Estudio del tráfico de fondo de Internet mediante un telescopio de red situado en España

Rodolfo García-Peñas
rodgar@correo.ugr.es

Rafael A. Rodríguez-Gómez
rodgom@ugr.es

Gabriel Maciá-Fernández
gmacia@ugr.es

Universidad de Granada - Network Engineering & Security Group (NESG)

Reunion nº 33 del Grupo de Operadores de Red Español
22-23 Mayo 2024

UNIVERSIDAD DE GRANADA

ES.NOG 33

Presentación

```
user@host:~$ finger kix
Login: kix                         Name: Rodolfo García Peñas
Company: Telefónica España         Shell: /bin/zsh
Linkedin: https://www.linkedin.com/in/rodolfogarciapenas/
On since 2001 Mon May 14 07:00 (CET) on console. No idle
A lot of mail.
Plan:
- Trabajo en Planificación de Núcleo e Interconexión IP.
- Gestiono el direccionamiento IP (RIPE, reparto,
recuperación, soporte), IPAM, etc.
- Proyectos:
- IPv6: Solicitud de /23. Plan de direccionamiento. Piloto
2012. Piloto 2022. Núcleo red, interconexión, sistemas
comunes BAM/BAF y parte de BAF (+ beta dual stack).
- RPKI
```

Índice

Introducción al tráfico IBR

El tráfico de fondo de Internet (IBR o IBN) se define como el tráfico de paquetes que son enviados a direcciones IP que no están en uso o puertos que no esperan recibir este tráfico.

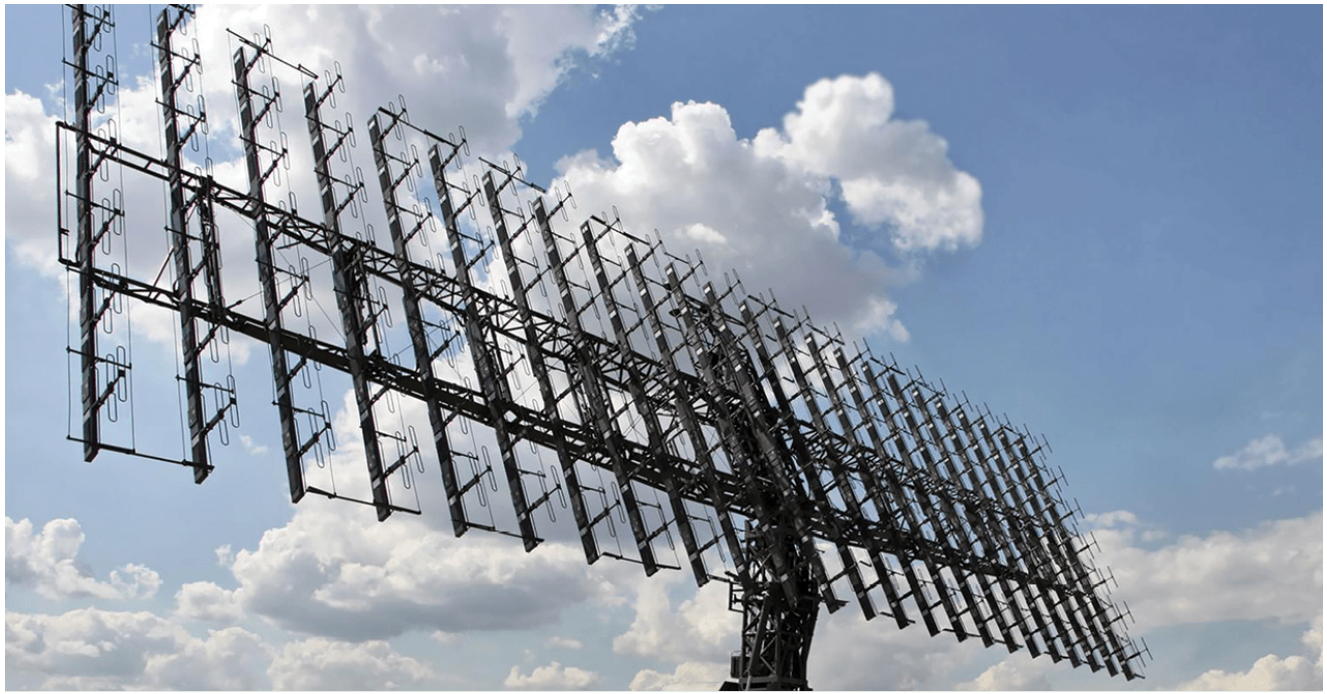


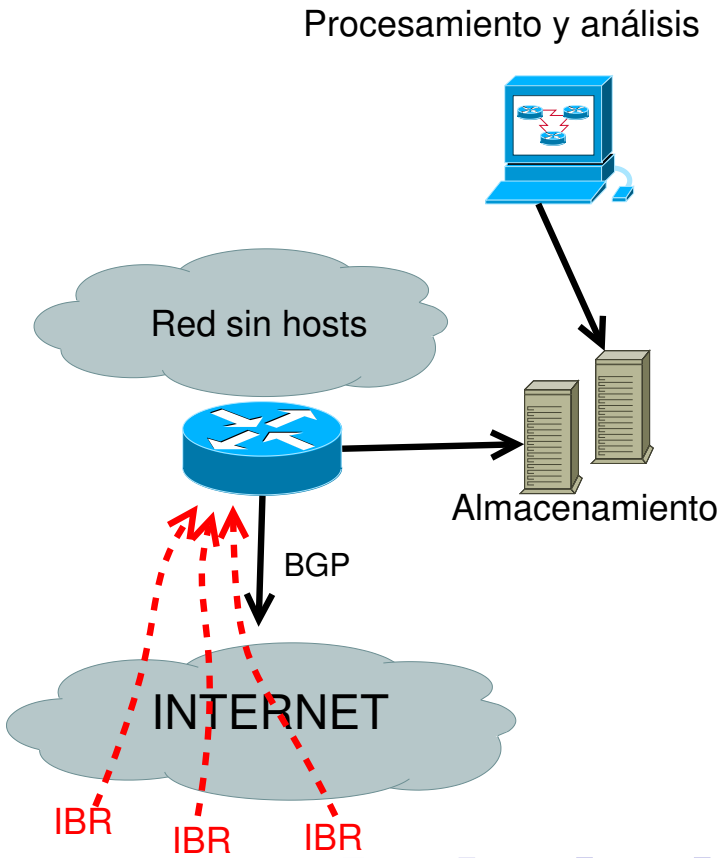
Imagen: https://circuitcellar.com/research-design-hub/an-intro-to-antenna-arrays/

Adquisición clásica del tráfico IBR

El tráfico IBR se adquiere mediante **telescopios de red***.

Los telescopios clásicos:

- Anuncian (BGP) redes.
- Las redes no tienen *hosts* activos.
- El tráfico recibido es por tanto IBR.
- Adquieren el tráfico recibido, para su posterior análisis.



Importancia del tráfico IBR

- Análisis del comportamiento:
  - Tráfico normal vs. tráfico anómalo.
  - Identificación de problemas o configuraciones erróneas.
- Identificación de amenazas:
  - Detección de ataques.
  - Nuevas tácticas.
  - Mitigación.
- Investigación y desarrollo en ciberseguridad:
  - Búsqueda de nuevas soluciones de seguridad.
  - Estudio de la evolución del tráfico.
  - Desarrollo de nuevas técnicas, tecnologías y enfoques.

Descripción del telescopio de red y de la muestra

Descripción del telescopio de red

- El telescopio está formado por cuatro redes /24 repartidas en dos clases A diferentes (dos redes en cada clase A).
- Direcciones están registradas en la BBDD de RIPE con país España.
- Las redes se anuncian mediante BGP y se ha comprobado durante el periodo de estudio que han sido visibles (372 *peers*).

Características de la muestra

- Los datos se han recogido durante el periodo de un año (2023).
- La información se ha almacenado en ficheros PCAP (*Packet CAPture*).
- El volumen total de datos almacenados es de 362,39 Gigabytes.

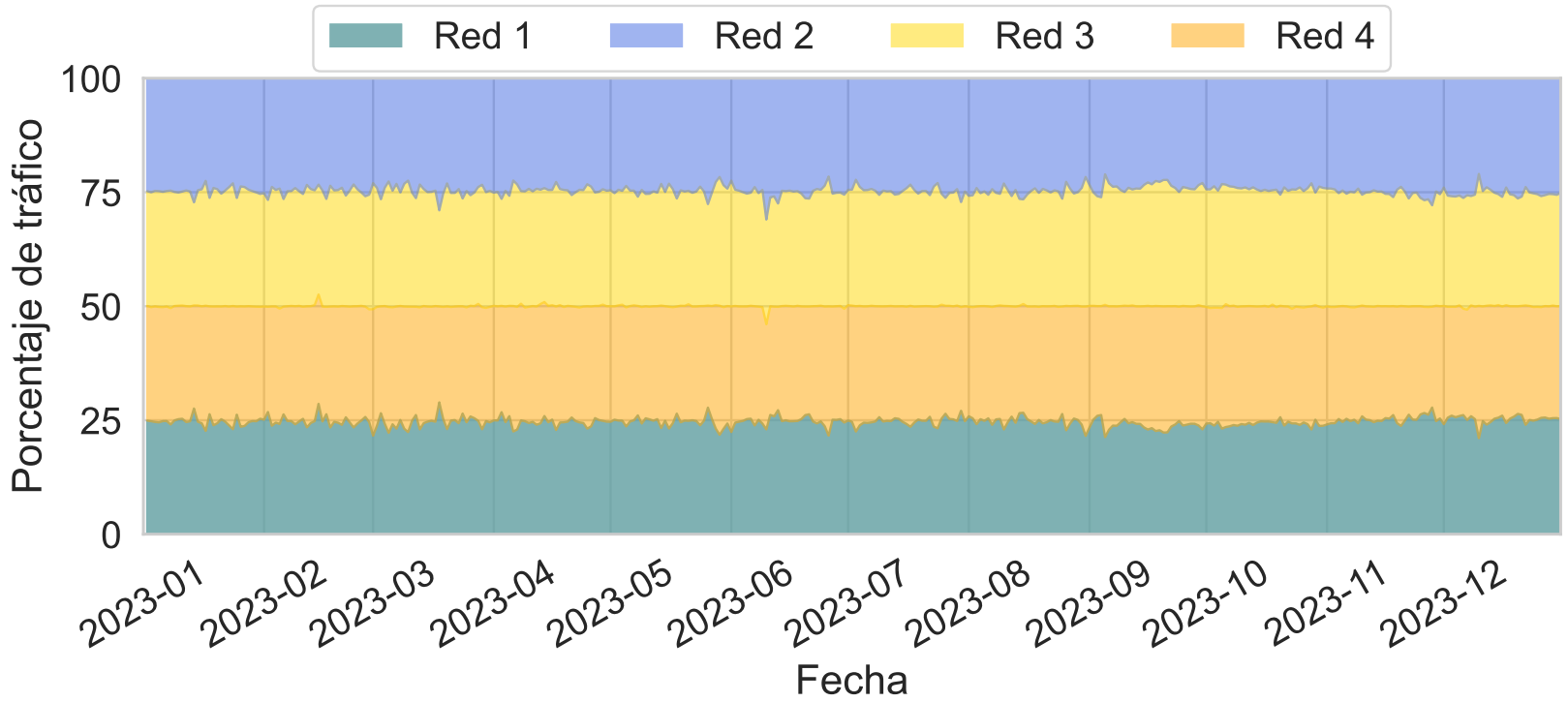
Volumen de datos elevado.

Metodología de análisis

Se han realizado análisis a diferente nivel:

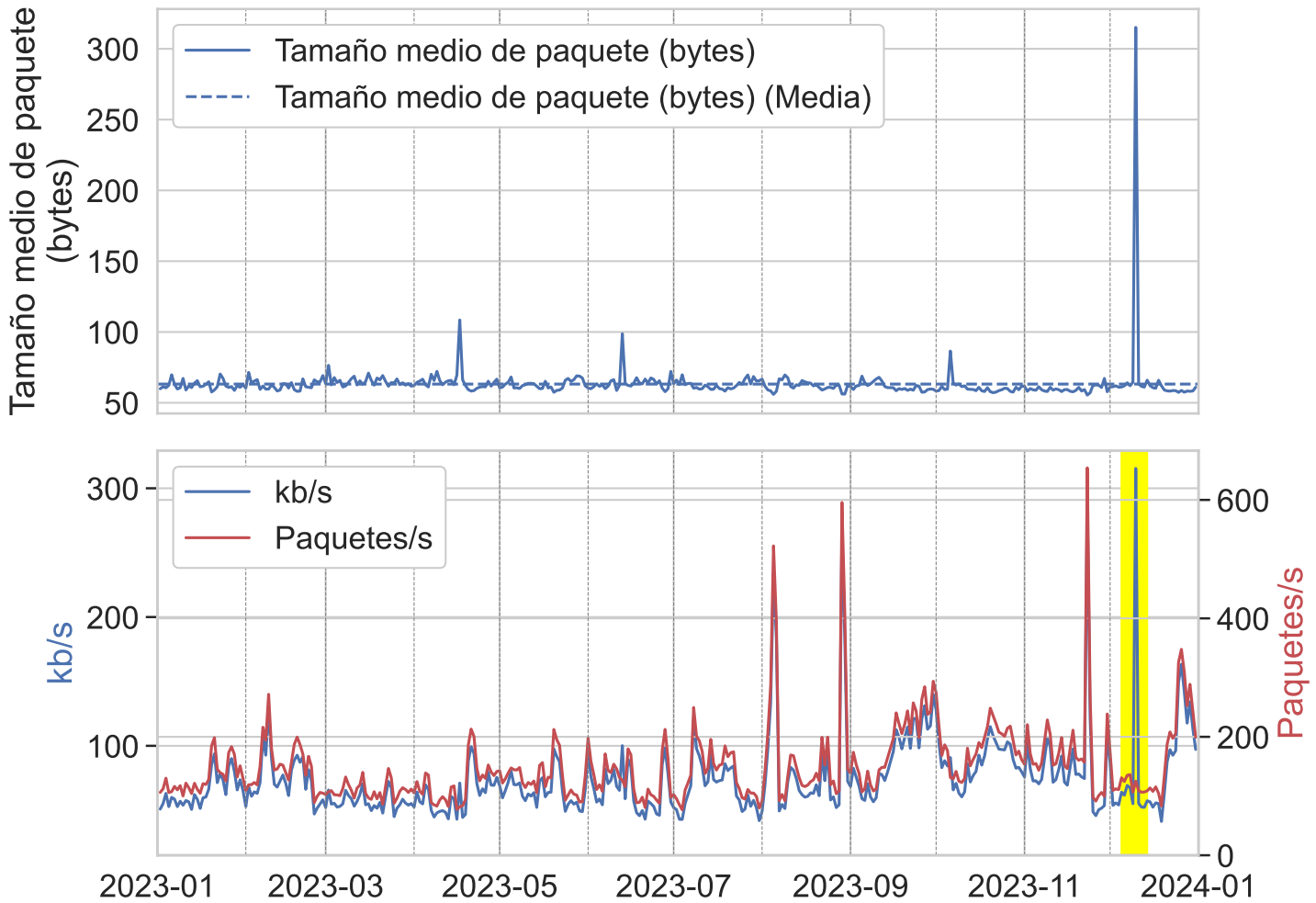
- Análisis estadístico de todo el periodo.
- Análisis detallado de un mes.
- Análisis específicos y de carga útil.

Porcentaje de paquetes recogidos por cada red

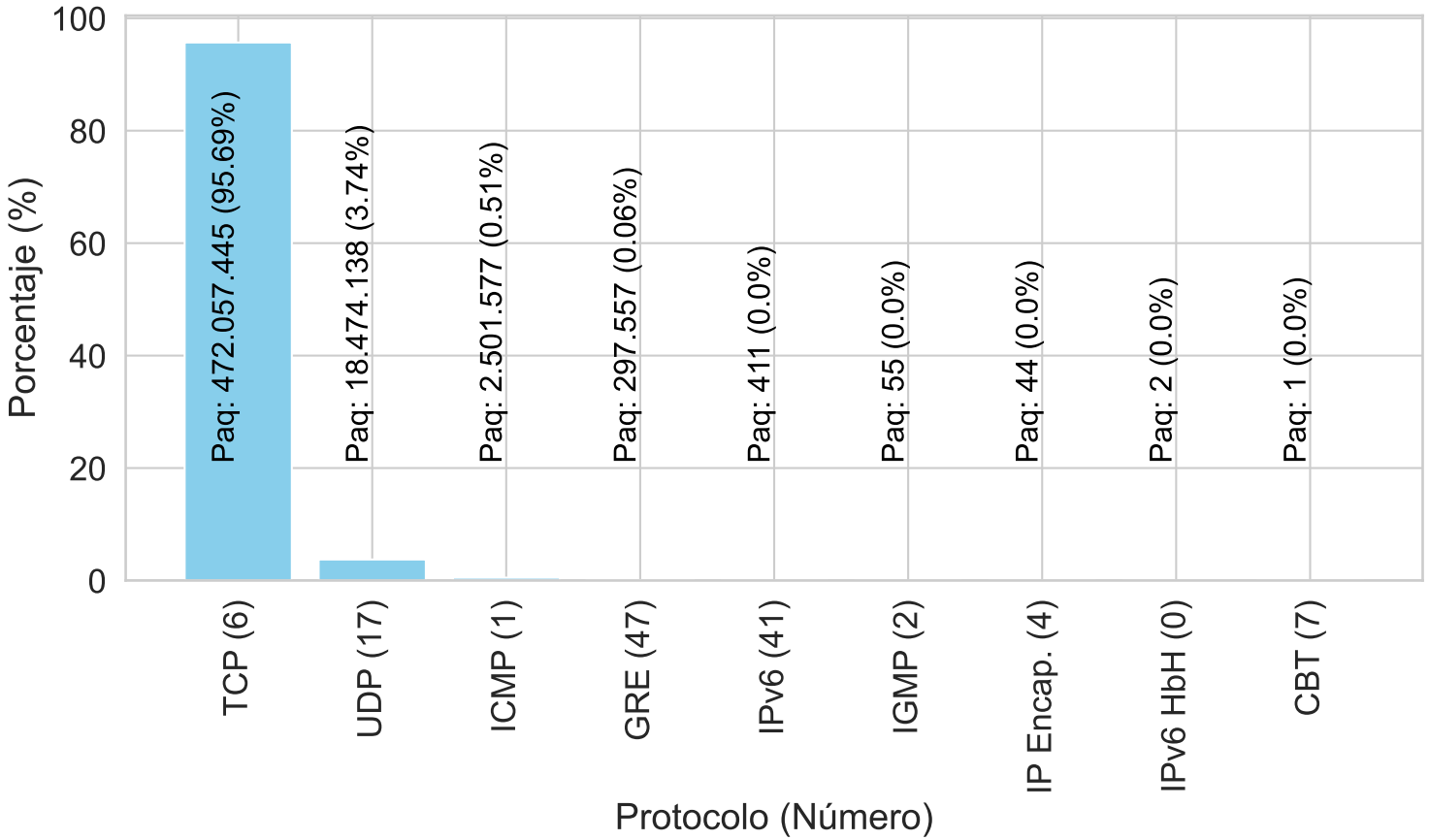


- Distribución uniforme entre redes dentro de una clase A. 50 %.
- Volumen de tráfico con variaciones similares en todas.
- Redes 3 y 4, ligero mayor volumen.

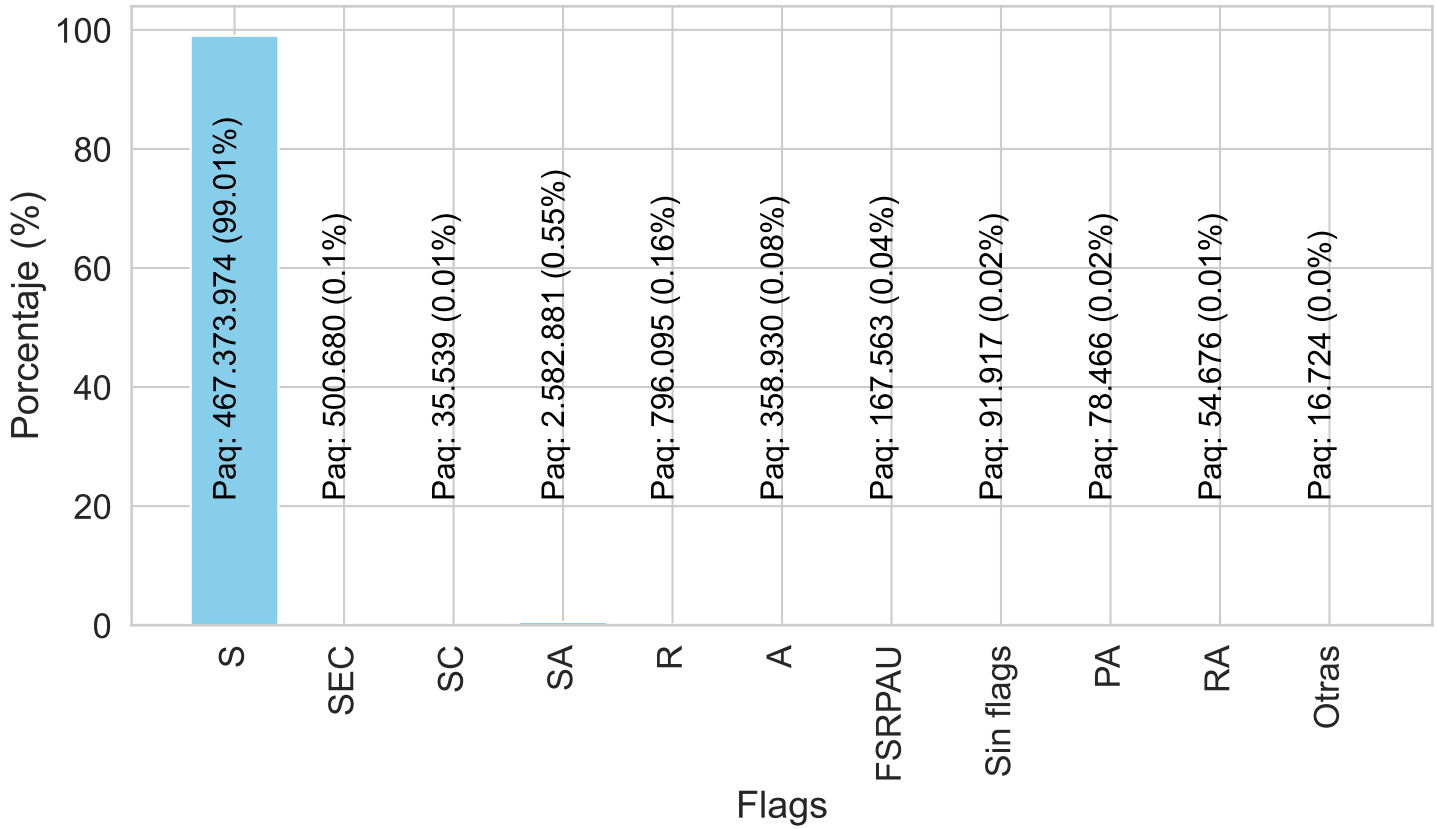
Volumen recibido



Distribución de protocolos en la cabecera IP



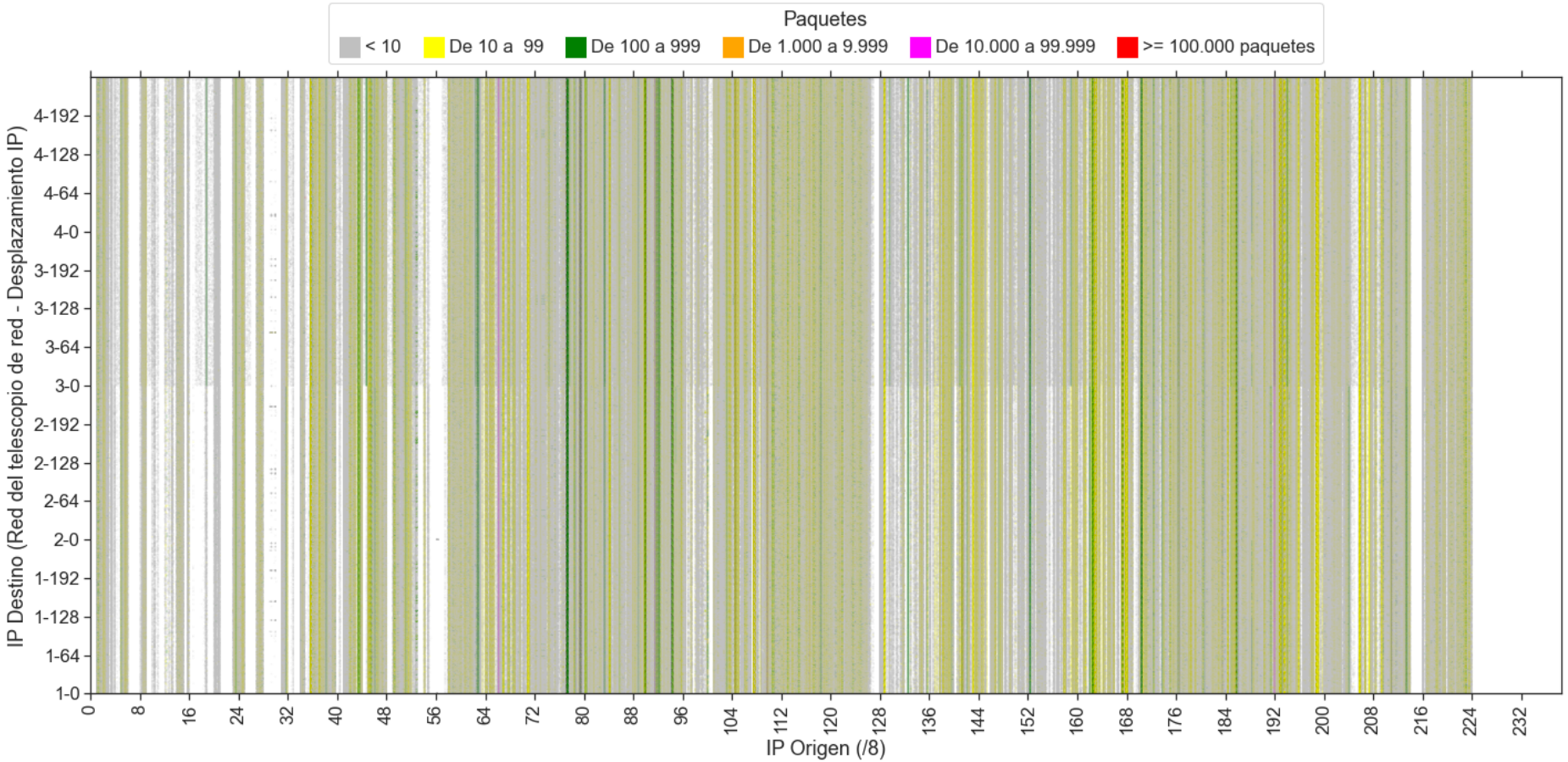
Protocol TCP - Distribución de *Flags*



Tráfico de enumeración *vs.* Tráfico *backscatter*.

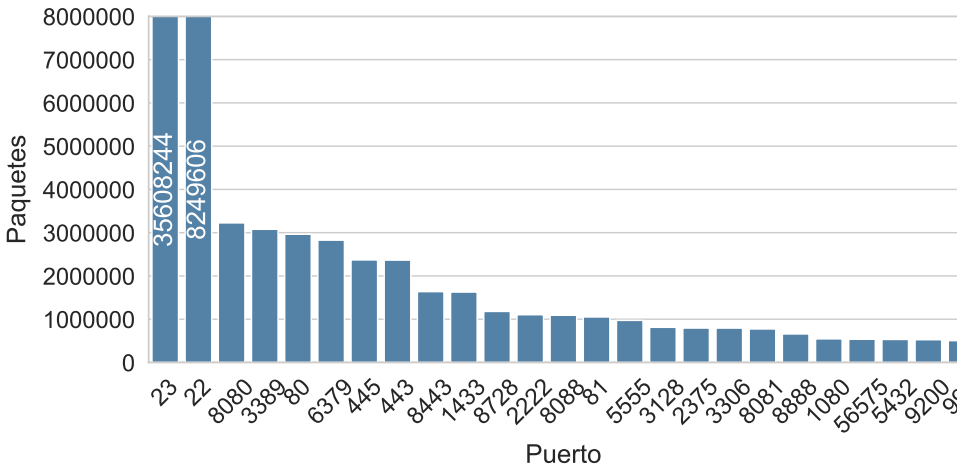
El 98,89 % del tráfico TCP no tiene payload.

TCP SYN. Origenes – Destinos

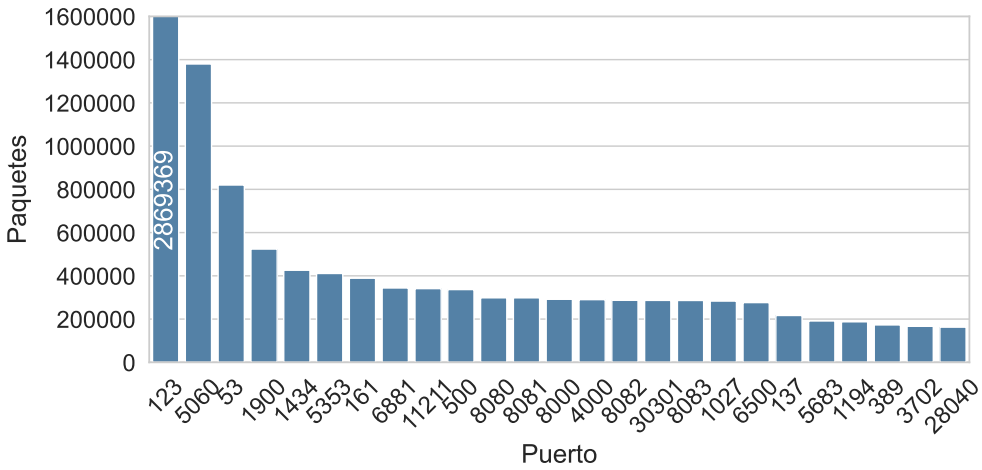


Puertos TCP / UDP - ICMP.

TCP



UDP



- Tamaños de *payload*: TCP 41,52 bytes, UDP 152,67 bytes.
- 30 % de los paquetes tienen el ID de la cabecera IP con el valor "54321"(ZMap). 18,7 % en TCP. Orígenes diferentes.
- ICMP: 97,95 % de los paquetes (2.450.412) son *Echo Request*

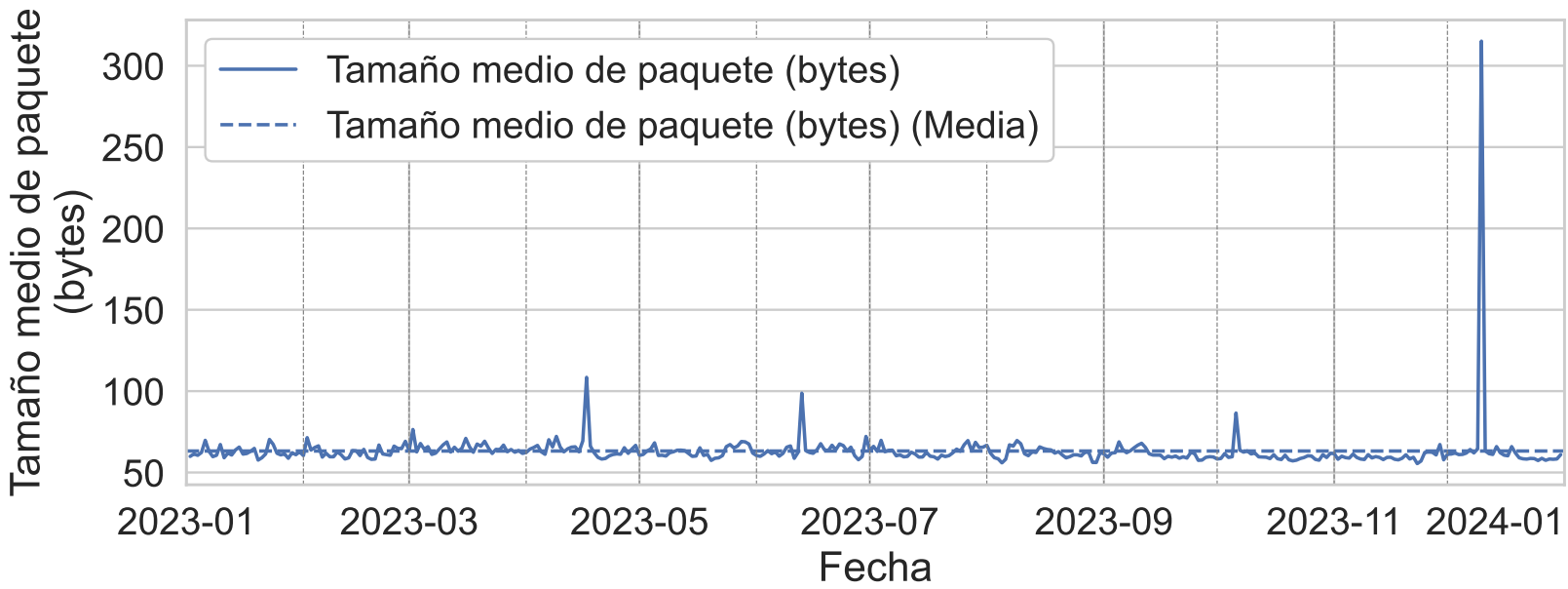
Ataques de reflexión NTP

- Ataque con solicitud `REQ_MON_GETLIST` o `REQ_MON_GETLIST_1`.
- Consulta de las últimas 600 direcciones IP que han consultado al servidor NTP.
- Se multiplica el tráfico de consulta más de 200 veces.

```
▾ User Datagram Protocol, Src Port: 52003, Dst Port: 123
    Source Port: 52003
    Destination Port: 123
    Length: 200
  ▸ Checksum: 0x0000 [zero-value ignored]
    [Stream index: 21220]
  ▸ [Timestamps]
    UDP payload (192 bytes)
▾ Network Time Protocol (NTP Version 2, private)
  ▸ Flags: 0x17, Version number: NTP Version 2, Mode: reserved for private use
  ▸ Auth, sequence: 0
    Implementation: XNTPD (3)
    Request code: MON_GETLIST_1 (42)
    0000 .... = Err: No error (0x00)
```

Ataques DDoS del 10 de diciembre

- Ataque DNS con múltiples solicitudes `"dig -t ANY sl"`.
- Obtiene el todos los registros (registro A, CNAME, claves criptográficas, etc.) del dominio de Sierra Leona (SL).
- Se multiplica el tráfico de consulta más de 100 veces.



Tráfico de evasión de censura

- Más utilizado en el mes de octubre (194.411 paquetes).
- Búsqueda de proxies para la creación de VPN entre usuario y proxy centralizado.
- *Ultrasurf* es el nombre del producto *freeware* que realiza la función de *proxy* de entrada.

```
GET /?q=ultrasurf HTTP/1.1\r\n
Host: modificado.com\r\n\r\n
```

Conclusiones del análisis

Se pueden extraer las siguientes conclusiones:

- Se han analizado las características y tipos de tráfico de un telescopio de red español durante 2023.
- Se han analizado 4,75 mil millones de paquetes IP.
- Principalmente el tráfico es de enumeración (95 % TCP, 99 % TCP-SYN) y sin payload.
- El tráfico IBR ha aumentado ligeramente respecto a estudios previos.
- No se ha detectado un mayor volumen de tráfico de redes con origen España.
- Se han analizado en mayor detalle algunos de los ataques detectados, como DDoS de amplificación NTP y DNS, y el de evasión de situaciones de censura, que no había sido reportado previamente.

Trabajos futuros

Como posibles líneas de trabajo futuro se propone:

- Realizar una comparativa con otros telescopios de red y con telescopios distribuidos que respondan a ciertos patrones de tráfico (HoDiNT).
- Utilizar herramientas de tipo *tcpflow* y *udpflow* para poder reensamblar los paquetes y realizar búsquedas de información.
- Realizar *clustering* automáticamente el tráfico capturado, priorizando aquellos que ofrezcan información relevante.

HoDiNT

HoDiNT: Home Distributed Network Telescope. Es un solución distribuida de telescopio de red, de bajo coste, fácil instalación y con soporte de detección de ataques en dos fases.

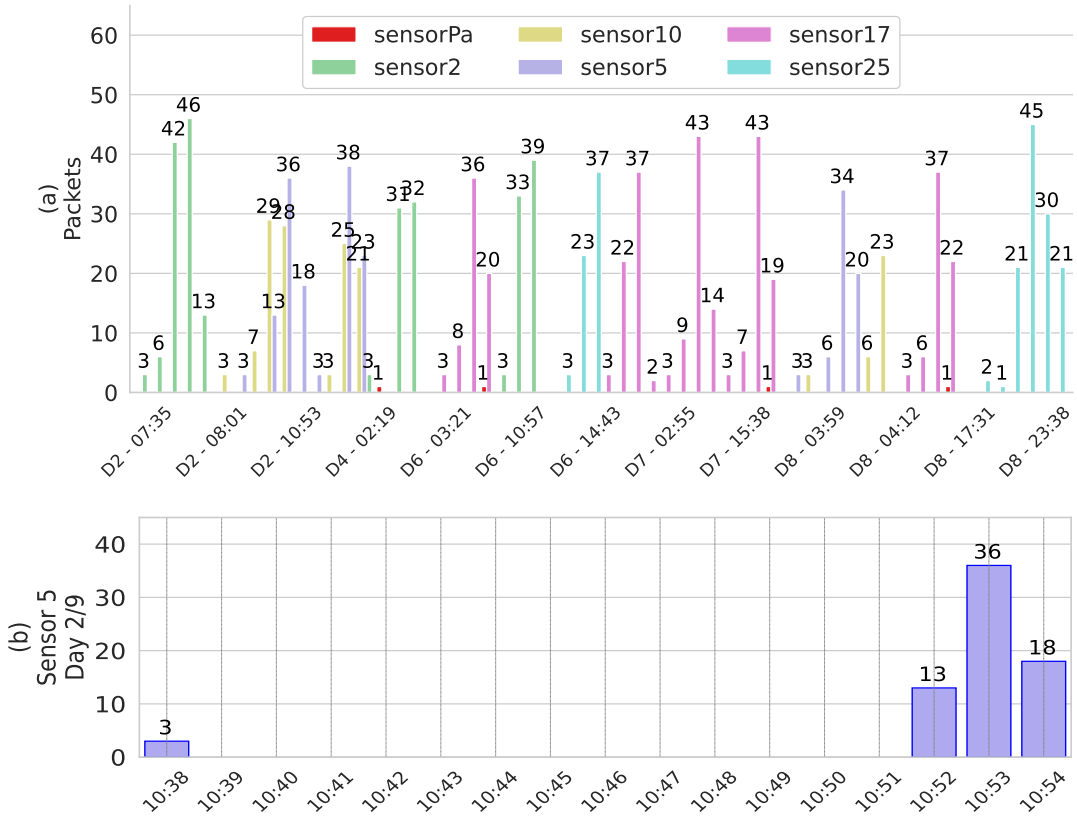
HoDiNT

Tráfico de los sensores de la muestra.

	TCP		UDP		ICMP	
Sensor	Entrada	Salida	Entrada	Salida	Entrada	Salida
s05 (R)	250.130	27.709	22.054	10.137	1.337	325
s14 (R)	211.638	38.132	13.633	13.358	255	35
s16 (-)	8.831	0	671	0	780	0
s17 (R)	205.793	37.639	11.618	5.337	650	183
s18 (-)	8.207	0	10.328	0	0	0
s19 (-)	8.508	0	457	0	294	0
s30 (R)	111.795	11.871	1.176	854	146	5
s67 (-)	6.985	0	403	0	0	0
s68 (R)	524.354	58.445	31.737	10.627	1.793	195
s69 (R)	163.883	28.325	18.318	5.827	2.369	989

- Mucho mayor el número de paquetes en los sensores que responden.
- Diferencia principal en TCP y UDP.
- El ratio responder/no responder es x30 en TCP y x6 en UDP.
- Al responder, por cada paquete TCP, se reciben 7 y en UDP, 2.

HoDiNT



https://www.sciencedirect.com/science/article/pii/S138912862400402X

Pero esto es para otro ES.NOG. . . Si queréis participar, poneos en contacto con nosotros.

Me gustaría agradecer a la persona que nos ha facilitado los ficheros

Para terminar...