Ciencias y Saberes

ISSN 2960-8430

ANÁLISIS DE FOURIER APLICADO A LA DETECCIÓN DE ANOMALÍAS EN SEÑALES DE RED

Carlos Alberto Bermeo Zamora
cbermeoz@uteq.edu.ec
ORCID: https://orcid.org/0000-0001-6532-7889
Universidad Técnica Estatal de Quevedo - Ecuador

Erika Mabel González Tobar
egonzalezt2@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-3984-1427
Universidad Técnica Estatal de Quevedo - Ecuador

Kimberly Magaly López Cedeño
klopezc2@uteq.edu.ec
ORCID: https://orcid.org/0000-0002-6838-1474
Universidad Técnica Estatal de Quevedo - Ecuador

Recibido: 25/03/26
Aceptado: 23/04/26
Publicado: 01/05/26

RESUMEN

El crecimiento sostenido del tráfico de datos en las redes de telecomunicaciones ha dificultado la identificación oportuna de patrones maliciosos, saturaciones de canal y fallos operativos. Esta investigación tuvo como objetivo evaluar la aplicación de la Transformada Rápida de Fourier (FFT) como criterio de detección de anomalías en el tráfico de red mediante análisis espectral. Se adoptó un enfoque cuantitativo de tipo experimental sustentado en simulación declarada: el comportamiento basal de la red se modeló en Python como una serie temporal con componentes periódicas y ruido gaussiano, sobre la que se inyectó una perturbación transitoria de alta frecuencia que emula una ráfaga de denegación de servicio (DDoS). El contraste entre el espectro del tráfico normal y el del tráfico comprometido evidenció que la anomalía concentra su energía en una banda claramente separada del perfil basal, con un pico dominante en 80 Hz que supera en más de diez veces el techo del ruido de fondo, lo que permitió definir un umbral de detección a partir de la razón de energía espectral. Se concluye que la descomposición espectral discrimina con eficacia los estados anómalos con una complejidad computacional baja, O (N log N), apta para escenarios de detección en tiempo real.

Palabras clave: procesamiento digital de señales, transformada de Fourier, detección de anomalías, seguridad de redes, densidad espectral.

FOURIER ANALYSIS APPLIED TO ANOMALY DETECTION IN NETWORK SIGNALS

The sustained growth of data traffic in telecommunication networks has hindered the timely identification of malicious patterns, channel saturation, and operational failures. This research aimed to evaluate the application of the Fast Fourier Transform (FFT) as an anomaly detection criterion for network traffic through spectral analysis. A quantitative, experimental approach based on declared simulation was adopted: baseline network behavior was modeled in Python as a time series composed of periodic components and Gaussian noise, into which a high-frequency transient disturbance emulating a denial-of-service (DDoS) burst was injected. The contrast between the spectrum of normal traffic and that of compromised traffic showed that the anomaly concentrates its energy in a band clearly separated from the baseline profile, with a dominant peak at 80 Hz exceeding the noise floor by more than tenfold, allowing a detection threshold to be defined from the spectral energy ratio. It is concluded that spectral decomposition effectively discriminates anomalous states with low computational complexity, O (N log N), suitable for real-time detection scenarios.

Key words: digital signal processing, Fourier transform, anomaly detection, network security, spectral density.

Correo principal para contacto: cbermeoz@uteq.edu.ec

1. INTRODUCCIÓN

Las redes de telecomunicaciones mueven hoy volúmenes de datos que hace una década habrían parecido improbables. Esa abundancia tiene un costo: cada vez resulta más difícil distinguir, dentro del flujo, lo que funciona bien de lo que empieza a fallar o de lo que ataca. Los mecanismos clásicos de supervisión, apoyados en firmas estáticas o en umbrales fijos de volumen, fueron pensados para amenazas que se repiten y pierden terreno frente a comportamientos que mutan o que sencillamente nunca se habían visto. De ahí, el giro hacia la detección de anomalías: en lugar de buscar lo conocido malo, modelar lo normal y vigilar sus desviaciones (Wang et al., 2021). Entre esas desviaciones, los ataques de denegación de servicio distribuido (DDoS) ocupan un lugar central por su frecuencia y su capacidad de daño. Investigaciones recientes dan cuenta de una carrera sostenida entre las variantes de ataque y los métodos para contenerlas (Javaheri et al., 2023). La preocupación no es ajena a la región: Arizaga Gamboa et al. (2022) evaluaron clasificadores de aprendizaje automático para separar tráfico legítimo de ráfagas DDoS y encontraron que la calidad de la detección depende, de manera crítica, de los datos disponibles para el entrenamiento.

Sin embargo, existe una ruta que no depende de datos históricos: tratar el flujo de red como una serie temporal discreta y examinarla con las herramientas del procesamiento digital de señales. La apuesta se apoya en una propiedad bien documentada del tráfico malicioso. Los ataques automatizados y en particular las inundaciones de paquetes, arrastran una cadencia repetitiva que el atacante difícilmente puede suprimir. Esa periodicidad se vuelve visible cuando la señal se observa en el dominio de la frecuencia (Liu et al., 2021). El instrumento matemático para esa transición es la Transformada Discreta de Fourier (DFT), que descompone una señal de tiempo discreto x[n] en sus componentes armónicos según la formulación clásica (Oppenheim & Schafer, 2010):

$$X[k] = \Sigma_{n=0}^{N-1} x[n] \cdot e^{-j(2\pi/N)kn}$$

Donde X[k] es un número complejo que codifica la amplitud y la fase de la componente de frecuencia k. En la práctica, el cálculo se realiza con la Transformada Rápida de Fourier (FFT), la familia de algoritmos que abarató el costo computacional de la DFT y sobre la que descansa buena parte del análisis espectral moderno, del filtrado en frecuencia y de la construcción de espectrogramas (Jaramillo Chamba & Chuquimarca Jiménez, 2022).

La idea de fondo es simple. En operación normal, el espectro del tráfico concentra su energía en bandas bajas, las de los ritmos regulares de usuarios y procesos automatizados: una ráfaga DDoS, un escaneo masivo o una exfiltración rompen ese reparto e introducen energía donde el perfil basal no la tiene. Distintos grupos han explotado esa huella con estrategias diversas: Liu et al. (2021) combinaron coeficientes de la FFT con entropía de la información para entrenar detectores sobre capturas reales del conjunto CICDDoS2019, mientras que Ahmad et al. (2022) convirtieron el tráfico de redes IoT en espectrogramas para reconocer visualmente los estados anómalos. Los estudios recientes sobre series temporales apuntan en la misma dirección: operar en frecuencia permite capturar los patrones de normalidad con un costo notablemente menor que el de los modelos que procesan la señal punto a punto (Chen et al., 2024),

y fusionar ambos dominios mejora la sensibilidad ante anomalías de patrón que el análisis temporal crudo deja pasar (Zhang et al., 2022).

Nada de esto ocurre al margen del auge del aprendizaje profundo. Arquitecturas basadas en redes transformadoras, como Informer, han alcanzado precisiones altas en la detección de anomalías de tráfico sobre sistemas de transporte inteligente (Peng et al., 2022). La revisión de Yi et al. (2023) documenta una familia creciente de redes neuronales que incorporan la transformada de Fourier como pieza interna de su arquitectura. Pero esa potencia tiene condiciones: fases intensivas de entrenamiento, dependencia de históricos representativos y un costo de inferencia que no todos los escenarios pueden pagar. En entornos de recursos limitados, los métodos espectrales deterministas conservan un valor difícil de sustituir como primera línea de detección.

Eso sí, la transformada de Fourier convencional tiene una limitación estructural conocida: al proyectar la ventana completa al dominio de la frecuencia se pierde la localización temporal del evento. El espectro dice qué frecuencias anómalas existen, no cuándo aparecieron. Las investigaciones enfrentan ese compromiso con ventanas móviles y representaciones tiempo-frecuencia como la Transformada de Fourier de Tiempo Corto (STFT), cuya resolución depende del tamaño de ventana elegido (Jaramillo Chamba & Chuquimarca Jiménez, 2022).

Trabajos muy recientes buscan conciliar la granularidad de ambos dominios para puntuar anomalías a nivel de punto individual (Nam et al., 2024). Sobre este marco, el presente artículo evaluó la FFT como criterio de detección de anomalías en señales de tráfico de red, mediante un experimento de simulación declarada: contrasta el espectro de un perfil basal con el de un tráfico comprometido por una ráfaga transitoria de alta frecuencia, cuantifica la sensibilidad del criterio, prueba su inmunidad ante picos legítimos de demanda y somete su robustez a validación estadística.

2. ESTRATEGIAS METODOLÓGICAS / MATERIALES Y MÉTODOS

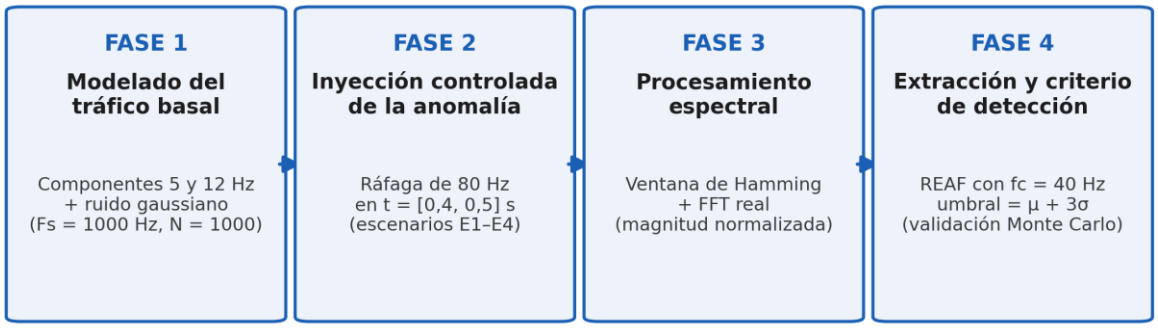
La investigación es cuantitativa y de diseño experimental, de tipo aplicado y con un alcance descriptivo-explicativo. El método consiste en descomponer espectralmente series temporales de tráfico mediante la Transformada Rápida de Fourier y evaluar cuánto se desvía la distribución de energía en frecuencia respecto de un perfil de operación basal. Como técnica, se empleó la simulación computacional declarada; el instrumento es un script en Python 3 ejecutado sobre el entorno Google Colab, con NumPy para el cálculo numérico, SciPy para el procesamiento de señales y Matplotlib para la generación de gráficos.

La elección de la simulación declarada no es un atajo sino una decisión metodológica con dos razones detrás. La primera es la reproducibilidad total: cualquier lector puede ejecutar el código con los mismos parámetros y obtener exactamente los mismos números, algo difícil de ofrecer con capturas de tráfico real sujetas a restricciones de privacidad. La segunda es el control de la verdad de terreno: se conoce de antemano dónde está la anomalía, cuánto dura y qué frecuencia tiene, de modo que el criterio de detección puede validarse de forma directa, sin depender de conjuntos etiquetados por terceros cuya calidad condiciona el desempeño de los enfoques de aprendizaje automático (Arizaga Gamboa et al., 2022).

El procedimiento se organiza en cuatro fases secuenciales, resumidas en la Figura 1 y aplicadas sobre cuatro escenarios experimentales: el caso base (E1), un análisis de sensibilidad a la intensidad del ataque (E2), una prueba de discriminación frente a un pico legítimo de demanda (E3) y una validación estadística por el método de Monte Carlo (E4).

Figura 1

Fases del procedimiento experimental.



Fuente: autoría propia (2026).

Fase 1. Modelado del tráfico basal. El volumen de tráfico normal se representa como una serie temporal discreta muestreada a Fs = 1000 Hz durante T = 1 segundo (N = 1000 muestras). El perfil basal combina dos componentes periódicas de baja frecuencia, una de 5 Hz que emula el ritmo agregado de la actividad de usuarios y otra de 12 Hz asociada a procesos automatizados secundarios, con ruido blanco gaussiano de media cero y desviación estándar 0,5 que modela la variabilidad aleatoria del tráfico. Esta composición reproduce la premisa, documentada en otras investigaciones, que el espectro del tráfico normal concentra su energía en bandas bajas con un comportamiento cíclico predecible (Liu et al., 2021).

Fase 2. Inyección controlada de la anomalía. Sobre la señal basal se superpone una perturbación transitoria en el intervalo t = [0,4, 0,5] segundos: una sinusoide de 80 Hz con amplitud 5,0; es decir, una ráfaga corta, intensa y de frecuencia notablemente superior al perfil basal, que emula el patrón repetitivo de una inundación de paquetes característica de un ataque DDoS (Javaheri et al., 2023). En el escenario E2 la amplitud se reduce progresivamente (5,0; 3,0; 2,0; 1,0; 0,5) para delimitar la frontera de detección y en el E3 la ráfaga se sustituye por una duplicación suave de la componente de usuarios, mediante una envolvente gaussiana centrada en t = 0,45 s, que representa un incremento legítimo y masivo de la demanda.

Fase 3. Procesamiento espectral. Cada señal se transforma al dominio de la frecuencia mediante el algoritmo FFT para señales reales, previa aplicación de una función de ponderación de Hamming que atenúa la fuga espectral provocada por la longitud finita de la ventana de observación (Oppenheim & Schafer, 2010). La ventana de Hamming se selecciona por su capacidad de cancelación del lóbulo lateral más próximo, propiedad que favorece la lectura limpia de picos espectrales (Jaramillo Chamba & Chuquimarca Jiménez, 2022). Las magnitudes resultantes se normalizan respecto de N para hacer comparables los espectros.

Fase 4. Extracción de características y criterio de detección. Como métrica de decisión, se define la razón de energía espectral de alta frecuencia (REAF), calculada como el cociente entre la energía contenida en la banda superior a una frecuencia de corte fc = 40 Hz y la energía espectral total. La frecuencia de corte se ubica deliberadamente por encima del contenido basal y por debajo de la banda anómala esperada; un incremento significativo de la REAF respecto del valor basal delata la presencia de energía anómala en alta frecuencia. En el escenario E4, el caso base se repite 100 veces con realizaciones independientes de ruido para caracterizar la distribución de la REAF en ambas condiciones y fijar el umbral de detección en la media basal más tres desviaciones estándar. Este criterio de umbralización sobre la distribución de energía es coherente con las aproximaciones espectrales reportadas para la detección de DDoS (Liu et al., 2021) y con la evidencia que las normalidades del tráfico son separables en el dominio de la frecuencia con bajo costo computacional (Chen et al., 2024).

El núcleo del script implementado se transcribe a continuación y queda a disposición para su ejecución directa en Google Colab. La fijación de la semilla del generador pseudoaleatorio asegura que el ruido gaussiano sea idéntico en cada ejecución, condición necesaria para la verificación independiente de los valores que se reportan en los resultados.

```
import numpy as np
from scipy.signal.windows import hamming


# 1. Parametros temporales
Fs = 1000                  # Frecuencia de muestreo (Hz)
T = 1.0                    # Duracion de la captura (s)
t = np.linspace(0, T, int(Fs*T), endpoint=False)
N = len(t)
rng = np.random.default_rng(42)   # Semilla fija: reproducibilidad


# 2. Modelado del trafico basal
componente_usuarios = np.sin(2*np.pi*5*t)      # Ritmo agregado (5 Hz)
componente_procesos = np.sin(2*np.pi*12*t)     # Procesos automatizados (12 Hz)
ruido = rng.normal(0, 0.5, size=t.shape)       # Ruido blanco gaussiano
trafico_normal = componente_usuarios + componente_procesos + ruido


# 3. Inyeccion de la anomalia (rafaga de 80 Hz en t = [0.4, 0.5] s)
anomalia = np.zeros_like(t)
idx = (t >= 0.4) & (t <= 0.5)
anomalia[idx] = 5.0 * np.sin(2*np.pi*80*t[idx])
```

```
trafico_anomalo = trafico_normal + anomalia


# 4. Procesamiento espectral con ventana de Hamming
ventana = hamming(N)
frecuencias = np.fft.rfftfreq(N, d=1/Fs)
fft_normal  = np.abs(np.fft.rfft(trafico_normal * ventana)) / N
fft_anomalo = np.abs(np.fft.rfft(trafico_anomalo * ventana)) / N


# 5. Criterio de deteccion: razon de energia espectral (fc = 40 Hz)
fc = 40
def reaf(espectro, frecs, corte):
    energia = espectro**2
    return energia[frecs > corte].sum() / energia.sum()


reaf_normal  = reaf(fft_normal,  frecuencias, fc)
reaf_anomalo = reaf(fft_anomalo, frecuencias, fc)
```


Los parámetros de la simulación deben leerse como un modelo a escala del fenómeno y no como magnitudes literales de una red en producción. La señal representa el volumen agregado de tráfico, paquetes por unidad de tiempo y sus frecuencias son relativas: lo determinante no es el valor absoluto en hercios sino la relación entre el ritmo del comportamiento basal y la tasa de repetición de la perturbación, que en este diseño es de aproximadamente 16 a 1. En una captura real con agregación cada $\Delta t = 1$ ms, el mismo análisis se aplica de forma directa con el eje de frecuencias reescalado, dado que la DFT es invariante ante ese cambio de escala temporal (Oppenheim & Schafer, 2010).

La estructura del modelo se ancla en dos propiedades documentadas del tráfico real. La primera: el volumen agregado de una red operativa exhibe ritmos regulares, ciclos de actividad de usuarios, tareas programadas, sondeos de monitoreo, superpuestos a una variabilidad aleatoria, lo que justifica la composición de componentes periódicas más ruido. La segunda: el tráfico de inundación generado por herramientas automatizadas posee una naturaleza repetitiva que el atacante difícilmente puede suprimir, verificada sobre capturas de ataques reales del conjunto CICDDoS2019 (Liu et al., 2021); la ráfaga sinusoidal inyectada representa el caso canónico de esa firma.

Se asumen de manera explícita tres simplificaciones de laboratorio: el ruido se modela como gaussiano, aunque el tráfico real presenta colas pesadas y rasgos de autosimilitud, la señal se trata como estacionaria dentro de la ventana de observación, y la anomalía se representa como un tono puro, mientras que un ataque real reparte su energía en una banda. Estas condiciones acotan el alcance de las conclusiones al

principio de detección demostrado y se retoman en la discusión como límites declarados del estudio.

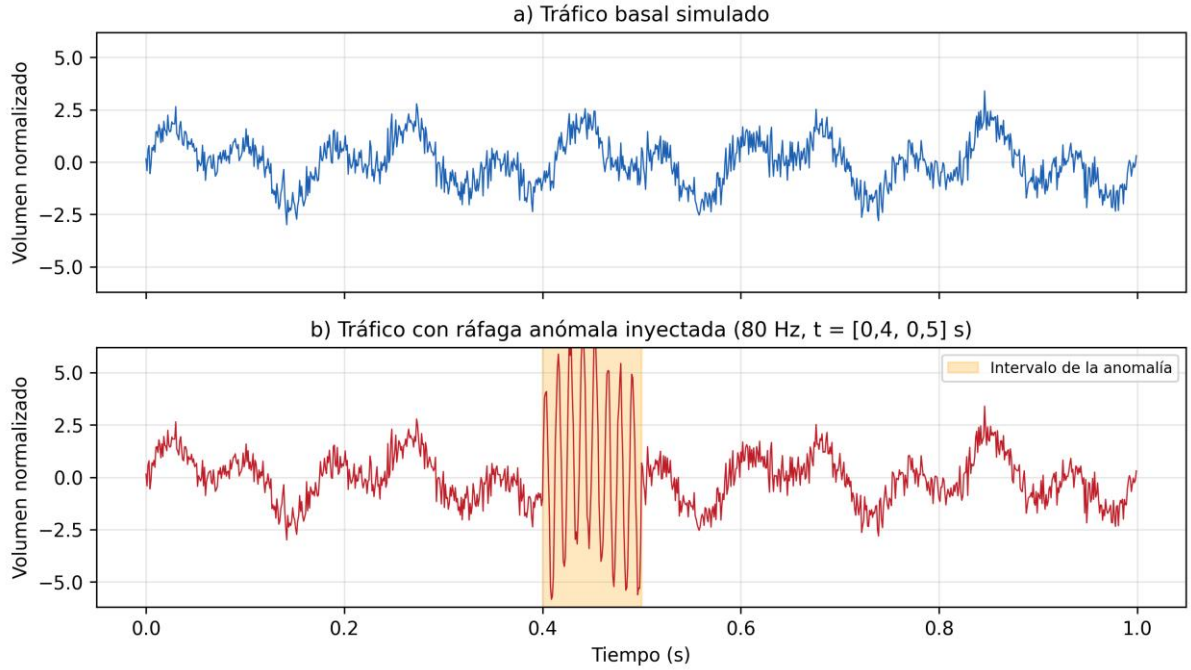
3. RESULTADOS

La ejecución del instrumento sobre los cuatro escenarios permitió caracterizar el comportamiento basal, verificar la separabilidad espectral de la anomalía y cuantificar la robustez estadística del criterio propuesto. Todos los valores que siguen son reproducibles mediante la semilla fija declarada en la metodología.

La Figura 2 presenta las series temporales de ambas condiciones. El tráfico basal exhibe una amplitud regulada que oscila entre −2,99 y +3,40 unidades normalizadas de volumen, producto de la superposición de las componentes periódicas de 5 Hz y 12 Hz con el ruido gaussiano de fondo. Al activarse la perturbación programada en el intervalo t = [0,4, 0,5] segundos, la señal cambia de morfología de forma abrupta: la amplitud máxima se eleva hasta el rango de −5,83 a +7,42, un incremento cercano al 120 % del valor pico basal.

Figura 2

Series temporales del tráfico basal (a) y del tráfico con la ráfaga anómala inyectada (b).



Fuente: autoría propia (2026).

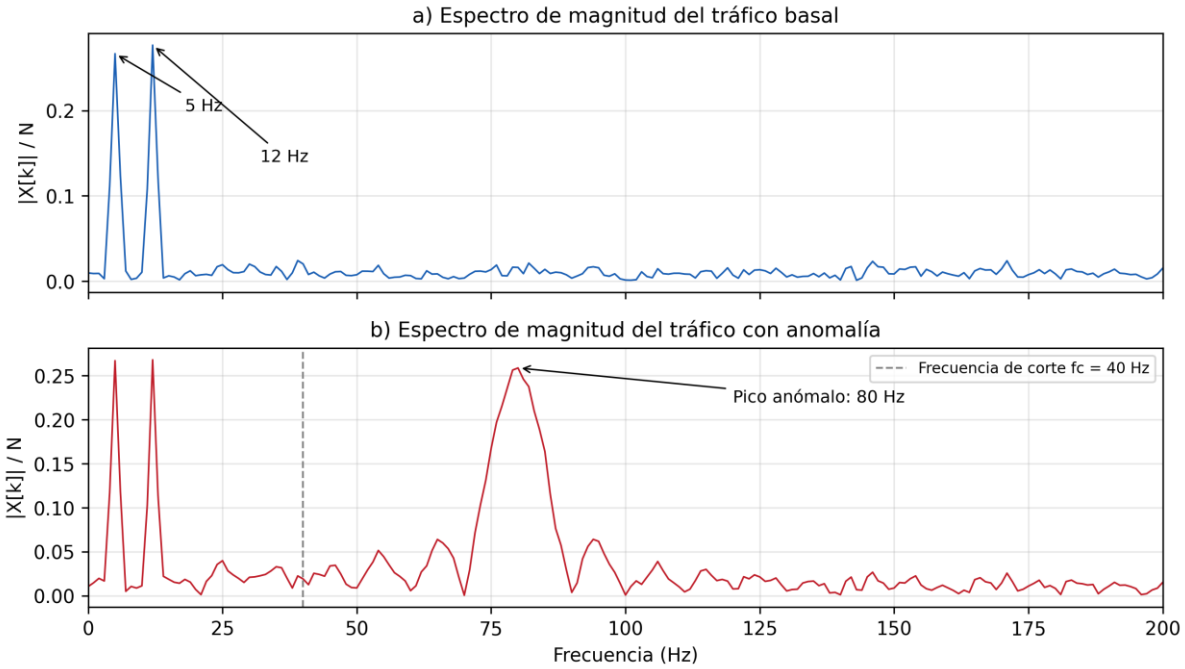
Ahora bien, mirar solo la dimensión temporal no basta para automatizar la decisión: una fluctuación de amplitud elevada puede corresponder tanto a una ráfaga maliciosa como a un incremento legítimo y masivo de la demanda. Esa ambigüedad es justamente la debilidad estructural de los detectores volumétricos basados en umbrales fijos (Wang et al., 2021). El escenario E3, analizado más adelante, materializa esa ambigüedad y muestra cómo el criterio espectral la resuelve.

La transformación espectral disuelve la ambigüedad. Como muestra la Figura 3a, el espectro del tráfico basal concentra su energía determinística en dos picos nítidos

de magnitud comparable, localizados en 5 Hz (|X| = 0,267) y 12 Hz (|X| = 0,277), sobre un piso de ruido distribuido cuyo techo en la banda superior a 40 Hz no excede de 0,025. El espectro del tráfico comprometido (Figura 3b) cuenta otra historia: emerge un pico dominante centrado exactamente en 80 Hz con magnitud 0,259, que supera en 10,4 veces el techo del ruido basal de alta frecuencia. La firma frecuencial de la anomalía queda aislada en una banda que el perfil normal no ocupa, en coherencia con la naturaleza periódica del tráfico de inundación documentada por Liu et al. (2021).

Figura 3

Espectros de magnitud del tráfico basal (a) y del tráfico con anomalía (b), con la frecuencia de corte fc = 40 Hz señalada.



Fuente: autoría propia (2026).

Sobre esta separación, se aplicó el criterio REAF. En condiciones basales, la razón de energía espectral de alta frecuencia se ubicó en 18,28 %, correspondiente a la contribución uniforme del ruido gaussiano; con la anomalía activa ascendió a 76,61 %, un incremento de 4,2 veces respecto del estado normal. La Tabla 1 sintetiza los valores característicos de ambas condiciones.

Tabla 1

Valores espectrales característicos del caso base (Escenario E1).

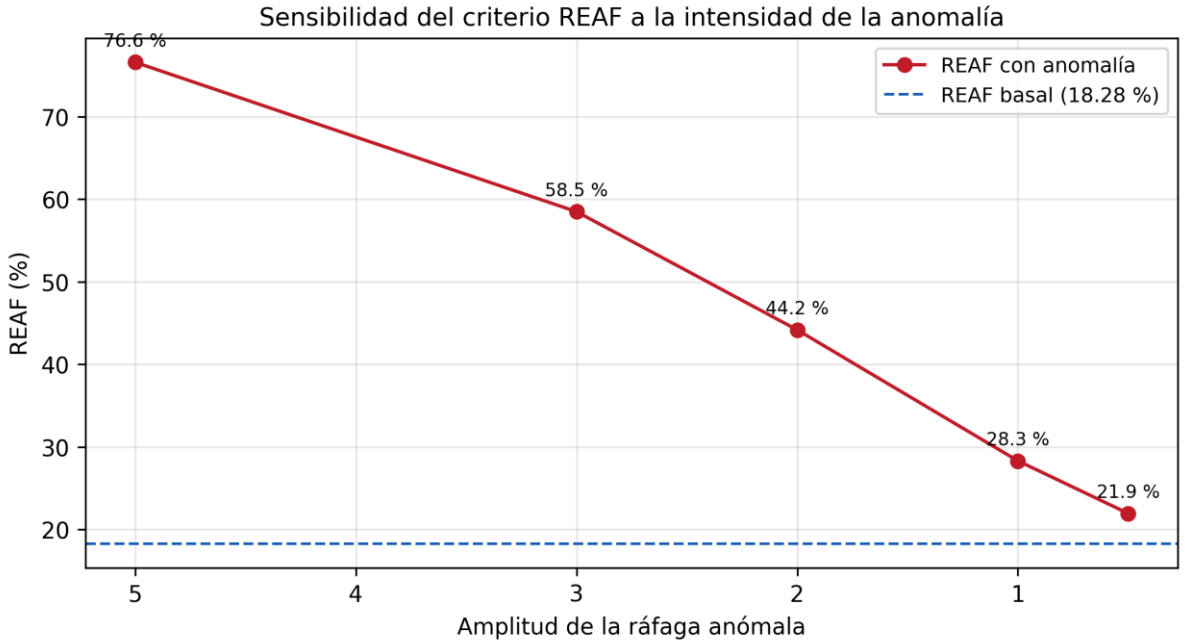
Indicador	Tráfico basal	Tráfico con anomalía
Amplitud temporal (mín., máx.)	(−2,99, +3,40)	(−5,83, +7,42)
Picos espectrales dominantes	5 Hz y 12 Hz	5 Hz, 12 Hz y 80 Hz
Magnitud del pico en 80 Hz	—	0,259 (10,4× el techo de ruido)
REAF (fc = 40 Hz)	18,28 %	76,61 %

Fuente: autoría propia (2026).

El escenario E2 evaluó la degradación del criterio ante ráfagas de intensidad decreciente. Los resultados de la Figura 4 describen una relación monótona entre la amplitud de la perturbación y la REAF: 76,61 % con amplitud 5,0; 58,50 % con 3,0; 44,18 % con 2,0; 28,30 % con 1,0; y 21,93 % con 0,5. Este último caso es particularmente ilustrativo. Con amplitud 0,5 la ráfaga queda por debajo de la desviación estándar del ruido y resulta visualmente indistinguible en la serie temporal; aun así, su REAF permanece por encima del umbral estadístico que se deriva en la validación de Monte Carlo, aunque con un margen tan reducido que anticipa el límite operativo del método.

Figura 4

Sensibilidad del criterio REAF a la intensidad de la ráfaga anómala (escenario E2).

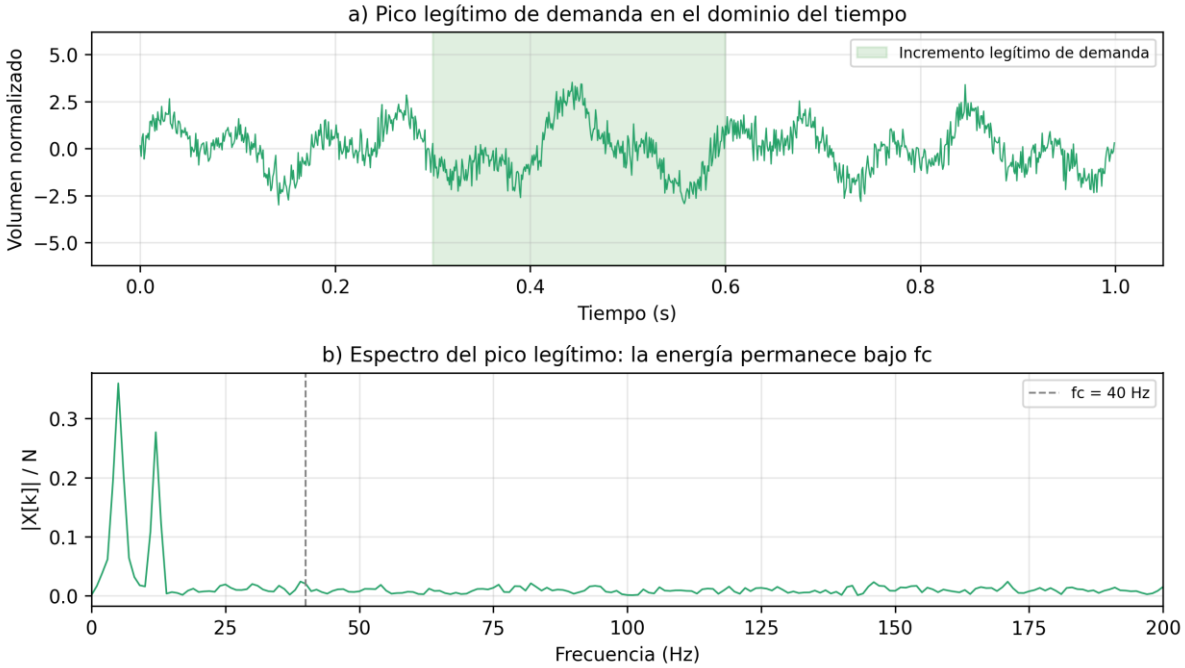


Fuente: autoría propia (2026).

El escenario E3 sometió el criterio a la prueba inversa: un incremento legítimo y masivo de la demanda, modelado como una duplicación suave de la componente de usuarios mediante una envolvente gaussiana centrada en t = 0,45 s. Pese a que la amplitud temporal del pico legítimo alcanza magnitudes comparables a las de la operación normal elevada, su REAF descendió a 12,39 %, un valor inferior incluso al basal. La lectura es directa: la demanda legítima agrega energía en las bandas bajas del espectro, de modo que la proporción de energía en alta frecuencia disminuye en lugar de aumentar (Figura 5). El criterio no solo evita el falso positivo; se aleja activamente de él y con ello confirma con datos la ventaja discriminativa del dominio frecuencial frente a los detectores volumétricos.

Figura 5

Pico legítimo de demanda: serie temporal (a) y espectro con la energía confinada bajo fc (b), escenario E3.



Fuente: autoría propia (2026).

Finalmente, el escenario E4 sometió el caso base a 100 repeticiones con realizaciones independientes de ruido gaussiano. La REAF del tráfico basal presentó una media de 18,25 % con desviación estándar de 1,06 %, mientras que la del tráfico comprometido promedió 75,50 % con desviación estándar de 0,86 %. A partir de la distribución basal se fijó el umbral de detección en la media más tres desviaciones estándar: 21,43 %. La Tabla 2 y la Figura 6 resumen el desempeño del clasificador resultante.

Tabla 2

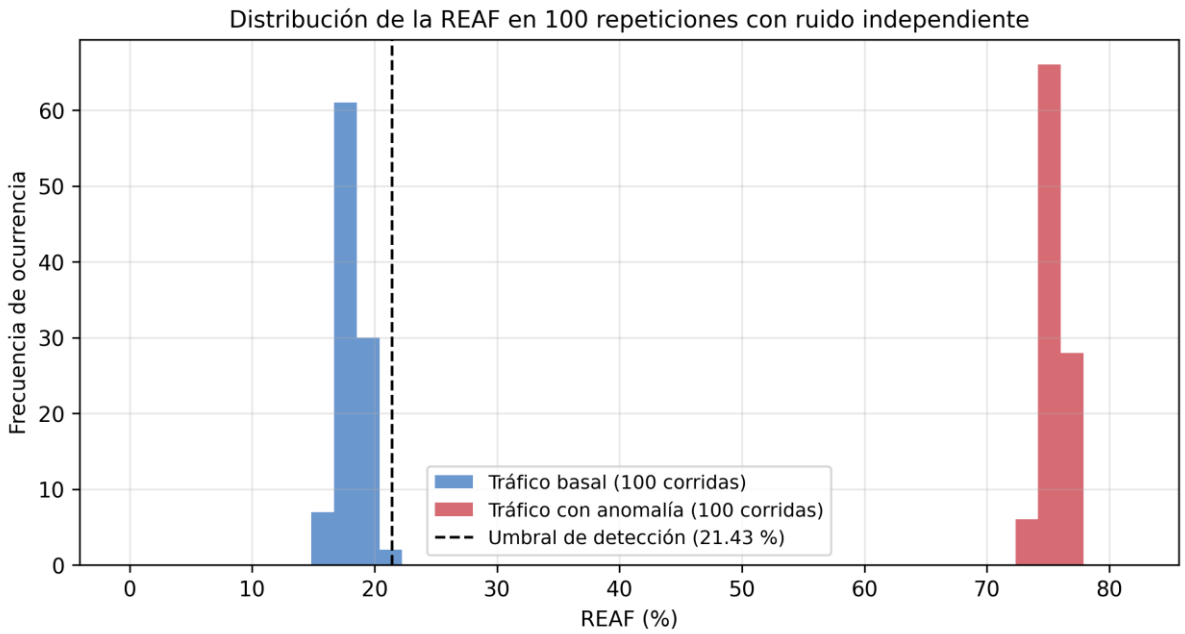
Desempeño del criterio REAF en 100 repeticiones Monte Carlo (escenario E4).

Métrica	Valor
REAF basal (media ± desviación estándar).	18,25 % ± 1,06 %
REAF anómala (media ± desviación estándar).	75,50 % ± 0,86 %
Umbral de detección (media + 3 desviaciones).	21,43 %
Tasa de detección verdadera (TPR).	100 %
Tasa de falsos positivos (FPR).	1 %
REAF anómala mínima observada.	72,83 %
REAF basal máxima observada.	21,43 %

Fuente: autoría propia (2026).

Figura 6

Distribución de la REAF en 100 repeticiones con ruido independiente y umbral de detección (escenario E4).



Fuente: autoría propia (2026).

Las dos distribuciones no se solapan: la realización anómala de menor energía (72,83 %) más que triplica la realización basal de mayor energía (21,43 %). Esto explica la tasa de detección del 100 %. El único falso positivo registrado corresponde a una realización de ruido cuya REAF coincidió con el valor exacto del umbral, algo esperable por construcción en un criterio de tres desviaciones estándar y corregible en despliegues reales mediante la confirmación sobre ventanas consecutivas. La brecha entre poblaciones sugiere, además, que el umbral admite holgura suficiente para absorber variaciones del piso de ruido sin comprometer la sensibilidad, en línea con la separabilidad de las normalidades del tráfico en el dominio de la frecuencia reportada en la literatura reciente (Chen et al., 2024).

Conviene precisar que la separación observada corresponde al régimen de ataque intenso definido en el caso base. El escenario E2 delimita el régimen operativo difícil: conforme la intensidad de la ráfaga desciende hacia el nivel del ruido, la brecha entre la REAF anómala y el umbral se estrecha hasta el caso límite de amplitud 0,5, donde la detección se mantiene, pero sin holgura. Esta gradación es consistente con lo esperable en condiciones reales, donde los ataques de baja tasa constituyen el principal desafío de los detectores espectrales.

4. DISCUSIÓN

Los resultados confirman que la transición al dominio de la frecuencia subsana la limitación central del análisis volumétrico de series temporales: la incapacidad de distinguir la naturaleza de una fluctuación a partir de su amplitud. El contraste entre los escenarios E1 y E3 condensa el aporte del estudio. Ante dos eventos de morfología temporal comparable, una ráfaga maliciosa y un pico legítimo de demanda, el criterio

Bermeo Zamora, C., González Tobar, E. y López Cedeño K. (2026). Análisis de Fourier aplicado a la detección de anomalías en señales de red. *Revista Ciencias y Saberes, 4(2)*, 313-328. https://ojs.rimanaeditorial.com/index.php/cys/article/view/82
mayo-agosto (2026). ISSN 2960-8430

REAF respondió en direcciones opuestas: subió de 18,28 % a 76,61 % en el primer caso y bajó a 12,39 % en el segundo. Un detector volumétrico habría marcado ambos eventos como sospechosos; el criterio espectral no solo evitó el falso positivo, sino que se alejó de él, porque la demanda legítima concentra su energía adicional en las bandas bajas que caracterizan al comportamiento humano agregado. Este hallazgo aporta evidencia cuantitativa a una debilidad de los sistemas tradicionales que las investigaciones venían señalando en términos cualitativos (Wang et al., 2021).

La comparación con las arquitecturas contemporáneas de aprendizaje profundo sitúa el resultado en su justa dimensión. Modelos basados en redes transformadoras como Informer alcanzan una precisión elevada en la detección de anomalías sobre series temporales de tráfico, pero exigen una fase intensiva de entrenamiento fuera de línea, dependen de conjuntos de datos históricos representativos y trasladan a la inferencia un costo computacional considerable (Peng et al., 2022). En cambio, el enfoque espectral evaluado opera de manera determinista sobre la ventana actual: no requiere entrenamiento, su complejidad O (N log N) resulta órdenes de magnitud más liviana y su desempeño no se degrada por la falta de datos etiquetados, condición que Arizaga Gamboa et al. (2022) identifican como el principal obstáculo práctico de los detectores basados en aprendizaje automático. La literatura reciente converge con esta lectura: los métodos que operan en frecuencia capturan las normalidades del tráfico con una eficiencia que los modelos punto a punto no alcanzan (Chen et al., 2024) y las propuestas híbridas más competitivas incorporan precisamente la información espectral como componente estructural (Zhang et al., 2022; Yi et al., 2023). La Tabla 3 resume el contraste operativo.

Tabla 3

Contraste operativo entre el análisis espectral y los modelos predictivos profundos.

Criterio de evaluación	Análisis espectral (FFT)	Modelos predictivos (Informer)
Complejidad computacional.	Baja, O(N log N).	Alta, entrenamiento e inferencia neuronal.
Dependencia de datos históricos.	Nula, determinista en la ventana actual.	Crítica, requiere corpus de entrenamiento.
Latencia de detección.	Mínima, apta para tiempo real.	Moderada a alta.
Discriminación de picos legítimos.	Alta, por firma frecuencial (E3).	Alta, condicionada a la variedad del entrenamiento.
Localización temporal del evento.	Limitada, requiere ventaneo.	Nativa, opera punto a punto.

Fuente: autoría propia (2026).

La última fila de la Tabla 3 introduce la restricción estructural del método, que los resultados también acotan. La transformada de Fourier convencional revela qué frecuencias anómalas existen en la ventana analizada, pero no cuándo ocurrieron dentro de ella: en el caso base, el pico de 80 Hz delata la ráfaga sin localizar el intervalo t = [0,4, 0,5] segundos que la contiene. Este compromiso entre resolución temporal y frecuencial es inherente a la transformación y explica el interés vigente por las representaciones tiempo-frecuencia, desde la STFT con ventana de Hamming (Jaramillo Chamba & Chuquimarca Jiménez, 2022) hasta las propuestas que concilian

la granularidad de ambos dominios para puntuar anomalías a nivel de punto individual (Nam et al., 2024) o que reconstruyen la señal enmascarando a la vez información temporal y frecuencial (Fang et al., 2024).

Asimismo, los resultados deben leerse dentro de los límites declarados del modelo. La simulación asume ruido gaussiano, estacionariedad dentro de la ventana y una anomalía de tono puro, condiciones de laboratorio que el tráfico real no cumple estrictamente: las capturas reales presentan colas pesadas, tendencias no estacionarias y ataques cuya energía se reparte en bandas, además de adversarios capaces de modular deliberadamente su tasa de emisión para difuminar la firma periódica (Javaheri et al., 2023). El escenario E2 anticipa el efecto de esa degradación, la brecha de detección se estrecha conforme la intensidad desciende, pero la cuantificación definitiva exige validar el criterio REAF sobre capturas reales etiquetadas; el conjunto CICDDoS2019, empleado por Liu et al. (2021) para verificar la periodicidad del tráfico de inundación, constituye el banco de prueba natural para esa extensión. Con esa salvedad, la evidencia obtenida sostiene que el análisis espectral conserva un lugar operativo propio como primera línea de detección liviana, complementaria y no excluyente de los modelos de aprendizaje profundo.

5. CONCLUSIONES / CONSIDERACIONES FINALES

Esta investigación partió de una pregunta sencilla: ¿puede la transformada de Fourier, una herramienta con más de dos siglos de historia, seguir compitiendo en un campo dominado por el aprendizaje profundo? Los resultados sugieren que sí y la razón es menos matemática de lo que parece. Un pico legítimo de demanda y una ráfaga de ataque pueden verse casi idénticos en el tiempo, pero nacen de procesos distintos: el primero hereda los ritmos lentos de la actividad humana; la segunda arrastra la cadencia mecánica y repetitiva del software que la genera. Esa diferencia de origen deja una huella en el espectro que ningún umbral de volumen puede ver. Cuando se inyecta la ráfaga, la razón de energía de alta frecuencia se multiplicó por 4,2; cuando se simula el pico legítimo, cayó incluso por debajo del valor basal. El detector no tuvo que adivinar la intención del tráfico: le bastó con mirar dónde vive su energía.

La validación estadística respalda que esto no fue suerte de una corrida afortunada. En cien repeticiones con ruido independiente, las distribuciones de tráfico normal y comprometido ni siquiera se rozaron: la peor realización anómala triplicó a la mejor realización basal y un umbral tan poco sofisticado como la media más tres desviaciones estándar bastó para detectar el 100 % de los ataques con un solo falso positivo marginal. Ahora bien, sería deshonesto presentar el método como infalible. El análisis de sensibilidad muestra que la ventaja se erosiona a medida que el ataque se debilita: con la ráfaga enterrada en el ruido, la detección sobrevive, pero sin margen. Los ataques de baja tasa son y seguirán siendo el terreno difícil.

Hay también un argumento práctico que pesa tanto como el estadístico. Este criterio no necesita entrenarse, no depende de datos históricos etiquetados, que en la práctica escasean o llegan sesgados y corre con complejidad O(N log N) sobre la ventana actual, lo que lo hace viable en tiempo real sobre equipos modestos. No pretende reemplazar a los modelos profundos que predicen mejor; pretende llegar antes y costar menos, como primera línea de un esquema de defensa por capas.

Queda trabajo por delante, y conviene nombrarlo sin rodeos. La simulación asume ruido gaussiano, señal estacionaria y una anomalía de tono puro; el tráfico real no concede ninguna de las tres cosas. Y la transformada estándar dice qué frecuencias anómalas hay, pero no cuándo aparecieron. Los pasos siguientes son claros: validar el criterio sobre capturas reales como las del conjunto CICDDoS2019, incorporar ventaneo deslizante con STFT para recuperar la localización temporal del evento y estresar el método frente a atacantes que modulen su periodicidad a propósito. Si el principio sobrevive a esas pruebas, habrá argumentos sólidos para devolverle al análisis espectral un lugar de serie en los sistemas de detección de intrusos.

6. REFERENCIAS

Ahmad, Zeeshan & Shahid Khan, Adnan & Aqeel, Sehrish & Ahmadi Julaihi, Azlina Binti & Tarmizi, Seleviawati & Annuar, Noralifah & Habeeb, Mohammed. (2022). *S-ADS: Spectrogram Image-based Anomaly Detection System for IoT networks*. 105-110. 10.1109/AiIC54368.2022.9914599.

Arizaga Gamboa, J., Chicala Arroyave, J., & Alvarado Unamuno, E. (2022). Detección de ataque de DDoS utilizando Machine Learning – algoritmo de Random Forest. *Serie Científica de la Universidad de las Ciencias Informáticas*, *15*(3), 45–53. https://dialnet.unirioja.es/servlet/articulo?codigo=8590684

Chen, F., Zhang, Y., Qin, Z., Fan, L., Jiang, R., Liang, Y., Wen, Q., & Deng, S. (2024). Learning multi-pattern normalities in the frequency domain for efficient time series anomaly detection. *2024 IEEE 40th International Conference on Data Engineering (ICDE)*, 747–760. IEEE.

Fang, Y., Xie, J., Zhao, Y., Chen, L., Gao, Y., & Zheng, K. (2024). Temporal-frequency masked autoencoders for time series anomaly detection. *2024 IEEE 40th International Conference on Data Engineering (ICDE)*, 1228–1241. IEEE.

Jaramillo Chamba, D., & Chuquimarca Jiménez, L. (2022). Estudio comprensivo de la Transformada de Fourier Discreta para el análisis de señales digitales. *Revista Científica y Tecnológica UPSE*, *9*(1), 75–84. https://doi.org/10.26423/rctu.v9i1.664

Javaheri, D., Gorgin, S., Lee, J.-A., & Masdari, M. (2023). Fuzzy logic-based DDoS attacks and network traffic anomaly detection methods: Classification, overview, and future perspectives. *Information Sciences*, *626*, 315–338.

Liu, Z., Hu, C., & Shan, C. (2021). Riemannian manifold on stream data: Fourier transform and entropy-based DDoS attacks detection method. *Computers & Security*, *109*, 102392. https://doi.org/10.1016/j.cose.2021.102392

Nam, Y., Yoon, S., Shin, Y., Bae, M., Song, H., Lee, J.-G., & Lee, B. S. (2024). Breaking the time-frequency granularity discrepancy in time-series anomaly detection. *Proceedings of the ACM Web Conference 2024*, 4204–4215. https://doi.org/10.1145/3589334.3645556

Oppenheim, A. V., & Schafer, R. W. (2010). *Discrete-time signal processing* (3.ª ed.). Pearson.

Peng, X., Lin, Y., Cao, Q., Cen, Y., Zhuang, H., & Lin, Z. (2022). Traffic anomaly detection in intelligent transport applications with time series data using Informer. *2022 IEEE 25th International Conference on Intelligent Transportation Systems (ITSC)*, 3309–3314. https://doi.org/10.1109/ITSC55140.2022.9922142

Wang, S., Balarezo, J. F., Kandeepan, S., Al-Hourani, A., Chavez, K. G., & Rubinstein, B. (2021). Machine learning in network anomaly detection: A survey. *IEEE Access*, *9*, 152379–152396.

Yi, K., Zhang, Q., Wang, S., He, H., Long, G., & Niu, Z. (2023). Neural time series analysis with Fourier transform: A survey. *arXiv*. https://arxiv.org/abs/2302.02173

Zhang, C., Zhou, T., Wen, Q., & Sun, L. (2022). TFAD: A decomposition time series anomaly detection architecture with time-frequency analysis. *Proceedings of the 31st ACM International Conference on Information & Knowledge Management (CIKM '22)*. ACM.