Peering into the Darkness: The Use of UTRS in Combating DDoS Attacks

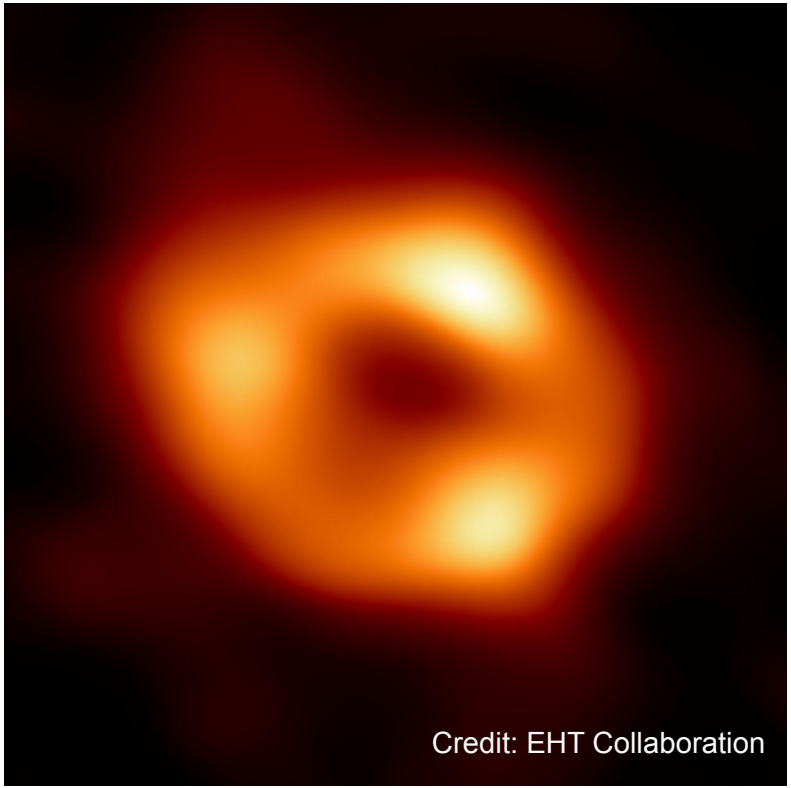
Radu Anghel[1], Swaathi Vetrivel[1], Elsa Turcios Rodriguez[1], Kaichi Sameshima[2], Daisuke Makita[3], Katsunari Yoshioka[2], Carlos Gañán[1] and **Yury Zhauniarovich**[1]

[1] TU Delft, [2] Yokohama National University,

[3] Yokohama National University/National Institute of Information and Communications Technology

Background

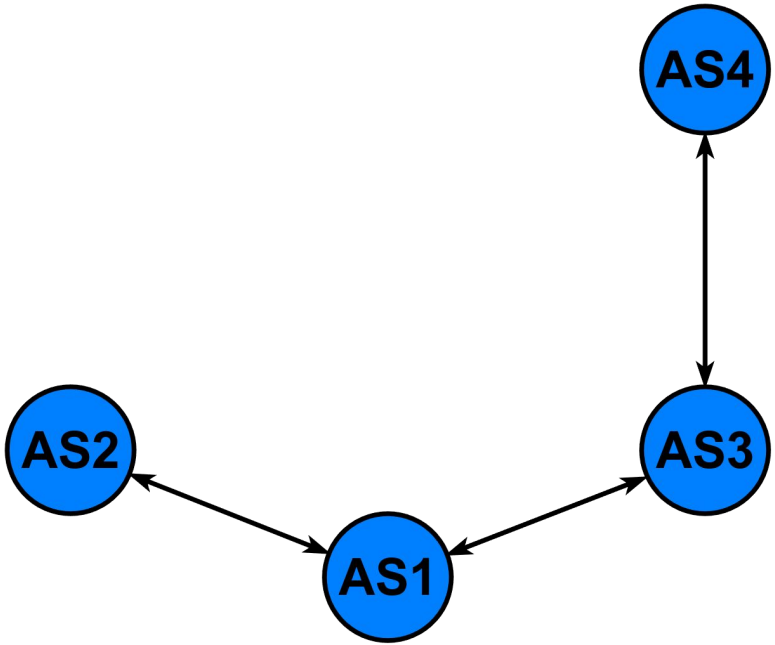
- **Border Gateway Protocol (BGP)** is a routing protocol responsible for ensuring the interconnectivity of **Autonomous Systems (ASes)**
- **BGP attributes** are used to provide additional value-added services, e.g., **Remotely Triggered Black Hole (RTBH)**:
- **RTBH** allows the victim AS to advertise an IP under attack using BGP [1]. Upon receiving this advertisement, the peers of the AS (or the community) start discarding the packets to that IP (null route, black hole)
- **Unwanted Traffic Removal Service (UTRS)** is a global free easy-to-join RTBH service operated by a trusted third-party (Team Cymru [2]).



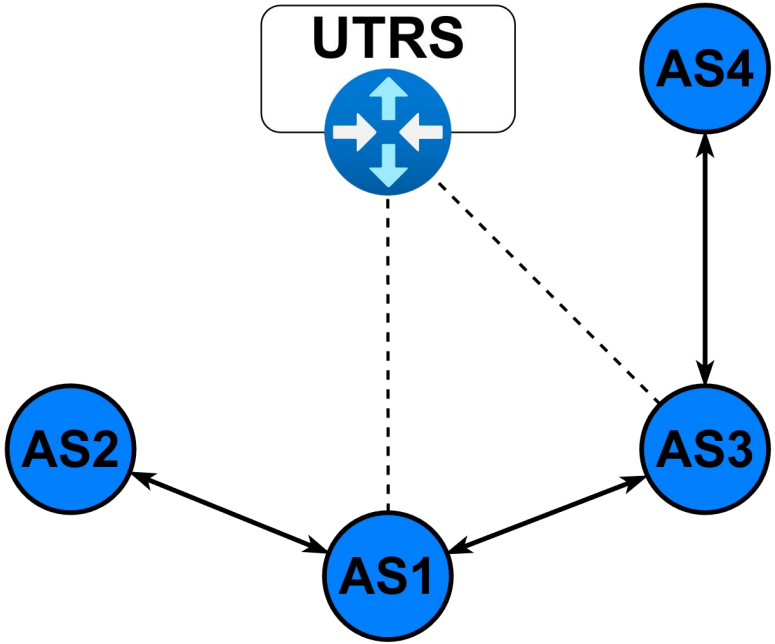
1. Doughan Turk. 2004. Configuring BGP to Block Denial-of-Service Attacks. RFC3882. https://doi.org/10.17487/RFC3882

2. https://www.team-cymru.com/ddos-mitigation-services

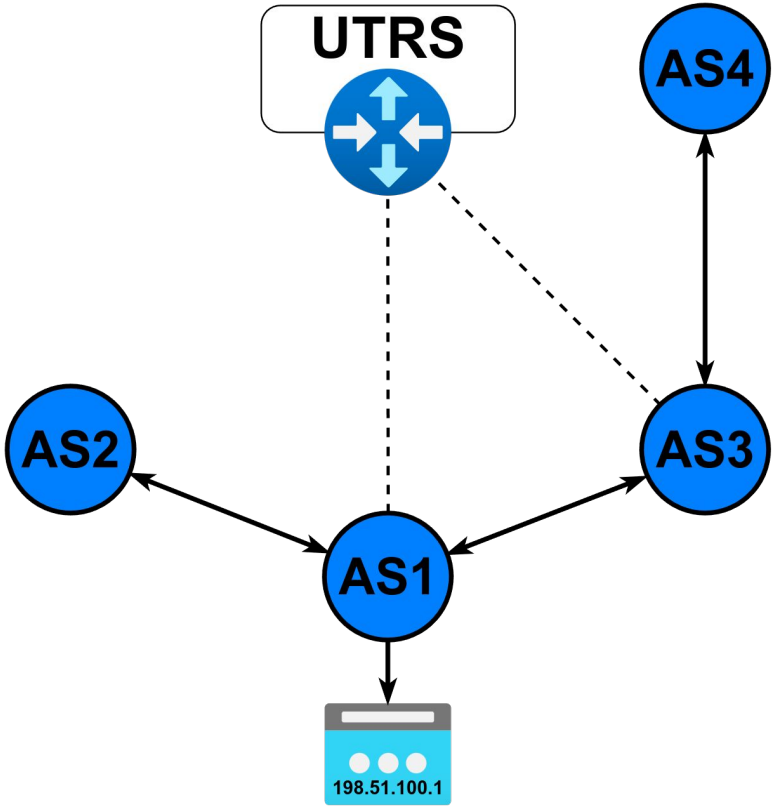
Background: Unwanted Traffic Removal Service



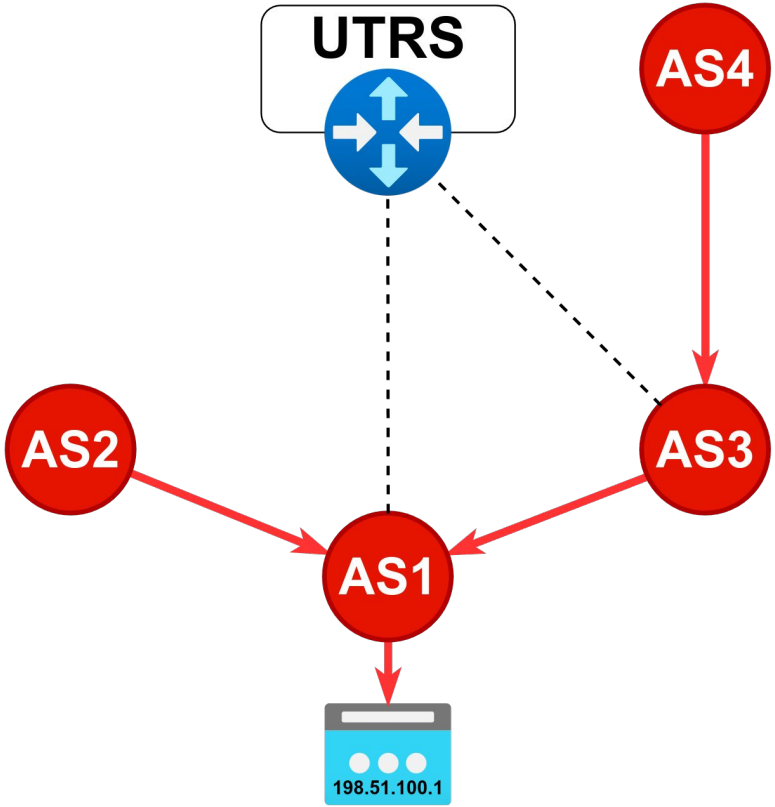
Background: Unwanted Traffic Removal Service



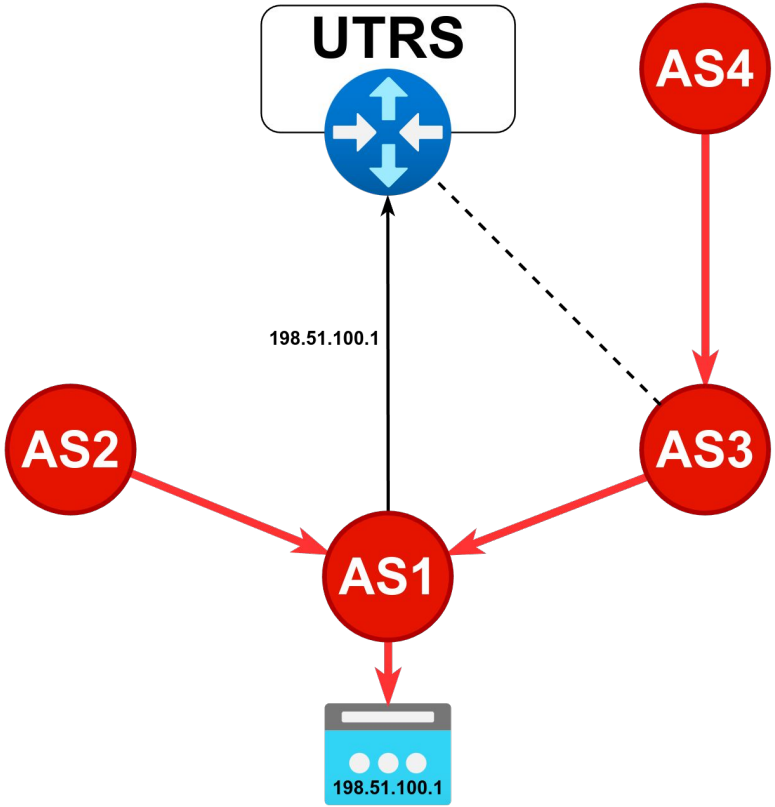
Background: Unwanted Traffic Removal Service



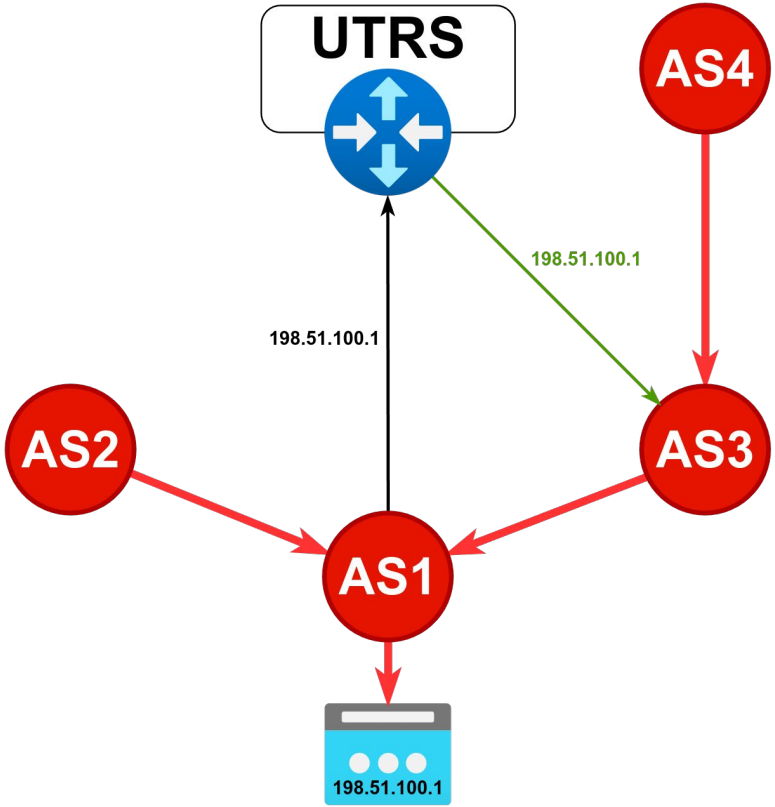
Unwanted Traffic Removal Service



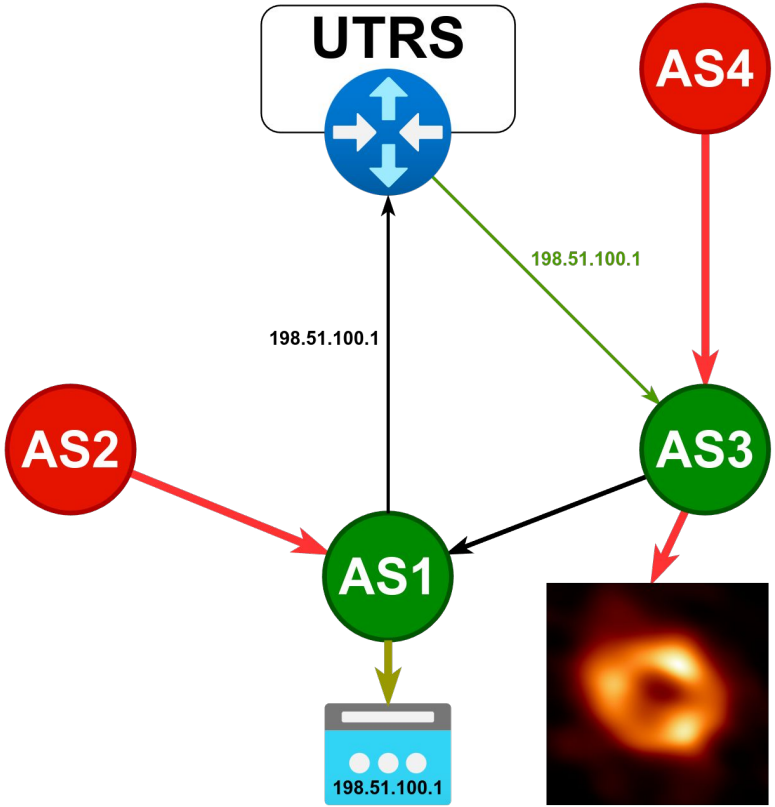
Background: Unwanted Traffic Removal Service



Background: Unwanted Traffic Removal Service



Background: Unwanted Traffic Removal Service

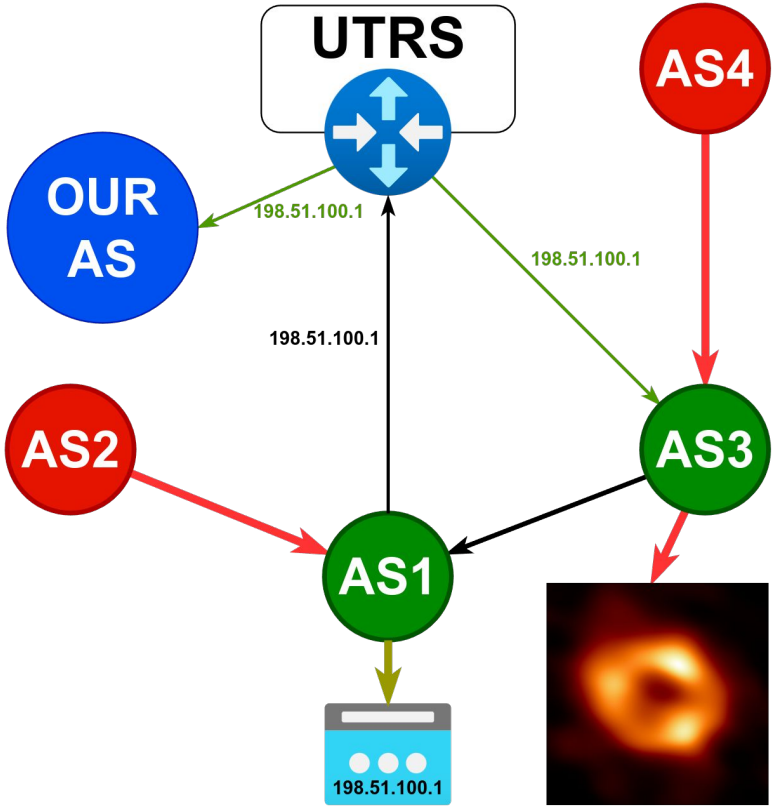


Research Questions

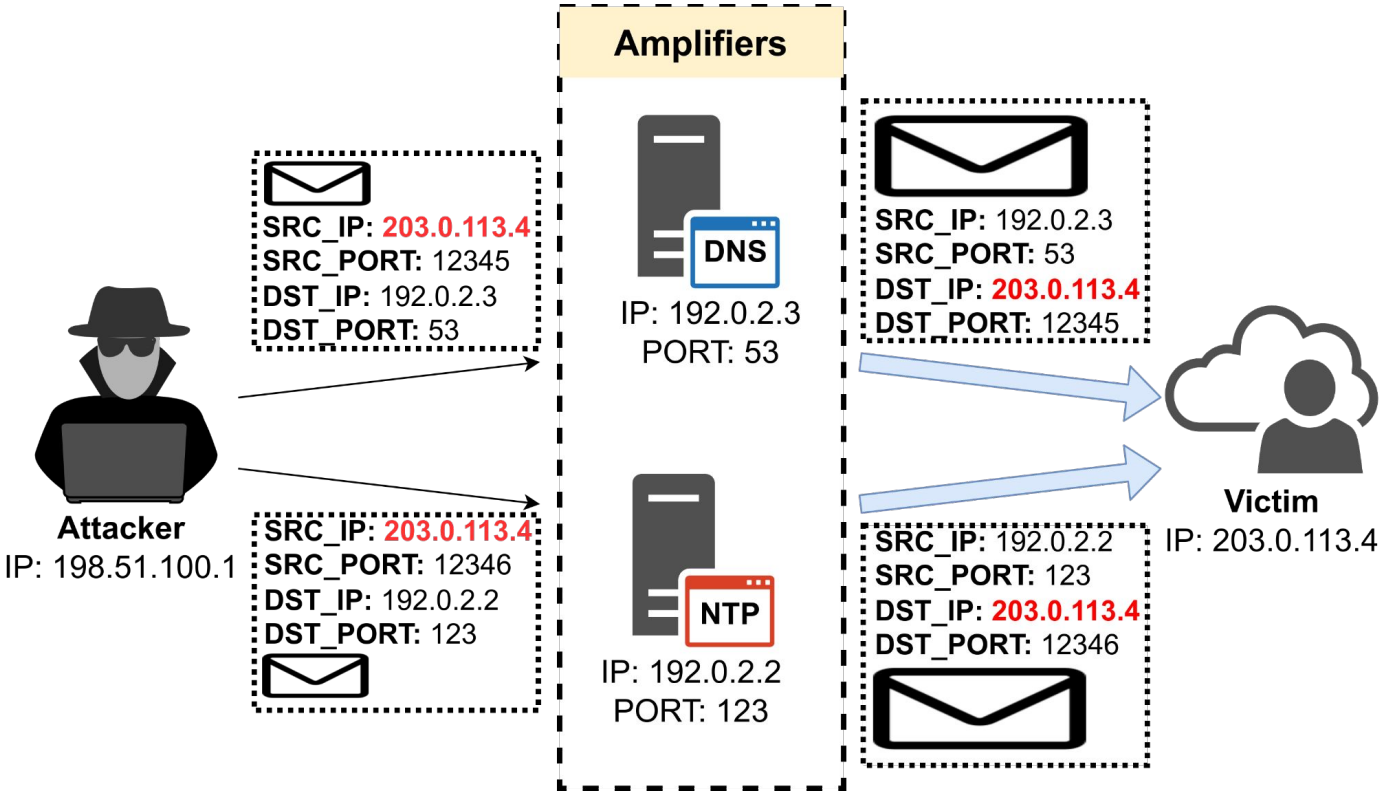
How extensively is UTRS used to counter DDoS attacks?

- RQ1: How many UTRS members use this service to mitigate attacks?
- RQ2: To what extent are DDoS attacks triggering mitigation attempts via UTRS?
- RQ3: To what extent can UTRS announcements be explained by amplification DDoS attacks?
- RQ4: To what extent can UTRS announcements be explained by IoT-botnet-driven DDoS attacks?

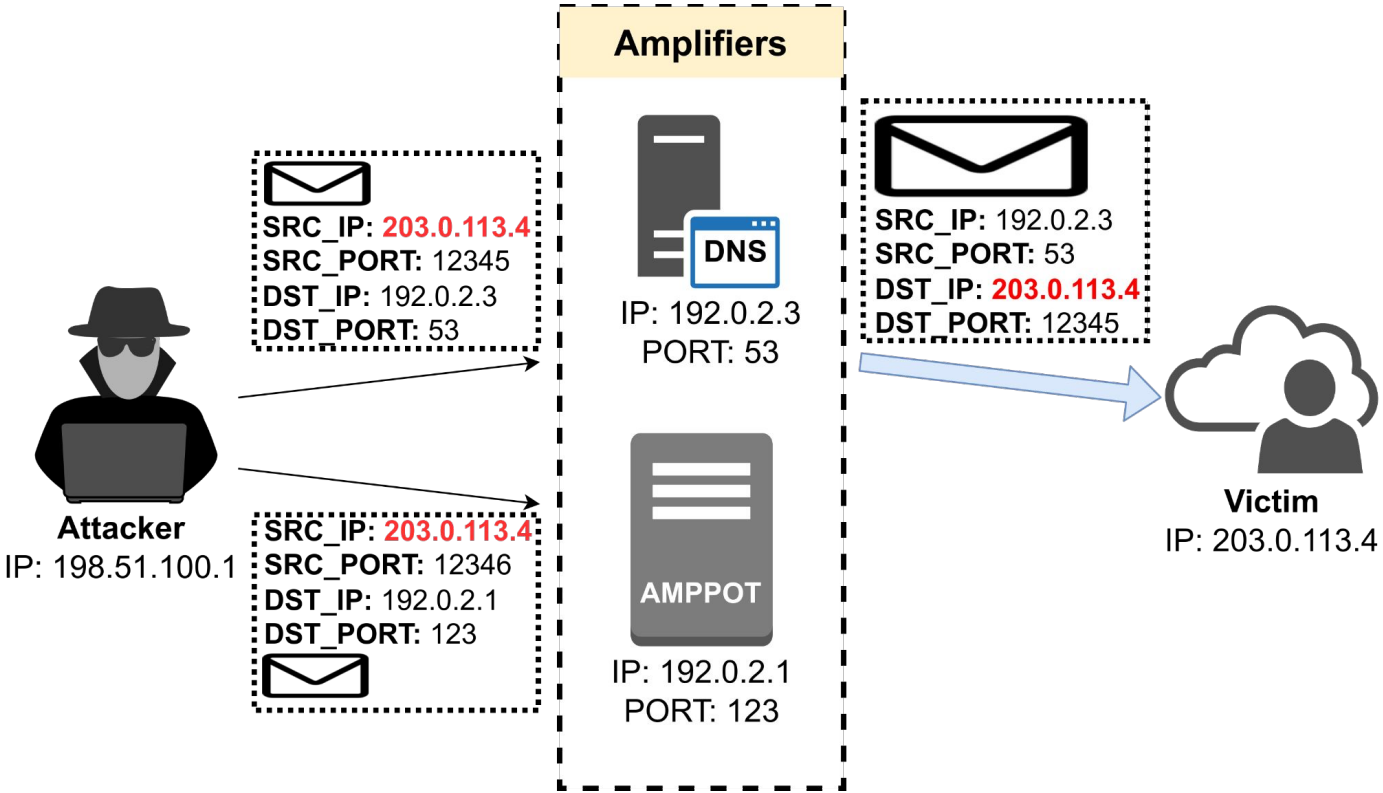
UTRS Dataset Collection



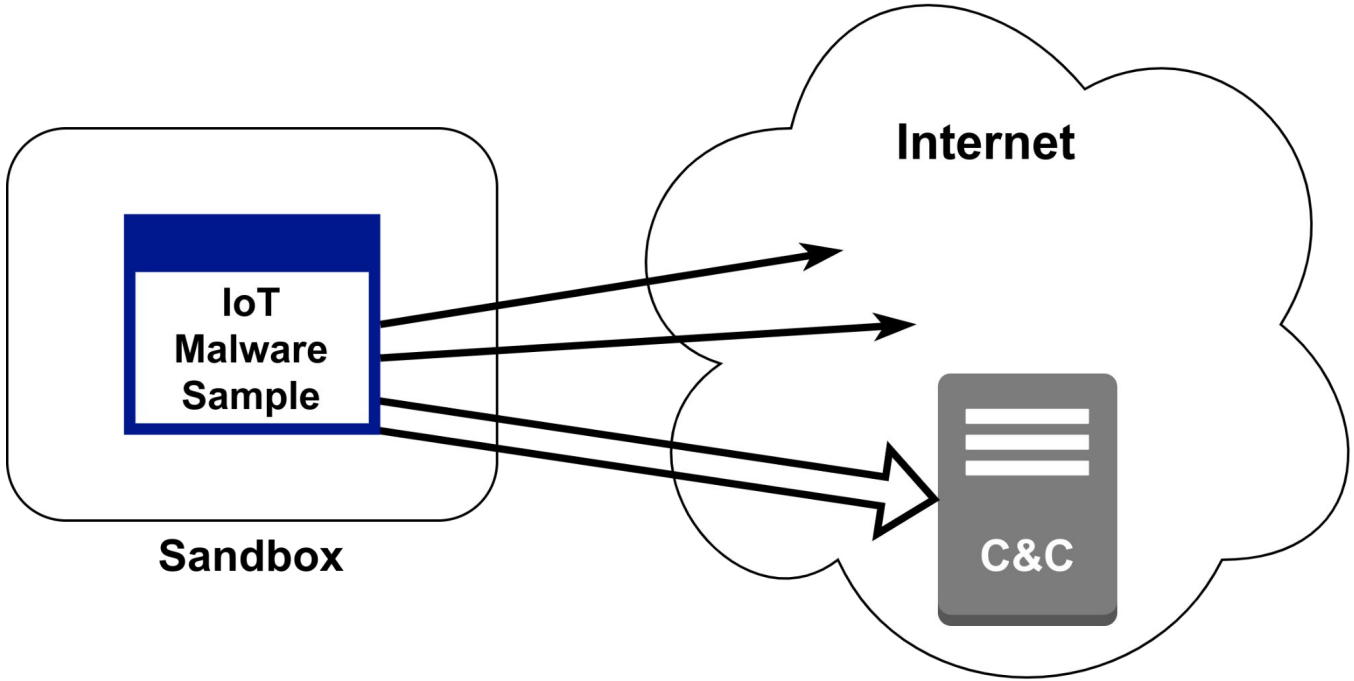
Amplification DDoS Attacks



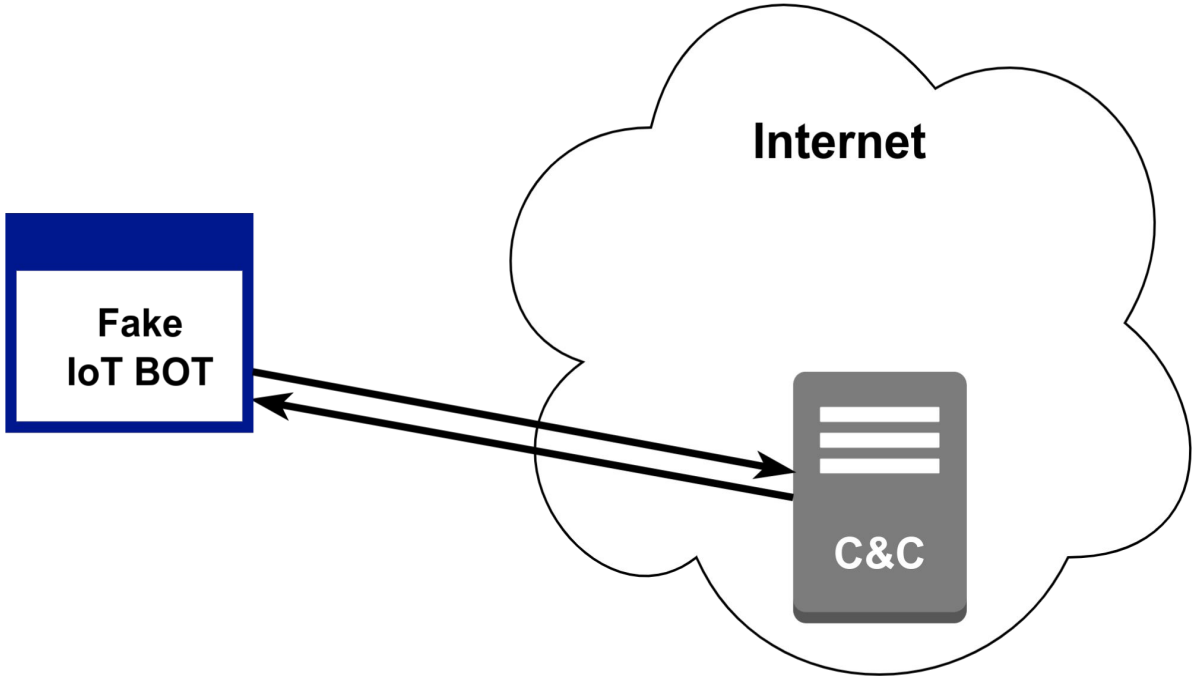
Amplification DDoS Attacks Dataset Collection



IoT DDoS Attacks Dataset Collection

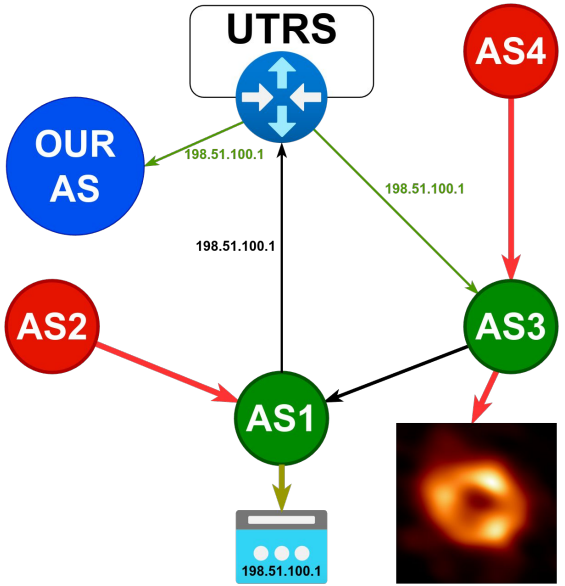


IoT DDoS Attacks Dataset Collection



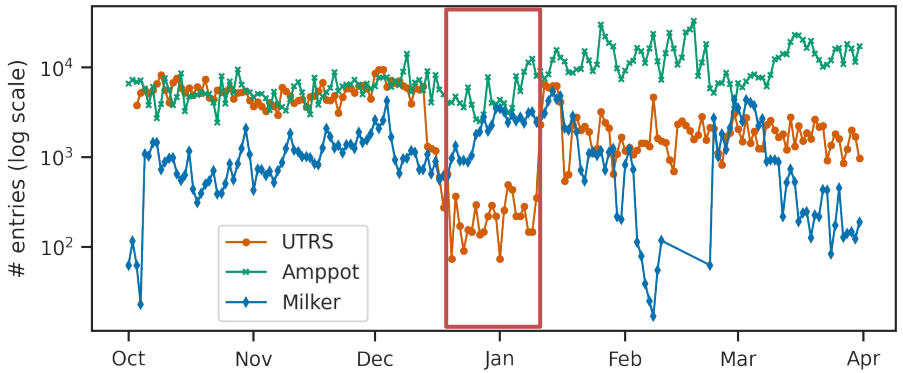
Datasets (6 months)

- UTRS
  - OUR AS collects snapshots of active UTRS-related BGP routes every 5 minutes
  - Stitch entries if the same target is in the two consecutive snapshots
- AmpPot [1]
  - Honeypot that pretends to be an amplifier
  - Collects the start and end time, target IP address, source port and volume of a DRDoS attack
- IoT Milker
  - Imitates IoT bot behavior, receiving attack commands from C&C servers
  - Collects the start time, target network and port, and duration of an IoT DDoS attack

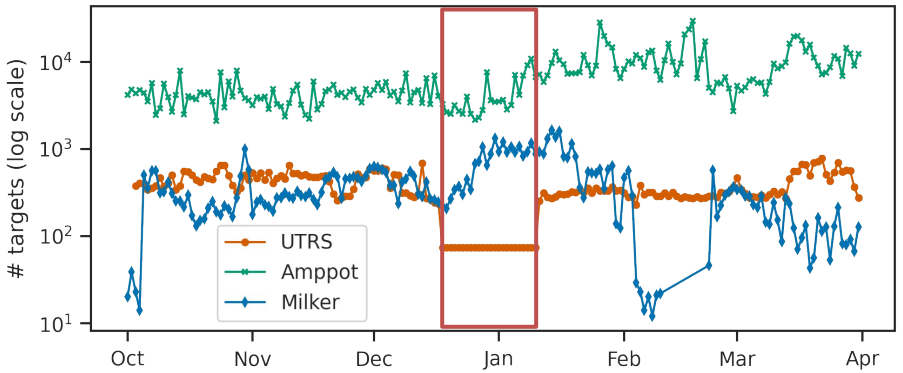


1. Krämer, L., Krupp, J., Makita, D., Nishizoe, T., Koide, T., Yoshioka, K., Rossow, C.: “AmpPot: Monitoring and Defending Against Amplification DDoS Attacks.” RAID, 2015

Datasets Description

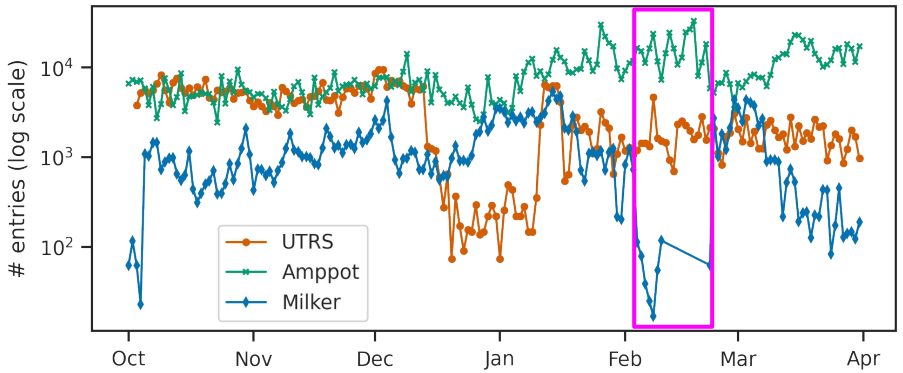


a) Number of entries per day

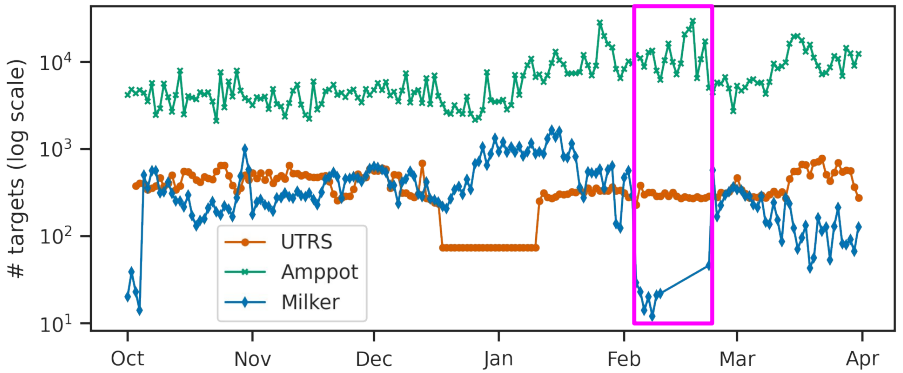


b) Number of targets per day

Datasets Description

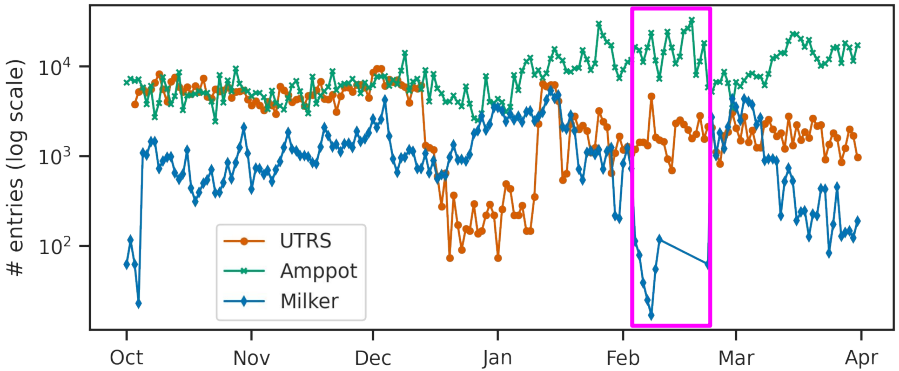


a) Number of entries per day

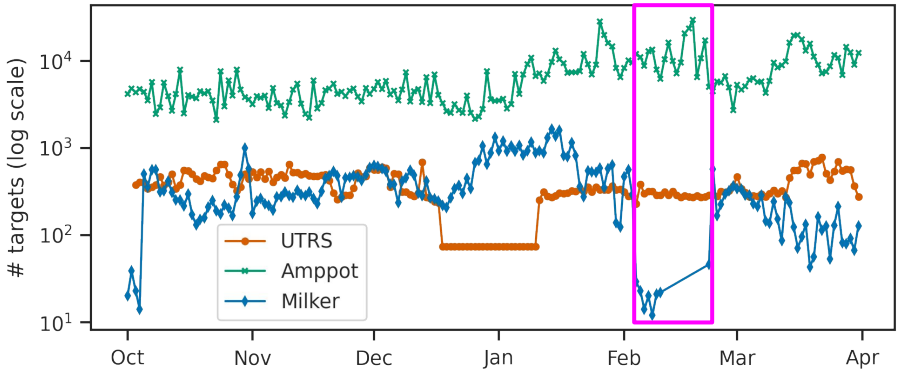


b) Number of targets per day

Datasets Description



a) Number of entries per day



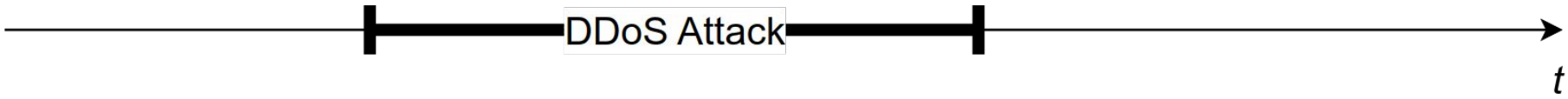
b) Number of targets per day

Dataset	# entries	# targets	# unique target IPs	Duration (sec)		
				min	mean	max
UTRS	533,257	7,820	7,830	300.0	4,682.7	413,700.0
AmpPot	1,616,184	1,080,770	1,080,770	0.5	891.5	1,949,571.0
Milker	223,267	46,764	2,787,522	1.0	93.0	3,600.0

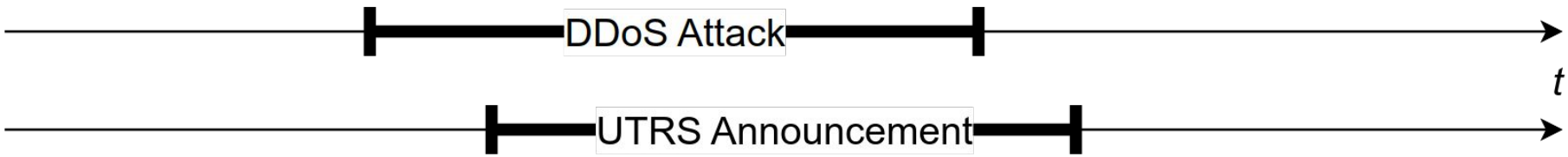
Findings: UTRS Dataset

- **Highlights:**
  - **Low usage:** minimum 74, mean 3,122, and maximum 9,427 announcements to minimum 74, mean 357, maximum 776 targets per day
  - **Sparse coverage:** the majority of UTRS announcements (533,255) target individual IP addresses (/32 prefix length), only 2 entries targeted the same /27 subnetwork within the same day
  - **Low conversion:** only 124 ASes out of 1,300+ UTRS members (around 10%) use this service to advertise IPs
  - **Short duration:** 21% of all announcements is less than 5 minutes, longest - 4 days, 18 hours and 55 minutes

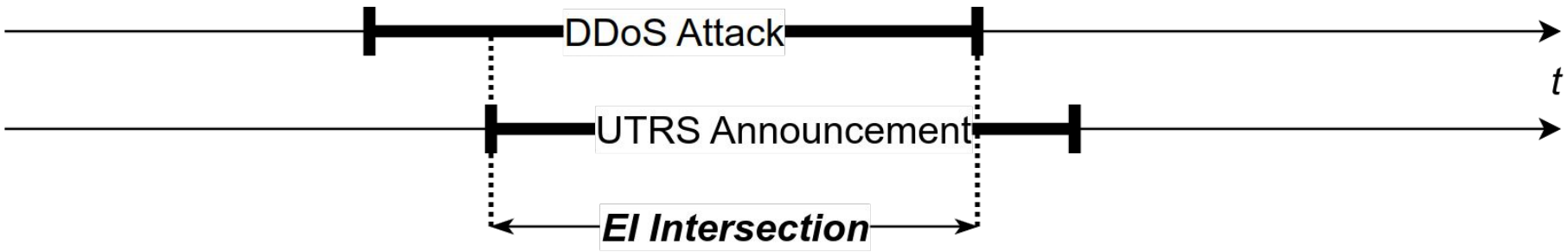
Datasets Intersection



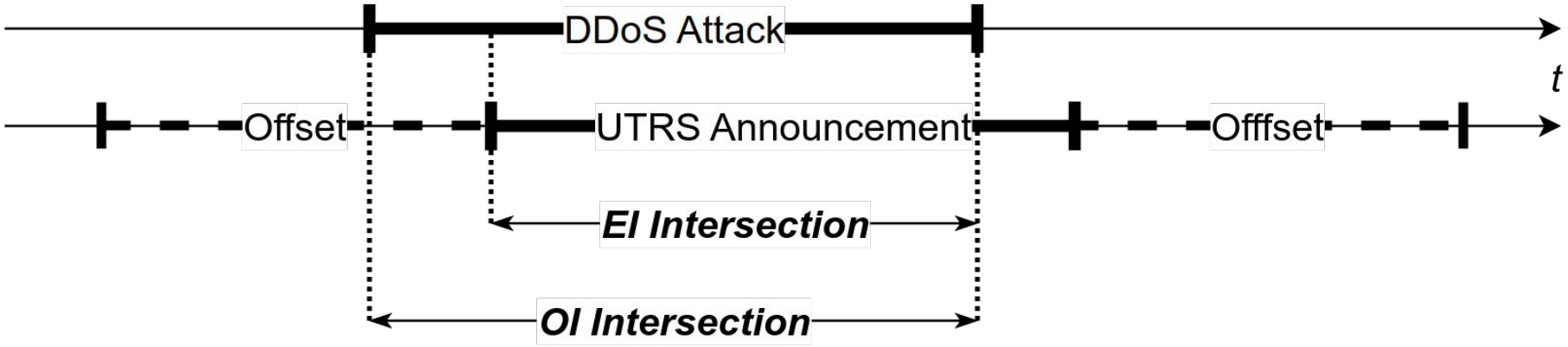
Datasets Intersection



Datasets Intersection: Exact Interval (EI)



Datasets Intersection: Offset Interval (OI)



1. Jonker, M., Pras, A., Dainotti, A., Sperotto, A.: “A First Joint Look at DoS Attacks and BGP Blackholing in the Wild.” IMC, 2018

Findings: Datasets Intersections

- Low number of intersections with DDoS datasets

Parameter	UTRS-AmpPot		UTRS-Milker	
	EI	OI	EI	OI
# of entries	468	6,774	9	791
# of unique DDoS attack targets	249	1,268	2	143
# of unique UTRS targets	249	1,268	8	163
# of unique UTRS ASNs	25	43	2	6
Mean entries # per UTRS announcement	1.55	1.76	1.12	1.88

Findings: Datasets Intersections

- Low number of intersections with DDoS datasets
- Low number (43 total) of ASNs for which an intersection is found
  - 11 ASNs are from Brasil, 9 from the USA, 7 from Argentina

Parameter	UTRS-AmpPot		UTRS-Milker	
	EI	OI	EI	OI
# of entries	468	6,774	9	791
# of unique DDoS attack targets	249	1,268	2	143
# of unique UTRS targets	249	1,268	8	163
# of unique UTRS ASNs	25	43	2	6
Mean entries # per UTRS announcement	1.55	1.76	1.12	1.88

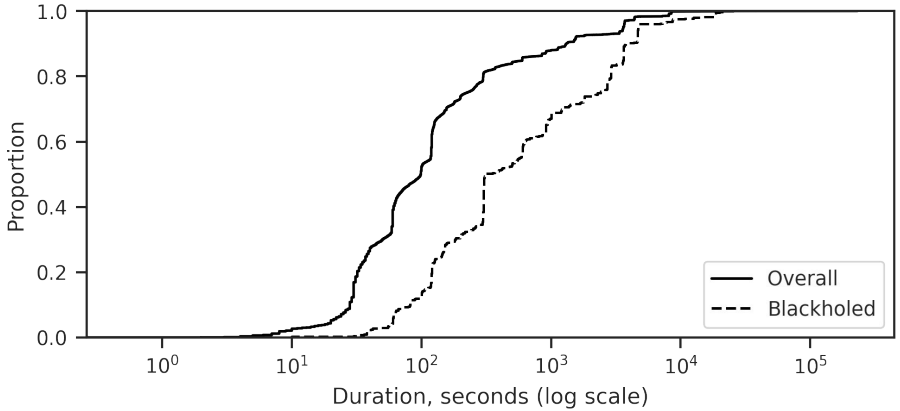
Findings: Datasets Intersections

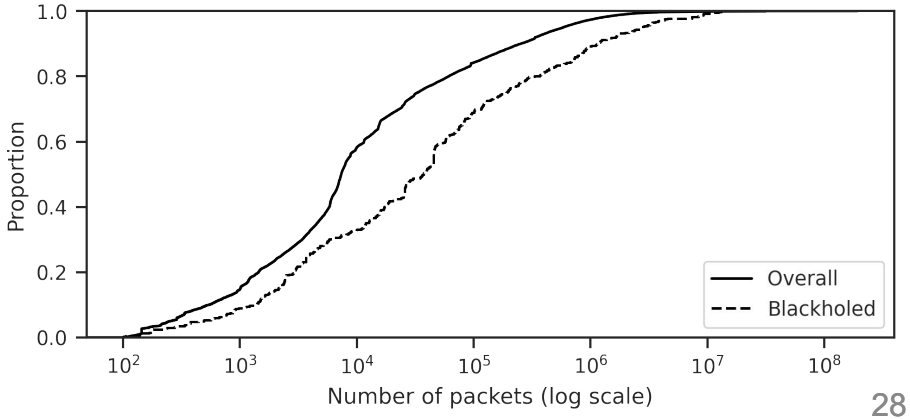
- Low number of intersections with DDoS datasets
- Low number (43 total) of ASNs for which an intersection is found:
  - 11 ASNs are from Brasil, 9 from the USA, 7 from Argentina
- Low percent of DDoS attacks **on the UTRS members** trigger mitigation:
  - 1.03% of AmpPot and 0.06% of Milker for EI
  - 8.86% of AmpPot and 6.88% of Milker for OI
- **Globally**, the percentage even lower:
  - 0.025% of AmpPot and 0.001% of Milker for EI
  - 0.212% of AmpPot and 0.147% of Milker for OI

Findings: Blackholed Attacks Characterisation

Overall - all AmpPot-recorder attacks on all ASNs triggering at least one mitigation attempt

Blackholed - all AmpPot-recorded attacks for which exact intersection with the UTRS data is found





Conclusions

- UTRS is a free, global, and low-effort-to-join alternative to RTBH
- **Takeaways:**
  - Around 1% of all ASNs are UTRS members
  - Only 124 ASes out of 1300+ UTRS members (around 10%) use this service to advertise IPs
  - UTRS announced maximum 776 targets per day
  - Only 0.025% of amplification and 0.001% of IoT-botnet-driven attacks are highly likely attempted to be mitigated using UTRS
- **Acknowledgements:**

  - RAPID project (Grant No. CS.007) supported by Dutch Research Council (NWO), the Netherlands
  - MITIGATE project (JPJ000254) supported by MIC, Japan
  - Commissioned research (No.05201) supported by NICT, Japan
  - JSPS KAKENHI Grants (Numbers 21H03444 and 21KK0178)