# Sugerencias para la Tesis Doctoral: Expansión de Simulaciones NS-3 para Evaluación de Protocolos de Ruteo en IoT

Para una tesis doctoral centrada en la evaluación de protocolos de ruteo en redes IoT, especialmente si planeas integrar redes neuronales y SDN, es crucial expandir la profundidad y amplitud de tus simulaciones. A continuación, se detallan sugerencias para métricas, protocolos y escenarios adicionales que pueden hacer que tu investigación sea más robusta y relevante.

## 1. Métricas Adicionales Sugeridas

Más allá de las métricas básicas de throughput, delay y packet loss, considera las siguientes para una evaluación más completa de los protocolos de ruteo en IoT:

* **Overhead de ruteo (Routing Overhead):**
  + **Descripción:** Cantidad de mensajes de control (por ejemplo, RREQ, RREP, HELLO en AODV/OLSR, o actualizaciones de tabla en DSDV) intercambiados por el protocolo para establecer y mantener las rutas.
  + **Relevancia para IoT:** En redes con recursos limitados (ancho de banda, energía), un alto overhead consume valiosos recursos y reduce la capacidad para el tráfico de datos útil. Es crucial para evaluar la eficiencia de los protocolos.
  + **Cómo obtenerlo:** NS-3 FlowMonitor puede proporcionar estadísticas sobre paquetes de control. También puedes implementar contadores en el código para mensajes específicos de cada protocolo de enrutamiento.
* **Tiempo de Convergencia (Convergence Time):**
  + **Descripción:** El tiempo que tarda la red en establecer rutas estables y completas después de un cambio significativo en la topología (por ejemplo, un nodo se une, un nodo se va, un enlace falla).
  + **Relevancia para IoT:** La rapidez con la que una red IoT se adapta a los cambios es vital, especialmente en escenarios con alta movilidad o nodos que entran y salen constantemente.
  + **Cómo obtenerlo:** Requiere trazar los estados de las tablas de ruteo o los mensajes de control después de un evento disruptivo. Puedes programar eventos en la simulación para simular fallos o nuevas adiciones de nodos y medir el tiempo hasta que las rutas se estabilizan.
* **Robustez / Resiliencia (Robustness / Resilience):**
  + **Descripción:** La capacidad de la red para mantener la conectividad y un nivel aceptable de rendimiento frente a fallos de nodos, fallos de enlaces, o la presencia de interferencia y ataques.
  + **Relevancia para IoT:** Las redes IoT suelen operar en entornos hostiles y descentralizados, donde los fallos son comunes.
  + **Cómo obtenerlo:** Se mide mediante la ejecución de simulaciones con fallos inducidos (por ejemplo, apagar nodos aleatoriamente, degradar enlaces) y observando cómo el PDR, throughput y conectividad general se ven afectados.
* **Costo de la Ruta (Path Cost):**
  + **Descripción:** Una métrica acumulativa asociada a una ruta desde el origen hasta el destino. Puede ser el número de saltos (hop count), el retardo total, el consumo de energía acumulado, o una combinación de estos.
  + **Relevancia para IoT:** Permite evaluar la “calidad” de las rutas encontradas por el protocolo desde diferentes perspectivas (no solo el camino más corto, sino el de menor energía, menor retardo, etc.).
  + **Cómo obtenerlo:** Utiliza FlowMonitor para obtener los nodos en la ruta y suma las métricas relevantes (ej. energía consumida por cada nodo en la ruta).
* **Estabilidad de la Ruta (Route Stability / Route Churn):**
  + **Descripción:** La frecuencia con la que las rutas cambian o se invalidan. Un alto “churn” indica inestabilidad de la ruta.
  + **Relevancia para IoT:** Rutas muy inestables generan más overhead de ruteo, mayor retardo y menor eficiencia.
  + **Cómo obtenerlo:** Requiere registrar los eventos de cambio de ruta (creación, invalidación, descubrimiento) y contarlos a lo largo del tiempo.
* **Consumo de Energía Detallado (Detailed Energy Consumption):**
  + **Descripción:** Desglosa el consumo de energía en diferentes estados de la radio (transmisión, recepción, inactivo, sueño).
  + **Relevancia para IoT:** La duración de la batería es un factor crítico en la mayoría de los dispositivos IoT. Entender dónde se gasta la energía permite optimizar los protocolos para prolongar la vida útil de los dispositivos.
  + **Cómo obtenerlo:** NS-3 Energy Module puede ser configurado para rastrear estos estados.
* **Calidad de la Señal Recibida (RSSI - Received Signal Strength Indicator):**
  + **Descripción:** La intensidad de la señal recibida por cada nodo.
  + **Relevancia para IoT:** Un bajo RSSI puede indicar una conectividad deficiente o la presencia de interferencia, lo que afecta directamente el rendimiento del enlace y, por ende, el ruteo.
  + **Cómo obtenerlo:** La capa física Wi-Fi en NS-3 puede proporcionar trazas de RSSI.

## 2. Protocolos Adicionales Sugeridos

Expandir la gama de protocolos de enrutamiento a evaluar te dará una perspectiva más completa:

* **RPL (Routing Protocol for Low-Power and Lossy Networks):**
  + **Descripción:** Es el protocolo de enrutamiento estándar de IETF para redes de baja potencia y con pérdidas (LLNs), comúnmente utilizado en IoT. Está optimizado para construir topologías de árbol (DODAGs) y manejar enlaces inestables.
  + **Relevancia:** Es *esencial* incluirlo, ya que la mayoría de las redes IoT reales se basan en este protocolo o sus variantes. Ofrece una comparación directa con los protocolos ad-hoc que ya estás usando.
  + **Implementación en NS-3:** NS-3 tiene un módulo RPL.
* **IEEE 802.15.4 (y sus capas superiores):**
  + **Descripción:** Este estándar define la capa física (PHY) y la capa de control de acceso al medio (MAC) para redes de área personal inalámbricas de baja tasa de datos (WPANs). Es la base de tecnologías como Zigbee, WirelessHART, y es muy relevante en IoT.
  + **Relevancia:** Permite simular escenarios donde los dispositivos IoT tienen limitaciones de ancho de banda y energía inherentes a este estándar.
  + **Implementación en NS-3:** NS-3 tiene un módulo 802.15.4.
* **Protocolos SDN (Software-Defined Networking):**
  + **Descripción:** En un entorno SDN, el plano de control (ruteo) se desacopla del plano de datos (envío de paquetes). Un controlador centralizado (o distribuido) toma las decisiones de ruteo.
  + **Relevancia:** Permite explorar cómo un enfoque centralizado podría optimizar el ruteo en IoT, ofreciendo mayor flexibilidad, programabilidad y optimización global de la red. Podrías simular OpenFlow o un controlador SDN simple que determine las rutas.
  + **Implementación en NS-3:** Requiere el módulo sdn o la implementación de un controlador externo que interactúe con los switches virtuales en NS-3.
* **Protocolos Híbridos o Basados en Clústeres:**
  + **Descripción:** Protocolos que combinan elementos de ruteo reactivo y proactivo, o que organizan los nodos en clústeres para una gestión más eficiente.
  + **Relevancia:** Pueden ofrecer un buen equilibrio entre overhead y adaptabilidad en redes IoT a gran escala.
  + **Implementación en NS-3:** Podrías modificar protocolos existentes o buscar implementaciones de investigación.

## 3. Escenarios Adicionales Sugeridos

Variar los escenarios de simulación te permitirá analizar la robustez y adaptabilidad de los protocolos bajo diferentes condiciones.

* **Densidad de Nodos Variable:**
  + **Descripción:** Ejecuta simulaciones con un rango mucho más amplio de cantidades de nodos (ej. 10, 50, 100, 200, 500, 1000).
  + **Relevancia:** Fundamental para evaluar la escalabilidad de los protocolos. ¿Cómo se degrada el rendimiento o aumenta el overhead a medida que la red crece?
* **Topologías Más Complejas y Realistas:**
  + **Descripción:** Más allá de una cuadrícula o distribución aleatoria, considera:
    - **Redes con agujeros (holes):** Áreas donde no hay nodos o la conectividad es limitada (ej. edificios, obstáculos).
    - **Redes con nodos concentrados:** Nodos agrupados en ciertas áreas, como en una ciudad inteligente con sensores en intersecciones, o en una fábrica con máquinas.
    - **Redes lineales o en “pasillo”:** Para escenarios como túneles, cadenas de producción largas, etc.
  + **Relevancia:** Evalúa cómo los protocolos se adaptan a entornos geográficos no ideales.
* **Modelos de Movilidad Más Realistas:**
  + **Descripción:** En lugar de solo RandomWalk2d, explora:
    - **Modelos basados en caminos (e.g., Manhattan Grid):** Para simular movimiento en áreas urbanas.
    - **Modelos de grupo (e.g., Reference Point Group Mobility Model):** Para simular grupos de dispositivos que se mueven juntos.
    - **Modelos de movilidad de vehículos (e.g., SUMO, TraNS):** Si tu IoT incluye vehículos o drones.
  + **Relevancia:** El impacto de la movilidad en el ruteo es enorme; modelos más realistas proporcionarán resultados más aplicables.
* **Patrones de Interferencia Variable:**
  + **Descripción:** Simula diferentes tipos y niveles de interferencia:
    - **Interferencia constante:** Como ya haces, pero variando la potencia.
    - **Interferencia intermitente:** Dispositivos que transmiten esporádicamente.
    - **Interferencia co-canal:** Otras redes Wi-Fi o IoT que operan en el mismo canal.
  + **Relevancia:** Evalúa la resiliencia de los protocolos de ruteo en entornos ruidosos.
* **Ataques Más Sofisticados:**
  + **Descripción:** Además de generar tráfico malicioso, implementa:
    - **Ataques de Agujero Negro (Blackhole Attack):** Un nodo malicioso se anuncia como la ruta más corta a todos los destinos y luego descarta los paquetes.
    - **Ataques de Agujero Gris (Grayhole Attack):** Similar al blackhole, pero descarta paquetes selectivamente.
    - **Ataques de Wormhole:** Dos nodos maliciosos crean un “túnel” de baja latencia entre ellos, engañando a los protocolos para que envíen tráfico a través de una ruta suboptimal.
    - **Ataques Sybil:** Un atacante crea múltiples identidades falsas de nodos para manipular el ruteo.
  + **Relevancia:** Permite evaluar la seguridad y robustez de los protocolos frente a amenazas comunes en redes ad-hoc/IoT.
* **Calidad de Servicio (QoS):**
  + **Descripción:** Introduce diferentes tipos de tráfico con requisitos de QoS (por ejemplo, tráfico de voz/video con baja latencia, tráfico de datos con alta tolerancia a la latencia).
  + **Relevancia:** Evalúa la capacidad de los protocolos para soportar servicios heterogéneos, una necesidad creciente en IoT. Requiere configurar prioridades en la aplicación y monitorear métricas específicas de QoS.
* **Escenarios de Control SDN Centralizado/Distribuido:**
  + **Descripción:** Diseña escenarios donde el ruteo es gestionado total o parcialmente por un controlador SDN. Varía el número de controladores, su ubicación y la lógica de ruteo que implementan.
  + **Relevancia:** Es el punto de partida para tu posible investigación en SDN y redes neuronales, mostrando cómo el control programable puede influir en el ruteo IoT.

## 4. Ajustes en Cantidad de Nodos y Tiempo de Simulación

* **Cantidad de Nodos:**
  + Para empezar, tus 20-30 nodos son un buen punto de partida. Para una tesis doctoral, deberías escalar a rangos de **100 a 500 nodos, e incluso 1000+** para pruebas de escalabilidad significativas. Esto requerirá mayor poder de cómputo y optimización de las simulaciones.
* **Tiempo de Simulación:**
  + Los 60 segundos actuales son adecuados para pruebas rápidas. Para análisis de convergencia, estabilidad a largo plazo, o escenarios con mucha movilidad, necesitarás aumentar el tiempo a **120, 300 segundos (5 minutos) o incluso 600 segundos (10 minutos) o más**. Simulaciones más largas capturan mejor el comportamiento dinámico de la red.

## 5. Relevancia para Futuras Implementaciones (Redes Neuronales y SDN)

Los datos y las métricas adicionales, junto con los escenarios de prueba expandidos, sentarán las bases para tu investigación más avanzada:

* **Evaluación de Línea Base:** Al tener un conjunto de datos robusto de los protocolos tradicionales bajo diversas condiciones, tendrás una línea base sólida para comparar el rendimiento de tus nuevas propuestas (ej. protocolos de ruteo basados en redes neuronales).
* **Identificación de Brechas:** Las simulaciones con escenarios más complejos (interferencia, ataques, movilidad) te ayudarán a identificar las debilidades de los protocolos existentes, justificando la necesidad de soluciones más inteligentes (NN, SDN).
* **Conjuntos de Datos para Entrenamiento:** Métricas detalladas como RSSI, consumo de energía por estado, y el overhead de control, pueden servir como *features* para entrenar modelos de redes neuronales que predigan el mejor camino, detecten anomalías o tomen decisiones de ruteo.
* **Validación de Estrategias SDN:** Los escenarios SDN te permitirán demostrar el valor del control centralizado o distribuido para mejorar la eficiencia y la seguridad del ruteo en IoT.

Al abordar estas expansiones, tu proyecto de simulación en NS-3 no solo será completo, sino que también generará los datos y la comprensión necesarios para una tesis doctoral innovadora en el ámbito de los protocolos de ruteo IoT con aprendizaje automático y SDN.