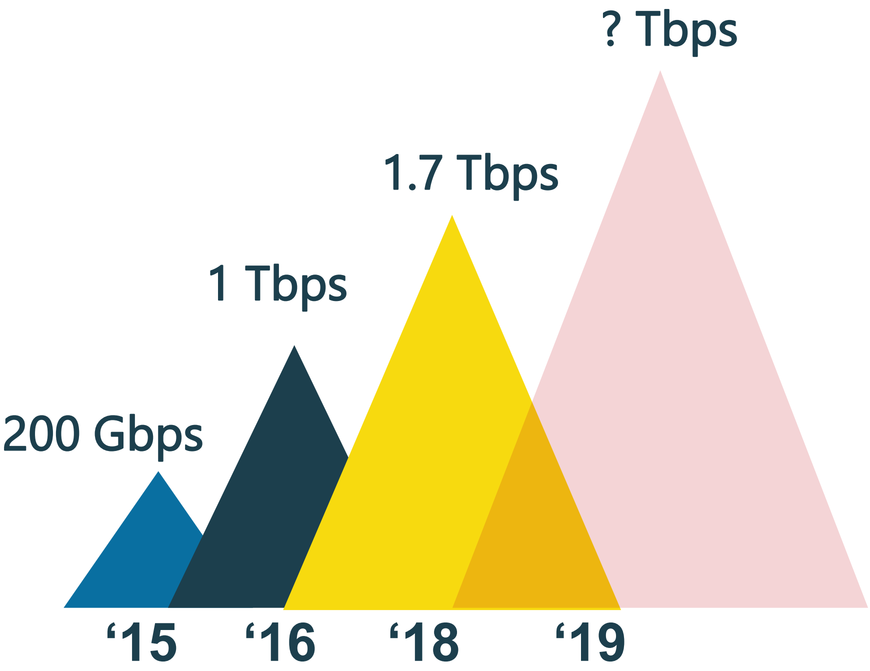
Next Gen Blackholing to Counter DDoS

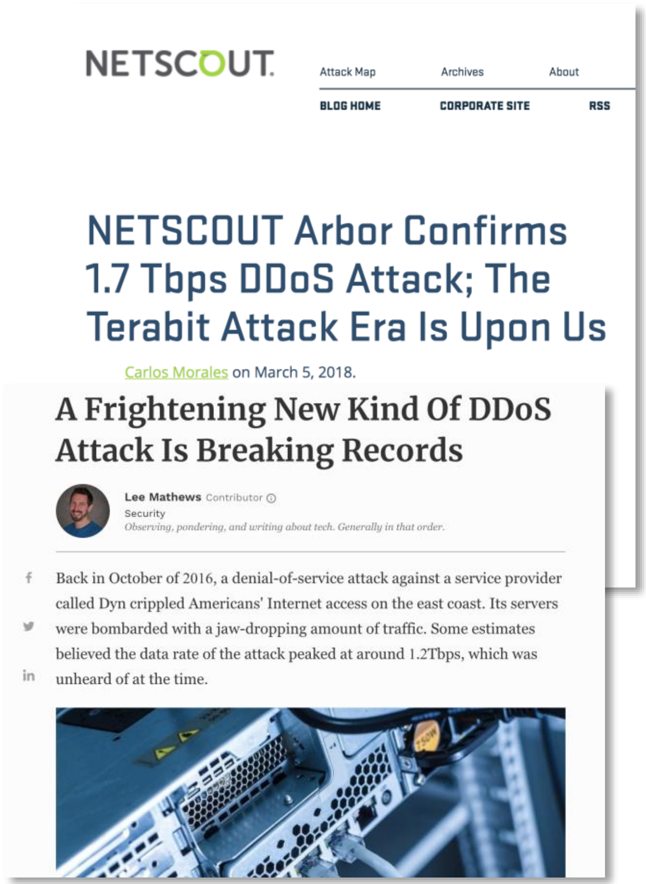
RIPE78, Reykjavik, Iceland

Christoph Dietzel [§*], **Matthias Wichtlhuber***, Georgios Smaragdakis [§], Anja Feldmann [†]

[§]TU Berlin, *DE-CIX, [†]MPI

Volumetric DDoS Attacks





NETSCOUT

Attack Map Archives About

BLOG HOME CORPORATE SITE RSS

NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us

Carlos Morales on March 5, 2018.

A Frightening New Kind Of DDoS Attack Is Breaking Records

Lee Mathews Contributor

Security

Observing, pondering, and writing about tech. Generally in that order.

Back in October of 2016, a denial-of-service attack against a service provider called Dyn crippled Americans' Internet access on the east coast. Its servers were bombarded with a jaw-dropping amount of traffic. Some estimates believed the data rate of the attack peaked at around 1.2Tbps, which was unheard of at the time.

ISP DDoS Defense Toolbox

ACL

- Filters at arbitrary granularity
- Vendor-specific
- Per device config

TSS (Traffic Scrubbing Services)

- Carefree service
- Redirects traffic to scrubbing centers
- On-demand vs. always on

Flowspec

- Configures rules at neighbor network
- Filters at arbitrary granularity
- Cooperation required

RTBH

- Configures rules at neighbor network
- Filters at IP granularity
- Cooperation required

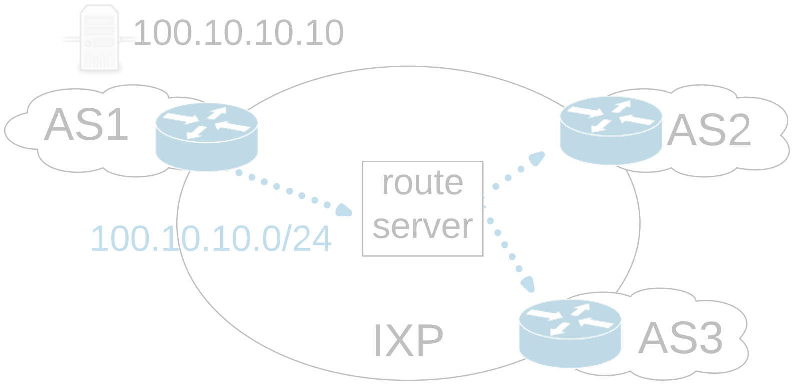
DDoS Defense at IXPs

→ Combine good properties of existing solutions

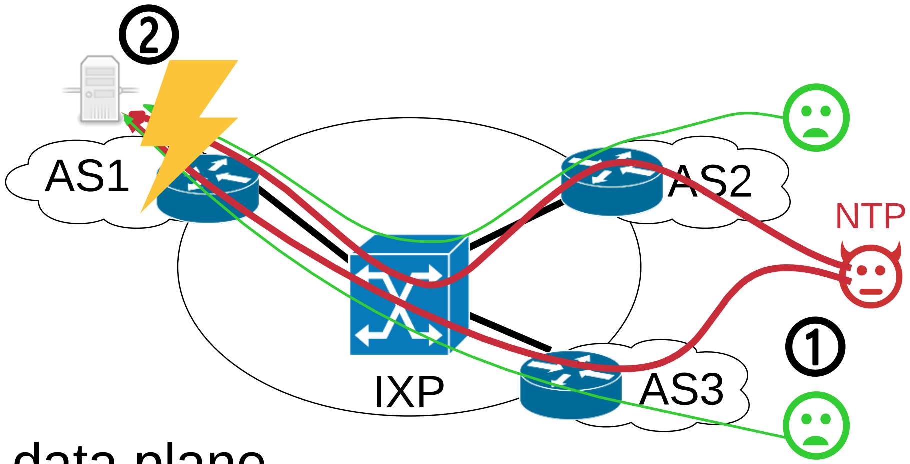
→ Eradicate current shortcomings

+ IXPs offer services to hundreds of Ases
+ IXPs have multiple Tbps capacity
+ Trusted part of the Internet community

Blackholing at IXPs

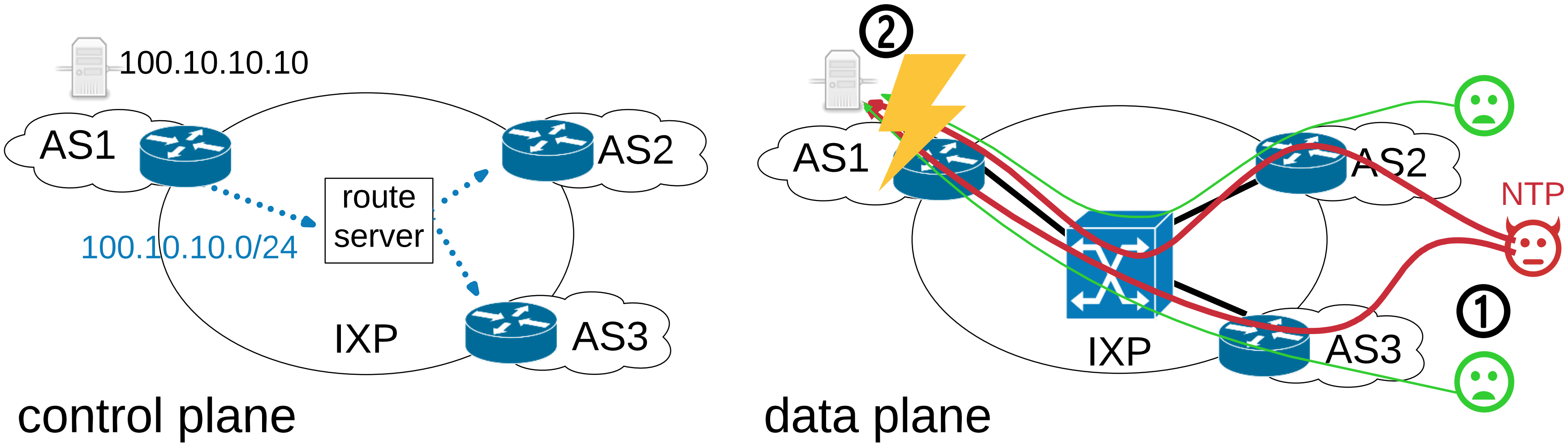


control plane

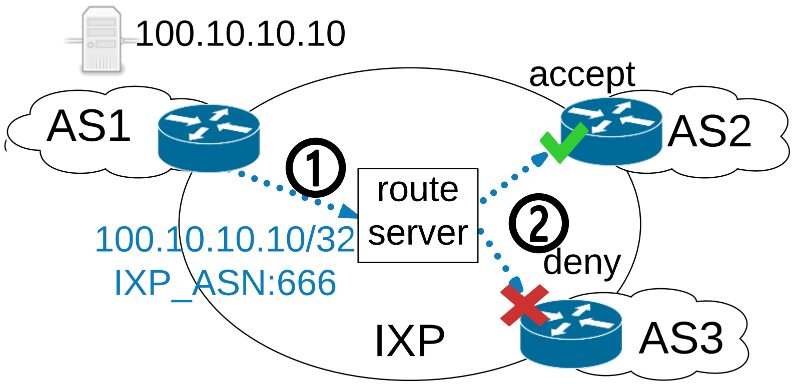


data plane

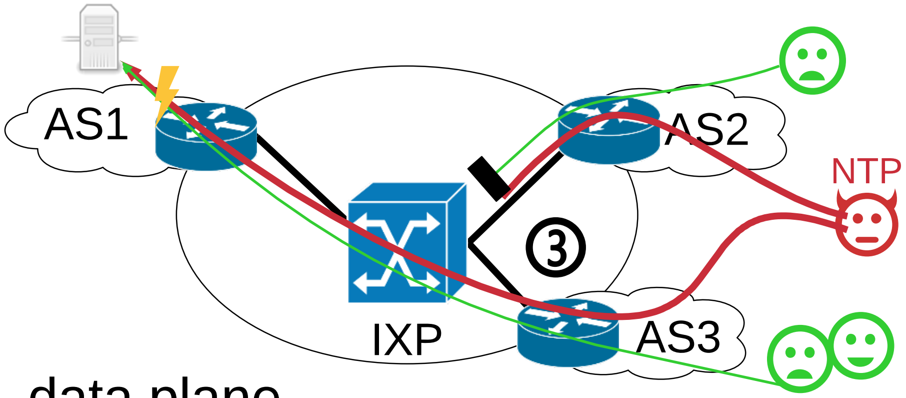
Blackholing at IXPs



Blackholing at IXPs

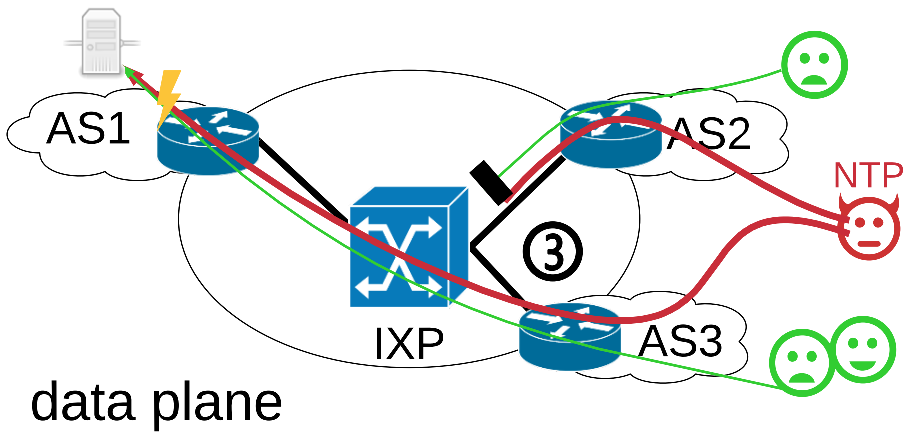


control plane



data plane

Blackholing – Limitations



→ Blocks unwanted and wanted traffic

→ No effect on a subset of peerings

→ Behavior is hard to predict

Blackholing – Limitations

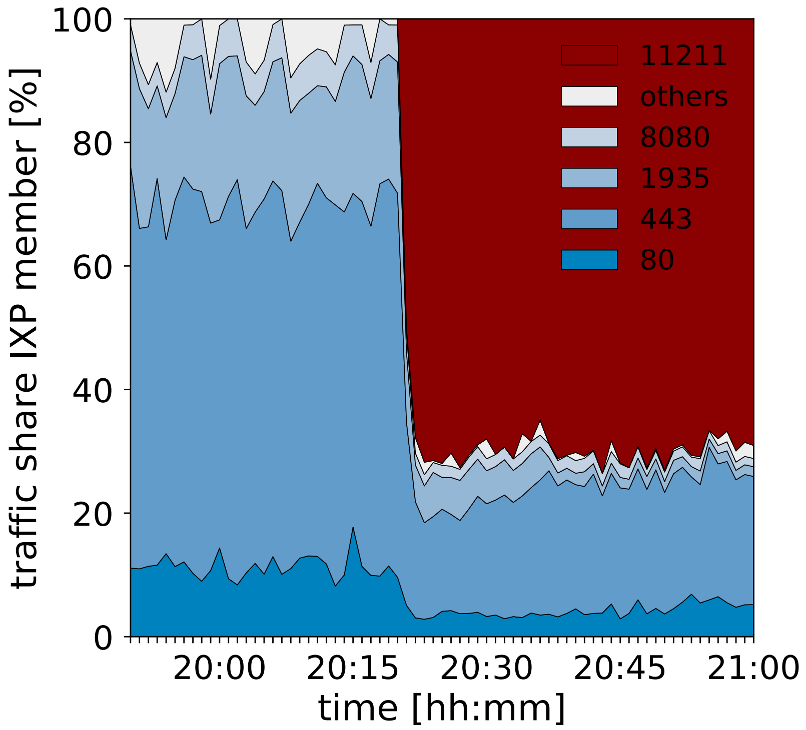
→ Relative traffic of 40GE IXP port

→ Mostly web traffic (80, 443, …)

→ Attack 70% memcached traffic

→ Still significant share of web traffic

→ **Collateral damage!**



Blackholing – Limitations

→ All or nothing approach

  → Prefix granularity

  → Per peer selection at IXPs

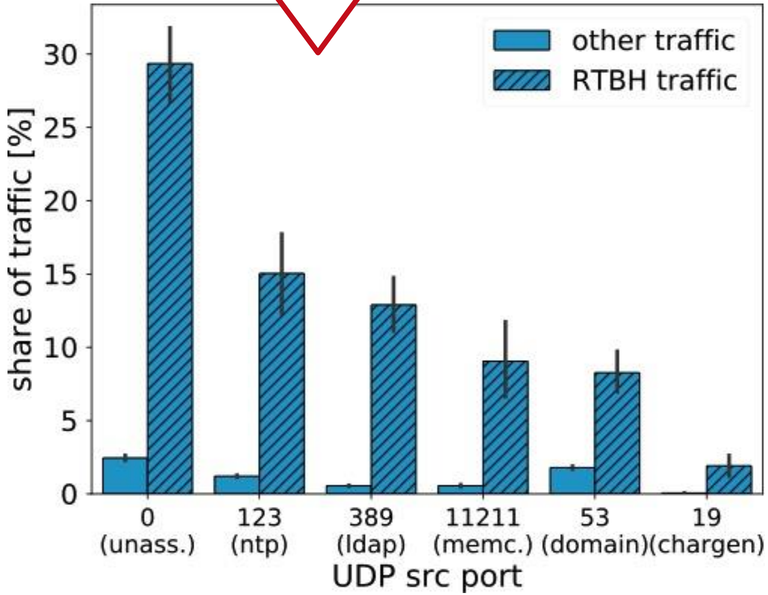
→ Blackholing traffic:

  → 99.94% UDP

  → Expected L4 ports (NTP, LDAP, …)

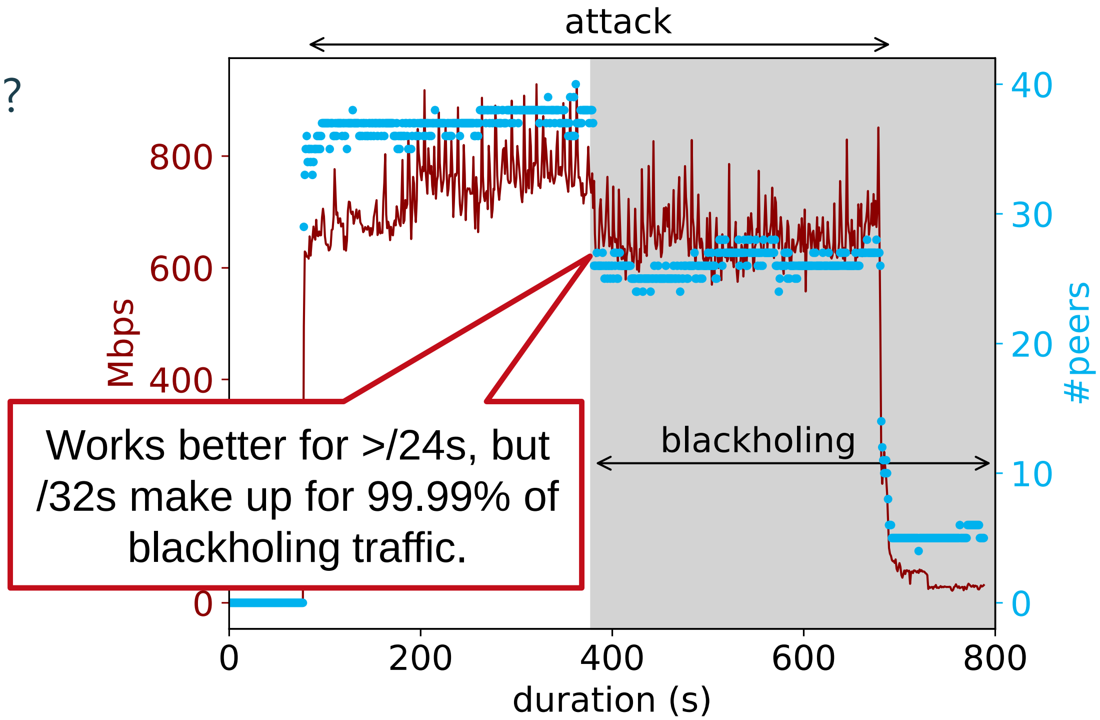
→ **More granularity needed!**

6 blocking rules are enough to filter 80% of DDoS traffic.



Blackholing – Limitations

- → How "ineffective" can it be?
  - → NTP DDoS attack
  - → AS at IXP via ML peering
  - → Attacks for 10 min to /32

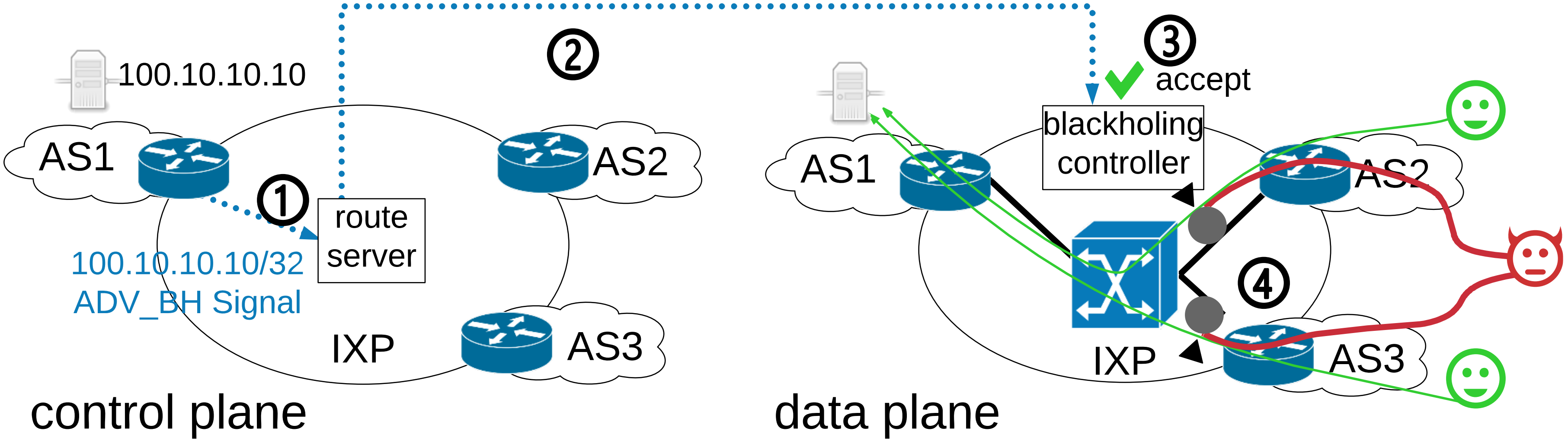


- → Drop all traffic to /32
- → Traffic: 800 to 600 Mbps
- → Peers: 38 to 26
- → **Signaling too complex!**

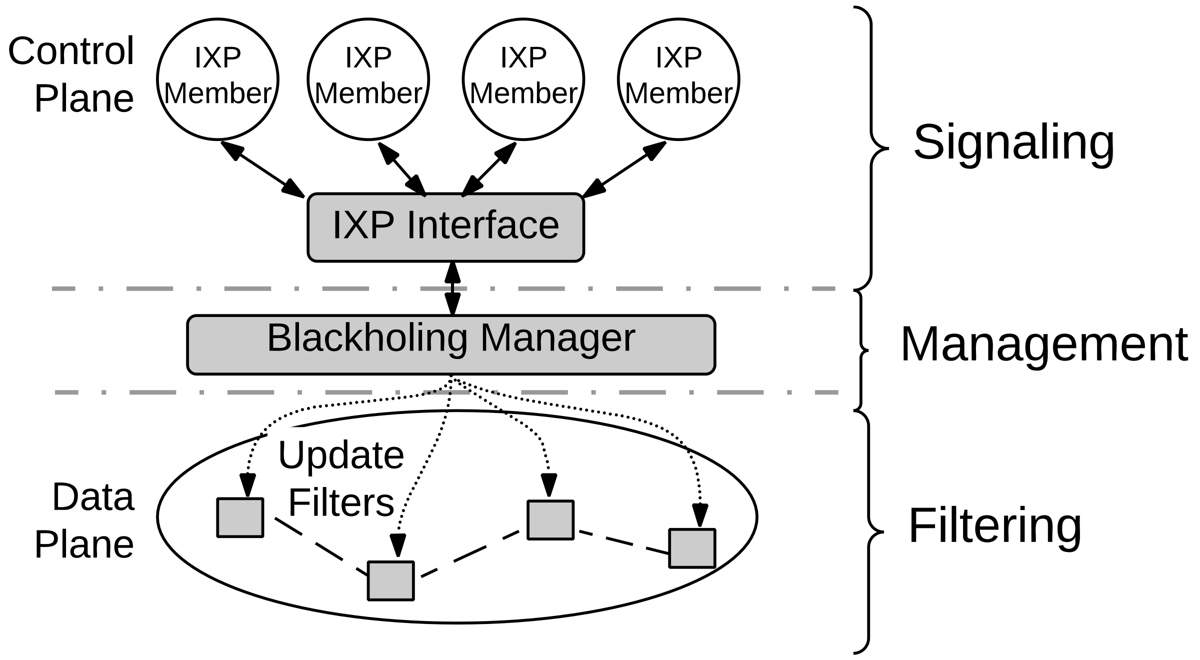
Advanced Blackholing Requirements

- → Granularity
  - → Fine-grained filtering (src/dst header fields)
- → Signaling complexity
  - → Easy to use, short setup time
- → Cooperation
  - → Lower levels of cooperation among the involved parties
- →Telemetry
  - → Feedback on the state of the attack at any time
- →Scalability
  - → Scale in terms of performance, filters, reaction time, config complexity
- → Cost
  - → Meeting all requirements with min. invest (CAPEX & OPEX)

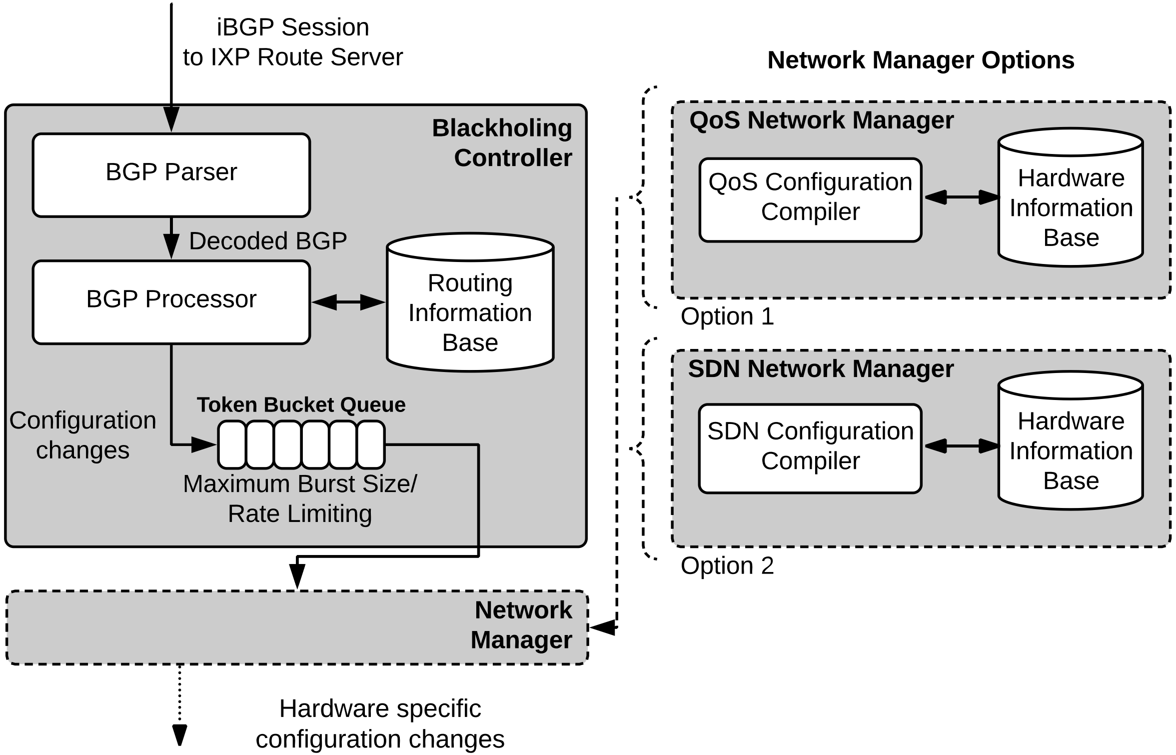
Advanced Blackholing System



Advanced Blackholing System



Advanced Blackholing Signaling (BGP part)



Building Blocks

✓ → Granularity

- UDP, TCP, Ports, …

✓ → Signaling complexity

- BGP communities or API

✓ → Cooperation

- Enforced by IXP

✓ → Telemetry

- Monitoring with statistics

✓ → Scalability

- Line-rate in hardware

✓ → Cost

- Implemented in existing hardware

Implementation Challenges

→ BGP processing

→ Configuration proxy

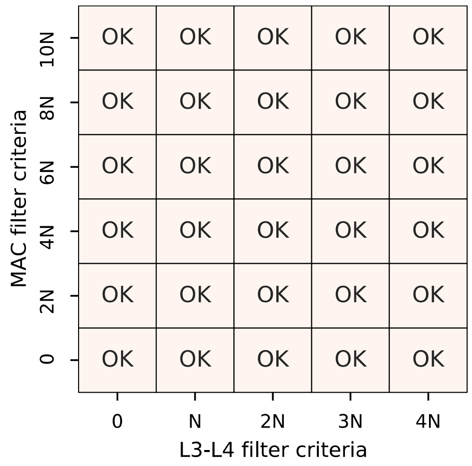
→ Why not FlowSpec?

Does it Scale?

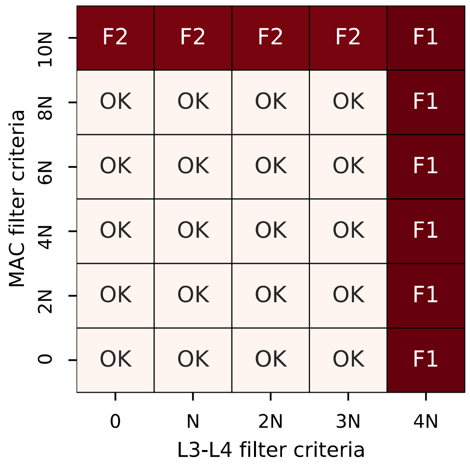
- Scalability wrt. number of filters & IXP ports (of switches/routers)
  - TCAM to match header fields
  - System limits & port limits (total/max no. of filters per port)
  - Results on next slide

- Scalability wrt. configuration update frequency limits (of config proxy)
  - Allows 4.33 filter updates per second
  - 70% of BH updates below 1 second

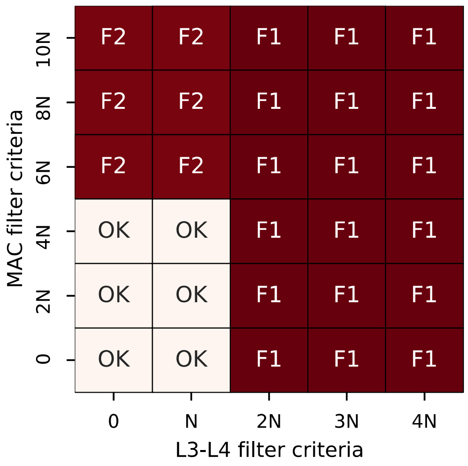
Stress Test on the IXP's Hardware



20% of IXP member ASes



60% of IXP member ASes

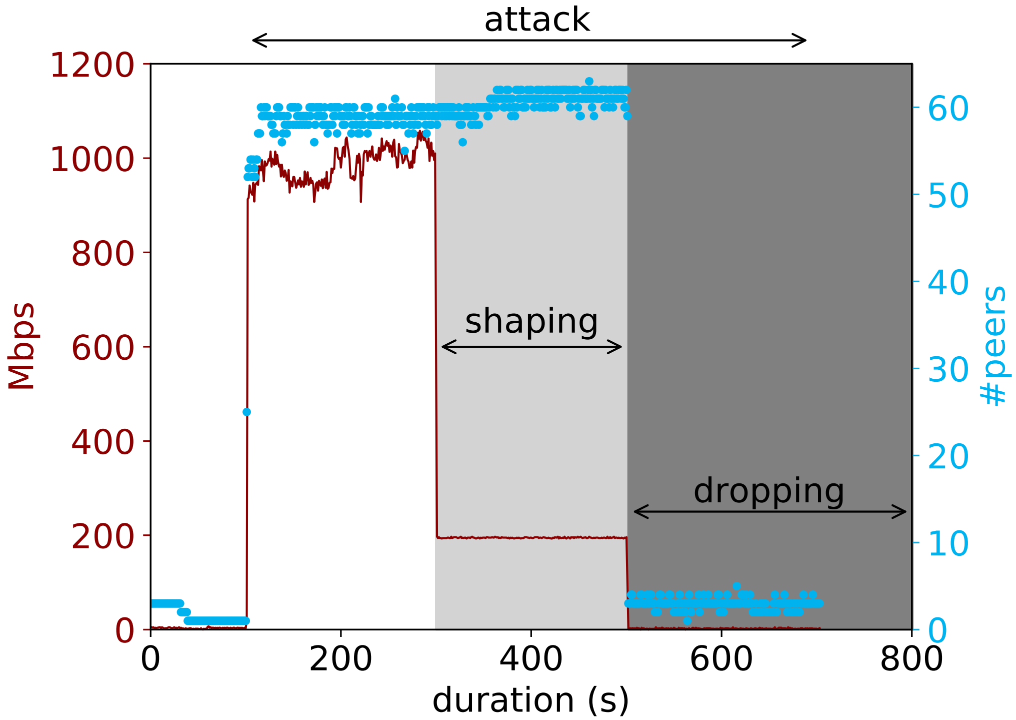


100% of IXP member ASes

Measurement Experiment

- How "effective" is it
  - NTP DDoS attack
  - AS at IXP via ML peering
  - Attacks for 10 min to /32

- Drop / shape UDP NTP
- Traffic: 1000 to 200 to 0 Mbps
- Peers: 60 to (almost) 0



Summary

→ A number of DDoS mitigation solutions exist, but …

→ We identify and measure Blackholing limitations

→ We propose Advanced Blackholing, combining the benefits and overcome problems of today's DDoS defense

→ We implement a new system with a BGP and API interface

→ We evaluated and proved good scales scaling

Q & A

matthias (dot) wichtlhuber (at) de-cix.net

Stellar: Network Attack Mitigation using Advanced Blackholing

Christoph Dietzel
TU Berlin/DE-CIX
christoph@inet.tu-berlin.de

Matthias Wichtlhuber
DE-CIX
matthias.wichtlhuber@rnd.de-cix.net

Georgios Smaragdakis
TU Berlin
georgios@inet.tu-berlin.de

Anja Feldmann
Max Planck Institute for Informatics
anja@mpi-inf.mpg.de

ABSTRACT

Network attacks, including Distributed Denial-of-Service (DDoS), continuously increase in terms of bandwidth along with damage (recent attacks exceed 1.7 Tbps) and have a devastating impact on the targeted companies/governments. Over the years, mitigation techniques, ranging from blackholing to policy-based filtering at routers, and on to traffic scrubbing, have been added to the network operator's toolbox. Even though these mitigation techniques provide some protection, they either yield severe collateral damage, e.g., dropping legitimate traffic (blackholing), are cost-intensive, or do not scale well for Tbps level attacks (ACL filtering, traffic scrubbing), or require cooperation and sharing of resources (Flowspec).

In this paper, we propose Advanced Blackholing and its system realization Stellar. Advanced blackholing builds upon the scalability of blackholing while limiting collateral damage by increasing its granularity. Moreover, Stellar reduces the required level of cooperation to enhance mitigation effectiveness. We show that fine-grained blackholing can be realized, e.g., at a major IXP, by combining available hardware filters with novel signaling mechanisms. We evaluate the scalability and performance of Stellar at a large IXP that interconnects more than 800 networks, exchanges more than 6 Tbps traffic, and witnesses many network attacks every day. Our results show that network attacks, e.g., DDoS amplification attacks, can be successfully mitigated while the networks and services under attack continue to operate untroubled.

CCS CONCEPTS

• **Networks** → **Denial-of-service attacks**; *Network components*; *Network measurement*; *Network services*;

KEYWORDS

BGP; IXP; Blackholing; DDoS Mitigation.

1 INTRODUCTION

The revolution of the digital age fueled by the Internet has attracted the good but the evil alike. While the threats executed over the Internet are multifaceted from a criminalistics perspective, e.g., fraud [...] is generated and steered towards a target service to make it unavailable. Once the network links to the target are congested due to the DDoS attack, legitimate traffic that traverses the same links is also affected.

DDoS threats are continuously increasing in terms of volume, frequency, and complexity. While the largest observed and publicly reported attacks were between 50 to 200 Gbps before 2015 [59, 60, 70], current peaks are an order of magnitude higher and exceeded 1 Tbps [9, 48] in 2016, and 1.7 Tbps [57] in early 2018. We also observe a massive rise in the number of DDoS attacks. Jonker et al. [41] report that a third of all active /24 networks were targeted by DDoS attacks between 2016 and 2017. Similar observations are reported by the security industry [3, 19]. A particularly prominent DDoS attack type is amplification attacks [64, 65]. They take advantage of protocol design flaws, whereby a relatively small request triggers a significantly larger response. With a spoofed source IP address [49] the response traffic is amplified and reflected to the target. Vulnerable protocols include classical protocols such as NTP, DNS, and/or SNMP [20, 64], as well as relatively new protocols, e.g., DNSSEC [74] and memcached [5, 57]. Amplification factors of up to 50, 000× have been witnessed in the wild [73]. To exemplify, a request of 15 bytes can trigger a 750 Kbytes response.

1.1 DDoS Mitigation: State of the Art

This alarming increase in DDoS attacks and their sophistication and severity, e.g., see [56, 77], demands scalable yet cost-effective countermeasures. However, at this point, we are left with various mitigation techniques and tools that can *partially* counteract the impact of the attacks. These include: (i) *Traffic Scrubbing Services (TSS)*, (ii) *Router Access Control List Filters (ACL)*, (iii) *Remotely Triggered Black Hole (RTBH)*, and (iv) *BGP Flowspec*.

Traffic Scrubbing Services (TSS): offer all-round carefree services to their subscribers. They redirect the traffic of a service to specialized hardware either via DNS redirection or BGP delegation [43]. There they classify traffic as unwanted or benign and send the benign "scrubbed" traffic to its original destination or move