Apéndice A: Características del flujo de red y glosario de términos para clasificación de tráfico de red

M. A. Pérez Ávila
Departamento de Computación
Instituto Tecnológico y de Estudios Superiores de Monterrey
Ciudad de México, México
A01369908@tec.mx

A. M. Sánchez Serratos
Departamento de Computación
Instituto Tecnológico y de Estudios Superiores de Monterrey
Ciudad de México, México
A01771843@tec.mx

***Resumen* - Este documento complementario describe en detalle las características del flujo de red utilizadas para entrenamiento y evaluación de modelos de clasificación, incluyendo definiciones de variables, rangos de valores y glosario de términos técnicos. Se proporciona como referencia para facilitar la interpretación de los resultados del estudio principal.**

I. GLOSARIO DE TÉRMINOS CLAVE

1. FLUJO (FLOW): Conjunto de paquetes que comparten las mismas direcciones IP de origen y destino, puertos y protocolo durante un intervalo temporal determinado. Representa una "conversación" de red.

2. FORWARD (FORWARD DIRECTION): Tráfico enviado desde el origen del flujo hacia el destino (por ejemplo, cliente → servidor).

3. BACKWARD (BACKWARD DIRECTION): Tráfico enviado desde el destino hacia el origen del flujo (por ejemplo, servidor → cliente).

4. PAQUETE (PACKET): Unidad de datos transmitida en la red que incluye cabecera (información de control) y payload (datos).

5. PAYLOAD: Datos contenidos dentro de un paquete que representan la información real transmitida, excluyendo cabeceras.

6. CABECERA (HEADER): Información de control dentro del paquete que indica origen, destino, tamaño, flags TCP/UDP, etc.

7. INTER-ARRIVAL TIME (IAT): Tiempo transcurrido entre la llegada de paquetes consecutivos dentro de un flujo. Se usa para evaluar la regularidad y velocidad del tráfico.

8. SUBFLUJO: División parcial de un flujo principal, usada para análisis granular de tráfico en intervalos o direcciones específicas.

9. FLAGS TCP (FIN, PSH, ACK, ETC.): Bits en la cabecera TCP que indican control de la conexión, transmisión de datos o finalización de comunicación.

10. VENTANA TCP (TCP WINDOW): Tamaño de ventana de recepción que indica la cantidad de datos que un receptor está dispuesto a aceptar antes de enviar un ACK.

11. ACTIVE/IDLE TIME: Periodos en los que se transmiten paquetes (active) o no hay transmisión (idle), útil para detectar pausas o ráfagas de tráfico.

II. TABLA DE CARACTERÍSTICAS

TABLA A1
DESCRIPCIÓN DETALLADA DE LAS CARACTERÍSTICAS DEL FLUJO DE RED UTILIZADAS PARA CLASIFICACIÓN

Núm.	Nombre de la característica	Tipo / Unidad	Rango Típico	Descripción detallada
1	Destination Port	Entero	0–65535	Número de puerto del destinatario del flujo, usado para identificar el servicio o aplicación final que recibe los datos (por ejemplo, 80 para HTTP, 443 para HTTPS). Es fundamental para detectar patrones de ataque dirigidos a servicios específicos.
2	Flow Duration	Entero [ms]	0–∞	Duración total del flujo, desde el primer hasta el último paquete. Permite distinguir flujos breves (por ejemplo, escaneo de puertos) de sesiones prolongadas (transferencia de archivos o DDoS sostenido).
3	Total Fwd Packets	Entero	0–∞	Cantidad total de paquetes enviados en la dirección forward (origen → destino). Ayuda a evaluar la actividad inicial de un flujo y detectar comportamientos anómalos.
4	Total Length of Fwd Packets	Entero [bytes]	0–∞	Suma total de los tamaños de los paquetes enviados forward, incluyendo cabecera y payload. Refleja volumen de datos transmitidos desde el origen al destino.
5	Fwd Packet Length Max	Entero [bytes]	0–1500	Longitud máxima de un paquete forward dentro del flujo. Puede indicar la presencia de paquetes fragmentados o payloads grandes, típico de exfiltración de datos.
6	Fwd Packet Length Min	Entero [bytes]	0–1500	Longitud mínima de un paquete forward. Útil para identificar flujos con paquetes uniformes o con tráfico “silencioso” que podría corresponder a sondas de red.
7	Fwd Packet Length Mean	Float [bytes]	0–1500	Tamaño promedio de paquetes forward, proporciona un resumen estadístico del flujo y permite comparar patrones normales vs. anómalos.
8	Fwd Packet Length Std	Float [bytes]	0–1500	Desviación estándar de los tamaños de paquetes forward. Valores altos indican variabilidad en la comunicación, mientras que valores bajos sugieren consistencia.
9	Bwd Packet Length Max	Entero [bytes]	0–1500	Tamaño máximo de paquetes en dirección backward (destino → origen). Importante para analizar respuestas de servidores, incluyendo grandes transferencias o ataques reflejados.

Núm.	Nombre de la característica	Tipo / Unidad	Rango Típico	Descripción detallada
10	Bwd Packet Length Min	Entero [bytes]	0–1500	Tamaño mínimo de paquetes backward. Útil para detectar tráfico de control o respuestas muy breves, típico en escaneos de red.
11	Bwd Packet Length Mean	Float [bytes]	0–1500	Tamaño promedio de paquetes backward, representando la carga de respuesta del servidor o receptor del flujo.
12	Bwd Packet Length Std	Float [bytes]	0–1500	Desviación estándar de los paquetes backward, indica variabilidad en las respuestas del destino y puede revelar anomalías en patrones normales de tráfico.
13	Flow Bytes/s	Float [bytes/s]	0–∞	Velocidad de transmisión del flujo en bytes por segundo. Indica la intensidad del flujo y ayuda a identificar ataques de alto ancho de banda, como DDoS.
14	Flow Packets/s	Float [packets/s]	0–∞	Número de paquetes transmitidos por segundo en el flujo completo, usado para evaluar la densidad de tráfico y posibles ráfagas anómalas.
15	Flow IAT Mean	Float [µs]	0–∞	Tiempo promedio entre la llegada de paquetes consecutivos en todo el flujo. Permite evaluar regularidad de la comunicación; valores bajos indican ráfagas rápidas, típicas de ataques automatizados.
16	Flow IAT Std	Float [µs]	0–∞	Desviación estándar del inter-arrival time en todo el flujo, refleja la consistencia temporal de la transmisión.
17	Flow IAT Max	Entero [µs]	0–∞	Intervalo máximo entre paquetes consecutivos, útil para detectar pausas largas o interrupciones en la comunicación.
18	Flow IAT Min	Entero [µs]	0–∞	Intervalo mínimo entre paquetes consecutivos, refleja velocidad mínima instantánea del flujo.
19	Fwd IAT Total	Entero [µs]	0–∞	Suma de los tiempos inter-arrival para paquetes forward. Indica cuánto tiempo total estuvo activo el flujo en dirección origen → destino.
20	Fwd IAT Mean	Float [µs]	0–∞	Tiempo promedio entre paquetes forward, evaluando la regularidad de envío de datos por el origen.
21	Fwd IAT Std	Float [µs]	0–∞	Variabilidad de los intervalos forward. Valores altos pueden indicar transmisiones irregulares o ataques adaptativos.
22	Fwd IAT Max	Entero [µs]	0–∞	Intervalo máximo forward, útil para detectar interrupciones o inactividad parcial del flujo.

Núm.	Nombre de la característica	Tipo / Unidad	Rango Típico	Descripción detallada
23	Fwd IAT Min	Entero [µs]	0–∞	Intervalo mínimo forward, indicando ráfagas rápidas de paquetes.
24	Bwd IAT Total	Entero [µs]	0–∞	Tiempo acumulado entre paquetes backward, refleja duración de la respuesta del servidor o destino.
25	Bwd IAT Mean	Float [µs]	0–∞	Tiempo promedio entre paquetes backward, evaluando ritmo de respuesta del destino.
26	Bwd IAT Std	Float [µs]	0–∞	Variabilidad de inter-arrival backward, indicando consistencia o irregularidad en respuestas.
27	Bwd IAT Max	Entero [µs]	0–∞	Intervalo máximo backward, útil para detectar retrasos o problemas en la red.
28	Bwd IAT Min	Entero [µs]	0–∞	Intervalo mínimo backward, refleja la menor latencia entre paquetes de respuesta.
29	Fwd Header Length	Entero [bytes]	0–∞	Longitud promedio de cabeceras TCP/UDP forward, útil para detectar cambios en protocolos o presencia de encabezados anómalos.
30	Bwd Header Length	Entero [bytes]	0–∞	Longitud promedio de cabeceras backward, relevante para evaluar respuestas del servidor o modificaciones de tráfico.
31	Fwd Packets/s	Float [packets/s]	0–∞	Frecuencia de envío de paquetes forward por segundo, útil para identificar flujos con tráfico concentrado.
32	Bwd Packets/s	Float [packets/s]	0–∞	Frecuencia de paquetes backward por segundo, reflejando la respuesta del servidor en términos de velocidad de transmisión.
33	Min Packet Length	Entero [bytes]	0–1500	Tamaño mínimo de cualquier paquete del flujo (forward o backward), útil para identificar paquetes de control muy pequeños.
34	Max Packet Length	Entero [bytes]	0–1500	Tamaño máximo de cualquier paquete del flujo, ayuda a detectar payloads anómalos o fragmentación inusual.
35	Packet Length Mean	Float [bytes]	0–1500	Promedio de longitud de todos los paquetes, resumido para caracterizar el flujo.
36	Packet Length Std	Float [bytes]	0–1500	Variabilidad de tamaños de paquete, indicando regularidad o irregularidad en la comunicación.
37	Packet Length Variance	Float [bytes²]	0–2.25e6	Varianza de la longitud de paquetes, medida de dispersión más general que std.

Núm.	Nombre de la característica	Tipo / Unidad	Rango Típico	Descripción detallada
38	FIN Flag Count	Entero	0–∞	Número de paquetes con flag FIN activado, indicando cierre de conexión TCP.
39	PSH Flag Count	Entero	0–∞	Número de paquetes con flag PSH, usado para acelerar la entrega del payload al destino.
40	ACK Flag Count	Entero	0–∞	Número de paquetes con flag ACK, usado para confirmar recepción de datos en TCP.
41	Average Packet Size	Float [bytes]	0–1500	Tamaño promedio de los paquetes, combinando forward y backward, refleja densidad de datos del flujo.
42	Subflow Fwd Bytes	Entero [bytes]	0–∞	Total de bytes transmitidos en un subflujo forward (porción del flujo principal), útil para análisis granular.
43	Init_Win_bytes_forward	Entero [bytes]	0–65535	Tamaño inicial de ventana TCP forward, indicando cantidad máxima de datos que el origen puede enviar antes de recibir un ACK.
44	Init_Win_bytes_backward	Entero [bytes]	0–65535	Tamaño inicial de ventana TCP backward, reflejando la capacidad de recepción del destino.
45	act_data_pkt_fwd	Entero	0–∞	Número de paquetes que contienen datos útiles (payload) forward, excluyendo control.
46	min_seg_size_forward	Entero [bytes]	0–1500	Tamaño mínimo de segmento TCP forward, relevante para identificar fragmentación de datos.
47	Active Mean	Float [µs]	0–∞	Promedio de duración de períodos activos (envío de paquetes) en el flujo, tanto forward como backward.
48	Active Max	Entero [µs]	0–∞	Máximo tiempo de actividad en un burst de paquetes.
49	Active Min	Entero [µs]	0–∞	Mínimo tiempo de actividad registrado en un burst de paquetes.
50	Idle Mean	Float [µs]	0–∞	Promedio de períodos de inactividad (sin transmisión de paquetes), útil para identificar pausas o intervalos entre bursts.
51	Idle Max	Entero [µs]	0–∞	Máximo tiempo sin transmisión en el flujo, indicador de pausas prolongadas.
52	Idle Min	Entero [µs]	0–∞	Mínimo tiempo sin transmisión, refleja micro-pausas entre paquetes.

Núm.	Nombre de la característica	Tipo / Unidad	Rango Típico	Descripción detallada
53	Attack Type	Categórico {0,1,...,6}	{0–6}	Clase de tráfico: normal o tipo de ataque específico. Cada valor numérico corresponde a un ataque concreto o tráfico legítimo, usado como etiqueta para entrenamiento y evaluación.