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

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

?

Agenda

Recap

How does BGP Blackholing work at IXPs?

Deployment Status

How well deployed is Blackholing in the real world?

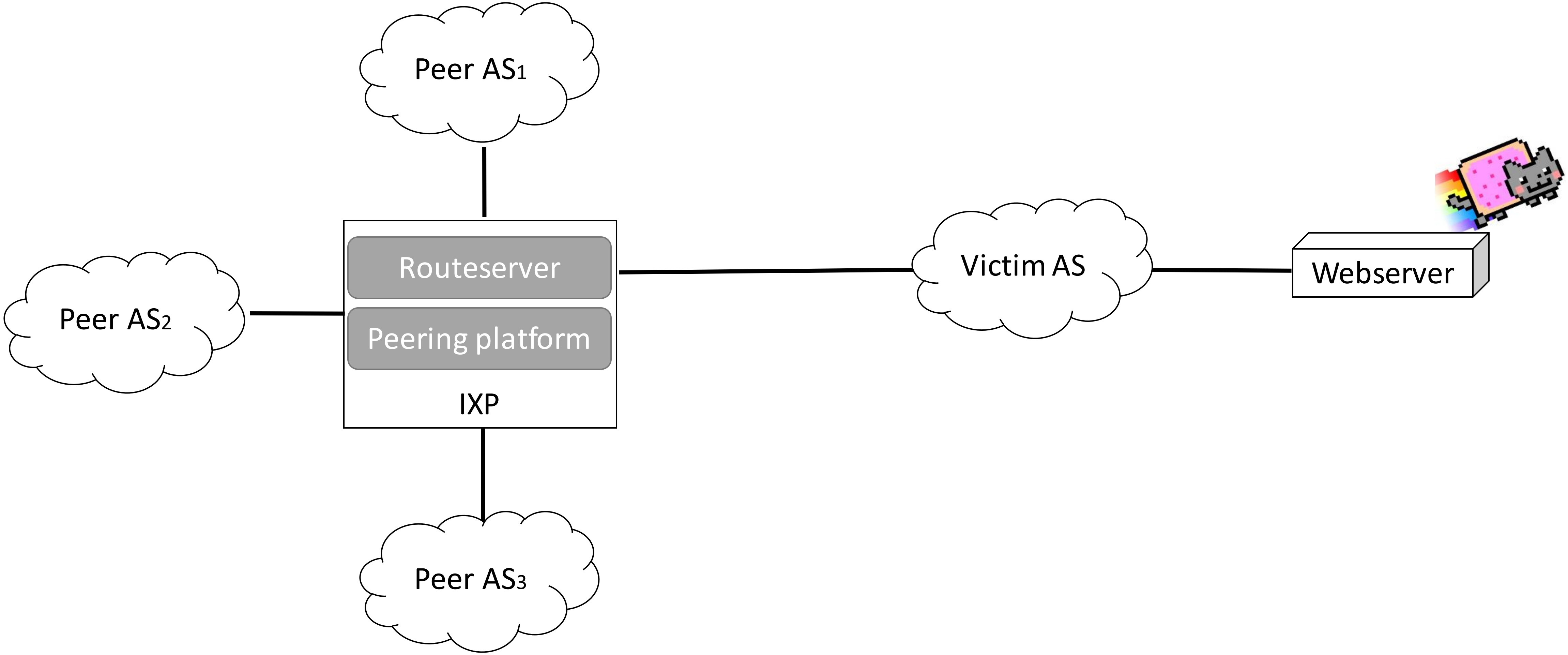
Future Enhancements

How should we configure fine-grained filtering?

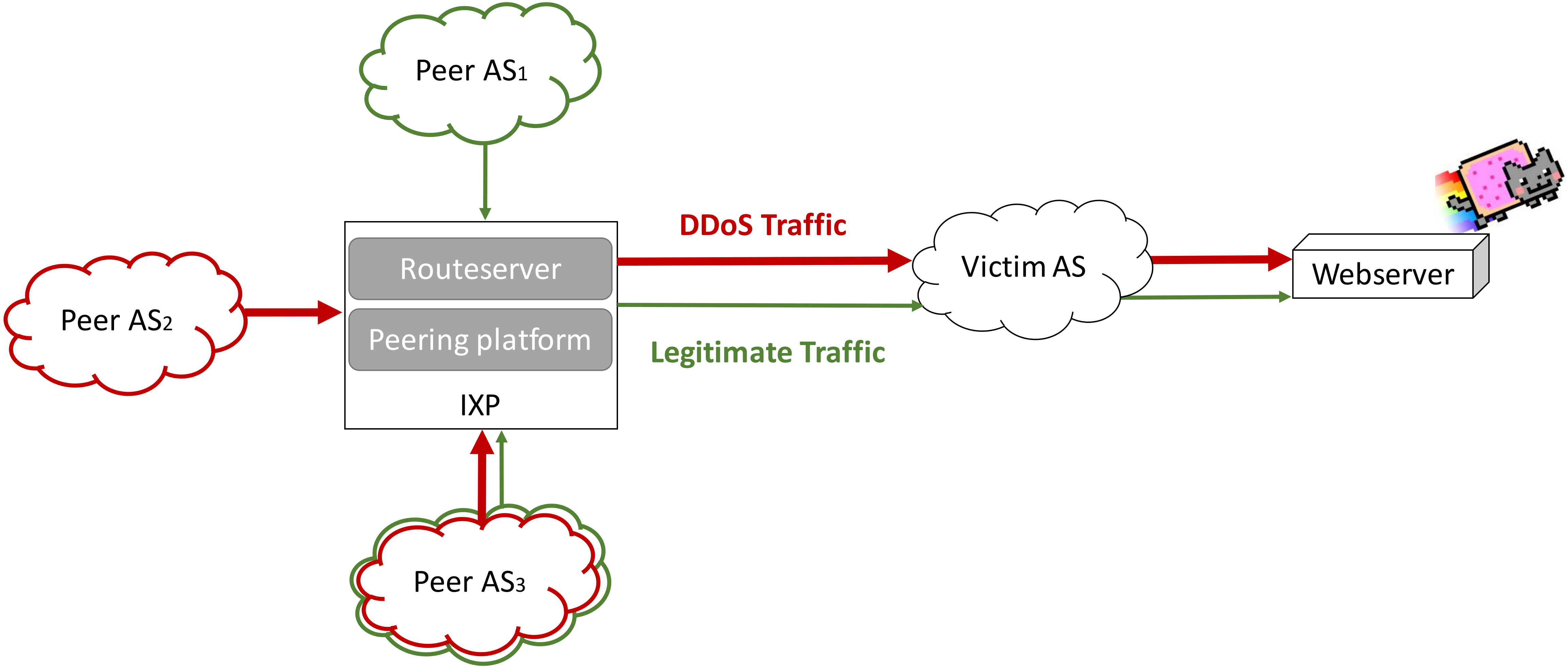
https://en.wikipedia.org/wiki/Black_hole#/media/File:Black_hole_-_Messier_87_crop_max_res.jpg

I. How does BGP Blackholing work at IXPs?

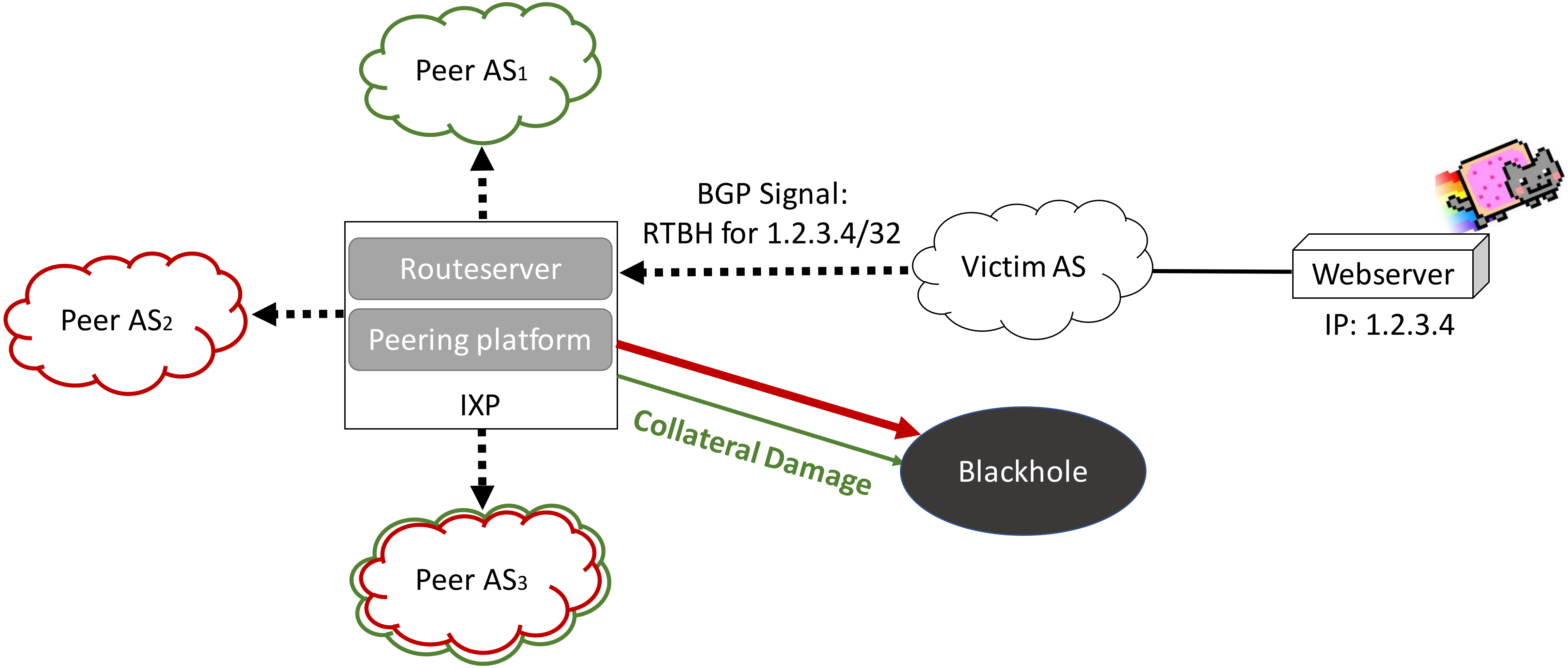
Remotely-Triggered Blackholing at IXPs



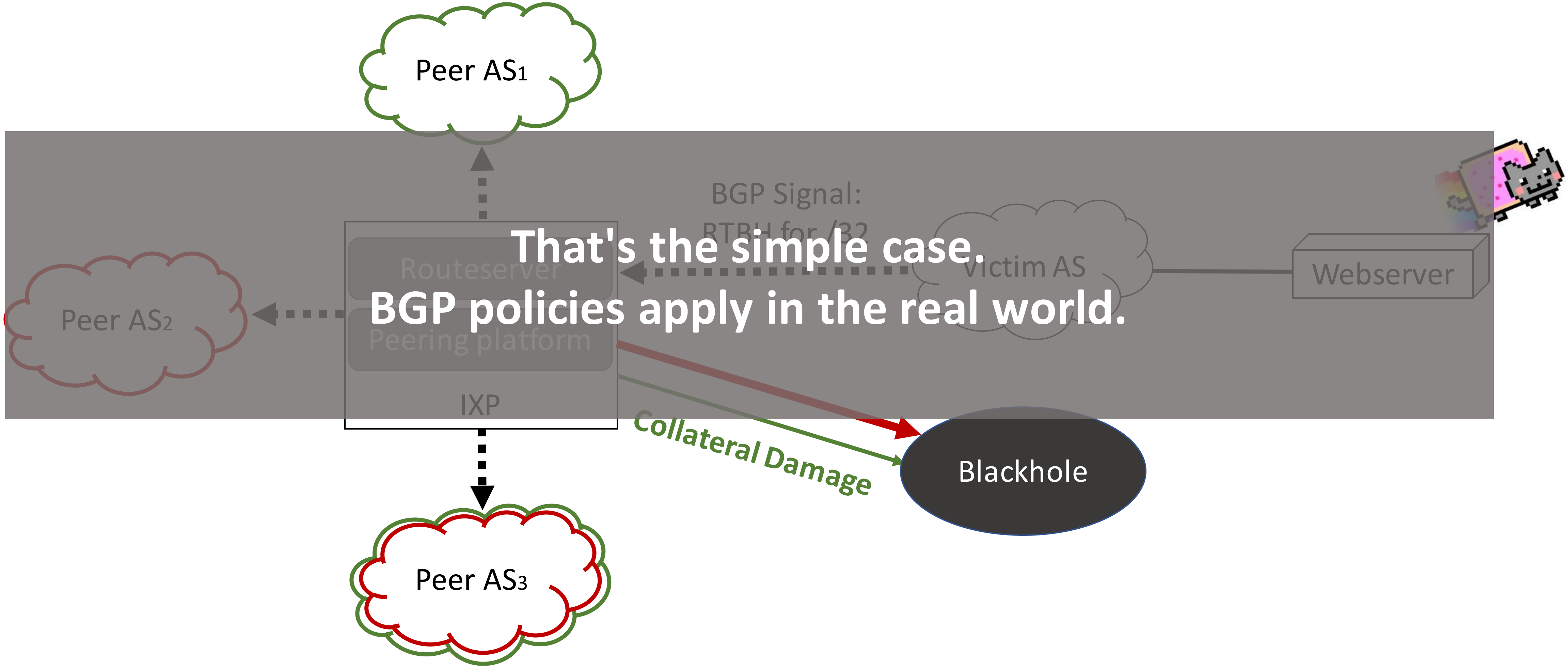
Remotely-Triggered Blackholing at IXPs



Remotely-Triggered Blackholing at IXPs



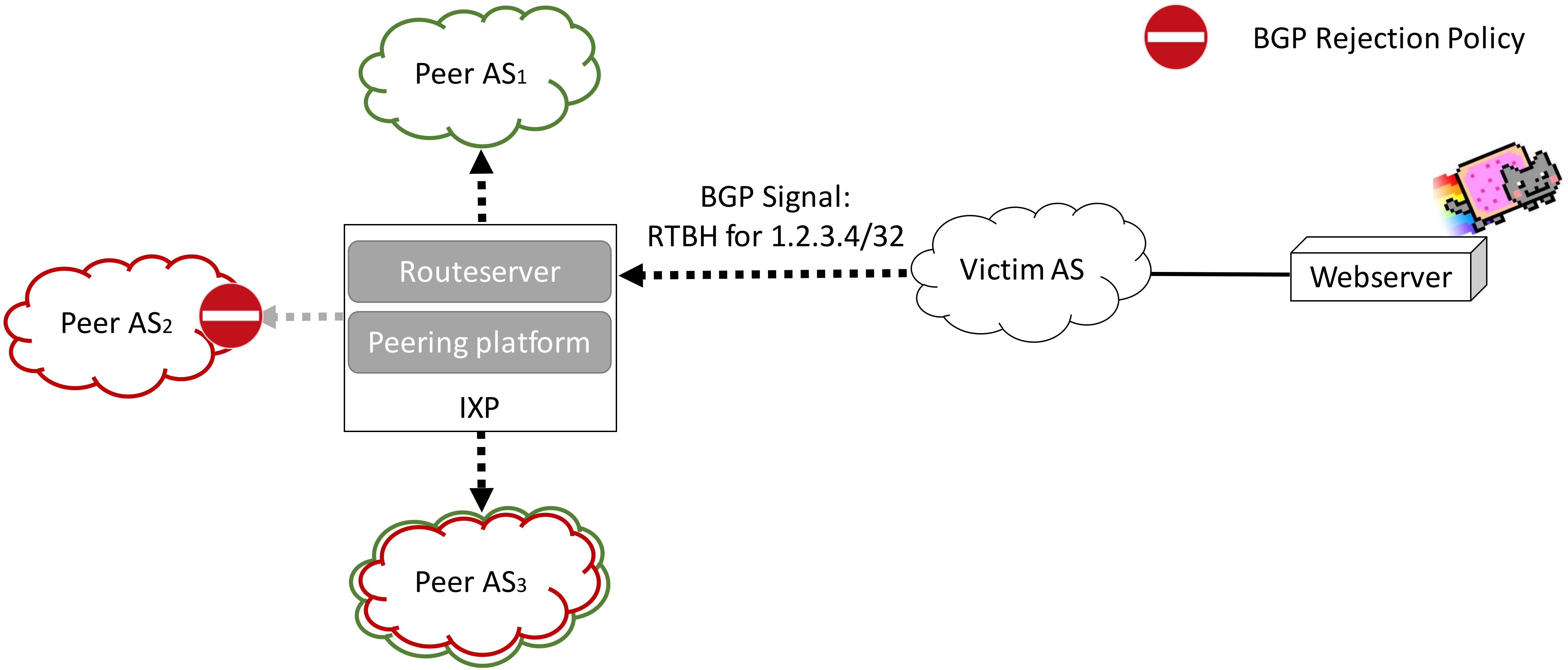
Remotely-Triggered Blackholing at IXPs



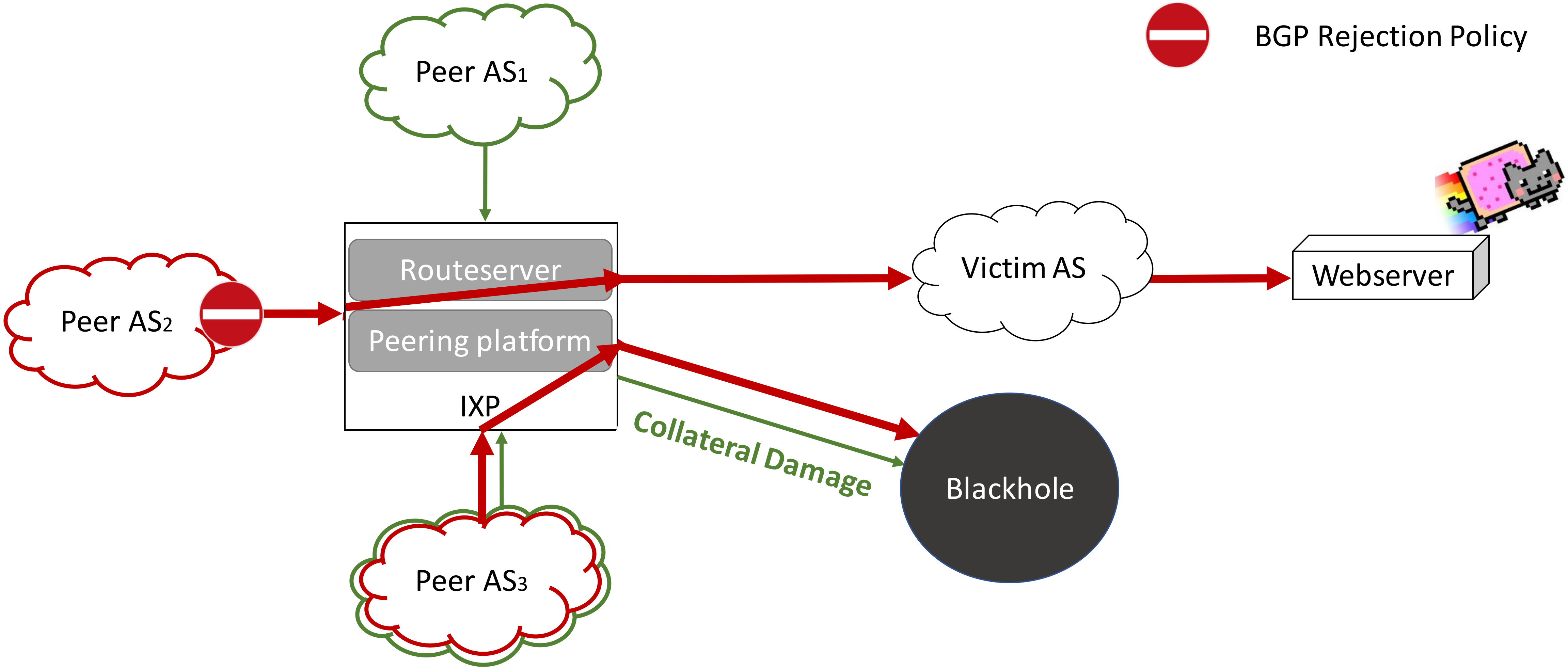
That's the simple case.

BGP policies apply in the real world.

Remotely-Triggered Blackholing and BGP Policies



Remotely-Triggered Blackholing and BGP Policies



https://www.deutschlandfunk.de/media/thumbs/9/94864ed50859e6db43efb6c572614a3av1_max_755x424_b3535db83dc50e27c1bb1392364c95a2.jpg?key=2814f7

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!**

BGP data

All RTBH messages from all route-servers

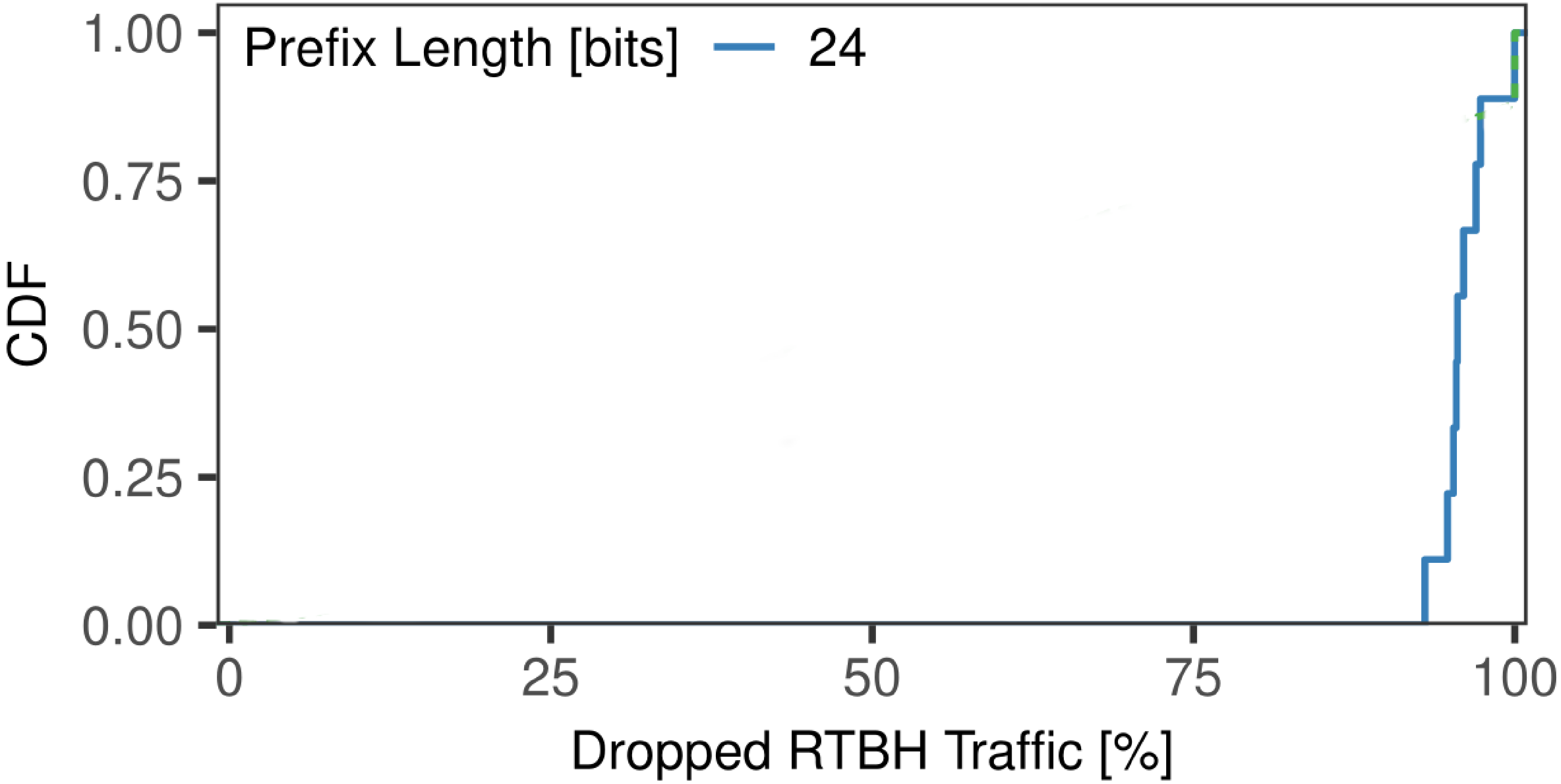
Flow data

All sampled packets from the public switch-fabric for prefixes which have been blackholed at least once

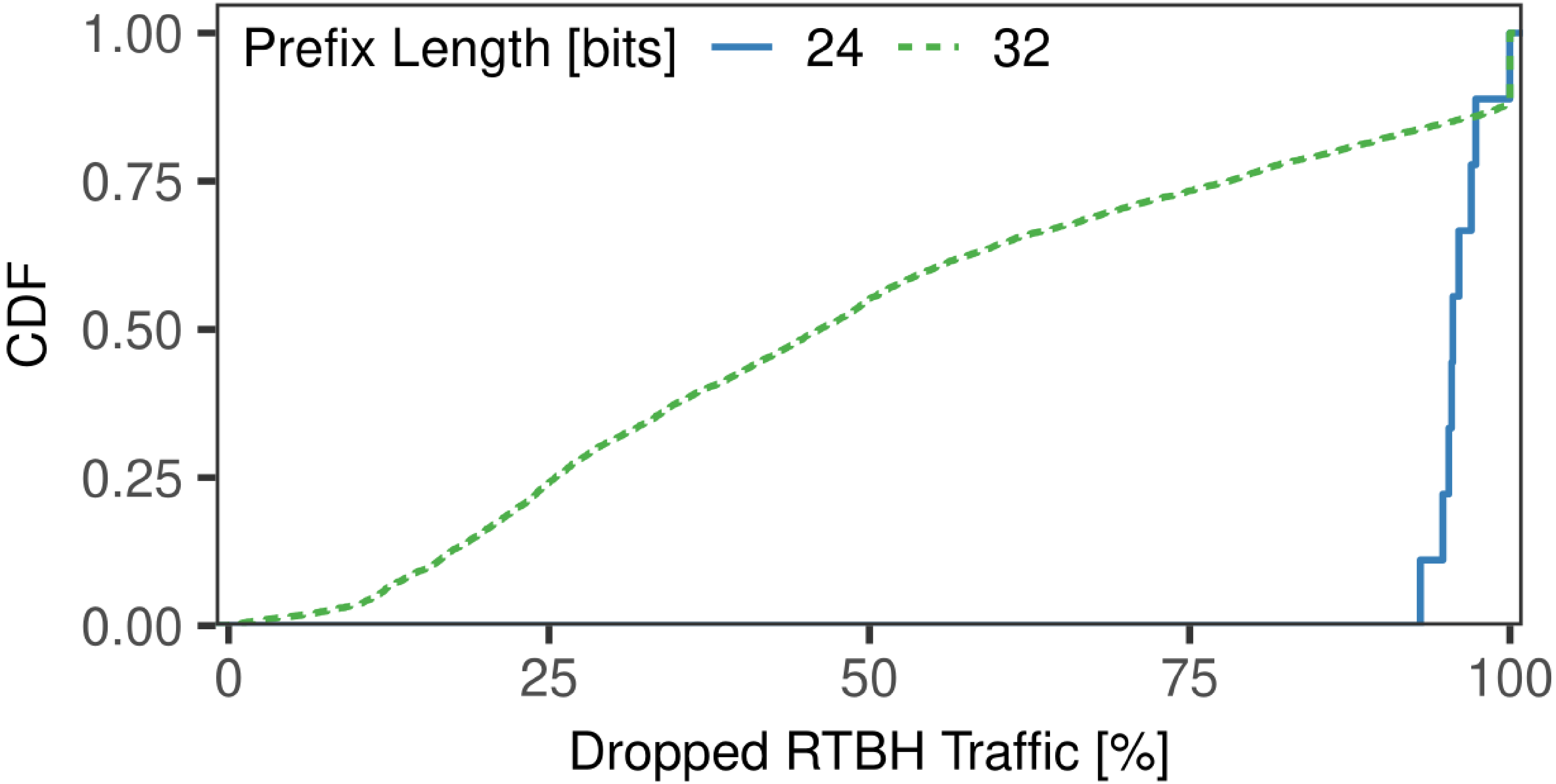
We verified: Time is in sync!

Do all IXP member accept RTBH announcements ?

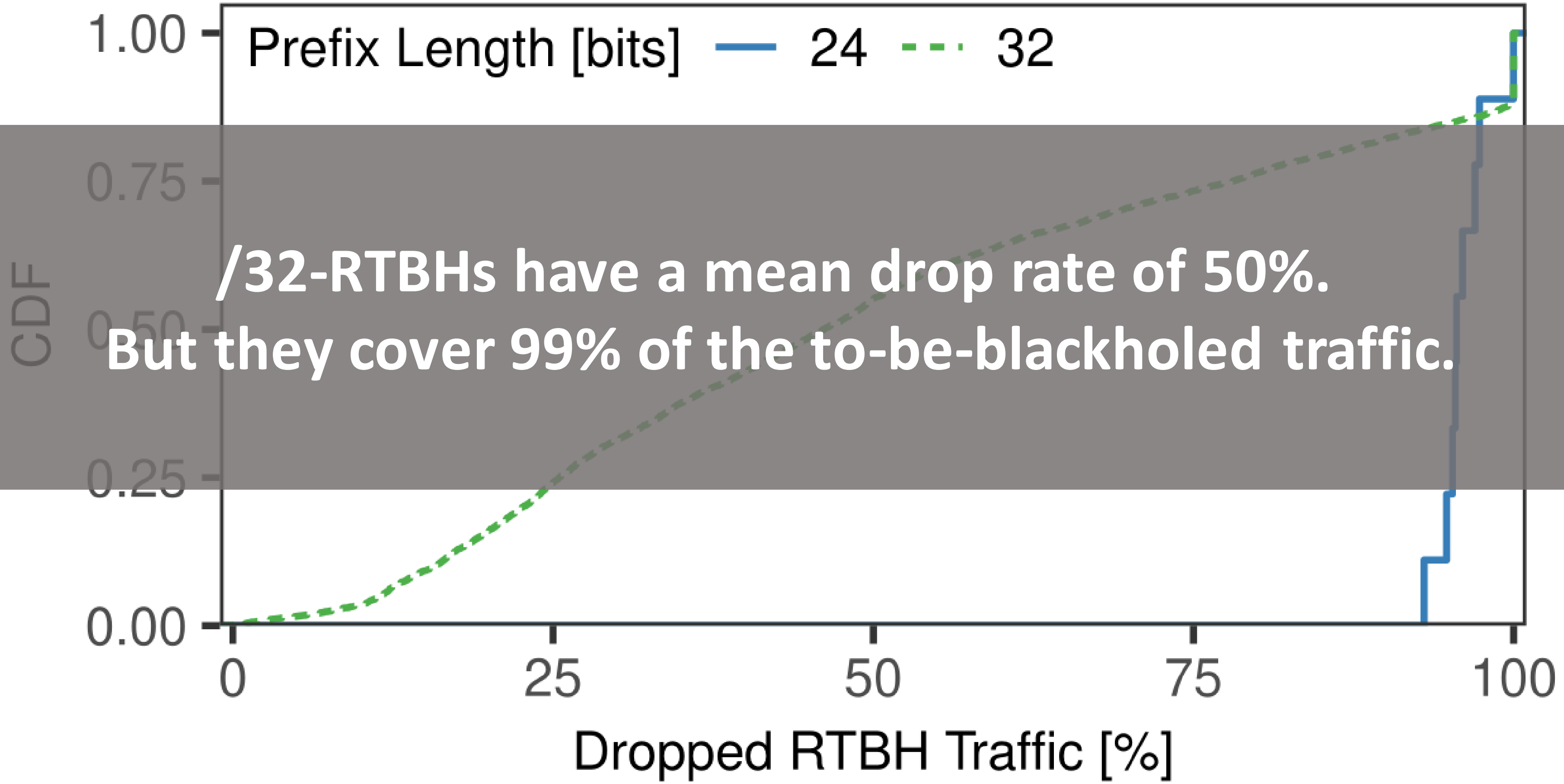
Successful mitigation depends on the announced RTBH prefix length



Successful mitigation depends on the announced RTBH prefix length



Successful mitigation depends on the announced RTBH prefix length

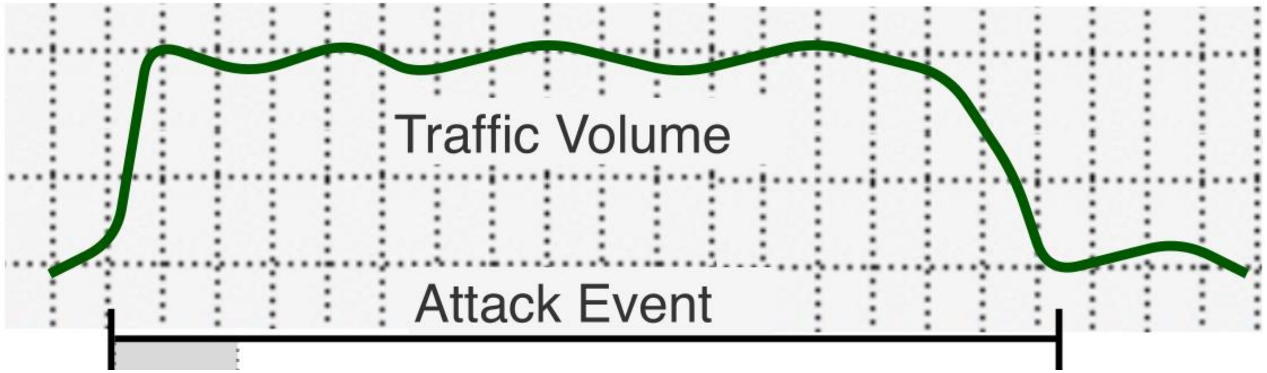


/32-RTBHs have a mean drop rate of 50%.
But they cover 99% of the to-be-blackholed traffic.

How fast do IXP members react to DDoS events?

Measurement challenge

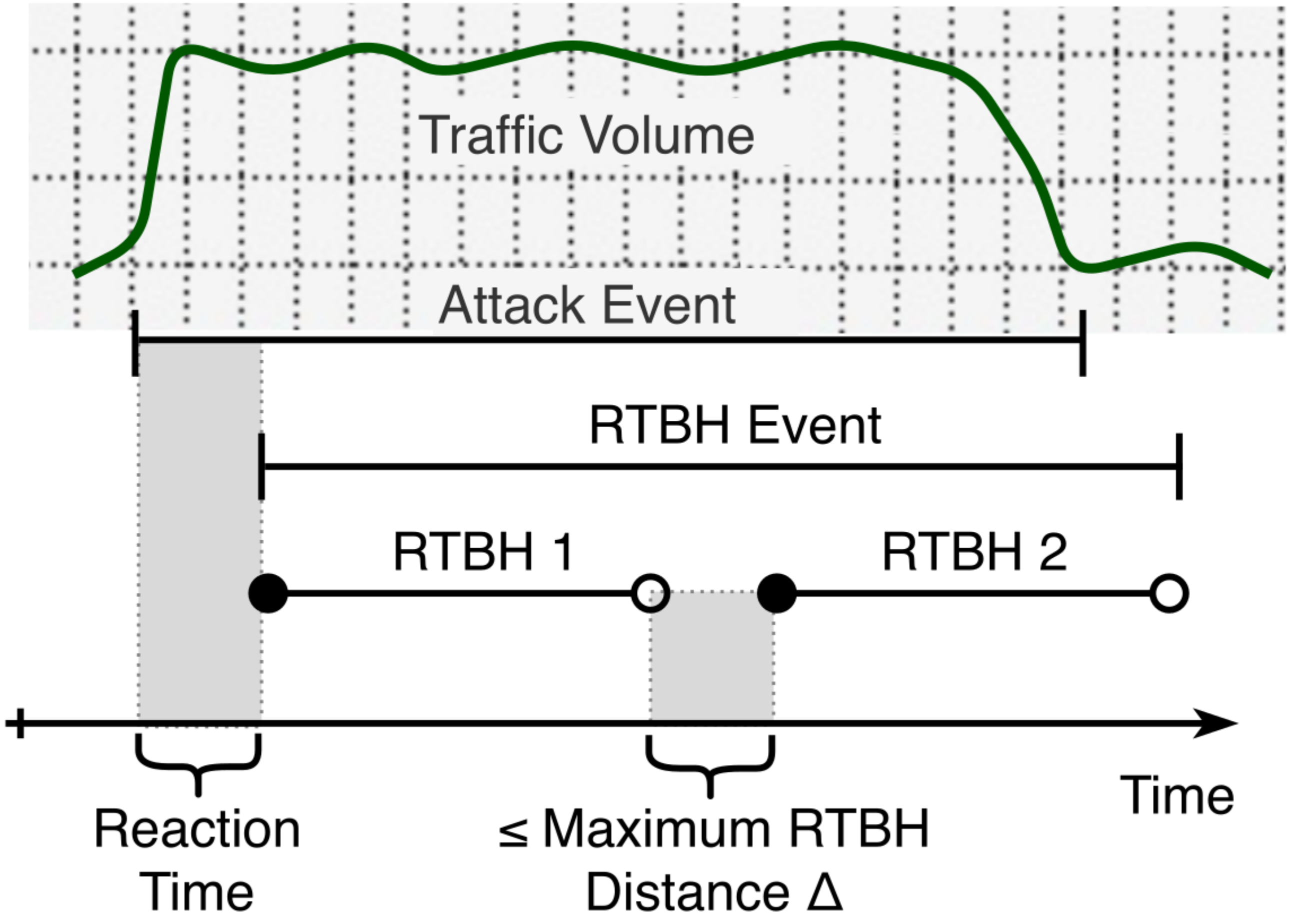
Multiple RTBHs cover the same attack



Data Plane (IPFIX)

Measurement challenge

Multiple RTBHs cover the same attack



Data Plane (IPFIX)

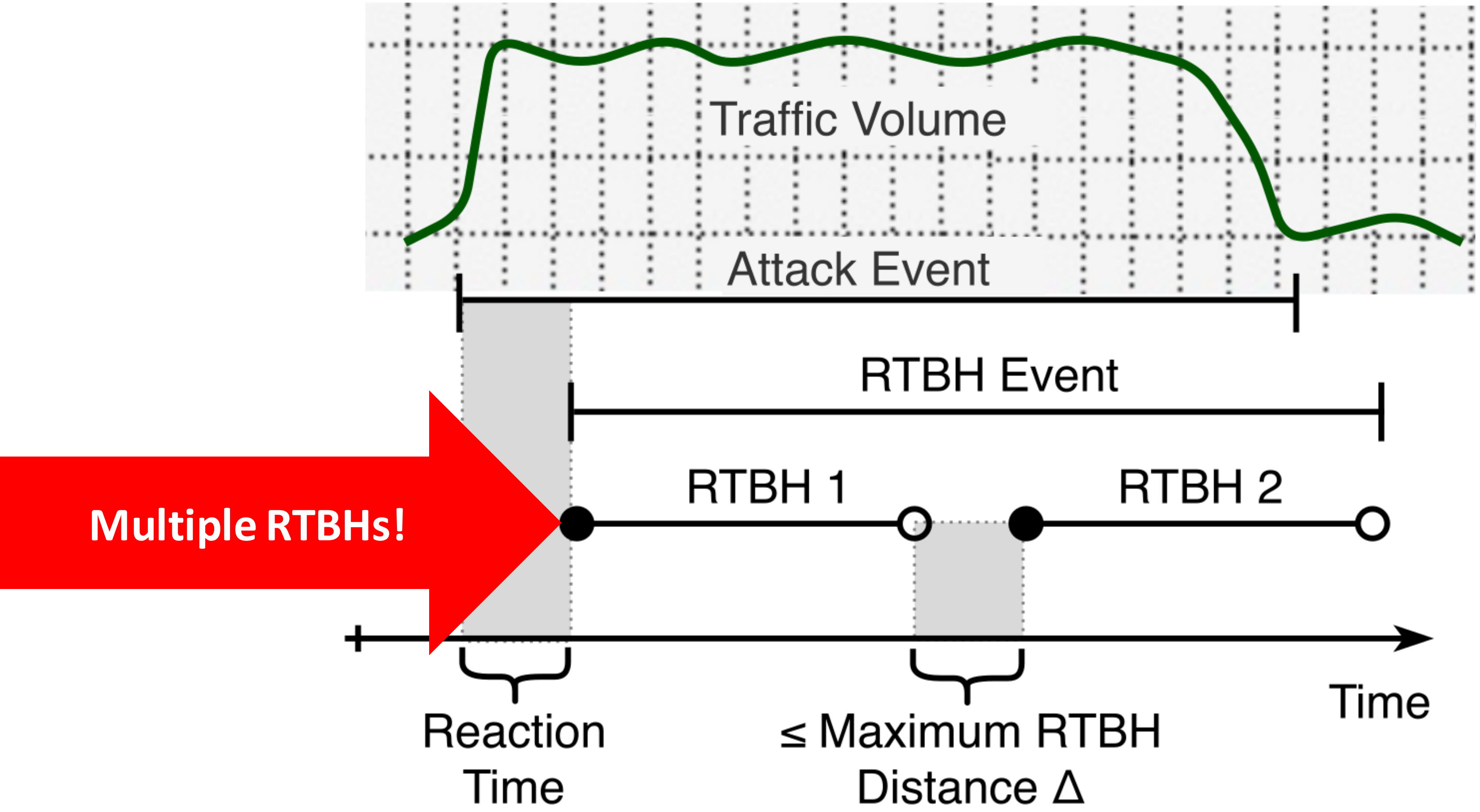
Control Plane (BGP)

● RTBH Announcement

○ RTBH Withdrawal

Measurement challenge

Multiple RTBHs cover the same attack



Data Plane (IPFIX)

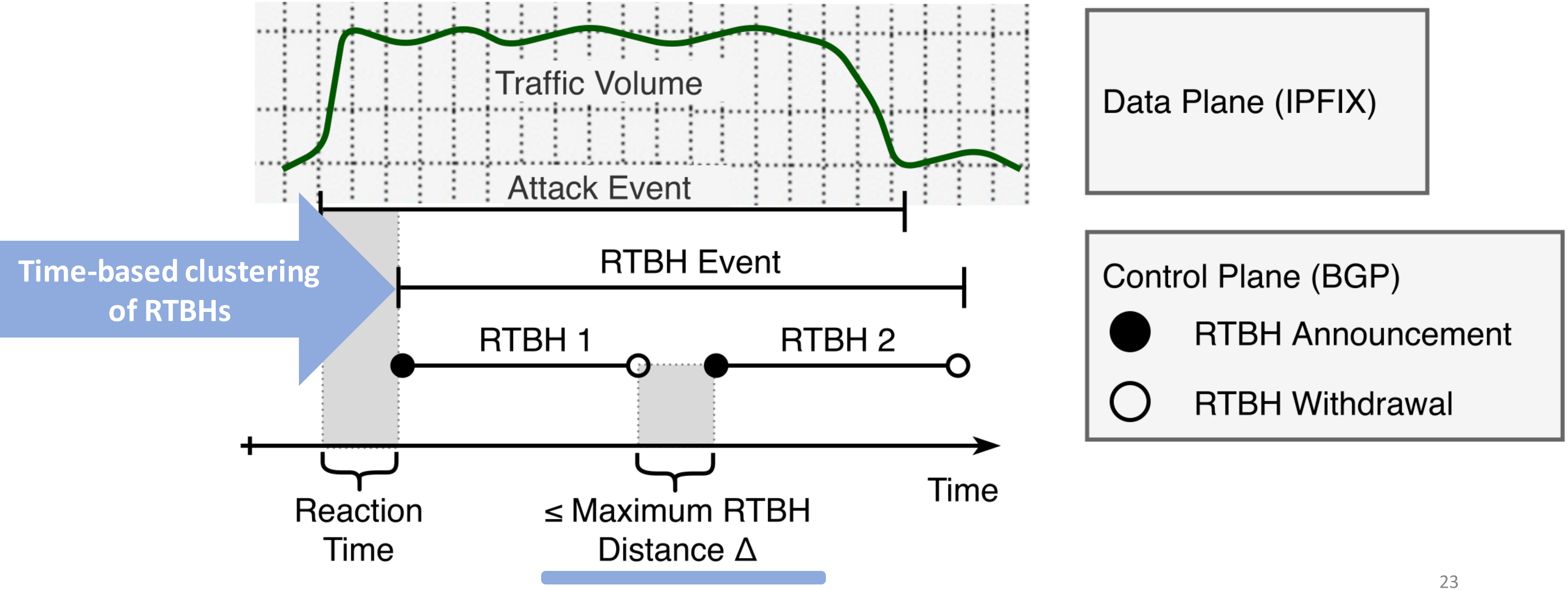
Control Plane (BGP)

● RTBH Announcement

○ RTBH Withdrawal

Measurement challenge

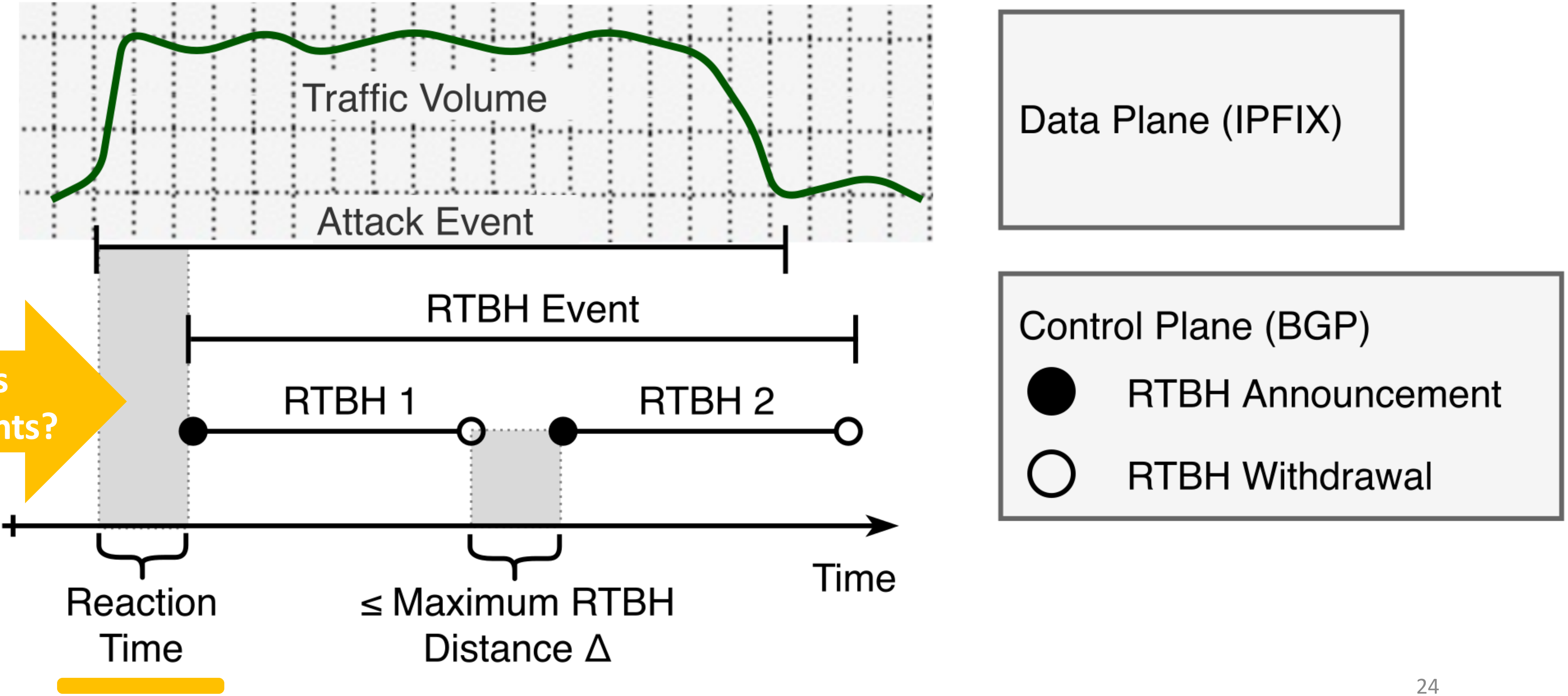
Multiple RTBHs cover the same attack



Time-based clustering of RTBHs

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:

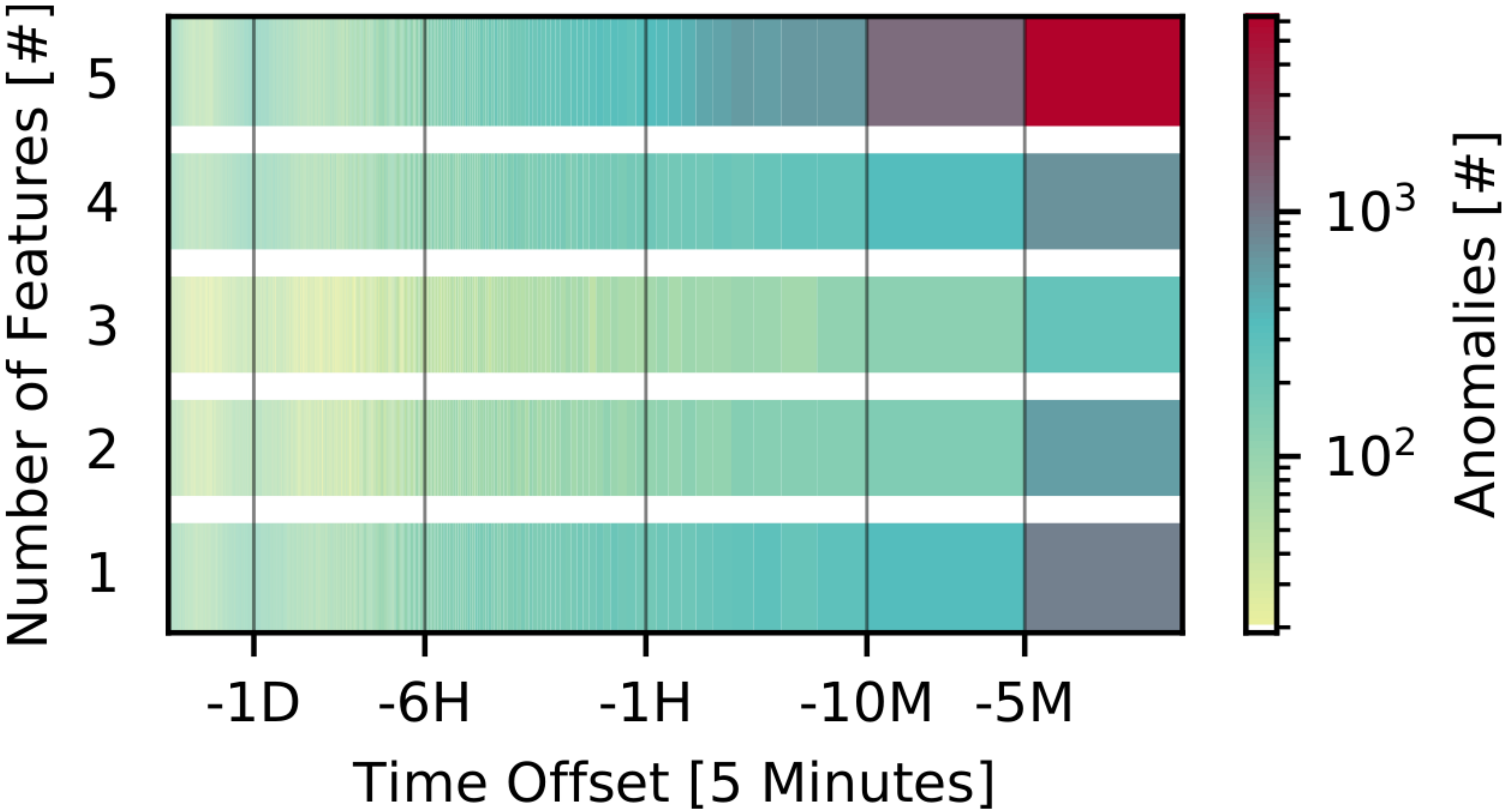
i. number of packets
ii. number of unique destination ports
iii. number of flows
iv. number of unique source IP addresses
v. number of non-TCP flows

Analysis of 72 hours before an RTBH Event

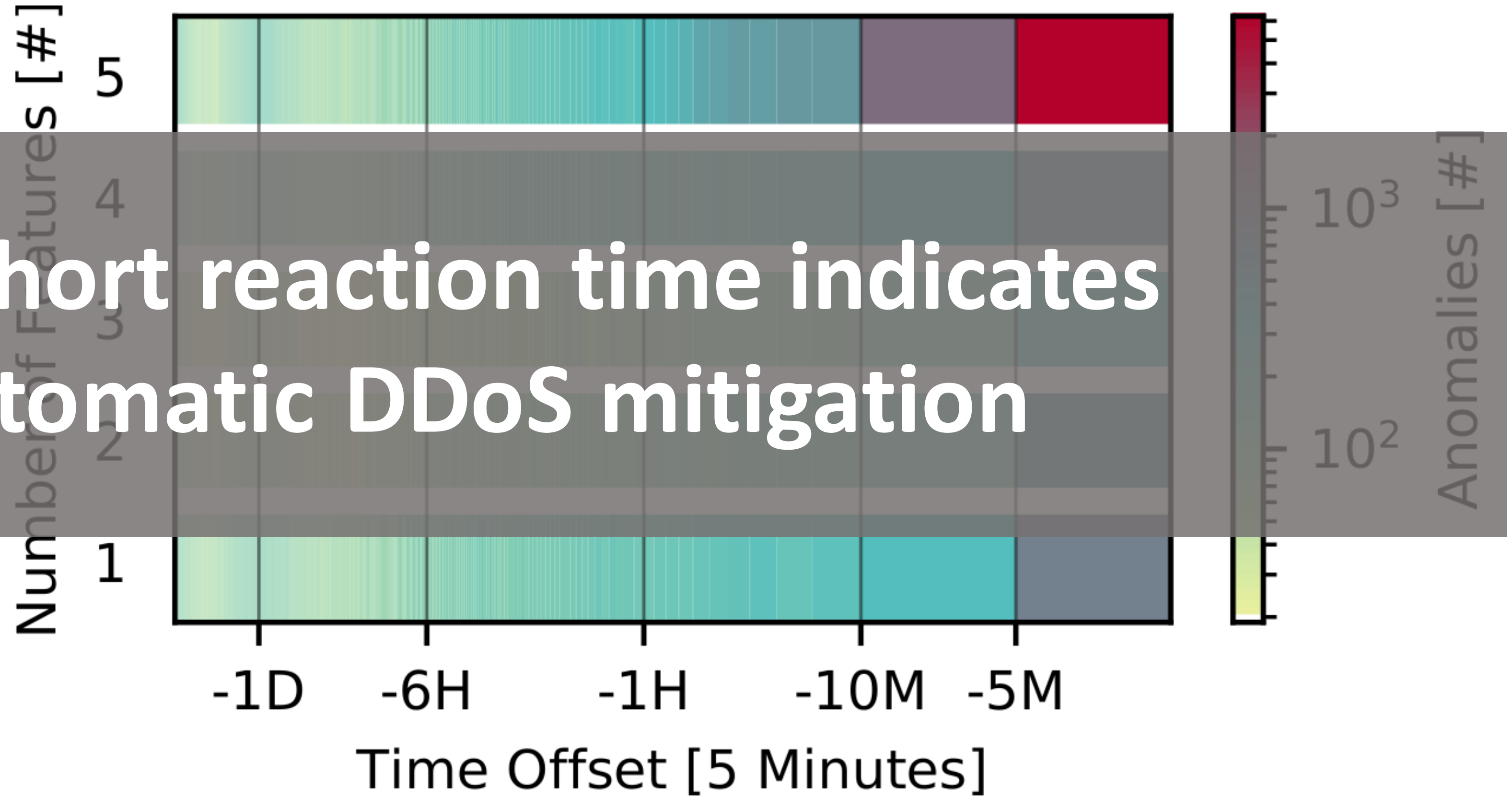
Use a sliding window algorithm (EWMA) to infer whether one of the **monitored features** exhibits an anomalous peak:

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

III. Should we configure fine-grained filtering?

https://www.steinchenspiel.de/

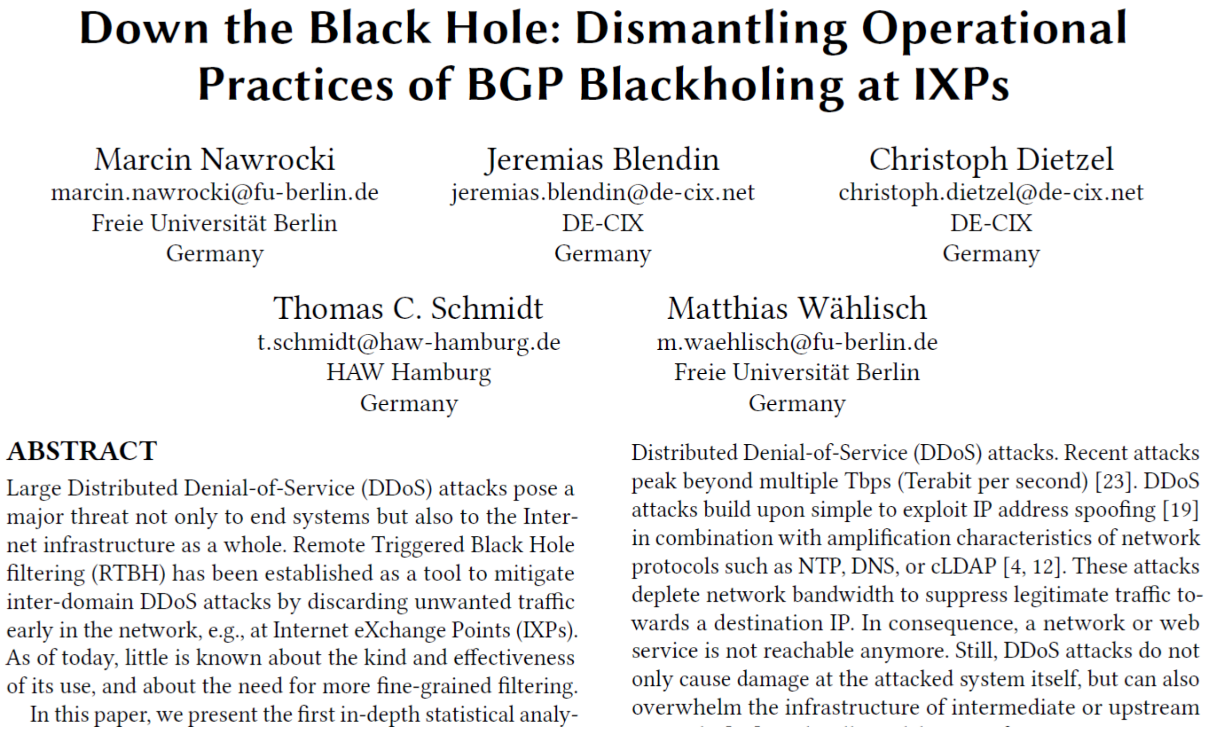
Many clients residing in DSL networks are DDoS'ed and blackholed

Whitelisting is not an option as no regular traffic patterns exist

Most attacks are very simple, **blacklisting** few attack vectors is very effective

More details:

ACM Internet Measurement Conference 2019



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

Marcin Nawrocki
marcin.nawrocki@fu-berlin.de
Freie Universität Berlin
Germany

Jeremias Blendin
jeremias.blendin@de-cix.net
DE-CIX
Germany

Christoph Dietzel
christoph.dietzel@de-cix.net
DE-CIX
Germany

Thomas C. Schmidt
t.schmidt@haw-hamburg.de
HAW Hamburg
Germany

Matthias Wählisch
m.waehlisch@fu-berlin.de
Freie Universität Berlin
Germany

ABSTRACT

Large Distributed Denial-of-Service (DDoS) attacks pose a major threat not only to end systems but also to the Internet infrastructure as a whole. Remote Triggered Black Hole filtering (RTBH) has been established as a tool to mitigate inter-domain DDoS attacks by discarding unwanted traffic early in the network, e.g., at Internet eXchange Points (IXPs). As of today, little is known about the kind and effectiveness of its use, and about the need for more fine-grained filtering.

In this paper, we present the first in-depth statistical analy-

Distributed Denial-of-Service (DDoS) attacks. Recent attacks peak beyond multiple Tbps (Terabit per second) [23]. DDoS attacks build upon simple to exploit IP address spoofing [19] in combination with amplification characteristics of network protocols such as NTP, DNS, or cLDAP [4, 12]. These attacks deplete network bandwidth to suppress legitimate traffic towards a destination IP. In consequence, a network or web service is not reachable anymore. Still, DDoS attacks do not only cause damage at the attacked system itself, but can also overwhelm the infrastructure of intermediate or upstream

Freie Universität Berlin

DE CIX

Hochschule für Angewandte
Wissenschaften Hamburg
Hamburg University of Applied Sciences

Summary. Operational advice.

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

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