UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE CIÊNCIA DA COMPUTAÇÃO

RODRIGO FAVALESSA PERUCH

Medindo a incidência de *spoofing* no contexto de tráfego IPv6 inter-domínio em um IXP

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharel em Ciência da Computação

Orientador: Prof. Dr. Marinho Pilla Barcellos
Co-orientador: Me. Lucas Fernando Müller

Porto Alegre
2019

“A felicidade às vezes é uma bênção
– mas geralmente é uma conquista.”
— PAULO COELHO

AGRADECIMENTOS

Durante meu período de graduação, tive a oportunidade de conhecer pessoas incríveis e que tornaram possível o sonho de me formar. Gostaria de escrever esta singela homenagem para as pessoas que foram decisivas na minha jornada, é pouco pelo que fizeram por mim, mas é de coração.

Em primeiro lugar gostaria de agradecer a meu orientador, Marinho, por todo seu tempo e energia investidos em mim. Espero um dia poder lhe retribuir de alguma forma. Agradeço também ao meu coorientador Lucas. Tenho a certeza de que sem a orientação de ambos, a experiência de escrever este trabalho não seria tão positiva quanto foi.

Agradeço também a minha família, em especial meu pai e minha mãe, que sempre me motivaram a estudar e seguir no caminho certo, desde pequeno. Sem eles eu sequer teria ingressado na universidade, que foi sem dúvida uma das maiores realizações da minha carreira acadêmica até o momento.

Tenho muito a agradecer a Nara, minha esposa, parceira e amiga acima de tudo, que durante minha trajetória na universidade sempre me apoiou, mesmo nos momentos mais difíceis, "segurando as pontas" quando foi preciso.

Agradeço também ao meu grande amigo e parceiro Júlio, que com seu alto astral e bom humor, me motivou a ver o lado positivo, mesmo nas situações mais adversas, quando achei que não conseguiria ir até o fim.

Agradeço aos guris do laboratório, em especial Fabrício e Pedro, que tiveram que me aturar lá enquanto redigia este trabalho. Brincadeiras à parte, esses dois me ajudaram um montão, sou muito grato por isso.

Agradeço a todo o corpo docente do Instituto de Informática da UFRGS por prover ensino de qualidade reconhecida internacionalmente, propiciando um ambiente que eu pude dar o máximo de mim, superando em várias situações meus próprios limites.

É com a satisfação de ter o dever cumprido que entrego o presente trabalho, que ao mesmo tempo representando o fim de uma etapa, também representa o início de uma nova, com desafios ainda maiores para serem transpostos. A partir de agora sigo rumo a voos mais altos, pois querem saber uma grande verdade? São os desafios que nos movem!

RESUMO

Spoofing é um tipo de ataque muito conhecido no qual o remetente falsifica o endereço de origem dos pacotes que transmite. Na Internet, o *spoofing* tem sido consistentemente usado como base para ataques de negação de serviço em massa. Obter uma visibilidade mais ampla no problema de *spoofing* na Internet é desafiador e exige o uso de sondagens ativas em redes ou a análise passiva de tráfego capturado em pontos de observação. Para a análise passiva, a identificação de pacotes com endereços de origem falsos depende do endereço que foi falsificado: os *bogons* (prefixos reservados) são mais simples de detectar, mas, caso contrário, é necessário verificar se o endereço de origem é válido naquele Sistema Autônomo (AS) específico e na direção em que está trafegando. Neste trabalho, os recentes avanços na detecção de *spoofing* na Internet, restritos ao IPv4, são aproveitados e estendidos à primeira análise sob o contexto do IPv6. Em particular, discutimos como usar os dados públicos do BGP para calcular uma hierarquia de ASes clientes abaixo de um AS raiz (conjunto denominado "cone de clientes") para cada AS e um intervalo válido de endereços IPv6 de origem, permitindo detectar passivamente, além de tráfego que sofreu *spoofing*, redes que não estão implementando mecanismos de Source Address Validation (SAV) dos pacotes que transmitem. Para avaliar os pontos fortes da metodologia, bem como expor suas limitações, aplicamos a metodologia a uma amostra de dados do sistema IX.BR e simulamos situações de *spoofing* via tráfego gerado sinteticamente.

Palavras-chave: Medindo *spoofing*. Protocolo IPv6. Ponto de troca de tráfego. Cone de clientes.

Measuring spoofing incidence in the context of inter-domain IPv6 traffic at an IXP

ABSTRACT

Spoofing is a very well-known type of attack in which the sender forges the source address of packets it transmits. In the Internet, spoofing has been consistently used as the basis for massive denial of service attacks. Acquiring broader visibility into the spoofing problem on the Internet is challenging, and requires the use of active probes on networks or passive capture analysis of traffic at large vantage points. For the passive analysis, identifying spoofed packets depends on the fake source address: bogons (reserved prefixes) are more simple to detect, but otherwise, it is necessary to check if the source address is valid at that specific AS and the direction it is going. In this graduation work, we leverage the recent advances on the assessment of spoofing on the Internet, which are restricted to IPv4, and extend them to the first analysis on the context of IPv6. In particular, we show how to use BGP public data to compute a "customer cone" for each AS and a valid range of source addresses that allow us to passively detect spoofed traffic and also networks that are not deploying Source Address Validation (SAV) mechanisms. In order to evaluate the methodology's strengths and to expose its limitations as well, we apply the methodology to a sample data of the IX.BR system and simulate *spoofing* situations via synthetically generated traffic.

Keywords: Measuring spoofing, IPv6 protocol, IXP, Customer Cone.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AS	Autonomous System
IP	Internet Protocol
c2p	customer-to-provider
p2c	provider-to-customer
CC	Cone de clientes
p2p	peer-to-peer
s2s	sibling-to-sibling
VP	Vantage Point
IXP	Internet Exchange Point
PTT	Ponto de Troca de Tráfego
BCP	Best Current Practice
DDoS	Distributed Denial of Service
ISP	Internet Service Provider
IETF	Internet Engineering Task Force
BGP	Border Gateway Protocol
RPF	Reverse Path Forwarding
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
RIB	Routing Information Base
SAV	Source Address Validation
ASN	Autonomous System Number
MAC	Media Access Control
PPV	Positive Predictive Value
RIR	Regional Internet Registry

ULA	Unique Local Address
HTTP	Hypertext Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure

SUMÁRIO

1 INTRODUÇÃO

Contexto e motivação. *Spoofing* é uma vulnerabilidade muito conhecida do protocolo IP no qual um atacante falsifica o endereço de origem dos pacotes IP que transmite. Na Internet, atacantes se aproveitam da dificuldade em se rastrear a origem de pacotes que sofreram IP *spoofing* e utilizam este mecanismo como base para ataques de negação de serviço distribuídos (DDoS) em massa (CLOUDFLARE, 2018).

A Best Current Practice (BCP) 38 recomenda a filtragem de ingresso na borda da rede em cada um de seus clientes (FERGUSON, 2000). Tal filtragem visa garantir que os pacotes originados pelo AS cliente possuam endereço de origem pertencentes à respectiva rede. A recomendação demanda uma gerência de listas de controle de acesso em diversos equipamentos, o que pode ser difícil de implantar e manter em redes de maior porte (NIC.br, 2019).

Em redes de maior complexidade, com maior número de equipamentos, manter centenas ou milhares de listas de acesso pode ser uma tarefa árdua e que induza a erros que podem causar sérios prejuízos (NIC.br, 2019), como o bloqueio de tráfego legítimo. Para esses casos a recomendação está descrita na BCP 84 (BAKER; SAVOLA, 2004) que basicamente indica o uso uma técnica denominada Reverse Path Forwarding (RPF) (KILLALEA, 2000).

Os mecanismos acima são medidas que podem prevenir *spoofing* e devem ser adotados como um esforço coletivo, beneficiando toda a Internet. Relatórios apontam que em grande parte das redes é possível realizar *spoofing* (CAIDA Spoofer, 2019), contrariando as recomendações propostas nas boas práticas do IETF. Isto indica que para muitos operadores de rede os incentivos de empregar tais boas práticas não são claros ou são insuficientes diante do risco de negar serviço a um cliente legítimo.

Problema. A identificação de pacotes com *spoofing* depende do endereço de origem falsificado: os *bogons* (prefixos reservados) são mais simples de detectar, mas caso contrário, é necessário verificar se o endereço de origem é válido naquele AS específico e na direção em que está trafegando. Na detecção de *spoofing* através do cone de clientes (CC), algoritmos que realizem a inferência das relações entre ASes são necessários e determinantes, uma vez que as relações de troca de tráfego entre os ASes são confidenciais.

As relações de troca de tráfego entre os ASes podem ser amplamente classificadas em *customer-to-provider* (c2p), *peer-to-peer* (p2p) e *sibling-to-sibling* (s2s) (LUCKIE et al., 2013). Elas podem ser utilizadas para a construção de um cone de clientes para cada

AS, permitindo definir um intervalo válido de endereços IPv6 de origem, habilitando em certos casos a detecção de tráfego que sofreu *spoofing* e também de redes que não estão implementando validações no endereço de origem (SAV) dos pacotes que transmitem.

Proposta. Neste trabalho, os recentes avanços na detecção de *spoofing* na Internet, atualmente restritos ao IPv4 (Müller, Lucas, 2019), são aproveitados e estendidos à primeira análise sobre o contexto do IPv6. Em particular, discutimos no Capítulo 5 como usar os dados públicos do BGP para calcular uma hierarquia de ASes clientes abaixo de um AS raiz (cone de clientes) para cada AS e um intervalo válido de endereços de origem, permitindo a detecção de tráfego que sofreu *spoofing* e também de redes que não estão implementando validações no endereço de origem (SAV) dos pacotes que transmitem $-$ uma condição que contribui para o aumento de *spoofing*.

Para avaliar os pontos fortes e suas limitações, aplicamos a metodologia a uma amostra de dados agregados de tráfego da Internet que foi coletada no sistema brasileiro de Pontos de Troca de Tráfego (PTTs). Em seguida, construímos um conjunto de teste sintético que viola a autenticidade de origem, permitindo ter uma visão inicial da eficácia da metodologia e suas limitações. Este trabalho busca responder as seguintes perguntas:

- Quais são os desafios em desenvolver uma metodologia para IPv6 baseada em cone de clientes para a detecção de *spoofing* e redes que não implementam SAV?
- Qual o impacto que a precisão do algoritmo de inferência de relações entre ASes causa na metodologia, no contexto do IPv6?
- Quais são as vantagens e desvantagens do uso de metodologias baseados em cone de clientes, no contexto do IPv6?

Contribuições. As contribuições deste trabalho são: (i) adaptação de uma metodologia para identificação de *spoofing* ao protocolo IPv6; (ii) análise qualitativa e quantitativa de *spoofing* sobre o protocolo IPv6; (iii) investigação das vantagens e limitações de metodologias baseadas em cone de clientes para classificação de tráfego *spoofing* e deteção de redes que não implementam SAV, sob o contexto de IPv6.

Organização. Inicialmente, os conceitos chave sobre inferências de relações, propriedades das relações entre ASes e conceitos sobre *spoofing* são introduzidos (Capítulo 2). Esses conceitos fornecem a base para discutir o estado-da-arte sobre a metodologia e esforços propostos ou realizados até o presente momento (Capítulo 3). O conjunto de dados utilizado e questões relacionadas a aquisição e processamento dos mesmos são abordados no Capítulo 4. Em seguida, a metodologia é apresentada (Capítulo 5). No

Capítulo 6 discutimos os resultados obtidos e em seguida (Capítulo 7) avaliamos a metodologia utilizando um conjunto de teste gerado sinteticamente. Por fim, no Capítulo 8 são apresentadas as conclusões finais e trabalhos futuros.

2 CONCEITOS

Neste capítulo, serão apresentados os principais conceitos relacionados necessários para um melhor entendimento dos próximos capítulos. Essas informações servirão como base teórica para o restante do trabalho e permitirão uma avaliação mais crítica sobre os trabalhos relacionados e sobre as análises realizadas.

2.1 Ataques utilizando *spoofing*

O ataque de *spoofing* consiste em enviar pacotes com endereço de origem falso, violando a integridade da informação de origem ou autenticidade. O ataque explora uma vulnerabilidade que está presente no protocolo IP desde os primórdios da Internet (BELLOVIN, 1989) e é tipicamente base para a realização de ataques de negação de serviço.

As recomendações para tratar a causa raiz do problema – e não os sintomas – vão em direção a filtragem do tráfego na borda entre AS origem e o ISP. Há uma falta de consistência em relação à capacidade de filtrar, por questões de desempenho, sobrecarga administrativa, risco associado ou outros motivos inerentes ao ISP, o que faz alguns não implementarem as boas práticas de validação de endereços de origem (SAV).

Ataques podem ser caros para os ISPs. Eles prejudicam a imagem da marca, as operações dos clientes e ainda têm impacto colateral em outros clientes além do atingido. Grande parte dos ataques de negação de serviço seriam evitáveis caso *spoofing* fosse inviabilizado (CLOUDFLARE, 2018).

A observação recente de grandes ataques utilizando *spoofing* (NETSCOUT, 2018) sugere que a filtragem de ingresso não está suficientemente implantada. Infelizmente, não há benefício direto para um ISP que implementa a filtragem de ingresso em sua rede. Há também uma crença generalizada de que a filtragem de ingresso só valeria a pena se fosse implantada universalmente (MANRS, 2019).

2.2 Relações entre ASes

Os ISPs, visando fornecer acessibilidade entre si ou para alguma parte da Internet, envolvem-se em acordos de interconexão que são tipicamente confidenciais (LUCKIE et al., 2013). Entretanto, algumas informações podem ser inferidas utilizando dados topoló-

gicos da Internet derivados de *traceroute* ou tabelas de roteamento obtidas por coletores em pontos de observação que são disponibilizadas publicamente na Internet (CAIDA As-Rank, 2019).

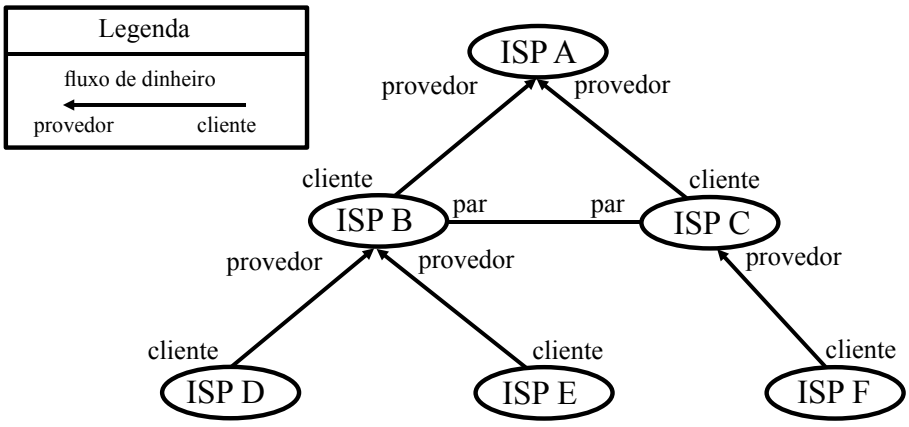
2.2.1 Tipos de relações

O modelo introduzido por (GAO, 2001) abstrai as relações de negócios entre ASes nos três tipos a seguir:

1. *customer-to-provider* (c2p) ou se visto no sentido oposto, *provider-to-customer* (p2c);
2. *peer-to-peer* (p2p);
3. *sibling-to-sibling* (s2s).

Esta classificação é feita a partir da observação de que um ISP precisa adquirir serviços de trânsito para tráfego destinado a partes da Internet que este não pode alcançar. Na Figura 2.1, as direções das setas refletem os fluxos de pagamentos: os níveis mais baixos são os clientes que pagam provedores (relações c2p) em níveis mais altos em troca do acesso ao resto da Internet. Na Figura 2.1, as relações D $\rightarrow$ B, E $\rightarrow$ B, F $\rightarrow$ C, B $\rightarrow$ A e C $\rightarrow$ A são relações c2p.

Figura 2.1: Tipos de relações entre ASes



Fonte: adaptado de (CAIDA As-Rank, 2019)

Uma relação p2p conecta dois ASes que trocam tráfego. Neste caso, os pares trocam tráfego entre si e com os clientes uns dos outros. A relação é chamada de *peering* e permite que os ISPs economizem dinheiro com trânsito. Na Figura 2.1, B $-$ C é uma relação p2p, pois nem B nem C pagam um ao outro pelo tráfego que trocam.

Uma relação s2s conecta dois ASes a um limite administrativo comum. Esse tipo de relação geralmente aparece como resultado de fusões e aquisições ou de certos cenários de gerenciamento de rede, quando por exemplo, uma organização tem sua rede distribuída em vários ASes.

Portanto, um caminho válido deve ter o seguinte padrão: zero ou mais relações c2p (tráfego subindo), seguidos por zero ou uma relação p2p (trafego na horizontal), seguidos por zero ou mais relações p2c (tráfego descendo). Além disso, as relações s2s podem aparecer em qualquer número em qualquer parte do caminho (LUCKIE et al., 2013).

2.3 Relações complexas

A maioria das relações entre ASes pode ser inferida de maneira relativamente simples em uma das três categorias citadas anteriormente. No entanto, existem relações que violam a abstração tradicional proposta por (GAO, 2001), prejudicando inferências realizadas pelos algoritmos existentes atualmente.

Embora existam outras, os dois tipos mais comuns de relações complexas são (GIOTSAS et al., 2014): relações híbridas, onde dois ASes têm relações diferentes em certos pontos de interconexão (p2c em um local e p2p em outro lugar) e relações parciais de trânsito, que restringem o escopo de uma relação p2c aos pares e clientes do provedor (mas não aos provedores). A Tabela 2.1 resume os dois tipos de relações.

Tabela 2.1: Dois tipos comuns de relações complexas

Tipo	Definição
Trânsito parcial	Um AS oferece a outro AS trânsito para seus pares e clientes, mas não para provedores.
Híbrido	Um AS oferece a outro AS uma combinação de trânsito total, trânsito parcial ou peering, de acordo com a localização da interconexão.

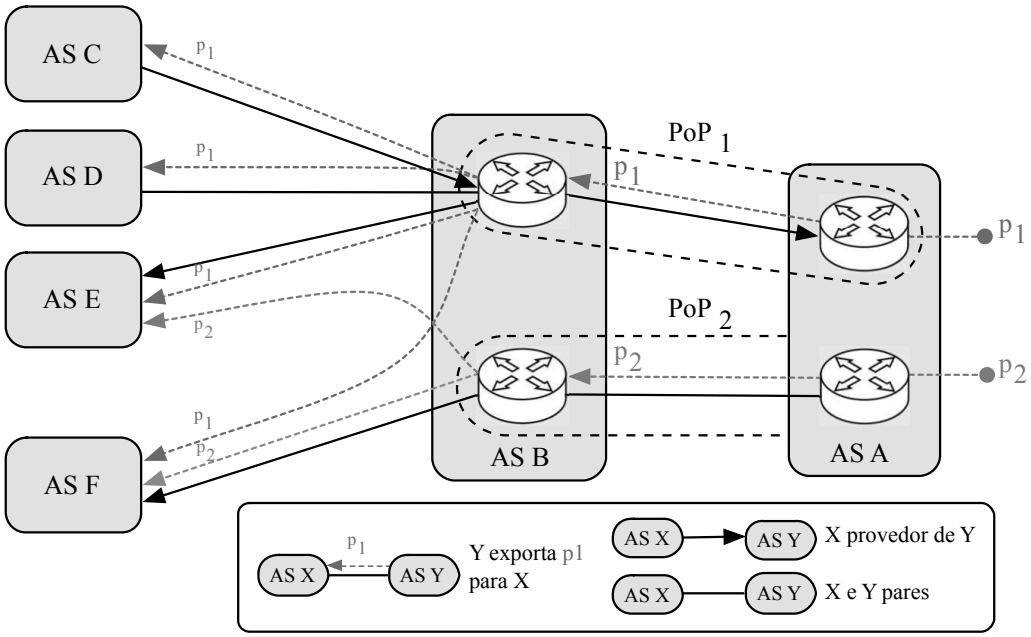
Fonte: (GIOTSAS et al., 2014)

2.3.1 Relações híbridas

Relações híbridas surgem quando dois ASes concordam com diferentes tipos de relações em diferentes pontos de presença (PoPs). Tipicamente, os ASes serão pares em determinadas regiões, mas em outras, um deles será cliente. A Figura 2.2 ilustra o

roteamento que resulta em tal relação: B pode anunciar o prefixo p2 para todos os seus vizinhos, mas B só pode anunciar p1 para seus clientes. Em alguns casos, B só pode anunciar p2 para clientes na região atendida por PoP2.

Figura 2.2: Exemplo de relação híbrida



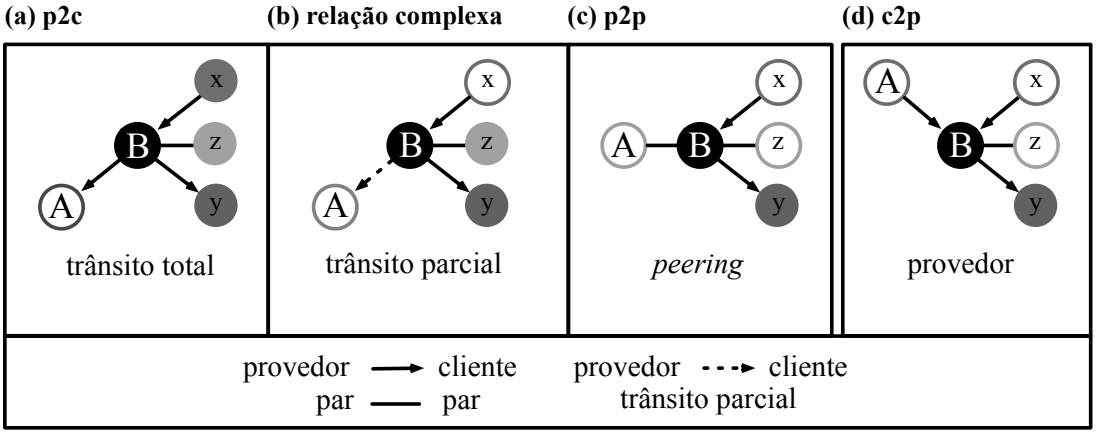
Fonte: adaptado de (GIOTSAS et al., 2014)

2.3.2 Relações parciais

Relações parciais de trânsito surgem quando um provedor vende acesso a seus clientes e pares, mas não o acesso a seus provedores. A Figura 2.3 compara diferentes cenários típicos de roteamento (p2c, p2p e c2p) com trânsito parcial:

- No cenário de trânsito total, B exporta as rotas de A aos seus clientes (y), pares (z) e provedores (x);
- No cenário de trânsito parcial, B exporta as rotas de A aos seus clientes (y), pares (z) mas não aos provedores (x);
- No cenário de *peering*, B exporta as rotas de seus clientes (y) ao seu par A;
- No cenário de provedor, B exporta as rotas de seus clientes (y) ao seu provedor A.

Figura 2.3: Comparação de cenários típicos de roteamento com trânsito parcial

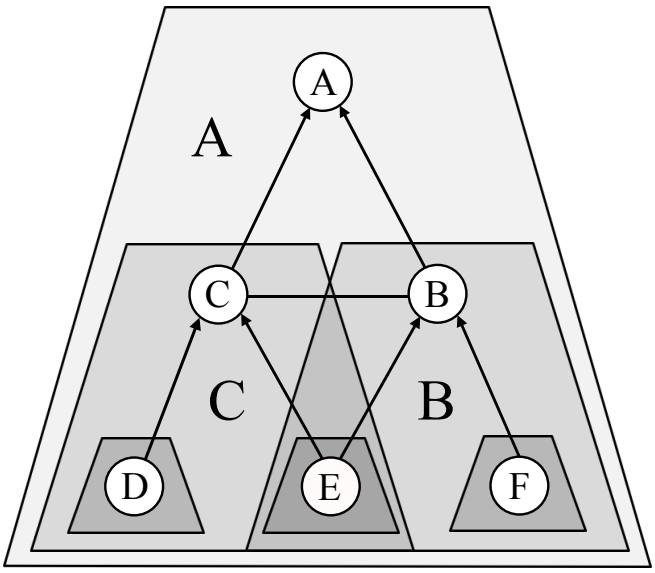


Fonte: adaptado de (GIOTSAS et al., 2014)

2.3.3 Cone de clientes

O cone de clientes de um AS A é definido com o próprio mais todos os ASes que podem ser alcançados a partir dele através de relações p2c. Em outras palavras, o cone de clientes de A contém A, além dos clientes de A, além dos clientes de seus clientes, e assim por diante (CAIDA As-Rank, 2019). O cone de clientes é uma métrica derivada a partir da observação das relações entre ASes e consiste em uma hierarquia de ASes clientes abaixo de um AS raiz.

Figura 2.4: Exemplo de cone de clientes



Fonte: adaptado de (CAIDA As-Rank, 2019)

A Figura 2.4 ilustra os cones de clientes dos ASes A, B, C, D, E e F e seus respec-

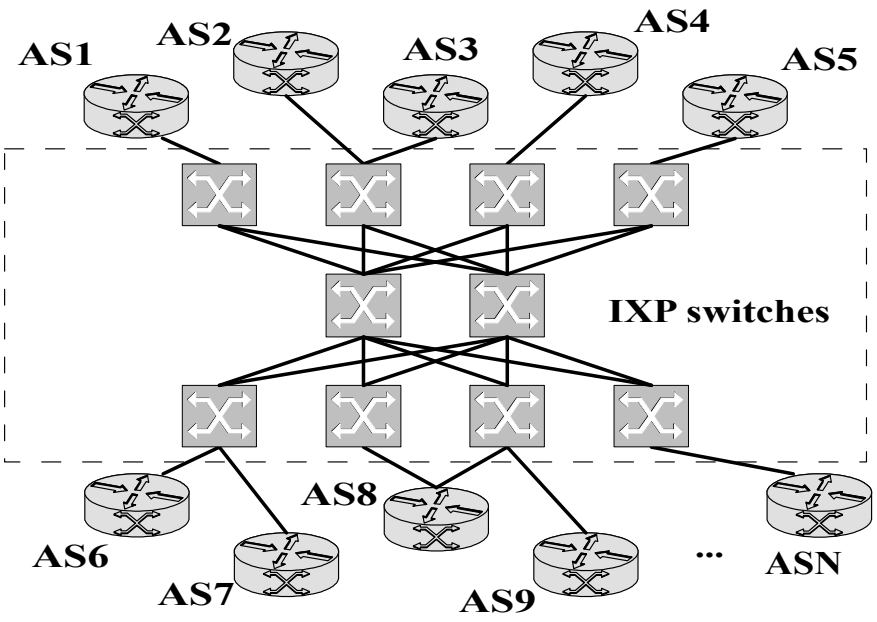
tivos tamanhos.

- Alguns ASes aparecem na base inferior da hierarquia, possuindo apenas um único AS em seu cone de clientes: eles mesmos;
- Ambos B e C empatam com 3 ASes. É importante ressaltar que B e C têm ambos E em seus respectivos cones de clientes, pois E é cliente de ambos;
- O AS A encontra-se no topo da hierarquia.

No topo desta hierarquia estão os ISPs comumente conhecidos como *Tier-1*, que não pagam pelo trânsito para nenhuma outra rede. Em vez disso, eles se juntam para fornecer conectividade a todos os destinos na Internet. No extremo oposto da hierarquia, estão os ASes com finalidade principal de conectar hospedeiros à Internet ou oferecer conteúdo, tipicamente pagando provedores para alcançar todos os destinos na Internet.

2.4 Arquitetura típica de um IXP

Figura 2.5: Arquitetura de um IXP



Fonte: (AGER et al., 2012)

A Figura 2.5 ilustra uma visão de alto nível da arquitetura típica de grandes IXPs em geral. O IXP fornece uma malha de comutação em camada 2 e cada um dos ASes membros conecta seu roteador de acesso a essa malha. Quando um par de ASes membros decide trocar tráfego, eles estabelecem uma sessão de BGP entre seus roteadores de

acesso, o que por sua vez permite a troca de tráfego IP por esse enlace na infraestrutura do IXP (AGER et al., 2012).

3 TRABALHOS RELACIONADOS

Neste capítulo, apresentaremos o estado-da-arte na área, agrupando trabalhos e comparando os mesmos com a presente proposta. Para orientar a análise dos trabalhos relacionados, revisamos o objetivo: detectar tráfego IPv6 com endereço de origem inválido (*spoofing*) e também redes que não implementam SAV. Para tal, utilizamos o algoritmo de inferência de relações proposto por (GIOTSAS et al., 2015) para inferir relações de troca de tráfego entre os ASes. Em seguida, de posse de uma estimativa de todas as relações entre os diferentes ASes na Internet, construimos o cone de clientes inerente à topologia IPv6 e aplicamos a metodologia passivamente a uma amostra de dados coletada no sistema brasileiro de Pontos de Troca de Tráfego (PTTs).

A detecção de *spoofing* realizada por esta metodologia é feita baseando-se na premissa de que tráfego, só deveria ser recebido de um AS caso o cone de clientes do mesmo contenha o endereço de origem do tráfego. Para ser viável esta classificação, são utilizados diversos conjuntos de dados, a serem apresentados no Capítulo 4. A seguir, primeiro serão analisadas as abordagens que realizam inferências de relações, e posteriormente as abordagens que utilizam as inferências para detecção passiva de *spoofing*, pois ambas as áreas estão contidas no contexto deste trabalho.

3.1 Inferência de relações

(LUCKIE et al., 2013), apresentaram um algoritmo para inferência de relações entre ASes que identifica relações c2p e p2p. Possui uma abordagem *top-down* que começa inferindo um clique *Tier-1*, aplica heurísticas para inferir relações c2p baseadas principalmente em como os vizinhos foram observados exportando rotas e assume o restante como p2p.

São utilizadas como entrada instâncias de tabelas de roteamento BGP (RIBs) dos cinco primeiros dias de cada mês. As mesmas foram obtidas dos projetos (ROUTE VIEWS, 2019) e (RIPE RIS, 2019), sendo considerados somente anúncios para prefixos IPv4, removendo artefatos nos caminhos como *prepending*, laços, ASes reservados, IXPs e *Tier-1* não adjacentes. Também são utilizadas políticas de roteamento (ALAETTINOGLU et al., 1999) obtidas em (RIPE DATABASE, 2019) como parte do conjunto de validação (outra parte foi obtida diretamente dos operadores de rede).

A abordagem utiliza as relações inferidas para a construção do cone de clientes.

O cone de clientes de um AS A é definido com o próprio mais todos os ASes que podem ser alcançados a partir dele através de relações p2c.

(GIOTSAS et al., 2015), adaptaram a proposta de (LUCKIE et al., 2013) para inferir relações da topologia IPv6. Na prática, introduz alterações em duas etapas no algoritmo de (LUCKIE et al., 2013), fazendo uso do mesmo de forma encapsulada nas etapas restantes. Foi também observado que a topologia do IPv6 não estava totalmente conectada devido às disputas de *peering* (Leber, M., 2009). Esta foi a primeira abordagem de inferência que trata especialmente do IPv6 e neste trabalho é referenciada como AS-Rank6.

São considerados somente anúncios para prefixos IPv6, removendo artefatos nos caminhos como *prepending*, laços, ASes reservados, IXPs e *Tier-1* não adjacentes. A abordagem utiliza as relações inferidas para a construção do cone de clientes IPv6.

(JIN et al., 2019), apresentaram uma proposta visando aumentar a precisão das inferências sobre relações complexas, tais como relações híbridas ou *peering* parciais. Para isso os autores propõem uma técnica probabilística para inferência de relações, porém não focam na construção de cones, nem mesmo avaliam seu impacto.

São utilizadas como entrada instâncias de tabelas de roteamento BGP (RIBs) obtidas a cada quatro meses em diferentes pontos de observação (ROUTE VIEWS, 2019) (RIPE RIS, 2019), sendo considerados somente anúncios para prefixos IPv4, filtrando caminhos com *prepending*, laços, ASes reservados e IXPs. O conjunto de validação é caracterizado pelo próprio autor como “melhor-esforço” e construído através do atributo comunidade BGP.

3.2 Detecção de *spoofing*

(LICHTBLAU et al., 2017), apresentaram uma abordagem que permite a detecção passiva de *spoofing*. A abordagem, chamada de Full Cone, não distingue relações p2p, s2s e c2p. Em vez disso, sempre que ela observa dois ASes vizinhos em um caminho, assume uma relação onde o AS à esquerda é considerado provedor do AS à direita. Com isso, os autores intencionalmente sacrificam especificidade com o objetivo de minimizar falsos positivos.

São utilizados como entrada todas as instâncias de tabelas de roteamento BGP (RIBs) e atualizações obtidas dos projetos (ROUTE VIEWS, 2019) e (RIPE RIS, 2019) sendo considerados somente anúncios para prefixos IPv4, descartando prefixos mais espe-

cíficos que /24 e menos específicos que /8. Também é utilizado um conjunto de dados com endereços *bogons* (TEAM CYMRU, 2019). A metodologia é utilizada para classificar um conjunto de dados coletado em um grande IXP Europeu.

(Müller, Lucas, 2019), apresentou uma abordagem passiva, chamada Spoofer-IX, para inferir redes que não implementam SAV, bem como tráfego que sofreu *spoofing*. A metodologia cria uma lista de endereços de origem válidos por AS. Em seguida, o autor usa a lista para determinar quais endereços de origem devem aparecer legitimamente em pacotes em algum ponto de observação em uma determinada janela de tempo, bem como a direção desses pacotes. Utiliza o cone de clientes para determinar um intervalo válido para endereços de origem de pacotes. Seu trabalho fez uma comparação crítica entre as abordagens *Full cone* e *Customer cone*. A metodologia é utilizada para classificar um conjunto de dados coletado em um IXP Brasileiro e não é voltada para o caso específico do IPv6. São utilizadas como entrada arquivos RIB, na frequência de um para cada dia durante a vigência dos estudos, obtidos dos projetos (ROUTE VIEWS, 2019) e (RIPE RIS, 2019), sendo considerados somente anúncios para prefixos IPv4, removendo artefatos nos caminhos como *prepending*, laços, ASes reservados, IXPs, *Tier-1* não adjacentes, descartando prefixos mais específicos que /24 e menos específicos que /8.

3.3 Discussão

As abordagens foram comparadas de forma crítica em função das sete diferentes características a seguir.

1. **Filtragem:** quais filtragens são realizadas nos dados de entrada;
2. **Atualização:** com que frequência a metodologia é alimentada com novos dados para inferências;
3. **Cone:** definição de cone de clientes que cada abordagem utiliza;
4. **Validação:** validações no cone de clientes que foi inferido pela abordagem;
5. **Relações complexas:** qual a precisão da abordagem em cenários incomuns de relações entre ASes;
6. **Detecção:** quais abordagens realizam detecção de *spoofing*;
7. **IPv6:** quais abordagens consideram IPv6.

A Tabela 3.1 contém o resultado da comparação realizada.

Tabela 3.1: Comparação dos trabalhos relacionados

Método	Filtragem	Atualização	Cone	Validação	Relações complexas	Detecção	IPv6
(LUCKIE et al., 2013)	*Prepending*, laços, ASes reservados, IXPs, *Tier-1* não adjacentes	Um RIB por VP nos 5 primeiros dias de cada mês	*Customer cone*	Sim	Sim	Não é o objetivo	Não
(GIOTSAS et al., 2015)	*Prepending*, laços, ASes reservados, IXPs, *Tier-1* não adjacentes	Um RIB por VP nos 5 primeiros dias de cada mês	*Customer cone*	Sim	Sim	Não é o objetivo	Sim
(LICHTBLAU et al., 2017)	Somente tamanho do bloco anunciado	Todos os RIB e atualizações são utilizados	*Full cone*	Não	Desconsidera	Passiva	Não
(JIN et al., 2019)	*Prepending*, laços, ASes reservados, IXPs	Um RIB por VP a cada quatro meses	–	Sim	Foca em melhorar a precisão	Não é o objetivo	Não
(Müller, Lucas, 2019)	*Prepending*, laços, ASes reservados, IXPs, tamanho do bloco, *Tier-1* não adjacentes	Um RIB por VP a cada dia do mês	*Customer cone*	Sim	Sim	Passiva	Não
Este trabalho	*Prepending*, laços, ASes reservados, IXPs, *Tier-1* não adjacentes	Um RIB por VP a cada dia do mês	*Customer cone*	Sim	Sim	Passiva	Sim

Fonte: os autores

4 CONJUNTO DE DADOS

Neste capítulo, discutimos a origem e o processo de coleta dos dados que foram utilizados neste trabalho. Também abordamos questões sobre o período e caracterização dos dados obtidos que referem-se ao período de 22 a 28 de abril de 2017, quando o tráfego foi coletado.

Tabelas RIB. Os dados BGP utilizados neste trabalho foram obtidos a partir dos projetos (RIPE RIS, 2019) e (ROUTE VIEWS, 2019). Esses projetos possuem coletores que fazem *peering* com diversos ASes, possibilitando a coleta de dados via BGP. Os dados são disponibilizados no formato MRT (BLUNK; KARIR; LABOVITZ, 2011), onde cada um representa uma instância de tabela de roteamento do coletor em um dado instante no tempo. Cada coletor é considerado um ponto de observação, pois ele possui uma visão da Internet na perspectiva dos ASes adjacentes.

Utilizamos este conjunto de dados na construção do cone de clientes IPv6 e para geração de uma lista que mapeia prefixos IP para ASN, visando determinar qual AS anunciou um dado prefixo no ecossistema BGP. Obtivemos um arquivo RIB por dia de 22 a 28 de abril de 2017 para 18 coletores do projeto (RIPE RIS, 2019) e 18 coletores do projeto (ROUTE VIEWS, 2019).

Tabelas PeeringDB. PeeringDB é um banco de dados onde estão centralizadas uma gama de informações sobre prontos de trocas, redes e infraestruturas. Os dados do PeeringDB são utilizados como informação adicional na construção do cone de clientes IPv6 pelo algoritmo AS-Rank6 (GIOTSAS et al., 2015). O PeeringDB possui uma interface web que pode ser utilizada para obter uma cópia dos dados das redes registradas e suas políticas de *peering*. Entretanto, dados históricos não são fornecidos. Por isso, foram utilizadas cópias de 22 a 28 de abril de 2017 coletados e armazenados pelo CAIDA (CAIDA PeeringDB, 2019).

Lista de provedores *Tier-1* IPv4. O projeto As-Rank (CAIDA As-Rank, 2019) disponibiliza uma lista de provedores *Tier-1* IPv4 e que é utilizada como apoio na inferência do clique *Tier-1* IPv6 pelo algoritmo AS-Rank6.

Lista de ASes operados por IXPs. O mesmo projeto (CAIDA As-Rank, 2019) disponibiliza uma lista de número de ASes operados por IXPs que é utilizada para que eles sejam removidos do atributo BGP *AS-path*, durante o processamento dos caminhos BGP obtidos das Tabelas RIB. Mais detalhes na Seção 5.1.1.

Relações derivadas de comunidades. O mesmo projeto (CAIDA As-Rank, 2019)

disponibiliza uma lista de relações entre ASes derivada a partir de comunidades BGP. Esta lista é utilizada como apoio na inferência do clique *Tier-1* IPv6 pelo algoritmo AS-Rank6, desconsiderando potenciais candidatos ao clique que possuam provedores (GIOTSAS et al., 2015).

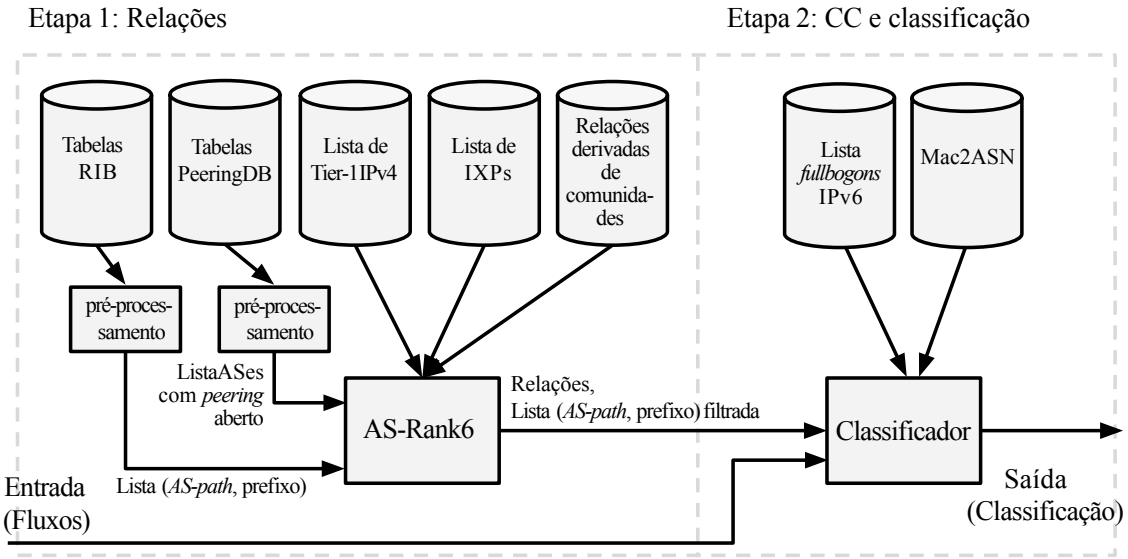
Lista fullbogons IPv6. A lista *fullbogons* IPv6 contém prefixos IPv6 (intervalos) que não foram alocados a RIRs ou que não foram atribuídos pelos RIRs a ISPs ou outro usuário final em uma certa data. Esta lista é mantida em (TEAM CYMRU, 2019) e é atualizada a cada 4 horas. Essa lista é utilizada para marcar tráfego que não deveria ser roteado na Internet, pois tais endereços além de serem não-alocados ou não-atribuídos, são frequentemente observados como origem em ataques DDoS. A lista *fullbogons* pode ser consultada no endereço web da empresa (TEAM CYMRU, 2019). No entanto, dados históricos não são fornecidos. Por isso foram utilizadas cópias de 22 a 28 de abril de 2017 coletados e armazenados pelo CAIDA (CAIDA Bogon, 2019).

Dados do ecossistema IX.BR. Foram utilizados dados de tráfego obtidos de um IXP pertencente ao ecossistema Brasileiro de IXPs (IX.BR, 2019) para estudo e avaliação desta metodologia. Este IXP transporta até 180 Gbps de tráfego entre mais de 200 membros. Também foram obtidas informações topológicas que mapeiam endereços MAC para ASN (Mac2ASN), fornecendo uma maneira de identificar fluxos em camada 2 de cada participante do IXP. O tráfego foi capturado via Netflow com uma taxa de amostragem de 1:4096 pacotes de 22 a 28 de abril de 2017. O tráfego foi filtrado mantendo-se somente tráfego IPv6 e atributos de interesse: endereços IP de origem/destino, portas de origem/destino, tipo de protocolo, duração, número de pacotes, número de bytes e Mac2ASN.

5 METODOLOGIA PROPOSTA: SPOOFER6-IX

O Spoofer6-IX, conforme ilustrado na Figura 5.1, está estruturado em duas etapas: relações e, em seguida, CC e classificação de tráfego. Na primeira etapa, diversos dados auxiliares são utilizados para inferência das relações entre os ASes. Em seguida, as relações inferidas são utilizadas para a construção do cone de clientes que, em linhas gerais, fornece ao classificador os limites de origem para o tráfego, considerando as motivações econômicas da Internet. A seguir, explicaremos os diferentes passos em cada etapa, adotando como referência a Figura 5.1.

Figura 5.1: Visão geral do Spoofer6-IX



Fonte: os autores

5.1 Etapa 1: relações

5.1.1 Pré-processamento de tabelas RIB

Primeiro, decodificamos as tabelas RIB utilizando a ferramenta BGP Scanner (ISOLARIO, 2019). Em seguida, o resultado é processado seguindo os seguintes passos:

1. São descartados anúncios para prefixos que não sejam IPv6;
2. Caso exista *AS-path prepending*, ele é desfeito;
3. Pares (*AS-path*, prefixo) duplicados são removidos.

É gerada uma saída em formato texto contendo *AS-path* e prefixo para cada anúncio BGP remanescente após a filtragem.

5.1.2 Pré-processamento de tabelas PeeringDB

Os dados do PeeringDB disponibilizados pelo CAIDA (CAIDA PeeringDB, 2019) estão no formato SQLite e necessitam ser convertidos e formatados para serem utilizados como entrada. As tabelas foram convertidas para texto e em seguida os atributos de interesse (ASN e política de *peering*) foram salvos, desconsiderando-se os demais atributos. É gerada uma saída em formato texto contendo ASN e o tipo de política de *peering* do mesmo.

5.1.3 AS-Rank6

Utilizamos o algoritmo AS-Rank6 (GIOTSAS et al., 2015) disponibilizado pelo autor para inferir relações entre os ASes registrados no ecossistema BGP. O AS-Rank6 foi proposto a partir da observação de que algoritmos tradicionais não inferiam de forma precisa o suficiente relações entre ASes no protocolo IPv6, pois uma vez que a topologia do IPv6 evoluiu em paralelo à topologia IPv4, nem todas as suposições utilizadas por tais algoritmos são válidas no contexto do IPv6 (DHAMDHERE et al., 2012), em particular, sobre a existência de um clique *Tier-1* no topo da topologia IPv6 totalmente conectado entre si (GIOTSAS et al., 2015).

O AS-Rank6 recebe como entrada:

- Lista de caminhos derivada a partir de tabelas RIB;
- Lista de ASes com políticas de *peering* aberto;
- Lista de ASes provedores *Tier-1* IPv4;
- Lista de ASes operados por IXPs;
- Relações derivadas de comunidades.

Como saída, o AS-Rank6 devolve um conjunto de relações estimadas entre os ASes observados e um conjunto contendo caminhos e prefixos, que é filtrado pelo algoritmo da seguinte maneira:

1. ASes utilizados por IXPs são removidos do *AS-path*;

2. São descartados anúncios onde os provedores *Tier-1* aparecem separados, pois isso implicaria que um provedor *Tier-1* estaria pagando por tráfego – o que viola a definição de ser *Tier-1*;
3. São descartados anúncios com laços.

A saída contém os *AS-paths* e seus respectivos prefixos. Ambos os conjuntos de relações e caminhos são repassados para o classificador.

5.2 Etapa 2: Cone de clientes e classificação

5.2.1 Construção do cone de clientes

O Spoofer6-IX adota uma definição de cone de clientes do tipo recursiva, onde o cone de um AS A é computado incluindo recursivamente cada AS alcançável a partir dele seguindo relações p2c. Por exemplo, se B é um cliente de A e C é um cliente de B, então o cone do cliente de A inclui B e C.

Esta definição assume propositadamente que um provedor receberá todas as rotas de seus clientes em detrimento de especificidade, pois como o problema de inferência de relações é complexo e ainda está aberto a otimizações, a idéia é minimizar falsos positivos na categoria fora do cone, que poderiam ser inferidos como tal por uma classificação mais estrita.

5.2.2 Classes de tráfego

A seguir, descreveremos as classes em que a metodologia classifica os fluxos analisados.

Controle. São fluxos onde o endereço de origem e destino pertencem a intervalos reservados do IPv6 para serviços específicos e que são válidos no contexto de uma rede local (IPv6.br, 2019). São considerados intervalos de controle endereços de origem e destino nas categorias *Local Link*, *Unique Local Address* (ULA) e *Multicast*.

Inválido. São fluxos onde o endereço de origem está contido na lista *fullbogons*. São intervalos de endereços reservados, não-alocados ou não-atribuídos. Pelo fato da lista *fullbogons* conter os prefixos que não deveriam ser observados na Internet, os ASes observados enviando tráfego com o endereço de origem *bogon* implementam pouco (ou

nenhuma) filtragem de ingresso. Tráfego classificado nesta categoria é potencialmente *spoofing*.

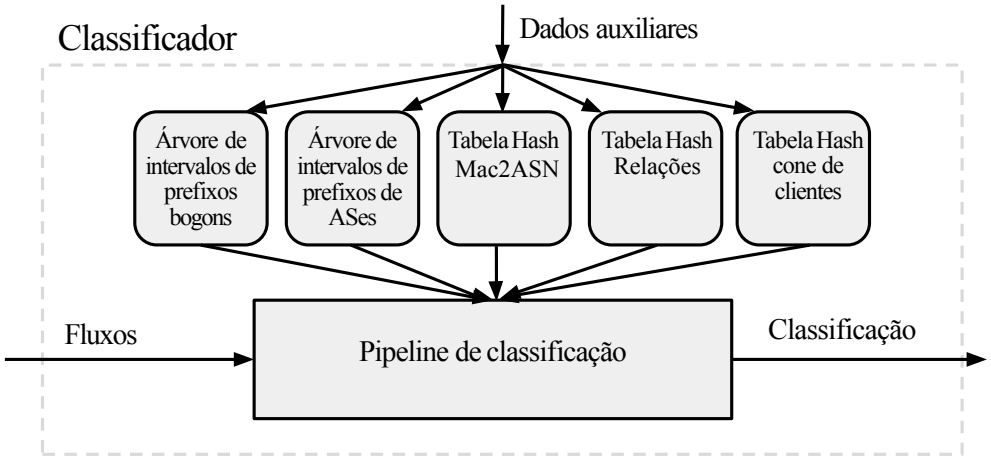
Não-verificável. São fluxos onde a metodologia é incapaz de classificar por falta de informações. Os motivos que levam a essa classificação são ausência de mapeamento MAC para ASN (portanto não se sabe por qual membro o pacote chegou), casos onde o AS de ingresso não foi observado nos anúncios BGP (portanto não existe CC para ele), ou ainda, casos onde AS originador do IP de origem não foi observado nos anúncios BGP.

Fora do cone. São fluxos em que o endereço de origem do pacote não está contido no intervalo do cone de clientes do AS que o ingressou no IXP. Tráfego classificado nesta categoria é potencialmente *spoofing*.

No cone. São fluxos em que o endereço de origem está contido no intervalo do cone de clientes do AS que o ingressou no IXP.

5.2.3 Classificador de fluxos

Figura 5.2: Visão geral do classificador de fluxos

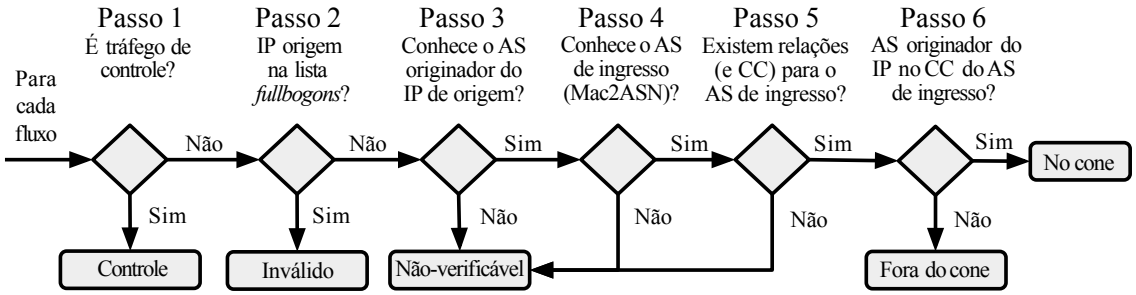


Fonte: os autores

O passo inicial executado no classificador de fluxos (Figura 5.2) é popular as estruturas de dados utilizadas como apoio com seus respectivos dados de entrada. Em seguida inicia-se a classificação dos fluxos. A Figura 5.3 contém um fluxograma ilustrando a lógica implementada no *pipeline* de classificação e será usada como referência no detalhamento dos passos a seguir.

No passo 1, o algoritmo verifica se o endereço IP de origem e destino pertencem a classe de controle. Fluxos onde a origem e destino estão no intervalo de controle são considerados válidos, pois não são destinados a endereços fora do contexto do enlace em

Figura 5.3: Fluxograma de classificação implementado pelo de classificador



Fonte: os autores

que se encontram. Em contrapartida, se um fluxo tiver endereço de origem no intervalo de controle e for destinado a um endereço roteável na Internet (e vice-versa), ele avança para o passo 2.

No passo 2, o algoritmo verifica se IP de origem do fluxo está contido na lista *fullbogons*. Caso esteja, é classificado como inválido. Caso contrário, avança para o passo 3.

No passo 3, o algoritmo verifica a qual AS pertence o endereço IP de origem do fluxo. Isto é feito através da consulta de qual AS o anunciou via BGP. Caso nenhum anúncio tenha sido observado para o prefixo, não sabemos a qual AS o IP de origem pertence e não podemos testar a restrição de cone. Neste caso, o fluxo é classificado como não-verificável. Caso contrário, avança para o passo 4.

No passo 4, o algoritmo realiza o casamento do endereço MAC de ingresso do fluxo ao seu respectivo AS. Esse mapeamento é feito através do catálogo Mac2ASN. Em fluxos onde o endereço MAC não está presente nesse catálogo, não é possível identificar o AS que está ingressando tráfego no IXP. Portanto, tais fluxos recebem classificação como não-verificável. Caso contrário, avança para o passo 5.

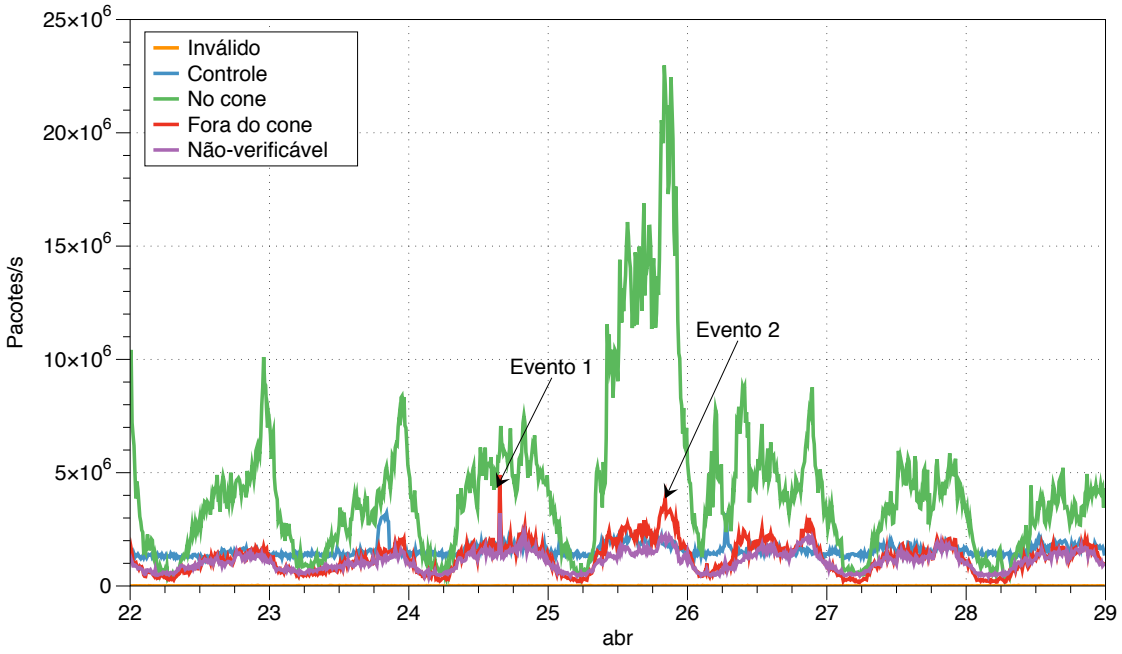
No passo 5, o algoritmo verifica se existem registros de relações no conjunto de dados para o AS de ingresso. Caso não existam, significa que não foram observados caminhos BGP contendo o AS, inviabilizando a construção de um cone de clientes para o mesmo. Isto pode acontecer caso os coletores tenham sofrido com visibilidade limitada durante o período do estudo. Neste caso, é classificado como não-verificável. Caso contrário, avança para o passo 6.

No passo 6, o algoritmo obtém o número do AS que anunciou o IP de origem via BGP. Em seguida, é verificado se tal AS está no cone de clientes do AS que está ingressando tráfego no IXP. Caso esteja, é classificado como no cone e caso contrário, é classificado como fora do cone.

6 ANÁLISE DAS MEDIÇÕES

A metodologia foi aplicada ao tráfego capturado em um IXP pertencente ao ecossistema Brasileiro de IXPs (IX.BR, 2019) na semana de 22 a 28 de abril de 2017, classificando o tráfego nas cinco categorias introduzidas na Seção 5.2.2. Observamos algumas variações repentinas na curva do tráfego classificado fora do cone, que sob uma primeira a análise, são compatíveis com curvas típicas de ataques. Neste capítulo, investigaremos tais variações e formularemos hipóteses visando explicar os dois eventos atípicos observados, denotados nas Figuras 6.1, 6.2, 6.3 e 6.4, como Evento 1 e Evento 2.

Figura 6.1: Tráfego ao longo da janela de tempo do estudo – em pacotes



Fonte: os autores

6.1 Evento 1

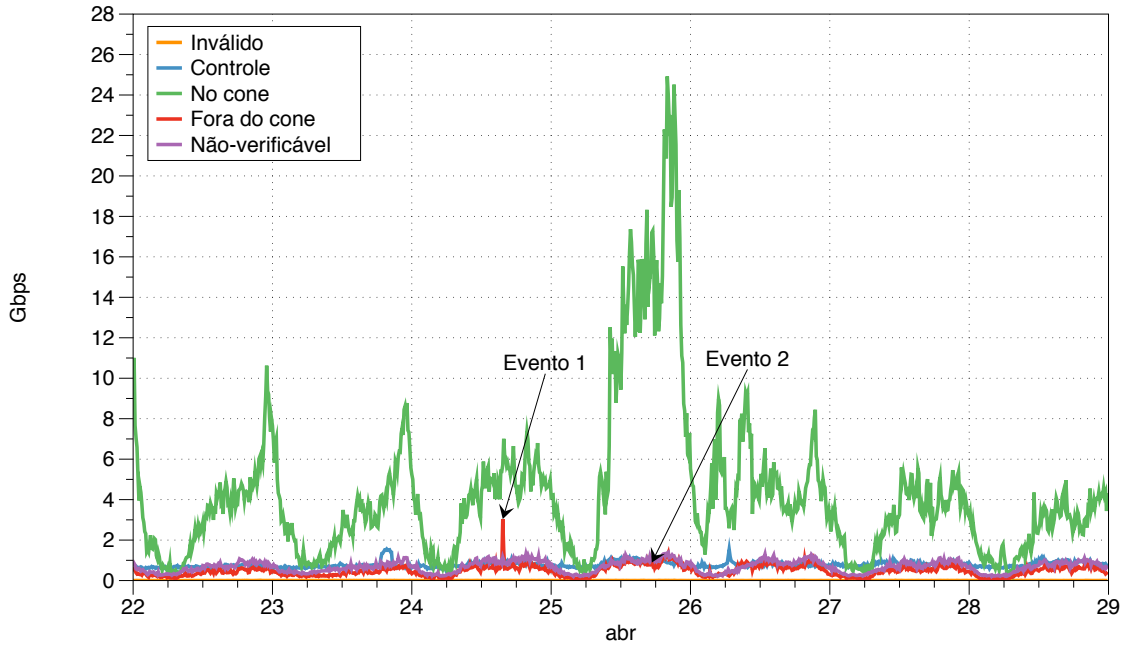
Este evento consiste em uma flutuação no tráfego classificado como fora do cone, chegando a atingir 3 Gbps e 5 Mpps por volta das 15h do dia 24 de Abril de 2017. Analisando em detalhes os fluxos que induziram a variação na curva do tráfego fora do cone, identificamos as características a seguir.

Classe. Fora do cone

Endereço. *Unicast* $\rightarrow$ *Unicast*

Protocolo predominante. UDP (70%), TCP (29.2%)

Figura 6.2: Tráfego ao longo da janela de tempo do estudo – em *Gbps*



Fonte: os autores

Origem. 2 endereços (provedor de busca)

Porta origem predominante. 443 (73.6%), 80 (8.2%)

Destino. 1 endereço (Cliente)

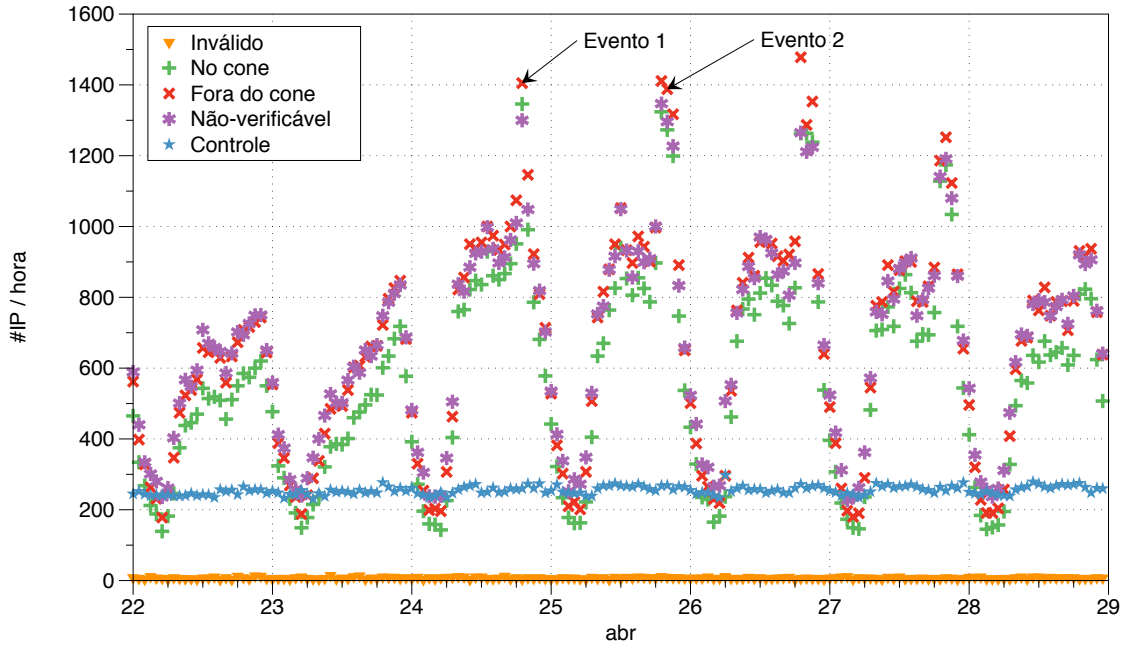
Porta destino predominante. Portas altas

Observando em detalhes as características dos fluxos, descobrimos que na verdade todo o tráfego vinha de dois endereços específicos, pertencentes a um provedor de busca. O tráfego estava sendo originado pelo provedor de busca e transportado até o IXP por um provedor *Tier-1*, que no contexto do IXP, entregava o tráfego ao AS membro de destino, um ISP regional. A julgar pelas características do fluxo, não acreditamos que se trate de um evento de ataque, mas sim de um falso positivo. Inspecionando o cone de clientes deste provedor *Tier-1*, descobrimos que o provedor de busca não está contido no cone. Portanto, acreditamos que o algoritmo de inferência de relações, apresentado na Seção 5.1.3, não foi capaz de inferir esta relação.

6.2 Evento 2

Este evento consiste em uma flutuação no tráfego classificado fora do cone, chegando a atingir 1.5 Gbps e 4 Mpps, por volta das 17h do dia 25 de Abril de 2017. Esta flutuação não chega a ser expressiva a nível de *bytes*. No entanto, a nível de pacotes, ela

Figura 6.3: Número de endereços de origem únicos ao longo da janela de tempo



Fonte: os autores

de fato chama a atenção. Analisando em detalhes os fluxos que induziram a variação na curva do tráfego fora do cone, identificamos as características a seguir.

Classe. Fora do cone

Endereço. *Unicast* $\rightarrow$ *Unicast*

Protocolo predominante. TCP 83%, UDP (12.3%)

Origem. 10 endereços (CDN)

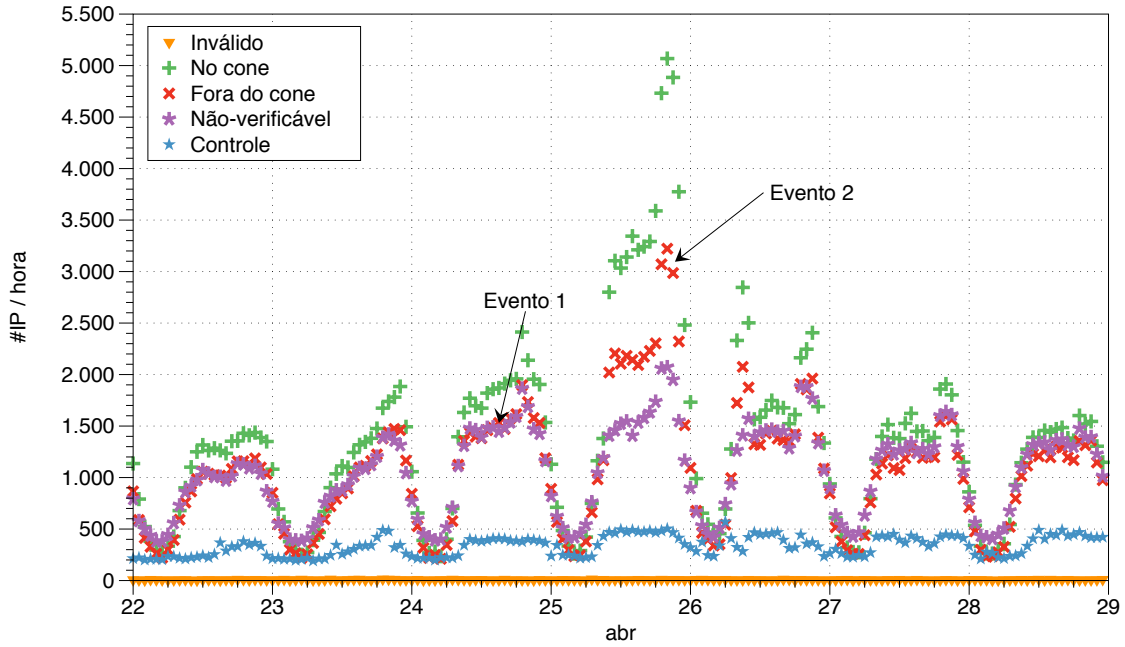
Porta origem predominante. Portas altas

Destino. 2000 endereços (Clientes)

Porta destino predominante. 443 (44.7%), 80 (27.2%)

Observando em detalhes as características dos fluxos, descobrimos que na verdade todo o tráfego era originado a partir de aproximadamente 10 endereços pertencentes a uma empresa de CDN. O tráfego estava sendo originado pela CDN, transportado até o IXP por um provedor de trânsito regional e entregue, através de um membro do IXP, a aproximadamente 2000 clientes de um ISP local. A julgar pelas características dos fluxos, mais uma vez, não acreditamos que se trate de um evento de ataque, mas sim de um falso positivo. Inspecionando o cone de clientes deste provedor de trânsito local, descobrimos que a CDN não está contida no cone. Através de nossas análises, observamos que algoritmos de inferência de relações, em geral, têm problemas para inferir relações onde uma das partes é uma empresa de CDN. Uma segunda questão curiosa neste evento é a numeração

Figura 6.4: Número de endereços de destino únicos ao longo da janela de tempo



Fonte: os autores

das portas de origem e destino, onde não fica claro se a CDN está servindo conteúdo, pois as portas HTTPS (443) e HTTP (80) estão do lado oposto a CDN, sugerindo que a CDN (origem do tráfego) estava se conectando a servidores nas redes dos clientes.

6.3 Discussão

Observamos que a qualidade da classificação está intrinsecamente relacionada com a qualidade das relações inferidas e do cone de clientes derivado das mesmas. Quase duas décadas desde o primeiro trabalho na área de inferência de relações (GAO, 2001), ainda não foi desenvolvido um mecanismo que seja preciso em todos os casos. Por isso, é esperado que exista ruído como resultado da classificação – tráfego válido classificado como inválido e vice-versa. Isto pode ser observado nos resultados medidos, onde nos dois eventos analisados, acreditamos não se tratarem de ataques, mas sim erros na classificação provocados por imprecisões originadas no processo de inferência de relações, que foram propagadas ao cone de clientes construído.

7 AVALIAÇÃO DA METODOLOGIA

Avaliar a eficácia da metodologia considerando somente os dados medidos é desafiador, pois exigiria um conjunto de validação que atestasse para o tráfego classificado, se a classificação foi correta ou não. Não existe um conjunto de dados que seja confiável e correto (*ground truth*) necessário para validação. Por isso, construímos um conjunto de teste sintético que viola a autenticidade de origem, permitindo ter uma visão inicial da eficácia da metodologia e suas limitações. Em seguida, discutimos sobre a precisão da metodologia em geral, comentando sobre suas vantagens e limitações.

7.1 Cenários de avaliação

Observações do Capítulo 6 sugerem a existência de tráfego válido classificado como inválido (falso positivo), em particular para dois casos discutidos nas Seções 6.1 e 6.2, mas não foi demonstrado o contrário. Portanto, visando avaliar a possível existência de casos em que a metodologia classifica tráfego como válido, mas que na verdade é inválido (falsos negativos), geramos situações onde o tráfego sintético consiste exclusivamente de tráfego que sofreu *spoofing*, comparando variações nos endereços de origem.

Como a análise de *spoofing* baseada em cone depende exclusivamente do endereço de origem e AS de ingresso no IXP, foram gerados quatro cenários de tráfego onde alteramos a forma como endereços de origem são gerados. Visando produzir uma análise mais próxima do real, simulamos em todos os casos, situações em que o tráfego poderia vir de qualquer AS membro: para cada fluxo gerado, sorteamos um membro do IXP para ser o AS de ingresso. A Tabela 7.1 resume as variações entre os cenários.

Cenário 1: classificação de *bogons*. Neste cenário, foi gerado tráfego com o endereço de origem falso de forma aleatória entre todo o espaço de endereçamento IPv6, sem nenhum critério limitador de origem e correspondente ao período entre 11h e 15h do dia 23 de Abril de 2017. Se trata de um caso visando testar o componente independente de cone da metodologia: a análise de *bogons*.

Cenário 2: vantagens do cone de clientes. Neste cenário, foi gerado tráfego correspondente ao período entre 21h e 23h do dia 25 de Abril de 2017, com o endereço de origem falso de forma aleatória entre um bloco de endereços IPv6 alocado para outro AS, e por isso, roteável na Internet. Por se tratar de um intervalo de *spoofing* além do intervalo *fullbogon*, consideramos este cenário para avaliar casos que não exploram fraquezas de

Tabela 7.1: Cenários de avaliação da metodologia

Cenário	Objetivo	Tipo de *spoofing*
1	Avaliar classificação de *bogons*	*Spoofing* de qualquer endereço do espaço IPv6
2	Avaliar vantagens do cone de clientes	*Spoofing* de endereços alocados
3	Avaliar limitações do cone de clientes	*Spoofing* de endereços alocados e contidos no CC
4	Avaliar a precisão das relações inferidas entre membros do IXP	*Spoofing* de endereços alocados a membros do IXP

Fonte: os autores

abordagens baseadas em CC.

Cenário 3: limitações do cone de clientes. Neste cenário, foi gerado tráfego correspondente ao período entre 10h e 14h do dia 26 de Abril de 2017, com o endereço de origem falso de forma aleatória contido no cone de clientes do AS que está ingressando o tráfego no IXP. O objetivo deste cenário é avaliar qual o impacto que o *spoofing* contido no CC provoca nos resultados da metodologia.

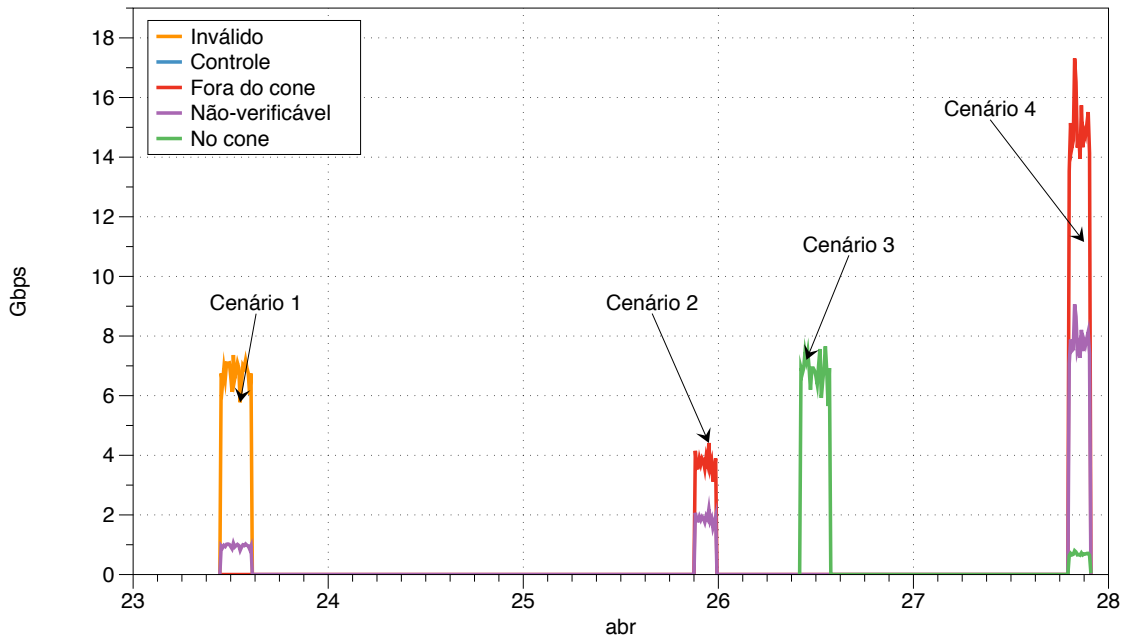
Cenário 4: precisão das relações inferidas entre membros do IXP. Neste cenário, foi gerado tráfego correspondente ao período entre 19h e 22h do dia 27 de Abril de 2017, com o endereço de origem falso de forma aleatória entre blocos de endereços IPv6 alocados para participantes do IXP. Primeiro, sorteamos um bloco pertencente a cada participante e o adicionamos como um possível intervalo de *spoofing*. Em seguida, geramos o tráfego sintético, sorteando para cada fluxo, um IP contido em um dos intervalos. Consideramos este cenário para avaliar, sob uma primeira perspectiva, a precisão das relações que o algoritmo de inferência realizou para casos de *peering* através do IXP estudado, e como isso afetaria os resultados da medição.

7.2 Resultados da avaliação

As Figuras 7.1, 7.2 e 7.3 ilustram o tráfego sintético sob perspectiva de tráfego, pacotes e número de endereços de origem.

Análise do cenário 1. Neste cenário, 2.395.144 fluxos foram analisados, onde em números absolutos, 87.5% foram classificados na categoria inválido (*bogons*). Os fluxos foram classificados desta maneira pois os endereços de origem pertenciam a inter-

Figura 7.1: Tráfego ao longo da janela de tempo do estudo – em *Gbps*



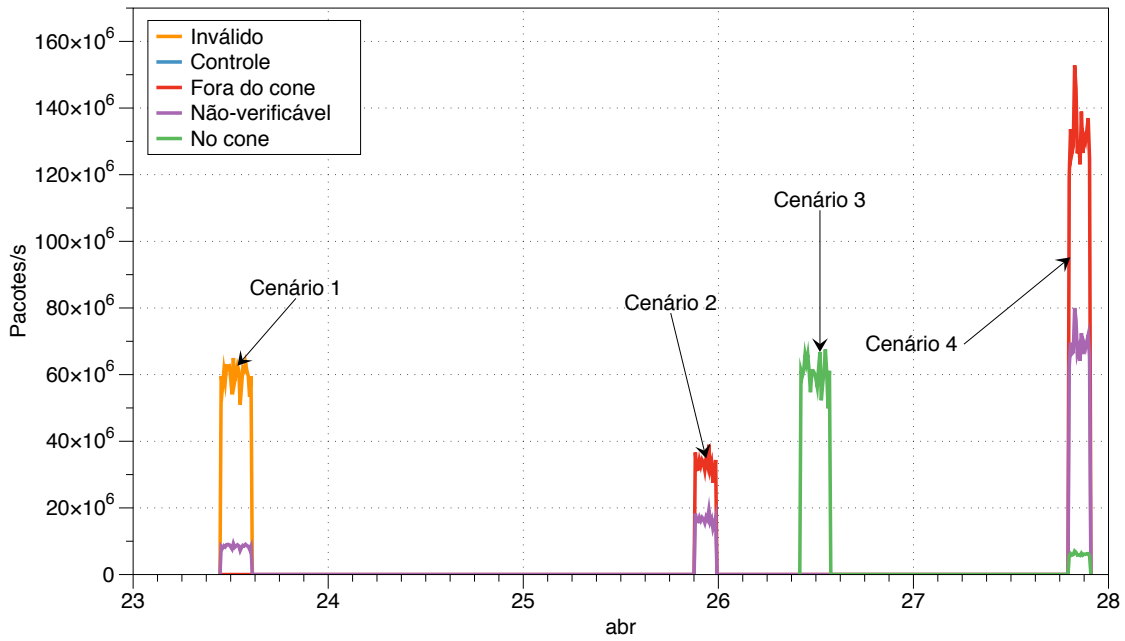
Fonte: os autores

valos não-alocados ou não-atribuídos, presentes na lista *fullbogons*. O restante dos fluxos (12.4%), foram classificados na categoria não-verificável, pois não foi possível determinar a qual AS pertence o endereço IP de origem do fluxo. A metodologia sem saber o número AS que corresponde com o IP de origem, não é capaz de testar a restrição de cone de clientes, como exposto na Seção 5.2.3. Por fim, uma quantia ínfima (0.004%) foi classificada como fora do cone. O resultado da análise deste cenário pode ser observado nas Figuras 7.1, 7.2, conforme indicado pela seta chamada Cenário 1.

Análise do cenário 2. Neste cenário, 1.236.480 fluxos foram analisados, onde em números absolutos, 66.7% foram classificados na categoria fora do cone. Os fluxos foram classificados desta maneira pois os endereços de origem violaram os limites do cone de clientes do AS que estava ingressando o tráfego no IXP. Os 33.3% restantes foram classificados como não-verificável, pois os ASes de ingresso não foram observados exportando rotas via BGP. Como não sabemos se foram nossos coletores que sofreram de visibilidade limitada ou se eles de fato (os ASes) não exportam rotas, este tipo de tráfego é classificado como não-verificável. Observa-se este cenário no local indicado pela seta chamada Cenário 2 nas Figuras 7.1, 7.2 e 7.3.

Análise do cenário 3. Neste cenário, 2.035.330 fluxos foram analisados, onde 100% foram classificados na categoria no cone. Eles foram classificados desta maneira pois os endereços de origem, embora falsos, pertenciam ao cone de clientes do AS que es-

Figura 7.2: Tráfego ao longo da janela de tempo do estudo – em pacotes



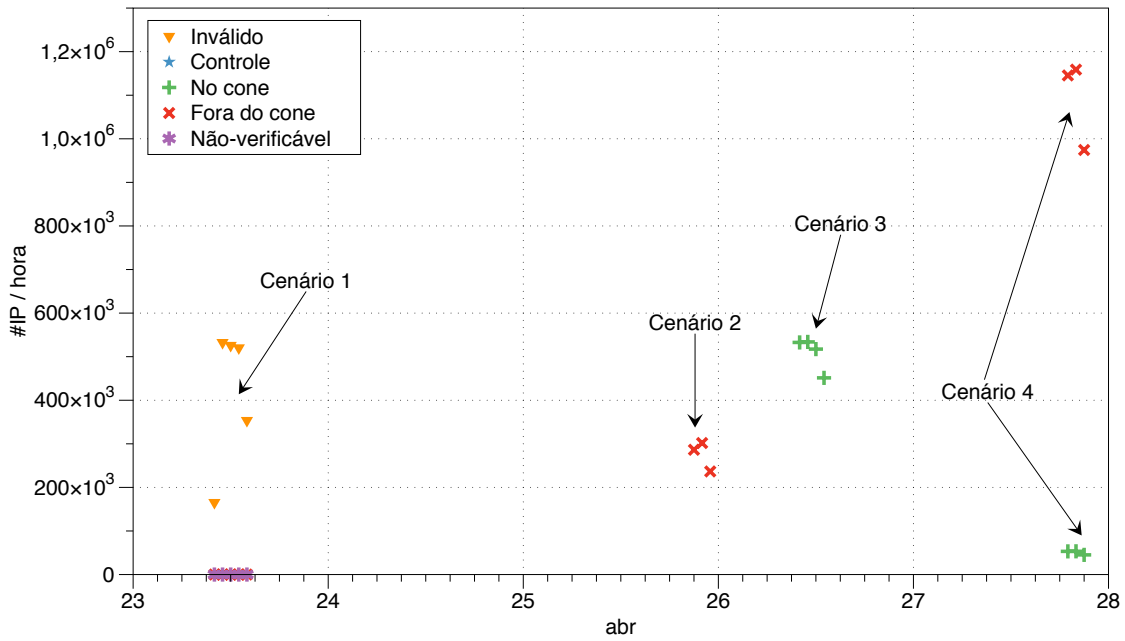
Fonte: os autores

tava ingressando tráfego no IXP. O resultado da análise deste cenário pode ser observado no local indicado pela seta chamada Cenário 3 nas Figuras 7.1, 7.2 e 7.3.

Visualmente observa-se variação significativa na curva, mas por se tratar de tráfego categorizado como no cone, pode induzir de início uma situação normal – mas não é. Esta situação ilustra uma limitação e também julgamos ser o maior desafio a ser superado para técnicas baseadas exclusivamente em cone de clientes. Um atacante de posse de informações privilegiadas sobre a topologia da Internet, poderia direcionar seu intervalo de *spoofing* para um pertencente ao cone de clientes do AS que vai encaminhar o tráfego mais adiante. Em contrapartida, quanto mais próximo das redes finais for posicionada a metodologia, mais efetiva é a detecção, pois reduz-se o intervalo violável de *spoofing*: o cone de clientes de um AS próximo da origem do tráfego tende a ser mais restritivo que o cone de um AS posicionado no núcleo da rede.

Análise do cenário 4. Neste cenário, 5.145.288 fluxos foram analisados, onde em números absolutos, 63.7% foram classificados como fora do cone, 33.3% como não-verificável e 2.95% no cone. A mesma razão mencionada no cenário 2 fez com que parte do fluxo deste cenário fosse classificada como não-verificável: os ASes de ingresso não foram observados exportando rotas via BGP. A avaliação deste cenário sugere que houveram imprecisões na inferência de relações entre os membros do IXP, devido ao número de falsos negativos. Observa-se os resultados no local indicado pela seta chamada

Figura 7.3: Número de endereços de origem únicos ao longo da janela de tempo



Fonte: os autores

Cenário 4, nas Figuras 7.1, 7.2 e 7.3.

7.2.1 Discussão

Nesta seção, comentamos dos resultados da avaliação da metodologia para cada cenário. Em seguida, discutimos sobre a precisão da metodologia em geral, discutindo suas vantagens e limitações. A Tabela 7.2 resume em quais das categorias o tráfego classificado pela metodologia é considerado válido, inválido (*spoofing*) ou inverificável e as razões que levaram a esta classificação.

Tabela 7.2: Avaliação do tráfego por categoria

Avaliação	Classificação	Observação
Válido	Controle	Tráfego valido no contexto local (de enlace) em que se encontra.
	No cone	Tráfego que respeita os limites do CC.
Inverificável	Não-verificável	Tráfego em que faltam informações para a classificação.
Inválido (*spoofing*)	Inválido	Tráfego oriundo de prefixos não roteáveis na Internet.
	Fora do cone	Tráfego que viola os limites do CC.

Fonte: os autores

Comparamos a precisão da classificação entre os diferentes cenários de *spoofing* gerados sinteticamente na Tabela 7.3. A precisão da metodologia, para cada cenário, foi computada a partir da divisão do número de fluxos que foram classificados corretamente nas categorias inválido ou fora do cone (verdadeiros positivos), que são as classes que podem conter tráfego *spoofing*, pela fração dos fluxos verificáveis (excluindo-se não-verificáveis).

Tabela 7.3: Resultados da avaliação

Cenário	Fluxos	Verificáveis	Verdadeiros positivos	Falsos negativos	Precisão (PPV)
1	2.395.144	2.097.307	2.097.307	0	100%
2	1.236.480	824.800	824.800	0	100%
3	2.035.330	2.035.330	0	2.035.330	0%
4	5.145.288	3.430.179	3.278.470	151.709	95.5%

Fonte: os autores

O cenário 3, conforme observado na Tabela 7.3 com 0% de precisão, ilustra a maior limitação da metodologia: *spoofing* feito em intervalo pertencente ao cone de clientes do AS que está ingressando tráfego no IXP. Embora a metodologia se tornar mais efetiva quanto mais próximo das redes finais estiver, o caso base vai persistir: *spoofing* dentro do cone do AS originador do tráfego vai passar como falso negativo. Para os casos (1 e 2), a lista *fullbogons* e o cone de clientes ofereceram limites de origem com uma boa precisão (100%). Nota-se em especial no cenários 3 e 4, a existência de falsos negativos, respondendo a pergunta introduzida no início deste Capítulo: sim, é possível a existência de casos em que a metodologia classifica tráfego como válido, mas que na verdade é inválido. Em especial no cenário 4, a metodologia obteve precisão de 95.5%, pois parte dos endereços utilizados no *spoofing* foram observados no cone de clientes.

Como mencionado acima, uma observação importante derivada da classificação é se a rede do AS de ingresso implementa SAV. O fato de não se observar tráfego inválido vindo de uma rede não é uma prova de que a mesma implemente mecanismos de SAV. No entanto, se for observado tráfego inválido oriundo de uma rede, é um indício de que a mesma não está empregando filtros de SAV, neste caso, indo no sentido oposto de políticas *antispoofing*. A Tabela 7.4 resume o que pode se concluir sobre SAV para cada classe de tráfego.

Tabela 7.4: Relação entre categorias de tráfego e SAV

Classificação	Implementa SAV
Controle	–
No cone	–
Não-verificável	–
Inválido	Evidências sugerem que não
Fora do cone	Evidências sugerem que não

Fonte: os autores

8 CONCLUSÕES

Neste trabalho, estendemos os recentes avanços baseados em cone de clientes para a detecção passiva de *spoofing* e de redes que não estão implementando validações no endereço de origem (SAV), restritos ao IPv4 (Müller, Lucas, 2019), à primeira análise e avaliação sob o contexto do IPv6.

Demonstramos como usar dados públicos do BGP para calcular uma hierarquia de ASes clientes abaixo de um AS raiz (conjunto este denominado "cone de clientes") e como utilizar este conjunto como limitante de intervalos válidos para endereços de origem, habilitando a classificação de tráfego nas cinco categorias que foram propostas. Em seguida, avaliamos a metodologia através de um conjunto de teste gerado sinteticamente sobreposto com dados medidos do sistema brasileiro de Pontos de Troca de Tráfego (PTTs). Discutimos, sob uma primeira perspectiva, em quais casos a metodologia funciona ou não, expondo seus pontos positivos e limitações. Para os casos em que ela não funciona, descrevemos os motivos.

Entre os principais desafios que enfrentamos ao desenvolver uma metodologia para IPv6, podemos citar o considerável custo computacional no processo de coleta e pré-processamento dos dados auxiliares, a inferência das relações entre ASes na topologia IPv6 e a análise dos resultados, em termos de falsos positivos. Através da análise dos eventos observados no Capítulo 6, onde na verdade se tratavam de falsos positivos, realçamos a importância que a precisão do algoritmo de inferência de relações possui na correta classificação do tráfego. Também demonstramos através de simulações de ataques, três casos a metodologia obteve alta precisão na classificação de tráfego verdadeiramente positivo: o tráfego que de fato era malicioso. Em um dos casos, demonstramos a principal limitação da metodologia: *spoofing* contido no CC do AS de ingresso no IXP.

Nossa metodologia pode servir como ponto de partida para novos trabalhos, se valendo das boas idéias que aqui foram apresentadas − e aprimorando nossas limitações. Como trabalhos futuros, consideramos propor melhorias na detecção de *spoofing* contido no cone de clientes, juntamente com a melhoria da precisão na inferência de relações complexas.

REFERÊNCIAS

AGER, B. et al. Anatomy of a large European IXP. **ACM SIGCOMM Computer Communication Review**, ACM, v. 42, n. 4, p. 163–174, 2012.

ALAETTINOGLU, C. et al. **Routing policy specification language (RPSL)**. [S.l.], 1999.

BAKER, F.; SAVOLA, P. **Ingress filtering for multihomed networks**. [S.l.], 2004. Best Current Practice; BCP 84.

BELLOVIN, S. M. Security problems in the tcp/ip protocol suite. **ACM SIGCOMM Computer Communication Review**, ACM, v. 19, n. 2, p. 32–48, 1989.

BLUNK, L.; KARIR, M.; LABOVITZ, C. Multi-threaded routing toolkit (mrt) routing information export format. **Internet Engineering Task Force, RFC**, v. 6396, 2011.

CAIDA As-Rank. **AS Rank project**. 2019. <http://as-rank.caida.org>. Online; accessed 22 May 2019.

CAIDA Bogon. **CYMRU Bogon Reference Dataset**. 2019. <https://www.caida.org/data/bogons/>. Online; accessed 03 Jun 2019.

CAIDA PeeringDB. **PeeringDB Dataset**. 2019. <https://www.caida.org/data/peeringdb/>. Online; accessed 03 Jun 2019.

CAIDA Spoofer. **Spoofer Project**. 2019. <https://spoofer.caida.org/summary.php>. Online; accessed 27 January 2019.

CLOUDFLARE. **The real cause of large DDoS - IP Spoofing**. 2018. <https://blog.cloudflare.com/the-root-cause-of-large-ddos-ip-spoofing/>. Online; accessed 29 January 2019.

DHAMDHERE, A. et al. Measuring the deployment of ipv6: topology, routing and performance. In: ACM. **Proceedings of the 2012 Internet Measurement Conference**. [S.l.], 2012. p. 537–550.

FERGUSON, P. **Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing**. [S.l.], 2000. Best Current Practice; BCP 38.

GAO, L. On inferring autonomous system relationships in the internet. **IEEE/ACM Trans. Netw.**, IEEE Press, Piscataway, NJ, USA, v. 9, n. 6, p. 733–745, dez. 2001. ISSN 1063-6692. Disponível em: <http://dx.doi.org/10.1109/90.974527>.

GIOTSAS, V. et al. Inferring complex as relationships. In: **Proceedings of the 2014 Conference on Internet Measurement Conference**. New York, NY, USA: ACM, 2014. (IMC '14), p. 23–30. ISBN 978-1-4503-3213-2. Disponível em: <http://doi.acm.org/10.1145/2663716.2663743>.

GIOTSAS, V. et al. Ipv6 as relationships, cliques, and congruence. In: SPRINGER. **International Conference on Passive and Active Network Measurement**. [S.l.], 2015. p. 111–122.

IPv6.br. **Endereçamento**. 2019. <http://ipv6.br/post/enderecamento/>. Online; accessed 03 Jun 2019.

ISOLARIO. **Isolario Project**. 2019. <https://www.isolario.it>. Online; accessed 29 January 2019.

IX.BR. **Ponto de Intercambio de Internet - IXP**. 2019. <http://ix.br>. Online; accessed 02 June 2019.

JIN, Y. et al. Stable and practical {AS} relationship inference with problink. In: **16th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 19)**. [S.l.: s.n.], 2019. p. 581–598.

KILLALEA, T. **Recommended internet service provider security services and procedures**. [S.l.], 2000.

Leber, M. **IPv6 internet broken**. 2009. <http://mailman.nanog.org/pipermail/nanog/2009-October/014017.html>. Online; accessed 27 May 2019.

LICHTBLAU, F. et al. Detection, classification, and analysis of inter-domain traffic with spoofed source IP addresses. In: **Proceedings of the 2017 Internet Measurement Conference**. New York, NY, USA: ACM, 2017. (IMC '17), p. 86–99. ISBN 978-1-4503-5118-8. Disponível em: <http://doi.acm.org/10.1145/3131365.3131367>.

LUCKIE, M. et al. As relationships, customer cones, and validation. In: **Proceedings of the 2013 Conference on Internet Measurement Conference**. New York, NY, USA: ACM, 2013. (IMC '13), p. 243–256. ISBN 978-1-4503-1953-9. Disponível em: <http://doi.acm.org/10.1145/2504730.2504735>.

MANRS. **Mutually Agreed Norms for Routing Security - antispoofing**. 2019. <https://www.manrs.org/isps/guide/antispoofing/>. Online; accessed 22 May 2019.

Müller, Lucas. **Improving Internet Infrastructure Security by Uncovering Spoofed Traffic in Inter-Domain Level Through the Lens of IXPs**. 2019. Thesis Proposal, UFRGS.

NETSCOUT. **NETSCOUT Arbor Confirms 1.7 Tbps DDoS Attack**. 2018. <https://www.netscout.com/blog/asert/netscout-arbor-confirms-17-tbps-ddos-attack-terabit-attack-era>. Online; accessed 03 Jun 2019.

NIC.br. **Portal de boas práticas para a Internet no Brasil - Antispoofing**. 2019. <https://bcp.nic.br/antispoofing>. Online; accessed 14 Jul 2019.

RIPE DATABASE. **RIPE Database**. 2019. <https://www.ripe.net/manage-ips-and-asns/db>. Online; accessed 28 May 2019.

RIPE RIS. **Routing Information Service (RIS)**. 2019. <https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data>. Online; accessed 29 January 2019.

ROUTE VIEWS. **Route Views Project**. 2019. <http://www.routeviews.org/routeviews/index.php/archive/>. Online; accessed 29 January 2019.

TEAM CYMRU. **THE BOGON REFERENCE**. 2019. <https://www.team-cymru.com/bogon-reference.html>. Online; accessed 28 May 2019.