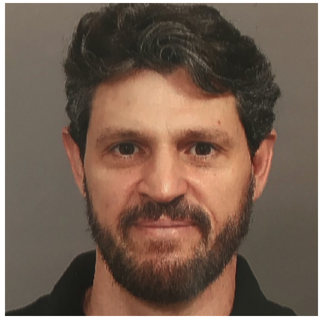
First CONCORDIA Workshop on Collaborative DDoS Mitigation
15 September 2022

Anycast Agility: Network Playbooks to Fight DDoS



ASM Rizvi*
USC/ISI

Leandro Bertholdo*
University of Twente

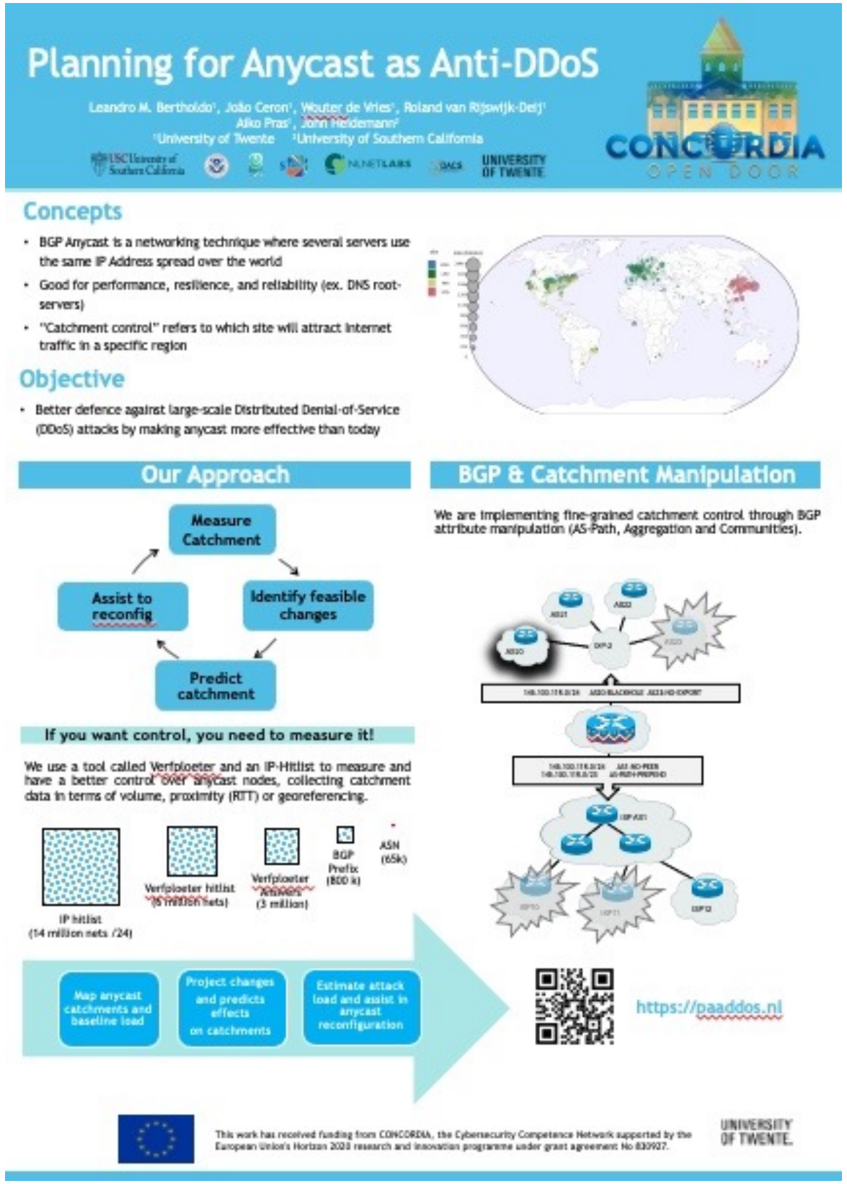
Joao M Ceron
SIDN Labs

John Heidemann
USC/ISI

* Indicates equal contribution

CONCORDIA Poster 2019

Planning for Anycast as Anti-DDoS



Planning for Anycast as Anti-DDoS

Leandro M. Bertholdo[1], João Ceron[1], Wouter de Vries[1], Roland van Rijswijk-Deij[1]
Aiko Pras[1], John Heidemann[2]
[1]University of Twente [2]University of Southern California

Concepts

- BGP Anycast is a networking technique where several servers use the same IP Address spread over the world
- Good for performance, resilience, and reliability (ex. DNS root-servers)
- "Catchment control" refers to which site will attract Internet traffic in a specific region

Objective

- Better defence against large-scale Distributed Denial-of-Service (DDoS) attacks by making anycast more effective than today

Our Approach

Measure Catchment → Identify feasible changes → Predict catchment → Assist to reconfig → Measure Catchment

If you want control, you need to measure it!

We use a tool called Verfploeter and an IP-Hitlist to measure and have a better control over anycast nodes, collecting catchment data in terms of volume, proximity (RTT) or georeferencing.

IP hitlist (14 million nets /24)
Verfploeter hitlist (6 million nets)
Verfploeter Answers (3 million)
BGP Prefix (800 k)
ASN (65k)

Map anycast catchments and baseline load → Project changes and predicts effects on catchments → Estimate attack load and assist in anycast reconfiguration

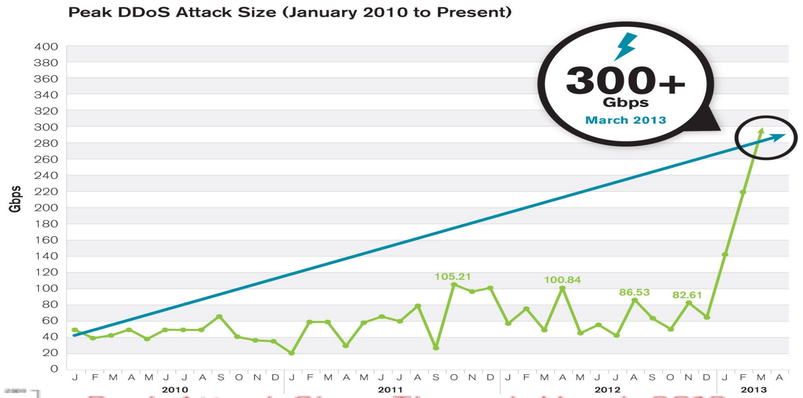
BGP & Catchment Manipulation

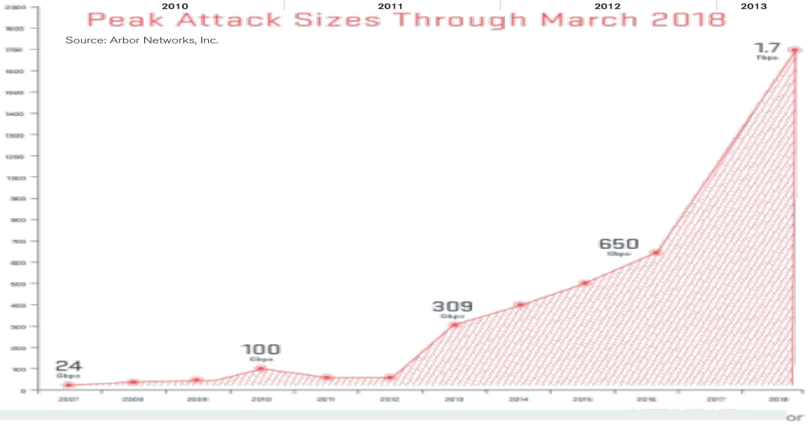
We are implementing fine-grained catchment control through BGP attribute manipulation (AS-Path, Aggregation and Communities).

https://paaddos.nl

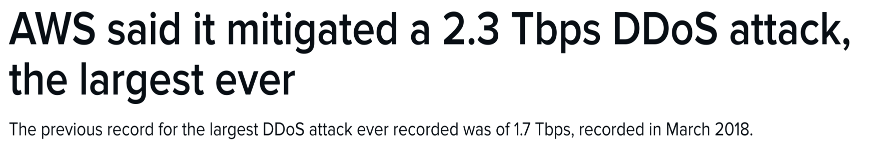
This work has received funding from CONCORDIA, the Cybersecurity Competence Network supported by the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

Distributed Denial-of-Service (DDoS) is Bad... and Getting Worse





Source: Arbor Networks, Inc.

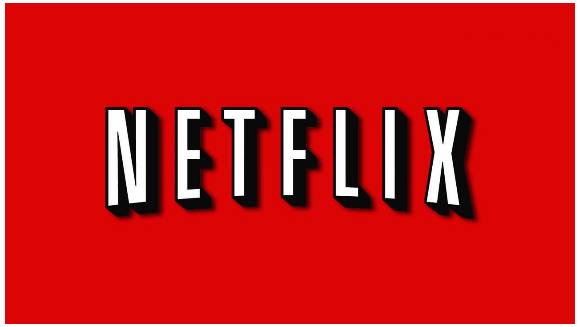


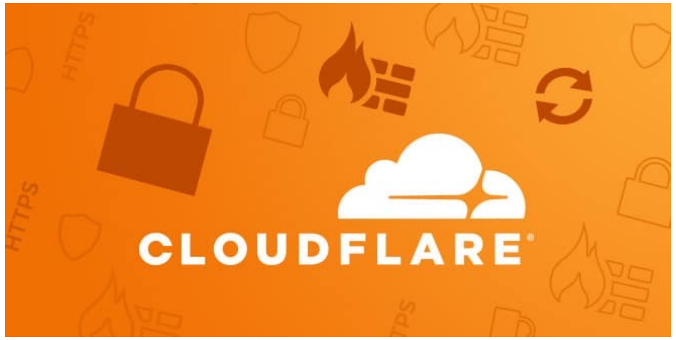
AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever

The previous record for the largest DDoS attack ever recorded was of 1.7 Tbps, recorded in March 2018.

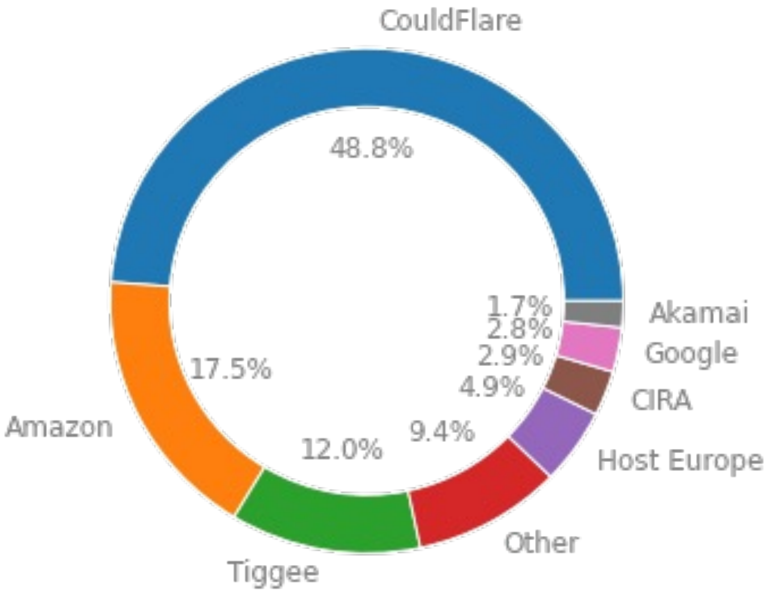
- DDoS is big
  - – Botnets
- DDoS is getting bigger
  - – Github 1.35Tbps → Amazon gets 2.3 Tbps
  - **– IoT & CPE devices**
  - **– Reflection attacks from Cloudproviders**
- DDoS-as-a-service is cheap
  - – starting at $1/attack [Santanna et al, 2015]

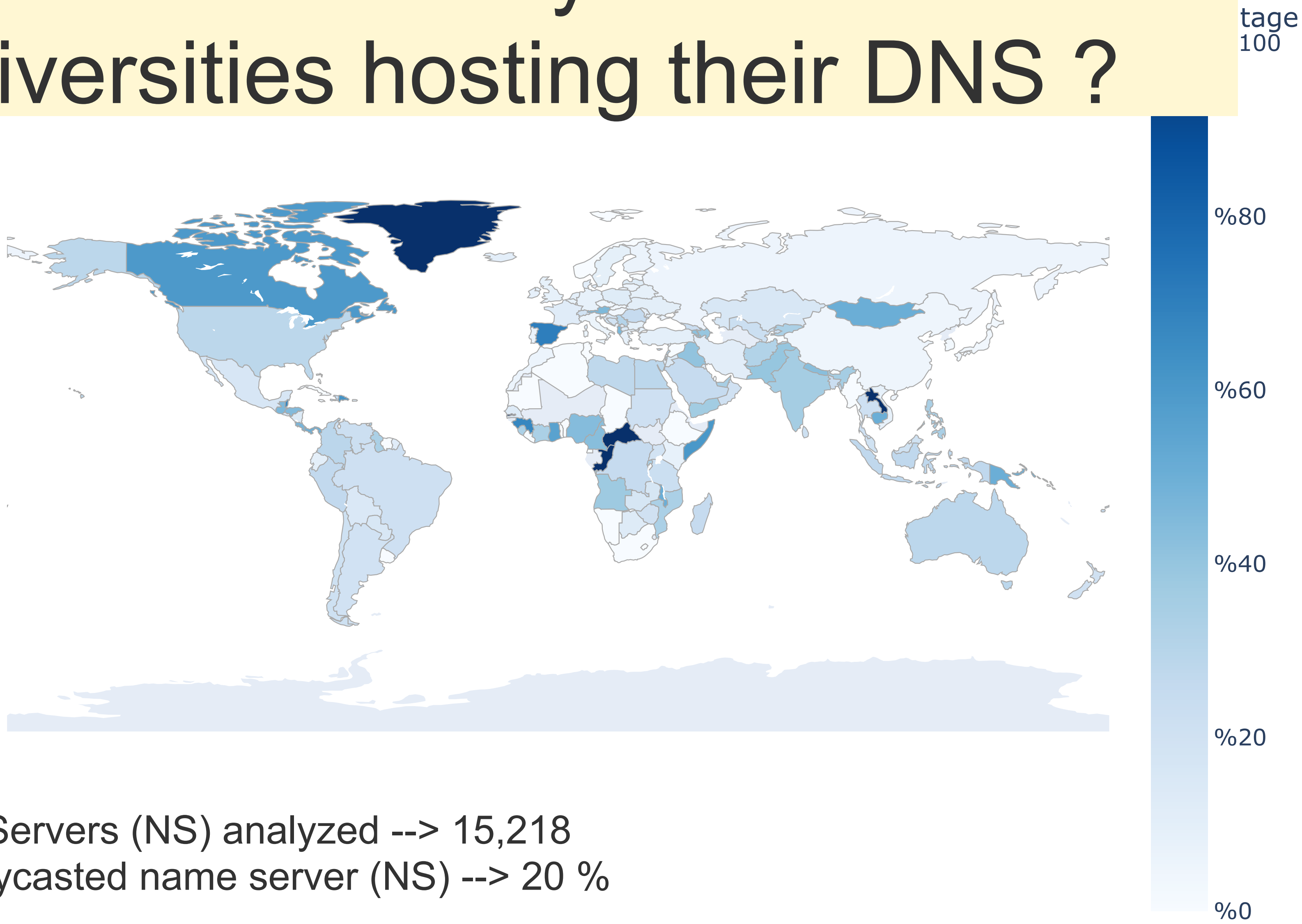
Why anycast?
Where do you use anycast in your daily life?





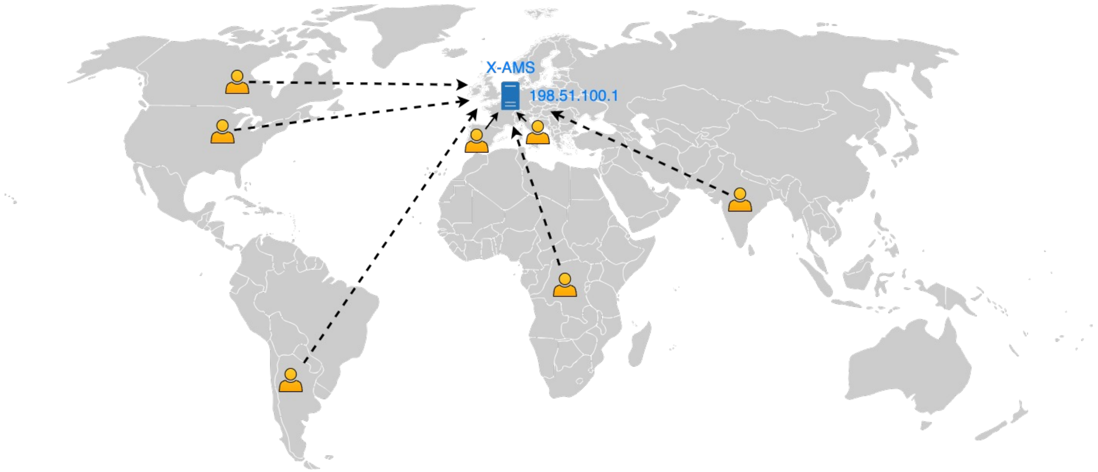
DNS case study:
Where are universities hosting their DNS ?



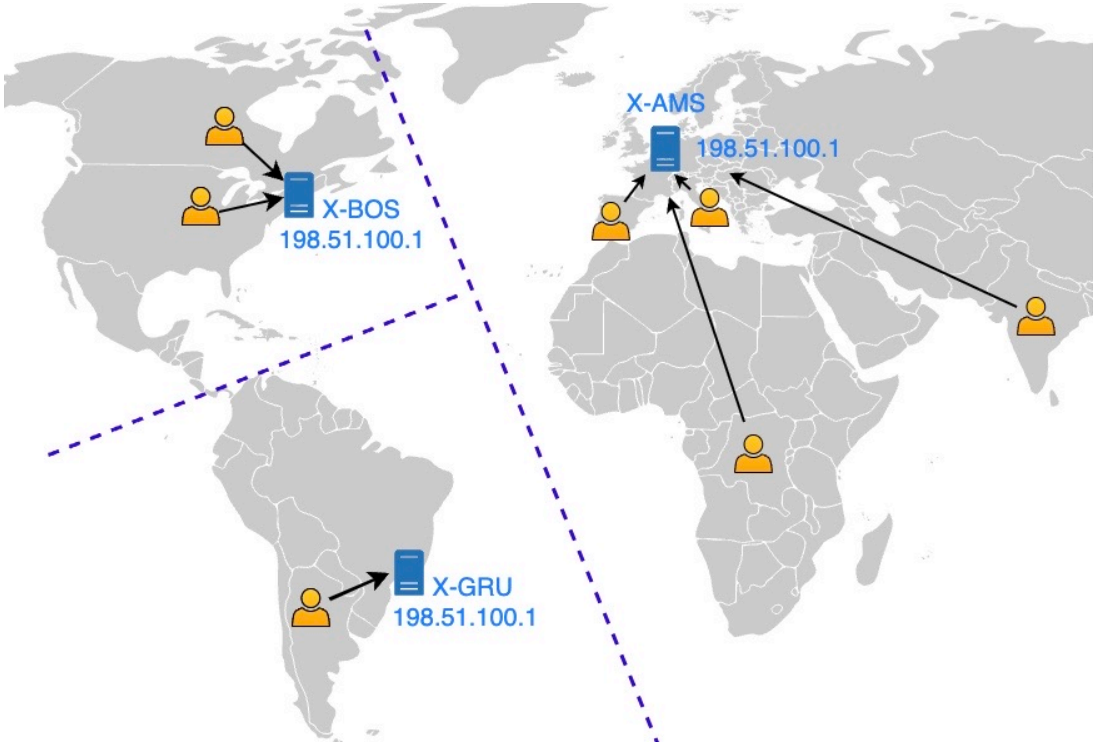


University Name Servers (NS) analyzed --> 15,218
University with anycasted name server (NS) --> 20 %

How Anycast works

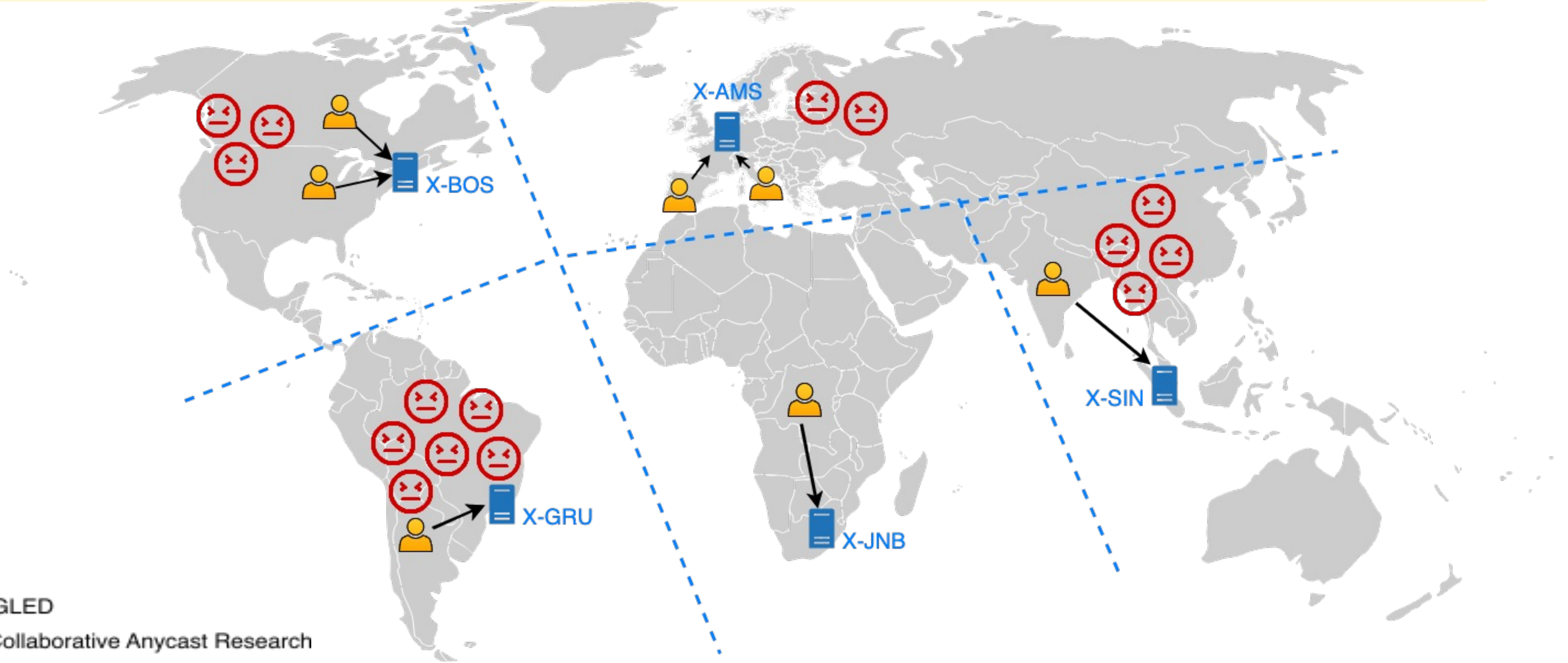


Unicast Service



Anycast Service

-- Anycast as a defense mechanism -- more sites the better resilience !



TANGLED
A Testbed for Collaborative Anycast Research

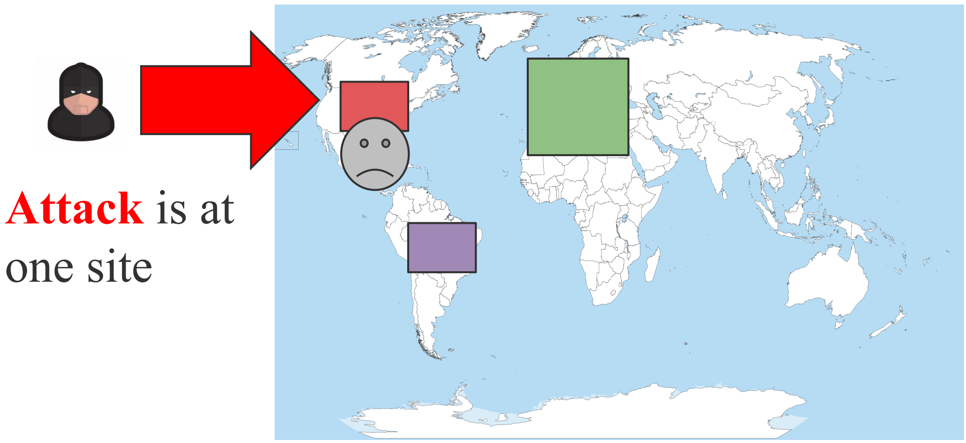
What we did…

https://youtu.be/ie5Gt7giMLw

Let's look the path to get there…

What happen in a DDoS Attack?

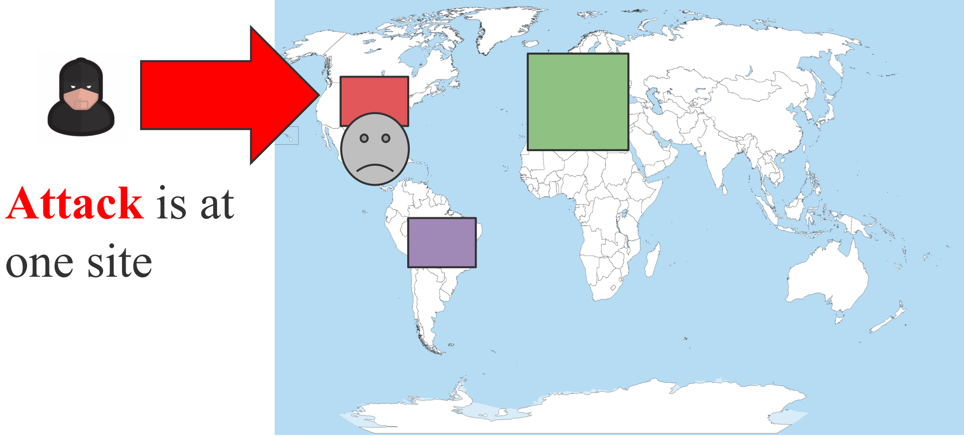
One site is **overwhelmed**



Attack is at one site

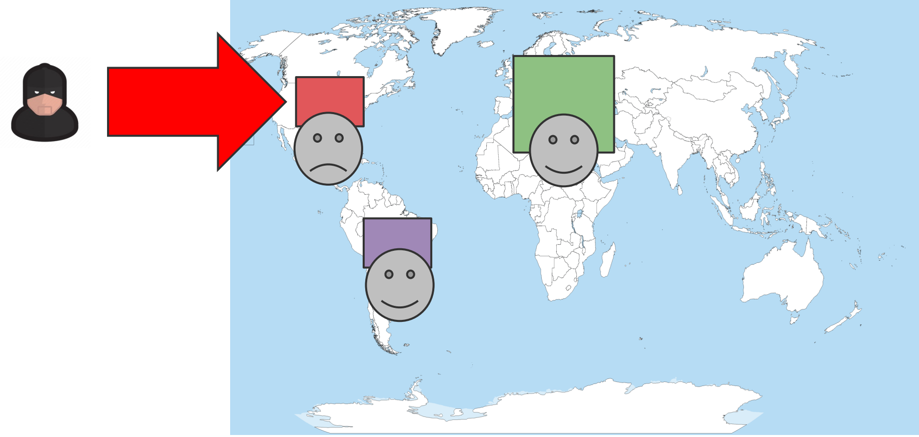
How to defend? 1- Absorb at One Site

One site is **overwhelmed**



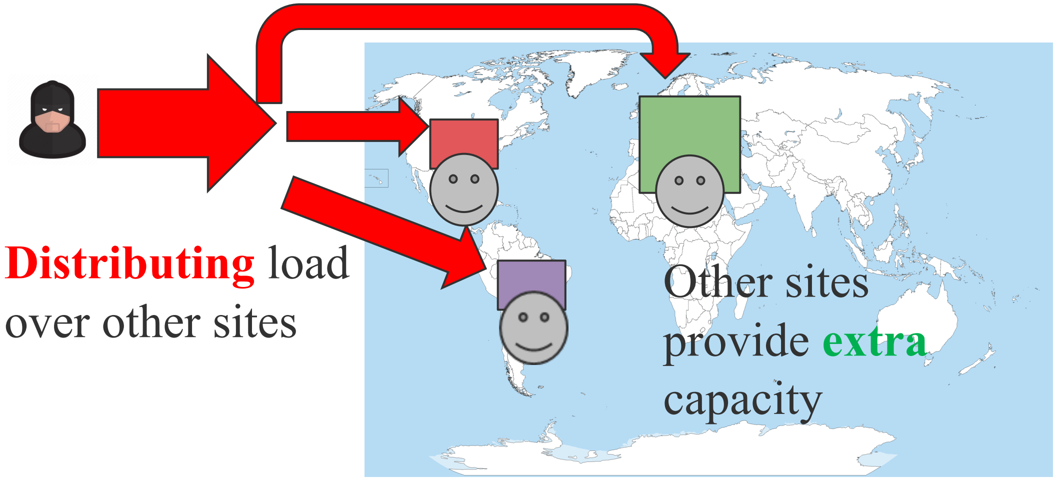
Attack is at one site

One site is hurt, but others are OK!



2- Spread Traffic 3- Shift Traffic

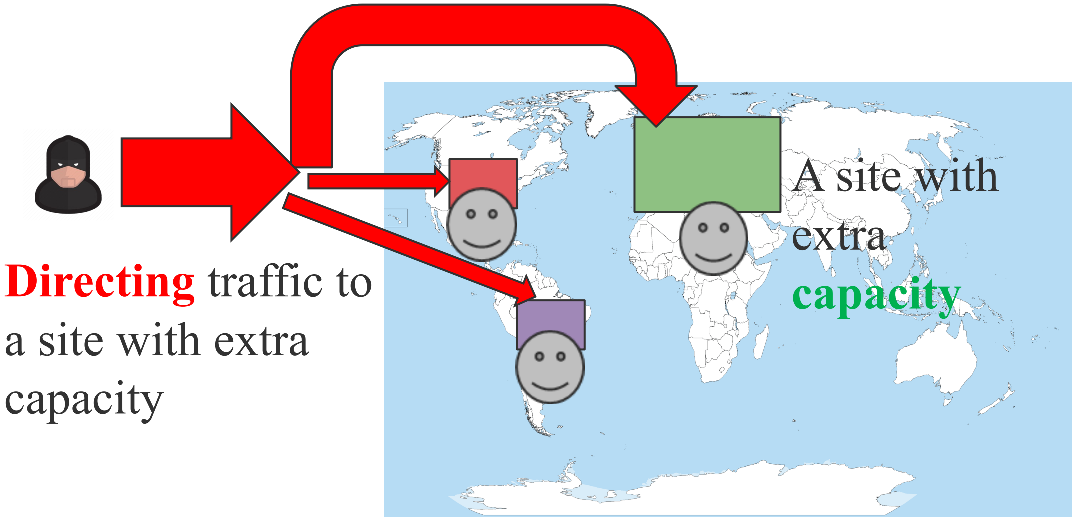
Rebalance the Network based on capacity



Distributing load over other sites

Other sites provide **extra** capacity

Shift to larger sites with spare/elastic capacity

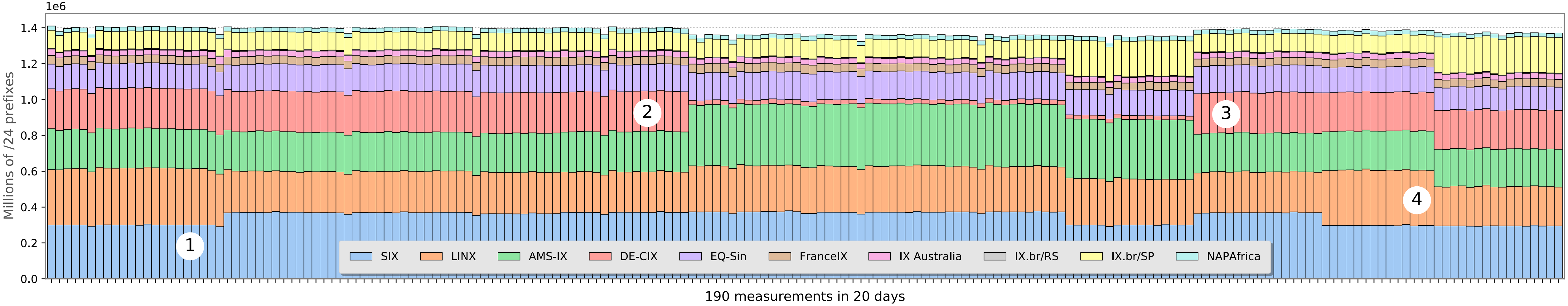


Directing traffic to a site with extra capacity

A site with extra **capacity**

How does the redistribution? **BGP is unpredictable !**

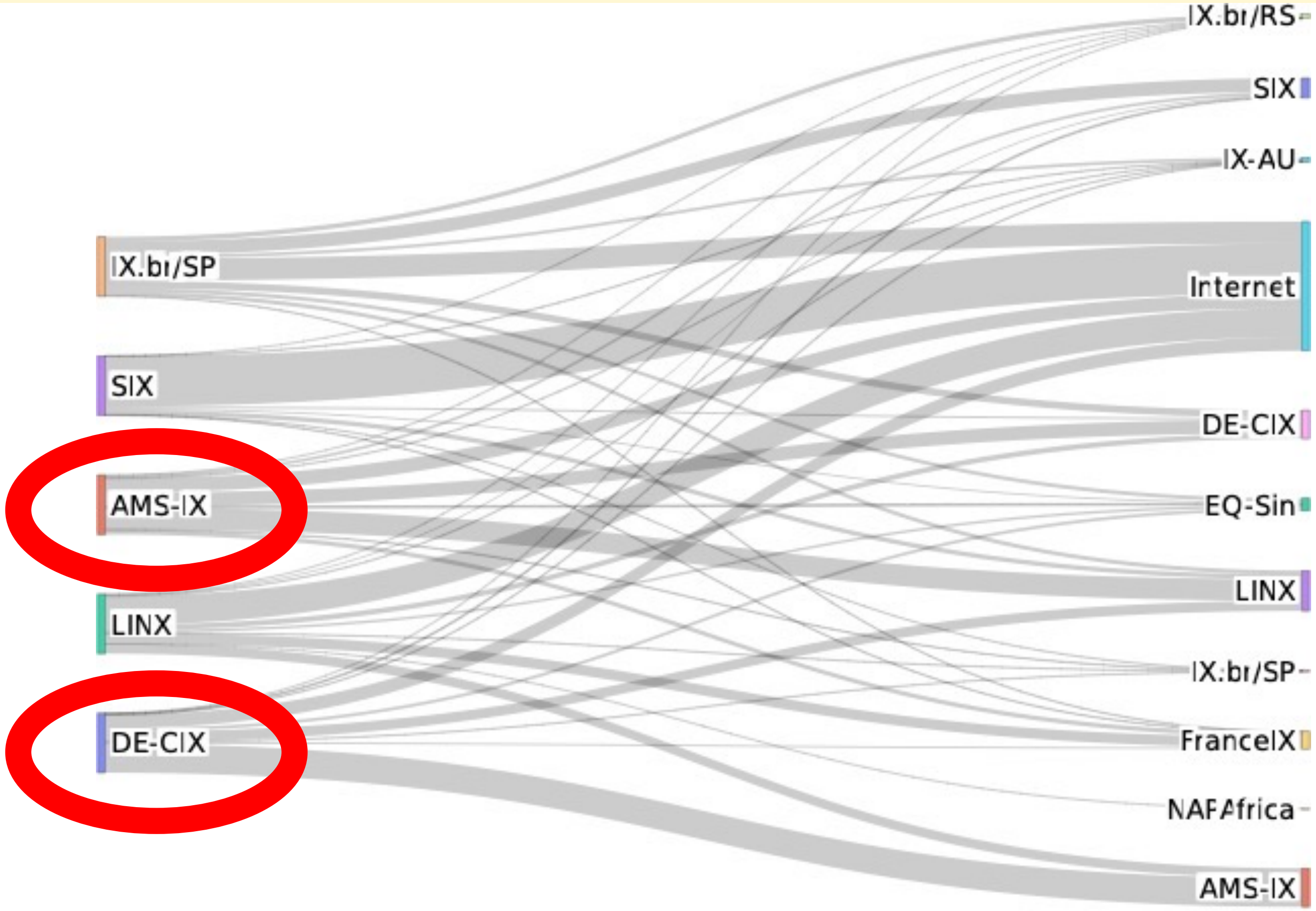
What do you mean by “BGP unpredictable”?



TANGLED

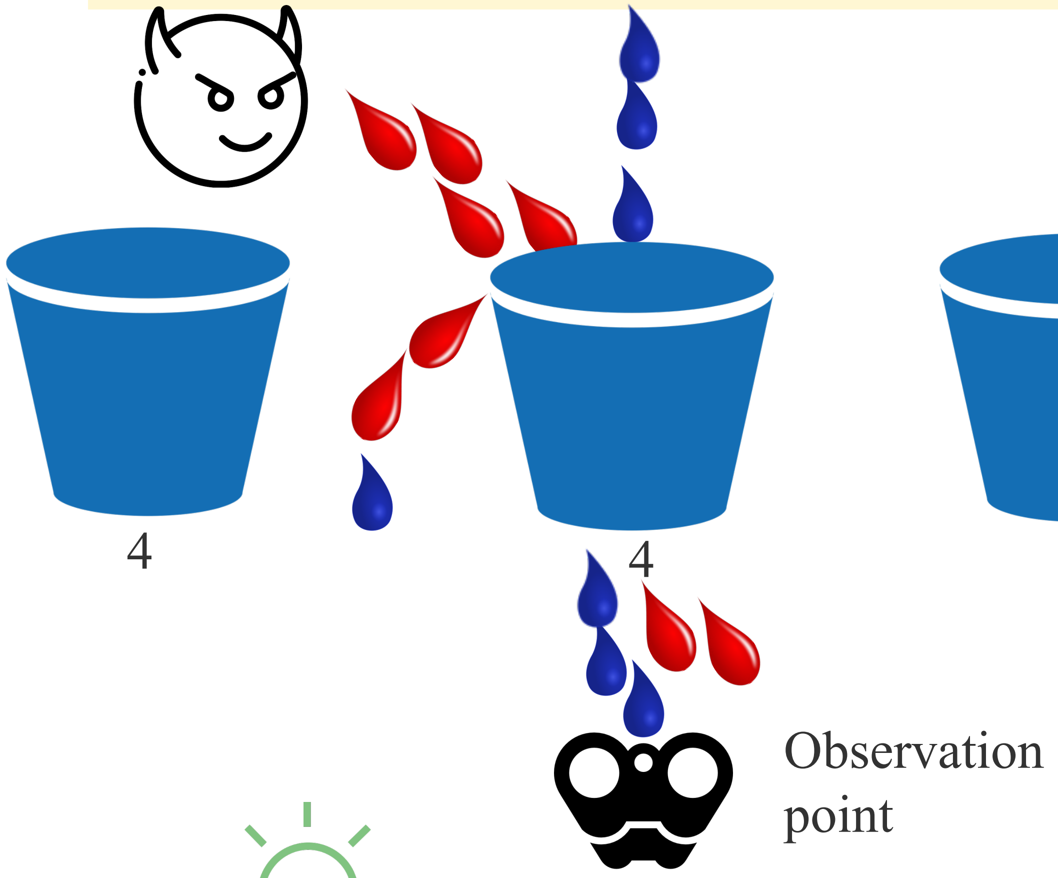
A Testbed for Collaborative Anycast Research

What do you mean by “BGP unpredictable”?



The Challenges

Challenge 1: Unknown Load

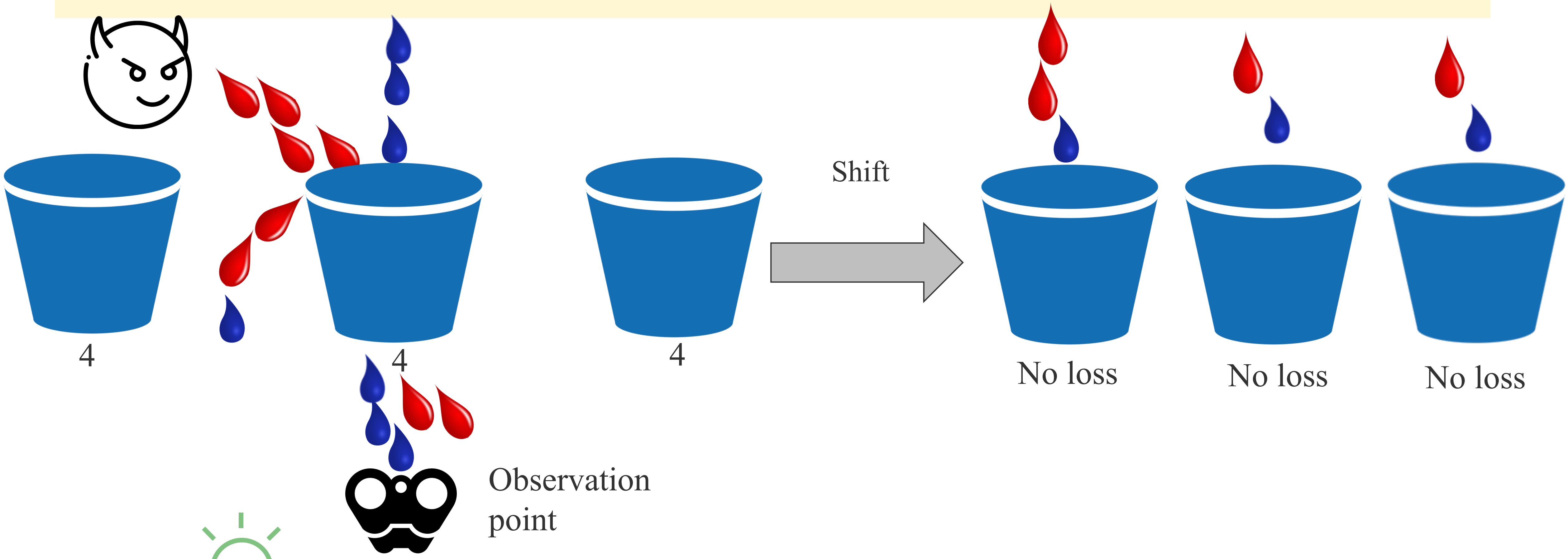


- What you see is
  - At full capacity: 50% attack traffic
- The truth is
  - At 175% capacity
  - 100% attack traffic
  - 75% legitimate
  - Lost 25% of legitimate traffic

Site observation under-estimates attack

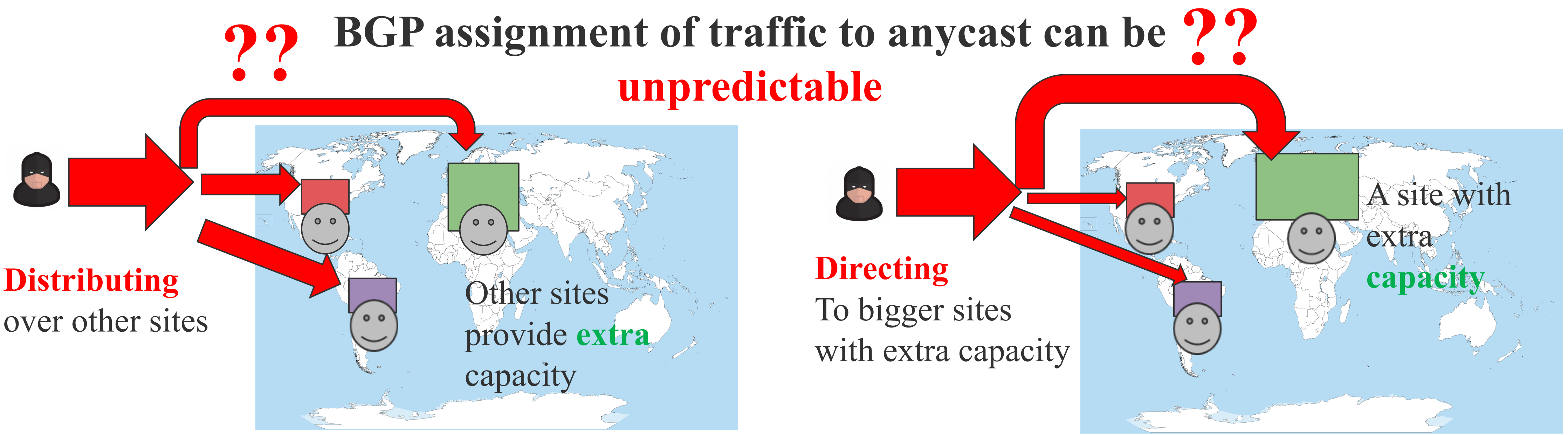
Our **contribution**: proposing a way to estimate the **attack x offered load**

Challenge 2: Controlled Traffic Engineering



Our **contribution**: we help the operator to get the **right** shift

Challenge 3: How to redistribute?



BGP assignment of traffic to anycast can be unpredictable

Distributing over other sites

Other sites provide **extra** capacity

Directing To bigger sites with extra capacity

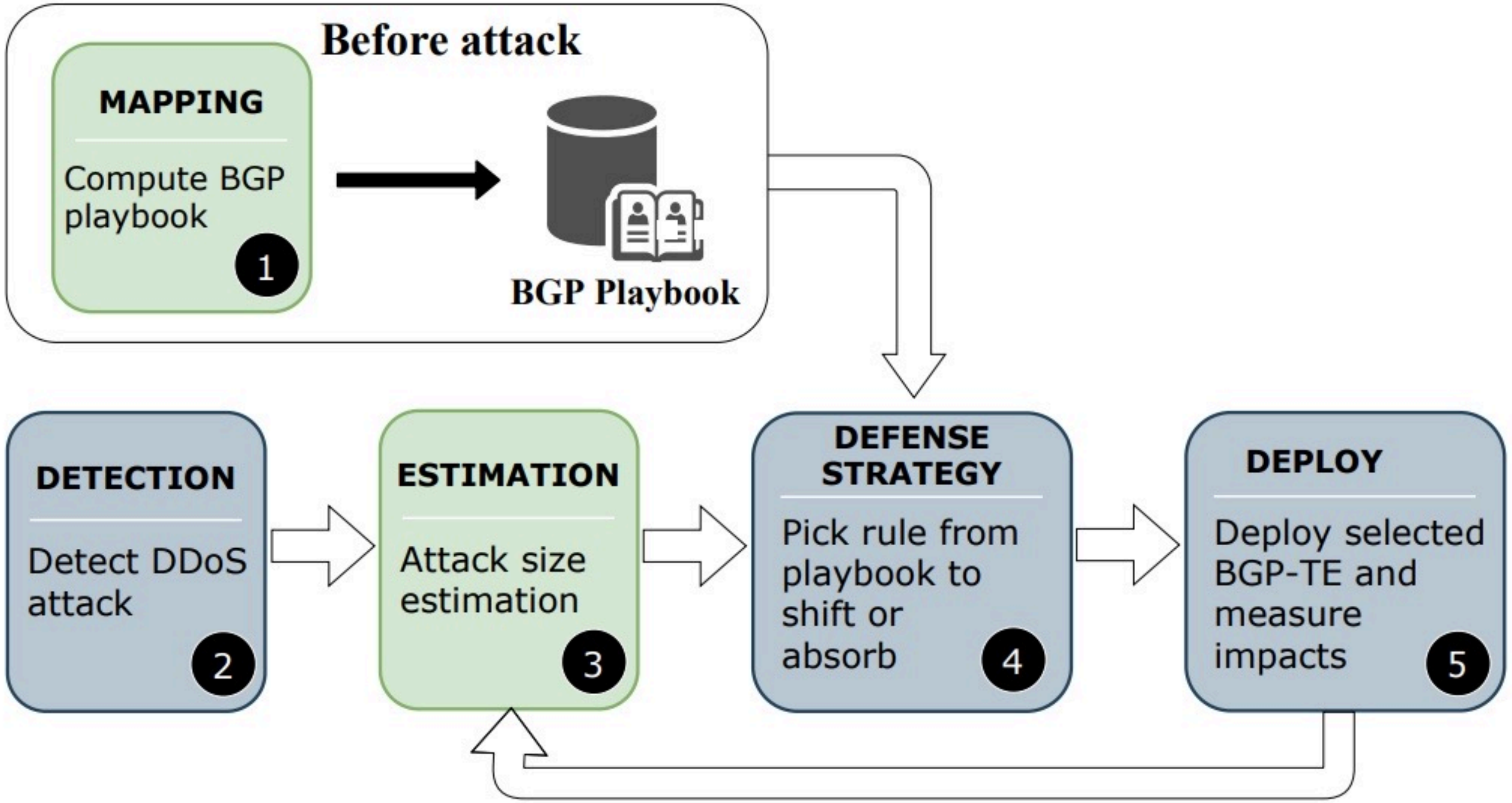
A site with extra **capacity**

Our **contribution**: how to build a **BGP playbook** to predict anycast ahead of time

Our Contribution

- New approach to **estimate the load** (challenge 1)
  - **Allows us to plan a defense**
- Define a method to build **BGP playbook** (challenge 2)
  - Allows us to **execute the correct defense**
- Show a **BGP playbook works in a real DDoS event** (challenge 3)
  - **Effectiveness of our approach in real attacks.**

How it works?



Before attack

MAPPING

Compute BGP playbook

1

BGP Playbook

DETECTION

Detect DDoS attack

2

ESTIMATION

Attack size estimation

3

DEFENSE STRATEGY

Pick rule from playbook to shift or absorb

4

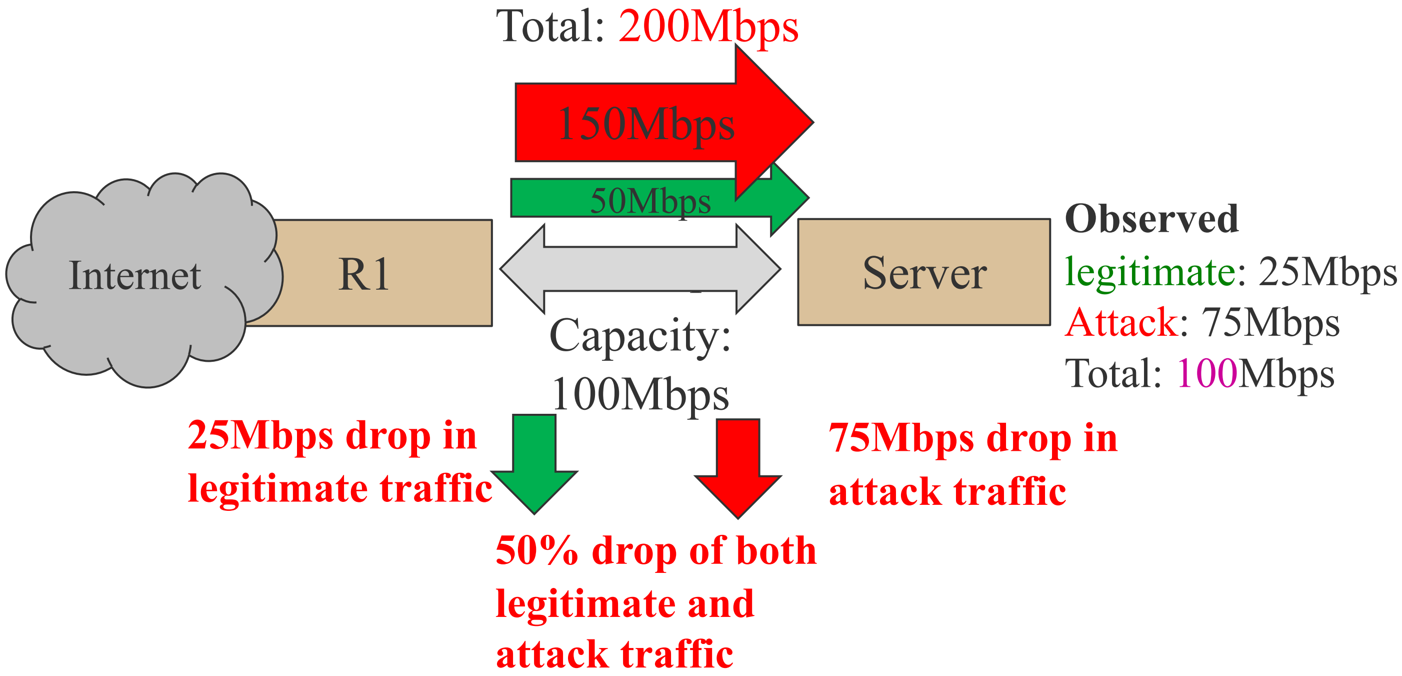
DEPLOY

Deploy selected BGP-TE and measure impacts

5

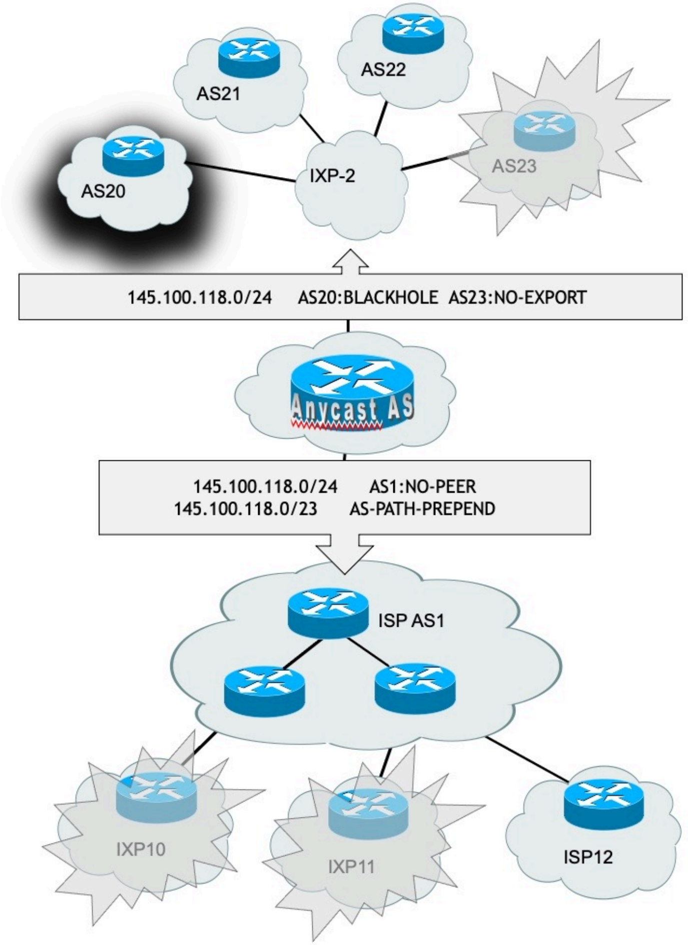
Methodology: Estimating Load

- **Problem:**
  - **upstream loss is invisible**
- Insight:
  - **Heavy hitters**
  - Sites have predictable known good traffic
  - Infer attack size by change in this traffic

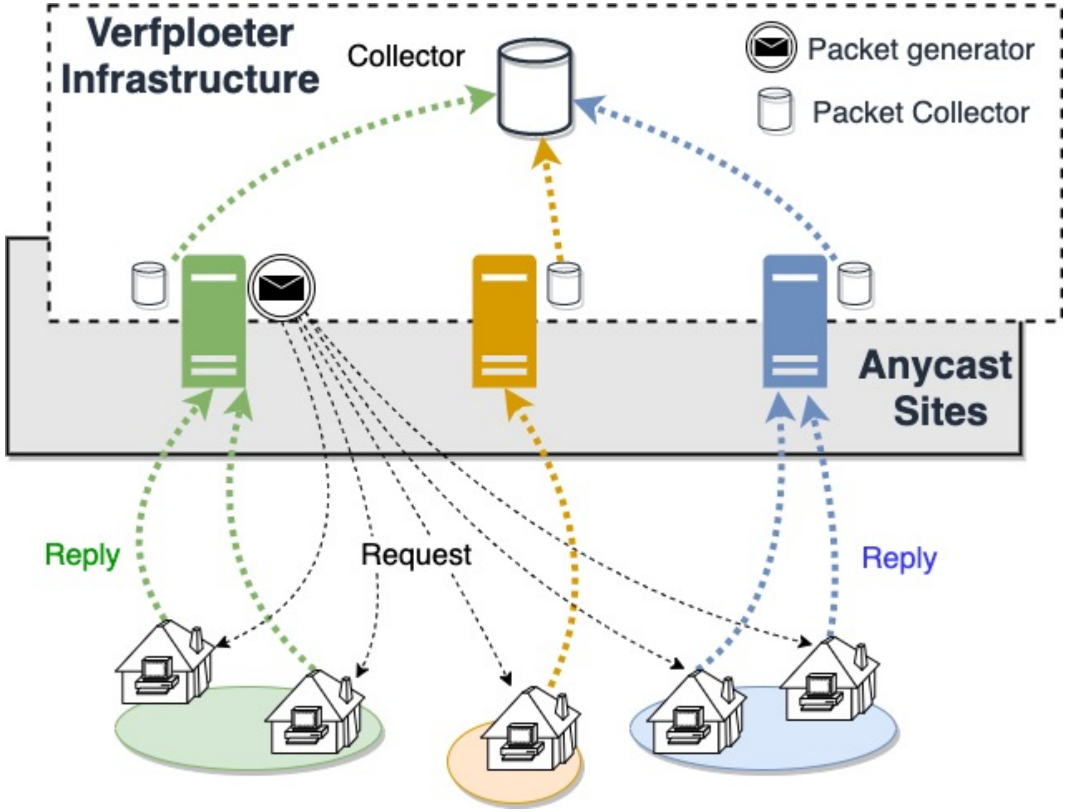


Methodology: Understanding Traffic Engineering (TE)

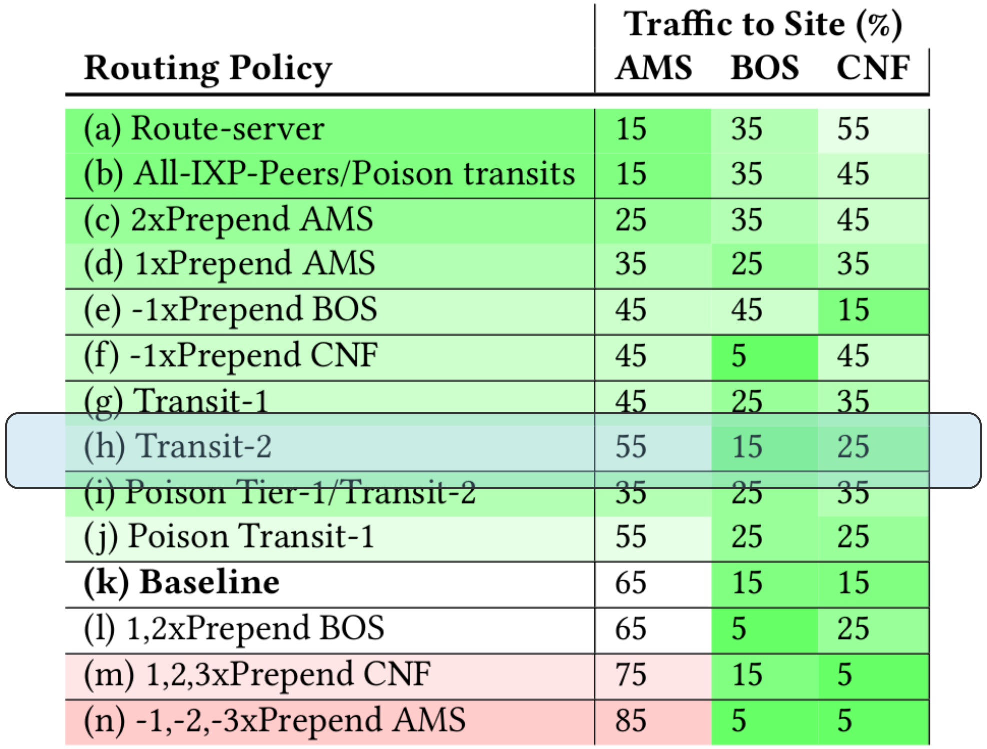
- We used three TE techniques
- Each TE method has tradeoffs (details in section 6)
  - Path prepending
    - Available in all sites
    - no granular control
  - Community strings
    - Not available in all sites
    - provide granular control
  - Path poisoning
    - Filtered when poisoning Tier-1 Ases
    - provide limited control


AS21
AS22
AS20
IXP-2
AS23
145.100.118.0/24 AS20:BLACKHOLE AS23:NO-EXPORT
Anycast AS
145.100.118.0/24 AS1:NO-PEER
145.100.118.0/23 AS-PATH-PREPEND
ISP AS1
IXP10
IXP11
ISP12

How we evaluate TE impact ?



How a playbook looks like?



Routing Policy	Traffic to Site (%)		
	AMS	BOS	CNF
(a) Route-server	15	35	55
(b) All-IXP-Peers/Poison transits	15	35	45
(c) 2xPrepend AMS	25	35	45
(d) 1xPrepend AMS	35	25	35
(e) -1xPrepend BOS	45	45	15
(f) -1xPrepend CNF	45	5	45
(g) Transit-1	45	25	35
(h) Transit-2	55	15	25
(i) Poison Tier-1/Transit-2	35	25	35
(j) Poison Transit-1	55	25	25
(k) Baseline	65	15	15
(l) 1,2xPrepend BOS	65	5	25
(m) 1,2,3xPrepend CNF	75	15	5
(n) -1,-2,-3xPrepend AMS	85	5	5

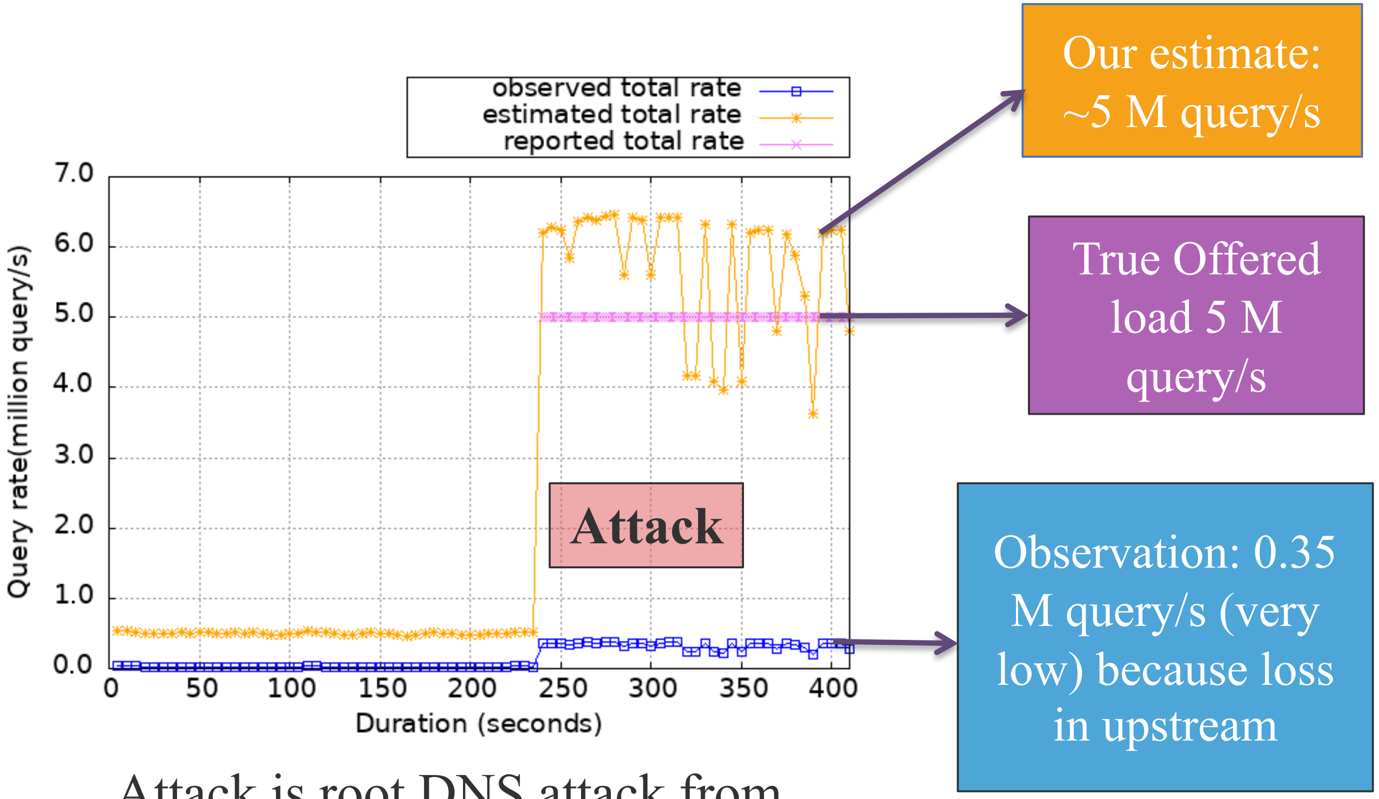
A sample playbook

Announcing only to **Transit-2:**
AMS: 55% traffic
BOS: 15% traffic
CNF: 25% traffic

Validation and Results

Offered Load Estimates are Accurate

- Question: **does estimation work?**
- Experiment:
  - **Replayed packet trace**
  - Measured observed traffic rate and access fraction to estimate
  - Compared the estimation with the reported rate
- **Answer: yes**



Our estimate: ~5 M query/s

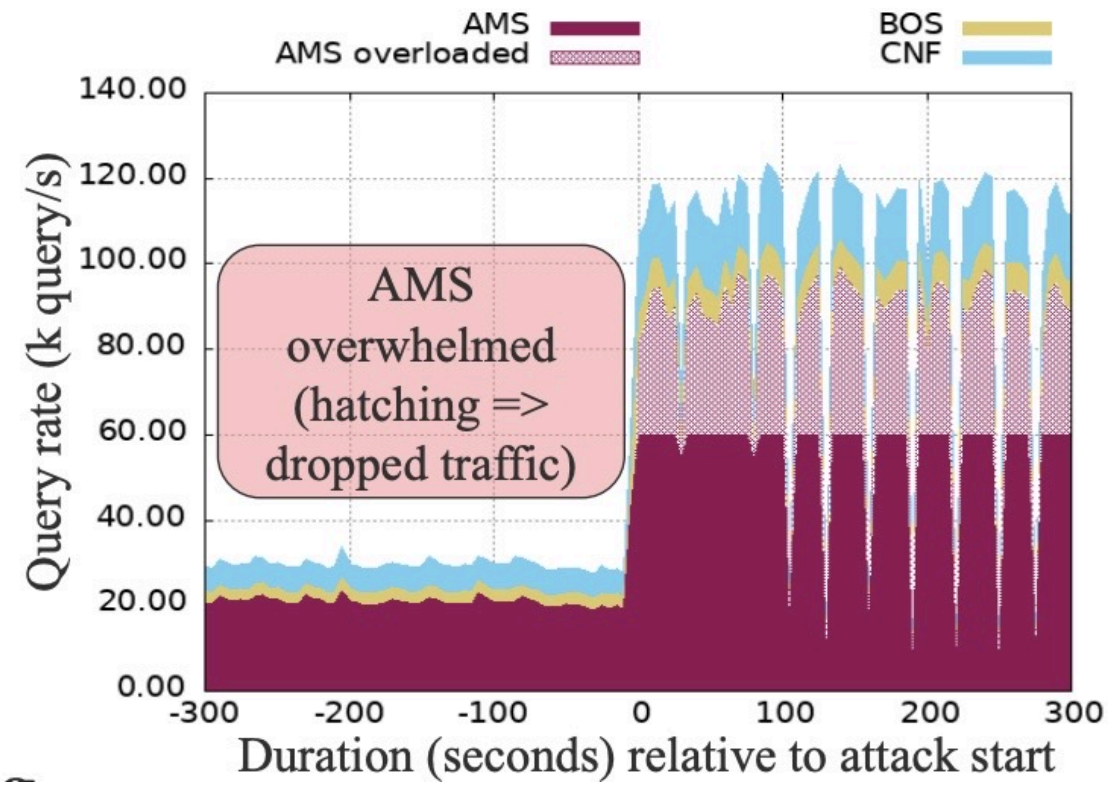
True Offered load 5 M query/s

Observation: 0.35 M query/s (very low) because loss in upstream

Attack is root DNS attack from 2015-11-30 with data from B-root

Using a Playbook to Defend

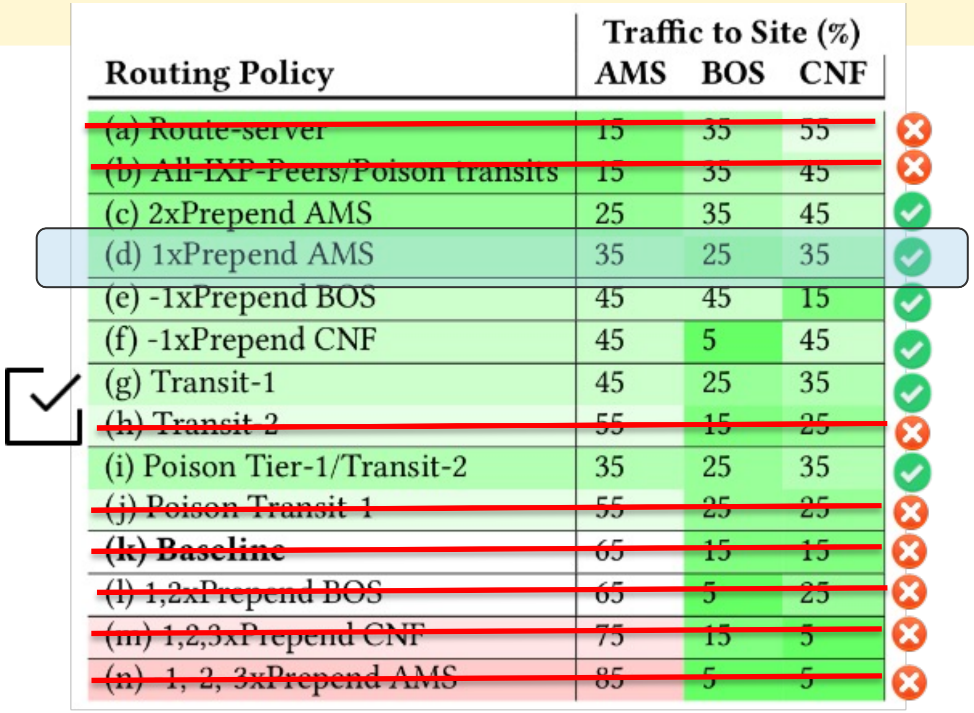
- **Question: how to use a playbook during an attack?**
- Experiment:
  - Simulate a DNS attack
    - B-root event from 2017-03-06
    - More events in section 8 of the paper
  - Against a 3-site anycast system
    - Each site has ~60k queries/s capacity



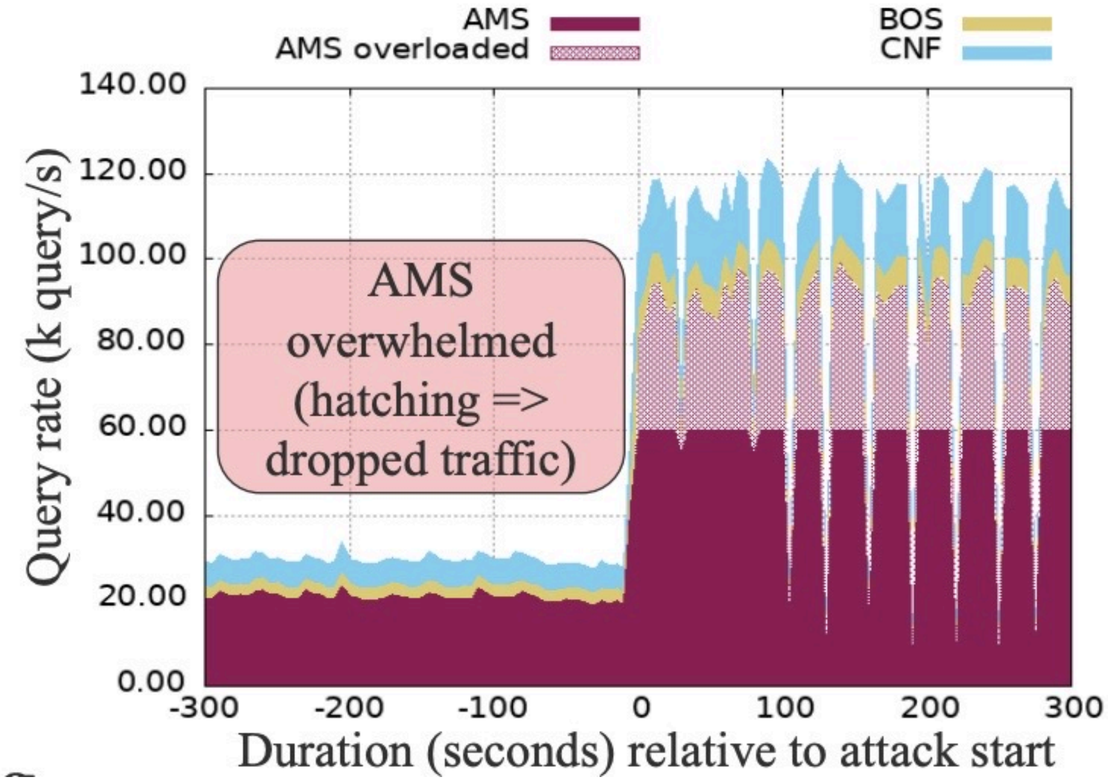
AMS overwhelmed (hatching => dropped traffic)

Let’s look at the BGP playbook.

Solution: Playbook to Get Routing Options



Routing Policy	Traffic to Site (%)			
	AMS	BOS	CNF	
~~(a) Route-server~~	~~15~~	~~35~~	~~55~~	✗
~~(b) All-IXP-Peers/Poison transits~~	~~15~~	~~35~~	~~45~~	✗
(c) 2xPrepend AMS	25	35	45	✓
(d) 1xPrepend AMS	35	25	35	✓
(e) -1xPrepend BOS	45	45	15	✓
(f) -1xPrepend CNF	45	5	45	✓
(g) Transit-1	45	25	35	✓
~~(h) Transit-2~~	~~55~~	~~15~~	~~25~~	✗
(i) Poison Tier-1/Transit-2	35	25	35	✓
~~(j) Poison Transit-1~~	~~55~~	~~25~~	~~25~~	✗
~~**(k) Baseline**~~	~~65~~	~~15~~	~~15~~	✗
~~(l) 1,2xPrepend BOS~~	~~65~~	~~5~~	~~25~~	✗
~~(m) 1,2,3xPrepend CNF~~	~~75~~	~~15~~	~~5~~	✗
~~(n) -1, 2, 3xPrepend AMS~~	~~85~~	~~5~~	~~5~~	✗

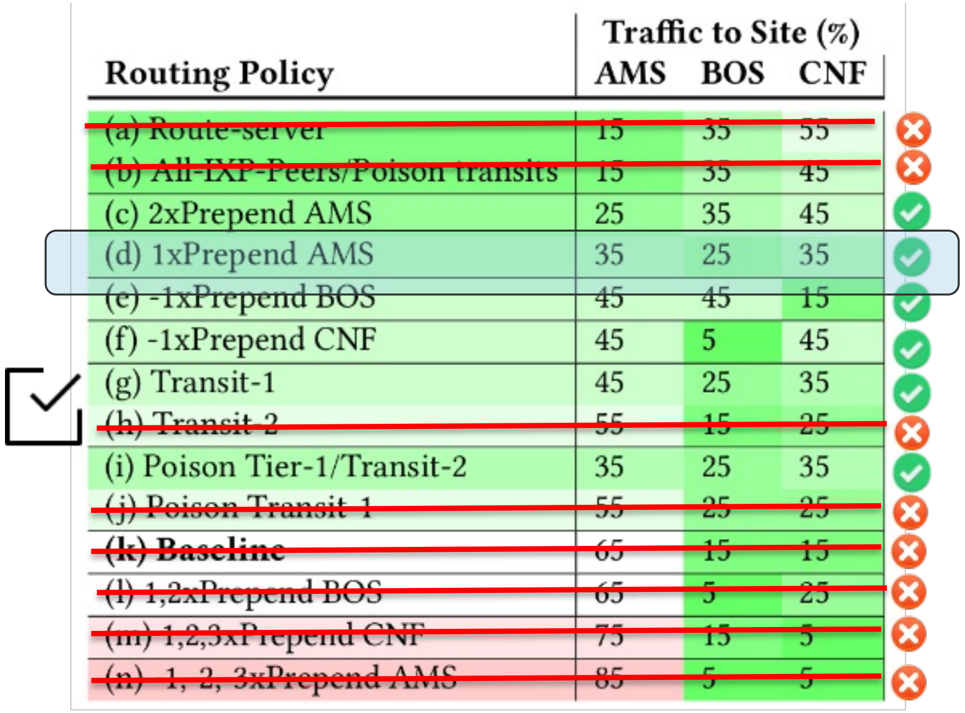


AMS overwhelmed (hatching => dropped traffic)

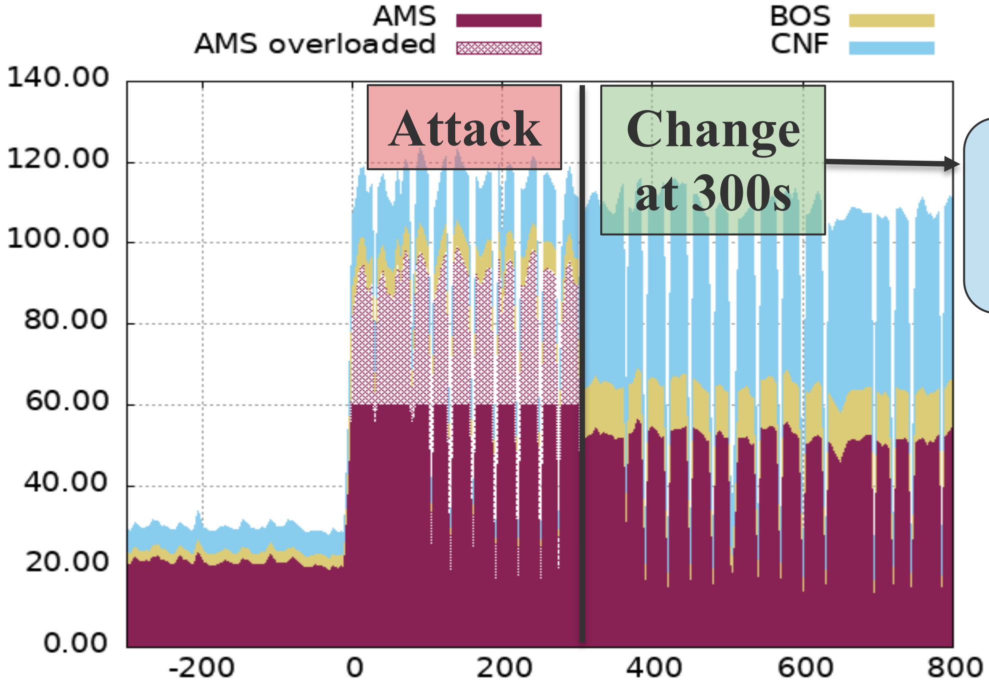
- Goal: lower traffic at AMS
- Several options work: c, d, e, f. g
- We pick **d** to avoid overloading other sites

Outcome after Applying a New BGP Policy

BGP changes at 300s; new traffic balance => no more drops (no hatching)



Routing Policy	Traffic to Site (%)			
	AMS	BOS	CNF	
~~(a) Route-server~~	~~15~~	~~35~~	~~55~~	✗
~~(b) All-IXP-Peers/Poison transits~~	~~15~~	~~35~~	~~45~~	✗
(c) 2xPrepend AMS	25	35	45	✓
(d) 1xPrepend AMS	35	25	35	✓
(e) -1xPrepend BOS	45	45	15	✓
(f) -1xPrepend CNF	45	5	45	✓
☑ (g) Transit-1	45	25	35	✓
~~(h) Transit-2~~	~~55~~	~~15~~	~~25~~	✗
(i) Poison Tier-1/Transit-2	35	25	35	✓
~~(j) Poison Transit-1~~	~~55~~	~~25~~	~~25~~	✗
~~**(k) Baseline**~~	~~65~~	~~15~~	~~15~~	✗
~~(l) 1,2xPrepend BOS~~	~~65~~	~~5~~	~~25~~	✗
~~(m) 1,2,3xPrepend CNF~~	~~75~~	~~15~~	~~5~~	✗
~~(n) -1, -2, -3xPrepend AMS~~	~~85~~	~~5~~	~~5~~	✗



No loss
Some AMS traffic => CNF

Conclusion

- New method to **estimate attack size** from known good traffic
- Propose **BGP playbook** to plan reactions to DDoS
- **Evaluations against real attacks**
- More information about software
  - **Paper** https://www.usenix.org/system/files/sec22-rizvi.pdf
  - **Artifacts:** https://zenodo.org/record/6473023

usenix
THE ADVANCED
COMPUTING SYSTEMS
ASSOCIATION

ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

ARTIFACT EVALUATED usenix ASSOCIATION REPRODUCED