Redes Definidas por Software: Software: Enrutamiento Inteligente y aspectos de seguridad

Las SDN revolucionan la gestión de redes mediante la separación de planos de control y reenvío.

Esta tecnología permite una prevención eficaz de la congestión a través de una gestión centralizada.

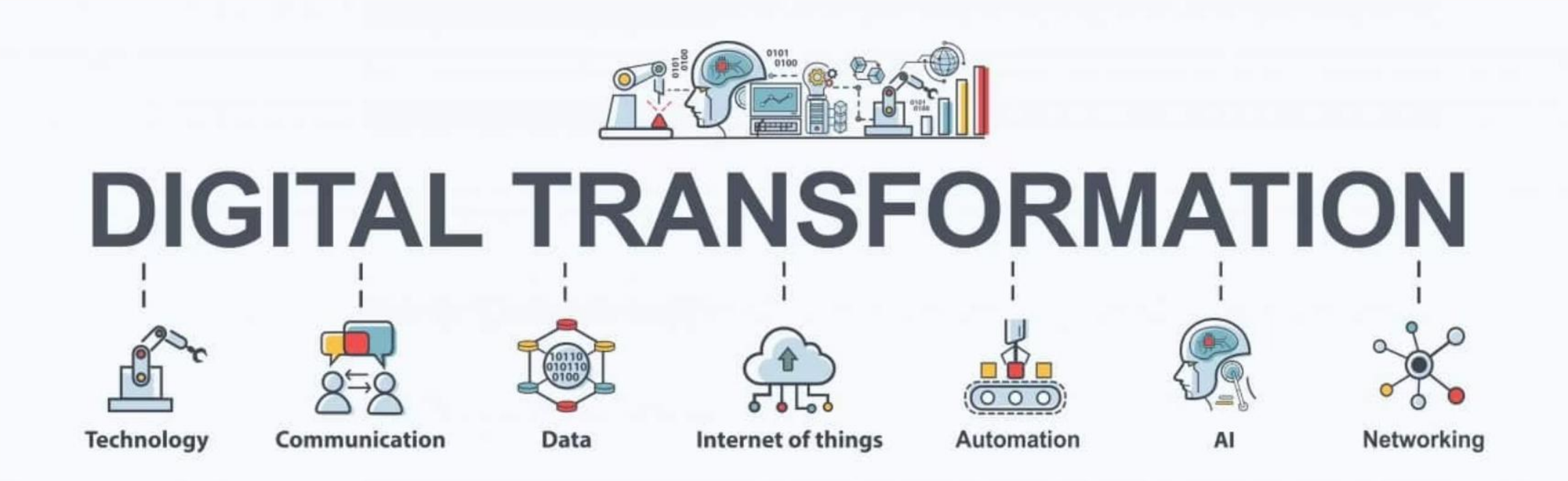
Su implementación crece rápidamente en entornos empresariales y centros de datos modernos.

Raul RIVERA RODRIGUEZ

Transformación digital

- Proceso de **integración** de **tecnologías digitales** en todos los aspectos de una **organización**.

- Cambio fundamental en **cómo se operan** y **entregan los servicios**.
- Implica una **reimaginación** de los **modelos de negocio** y operativos tradicionales.



https://smartway2.com/blog/8-successful-examples-of-digital-transformation/

Redes de próxima generación

¿Qué son?

Redes innovadoras que combinan **tecnologías emergentes** para resolver desafíos de **conectividad**, **escalabilidad, seguridad** y **gestión** en entornos complejos.

Necesidad actual:

- Explosión de dispositivos conectados: Internet of Things (IoT).
- Movilidad y baja latencia: Vehicular Ad-hoc Networks (VANET)
- Flexibilidad y programabilidad: Software Defined Network (SDN).

Internet de las Cosas - IoT

Red de objetos físicos con sensores, software y conectividad para intercambiar datos.

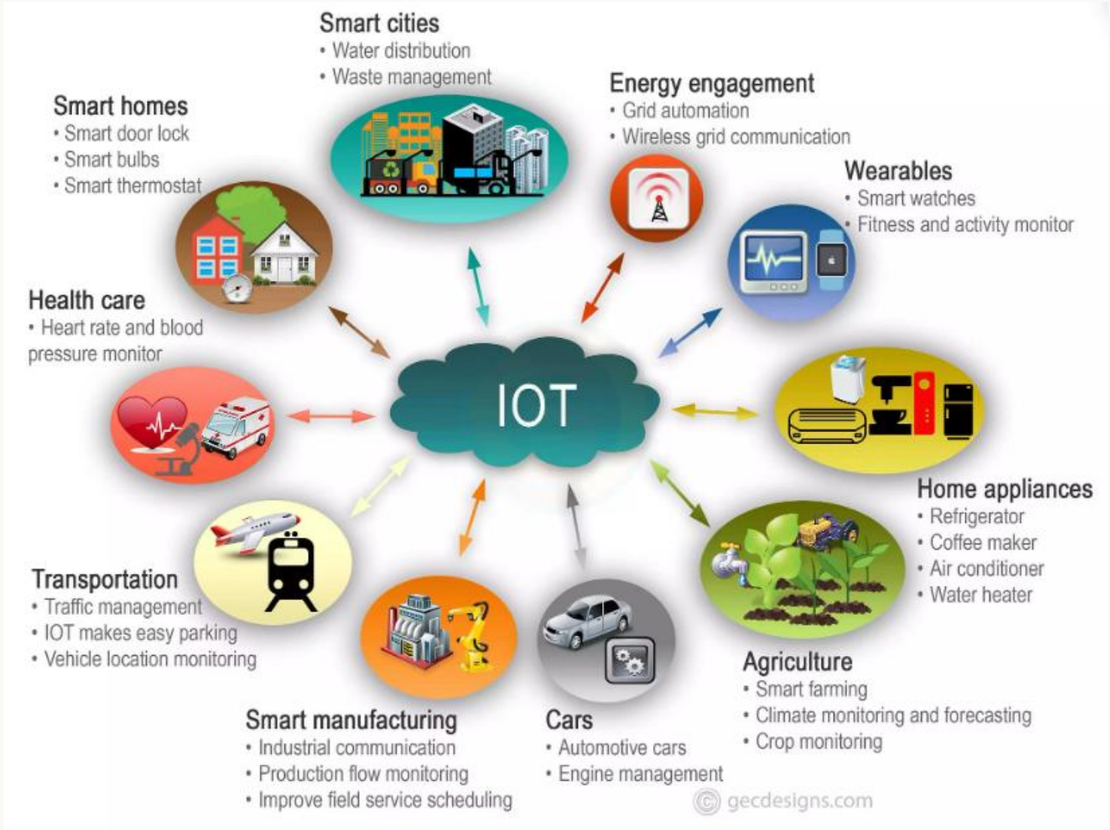
Características clave:

- Escalabilidad masiva.
- Heterogeneidad de dispositivos.
- Conectividad omnipresente.

Retos:

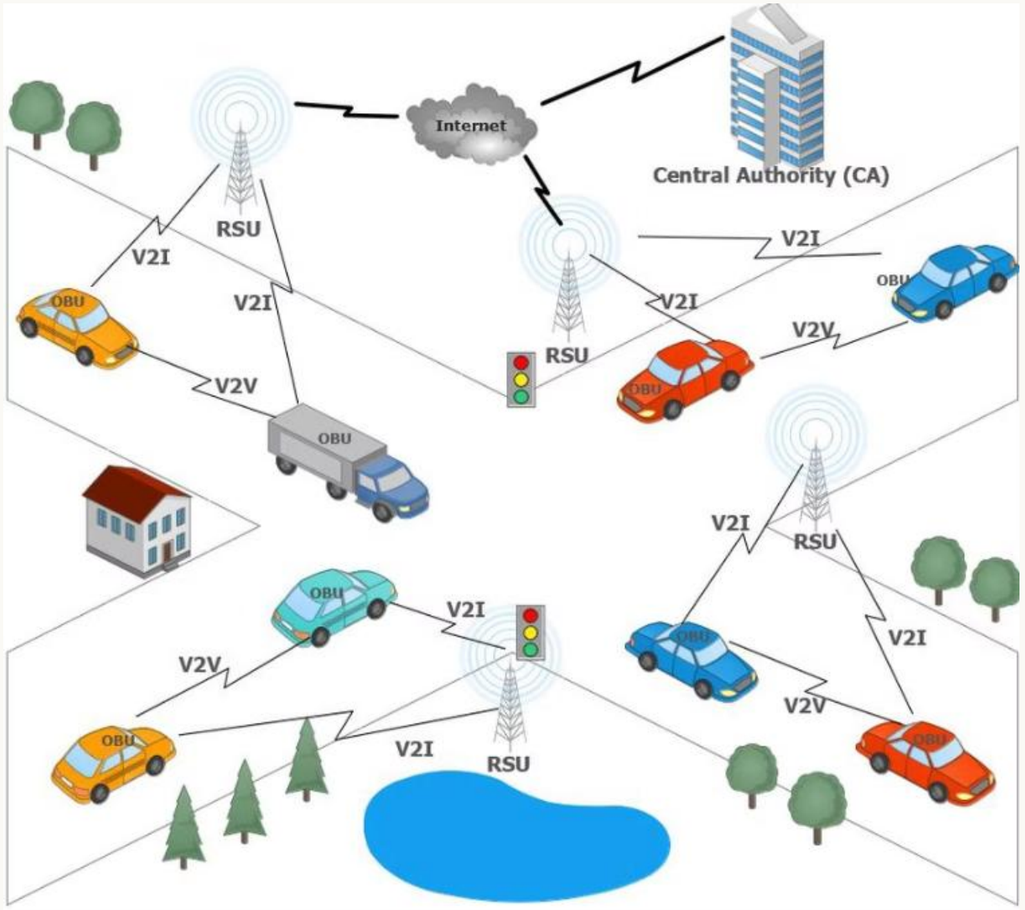
- Gestión de tráfico

- **Seguridad**, consumo energético, gestión de datos.



https://mungfali.com/explore/Iot-Map

VANET



https://www.researchgate.net/publication/370916477_A_Novel_Identity-Based_Privacy-Preserving_Anonymous_Authentication_Scheme_for_Vehicle-to-Vehicle_Communication

Redes inalámbricas dinámicas

entre vehículos e infraestructura vial para comunicación V2V (**vehicle-to-vehicle**) y V2I (**vehicle-to-infrastructure**)

Características clave:

- Topología altamente dinámica.
- Requisitos de latencia ultra-baja.
- Aplicaciones críticas para seguridad vial.

Retos:

Alta movilidad, interferencias, escalabilidad y **seguridad**.

Fundamentos de SDN

Definición

Uso de controladores de software y APIs para gestionar redes de forma centralizada.

Separación

Desacoplamiento de planos de control (enrutamiento) y datos (transferencia).

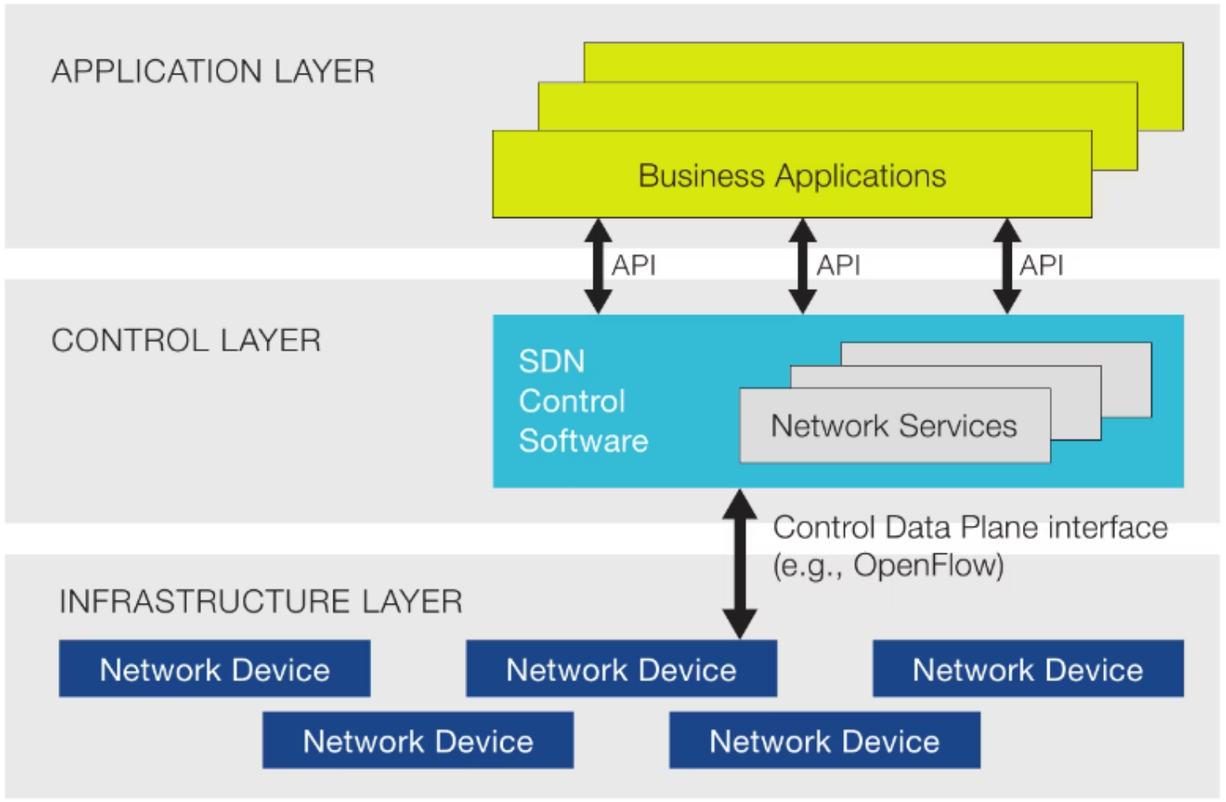
Centralización

Decisiones sobre trayectorias de paquetes tomadas desde un punto central.

OpenFlow

Protocolo estándar principal que facilita la implementación de SDN.

Redes Definidas por Software (SDN)



Arquitectura que separa el **plano de control** del **plano de datos**, permitiendo **gestión centralizada y programable**

Características clave:

- Programabilidad mediante APIs.
- Visibilidad global de la red.
- Flexibilidad.

Retos:

- Cuellos de botella en el controlador, estandarización, **seguridad**.

https://blog.zhaw.ch/icclab/an-introduction-to-software-defined-networking-sdn/

Redes de próxima generación (integración)

Plano de Aplicación:

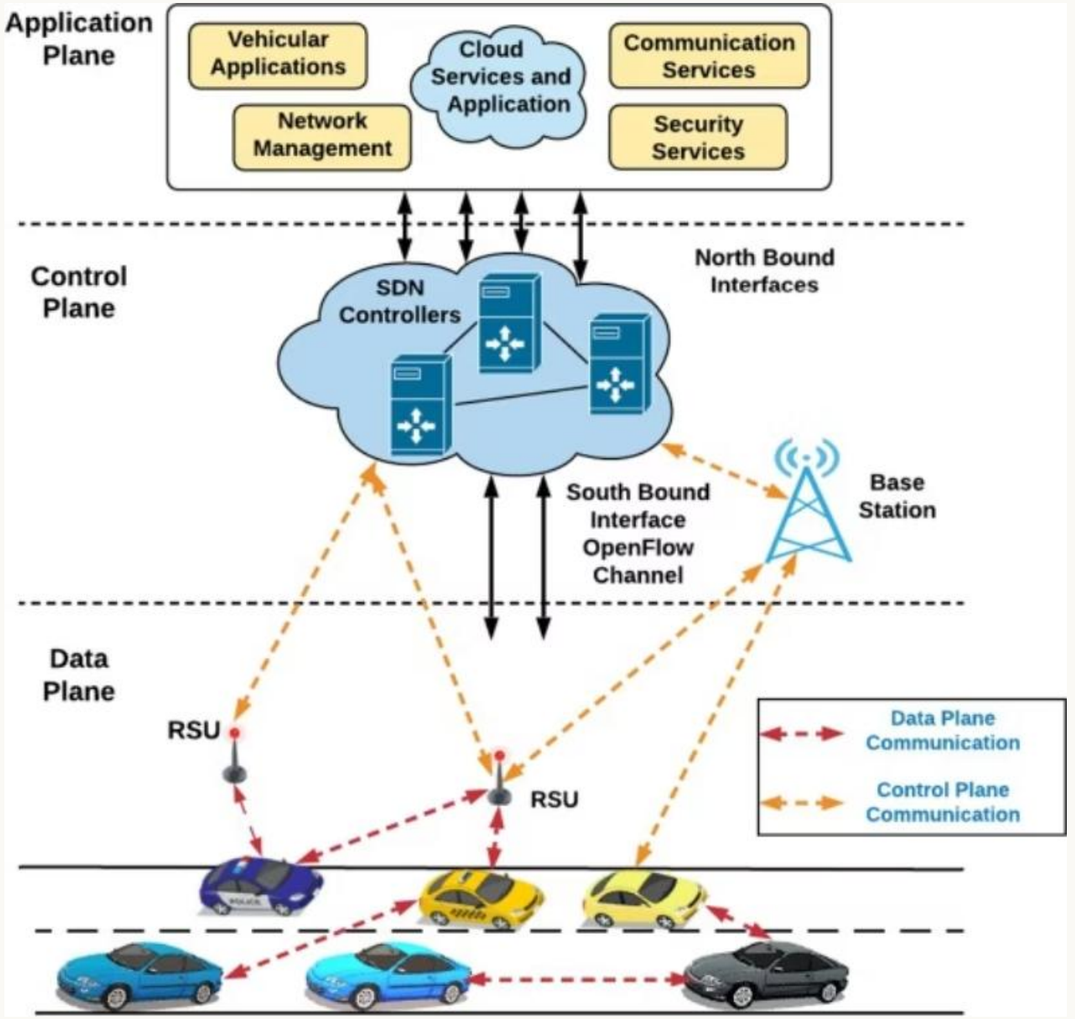
- Aplicaciones Vehiculares: Sistemas anticolisión, navegación adaptativa.
- Servicios en la Nube: Procesamiento de datos masivos.
- Servicios de Seguridad: Autenticación centralizada para vehículos y dispositivos IoT, gestionada por SDN.

Plano de Control (SDN):

- Controladores SDN: Coordinan políticas de red IoT.
- Interfaces Norte/Sur: La norte puede enviar datos de congestión a la nube. La sur gestiona físicamente RSUs, estaciones base y dispositivos IoT.

Plano de Datos:

- RSUs: Actúan como nodos de comunicación.
- Estación Base.



Definición de la Congestión

Saturación

Exceso de paquetes que sobrepasan la capacidad de procesamiento.

Retrasos

Aumento en tiempos de respuesta y latencia en la red.

Pérdidas

Descarte de paquetes por sobrecarga en buffers.

4 Degradación

Reducción del rendimiento general de la red.

Prevención de Congestión

Monitoreo en tiempo real

Análisis continuo de patrones de tráfico en toda la red.

Enrutamiento adaptativo

Ajuste dinámico de rutas basado en condiciones actuales.

Optimización automática

Redistribución inteligente de cargas para maximizar eficiencia.

Reducción de costos

Menor dependencia de hardware especializado y operación simplificada.

Redes Neuronales de Grafos en SDN

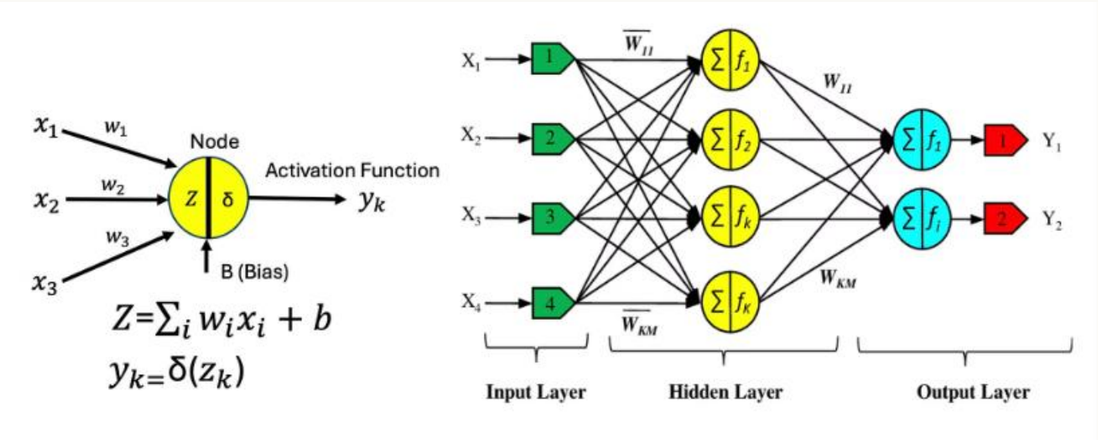
Soluciones avanzadas para gestión y seguridad de redes definidas por software.

¿Qué es una Red Neuronal Básica?

Una red neuronal básica es un modelo computacional inspirado en el funcionamiento del cerebro humano. Está compuesta por unidades llamadas neuronas artificiales conectadas entre sí para transmitir y procesar información.

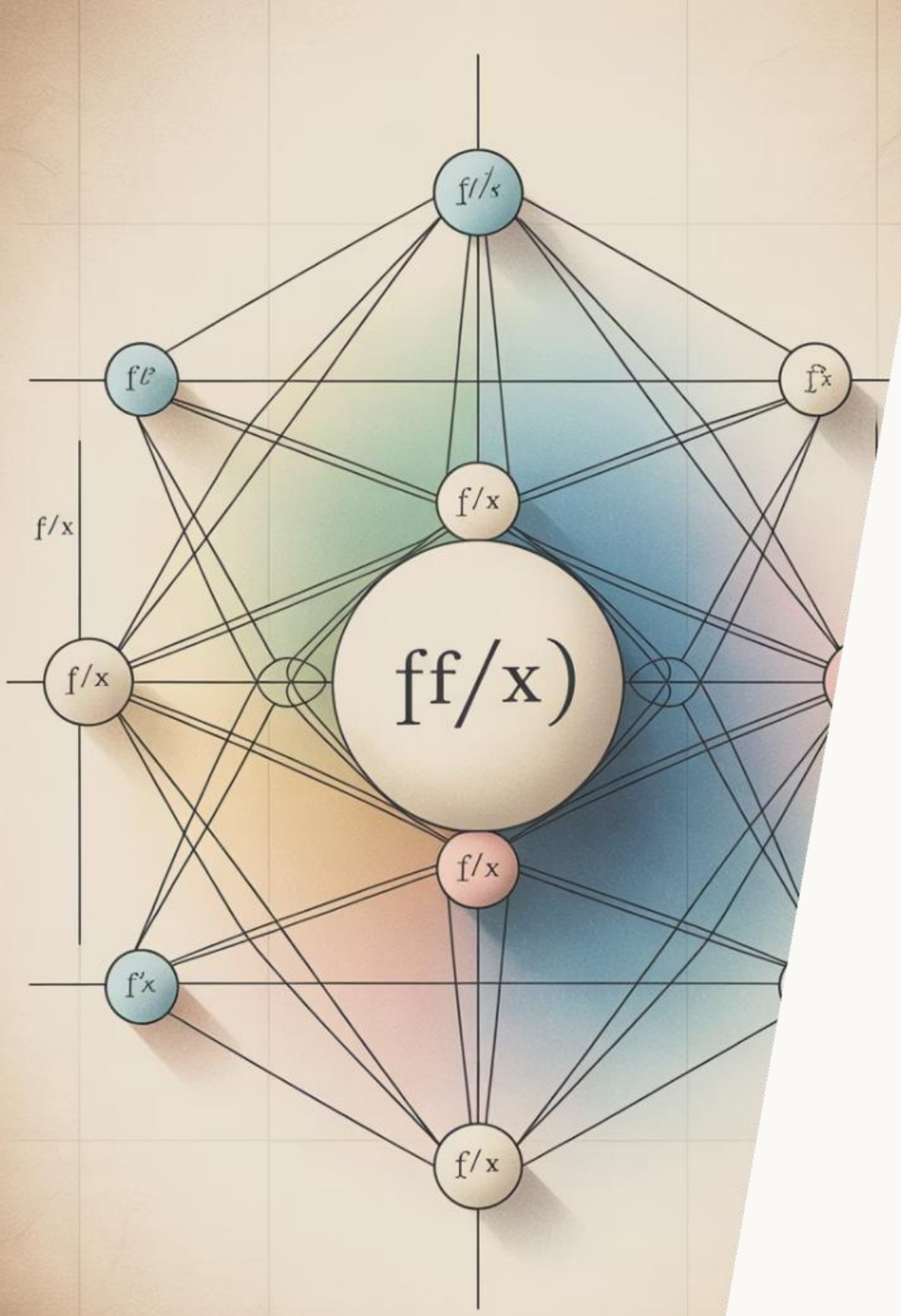
Componentes Principales

- Neuronas (nodos): Unidades de procesamiento que reciben, procesan y transmiten señales
- Conexiones (pesos): Enlaces entre neuronas que determinan la importancia de cada entrada
- Función de activación: Determina si y cómo una neurona se activa basándose en sus entradas
- Capas: Organizan las neuronas en grupos (entrada, ocultas, salida)



Estructura básica de una red neuronal con capa de entrada, capa oculta y capa de salida

A través del entrenamiento con ejemplos, la red neuronal ajusta sus pesos para minimizar el error y mejorar su capacidad de realizar tareas como clasificación, regresión o reconocimiento de patrones.



¿Qué son las Redes Neuronales Neuronales de Grafos?

Las GNN son una evolución de las redes neuronales artificiales diseñadas específicamente para procesar datos estructurados como grafos.

Procesamiento de Grafos Grafos

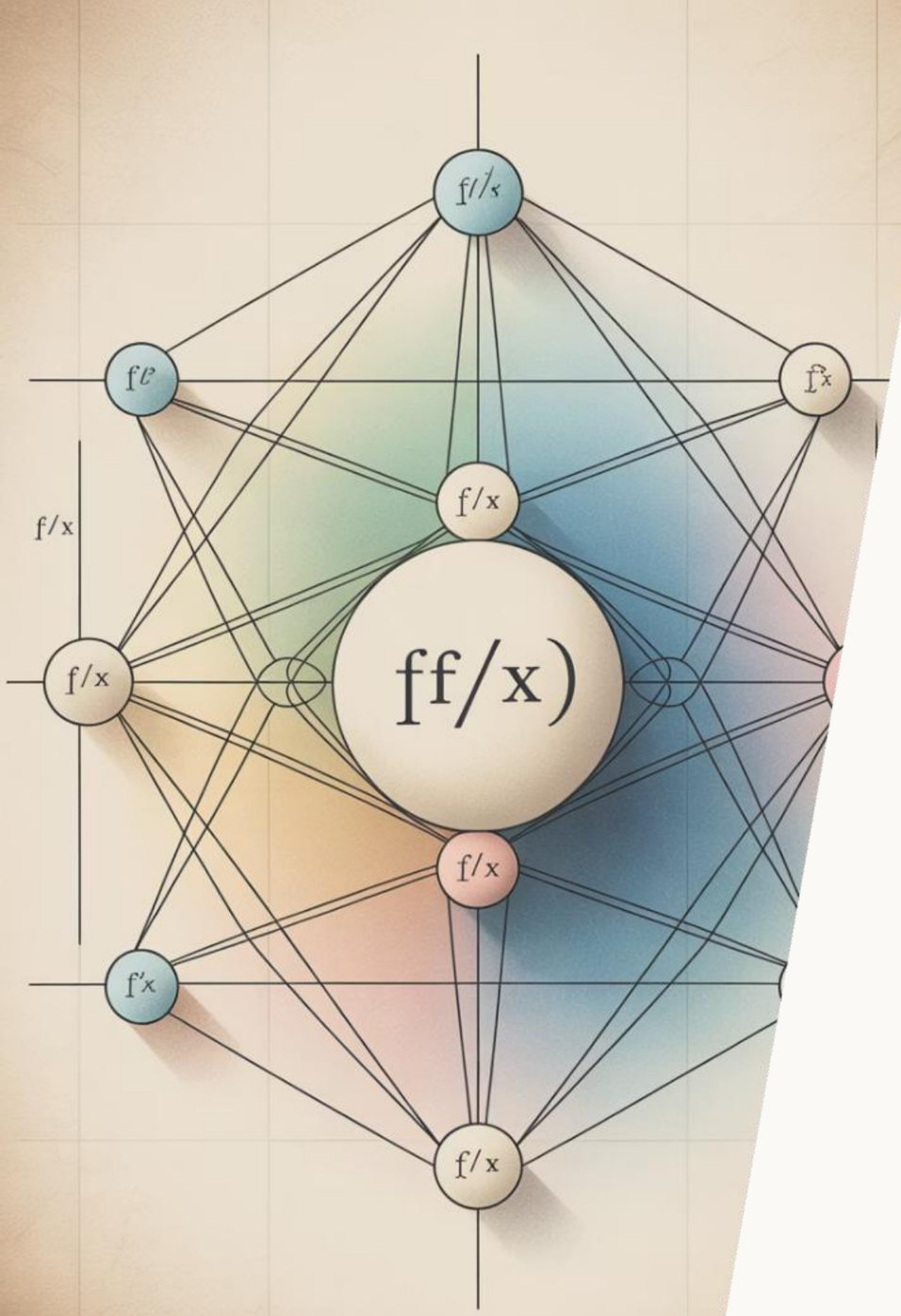
Operan directamente sobre estructuras de grafos, preservando las relaciones entre nodos.

Aprendizaje Relacional Relacional

Capturan dependencias complejas entre elementos interconectados de la red.

Aplicación en SDN

Ideales para redes definidas por software donde la topología es dinámica.



¿Qué son las Redes Neuronales de Grafos?

Red neuronal para datos datos estructurados

Diseñada específicamente para grafos

Nodos y aristas

Representan entidades y sus relaciones

Paso de mensajes

Comunicación entre nodos vecinos

¿Por qué usar GNN en SDN?

Representación natural

Las redes son grafos por naturaleza

Captura de dependencias

Entre topología, enrutamiento y tráfico

Generalización

Adaptable a nuevas topologías

Control centralizado

SDN proporciona datos para entrenamiento

Predicción de Congestión en SDN

Problema

Congestión afecta rendimiento

Monitorización

SDN permite control centralizado

Predicción

GNN aprende de patrones históricos

Modelado de Red para Predicción

Topología como grafo

Nodos: dispositivos, aristas: enlaces

Características

Carga, ancho de banda, latencia

Predicción

Probabilidad de congestión en enlaces

Procesamiento GNN

Análisis del grafo completo

Tipos de GNN para Predicción

Redes Convolucionales de Grafos (GCN)

Aplican convoluciones a grafos

Redes de Atención de Grafos Grafos (GAT)

Utilizan mecanismos de atención

Redes Espacio-Temporales (STGNN)

Para datos de tráfico dinámicos

Casos de Uso: Predicción de Congestión

Optimización de enrutamiento

Evita enlaces congestionados

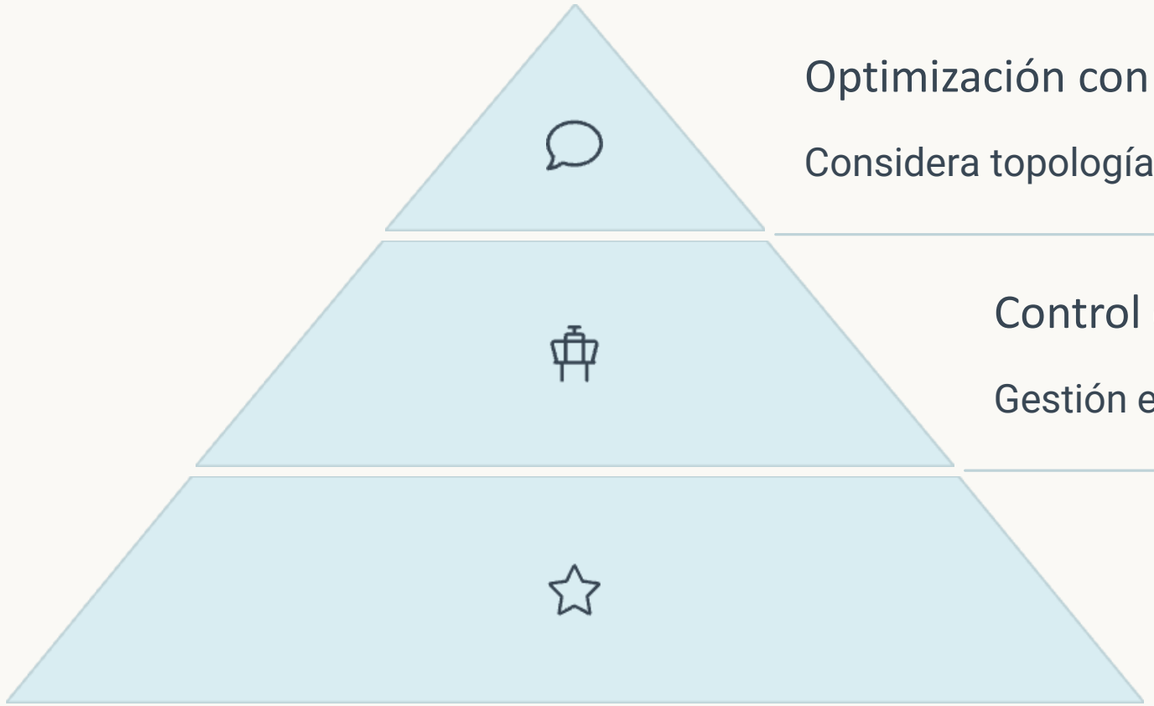
Asignación proactiva

Previene congestión futura

Mejora de QoS

Para aplicaciones sensibles a latencia

Enrutamiento IoT en SDN con GNN



Optimización con GNN

Considera topología y tráfico

Control centralizado SDN

Gestión eficiente del enrutamiento

Dispositivos IoT

Recursos limitados, desafíos únicos

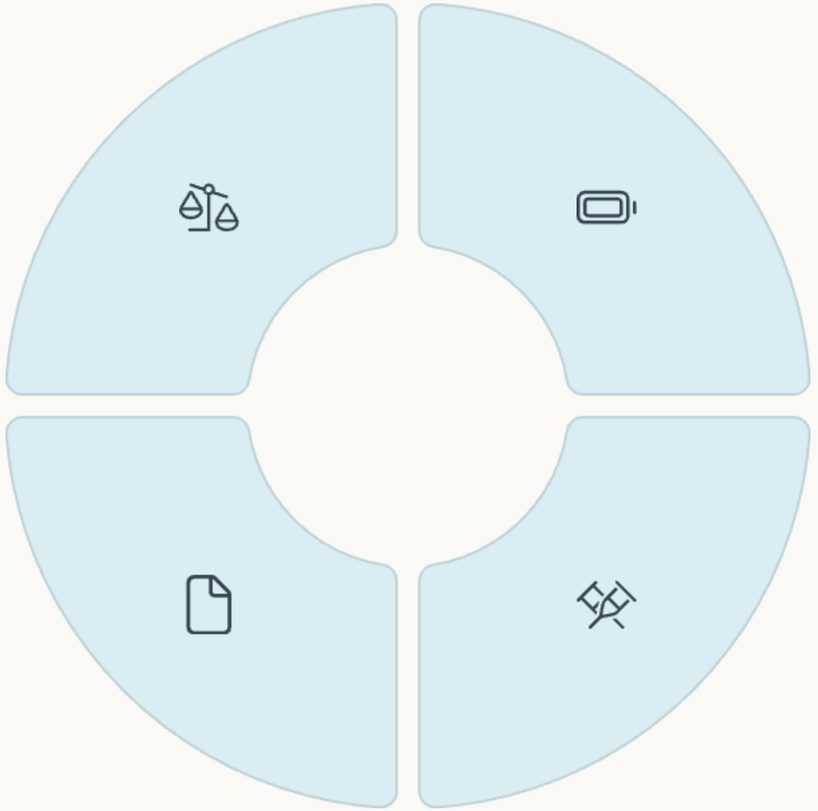
Desafíos del Enrutamiento IoT

Escalabilidad

Gran número de dispositivos

Recursos limitados

Energía, computación, ancho de banda



Requisitos QoS

Necesidades diversas según aplicación

Topologías dinámicas

Movilidad de dispositivos

GNN para Optimización de Rutas IoT

Modelado de topología

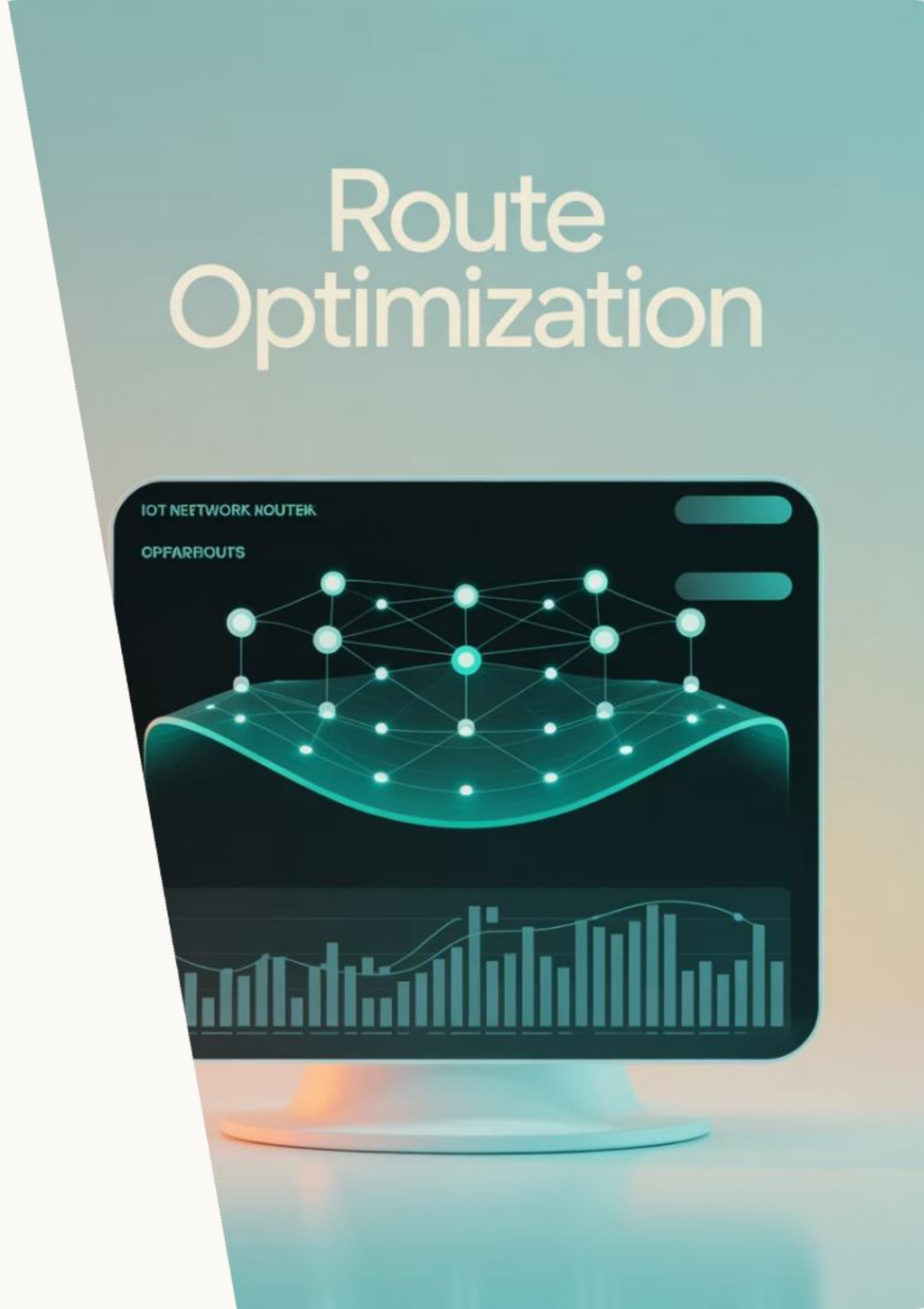
Red IoT representada como grafo

Políticas eficientes

Minimiza latencia y consumo energético

Aprendizaje por refuerzo

GNN+DRL para enrutamiento adaptativo



Caso de estudio

Enrutamiento inteligente con prevención de congestión.

Objetivo

Desarrollar un algoritmo de enrutamiento inteligente para redes definidas por software (SDN) que garantice la calidad de servicio (QoS) y administre eficientemente los recursos de la red, reduciendo los problemas de congestión.

$G(V,E)$:Una red de telecomunicaciones se representa como un grafo dirigido acíclico.

$V = \{n_1, n_2, \ldots n_k\}$:Conjunto de nodos en la red, n_i(equipos finales, enrutadores, switches).

$E = \{(i,j)\} | i,j \in I, i \neq j\}$:Conjunto de enlaces en la red, $l_{i,j}$(Enlace de red de los nodos i, j).

$\lambda_{i,j}$:Ancho de banda disponible entre los nodos i y j.

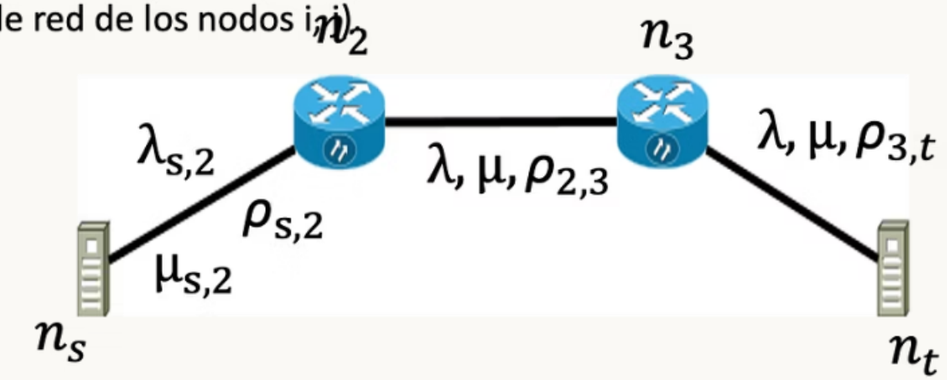
$\mu_{i,j}$:Retardo entre los nodos i y j.

$\rho_{i,j}$:pérdida de paquetes entre los nodos i y j.

$h_{i,j}$:Salto del nodo i al j.

s :Nodo de origen.

t :Nodo de destino.



Selección de ruta:

$P_{s,t} = \{p_1, p_2, \ldots, p_n\}$:Conjunto de rutas de enrutamiento del nodo de origen n_s al nodo de destino n_t.

$p_n = \{e_1, e_2 \ldots e_m\}, p \in P_{s,t}$:Ruta de extremo a extremo n_s a n_t .

$H = \sum_{e \in P} e$:Ruta con el mínimo número de enlaces.

$B = min_{\forall e \in p} \left\{ \frac{1}{\lambda} \right\}$:Ruta con el mínimo costo de ancho de banda.

$D = \sum_{e \epsilon p} \mu$:Ruta con el menor retardo.

$PL = 1 - \prod_{e \epsilon p}(1 - e_\rho)$:Ruta con la menor pérdida de paquetes.

$$\boldsymbol{min_{e \in P}(D, B, PL, H)}$$

$$t_h = \frac{Pk_{sc}}{T_t}$$: Throughput;

Donde:
Pk_{sc}= paquetes recibidos. T_t=Tiempo total de transmisión.
Pk_f= paquetes Fallidos.

$$Pk_{sc} = \frac{Pk_{tx} - (Pk_{rx} + \sum_{i=1}^{Prx} Pk_f)}{T_t}$$

Descripción formal del proceso de enrutamiento

Proceso de enrutamiento en SDN

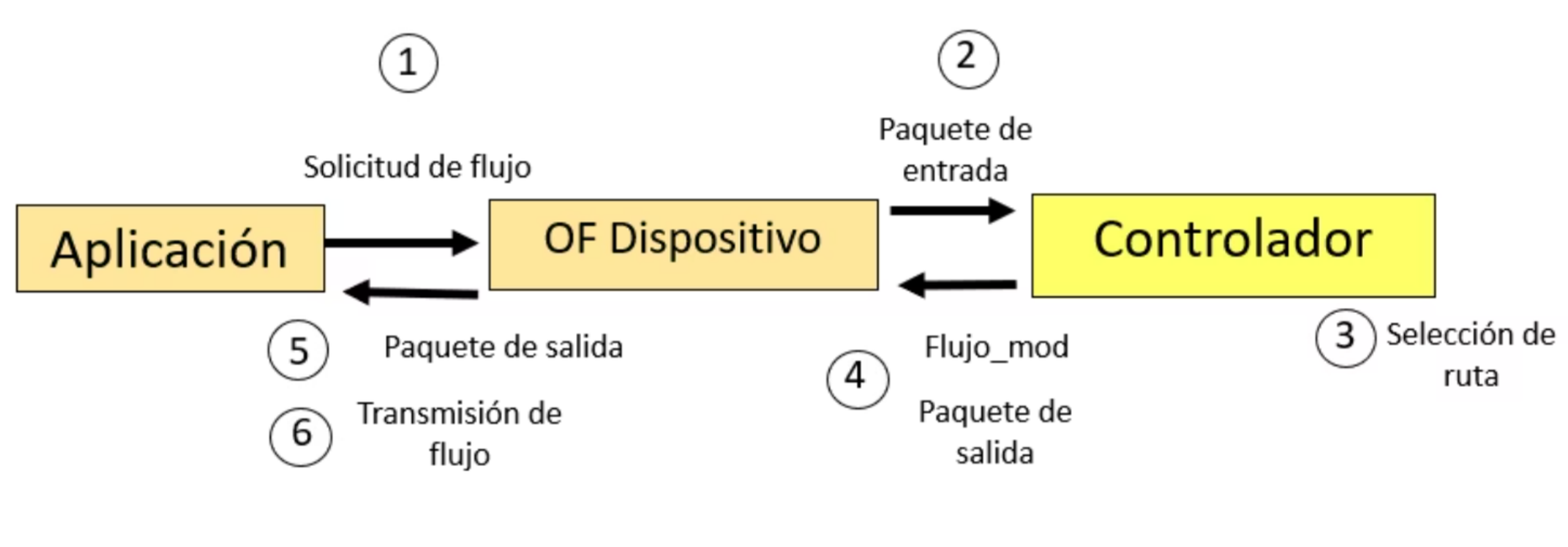


Figura 8. Proceso de enrutamiento orientado a conexión en SDN.

Donde:

OF: Dispositivo OpenFlow.

Paquete de entrada: Mensaje enviado por conmutador cuando un paquete no tiene ninguna entrada de flujo en las tablas de flujo.

Paquete de salida: Mensaje con respuesta del controlador.

Flujo_mod: Reglas de flujo.

Propuesta de enrutamiento en SDN

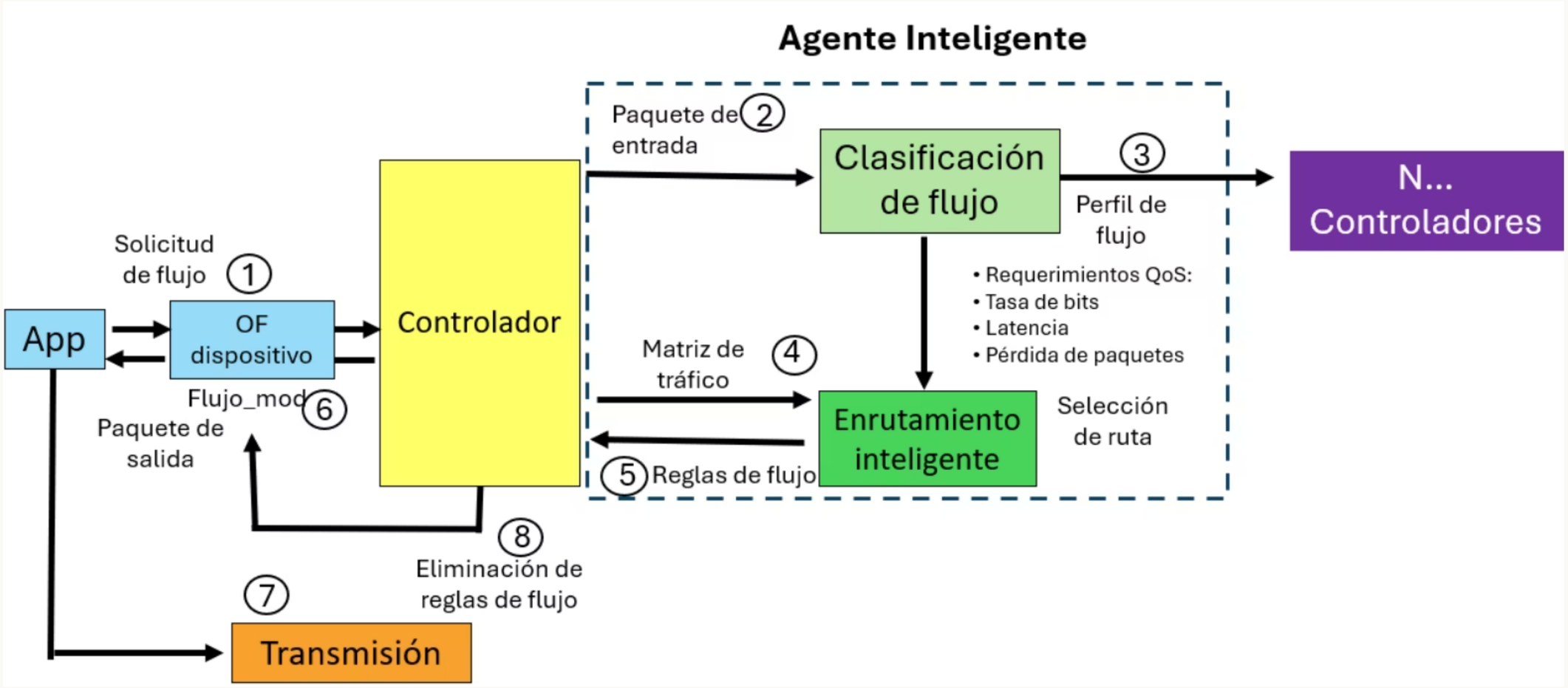


Figura 9. Arquitectura propuesta para el proceso de enrutamiento en SDN.

Redes Neuronales de Grafos (GNN)

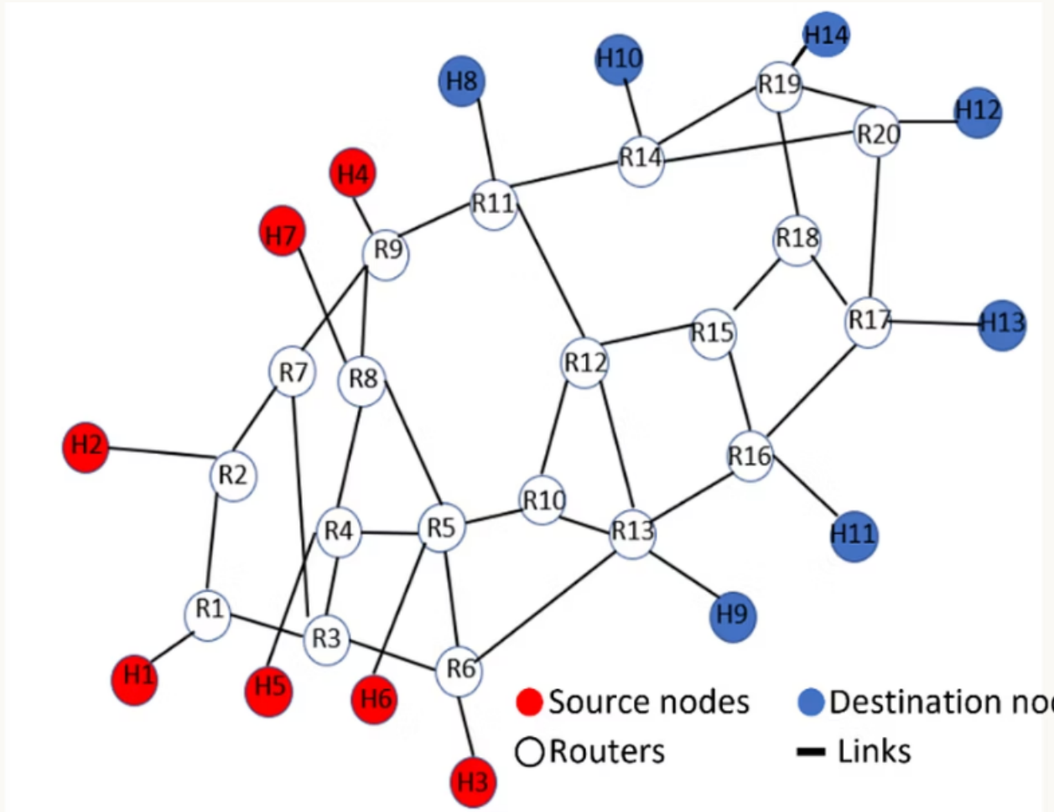


Figura 24. Topología de ARPANET para enrutamiento dinámico [11, 12].

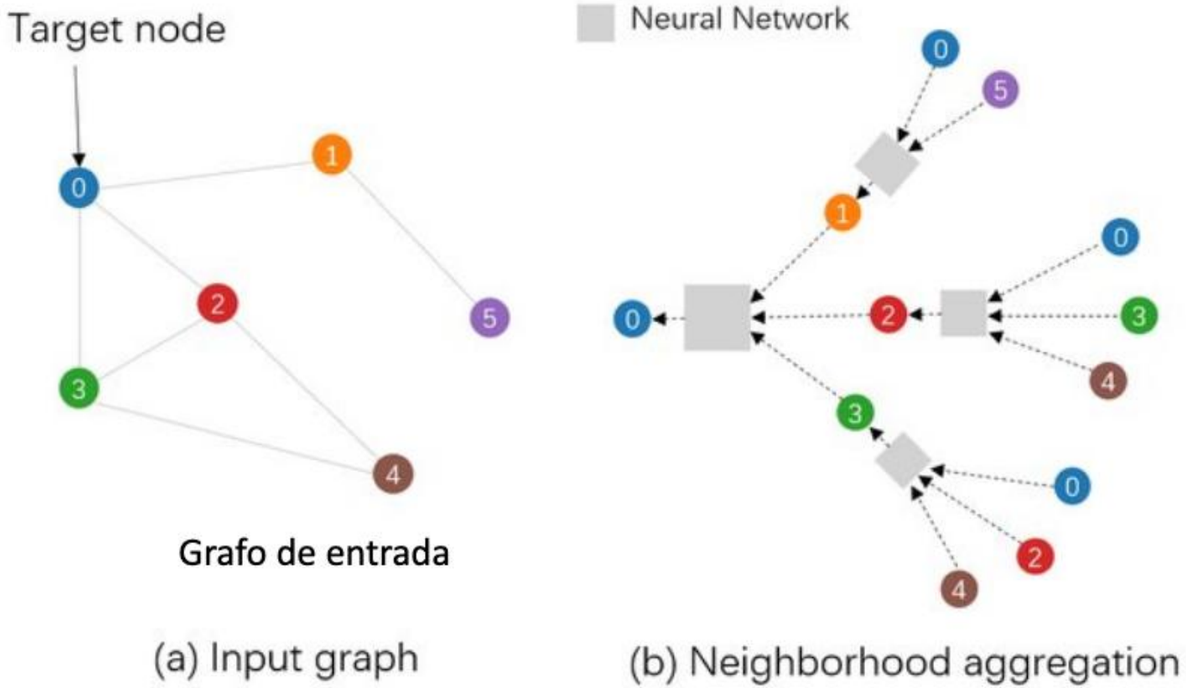
Tabla 3. Parámetros de flujo 5QI (3GPP TS 23.501) [13]

Prioridad	Aplicación	Duración (s)	Ancho de banda(Mbps)	Retardo (ms)	Pérdida de paquetes(%)
1	VoIP	120	10	11	10^{-2}
2	Audio	105	15	10	10^{-3}
3	Videoconferencia	60	25	12	10^{-2}
4	Video	45	20	14	10^{-4}
5	Mejor esfuerzo	30	5	15	N/A

[11] Building a Digital Twin for network optimization using Graph Neural Networks (November, 2022) https://www.sciencedirect.com/science/article/pii/S1389128622003681
[12] Deep Reinforcement Learning Based Routing in IP Media Broadcast Networks: Feasibility and Performance (June 2022) https://ieeexplore.ieee.org/abstract/document/9793657 (September, 2022)
[13] Saboorian, T., Xiang, A., & Thiébaut, L. (2017). Network slicing and 3GPP service and systems aspects (SA) standard. *IEEE Software Defined Networks, IEEE Softwarization: Piscataway, NJ, USA*, *7*.

Evaluación

Red Neuronal de Grafo (GNN)



Grafo de entrada

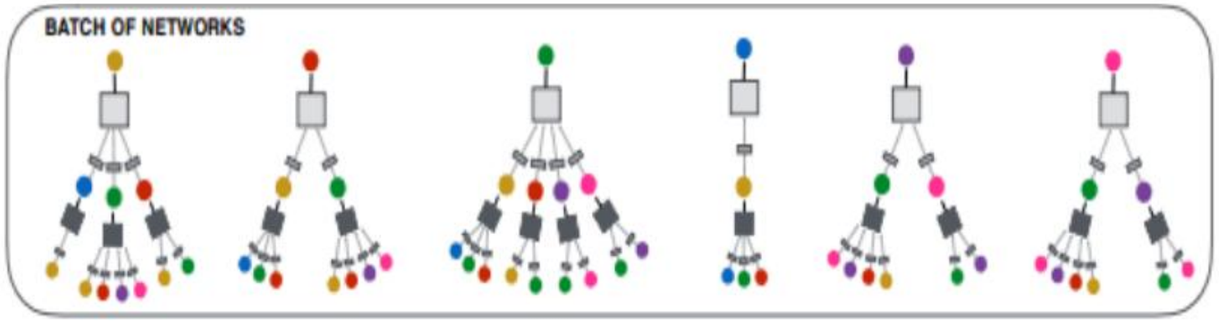


Figure 20. Representación de Red Neuronal de Grafo (GNN) [10].

Message Passing Update and Aggregation Functions

$$h_i' = \delta \sum_{j \epsilon N(i)} W * h_j$$

Attention coeffect

$$e_{i,j} = a(\overline{W}h_i || \overline{W}h_j)$$

Normalized Attention Coeffect

$$a_{i,j} = softmax_j(e_{i,j}) = \frac{\exp(e_{i,j})}{\sum_k \exp(e_{i,k})}$$

$k \epsilon N(i)$

[10] Jin, Z., Wang, Y., Wang, Q., Ming, Y., Ma, T., & Qu, H. (2022). Gnnlens: A visual analytics approach for prediction error diagnosis of graph neural networks. *IEEE Transactions on Visualization and Computer Graphics*.

Enrutamiento Inteligente

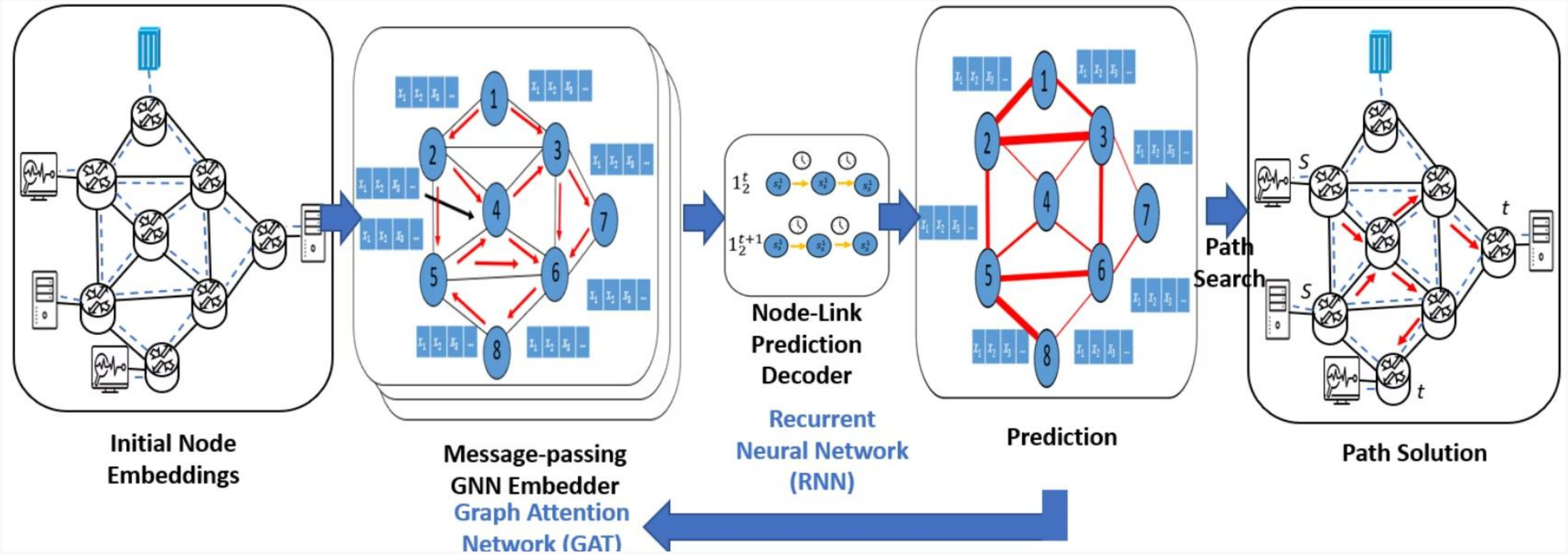
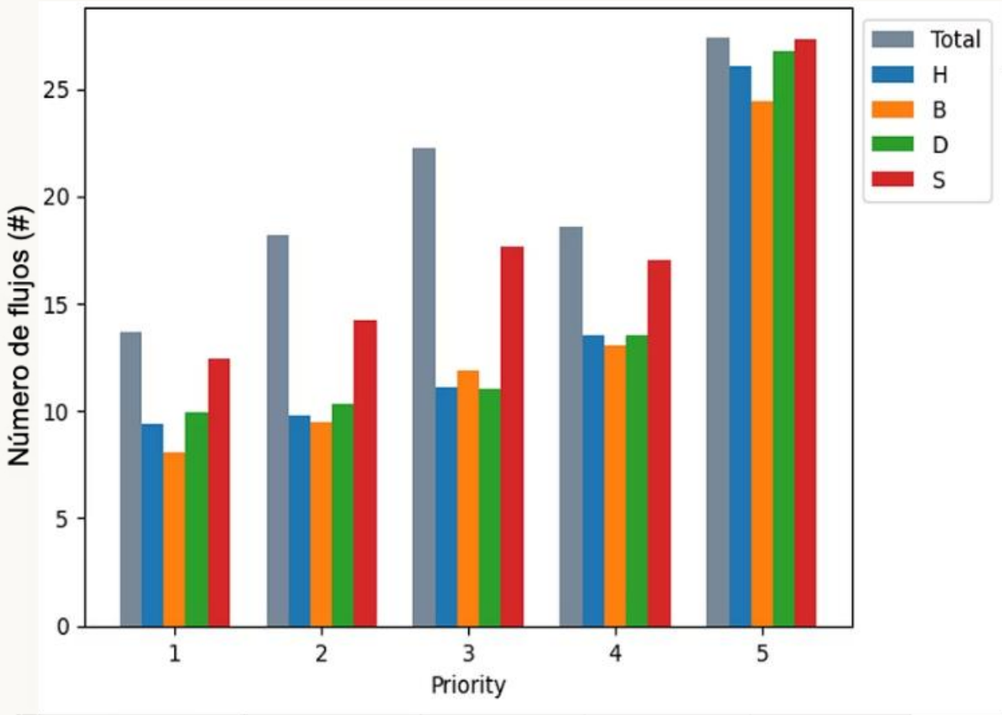


Figure 23. Representation of the routing process with GNN.



Método de enrutamiento	H	B	D	S
Puntuación normalizada	0.6660	0.6318	0.6861	0.8755

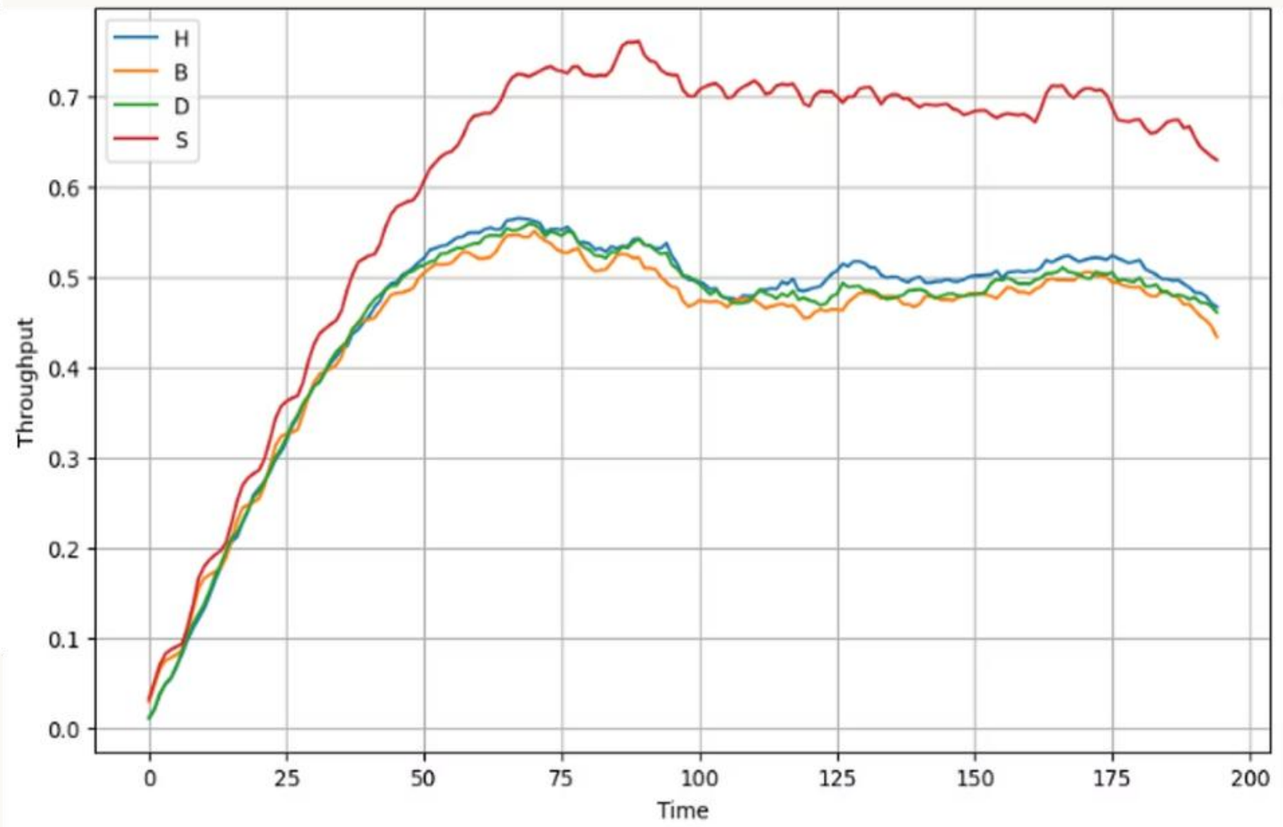


Figura 26. Promedio de flujos enrutados satisfactoriamente (distribución Poisson P0=0.488 P1=0.0756, P2=0.0924, P3=0.1104, P4=0.0972, P5=0.1356). a)Número promedio de flujos satisfactorios. b) Volumen de tráfico: Métodos de enrutamiento: (H) ruta más corta, (B) ruta con mayor ancho de banda disponible, (D) ruta con menor retardo y (S) enrutamiento inteligente.

Resultados

Ciberseguridad en SDN con GNN

Visibilidad mejorada

SDN ofrece mejor control

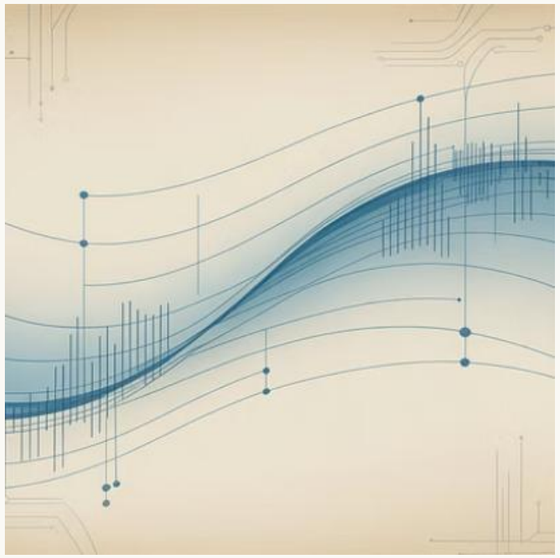
Modelado de comportamiento

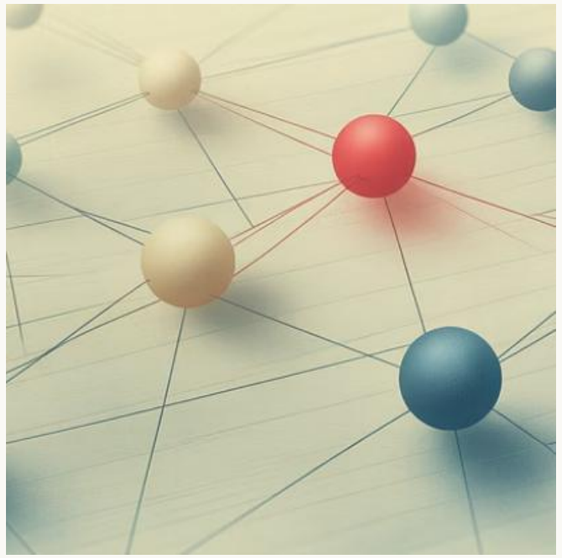
GNN analiza patrones de tráfico

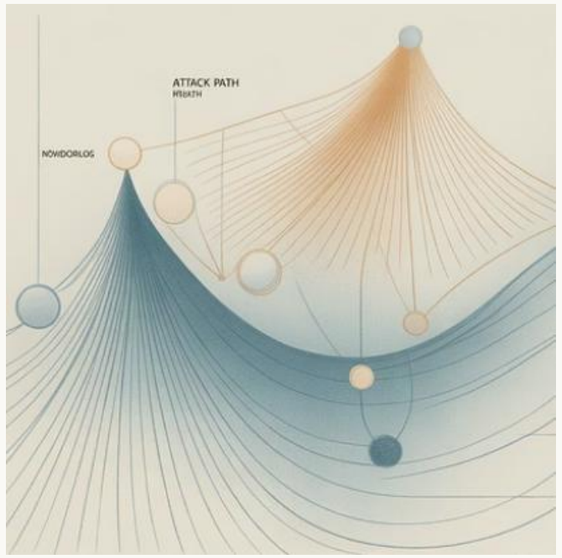
Detección de amenazas

Intrusiones, malware, ataques DDoS

Modelado de Ciberseguridad

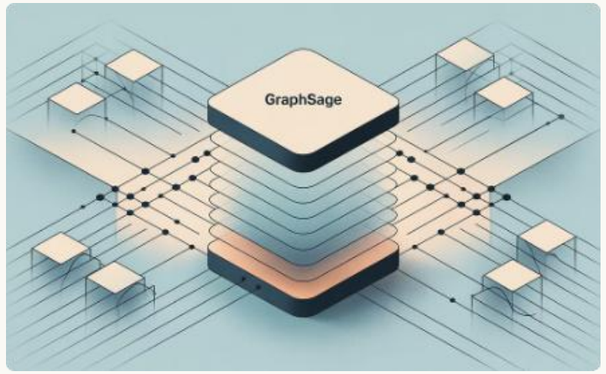






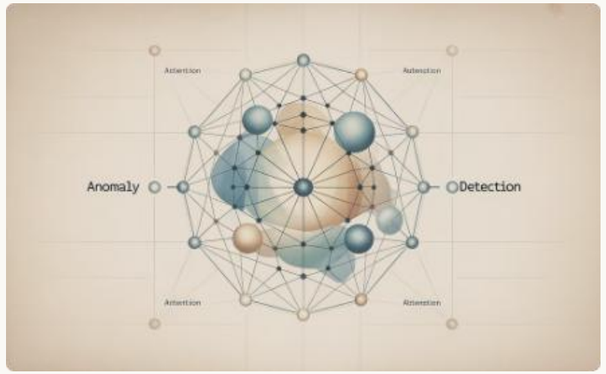
GNN aprende patrones normales e identifica desviaciones como ataques potenciales.

Tipos de GNN para Ciberseguridad



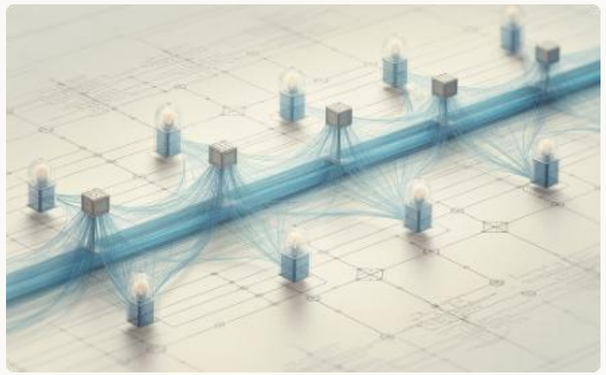
GraphSAGE

Detección de intrusiones en IoT



GAT

Detección de anomalías contextuales



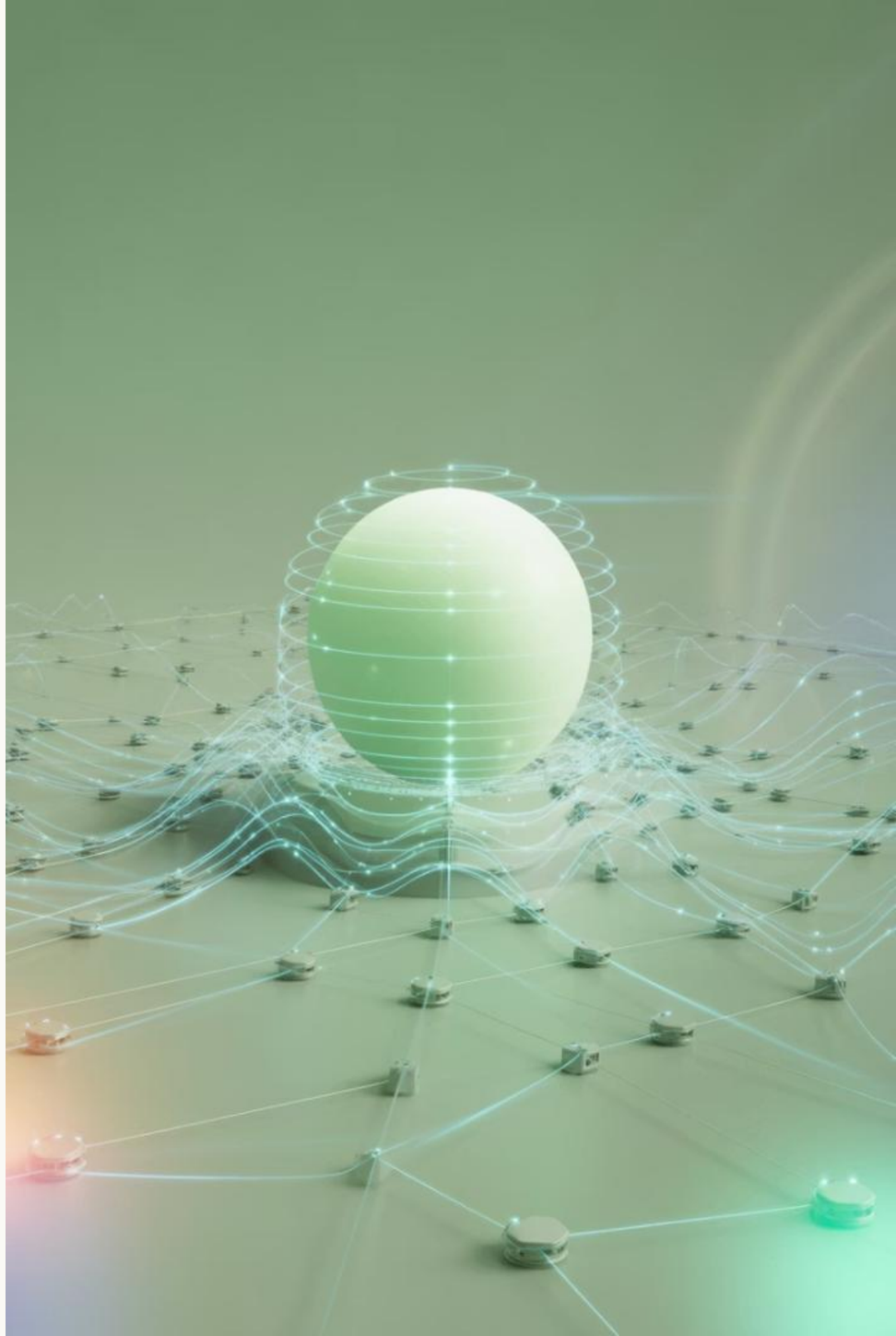
Aprendizaje Federado

Preserva privacidad en detección

Uso de GNN para Detección de Ataques DDoS en Redes SDN

Las redes definidas por software (SDN) revolucionan las comunicaciones modernas. Sin embargo, son vulnerables a ataques distribuidos de denegación de servicio.

Exploraremos cómo las Graph Neural Networks pueden transformar la detección de estos ataques.



¿Qué es SDN y por qué es vulnerable?

Arquitectura SDN

Separa el plano de control del plano de datos. Permite programabilidad y flexibilidad sin precedentes.

Facilita la gestión centralizada de toda la red desde un único punto.

Vulnerabilidades críticas

El controlador centralizado representa un punto único de fallo. Si cae, toda la red queda comprometida.

La arquitectura abierta expone nuevas superficies de ataque.

Ataques DDoS en Entornos SDN

Inundación de tráfico

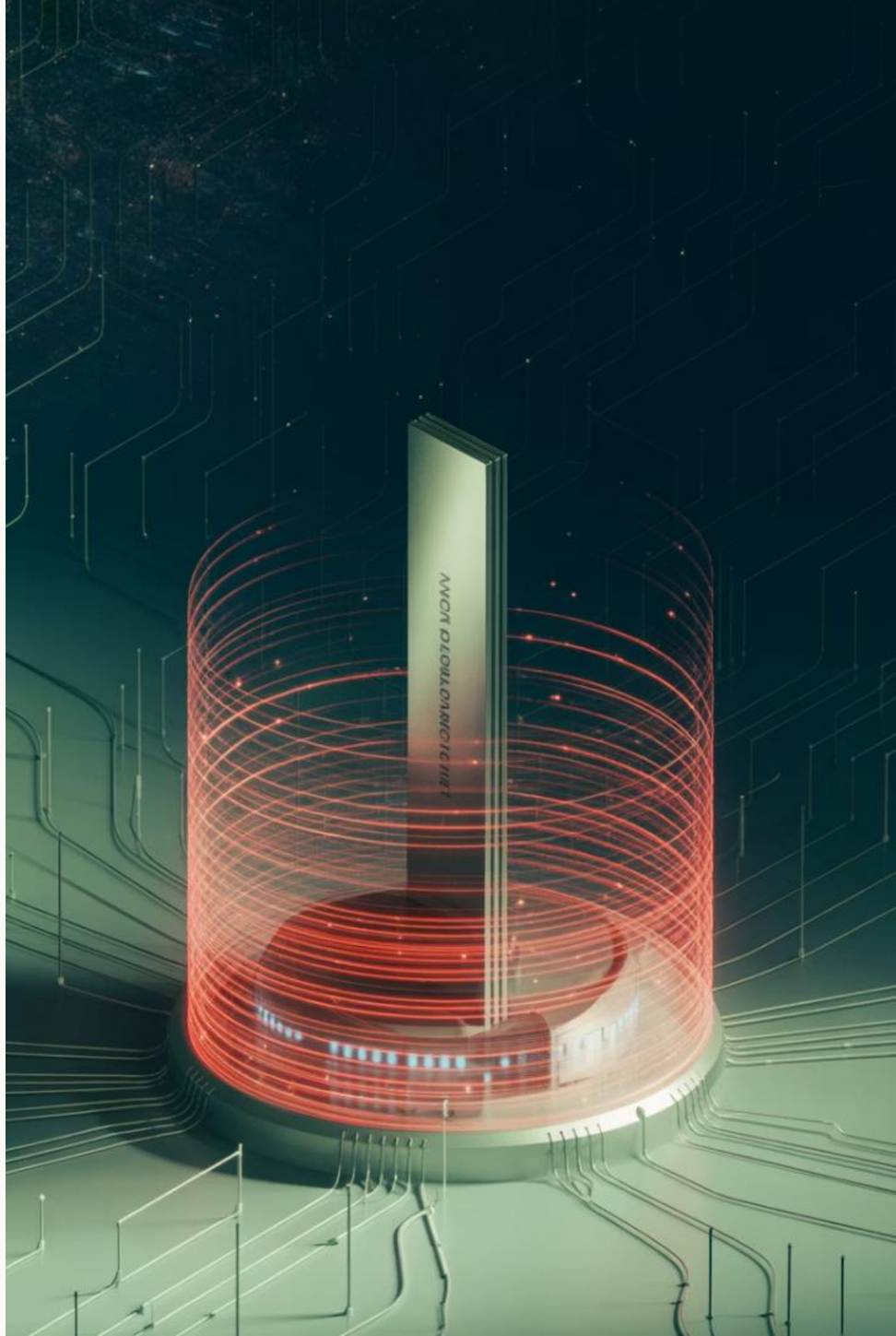
Los atacantes envían miles de paquetes que saturan el controlador SDN.

Sobrecarga de recursos

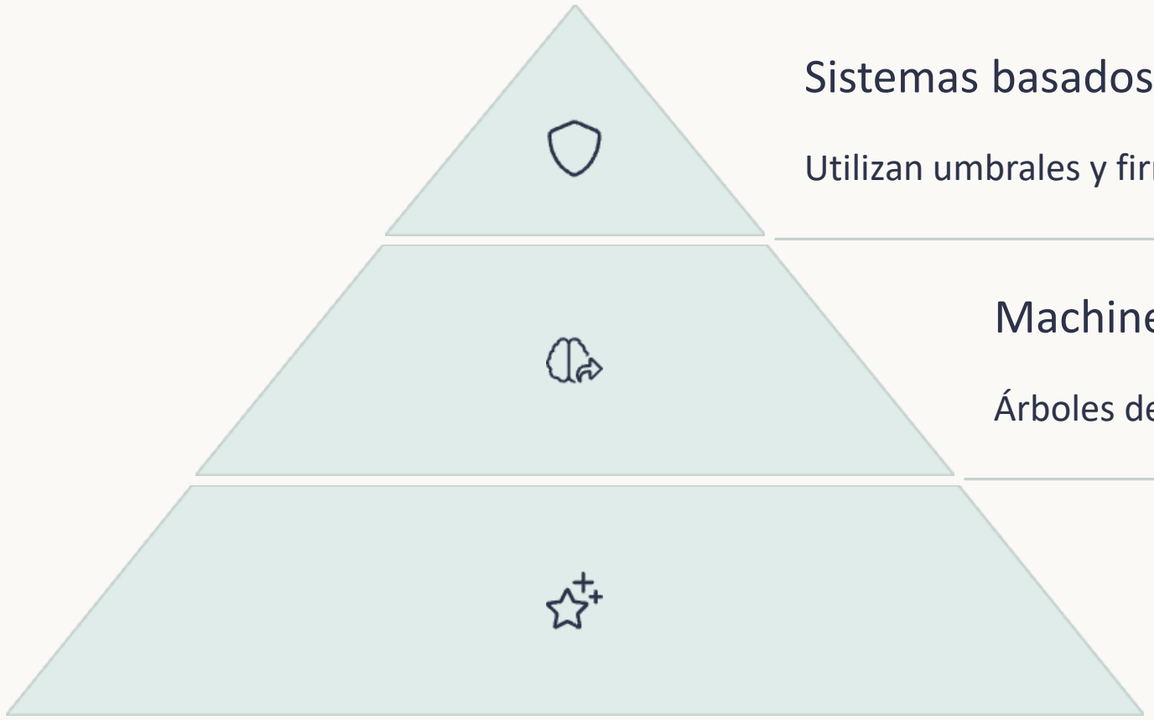
El controlador agota memoria y CPU procesando solicitudes maliciosas.

Degradación de servicio

La red sufre latencia elevada o deja de responder completamente.



Técnicas Clásicas de Detección de DDoS



Sistemas basados en reglas

Utilizan umbrales y firmas predefinidas

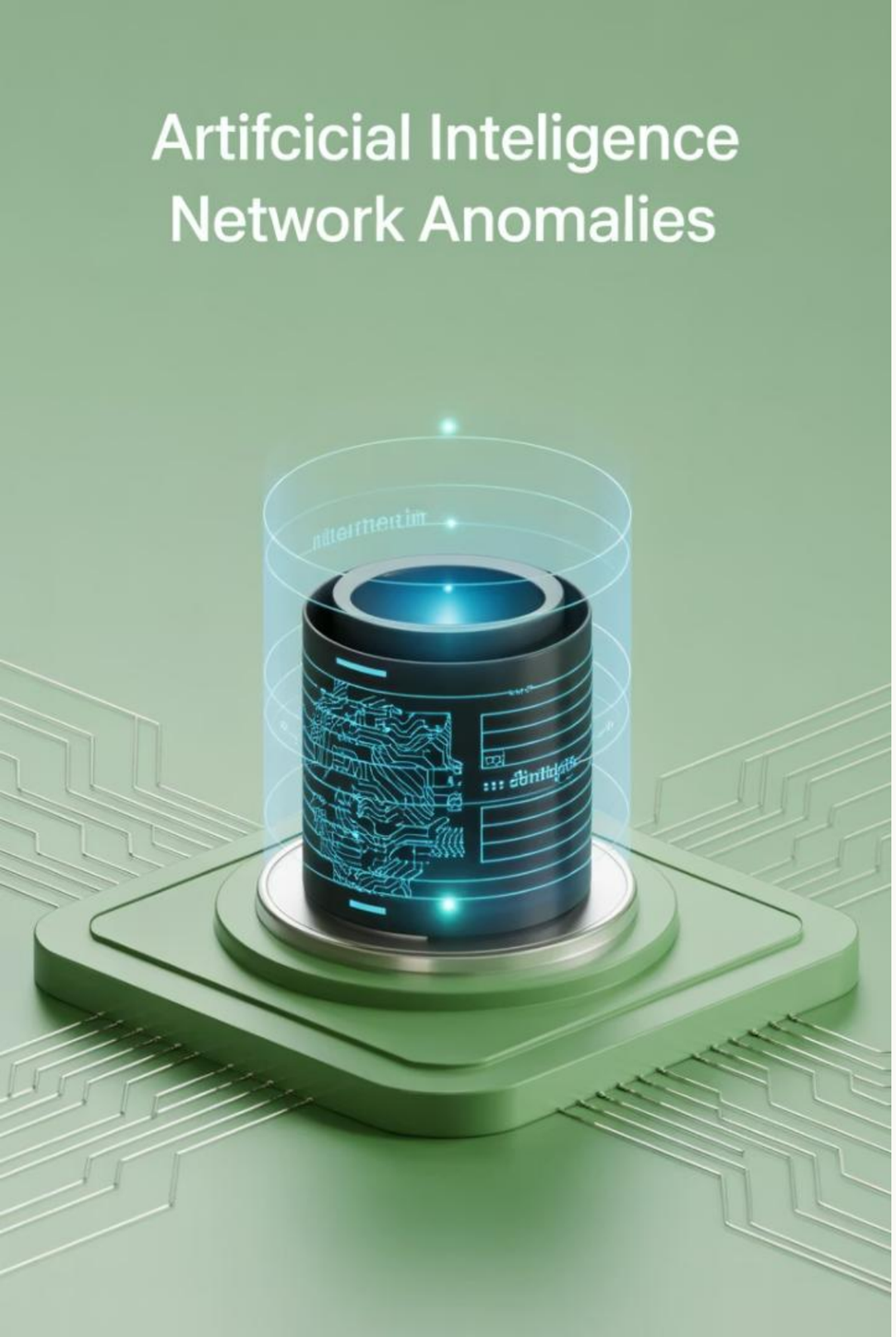
Machine learning tradicional

Árboles de decisión, SVM, Naïve Bayes

Análisis estadístico

Detección de anomalías en patrones de tráfico

Estas técnicas enfrentan limitaciones importantes al no capturar la naturaleza relacional del tráfico de red.



Inteligencia Artificial en Seguridad SDN

Análisis en tiempo real

La IA procesa millones de paquetes simultáneamente, identificando anomalías instantáneamente.

Adaptación continua

Los modelos aprenden de cada ataque, mejorando su capacidad de detección con el tiempo.

Reducción de falsos positivos

Distingue con precisión entre tráfico legítimo y malicioso, minimizando alertas innecesarias.

Uso de Graph Neural Networks (GNN)

Modelado en grafo

Representa la red como nodos interconectados, capturando su estructura natural.

Detección de anomalías

Identifica subgrafos anómalos que representan comportamientos maliciosos.

Propagación de mensajes

Los nodos comparten información con sus vecinos, creando representaciones contextuales.

Aprendizaje profundo

Extrae patrones complejos que métodos tradicionales no pueden detectar.

Caso Práctico: Detección de DDoS en SDN con GNN

Modelado de la topología

La red SDN se representa como un grafo donde cada nodo es un switch o host. Las conexiones son enlaces de red.

Extracción de características

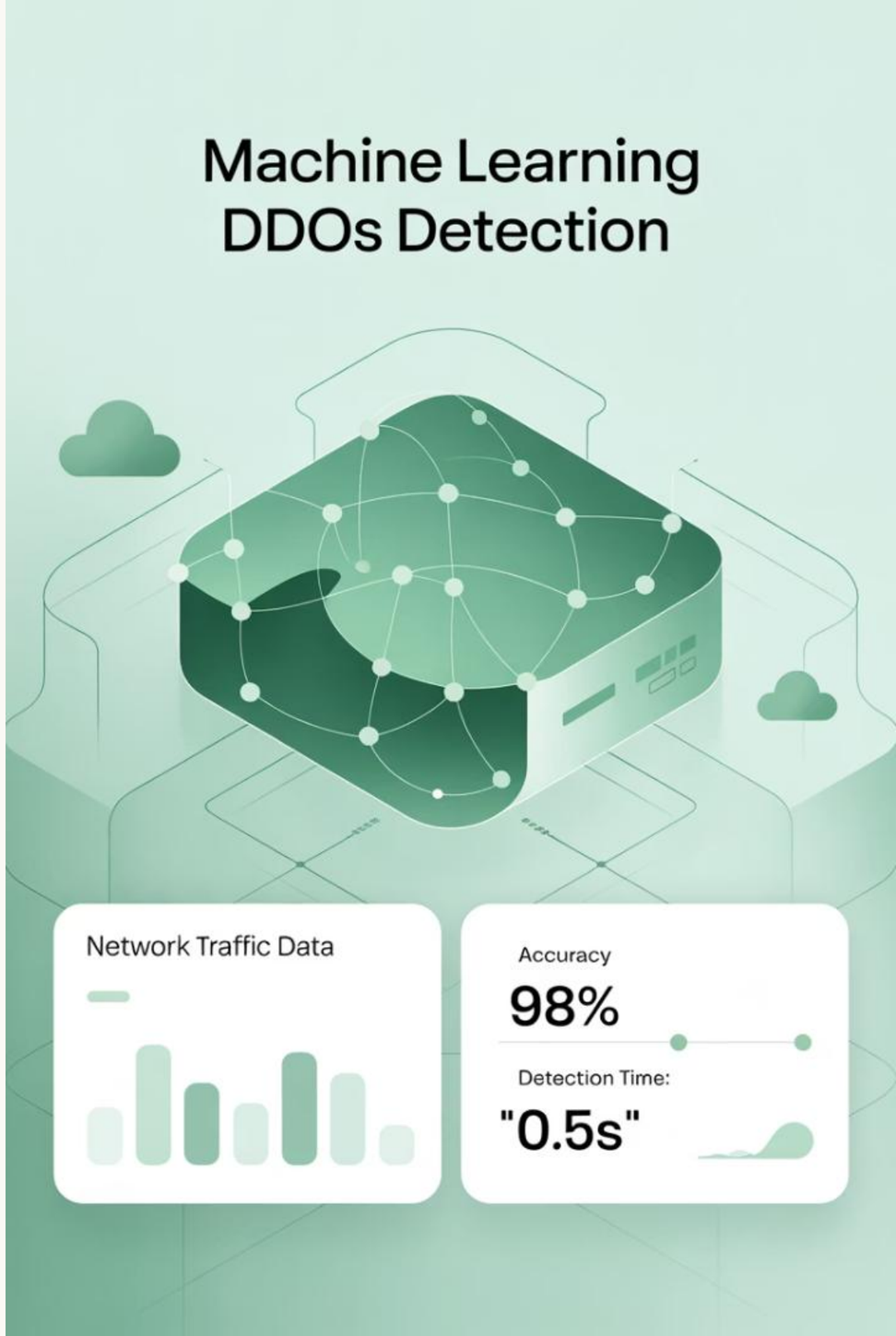
Se capturan métricas de flujo como volumen, distribución de puertos y patrones temporales.

Entrenamiento del modelo

La GNN aprende a distinguir patrones legítimos de maliciosos con datasets etiquetados.

Evaluación y despliegue

El modelo logra 97% de precisión, superando a métodos tradicionales por 15%.



Conclusiones y Retos Futuros

1

Ventajas actuales

Las GNN ofrecen detección superior de ataques complejos con menor tasa de falsos positivos.

2

Desafíos pendientes

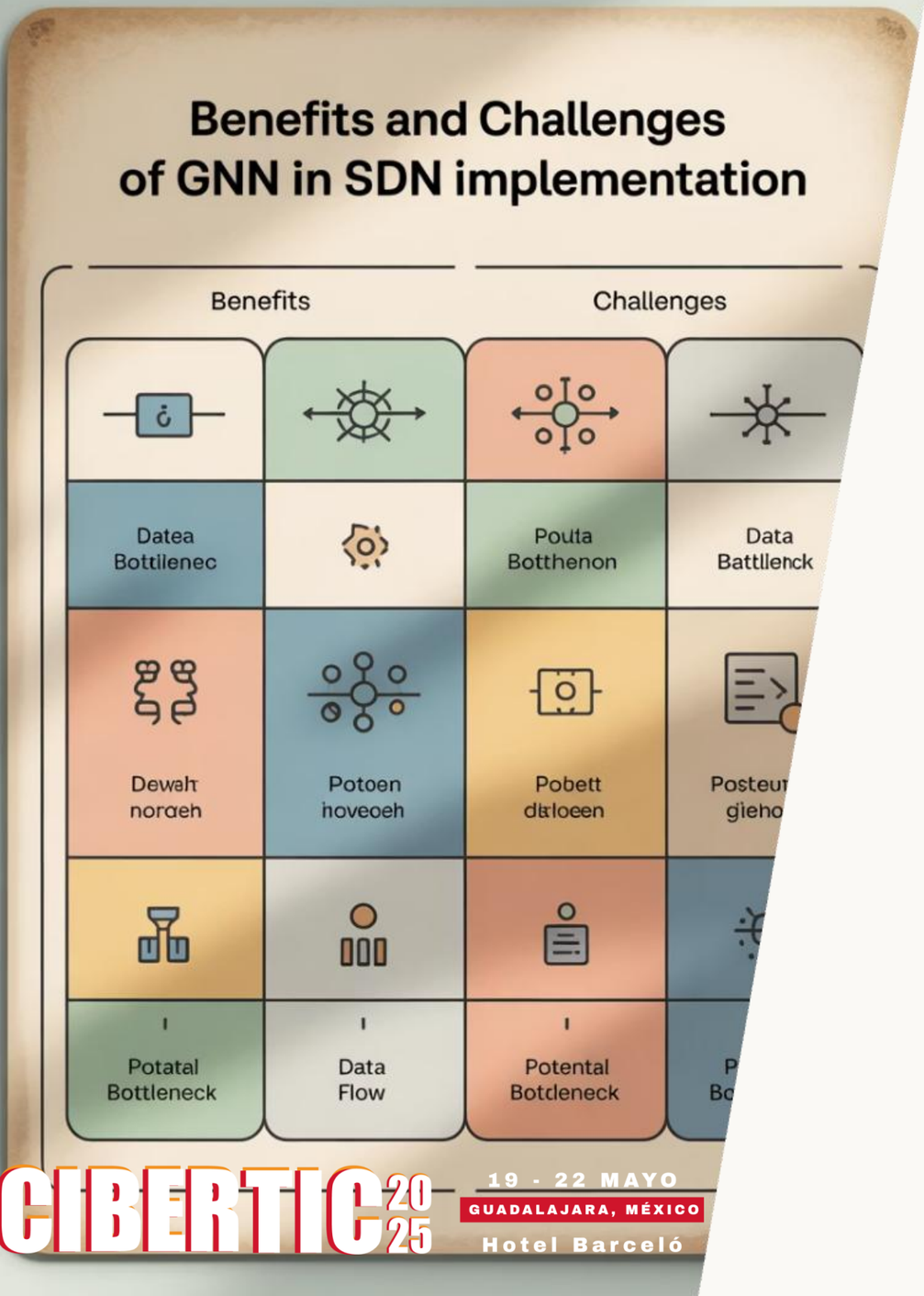
La escalabilidad sigue siendo un reto en redes muy grandes. El tiempo de respuesta debe optimizarse.

3

Próximos pasos

Integración con sistemas de mitigación automática y desarrollo de datasets más representativos.

El futuro de la seguridad en redes SDN será una combinación de inteligencia artificial avanzada y experiencia humana.



Desafíos y Retos

99.2%

Precisión en detección

Mejora significativa en seguridad

45%

Reducción de energía

En dispositivos IoT con rutas optimizadas

85%

Predicción de congestión

Exactitud en condiciones dinámicas

<5ms

Latencia de decisión

Desafío para implementación en tiempo real

Grupo de Investigación

Estudiantes están Invitados al posgrado EyT y CC

Dr. Raúl Rivera Rodríguez

Dr. Andrey Tchernykh

José Lozano Rizk

José E. González

Joan D. González