Challenges in Inferring Spoofed Traffic at IXPs

Lucas Müller  
UFRGS/CAIDA

Matthew Luckie  
University of Waikato

Bradley Huffaker  
CAIDA/UC San Diego

Kc Claffy  
CAIDA/UC San Diego

Marinho Barcellos  
UFRGS/University of Waikato

ACM CoNEXT 2019 — Orlando, Florida, U.S.A.  
December 9-12, 2019
Broader visibility of networks that do not filter spoofed packets
Consequences:
spoofed denial-of-service (DoS) attacks
Consequences: spoofed denial-of-service (DoS) attacks

400Gbps: Winter of Whopping Weekend DDoS Attacks

03 Mar 2016 by Marek Majkowski.

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

Carlos Morales on March 5, 2018.

Brazil hit by 30 DDoS attacks per hour in 2017

The country is part of a global ranking of the five nations most targeted by cybercriminals, says study.

By Angelica Mari for Brazil Tech | February 21, 2018 -- 14:59 GMT (06:59 PST) | Topic: Security
Consequences:
spoofed denial-of-service (DoS) attacks

400Gbps: Winter of Whopping Weekend DDoS Attacks
03 Mar 2016 by Marek Majkowski.

Security
How many Internet of S**t devices knocked out Dyn? Fewer than you may expect
DNS really needs to be fixed if it can be taken out by 100,000 home devices
By Richard Chirgwin 27 Oct 2016 at 01:30

Bezos DDoS'd: Amazon Web Services' DNS systems knackered by hours-long cyber-attack
Distributed assault hampering connectivity for websites, apps, customers are
By Chris Williams, Editor in Chief 22 Oct 2019 a

NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack; The Terabit Attack Era Is Upon Us
Carlos Morales on March 5, 2018.

Brazil hit by 30 DDoS attacks per hour in 2017
The country is part of a global ranking of the five nations most likely
By Angelica Mari for Brazil Tech | February 21, 2018 -- 14:59 GMT (06:59 PST) | Topic: Se

Rio 2016 Olympics Suffered Sustained 540Gbps DDoS Attacks
Ben Sullivan, August 31, 2016, 5:31 pm

US service provider survives the biggest recorded DDoS in history
Nearly 100,000 memcached servers are imperiling the stability of the Internet.
DAN GOODIN - 3/5/2018, 1:24 PM
Consequences:
spoofed denial-of-service (DoS) attacks

Bezos DDoS'd: Amazon Web Services' DNS systems knackered by hours-long cyber-attack
Distributed assault hampering connectivity for websites, apps, customers are

NETSCOUT Arbor Confirms
The 2016 Olympics
Sustained
Gbps DDoS
Attacks

The real cause of large DDoS - IP Spoofing
06 Mar 2018 by Marek Majkowski.

US service provider survives the biggest recorded DDoS in history
Nearly 100,000 memcached servers are imperiling the stability of the Internet.

Brazil hit by 30 DDoS attacks per hour in 2017
The country is part of a global ranking of the five nations most...
IP Spoofing

Architectural limitation that provides an attacker with the ability to send packets using spoofed source IP addresses
IP Spoofing

Architectural limitation that provides an attacker with the ability to send packets using spoofed source IP addresses

IETF introduced Best Current Practices (BCPs) recommending that networks block these packets — i.e., implement Source Address Validation (SAV)
IP Spoofing

Architectural limitation that provides an attacker with the ability to send packets using spoofed source IP addresses

IETF introduced Best Current Practices (BCPs) recommending that networks block these packets — i.e., implement Source Address Validation (SAV)

- Compliance with these filtering practices has misaligned incentives
- Deploying SAV is primarily for the benefit of other networks
Remediation and Policy Interventions
Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale.
Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

- Definitive method requires an active probing vantage point in each network being tested
Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

- Definitive method requires an active probing vantage point in each network being tested

- ~65K independently routed networks
Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

• Definitive method requires an active probing vantage point in each network being tested

• ~65K independently routed networks

• Limited feasibility for a comprehensive assessment of Internet spoofing

CAIDA’s 2017 visualization of IPv4 Internet topology at the Autonomous System (AS) level
Remediation and Policy Interventions

We need to identify networks lacking SAV deployment, but doing this is challenging at Internet scale

- Definitive method requires an active probing vantage point in each network being tested
- ~65K independently routed networks
- Limited feasibility for a comprehensive assessment of Internet spoofing

Broader visibility may lie in the capability to infer lack of SAV compliance from aggregated Internet traffic data
our goal

design and develop a methodology to identify spoofed traffic crossing an IXP and infer lack of SAV
Programa por uma Internet mais Segura
Ações no IX.br

Introdução

O IX.br está presente em 31 localidades no Brasil, por meio da Troca de Tráfego Multilateral (ATM), chamado em inglês de Multi-Access Telecommunications e (ii) a Troca de Tráfego Bilateral, em inglês Bilateral Peering. O ATM troca tráfego entre si, como regra geral, cada AS troca tráfego com um ou mais ASs próximos na Troca de Tráfego Bilateral apenas dois ASs participam, utilizando a camada 2 exclusiva (uma VLAN bilateral).

O Acordo de Troca de Tráfego Multilateral (ATM) na compartilhação para a troca de tráfego IPv4 (ATMv4) e outra. Cada PTT possui dois ou mais route servers, que também são route servers em ATM v4 para centralizar o recebimento de tráfego e permitir que, com uma única localidade seja carregada e mantida. O estabelecimento de um ATM de tráfego de ATM multilateral, nem todos. Mesmo que os route servers possam estarem presentes nas VLANs do ATMv4 ou ATMv6, para fins.

Existem casos em que o participante esteja presente na VLAN de sessão BGP com o route server, mas fecha sessão BGP com os route servers internos e existem route servers em ATM v4 para centralizar o recebimento de tráfego e permitir que, com uma única localidade seja carregada e mantida. O estabelecimento de um ATM de tráfego de ATM multilateral, nem todos. Mesmo que os route servers possam estarem presentes nas VLANs do ATMv4 ou ATMv6, para fins.

Existem casos em que o participante esteja presente na VLAN de sessão BGP com o route server, mas fecha sessão BGP com os route servers internos e existem route servers em ATM v4 para centralizar o recebimento de tráfego e permitir que, com uma única localidade seja carregada e mantida. O estabelecimento de um ATM de tráfego de ATM multilateral, nem todos. Mesmo que os route servers possam estarem presentes nas VLANs do ATMv4 ou ATMv6, para fins.

Desta forma, neste cenário, temos em cada PTT do IX.br:

- um ambiente privado, formado pelos Acordos Bilaterais através VLANs, sejam VLANs bilaterais ou as VLANs de PTTs;
- um ambiente compartilhado por meio deroute servers com o route server e/ou ATMv6 e com sessões BGP com os route servers.

MANRS is an important step toward a globally robust and secure routing infrastructure

The MANRS Actions were initially designed for network operators, but Internet Exchange Points (IXPs) should also play an active role in protecting the Internet. IXPs represent active communities with common operational objectives and already contribute to a more resilient and secure Internet infrastructure.

MANRS can help IXPs build safe neighborhoods, leveraging the MANRS security baseline. It also demonstrates an IXP’s commitment to security and sustainability of the Internet ecosystem, and dedication to providing high quality services.

IXPs are important partners in the MANRS community
Contributions
Contributions

1. Challenges

Provide detailed analysis of methodological challenges for inferring spoofed packets at IXPs
Contributions

1. Challenges
Provide detailed analysis of methodological challenges for inferring spoofed packets at IXPs

2. Methodology
Developed a methodology to classify flows, navigating through all challenges identified
Contributions

1. Challenges
Provide detailed analysis of methodological challenges for inferring spoofed packets at IXPs

2. Methodology
Developed a methodology to classify flows, navigating through all challenges identified

3. Observations and Lessons
Used our methodology and compare it with the state-of-the-art[1] at an IXP in Brazil, reporting our findings

Bird’s Eye View
Bird’s Eye View

IXP traffic flow data and topology information
Bird’s Eye View

IXP traffic flow data and topology information

valid IP address space per Autonomous System (AS)
Bird’s Eye View

IXP traffic flow data and topology information

valid IP address space per Autonomous System (AS)

Classification Pipeline Methodology

list of networks with and without SAV, with evidence to support
Challenges: Pieces of the Puzzle
Challenges: Pieces of the Puzzle

1. Identify Valid Source Address Space
Challenges: Pieces of the Puzzle

1. Identify Valid Source Address Space
   - there is no global registry that contains ground truth
Challenges: Pieces of the Puzzle

1. Identify Valid Source Address Space
   - there is no global registry that contains ground truth
   - need to infer the set of valid source addresses
Challenges: Pieces of the Puzzle

1. Identify Valid Source Address Space
   - there is no global registry that contains ground truth
   - need to infer the set of valid source addresses

2. Tackle IXP Topology and Traffic Visibility Properties
Challenges: Pieces of the Puzzle

1. Identify Valid Source Address Space
   - there is no global registry that contains ground truth
   - need to infer the set of valid source addresses

2. Tackle IXP Topology and Traffic Visibility Properties
   - understand modern IXP interconnection practices
Challenges: Pieces of the Puzzle

1. Identify Valid Source Address Space
   - there is no global registry that contains ground truth
   - need to infer the set of valid source addresses

2. Tackle IXP Topology and Traffic Visibility Properties
   - understand modern IXP interconnection practices
   - implications on visibility of both topology and traffic
1. Identify Valid Source Address Space

IP Address Space
1. Identify Valid Source Address Space

- IP Address Space
  - Usable
  - IETF Reserved Bogons
1. Identify Valid Source Address Space

- IP Address Space
  - Usable
    - Routed
    - Unassigned
  - IETF Reserved Bogons
1. Identify Valid Source Address Space

IP Address Space

Usable

Routed

Unassigned

IETF Reserved Bogons

Inferred based on BGP data and the links established by each AS
1. Identify Valid Source Address Space

IP Address Space

- Usable
  - Routed
  - Unassigned

- IETF Reserved Bogons

Inferred based on BGP data and the links established by each AS

Customer Cones
Define the set of ASes a given AS can reach through its customers
2. Tackle IXP Topology and Traffic Visibility Properties

Focus on understanding operational complexities of the vantage point

AS64505
Prefix-level
Customer Cone

168.228.252.0/22
200.17.80.0/20
200.132.59.0/24
200.236.32.0/19
200.19.0.0/21
200.238.0.0/18
...

AS64500

NETFLIX

AS64620

amazon

AS64250

YouTube

AS65520

Facebook

AS65500

LinkedIn

IXP

Amazon’s AS
Prefix-level
Customer Cone

13.32.136.2/23
52.216.180/24
75.2.82.0/24
161.38.206.0/23
216.137.62.0/24
...

...
2. Tackle IXP Topology and Traffic Visibility Properties

Focus on understanding operational complexities of the vantage point.
2. Tackle IXP Topology and Traffic Visibility Properties
2. Tackle IXP Topology and Traffic Visibility Properties
2. Tackle IXP Topology and Traffic Visibility Properties

Legend:
- **Switch**: Physical connection
- **Switch**: Physical connection and VLAN configured to neighbor
- **CF**: Colocation Facility
- **AS Z**: Autonomous System

AS A — AS B
AS C — AS D
CF #1 — Core Switch — CF #2
CF #3 — Core Switch — CF #4

IXP switching fabric #X

AS A
AS C
CF #1
CF #3

AS B
AS D
CF #2
CF #4

Legend:
- Physical connection
- Physical connection and VLAN configured to neighbor
- CF: Colocation Facility
- AS Z: Autonomous System
2. Tackle IXP Topology and Traffic Visibility Properties

Legend:
- **Switch**: Physical connection
- **Physical connection and VLAN configured to neighbor**
- **CF: Colocation Facility**
- **AS Z**: Autonomous System
- **Reseller**
- **Reseller-Tag**: Stacked VLAN (IEEE 802.1q, QinQ)
- **IXP-Tag**: Stacked VLAN (IEEE 802.1q, QinQ)
2. Tackle IXP Topology and Traffic Visibility Properties

Legend:
- **Switch**: Physical connection
- **Physical connection and VLAN configured to neighbor**
- **CF: Colocation Facility**
- **AS Z**: Autonomous System
- **Res Z**: Reseller
- **Reseller-Tag**: Stacked VLAN (IEEE 802.1q, QinQ)
- **IXP-Tag**:
2. Tackle IXP Topology and Traffic Visibility Properties
2. Tackle IXP Topology and Traffic Visibility Properties

- In practice IXPs, CFs and resellers offer complex services
- Interconnection practices occur below and are thus not visible to the IP layer or in the BGP Protocol
- Must take them into account during the traffic classification processing
### 2. Tackle IXP Topology and Traffic Visibility Properties

<table>
<thead>
<tr>
<th>(1) <strong>c2p</strong>: customer-to-provider</th>
<th>(2) <strong>p2p</strong>: peer-to-peer</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Legend

<table>
<thead>
<tr>
<th><strong>Pr</strong>: Provider</th>
<th><strong>Pe</strong>: Peer</th>
<th><strong>Cu</strong>: Customer</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>(3) <strong>p2c</strong>: provider-to-customer</th>
<th>(4) <strong>s2s</strong>: sibling-to-sibling</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(Y will not transit packets sourced in Z to X.)

(Z will transit packets sourced in Z to X.)
2. Tackle IXP Topology and Traffic Visibility Properties

(1) **c2p**: customer-to-provider

(2) **p2p**: peer-to-peer

(3) **p2c**: provider-to-customer

(4) **s2s**: sibling-to-sibling

Legend:

- **Pr**: Provider
- **Pe**: Peer
- **Cu**: Customer

**A**

**B**

**Cu**

**customer** B to **provider** A

**Pr**

**Pe**

**G**

**H**

**E**

**F**

**sibling** G to **sibling** H

**Y** will not transit packets sourced in Z to X.

**Y** will transit packets sourced in Z to X.
2. Tackle IXP Topology and Traffic Visibility Properties

(1) **c2p**: customer-to-provider

- **customer** B to **provider** A

(2) **p2p**: peer-to-peer

- **peer** C to **peer** D

(3) **p2c**: provider-to-customer

(4) **s2s**: sibling-to-sibling

---

**Legend**

- **Pr**: Provider
- **Pe**: Peer
- **Cu**: Customer
2. Tackle IXP Topology and Traffic Visibility Properties

(1) **c2p**: customer-to-provider

- **A** (Provider)
- **B** (Customer) to **A** (Provider)

(2) **p2p**: peer-to-peer

- **C** (Peer)
- **D** (Peer)

(3) **p2c**: provider-to-customer

(4) **s2s**: sibling-to-sibling

**Legend**

- **Pr**: Provider
- **Pe**: Peer
- **Cu**: Customer

**Transits only traffic from its customer cone**
2. Tackle IXP Topology and Traffic Visibility Properties

(1) **c2p**: customer-to-provider

- **A** (Provider) to **B** (Customer)
- **B** to **A** (Provider)

(2) **p2p**: peer-to-peer

- **C** (Provider) to **D** (Peer)
- **D** to **C** (Provider)

(3) **p2c**: provider-to-customer

- **Pr** (Provider) to **Pe** (Peer) to **Cu** (Customer)
- **Pe** to **Cu** (Customer) to **Pr** (Provider)

(4) **s2s**: sibling-to-sibling

- **E** (Provider) to **F** (Customer)
- **F** to **E** (Provider)

**Legend**

- **Pr**: Provider
- **Pe**: Peer
- **Cu**: Customer

Transits only traffic from its customer cone
2. Tackle IXP Topology and Traffic Visibility Properties

(1) **c2p**: customer-to-provider

- Customer B to Provider A

(2) **p2p**: peer-to-peer

- Peer C to Peer D

(3) **p2c**: provider-to-customer

- Provider E to Customer F

(4) **s2s**: sibling-to-sibling

- Sibling G to Sibling H

**Legend**

<table>
<thead>
<tr>
<th>Pr</th>
<th>Pe</th>
<th>Cu</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider</td>
<td>Peer</td>
<td>Customer</td>
</tr>
</tbody>
</table>

- Y will not transit packets sourced in Z to X.
- Y will transit packets sourced in Z to X.

- Transits only traffic from its customer cone
2. Tackle IXP Topology and Traffic Visibility Properties

(1) **c2p**: customer-to-provider

`A` to `B`
`B` to `A`

**Legend**
- **Pr**: Provider
- **Pe**: Peer
- **Cu**: Customer

(2) **p2p**: peer-to-peer

`C` to `D`
`D` to `C`

(3) **p2c**: provider-to-customer

`Pr` to `Cu`
`E` to `F`

(4) **s2s**: sibling-to-sibling

`Pr` to `Pe`
`Cu` to `G`

**Legend**
- **Pr**: Provider
- **Pe**: Peer
- **Cu**: Customer

**Transits only traffic from its customer cone**

**Transits all traffic**
Spoofer-IX Inference Method: Putting the Pieces Together

See paper for details
Spoofer-IX Inference Method: Putting the Pieces Together

Divided into two stages

See paper for details
Spoofer-IX Inference Method: Putting the Pieces Together

Divided into two stages

- Stage 1: build the Customer Cone

See paper for details
Spoofer-IX Inference Method: Putting the Pieces Together

Divided into two stages
- Stage 1: build the Customer Cone
- Stage 2: classify IXP traffic

See paper for details
Stage 1: Build the Customer Cone

Subtleties in Cone Construction

**Full Cone**
(state-of-the-art [1])

**Customer Cone**
(Prefix-level Customer Cone)

Brief overview in this talk
See paper for full details
Stage 1: Build the Customer Cone

Subtleties in Cone Construction

**Full Cone**
(state-of-the-art [1])

- Do not distinguish types of AS-relationships

**Customer Cone**
(Prefix-level Customer Cone)

- Takes into account the semantics of AS-relationships [2]

Brief overview in this talk
See paper for full details
Stage 1: Build the Customer Cone

Subtleties in Cone Construction

**Full Cone**  
(state-of-the-art [1])

- Do not distinguish types of AS-relationships
  - More permissive
  - Aims to minimize false positives
  - Acknowledge that intentionally sacrifices specificity, i.e., inflating the address space considered legitimate
  - Limited input BGP data sanitization

---

**Customer Cone**  
(Prefix-level Customer Cone)

- Takes into account the semantics of AS-relationships [2]


Brief overview in this talk  
See paper for full details
Stage 1: Build the Customer Cone

Subtleties in Cone Construction

**Full Cone**
(state-of-the-art [1])

- Do not distinguish types of AS-relationships
- More permissive
- Aims to minimize false positives
- Acknowledge that intentionally sacrifices specificity, i.e., inflating the address space considered legitimate
- Limited input BGP data sanitization

**Customer Cone**
(Prefix-level Customer Cone)

- Takes into account the semantics of AS-relationships [2]
- More restrictive
- Aims to be accurate
- Rigorous AS-Path (BGP) sanitization
- Accounts for hybrid relationships and accommodates traffic engineering practices

---


Brief overview in this talk
See paper for full details
Stage 2: Classify IXP Traffic

start: for each flow

- Is SRC IP Bogon? No → Yes → Phase 1
  - Yes: Bogon
  - No: Is SRC IP Unassigned? Yes → Out-of-Cone
  - No: Is SRC IP Unassigned? No → Phase 2
    - Yes: Unverifiable
    - No: Is SRC AS in Ingress AS's Customer Cone? Yes → In-cone
    - No: Out-of-Cone

source IP only + VLANs

source IP + ingress and egress AS + VLANs
Stage 2: Classify IXP Traffic

**Phase 1: filter Bogon and Unassigned addresses**
this phase is independent of any routing semantics

start: for each flow

- **Is SRC IP Bogon?**
  - Yes → **Bogon**
  - No → **Is SRC IP Unassigned?**

- **Is SRC IP Unassigned?**
  - Yes → **Phase 1**
  - No → **Do we have Mac-to-AS Mapping (ingress, egress) validation?**

- **Do we have Mac-to-AS Mapping (ingress, egress) validation?**
  - Yes → **Given the ingress and egress ASs, is there a verifiable Customer Cone?**
  - No → **Unverifiable**

- **Given the ingress and egress ASs, is there a verifiable Customer Cone?**
  - Yes → **Is SRC AS in Ingress AS's Customer Cone?**
  - No → **Out-of-Cone**

- **Is SRC AS in Ingress AS's Customer Cone?**
  - Yes → **In-cone**
  - No → **Phase 3**
Stage 2: Classify IXP Traffic

Phase 2: filter Unverifiable packets
packets that are not suitable to inference of spoofing using the inferred cones or due to IXP topology and traffic visibility impediments
Stage 2: Classify IXP Traffic

Phase 3: classify Packets with Customer Cone

packets whose source IP belongs to the sending AS’s customer cone address space are classified as *in-cone*. Otherwise, we classify the packet as *out-of-cone*.
Longitudinal Study

• Study realized at the third largest IXP at the Brazilian IX.br ecosystem

• Transports up to 200 Gbps of traffic among 200+ members

• Two uninterrupted sFlow datasets:
  - April 1 to May 6, 2017 (5 weeks)
  - May 1 to June 5, 2019 (5 weeks)
  - sampling rate 1/4096

• Compare our method with Full Cone (state-of-the-art) [1]

What Have We Found?

• No strong evidence of pervasive presence of spoofed traffic for the different observation periods in 2017 and 2019

• Found an upper bound volume of out-of-cone traffic to be more than an order of magnitude less than the state-of-the-art method

• Our method reveals inaccuracies in methods that are agnostic to AS-relationship semantics

Brief overview
See paper for details
Longitudinal Traffic Classification

(i) In-cone

(ii) Unverifiable

(iii) Out-of-cone

(iv) Bogon

Apr 1 - May 6, 2017

May 1 - Jun 5, 2019
Longitudinal Traffic Classification

(i) In-cone

(ii) Unverifiable

(iii) Out-of-cone

(iv) Bogon

Apr 1 - May 6, 2017

May 1 - Jun 5, 2019
Longitudinal Traffic Classification

(i) In–cone

(ii) Unverifiable

(iii) Out–of–cone

3.7 Mbps

(iv) Bogon

Apr 1 - May 6, 2017

(i) In–cone

(ii) Unverifiable

(iii) Out–of–cone

40 Mbps

(iv) Bogon

May 1 - Jun 5, 2019
Longitudinal Traffic Classification

15.3% of total traffic exchanged at the IXP

(i) In–cone

(ii) Unverifiable

(iii) Out–of–cone

3.7 Mbps

(iv) Bogon

15.3% of total traffic exchanged at the IXP

(i) In–cone

(ii) Unverifiable

(iii) Out–of–cone

40 Mbps

(iv) Bogon

Apr 1 - May 6, 2017

May 1 - Jun 5, 2019
Longitudinal Traffic Classification

84.65% of the traffic classified as In-cone

84.65% of the traffic classified as In-cone

3.7 Mbps

40 Mbps

Apr 1 - May 6, 2017

May 1 - Jun 5, 2019
Longitudinal Traffic Classification

(i) In–cone

(ii) Unverifiable

(iii) Out–of–cone

(iv) Bogon

Traffic Volume (Gbps)

Week 1 | Week 2 | Week 3 | Week 4 | Week 5

(i) In–cone

(ii) Unverifiable

(iii) Out–of–cone

(iv) Bogon

Traffic Volume (Gbps)

Apr 1 - May 6, 2017

May 1 - Jun 5, 2019
Comparison of Out-of-cone Traffic Inferred by Each Method

(a) Spoofer-IX

(b) State-of-the-art
Comparison of Out-of-cone Traffic Inferred by Each Method

(a) Spoofer-IX

Spoofer-IX inferred a peak of 40 Mbps

(b) State-of-the-art
Comparison of Out-of-cone Traffic Inferred by Each Method

(a) Spoofer-IX

Spoofer-IX inferred a peak of 40 Mbps

(b) State-of-the-art

Full Cone method inferred a peak of 2.5 Gbps
92.6% was sent from a provider to a customer across the exchange — where no cone of valid addresses applies.
Comparison of Out-of-cone Traffic Inferred by Each Method

(a) Spoofer-IX

(i) Out-of-Cone Traffic

(ii) IP Address Churn

(b) State-of-the-art

(i) Out-of-Cone Traffic

(ii) IP Address Churn

activity and churn in active IP addresses
Comparison of Out-of-cone Traffic Inferred by Each Method

(a) Spoofer-IX

(ii) IP Address Churn

(iii) ASes and Countries

(b) State-of-the-art

(ii) IP Address Churn

(iii) ASes and Countries

spatio-temporal properties in active IP addresses
Comparison of Out-of-cone Traffic Inferred by Each Method

(a) Spoofer-IX

(i) Out-of-Cone Traffic

(ii) IP Address Churn

(iii) ASes and Countries

(b) State-of-the-art

(i) Out-of-Cone Traffic

(ii) IP Address Churn

(iii) ASes and Countries

None of the metrics results correlated with a typical attack pattern
Takeaways

• Few efforts have tried to empirically measure SAV compliance for networks attached to the global Internet

• We have exposed fundamental challenges and developed a new method to classify traffic flows

• We hope that our work be used to further improve our collective ability to measure and expand deployment of SAV filtering
• Few efforts have tried to empirically measure SAV compliance for networks attached to the global Internet

• We have exposed fundamental challenges and developed a new method to classify traffic flows

• We hope that our work be used to further improve our collective ability to measure and expand deployment of SAV filtering