Down the Black Hole: Dismantling Operational Practices of BGP Blackholing at IXPs

Marcin Nawrocki, Jeremias Blendin, Christoph Dietzel,
Thomas C. Schmidt, Matthias Wählisch

Freie Universität Berlin

DE CIX

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Christmas is near!

https://www.shutterstock.com/video/clip-1584091-small-red-christmas-present-looping-on-white

amazon

All | funny techy gifts

Deliver to Germany

Today's Deals | Help | Registry | Gift Cards | Sell | Your Amazon.com

1-48 of over 2,000 results for **"funny techy gifts"**

Department

- Novelty & More
  - Women's Novelty Clothing
  - Women's Novelty Tops & Tees
  - Boys' Novelty Tops & Tees
  - Girls' Novelty Tops & Tees
- Handmade Products
  - Handmade Signs & Plaques
- Kitchen & Dining
  - Travel Mugs & Tumblers
- See All 15 Departments

Avg. Customer Review

★★★★☆ & Up
★★★☆☆ & Up
★★☆☆☆ & Up
★☆☆☆☆ & Up

Home Décor Material

☐ Wood

Furniture & Décor Style

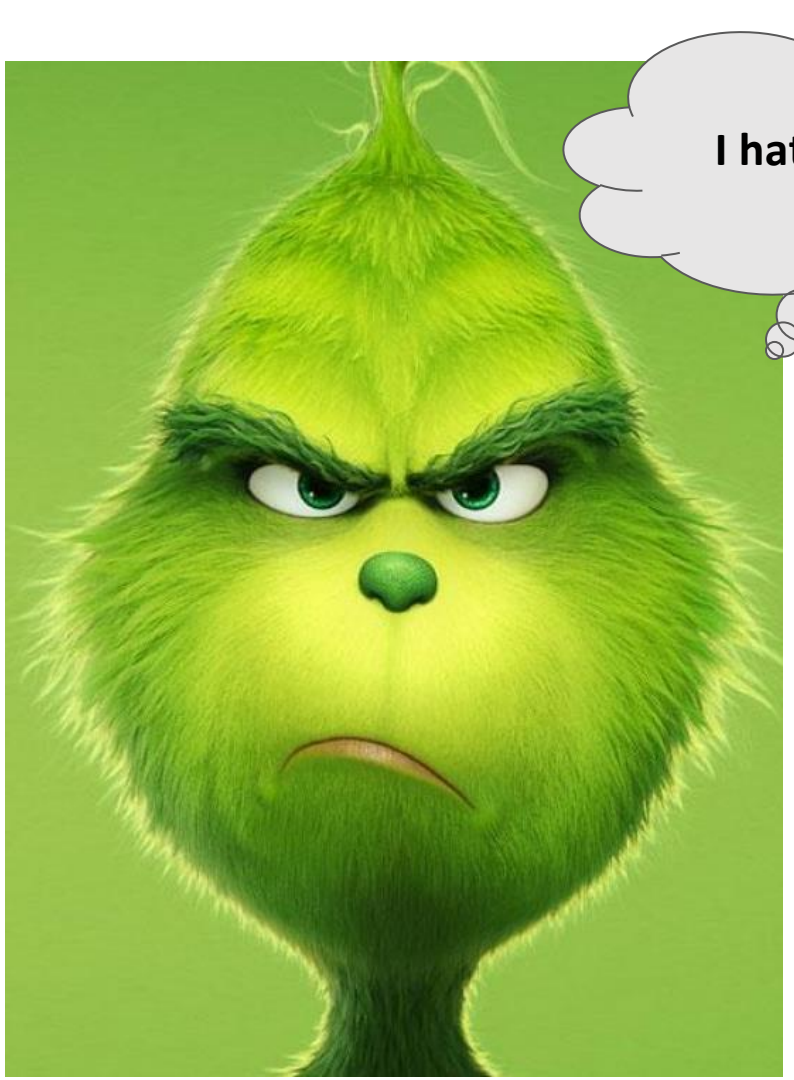
Price and other details may vary based on size and color

Funny Tech Support Checklist Helpdesk Hotline Coffee & Tea Gift

USB Floppy Disk I Am Your Father TShirt |Funny Nerd Geek Tee

Hello Have You Tried Turning It Off and On Again??: Journal and

https://indac.org/blog/the-grinch-official-trailer-3/



amazon

https://indac.org/blog/the-grinch-official-trailer-3/

https://blogvaronis2.wpengine.com/wp-content/uploads/2019/09/ddos-attack-hero-1200x401.png

Hmm. We're having trouble finding that site.

We can't connect to the server at www.amazon.com.

If that address is correct, here are three other things you can try:

- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

Try Again

The Internet suffers

DDoS

The problem!

Blackholing

The solution?

Common belief

Blackholing is an effective measure to mitigate DDoS

Common (mis) belief

?

Blackholing is an effective measure

to mitigate DDoS

?

Our results. In a nutshell.

Efficiency

Blackholing drops only **50% of unwanted traffic.**

Fine-grained blacklisting of attack signatures is an effective mitigation strategy.

Use Cases

Only **27% of Blackhole Events correlate with DDoS**.

Other use cases exist for Blackholing but are very rare.

Agenda

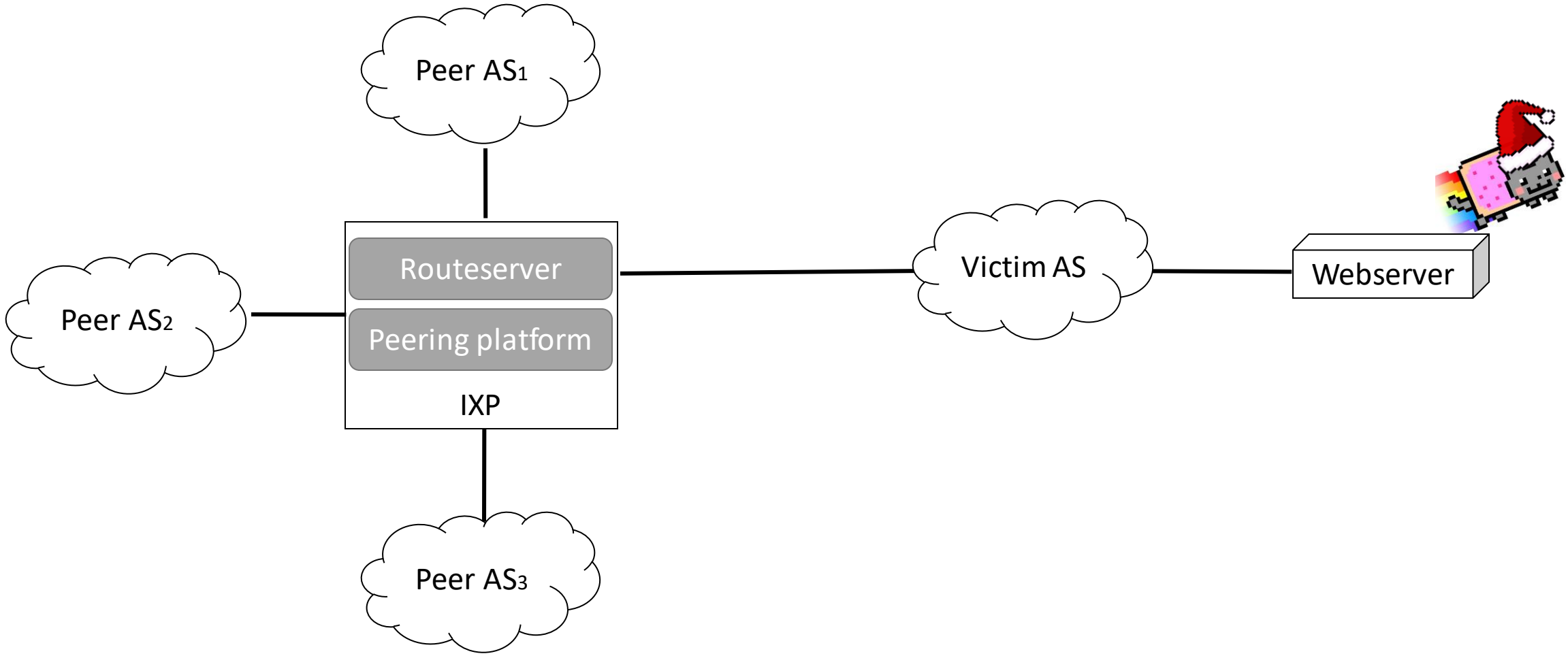
I. Background
How does BGP Blackholing work at IXPs?

II. Deployment Status
How well deployed is Blackholing in the real world?

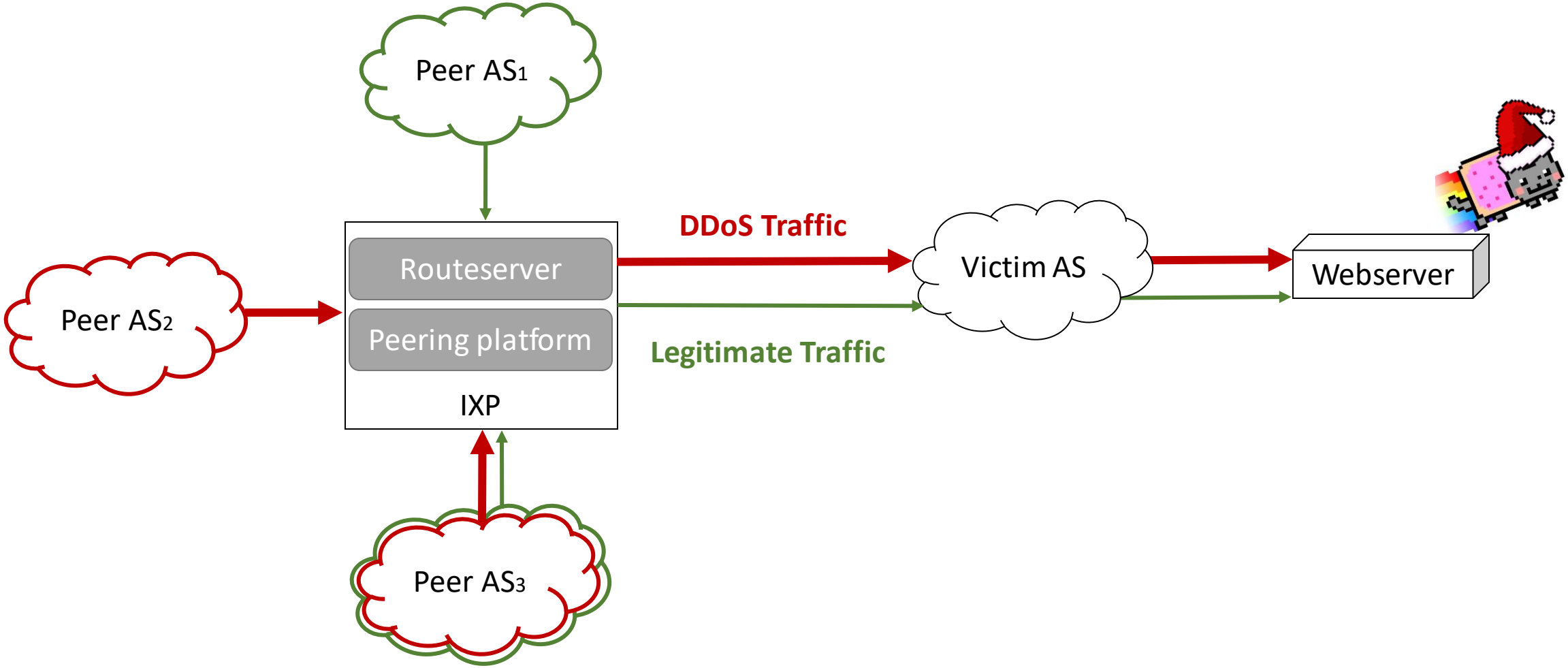
III. Future Enhancements
How should we configure fine-grained filtering?

I. How does BGP Blackholing work at IXPs?

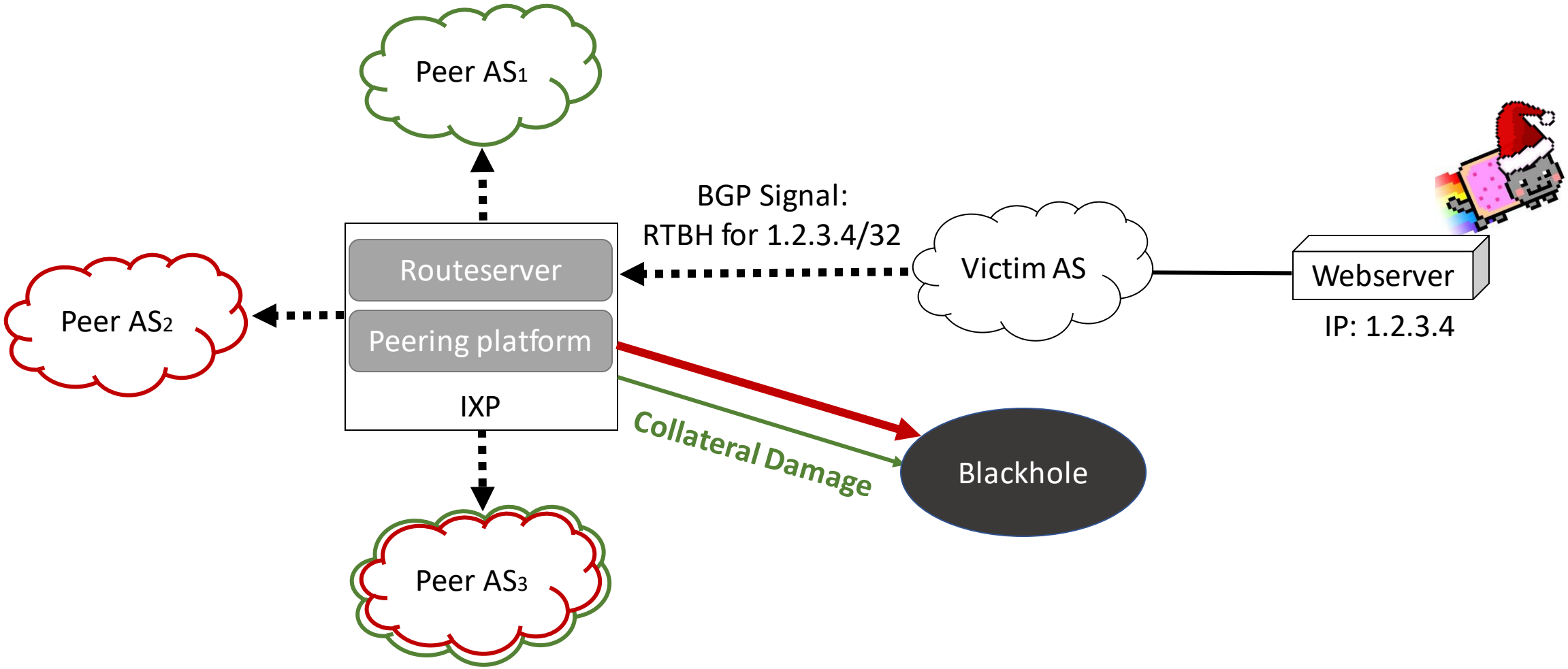
Remotely-Triggered Blackholing at IXPs



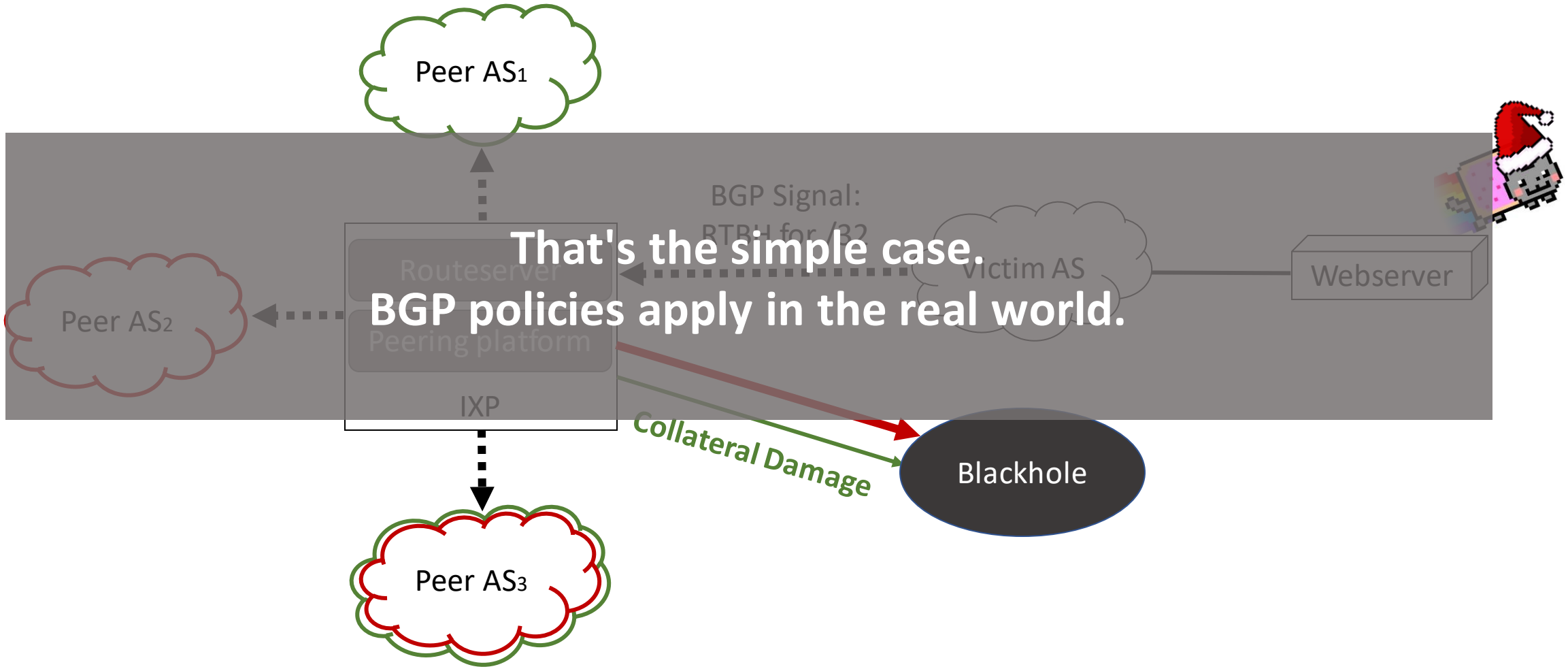
Remotely-Triggered Blackholing at IXPs



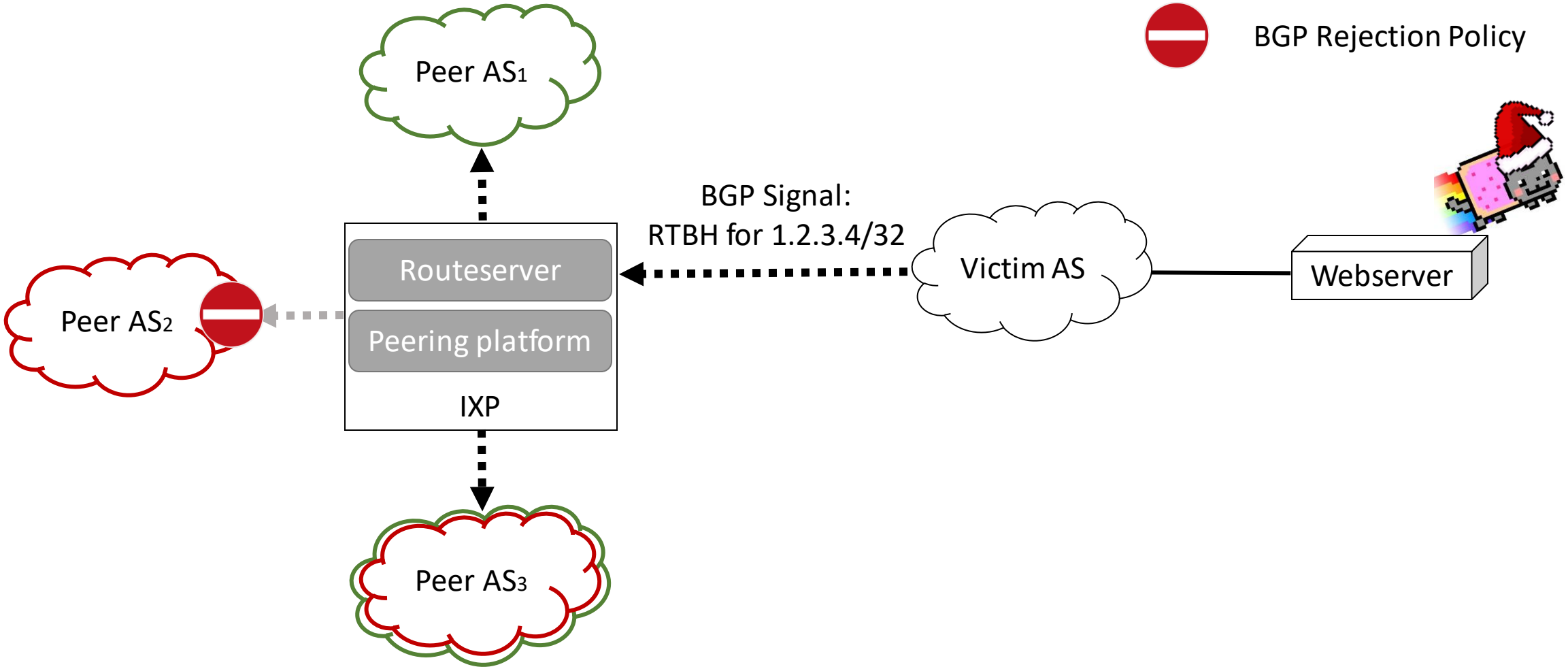
Remotely-Triggered Blackholing at IXPs



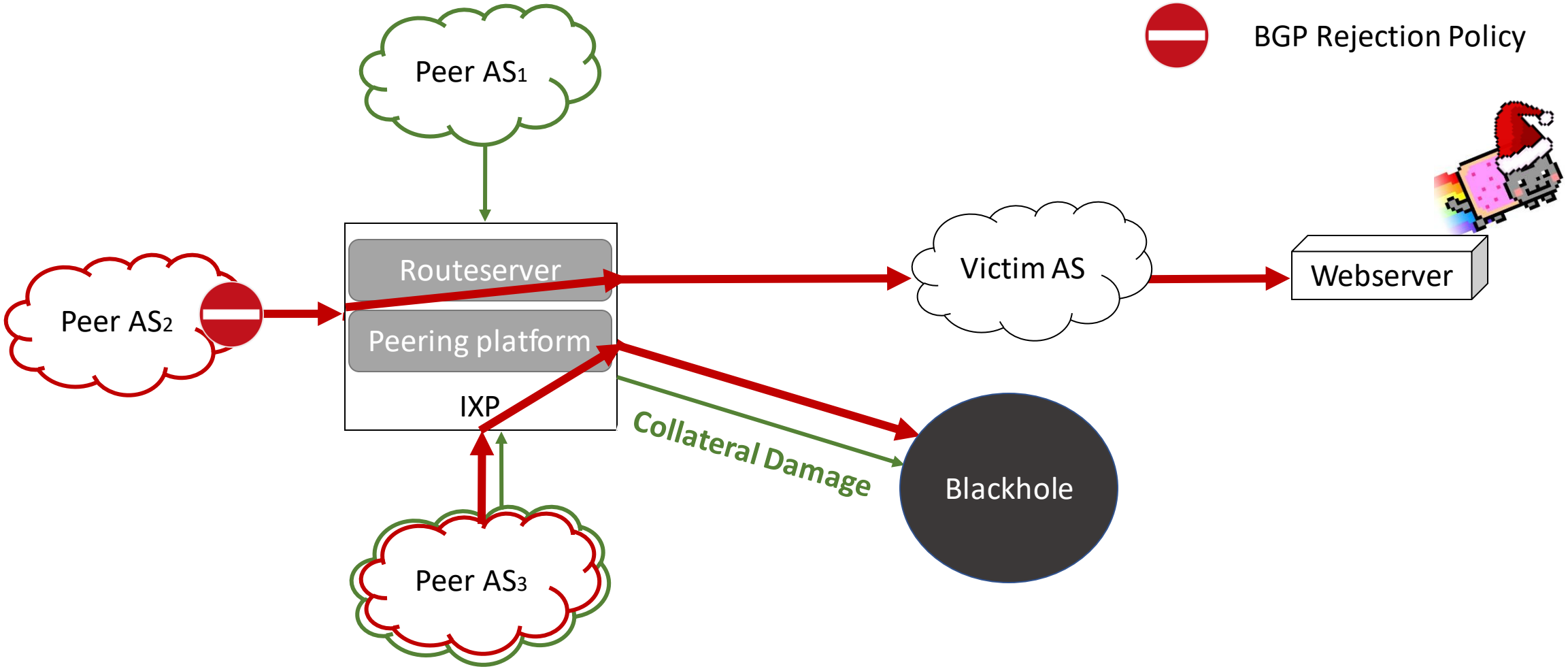
Remotely-Triggered Blackholing at IXPs



Remotely-Triggered Blackholing and BGP Policies



Remotely-Triggered Blackholing and BGP Policies



https://unternehmensberatungralfmueller.wordpress.com/2011/12/15/weihnachten-einfach-weihnachten/

II. How well deployed is BGP Blackholing in the real world?

Our measurement approach

One of the worlds-largest IXPs as a central vantage point

Wholistic view: >100 days, all related data - **no exceptions!**

Our measurement approach

One of the worlds-largest IXPs as a central vantage point

Wholistic view: >100 days, all related data - **no exceptions!**

BGP data

- All RTBH messages from all route-servers
- RTBH announcements identifiable by BGP community and next-hop-IP

BGP Signal:
RTBH for 1.2.3.4/32

Our measurement approach

One of the worlds-largest IXPs as a central vantage point

Wholistic view: >100 days, all related data - **no exceptions!**

Flow data

- All packets from/to prefixes, which have been blackholed at least once
- All packets which traverse the public switch-fabric (Sampling: 1/10000)
- *Dropped* packets identifiable by special MAC-address

Our measurement approach

One of the worlds-largest IXPs as a central vantage point

Wholistic view: >100 days, all related data - **no exceptions!**

BGP data

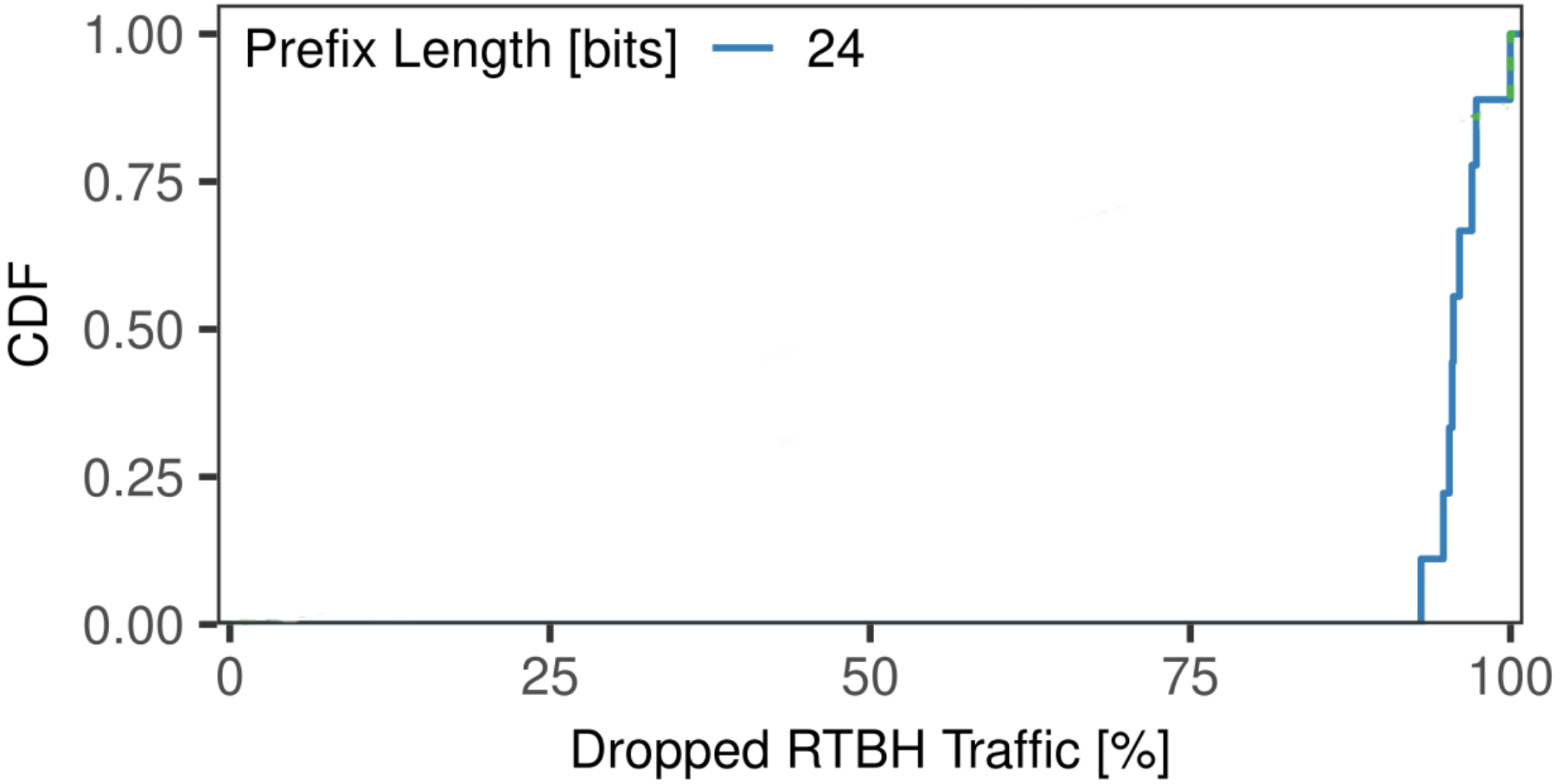
- All RTBH messages from all route-servers
- RTBH announcements identifiable by BGP community and next-hop-IP

Flow data

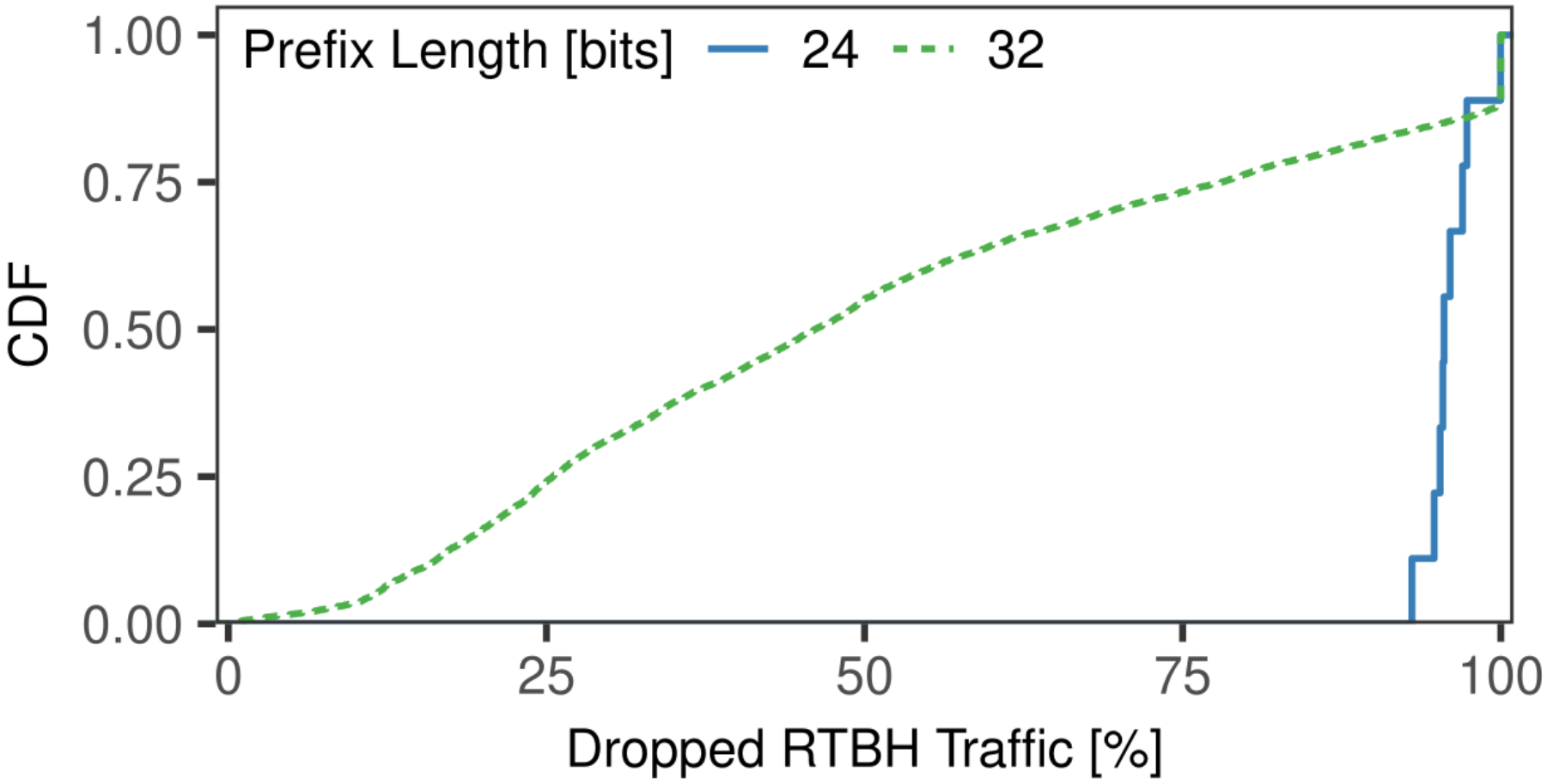
- All packets from/to prefixes, which have been blackholed at least once
- All packets which traverse the public switch-fabric (Sampling: 1/10000)
- *Dropped* packets identifiable by special MAC-address

Do all IXP member accept RTBH announcements ?

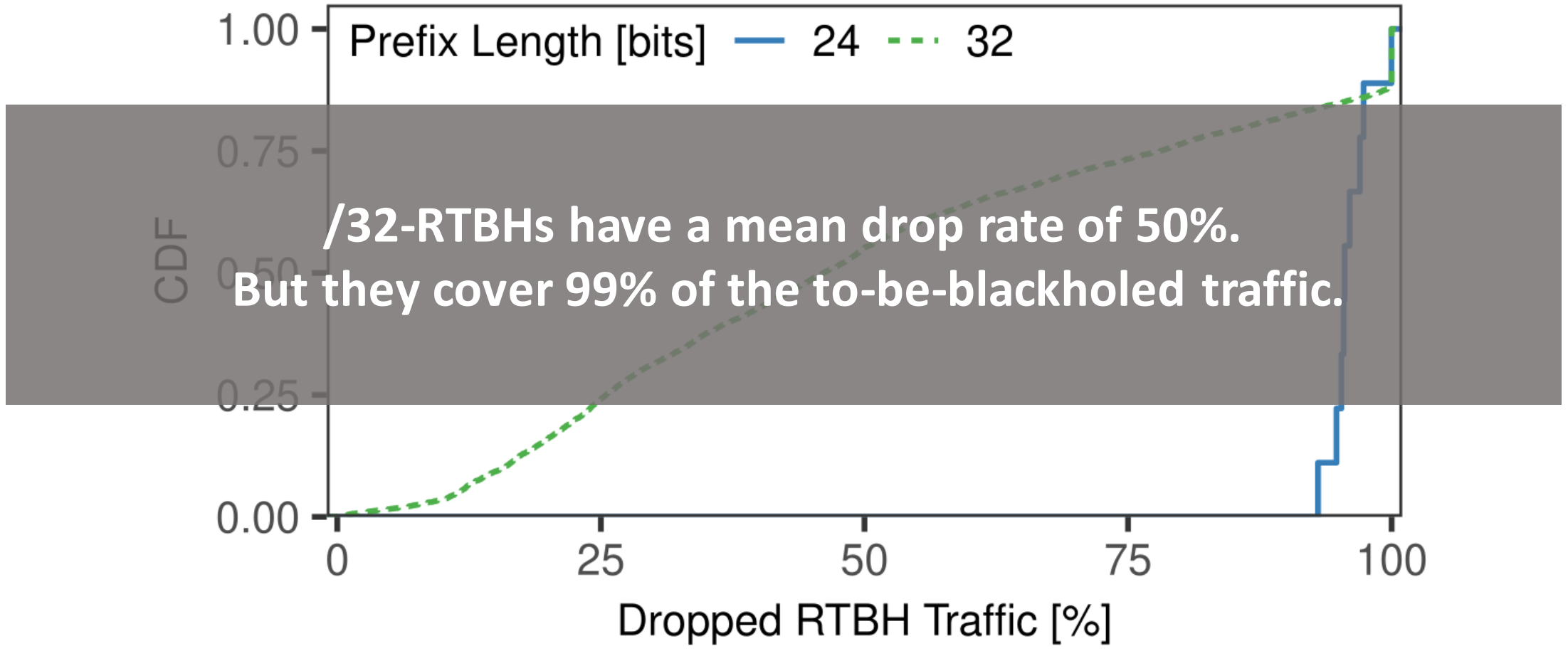
Successful mitigation depends on the announced RTBH prefix length



Successful mitigation depends on the announced RTBH prefix length

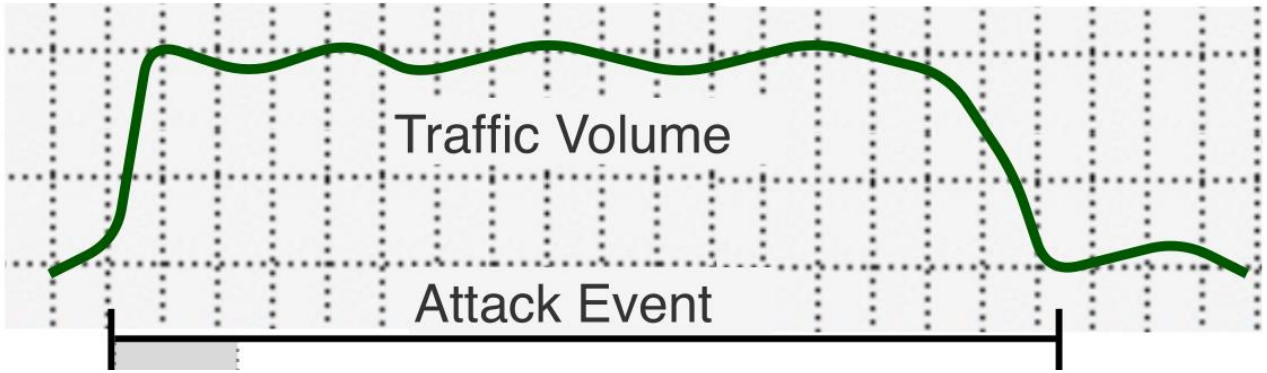


Successful mitigation depends on the announced RTBH prefix length



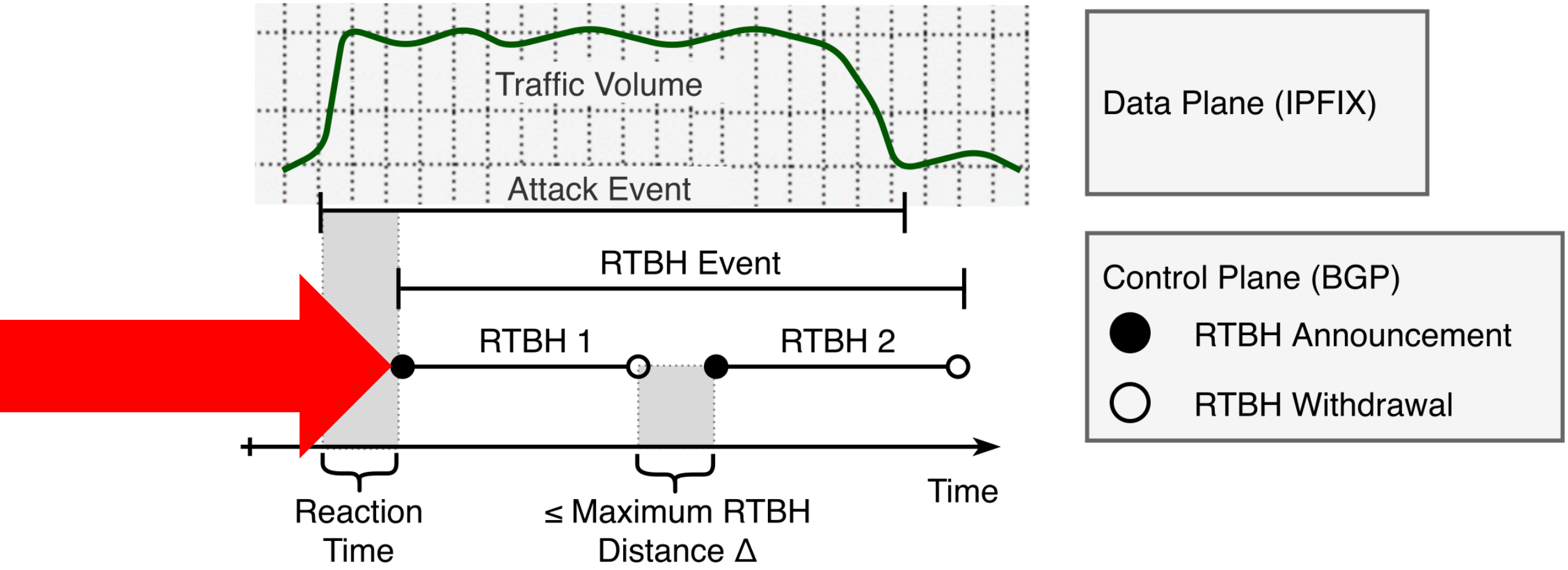
How fast do IXP members react to DDoS events?

Measurement challenge
Multiple RTBHs cover the same attack

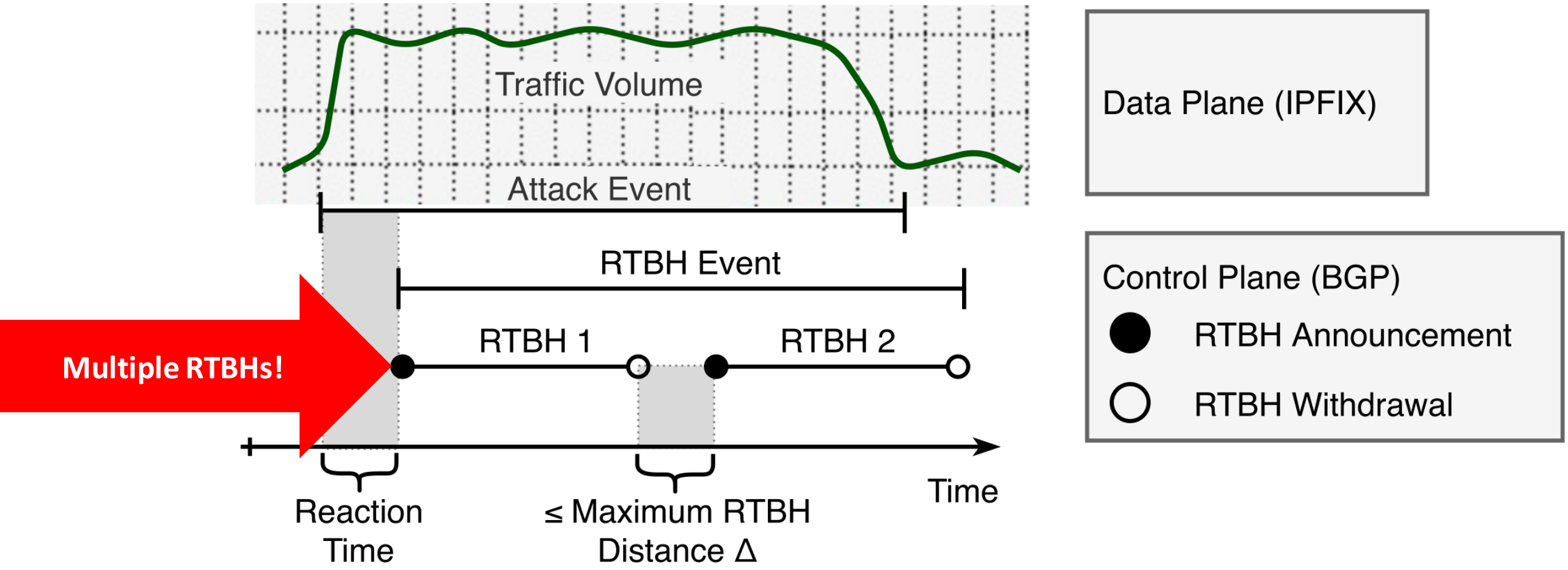


Data Plane (IPFIX)

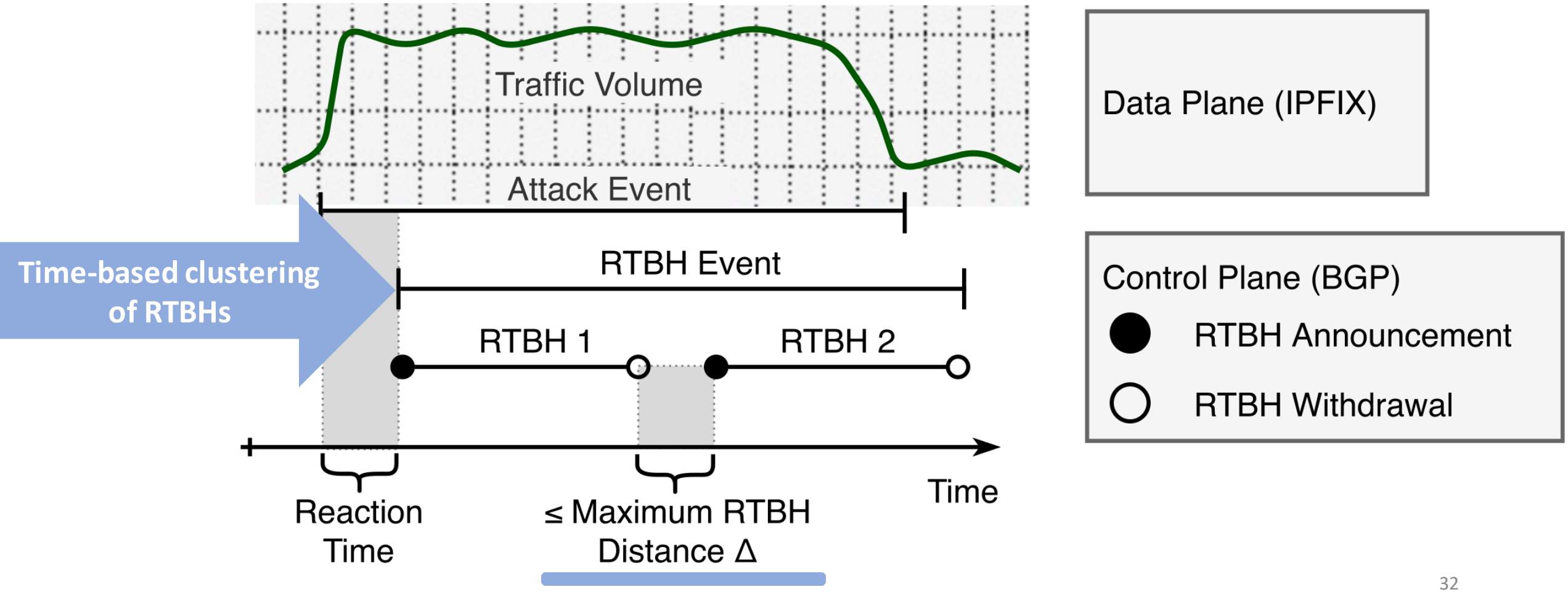
Measurement challenge
Multiple RTBHs cover the same attack



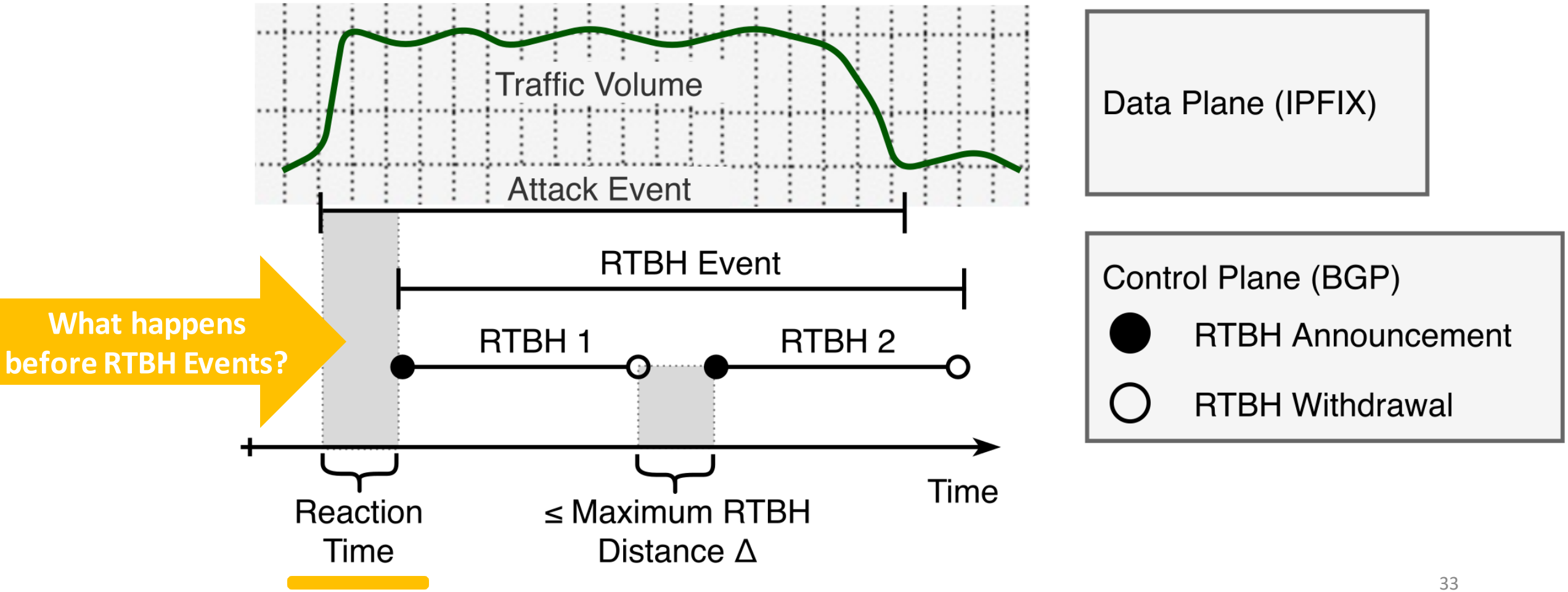
Measurement challenge
Multiple RTBHs cover the same attack



Measurement challenge
Multiple RTBHs cover the same attack



Measurement challenge
Multiple RTBHs cover the same attack



Analysis of 72 hours before an RTBH Event

Use a sliding window algorithm (EWMA) to infer whether one of the **monitored features** exhibits an anomalous peak:

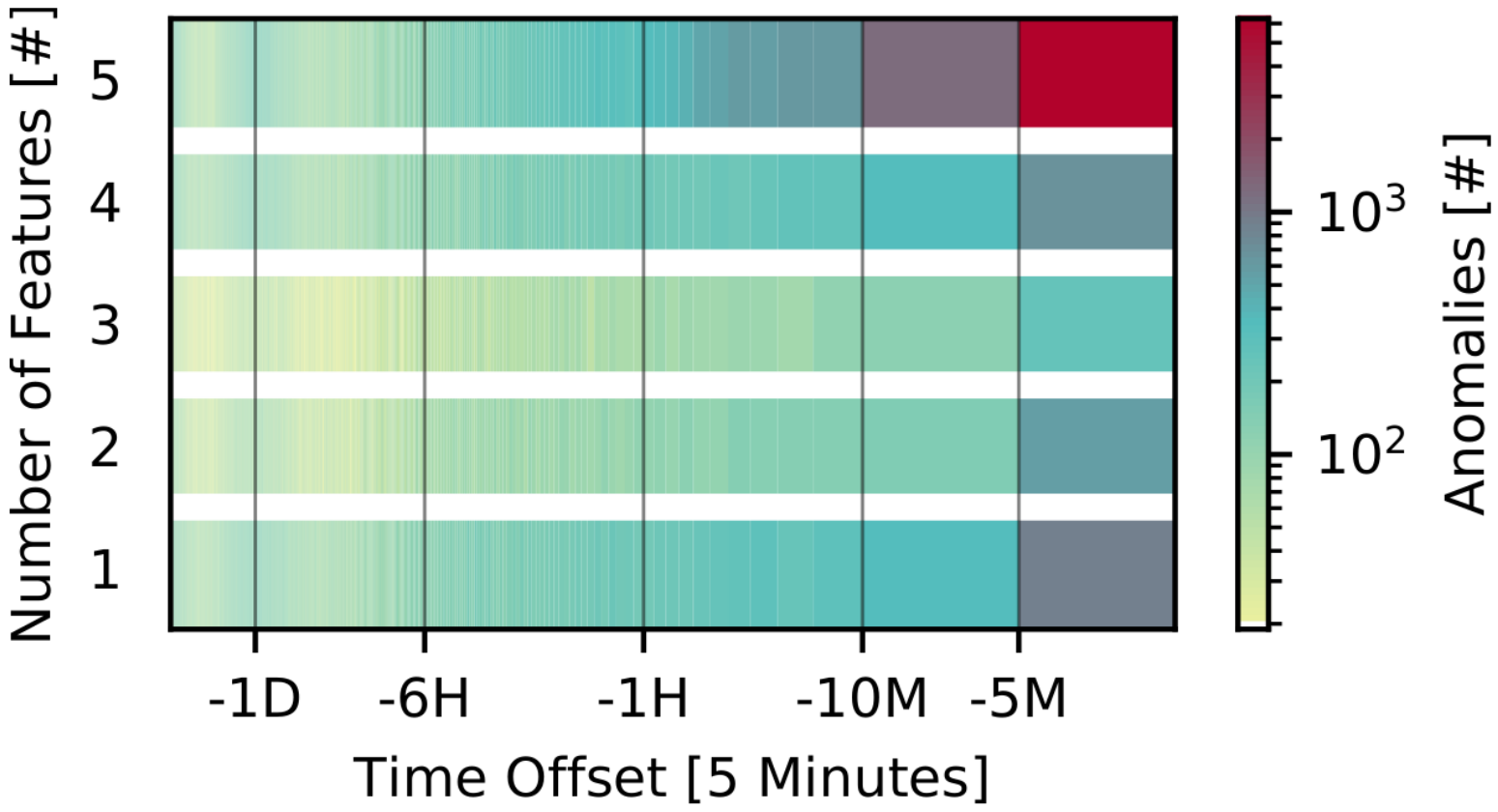
i. number of packets
ii. number of unique destination ports
iii. number of flows
iv. number of unique source IP addresses
v. number of non-TCP flows

Analysis of 72 hours before an RTBH Event

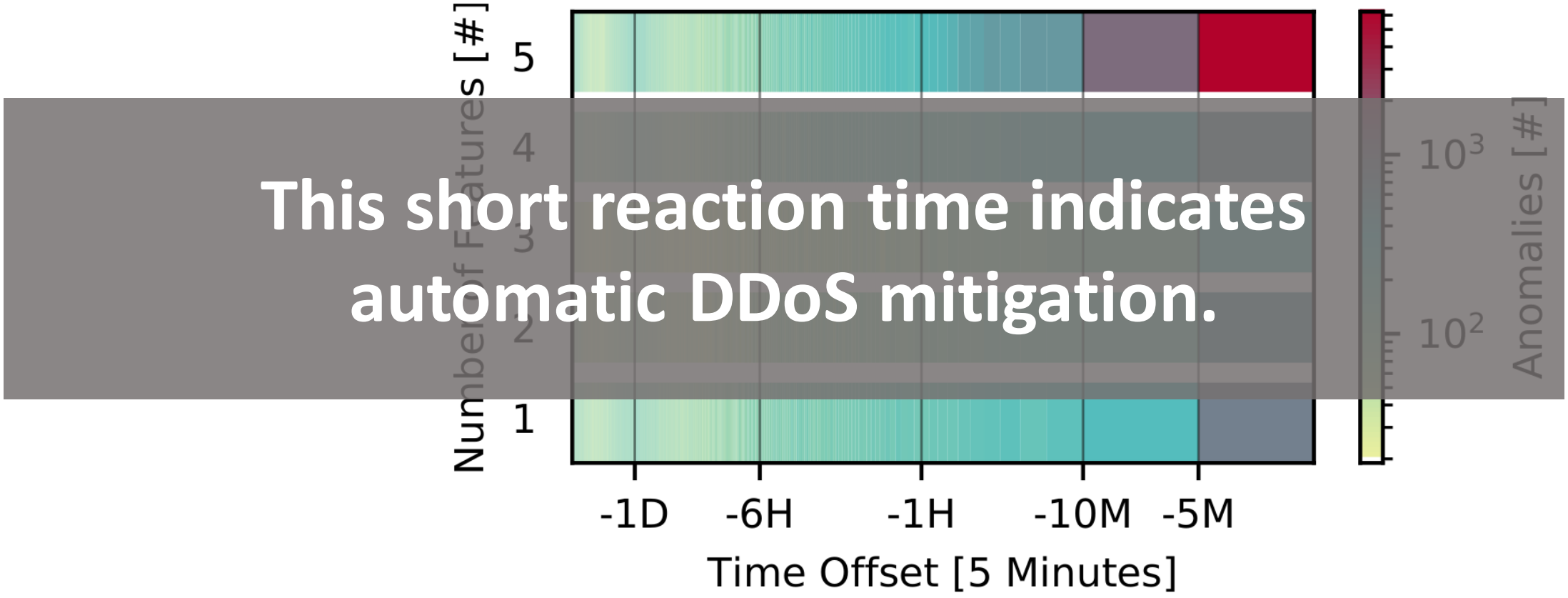
Use a sliding window algorithm (EWMA) to infer whether one of the **monitored features** exhibits an anomalous peak:

Amplification Attacks	i. number of packets
	ii. number of unique destination ports
TCP SYN Attacks	iii. number of flows
	iv. number of unique source IP addresses
GRE Floods	v. number of non-TCP flows

Most anomalies occur up to 10 minutes before an RTBH Event



Most anomalies occur up to 10 minutes before an RTBH Event



This short reaction time indicates automatic DDoS mitigation.

But: Anomalies before RTBH are uncommon!

Traffic ≤ 72 hours	Anomaly ≤ 10 min	% RTBH Events
✓	✓	27%
✓	X	27%
X	-	46%

WHY?

Other use-cases?

Prefix Squatting Protection

Prevent hijacking of address space that is assigned but not announced.

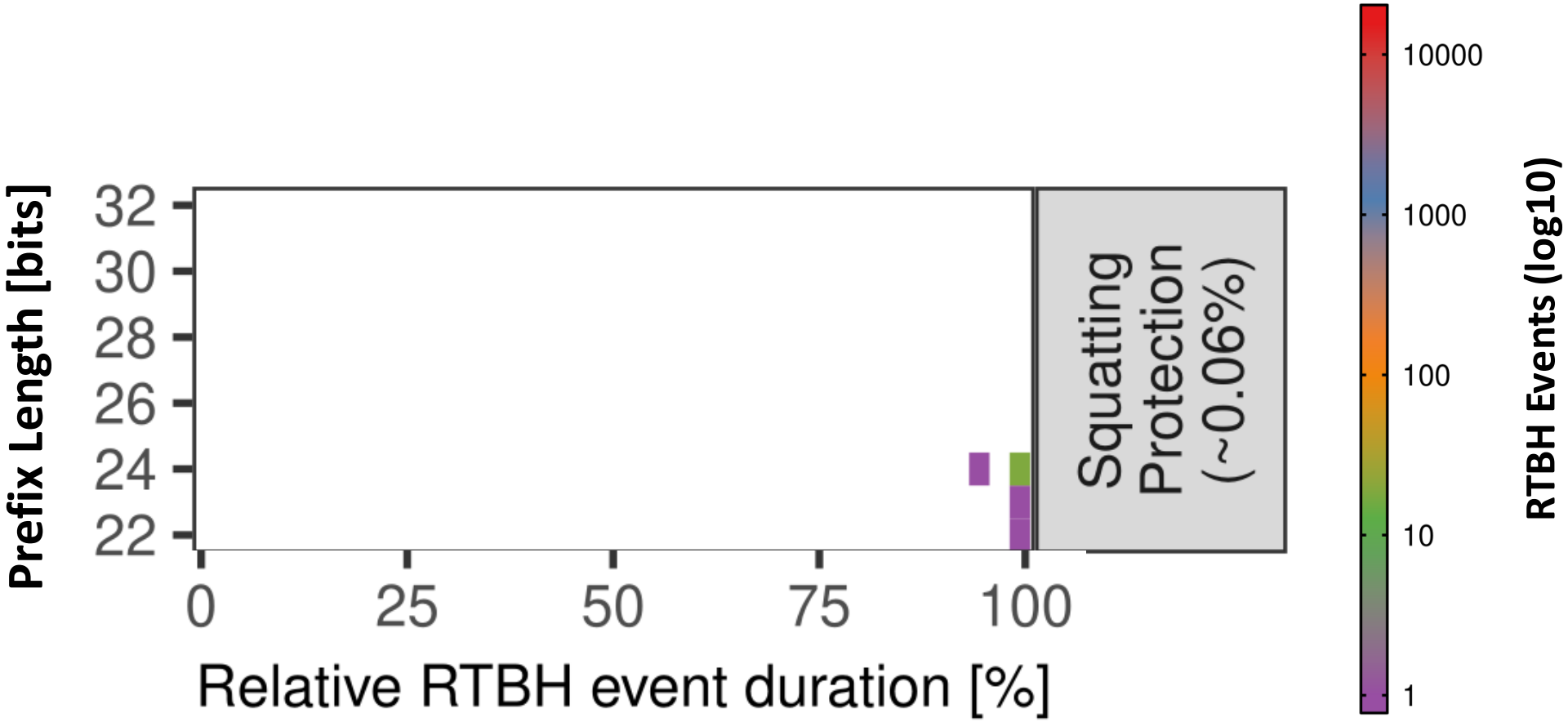
Prefix squatting is easy to deploy because there is no competitive announcement.

Content Blocking

Deploy censorship by blackholing traffic to content servers.

Block malicious clients, e.g., port & vulnerability scanners.

Prefix Squatting Protection



Other use-cases?

Prefix Squatting Protection

Prevent hijacking of address space that is assigned but not announced.

Prefix squatting is easy to deploy because there is no competitive announcement.

Content Blocking

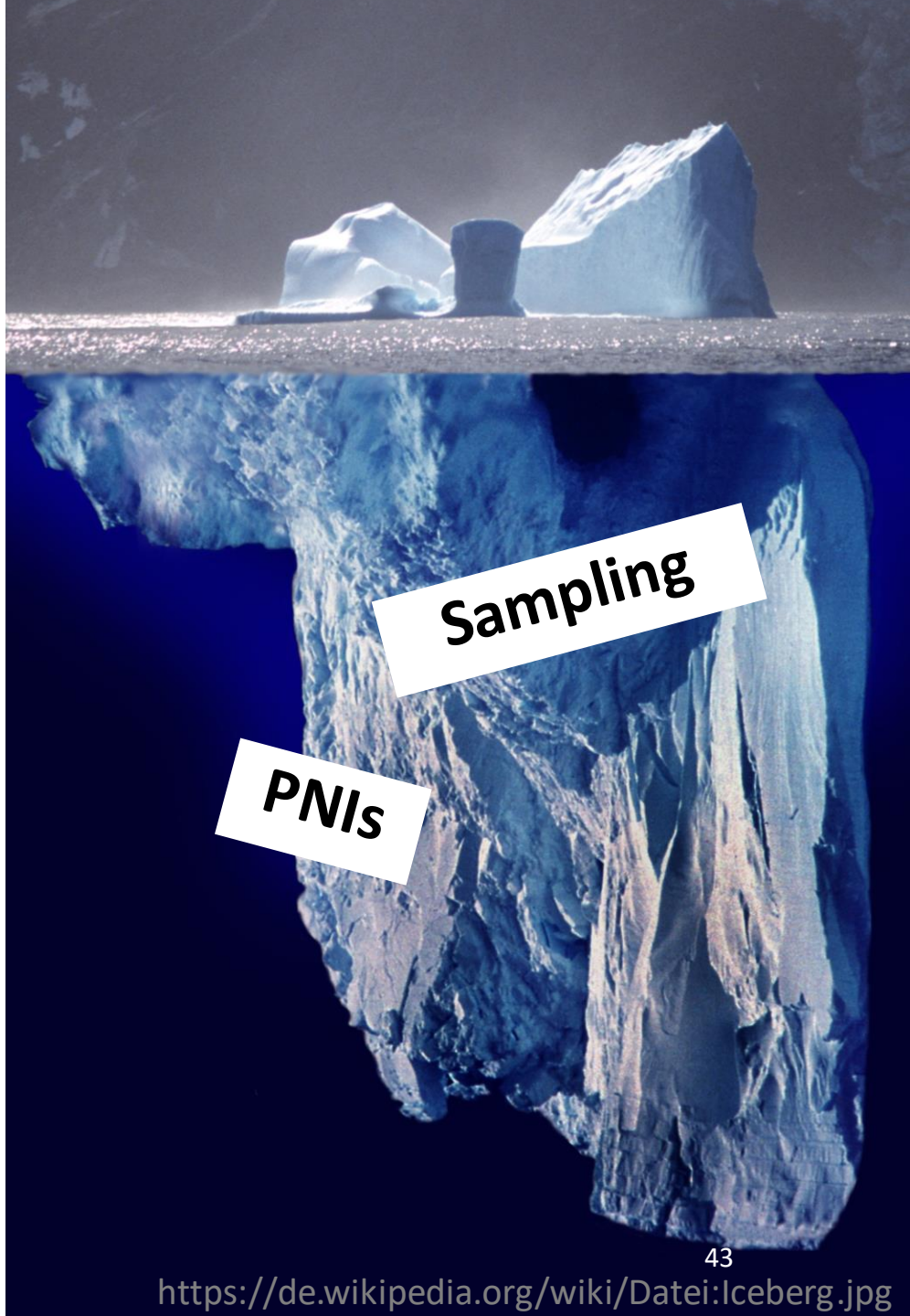
Mitigate attacks by blackholing traffic to content servers.

Block malicious clients, e.g., port & vulnerability scanners.

New use-cases are infrequent.
70% of RTBH Events still inexplicable.

Vantage point bias?

1. Packet sampling and private-network-interconnections hide traffic.

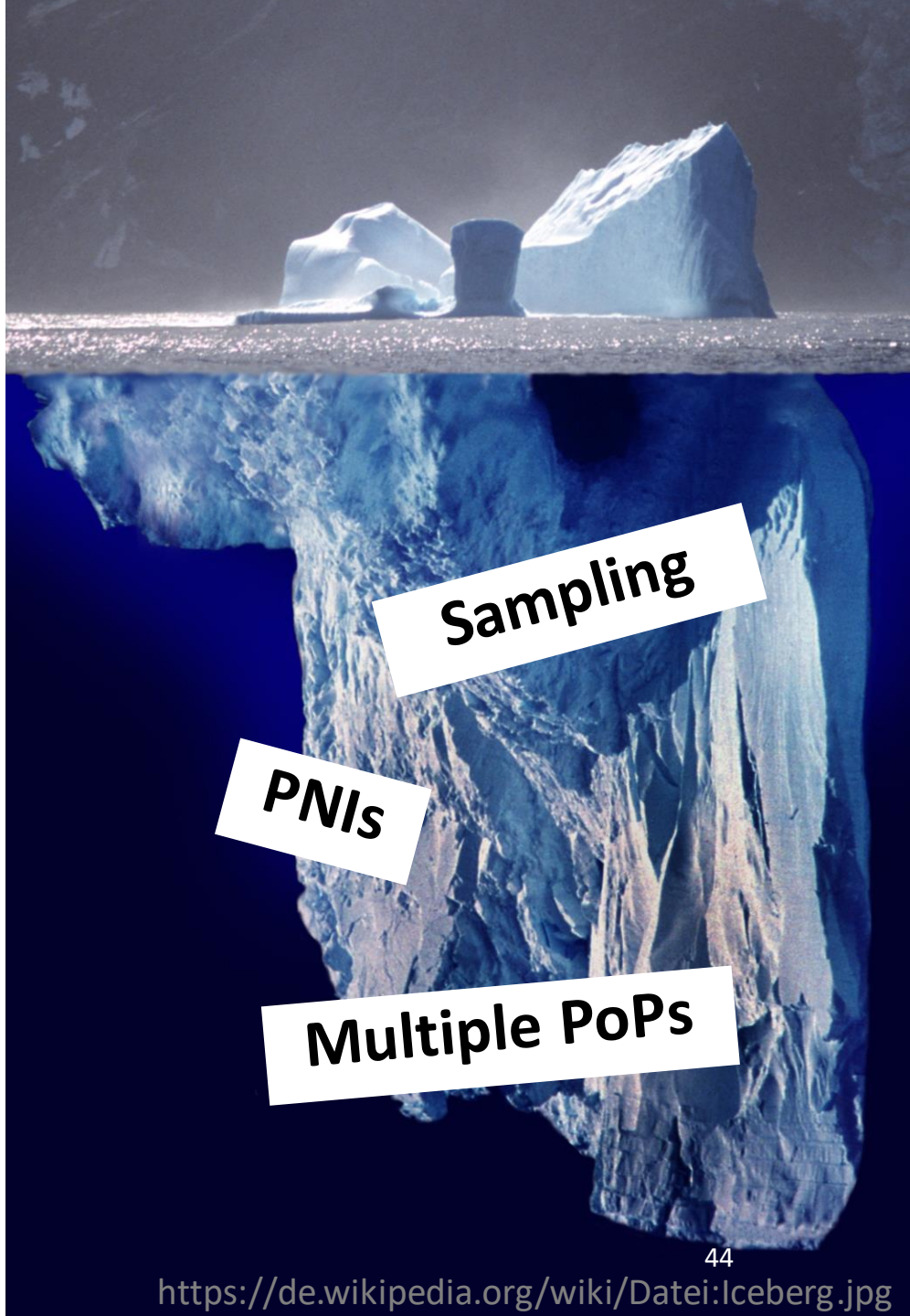


https://de.wikipedia.org/wiki/Datei:Iceberg.jpg

Vantage point bias?

1. Packet sampling and private-network-interconnections hide traffic.

2. ASes might announce RTBHs at all point-of-presence despite local attacks.



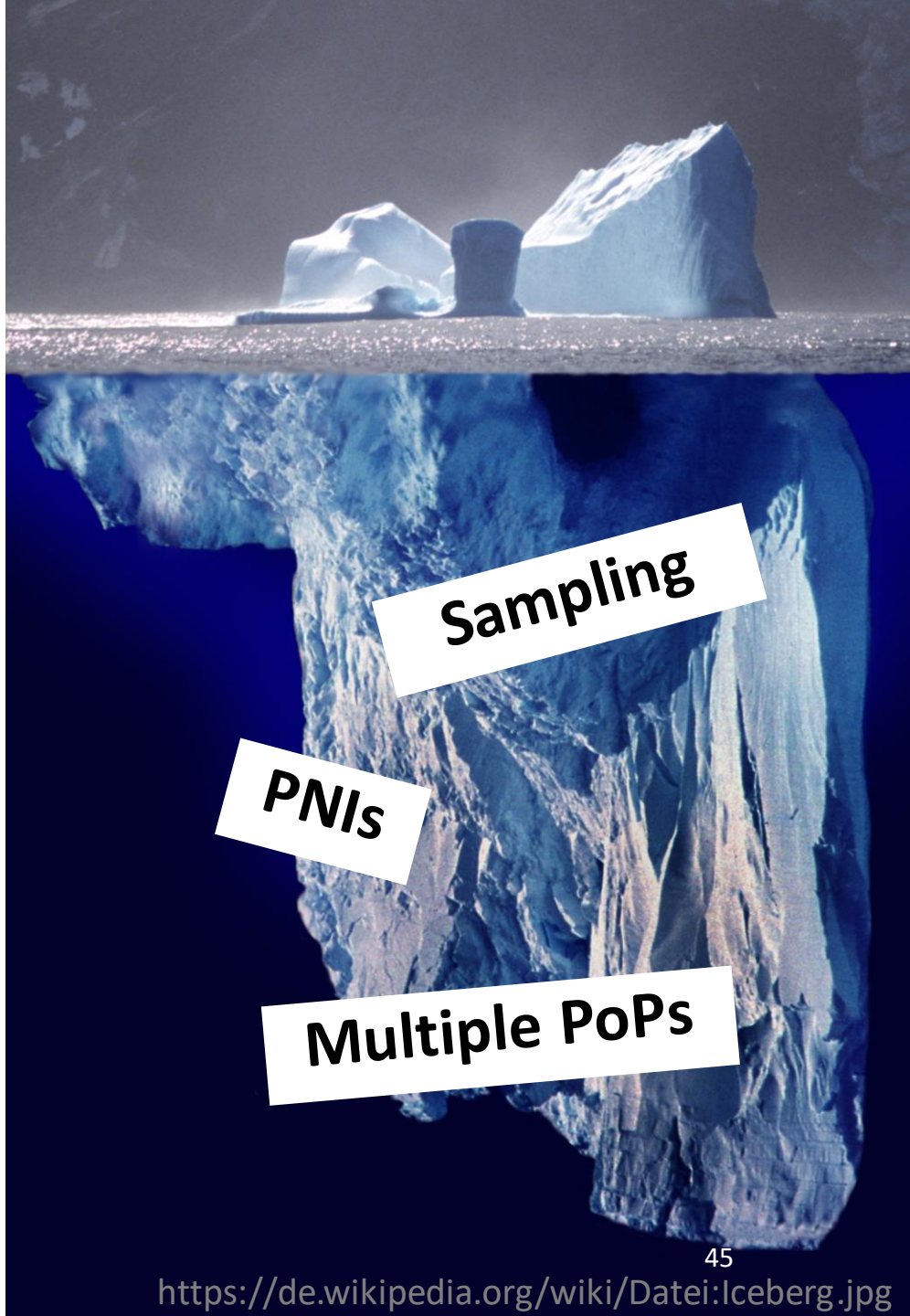
https://de.wikipedia.org/wiki/Datei:Iceberg.jpg

Vantage point bias?

1. Packet sampling and private-network-interconnections hide traffic.

2. ASes might announce RTBHs at all point-of-presence despite local attacks.

But: Related work [IMC'18] using **distributed** measurements reached similar results!



Jonker et al, A First Joint Look at DoS Attacks and BGP Blackholing, IMC 2018

https://de.wikipedia.org/wiki/Datei:Iceberg.jpg

https://community.today.com/parentingteam/post/what-are-the-best-christmas-gifts-for-kids-this-year
https://www.youtube.com/watch?v=-pH9VX324rI

III. How should we configure fine-grained filtering?

RTBH - Pro and Con

THE GOOD

RTBHs drop DDoS traffic early in the network.

THE UGLY

RTBHs complete the attack, the victim is unreachable.

RTBH - Pro and Con

THE GOOD

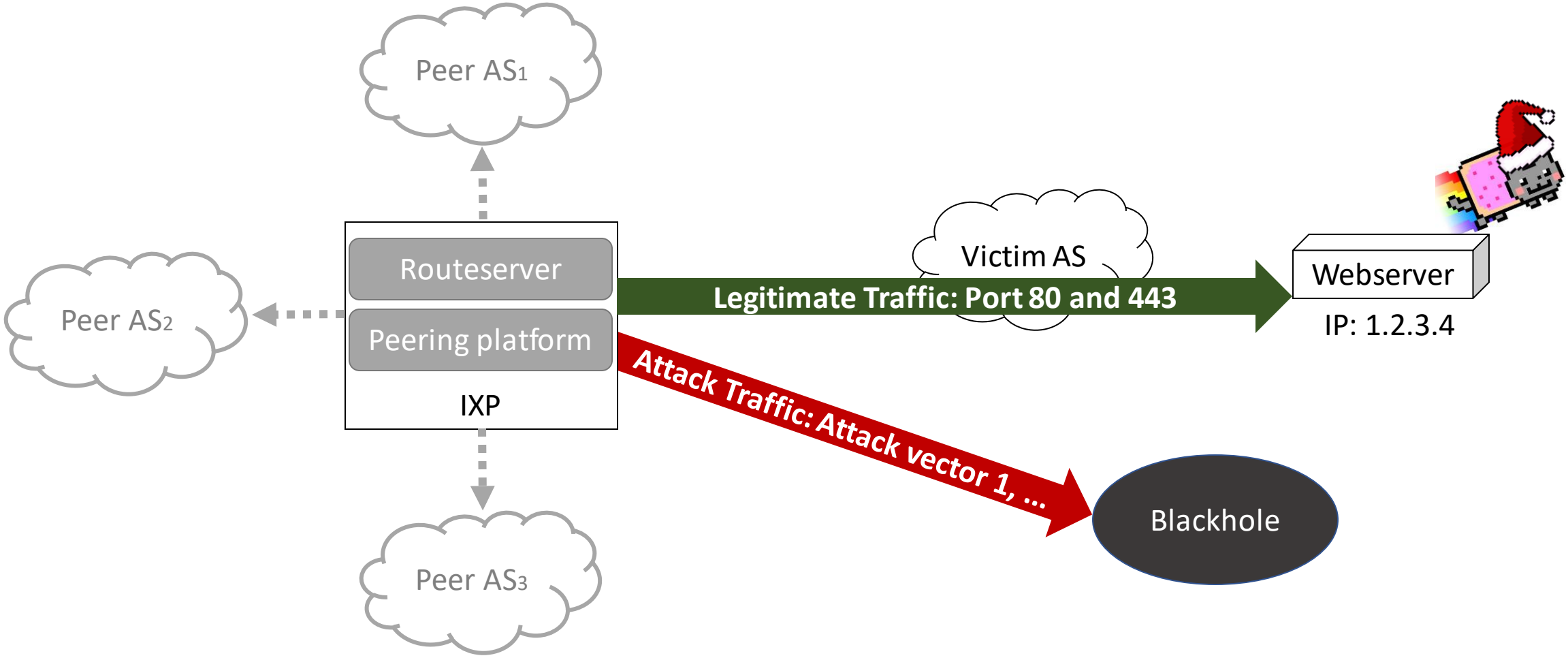
RTBHs drop DDoS traffic early in the network.

THE UGLY

RTBHs complete the attack, the victim is unreachable.

Fine-grained filtering would keep a service reachable.

Whitelisting vs. blacklisting of ports



Challenge

We cannot whitelist client traffic, because client traffic is highly variable.

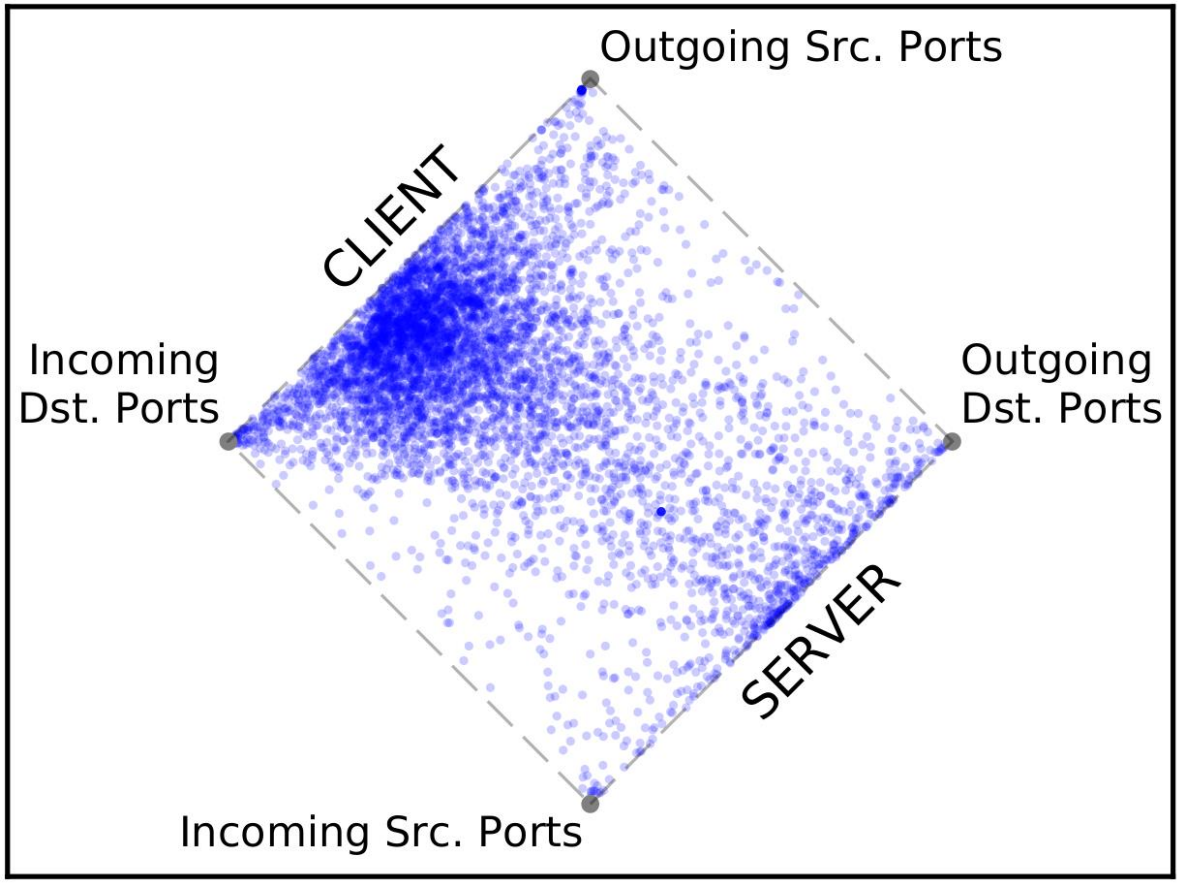
RadViz Projection

Visualizing multidimensional port information allows a classification into clients and servers

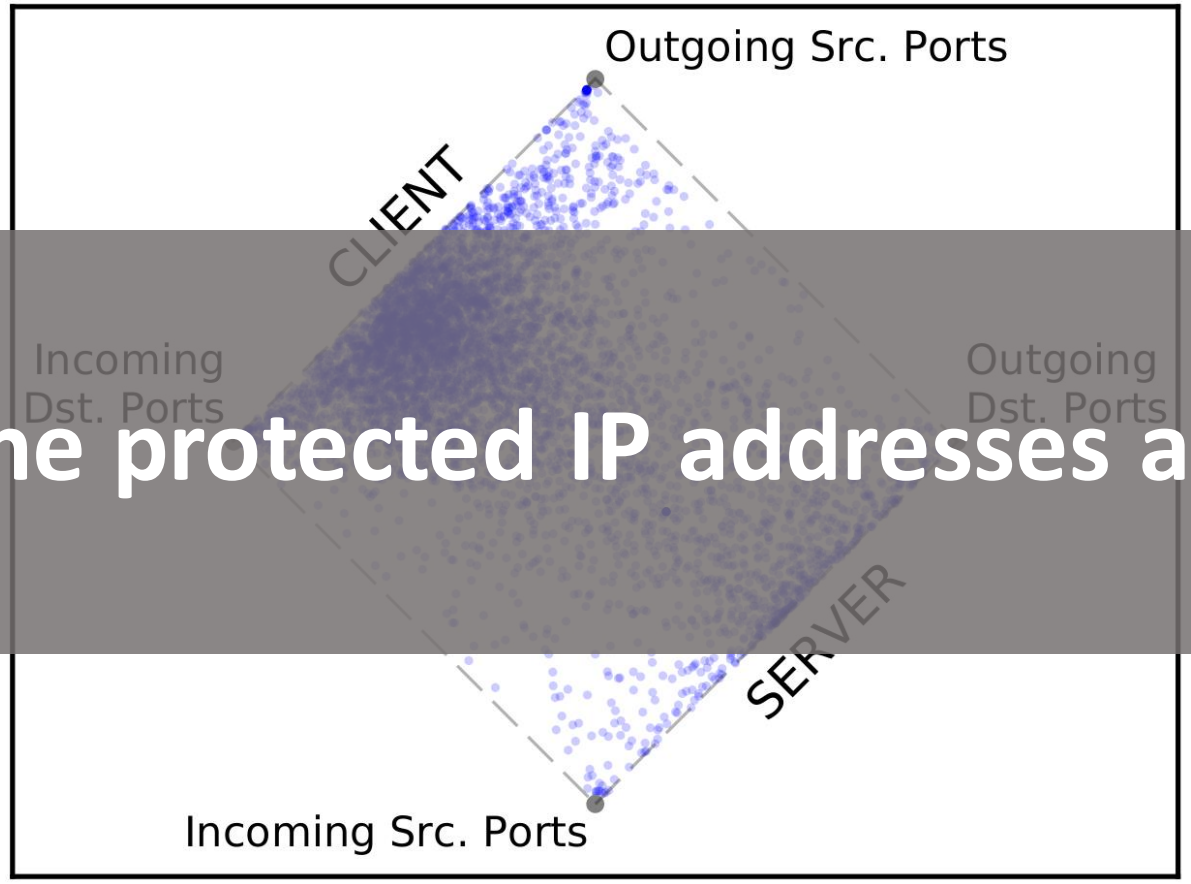
RadViz Projection

Visualizing multidimensional port information allows a classification into clients and servers

Many blackholed IP addresses exhibit high port fluctuations



Many blackholed IP addresses exhibit high port fluctuations



Most of the protected IP addresses are clients.

Cross-validation using PeeringDB

Type	Clients	Server
# Hosts	4057	1036
Content	2%	**34%**
Cable/DSL/ISP	**60%**	14%
NSP	14%	13%
Enterprise	1%	1%
Unknown	23%	38%

Cross-validation using PeeringDB

Most clients located in DSL networks.
PeeringDB supports our classification.

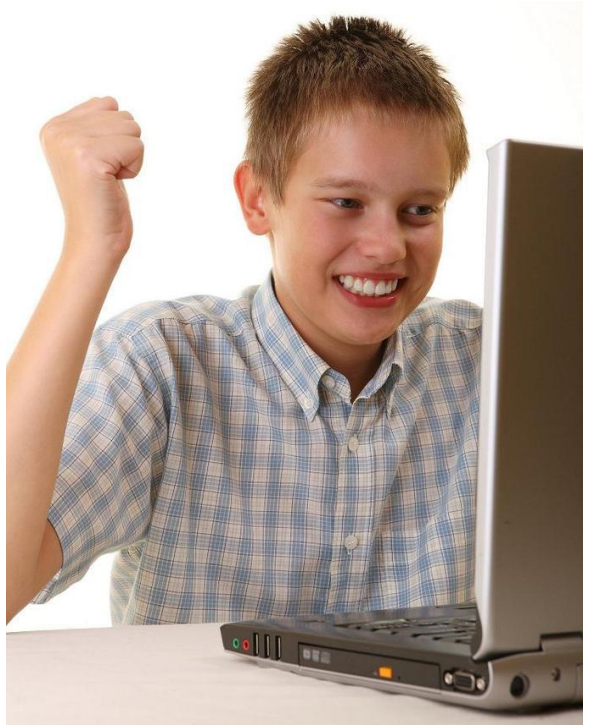
Type	Clients	Server
# Hosts	1057	1036
Content	2%	**34%**
Cable/DSL/ISP	**80%**	14%
NSP	14%	13%
Enterprise	1%	1%
Unknown	23%	38%

Esports Disputes

https://www.nytimes.com/2018/11/07/movies/the-grinch-review.html

Esports Disputes

https://www.nytimes.com/2018/11/07/movies/the-grinch-review.html



https://knowyourmeme.com/memes/first-day-on-the-internet-kid

Esports Disputes

https://www.nytimes.com/2018/11/07/movies/the-grinch-review.html

https://knowyourmeme.com/memes/first-day-on-the-internet-kid

https://blogvaronis2.wpengine.com/wp-content/uploads/2019/09/ddos-attack-hero-1200x401.png

Potentials of fine-grained whitelisting?

Clients are often affected by BGP Blackholing.

Whitelisting of regular, expected traffic patterns **is not an option**.

Can we easily improve by **blacklisting** attack traffic?

Most RTBH traffic is UDP traffic

- >90% of RTBH Events (with packets and a preceding anomaly) contain almost exclusively UDP amplification traffic

- Multi-vector attacks are common, but usually do not utilize more than three amplification vectors:

Different protocols* [#]	0	1	2	3	4	5
Events [%]	6	40	45	8.3	0.6	0.1

Fine-Grained Blacklisting

Fine-grained filtering based on source-ports is very effective and potentially saves legitimate traffic!

Filter example: CharGEN/19, DNS/53, NTP/123

http://phdcomics.com/comics/archive.php?comicid=395

Summary. Advices for operators.

1. **Check BGP policies.**
   Accept more specific prefixes, in particular /32, in case of RTBH announcements.

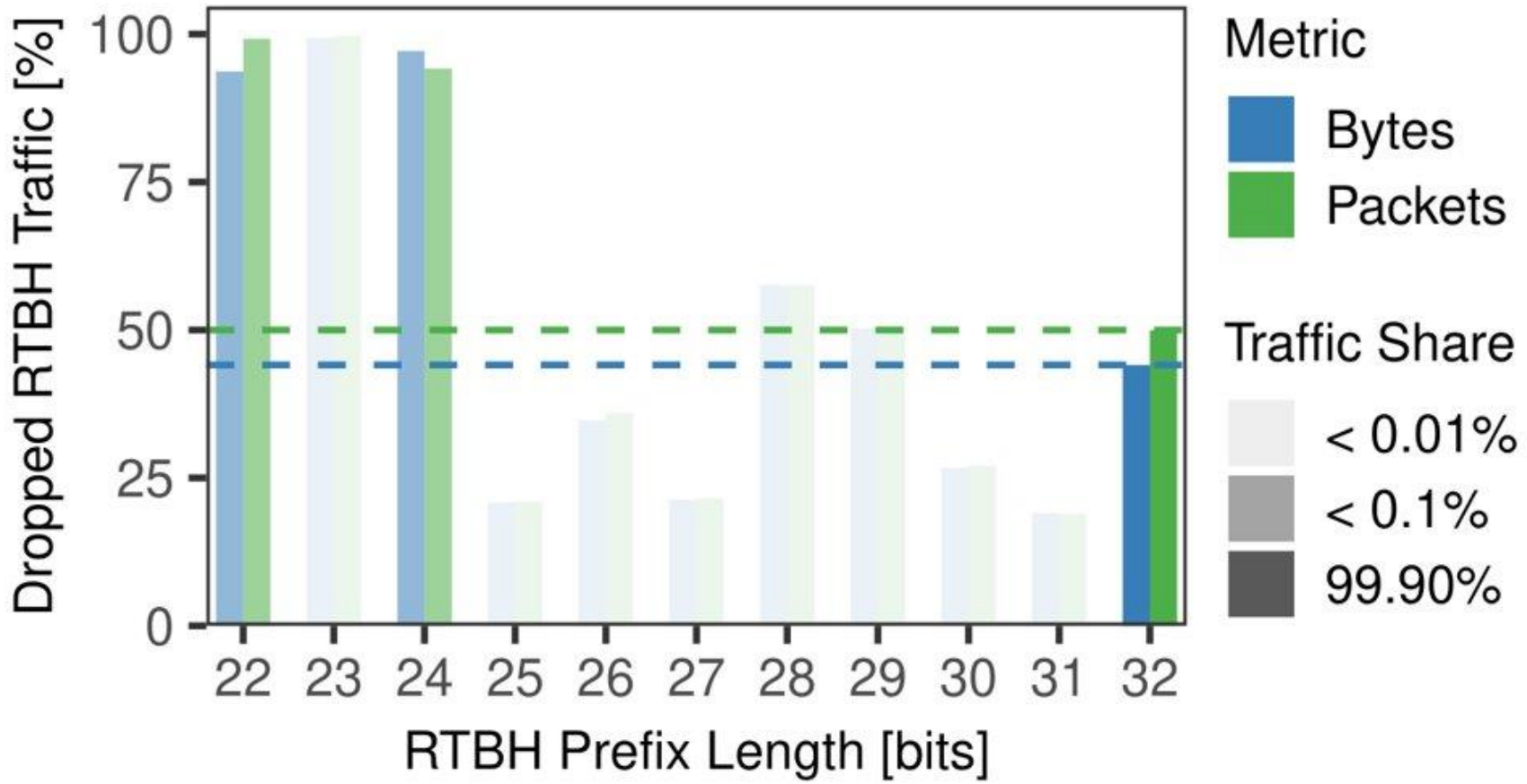
2. **Check routing tables for RTBH 'zombies'.**
   Routing tables may contain many unnecessary/inexplicable RTBH entries. Contact peers to understand the RTBH use cases.

3. **Consider fine-grained filtering.**
   Majority of DDoS attacks are still not complex. Simple port-based blacklisting (ACLs, BGP Flowspec) can be very effective.

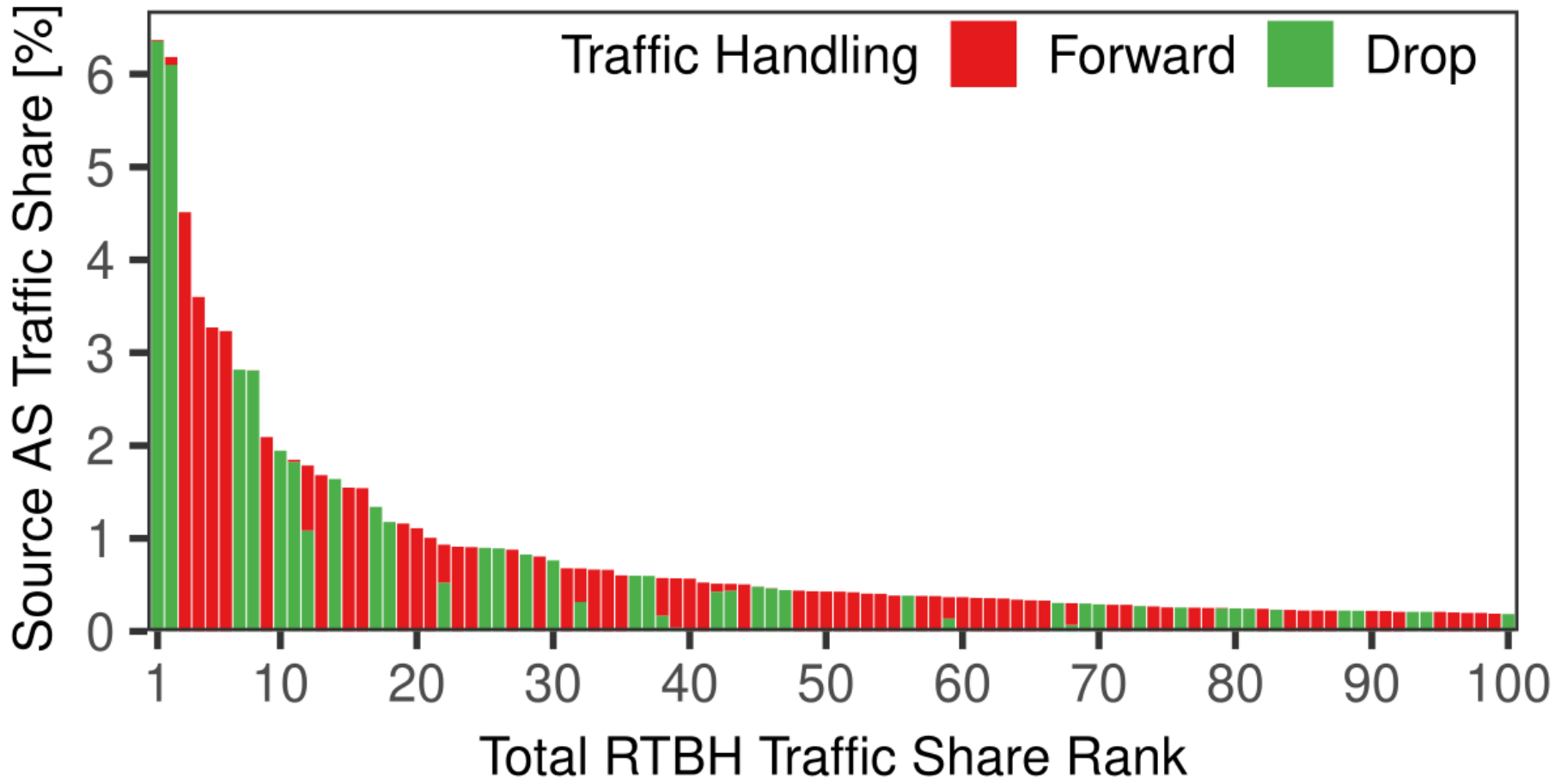

Merry
Christmas!
Pusheen.com

BACKUP SLIDES

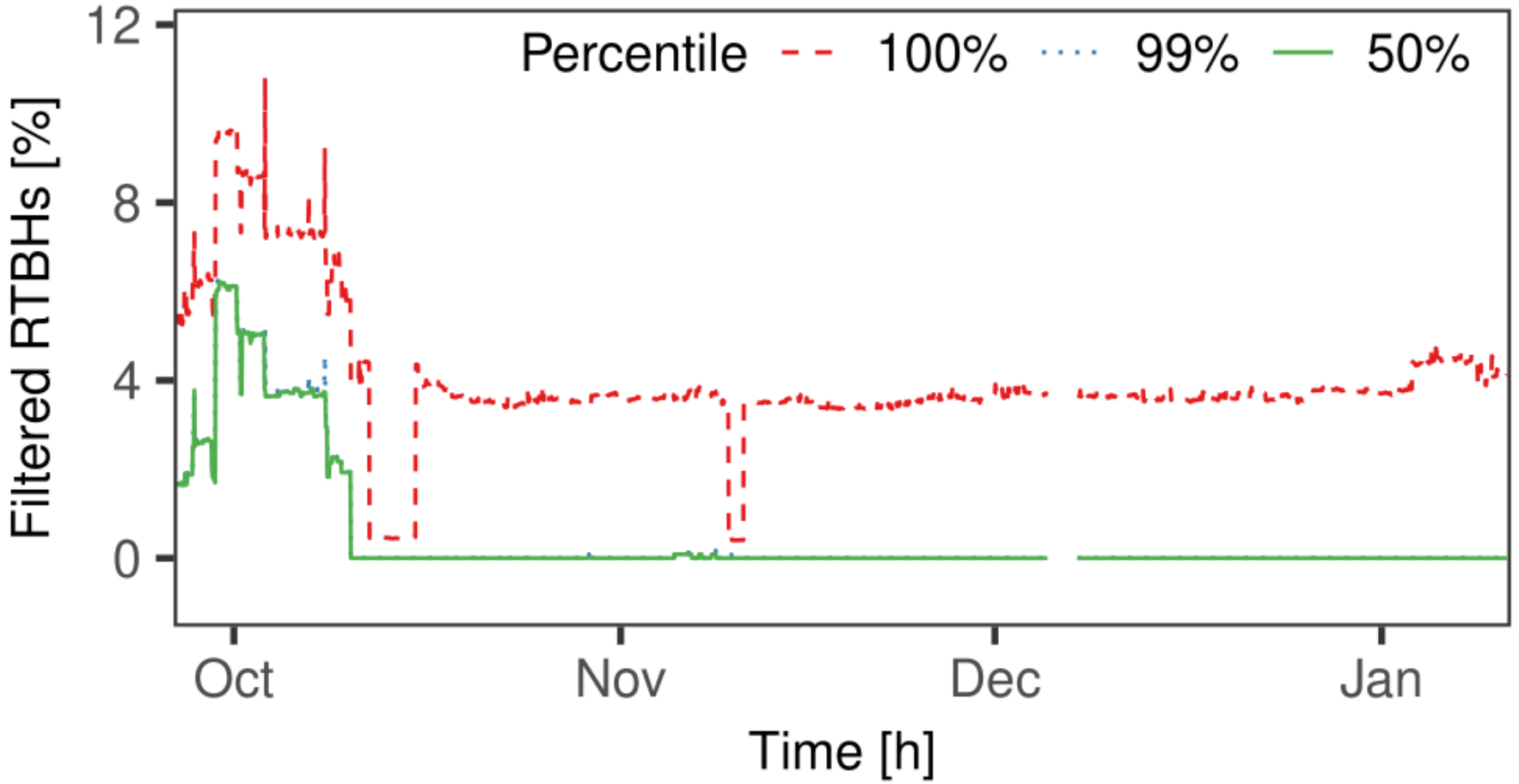
Prefix Lengths and Traffic Share



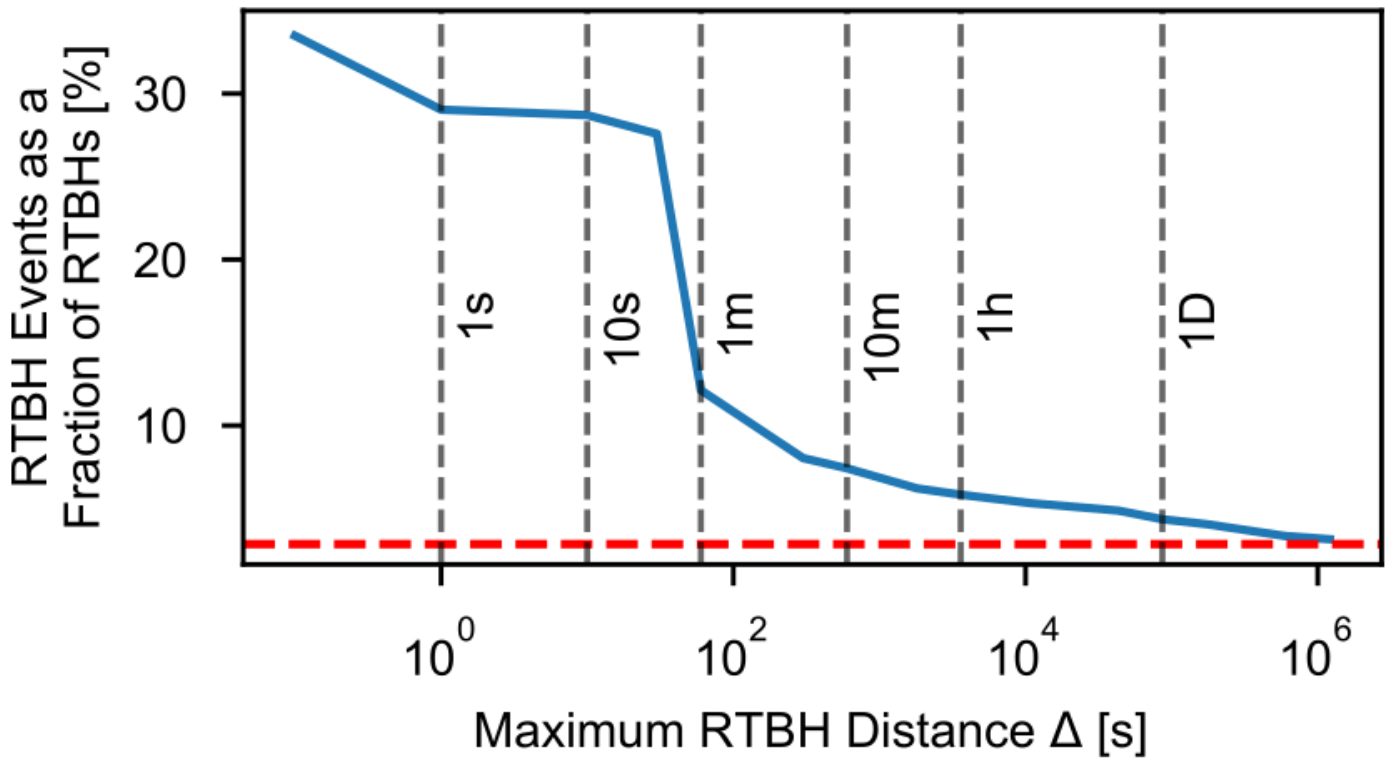
AS Drop Consistency



RTBH Propagation Filter



Maximum RTBH Distance Δ



Attack Visibility and Sampling

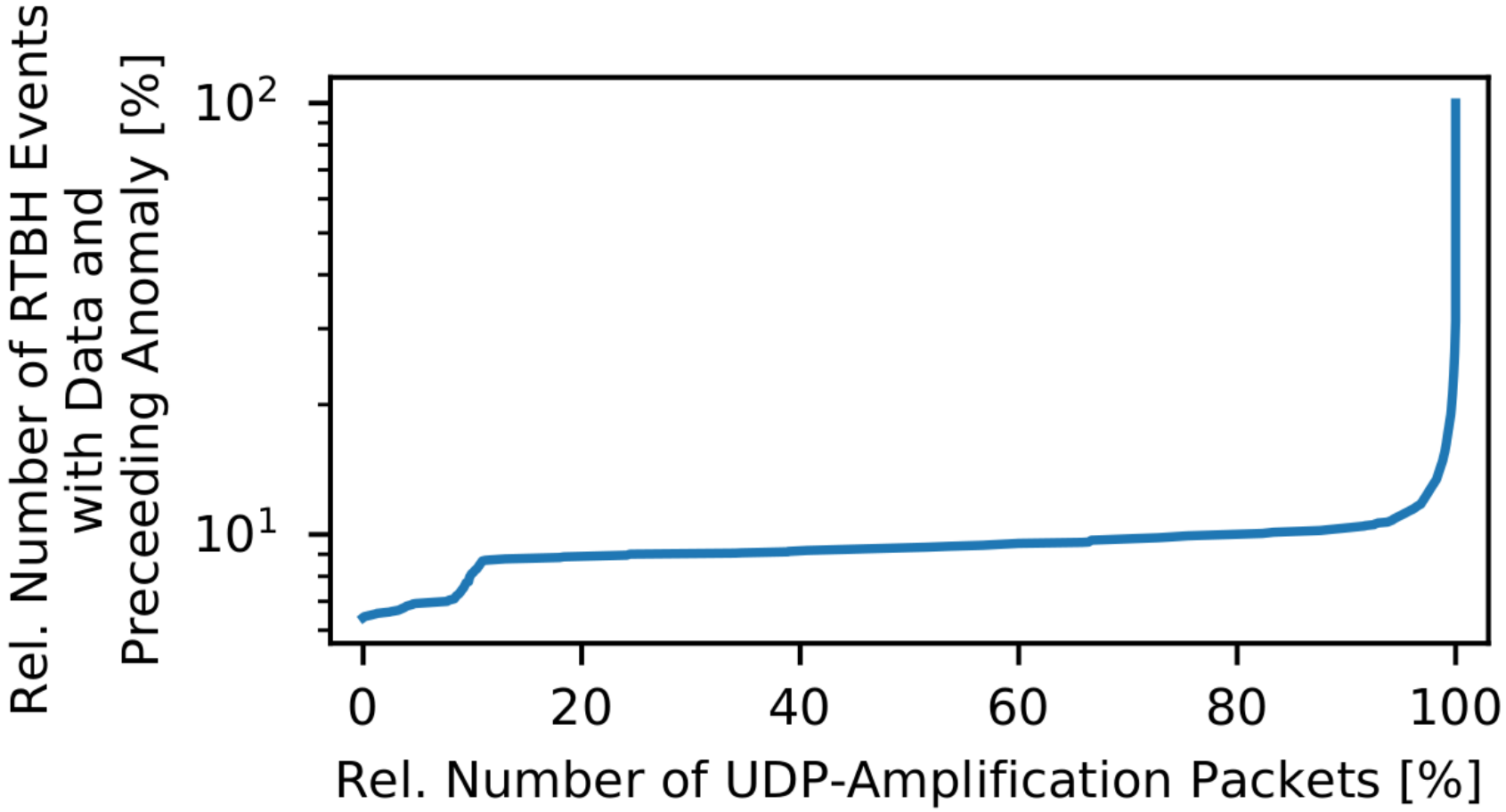
- Median DDoS attack size in mid 2018 was 1287 Mbps
- Dividing by a MTU of 1500 Bytes, this corresponds up to 100k packets per second
- We expect to observe attacks despite sampling!

List of Amplification Protocols

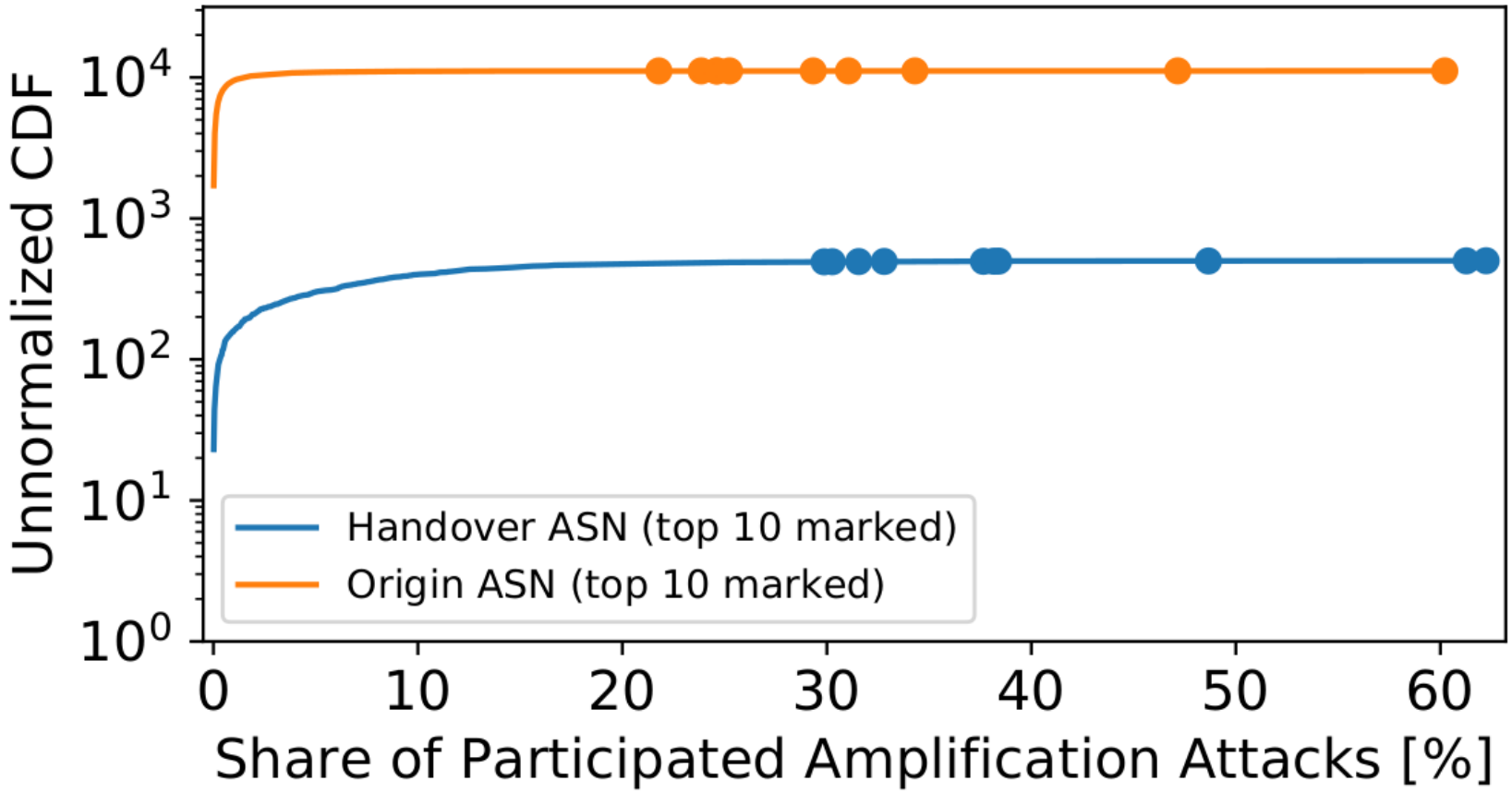
Different protocols* [#]	0	1	2	3	4	5
Events [%]	6	40	45	8.3	0.6	0.1

*Considering the following known amplification protocols/UDP ports: QOTD/17, CharGEN/19, DNS/53, TFTP/69, NTP/123, NetBIOS/138 SNMPv2/161, LDAP/389, RIPv1/520, SSDP/1900, Game/3659 Game/3478, SIP/5060, BitTorrent/6881, Memcache/11211 Game/27005, Game/28960, Fragmentation/–.

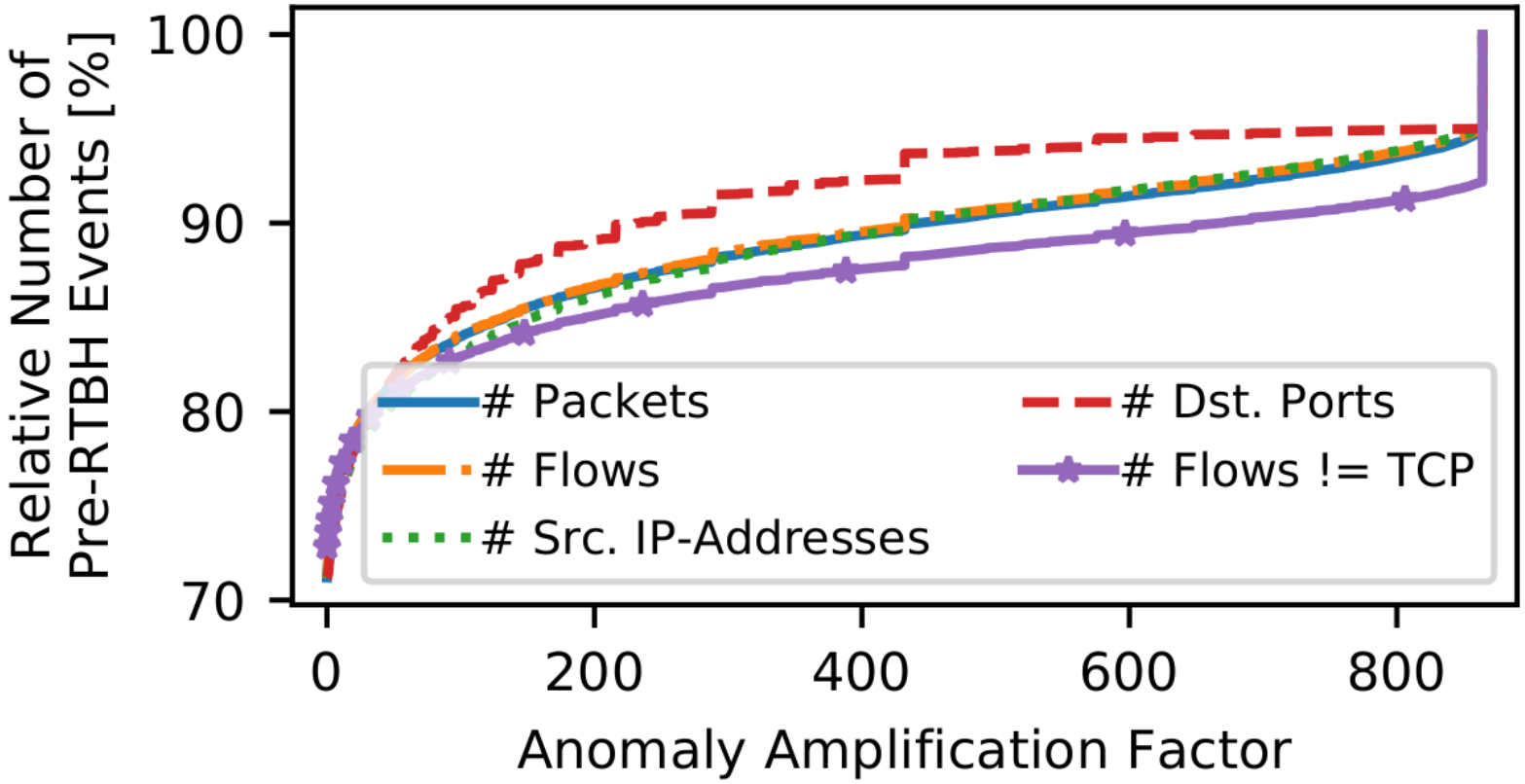
Share of UDP Amplification Traffic



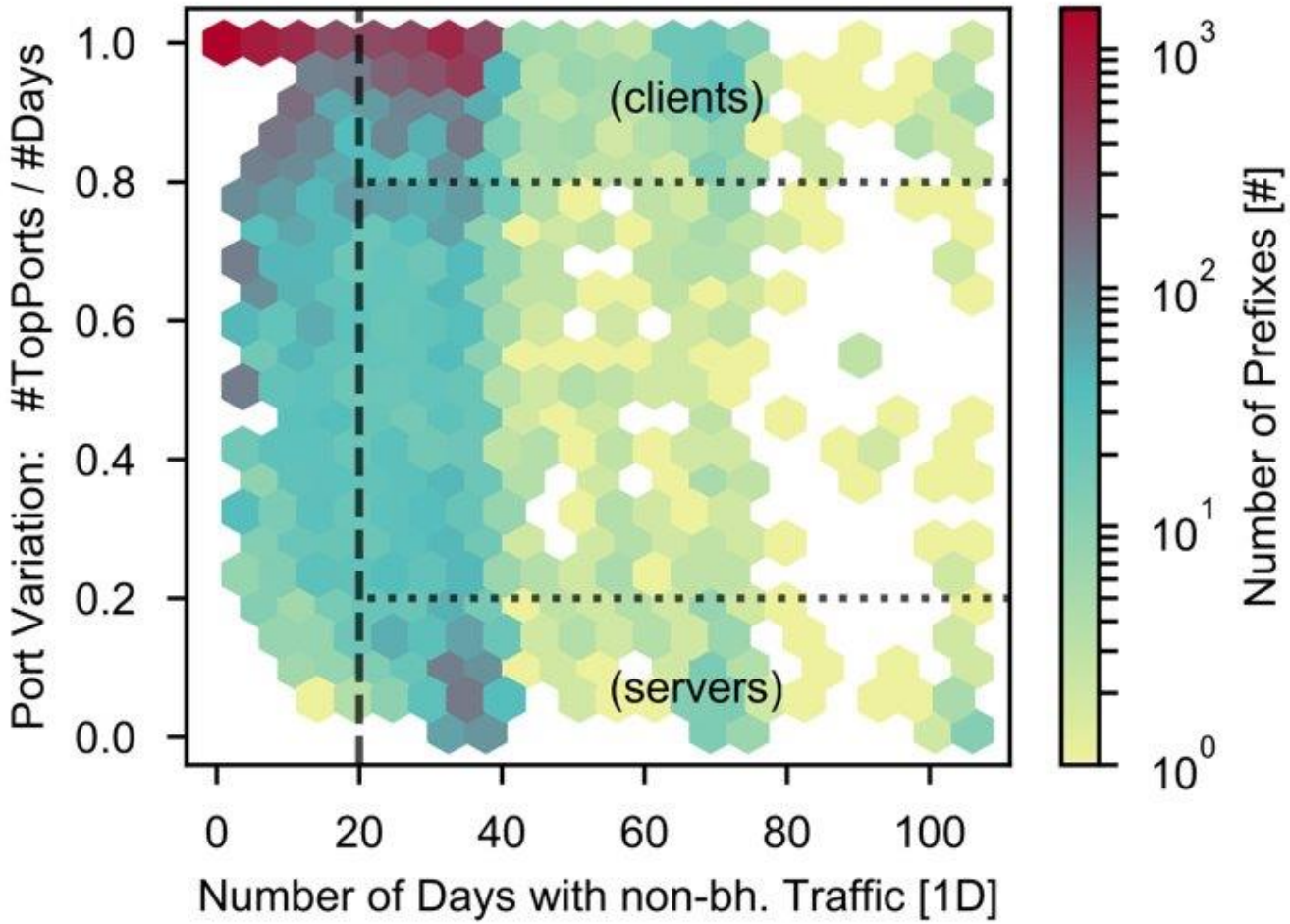
Sources of amplification attacks



EWMA and Anomaly Amplification Factor



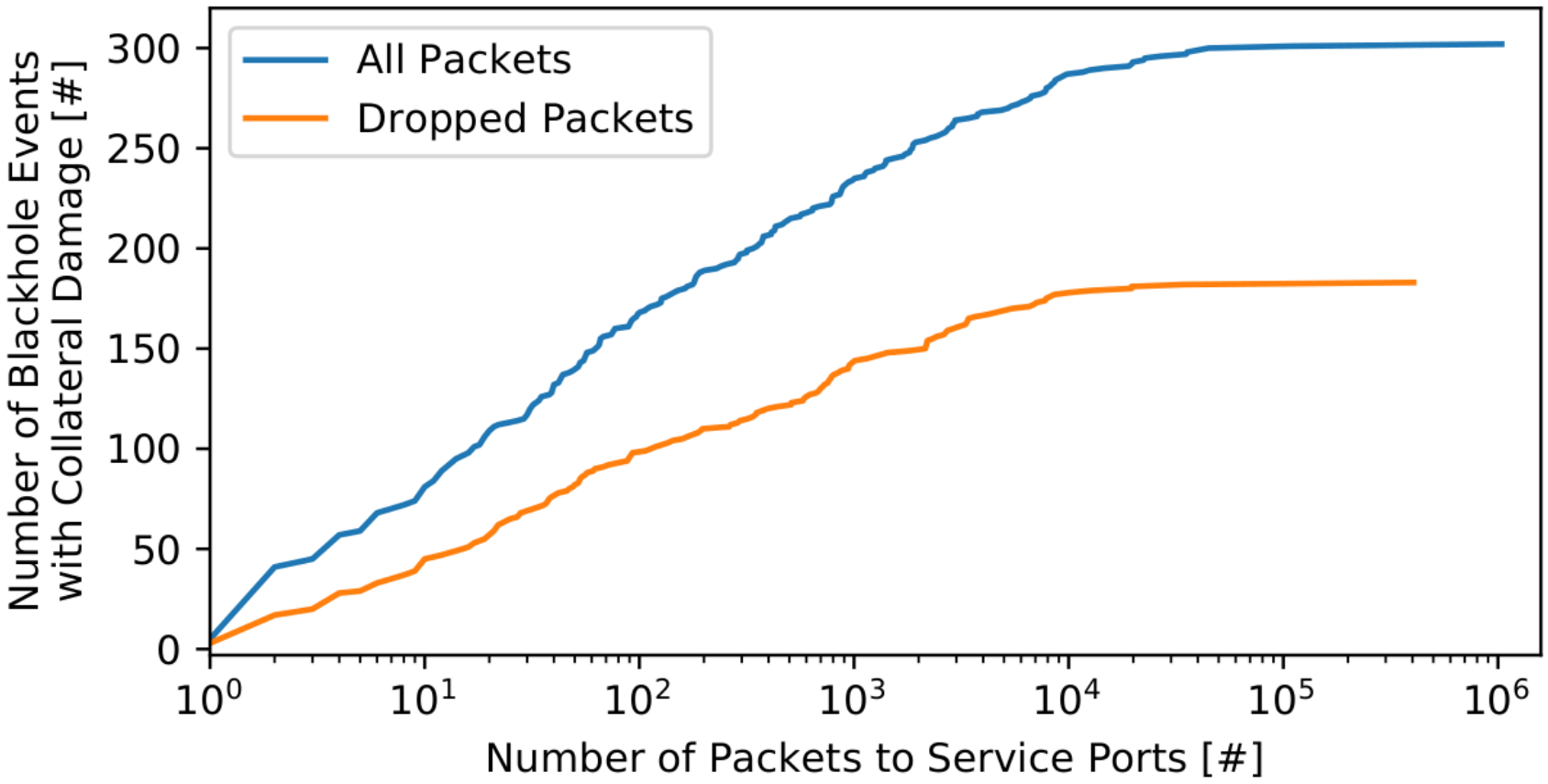
Port Variance vs Port Stability



Challenges of Quantifying Collateral Damage

1. Servers and clients are victims of DDoS
2. Passive inference of services is biased by scans and spoofed traffic
3. Very sparse data outside of RTBH Events
4. Attack traffic might be also present outside of RTBH Events
5. Legitimate traffic pattern change during an attack

Collateral Damage for Servers



Classification Result