UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM COMPUTAÇÃO

LEANDRO EMERSON MONDIN

Metodologia para Comparação de Desempenho do Plano de Dados de Sistemas Autônomos

Dissertação apresentada como requisito parcial para a obtenção do grau de Mestre em Ciência da Computação

Orientador: Prof. Dr. Marinho Pilla Barcellos

Porto Alegre
2022

CIP — CATALOGAÇÃO NA PUBLICAÇÃO

Mondin, Leandro Emerson

Metodologia para Comparação de Desempenho do Plano de Dados de Sistemas Autônomos / Leandro Emerson Mondin. – Porto Alegre: PPGC da UFRGS, 2022.

80 f.: il.

Dissertação (mestrado) – Universidade Federal do Rio Grande do Sul. Programa de Pós-Graduação em Computação, Porto Alegre, BR–RS, 2022. Orientador: Marinho Pilla Barcellos.

1. Internet. 2. Sistemas Autônomos. 3. Traceroute. 4. Medição. 5. Qualidade. 6. Séries Temporais. 7. Metodologia. I. Barcellos, Marinho Pilla. II. Título.

AGRADECIMENTOS

Essa dissertação é o fim de uma jornada, não apenas acadêmica, mas de uma importante página da minha vida. Se quando iniciei essa caminhada eu vivia uma vida, por assim dizer, estável e com caminhos previsíveis, o homem, que agora vira esta página, vive o oposto. Isso não significa que estas mudanças sejam ruins, pois, como diz um sábio ditado, "a vida começa onde acaba a sua zona de conforto". Mas aceitar as imprevisibilidades decorrentes das mudanças não é um opção fácil. Há o peso de ter que deixar coisas para trás, muitas delas importantes, para que seja possível seguir em frente.

Por que isso é relevante nestes agradecimentos? Porque sem a compreensão e apoio de muitas pessoas que eu tive o privilégio de fazerem parte da minha vida, essa dissertação teria sido uma, entre tantas outras coisas importantes, que eu tive que abandonar para seguir em frente.

A primeira pessoa que eu gostaria de agradecer, do fundo do meu coração, é o meu orientador, e agora amigo, Prof. Marinho Barcellos. Não existem palavras capazes de dimensionar o meu agradecimento à ele. Lembro que esta seção de agradecimentos, desde a primeira versão deste documento, continha apenas a seguinte frase: "Fica para o final, se houver um....". Em todas as revisões enviadas, o professor Marinho sempre adicionou um comentário de incentivo sobre esta frase. Embora este seja um exemplo singelo, ele representa o que o professor Marinho fez por mim durante estes vários anos de mestrado: nunca me deixou desistir. Muito obrigado meu amigo Marinho Barcellos pelos ensinamentos, compreensão e, principalmente, por não permitir que eu deixasse de concluir esta importante etapa da minha vida.

Outra pessoa fundamental nesta jornada, que ajudou muito na escolha do tema dessa dissertação e nos caminhos explorados durante o trabalho é o Professor Pedro Botelho Marcos. Agradeço muito ao Pedro pelos ensinamentos, suporte e apoio incondicional. Embora o nome do Pedro não esteja como co-orientador dessa dissertação, é justo dizer que este resultado também é mérito dele. Muito obrigado Pedro!!!!

Durante o meu engatinhar na área de pesquisa, também contei com colegas que merecem todo o meu agradecimento pela troca de ideias, dicas e ensinamentos. Dedico um especial agradecimento ao Lucas Leal, Fabrício Mazzola e Rodrigo Oliveira por terem me ajudado a caminhar em um meio diferente daqueles que estou

habituado.

Também gostaria de agradecer muito aos professores Jeferson Campos Nobre (UFRGS), Luciano Paschoal Gaspary (UFRGS) e Ricardo de Oliveira Schmidt (UPF) pelos valiosos *feedbacks* e contribuições que me ofereceram como membros do comitê de avaliação desta dissertação. Agradeço muito pelo privilégio de ter tido-os como avaliadores deste trabalho.

Trabalhar e construir este trabalho, ao mesmo tempo, não foi uma tarefa fácil. Gostaria de agradecer a compreensão e apoio de dois profissionais que tive o privilégio de trabalhar durante o período desta dissertação: Gustavo Neves Dias (RNP) e Valneis Signor Junior (Siemens Digital Industries Software). Muito obrigado a ambos. São líderes que me inspiram na vida profissional e o apoio deles viabilizou este resultado.

Se na academia e na vida profissional eu tive pessoas que tornaram possível a conclusão desta jornada, na vida pessoal não foi diferente. Agradeço a minha mãe (*in memoriam*), Irene Francisca Cardoso, ao meu pai, Silvio Airan Mondin, minha irmã, Lais Cristiane Mondin, e minha ex-esposa, Ana Lúcia Arrial da Rosa, pelo apoio e incentivo nesta e em todas as outras jornadas da minha vida até aqui. A confiança que eles sempre depositaram em mim, mesmo em situações onde eu mesmo não acreditava, foi sempre o incentivo decisivo que me fez seguir em frente.

Dedico um agradecimento especial à minha namorada e, se Deus quiser, futura esposa, Danielle Freitas Pereira, pela dedicação, amor, sugestões, correções e suporte durante a fase final deste trabalho. Muito obrigado Dani!!!!

Por fim, agradeço meu filho, Eric Arrial Mondin, pela singela razão de existir na minha vida. Ser pai do Eric colocou uma razão em minha existência e o amor que sinto por ele é, e sempre será, a força motriz por trás de tudo que faço. Espero que concluir este mestrado, com quase 50 anos, sirva, ao menos um pouco, de inspiração para ele, para nunca deixar de aprender e evoluir, independente da idade, enquanto ser humano e profissional. Eric, lembre-se sempre: "A maior lição da vida é a oportunidade de aprender algo novo a cada dia!!!".

RESUMO

A ausência de uma abordagem sistemática que possibilite a avaliação da qualidade de interconectividade provida por um Sistema Autônomo (AS - *Autonomous System*) pode ser uma limitação imposta aos operadores de rede na busca por melhores acordos de interconexão. Para avaliar diferentes provedores de trânsito ou mesmo possíveis parceiros para a troca de tráfego, um AS precisa estabelecer um acordo de interconexão por algum tempo para, então, estar habilitado a fazer esta comparação. Essa abordagem de tentativa e erro não é o ideal em um ambiente real, o que leva os operadores hoje a estabelecerem acordos com base em fatores subjetivos, como indicações de terceiros ou mesmo o reconhecimento pelo mercado de um fornecedor, podendo levar a acordos que não sejam os melhores possíveis. Este trabalho apresenta uma proposta de metodologia que busca inferir métricas objetivas sobre a qualidade do plano de dados de um AS sem que seja necessário estabelecer um acordo de interconexão com o mesmo. Nossa metodologia se vale de acordos de interconexão já estabelecidos com terceiros para determinar a latência entre os diferentes nós do caminho e através disso inferir potenciais situações de congestionamento. Para isso, usamos duas estratégias complementares: 1) Uma infraestrutura pública de medições na Internet, que possui *pontos de observação e medidas* instalados em diferentes ASes, usada para inferir métricas de qualidade de um AS; 2) Aplicamos uma abordagem de medição inspirada no TSLP (*Time-Sequence Latency Probes*), uma técnica utilizada para inferir congestionamentos persistentes em conexões inter-domínio, com o propósito de inferir métricas que possibilitem comparar a qualidade do plano de dados de diferentes ASes. Para avaliar a metodologia, nós realizamos uma série de medições, observando e comparando os resultados obtidos em diferentes ASes. Nós apresentamos um conjunto de estudos de caso que ajudam a ilustrar situações onde as métricas podem ser úteis a operadores.

Palavras-chave: Internet. Sistemas Autônomos. Traceroute. Medição. Qualidade. Séries Temporais. Metodologia.

A Methodology for Comparing the Performance of the Autonomous Systems Data Plan

ABSTRACT

The lack of a systematic approach that makes it possible to assess the quality of interconnectivity provided by an Autonomous System (AS) could be a limitation imposed for network operators to establish better interconnection agreements. In order to evaluate different transit providers or even possible partners for the traffic exchange, an AS has to establish an interconnection agreement and try it for some time before it´s able to make a comparison. Nowadays, this trial-and-error approach is not feasible in a real environment, leading operators to establish agreements based on subjective factors, such as third-party referrals or brand recognition that could lead to agreements not as good as they could be. This work presents a methodology that seeks to obtain objective and representative metrics on the quality of an AS data plan, without having to sign an interconnection agreement with it. Our methodology uses AS´s already established agreements with third-parties to determine latency in the hops of package flow and, thus, infer potential traffic jam situations. In order to do that, we combined 2 strategies: Using as VP (*Vantage Point*) a public infrastructure of *probes* available in different ASes on the Internet, we apply to our methodology principles inspired in TSLP (*Time-Sequence Latency Probes*), a technique used to infer persistent congestion on interdomain links. Using the same approach as this technique, we seek to infer metrics that make it possible to compare the quality of the data plan from different Autonomous Systems. To validate the methodology, we conducted measurements in different ASes looking to infer such metrics. We discuss the evidences that make it possible to believe that the approach proposed by this methodology has good foundations to achieve its purpose.

Keywords: Internet, Autonomous System, Measurement, Quality, Methodology, Data Plan, Time Series, Traceroute.

LISTA DE ABREVIATURAS E SIGLAS

AS	Autonomous system
ASes	Autonomous systems
ASN	Autonomous System Number
API	Application Programming Interface
BGP	Border Gateway Protocol
c2p	Consumer to Provider
CAIDA	Center for Applied Internet Data Analysis
CDN	Content Delivery Network
CSV	Comma Separated Values
eBGP	External Border Gateway Protocol
iBGP	Internal Border Gateway Protocol
ICMP	Internet Control Message Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IS-IS	Intermediate System to Intermediate System
ISP	Internet Service Provider
IX.br	Internet eXchange Brazil
IXP	Internet eXchange Point
json	JavaScript Object Notation
NDA	Non-disclosure Agreement
OSPF	Open Shortest Path First
p2p	Peer to Peer

RIPE	Réseaux IP Européens Network Coordination Centre
RTT	Round Trip Time
SLA	Service Level Agreement
TCP	Transmission Control Protocol
TSLP	Time-Sequence Latency Probes
TTL	Time To Live
VP	Vantagem Point

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A Internet é formada pela interconexão de milhares de sistemas autônomos (ASes). Um AS é uma área administrativa dentro da Internet com suas próprias políticas, interesses econômicos, rede e infraestrutura computacional. As interconexões entre os ASes é um fator crítico no desempenho dos fluxos de pacotes na Internet (AWDUCHE; AGOGBUA; MCMANUS, 1998).

O tráfego enviado através da Internet, normalmente, passa por um conjunto de ASes antes de chegar ao seu destino final (CHIU et al., 2015). Todos os ASes percorridos pelo fluxo de pacotes, entre a origem e o destino, podem ser afetados por congestionamentos dentro de sua rede ou na sua interconexão com outros ASes. A degradação no desempenho de qualquer um dos ASes envolvidos no fluxo de dados afetará o resultado experimentado pela origem.

Idealmente, um AS poderia melhorar o desempenho fim a fim se pudesse realizar sua decisão de próximo *hop* conhecendo o desempenho de cada opção de caminho até o destino dos pacotes. No entanto, o protocolo BGP (*Border Gateway Protocol*), que é o protocolo padrão *de facto* para o roteamento entre ASes na Internet, pode levar os roteadores de borda a realizarem escolhas de encaminhamento não ideais em termos de desempenho. O processo de escolha da melhor rota pelo protocolo BGP não leva em consideração critérios de desempenho, como latência até o destino, por exemplo, na escolha de próximo *hop*.

1.1 Motivação

Atualmente, os operadores de rede carecem de uma maneira sistemática e objetiva para avaliar a qualidade do plano de dados de ASes com os quais tenham interesse em estabelecer algum tipo de acordo de interconexão. A ausência de um método que possibilite uma escolha baseada em dados reais leva os ASes a realizarem suas escolhas de interconexão através de fatores subjetivos. Estudos recentes relatam que estas escolhas são baseadas em fatores como reconhecimento da marca e relacionamentos pré-estabelecidos (MARCOS et al., 2020). Esta estratégia de seleção é *ad-hoc* e baseada em tentativa e erro: a qualidade da interconexão com outros ASes é descoberta **após** o acordo ter sido estabelecido. Dessa forma, os ASes podem estar perdendo acordos melhores, por não serem capazes de determinar o

desempenho de um AS antes de estabelecer um acordo. Essa combinação de fatores pode levar a escolhas abaixo do ideal e gerar impactos financeiros e de desempenho.

Encontrar e avaliar melhores oportunidades de interconexão, sob bases objetivas, necessitaria que as informações de desempenho, estabilidade e respeito ao acordo de nível de serviço (SLA - *Service Level Agreement*) de um determinado AS fossem compartilhadas pelos seus parceiros e clientes. No entanto, cláusulas de confidencialidade impedem que estas informações sejam reveladas a terceiros (NORTON, 2014b). Dada esta limitação, hoje, para um AS escolher seus parceiros de interconexão com base em critérios de desempenho, ele deve experimentar os seus serviços por um tempo e colher métricas de desempenho para, então, compará-los. Em termos práticos, no entanto, isto não é o ideal.

A avaliação do desempenho do plano de dados de um AS pode não estar relacionada, exclusivamente, à busca por um melhor parceiro de interconexão, mas também pode influenciar as políticas de engenharia de tráfego de um AS. Um AS pode, através de seus acordos de interconexão, possuir múltiplas opções de encaminhamento do tráfego, tendo em conta um determinado destino. Essas múltiplas opções derivam dos acordos estabelecidos, sejam de *peering* ou *trânsito*. Um AS, que busque melhorar seu desempenho no encaminhamento de pacotes, deve escolher a melhor entre estas conexões, tendo em conta o desempenho de cada uma. Esta escolha deve ser expressa através da engenharia de tráfego do AS, já que os protocolos de roteamento inter-AS e intra-AS não utilizam o desempenho como um fator direto de suas escolhas. Mais detalhes sobre como estas escolhas podem ser realizadas estão discutidas no Capítulo 2.

Uma forma sistemática de encontrar oportunidades de acordos mais vantajosos técnica e economicamente e/ou melhorar o desempenho do seu próprio plano de dados, com o melhor uso dos acordos atuais, seriam duas das principais motivações que levariam um sistema autônomo a usar uma nova metodologia. Tal metodologia poderia ser capaz de responder a uma série de questões de desempenho benéficas/importantes aos ASes da Internet, tais como:

1. Em um determinado IXP (*Internet exchange point*), quais ASes provêm o serviço de *trânsito* com menor latência e *jitter* até um dado destino?
2. Qual provedor de *trânsito* possui maior estabilidade (ausência de congestionamentos) em relação a um conjunto de destinos?
3. Qual AS oferece menor latência para um acordo *peering* considerado um dado

grupo de destinos?

4. Existe algum provedor de *trânsito*, com o qual ainda não se tenha um acordo de interconexão, que possua métricas de desempenho melhor do que os provedores usados atualmente por um determinado AS?

1.2 Questões de Pesquisa

Considerando as motivações discutidas nesta proposta de metodologia, buscamos responder às seguintes questões de pesquisa:

1. É possível obter métricas objetivas e representativas sobre a qualidade do plano de dados de um sistema autônomo, sem que seja necessário ter um acordo de interconexão já estabelecido com este AS?
2. Estas métricas permanecem representativas ao longo do tempo?
3. É possível obter estas métricas sem que seja necessário alterar a infraestrutura dos ASes e sem impactar o desempenho dos mesmos?

1.3 Proposta e Principais Contribuições

A metodologia que propomos e avaliamos nesta dissertação busca obter métricas objetivas sobre o plano de dados de um sistema autônomo fazendo uso de *probes* disponibilizados por uma infraestrutura pública de experimentação na Internet, o RIPE ATLAS (NCC, 2021a). Os *probes* são usados como *Vantage Points* (VP) pela metodologia e permitem realizar medições em um AS fazendo uso dos acordos de interconexão já estabelecidos pelo mesmo.

Para inferir congestionamentos internos e métricas de desempenho do plano de dados dos ASes, implementamos uma variação do TSLP (*Time-Sequence Latency Probes*)(LUCKIE et al., 2014). Na validação realizada em (DHAMDHERE et al., 2018), este método mostrou-se eficaz para inferir congestionamentos nas filas de encaminhamento de pacotes dos roteadores em um fluxo de dados. O TSLP detecta o congestionamento em conexões inter-domínio ao observar as variações de RTT (*Round Trip Time*) dos roteadores localizados nas duas extremidades do enlace.

A aplicação dos mesmos princípios do TSLP em nossa metodologia possibilita o atendimento de duas premissas importantes do nosso trabalho: 1) A metodologia

concebida deve ser aplicável sem a necessidade de suporte a novos protocolos ou de alterações na infraestrutura atual dos ASes; 2) As medições realizadas não devem influir na operação normal do sistema autônomo sob avaliação.

A seguir estão apresentadas as principais contribuições deste trabalho:

- **Método de identificação e escolha de *probes* para as medições**: Como parte deste trabalho desenvolvemos um método para identificar e escolher o melhor conjunto de *probes* da infraestrutura do RIPE ATLAS para realizar nossas medições dado o interesse de avaliar o desempenho de latência do plano de dados de um determinado AS;
- **Método inspirado no TSLP para inferir possíveis congestionamentos em sistemas autônomos.** Partindo dos mesmos princípios do TSLP, concebemos um método que busca inferir congestionamentos internos em sistemas autônomos e para gerar medições de latência sobre o plano de dados deste AS;
- **Avaliação da metodologia.** Apresentamos cinco estudos de caso demonstrando o uso da metodologia em cenários reais. Mostramos que o método é capaz de apresentar indícios de congestionamentos internos em sistemas autônomos e inferir métricas de latência que possibilitem a comparação entre ASes, dado um conjunto de destinos na Internet.

1.4 Principais Desafios

Os principais desafios para atingir os propósitos deste trabalho estão listados a seguir:

1. Disponibilidade de *probes*, em quantidade adequada, dados os objetivos de uma campanha de medição utilizando a metodologia proposta;
2. O fluxo de *traceroutes* originado nos *probes* deve percorrer o sistema autônomo que se pretende avaliar. Os ASes onde os *probes* estão instalados podem possuir diversos acordos, não apenas com o AS sob avaliação. Assim, as políticas de roteamento de cada AS que hospeda os *probes* é que determinarão se o fluxo de pacotes percorrerá o AS sob avaliação. Inferir estas políticas com base nos destinos experimentados é um dos principais desafios deste trabalho;
3. A dinâmica de roteamento da Internet pode levar os fluxos de *traceroutes*

a sofrerem alterações de caminho durante as medições. Como as medições desta metodologia são realizadas por longos períodos de tempo, tais mudanças podem impactar ou mesmo invalidar aquelas medições em andamento;

4. Lidar com as limitações inerentes às medições de latência com o protocolo ICMP, como, por exemplo, a assimetria de rotas e a ausência de resposta dos roteadores aos pacotes RTT;
5. Adaptar o uso do TSLP a um ambiente com mais variáveis envolvidas do que aquele onde o método foi validado;
6. Extrair métricas de desempenho, que sejam representativas, ao longo do tempo, sobre a qualidade no encaminhamento de pacotes de um determinado AS.

Na metodologia concebida como parte desta dissertação lidamos de formas diferentes com os desafios apresentados acima. Com relação aos desafios 2, 5 e 6, adotamos soluções que atendem às necessidades da metodologia. Já com relação aos 1, 3 e 4, embora tenhamos adotado estratégias para minimizar os seus impactos nas medições que realizamos, eles permanecem desafios a serem tratados de forma mais adequada em trabalhos futuros.

1.5 Estrutura do Trabalho

Esta dissertação está organizada conforme a seguir: No Capítulo 2, apresentamos os conceitos fundamentais envolvidos no trabalho. Apresentamos no Capítulo 3 uma revisão de trabalhos que buscaram resolver problemas semelhantes àqueles desta dissertação. A metodologia construída como parte desta dissertação está apresentada no Capítulo 4. No Capítulo 5 apresentamos os resultados obtidos com o uso da metodologia a partir de cinco estudos de caso. Ao final, no Capítulo 6, trazemos as conclusões sobre os resultados obtidos com o uso da metodologia, algumas limitações identificadas e oportunidades de evolução.

2 CONCEITOS FUNDAMENTAIS

Neste capítulo estão apresentados alguns conceitos importantes para o melhor entendimento da metodologia proposta. Dado os objetivos deste trabalho, definir o que é um sistema autônomo, como se dá o roteamento entre ASes na Internet e que tipo de acordos são formalizados entre estes sistemas, são conceitos importantes para a leitura do restante desta dissertação. Na Seção 2.1 está apresentada uma definição sobre o que é um sistema autônomo, bem como, os tipos de roteamento realizados por estes sistemas. Na Seção 2.2 alguns aspectos relevantes sobre o roteamento inter-domínio estão apresentados. Já as Seções 2.3 e 2.4 apresentam, respectivamente, como os ASes costumam ser classificados e os tipos de acordos de interconexão normalmente estabelecidos entre os sistemas autônomos na Internet.

Para realizas as medições apresentados no Capítulo 5, foram utilizadas duas ferramentas que contribuem com a acuracidade dos resultados observados: *Paris traceroute* e *bdrmapIT*. A primeira, que está apresentada na Seção 2.5, possui melhorias importantes sobre *traceroute* "clássico" e possibilita à metodologia proposta uma melhor compreensão sobre o caminho percorrido pelos fluxos de medição. Já os detalhes da ferramenta *bdrmapIT*, que é utilizada pela metodologia proposta para identificar as bordas dos sistemas autônomos percorridos pelos *traceroutes*, estão apresentados na Seção 2.6.

Ao final, na Seção 2.7 estão detalhados de que forma estes conceitos e ferramentas estão ligados à metodologia proposta nesta dissertação.

2.1 Sistemas Autônomos - ASes

A Internet consiste da interconexão física e lógica entre mais de 108.000 sistemas autônomos (MAIGRON, 2021). Os ASes são áreas administrativas independentes, formadas por uma ou mais redes, com uma política de roteamento definida (HAWKINSON; BATES, 1996). Apesar da independência operacional e econômica, as decisões de interconexão tomadas por cada AS influenciam diretamente na topologia e nos padrões de tráfego observados na Internet. Conhecer como são estabelecidas as relações entre os ASes e suas decisões de roteamento são do interesse deste trabalho já que estes fatores impactam diretamente nas métricas de desempenho que buscamos inferir.

Quando se diz que dois sistemas autônomos possuem uma interconexão (ou um relacionamento) deve-se considerar dois níveis:

- *Conexão Física*: Entre os dois ASes há uma interconexão física que pode ser efetivada de muitas formas, como através de um cabo de fibra óptica, por exemplo. Em cada lado desta interconexão há ao menos um roteador de borda pertencente a cada um dos ASes. São estes roteadores que são utilizados para o encaminhamento de tráfego de um AS para o outro;
- *Sessão BGP*: Nos dois ASes participantes da interconexão existem roteadores chamados de *BGP speakers*. Entre estes roteadores é estabelecida uma sessão BGP, pela qual todas as rotas alcançáveis através de cada AS são divulgadas ao outro. Os *BGP speakers* podem ser também os roteadores de borda, mas isso não é uma condição mandatória.

Os sistemas autônomos realizam dois tipos de roteamento: *inter-AS* e *intra-AS*. *Intra-AS* refere-se ao roteamento realizado entre os roteadores internos do sistema autônomo e normalmente é realizado com o uso dos protocolos IS-IS (*Intermediate System to Intermediate System*) ou OSPF (*Open Shortest Path First*). Os detalhes do roteamento *intra-AS* não são visíveis a outros ASes. Já o roteamento *inter-AS* refere-se às políticas e protocolos usados pelo AS para receber e enviar tráfego de/para outros ASes. Considerando os interesses deste trabalho, na seção a seguir aprofundamos as discussões sobre o roteamento inter-domínio.

2.2 Roteamento Inter-Domínio

No roteamento entre ASes, ou inter-domínio, o procolo BGP desempenha um papel fundamental. É com base no aprendizado de rotas deste protocolo e no algoritmo de escolha de melhor rota que as decisões de encaminhamento de pacotes serão tomadas. Um AS pode estar conectado a diversos outros ASes, o que pode levar ao aprendizado de diferentes rotas para um mesmo prefixo.

Entre os vários caminhos aprendidos para se chegar a um prefixo na Internet, o BGP deve escolher qual o roteador *ingress* de outro AS os pacotes devem ser encaminhado. O processo de decisão do BGP está apresentado na Figura 2.1 (TEIXEIRA et al., 2004). Ele consiste em uma sequência de passos eliminatórios, com o objetivo final de selecionar uma única rota, que representa a melhor escolha.

O algoritmo de seleção do BGP percorre a lista da Figura 2.1 de cima para baixo. Sempre que uma das etapas gerar uma escolha única, o BGP interrompe os próximos passos e encaminha o pacote com base nesta escolha. Quando um passo não consegue selecionar uma única opção ele encaminha para o passo seguinte apenas as opções que ele não foi capaz de determinar a melhor.

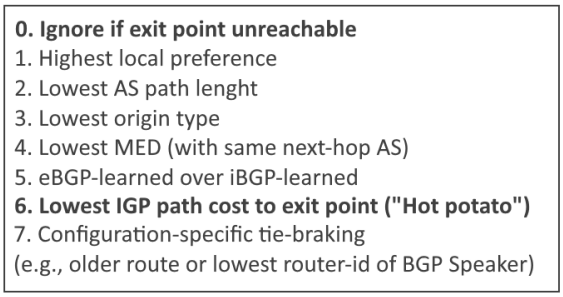


Figura 2.1 – Principais passos do processo de decisão do BGP - Reprodução da tabela 1 em (TEIXEIRA et al., 2004))

Outros passos podem estar presentes na lista da Figura 2.1, como, por exemplo, *Highest Weight*, *Oldest Path* e *Prefer eBGP over iBGP*, dependendo do fabricante do roteador. No entanto, independente dos fatores disponíveis, os parâmetros do BGP não possuem uma relação direta com métricas tradicionais de desempenho, como perda de pacotes ou latência, por exemplo. Devido a isso o BGP é considerado um protocolo agnóstico em termos de desempenho de rede.

Dos passos envolvidos no algoritmo de decisão do BGP apresentados na Figura 2.1, destacamos três que possuem diferentes influências nos resultados deste trabalho. O primeiro, *Highest local preference*, permite aos operadores de rede definirem preferências de encaminhamento de pacotes. Através desta opção, um AS pode determinar o próximo *hop* em direção a um prefixo, independente de qualquer outro critério do BGP. Esta preferência pode ser determinada por fatores técnicos e/ou econômicos. Com este parâmetro os operadores de rede podem, por exemplo, dar preferência ao encaminhamento de pacotes via um provedor com um custo de *trânsito* melhor frente as outras opções que ele possui. Outra possibilidade, que ampara algumas das principais motivações deste trabalho, seria os operadores de rede configurarem o próximo *hop* com base em métricas de desempenho em relação a um prefixo de destino na Internet.

O segundo parâmetro é o *Lowest AS path length*. Este parâmetro, que é o segundo passo no algoritmo de escolha do BGP, define que as decisões de encaminhamento de pacotes considerará o custo, em número de *hops*, até o destino. Dentre

os possíveis caminhos até o prefixo de destino aquele que possuir o menor custo, em número de *hops*, será o escolhido. O terceiro parâmetro que destacamos aqui é o *Lowest IGP path cost to exit point*. Quando o processo de decisão do BGP chega a este passo sem ter uma única rota definida até o destino, ele elege encaminhar os pacotes à outro AS usando o menor custo (em número de *hops*) de roteamento interno. Esta prática é conhecida como *hot potato* e pode impactar diretamente medições com ICMP, como aquelas usadas no neste trabalho.

2.3 Classificação de ASes

A RFC 1655 (GROSS; REKHTER, 1994) classifica os ASes conforme a maneira como eles lidam com o tráfego de *trânsito*, categorizando-os da seguinte forma:

- *stub AS*: Um AS que possui apenas uma única conexão a outro AS;
- *multihomed AS*: Um AS que conecta-se a mais de um AS mas que não realiza *trânsito* na sua infraestrutura para outros ASes;
- *transit AS*: São ASes de *trânsito* aqueles que conectam-se a mais de um AS e que utilizam sua infraestrutura para transportar seu próprio tráfego e de ASes que o contrataram para realizar o serviço de *trânsito*.

2.4 Tipos de Acordo entre ASes

As relações entre ASes são definidas, tipicamente, como *customer-to-provider* (*c2p*) e *peer-to-peer* (*p2p*) (LUCKIE et al., 2013). No relacionamento *c2p*, o cliente (*customer*) paga ao provedor (*provider*) para que este leve o tráfego ao restante da Internet. Neste tipo de relação, o provedor de *trânsito*, além de transportar o tráfego do cliente, deve também anunciar suas rotas ao restante da Internet e vice-versa. Em um relacionamento *p2p*, dois ASes proveem, reciprocamente, o acesso aos seus clientes, anunciando suas rotas entre si. Esta relação, tipicamente, não envolve custos, medições ou compromissos de SLA (NORTON, 2014a). Entretanto, em relações consideradas desbalanceadas, ou seja, quando um AS obtém maior benefício no encaminhamento de tráfego ao outro, podem ocorrer disputas ou até mesmo pagamentos por uma das partes (LUCKIE et al., 2014). Há, ainda, um terceiro tipo de relacionamento chamado *sibling-to-sibling* (s2s). Neste tipo relação, dois ASes

pertencentes a mesma organização ou área administrativa realizam trocas de tráfego entre si e com outros "irmãos"da mesma organização em relacionamentos *c2p* e *p2p* (LUCKIE et al., 2013).

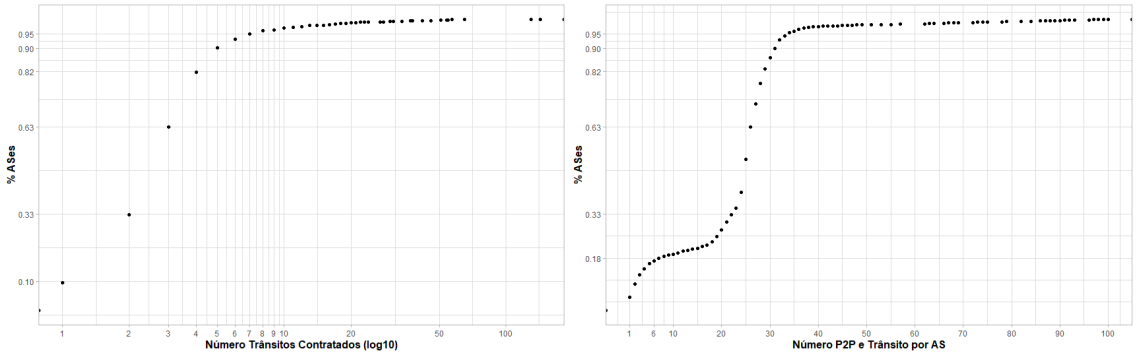
Benefícios econômicos e melhoras de desempenho têm sido os principais fatores observados para uma crescente adoção de relações *p2p* na Internet. Sob a perspectiva econômica, a opção de dois ASes trocarem o tráfego dos seus clientes diretamente, entre si, reduz os custos de *trânsito*. Em termos de desempenho, relações de *peering* podem oferecer caminhos mais curtos até o destino em estando ele localizado no parceiro de interconexão (AHMED et al., 2017). Outro aspecto importante nas relações *p2p* são os provedores de conteúdo (CDN - *Content Delivery Network*), particularmente, aqueles que operam como servidores de vídeo sob demanda (NETFLIX, Youtube), que hoje são responsáveis pela maior parte do tráfego na Internet (SANDVINE, 2021). Nesta relação, não há o interesse do provedor de conteúdo em obter uma relação simétrica, mas em oferecer uma melhor experiência aos seus usuários. Assim, mesmo que desbalanceada, esta relação permanece mutualmente benéfica.

Nos gráficos das Figuras 2.2b e 2.2a apresentamos uma análise realizada sobre o IX de São Paulo onde buscamos identificar os tipos de conexões estabelecidas por cada um dos ASes presente neste IXP[1]. Os resultados nos permite observar que os ASes buscam estabelecer múltiplos acordos e de diferentes tipos. Uma prática crescente nas relações entre ASes, que traz benefícios técnicos e econômicos, é estabelecer o maior número de acordos *p2p* possível e possuir relações *c2p* ajustadas às necessidades do restante do tráfego não supridos pelas relações *p2p* (NORTON, 2014a). Por exemplo, se um ISP (*Internet Service Provider*) possui acordos *p2p* com provedores de conteúdo de vídeo e os serviços de *streaming* correspondem a maior parte da demanda dos seus clientes, o ISP poderá tirar vantagem da relação *p2p* como o provedor de conteúdo, que geralmente não envolve custos, e contratar a banda do serviço de *trânsito* ajustada ao restante do seu tráfego.

2.5 Paris Traceroute

Para nossas medições utilizamos o *Paris Traceroute*, que traz uma série de melhorias em relação ao *traceroute* tradicional. Conforme (AUGUSTIN et al., 2006),

[1]Scripts Python usados para os cálculos disponíveis em https://github.com/lmondin/scripts



(a) CDF ASes vs Número Trânsitos Contratados (b) CDF ASes vs Número Trânsitos e P2P

Figura 2.2 – CDF Relacionamentos ASes IX-São Paulo

onde existir algum tipo de balanceamento de carga entre roteadores, não há uma rota única entre a origem e o destino dos pacotes. Existem diferentes técnicas de balanceamento de cargas, mas as duas mais comumente usadas são por destino ou fluxo.

No balanceamento por destino, o *traceroute* não sofre impacto, já que todos *ICMPs requests* enviados com o incremento gradual do TTL têm o mesmo destino. Porém, o balanceamento de carga por fluxo, que tem por objetivo encaminhar todos os pacotes pertencentes a um mesmo fluxo pelo mesmo caminho, traz um impacto direto aos resultados observados em um *traceroute*.

Na investigação realizada em (AUGUSTIN et al., 2006), o *checksum* do cabeçalho dos pacotes é um dos campos levados em consideração na decisão dos balanceadores de carga sobre que pacote pertence ao mesmo fluxo. Como o *traceroute* tradicional usa o incremento sucessivo do campo TTL para mapear o caminho dos pacotes até o destino, o *ICMP header checksum* é alterado nos sucessivos *ICMP Requests* enviados, mesmo que eles façam parte da mesma medição. Isso pode levar os balanceadores de carga a interpretarem os *ICMP Requests* da mesma campanha de medição como pertencentes a fluxos diferentes, levando-os a serem encaminhados por caminhos diferentes

Em termos práticos, o comportamento descrito anteriormente pode levar a um entendimento errôneo da topologia de rede entre o *host* que origina os pacotes e o destino dos mesmos. A Figura 2.3 (AUGUSTIN et al., 2006) pode auxiliar no entendimento desta limitação. Neste exemplo, **L** é um balanceador de carga localizado no *hop 1* do *host* que gera os pacotes de *traceroute*. A topologia real do *hop 1* ao *4* está apresentada à esquerda na figura. Os roteadores são representados como círculos e suas interfaces estão numeradas. Ao alterar o TTL para descobrir o próximo

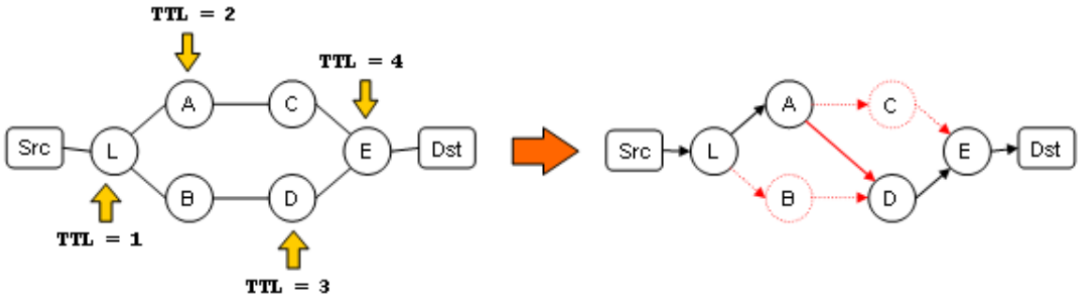


Figura 2.3 – Paris Traceroute (Augustin B. et al)

hop no caminho até o destino, o *traceroute* altera o *checksum* do cabeçalho, o que pode levar o balanceador de carga a interpretá-lo como um pacote não pertencente ao mesmo fluxo. As setas em amarelo mostram esta situação, ou seja, qual roteador recebeu o pacote com qual TTL. Observe-se que os pacotes com TTL 2 e 3 seguiram rotas diferentes, sem que o *traceroute* seja capaz de perceber isso, podendo levar a interpretação dos seus resultados a um entendimento equivocado sobre a topologia da rede. A interpretação do *traceroute* poderia levar a uma topologia como aquela apresenta à direita na figura. Este erro é tão impactante que alguém interpretando o resultado poderia entender que há uma interconexão direta entre os roteadores A e D, o que não corresponde à topologia real.

O *Paris traceroute* altera o cabeçalho do pacote IP de forma a manter o mesmo *checksum*, mesmo com a alteração de TTL, induzindo os balanceadores de carga a entenderem que os múltiplos pacotes enviados, durante uma medição utilizando o *Paris traceroute*, pertencem ao mesmo fluxo, levando-os os balanceadores à encaminha-los pelo mesmo caminho.

2.6 Identificação das Bordas de Sistemas Autônomos

Para poder modelar adequadamente o comportamento de um sistema autônomo usando nossa metodologia é necessário identificar corretamente as bordas do AS sob investigação.

Determinar a borda de um sistema autônomo não é uma tarefa simples. A solução mais intuitiva é identificar a que AS pertence cada IP no caminho do *traceroute*. Realizando esta conversão, temos cada roteador que respondeu ao ICMP associado a um IP, cujo prefixo pertence a um determinado AS. Um segundo passo seria agrupar os roteadores do mesmo AS no fluxo do *traceroute*. O resultado es-

perado é que roteadores do mesmo AS estejam em sequência, indicando o caminho que os pacotes percorreram dentro deste AS. O primeiro e o último roteadores desta sequência de IPs, representariam os roteadores de borda. A Figura 4.10, pode ajudar no entendimento desta abordagem simplificada.

Entretanto, há um conjunto de práticas na interconexão de sistemas autônomos que pode levar esta abordagem a identificar erradamente as bordas dos ASes, entre as quais podemos destacar algumas com base estudo realizado em (LUCKIE et al., 2016):

- *O endereço IP das interfaces dos roteadores podem pertencer ao AS vizinho*: Quando dois ASes interconectam-se através de um enlace ponto a ponto, eles tipicamente usam uma sub-rede do espaço de endereços IP de um deles (usualmente uma máscara /30 ou /31 em IPv4). Em uma relação *c2p*, o provedor tipicamente fornece o IP utilizado nos dois roteadores presentes nas duas extremidades da interconexão. Ao cruzar este link, o *traceroute* responderá em ambos roteadores com o IP do provedor e identificará erradamente o roteador de borda do AS cliente nesta relação;
- *Roteadores de borda podem ser configurados para bloquear pacotes ICMP*: Devido a questões de segurança, um operador de rede pode configurar seus roteadores de borda para descartar pacotes ICMP;
- *Roteadores virtuais podem usar uma interface diferente para responder ao ICMP*. Os operadores podem usar funcionalidades de roteamento virtual para isolar tabelas de roteamento de diferentes clientes. Cada roteador virtual usa um endereço IP diferente para a troca de mensagens BGP com os roteadores vizinhos. Quanto um pacote ICMP é enviado a um dos ASes atendidos por uma interface virtual com o TTL expirado, o roteador responderá ao ICMP com o endereço IP da tabela virtual e não com o endereço da interface física;
- *O comportamento de ASes com relacionamento sibling (dois ASes que pertençam a mesma instituição) pode confundir os algoritmos na tentativa de inferir a conectividade entre diferentes ASes*: ASes diferentes, mas pertencentes ao mesmo controle administrativo (*siblings*), podem originar diferentes prefixos, inclusive um do outro. O uso de inferências sobre a quem pertence um IP nestes casos, usando a ferramenta WHOIS, por exemplo, possui diversas limitações conhecidas(LUCKIE et al., 2016);

- *Endereços IP pertencentes ao IXP aparecem de forma inconsistentes no caminho dos pacotes*: Uma das formas dos IXPs promoverem o *peering* entre seus membros é compartilhar uma infraestrutura *fabric* e disponibilizar IPs do seu prefixo para o uso dos membros no roteamento dentro do IXP. O prefixo do IXP pode não ser anunciado pelo mesmo ao restante da Internet ou mesmo um AS pode anunciar, inadvertidamente, o prefixo do IXP ao restante da Internet, levando ao mapeamento equivocado sobre a qual AS pertence o IP;
- *Diferentes ASes podem anunciar o mesmo prefixo via BGP*: Alguns prefixos são originados por múltiplos ASes, que podem pertencer a uma mesma organização administrativa (*Sibling*) ou mesmo a organizações distintas. Quanto mais ASes originarem um prefixo, mais complexo é interpretar as transições entre ASes em um *traceroute*.

A lista apresentada acima demonstra que apenas mapear o endereço IP dos diferentes *hops* para determinar as bordas de um AS está sujeita a diversas falhas. Mais detalhes sobre as limitações apresentadas acima e o impacto delas na definição das bordas de um AS estão detalhadas no artigo (LUCKIE et al., 2016).

O *bdrmapIT* utiliza como ponto de partida para sua metodologia dois trabalhos anteriores, que, com o uso de um conjunto de heurísticas aplicadas a diferentes partes do problema, gera uma identificação mais precisa das bordas dos sistemas autônomos. O *bdrmap* (LUCKIE et al., 2016) desenvolveu um conjunto de heurísticas para analisar um gráfico baseado no roteamento IP observado em diversos *Vantage Points*. Já o segundo trabalho, o MAP-IT (MARDER; SMITH, 2016), aplica sua análise heurística com base em interfaces de rede, previamente obtidas a partir de diversos *Vantage Points*. O *bdrmapIT* faz uso de ambas as evoluções alcançadas por estes trabalhos e usa os resultados obtidos com o *bdrmap* como uma entrada adicional ao algoritmo de localização de bordas do *MAP-IT*.

De acordo com os autores, o *bdrmapIT* obteve uma acuracidade de identificação correta das bordas de sistemas autônomos, nos experimentos realizados, entre 91,8% e 98,8% .

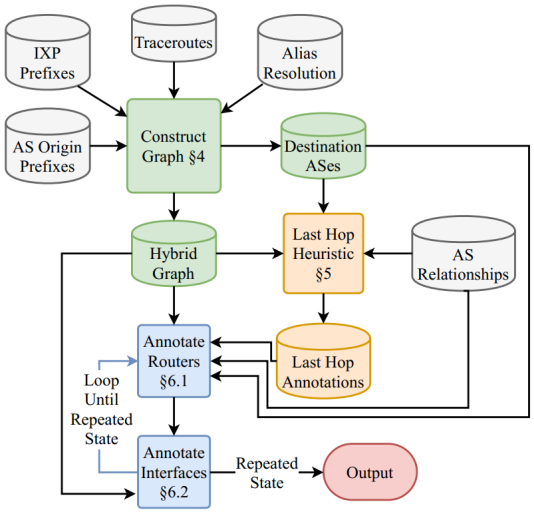


Figura 2.4 – *bdrmapIT* - extraído do trabalho (MARDER et al., 2018-11)

2.7 Sumário

Neste capítulo foram revisados alguns conceitos, definições, ferramentas e práticas de roteamento entre ASes, que são importantes para o melhor entendimento da metodologia proposta. Nas Seções 2.1, 2.2, 2.3 e 2.4 foram apresentados conceitos sobre sistemas autônomos, como eles são classificados nessa dissertação, formas de roteamento e os tipos de acordos de interconexão realizados entre os mesmos na Internet. Dentre os vários conceitos apresentados é importante ressaltar dois deles. O primeiro são os tipos de acordos de interconexão estabelecidos entre os sistemas autônomos. É do interesse da metodologia proposta possibilitar a comparação de desempenho de um determinado AS frente a diferentes acordos (*p2p* ou *c2p*). Já o segundo conceito está relacionado aos critérios utilizados pelo BGP para tomar decisões de roteamento. As decisões de roteamento de pacotes tomadas pelo protocolo BGP não levam em consideração métricas de desempenho normalmente presentes em SLAs (latência, *jitter*, perda de pacotes, entre outras). A metodologia proposta nesta dissertação pode avaliar a qualidade destas decisões ou até mesmo oferecer subsídios que poderiam ser usados na engenharia de tráfego de um AS.

O *Paris traceroute*, apresentado na seção 2.5, é utilizado em todas as medições da metodologia proposta. O *Paris traceroute* possui um evolução importante sobre o *traceroute* "clássico", presente na maior parte dos Sistemas Operacionais, que evita que balanceadores de carga, quando presentes no fluxo de medição, gerem resultados de *traceroutes* que não representam fielmente a topologia de rede percorrida pelos pacotes ICMP. Topologias inferidas utilizando o *traceroute* "clássico"

estão sujeitas a erros, conforme discutido na Seção 2.5, o que pode levar à falsa identificação dos roteadores de borda dos sistemas autônomos e, por consequência, ao uso equivocado da metodologia. No restante desta dissertação, ao nos referirmos a *traceroutes* estamos nos referindo ao *Paris Traceroute*, exceto quando o contrário for informado.

Identificar os roteadores de borda dos ASes nos resultados gerados pelo *Paris traceroute* é um aspecto crítico para o uso da metodologia. Para avaliar o comportamento de um determinado AS sob investigação é essencial identificar, precisamente, o roteador de entrada (*ingress*) e saída (*egress*) dos sistemas autônomos presentes nos resultados dos *traceroutes*. A partir desta identificação, métricas de desempenho do AS sob investigação podem ser obtidas com o uso da metodologia. Neste trabalho, foi utilizada a ferramenta *bdrmapIT*, descrita na Seção 2.6, que representa hoje o estado da arte na identificação das bordas de sistemas autônomos em resultados de medições.

3 TRABALHOS RELACIONADOS

Trabalhos anteriores já propuseram soluções para avaliar métricas que representem o desempenho do plano de dados de sistemas autônomos, bem como, comparar o desempenho de relações *c2p* e *p2p* e detectar congestionamentos no fluxo de pacotes.

Avaliação do respeito ao SLA acordado entre ASes. Uma das principais motivações para monitorar o nível de serviço de um provedor de *trânsito* está em verificar se o mesmo está cumprindo com as métricas estabelecidas no acordo assinado entre as partes. De acordo com (MARTIN; NILSSON, 2002), entre as principais métricas utilizadas nos acordos de SLA estão latência, perda de pacotes e *jitter*, além da disponibilidade do serviço. Metodologias para medir estas métricas têm sido propostas pela comunidade científica usando diferentes abordagens. Em (ARGYRAKI; MANIATIS; SINGLA, 2010) os autores propõem um mecanismo verificável, onde cada AS declara suas medidas de desempenho, que podem ser verificadas pelos outros ASes. Em (KOMPELLA et al., 2009), a proposta baseia-se na colaboração entre todos os roteadores envolvidos em um fluxo de pacotes para, coordenadamente, medir a latência e a perda de pacote através dos diferentes ASes. Já em (SOMMERS et al., 2007), são propostos novos métodos para avaliar, de forma mais precisa, métricas presentes em SLAs como perda de pacotes, atraso médio e vazão. Embora a validação do trabalho tenha sido realizada em experimentos laboratoriais, o propósito do método é um AS poder usar esta metodologia para avaliar seus parceiros. Para a primeira e a segunda proposta são necessárias alterações na infraestrutura dos sistemas autônomos. Já a terceira pressupõe um acordo de interconexão pré-estabelecido com um provedor de *trânsito* que se pretende avaliar o respeito ao SLA acordado.

Trabalhos como (MARCOS et al., 2018) e (CASTRO et al., 2015) propõem novos métodos onde os ASes são avaliados de forma anônima por seus parceiros de interconexão. Entendemos que estes trabalhos apresentam um avanço importante na dinâmica de acordos entre ASes, mas ainda são carregados de fatores subjetivos. A ausência de métricas e metodologias unificadas para estas avaliações podem gerar percepções diferentes sobre o que representa a qualidade de cada AS. Somado a isso, conforme os resultados deste trabalho demonstram, é bastante complexo definir uma visão unificada sobre a qualidade de um AS sem estratificar os resultados por destino. Acreditamos que estes trabalhos poderiam ser um complemento à metodologia que

propomos aqui.

Métricas de Desempenho. Outra importante motivação para monitorar a qualidade provida por um sistema autônomo é avaliar o desempenho fim a fim de pacotes que percorrem este AS. Em (KOMPELLA et al., 2009) foi proposto um mecanismo de roteamento que é usado para medir a latência e *jitter*, *hop* a *hop*, no fluxo de pacotes. Apesar desta proposta oferecer métricas válidas para a avaliação de desempenho de um AS, ela também requer alterações de infraestrutura em todos os ASes presentes no fluxo.

Inferir congestionamentos em enlaces inter-domínio e fluxos TCP. Em (DHAMDHERE et al., 2018) foi utilizado o método TSLP para inferir congestionamentos em enlaces inter-domínio. Neste trabalho, os autores demonstram a eficácia do método e tiveram a oportunidade de confirmar junto aos ASes investigados os eventos de congestionamento observados. Com um objetivo similar, (SUNDARESAN et al., 2017) usou uma abordagem baseada em RTT para detectar congestionamentos em fluxos TCP (*Transmission Control Protocol*). Enquanto estes estudos buscam responder perguntas diferentes das nossas, eles são similares a nossa proposta sob três aspectos: buscam extrair suas métricas de qualidade de forma não intrusiva, fazem uso de protocolos padronizados da Internet e se baseiam em infraestruturas públicas de medição na Internet.

Em (FONTUGNE et al., 2017) os autores buscam identificar, em tempo real, eventos que possam ser interpretados como falhas nas interconexões entre ASes. Os autores argumentam que os operadores de rede possuem pouca visibilidade da Internet fora de suas bordas e, que tal ferramenta, auxilia o processo de depuração caso a falha observada não esteja dentro do AS. Com base nas medições diárias do RIPE ATLAS coletadas em tempo real, a implementação dos autores demonstrou ser eficaz nos seus objetivos. Enquanto este trabalho busca identificar falhas no roteamento inter-domínio na Internet, nosso trabalho tem um objetivo significativamente diferente já que busca analisar e extrair métricas de latência de um sistema autônomo em específico.

Para realizar uma comparação de desempenho entre interconexões baseadas em relações *peering* e *trânsito*, em (AHMED et al., 2017) os autores realizaram um experimento de larga escala, tendo como perspectiva redes de distribuição de conteúdo (CDN - *Content Distrubution Network*). Os autores colaboraram com uma CDN de escala global, presente em diversos IXPs no mundo, *embarcando* códigos

javascript em páginas hospedadas pelos provedores. Estes *scripts* realizaram testes de vazão, perda de pacotes e latência do *host* do usuário até a rede da CDN. Essa proposta distancia-se da nossa em alguns aspectos importantes: 1) Ela busca comparar o desempenho de relações *p2p* e *c2p* apenas sob a perspectiva de uma rede de distribuição de conteúdo; 2) Os resultados obtidos pelos autores fazem uma avaliação fim a fim, mas não isolam a participação do serviço de *trânsito* ou *p2p* no resultado final; 3) Para que pacotes, ICMP ou não, sejam encaminhados entre ASes, deve haver algum tipo de acordo estabelecido entre os mesmos. Com isso, para avaliar as métricas deste trabalho, devem existir acordos pré-estabelecidos entre o CDN e os ASes que serão avaliados.

4 METODOLOGIA

Nossa abordagem para inferir congestionamentos e métricas de qualidade de ASes é inspirada no TSLP, cujo exemplo de topologia está apresentado na Figura 4.1. A ideia por trás deste método é enviar, repetidamente, pacotes de *ICMP Echo Request* para os roteadores *near end* e *far end*, localizados nas duas extremidades de um enlace inter-domínio. Caso a latência observada no roteador *far end* aumente, de forma persistente, sem que um aumento equivalente seja observado no roteador *near end*, o método infere que há um congestionamento neste enlace.

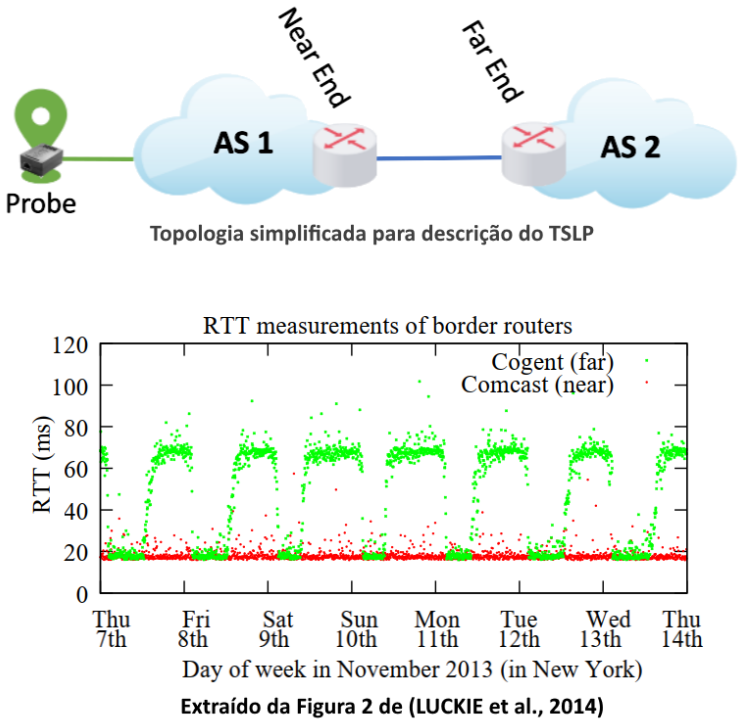


Figura 4.1 – Topologia método TSLP e exemplo de medições dos roteadores *near* e *far end*

Embora o TSLP tenha sido concebido para detectar congestionamentos em enlaces inter-domínio, adaptamos sua aplicação aos propósitos deste trabalho. Como um sistema autônomo envolve um conjunto maior de variáveis do que um enlace inter-domínio, nossa adaptação do TSLP envolveu a medição de diversas outros parâmetros envolvidos nos fluxos de teste. Ao percorrer os diversos passos da nossa metodologia, onde estes diferentes parâmetros são analisados de forma complementar, buscamos coletar um conjunto de indícios que indiquem que o AS investigado pode ter sofrido algum grau de congestionamento durante as medições.

Somado à inferência de possíveis congestionamentos, nossa metodologia também busca inferir outras métricas de latência do plano de dados de um AS. As medições ativas nos fornecem informações que, se interpretadas corretamente, permitem inferir métricas adicionais como o tempo de roteamento interno de um AS e o impacto na latência fim a fim das decisões de roteamento inter-AS deste sistema autônomo.

Outro aspecto relevante, que herdamos do TSLP, são as observações de longa duração representadas graficamente através de séries temporais. O objetivo das observações de longa duração é tentar estabelecer um "padrão de normalidade" para as métricas de latência obtidas em relação ao AS de interesse. Valores fora do comum podem indicar anomalias de desempenho e gerar alertas para que sejam investigados.

Exemplo. A Figura 4.2 apresenta um exemplo simplificado que será usado no restante deste documento para ilustrar como a metodologia proposta opera. O aspecto central do nosso método é o uso da combinação de diferentes *probes* e destinos para inicializar *traceroutes* que percorram um AS que se deseje avaliar. No exemplo, este AS está identificado como **ASN2** e, sempre que nos referirmos ao ASN2 no restante deste documento, estamos nos referindo ao sistema autônomo sob avaliação.

Ainda com relação à topologia de referência, sempre que mencionarmos o **ASN1** estamos nos referindo a um AS que hospeda *probes*. Esses *probes* são usados para gerar os *traceroutes* que percorrerão o ASN2.

Por sua vez, **ASN3** se refere ao roteador seguinte ao ASN2 no caminho *hop-a-hop* do *traceroute*, ou seja, o AS seguinte no caminho do *traceroute* atravessando a infraestrutura do ASN2 tendo um destino específico como alvo.

O princípio básico da metodologia é gerar, a partir de um conjunto de *probes* selecionados, *traceroutes* em direção a determinados destinos, tendo que o fluxo deste *traceroute* percorrer, necessariamente, o ASN2 sob avaliação. Ao realizar as medições por um longo período de tempo, a metodologia busca inferir possíveis congestionamentos no ASN2 e gerar métricas que possam ser representativas sobre a qualidade do plano de dados deste AS e de suas decisões de roteamento inter-domínio, tendo a latência como parâmetro de avaliação.

Um aspecto importante da metodologia proposta é o uso do que denominamos *campanhas de medição*. Os *traceroutes* inicializados em diferentes *probes*, simultaneamente, com o propósito de avaliar ou comparar sistemas autônomos, são

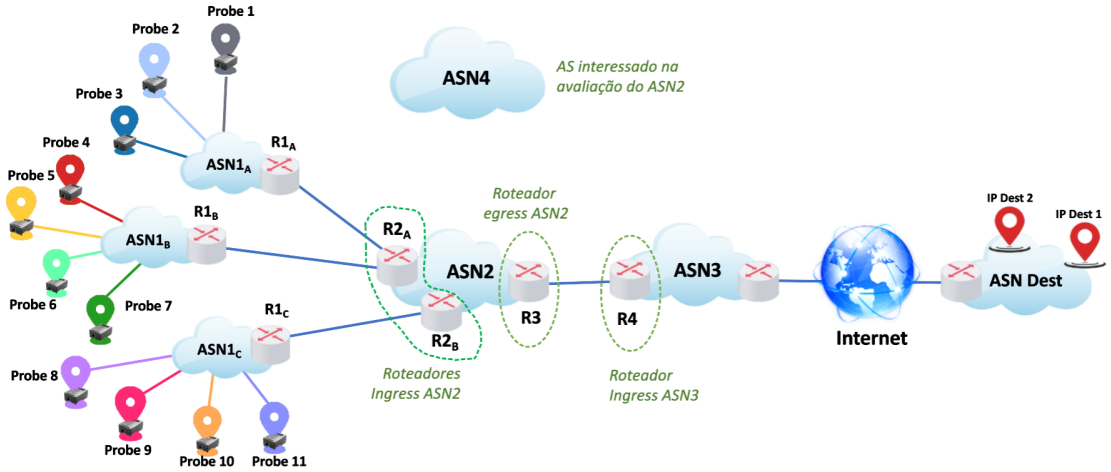


Figura 4.2 – Topologia de Referência

chamados nesta dissertação de *campanhas de medição*.

Em síntese, a metodologia proposta usa quatro estratégias complementares para atingir aos objetivos deste trabalho:

1. *Uso de uma infraestrutura pública de medição na Internet:* Os *probes* do RIPE ATLAS permitem à metodologia avaliar o desempenho de um AS, sob o ponto de vista das latências, com base nas relações já estabelecidas por este AS. Esta estratégia nos permite realizar medições do AS sob a perspectiva de um cliente (*c2p*) ou parceiro (*p2p*) de interconexão, sem que seja necessário estabelecer um novo acordo. Para inferir os acordos de interconexão entre estes ASes nós usamos o *dataset* disponibilizado pelo CAIDA (CAIDA, 2021a);
2. *Método inspirado no TSLP onde buscamos inferir possíveis congestionamentos e outras métricas de latência do AS sob investigação*;
3. *Campanhas de medições utilizando diversos probes:* O uso de diversos *probes*, especialmente se estes estiverem hospedados em ASN1s diferentes, ajuda a reduzir o impacto de outros fatores, como por exemplo o tipo de acordo estabelecido entre o ASN1, onde o *probe* está hospedado, e o ASN2;
4. *Análise dos resultados cruzando diferentes informações:* Múltiplas medições ativas e diferentes métricas (conforme apresentado na próxima seção) são combinadas para ajudar a reduzir o nível de incerteza. Apresentaremos os detalhes sobre essas análises na Seção 5.4.5.

4.1 Métricas de Interesse

Nossa metodologia busca inferir uma série de métricas que sejam representativas na comparação do desempenho, em termos de latência, entre sistemas autônomos. A principal métrica obtida pela metodologia é ΔASN2, que calcula a diferença da latência observada entre os roteadores *egress* e *ingress* do ASN2. Para minimizar os efeitos do *hot potato*, é parte essencial da metodologia escolher *probes* localizados em ASN1s que possuam um acordo de interconexão ativo com o ASN2 sob investigação. Com esta abordagem, o roteamento envolvido nos pacotes *ICMP Echo Request* em direção ao roteador *egress* do ASN2, bem como a resposta deste roteador, percorrerão apenas as infraestruturas do ASN1 e ASN2, minimizando assim os possíveis efeitos das assimetrias de pacotes.

Considerando o caminho de ida e de volta feito pelos pacotes dos *traceroute*, definimos na metodologia proposta uma série de métricas baseadas em latência. Estas métricas estão representadas na Figura 4.3 e definidas a seguir:

- Δ*ASN2: Diferença entre as latências medidas nos roteadores de borda do ASN2.* Esta métrica calcula a diferença do RTT medido entre os roteadores *egress* e *ingress* do ASN2. Ela nos permite inferir o tempo que os pacotes levam para percorrer a infraestrutura de rede do ASN2. O ΔASN2 também nos mostra uma primeira evidência da ocorrência de possíveis congestionamentos internos neste AS;
- $\Delta ASN3_{ingress}$*-Dest: Diferença entre o RTT medido no roteador ingress ASN3 e o destino dos pacotes.* O principal uso desta métrica é ajudar na avaliação das escolhas de roteamento inter-AS do ASN2. Ao comparar diferentes ASN2s, o $\Delta ASN3_{ingress}$-Dest ajuda a avaliar se o ASN2 possui bons acordos para o encaminhamento de pacotes em relação a um dado destino na Internet;
- $\Delta ASN2_{egress}$*-Dest*: Semelhante à métrica $\Delta ASN3_{ingress}$-Dest, porém inclui na medição o tempo de transporte dos pacotes pelo enlace entre ASN2 e ASN3;
- *RTT Probe-Destino: RTT medido do probe até o destino dos pacotes.* Além de ser uma métrica relevante ao comparar diferentes possibilidades de ASN2, ela também ajuda a mostrar a relevância de cada métrica proporcionalmente às demais;
- *RTT Probe-*$ASN2_{egress}$*: RTT medido do probe até o roteador* egress *do ASN2.*

Nesta medida estão incluídos o tempo total de roteamento do ASN1, ASN2 e o tempo de transporte do enlace entre ASN1 e ASN2;

- *RTT Probe-ASN3$_{ingress}$: RTT medido do probe em relação ao roteador ingress do ASN3*. Esta métrica é útil, em conjunto com RTT Probe-ASN2$_{\text{egress}}$, para medir a latência do enlace inter-domínio entre ASN2 e ASN3;
- *#Hops Probe-Destino: Número de* hops *entre o probe e o destino*: Esta métrica informa a contagem de *hops* percorridos pelo fluxo do *Paris traceroute* entre o *probe*, que gera os pacotes, e o destino;
- *#Hops$_{inter\text{-}ASN2}$: Número de* hops *percorridos pelos* traceroutes *na infraestrutura interna do ASN2*: Esta métrica informa a contagem de *hops* percorridos pelo fluxo de *traceroute* dentro do ASN2, excluindo os roteadores *ingress* e *egress*;
- *% de perda de pacotes*: Esta métrica determina o % da perda de pacotes a cada 30 medições realizadas. Utilizamos esta medição na busca por indícios que possam sugerir possíveis congestionamentos no ASN2;
- *# pacotes perdidos por medição*: Para cada medição realizada durante a campanha, tipicamente a cada 3 minutos, esta métrica informa o número de pacotes perdidos por *hop* medido pelo *Paris Traceroute*. Por medido, estamos nos referindo ao envio de pacotes *ICMP Echo Request*s este *hop*. O resultado desta métrica é a contagem, por *hop*, de quantos pacotes *ICMP Echo Request* foram respondidos pelos roteadores. O valor possívei para esta métrica é entre 0 (nenhum pacote *ICMP Echo Request* foi respondido) e 3 (todos foram respondidos).

4.2 Descrição da Metodologia

Conforme apresentado na Figura 4.4, a metodologia proposta é composta de cinco etapas. Na primeira, devem ser selecionados e validados os *probes* e destinos que serão utilizados em uma campanha de *traceroutes*. Na segunda, a infraestrutura do RIPE ATLAS deve ser configurada para realizar os *traceroutes*. Já na terceira etapa, as medições, que tipicamente são de longa duração, devem ser monitoradas e as operações de *traceroutes*, se necessárias, ajustadas de forma a garantir que alterações decorrentes da dinâmica de roteamento da Internet não invalidem os

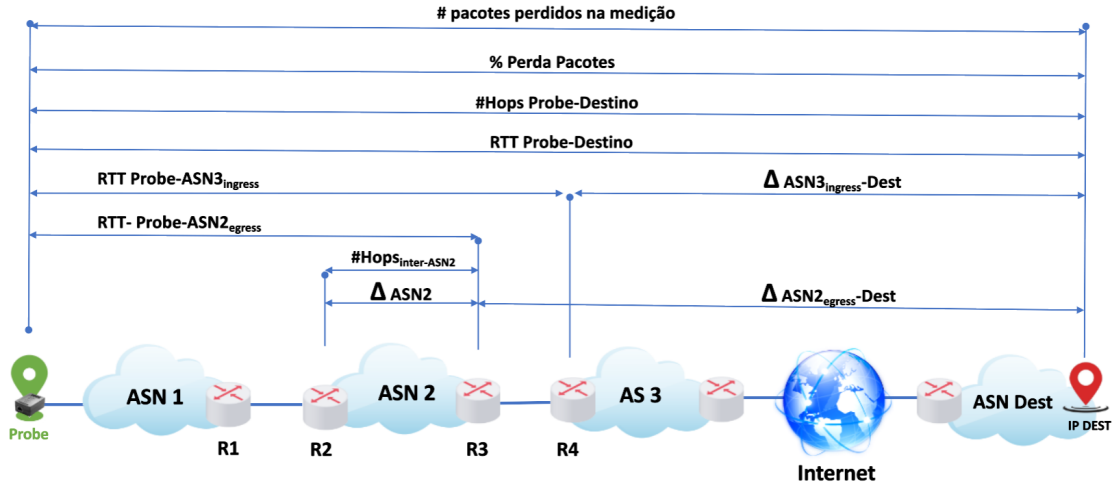


Figura 4.3 – Métricas de Interesse

resultados. Por fim, na quarta etapa, os resultados das medições devem ser coletados, normalizados e posteriormente analisados.

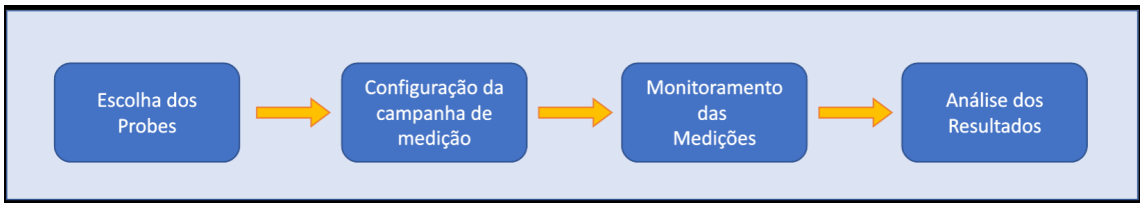


Figura 4.4 – As quatro etapas da metodologia

As seções a seguir apresentam os detalhes de cada uma destas etapas.

4.2.1 Seleção de Probes

O primeiro passo da metodologia é identificar um conjunto de *probes* que sejam os mais adequados à avaliação de um determinado ASN2. O processo de seleção de *probes* busca identificar na infraestrutura do RIPE ATLAS aqueles *probes* que possam ser usados para avaliar um dado ASN2.

A Figura 4.5 apresenta a primeira etapa do processo de escolha de *probes*, onde construímos uma base de informações para medições que chamamos de *Lista de Caminhos Conhecidos*. Nesta lista, armazenamos informações sobre todas combinações identificadas de *probes* e destinos que levam um *traceroute* a percorrer um ASN2. Quando iniciamos uma campanha, consultamos esta lista em busca de combinações de *probes* e destinos que viabilizem as medições sobre o ASN2 que desejamos avaliar. O Algoritmo 1 descreve os passos envolvidos na seleção de tuplas da lista

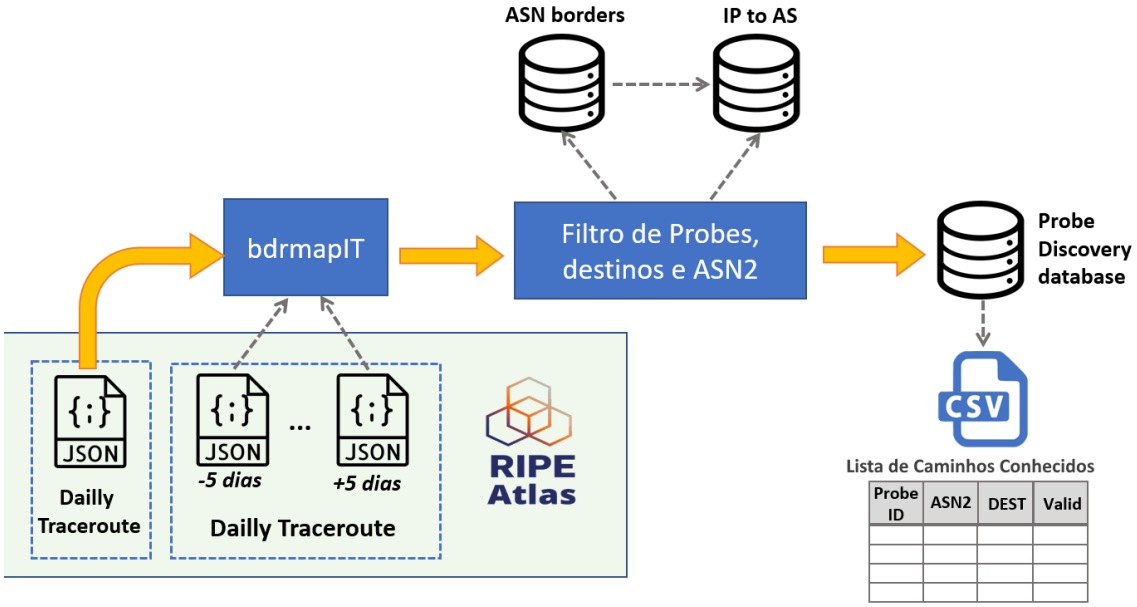


Figura 4.5 – Seleção de Probes

de caminhos conhecidos que atendam aos interesses da campanha de medições, ou seja, qual ASN2 se deseja avaliar em relação a qual *ASN Dest* na Internet.

Para criar uma primeira versão da *lista de caminhos conhecidos*, utilizamos medições públicas realizadas na infraestrutura do RIPE ATLAS por outros usuários e disponibilizadas diariamente em (NCC, 2021c). Esse conjunto de medições servem como um ponto de partida para as próximas campanhas de medições a serem realizadas. Saber de antemão que determinadas combinações de *probes* e destinos levam um fluxo de pacotes a percorrer um ASN2 em específico nos permite iniciar os *traceroutes* de forma mais assertiva, aumentando o índice de acerto nas escolhas dos *probes*.

Antes desta abordagem, buscamos utilizar outro método, onde partíamos do levantamento de quais ASes possuíam relações com o ASN2 que tínhamos interesse em avaliar. Uma vez identificadas estas relações, buscávamos *probes* dentro destes ASes e, então, iniciávamos *traceroutes* em direção a diversos destinos considerados populares na Internet, listados em (AMAZON, 2021)). Essa abordagem mostrou-se excessivamente trabalhosa e baseada em tentativa e erro, tendo em vista a impossibilidade de termos acesso às políticas de roteamento de cada ASN1. Durante estas avaliações preliminares, nossa taxa de sucesso foi excessivamente baixa (em menos de 3% os *traceroutes* percorriam o ASN2).

Como forma de aumentar a efetividade das campanhas de medição, passamos a usar as medições diárias disponibilizadas pelo RIPE ATLAS para construir uma

primeira versão da *lista de caminhos conhecidos*. Nessa nova abordagem, utilizamos sempre resultados recentes de *traceroutes* de outros usuários do RIPE ATLAS, o que elevou significativamente o índice de acerto nas escolhas de *probes* e destinos em nossas medições. Em avaliações realizadas durante a comparação das duas abordagens, verificamos que o índice de acerto pode chegar a 80% nas escolhas dos *probes* e destinos que levam um *traceroute* a percorrer um ASN2.

Data: AS para avaliação (*ASN2*) & AS de destino (*ASN Dest*).
Result: Tuplas da lista de caminhos conhecidos que contenham o *ASN2* e *ASN Dest* informados.
Inicialização: Lê a lista de caminhos conhecidos e inicializa a lista *listatuplas*;
while *não percorreu todas as tuplas da lista de caminhos conhecidos* **do**
    Lê a tupla da lista de caminhos conhecidos;
    if ASN2 *e* ASN Dest *presentes na tupla* **then**
        Adiciona a tupla a *listatuplas*;
    end
end
return *listatuplas*;

Algoritmo 1: Busca de *probes* na lista de caminhos conhecidos

Porém, há um problema que percebemos com esta abordagem, ainda durante a fase de avaliação, que chamamos de "envelhecimento" da lista de caminhos conhecidos. A dinâmica de roteamento da Internet leva parte dos dados presentes na lista de caminhos conhecidos a tornarem-se inválidos ao longo do tempo.

Para lidar com o "envelhecimento" da lista de caminhos conhecidos, adotamos duas estratégias. Primeira, realizamos uma pré-validação dos *probes* e destinos escolhidos para uma campanha antes de iniciarmos as medições de longa duração. Conforme apresentado na Figura 4.6 e no Algoritmo 2, caso durante a pré-validação seja detectado que o ASN2 percorrido pelo *traceroute* não é o esperado, a medição usando esta tupla não é realizada e a lista de caminhos conhecidos é atualizada. A segunda estratégia está relacionada ao tempo decorrido desde a última atualização da lista. Caso não tenham ocorrido medições pelos últimos 7 dias (período que observamos que entre 25% e 35% das tuplas validadas anteriormente deixam de percorrer

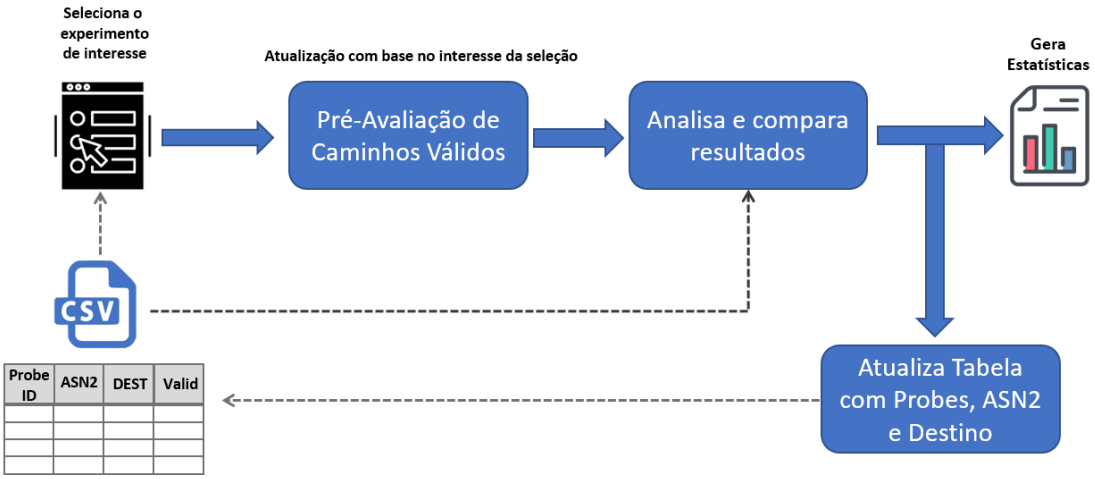


Figura 4.6 – Pré-Validação dos Caminhos Conhecidos

o mesmo ASN2), nós realizamos uma atualização da lista de caminhos conhecidos utilizando novos *datasets* de coleta diárias do RIPE ATLAS (NCC, 2021c).

As medições de outros usuários coletadas do RIPE ATLAS, utilizadas para gerar uma primeira versão ou para atualizar a lista de caminhos conhecidos, passam por etapas de tratamento e validação de dados antes das suas informações serem adicionadas à lista. Os resultados coletados são submetidos ao *bdrmapIT* para a identificação das bordas dos ASes envolvidos nos *traceroutes*. A seguir, as medições passam por um processo de sanitização de dados, descrito em detalhes na Seção 4.2.4. Este processo de filtragem dos resultados coletados tem por objetivo adicionar apenas dados de medições que atendam nossas necessidades de análise à lista de caminhos conhecidos.

A validade dos caminhos conhecidos e o ASN1 que hospeda o *probe* não são os únicos fatores levados em consideração pela metodologia na escolha dos *probes*. Em geral, havendo abundância de *probes* e destinos que viabilizem a medição de um determinado ASN2, buscamos escolher aqueles que tenham diferentes acordos entre ASN1 e ASN2, de forma a também avaliar esta variável.

Outros critérios diferentes daqueles discutidos nesta seção podem ser utilizados na escolha de *probes*, dependendo do objetivo da avaliação. Comparar ASes considerando um determinado destino ou qual AS possui o melhor desempenho em termos de latência para um acordo *c2p* são exemplos de objetivos possíveis para o uso da metodologia que podem implicar em critérios diferentes de escolha dos *probes*.

Data: Resultado do *traceroute* de pré-validação da tupla.
Result: Atualização da Lista de Caminhos Conhecidos e informa se o *traceroute* é válido
Inicialização: coleta o resultado do *traceroute* de pré-validação;
if *É possível identificar os roteadores de borda do ASN2* **then**
  // Resultado passou com sucesso pela sanitização
  if *resultado do* traceroute *percorreu o ASN2 esperado* **then**
    // ASN2 presente na tupla foi percorrido pelo traceroute
    Valida a tupla na lista de caminhos conhecidos (atualiza *timestamp*);
    // Medições com a tupla podem ser inicializadas
    Retorna que o *traceroute* é **válido** para o prosseguimento das medições de longa duração;
  else
    *// presente na tupla **não** foi percorrido pelo* traceroute
    Invalida a tupla na lista de caminhos conhecidos;
    // Medição não pode ser realizada
    Retorna que o *traceroute* é **inválido** para o prosseguimento das medições de longa duração;
  end
else
  // Experimento não pode ser realizado pois o resultado do traceroute *não permite identificar o ASN2*
  Invalida a tupla na lista de caminhos conhecidos;
  // Medição não pode ser realizada
  Retorna que o *traceroute* é **inválido** para o prosseguimento das medições de longa duração;
end

Algoritmo 2: Validação das tuplas selecionadas da lista de caminhos conhecidos

4.2.2 Configurando e Inicializando as Medições no RIPE ATLAS

Uma vez definido(s) o(s) ASN2 que se deseja avaliar, escolhidas e validadas as tuplas de *probes* e destinos que serão utilizadas para gerar os *traceroutes*, o passo seguinte é configurar a infraestrutura do RIPE ATLAS para realizar as medições. A Figura 4.7 apresenta a representação gráfica dos blocos envolvidos nesta configuração.

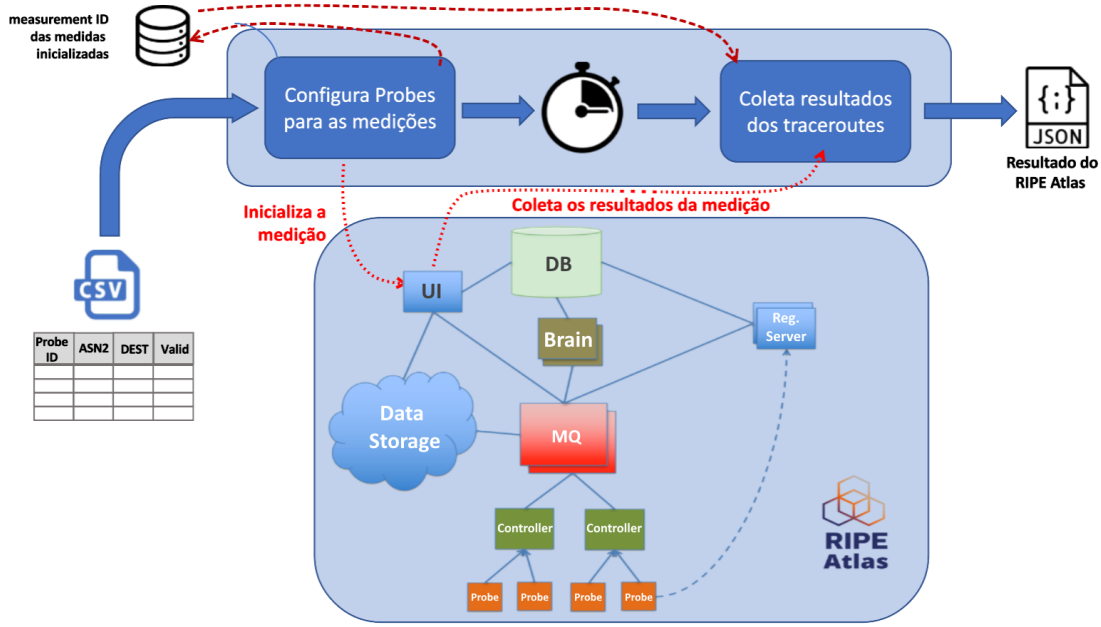


Figura 4.7 – Algoritmo de configuração de medição e coleta do RIPE ATLAS

Para a configuração da infraestrutura do RIPE ATLAS, utilizamos uma API REST, de forma que o algoritmo da metodologia realize esse processo de forma automatizada. O RIPE ATLAS oferece diversos parâmetros para a configuração dos *traceroutes*. A tabela da Figura 4.8 apresenta os parâmetros utilizados pela metodologia para a configuração dos *traceroutes*.

A infraestrutura do RIPE ATLAS retorna uma mensagem informando sobre o sucesso ou não da configuração da medição. No primeiro caso, o algoritmo recebe um *measurement id* como resposta. Esse ID corresponde a um número único na base de dados de medições do RIPE ATLAS e deve ser usado no momento da coleta dos resultados. Em caso de falha, um código de erro é informado.

Tipicamente, os erros reportados pelo RIPE ATLAS na etapa de configuração estão associados ao excesso de medições na infraestrutura em relação a um destino (o RIPE ATLAS permite no máximo até 100 medições simultâneas na infraestrutura para um mesmo IP de destino) ou a indisponibilidade do *probe* selecionado. Para a

PARÂMETRO	TIPO	DESCRIÇÃO	VALOR CONFIGURADO
probes	string	Configura que *probes* participarão da campanha de medição.	O *ProbeID* que identifica o *probe* escolhido na lista de caminhos conhecidos é informada neste campo.
start_time	string	Configuração do horário de inicio das medições (*Unix Timestamp*).	Em campanhas de medição este horário normalmente é configurado de forma que todos os *probes* participantes da campanha iniciem as medições no mesmo horário.
stop_time	string	Configuração do horário de término das medições do probe (*Unix Timestamp*).	Todos os *probes* de uma campanha são configurados para terminar simultaneamente.
type	string	Tipo de medição. Valores suportados: 'ping', 'traceroute', 'dns', 'sslcert', 'http', 'ntp' ou 'wifi'.	*Traceroute*.
paris	inteiro	Número de variações de cabeçalho a serem experimentadas pela campanha de medições com o Paris *Traceroute*. Valores: 0 (desabilita o Paris *Traceroute*) a 64	Em investigações preliminares, onde buscávamos mapear a topologia do AS sob investigação, usamos até 16 variações. Nas campanhas de medição, esse valor é configurado para 1, de forma a manter uma o cabeçalho ICPM constante, evitando o efeito dos balanceadores de carga no caminho do traceroute.
Protocol	string	Protocolo da medição. Valores possíveis: 'ICMP', 'UDP' ou 'TCP'	ICMP
Destination	string	Endereço IP de destino da medição	IP de destino extraído da lista de caminhos conhecidos.

Figura 4.8 – Parâmetros configurados no RIPE ATLAS

primeira situação, buscamos na lista de caminhos conhecidos outro IP de destino que pertença ao mesmo prefixo. Já para o segundo caso, também buscamos a solução na lista de caminhos conhecidos, mas neste caso a procura é por uma outra combinação de *probe* e destino que atendam as mesmas premissas usadas para a escolha do *probe* indisponível.

4.2.3 Monitoramento das Medições

Durante a execução de uma medição de longo prazo, podem ocorrer mudanças na topologia da rede da Internet que modifiquem as condições de medição. Por exemplo, um determinado tráfego gerado por um *probe* em direção a um destino pode deixar de percorrer o ASN2 que temos intenção de avaliar.

Realizamos coletas parciais a cada 30 minutos e efetuamos uma análise comparativa dos resultados da validação anterior. Se não houver alteração do ASN2 percorrido pelo fluxo de pacotes, mesmo que o roteamento interno ou os roteadores *ingress* ou *egress* do ASN2 tenham alterado, a medição segue normalmente.

Caso altere o ASN2 percorrido pelo fluxo do *traceroute*, a medição é interrompida e buscamos na lista de caminhos conhecidos outro *probe* que atenda aos requisitos da campanha de medição. Este novo *probe* passa pelo processo de validação e, então, um novo *traceroute* é iniciado.

Os resultados parciais coletados até a interrupção e os que serão gerados pelo novo *traceroute* devem ser tratados adequadamente na fase de análise. O princípio que norteou esta decisão de projeto foi manter o mesmo número de medições simultâneas planejadas no início da campanha.

4.2.4 Análise das Medições

A Figura 4.9 apresenta o *pipeline* para o tratamento das medições coletadas. O primeiro passo do *pipeline* é a sanitização dos dados. Conforme apresentado brevemente na Seção 1.4, um dos diversos problemas relacionados ao uso do *traceroute* é a não resposta de alguns roteadores aos pacotes ICMP. Esta situação pode estar relacionada a uma falha momentânea (um congestionamento, por exemplo) ou a uma configuração dos operadores de rede do AS para que os roteadores não respondam a este protocolo. A metodologia proposta diferencia estas situações na etapa de sanitização dos dados.

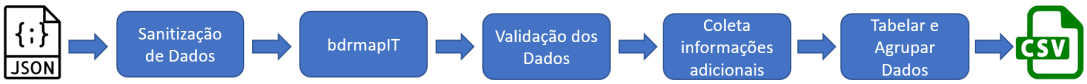


Figura 4.9 – Pipeline para tratamento das medições coletadas

Para identificar corretamente as bordas do ASN2, é necessário que um conjunto mínimo de respostas aos pacotes *ICMP Echo Request* sejam respondidos pelos roteadores percorridos pelo *traceroute*.

A Figura 4.10 apresenta um exemplo de um *traceroute* onde todos roteadores presentes no fluxo de pacotes responderam aos *ICMP echo request* enviados pelo *probe*. Este pode ser considerado um resultado ideal, embora atípico, e possibilita a identificação das bordas de todos ASes presentes no fluxo de pacotes.

Já a Figura 4.11 apresenta o mesmo *traceroute*, porém com os roteadores identificados na figura como R4, R5 e R6 não respondendo os pacotes *ICMP echo request*. A ausência das respostas destes roteadores é crítica e impossibilita que se identifique as bordas do ASN2. Medidas como esta, se não resolvidas pelo *bdrmapIT*, devem ser descartadas.

Por outro lado, através de inferências, é possível ainda aproveitar medições com a ausência da resposta ao *ICMP echo request* de um grande número de rote-

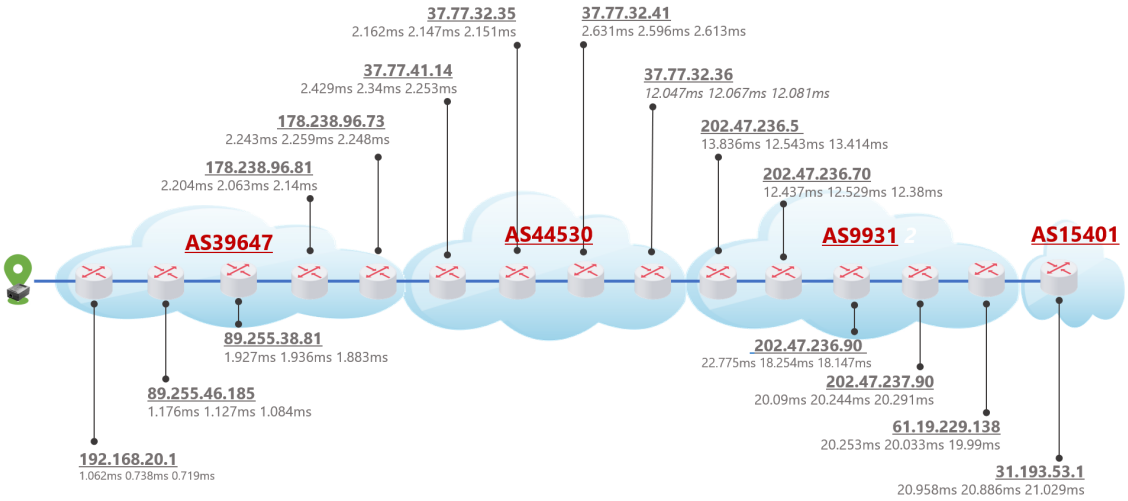


Figura 4.10 – Exemplo de Traceroute Fim a Fim

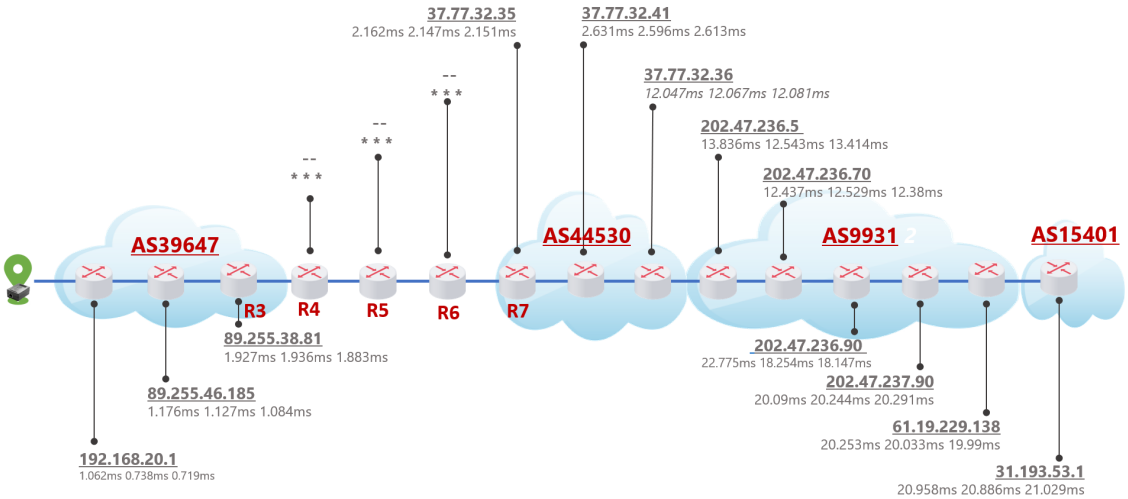


Figura 4.11 – Exemplo de Traceroute com roteadores sem resposta

adores no caminho dos pacotes. Na Figura 4.12, por exemplo, dos 15 roteadores presentes no fluxo de dados entre o *probe* e o destino, um total de 6 não responderam a estes pacotes. Ainda assim é possível identificar adequadamente as bordas do ASN2, o que torna medidas como esta válidas para o uso da metodologia.

É importante mencionar que este processo também é realizado na etapa da escolha dos *probes* e nos testes executados antes de iniciar um conjunto de medições. Buscamos com isso evitar inicializar *traceroutes* de longo duração cujo resultado possa inviabilizar as análises.

Na segunda etapa do *pipeline* para tratamento das medições coletadas, os resultados são submetidos ao *bdrmapIT*, que fornece informações sobre as bordas dos sistemas autônomos com um alto grau de acuracidade.

Na terceira etapa do *pipeline* realizamos uma validação dos dados, com o

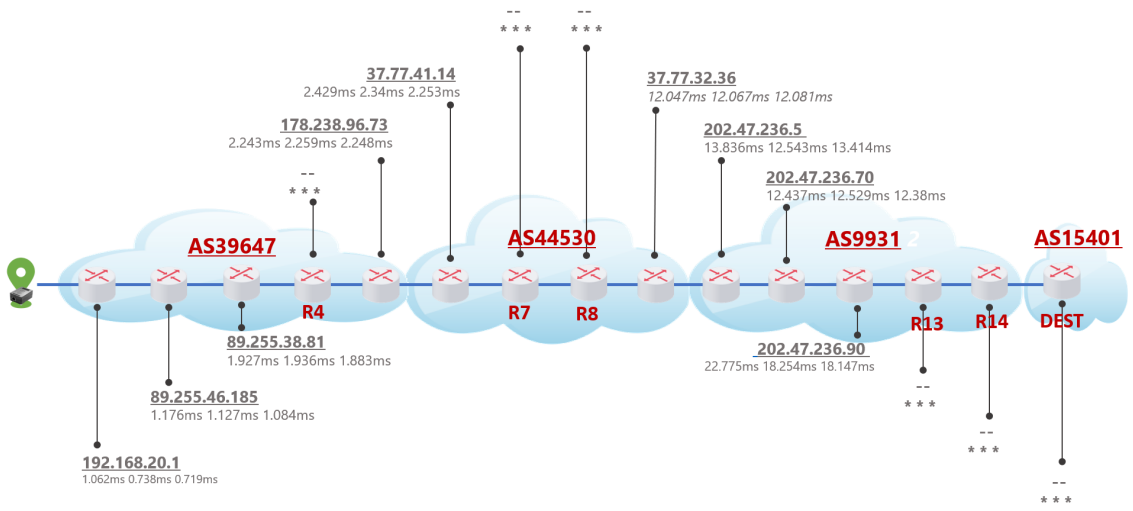


Figura 4.12 – Exemplo 2 de Traceroute com roteadores sem resposta

objetivo de avaliar se as premissas da campanha de medição foram atendidas. Por exemplo, se o ASN2 de interesse foi realmente aquele percorrido pelo fluxo de pacotes. Na quarta etapa, algumas informações adicionais são coletadas, como, por exemplo, os relacionamentos dos ASes presentes em todo o fluxo de pacotes, a nome dos sistemas autônomos percorridos pelos pacotes (nesta etapa temos apenas o *AS Number*), entre outras informações que podem ser úteis nas análises ou em futuras medições.

Na quinta e última etapa os dados são convertidos do formato *json* (*JavaScript Object Notation*) para *csv* (*Comma Separated Values*), cujo formato é mais apropriado para o uso em ferramentas estatísticas.

Uma vez concluído o tratamento preliminar, os resultados devem ser preparados para a análise. Utilizamos o ambiente e a linguagem R (FOUNDATION, 2021). Para calcular as métricas de latência, gerar as séries temporais e os gráficos comparativos no ambiente R, os resultados pertencentes a uma mesma campanha de medições devem ser agrupados, conforme representado na Figura 4.13.

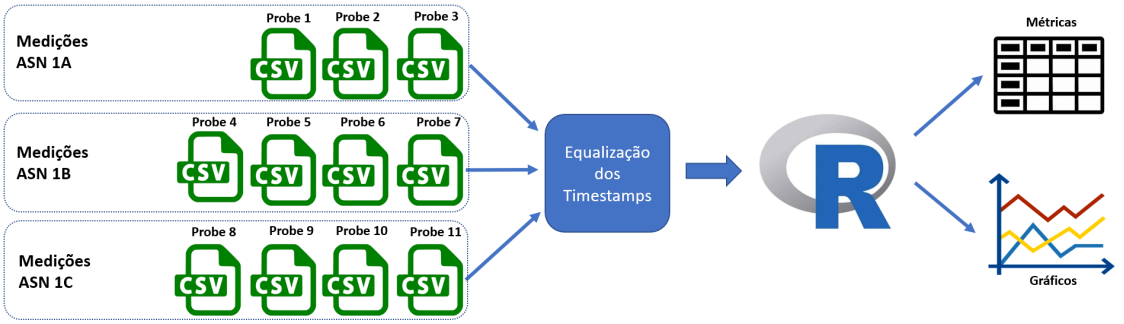


Figura 4.13 – Análise dos Resultados das Campanhas de Medição

Duas ações são necessárias para unificar os resultados dos *traceroutes* pertencentes a uma mesma campanha de medição em um único *dataframe* R:

- A Figura 4.14 contém um exemplo de como os resultados são coletados do RIPE ATLAS. Para cada *hop* no fluxo do *traceroute*, são realizadas três medições de ICMP. Usamos a *mediana* dos três valores de RTT obtidos para representar cada medição;
- Conforme apresentado na Figura 4.13, é necessário realizar uma equalização dos *timestamps* para comparar medições que foram realizadas em momentos diferentes. Mesmo que nosso algoritmo configure a infraestrutura do RIPE ATLAS para iniciar todos *traceroutes* ao mesmo tempo, as medidas de cada *probe* não são sincronizadas e ocorrem em momentos diferentes e a cada 3 minutos. Essas medições são equalizadas, sabendo-se que, a cada três minutos, uma medição é efetuada. A partir disto, geramos um valor médio para o *timestamp* em que a medida ocorreu em todos os *traceroutes* de uma mesma campanha de medições;


```
{"fw":5020,"mver":"2.2.1","lts":10,"endtime":1631565618,"dst_name":"80.252.103.22
2","dst_addr":"80.252.103.222","src_addr":"172.18.50.178","proto":"ICMP","af":4,"
size":48,"paris_id":1,"result":[{"hop":1,"result":
[{"from":"172.18.50.1","ttl":64,"size":76,"rtt":0.612},
{"from":"172.18.50.1","ttl":64,"size":76,"rtt":0.537},
{"from":"172.18.50.1","ttl":64,"size":76,"rtt":0.539}]},{"hop":2,"result":
[{"from":"217.19.16.21","ttl":254,"size":52,"rtt":1.298,"ittl":0},
{"from":"217.19.16.21","ttl":254,"size":52,"rtt":1.219,"ittl":0},
{"from":"217.19.16.21","ttl":254,"size":52,"rtt":1.214,"ittl":0}]},
{"hop":3,"result":[{"from":"217.19.16.6","ttl":253,"size":28,"rtt":1.517},
{"from":"217.19.16.6","ttl":253,"size":28,"rtt":1.458},
{"from":"217.19.16.6","ttl":253,"size":28,"rtt":1.503}]},{"hop":4,"result":
[{"from":"154.14.67.33","ttl":251,"size":28,"rtt":2.251},
{"from":"154.14.67.33","ttl":251,"size":28,"rtt":2.354},
{"from":"154.14.67.33","ttl":251,"size":28,"rtt":1.513}]},{"hop":5,"result":
[{"from":"4.68.38.121","ttl":250,"size":28,"rtt":2.624},
{"from":"4.68.38.121","ttl":250,"size":28,"rtt":1.573},
{"from":"4.68.38.121","ttl":250,"size":28,"rtt":1.807}]},{"hop":6,"result":
[{"from":"4.69.142.218","ttl":249,"size":28,"rtt":7.052},
{"from":"4.69.142.218","ttl":249,"size":28,"rtt":7.238},
{"from":"4.69.142.218","ttl":249,"size":28,"rtt":6.797}]},{"hop":7,"result":
[{"from":"62.67.25.2","ttl":248,"size":28,"rtt":10.854},
{"from":"62.67.25.2","ttl":248,"size":28,"rtt":10.712},
{"from":"62.67.25.2","ttl":248,"size":28,"rtt":10.685}]},{"hop":8,"result":
[{"from":"212.53.201.211","ttl":56,"size":28,"rtt":13.188},
{"from":"212.53.201.211","ttl":56,"size":28,"rtt":15.205},
{"from":"212.53.201.211","ttl":56,"size":28,"rtt":14.433}]},{"hop":9,"result":
[{"from":"80.252.103.222","ttl":55,"size":48,"rtt":10.861},
{"from":"80.252.103.222","ttl":55,"size":48,"rtt":10.8},
{"from":"80.252.103.222","ttl":55,"size":48,"rtt":10.87}]}],"msm_id":32277151,"pr
b_id":28508,"timestamp":1631565617,"msm_name":"Traceroute","from":"84.245.9.226",
"type":"traceroute","group_id":32277151,"stored_timestamp":1631565699}
```


Figura 4.14 – Exemplo de resultado de medição coletado do RIPE ATLAS

Uma vez unificados em um mesmo *dataframe* os resultados dos *traceroutes*, são gerados um conjunto de artefatos para análise dos resultados, como tabelas de resultados estatísticos e gráficos de séries temporais. Embora esses artefatos possam mudar de caso para caso, a lista a seguir apresenta aqueles que normalmente estão presentes em todas as análises:

- *Gráfico de Dispersão* comparativo das séries temporais das métricas RTT Probe-Destino e ΔASN2 para todos os *traceroutes* participantes de uma mesma campanha de medições;
- *Gráfico de Dispersão* comparativo entre as séries temporais das métricas RTT Probe-Destino, ΔASN2 e $\Delta ASN3_{ingress}$-Dest para fluxos onde é necessário investigar possíveis congestionamentos;
- Tabelas com cálculo dos valores médios, desvio padrão, mediana e range de valores para as métricas mencionadas acima para cada um dos *traceroutes*.

Em geral, as tabelas e gráficos gerados pelo sistema que implementa a metodologia podem ser usados por um humano com o devido conhecimento na comparação entre sistemas autônomos tendo em vista o comportamento observado para a latência em cada uma das métricas medidas. O interesse do operador (o seu objetivo) é que determinará a relevância de cada uma das métricas. Por exemplo, se o objetivo é encontrar um provedor de trânsito com menor latência e *jitter* de pacotes, deve-se observar os valores médio, o desvio padrão e o range de valores observados para a métrica ΔASN2. Se o objetivo é observar este provedor de trânsito com relação a um destino em específico na Internet, estes mesmos dados estatísticos devem ser observados em relação ao RTT Probe-Destino. O Capítulo 5 demonstra como estes valores são usados na análise de cada um dos estudos de caso.

Há porém um caso específico onde as métricas devem ser usadas de forma conjunta e em muitas situações algumas investigações adicionais devem ser realizadas: os congestionamentos internos no ASN2. A seção a seguir apresenta como aplicamos a metodologia para isolar casos de congestionamento e de que forma as diferentes informações coletadas durante as medições são usadas para inferir estes eventos.

A detecção de possíveis congestionamentos internos em um ASN2 envolve a análise de uma série de métricas e series temporais. Um primeiro passo é observar a série temporal da métrica ΔASN2. Aumentos do valor desta métrica durante

as medições podem indicar um congestionamento neste sistema autônomo. Porém, conforme já discutido em outras partes deste trabalho, um AS pode aumentar seu tempo de roteamento interno por ter encontrado um caminho de menor custo para o roteamento inter-AS em direção ao destino.

Para investigar esta hipótese, devemos verificar se a série temporal de RTT Probe-Destino também apresentou uma elevação no valor observado, de forma síncrona ao aumento do ΔASN2. Se este for o caso, um congestionamento interno permanece como uma hipótese possível.

No passo seguinte, deve-se observar o aumento da perda de pacotes durante os aumentos observados nas métricas ΔASN2 e RTT Probe-Destino. Caso isto seja verdadeiro, um possível congestionamento interno em ASN2 permanece uma hipótese válida. Importante mencionar que a observação da perda de pacotes como parte da nossa investigação sobre possíveis congestionamentos no ASN2 derivam de observações semelhantes relatadas nos trabalhos (LUCKIE et al., 2014) e (DHAMDHERE et al., 2018). A figura 4.15, extraída de (DHAMDHERE et al., 2018), demonstra a correlação observada pelos autores entre a ocorrência de congestionamentos e o aumento da perda de pacotes detectados no uso do TSLP.

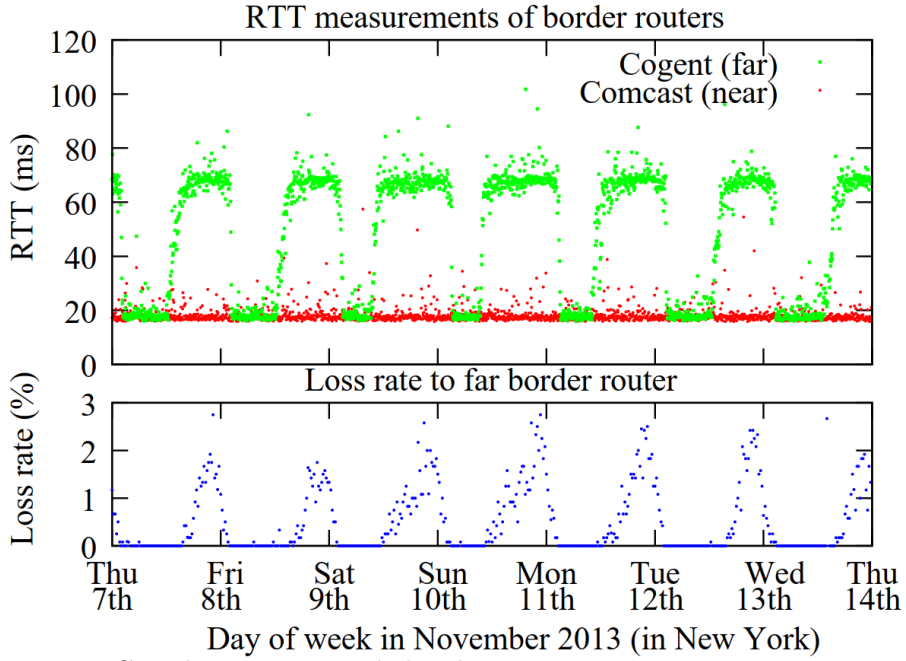


Figura 4.15 – Correlação entre períodos de congestionamentos e o aumento da perda de pacotes observada em (DHAMDHERE et al., 2018)

Mesmo que um possível congestionamento permaneça uma hipótese válida após as verificações anteriores, ainda é possível que o aumento no tempo de roteamento interno ao ASN2, ou mesmo o aumento da perda de pacotes, tenha ocorrido

por uma mudança no roteamento inter-AS a partir do ASN2. Por exemplo, se por razões externas ao ASN2 o destino dos pacotes deixou de ser alcançado pelo roteamento inter-AS realizado até então, o ASN2 pode utilizar outra rota até o destino mesmo que para isso tenha um custo de roteamento interno maior.

A seguir, para avaliar se houve alguma alteração no roteamento inter-domínio do ASN2, deve-se avaliar os resultados dos *traceroutes* no momento anterior, durante e após o evento observado. Nesta investigação deve-se verificar se os roteadores *egress* do ASN2 e *ingress* do ASN3 foram alterados. Se este for o caso, não é possível afirmar que houve qualquer degradação no funcionamento do ASN2.

Porém, se os roteadores *egress* do ASN2 e *ingress* do ASN3 permaneceram os mesmos durante o aumento do ΔASN2, RTT Probe-Destino e o aumento da perda de pacotes, temos um conjunto de indícios que sugerem um possível congestionamento no ASN2.

Como congestionamentos internos podem indicar que um determinado sistema autônomo está operando no limite de sua capacidade, a observação destes eventos pode ser um fator de escolha para um parceiro de interconexão na Internet. Consideramos esta a métrica mais importante dentre aquelas inferidas por esta metodologia.

4.3 Uso dos Resultados da Metodologia para Comparar ASes

Conforme discutido anteriormente, a metodologia que propomos neste trabalho pode ser utilizada com dois propósitos, que podem ser aplicados de forma complementar ou isoladas: 1) Detectar possíveis congestionamentos em sistemas autônomos; 2) Inferir métricas que possibilitem a comparação da latência do plano de dados entre ASes.

Para o primeiro uso, não é necessário realizar campanhas de medições comparativas. O congestionamento interno em um AS pode ser um evento suficientemente relevante para desencorajar outros ASes a estabelecerem um acordo de interconexão com o mesmo. Porém, para o segundo caso, onde congestionamentos não são detectados ou não são um aspecto importante para quem realiza a avaliação, a maior contribuição que a metodologia proposta pode oferecer é inferir métricas que possibilitem a comparação da latência observada no plano de dados de ASes.

Embora a comparação não seja uma condição necessária, métricas como RTT

Probe-Destino, ΔASN2$_{\text{egress}}$-Dest e ΔASN3$_{\text{ingress}}$-Dest sofrem uma grande influência da dinâmica de roteamento da Internet. Por exemplo, se durante as medições ocorrer um congestionamento no AS do destino do *traceroute*, se as medições não estiverem ocorrendo de forma simultânea, a comparação entre os ASes poderá não ser justa. Assim, para aplicações da metodologia em cenários como estes, é recomendado que as medições sejam realizadas de forma simultânea em ambos os ASes.

Para a comparação entre ASes, a metodologia oferece um conjunto de métricas que possibilita a segmentação da latência observada em diferentes partes do caminho percorrido pelo *traceroute*. A métrica ΔASN2, por exemplo, possibilita a comparação do tempo de roteamento interno de um AS tendo em vista um determinado destino na Internet. Pode-se usar a métrica #Hops$_{\text{inter-ASN2}}$ para complementar esta avaliação.

Com ΔASN3$_{\text{ingress}}$-Dest é possível comparar as escolhas de encaminhamento de pacotes realizadas pelos ASN2s. ASes que possuírem melhores acordos para o encaminhamento de pacotes em direção ao destino avaliado ou que realizem um roteamento interno *cold potato*, podem obter resultados melhores para esta métrica. A métrica ΔASN2$_{\text{egress}}$-Dest é semelhante a ΔASN3$_{\text{ingress}}$-Dest, porém adiciona à avaliação a latência do enlace entre o ASN2 e ASN3. Já RTT Probe-Destino é uma métrica essencial para realizar qualquer comparação entre ASes.

Extrair informações relevantes dos gráficos de dispersão das séries temporais requer o devido conhecimento do operador que realiza a comparação entre ASes, podendo ser esta uma limitação no uso desta metologia. Com o objetivo de gerar resultados comparativos de ASes, que requeiram um menor grau de especialização na comparação dos resultados, a metodologia proposta também gera um conjunto de dados estatísticos sobre as métricas obtidas pelas campanhas de medição.

São gerados como parte da metodologia resultados estatísticos como *média*, *mediana*, *desvio padrão* e *range de valores*. O uso destes dados podem auxiliar na inferência sobre possíveis congestionamentos em ASes ou na comparação dos valores de latência do plano de dados entre sistemas autônomos. A figura 4.16 apresenta algumas das análises que podem ser realizadas sobre os resultados estatísticos gerados pela metodologia.

A principal característica de um possível congestionamento persistente durante uma campanha de medições é o aumento da latência em uma ou mais métricas observadas pela metodologia. Se o congestionamento ocorrer dentro do ASN2, a

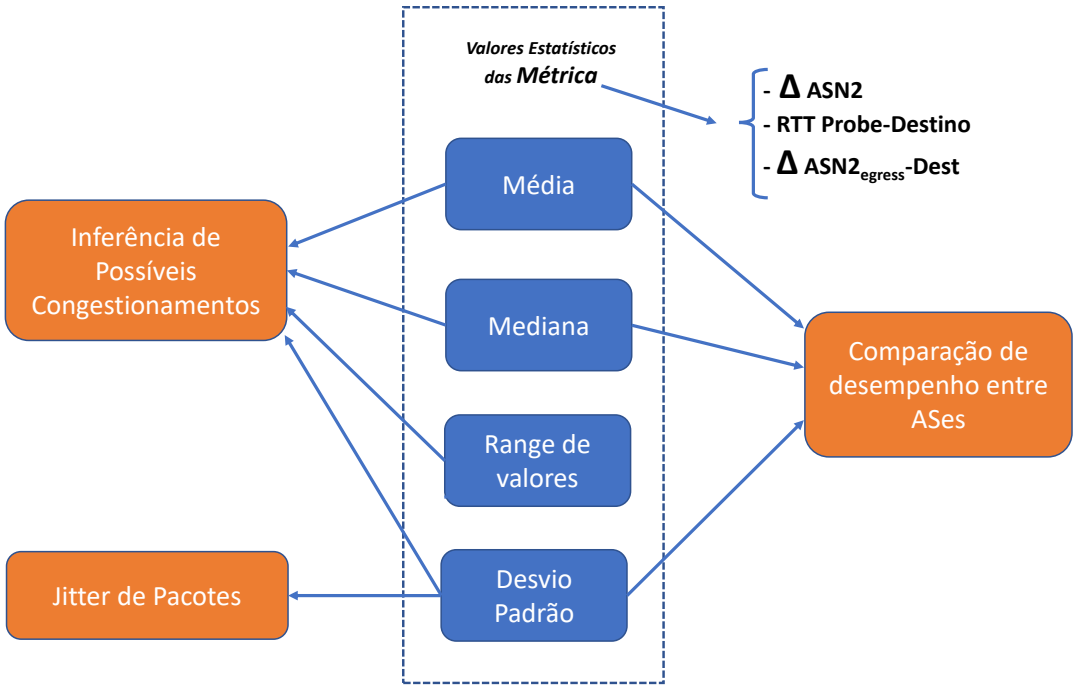


Figura 4.16 – Dados estatísticos sobre as métricas

métrica ΔASN2 apresentará um aumento da diferença das latências medidas pelo ICMP nos roteadores *ingress* e *egress* do ASN2. Já se o congestionamento ocorrer entre o ASN2 e o destino, a métrica $\Delta ASN2_{egress}$-Dest apresentará um aumento na diferença da latência entre o roteador *egress* do ASN2 e o destino do *traceroute*. Para qualquer congestionamento persistente no caminho do *traceroute* entre o *probe* e o destino, a métrica RTT Probe-Destino apresentará um aumento na latência. Porém, o uso da métrica RTT Probe-Destino para detectar congestionamentos deve ser acompanhado de uma investigação complementar, já que o congestionamento pode ocorrer no ASN1 ou no enlace entre o ASN1 e ASN2, o que fugiria dos objetivos desta metodologia de avaliar o desempenho e as escolhas de roteamento do ASN2. No Capítulo 5 estão apresentados casos onde as análises dos resultados partem da observação da métrica RTT Probe-Destino.

Conforme observado em (DHAMDHERE et al., 2018), congestionamentos persistentes geram um aumento na latência medida no *hop* subsequente ao segmento de rede que enfrenta esta degradação. Assim, ao comparar as latências dos diferentes *hops* percorridos pelo *traceroute* é possível inferir o segmento de rede que pode estar enfrentando um congestionamento. Como apresentado no parágrafo ante-

rior, para cada um dos segmentos de rede percorridos pelo *traceroute* a metodologia possui uma ou mais métricas que buscam refletir estas alterações de latência. Com isso, dependendo da intensidade e duração do congestionamento, é esperado que os valores de *desvio padrão* e *range de valores* calculados para a métrica afetada pelo congestionamento apresentem resultados compatíveis com o impacto deste evento. No Capítulo 5 estão apresentados estudos de caso que demonstram o impacto de possíveis congestionamentos nos valores de *desvio padrão* e *range de valores* calculados para as métricas afetadas.

A comparação entre os valores da *média* e *mediana* também pode ser utilizado para contribuir com a inferência de possíveis congestionamentos. De forma isolada, estes dois dados estatísticos não contribuem com este objetivo já que eles não revelam variações nos valores medidos. Porém, ao compara-los é possível identificar situações que podem estar relacionadas à congestionamentos. Considere-se, para objetivos didáticos, uma medição hipotética onde uma determinada métrica apresentou um valor de 50ms durante 70% do tempo da campanha de medição e 100ms no restante do tempo. Os valores calculados da *média* e *mediana* para estes resultados hipotéticos seriam 65ms e 50ms, respectivamente. O valor da *mediana* indica que 50% das medições realizadas foram iguais ou menores do que 50ms. Porém, ao comparar a *média* com a *mediana* podemos concluir que ocorreram medições com valores superiores a 50ms, que geraram um valor médio de medições 30% acima da *mediana* calculada. Esta diferença de valores pode sugerir que durante as medições ocorreram variações importantes na métrica observada que podem estar relacionados a possíveis congestionamentos.

O uso combinado dos valores de *média*, *mediana*, *desvio padrão* e *range de valores* de uma determinada métrica pode auxiliar na detecção de possíveis congestionamentos, sem que para isso seja necessário analisar os gráficos de dispersão das séries temporais. Embora esta análise não seja trivial, ela pode em trabalhos futuros ser formalizada através de algoritmos que representem as análises heurísticas apresentadas no Capítulo 5, simplificando o uso da metodologia proposta.

Os valores calculados de *média*, *mediana*, *desvio padrão* e *range de valores* de uma determinada métrica podem também ser utilizados na comparação de desempenho, em termos de latência, entre sistemas autônomos, conforme sugerido na Figura 4.16. Estes valores possibilitam a um operador de rede e/ou coordenador de *peering*, por exemplo, compara ASes em busca daquele que possui a menor latência

e *jitter* de pacotes em relação a um destino na Internet, sem que seja necessário possuir um acordo de interconexão estabelecido com os ASes avaliados.

5 RESULTADOS

Implementamos uma prova de conceito da metodologia proposta e a utilizamos na avaliação e comparação de diversos sistemas autônomos na Internet. Durante as campanhas de medições, diversos ASes foram avaliados com diferentes objetivos. Dentre as campanhas realizadas, trazemos neste capítulo cinco estudos de caso que apresentam diferentes usos da metodologia:

- *Estudo de Caso 1*: No primeiro estudo de caso realizamos uma comparação na performance de 2 ASes tendo um destino em comum na Internet;
- *Estudo de Caso 2*: O segundo estudo de caso teve por objetivo reproduzir um cenário típico do interesse de alguns ISPs que conversamos durante a construção deste trabalho: reduzir a latência dos serviços de Internet do ISP em relação a um servidor de jogos na Internet;
- *Estudo de Caso 3*: Já o terceiro estudo de caso buscou avaliar o comportamento de um sistema autônomo tendo diferentes destinos na Internet. Conforme discutido no Capítulo 4, os destinos usados nos *traceroutes* são uma variável com alto impacto nos resultados inferidos pela nossa metodologia. Neste caso, buscou-se avaliar o comportamento de um AS de uma forma mais ampla, ou seja, comparando o comportamento do mesmo em relação à diferentes destinos;
- *Estudo de Caso 4*: No estudo de caso 4 apresentamos uma comparação entre dois ASes, um Tier-1 e outro Tier-2, usando diversos *probes* para a avaliação. A abundância de *probes* para as medições é uma limitação das avaliações que realizamos da metodologia, conforme discutido no Capítulo 6. Este cenário, porém, aproxima-se daquele que consideramos ideal em termos de quantidade de *probes* e, devido a isso, ele está apresentado neste capítulo;
- *Estudo de Caso 5*: O quinto estudo de caso traz um cenário onde detectamos indícios de um possível congestionamento em 2 dos 3 fluxos de *traceroutes* utilizados na campanha de medição. Dentre todas as campanhas de medição realizadas, este foi o único caso em que observamos tal comportamento.

Nas seções a seguir apresentamos o detalhamento de cada um destes estudos de caso.

5.1 Estudo de Caso 1: Medição com métricas ΔASN2 e RTT Probe-Destino na comparação de ASes

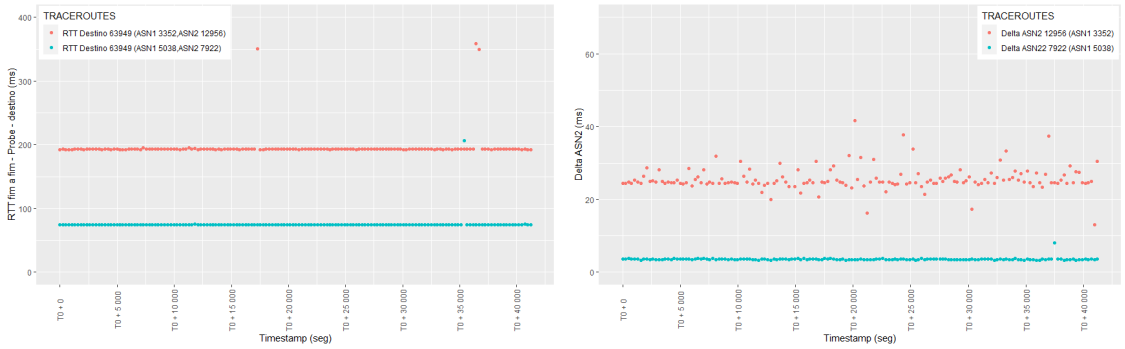
Neste primeiro estudo de caso, realizamos uma avaliação comparativa entre dois ASN2s, ASN 7922 e 12956, tendo os *traceroutes* que percorreram estes ASes o mesmo destino na Internet. O objetivo desta campanha de medições foi avaliar qual destes ASes apresentava a maior estabilidade (ausência de congestionamentos) e o melhor desempenho em termos de *jitter* de pacotes e latência.

A Figura 5.1a apresenta as séries temporais da métrica RTT Probe-Destino para os *traceroute* que percorreram os ASes 7922 e 12956 durante a campanha de medição. Os resultados observados em RTT Probe-Destino não apresentaram variações durante o período de medição. Conforme discutido no Capítulo 4, como nossas medições, mesmo que de longa duração, ainda possuem um caráter temporal, não podemos inferir, a priori, que o comportamento observado é normal ou um congestionamento que persistiu durante toda a medição. Em nossa metodologia buscamos em outras métricas observadas dados que possibilitem um melhor entendimento sobre o que foi observado.

Conforme o estudo realizado em (LUCKIE et al., 2014) e discutido na Seção 4.2.4, congestionamentos persistentes, normalmente, vêm acompanhados de um aumento na taxa de perda de pacotes. Em (LUCKIE et al., 2014), os autores relatam que a perda de pacotes durante congestionamentos é observada nas medições de latência do roteador remoto (*far end*) do enlace inter-domínio e chegam a até 3% de perdas. Usamos em nossa metodologia as métricas *# pacotes perdidos por medição* e *% de perda de pacotes* para realizar uma avaliação semelhante.

O resultado da métrica *# pacotes perdidos por medição* para os dois *traceroutes* está apresentado na Figura 5.3. Nas duas medições ocorreram poucas perdas de pacote. O *traceroute* que percorreu o AS 7922 durante a medição não apresentou nenhuma perda de pacotes. Já o *traceroute* que percorreu o AS 12956 teve apenas 2 pacotes *ICMP Echo Request* não respondidos. Conforme discutido no parágrafo anterior, situações que sugerem congestionamentos apresentam uma perda de pacotes maior.

Na figura 5.1b estão apresentadas as séries temporais da métrica ΔASN2 para os dois *traceroutes*, que correspondem ao tempo de encaminhamento interno dos pacotes no ASN2, neste caso, os ASes 7922 e 12956. Na Figura 5.1b é possível



(a) RTT fim a fim (b) ΔASN2

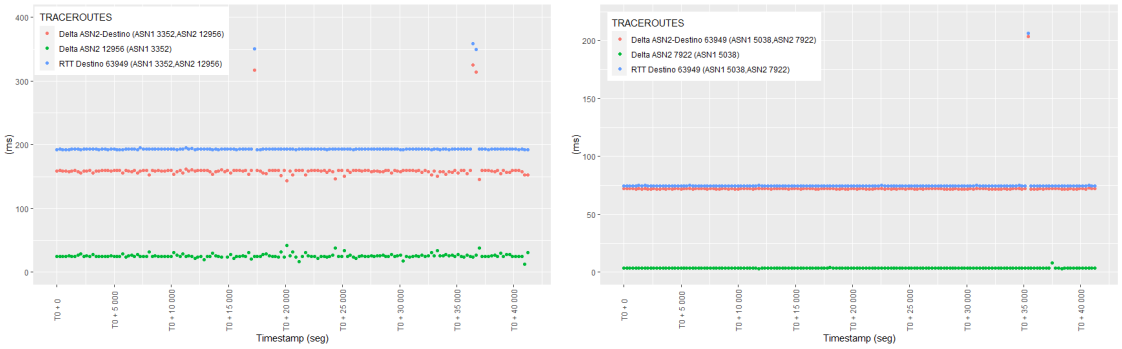
Figura 5.1 – Comparação RTT fim a fim e ΔASN2

observar comportamentos distintos nas duas medições. Enquanto o encaminhamento de pacotes do AS 7922 apresenta pouca variação nas medições do ΔASN2, os valores medidos para o AS 12956 apresentam uma variação maior. É interessante observar que a dispersão observada na série temporal do ΔASN2 do AS 12956 não repercute, de forma evidente, no RTT Probe-Destino. Embora graficamente esta dispersão pareça significativa, o tempo médio de encaminhamento dos pacotes deste AS, de aproximadamente 25ms, representa pouco menos de 13% do RTT fim a fim medido.

Nas Figuras 5.2a e 5.2b estão apresentadas as séries temporais das métricas RTT Probe-Destino, ΔASN2 e $\Delta ASN2_{egress}$-Dest dos ASes 12956 e 7922, respectivamente. Comparações como esta possuem pouca utilidade em resultados onde a métrica RTT Probe-Destino permaneceu constante durante todo a medição, mas podem auxiliar em situações onde se observam aumentos persistentes nos valores medidos para esta métrica.

Para a definição dos *outliers*, utilizamos critérios semelhantes aos aplicados em (DHAMDHERE et al., 2018). Uma mudança na série temporal é considerada relevante se o novo valor medido persistir por cinco medições consecutivas (aproximadamente 15 minutos).

Note-se que nas séries temporais apresentadas na figura 5.2a algumas medições apresentam variações nos valores observados, mas ao não persistirem por cinco medições consecutivas foram consideradas *outliers*. Note-se também que os *outliers* presentes na métrica RTT Probe-Destino não possuem eventos correspondente na medição do ΔASN2. Porém, outra métrica apresentada neste gráfico, $\Delta ASN2_{egress}$-Dest, apresentou *outliers* sincronizados com aqueles presentes em RTT Probe-Destino. Com base nestes resultados, pode-se concluir que os *outliers* ocorreram entre o enlace inter-domínio ASN2/ASN3 e o destino.



(a) Comparação de métricas do ASN2 12956 (b) Comparação de métricas do ASN2 7922

Figura 5.2 – Comparação das métricas RTT Probe-Destino, ΔASN2 e $\Delta ASN2_{egress}$-Dest dos ASN2 7922 e 12956

As séries temporais das mesmas métricas do AS 7922, apresentadas na Figura 5.2a, mostram um comportamento semelhante. Os *outliers* observados nas medições no $\Delta ASN2_{egress}$-Dest foram sempre acompanhados de um aumento semelhante na métrica RTT Probe-Destino.

A tabela 5.1 apresenta os resultados calculados de *média*, *mediana*, *desvio padrão* e *range de valores*. Conforme discutido na Seção 4.3, os valores semelhantes da *média* e *mediana*, além da baixa dispersão dos resultados, indicada pelos valores do *desvio padrão* e *range de valores*, reforçam as observações realizadas sobre as séries temporais, ou seja, não existem indícios de que ocorreram congestionamentos durante a campanha de medições.

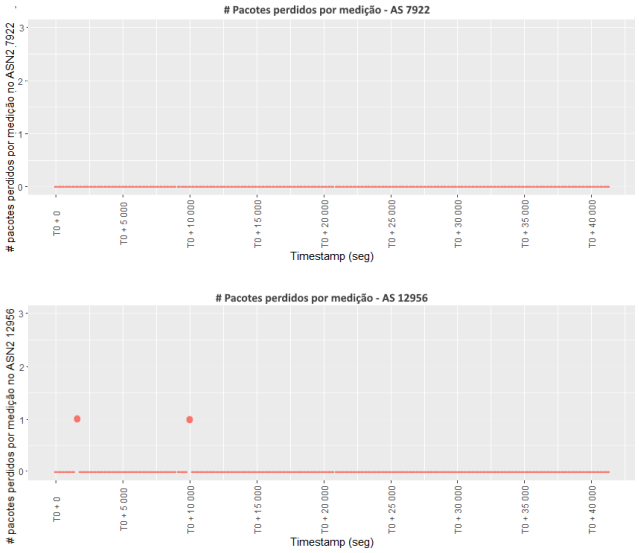


Figura 5.3 – Perda de pacotes no RTT fim a fim - ASes 7922 e 12956

Tendo em vista os objetivos deste estudo de caso, ou seja, comparar o comportamento dos ASes 7922 e 12956 com relação ao mesmo destino na Internet, devemos recorrer aos resultados da Tabela 5.1 para definir aquela que apresentou

	Média (ms)	**Desvio Padrão**	**Mediana (ms)**	**Variação (ms)**
ΔASN2 12956	25,37	4,21	24,73	8,72 a 41,72
ΔASN2 7922	3,55	0,37	3,52	3,20 a 8,09
RTT Probe-Destino 12956	195,55	21,91	192,86	192 a 358
RTT Probe-Destino 7922	75,50	10,46	74,66	74 a 66
$\Delta ASN2_{egress}$-Dest 12956	161	22,19	159	143 a 325
$\Delta ASN2_{egress}$-Dest 7922	72,81	10,46	71,97	71 a 203

Tabela 5.1 – Métricas comparativas entre os ASes 7922 e 12956

melhor resultado durante a campanha. Como os resultados analisados não sugerem que congestionamentos ocorreram durante as medições, ou seja, ambos ASes mostraram-se igualmente estáveis, deve-se recorrer a outros critérios para se determinar, de acordo com a metodologia proposta, qual destes ASes apresenta o menor *jitter* de pacotes e latência fim a fim.

Considerando-se os resultados da métrica RTT Probe-Destino (RTT fim a fim) na Tabela 5.1, o AS 7922 apresentou uma latência média e *jitter* de pacotes (emphdesvio padrão) menor do que o AS 12956. Assim, de acordo com os objetivos deste estudo de caso e com base na aplicação da metodologia proposta, o AS 7922 foi aquele que apresentou os melhores resultados.

Análise do uso da metodologia no Estudo de Caso 1

Para a avaliação dos ASes 12956 e 7922 com o uso da metodologia proposta, foram selecionados dois *probes*, da lista de caminhos conhecidos, localizados em ASes que possuem relação *c2p* com estes sistemas autônomos. A partir destes *probes* foram gerados *traceroutes* que percorreram durante todo o período da campanha de medição os ASes sob avaliação.

A ausência de variações representativas de latência nas séries temporais das métricas RTT Probe-Destino, ΔASN2 e $\Delta ASN2_{egress}$-Dest, bem como, a inexistência de perdas de pacotes relevantes durante as medições (menos de 0,05% dos pacotes ICMP enviados foram perdidos), constituem dois indícios importantes da inexistência de congestionamentos nos fluxos de medições. A proximidade dos valores da *média* e *mediana*, assim como, a pequena dispersão nos valores de *desvio padrão* e *range de valores* de todas as métricas avaliadas, corroboram com estes indícios, conforme discutido na Seção 4.3. Considerando-se que é improvável que um congestionamento tenha ocorrido durante as medições, pode-se dizer que os ASes avaliados apresentaram um comportamento estável durante toda a campanha.

Análise do uso da metodologia no Estudo de Caso 1 (continuação)

No passo seguinte da metodologia, foram comparados os resultados de latência das diferentes métricas apresentadas na Tabela 5.1, com o objetivo de determinar o AS com melhores resultados de desempenho. Com relação ao destino na Internet avaliado e considerando as técnicas de medições utilizadas, o AS 7922 apresentou os melhores resultados de latência e *jitter* de pacotes na comparação com o AS 12956.

É importante mencionar que, dependendo da política de priorização dos pacotes ICMPs dos ASes percorridos pelo *traceroute*, os resultados da Tabela 5.1 podem não representar precisamente o desempenho, em termos de latência, dos ASes avaliados. No Capítulo 6 estão discutidas alternativas ao uso de ICMP para as medições de latência, que podem contornar esta possível limitação sem impactos no restante de metodologia.

Independente da possível limitação apresentada no parágrafo anterior, os resultados obtidos pela metodologia no estudo de caso 1 representam um ponto de partida, inexistente até então, na avaliação e comparação do desempenho dos ASes 12956 e 7922, sem que tenha sido necessário possuir um acordo de interconexão pré-estabelecido com os mesmos.

5.2 Estudo de Caso 2: Reduzir a latência dos usuários de um ISP em relação a um servidor de jogos online

O segundo estudo de caso que realizamos foi motivado a partir de conversas com ISPs sobre suas demandas mais comuns na busca de novos parceiros de interconexão. Uma demanda frequente é buscar acordos que possam reduzir a latência dos usuários de jogos online em relação aos servidores dos jogos na Internet. Essa demanda também está refletida nas entrevistas realizadas em (MARCOS et al., 2020), onde 81.1% dos operadores de rede e coordenadores de *peering* entrevistados indicaram que a latência é uma das razões para estabelecer novos acordos de interconexão. De acordo com (CLAYPOOL; CLAYPOOL, 2010), jogos de tiro em primeira pessoa são altamente impactados pela atraso de rede, trazendo desvantagens nítidas para os usuários com maior latência. Se observamos os 10 jogos online mais populares em 2021 (SPORTS, 2021), três deles podem ser classificados nesta categoria (*PUBG Battleground*, *Apex Legends* e *Counter Strike: Global Offensive*).

Neste estudo de casos, avaliamos 3 possíveis provedores de *trânsito* presentes

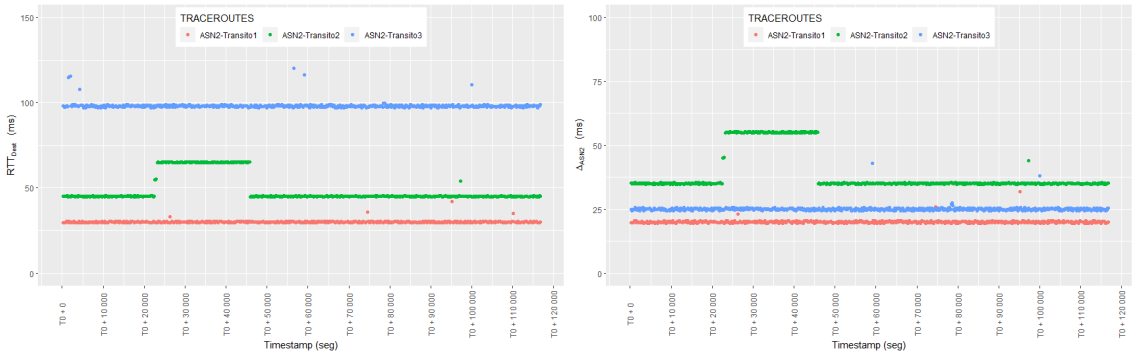
em um IXP, que chamaremos aqui de IXP1, tendo em consideração o endereço IP de um servidor de jogos, que realiza troca de tráfego em outro IXP, que chamaremos aqui de IXP2. Esta investigação busca reproduzir uma prática comum na contratação de serviços de *trânsito* por ISPs que não estão presentes em IXPs onde os servidores de jogos trocam tráfego, em relações *p2p*, com outros ASes. Os resultados obtidos com estas medições podem ser úteis para qualquer AS presente no IXP1 e que tenha interesse em identificar um provedor de *trânsito* com uma latência menor em relação ao servidor de jogos.

As escolhas de *probes* nesta campanha de medição utilizou como critério o uso de ASN1s presentes no IXP1 que possuam acordos de *trânsito* com os provedores investigados. Embora não seja possível afirmar que a troca de tráfego entre estes ASes ocorra na infraestrutura do IXP1, não existem razões técnicas ou legais que impeçam este procedimento. Os provedores de *trânsito* investigados são nomeados $\text{AS}_{\text{Transit}}1$, $\text{AS}_{\text{Transit}}2$ e $\text{AS}_{\text{Transit}}3$ nos resultados apresentados nesta seção.

A Figura 5.4a apresenta a série temporal da métrica mais relevante para esta medição, a RTT Probe-Destino. A partir dos resultados das séries temporais desta métrica, destacamos a seguir alguns aspectos relevantes observados:

- Há uma diferença significativa nos valores de latência observados entre as três medições. O $\text{AS}_{\text{Transit}}1$ apresentou a menor latência enquanto o provedor de *trânsito* $\text{AS}_{\text{Transit}}3$ apresentou a maior;
- Os *traceroutes* que percorreram os provedor de *trânsito* $\text{AS}_{\text{Transit}}1$ e $\text{AS}_{\text{Transit}}3$ mostraram-se estáveis durante toda a medição, com a ocorrência esporádica de *outliers*. Já o fluxo que percorreu o $\text{AS}_{\text{Transit}}2$ apresentou um aumento significativo no RTT fim a fim entre os tempos *T0 + 22618* e *T0 + 22618 segundos* da campanha de medições;
- De acordo com os passos propostos para a metodologia, discutidos na Seção 4.2.4, o fluxo que percorreu o $\text{AS}_{\text{Transit}}2$ deve ser investigado. Os resultados observados na série temporal do RTT Probe-Destino deste *traceroute* são compatíveis com o comportamento que consideramos suspeito de congestionamento.

A Figura 5.4b apresenta as séries temporais das latências medidas para a métrica ΔASN2 dos três fluxos de medição da campanha. Da mesma forma que o observado nas séries temporais da métrica RTT Probe-Destino, o *traceroute* que



(a) RTT Probe-Destino (b) ΔASN2 - Destino: Servidor de jogos

Figura 5.4 – Comparativo de métricas provedores de trânsito

percorre o $AS_{Transit}2$ também sofre uma elevação semelhante àquela observada na RTT Probe-Destino.

A Figura 5.5 apresenta as séries temporais das métricas RTT Probe-Destino e ΔASN2 do *traceroute* que percorre o $AS_{Transit}2$, bem como, o *% de perda de pacotes* observado durante toda a campanha de medição. É possível observar nestes gráficos um sincronismo na mudança de comportamento das três métricas. Enquanto a simetria entre RTT Probe-Destino e ΔASN2 indicam que o aumento da latência observada no RTT fim a fim ocorreu dentro do ASN2, a mesma simetria observada no aumento do número de pacotes perdidos reforçam que o evento pode ser um congestionamento. Conforme discutido na Seção 4.2.4, o aumento da perda de pacotes, se sincronizados com o aumento da latência em uma ou mais métricas observadas, são um comportamento compatível com congestionamentos enfrentados em algum segmento de rede percorrido pelo *traceroute*.

Ainda como parte da análise do aumento da latência ocorrido nas medições realizadas sobre o $AS_{Transit}2$, analisamos os resultados dos *traceroutes*, antes, durante e após o aumento de latência observado no RTT Probe-Destino. Uma possível explicação para o aumento da latência, e mesmo para o aumento da perda de pacotes, seria uma alteração de roteamento realizada pelo $AS_{Transit}2$. Porém, ao analisarmos os roteadores *egress* do $AS_{Transit}2$ e *ingress* do ASN3 percorridos pelo *traceroute*, não observamos qualquer alteração nos IPs dos mesmos. Isto evidencia que não houveram alterações no roteamento inter-AS realizadas pelo $AS_{Transit}2$ durante a campanha de medição.

A Tabela 5.2 apresenta os resultados estatísticos para as métricas RTT Probe-Destino e ΔASN2 dos três fluxos de *traceroute*. Estes dados oferecem importantes informações sobre as métricas e a dispersão dos resultados, que podem ser usados na

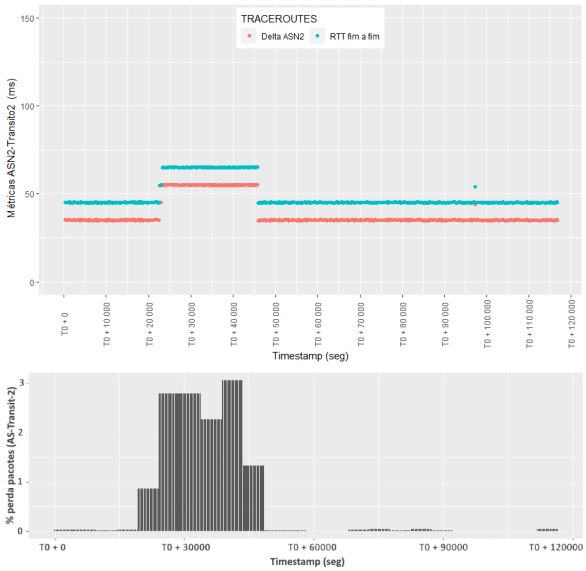


Figura 5.5 – Métricas RTT Probe-Destino, ΔASN2 e % Perda de Pacotes do $AS_{Transit}2$

	Média (ms)	**Desvio Padrão**	**Mediana (ms)**	**Variação (ms)**
RTT Probe-Destino $AS_{Transit}1$	30,07	0,91	31	29 a 45
RTT Probe-Destino $AS_{Transit}2$	49,06	7,94	45	44 a 65
RTT Probe-Destino $AS_{Transit}3$	98,23	1,87	97	96 a 120
ΔASN2 $AS_{Transit}1$	20,07	0,81	21	19 a 35
ΔASN2 $AS_{Transit}2$	39,06	8,15	33	34 a 55
ΔASN2 $AS_{Transit}3$	25,09	1,06	25	24 a 43

Tabela 5.2 – Métricas dos ASes $AS_{Transit}1$, $AS_{Transit}2$ e $AS_{Transit}3$

comparação entre ASes. Os resultados apresentados indicam que o $AS_{Transit}1$ apresentou a menor latência e *jitter* de pacotes tendo como destino o servidor de jogos investigado. Somado a isso, este mesmo AS não apresentou durante as medições comportamentos que, de acordo com a metodologia proposta, são compatíveis com congestionamentos no fluxo de medições.

Análise do uso da metodologia no Estudo de Caso 2

Tendo como destino um servidor de jogos na Internet, este estudo de caso avaliou três provedores de trânsito presentes em um dado IXP. Utilizando-se da lista de caminhos conhecidos, construída como parte da metodologia, foram identificados três *probes*, localizados em ASes com relacionamento *c2p* com os sistemas autônomos avaliados, a partir dos quais foram gerados *traceroutes* tendo como destino o IP do servidor de jogos escolhido.

Análise do uso da metodologia no Estudo de Caso 2 (continuação)

Durante o período das medições, o $AS_{Transit}2$ apresentou variações nas métricas RTT Probe-Destino e ΔASN2, observadas através das séries temporais, compatíveis com um possível congestionamento. Como passos adicionais, foram avaliados a perda de pacotes e o caminho de rede percorrido pelo *traceroute*, antes, durante e após o evento suspeito. Os resultados destas análises corroboraram com a hipótese de congestionamento, já que a perda de pacotes neste *traceroute* aumentou durante o período de aumento da latência nas métricas RTT Probe-Destino e ΔASN2. Somado a isso, não foram observadas mudanças de roteamento inter-AS que poderiam justificar o observado. Os *traceroutes* que percorreram os ASes $AS_{Transit}1$ e $AS_{Transit}3$ não apresentaram resultados semelhantes, o que nos levou a classificar a operação destes ASes como estáveis durante a campanha de medição.

Com relação a tabela 5.2, a dispersão observada nos valores do *desvio padrão* e *range de valores* nas medições sobre o $AS_{Transit}2$ reforçam a hipótese de que um congestionamento temporário pode ter ocorrido.

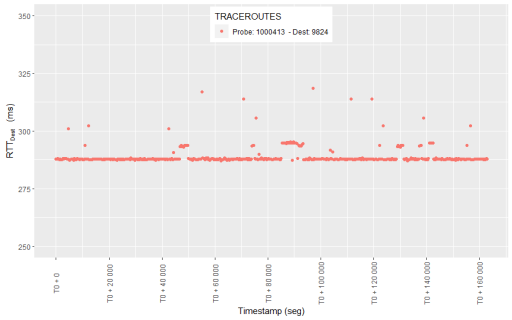
Ainda com relação às medições sobre o $AS_{Transit}2$, a diferença entre os valores da *média* e *mediana*, embora exista, é de apenas *4ms*. A baixa amplitude desta diferença indica que o evento ocorrido teve uma curta duração ou o aumento temporário da latência, observado durante o evento, teve um baixo impacto no RTT fim a fim.

Considerando os objetivos desta campanha de medição, o $AS_{Transit}1$ foi aquele que apresentou os melhores resultados de latência fim a fim e *jitter* de pacotes, além das medições sobre este AS não sugerirem que um congestionamento foi observado.

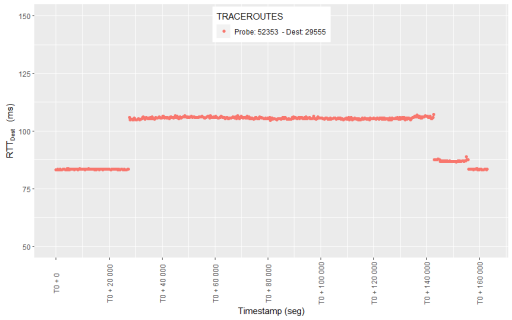
5.3 Estudo de Caso 3: Comparação entre ASes considerando destinos diversos

Nossa metodologia também pode ser utilizada para realizar uma avaliação de desempenho mais abrangente de um sistema autônomo, realizando medições com diferente destinos de interesse na Internet, simultaneamente. Conforme nossas medições demonstram, o desempenho do plano de dados de um AS apresenta resultados diferentes, tanto no roteamento interno quanto no encaminhamento de pacotes, dependendo do destino do *traceroute*.

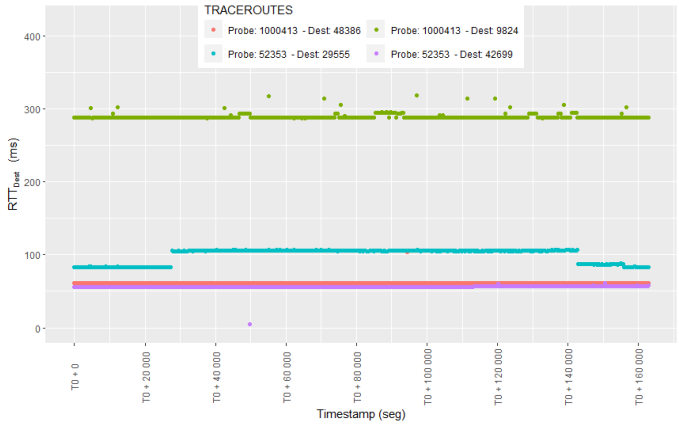
Neste estudo de caso, avaliamos o AS 35320 com relação a destinos localizados



(a) RTT fim a fim destinos ASes 9824



(b) RTT fim a fim destinos ASes 29555



(c) RTT fim a fim destinos ASes 48386, 29555, 9824 e 42699

Figura 5.6 – RTT fim a fim via AS 35320

nos ASes 48386, 29555, 9824 e 42699 durante, aproximadamente, 45 horas. A Figura 5.6c apresenta as séries temporais da métrica RTT Probe-Destino para os destinos avaliados.

Ao analisar os resultados das séries temporais da RTT Probe-Destino, observa-se que o *traceroute* para o destino 29555 apresentou variações importantes. O destino 9824 também apresentou variações que, embora com duração menor, extrapolam nosso critério de *outlier*. Um aspecto importante do processo de análise de nossa metodologia é verificar se há um sincronismo entre os eventos que podem ser congestionamentos. Isso poderia indicar um congestionamento mais amplo no AS 35320 e não relacionado a um destino em específico. Observando-se os momentos em que os eventos ocorreram e a característica diferente deles, em uma primeira análise, não parece haver qualquer tipo de sincronismo entre eles. Nas Figuras 5.6a e 5.6b estão individualizadas as séries temporais dos *traceroutes* em direção aos destinos 9824 e 29555, respectivamente.

Embora as séries temporais dos *traceroutes* com destinos nos ASes 48386 e 42699 tenham apresentado um comportamento homogêneo durante toda a campanha de medição, conforme discutido na Seção 5.1, não é possível apenas com esta métrica

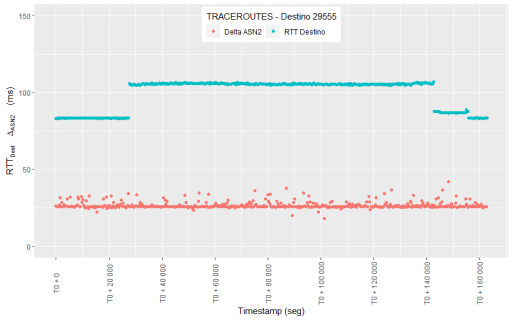
inferir que o AS 35320, ou suas escolhas de roteamento inter-domínio, não estiveram congestionadas durante toda a campanha. Somado ao longo tempo das medições, em nossa metodologia nós também utilizamos a métrica *# pacotes perdidos por medição* como um complemento à análise sobre o comportamento homogêneo de medições durante toda a campanha. Conforme a Figura 5.8 apresenta, não ocorreram perdas de pacotes nos *traceroutes* em direção a destinos nos ASes 48386 e 42699, reforçando os indícios de que estes ASes não enfrentaram possíveis congestionamentos durante a campanha de medição.

Ainda com relação à métrica *# pacotes perdidos por medição*, a Figura 5.8 também apresenta os resultados da perda de pacotes para os *traceroutes* com destino nos ASes 29555 e 9824. É interessante observar que, durante o período de alteração na latência da métrica RTT Probe-Destino para os fluxos, não ocorreram aumentos na perda de pacotes. Conforme discutido na Seção 4.2.4, ou aumento da perda de pacotes é um dos indícios usados pela nossa metodologia para inferir possíveis congestionamentos no caminho percorrido pelo fluxo de medição na Internet.

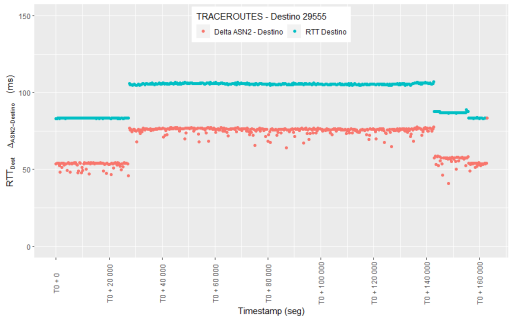
Para determinar se os eventos observados no RTT Probe-Destino dos *traceroutes* em direção aos destinos 29555 e 9824 foram gerados pelo roteamento interno do ASN2, devemos observar as métricas ΔASN2, $\Delta\text{ASN2}_{\text{egress}}$-Dest e $\Delta\text{ASN3}_{\text{ingress}}$-Dest. A Figura 5.7a apresenta a comparação das séries temporais das métricas RTT Probe-Destino e ΔASN2 do *traceroute* com destino no AS 29555. Pode-se observar que, apesar da dispersão dos resultados, não há uma correlação direta entre o aumento de RTT Probe-Destino e o tempo de encaminhamento dos pacotes do AS 35320. A própria dispersão do ΔASN2 não é observada no RTT fim a fim (RTT Probe-Destino).

O gráfico da Figura 5.7b apresenta a série temporal da métrica $\Delta\text{ASN2}_{\text{egress}}$-Dest para o *traceroute* com destino no AS 29555. Com esta métrica, buscamos observar se o aumento do tempo ocorre após o ASN2, já que ela representa a diferença entre o RTT observado no roteador *egress* do ASN2 e o destino. Neste caso, há uma correlação clara entre os eventos, ou seja, o aumento do RTT ocorreu no encaminhamento de pacotes entre o AS 35320 e o ASN3.

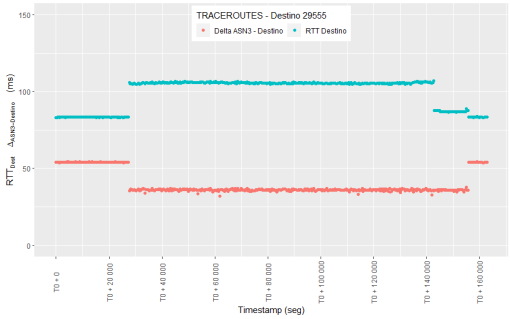
Já a terceira métrica, a $\Delta\text{ASN3}_{\text{ingress}}$-Dest, nos permite avaliar se o aumento do RTT no fluxo em direção ao AS 29555 ocorreu após o ASN3 receber os pacotes ou no enlace entre ASN2 e ASN3. A Figura 5.7c apresenta o resultado da série temporal desta métrica. É interessante observar que ocorreu uma redução no latência da



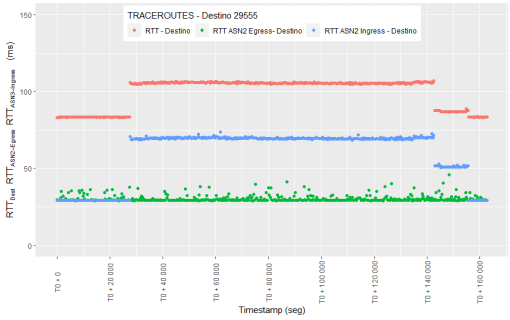
(a) RTT Probe-Destino, ΔASN2 - Destino 29555



(b) RTT Probe-Destino, $\Delta ASN2_{egress}$-Dest - Destino 29555



(c) RTT Probe-Destino, $\Delta ASN3_{ingress}$-Dest - Destino 29555



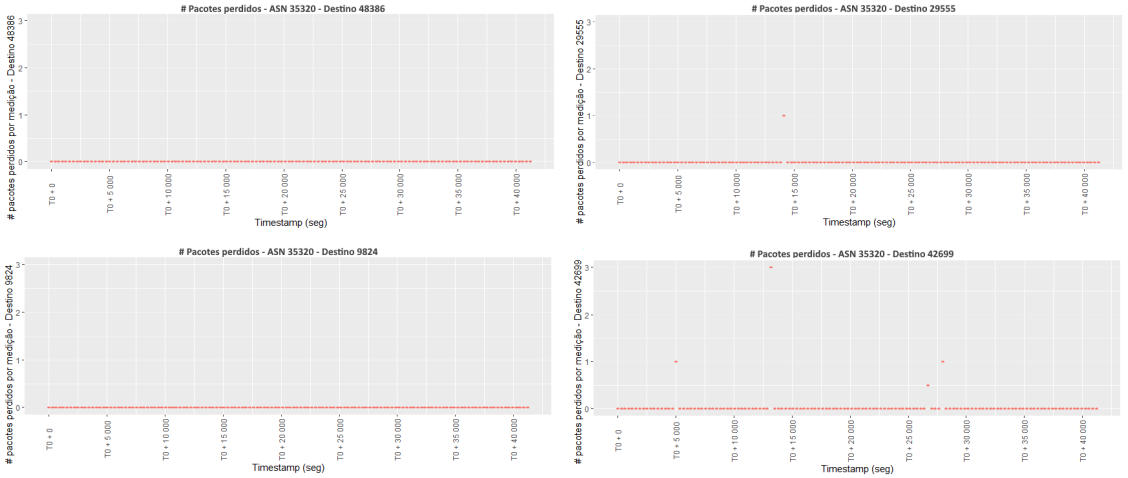
(d) RTT Probe-Destino, RTT Probe-$ASN2_{egress}$, RTT Probe-$ASN3_{ingress}$

Figura 5.7 – Métricas ASN2 35320 - Destino 29555

métrica $\Delta ASN3_{ingress}$-Dest, justamente, no momento onde ocorreu o aumento do RTT fim a fim. Este resultado sugere que o caminho percorrido pelo *traceroute* a partir do roteador *ingress* do ASN3, aparentemente, possui uma latência menor em relação ao destino do que aquele percorrido antes do aumento de latência no RTT Probe-Destino. Essa observação sugere que houve alguma alteração de roteamento inter-domínio entre ASN2 e ASN3.

Adicionando outras duas métricas à nossa análise, RTT Probe-$ASN2_{egress}$ e RTT Probe-$ASN3_{ingress}$, buscamos isolar o tempo de propagação do enlace entre o AS 35320 e o ASN3. A Figura 5.7d apresenta o resultado desta investigação. Enquanto a métrica RTT Probe-$ASN2_{egress}$ permaneceu inalterada durante todo a medição, RTT Probe-$ASN3_{ingress}$ sofre um aumento no RTT de forma síncrona com o aumento observado em RTT Probe-Destino, indicando que o aumento da latência ocorreu no enlace inter-domínio entre estes dois ASes. Esse aumento pode estar relacionado a um congestionamento no enlace inter-domínio entre ASN2 e ASN3 ou em uma mudança de roteamento inter-domínio realizada pelo ASN2 no encaminhamento dos pacotes. Estas situações devem ser diferenciadas pela investigação da metodologia.

Para melhor entender o ocorrido, investigamos os resultados dos *traceroutes* antes, durante e após o aumento da latência observada em RTT Probe-Destino.



(a) Perda de pacote no RTT fim a fim para os destinos 48386 e 9824

(b) Perda de pacote no RTT fim a fim para os destinos 29555 e 42699

Figura 5.8 – Perda de pacotes no RTT fim a fim para os destinos 48386, 9824, 29555 e 42699

Nesta investigação, observamos que o roteador *ingress* do ASN3 foi alterado no exato momento em que ocorreu o aumento da latência em RTT Probe-Destino. Apesar do roteador *ingress* ter sido alterado, ele ainda pertence ao mesmo ASN3, ou seja, o roteador para o qual o ASN2 encaminha os pacotes foi alterado mas o ASN3 não. Ainda sobre a análise dos resultados, o roteador *egress* utilizado pelo AS 35320 para encaminhar os pacotes ao ASN3 foi o mesmo durante toda a campanha de medição.

Apesar de não termos acesso às políticas de roteamento do AS 35320, uma das possibilidades para a alteração do roteador para o qual o AS 35320 encaminha os pacotes seria um anúncio de rotas recebido por este AS com um caminho de menor custo (menos *hops*) até o destino. Um indício que reforça está hipótese é o número de *hops* percorrido pelo *traceroute*, medido pela métrica #Hops Probe-Destino. Antes de ocorrer o aumento dos valores observados nas métricas $\Delta ASN2_{egress}$-Dest e RTT Probe-Destino, estavam sendo percorridos 16 *hops* entre o *probe* e o destino. Durante o aumento da latência observada em RTT Probe-Destino, o número de *hops* reduziu para 14. A redução de dois *hops* no caminho do *traceroute* ocorreu entre ASN3 e o destino.

Como discutido no Capítulo 2, o protocolo BGP não leva em consideração métricas de desempenho normalmente presentes em SLAs, como latência e perda de pacotes, por exemplo, em suas escolhas de roteamento. Considerando que o menor número de *hops* até o destino foi o que levou à mudança de roteamento, é

	Média (ms)	**Desvio Padrão**	**Mediana (ms)**	**Variação (ms)**
ProbeID:1000413, Destino:48386	61,47	1,87	61,40	61 a 104
ProbeID:1000413, Destino:9824	288,96	3,69	287,80	287 a 318
ProbeID:52353, Destino:29555	99,41	9,74	105,40	83 a 107
ProbeID:52353, Destino:42699	56,04	2,38	55,68	55 a 61

Tabela 5.3 – Métricas de RTT Probe-Destino do AS 35320

importante notar que, apesar da redução no número de *hops* até o destino, o novo caminho escolhido pelo BGP possui uma latência significativamente maior, o que pode impactar a experiência dos usuários.

O aumento de latência em aproximadamente 40ms no novo enlace entre ASN2 e ASN3 pode ter sido causado por uma característica inerente deste novo enlace ou a um congestionamento observado no mesmo durante todo o período em que ele foi utilizado para o roteamento. Em termos da metodologia proposta, o fato de não ocorrerem perda durante o período que o novo enlace foi utilizado para o encaminhamento dos pacotes entre o ASN2 e ASN3, sugere que esta pode ser uma característica de latência inerente do enlace utilizado.

A Tabela 5.3 apresenta os dados estatísticos para a métrica RTT Probe-Destino para os 4 *traceroute* que percorreram o AS 35320. Considerando o valor médio da latência observada no fluxo de medições que percorre o AS 35320 em direção ao destino localizado no AS 29555, de *99,41ms*, o valor da dispersão observado no *desvio padrão* torna-se representativo. Este resultado de dispersão é compreensível pelo impacto da mudança de roteamento ocorrida neste fluxo durante as medições, mesmo que não tenha ocorrido um congestionamento. A proximidade dos valores de *media* e *mediana* dos demais fluxos sugerem que congestionamentos não foram observados nestes fluxos, conforme discutido na Seção 4.2.4.

Análise do uso da metodologia no Estudo de Caso 3

A avaliação do AS 35320 em relação à quatro diferentes destinos na Internet foi o objetivo deste estudo de caso. A partir da lista de caminhos conhecidos, foram escolhidos quatro *probes*, localizados em dois ASes com relação *c2p* com o AS 35320, a partir dos quais foram gerados *traceroutes* tendo como destino IPs localizados nos sistemas autônomos 48386, 9824, 29555 e 42699.

Análise do uso da metodologia no Estudo de Caso 3 (continuação)

Os resultados do *traceroute* em direção ao AS 29555 foram analisados através da série temporal da métrica RTT Probe-Destino, que sugeriu, em um primeiro momento, a possibilidade de um congestionamento ter ocorrido durante a campanha. As investigações dos resultados deste *traceroute* usando outras métricas possibilitou isolar um aumento de latência de aproximadamente 40ms no enlace entre o AS 35320 e o roteador *ingress* do ASN3.

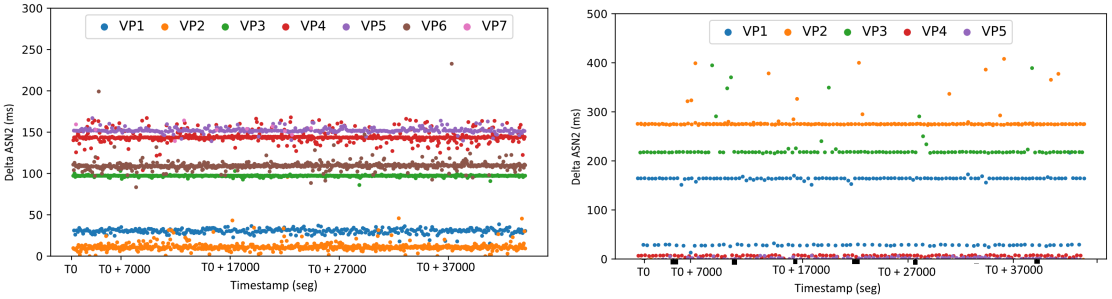
Ao avaliar as perdas de pacotes no resultado do *traceroute* em direção ao AS 29555, observou-se que elas foram praticamente irrelevantes ao longo de toda a medição e não sofreram qualquer alteração no período em as latências medidas nas métricas $\Delta ASN3_{ingress}$-Dest e RTT Probe-Destino aumentaram. A ausência de perda de pacotes durante o aumento de latência observado implicou em investigações adicionais para entender o fenômeno, já que possíveis congestionamentos, de acordo com a metodologia proposta, estão geralmente correlacionados com o aumento da perda de pacotes. Durante esta investigação, observou-se que ocorreram alterações no roteamento inter-domínio entre o AS 35320 e o ASN3.

Ao investigar os resultados dos *traceroutes* em direção ao destino no AS 29555, observou-se que, durante o aumento da latência fim a fim, o número de *hops* percorridos pelos pacotes reduziu em 2 *hops*. A alteração de roteamento inter-domínio foi realizada pelo AS 35320, que, aparentemente, encontrou um caminho de menor custo, em termos de *hops*, até o destino dos pacotes.

Apesar da redução do número de *hops* entre o roteador *ingress* do ASN3 e o destino, o que provavelmente levou o BGP do AS 35320 a realizar esta escolha, houve um aumento de aproximadamente 40ms no transporte dos pacotes entre o AS 35320 e o novo roteador *ingress* do ASN3. Este é um comportamento, discutido na Seção 2.2, ao qual o BGP está sujeito em função dos critérios usados por este protocolo para tomar suas decisões de roteamento. Assim, apesar da nova rota escolhida possuir um menor número de *hops* até o destino, o enlace entre o AS 35320 e o ASN3 possuía uma latência bastante superior ao benefício obtido com a redução do número de *hops* até o destino.

Os demais fluxos observados neste estudo de caso não apresentaram comportamentos semelhantes ao *traceroute* em direção ao destino no AS 29555 e mantiveram-se estáveis durante todo o experimento.

Este estudo de caso ajuda a ilustrar um possível uso da metodologia proposta para apoiar decisões da engenharia de tráfego de um AS em busca de melhores decisões de encaminhamento de pacotes.



(a) AS A (b) AS B

Figura 5.9 – Comparação de RTT de dois provedores de trânsito.

5.4 Estudo de Caso 4: Comparação entre ASes Tier-1 e Tier-2

Nossa metodologia possui diversas limitações para uma correta avaliação de ASes Tier-1, principalmente relacionadas à escala global deste tipo de AS. Como ASes desta categoria possuem muitos roteadores *egress* e *ingress*, mundialmente distribuídos, as investigações que realizamos podem ser inviabilizadas devido à complexidade deste ecossistema. Mesmo considerando esta limitação, apresentamos neste estudo de caso a comparação do tempo de encaminhamento de pacotes de um AS Tier-1 e um AS Tier-2. O AS Tier-1, que chamaremos aqui de *AS A*, possui aproximadamente 34 mil ASes no seu *customer cone*, de acordo com o *CAIDA AS Rank* (CAIDA, 2021b). Já o AS Tier-2, que chamaremos nesta seção de *AS B*, possui aproximadamente 1,5 mil ASes no seu *customer cone*.

A Figura 5.9 apresenta os resultados da métrica ΔASN2 dos ASes A e B. Para a medição do AS A, foram utilizados sete *probes*, enquanto que para o AS B foram utilizados cinco *probes*. Observe-se que a disponibilidade de *probes* em ASes de maior porte, como os ASes A e B, resolvem muitas das dificuldades em encontrar *probes* em número adequado para nossas campanhas de medição.

Os resultados sugerem um comportamento estável durante todo o período da campanha, sendo que observamos apenas *outliers* e variações de latência que podem ser consideradas normais. A métrica ΔASN2 corresponde à diferença entre o RTT dos roteadores *egress* e *ingress*, indicando o tempo que os *traceroutes* demoram para percorrer o AS avaliado. Note-se que os fluxos gerados por diferentes *probes* apresentam séries temporais para a métrica ΔASN2 diferentes, mesmo que os fluxos tenham percorrido o mesmo ASN2. Estas variações estão associadas ao caminho interno percorrido por cada fluxo de pacote, que pode variar em função do roteador *ingress*, roteamento interno e do roteador *egress* utilizado para o encaminhamento

dos pacotes para ASN3.

Quando comparamos os valores de média de ΔASN2 entre os dois ASes, vemos que o AS *A* tem uma latência interna menor que o AS *B* (observe-se que, nas Figuras 5.9b e 5.9a, a escala do eixo Y estão diferentes para facilitar a observação das variações das medições). Este resultado poderia ser utilizado por alguém em busca de uma menor latência para um provedor de *trânsito*, considerando os destinos investigados.

Outro aspecto a ser observado é a maior quantidade de *outliers* nas medições realizadas sobre o AS *B*. Embora eles não sejam representativos no valor médio da ΔASN2 dos *traceroutes*, eles ocorrem com uma frequência maior do que nas medições do AS *A*.

Por outro lado, as séries temporais da ΔASN2 do AS *A* apresentam uma maior variação (*jitter*) nos resultados de algumas medições. Por exemplo, o fluxo originado no *probe VP4* apresentou uma variação de até 50ms nos valores medidos, o que pode ser um *jitter* relevante para determinadas aplicações. Assim, considerando os destinos investigados, para alguém que busque uma estabilidade maior na latência, o AS *B* poderia ser uma melhor opção.

De qualquer forma, apesar de alguns eventos isolados no AS *B* de alterações seguidas no ΔASN2, não foi observado nenhum comportamento que pudesse ser classificado como um congestionamento persistente e que merecesse investigações adicionais.

Análise do uso da metodologia no Estudo de Caso 4

Este estudo de caso foi incluído neste capítulo com o propósito de demonstrar o uso da metodologia com a abundância de *probes* disponíveis para as medições. Como os ASes avaliados são de grande e médio porte, o número de acordos existentes com outros ASes, que possuem *probes* instalados, torna o nosso método de seleção de *probes*, a partir da lista de caminhos conhecidos, mais efetivo.

Neste estudo de caso dois ASes foram comparados a partir de um conjunto abrangente de *probes*, instaladas em sistema autônomo com diferentes tipos de acordos de interconexão com os ASes investigados (*p2p* e *c2p*). A ausência de alterações de latência persistentes nas métricas investigadas para todos os fluxos de medição, bem como, a ausência de perdas de pacotes, sugerem que, durante a campanha, possivelmente, não ocorreram congestionamentos em nenhum dos fluxos de medição.

Análise do uso da metodologia no Estudo de Caso 4 (continuação)

A disponibilidade de *probes* para as medições, explorada de maneira mais efetiva neste estudo de caso, é um dos aspectos que limitaram os estudos de caso apresentados nesta seção. No Capítulo 6 estão apresentadas algumas possibilidades de evolução deste trabalho que poderiam melhorar a disponibilidade de *probes* para medições usando esta metodologia.

5.5 Estudo de Caso 5: Detecção de Congestionamentos Persistentes

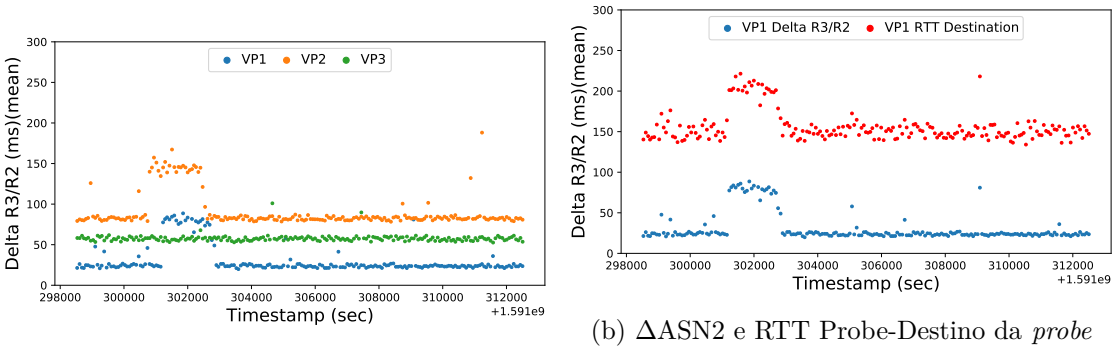
Nesta seção, apresentamos um estudo de caso onde um conjunto de indícios, baseados em nossa análise metodológica, foram coletados indicando que o ASN2 avaliado pode ter enfrentando um congestionamento durante as medições. Como discutido anteriormente, em campanha de medições com o objetivo de identificar congestionamentos internos em sistemas autônomos não é necessário realizar comparações entre ASes.

Neste estudo de caso foram utilizados três *probes* (*VP1*, *VP2* e *VP3*) com o destino dos *traceroutes* localizados em três3 diferentes ASes na Internet. A Figura 5.10a apresenta os resultados das séries temporais da métrica ΔASN2 dos três fluxos de *traceroute*. É possível perceber que, mesmo originados de diferentes *probes* e direcionados a destinos diferentes, dois dos fluxos de pacote apresentaram um aumento de latência em um período de tempo praticamente idêntico durante toda a campanha.

A priori, pelo fato do fluxo originado pelo *probe VP3* não apresentar um comportamento semelhante, descartamos a hipótese de um congestionamento generalizado no ASN2.

A Figura 5.10b apresenta as séries temporais das métricas ΔASN2 e RTT Probe-Destino para o fluxo de pacotes originado no *probe VP1*. O gráfico sugere que a métrica RTT Probe-Destino está sofrendo um aumento de forma síncrona com as alterações observadas no ΔASN2, o que pode indicar uma mudança de roteamento no ASN2 ou um possível congestionamento. Os resultados destas séries temporais para o fluxo de *traceroute* gerado no *probe VP2* apresentam resultados semelhantes.

A investigação deste estudo de caso possui algumas limitações que nos impediram de definir onde exatamente o possível congestionamento ocorreu dentro do



(a) ΔASN2 ASN2.

(b) ΔASN2 e RTT Probe-Destino da *probe VP1*.

Figura 5.10 – Análise de possível congestionamento interno no ASN2.

ASN2. Porém, ao observamos os resultados do *Paris traceroute* antes, durante e depois do aumento da latência em ΔASN2, podemos inferir algumas conclusões que podem ser relevantes para alguém considerando um acordo de interconexão com este ASN2:

- Os roteadores *ingress* e *egress* dos *traceroutes* originados pelos *VP1* e *VP2* não alteraram durante os aumentos de latência, ou seja, durante toda a campanha de medição os roteadores de borda do ASN2 permaneceram os mesmos;
- Os roteadores *egress* dos ASN3s para os fluxos originados pelos *probes VP1* e *VP2* permaneceram os mesmos durante a campanha;
- O fluxo originados no VP1 percorreu cinco *hops* dentro do ASN2, sendo que três destes roteadores não responderam aos pacotes *ICMP Echo Request*;
- O fluxo originados no VP2 percorreu oito *hops* dentro do ASN2, sendo que quatro destes roteadores não responderam aos pacotes *ICMP Echo Request*;
- O fato de alguns roteadores internos não responderem ao *ICMP Echo Request* do *traceroute* não nos permitiu verificar se ambos fluxos percorriam em algum ponto os mesmos caminhos dentro do ASN2;
- A ocorrência de perdas de pacotes nos momentos que antecederam ao aumento de latência nas métricas ΔASN2 e RTT Probe-Destino praticamente inexistia. Porém, durante o período de aumento da latência observada por estas métricas, passaram a ocorrer perdas entre 2,3 e 3% dos pacotes.

Considerando os apontamentos apresentados acima, não foi possível determinar se houveram alterações de roteamento internas no ASN2 que justificassem o aumento do tempo de encaminhamento de pacotes por este AS. Porém, independente das causas do aumento das métricas, o conjunto de indícios coletados indicam

que pode ter ocorrido um congestionamento interno no ASN2 em direção a dois diferentes destinos na Internet.

Análise do uso da metodologia no Estudo de Caso 5

O método de seleção de *probes* proposto neste trabalho propiciou a avaliação do ASN2 deste estudo de caso usando três *probes*, hospedados em ASes diferentes, sem que fosse necessário para as medições possuir um acordo de interconexão com o sistema autônomo avaliado. Os resultados das medições de dois *traceroutes*, gerados pelos *probes VP1* e *VP2*, apresentaram variações na métrica RTT Probe-Destino compatíveis com situações suspeitas de congestionamento. Ao aplicar os passos descritos na Seção 4.2.4, fomos capazes de isolar o roteamento interno do ASN2 como o local onde o aumento da latência ocorreu em ambos os fluxos de medição.

Um aspecto importante neste estudo de caso é a simetria dos aumentos de latência observados nos *traceroutes* gerados por *VP1* e *VP2*. Todas análises aplicadas sobre as métricas destes fluxos apresentaram resultados semelhantes e simétricos, ou seja, a degradação ocorrida no ASN2 afetou de forma semelhante estes dois fluxos.

A seguir, seguindo os passos da metodologia, verificamos que as métricas de perda de pacotes se elevaram de forma sincronizada com o aumento de latência nos fluxos de medição gerados por *VP1* e *VP2*. Esse segundo indicio de um possível congestionamento nos levou a analisar os roteadores percorridos pelos *traceroutes*, antes, durante e após o aumento da latência e do percentual de pacotes perdidos. Observamos que não ocorreram, durante as medições, alterações nos roteadores *ingress* e *egress* do ASN2, bem como, do roteador *ingress* do ASN3, para nenhum dos *traceroutes* gerados.

De acordo com a metodologia proposta, este conjunto de indícios sugerem que um congestionamento foi enfrentando no ASN2 durante as medições realizadas. Como o *traceroute* gerado pelo *probe VP3* não apresentou resultados semelhantes, consideramos possível que o ASN2 tenha enfrentando um congestionamento parcial durante a campanha de medição.

6 CONSIDERAÇÕES FINAIS

O principal objetivo deste trabalho foi propor e avaliar, de forma preliminar, uma metodologia que visa inferir possíveis congestionamentos internos em ASes e coletar métricas que possam representar a qualidade do plano de dados do mesmo, assim como suas escolhas de roteamento inter-AS. Um dos principais aspectos da metodologia proposta é que esta avaliação pode ser realizada sem que o AS interessado na avaliação possua um acordo de interconexão estabelecido com o sistema autônomo a ser avaliado. Nossa estratégia para viabilizar estas medições sem acordos pré-estabelecidos foi utilizar *probes* do RIPE ATLAS para realizar as medições, possibilitando assim investigar as relações já estabelecidas pelo AS avaliado. Para inferir possíveis congestionamentos internos e medir as métricas de latência de um AS, nós concebemos um método de medições inspirado no TSLP.

Ao longo das dezenas de campanhas de medição que realizamos, pudemos observar que os principais objetivos do nosso trabalho foram atingidos. Apesar das análises de estudos de caso apresentadas no Capítulo 5 carecerem de dados de *ground truth* que confirmem, ou não, nossas inferências, coletamos um conjunto de indícios, com bases nas métricas e passos metodológicos utilizados, que sugerem que possíveis congestionamentos foram detectados durante algumas medições. Somado a isso, geramos um conjunto de dados estatísticos sobre as principais métricas da metodologia que podem ser utilizadas na comparação entre sistemas autônomos.

Entre as campanhas de medição apresentadas no Capítulo 5, destacamos o estudo de caso 3, que teve como objetivo reproduzir um dos principais motivadores para ISPs buscarem novos acordos de interconexão: reduzir a latência dos seus serviços de Internet em relação a servidores de jogos online. Neste estudo de caso, partindo da presença em um determinado IXP, identificamos três ASes que poderiam prover o serviço de *trânsito*, a qualquer ISP presente neste IXP, até um determinado servidor de jogos na Internet. Coletamos um conjunto representativo de métricas de latência destes provedores em relação ao servidor de jogos online, que poderiam ser utilizadas na comparação de desempenho entre eles. Embora essa investigação tenha utilizado provedores de *trânsito* presentes em um IXP específico, esse mesmo processo pode ser aplicado a qualquer IXP. Um IXP pode ser um ente facilitador, em termos de infraestrutura, para o estabelecimento de novos acordos de interconexão entre ASes.

Este e outros exemplos que apresentamos no Capítulo 5 são uma pequena amostra do potencial do uso da metodologia para estabelecer uma nova dinâmica na escolha de parceiros de interconexão entre sistemas autônomos na Internet.

6.1 Trabalhos Futuros

Durante o desenvolvimento e validação da nossa metodologia, nos deparamos com uma série de limitações e possíveis evoluções que, por diferentes razões, acabaram não sendo incluídas no escopo deste trabalho. A principal limitação que enfrentamos está relacionada ao método que adotamos para identificar combinações de *probes* e destinos que possibilitam a avaliação de um sistema autônomo. A lista de caminhos conhecidos da metodologia foi criada a partir das medições realizadas por nós e por outros usuários do RIPE ATLAS. Ainda que tenhamos tido sucesso nos nossos objetivos, campanhas de medição de maior escala irão requerer um aprimoramento neste método, de forma a gerar um conjunto maior de caminhos conhecidos, aumentando a disponibilidade de *probes*.

Ainda sobre os caminhos conhecidos, observamos que entre 25% e 35% das tuplas *probe*/destino previamente validadas tornam-se inválidas dentro de 7 dias. Isso nos fez adicionar a etapa de pré-validação antes de toda campanha de medição. Contudo, esta observação não foi aprofundada para um melhor entendimento dos fatores preponderantes no envelhecimento dos caminhos conhecidos. As tuplas que tornam-se inválidas mais rapidamente estão ligadas a um tipo de AS? Poderíamos observar as tabelas de roteamento anunciada pelos ASes para inferir quando uma tupla deixa de ser válida? Perguntas como estas precisarão ser respondidas para um aprimoramento da técnica de caminhos conhecidos utilizada nesta metodologia.

Não fez parte do escopo do nosso trabalho avaliar qual seria o tempo mínimo necessário para modelar, com um certo grau de confiança, o comportamento de um AS. Determinar o tempo mínimo necessário para se obter métricas representativas de um AS seria um outro avanço importante para este trabalho.

A ausência de dados de *ground truth* tornam nosso trabalho de análise dos resultados manual, trabalhosa e carente de uma comprovação prática do que observamos. Embora seja bastante complexo conseguir estes dados, uma possível abordagem seria cruzar os resultados das nossas medições com aqueles obtidos por outras ferramentas, como, por exemplo, a gerada pelo trabalho (FONTUGNE et al., 2017).

REFERÊNCIAS

AHMED, A. et al. Peering vs. transit: Performance comparison of peering and transit interconnections. In: **2017 IEEE 25th International Conference on Network Protocols (ICNP)**. Los Alamitos, CA, USA: IEEE Computer Society, 2017. p. 1–10. Available from Internet: <https://doi.ieeecomputersociety.org/10.1109/ICNP.2017.8117549>.

AMAZON. **Alexa TOP Sites**. 2021. Available from Internet: <https://www.alexa.com/topsites>.

ARGYRAKI, K.; MANIATIS, P.; SINGLA, A. Verifiable network-performance measurements. In: **Proceedings of the 6th International Conference**. New York, NY, USA: Association for Computing Machinery, 2010. (Co-NEXT '10). ISBN 9781450304481. Available from Internet: <https://doi.org/10.1145/1921168.1921170>.

AUGUSTIN, B. et al. Avoiding traceroute anomalies with paris traceroute. In: **Proceedings of the 6th ACM SIGCOMM Conference on Internet Measurement**. New York, NY, USA: Association for Computing Machinery, 2006. (IMC '06), p. 153–158. ISBN 1595935614. Available from Internet: <https://doi.org/10.1145/1177080.1177100>.

AWDUCHE, D.; AGOGBUA, J.; MCMANUS, J. An approach to optimal peering between autonomous systems in the internet. In: **Proceedings 7th International Conference on Computer Communications and Networks (Cat. No.98EX226)**. [S.l.: s.n.], 1998. p. 346–351.

CAIDA. **The CAIDA AS Relationships Dataset**. 2021. Available from Internet: <http://data.caida.org/datasets/as-relationships/>.

CAIDA. **CAIDA ASes RANK**. 2021. Available from Internet: <https://asrank.caida.org/>.

CASTRO, I. et al. Route bazaar: Automatic interdomain contract negotiation. In: **15th Workshop on Hot Topics in Operating Systems (HotOS XV)**. Kartause Ittingen, Switzerland: USENIX Association, 2015. Available from Internet: <https://www.usenix.org/conference/hotos15/workshop-program/presentation/castro>.

CHIU, Y.-C. et al. Are we one hop away from a better internet? In: **Proceedings of the 2015 Internet Measurement Conference**. [S.l.: s.n.], 2015. p. 523–529.

CLAYPOOL, M.; CLAYPOOL, K. Latency can kill: Precision and deadline in online games. In: **Proceedings of the First Annual ACM SIGMM Conference on Multimedia Systems**. New York, NY, USA: Association for Computing Machinery, 2010. (MMSys '10), p. 215–222. ISBN 9781605589145. Available from Internet: <https://doi.org/10.1145/1730836.1730863>.

DHAMDHERE, A. et al. Inferring persistent interdomain congestion. In: **Proceedings of the 2018 Conference of the ACM Special Interest Group**

on Data Communication. New York, NY, USA: Association for Computing Machinery, 2018. (SIGCOMM '18), p. 1–15. ISBN 9781450355674. Available from Internet: <https://doi.org/10.1145/3230543.3230549>.

FONTUGNE, R. et al. Pinpointing delay and forwarding anomalies using large-scale traceroute measurements. In: **Proceedings of the 2017 Internet Measurement Conference**. New York, NY, USA: Association for Computing Machinery, 2017. (IMC '17), p. 15–28. ISBN 9781450351188. Available from Internet: <https://doi.org/10.1145/3131365.3131384>.

FOUNDATION, R. **Linguagem R**. 2021. Available from Internet: <https://www.r-project.org/>.

GROSS, P. G.; REKHTER, Y. **Application of the Border Gateway Protocol in the Internet**. RFC Editor, 1994. RFC 1655. (Request for Comments, 1655). Available from Internet: <https://rfc-editor.org/rfc/rfc1655.txt>.

HAWKINSON, J. A.; BATES, T. J. **Guidelines for creation, selection, and registration of an Autonomous System (AS)**. RFC Editor, 1996. RFC 1930. (Request for Comments, 1930). Available from Internet: <https://rfc-editor.org/rfc/rfc1930.txt>.

KOMPELLA, R. R. et al. Every microsecond counts: Tracking fine-grain latencies with a lossy difference aggregator. In: **Proceedings of the ACM SIGCOMM 2009 Conference on Data Communication**. New York, NY, USA: Association for Computing Machinery, 2009. (SIGCOMM '09), p. 255–266. ISBN 9781605585949. Available from Internet: <https://doi.org/10.1145/1592568.1592599>.

LUCKIE, M. et al. Challenges in inferring internet interdomain congestion. In: **Proceedings of the 2014 Conference on Internet Measurement Conference**. New York, NY, USA: Association for Computing Machinery, 2014. (IMC '14), p. 15–22. ISBN 9781450332132. Available from Internet: <https://doi.org/10.1145/2663716.2663741>.

LUCKIE, M. et al. Bdrmap: Inference of borders between ip networks. In: **Proceedings of the 2016 Internet Measurement Conference**. New York, NY, USA: Association for Computing Machinery, 2016. (IMC '16), p. 381–396. ISBN 9781450345262. Available from Internet: <https://doi.org/10.1145/2987443.2987467>.

LUCKIE, M. et al. As relationships, customer cones, and validation. In: **Proceedings of the 2013 Conference on Internet Measurement Conference**. New York, NY, USA: Association for Computing Machinery, 2013. (IMC '13), p. 243–256. ISBN 9781450319539. Available from Internet: <https://doi.org/10.1145/2504730.2504735>.

MAIGRON, P. **Regional Internet Registries Statistics**. 2021. Available from Internet: <https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/World/ASN-ByNb.html>.

MARCOS, P. et al. A survey on the current internet interconnection practices. **SIGCOMM Comput. Commun. Rev.**, Association for Computing Machinery, New York, NY, USA, v. 50, n. 1, p. 10–17, mar. 2020. ISSN 0146-4833. Available from Internet: <https://doi.org/10.1145/3390251.3390254>.

MARCOS, P. et al. Dynam-ix: a dynamic interconnection exchange. In: **ACM CoNEXT 2018**. [S.l.: s.n.], 2018.

MARDER, A. et al. Pushing the boundaries with bdrmapit: Mapping router ownership at internet scale. In: **ACM Internet Measurement Conference (IMC)**. [S.l.: s.n.], 2018–11. p. 56–69.

MARDER, A.; SMITH, J. M. Map-it: Multipass accurate passive inferences from traceroute. In: **Proceedings of the 2016 Internet Measurement Conference**. New York, NY, USA: Association for Computing Machinery, 2016. (IMC '16), p. 397–411. ISBN 9781450345262. Available from Internet: <https://doi.org/10.1145/2987443.2987468>.

MARTIN, J.; NILSSON, A. On service level agreements for ip networks. In: **Proceedings.Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies**. [S.l.: s.n.], 2002. v. 2, p. 855–863 vol.2.

NCC, R. **RIPE ATLAS**. 2021. Available from Internet: <https://atlas.ripe.net>.

NCC, R. **RIPE ATLAS daily dumps**. 2021. Available from Internet: <https://data-store.ripe.net/datasets/atlas-daily-dumps/>.

NCC, R. **RIPE ATLAS daily measurements**. 2021. Available from Internet: <https://ftp.ripe.net/ripe/atlas/measurements/>.

NORTON, W. B. **The 2014 Internet Peering Playbook: Connecting to the Core of the Internet**. [S.l.]: DrPeering Press, 2014.

NORTON, W. B. **The Internet Peering Playbook: connecting to the core of the Internet**. [S.l.]: DrPeering Press, 2014.

PREHN, L.; FELDMANN, A. How biased is our validation (data) for as relationships? In: **Proceedings of the 21st ACM Internet Measurement Conference**. New York, NY, USA: Association for Computing Machinery, 2021. (IMC '21), p. 612–620. ISBN 9781450391290. Available from Internet: <https://doi.org/10.1145/3487552.3487825>.

SANDVINE. **The Mobile Internet Phenomena Report - May'21**. 2021. Available from Internet: <https://www.sandvine.com/hubfs/Sandvine_Redesign_2019/Downloads/2021/Phenomena/MIPR%20Q1%202021%2020210510.pdf>.

SOMMERS, J. et al. Accurate and efficient sla compliance monitoring. In: . New York, NY, USA: Association for Computing Machinery, 2007. (SIGCOMM '07), p. 109–120. ISBN 9781595937131. Available from Internet: <https://doi.org/10.1145/1282380.1282394>.

SPORTS, F. **Top 10 Most Popular Online Games In 2021**. 2021. Available from Internet: <https://firstsportz.com/top-10-most-popular-online-games-in-2021/>.

SUNDARESAN, S. et al. Tcp congestion signatures. In: **Proceedings of the 2017 Internet Measurement Conference**. [S.l.: s.n.], 2017. p. 64–77.

TEIXEIRA, R. et al. Network sensitivity to hot-potato disruptions. In: **Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications**. New York, NY, USA: Association for Computing Machinery, 2004. (SIGCOMM '04), p. 231–244. ISBN 1581138628. Available from Internet: <https://doi.org/10.1145/1015467.1015493>.