United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale

Daniel Wagner[1,2]

Daniel Kopp[1], Matthias Wichtlhuber[1], Christoph Dietzel[1,2], Oliver Hohlfeld[3],

Georgios Smaragdakis[4] and Anja Feldmann[2]

1 DE-CIX

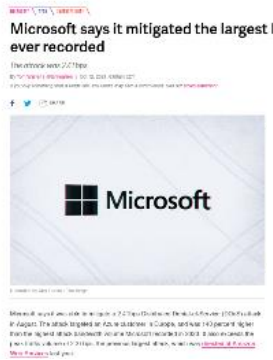
2 MAX-PLANCK-GESELLSCHAFT

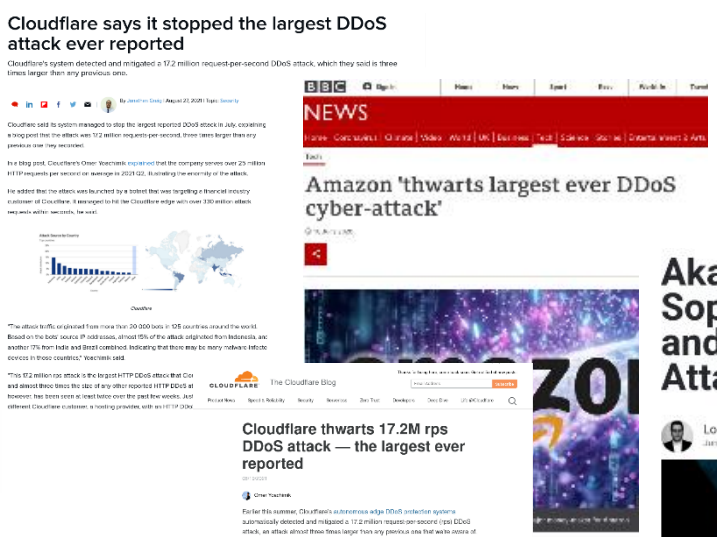
3 b-tu Brandenburgische Technische Universität Cottbus

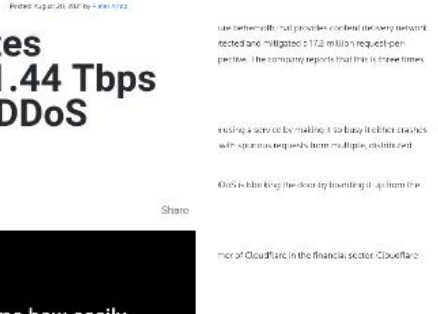
4 TU Delft

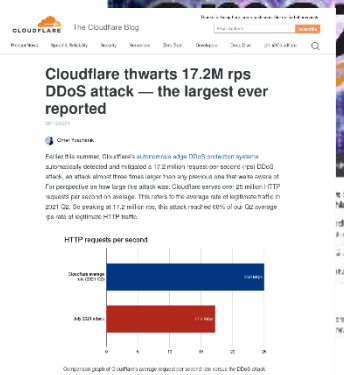
Distributed Denial of Service (DDoS)

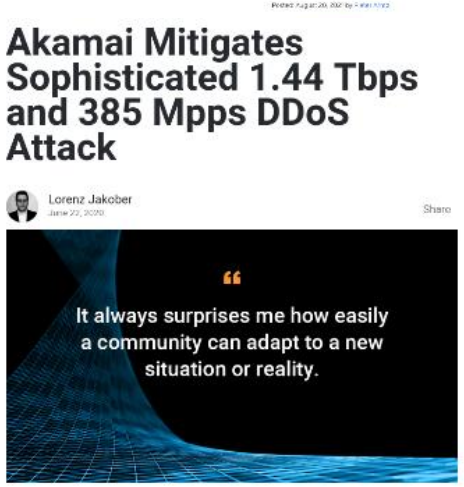
- Network attack causing service downtime
- Targets: Financial services, health sector, …



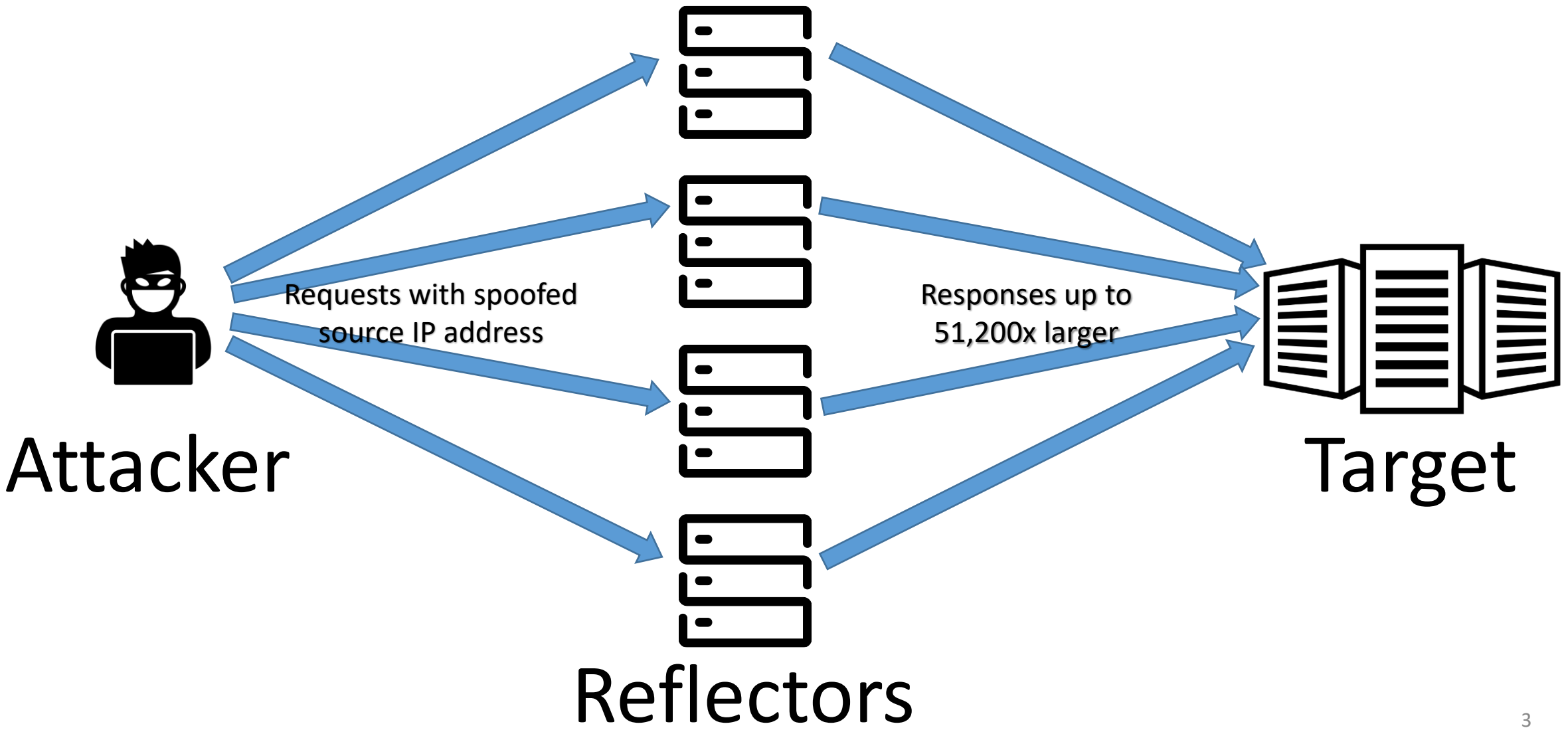




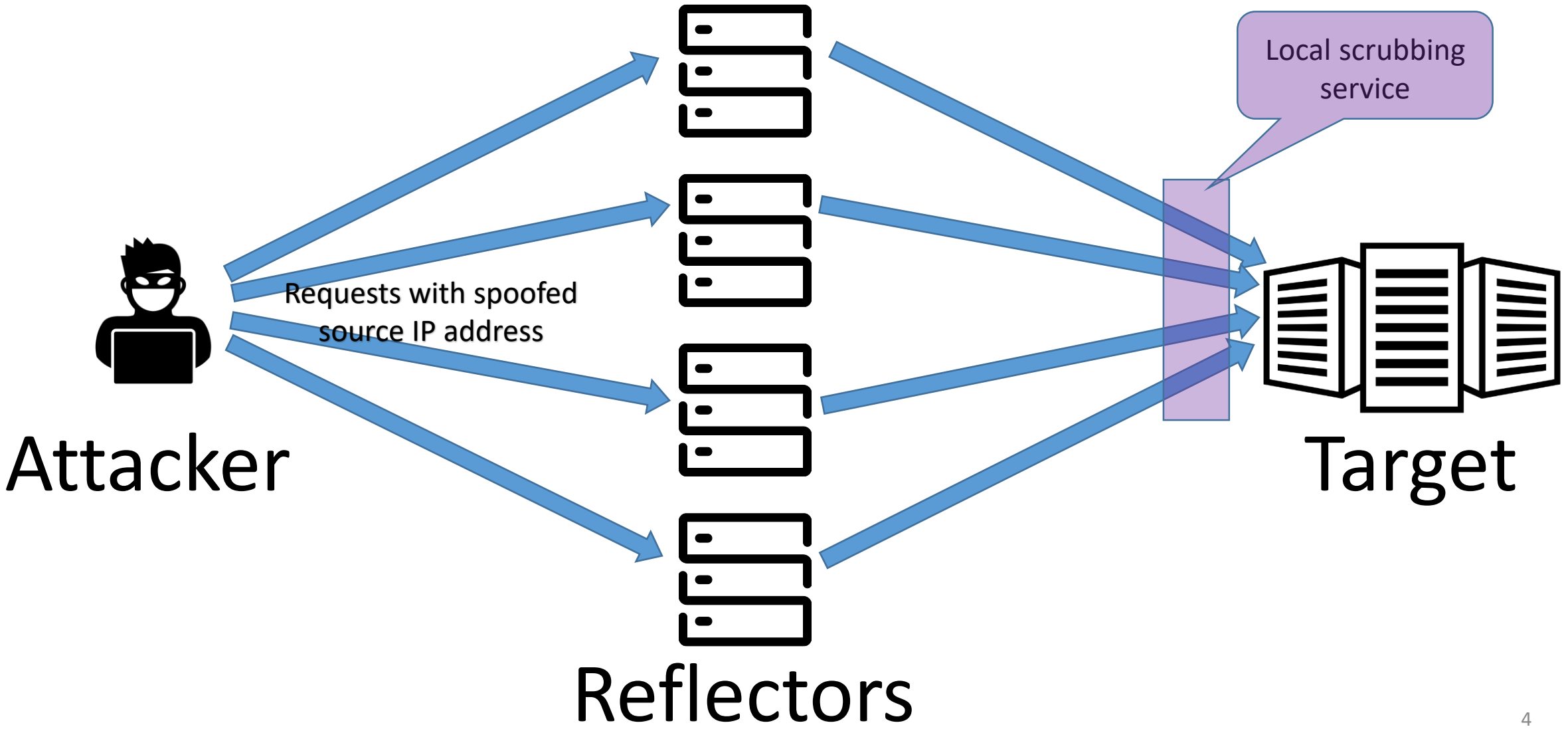




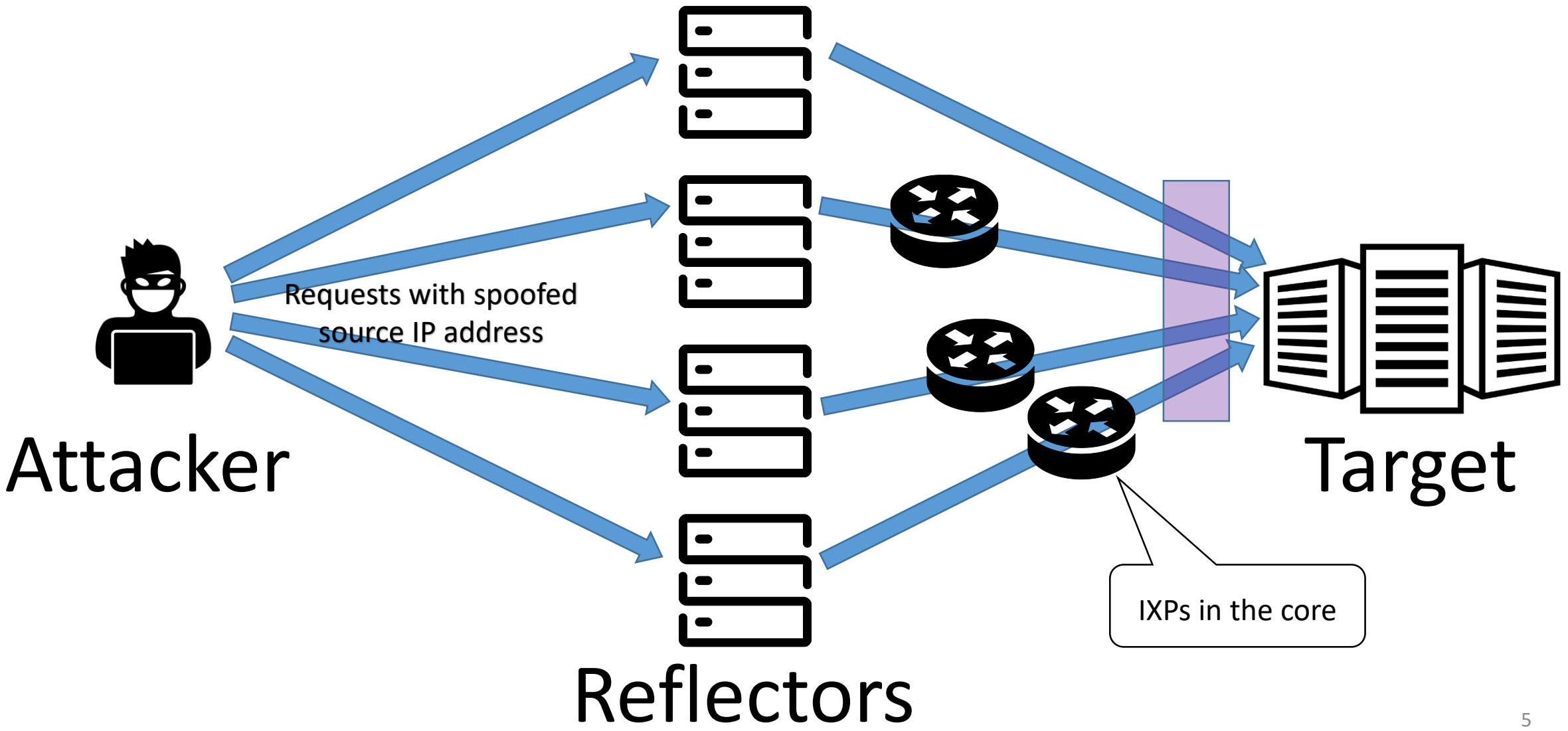
Amplification DDoS Attacks



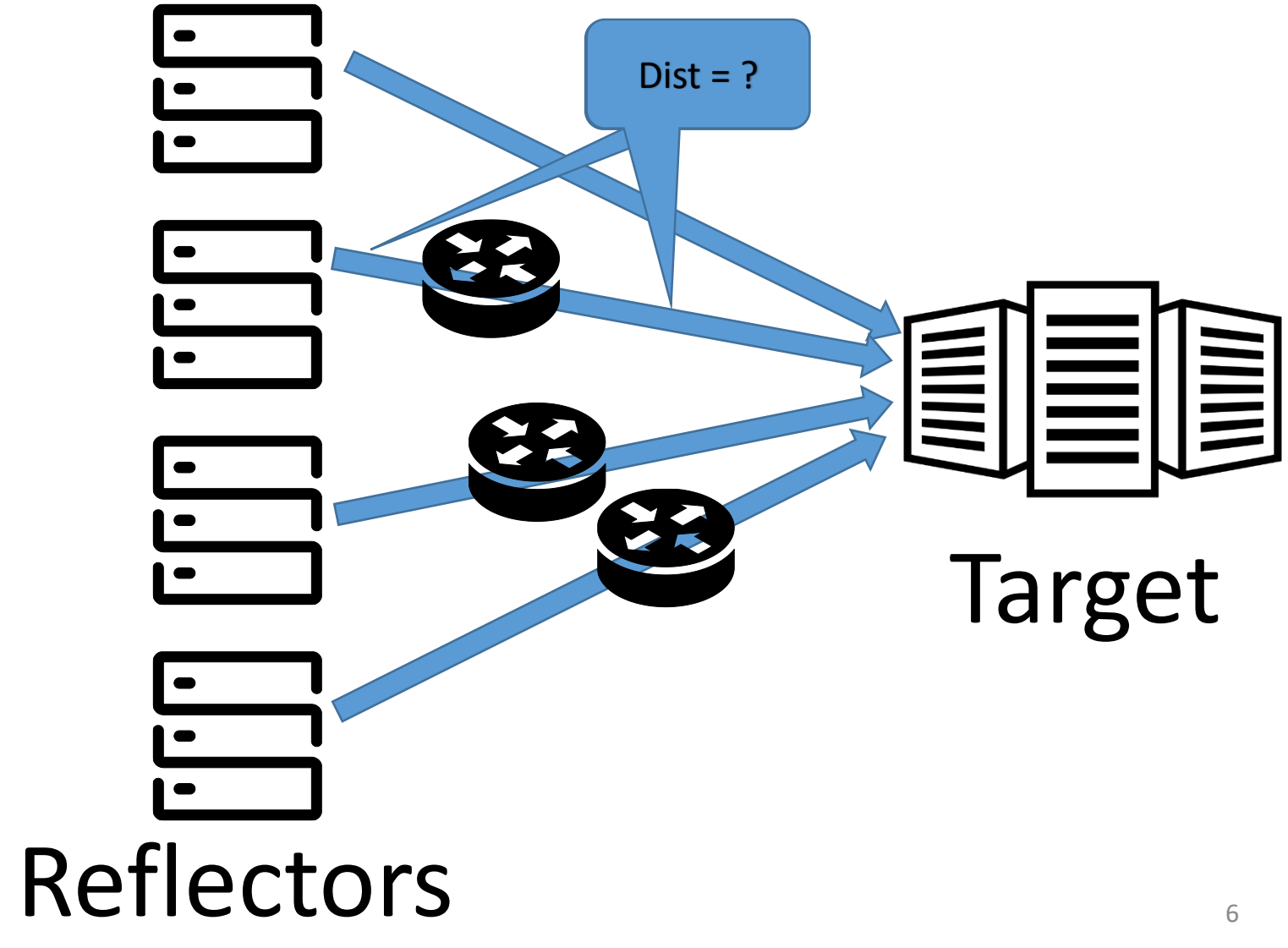
Amplification DDoS Attacks



Amplification DDoS Attacks

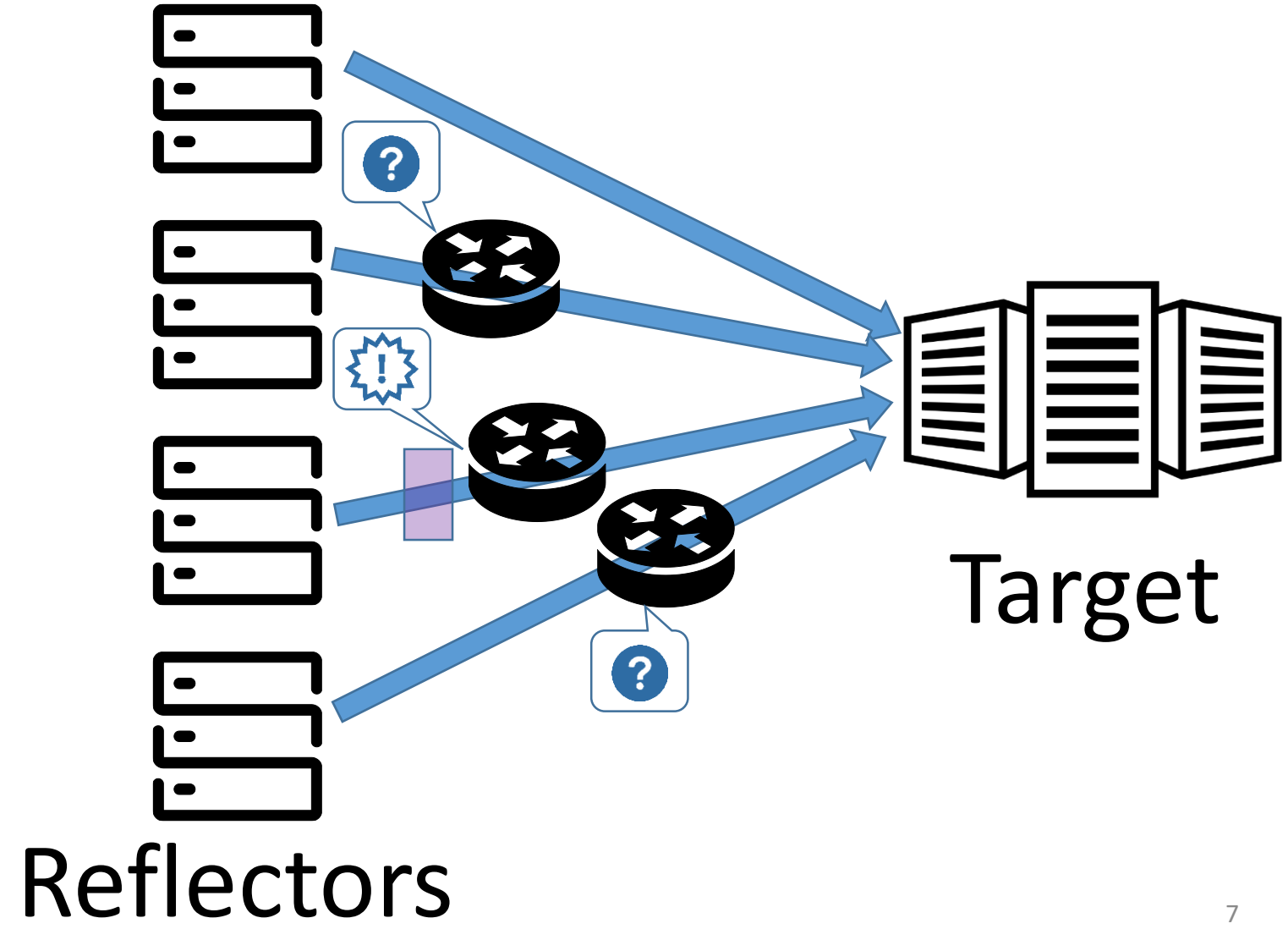


Amplification DDoS Attacks



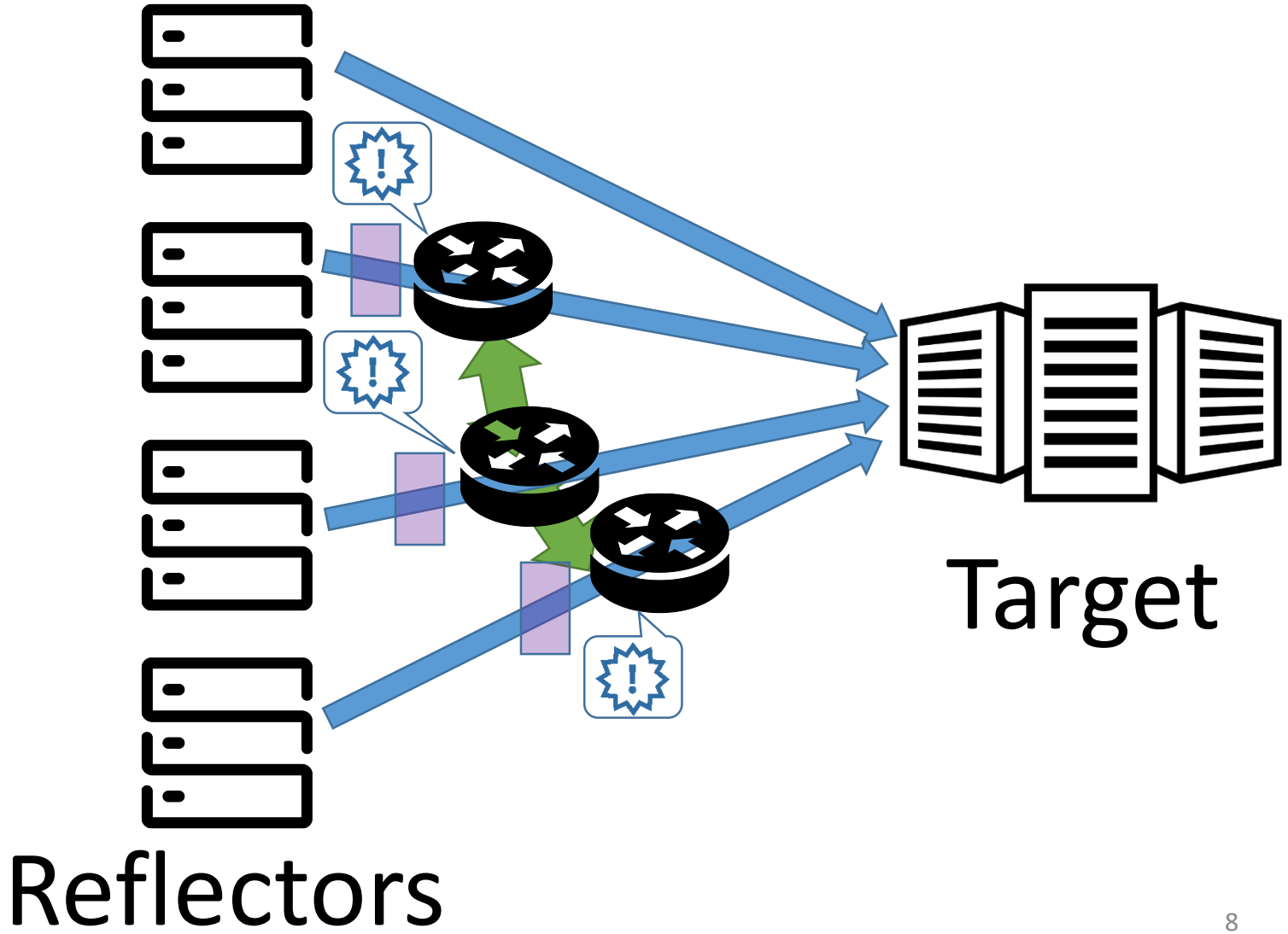
- Distance analysis
  - #hops from refelctor?
  - #hops to target?

Amplification DDoS Attacks



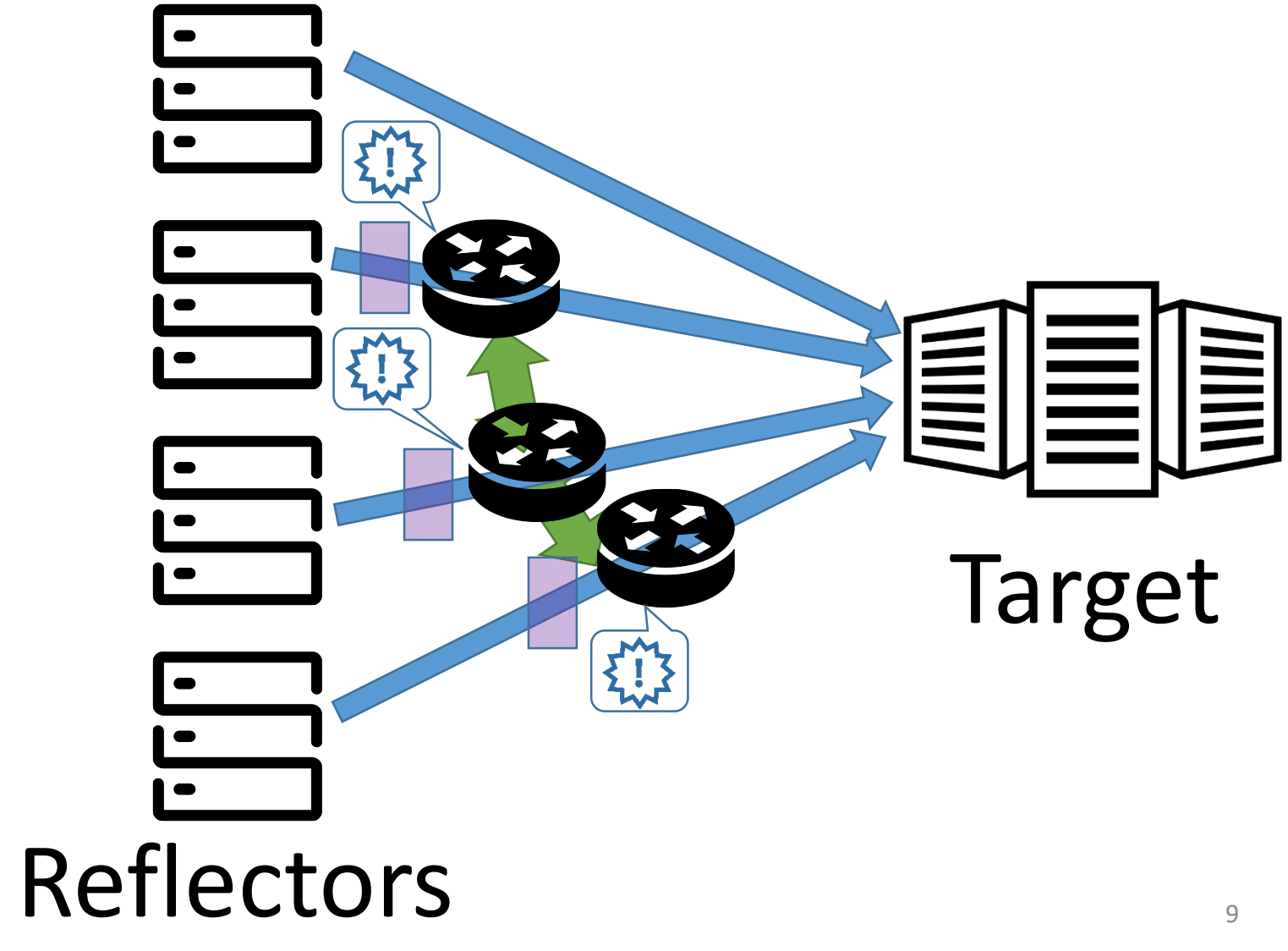
- Distance analysis
  - #hops from refelctor?
  - #hops to target?
- Collaboration benefit

Amplification DDoS Attacks



- Distance analysis
  - #hops from refelctor?
  - #hops to target?
- Collaboration benefit
- Information exchange platorm

Amplification DDoS Attacks



- Distance analysis
  - #hops from refelctor?
  - #hops to target?
- Collaboration benefit
- Information exchange platorm

- Let‘s leverage some data!

Data Set

- Flow data from 11 IXPs, April 2020 – October 2020

IXP Code	#Networks	Peak traffic	Region	#sampled Flows
CE1	>900	>9000 Gb/s	Central Europe	1.08 Trillion
CE2	>200	>150 Gb/s	Central Europe	9.9 Billion
CE3	>200	>150 Gb/s	Central Europe	3.2 Billion
CE4	>200	>100 Gb/s	Central Europe	3.6 Billion
NA1	>200	>800 Gb/s	North America	78 Billion
NA2	>75	>150 Gb/s	North America	16.7 Billion
SE1	>175	>400 Gb/s	South Europe	30.5 Billion
SE2	>75	>100Gb/s	South Europe	12.2 Billion
SE3	>40	>10 Gb/s	South Europe	2.2 Billion
SE4	>30	>100 Gb/s	South Europe	17.9 Billion
SE5	>20	>50 Gb/s	South Europe	2 Billion

Traffic Filtering

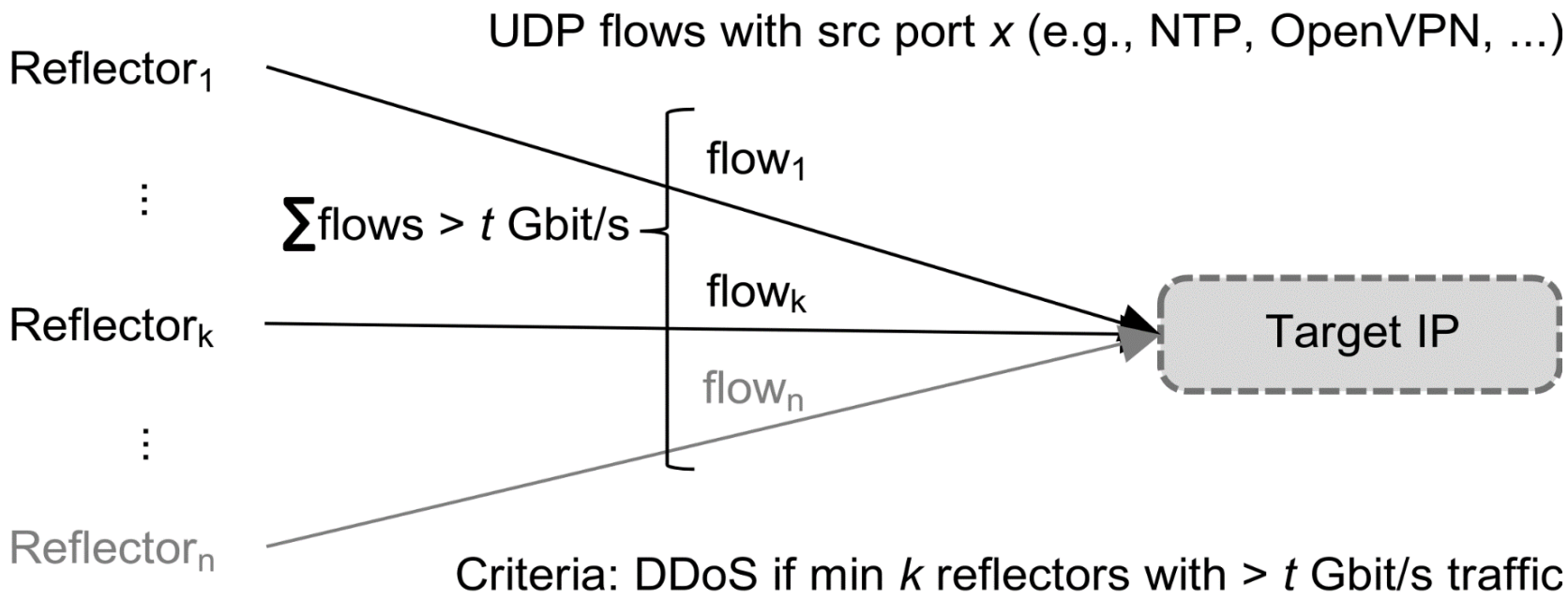
- UDP only
- Filtering for typical DDoS amplification protocols[2]
- Packet size[2]

Protocol	Chargen	DNS	RPC	NTP	SNMP	CLDAP	OpenVPN	SSDP	ARMS	WS Discovery	Device Discovery	memcached
Transport port	19	53	111	123	161	389	1194	1900	3283	3702	10001	11211

[2] “DDoS Never Dies? An IXP Perspective on Amplifcation DDoS Attacks“, PAM 2020, D. Kopp et al.

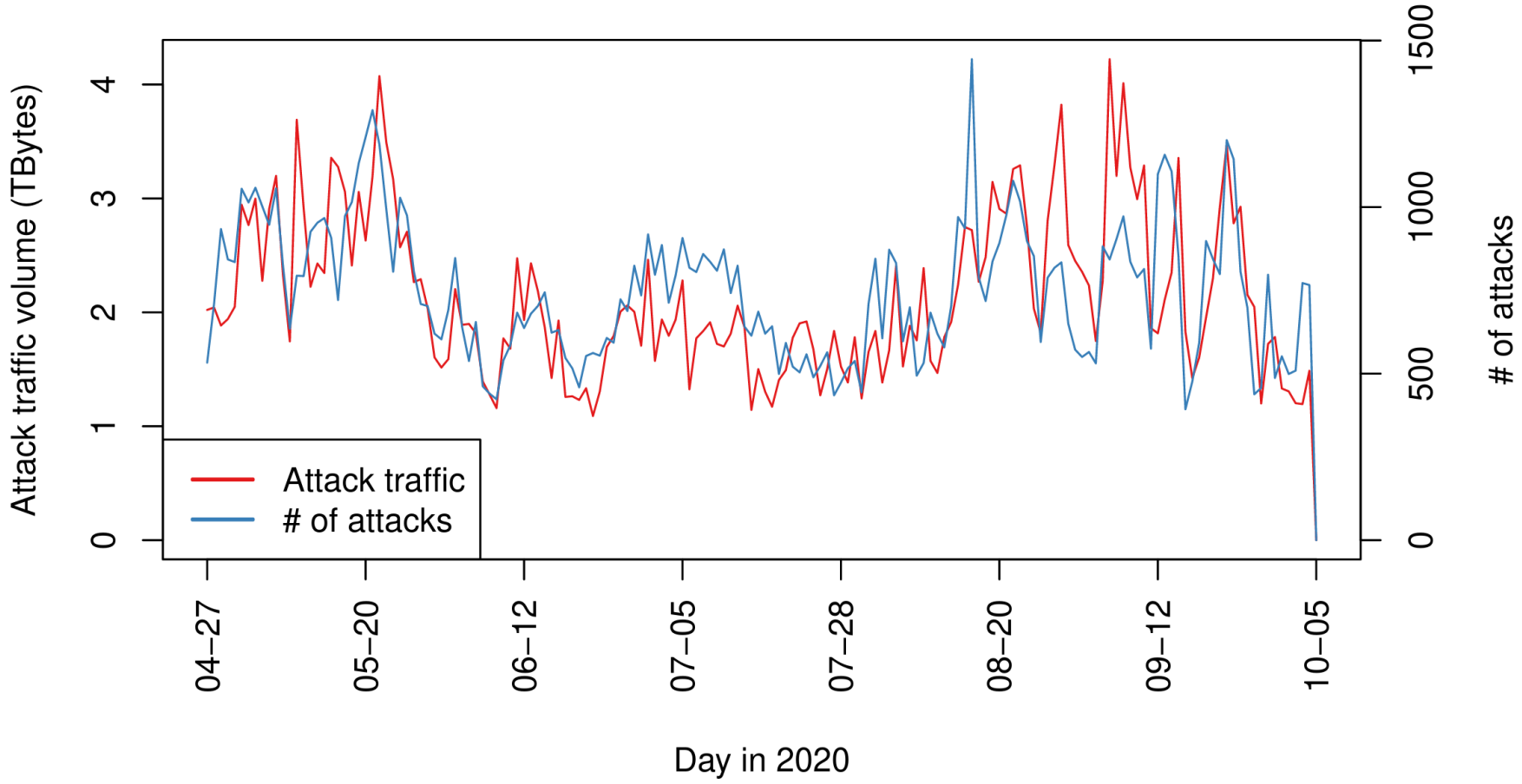
Attack Detection

[2]



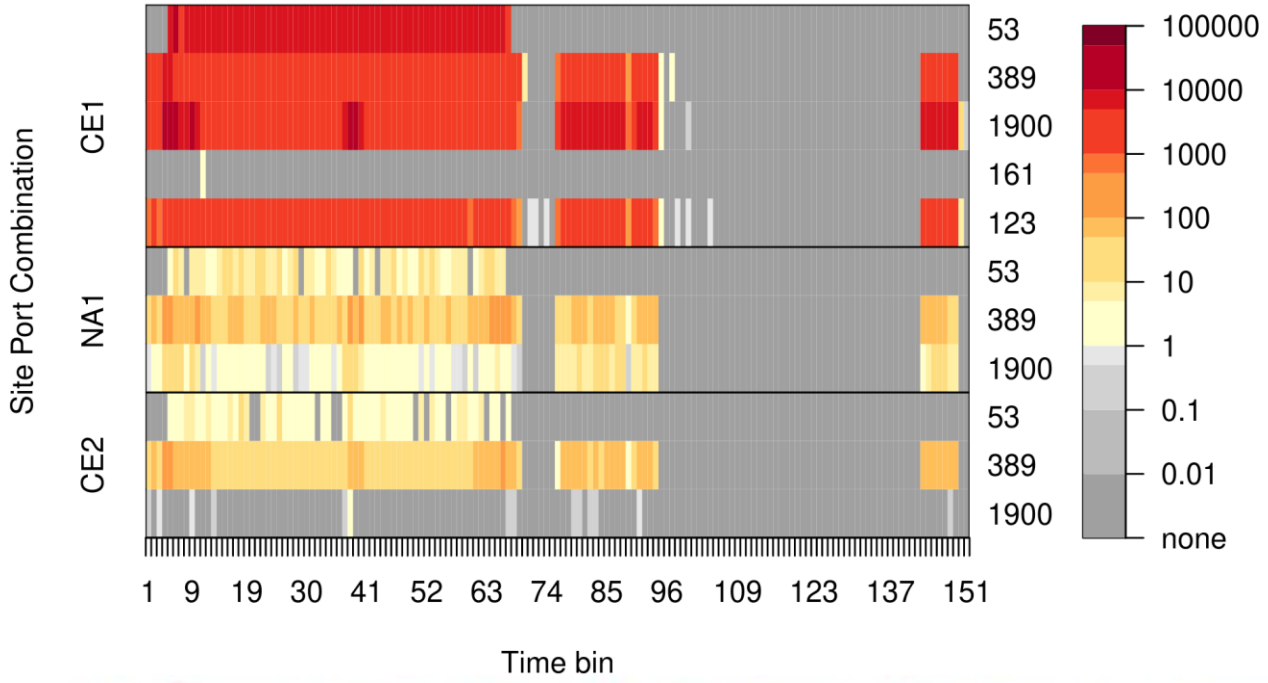
- Global attack traffic with n>=10 reflectors, t>1Gbps attack traffic
- We identified >120k DDoS attacks
- Including confirmed attacks

Number of DDoS Attack Events per Day

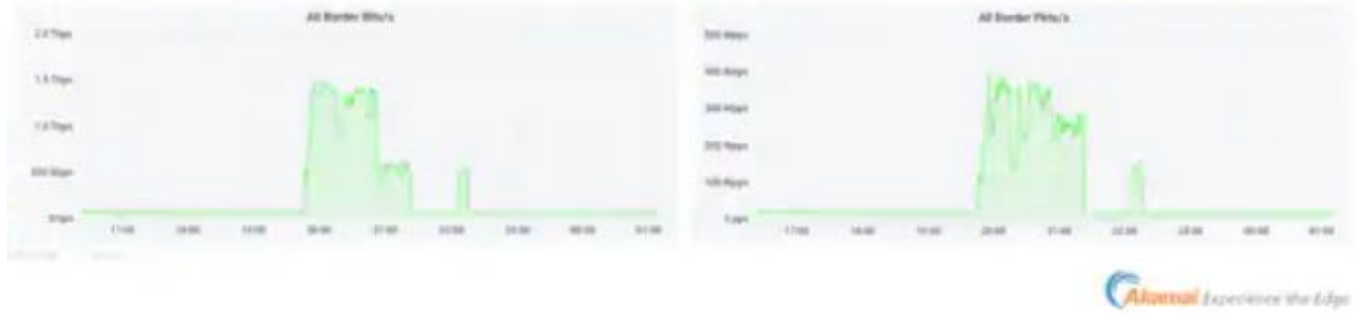


- Thousands of attacks every day!

Case study: Attack to Akamai



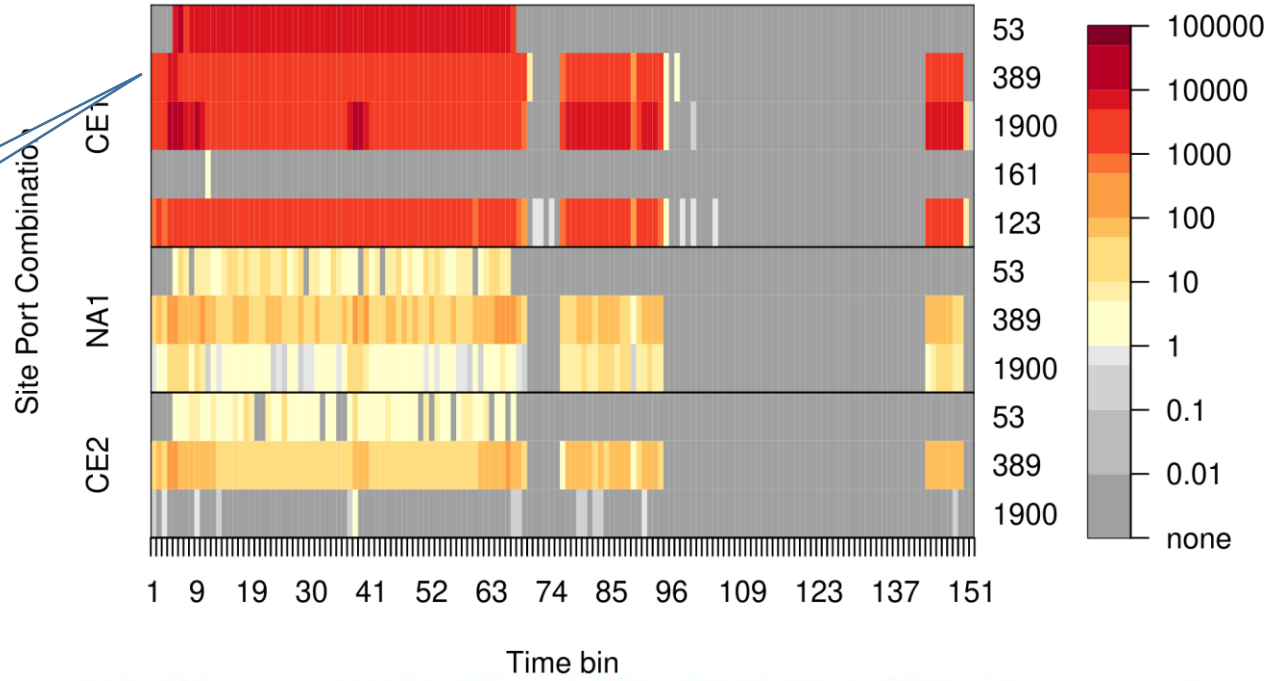
[1]



[1] “Akamai Mitigates Sophisticated 1.44 Tbps and 385 Mpps DDoS Attack”, Akamai.com

Case study: Attack to Akamai

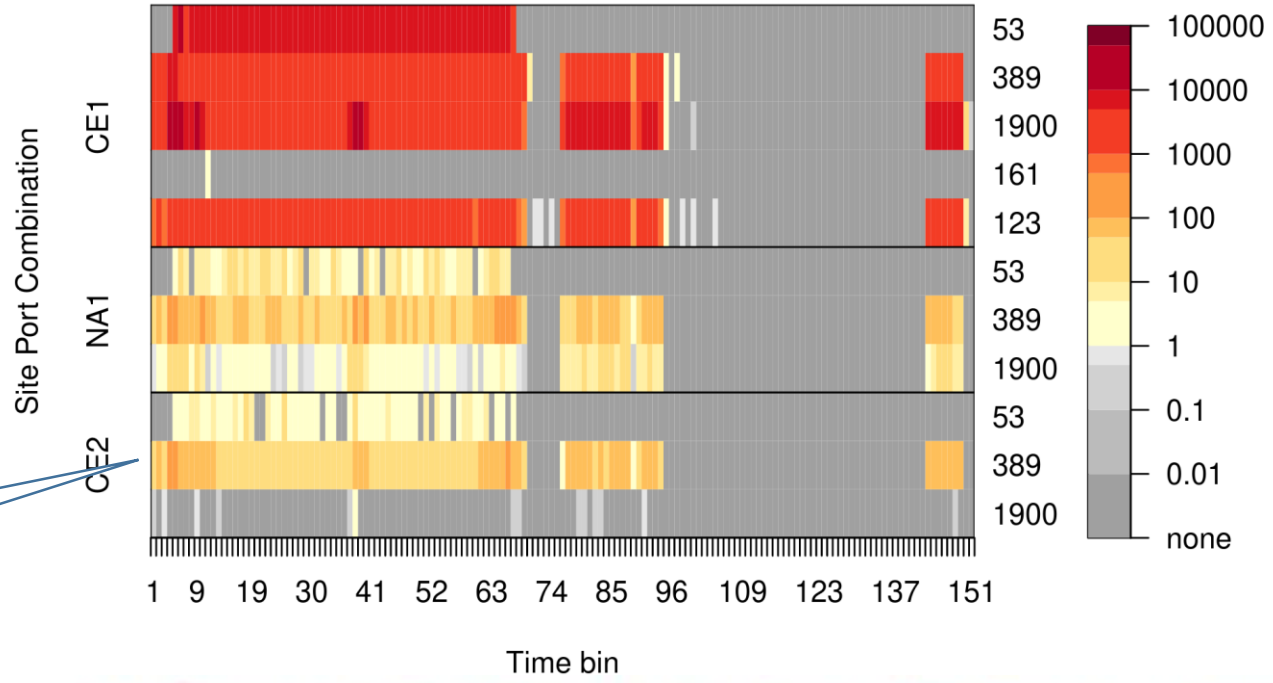
Local detection feasible



[1]

[1] “Akamai Mitigates Sophisticated 1.44 Tbps and 385 Mpps DDoS Attack”, Akamai.com

Case study: Attack to Akamai



Local detection infeasible

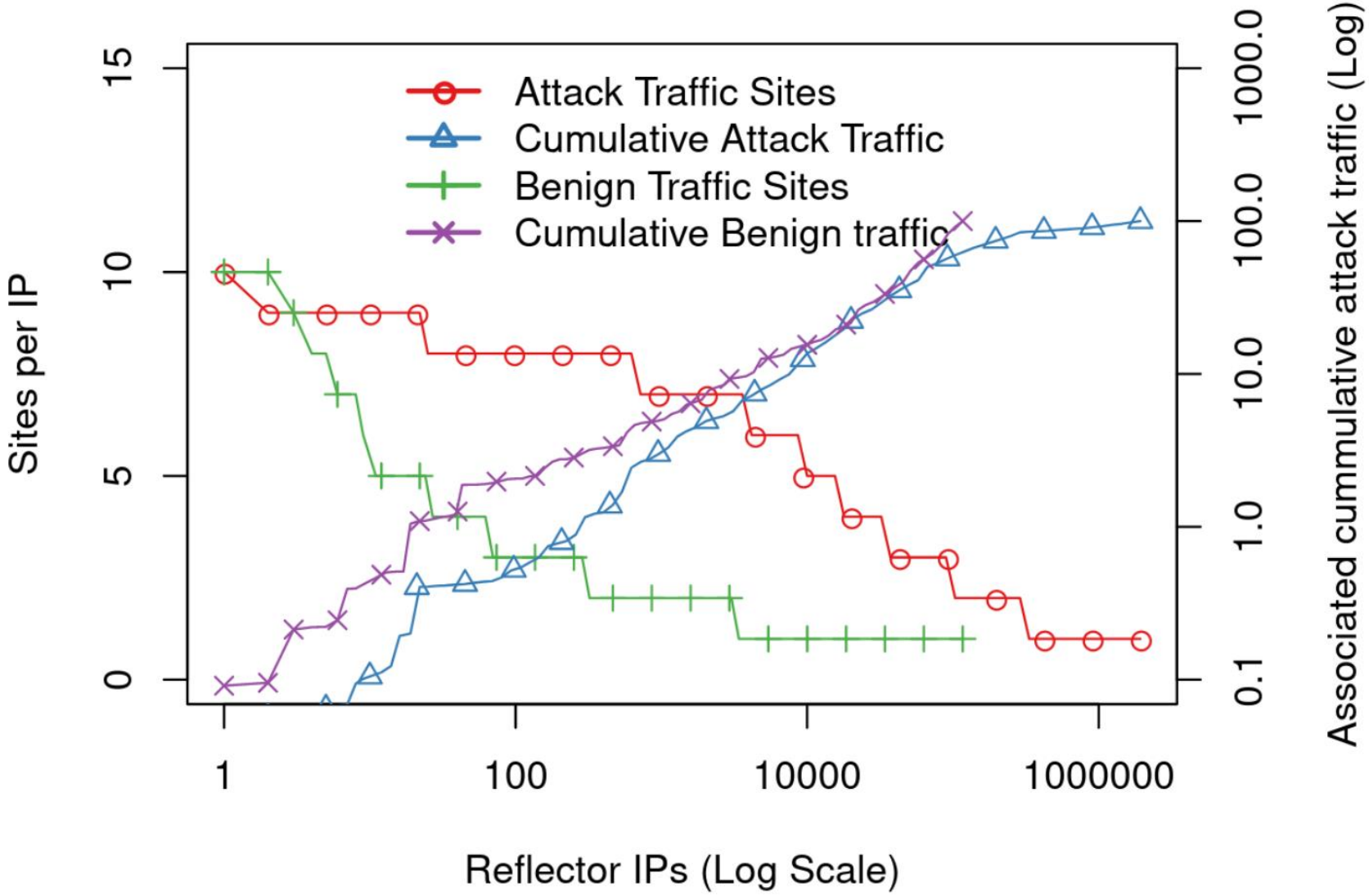
[1]

[1] “Akamai Mitigates Sophisticated 1.44 Tbps and 385 Mpps DDoS Attack”, Akamai.com

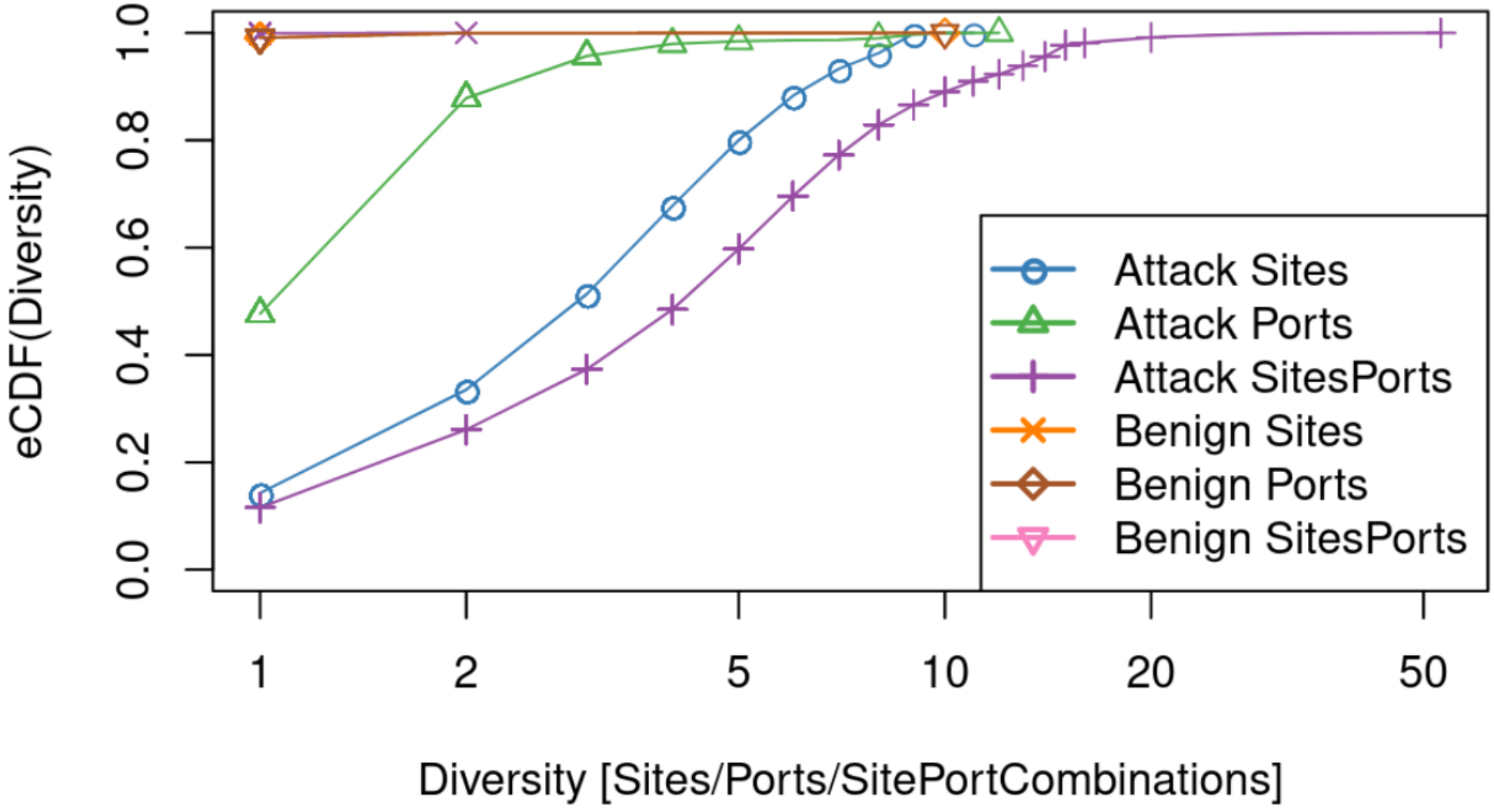
How accurate are we?

- Compare found events to bengin data
  - Traffic to IP addresses that was
    - Caught by the filter
    - Not caught by the detection mechansism
  - Compare traffic characteristics
  - Geographical distribution and port combinations
- Fire up self-attacks to get ground truth
  - Derive and compare features
  - Compare packet sizes

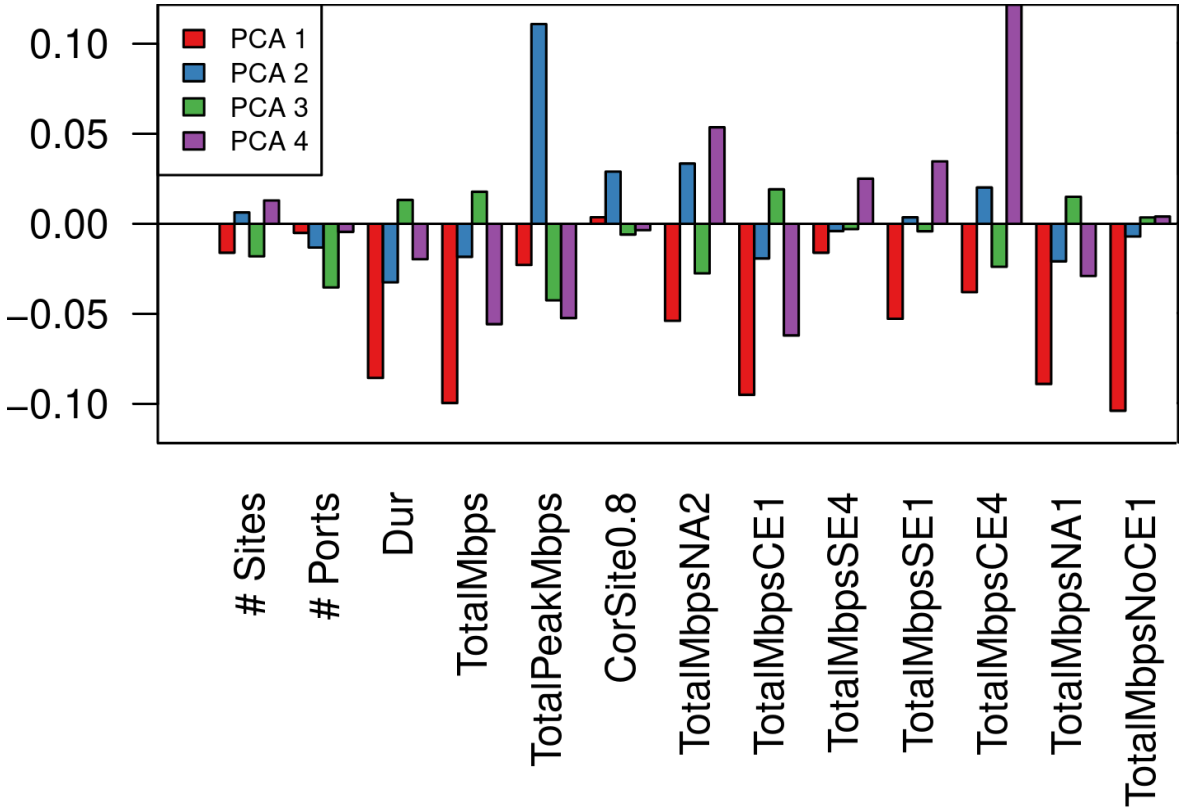
Benign Traffic vs. Attacks: Source IPs



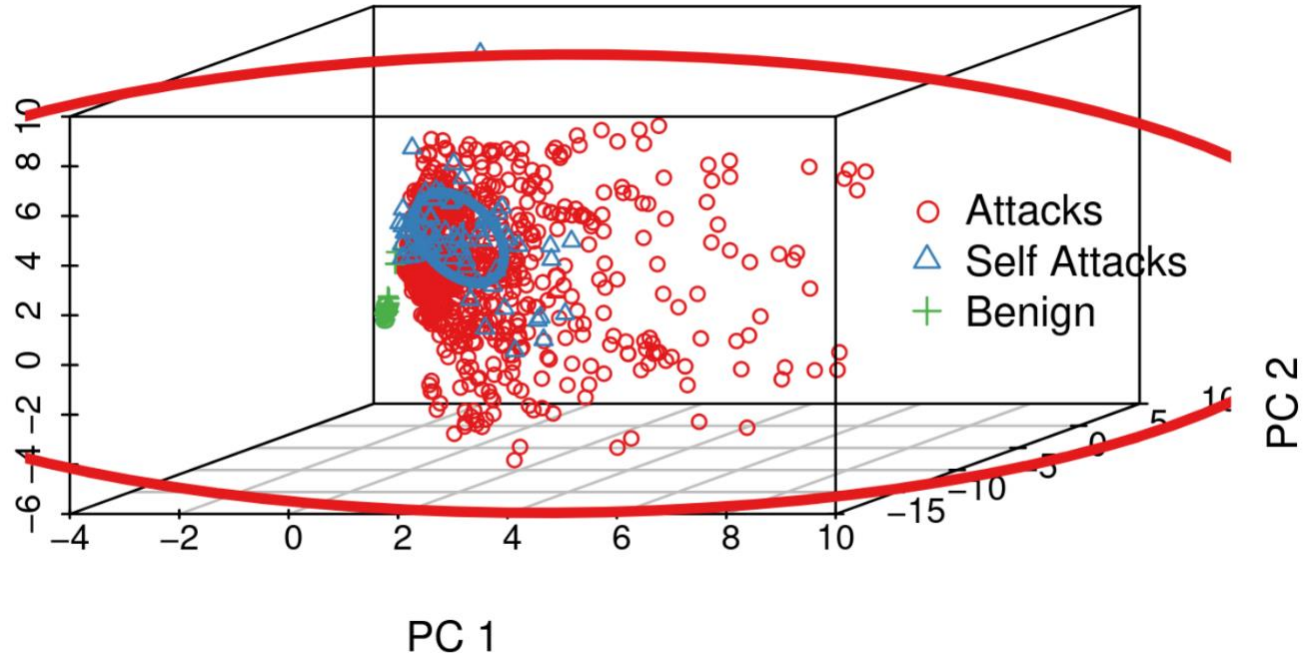
Benign Traffic vs. Attacks: Sites / Ports



Self-Attacks: Features and Clustering

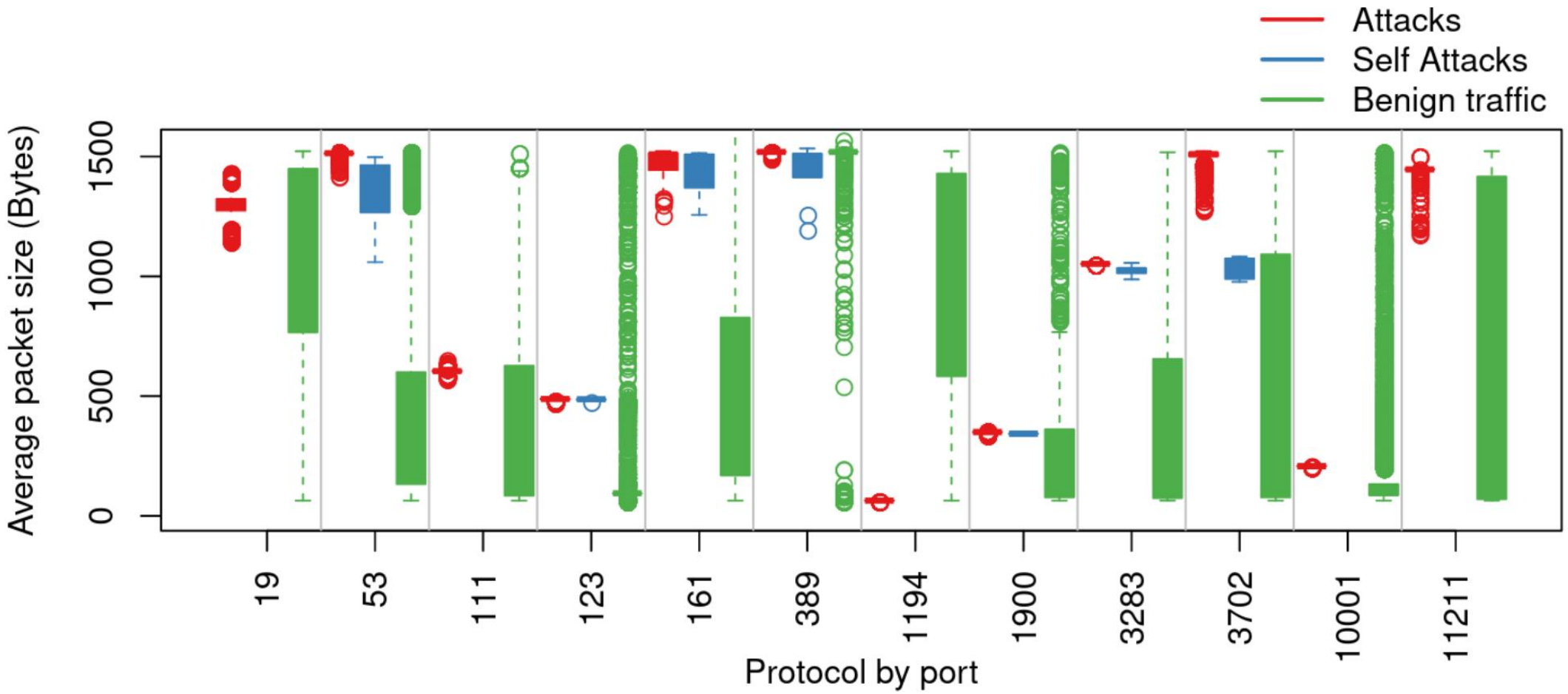


Sample features to the rotation of the first 4 PCAs

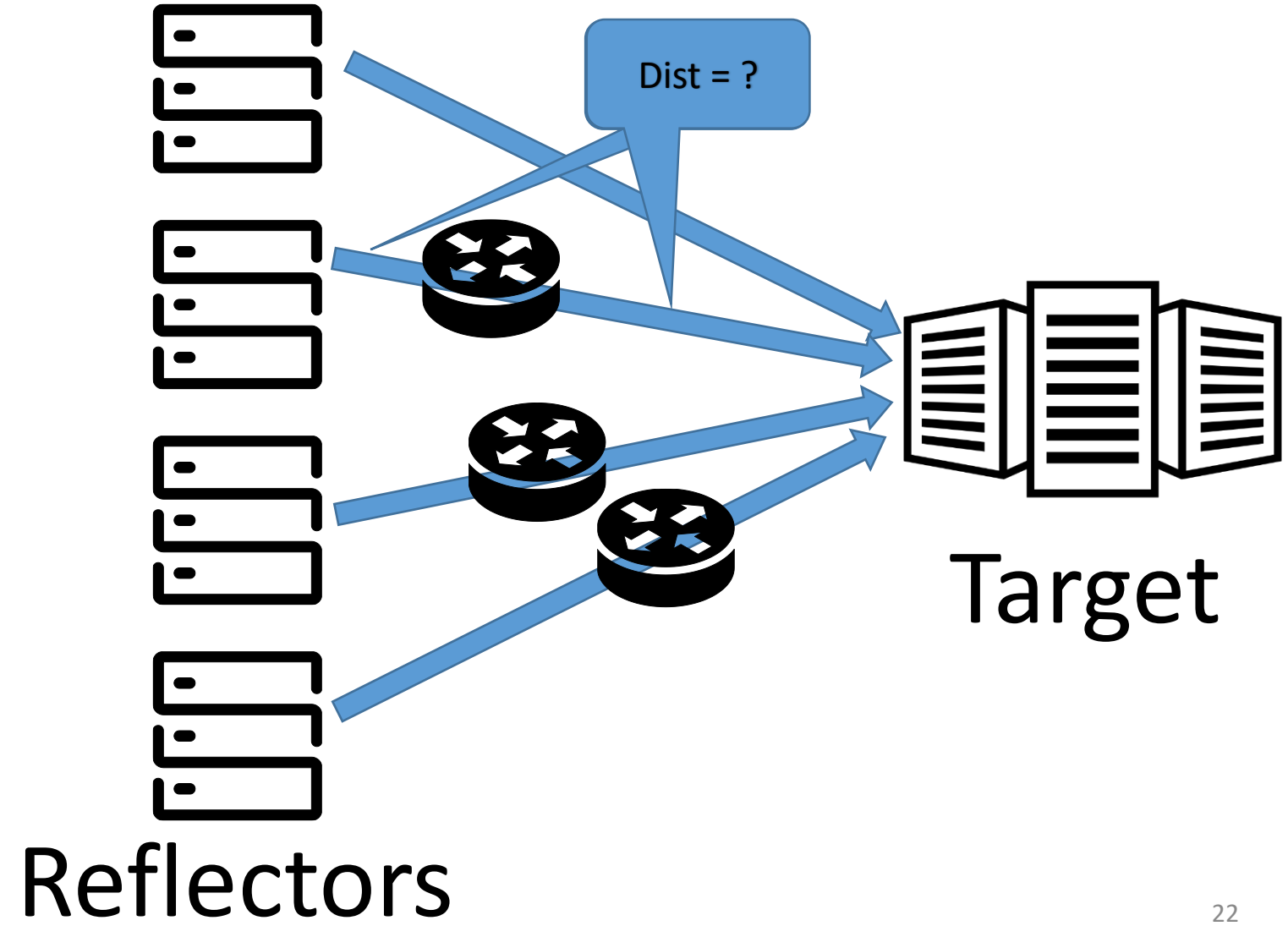


3 most explaining PCs (25% of the variance)

Packet Sizes

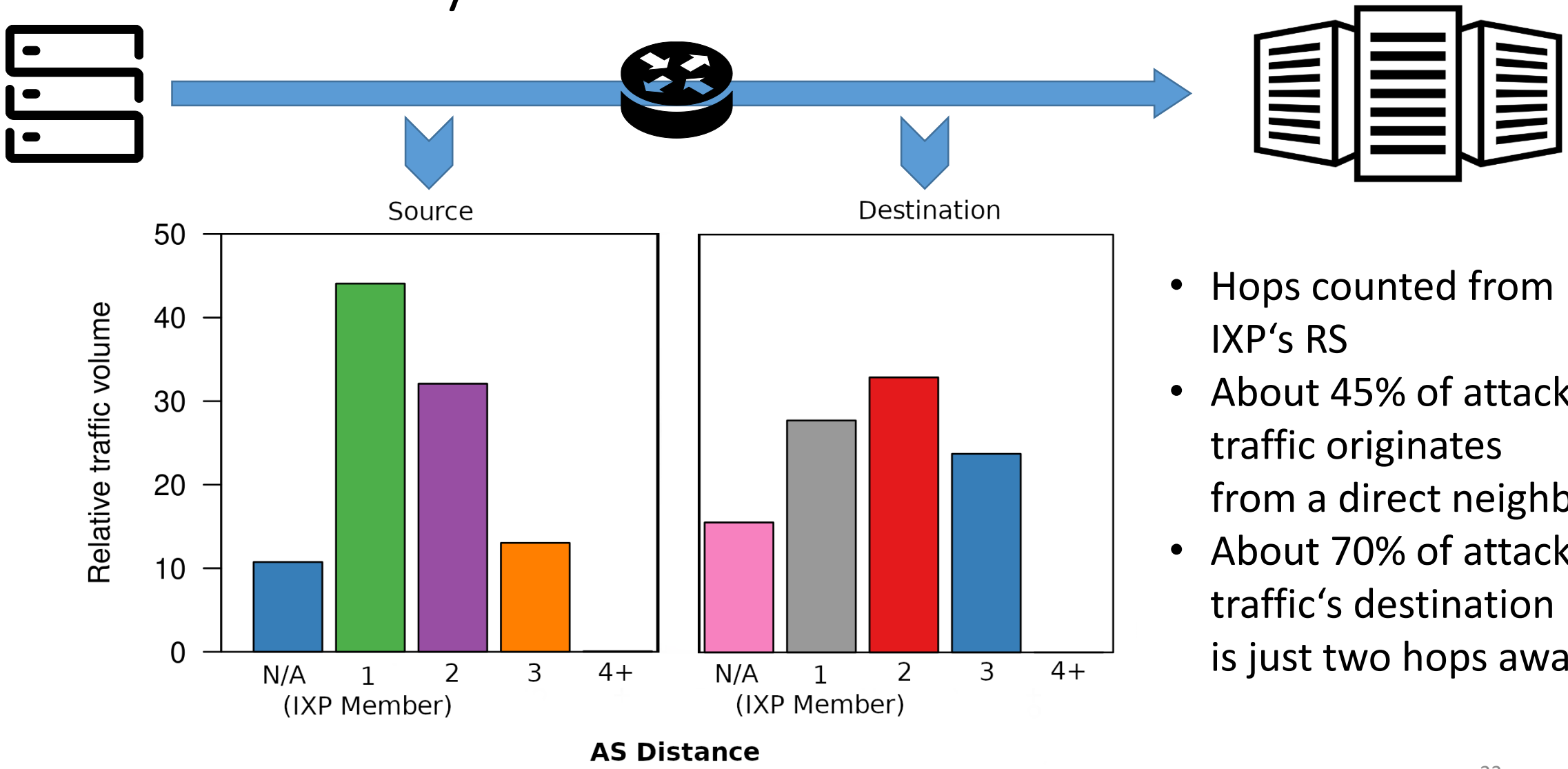


Amplification DDoS Attacks



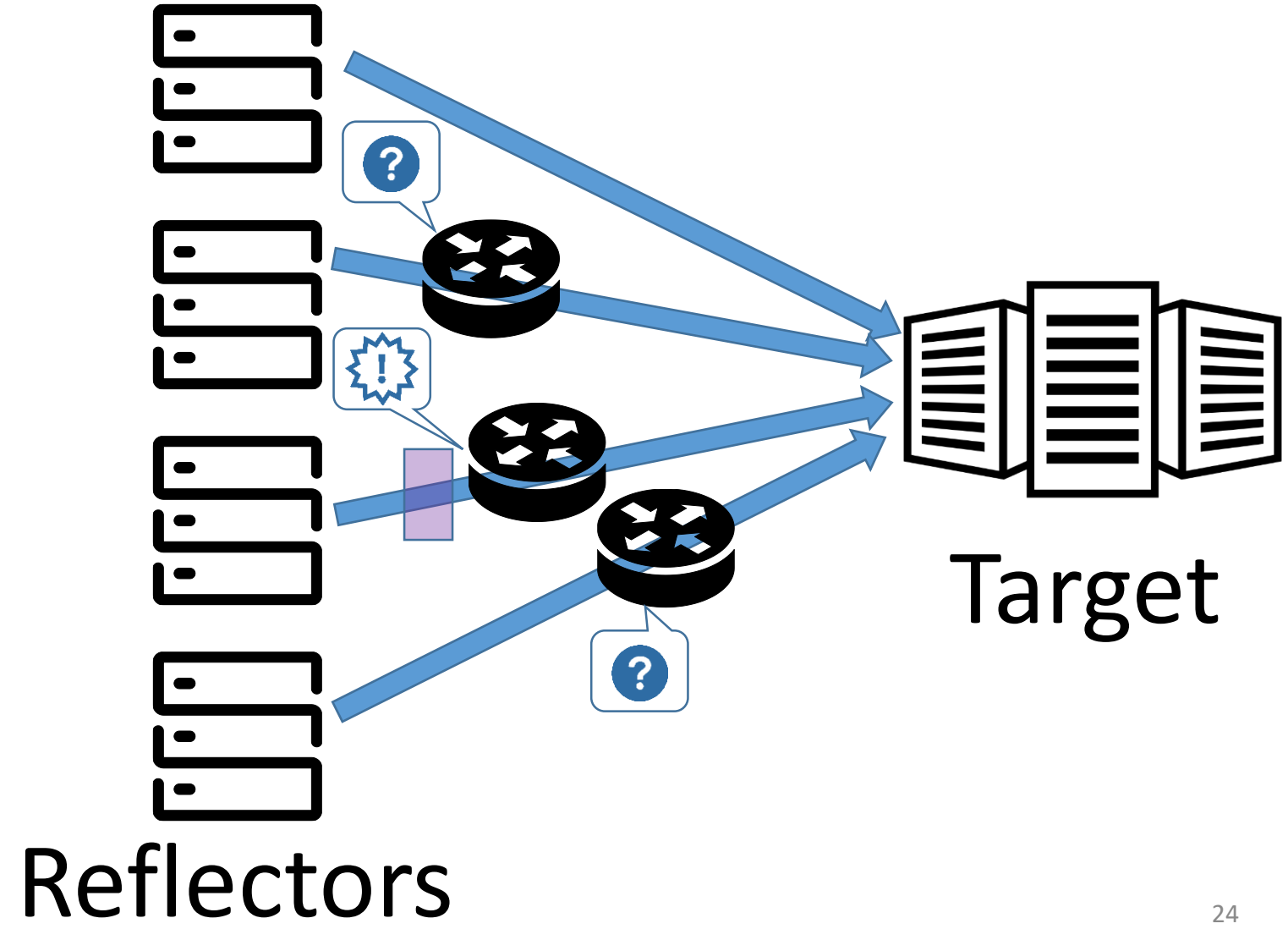
- Distance analysis
  - #hops from refelctor?
  - #hops to target?
- Collaboration benefit
- Information exchange platorm

Distance analysis



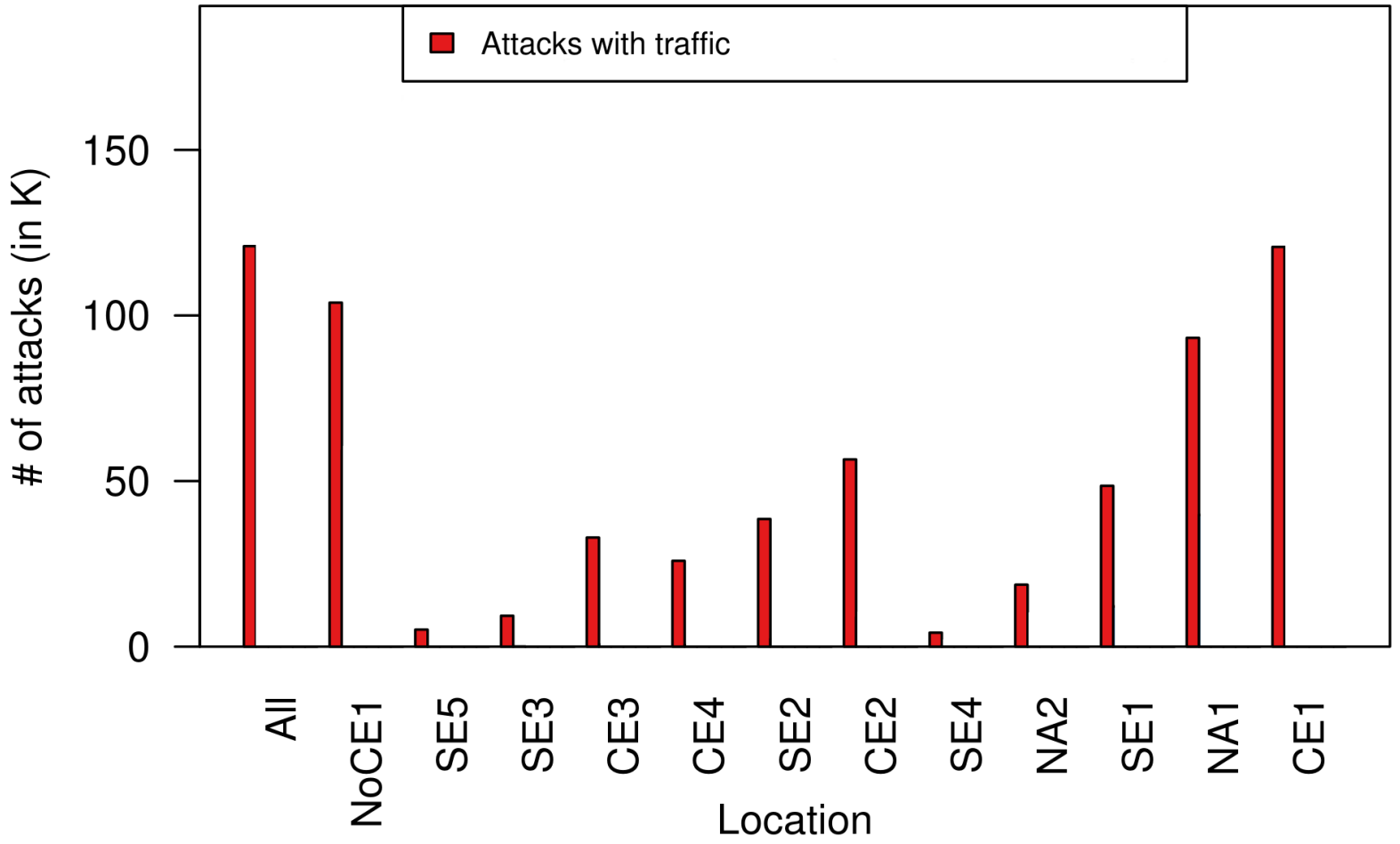
- Hops counted from IXP‘s RS
- About 45% of attack traffic originates from a direct neighbor
- About 70% of attack traffic‘s destination is just two hops away

Amplification DDoS Attacks



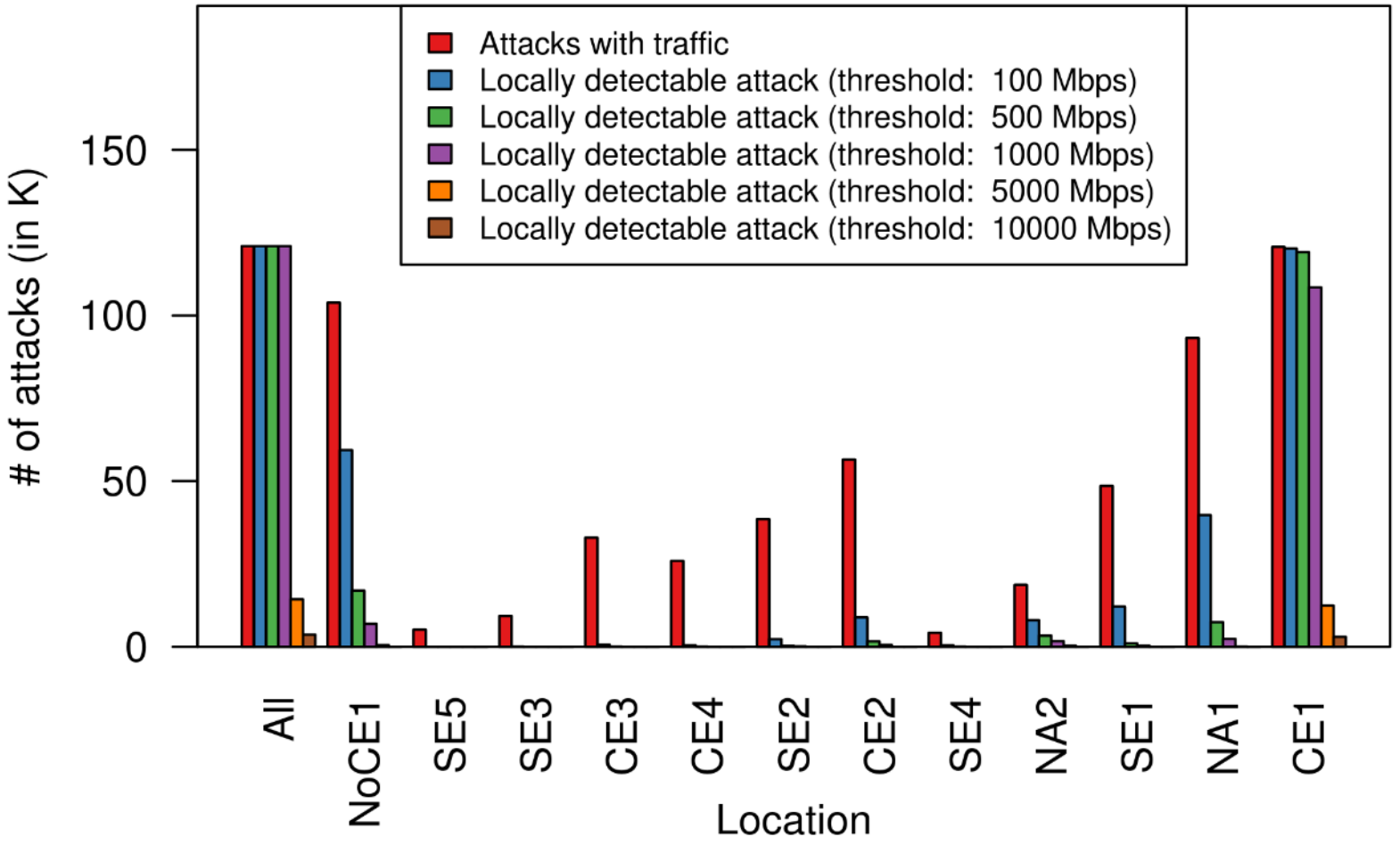
- Distance analysis
  - #hops from refelctor?
  - #hops to target?
- Collaboration benefit
- Information exchange platorm

Attack Events



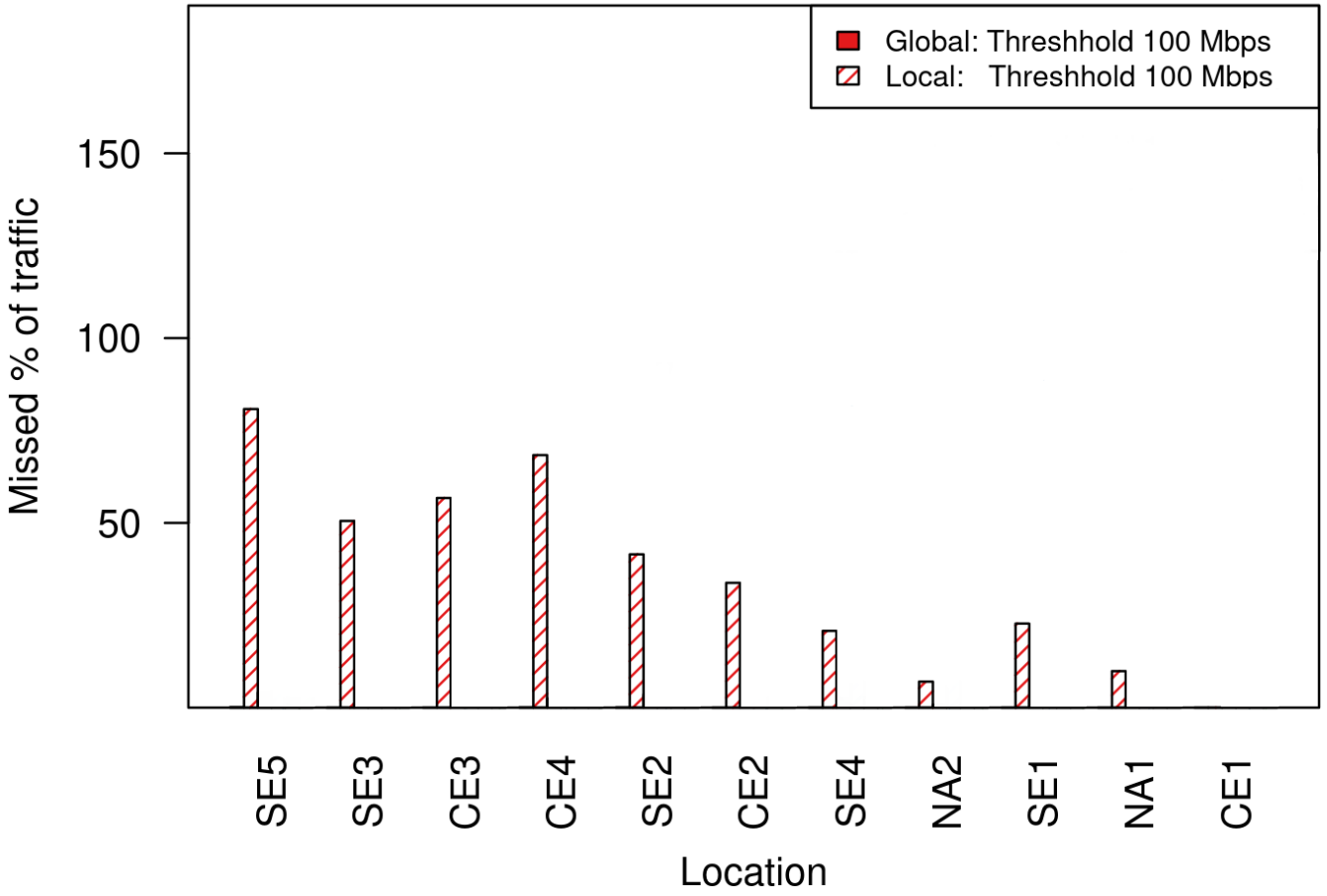
- Ground truth of combined data

Attack Events

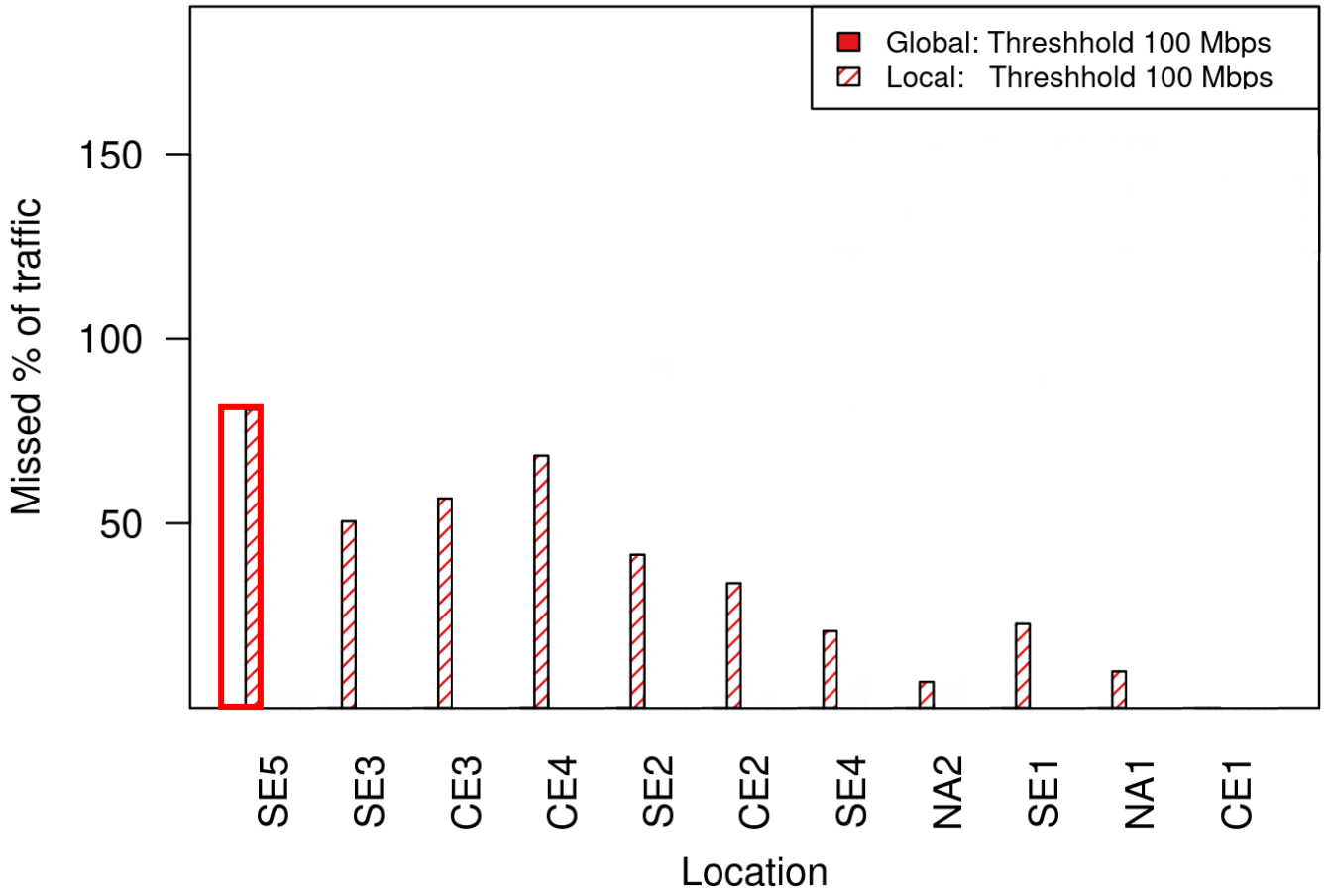


- Ground truth of combined data
- Versus local detectable attack traffic

Collaboration benefit

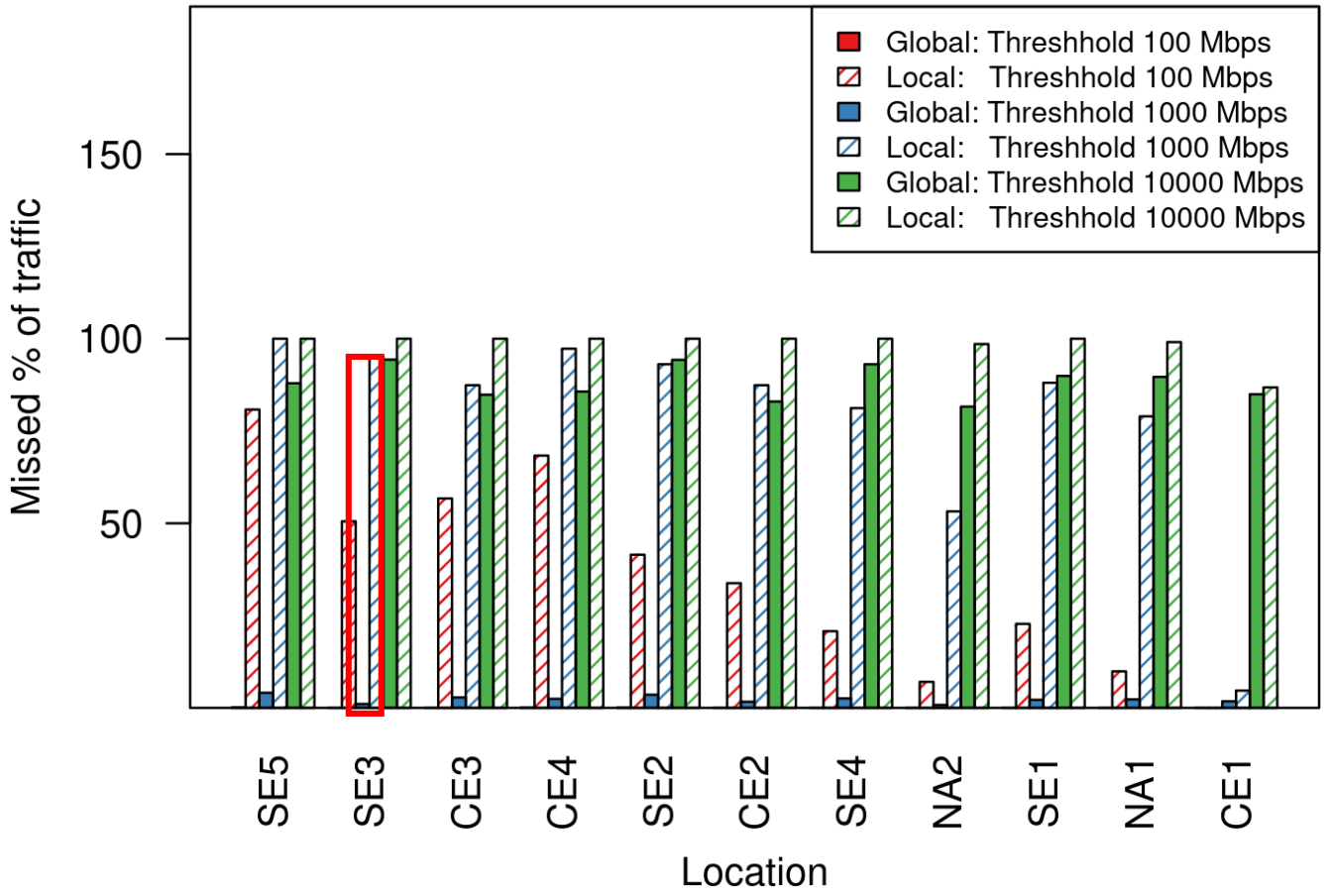


Collaboration benefit



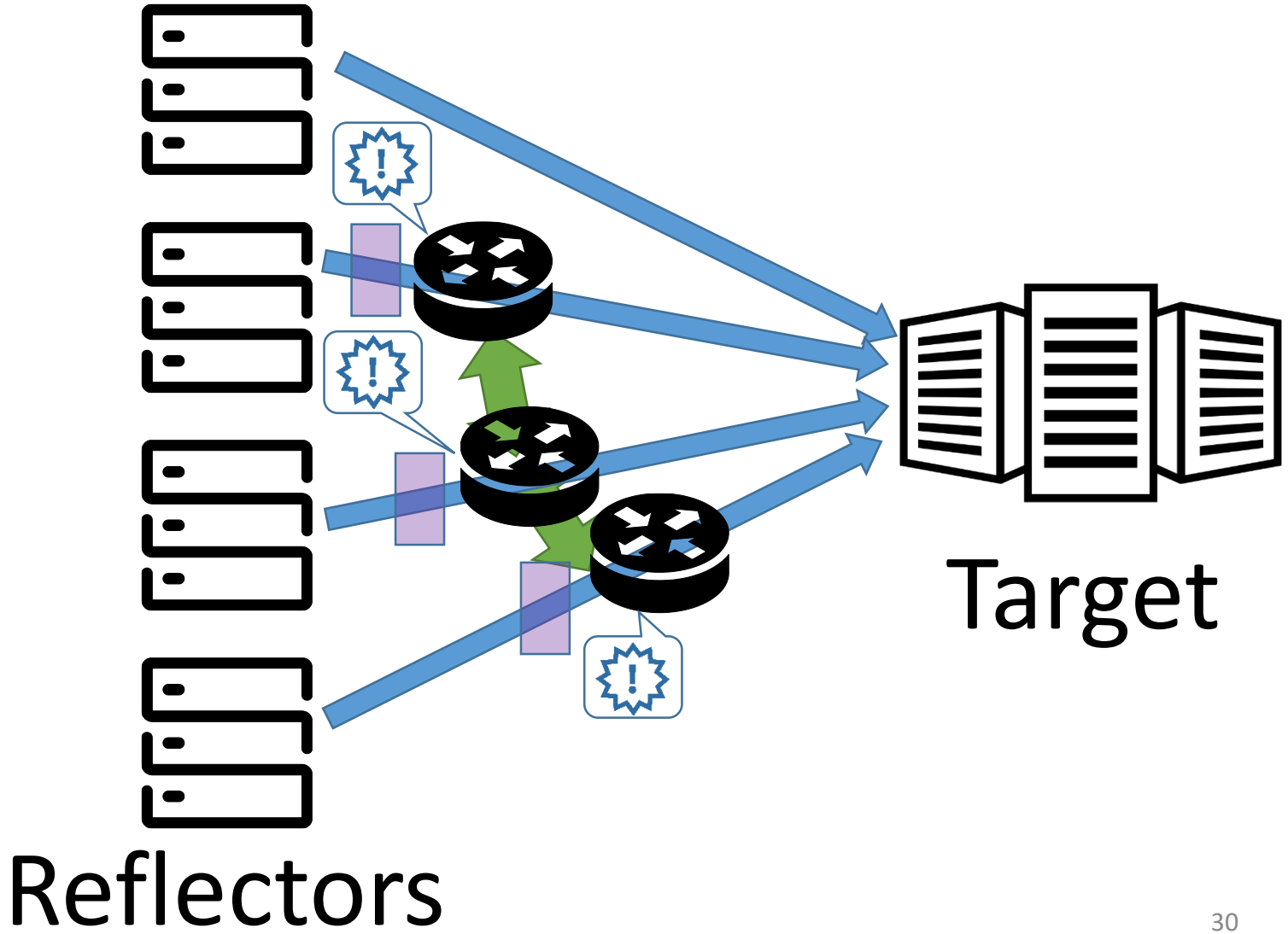
- Up to ~80% of attacks locally undetected („missed“)

Collaboration benefit



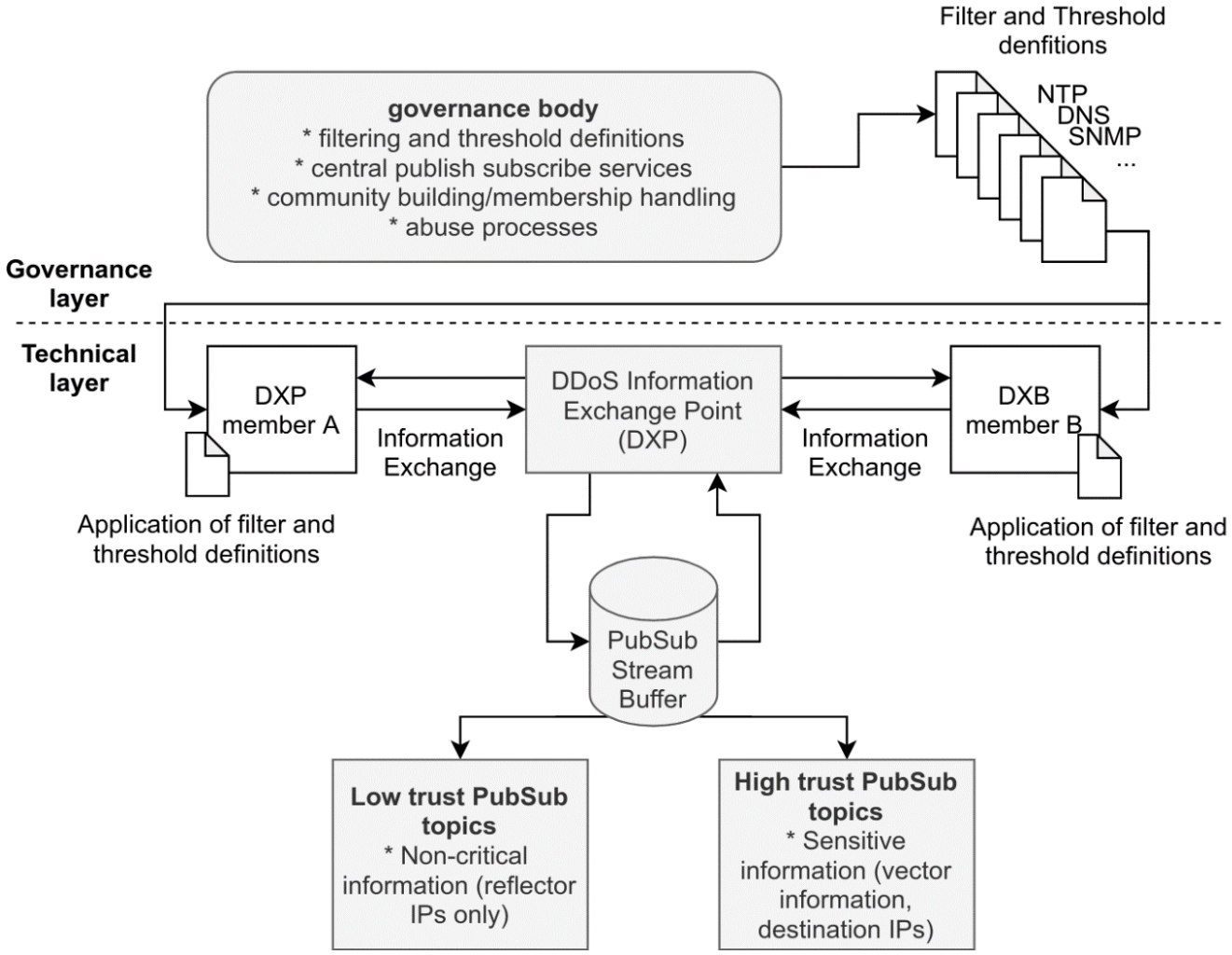
- Up to ~80% of attacks locally missed (100mb/s)
- Up to ~90% of attacks locally missed (1Gb/s)

Amplification DDoS Attacks



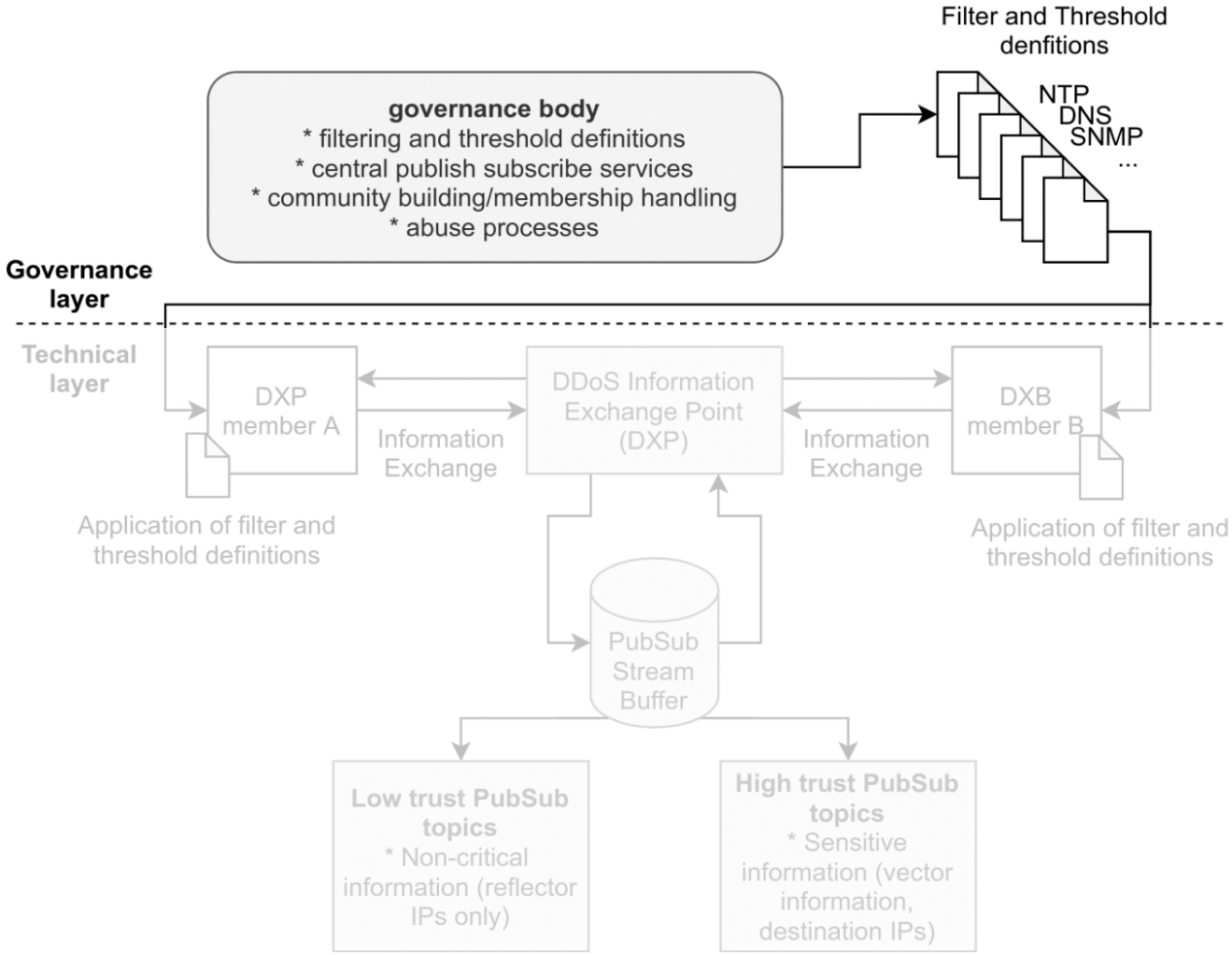
- Distance analysis
  - #hops from refelctor?
  - #hops to target?
- Collaboration benefit
- Information exchange platform

DDoS Information Exchange Point (DXP)



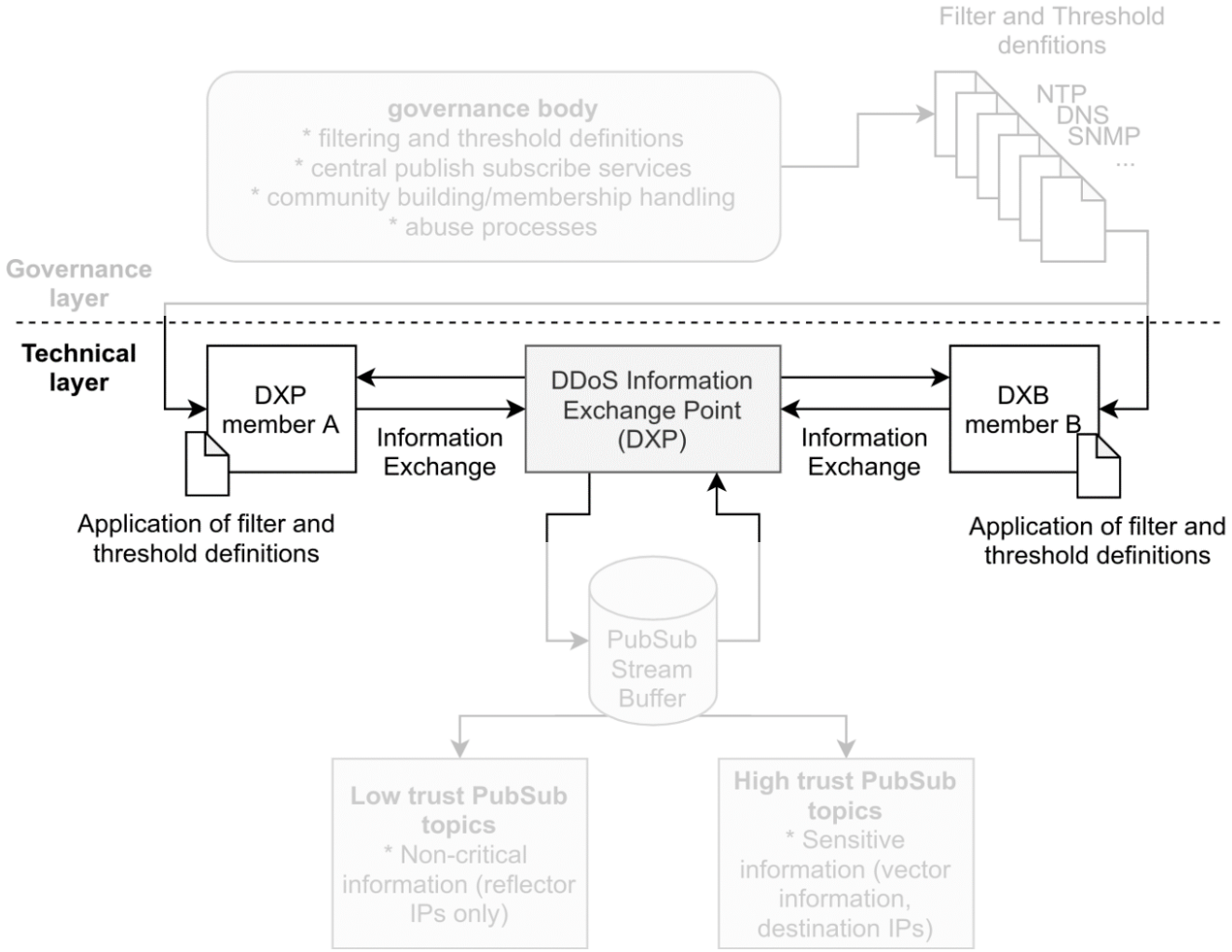
DDoS Information Exchange Point (DXP)

- Governance body
- Defines filters and thresholds
- Builds community
- Handles SLAs
- Processes abuse cases



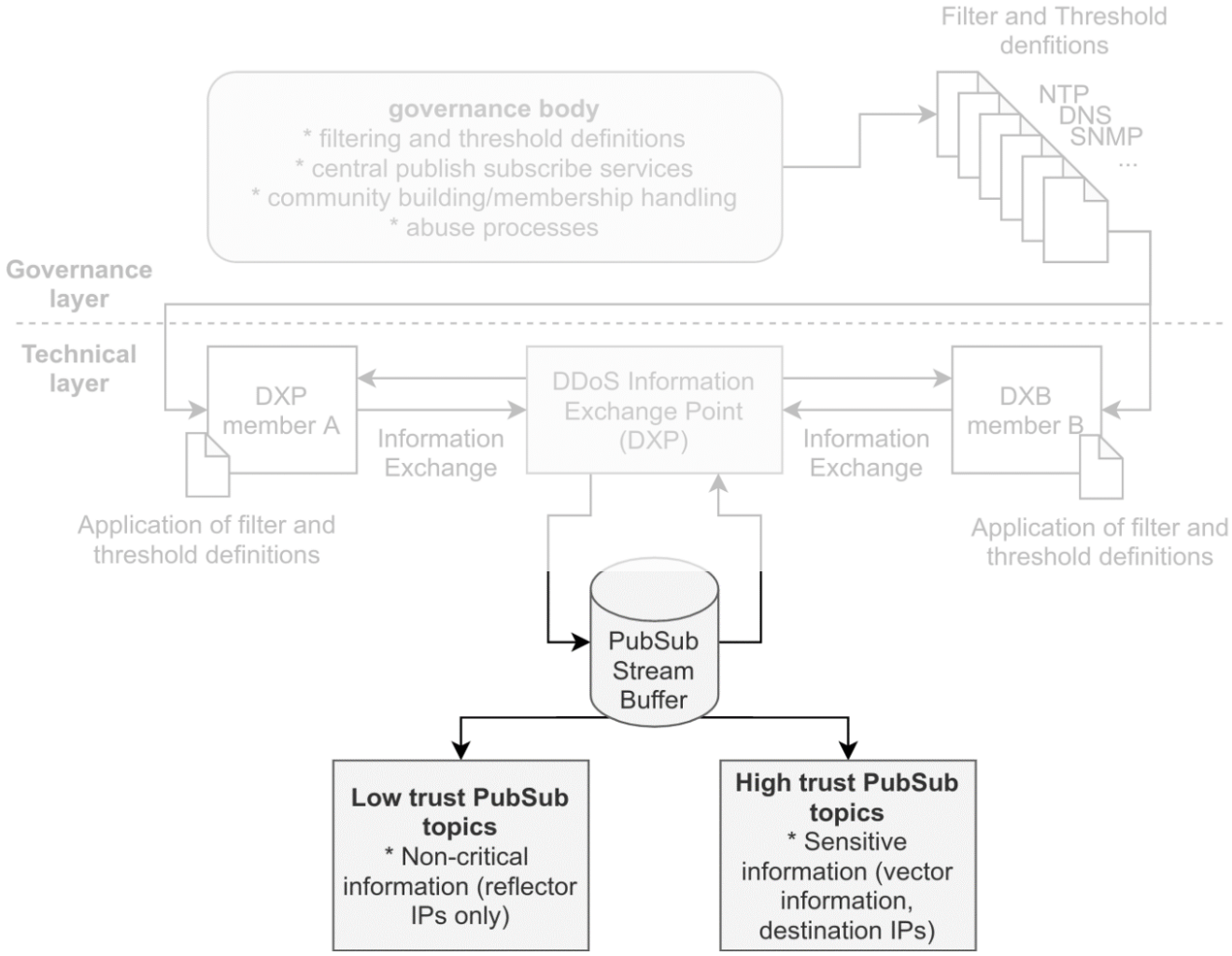
DDoS Information Exchange Point (DXP)

- Members pull and push rules from / to the DXB
- Apply filters
- Choose a trust scenario

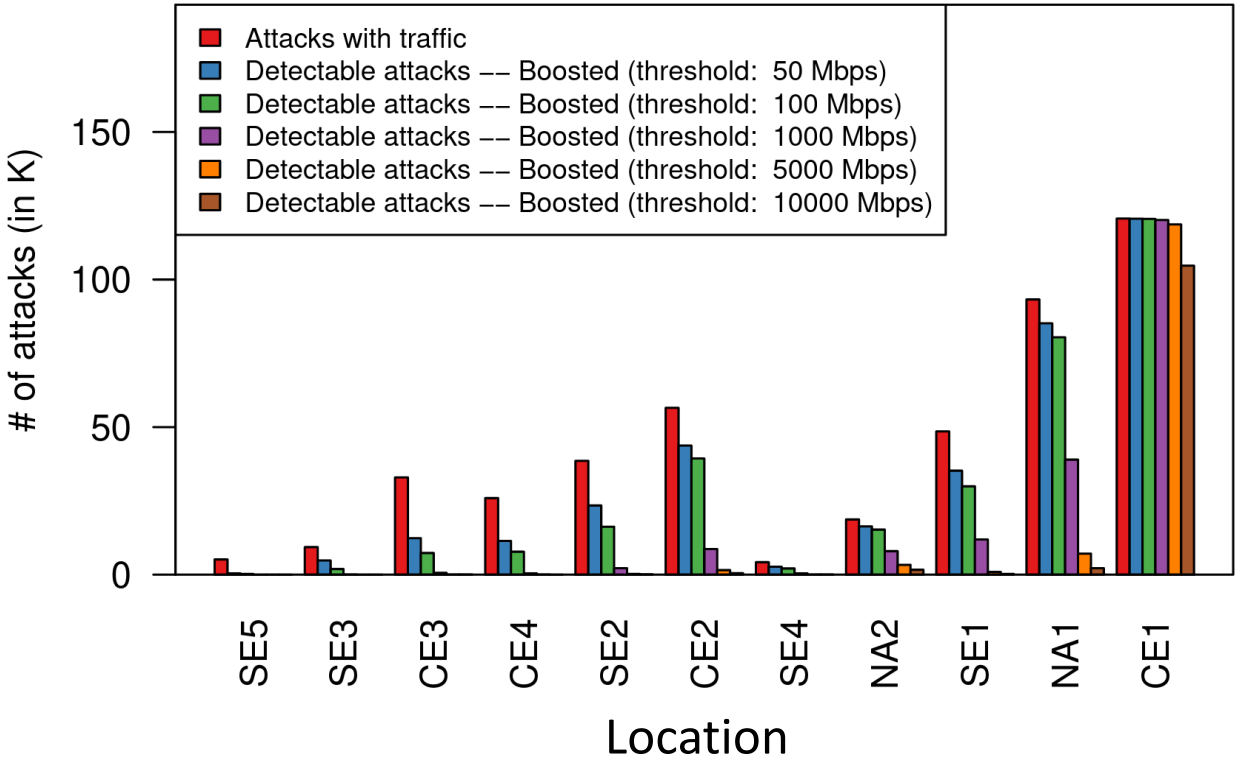


DDoS Information Exchange Point (DXP)

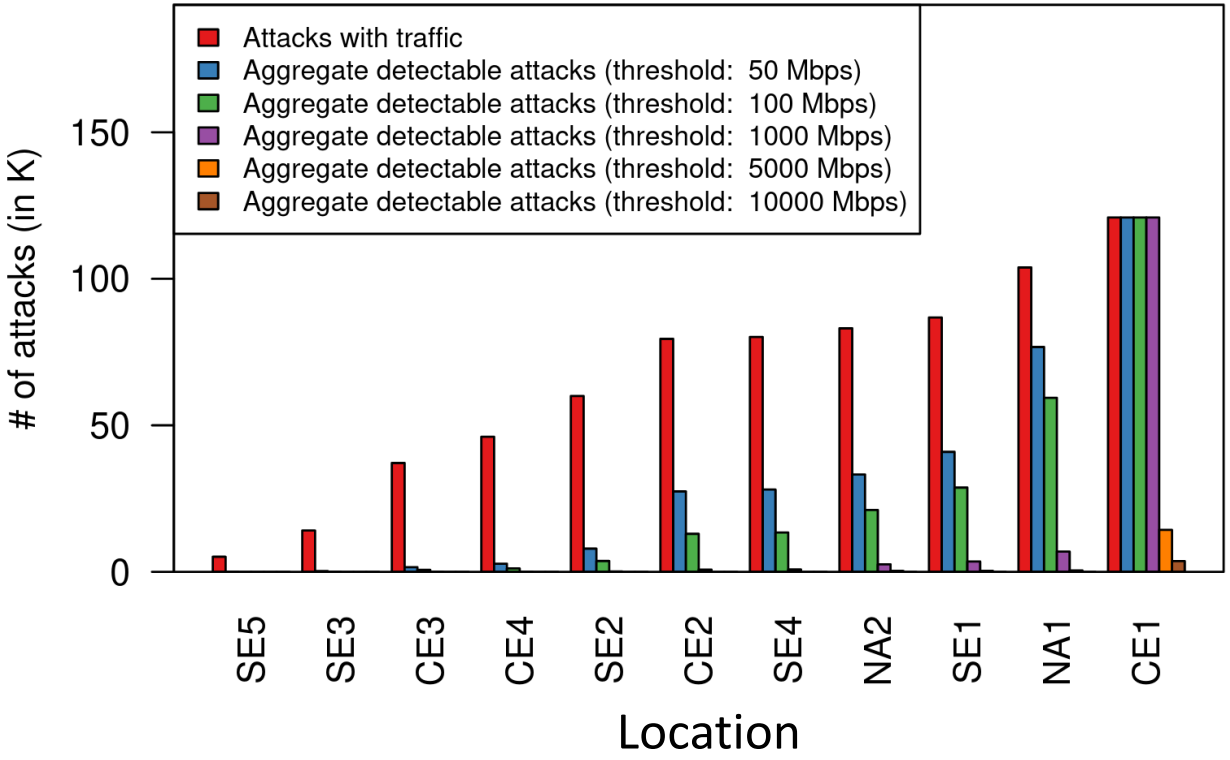
- Low trust:
  - Reflector‘s IP shared
  - Semi-sensitive
- High trust:
  - All information shared
    - Scr/dst IP & port
    - Traffic volume
    - Duration
    - ….



DXP Evaluation: Low Trust - High Trust



Low trust



High trust

Conclusion

- Quantification of DDoS origin distribution
  - About 50% of attacks in >=3 locations, about 25% in >=5 locations

Conclusion

- Quantification of DDoS origin distribution
  - About 50% of attacks in >=3 locations, about 25% in >=5 locations
- Quantification of collaboration benefit
  - >80% of the globally detectable attacks are not detected locally

Conclusion

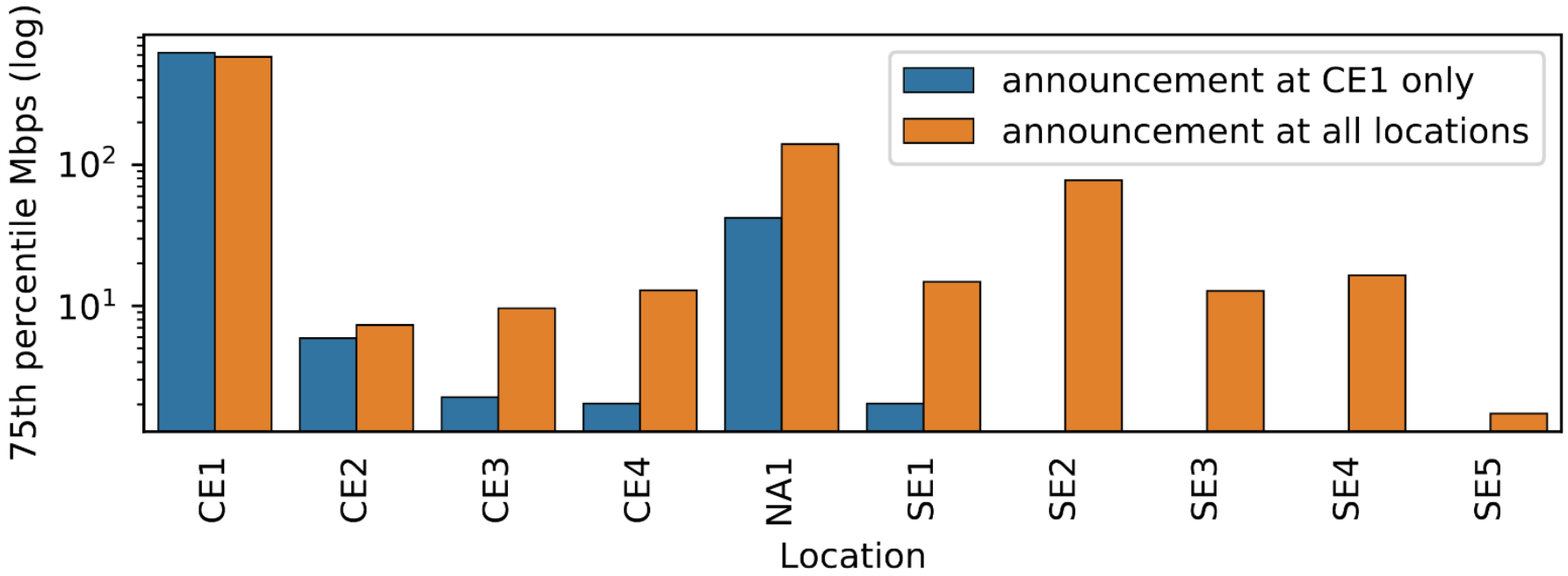
- Quantification of DDoS origin distribution
  - About 50% of attacks in >=3 locations, about 25% in >=5 locations
- Quantification of collaboration benefit
  - >80% of the globally detectable attacks are not detected locally
- Emphasis on IXP's critical role for DDoS mitigation
  - About 45% of the reflectors and about 30% of the targets are an IXP member

Conclusion

- Quantification of DDoS origin distribution
  - About 50% of attacks in >=3 locations, about 25% in >=5 locations
- Quantification of collaboration benefit
  - >80% of the globally detectable attacks are not detected locally
- Emphasis on IXP's critical role for DDoS mitigation
  - About 45% of the reflectors and about 30% of the targets are an IXP member
- Collaboration platform proposal and evaluation
  - DXP
  - Up to 90% more attack traffic detectable at a site due to collaboration

(Backup Slides)

Distance / geographical distribution analysis



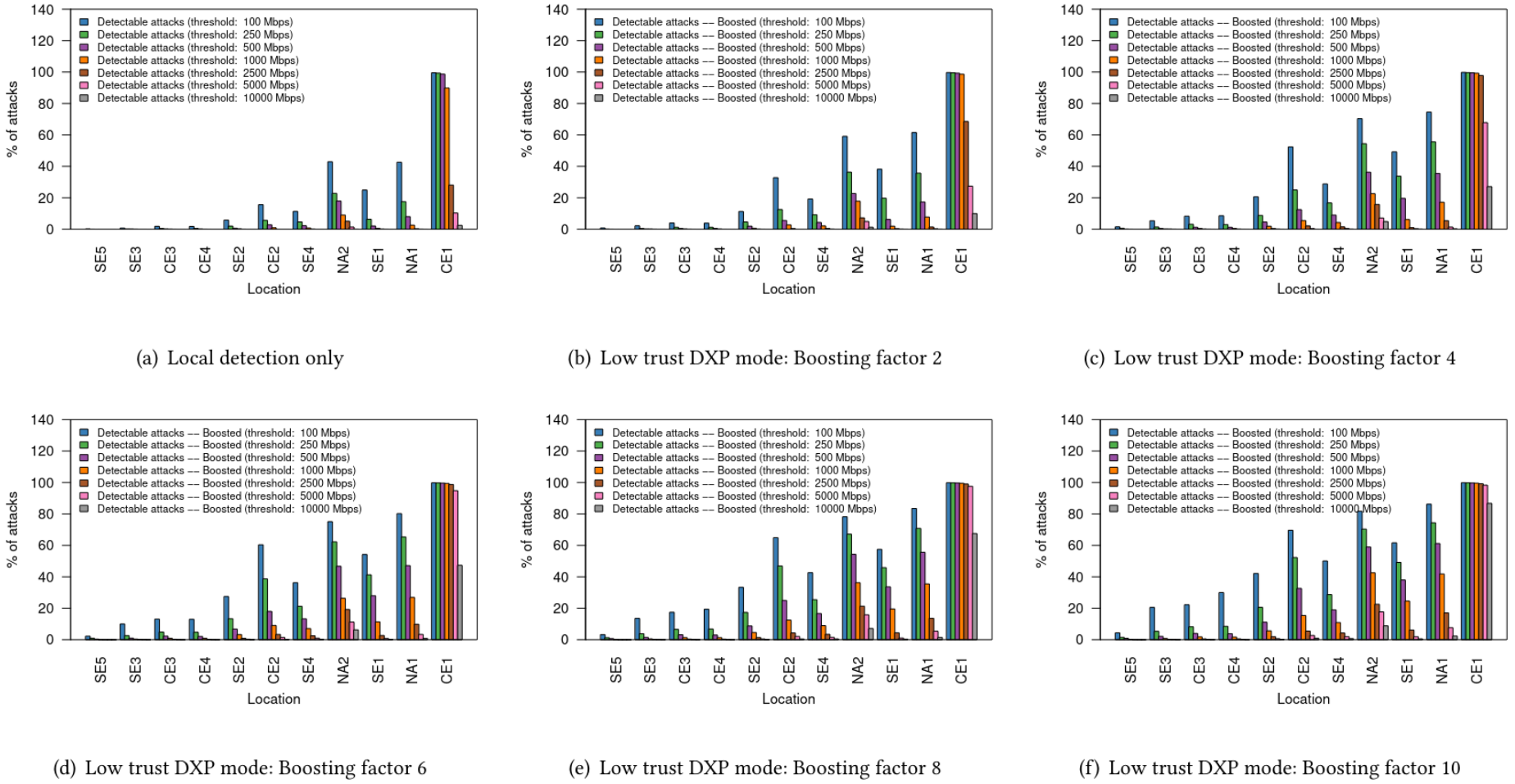
Features

Feature Class	Feature Count	Description
Sites	1	Number of sites involved in the attack
Ports	1	Number of source transport ports involved in the attack
SitesPorts	1	Sum of source transport ports seen at the sites, where the attack is visible
Dur	1	Total duration of the attack in minutes
DurAttack	1	Duration in minutes where the attack volume is greater than t (In our study: 1 Gbps)
TotalMbps	1	Volume of the attack in Mbps, summed across all sites and all source transport ports
TotalMbpsAttack	1	Volume of the attack in Mbps, summed across all sites and all source transport ports, while the volume is greater than t
TotalPeakMbps	1	Peak of the attack volume in Mbps, summed across all sites and all source transport ports
Peak Mbps	1	Peak of the attack volume in Mbps, single site, single source transport port
TotalMbpsCE1	1	Sum of the attack traffic across all source transport ports in Mbps, seen at site CE1
TotalMbpsAttackCE1	1	Sum of the attack volume across all source transport ports in Mbps, seen at site CE1 while exceeding t
TotalPeakMbpsCE1	1	Peak attack volume across all source transport ports, seen at site CE1, in Mbps
PeakMbpsCE1	1	Peak attack volume of a single source transport port, seen at site CE1, in Mbps
TotalMbpsNoCE1	1	Volume of the attack in Mbps, seen at all sites but CE1, all source transport ports
TotalMbpsAttackNoCE1	1	Volume of the attack in Mbps, seen at all sites but CE1, all source transport ports while exceeding t
TotalPeakMbpsNoCE1	1	Peak volume of the attack in Mbps, seen at all sites but CE1, across all source transport ports
PeakMbpsNoCE1	1	Peak volume of the attack in Mbps, seen at all sites but CE1, across a single transport port
Cor[Site|Port]{0.7,0.8,0.9}	6	Counter for correlation of the attack between sites and source transport ports, respectively, being greater than .7, .8, .9, respectively per minute.
TotalMbps[IXP*]	11	Volume of the attack in Mbps, as seen at the 11 sites, all source transport ports, respectively
TotalMbps[PORT*]	12	Volume of the attack in Mbps, summed across all sites, for each of the 12 source transport ports in our study
PeakMbps[IXP*]	11	Peak volume of the attack in Mbps, as seen at the 11 sites, respectively, single source transport port
PeakMbps[PORT*]	12	Peak volume of the attack in Mbps, summed across all sites, for each of the 12 source transport ports in our study
TotalMpps	1	Sum of packets transmitted for the attack across all sites, all source transport protocols, in Mpps
TotalMppsAttack	1	Sum of packets transmitted for the attack across all, all source transport ports, sites while exceeding t, in Mpps
TotalPeakMpps	1	Peak of packets transmitted for the attack, summed across all sites, all source transport ports, in Mpps
PeakMpps	1	Peak of packets transmitted for the attack at any site, single transport port, in Mpps
TotalMpps[IXP*]	11	Sum of packets transmitted across all source transport ports, at the 11 sites, respectively
TotalMpps[PORT*]	12	Sum of packets transmitted at all sites, for each of the 12 source transport protocols in our study
TotalMbpsNorm	1	Volume of the attack, summed across all source transport ports and all sites, normalized by their size

Features (cont.)

Feature Class	Feature Count	Description
TotalMbpsAttackNorm	1	Volume of the attack in Mbps, summed across all source transport ports, all sites, normalized by their size, while exceeding t
TotalPeakMbpsNorm	1	Peak of the attack volume in Mbps, summed across all source transport ports, all sites, normalized by their size
PeakMbpsNorm	1	Peak of the attack volume in Mbps, single source transport port, at a single site, normalized by their size
TotalMbpsNormNoCE1	1	Volume of the attack in Mbps, all source transport ports, seen at all sites but CE1, normalized by their size
TotalMbpsAttackNormNoCE1	1	Volume of the attack in Mbps, all source transport ports, seen at all sites but CE1, normalized by their size, while exceeding t
TotalPeakMbpsNormNoCE1	1	Peak volume of the attack, summed all source transport ports, seen at all sites but CE1, normalized by their size
PeakMbpsNormNoCE1	1	Peak volume of the attack, single source transport ports, seen at all sites but CE1, normalized by their size
TotalMbpsNorm[IXP*]	11	Volume of the attack in Mbps, all source transport ports, as seen at the 11 sites, normalized by their size, respectively
PeakMbpsNorm[IXP*]	11	Peak volume of the attack in Mbps, single source transport port, as seen at the 11 sites, normalized by their size, respectively
Allthresh-Before-[THRESHHOLD*]	7	Volume of traffic across all source ports that belong to an attack, greatest volume of a single site, before the respective threshold was exceeded
Allthresh-Detect-[THRESHHOLD*]	7	Volume of traffic across all source ports that belong to an attack, greatest volume of a single site, while the respective threshold is exceeded
Allthresh-After-[THRESHHOLD*]	7	Volume of traffic across all single source transport ports that belong to an attack, greatest volume of a single site, after the respective threshold is no longer exceeded
Allthresh-Time-[THRESHHOLD*]	7	Amount of time bins for which the attack volume across all source transport ports, greatest of al single site, exceeded the respective threshold
Allthreshnorm-Before-[THRESHHOLD*]	7	Volume of traffic across all source ports that belong to an attack, greatest of a single site, normalized by its size, before the respective threshold was exceeded
Allthreshnorm-Detect-[THRESHHOLD*]	7	Volume of traffic across all source ports that belong to an attack, greatest of a single site, normalized by its size, while the respective threshold is exceeded
Allthreshnorm-After-[THRESHHOLD*]	7	Volume of traffic across all source transport ports that belong to an attack, greatest of a single site, normalized by its size, after the respective threshold is no longer exceeded
Allthreshnorm-Time-[THRESHHOLD*]	7	Amount of time bins for which the attack volume across all source transport ports, greatest of a single site, normalized by its size, exceeded the respective threshold
SiteThresh-[IXP*]-Before-[THRESHHOLD*]	77	Volume of the attack, for every site respectively, single source transport port, before exceeding the respective threshold
SiteThresh-[IXP*]-After-[THRESHHOLD*]	77	Volume of the attack, for every site respectively, single source transport port, after the respective threshold is no longer exceeded
SiteThresh-[IXP*]-Detect-[THRESHHOLD*]	77	Volume of the attack, for every site respectively, single source transport port, while exceeding the respective threshold
SiteThresh-[IXP*]-Time-[THRESHHOLD*]	77	Amount of time bins, for every site respectively, for every threshold, single source transport port, before exceeding the respective threshold
GlobalThresh-[IXP*]-Before-[THRESHHOLD*]	77	Volume of the attack, adding all site's volume to every site respectively, all source transport ports, before exceeding the respective threshold
GlobalThresh-[IXP*]-After-[THRESHHOLD*]	77	Volume of the attack, adding all site's volume to every site respectively, all source transport ports, after the respective threshold is no longer exceeded
GlobalThresh-[IXP*]-Detect-[THRESHHOLD*]	77	Volume of the attack, adding all site's volume to every site respectively, all source transport ports, while exceeding the respective threshold
GlobalThresh-[IXP*]-Time-[THRESHHOLD*]	77	Amount of time bins, when adding all site's volume to the respective site, for every threshold, all source transport ports, while exceeding the respective threshold
SiteThreshNorm-[IXP*]-Before-[THRESHHOLD*]	77	Volume of the attack, for every site, normalized by its size, single source transport port, before exceeding the respective threshold
SiteThreshNorm-[IXP*]-After-[THRESHHOLD*]	77	Volume of the attack, for every site respectively, normalized by its size, single source transport port, after the respective threshold is no longer exceeded
SiteThreshNorm-[IXP*]-Detect-[THRESHHOLD*]	77	Volume of the attack, for every site respectively, normalized by its size, single source transport port, while exceeding the respective threshold
SiteThreshNorm-[IXP*]-Time-[THRESHHOLD*]	77	Amount of time bins, for every site respectively, normalized by its size, for every threshold, single source transport port, before exceeding the respective threshold
Total	1106	

Boosting Factor evaluation (1)



(a) Local detection only

(b) Low trust DXP mode: Boosting factor 2

(c) Low trust DXP mode: Boosting factor 4

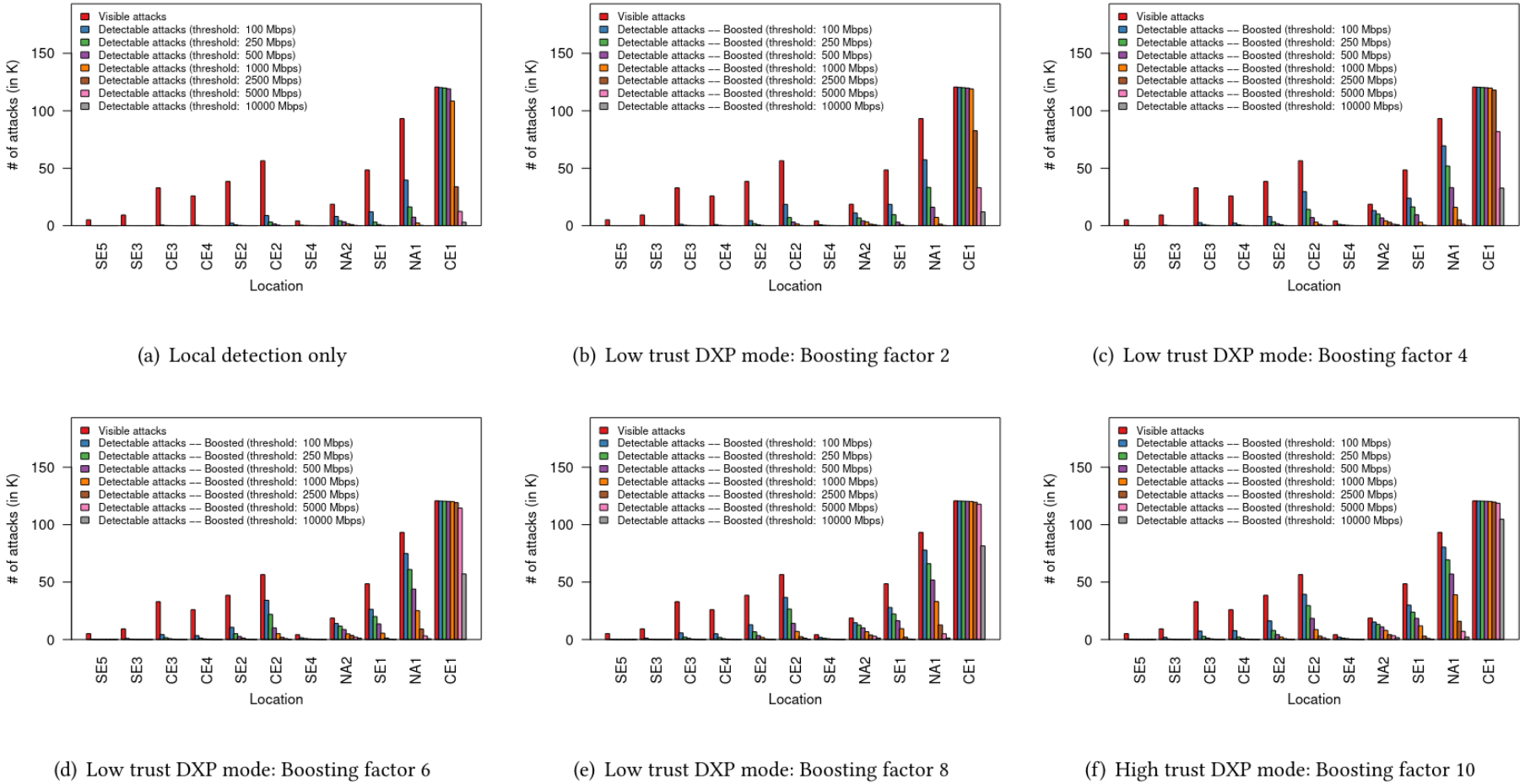
(d) Low trust DXP mode: Boosting factor 6

(e) Low trust DXP mode: Boosting factor 8

(f) Low trust DXP mode: Boosting factor 10

Figure 21: Relative: Sensitivity of the detectable DDoS attacks in the low trust DXP setting for different boosting factors.

Boosting Factor evaluation (2)



(a) Local detection only

(b) Low trust DXP mode: Boosting factor 2

(c) Low trust DXP mode: Boosting factor 4

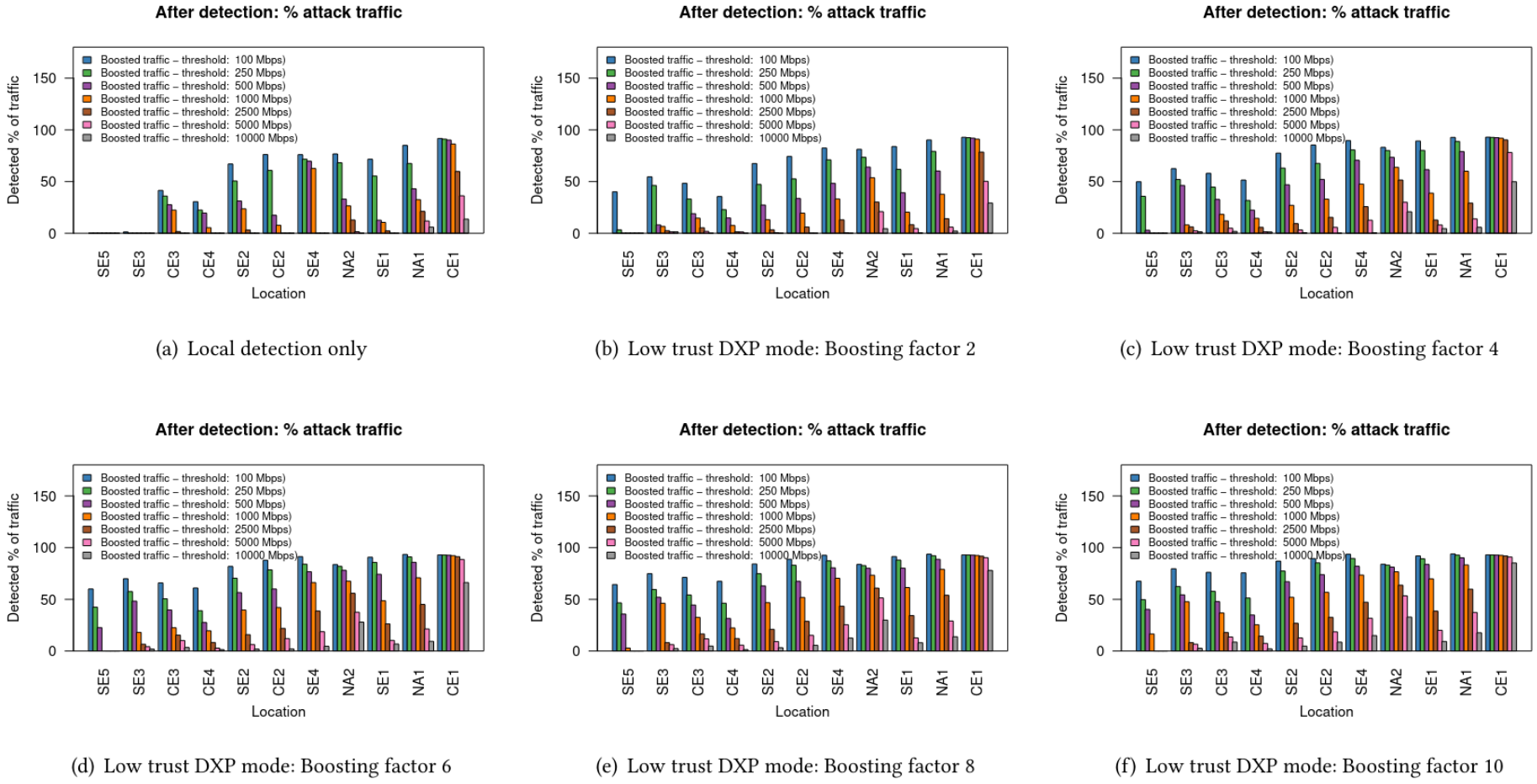
(d) Low trust DXP mode: Boosting factor 6

(e) Low trust DXP mode: Boosting factor 8

(f) High trust DXP mode: Boosting factor 10

Figure 22: Absolute: Sensitivity of the detectable DDoS attacks in the low trust DXP setting for different boosting factors.

Boosting Factor evaluation (3)



(a) Local detection only

(b) Low trust DXP mode: Boosting factor 2

(c) Low trust DXP mode: Boosting factor 4

(d) Low trust DXP mode: Boosting factor 6

(e) Low trust DXP mode: Boosting factor 8

(f) Low trust DXP mode: Boosting factor 10

Figure 23: Sensitivity of the share of the attack traffic detected in the low trust DXP setting for different boosting factors.