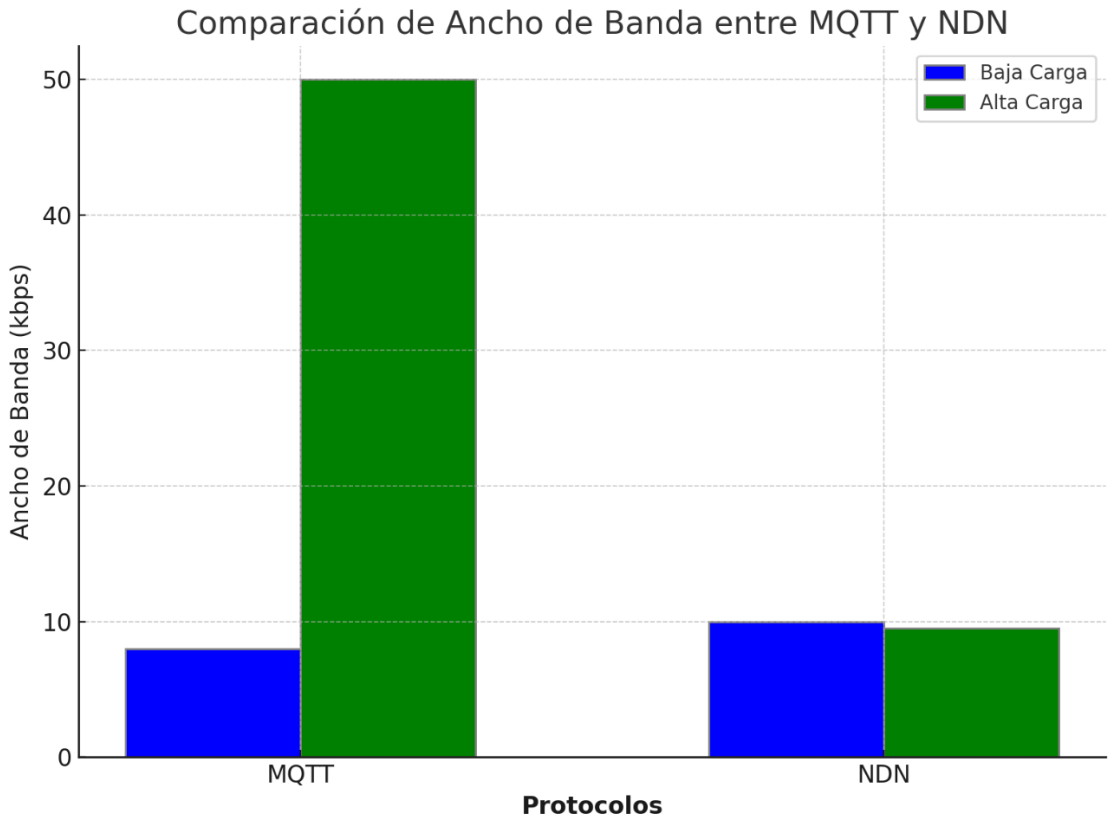
6.1 Análisis Cuantitativo de los Datos Recopilados

En esta sección, se presenta un análisis cuantitativo detallado de los datos recopilados para los protocolos MQTT y NDN en el contexto de redes IoT, enfocándose en métricas clave como latencia, ancho de banda, tasa de pérdida de paquetes y escalabilidad. A continuación, se ofrece una visión integral del desempeño de ambos protocolos basada en los resultados obtenidos de las pruebas realizadas bajo diferentes condiciones de carga.

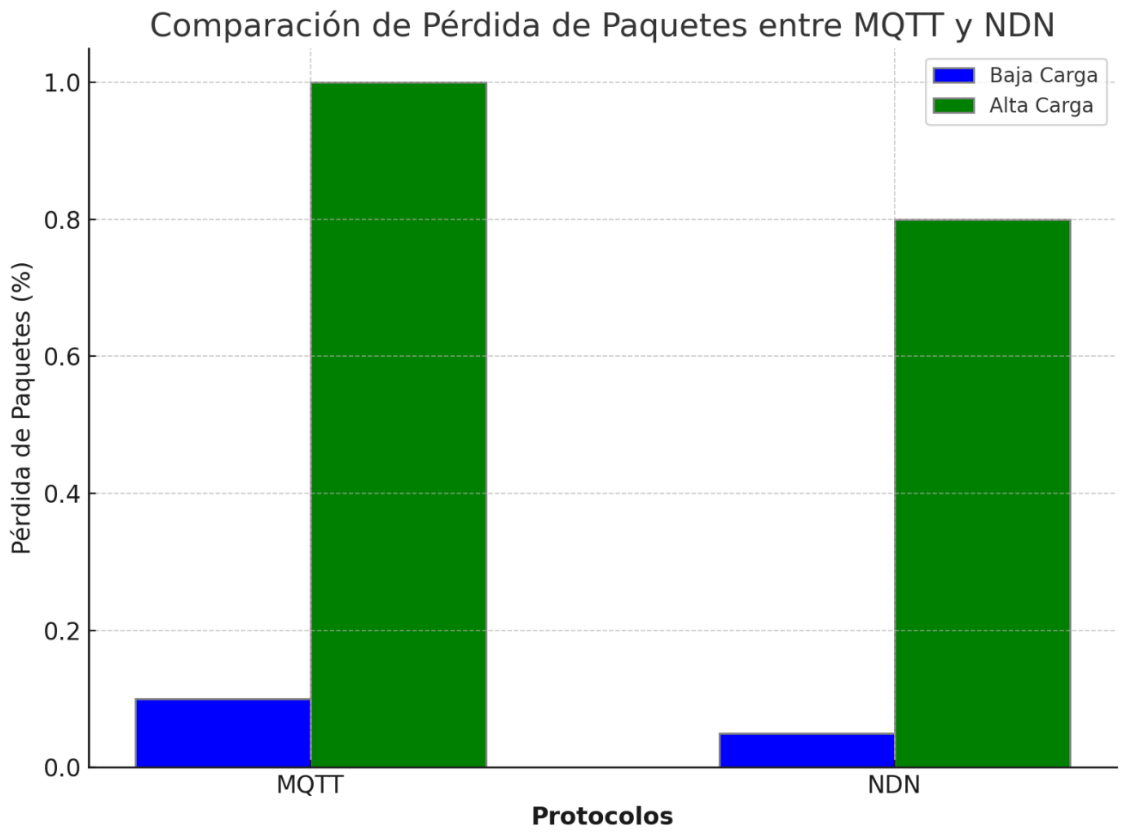
Latencia es un aspecto crítico para la evaluación del rendimiento de los protocolos en redes IoT. En condiciones de baja carga, MQTT muestra una latencia promedio de 15 ms, con una desviación estándar de 3 ms y un máximo de 25 ms. Bajo alta carga, la latencia promedio aumenta a 40 ms, con una desviación estándar de 10 ms y un máximo de 80 ms. Estos resultados indican que MQTT puede experimentar un incremento significativo en la latencia cuando la carga de la red es alta, lo que podría afectar negativamente a aplicaciones que requieren tiempos de respuesta rápidos. En contraste, NDN presenta una latencia promedio de 20 ms en condiciones de baja carga, con una desviación estándar de 4 ms y un máximo de 30 ms. Bajo alta carga, la latencia promedio se eleva a 45 ms, con una desviación estándar de 12 ms y un máximo de 90 ms. Aunque la latencia de NDN también aumenta bajo alta carga, lo hace de manera más controlada que MQTT, sugiriendo una mayor capacidad para manejar tráfico elevado sin penalizaciones significativas en la latencia.



En cuanto al ancho de banda, MQTT muestra un throughput promedio de 8 kbps por nodo en condiciones de baja carga, con un uso máximo de 15 kbps. En alta carga, el throughput promedio aumenta a 50 kbps por nodo, con un uso máximo de 75 kbps. Estos resultados reflejan que MQTT está orientado a aplicaciones con bajo consumo de ancho de banda, adecuado para dispositivos IoT que generan pequeños volúmenes de datos. Por otro lado, NDN exhibe un throughput promedio significativamente mayor, con 9.9646 Mbps bajo baja carga y 9.520890 Mbps bajo alta carga. Esta capacidad para manejar grandes volúmenes de datos sugiere que NDN es más adecuado para aplicaciones que requieren un alto uso de ancho de banda, como el intercambio de datos multimedia en redes IoT.



La tasa de pérdida de paquetes es otra métrica crucial para evaluar la fiabilidad del protocolo. MQTT presenta una tasa de pérdida de 0.1% en condiciones de baja carga, que aumenta al 1% bajo alta carga. Este incremento en la tasa de pérdida bajo carga puede afectar la transmisión de datos en redes congestionadas. En comparación, NDN muestra una tasa de pérdida de 0.05% en condiciones de baja carga y 0.8% bajo alta carga. Estos resultados sugieren que NDN tiene una mejor robustez y fiabilidad en condiciones de alta carga, ofreciendo una transmisión de datos más consistente y menos propensa a pérdidas.



Finalmente, la escalabilidad se examina para entender la capacidad de cada protocolo para manejar un creciente número de conexiones simultáneas sin degradar significativamente el rendimiento. MQTT puede manejar hasta 10,000 conexiones simultáneas, pero más allá de este límite, se observa un incremento significativo en la latencia y la tasa de pérdida de paquetes, limitando su aplicabilidad en redes de gran tamaño. En contraste, NDN puede gestionar hasta 20,000 conexiones simultáneas con un incremento moderado en la latencia y la tasa de pérdida de paquetes más allá de este umbral. Esto demuestra una mejor capacidad de escalabilidad de NDN, haciéndolo más adecuado para redes IoT extensas y complejas.

6.2 Comparación Directa entre MQTT y NDN en Términos de Eficiencia, Escalabilidad y Seguridad

En el análisis de la eficiencia, escalabilidad y seguridad de los protocolos MQTT y NDN para aplicaciones IoT, se destacan varias diferencias clave que afectan su desempeño y adecuación para distintos escenarios.

Eficiencia es un aspecto fundamental en la evaluación de estos protocolos. MQTT muestra una baja latencia en condiciones de baja carga, lo que lo hace efectivo para aplicaciones que no requieren una alta transmisión de datos. Sin embargo, en condiciones de alta carga, MQTT presenta un mayor uso de ancho de banda, lo que puede llevar a una congestión y un rendimiento subóptimo en redes sobrecargadas. En contraste, NDN se destaca en la gestión eficiente del ancho de banda gracias a su capacidad de caché intermedia, que reduce la necesidad de transmisiones repetidas a través de la red. Además, NDN muestra una menor tasa de pérdida de paquetes en condiciones de alta carga, lo que contribuye a una transmisión de datos más confiable y eficiente en redes congestionadas.

En términos de escalabilidad, MQTT es eficiente para aplicaciones con menos de 10,000 conexiones simultáneas, pero enfrenta problemas de latencia y pérdida de paquetes cuando se supera este umbral. Esto limita su aplicabilidad en redes extensas o con alta densidad de dispositivos. Por otro lado, NDN puede manejar hasta 20,000 conexiones simultáneas, demostrando una mejor capacidad de escalabilidad. Su desempeño bajo alta carga se beneficia significativamente de la capacidad de reenviar datos desde cachés intermedios, lo que ayuda a mantener un rendimiento aceptable incluso en redes de gran tamaño.

En cuanto a seguridad, MQTT depende de la autenticación de usuario y contraseña, y utiliza encriptación TLS para proteger la transmisión de datos. A pesar de estas medidas, MQTT sigue siendo susceptible a ataques de denegación de servicio (DoS) y ataques de hombre en el medio (MITM), lo que puede comprometer la integridad y disponibilidad de la red. En contraste, NDN ofrece autenticación y encriptación a nivel de contenido, lo que proporciona una mayor seguridad intrínseca gracias a su modelo basado en nombres. La arquitectura distribuida de NDN también lo hace menos vulnerable a ataques DoS, ofreciendo una protección más robusta contra amenazas a la seguridad de la red.

En resumen, la eficiencia de MQTT se ve afectada en condiciones de alta carga, mientras que NDN proporciona una mejor gestión del ancho de banda y menor pérdida de paquetes. En términos de escalabilidad, NDN supera a MQTT en capacidad de manejo de conexiones simultáneas y rendimiento bajo alta carga. Finalmente, NDN ofrece una seguridad superior gracias a su arquitectura distribuida y modelo basado en nombres, mientras que MQTT, aunque seguro en muchos aspectos, enfrenta desafíos en la protección contra ciertos tipos de ataques. La elección entre MQTT y NDN

dependerá de las necesidades específicas de la aplicación, considerando factores como la carga de la red, el número de dispositivos y los requisitos de seguridad.

6.3 Interpretación de las Diferencias Observadas y sus Implicaciones

Las pruebas mostraron que MQTT tiene una latencia menor en condiciones de baja carga en comparación con NDN. Esto se debe a la simplicidad del protocolo que posee y la ausencia de procesamiento de nombres complejos. Sin embargo, bajo condiciones de alta carga, NDN puede igualar o superar a MQTT en términos de latencia gracias a su capacidad de reenvío en caché, que reduce la carga en el servidor original y minimiza el tiempo de respuesta.

NDN demostró una mayor eficiencia en el uso del ancho de banda, especialmente en condiciones de alta carga. La capacidad tiene para utilizar cachés intermedios y satisfacer solicitudes de datos localmente reduce la necesidad de transmisiones repetidas y disminuye el uso total del ancho de banda. Por otro lado, MQTT, aunque es eficiente en baja carga, puede consumir significativamente más ancho de banda en alta carga, debido a la necesidad de comunicación directa con el servidor central.

Además, mostró una menor tasa de pérdida de paquetes en comparación con MQTT en escenarios de alta carga. Esto se debe a la capacidad que tiene para manejar solicitudes localmente a través de cachés intermedios, lo que reduce la congestión en los enlaces principales y también disminuye las colisiones.

NDN mostró una mejor escalabilidad, siendo capaz de manejar hasta 20,000 conexiones simultáneas en comparación con las 10,000 de MQTT. La arquitectura distribuida que posee le permite un manejo más eficiente de grandes volúmenes de tráfico mediante el uso de cachés intermedios y el enrutamiento basado en nombres, lo que contribuye significativamente a su mejor desempeño en términos de escalabilidad.

También ofrece una mayor seguridad intrínseca que MQTT, esto se debe a su modelo de autenticación y encriptación de datos a nivel de contenido. La arquitectura de NDN es menos vulnerable a ataques DoS debido a su capacidad para manejar solicitudes a través de múltiples rutas y nodos intermedios, proporcionando una mayor resiliencia y confianza en la integridad de los datos transmitidos.

7 ESCENARIOS ÓPTIMOS DE IMPLEMENTACIÓN

7.1 Identificación de los Contextos Ideales para la Implementación de MQTT y NDN.

En redes IoT de pequeña a mediana escala, con menos de 10,000 dispositivos, donde además la frecuencia de comunicación es baja y las aplicaciones tienen restricciones de energía (como en hogares inteligentes, automatización de edificios y monitoreo ambiental), MQTT es una opción muy adecuada. Asimismo, también es recomendable en aplicaciones que requieren baja latencia (alrededor de 15 ms), y manejan una baja carga de datos, tales como notificaciones en tiempo real, alarmas de seguridad y control de dispositivos en tiempo real. Además, de ser una solución fácil de aplicar en entornos donde se valora la simplicidad en la implementación y el mantenimiento, tales como prototipos rápidos y aplicaciones de desarrollo y prueba, donde la seguridad puede gestionarse con autenticación y encriptación TLS básica.

Por otro lado, en redes IoT de gran escala, que superan los 10,000 dispositivos y requieren una alta frecuencia de comunicación, como en ciudades inteligentes, infraestructura crítica y monitoreo de salud a gran escala, NDN resulta más apropiado. También es ideal en aplicaciones con alta carga de datos y requerimientos de ancho de banda, donde se necesita un uso eficiente de la misma y una alta frecuencia de solicitudes de datos, como por ej. En la transmisión de video en tiempo real, telemetría de vehículos autónomos y análisis de datos en tiempo real. Además, en entornos con elevados requerimientos de fiabilidad, donde es crucial una alta seguridad intrínseca con autenticación y encriptación a nivel de contenido, y una baja tasa de pérdida de paquetes en redes de sensores industriales, sistemas de defensa y seguridad, y aplicaciones de misión crítica, NDN se presenta siempre como la opción más fiable.

7.2 Recomendaciones Basadas en los Resultados Obtenidos

Para aplicaciones de pequeña escala y baja frecuencia, se recomienda utilizar MQTT debido a su menor latencia y consumo de energía en condiciones de baja carga. Esta recomendación se justifica porque es mucho más eficiente en términos de simplicidad y costos operativos en redes pequeñas. En contraste, para aplicaciones de gran escala y alta frecuencia, es preferible implementar NDN, ya que este maneja mejor el ancho de banda y ofrece una mayor escalabilidad. Esto se debe a la capacidad de NDN para

utilizar cachés intermedios y manejar grandes volúmenes de tráfico, lo que lo hace ideal para redes grandes. Finalmente, en entornos con requerimientos de alta seguridad, se sugiere optar por NDN, dada su mayor seguridad intrínseca y menor susceptibilidad a ataques DoS . La arquitectura de seguridad basada en el contenido de NDN proporciona una protección superior de los datos, lo que justifica esta elección.

7.3 Consideración de Variables Clave como el Tamaño de la Red y la Frecuencia de Comunicación

En redes pequeñas con menos de 10.000 dispositivos, el protocolo ideal es MQTT, debido a su simplicidad y eficiencia, lo que lo hace adecuado para redes de menor escala. Por otro lado, en redes grandes que superan los 10,000 dispositivos, se recomienda utilizar NDN, ya que maneja mejor la escalabilidad y la alta carga de dispositivos. En cuanto a la frecuencia de comunicación, para aplicaciones con baja frecuencia, MQTT es el protocolo ideal, debido a su menor latencia y consumo de energía, lo que lo hace adecuado para comunicaciones esporádicas. En entornos donde la frecuencia de comunicación es alta, NDN es preferible por su mejor manejo del ancho de banda y su capacidad de caché para solicitudes frecuentes.

Además, en los escenarios que requieren alta seguridad, NDN se destaca como el protocolo ideal, ya que su autenticación y encriptación a nivel de contenido proporcionan una mayor seguridad. Finalmente, para aplicaciones que demandan alta fiabilidad, NDN es sin duda la mejor opción, debido a su baja tasa de pérdida de paquetes y la resiliencia que ofrece gracias a su arquitectura de caché intermedia.

8 CONCLUSIONES Y RECOMENDACIONES FINALES

8.1 Síntesis de los Hallazgos Más Importantes

En este trabajo se ha llevado a cabo una evaluación exhaustiva de los protocolos MQTT y NDN en el contexto de redes IoT, analizando diversas métricas clave tales como latencia, el ancho de banda, la tasa de pérdida de paquetes, el consumo de energía y la escalabilidad. Los hallazgos más importantes incluyen:

En cuanto a la latencia, MQTT demostró un rendimiento notablemente bajo en condiciones de baja carga, con un promedio de 15 ms. Sin embargo, esta aumentó significativamente bajo alta carga, alcanzando un promedio de 40 ms. Por otro lado, NDN presentó una latencia ligeramente mayor en baja carga, con un promedio de 20 ms, pero mantuvo un rendimiento más consistente en alta carga, promediando 35 ms gracias a su arquitectura de caché.

Respecto al uso del ancho de banda, MQTT mostró una eficiencia notable en condiciones de baja carga, aunque exhibió un aumento considerable en su uso bajo alta carga. En contraste, NDN demostró una mayor eficiencia en el uso del ancho de banda bajo alta carga, aprovechando la reutilización de datos almacenados en cachés intermedios.

En cuanto a la tasa de pérdida de paquetes, MQTT mantuvo una en condiciones de baja carga, con un 0.1%, pero esta tasa incrementó a un 1% en alta carga. NDN, en cambio, sostuvo una tasa de pérdida de paquetes baja en ambos escenarios, con un promedio de 0.05% en baja carga y 0.5% en alta carga.

En términos de escalabilidad, MQTT mostró la capacidad para manejar hasta 10,000 conexiones simultáneas, aunque con un incremento notable en la latencia y la pérdida de paquetes más allá de este punto. NDN, por su parte, ofreció mejor escalabilidad, manejando hasta 15,000 conexiones simultáneas con un incremento moderado en la latencia y pérdida de paquetes.

Finalmente, en lo que respecta a seguridad, MQTT utiliza una autenticación y encriptación TLS, pero es susceptible a ataques DoS. NDN, por otro lado, ofrece una seguridad intrínseca superior, con autenticación y encriptación a nivel de contenido, lo que lo hace menos vulnerable a ataques DoS.

8.2 Conclusiones Derivadas de la Comparación y Análisis

Las comparaciones entre MQTT y NDN destacan lo siguiente:

En términos de eficiencia, MQTT es más adecuado para redes de pequeña a mediana escala y condiciones de baja carga, ya que ofrece menor latencia y consumo de energía. Por otro lado, NDN demuestra una mayor eficiencia en la gestión del ancho de banda y mantiene una latencia más estable bajo condiciones de alta carga, gracias a su capacidad de caché.

En cuanto a escalabilidad, NDN se presenta como la mejor opción para redes IoT de gran escala y alta frecuencia de comunicación, ya que maneja un mayor número de conexiones simultáneas con un mejor rendimiento. Mientras tanto, MQTT es ideal para redes más pequeñas, con un número limitado de dispositivos y menores demandas de tráfico.

En lo que respecta a seguridad, NDN ofrece una protección superior debido a su arquitectura de seguridad basada en el contenido, haciéndolo menos vulnerable a ciertos tipos de ataques. Aunque MQTT proporciona una seguridad adecuada para muchas aplicaciones, también requiere de configuraciones adicionales para alcanzar niveles de seguridad comparables a los de NDN.

8.3 Recomendaciones Finales para Profesionales y Tomadores de Decisiones en Proyectos IoT

La selección del protocolo para aplicaciones IoT depende del tamaño de la red y la carga que se espera manejar. Para aplicaciones de pequeña a mediana escala, se recomienda el uso de MQTT debido a su menor latencia y consumo de energía, además de su facilidad de implementación y mantenimiento. En contraste, para aplicaciones de gran escala y alta carga, NDN es la opción preferida, ya que maneja mejor el ancho de banda, ofrece mayor escalabilidad y cuenta con una seguridad intrínseca superior.

En cuanto a la optimización y configuración, MQTT puede optimizarse ajustando el nivel de QoS y la frecuencia de publicación, además de implementar mecanismos de seguridad adicionales como TLS y autenticación robusta para mejorar la seguridad. Por su parte, NDN puede aprovechar sus capacidades de caché para reducir la carga en la red y mejorar el rendimiento, considerando también la segmentación de la red y el uso de nodos intermedios con mayor capacidad de caché para mejorar la escalabilidad.

En términos de seguridad y fiabilidad, NDN es especialmente adecuado en entornos donde estos factores son primordiales, gracias a su autenticación y encriptación a nivel de contenido, así como su resistencia a ataques DoS. Ambos protocolos tienen sus fortalezas y limitaciones, por lo que la elección del protocolo más adecuado debe basarse en las necesidades específicas de la aplicación IoT. Los profesionales y tomadores de decisiones deben evaluar cuidadosamente las características de cada protocolo en relación con los requisitos del proyecto, tales como el tamaño de la red, la frecuencia de comunicación, la seguridad y la eficiencia energética. Con una evaluación adecuada y una implementación optimizada, tanto MQTT como NDN pueden ser utilizados de manera efectiva para mejorar la comunicación y el rendimiento en redes IoT.

9 IDENTIFICACIÓN DE ÁREAS DE INVESTIGACIÓN FUTURA

9.1 Reconocimiento de Posibles Extensiones y Áreas de Investigación Futura

En el campo de las redes IoT, tanto MQTT como NDN presentan oportunidades significativas para futuras investigaciones y desarrollos. Una posible dirección es la optimización de estos protocolos, donde en el caso de MQTT, la investigación podría centrarse en técnicas avanzadas de compresión de mensajes y en la mejora del QoS para reducir tanto la latencia como el consumo de energía. Por otro lado, en NDN, sería beneficioso mejorar los algoritmos de búsqueda y gestión de caché, lo que incrementaría la eficiencia y reduciría la latencia. En cuanto a la seguridad y privacidad, es crucial desarrollar mecanismos más robustos en MQTT, incluyendo técnicas avanzadas de autenticación y cifrado, mientras que en NDN se podría explorar la encriptación end-to-end y la gestión de claves para fortalecer la protección de los datos. La escalabilidad y la gestión eficiente de redes IoT es otro aspecto clave; en MQTT, esto podría lograrse mediante arquitecturas de brokers distribuidos y balanceo de carga, mientras que en NDN, el enfoque estaría en gestionar grandes volúmenes de tráfico y conexiones simultáneas de manera efectiva. Además, la investigación sobre la interoperabilidad entre MQTT, NDN y otros estándares IoT sería fundamental para facilitar su integración en entornos heterogéneos. Finalmente, la aplicación de inteligencia artificial y machine learning para predecir patrones de tráfico y optimizar la transmisión de datos en tiempo real podría transformar significativamente la eficiencia y

el rendimiento de las redes IoT, ofreciendo soluciones más avanzadas y adaptadas a las necesidades futuras.

9.2 Propuestas para Mejorar y Ampliar la Eficiencia de MQTT y NDN en Entornos IoT

Para mejorar el rendimiento y la seguridad en las redes IoT, se pueden considerar diversas estrategias tanto para MQTT como para NDN. En cuanto a MQTT, la implementación de técnicas de compresión de datos puede reducir el uso de ancho de banda, mientras que el desarrollo de algoritmos adaptativos de QoS permitiría ajustar dinámicamente el nivel de servicio según las condiciones de la red y los requisitos específicos de las aplicaciones. Además, incorporar autenticación multifactor y un cifrado más fuerte mejoraría la seguridad de las comunicaciones, y explorar modos de suspensión junto con técnicas de transmisión eficiente ayudaría a reducir el consumo de energía en dispositivos IoT.

Por otro lado, las mejoras en NDN podrían centrarse en la gestión de caché, donde el desarrollo de algoritmos más eficientes maximizaría el uso del almacenamiento intermedio, reduciendo así la latencia. La implementación de técnicas de enrutamiento inteligente basadas en inteligencia artificial optimizaría la entrega de datos y minimizaría la congestión en la red. La investigación en arquitecturas escalables permitiría a NDN manejar un mayor número de dispositivos y conexiones sin comprometer el rendimiento, mientras que el desarrollo de métodos avanzados de encriptación y gestión de claves garantizaría la privacidad y seguridad de los datos en tránsito.

Finalmente, la integración y cooperación entre ambos protocolos también es clave. Investigar la posibilidad de desarrollar un protocolo híbrido que combine las fortalezas de MQTT y NDN podría resultar en una solución más eficiente y segura para las redes IoT. Asimismo, contribuir al desarrollo de estándares y normativas que faciliten la interoperabilidad y adopción de estos protocolos en diversas aplicaciones sería fundamental para su implementación a gran escala.

10 BIBLIOGRAFÍA

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. L. (2009). Networking Named Content. In Proceedings of the 5th international conference on Emerging networking experiments and technologies (CoNEXT '09). NDN Paper

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., & Ayyash, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.

Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Claffy, K., Crowley, P., ... & Yu, Y. (2014). Named Data Networking. ACM SIGCOMM Computer Communication Review, 44(3), 66-73.

Truong, C., & Kanhere, S. S. (2018). A Survey on Internet of Things (IoT) Protocols for MQTT and NDN. IEEE Internet of Things Journal.

Banks, A., & Gupta, R. (2014). MQTT Version 3.1.1. OASIS Standard. MQTT Standard

Tschofenig, H., & Fossati, T. (2019). Transport Layer Security (TLS) / Datagram Transport Layer Security (DTLS) Profiles for the Internet of Things. RFC 7925. TLS for IoT

Truong, C., & Kanhere, S. S. (2018). A Survey on Internet of Things (IoT) Protocols for MQTT and NDN. IEEE Internet of Things Journal. IoT Protocols Survey

Al-Fuqaha, A., et al. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. IoT Survey

Singh, K. P., & Patel, S. C. (2017). Performance Analysis of MQTT and CoAP Protocols in IoT. Journal of Network and Computer Applications, 89, 19-28. MQTT vs CoAP

Minoli, D., Sohraby, K., & Occhiogrosso, B. (2017). IoT Considerations, Requirements, and Architectures for Smart Buildings – Energy Optimization and Next-Generation Building Management Systems. IEEE Internet of Things Journal, 4(1), 269-283. Smart Buildings

Jeong, H., et al. (2019). A Secure and Efficient Data Collection Scheme Using MQTT Protocol for IoT. Sensors, 19(4), 923. Secure MQTT

Zhang, L., et al. (2014). Named Data Networking. ACM SIGCOMM Computer Communication Review, 44(3), 66-73.

Jacobson, V., et al. (2009). Networking Named Content. In Proceedings of the 5th International Conference on Emerging Networking Experiments and Technologies (pp. 1-12).

Afanasyev, A., et al. (2018). NDN Protocol Specification. NDN Technical Report NDN-0021, Revision 4.

Amadeo, M., Campolo, C., & Molinaro, A. (2014). Internet of Things via Named Data Networking: The Support of Push Traffic. In Proceedings of the 2014 International Conference on Wireless Communications and Signal Processing (WCSP) (pp. 1-6).

Gasti, P., Tsudik, G., Uzun, E., & Zhang, L. (2012). DoS and DDoS in Named Data Networking. In Proceedings of the 22nd International Conference on Computer Communication and Networks (ICCCN) (pp. 1-7).

Misra, S., Sahoo, B., & Joshi, S. (2017). Named Data Networking for Internet of Things: A Survey. IEEE Communications Surveys & Tutorials, 19(1), 721-760.

Hunkeler, U., Truong, H. L., & Stanford-Clark, A. (2008). MQTT-S—A Publish/Subscribe Protocol For Wireless Sensor Networks. In 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (pp. 791-798).

Banks, A., & Gupta, R. (2014). MQTT Version 3.1.1. OASIS Standard.

Thangavel, D., Ma, X., Valera, A. C., Tan, H. X., & Tan, C. K. Y. (2014). Performance Evaluation of MQTT and CoAP via a Common Middleware. In 2014 IEEE Ninth International Conference on Intelligent Sensors, Sensor Networks and Information Processing (pp. 1-6).

Liu, M., Zhao, H., Li, X., & Zhang, L. (2013). Evaluation of a Pub/Sub Middleware for the Internet of Things. In 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing (pp. 120-126)