# Enrutamiento Inteligente en Redes IoT/Mesh

Comparación de Protocolos Clásicos y Adaptativos Basados en Machine Learning mediante Simulación en NS-3

## Objetivo

El presente informe detalla un plan de investigación integral cuyo objetivo principal es desarrollar y comparar protocolos de enrutamiento clásicos con versiones adaptativas basadas en inteligencia artificial (IA) y aprendizaje automático (ML) dentro de escenarios realistas de redes IoT/mesh. La evaluación se centrará en el impacto de estos protocolos en métricas clave de rendimiento y resiliencia, utilizando simulaciones avanzadas en NS-3

## Plan de Trabajo

### 1. Revisión del Estado del Arte

Esta sección ofrece una visión exhaustiva de los protocolos de enrutamiento existentes en redes IoT/mesh y las aplicaciones emergentes de la IA y el ML en este ámbito. Se destacarán las motivaciones para integrar el ML, las tendencias actuales de investigación y las brechas identificadas en la literatura.

#### Protocolos de Enrutamiento en Redes IoT/Mesh

La investigación en enrutamiento inteligente requiere una comprensión profunda de los protocolos de enrutamiento clásicos, que sirven como base comparativa y, en algunos casos, como cimientos para enfoques híbridos de ML. Se analizarán en detalle protocolos como AODV, OLSR, DSDV, DSR, HWMP, Babel, BATMAN y RPL (AODV, OLSR, DSDV, DSR solo estan ya implemnetados en NS3 a investigar el resto). La evaluación de sus fortalezas y debilidades inherentes en diversos escenarios es fundamental para diseñar mejoras efectivas basadas en ML.

La comparación de protocolos clásicos con versiones basadas en ML es un pilar de este proyecto. Esto implica que los protocolos tradicionales no son meramente puntos de referencia estáticos, sino que su estudio profundo revela las limitaciones que impulsan la necesidad de la IA. Por ejemplo, su naturaleza reactiva en entornos dinámicos, complejos o adversos, como se observa en escenarios con movilidad, interferencia o ataques, subraya la necesidad de una adaptación más inteligente. Esto sugiere que la IA en el enrutamiento no siempre busca reemplazar completamente los protocolos existentes, sino más bien potenciarlos para manejar situaciones donde las reglas fijas demuestran ser insuficientes. Este enfoque dual conduce a diseños de red más robustos y adaptables.

#### Aplicaciones de IA/ML en Redes IoT/Mesh

La integración de IA/ML en el enrutamiento de redes IoT/mesh está transformando la forma en que estas redes operan, permitiendo una adaptabilidad y eficiencia sin precedentes.

* **Protocolos de Enrutamiento Adaptativos:** Los modelos de ML se emplean para tomar decisiones óptimas de enrutamiento en tiempo real, ajustándose dinámicamente a cambios en la topología, interferencias, congestión y ataques. Esta es una de las aplicaciones centrales de la IA en este campo.
* **Predicción de Fallos y Congestión:** Algoritmos de ML, como redes neuronales, árboles de decisión, Q-learning y LSTM, tienen la capacidad de predecir enlaces que podrían fallar o congestionarse. Esta capacidad predictiva permite que el protocolo evite proactivamente rutas problemáticas antes de que los inconvenientes se manifiesten. Los protocolos clásicos, en gran medida, son reactivos, respondiendo a los cambios una vez que estos ya han ocurrido, como fallos de enlace o congestión. La introducción de capacidades predictivas mediante ML representa un cambio fundamental hacia un paradigma de enrutamiento proactivo. Esta capacidad de anticipación es particularmente valiosa en escenarios dinámicos y extremos, como los de resiliencia urbana, donde la adaptación rápida es crucial para mantener la continuidad del servicio. La habilidad de predecir y anticipar problemas de red podría reducir significativamente el tiempo de inactividad, mejorar la calidad de servicio (QoS) y aumentar la seguridad, impulsando así los límites de la autonomía y las capacidades de auto-curación de la red.
* **Balanceo de Carga Inteligente:** Se utilizan modelos entrenados para distribuir el tráfico de manera óptima, previniendo cuellos de botella y mejorando el rendimiento global de la red.
* **Detección de Anomalías y Nodos Maliciosos:** El ML es fundamental para identificar patrones de tráfico anómalos o sospechosos, lo que permite activar mecanismos de defensa o aislar nodos maliciosos. La seguridad tradicional a menudo se basa en la detección por firmas o reglas predefinidas. La capacidad del ML para identificar anomalías permite la detección de ataques novedosos o sofisticados, lo cual es vital en los entornos complejos, dinámicos y potencialmente adversos que se prevén. Esta capacidad se vincula directamente con la simulación de "nodos maliciosos" 1 y el objetivo más amplio de evaluar la "tolerancia ante fallos y ataques". La IA no solo optimiza el rendimiento; es un componente integral para construir redes IoT/mesh más seguras y robustas, capaces de resistir amenazas en evolución y mantener servicios críticos incluso bajo coacción.
* **Aprendizaje Federado:** Este enfoque implica que cada nodo entrena un modelo localmente y comparte solo los parámetros del modelo, no los datos brutos. Esto protege la privacidad y acelera la convergencia en redes distribuidas. Las redes IoT son inherentemente distribuidas y, a menudo, compuestas por dispositivos con recursos limitados y preocupaciones de privacidad. El aprendizaje federado aborda directamente estos desafíos al minimizar la transferencia de datos y proteger la información sensible. Este enfoque se alinea bien con los enfoques innovadores de "colaboración multi-red" y "aprendizaje transferido y federado", sugiriendo un método escalable y que preserva la privacidad para desplegar la IA en el borde de la red. El aprendizaje federado podría ser un catalizador para el despliegue de enrutamiento inteligente en implementaciones reales de IoT a gran escala, superando las limitaciones de ancho de banda y los obstáculos de privacidad que dificultan los enfoques centralizados de IA.

#### Ejemplos de Investigaciones Recientes

La investigación actual ha explorado diversas técnicas de IA/ML aplicadas al enrutamiento:

* **Q-Routing y Deep Q-Networks (DQN):** Adaptaciones del aprendizaje por refuerzo donde cada nodo aprende la mejor acción (siguiente salto) según el estado de la red.
* **Enrutamiento basado en LSTM:** Uso de redes neuronales recurrentes para predecir la calidad de los enlaces basándose en el historial de métricas.
* **Protocolos híbridos ML-clásicos:** El protocolo clásico toma la decisión por defecto, pero un módulo de ML puede anularla en situaciones críticas (alta congestión, movilidad extrema, ataque detectado).
* **Optimización multiobjetivo:** Algoritmos genéticos o de refuerzo que consideran simultáneamente latencia, consumo energético, fiabilidad y seguridad.

## 2. Identificación de Oportunidades

Se han identificado varias áreas con potencial para una investigación más profunda:

* Integración efectiva de ML en simuladores, abordando los desafíos de los módulos externos.
* Desarrollo de escenarios de resiliencia urbana.
* Exploración del aprendizaje federado y transferido.
* Comparación rigurosa de ML frente a heurísticas clásicas bajo condiciones extremas.

### 3. Diseño y Validación de Escenarios de Simulación

Esta sección detalla la metodología para crear entornos de simulación robustos, realistas y reproducibles en NS-3, progresando desde condiciones aisladas hasta escenarios híbridos complejos que reflejan despliegues reales de IoT/mesh.

#### Definición de Escenarios

Se definirán escenarios tanto separados como combinados para permitir un análisis controlado y realista del rendimiento de los protocolos.

* **Escenarios Separados (para análisis controlado):**
  + **Red estática:** Nodos fijos, sin movilidad ni interferencia, sirviendo como línea base de rendimiento.
  + **Red móvil:** Nodos con modelos de movilidad realistas, como Random Waypoint, o trayectorias basadas en mapas urbanos y herramientas como SUMO.
  + **Red con interferencia:** Nodos que generan tráfico disruptivo o ruido en el canal.
  + **Red con nodos maliciosos:** Simulación de ataques específicos como flooding, blackhole o manipulación de rutas.
  + **Escenarios VANET:** Simulación de vehículos en movimiento en mapas reales, lo que es relevante para la movilidad extrema y las topologías dinámicas.

Aunque el proyecto enfatiza los escenarios híbridos, los escenarios separados iniciales no son solo un punto de partida; cumplen un propósito científico crucial. Al aislar variables como la movilidad, la interferencia o los ataques, los investigadores pueden atribuir con precisión los cambios de rendimiento a factores específicos. Esto es esencial para validar la eficacia de los algoritmos de ML o las modificaciones de protocolo. Esta experimentación controlada es vital para la fase de entrenamiento de los modelos de ML, donde los datos limpios bajo condiciones específicas pueden conducir a un aprendizaje del modelo más robusto antes del despliegue en entornos complejos. Una metodología de investigación rigurosa exige tanto experimentos controlados y aislados para una comprensión fundamental, como escenarios complejos e integrados para la aplicabilidad en el mundo real. Este enfoque dual garantiza tanto la validez científica como la relevancia práctica.

* **Escenarios Híbridos y Combinados (para análisis realista):**
  + **Smart City/Campus/Aeropuerto:** Combinación de nodos fijos y móviles, nodos interferentes y maliciosos, y patrones de tráfico heterogéneos.
  + **Escenario de Resiliencia Urbana:** Simulación de desastres (apagones, cortes de red troncal, eventos climáticos) y observación de la auto-organización de la red, la recuperación de rutas y el mantenimiento de servicios críticos. Este es un enfoque innovador y diferenciador.
  + **Escenarios Basados en Mapas Reales:** Utilización de datos georreferenciados de OpenStreetMap y herramientas como SUMO para simular trayectorias realistas de vehículos y peatones, reflejando la infraestructura urbana.
  + **Escenarios Dinámicos y Adaptativos:** Introducción de eventos súbitos durante la simulación, como la aparición de interferencia, ataques maliciosos activados en momentos aleatorios, fallas de nodos críticos o cambios abruptos en los patrones de tráfico.
  + **Escenarios Multi-escala:** Combinación de micro-escenarios (ej., una intersección congestionada) dentro de un macro-escenario (ej., una ciudad completa), permitiendo analizar el comportamiento local y global de los protocolos.
  + **Escenarios de Colaboración Inter-red:** Simulación de la interacción entre diferentes tecnologías de red (WiFi, 802.11s, 6LoWPAN, LTE, LoRa) y evaluación de cómo los protocolos de enrutamiento se adaptan a la coexistencia y al handover inteligente entre redes.

El paso de escenarios simples a híbridos, basados en mapas reales, dinámicos o multiescala refleja directamente la complejidad de los entornos IoT del mundo real. Los protocolos clásicos a menudo encuentran dificultades en estos entornos debido a sus reglas fijas. Esta complejidad inherente demanda soluciones adaptativas como el enrutamiento basado en ML, ya que los modelos de ML están diseñados para aprender y adaptarse a datos dinámicos y de alta dimensión. Los vacíos y oportunidades identificados en el estado del arte, como la "integración real de ML en simuladores" y los "escenarios de resiliencia urbana" 1, se abordan precisamente con estos diseños de escenarios avanzados. El verdadero valor y la diferenciación de los protocolos de enrutamiento basados en ML solo pueden demostrarse y validarse rigurosamente en escenarios que capturen con precisión el dinamismo, la heterogeneidad y los desafíos de las implementaciones reales. Esto hace que el diseño de escenarios sofisticados no sea solo un paso metodológico, sino un habilitador crítico para una investigación significativa de ML en redes.

#### Validación de Escenarios

La validación de los escenarios es crucial para garantizar la fiabilidad de los resultados. Se asegurará la repetibilidad, robustez y escalabilidad de los escenarios.1 Cada elección de escenario se justificará en función de su relevancia práctica y su alineación con la literatura existente.1 Se documentarán meticulosamente los parámetros clave, incluyendo el número de nodos, el área de simulación, la duración, los patrones de tráfico y los roles de los nodos.

### 4. Implementación de Protocolos Clásicos y Adaptativos

Esta sección detalla los pasos técnicos para integrar protocolos de enrutamiento tanto estándar como mejorados con ML dentro del entorno de simulación NS-3, haciendo hincapié en los desafíos prácticos y las soluciones para la integración de ML.

#### Integración de Protocolos Clásicos

La implementación de protocolos clásicos en NS-3 varía según su disponibilidad en el simulador.

* **Nativos en NS-3:** Protocolos como AODV, OLSR, DSDV y DSR están incluidos por defecto en NS-3 y se habilitan fácilmente utilizando sus respectivos helpers en el script de simulación.
* **HWMP (IEEE 802.11s Mesh):** Este protocolo está integrado en el módulo mesh de NS-3 y su configuración es directa. (AUN NO LO PROBE!)
* **Babel (Módulo Externo):** Babel no es un protocolo nativo en NS-3, por lo que requiere la integración de un módulo externo compatible. Una implementación notable es la desarrollada por la Universidad Técnica de Múnich (TUM), descrita en el paper "An Implementation of the Babel Routing Protocol for ns3" (2022).1 Los pasos para su integración incluyen descargar el módulo, copiarlo a src/babel dentro de la instalación de NS-3, modificar el archivo wscript para incluirlo en la compilación y, finalmente, recompilar NS-3. Una vez integrado, se utiliza el BabelHelper en los scripts de simulación.1 Las limitaciones de esta implementación incluyen que es principalmente para IPv6, puede no implementar todas las características del RFC y no es interoperable fuera del entorno NS-3.1

Si bien NS-3 es una plataforma de código abierto, la integración de módulos externos como Babel y BATMAN destaca que el "código abierto" no siempre implica una funcionalidad de "conectar y usar". A menudo, la integración requiere pasos manuales, comprobaciones de compatibilidad y, en ocasiones, depuración, especialmente con versiones específicas de NS-3 o dependencias. Esto afecta directamente la reproducibilidad del proyecto. Si los módulos externos son difíciles de integrar o no se mantienen activamente, la reproducción de los resultados se convierte en un desafío. Esto exige una documentación meticulosa de la versión exacta de NS-3 y las versiones de los módulos utilizados. Los investigadores deben considerar la sobrecarga de integrar y mantener módulos externos, que puede ser significativa. Esto también sugiere la necesidad de repositorios de módulos mejor mantenidos por la comunidad o mecanismos de integración más estandarizados dentro de los marcos de simulación para fomentar verdaderamente la investigación abierta y reproducible.

* **BATMAN (Módulo Externo):** Al igual que Babel, BATMAN no está incluido oficialmente en NS-3. La integración se realiza a través de módulos de la comunidad, como el proyecto BATSEN. El proceso es similar al de Babel: descargar el módulo BATSEN, copiar la carpeta batmand a src/, modificar el wscript y recompilar NS-3. A pesar de su utilidad en simulaciones académicas, no es parte del core oficial de NS-3, su desarrollo comunitario se pausó en 2020, y podría requerir adaptaciones para versiones recientes de NS-3

#### Desarrollo de Versiones Adaptativas (Basadas en ML)

La implementación de protocolos adaptativos basados en ML es un componente central de la investigación.

* **ML Embebido (C++):** Consiste en implementar el modelo de ML directamente dentro del código C++ de NS-3
* **ML Externo (Bindings de Python):** Una alternativa es entrenar modelos de ML fuera de NS-3 (utilizando frameworks como PyTorch o TensorFlow) e integrarlos a través de bindings de Python (como PyBind o el módulo Python de NS-3). Esto permite que el simulador consulte al modelo de ML para las decisiones de enrutamiento.1

La opción de modelos de ML embebidos en C++ o externos en Python presenta una decisión arquitectónica crucial. Si bien C++ ofrece rendimiento, Python con frameworks como TensorFlow/PyTorch proporciona prototipado rápido, acceso a bibliotecas avanzadas de ML y un manejo de datos más sencillo. El uso de bindings de Python es clave para aprovechar lo mejor de ambos mundos. Este método de integración apoya directamente la oportunidad de una "integración real de ML en simuladores" identificada en la revisión del estado del arte. También implica la necesidad de mecanismos robustos de intercambio de datos entre el entorno de simulación C++ y el entorno de ML Python. La capacidad de integrar sin problemas frameworks de ML externos en NS-3 democratiza la investigación de redes basada en ML, permitiendo a los investigadores centrarse en algoritmos de ML novedosos y su impacto en la red en lugar de reimplementar modelos complejos de ML en C++. Esto fomenta la colaboración interdisciplinaria.

* **Detección de Anomalías:** Se utilizará ML para identificar nodos maliciosos o interferentes en tiempo real, integrando esta capacidad en el proceso de decisión de enrutamiento.1
* **Definición de Entrada/Salida para ML:** Es crucial definir claramente el estado de la red (entrada) y la decisión o acción de enrutamiento (salida) para el modelo de ML.
* **Estrategias de Entrenamiento ML:**
  + **Entrenamiento Offline:** Recopilación de métricas de red de simulaciones previas para entrenar el modelo externamente.1
  + **Aprendizaje en Línea (**Online Learning**):** Implementación de modelos que mejoran a medida que avanza la simulación, adaptándose dinámicamente a los cambios en la red.

El énfasis en la recopilación de métricas de red para el entrenamiento y la elección entre el aprendizaje offline u online resaltan que el enrutamiento basado en ML se fundamenta en los datos. La calidad y representatividad de los datos de entrenamiento impactan directamente el rendimiento del modelo de ML y su capacidad para generalizar a condiciones de red no vistas. Esto se relaciona con el diseño y validación de escenarios de simulación.1 Los escenarios realistas y diversos son esenciales no solo para las pruebas, sino también para generar los conjuntos de datos ricos necesarios para entrenar modelos de ML robustos. El éxito del enrutamiento basado en ML depende de una relación simbiótica entre entornos de simulación realistas (para la generación de datos) y modelos de ML sofisticados (para aprender de esos datos). Esto subraya la importancia de un enfoque holístico que considere la recopilación de datos, el entrenamiento de modelos y la validación de la simulación como componentes interconectados.

### 5. Plan de Simulaciones y Métricas

Esta sección describe el enfoque sistemático para llevar a cabo simulaciones y recopilar métricas de rendimiento, garantizando la validez estadística y una evaluación exhaustiva de los protocolos desarrollados.

#### Métricas Principales

Para una evaluación completa, se recolectarán y analizarán las siguientes métricas clave:

* **Throughput:** Cantidad de datos entregados por unidad de tiempo.
* **Latencia:** Tiempo de extremo a extremo de los paquetes.
* **Jitter:** Variación de la latencia.
* **Pérdida de paquetes:** Porcentaje de paquetes no entregados.
* **Overhead de control:** Proporción de mensajes de control respecto al tráfico total.
* **Tiempo de convergencia:** Tiempo hasta que la red se estabiliza tras un cambio.
* **Consumo energético:** Si es relevante y los módulos lo permiten.
* **Tolerancia ante fallos y ataques:** Capacidad de mantener conectividad y rendimiento ante fallos o ataques.

La lista completa de métricas indica que el rendimiento de la red no es un valor único, sino un concepto multidimensional. Optimizar una métrica (ej., throughput) podría degradar otra (ej., latencia u overhead). Los protocolos de ML, especialmente aquellos diseñados para la optimización multiobjetivo, deben evaluarse en todo este espectro. La inclusión de "tolerancia ante fallos y ataques" como una métrica clave se vincula directamente con los escenarios innovadores y las capacidades de ML para la detección y predicción de anomalías. Esta métrica es crucial para validar la naturaleza adaptativa de las soluciones basadas en ML. Una evaluación exhaustiva requiere una visión holística del comportamiento de la red. Esto significa no solo informar números brutos, sino también analizar las compensaciones entre diferentes métricas, particularmente al comparar protocolos clásicos de reglas fijas con los adaptativos impulsados por ML. El "mejor" protocolo dependerá de las prioridades de la aplicación específica.

#### Plan Experimental

Se planificarán simulaciones sistemáticas para cada combinación de escenario y protocolo. Para garantizar la validez estadística de los resultados, cada simulación se repetirá varias veces utilizando distintas semillas aleatorias. Los resultados serán sometidos a un análisis estadístico riguroso, incluyendo el cálculo de la media, la desviación estándar y los intervalos de confianza.1 Se prestará especial atención a la evaluación bajo condiciones extremas, como las simulaciones de resiliencia urbana o eventos disruptivos.

En NS-3, la recolección de métricas se realizará utilizando los sistemas de tracing y logging nativos del simulador. Los resultados se exportarán a archivos para su posterior análisis con herramientas como Python, R o Excel. La presentación de los resultados se realizará mediante tablas y gráficos claros, incluyendo gráficos de caja, líneas de tiempo y mapas de calor, para facilitar la interpretación y la visualización de las tendencias.

### 6. Enfoque Innovador y Diferenciador

Esta sección destacará las contribuciones únicas de la investigación, centrándose en escenarios novedosos y técnicas avanzadas de ML que amplían los límites del enrutamiento inteligente en redes IoT/mesh.

#### Escenarios de Resiliencia Urbana

Un enfoque innovador y diferenciador de esta investigación es la simulación de eventos de resiliencia urbana. Esto implica simular desastres (apagones, cortes de red troncal, eventos climáticos) y observar la capacidad de auto-organización de la red. Se evaluará cómo los protocolos logran la recuperación de rutas y cómo se produce la degradación o la gracia del servicio ante fallos masivos. El objetivo es determinar la capacidad de la red para mantener servicios críticos (salud, seguridad, transporte) bajo condiciones extremas y disruptivas.

El fuerte énfasis en la "resiliencia urbana" representa un cambio significativo con respecto a la investigación tradicional en redes, que a menudo se centra únicamente en métricas de rendimiento (throughput, latencia). Este proyecto apunta explícitamente a la capacidad de la red para resistir y recuperarse de eventos catastróficos, entrando en el ámbito de la infraestructura crítica. Esto aprovecha directamente las capacidades de ML para la detección de anomalías y el enrutamiento adaptativo 1, ya que estas son esenciales para que una red se autoorganice y mantenga los servicios cuando se enfrenta a interrupciones impredecibles y a gran escala. Esta investigación tiene profundas implicaciones sociales. Al demostrar cómo el enrutamiento inteligente puede garantizar la conectividad durante desastres, contribuye directamente a las iniciativas de ciudades inteligentes y a los sistemas de respuesta a emergencias, haciendo que los entornos urbanos sean más seguros y robustos. Esto eleva la investigación más allá del interés puramente académico a aplicaciones prácticas que pueden salvar vidas.

#### Aprendizaje Transferido y Federado

Se explorarán paradigmas avanzados de ML para mejorar la adaptabilidad y la privacidad:

* **Aprendizaje Transferido:** Se entrenarán modelos de ML en un entorno de simulación y se validará su desempeño en otro diferente, evaluando la capacidad de generalización del modelo a nuevas condiciones.1
* **Aprendizaje Federado:** Cada nodo entrenará localmente un modelo y compartirá únicamente los parámetros del modelo (no los datos brutos), lo que protege la privacidad de los datos y acelera la convergencia en redes distribuidas.

El aprendizaje transferido y federado son paradigmas avanzados de ML que abordan directamente las preocupaciones de escalabilidad y privacidad inherentes a las redes IoT/mesh a gran escala. El aprendizaje transferido reduce la necesidad de un reentrenamiento extenso en nuevos entornos, mientras que el aprendizaje federado permite la inteligencia distribuida sin centralizar datos sensibles. Esto apoya directamente la viabilidad de desplegar enrutamiento basado en ML en entornos IoT heterogéneos y del mundo real 1 donde la recopilación centralizada de datos y las actualizaciones de modelos podrían ser poco prácticas o indeseables. Estas técnicas de ML son cruciales para llevar el enrutamiento basado en ML de la simulación al despliegue práctico. Permiten un comportamiento inteligente de la red en entornos diversos y en evolución, al tiempo que respetan la privacidad de los datos, lo cual es cada vez más crítico para la aceptación pública y el cumplimiento normativo en IoT.

#### Comparativa ML vs. Heurísticas Clásicas

Se realizará un análisis exhaustivo para determinar bajo qué condiciones el ML supera a los protocolos tradicionales y viceversa.1 El enfoque se centrará en condiciones extremas y dinámicas donde las reglas fijas de los protocolos clásicos podrían fallar.1

#### Colaboración Multi-red

Se investigará el enrutamiento inteligente en redes híbridas que combinan diversas tecnologías como WiFi, mesh, 6LoWPAN y LTE, incluyendo la evaluación de mecanismos de handover inteligente entre ellas.

## Detalles de Simulaciones y Métricas en NS-3

Esta sección proporciona un resumen conceptual consolidado de los parámetros clave y las metodologías para las simulaciones en NS-3 y la recolección de métricas.

* **Escenarios:** Se contemplarán simulaciones en redes fijas y móviles, con y sin interferencia, con y sin ataques, así como escenarios híbridos y de resiliencia. Las topologías incluirán malla regular, aleatoria y basadas en mapas reales. Los patrones de tráfico abarcarán CBR, ráfagas, multimedia y tráfico de emergencia.1
* **Métricas:** Las métricas a evaluar serán throughput, latencia, jitter, pérdida de paquetes, overhead de control, tiempo de convergencia, consumo energético (si es relevante) y resiliencia.1
* **Variables de control:** Se manipularán variables como el número de nodos, la densidad, la movilidad, la intensidad de interferencia, el porcentaje de nodos maliciosos y los patrones de tráfico.1
* **Repetibilidad:** Cada experimento se ejecutará múltiples veces con distintas semillas aleatorias para asegurar la validez estadística de los resultados.1
* **Análisis:** Se aplicará estadística descriptiva y comparativa. Los resultados se visualizarán mediante gráficos de caja, líneas de tiempo y mapas de calor para una interpretación clara.1