Fiscalização da Neutralidade da Rede: Conceitos e Técnicas

Chapter · May 2017

CITATIONS
0

READS
215

5 authors, including:

Ligia Eliana Setenareski
Universidade Federal do Paraná
9 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Thiago Garrett
University of Oslo
13 PUBLICATIONS **55** CITATIONS
SEE PROFILE

Luis Carlos Erpen Bona
Universidade Federal do Paraná
120 PUBLICATIONS **952** CITATIONS
SEE PROFILE

Capítulo
4

Fiscalização da Neutralidade da Rede: Conceitos e Técnicas

Ligia E. Setenareski (UFPR), Thiago Garrett (UFPR), Letícia M. Peres (UFPR), Luis C. E. Bona (UFPR), Elias P. Duarte Jr. (UFPR)

Abstract

Network Neutrality (NN) is becoming increasingly important as the global debate intensifies and governments worldwide implement regulations. According to NN, all types of traffic must be processed without discrimination, regardless of origin, destiny and/or content. The discrimination between different types of traffic compromises innovation, fair competition and the freedom of choice of consumers. However, ensuring that ISPs are not employing discriminating practices is still a challenge. This tutorial presents an overview of several existing solutions to detect "traffic differentiation". These solutions differ mainly on the monitoring topology, metrics and statistical methods employed. An introduction to the global debate around NN is also presented, as well as an overview of different regulations defined in Brazil and other countries around the world.

Resumo

A Neutralidade da Rede (NR) torna-se cada vez mais importante à medida que o debate sobre este princípio se intensifica, levando mais países a promoverem sua normatização. Segundo a NR, todo tipo de tráfego deve ser tratado da mesma forma, independente de sua origem, destino e/ou conteúdo. Discriminar tipos diferentes de tráfegos de dados compromete a inovação, concorrência justa e liberdade de escolha dos consumidores. Porém, fiscalizar se provedores de acesso estão praticando alguma diferenciação de tráfego ainda é um desafio. Este minicurso tem como objetivo principal apresentar diversas soluções para a detecção destas práticas. Estas soluções diferem principalmente na topologia utilizada para medição, nas métricas empregadas e nos métodos estatísticos utilizados. Também é apresentada uma introdução ao debate da NR, bem como um panorama da sua normatização no Brasil e no mundo.

Todos os autores são filiados à Universidade Federal do Paraná (UFPR). Emails: {ligia,tgarrett,lmperes,bona,elias}@inf.ufpr.br

4.1. Introdução

A importância da Internet na sociedade moderna tem aumentado significativamente, conforme a quantidade de usuários e serviços disponíves na rede cresce [K.G. Coffman 2002]. Adequar e manter a estrutura da rede para atender esta demanda crescente é um desafio, em especial porque além dos aspectos tecnológicos, devem ser considerados também aspectos econômicos. Os provedores de acesso (*Internet Service Providers*, ISPs) podem empregar técnicas de gerência de tráfego de rede para reduzir e/ou postergar investimentos na infraestrutura de rede [van Schewick and Farber 2009]. Entretanto, muitas destas técnicas de gerência de tráfego podem ser consideradas discriminatórias e podem ser utilizadas para outros fins, como para obter vantagens competitivas ou cobrar taxas extras de usuários e provedores de conteúdo.

Práticas discriminatórias consistem em manipular o tráfego de dados de forma a priorizar ou degradar algum tipo específico [Ravaioli et al. 2012] – baseando-se no tipo de informação sendo trafegada ou no destino/origem dos pacotes, por exemplo. Este tipo de manipulação configura a chamada diferenciação de tráfego (DT). Em geral a DT é empregada por um ISP devido a três fatores: (i) congestionamento, no qual limita-se a largura de banda utilizada por aplicativos que geram muito tráfego, como compartilhamento de arquivos P2P e *streaming* de vídeo [Mueller and Asghari 2012]; (ii) acordos comerciais, em que provedores de serviço pagam taxas extras para ter seu tráfego priorizado pelo ISP, as chamadas *fast-lanes* [Habibi Gharakheili et al. 2016]; e (iii) obtenção de vantagem competitiva, em que o tráfego do próprio ISP é priorizado ou o tráfego de concorrentes é degradado [Kendrick 2009, Lomas 2016].

A DT faz parte de um longo e controverso debate mundial sobre o princípio da Neutralidade da Rede (NR) [Joch 2009]. Este princípio já foi instituído em diversos países do mundo por meio de leis, diretrizes, regras e/ou princípios [Habibi Gharakheili et al. 2016]. Uma definição da NR comum às estas diversas normatizações diz que, em uma rede neutra, todo tipo de tráfego deve ser tratado da mesma forma, sem distinção por origem, destino e/ou conteúdo, ou seja, a DT não é permitida [Crowcroft 2007].

Para os defensores da NR, a DT ameaça três conceitos que foram fundamentais para o sucesso da Internet: inovação, concorrência justa e liberdade de escolha dos consumidores [Berners-Lee 2010]. Em um mundo sem NR, um ISP poderia ter controle sobre quais serviços teriam mais chances de serem consumidos pelos usuários e quais serviços teriam maior chance de serem bem sucedidos [van Schewick and Farber 2009].

A inovação em uma Internet não-neutra seria conduzida pelos ISPs e pelas grandes corporações [van Schewick and Farber 2009], as quais teriam recursos suficientes para ter seus dados priorizados. Novos serviços e soluções inovadoras encontrariam dificuldades para obter sucesso, já que não teriam capacidade de competir em iguais condições com os serviços já bem estabelecidos no mercado [Guo and Easley 2016, Cooper and Brown 2015]. Por outro lado, os mais conservadores afirmam que a falta de controles restritivos adicionais sobre os ISPs configura um mercado mais competitivo [Joch 2009]. Portanto, garantir que a Internet continue a ser um ambiente que fomente inovação é o tema central do debate da NR [Weitzner 2008].

Entretanto, apenas a existência das normatizações da NR não garante que os

ISPs irão respeitá-las. Além disso, podem haver práticas discriminatórias não previstas pelas normatizações [Knutson and Ramachandran 2016]. Assim, é importante a criação de soluções que auxiliem na fiscalização das normatizações da NR, aumentando a transparência das práticas de gerência de tráfego empregadas pelos ISPs. Estas soluções devem detectar a ocorrência de violações da NR, ou seja, a presença de práticas de DT.

Porém, a detecção de DT ainda é um desafio [Tariq et al. 2009]. Uma das dificuldades encontradas deve-se às diversas diferentes formas que ISPs podem implementar a DT. Um tráfego pode ser discriminado baseado no protocolo utilizado, no destino, origem ou conteúdo das mensagens, por exemplo. Além disso, diversas técnicas podem ser empregadas, como engenharia de tráfego (*traffic shaping*), diferentes rotas internas e vigilância de tráfego (*traffic policing*). Outro desafio é descobrir em qual ISP entre a origem e o destino do tráfego a diferenciação está ocorrendo, já que não se tem nenhum conhecimento prévio sobre a estrutura interna da rede. Além disso, diversos outros fatores além da DT podem afetar o desempenho de um tráfego de dados na Internet, como congestionamento, tráfego de fundo e balanceamento de carga, os quais podem ser mal interpretados como DT.

Este minicurso tem como objetivo principal apresentar soluções existentes para a detecção de DT. São apresentados a definição do problema, as técnicas utilizadas pelas soluções existentes, assim como o funcionamento, requisitos e limitações de cada solução. Além disso, o minicurso também apresenta uma visão geral do debate em torno da NR e das normatizações já implantadas no Brasil e em diversos países do mundo. A maioria das soluções existentes para detecção de DT são baseadas em medições de rede e inferência estatística. Em geral, estas soluções efetuam medições a partir de um ou diversos *hosts* e utilizando diferentes tipos de tráfego. Os dados obtidos são então comparados para inferir se houve ou não uma diferença significativa entre conjuntos diferentes de medições. Modelos estatísticos robustos são necessários para diferenciar variações causadas por DT das causadas por outros fenômenos, como congestionamento, entre outros. Dentre as soluções descritas neste minicurso, diversas geram tráfegos artificiais, correspondentes a diferentes aplicações entre dois *hosts* e comparam o desempenho fim-a-fim destes tráfegos. Já outras soluções obtém medições a cada *hop* do caminho entre os *hosts*, com o objetivo de identificar exatamente onde a DT ocorre. Há ainda soluções que capturam passivamente os tráfegos de diferentes aplicações, comparando-os posteriormente.

O restante deste minicurso está organizado da seguinte maneira. Primeiramente, apresentamos na seção 4.2, como motivação do trabalho, uma linha do tempo com diversos casos reais de violações da NR ocorridos em vários lugares do mundo nos últimos anos. Em seguida, a seção 4.3 apresenta uma visão geral do debate sobre a NR e das normatizações ao redor do mundo. A seção 4.4 apresenta uma fundamentação sobre como a DT é empregada na Internet e define o que é uma rede neutra e o problema de detecção de DT. A seção 4.5 descreve diversas soluções já existentes para o problema, seus requisitos e limitações. São apresentadas também uma comparação destas soluções e as diversas técnicas que podem ser utilizadas na detecção de DT, extraídas das soluções existentes. Concluímos então o minicurso na seção 4.6.

4.2. Casos Reais de Violações da NR

Denúncias de casos de violações da NR tornam-se cada vez mais comuns à medida que cresce a quantidade de usuários da Internet e cada vez mais países implementam a NR em seus territórios, fomentando o debate sobre o tema. Esta seção apresenta, em ordem cronológica, diversos casos reais de violações da NR ao redor do mundo. Estes casos consistem não apenas de trabalhos científicos, mas também de denúncias de usuários e da imprensa.

Começamos por um caso típico de violação da NR por meio do bloqueio de páginas Web. Em 21 de julho de 2005, os membros do sindicato canadense dos trabalhadores de telecomunicações, a *Telecommunications Workers Union* (TWU), entraram em greve contra a Telus, um ISP do país. Em 22 de julho (dia seguinte), a operadora Telus bloqueou o acesso de seus usuários à página Web *Voices for Change*, dirigida por e para os membros da TWU, alegando que o seu contrato de serviço com os usuários lhe permitia bloquear qualquer página Web [Austen 2005]. Em 28 de julho, a operadora Telus libera novamente o acesso à página Web após receber uma liminar.

Em 24 de julho de 2007, foi lançada a ferramenta Web Tripwires, que detecta modificação de conteúdo em páginas Web [Reis et al. 2008]. Os dados coletados nos primeiros 20 dias de funcionamento da ferramenta mostraram que ISPs provocaram mudanças intencionais no tráfego de 46 dos 50171 *hosts* medidos, entre outros resultados.

Também em 2007, em um fórum de discussões da página Web DSLReports [Topolski 2007], Topolski relata que a operadora Comcast utilizou equipamentos da Sandvine [Sandvine] para controlar sessões de comunicação de aplicativos P2P. Segundo Topolski, o equipamento da Sandvine verificava todos os pacotes que ingressam na rede da Comcast. Caso o tráfego de pacotes referentes a aplicativos P2P fosse maior que um limite estabelecido pelo ISP, o equipamento passava a interromper os fluxos de tais aplicativos. Topolski afirma que estas interrupções foram feitas por meio de pacotes forjados do tipo *reset* (RST) do protocolo TCP injetados no fluxo de comunicação dos aplicativos.

Em abril de 2009, Kendrick afirmou na página Web Gigaom [Kendrick 2009] que a operadora T-Mobile da Alemanha estava bloqueando o uso do aplicativo Skype em todas as suas redes, fato confirmado pela própria operadora. A operadora T-Mobile afirma que os motivos para bloquear todo tráfego VoIP em suas redes são apenas técnicos e não econômicos. Segundo a operadora, o elevado tráfego do aplicativo prejudicaria o desempenho da rede e caso o aplicativo passasse a não funcionar corretamente, os consumidores culpariam a T-Mobile.

Em junho de 2009, a *British Telecommunications* (BT), a empresa britânica de telecomunicações, foi acusada de degradar todo o tráfego de vídeos da página Web da emissora de TV britânica BBC, limitando a largura de banda máxima [Cellan-Jones 2009]. A BT alegou apenas que todas as suas práticas de gerência de tráfego buscam otimizar a experiência de todos os consumidores.

Em 2010, os autores em [Ling et al. 2010] apresentam os argumentos contra e a favor da NR, utilizando como exemplo o caso de bloqueio de serviços P2P efetuado pela operadora Comcast. Os autores afirmam que os serviços P2P não prejudicam a qualidade da Internet, apenas transferem a necessidade de investimento dos provedores de conteúdo

para os ISPs. Segundo os autores, o único dano causado pelos aplicativos P2P em uma rede neutra é aos ISPs, que não podem cobrar taxas extras de provedores de conteúdo para trafegar seus dados.

Em fevereiro de 2011 foi formada a GreatFire [GreatFire.org], uma organização sem fins lucrativos que monitora e publica o estado das páginas Web e palavras-chave censuradas na China por meio do chamado "Grande Firewall da China" (*Great Firewall of China*). A página Web da organização ajuda usuários chineses da Internet a acessar alguns conteúdos bloqueados, a testar suas conexões e publica os dados do monitoramento de páginas e palavras-chave bloqueadas. Dos 49720 domínios monitorados, por exemplo, 4329 são bloqueados na China, entre outras informações disponíveis.

Em abril de 2011, os autores da ferramenta CensMon [Sfakianakis et al. 2011], de detecção de censura, conduziram um experimento no PlanetLab. Foram utilizados 174 *hosts* do *testbed*, localizados em 33 países diferentes. A duração do experimento foi de 14 dias. Neste período a ferramenta testou 4950 endereços Web em 2500 domínios. Foram detectados 951 endereços e 193 domínios filtrados. A maior parte dos domínios bloqueados (176) foram detectados pelo *host* localizado na China.

A página Web europeia *Respect My Net* [Respect My Net] foi lançada em 22 de setembro de 2011. O objetivo desta página é permitir que usuários da Internet relatem violações da NR. A página contém uma lista de todos os casos relatados, com confirmações e provas fornecidas pelos usuários. Os casos não considerados como violações da NR – de acordo com as diretrizes da página – são removidos. A lista conta com um total de 219 relatos confirmados, que envolvem 18 países da Europa e 71 ISPs. Entre os casos relatados, três, tiveram um grande impacto: (i) degradação do tráfego do serviço YouTube na França, pelo ISP Free, com confirmação de 431 pessoas; (ii) bloqueio DNS à página Web *thepiratebay.org* na Bélgica, pela operadora Mobile Vikings, com confirmação de 18 pessoas; e (iii) bloqueio da porta 25 para todos os serviços SMTP pela operadora Belgacom, na Bélgica, com exceção do seu próprio serviço, com confirmação de 21 pessoas.

Em 2012 foi publicado um estudo sobre 2 casos de violações da NR utilizando a técnica de *Deep Packet Inspection* (DPI) nos E.U.A. e no Canadá [Mueller and Asghari 2012]. Nestes casos, ISPs destes países bloqueavam ou degradavam o tráfego de aplicativos P2P, gerando protestos, processos jurídicos, entre outros. O estudo descreve o impacto das práticas de DPI nos aspectos políticos e econômicos que envolvem a Internet (como inovação, competitividade e transparência, por exemplo). Os autores afirmam que utilizaram dados obtidos pela ferramenta Glasnost para o estudo.

Os autores da ferramenta Adkintun [Bustos-Jiménez et al. 2013], descrita mais à frente na seção 4.5, apresentam em [Bustos-Jiménez and Fuenzalida 2014] três casos referentes à utilização da ferramenta no Chile, entre os anos de 2011 e 2013. Em um destes casos, a ferramenta foi utilizada, a pedido do órgão regulador do país (SUBTEL), para avaliar o comportamento de dois ISPs chilenos, VTR e Movistar, que juntos controlam em torno de 80% dos serviços de banda larga no Chile. Os resultados mostraram que a velocidade de *download* durante o período da noite, para as duas operadoras, foi significativamente abaixo do contratado pelos usuários. No segundo caso, o canal estatal de televisão do país noticiou que o número de reclamações de usuários para a SUBTEL aumentou significativamente após o lançamento da Adkintun, assim como a qualidade de

serviço entregue pelos ISPs. O terceiro caso descrito trata de um processo contra a SUBTEL que acusa o órgão de não ter tomado medidas contra ISPs chilenos que não estavam cumprindo todas as exigências da Lei da NR. Esta acusação foi embasada nos dados coletados e publicados pela ferramenta Adkintun, mantida pela própria SUBTEL. Segundo os autores, este foi o primeiro caso no qual a infraestrutura de uma instituição governamental, voltada para garantir a NR, foi utilizada contra a mesma. Os autores afirmam ainda que a Adkintun foi totalmente implantada e tem coletado dados desde setembro de 2011 e já foi utilizado por mais de 10000 usuários.

A ferramenta HAKOMetar [Weber et al. 2013], descrita posteriormente na seção 4.5, foi utilizada por usuários finais na Croácia entre novembro de 2012 e março de 2013, período no qual o número total de medições excedeu 25000. Os resultados destas medições identificaram dezenas de casos em que largura de banda entregue aos usuários foi significativamente menor do que a contratada. Os autores relatam que estas medições motivaram reclamações dos usuários contra 3 das 16 operadoras medidas. Os dados obtidos pela HAKOMetar foram anexados a estas reclamações, as quais tiveram resultados positivos para os usuários.

Em 2013, Anderson descreve um estudo sobre a degradação de tráfego BitTorrent no Irã [Anderson 2013]. Foram analisados dados coletados por diversos clientes utilizando a ferramenta *Network Diagnostic Tool* (NDT), hospedada na plataforma de medição M-Lab. Os resultados da análise indicaram a presença de dois períodos longos em que houve degradação do tráfego BitTorrent. Entre 30 de novembro de 2011 e 15 de agosto de 2012 houve uma diminuição de 77% na taxa de transferência. Já entre 4 de outubro e 22 de novembro de 2012 a diminuição detectada foi de 69%.

Em 24 de junho de 2013, leitores do jornal *online Zambianwatchdog.com*, da Zâmbia, relataram terem recebido apenas mensagens de erro ao acessar a página Web [Mr T. 2013]. O jornal é considerado a maior página Web na Zâmbia após o Facebook, Google e YouTube. Foram executados testes com a ferramenta Ooni, os quais revelaram que a página era a única sendo bloqueada pelo governo do país.

A dissertação de mestrado de Shadi Esnaashari [Esnaashari 2014] apresenta a ferramenta *Web Censorship Monitoring Tool* (WCMT) utilizada entre julho e setembro de 2013 para identificar bloqueio de acesso a páginas Web e serviços da Internet na rede de diferentes organizações e ISPs em Wellington, na Nova Zelândia. Os resultados mostraram que todas as organizações e ISPs avaliados efetuaram bloqueio de algum conteúdo. Porém, houve uma variedade grande de conteúdos diferentes bloqueados em redes diferentes. O autor afirma que isto demonstra a falta de critérios das organizações ao definir o que deve ser bloqueado.

Shankesi propõe em 2013 na sua tese de doutorado, uma infraestrutura para detecção de manipulação de rede chamada Friendsourcing [Shankesi 2013]. O Friendsourcing baseia-se em colaboração coletiva (*crowdsourcing*), utilizando redes sociais para que um usuário receba auxílio de seus contatos para detectar se sua rede está sofrendo algum tipo de manipulação. O autor conduziu experimentos com 54 usuários reais na Índia. Os resultados mostraram que 64 endereços Web foram bloqueados por vários ISPs na Índia.

Em fevereiro de 2014, um usuário do fórum de discussões Reditt relatou um caso

de degradação de tráfego quando conectado em uma VPN utilizando a porta padrão do serviço OpenVPN [reddit 2014]. O usuário afirmou que, caso utilizasse outra porta, seu tráfego não era degradado. Diversos outros usuários confirmaram a denúncia. Também em 2014, Brodkin relata que a velocidade média de transferência no serviço Netflix teve uma queda nos últimos três a quarto meses na rede dos ISPs Verizon e Comcast [Brodkin 2014].

Em 1 de fevereiro de 2016, van Schewick envia ao Presidente da *Federal Communications Commission* (FCC) – o órgão regulador das telecomunicações nos E.U.A. um relatório no qual aponta que o serviço Binge On da operadora T-Mobile viola a NR, prejudicando a liberdade de escolha do usuário, a inovação, a concorrência e a liberdade de expressão na Internet [van Schewick 2016]. Segundo a autora, em novembro de 2015 a operadora T-Mobile, o terceiro maior provedor de acesso à Internet móvel nos EUA, lançou um novo serviço chamado Binge On no qual oferece transferência de vídeo ilimitada de provedores selecionados. Assim, os clientes podem acessar vídeos de 42 provedores, como Netflix, Amazon, Hulu, HBO, entre outros, sem o uso dos seus planos de dados, uma prática conhecida como "taxa zero". A autora afirma que esta prática configura um caso de DT, pois o ISP está favorecendo um conjunto de serviços em detrimento de outros. Já em 7 de fevereiro de 2016, a operadora Verizon é também acusada de violar a NR pela prática de "taxa zero" com seu serviço móvel de vídeo chamado Go90. Este serviço exclui o tráfego de vídeo da própria Verizon da franquia de dados de seus clientes [Lomas 2016].

Em 2 de março de 2016, a Public Knowledge, uma organização sem fins lucrativos que defende a NR e outros direitos do usuário na Internet, registrou uma queixa junto à FCC sobre o serviço Stream TV da operadora Comcast [Dreier 2016]. A denúncia diz que a Comcast não computa o tráfego do seu serviço Stream TV na franquia de dados de seus clientes, configurando assim a prática de "taxa zero" e, portanto, uma violação da NR. A Public Knowledge solicita então que a FCC interrompa o serviço discriminatório da operadora Comcast [Public Knowledge 2016].

Em 24 de março de 2016, o Netflix declarou que limita seu tráfego de vídeo em 600 Kbps para clientes acessando o serviço a partir de redes móveis [Knutson and Ramachandran 2016]. Segundo o Netflix, esta prática tem o objetivo de proteger seus clientes de cobranças adicionais por excederem suas franquias de dados. Em 25 de março de 2016, a *American Cable Association* (ACA) divulga uma declaração reprovando esta prática do Netflix [American Cable Association 2016]. Segundo a ACA, a FCC deve investigar os provedores de conteúdo e revisar sua regulamentação sobre a NR para incluir restrições também aos provedores de conteúdo e não somente aos ISPs. A FCC responde que, embora provedores de conteúdo não estejam incluídos na regulamentação da NR, a Netflix teve um comportamento que pode ser considerado incoerente. E conclui que esta revelação da Netflix põem em dúvida todo o fundamento e a razão de ser da decisão da NR [O'Rielly 2016].

Em 01 de abril de 2016, um grupo de mais de 50 organizações de interesse público e de defesa do consumidor pressionam a FCC para que tome medidas contra as práticas de "taxa zero" [Campbell 2016]. Segundo o grupo, estas práticas de ISPs como a Verizon, AT&T e T-Mobile, prejudicam a livre concorrência, a inovação, limitam a escolha do

usuário e elevam os preços.

A partir dos diversos casos apresentados, observa-se que houveram reclamações e estudos sobre violações da NR em diversos lugares do mundo e ao longo de todo o debate da NR. Assim, é possível afirmar que garantir o cumprimento da NR não é uma tarefa trivial, visto que diversos órgãos reguladores têm falhado em fiscalizar os ISPs.

4.3. Debate e Normatização Mundial da NR

Esta seção apresenta uma introdução ao debate da NR e descreve um panorama da normatização da NR em diversos países ao redor do mundo. Estas normatizações consistem em regras, princípios e/ou Leis instituídos com o objetivo de garantir um tráfego neutro na Internet. O processo de normatização da NR ocorreu de forma relativamente diferente ao redor do globo.

O debate mundial acerca da NR iniciou-se em 2002 quando a *Federal Communications Commission* (FCC), o órgão regulador das telecomunicações nos E.U.A, alterou a classificação do serviço de banda larga no país. O serviço anteriormente era equivalente a um serviço de telecomunicações comum, como a telefonia fixa, por exemplo. A nova classificação passou a ser de "serviço de informação" (*information service*) [Federal Communications Commission 2002], desvinculando a banda larga das leis que regulavam as telecomunicações. As leis que regem as telecomunicações garantiam uma Internet neutra no país. Assim, com a nova classificação, os ISPs ganharam o poder de priorizar ou bloquear um tipo de tráfego de dados em detrimento de outros. Neste contexto, inicia-se então o debate sobre a "Neutralidade da Rede", termo criado por Tim Wu [Wu 2002] ainda em 2002.

Em 2003, Tim Wu e Lawrence Lessig, um dos criadores da Creative Commons [Lessig 2001], enviaram uma carta à FCC apresentando uma proposta sobre a NR [Wu and Lessig 2003]. Esta proposta estabelecia um equilíbrio entre a proibição de ISPs em restringir o que os usuários fazem com suas conexões à Internet e a liberdade dos ISPs para gerenciar suas próprias redes.

A partir de então, cada vez mais indivíduos, empresas e instituições públicas e privadas passaram a fazer parte do debate da NR ao redor do planeta. Diversos provedores de conteúdo, como Google e Netflix, defendem a NR, enquanto a oposição é formada principalmente pelos ISPs. A comunidade científica mundial também ingressou no debate, trazendo conceitos, técnicas e outros aspectos relevantes que embasam as discussões e normatizações da NR ao redor do mundo.

Um conceito importante no debate da NR, e presente em diversas normatizações, é a gerência razoável do tráfego. O conceito da gerência razoável do tráfego determina quais práticas de gerência de tráfego os ISPs podem efetuar sem que a NR seja violada. A gerência de tráfego de um ISP pode ser considerada razoável se esta não for anticompetitiva, não causar danos indevidos aos consumidores e não prejudicar injustificadamente a liberdade de expressão [Jordan 2009b, Jordan 2009a].

Descrevemos abaixo, na subseção 4.3.1, em ordem cronológica, alguns dos pontos principais da normatização de diversos países.

4.3.1. Normatização Mundial da NR

Em 19 de setembro de 2006, o Japão, por meio do Ministério de Assuntos Internos e Comunicações (MIC), lança um programa (*New Competition Promotion Program 2010*) [Ministry of Internal Affairs and Communications 2006] que estabelece uma série de medidas a serem implementadas até 2010. O objetivo destas medidas é garantir a concorrência justa no mercado de telecomunicações e assegurar os direitos do consumidor. Este programa criou um grupo de trabalho para estudar o tema da NR e como ela deve ser implementada no país. Este grupo de trabalho apresentou o seu primeiro relatório em 20 de setembro de 2007 [Ministry of Internal Affairs and Communications 2007] e, em 07 de março de 2008, apresentou um segundo relatório [Ministry of Internal Affairs and Communications 2008] contendo recomendações para a manutenção da NR. Estas recomendações incluem: estudos sobre o mercado de telecomunicações e a utilização da infraestrutura de rede disponível; a criação de sistemas para fiscalizar a qualidade de serviço fornecida pelos ISPs; e o estabelecimento de regras que garantam um tráfego neutro, permitam novos modelos de negócio e protejam os usuários.

A Noruega lançou em 24 de fevereiro de 2009 suas diretrizes para a NR por meio de seu órgão regulador, o *Norwegian Communications Authority* (Nkom) [Norwegian Communications Authority a]. Estas diretrizes estabelecem que os usuários devem receber dos ISPs exatamente o serviço contratado, sem discriminação ou bloqueio de conteúdo. A Nkom também afirma que o modelo norueguês da NR [Norwegian Communications Authority b] busca mediar os interesses dos provedores de conteúdo, provedores de acesso e consumidores. Em 18 de novembro de 2014, Frode Sørensen, conselheiro sênior da Nkom, afirma que a prática de "taxa zero" viola as diretrizes norueguesas da NR [Sørensen 2014]. Nesta prática, o tráfego de um aplicativo específico não é considerado na franquia de dados do consumidor. Assim, segundo Sørensen, esta prática configura um caso de discriminação de tráfego, já que, caso o consumidor tenha utilizado toda a sua franquia, tal aplicativo não tem seu tráfego bloqueado ou estrangulado como acontece com os demais.

Em 21 de outubro de 2009, o Canadá, por meio da *Canadian Radio-television and Telecommunications Commission* (CRTC), publicou sua regulamentação em relação às práticas de gerência do tráfego da Internet empregadas pelos ISPs [Canadian Radio-television and Telecommunications Commission 2009]. A regulamentação estabelece que toda gerência de tráfego deve ser feita de forma transparente e sem discriminação, e que os ISPs devem manter investimentos na rede como a principal solução para evitar congestionamentos.

Em 18 de agosto de 2010, o governo do Chile decretou a Lei n. 20.453 [Subsecretaría de Telecomunicaciones 2010] que instituiu a NR no país. A Lei estabelece regras para órgãos públicos e empresas privadas que fornecem serviços de telecomunicações. Estas regras proíbem o bloqueio, interferência ou discriminação no acesso dos usuários a qualquer conteúdo legal, quaisquer que sejam os equipamentos utilizados, desde que não prejudiquem a rede. A Lei também exige que os provedores de acesso à Internet publiquem todas as características dos serviços prestados (largura de banda, disponibilidade, garantias, entre outros) e forneçam aos consumidores serviços de controle parental para filtrar conteúdos ilegais ou que os consumidores julguem impróprios.

Em 16 de novembro de 2011, a Secretaria Nacional de Telecomunicações do Chile (SUBTEL) afirma que os ISPs não estão fornecendo as informações exigidas por lei de forma suficientemente transparente e padronizada [Subsecretaría de Telecomunicaciones 2011]. Assim, a SUBTEL padronizou as informações que devem ser publicadas pelos ISPs, a fim de que os consumidores possam facilmente comparar os diferentes provedores de acesso. Em 27 de maio de 2014, a SUBTEL, com base na Lei de NR, proíbe a pratica de "taxa zero", sob pena de multa [Subsecretaría de Telecomunicaciones 2014]. Assim, os ISPs do Chile não podem mais comercializar serviços que incluem as chamadas "redes sociais gratuitas".

Em 16 de junho de 2011, o governo da Colômbia aprovou a Lei 1.450 referente ao Plano Nacional de Desenvolvimento para os anos de 2010 a 2014 [El Congreso de Colombia 2011]. O Art. 56 desta Lei trata da "Neutralidade na Internet", estabelecendo regras para os prestadores de serviço de Internet. Estas regras proíbem o bloqueio, modificação e discriminação de qualquer tráfego na rede, além de exigir que os ISPs publiquem todas as características dos serviços prestados. A Lei também exige que os ISPs forneçam serviços de controle parental aos consumidores e que implementem mecanismos para preservar a privacidade dos usuários. Em 16 de dezembro de 2011, o governo publica a Resolução 3502, que define regras para o cumprimento da NR estabelecida no Art. 56 da Lei 1.450, aprovada anteriormente [Comisión de Regulación de Comunicaciones 2011]. Estas regras tratam dos princípios e aspectos técnicos referentes à NR que devem ser seguidos. Estes princípios incluem: a livre escolha do usuário ao utilizar a rede, tráfego sem discriminação, transparência na gerência de tráfego e informação quanto aos serviços prestados pelos ISPs. Também são definidas quais práticas de gerência de tráfego são permitidas.

Em 3 de julho de 2012, a *Korea Communications Commission* (KCC), agência reguladora das telecomunicações da Coréia do Sul, publicou seu relatório anual referente ao ano de 2011 [Korea Communications Commission 2012]. Neste relatório, a KCC estabelece as diretrizes a serem seguidas para implementar a NR no país. Estas diretrizes proíbem o bloqueio e discriminação de tráfego e garantem direitos do consumidor como a transparência sobre as práticas de gerência adotadas pelos ISPs e as características dos serviços fornecidos, entre outros. O documento também define quais práticas de gerência de tráfego são aceitáveis, sem que a NR seja violada.

O debate sobre a NR no Brasil iniciou em 2009, quando o Comitê Gestor da Internet no Brasil (CGI.br), o órgão responsável pela governança da Internet no país, lança uma Resolução com os 10 Princípios para a Governança e Uso da Internet no Brasil [Comitê Gestor da Internet no Brasil 2009], o qual inclui a NR. A partir destes princípios iniciou-se um processo colaborativo que resultou no Projeto de Lei 2126/2011 [Poder Executivo 2011], apresentado em 24 de agosto de 2011, o qual torna-se Lei Ordinária 12965/2014 em 23 de abril de 2014, o chamado "Marco Civil da Internet" [Presidência da República 2014]. A Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. A NR é tratada no Artigo 9º desta Lei, estabelecendo que ISPs tem o dever de tratar todo pacote de dados da mesma forma, sem nenhum tipo de DT. A Lei ainda estabelece que a DT poderá ocorrer em casos especiais a serem regulamentados posteriormente pelos órgãos reguladores competentes, desde que seja transparente e não cause danos ao usuário. A regulamentação da Lei é decretada em 11 de maio de 2016 [Presidência da República 2016], com base em consultas públicas [Ministério da Justiça]. Quanto

à NR, esta regulamentação trata dos casos especiais em que a discriminação de tráfego é permitida e estabelece parâmetros para a fiscalização de violações. Em particular, a regulamentação proíbe as práticas de "taxa zero".

Em 14 de julho de 2014, o governo mexicano alterou a Lei Federal de Telecomunicações e Radiodifusão [Secretaria de Comunicaciones y Transportes 2014], incluindo itens que instituem a NR no México. Estes itens estabelecem que ISPs não podem bloquear, discriminar nem modificar qualquer conteúdo legal acessado pelos usuários e devem preservar a privacidade dos mesmos. A Lei também passa a exigir que ISPs mantenham uma qualidade mínima de serviço, sempre fornecendo aos usuários exatamente o que consta em contrato e mantendo públicas todas as características dos serviços oferecidos. Além disso, permite aos ISPs práticas de gerência de tráfego que tenham como objetivo garantir a qualidade ou a velocidade do serviço contratado pelo usuário, desde que isto não configure uma prática contrária à livre concorrência.

A NR foi instituída nos E.U.A. em 26 de fevereiro de 2015, pela FCC [Federal Communications Commission 2015]. Entretanto, o debate sobre a NR nos E.U.A iniciou em 2002, quando o orgão alterou a classificação do serviço de banda larga no país, como descrito acima. Em 5 de agosto de 2005, a Suprema Corte concordou com a posição adotada em 2002 pela FCC, de que o serviço de banda larga é um serviço de informação [Federal Communications Commission 2005]. Em 21 de dezembro de 2010, a FCC adota três regras básicas para preservar a Internet como uma plataforma aberta para a inovação, o investimento, a criação de emprego, o crescimento econômico, a concorrência e a livre expressão [Federal Communications Commission 2010]: a transparência (*Transparency*), nenhum bloqueio (*No blocking*) e nenhuma discriminação não razoável (*No unreasonable discrimination*). Em 14 de janeiro de 2014, estas três regras adotadas pela FCC em 2010 são julgadas pela Corte de Apelação do Distrito de Columbia. Como resultado do julgamento, esta Corte de Apelação sanciona a regra da transparência, mas anula as regras de não bloqueio e de discriminação não razoável, por considerar que não são práticas ilícitas quando classificadas em "serviços de informação" [Federal Communications Commission 2014]. Assim, somente na regulamentação de 26 de fevereiro de 2015 [Federal Communications Commission 2015] a FCC volta a classificar o serviço de acesso à Internet como um serviço de telecomunicações, o que lhe garante o fundamento jurídico necessário para preservar e proteger a Internet aberta. Dentre as regras estabelecidas destaca-se que os ISPs não podem bloquear nem degradar pacotes de dados, independente de sua origem, destino e conteúdo. Também fica proibida a chamada "priorização paga", que ocorre quando um ISP aceita pagamento (monetário ou não) para gerenciar sua rede de forma a beneficiar um determinado conteúdo, aplicação, serviço ou dispositivo. Desde a adoção destas regras, a FCC vem sofrendo pressão dos opositores, como por exemplo: em 25 de fevereiro de 2016, um projeto de Lei é proposto para proibir a FCC de reclassificar o serviço de banda larga e de impor regras sobre os prestadores de tal serviço [Lee 2016]; em 11 de abril de 2016, o presidente da FCC, Tom Wheeler, afirma que a política de "taxa zero" está sendo revista e que não há uma data final definida [Federal Communications Commission 2016]; e em 15 de abril de 2016, a Câmara dos Deputados dos Estados Unidos aprovou, com apoio bipartidário, uma Lei que proíbe a FCC de regular as taxas cobradas pelo acesso à Internet de banda larga [Kinzinger 2016].

Em 30 de junho de 2015, a Comissão Europeia publicou uma nova regulamen-

tação que institui a NR em todos os países da União Europeia [European Commission 2015]. Esta regulamentação foi resultado de anos de negociação entre a Comissão Europeia, o Parlamento Europeu e o Conselho Europeu, além de consultas públicas [European Commission 2009, European Commission 2010, European Commission 2014]. A regulamentação estabelece que não pode haver bloqueio, degradação e discriminação de nenhum conteúdo, aplicação ou serviço na Internet. O estabelecimento de diretrizes para a implementação e fiscalização desta regulamentação ficou a cargo do *Body of European Regulators of Electronic Communications* (BEREC), agência reguladora das telecomunicações da União Europeia criada em 25 de novembro de 2009 [European Parliament and Council of the European Union 2009, Body of European Regulators for Electronic Communications].

Em 8 de fevereiro de 2016, o órgão regulador das telecomunicações da índia, a *Telecom Regulatory Authority of India* (TRAI), publicou um regulamento [Telecom Regulatory Authority of India 2016] proibindo a "taxa zero" e a cobrança de taxas extras dos provedores de conteúdo e dos usuários que acessem conteúdos específicos. Estas práticas estavam sendo implantadas por um ISP indiano, o que fomentou o debate sobre a NR no país [Press Trust of India 2015].

Este panorama global da normatização da NR mostra que existe uma preocupação dos governos ao redor do mundo com a manutenção de uma Internet neutra. Outros países tem discutido a NR, como a Nova Zelândia [InternetNZ 2015] e a Rússia [Federal Antimonopoly Service 2016], por exemplo, mas não foram encontrados documentos indicando que a NR já tenha sido instituída nestes países. Com base neste panorama, é possível extrair aspectos comuns às diversas normatizações. A DT está presente em todas as normatizações, tornando-a assim um elemento chave no contexto da NR.

4.4. Fundamentação

Esta seção apresenta uma fundamentação sobre a DT, a NR e o problema de detecção de DT. A subseção 4.4.1 trata da DT, apresentando conceitos relacionados à organização e funcionamento da Internet e de que forma a DT pode ser implementada. A subseção 4.4.2 apresenta uma definição da NR e as propriedades que uma rede neutra deve ter. Finalmente, na subseção 4.4.3, o problema de detecção de DT é definido.

4.4.1. Diferenciação de Tráfego

A Internet é uma rede global formada pela interconexão de diversas redes independentes, chamadas de Sistemas Autônomos (*Autonomous Systems*, ASes). Cada AS representa um conjunto diferente de prefixos de roteamento na Internet e é controlado por um ou mais ISPs. Os ISPs são hierarquicamente divididos em três camadas, chamadas *Tiers*. Os ISPs do *Tier* 1 são redes de alta capacidade que interconectam globalmente as redes dos ISPs *Tier* 2, constituindo o "núcleo" da Internet. ISPs *Tier* 2 fornecem conectividade aos ISPs *Tier* 3, que são, por exemplo, os ISPs residenciais, os quais fornecem acesso à Internet para os consumidores finais.

Um pacote de dados enviado de um *host* final para outro, potencialmente pode atravessar ASes de ISPs de todas os *Tiers*, especialmente se os *hosts* estiverem geograficamente distantes. Assim, a DT pode ocorrer em qualquer uma dos *Tiers* e de inúmeras

formas, já que cada AS pode empregar tecnologias diferentes, assim como políticas internas de roteamento e gerência de tráfego distintas.

Pacotes de dados em um AS qualquer atravessam diversos roteadores deste AS, desde o ponto de entrada (o primeiro *hop*) até o ponto de saída (o último *hop*). Ao sair de um AS, um pacote de dados entrará na rede de outro ou terá chegado em seu destino. Assim, uma possível DT praticada por um ISP acontecerá em um ou diversos *hops* entre o ponto de entrada e o ponto de saída do AS.

Em geral, o tráfego é segmentado em classes e tratado de forma diferente conforme a classe atribuída. Existem inúmeros mecanismos que podem ser utilizados para classificar e posteriormente discriminar um tráfego de dados. A classificação de um tráfego de dados pode ocorrer, por exemplo, apenas no ponto de entrada da rede e ser inserida no cabeçalho dos pacotes (cabeçalho do protocolo interno do AS), informando os roteadores seguintes como estes pacotes devem ser tratados. É possível também que todos os roteadores, por onde os pacotes de um tráfego de dados passam, efetuem tanto a classificação quanto a discriminação em si. Técnicas de Redes Definidas por Software (*Software-Defined Networking, SDN*) também podem ser utilizadas [Qazi et al. 2013]. As possibilidades de implementação são diversas.

A classificação de um tráfego de dados pode basear-se em diversos critérios, como origem, destino, porta de origem, porta de destino, protocolo de aplicação, AS anterior (de onde o pacote veio) ou próximo AS (para o qual o pacote será roteado), entre outros. Há ainda a técnica *Deep Packet Inspection* (DPI), que consiste em analisar não apenas o cabeçalho dos pacotes, mas também os dados (*payload*). O objetivo do DPI é identificar com maior acurácia a qual aplicação correspondem os pacotes.

Os mecanismos mais comuns de DT são engenharia de tráfego (*traffic shaping*) [Kanuparthy and Dovrolis 2011] e vigilância de tráfego (*traffic policing*) [Flach et al. 2016]. Outros exemplos incluem: a injeção de pacotes TCP do tipo *reset* (RST) forjados, a fim de forçar o encerramento de conexões TCP, interrompendo a comunicação entre dois *hosts* finais; o encaminhamento de pacotes para rotas diferentes conforme a sua classificação, sendo que uma das rotas é propositalmente menos congestionada, configurando assim uma *fast-lane*; *middleboxes* [Detal et al. 2013], os quais podem interferir no tráfego entre dois *hosts* finais; Redes de Distribuição de Conteúdo (*Content Delivery Networks*, CDN) [Maille et al. 2016], as quais cobram para entregar conteúdo de terceiros, podendo assim caracterizar uma priorização.

A engenharia e a vigilância de tráfego são efetuadas, em geral, por equipamentos dedicados ou pelos próprios roteadores da rede de um AS. Estes mecanismos diferem na forma com que os pacotes são processados conforme chegam nos roteadores ou outros equipamentos.

A engenharia de tráfego baseia-se no enfileiramento de pacotes em *buffers*. Idealmente, um pacote de dados, ao chegar em um roteador, é imediatamente encaminhado para o próximo *hop* de sua rota – a qual, em geral, é decidida por meio de uma tabela de roteamento. Porém, caso o roteador esteja sobrecarregado e não consiga encaminhar o pacote imediatamente, o pacote é colocado em um *buffer*. Uma política de escalonamento é então empregada para decidir a ordem em que os pacotes pendentes serão retirados do

buffer e encaminhados. Caso o *buffer* fique cheio, uma política de descarte é empregada, descartando os novos pacotes que chegarem ou até mesmo pacotes já presentes no *buffer*.

Já a vigilância de tráfego emprega políticas de descarte assim que pacotes em excesso começam a chegar, diferentemente da engenharia de tráfego que as emprega apenas quando o *buffer* está cheio. Assim, a vigilância de tráfego não baseia-se no enfileiramento de pacotes, já que estes são descartados antes que acumulem.

As políticas de escalonamento de pacotes mais comuns são [Kanuparthy and Dovrolis 2010, Weinsberg et al. 2011]: (i) *First Come First Served* (FCFS), em que os pacotes que chegaram primeiro são escalonados primeiro; (ii) *Strict Priority* (SP), em que o escalonador sempre dá prioridade para uma classe específica; (iii) *Leaky Bucket*, em que cada classe tem um limite máximo de largura de banda; (iv) *Token Bucket*, em que cada classe tem um limite para a largura de banda média consumida pelos fluxos; e (v) *Weighted Fair Queuing* (WFQ), em que a largura de banda permitida para cada classe é dividida com base em pesos. Já as políticas de descarte mais comuns são: (i) *Drop-Tail* (DT), no qual em caso de *buffer* cheio os próximos pacotes a chegarem são descartados e *Weighted Random Early Detection* (WRED), em que pacotes de menor prioridade tem maior probabilidade de serem descartados.

4.4.2. Rede Neutra

O projeto original da Internet foi guiado por dois princípios fundamentais que são elementos-chave no contexto da NR [Krämer et al. 2013]: fim-a-fim (*end-to-end*) e melhor esforço (*best-effort*). O princípio fim-a-fim diz que as mensagens são fragmentadas em pacotes de dados que devem ser roteados através da rede de forma autônoma. Um *hop* intermediário (roteador) deve decidir apenas qual será o próximo *hop* para um pacote qualquer, enviando-o pelo menor caminho segundo sua tabela de roteamento. Assim, um roteador não tem controle do caminho completo que o pacote percorre da origem até o destino final. Já o princípio do melhor esforço garante que todos os pacotes de dados serão enviados pela rede tão rápido quanto possível. Se a taxa de chegada de pacotes em um roteador é maior que sua capacidade de envio, os pacotes serão enfileirados. Se a fila de pacotes encher, os próximos pacotes a chegar serão descartados, independentemente dos seus conteúdos, origens ou destinos.

No contexto da NR, estes princípios estabelecem que todos os pacotes de dados enviados pela rede devem ser tratados com igualdade e que nenhum *hop* intermediário pode exercer controle sobre a rede como um todo. Entretanto, não há uma definição amplamente aceita da NR, havendo algumas diferenças [Hahn and Wallsten 2006, Internet Society , Scott 2014, Ganley and Allgrove 2006, Crowcroft 2007]. Um conceito comum aos diversos trabalhos, normatizações e princípios fundamentais da Internet trata da DT. Assim, neste trabalho consideramos que para uma rede ser considerada neutra, todo pacote de dados deve ser tratado da mesma forma, ou seja, a DT não é permitida.

Portanto, em uma rede neutra, os roteadores de um ISP devem escalonar os pacotes a serem encaminhados seguindo a política FCFS (*First Come First Served*) e a política de descarte de pacotes deve ser DT (*Drop-Tail*) [Kanuparthy and Dovrolis 2010]. O próximo pacote a ser encaminhado é sempre o que chegou antes e em caso de *buffer* cheio os próximos pacotes a chegarem são descartados, independentemente da classifi-

cação. Assim, todo tipo de tráfego está sujeito às mesmas condições de atraso e perdas.

4.4.3. O Problema de Detecção de DT

O problema de detecção de DT tratado neste trabalho é defino como: inferir se um tráfego de dados está sendo tratado de forma diferente de outro(s) tráfego(s). Em outras palavras, o problema consiste em detectar se pacotes de diferentes tráfegos estão sujeitos a diferentes tratamentos de rede, apenas por terem propriedades distintas (gerados por aplicações diferentes, por exemplo).

4.5. Soluções para Detecção de Diferenciação de Tráfego

Segundo o *Body of European Regulators of Electronic Communications* (BEREC), a associação das agências reguladoras das telecomunicações da União Europeia, apenas a normatização da NR não garante seu cumprimento por parte dos ISPs. É importante que os usuários finais tenham conhecimento dos serviços efetivamente oferecidos a eles pelos ISPs contratados [Body of European Regulators for Electronic Communications 2012a, Body of European Regulators for Electronic Communications 2012b]. Assim, soluções para detectar possíveis práticas de DT são necessárias. Esta seção apresenta diversas soluções já existentes para o problema da detecção de DT, assim como um apanhado das técnicas utilizadas por estas soluções.

A DT pode afetar um tráfego de dados de diversas formas. Mecanismos de engenharia de tráfego, por exemplo, podem resultar em atrasos maiores para o tráfego discriminado. Já a vigilância de tráfego pode resultar em maiores taxas de perda de pacotes. Caso pacotes de diferentes tipos sejam encaminhados por rotas diferentes, estes podem apresentar um desempenho de rede diferente se uma das rotas está congestionada e a outra não. Assim, as soluções existentes para detecção de DT utilizam medições de rede para detectar estas diferenças de desempenho e inferir se um determinado tipo de tráfego está sendo discriminado em relação a outros.

Porém, diversos outros fatores além da DT podem resultar em uma diferença no desempenho medido para tipos de tráfegos diferentes – as chamadas variáveis de confusão. Exemplos incluem diferença de rotas, tráfego de fundo, mudanças constantes nas condições da rede, congestionamento, configuração dos *hosts* finais, além das próprias limitações das técnicas de medição utilizadas. Assim, modelos estatísticos robustos são necessários para se obter resultados confiáveis [Tariq et al. 2009].

As medições de rede efetuadas pelas soluções podem ser ativas ou passivas. Em uma medição ativa, as medições são obtidas a partir de tráfegos de dados artificiais entre um ou mais pares de *hosts*. Já na medição passiva, as medições são obtidas apenas observando-se tráfegos de dados reais, sem introduzir novos pacotes na rede. No caso da DT, dependendo de qual métrica esteja sendo utilizada, é possível que diferenças significativas nas medições para tráfegos diferentes sejam observáveis apenas quando a rota entre os *hosts* estiver congestionada. Assim, medições ativas, em geral, criam uma grande quantidade de tráfego para saturar a banda disponível no caminho entre dois *hosts* finais, forçando que atrasos e/ou perdas de pacotes aconteçam. As principais métricas utilizadas na soluções descritas nesta seção são: taxa de perda de pacotes, taxa de transferência e atraso.

As soluções apresentadas nesta seção diferem, em geral, na topologia de medição, nas métricas, nos modelos estatísticos e nos tipos de tráfegos de dados empregados nas medições. Diversas soluções efetuam medições ativas entre um ou mais pares de *hosts* – utilizando tráfegos correspondentes a aplicações diferentes – e comparam as medições obtidas a fim de detectar variações significativas. Outras soluções efetuam medições a cada *hop* do caminho entre um ou mais pares de *hosts*, com o objetivo de identificar exatamente onde a DT ocorre. Há ainda soluções que utilizam medições passivas de tráfegos de diferentes aplicações.

O restante desta seção está organizado da seguinte forma. As subseções 4.5.1 até 4.5.9 descrevem soluções que detectam DT. A subseção 4.5.10 apresenta um resumo comparativo das soluções. Na subseção 4.5.11, outros trabalhos relacionados à NR, mas que não se referem diretamente à detecção de DT, são apresentados.

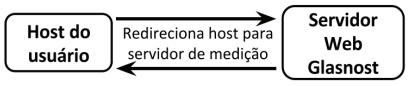
4.5.1. Glasnost, BTTest e BonaFide

Glasnost [Dischinger et al. 2010] é uma ferramenta que permite a usuários finais da Internet detectarem se seus ISPs estão praticando DT baseado nas aplicações em uso. O sistema já foi utilizado por milhares de usuários ao redor do mundo, incluindo usuários residenciais sem conhecimento técnico. A ferramenta foi inicialmente aplicada para detecção de DT de BitTorrent, mas pode também ser utilizada para qualquer outro protocolo de aplicação.

A ferramenta Glasnost foi projetada para ser de fácil utilização por qualquer usuário, independentemente de seu conhecimento técnico. O funcionamento da Glasnost é ilustrado na Figura 4.1. Primeiramente o usuário acessa a página Web da ferramenta[1] e é redirecionado para um servidor de medição, como mostra a Figura 4.1a. Existem vários servidores de medição e os usuários são redirecionados dinamicamente para um destes servidores, tornando difícil para os ISPs empregarem medidas contra servidores específicos. O navegador do usuário obtém então a aplicação cliente da Glasnost, como ilustrado na Figura 4.1b. A aplicação cliente é um *applet* Java executado pelo navegador do usuário que conecta-se ao servidor de medição e emula uma sequência de fluxos de dados, efetuando os testes de taxa de transferência para diferentes aplicações, como mostra a Figura 4.1c. Cada teste é composto por dois fluxos de dados em sequência. Um destes fluxos corresponde à aplicação sendo testada, sendo constituído pelo protocolo e dados específicos da aplicação. O outro fluxo é idêntico ao primeiro em quantidade de mensagens, ordem e tamanho dos pacotes, porém com conteúdo definido de forma aleatória, servindo como um *baseline* para comparação com o fluxo da aplicação. A partir da medição da taxa de transferência dos diferentes fluxos, é possível detectar se um ISP está praticando DT baseada no conteúdo das mensagens, como descrito abaixo.

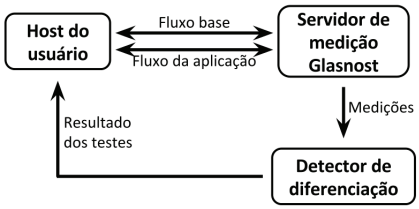
Cada fluxo de dados entre a aplicação cliente e o servidor de medição dura diversos segundos, tempo suficiente para que o TCP chegue a uma taxa de transferência estável. Os testes são repetidos múltiplas vezes, a fim de diminuir o ruídos nas medições obtidas. Ao término da série de testes, o servidor de medição processa os dados obtidos e mostra uma página de resultados ao usuário. As métricas computadas são o valor mínimo, máximo e a mediana das taxas de transferência medidas.

[1] `http://broadband.mpi-sws.org/transparency/glasnost.php`



(a) Usuário redirecionado para um servidor de medição.

(b) Obtenção da aplicação cliente.



(c) Execução de testes de taxa de transferência.

Figura 4.1: Funcionamento da ferramenta Glasnost.

Para detectar a DT, a Glasnost verifica se a diferença entre a taxa máxima de transferência dos dois fluxos de dados é maior que um limiar σ. Este limiar é um compromisso entre a capacidade de detectar DT e a produção de falso-positivos (falsas acusações de DT). Se o valor de σ for grande, como 50%, por exemplo, a ferramenta detecta DT apenas se a taxa máxima de transferência de um fluxo for metade da taxa máxima do outro fluxo. Por outro lado, se σ tiver um valor pequeno, 5%, por exemplo, a ferramenta pode erroneamente detectar DT quando houve apenas influência de algum tráfego secundário. Os autores afirmam que 20% é um bom valor para o limiar σ.

Os autores relatam que, em 2010, a Glasnost detectou que 10% dos seus usuários sofreram DT de BitTorrent. Dentre os casos detectados, a grande maioria ocorreu apenas no envio de dados (*upstream*), com poucos casos de DT detectados no recebimento (*downstream*) e 20% em ambos. Um resultado surpreendente é que, depois de concluir-se que um ISP estava praticando DT, apenas 21% dos usuários do ISP foram efetivamente afetados (mediana). Os autores listam 3 possíveis explicações para este cenário: (i) apenas usuários geradores de uma quantidade grande de tráfego foram afetados; (ii) apenas algumas partes do ISP foram afetadas; e (iii) a DT foi aplicada apenas durante períodos específicos, como horários de pico, por exemplo. Os autores também relatam que cerca de 6% dos usuários alegaram que a ferramenta não detectou DT que eles acreditavam estarem sofrendo. Uma possível explicação para isto é que a decisão de minimizar os falso-positivos pode aumentar os falso-negativos.

Uma ferramenta anterior à Glasnost, BTTest [Dischinger et al. 2008], foi criada por alguns dos autores da Glasnost e claramente serviu de base para a mesma. A BTTest detecta se um ISP está bloqueando tráfego BitTorrent. O funcionamento da BTTest é muito similar ao da Glasnost, exceto que a BTTest detecta apenas bloqueio de tráfego e apenas para BitTorrent. A BTTest foi disponibilizada por um período de 17 semanas, no qual mais de 47300 usuários finais utilizaram a ferramenta ao redor do mundo. Os dados obtidos neste período foram analisados e concluiu-se que em cerca de 8% dos testes foi detectado o bloqueio de tráfego BitTorrent, principalmente nos EUA. Além disso, a grande maioria dos bloqueios, cerca de 99%, ocorreu no envio de dados (*upstream*) e não

no recebimento (*downstream*).

Foi também desenvolvida posteriormente por outros autores outra ferramenta similar, BonaFide [Bashko et al. 2013]. BonaFide é uma adaptação da Glasnost focada em detectar DT em redes móveis. A ferramenta foi desenvolvida para o sistema Android e funciona de forma muito similar à Glasnost, mas com algumas modificações relacionadas às restrições presentes em dispositivos móveis. Na BonaFide, uma aplicação cliente executada no dispositivo móvel comunica-se com um servidor de medição executando assim os testes. Cada teste é constituído de 2 fluxos de dados, como na Glasnost. O BonaFide suporta diversos protocolos de aplicação, como VoIP e BitTorrent, por exemplo.

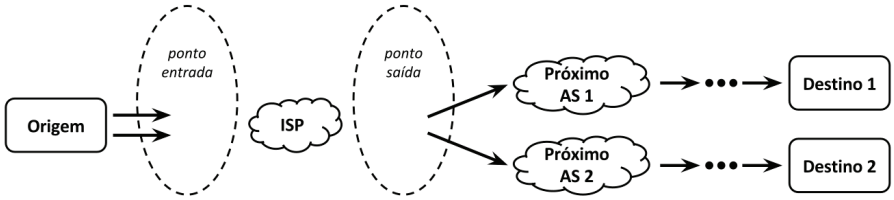
4.5.2. NetPolice e NVLens

NetPolice [Zhang et al. 2009] é uma ferramenta para detecção de DT em ISPs do "núcleo" da Internet (*Tier* 1). Os autores afirmam que detectar DT no núcleo tem impacto maior do que a detecção nos ISPs que atendem diretamente os usuários finais, já que a DT no núcleo potencialmente afeta uma quantidade maior de tráfego. A detecção de DT da NetPolice utiliza a taxa de perda de pacotes como métrica, que é medida a partir de diversos pontos de vista – *hosts* finais – em relação a um mesmo núcleo.

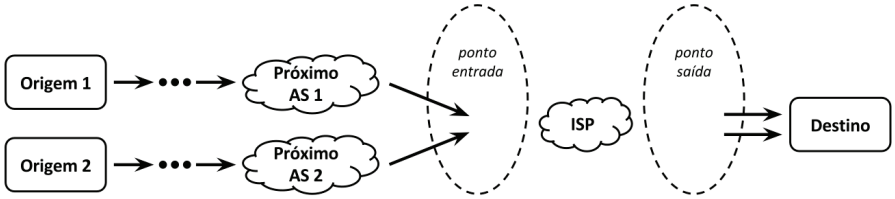
A NetPolice detecta DT baseada em conteúdo e em roteamento. A DT baseada em conteúdo ocorre quando os tráfegos gerados por diferentes aplicações são tratados de forma diferente, isto é, de acordo com a porta destino ou conteúdo dos pacotes, um ISP pode dar prioridade maior/menor aos mesmos ou até bloqueá-los. A DT baseada em roteamento ocorre quando pacotes são tratados de forma diferente dependendo dos seus dados de roteamento como, por exemplo, de qual AS veio o pacote ou para qual AS o pacote será encaminhado.

A Figura 4.2 mostra como a NetPolice detecta cada tipo de DT – baseada em conteúdo e roteamento. Na Figura 4.2a, as medições são feitas usando uma mesma origem e destinos diferentes, selecionados de forma que os *hops* imediatamente posteriores ao ponto de saída do ISP correspondam a ASes diferentes. Assim, é possível detectar se o ISP faz DT baseada no próximo AS para o qual o pacote será encaminhado. Na Figura 4.2b, as medições são feitas usando um mesmo destino e origens diferentes, selecionadas de forma que os *hops* imediatamente anteriores ao ponto de entrada do ISP sejam de ASes diferentes. Desta forma, é possível detectar se o ISP faz DT dependendo do AS anterior à sua rede. Na Figura 4.2c, as medições são feitas usando a mesma origem e destino, mas com pacotes de aplicações diferentes (porta destino e conteúdo). Assim, é possível detectar quando o ISP pratica DT baseada no conteúdo dos pacotes.

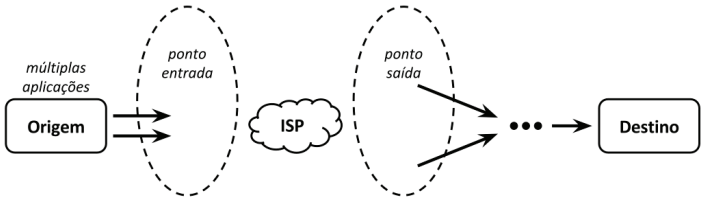
A detecção de DT da NetPolice baseada nas medições de perda de pacotes segue 4 etapas, ilustradas na Figura 4.3. A primeira etapa consiste em descobrir todos os caminhos que atravessam o ISP a ser avaliado, a partir de diversas origens (*probers*). Neste processo um grande número de rastreamentos de rota (usando o comando *traceroute*, por exemplo) é executado a partir de cada origem e para a maior quantidade possível de destinos na Internet (prefixos). Assim, além dos caminhos, são também obtidas as distâncias entre os pontos de entrada e saída do ISP, bem como os ASes anteriores e posteriores a estes pontos. Com esta informação, o NetPolice pré-calcula os valores de TTL (*Time to Live*) para alcançar cada par de pontos de entrada e saída do ISP alvo, a partir de todas as



(a) Detecção de DT baseada no próximo AS.



(b) Detecção de DT baseada no AS anterior.



(c) Detecção de DT baseada em conteúdo.

Figura 4.2: Detecção de diferentes tipos de DT na ferramenta NetPolice.

origens. O conjunto de caminhos e demais informações obtidas nesta etapa são chamados de *path view*.

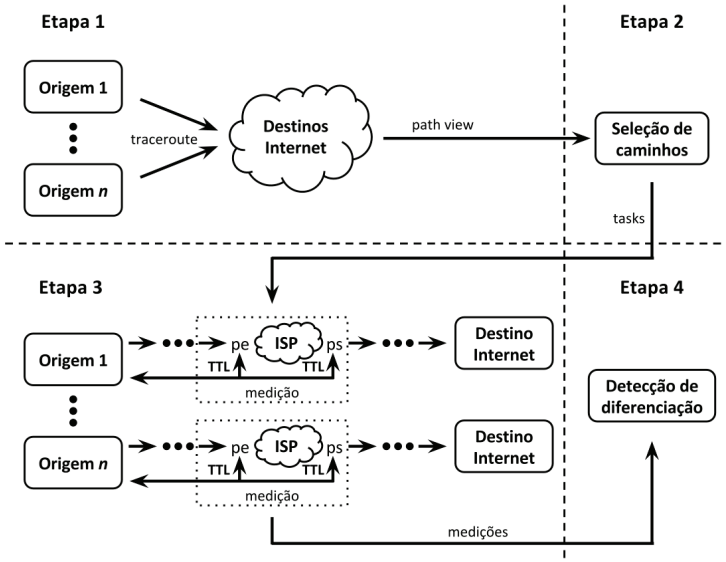


Figura 4.3: Funcionamento da ferramenta NetPolice.

Na segunda etapa são selecionados, a partir do *path view* criado na etapa anterior, quais caminhos serão efetivamente medidos, já que não é factível medir todos. Esta se-

leção de caminhos a serem medidos deve resultar em uma boa cobertura da rede interna do ISP alvo. A escolha deve ser inteligente, para que não sejam escolhidos origens e destinos que passem pelos mesmos caminhos internos do ISP ou caminhos que não atravessem o ISP. A seleção é modelada como um problema de otimização, com as seguintes restrições: cada tupla *(origem,entrada,saída)* deve ser percorrida pelo menos *R* vezes por caminhos para diferentes destinos; cada tupla *(entrada,saída,destino)* deve ser percorrida pelo menos *R* vezes por caminhos a partir de origens diferentes; e não podem haver mais que *m* caminhos a partir da mesma origem. O conjunto de caminhos a serem medidos é chamado de *tasks*.

Na terceira etapa são feitas as medições dos caminhos selecionados na etapa anterior para diferentes aplicações: HTTP, BitTorrent, SMTP, PPLive e VoIP. A medição de um caminho consiste em, uma vez a cada 200 segundos e para cada aplicação, enviar 2 pacotes: um pacote com o valor de TTL pré-calculado para alcançar apenas o ponto de entrada (*pe*) e gerar uma resposta ICMP de tempo excedido; e outro pacote com TTL pré-calculado para alcançar o ponto de saída (*ps*). Assim, subtrai-se a taxa de perda de pacotes do ponto de entrada do ISP da taxa do ponto de saída, obtendo-se a medição apenas para o caminho interno do ISP.

A quarta e última etapa consiste em inferir se o ISP está praticando DT baseada em roteamento ou conteúdo. Esta inferência utiliza o teste Kolmogorov-Smirnov (KS) [Noether 2012] para comparar as distribuições dos dados de medição obtidos. A detecção de DT por conteúdo é feita então comparando-se as distribuições de dados de cada aplicação com a distribuição de dados da aplicação HTTP, isto é, testes KS são aplicados para determinar se um conjunto de dados medidos para uma aplicação é significativamente diferente do conjunto de dados para a aplicação HTTP, caracterizando assim uma DT. A detecção de DT baseada em roteamento é feita de forma similar, mas comparando-se as distribuições de dados de caminhos diferentes para uma mesma aplicação.

Resultados experimentais com a NetPolice foram obtidos no PlanetLab. Nestes experimentos, 18 ISPs distribuídos em 3 continentes foram estudados em um período de 10 semanas. Os resultados mostraram que 4 ISPs realizaram DT em 4 aplicações e 10 ISPs realizaram DT baseada no AS anterior dos pacotes. As taxas de perda de pacotes medidas nestes casos chegaram a ser até 5% diferentes. Os autores também observaram, a partir dos resultados obtidos, que a DT pode depender da carga da rede. Já para alguns ISPs, os valores atribuídos ao campo TOS do cabeçalho dos pacotes tem forte relação com a DT (diferente priorização) e esta atribuição de valores é baseada apenas na porta de destino dos pacotes, não no conteúdo (não é feito DPI). Outra observação foi que a DT não é feita de forma homogênea em todos os roteadores dos ISPs.

Um trabalho anterior à NetPolice foi publicado pelos mesmos autores e apresenta uma versão anterior da ferramenta, com o nome de NVLens [Zhang et al. 2008]. No trabalho mais recente [Zhang et al. 2009], os autores detalharam diversos experimentos no PlanetLab, expandiram a análise dos dados obtidos e reformularam a última etapa do processo de detecção (teste para comparação das distribuições de dados).

4.5.3. DiffProbe

A DiffProbe [Kanuparthy and Dovrolis 2010] é uma ferramenta de detecção de DT que utiliza atraso e/ou descarte de pacotes como métrica. Esta detecção é feita por meio de medições feitas em fluxos de dados simultâneos entre um *host* cliente e um servidor. A ferramenta assume que um ISP classifica cada pacote como sendo de alta prioridade (classe H) ou baixa prioridade (classe L). Os autores afirmam que esta estratégia é genérica, abrangendo qualquer método específico de classificação que possa ser empregado por um ISP. Pacotes classificados como de baixa prioridade (L) podem sofrer atrasos e/ou perdas maiores dependendo das políticas de escalonamento e descarte empregadas por um ISP.

A DiffProbe requer 2 agentes: um cliente conectado à rede do ISP a ser verificado e um servidor. O funcionamento da ferramenta pode ser dividido em 3 etapas, ilustradas na Figura 4.4. A primeira etapa (1) consiste em um gerador de fluxos de dados. São gerados 2 fluxos diferentes: um fluxo de dados correspondente a uma aplicação suspeita de estar sofrendo DT (A) e outro fluxo de dados de medição (P). Os autores assumem que o fluxo P é da classe H (alta prioridade) e portanto não sofre nenhuma deterioração. A segunda etapa é responsável por executar os fluxos de dados. Os fluxos são enviados simultaneamente pela rede, primeiro do cliente para o servidor e em seguida no sentido contrário. A terceira etapa (3) da ferramenta é responsável por detectar se houve alguma DT. Nesta detecção são utilizadas as medições de atraso e perda de pacotes obtidas pelo cliente e servidor. A detecção baseia-se em uma comparação estatística entre as medidas correspondentes a cada fluxo. Estas três etapas da DiffProbe são descritas em mais detalhes abaixo.

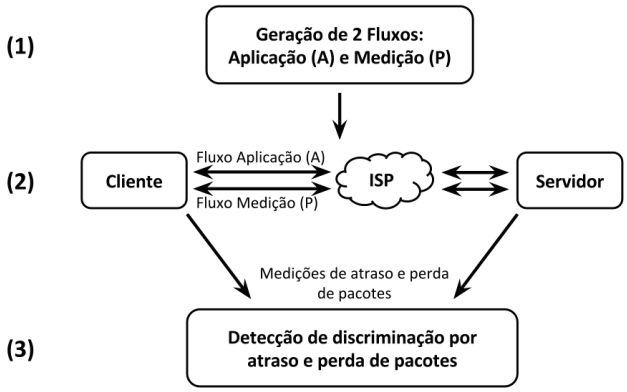


Figura 4.4: Funcionamento da ferramenta DiffProbe.

O fluxo de dados A é gerado a partir de um fluxo real, pré-armazenado, de uma aplicação. A DiffProbe dá duas opções de aplicação para o usuário: Skype e Vonage. Para criar o fluxo A são mantidos os protocolos de transporte, tamanhos de pacotes, portas, dados e intervalos de envio do fluxo original da aplicação. A geração do fluxo P é baseada no fluxo A, mas com restrições: o fluxo P deve ser suficientemente diferente do fluxo A, garantindo que P não seja classificado da mesma forma que A, ou seja, o fluxo P não pode ser classificado como de baixa prioridade. Por outro lado, o fluxo P deve ter características de rede (como tamanho dos pacotes) similares ao fluxo A para que possam ser posteriormente comparados. Na prática, a DiffProbe cria os pacotes do fluxo P

conforme o fluxo A é enviado. Um pacote qualquer do fluxo P tem o mesmo tamanho do último pacote do fluxo A enviado até então, com dados aleatórios e uma porta com baixa probabilidade de ser considerada de baixa prioridade.

A execução dos fluxos é feita em duas fases. Na primeira fase, os pacotes dos dois fluxos são enviados simultaneamente em uma taxa de envio igual. Na segunda fase, a taxa de envio do fluxo P é aumentada, enviando-se mais pacotes do fluxo P do que do fluxo A. O objetivo desta segunda fase é maximizar a chance de ocorrer enfileiramento de pacotes nos roteadores do ISP, já que, como dito anteriormente, não é possível detectar DT quando a carga da rede é baixa e os roteadores não precisam escalonar os pacotes a serem roteados. A DiffProbe não altera a taxa de envio do fluxo A, pois isso pode alterar a classificação do mesmo (se a classificação for baseada em fluxo, por exemplo). Com o aumento da taxa de envio de pacotes do fluxo P, são coletadas mais medidas para o fluxo P do que para o fluxo A. Assim, para os pacotes do fluxo P, a DiffProbe considera na detecção apenas as medidas referentes aos pacotes enviados imediatamente depois de algum pacote do fluxo A, resultando na mesma quantidade de medidas para os 2 fluxos. A primeira fase serve apenas para verificar se a DT é identificável: os maiores valores de atraso do fluxo P na segunda fase devem ser significativamente maiores que os atrasos médios do fluxo P na primeira fase para que a DT seja estatisticamente identificável.

A detecção de DT por atraso é feita comparado-se as distribuições dos atrasos medidos para cada fluxo: no caso de um escalonamento FCFS, os dois fluxos devem apresentar uma distribuição similar de atrasos dos pacotes. Caso exista despriorização dos pacotes do fluxo A, a distribuição dos atrasos do fluxo A será significativamente maior que a distribuição dos atrasos do fluxo P. O teste de igualdade para as distribuições de atrasos usado pela DiffProbe baseia-se na divergência de Kullback-Leibler. A detecção de DT por perda de pacotes também é feita comparando-se as distribuições das taxas de perda medidas para cada fluxo, de forma análoga. Porém, o teste de igualdade utilizado pela ferramenta para esta comparação é o teste Z para comparação de duas proporções (*two-proportion z-test*).

Os autores avaliaram a DiffProbe por meio de simulações, utilizando NS2, e da emulação de um ambiente real. Para este ambiente emulado, foram utilizados um cliente conectado a um ISP residencial e um servidor hospedado em uma universidade. A DT foi emulada por um roteador entre o *host* cliente e o ISP. Tanto as simulações quanto os experimentos no ambiente emulado mostraram que, quando a DT é identificável e o fluxo de medição foi capaz de gerar enfileiramento de mensagens, a detecção foi precisa.

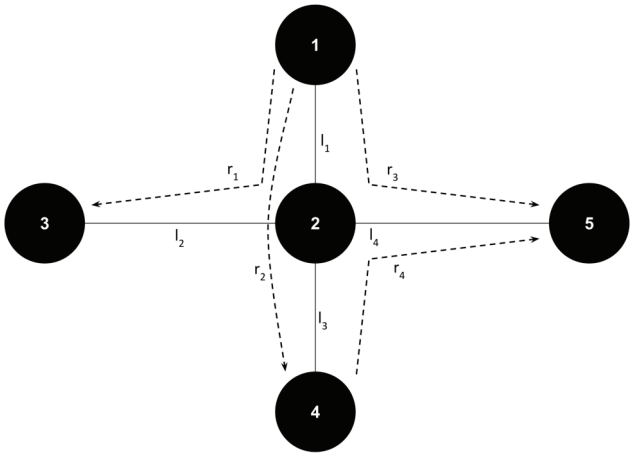
4.5.4. Inferência Baseada em Tomografia de Redes

Em [Zhang et al. 2014] os autores propõem um algoritmo baseado em técnicas de tomografia de rede para inferir se houve DT em uma rede qualquer. O algoritmo também é capaz de identificar especificamente em qual *link* ou sequência de *links* a violação da NR ocorreu, baseando-se apenas em observações externas (medições fim-a-fim), ou seja, sem medir diretamente *links* internos da rede. Os autores fornecem provas formais demonstrando em quais condições o algoritmo atinge estes resultados.

A tomografia de rede [Coates et al. 2002] consiste em inferir métricas sobre os *links* internos de uma rede (como atraso e taxa de perda de pacotes, por exemplo) apenas

a partir de medições fim-a-fim, ou seja, sem medir diretamente cada *link*. Em uma das técnicas existentes, de maneira simplificada, forma-se um sistema de equações $y = Ax$, em que y é um vetor com as medições fim-a-fim, A é uma matriz de roteamento que especifica a relação entre os *links* da rede e as rotas entre os pontos de medição (quais *links* estão em cada rota) e x é um vetor com as métricas a serem inferidas para cada *link*. Obtém-se então uma estimativa de x resolvendo o sistema ou, em caso de múltiplas soluções, escolhendo a solução mais adequada, como a solução que ocorre com a maior probabilidade ou com menor número de *links* problemáticos, por exemplo.

A Figura 4.5 exemplifica a técnica de tomografia de redes utilizada pelo algoritmo. A Figura 4.5a mostra uma rede com 5 *hosts*, numerados de 1 a 5, interligados pelos *links* $l_i, 1 \leq i \leq 4$. Neste exemplo, foram feitas 4 medições fim-a-fim cujas rotas estão representadas na Figura 4.5a por $r_j, 1 \leq j \leq 4$. A Figura 4.5b mostra a matriz de roteamento A para as 4 rotas medidas. Na matriz, as linhas são as rotas medidas e as colunas os *links*. O valor de uma posição da matriz é 1 se a rota (linha) atravessa o *link* (coluna) ou 0 caso contrário. A Figura 4.5c mostra o sistema de equações $y = Ax$ resultante. No sistema, $y = \{y_1, y_2, y_3, y_4\}$ e $x = \{x_1, x_2, x_3, x_4\}$, sendo y_j o valor medido para a rota r_j e x_i o valor da métrica a ser estimado para o *link* l_i. Se o *link* l_4 não for neutro, por exemplo, poderá haver uma inconsistência nas medições referentes às rotas r_3 e r_4, que compartilham este *link*. Neste caso, o valor de x_4 seria efetivamente diferente para cada uma das medições, resultando em um sistema de equações inconsistente e, portanto, sem solução.



(a) Exemplo de rede com 5 *hosts* e 4 medições fim-a-fim.

	l_1	l_2	l_3	l_4
r_1	1	1	0	0
r_2	1	0	1	0
r_3	1	0	0	1
r_4	0	0	1	1

(b) Matriz de roteamento A.

$$y_1 = x_1 + x_2$$
$$y_2 = x_1 + x_3$$
$$y_3 = x_1 + x_4$$
$$y_4 = x_3 + x_4$$

(c) Sistema de equações resultante das 4 medições fim-a-fim.

Figura 4.5: Técnica de tomografia de redes utilizada no algoritmo.

A técnica de tomografia de rede utilizada assume que a rede é neutra: cada *link* trata qualquer tráfego de qualquer rota da mesma forma. Caso isto não ocorra, torna-se impossível expressar as medições de diferentes rotas como função das métricas dos *links*

e o sistema de equações resultante não tem, portanto, solução. Assim, enquanto as técnicas convencionais de tomografia de redes tentam construir sistemas de equações com solução, o algoritmo proposto [Zhang et al. 2014] tenta construir sistemas de equações sem solução, revelando assim violações da NR. A ideia central deste algoritmo é que, quando uma rede não é neutra, observações feitas de pontos de vista distintos serão inconsistentes entre si.

A técnica de tomografia utilizada impõe restrições quanto à métrica empregada para realizar as medições entre os *hosts* finais. Esta deve ser aditiva, ou seja, considerando uma rota entre 2 *hosts* finais, a soma dos valores medidos para cada *link* da rota, utilizando tal métrica, deve ser igual ao valor medido entre os *hosts* finais (a rota toda). Atraso e taxa de perda de pacotes são exemplos de métricas aditivas.

O algoritmo recebe como entrada a topologia da rede e um conjunto de medições fim-a-fim com as respectivas rotas entre os *hosts* finais a partir dos quais as medições foram feitas. A saída do algoritmo é um conjunto de sequências de *links* não neutras, ou seja, em quais *links*, ou sequências de *links*, houve alguma violação da NR. As medições entre os *hosts* finais podem ser feitas utilizando em seus pacotes dados de diferentes aplicações, assim como dados de uma mesma aplicação com origem/destino diferentes. Desta forma, é possível detectar DT baseada tanto no conteúdo quanto na origem ou destino das mensagens.

Como mencionado acima, o algoritmo consiste em buscar sequências de *links* que geram um sistema de equações sem solução. Para cada sequência de *links* que esteja presente em mais de uma rota, forma-se um sistema de equações utilizando todas as medições cujas rotas atravessam esta sequência de *links*. Caso o sistema de equações construído não tenha solução, a sequência de *links* é não neutra. Caso contrário, a sequência é neutra ou a DT para esta sequência de *links* não é identificável (falso-negativo). Em outras palavras, o algoritmo confronta as medições cujos pacotes atravessaram um mesmo segmento da rede, tentando encontrar inconsistências que podem ser atribuídas a alguma DT ocorrida nestes segmentos.

O Algoritmo 1 especifica a estratégia de detecção de DT. O conjunto R é dado como entrada e contém todas as rotas medidas. Nas linhas 3 a 10, cada sequência de *links* λ comum a pelo menos um par de rotas distintas de R é armazenada em Λ_n. Já em π_λ são armazenados os conjuntos de rotas que tem em comum cada sequência λ. No próximo laço, linhas 11 a 16, são consideradas apenas as sequências λ que sejam comuns a pelo menos 2 pares de rotas distintos (linha 12). Para cada uma destas sequências, é formado um sistema de equações utilizando todos os conjuntos de rotas em π_λ. Se este sistema de equações não tiver solução (linha 12), então λ é uma sequência de *links* não neutra e é adicionada em $\Lambda_{\bar{n}}$ (linha 14). Por fim, retorna-se $\Lambda_{\bar{n}}$ contendo todas as sequências de *links* não neutras identificadas (linha 17).

Os autores afirmam que este algoritmo não gera falso-positivos, ou seja, nunca acusa erroneamente uma sequência de *links* como não neutra. A razão para isto é que medições que englobam uma sequência de *links* neutra sempre resultarão em um sistema de equações com solução. Já no caso de falso-negativos, os autores afirmam que ocorrem com pouca frequência. Nestes casos, o algoritmo considera como neutra uma sequência de *links* que na verdade não é neutra.

Algorithm 1 Algoritmo de inferência de NR.

Λ_n: conjunto de sequências de *links* a serem avaliadas
$\Lambda_{\bar{n}}$: conjunto de sequências de *links* não neutras
π_λ: conjunto de conjuntos de rotas que tem a sequência de *links* λ em comum
R: conjunto de todas as rotas medidas
$Links(r)$: sequência de *links* da rota r (atravessados pela medição)
$Sistema(\pi_\lambda)$: sistema de equações formado pelos conjuntos de rotas em π_λ

$\Lambda_n \leftarrow \emptyset$
$\Lambda_{\bar{n}} \leftarrow \emptyset$
for cada par de rotas $\{r_i, r_j\} : r_i, r_j \in R, r_i \neq r_j$ **do**
    $\lambda \leftarrow Links(r_i) \cap Links(r_j)$
    if $\lambda \notin \Lambda_n$ **then**
        $\Lambda_n \leftarrow \Lambda_n \cup \{\lambda\}$
        $\pi_\lambda \leftarrow \emptyset$
    end if
    $\pi_\lambda \leftarrow \pi_\lambda \cup \{\{r_i\}, \{r_j\}, \{r_i, r_j\}\}$
end for
for cada sequência $\lambda \in \Lambda_n$ **do**
    if $|\pi_\lambda| > 4$ e $Sistema(\pi_\lambda)$ não tem solução **then**
        $\Lambda_n \setminus \{\lambda\}$
        $\Lambda_{\bar{n}} \cup \{\lambda\}$
    end if
end for
retorna $\Lambda_{\bar{n}}$

Para avaliar o algoritmo, foram feitas duas séries de experimentos em ambientes emulados, com diferentes topologias. Primeiramente foi utilizada uma topologia com um único *link* discriminatório. Neste experimento, todas as medições foram feitas atravessando este *link*. Foram testados diferentes cenários, variando o comportamento do *link* discriminatório. Em todos os casos o algoritmo decidiu corretamente se o *link* era neutro ou não. Na segunda série de experimentos foi utilizada uma topologia com diversos *links* discriminatórios. Cada *link* destes teve um comportamento diferente. Assim como na primeira série, o algoritmo detectou corretamente os *links* não neutros em todos os experimentos.

Os autores também discutem os desafios para implementar a solução proposta em um ambiente real. A opção mais viável na prática, segundos os autores, é dispor de um conjunto de *hosts* finais que efetuam periodicamente medições das rotas entre eles e enviam estes dados para serem processados em um servidor central. Também é necessário o uso de alguma solução para descobrir a topologia da rede que conecta os *hosts* envolvidos nas medições, um requisito do algoritmo. Outro desafio é coletar medições a partir de uma quantidade suficiente de pontos de vista diferentes.

4.5.5. NANO

A NANO (*Network Access Neutrality Observatory*) [Tariq et al. 2009] é uma ferramenta cujo objetivo é inferir se um ISP está discriminando o tráfego de alguma aplicação específica. Isto é feito verificando-se se um ISP está causando degradação do desempenho de uma aplicação quando comparado ao desempenho da mesma aplicação em outros ISPs. Se o desempenho de uma aplicação medido na rede de um ISP é estatística e significati-

vamente menor que o desempenho da mesma aplicação medido na rede de outros ISPs, é possível que DT esteja sendo praticada. A NANO utiliza um modelo de inferência causal, tentando estabelecer uma relação entre a degradação de desempenho observada e as políticas de um ISP. As medições de desempenho na NANO são obtidas de forma passiva, ou seja, apenas são feitas medições do tráfego real das aplicações observadas.

As principais diferenças entre a NANO e outras soluções existentes na época de sua publicação para detecção de DT são, segundo os autores: (i) outras soluções detectam discriminação baseada em características específicas como, por exemplo, porta e conteúdo dos pacotes, enquanto a NANO tem um abordagem mais genérica, medindo o desempenho das aplicações independentemente dos mecanismos específicos de DT empregados pelos ISPs; (ii) outras soluções utilizam medições ativas das redes dos ISPs, enquanto a NANO captura suas métricas de forma passiva, o que torna mais difícil para os ISPs detectar e escapar da inferência da NANO; e (iii) as demais soluções comparam métricas de aplicações diferentes em um mesmo ISP, enquanto a NANO compara métricas de uma mesma aplicação em ISPs diferentes.

A estratégia de detecção de DT da NANO apresenta 3 grandes desafios: (i) o mecanismo de DT empregado pelo ISP pode não ser conhecido, assim a estratégia de detecção precisa ser genérica; (ii) o desempenho padrão de uma aplicação em um determinado ISP não é conhecido, dificultando a detecção de possíveis degradações, já que não há um valor base para comparação; e (iii) muitos fatores, além da DT, podem causar degradação no desempenho de aplicações, como sobrecarga, localização geográfica, *software*, *hardware* e outras particularidades da rede.

Os diferentes fatores, além da DT, que podem causar degradação no desempenho de uma aplicação, são representados, no modelo estatístico utilizado pela NANO, por variáveis de confusão [Sander Greenland 1999]. Assim, é necessário identificar quais são as variáveis de confusão e coletar dados não somente sobre o desempenho de aplicações, mas também sobre estas variáveis. A detecção de DT da NANO é feita, portanto, comparando-se o desempenho de uma mesma aplicação em ISPs diferentes, usando medições cujas variáveis de confusão são similares. Um exemplo de variável de confusão é o horário do dia: não se deve comparar medições obtidas em horários distintos, já que aplicações podem ter um desempenho diferente conforme o horário (devido a uma maior carga, por exemplo).

A NANO utiliza a técnica de estratificação para agrupar as medições de desempenho conforme o valor das respectivas variáveis de confusão. Esta técnica coloca cada medição em um estrato, de forma que as variáveis de confusão referentes a cada amostra em um mesmo estrato têm valores similares. São definidas três categorias de variáveis de confusão: (i) variáveis referentes ao cliente (exemplos incluem *softwares* que podem afetar o desempenho da aplicação medida, como sistema operacional ou um navegador Web específico); (ii) variáveis referentes à rede (como localização geográfica, por exemplo); e (iii) variáveis temporais (como o horário do dia, por exemplo, que podem afetar o desempenho da aplicação sendo medida).

Após a estratificação, a NANO estima, para cada estrato, quanto o desempenho de uma aplicação muda quando acessada através de um ISP, em relação ao desempenho obtido quando não se utiliza tal ISP – o desempenho médio (*baseline*). O desempenho

médio é a média do desempenho de todos os outros ISPs dentro do estrato, excluindo o ISP sendo avaliado. Estas estimativas representam uma quantificação da relação causal entre cada ISP e uma possível DT sendo praticada.

A partir das estimativas de cada estrato, o último passo na detecção de DT da NANO consiste em agregar as estimativas de todos os estratos e verificar se os valores obtidos são estatisticamente significativos. A ideia central é que se, na média, o desempenho de uma aplicação degradou-se significativamente ao utilizar-se um ISP específico, então tem-se uma relação causal entre o ISP e a prática de DT.

A implementação da NANO é dividida em duas partes: os agentes e um servidor. Um agente é executado em cada *host* cliente, sendo responsável por monitorar o desempenho da aplicação, medindo seu tráfego real a partir do *host* cliente. As métricas utilizadas são específicas de cada aplicação, conforme o que for mais adequado para cada um. Além dos dados de desempenho das aplicações, os agentes também coletam os dados referentes às variáveis de confusão. Todos os dados adquiridos pelos agentes são enviados periodicamente para o servidor. Os agentes são implementados como *sniffers* de rede, analisando todos os pacotes recebidos e enviados pelo *host*. Já o servidor da NANO recebe todos os dados coletados pelos agentes e é responsável por realizar a detecção de DT com base nestes dados.

A Figura 4.6 ilustra o funcionamento da NANO. Em (1) cada cliente executa um agente. Os agentes monitoram o tráfego real das aplicações sendo avaliadas. Os dados coletados são enviados para o servidor, que primeiramente os separa em estratos conforme as variáveis de confusão (2). Por fim, o servidor infere (3), seguindo o modelo causal, quais ISPs praticaram DT para cada aplicação medida.

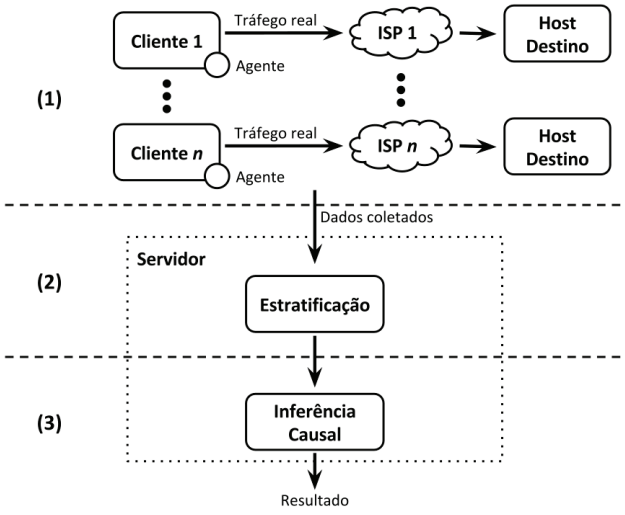


Figura 4.6: Funcionamento da ferramenta NANO.

Para avaliar a NANO, os autores conduziram experimentos em um ambiente controlado, utilizando os *testbeds* PlanetLab e Emulab. Foram selecionados nodos do PlanetLab geograficamente distribuídos. Estes nodos foram utilizados como servidores das aplicações a serem avaliadas. Um conjunto de ISPs foi criado no Emulab, cada um com um conjunto diferente de clientes. Cada ISP fornecia conectividade à Internet para os

seus clientes. Assim, todo acesso dos clientes às aplicações hospedados nos nodos do PlanetLab passava por estes ISPs, permitindo a emulação de diferentes práticas de DT e de diferentes variáveis de confusão.

Os resultados dos experimentos mostraram que a NANO é capaz de detectar DT praticada de diferentes formas e para diferentes tipos de aplicação, desde que todos os fatores que possam confundir significativamente a relação entre um ISP e o desempenho observado de uma aplicação – as variáveis de confusão – sejam conhecidos e medidos. A estratégia de detecção da NANO mostrou-se genérica o suficiente, detectando a discriminação de tráfego mesmo sem conhecer quais as políticas de DT empregadas pelos ISPs.

Porém, se a NANO não considerar todas as variáveis de confusão, a relação causal entre o ISP e uma possível DT pode ser erroneamente calculada – resultando em falso-negativos e falso-positivos. Não há formas automatizadas para enumerar todas as variáveis de confusão pertinentes ou concluir se um conjunto de variáveis de confusão é suficiente, o que pode inviabilizar a aplicação da NANO em um ambiente real.

4.5.6. Gnutella RSP

Os autores em [Beverly et al. 2007] apresentam uma estratégia para quantificar as práticas de bloqueio de portas efetuadas por ISPs na Internet utilizando a rede Gnutella[2]. A estratégia explora o procedimento de ingresso de novos clientes na rede para efetuar medições, aproveitando a infraestrutura já existente da rede Gnutella. Foi um dos primeiros trabalhos publicados sobre medições relacionadas à NR.

Gnutella é uma rede P2P totalmente descentralizada. Os *hosts* participantes da rede são de 2 tipos: os *superpeers* e as folhas (clientes). Cada *superpeer* é conectado com outros *superpeers* e tem um conjunto de folhas conectadas a ele. Para uma nova folha ingressar na rede, é necessário conectar-se a um *superpeer*. O *superpeer* pode aceitar a nova folha, mantendo-a ligada a ele, ou pode informar à folha que está ocupado – caso já tenha muitas folhas, por exemplo. Caso o *superpeer* rejeite a folha, ele indica outro *superpeer* ao qual a folha deve conectar-se para ingressar na rede. Esta indicação contém o endereço IP e a porta TCP do outro *superpeer*.

A estratégia para medição de bloqueio de portas apresentada utiliza 2 *hosts* diferentes: um *host* de medição e um *superpeer* chamado de RSP (*Rogue SuperPeer*). Quando um cliente conecta-se ao RSP para ingressar na rede, o RSP envia uma resposta informando que está ocupado e indica o *host* de medição. O cliente pode então seguir esta indicação e iniciar uma conexão com o *host* de medição na porta indicada. Caso o faça com sucesso, sabe-se então que tal porta não é bloqueada. A ideia central desta estratégia é, portanto, induzir os clientes Gnutella a se conectarem ao *host* de medição para verificar se esta conexão é permitida ou não. Os autores concluíram empiricamente que a probabilidade de um cliente Gnutella não seguir a indicação do RSP, ou seja, não conectar-se ao *host* de medição, é de 80%.

O RSP e o *host* de medição ambos registram as conexões vindas dos clientes Gnutella em um servidor centralizado. Este servidor também é responsável por informar

[2]`http://www.gnutellaforums.com`

qual porta será indicada aos clientes pelo RSP e qual porta o *host* de medição deverá escutar. O servidor altera esta porta a cada 5 minutos, visando obter dados suficientes sobre todas as portas a serem observadas.

Com base nos dados coletados pelo servidor central é feita uma inferência probabilística para determinar quais portas foram bloqueadas. Note que a estratégia proposta considera que o bloqueio de portas pode acontecer em qualquer ponto entre o cliente e o *host* de medição, não sendo capaz de identificar em que parte do caminho o bloqueio aconteceu. Determinar se uma porta não foi bloqueada é trivial: basta que o *host* de medição tenha recebido pelo menos uma conexão de um cliente Gnutella após a indicação do RSP. Porém, caso nenhuma conexão tenha sido feita com o *host* de medição em uma dada porta, isto não implica que tal porta foi bloqueada. É possível que todos os clientes redirecionados para tal porta não tenham seguido a indicação. Assim, segundo os autores, são necessárias pelo menos 50 indicações para concluir, com probabilidade de 99.5%, que uma porta foi bloqueada.

A Figura 4.7 ilustra o funcionamento da estratégia. Em (1) um cliente Gnutella conecta-se no RSP a fim de ingressar na rede. O RSP responde o cliente informando que está ocupado, e indica outro *host* (endereço IP e porta) com o qual o cliente deve tentar conectar-se. O *host* indicado pelo RSP é o *host* de medição. O cliente então inicia uma conexão com o *host* de medição (2). O *host* de medição e o RSP ambos registram as conexões vindas do cliente, informação utilizada para inferir probabilisticamente quais portas foram bloqueadas.

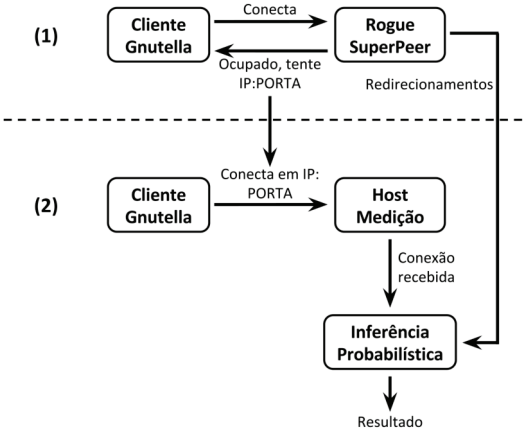


Figura 4.7: Funcionamento da estratégia RSP.

A estratégia do RSP foi executada durante 2 meses. Neste período, o RSP enviou aproximadamente 150 mil indicações para cerca de 72 mil clientes Gnutella distintos, distribuídos em aproximadamente 31 mil prefixos diferentes – uma fração significativa da Internet. Os resultados mostraram que dos 31 mil prefixos, em 256 houve bloqueio de pelo menos uma porta. A porta bloqueada com maior frequência foi a 136 e as bloqueadas com menor frequência foram a 80 (HTTP), 6346 (Gnutella) e 6969 (observada apenas para comparação). Algumas portas referentes a serviços de *e-mail* (25, 110 e 143) foram bloqueadas com frequência cerca de duas vezes maior do que a porta 6969. Depois da 136, as outras portas mais frequentemente bloqueadas foram as referentes ao serviços

FTP, SSH, Bittorrent e VPNs. Os autores também relatam que algumas universidades e ISPs bloquearam portas de serviços P2P (1214, 4662, 6346, 6881) e alguns ISPs no Canadá, E.U.A. e Polônia bloquearam portas do Skype.

4.5.7. Packsen

Packsen [Weinsberg et al. 2011] é um *framework* para geração de fluxos de dados utilizado com o objetivo de detectar se um ISP está praticando DT por meio de engenharia de tráfego. O Packsen também é capaz de inferir qual o tipo de escalonador está sendo empregado e seus parâmetros. A inferência do Packsen é baseada em uma comparação estocástica entre os tempos de chegada dos pacotes de dois fluxos de dados – um fluxo base e um fluxo de medição.

O Packsen considera que um modelador de tráfego (*traffic shaper*) mantém múltiplas filas de pacotes, correspondentes a diferentes classes de tráfego. Cada fluxo de dados é classificado em uma das classes, determinando em qual fila os pacotes do fluxo serão inseridos. Esta classificação pode basear-se em diferentes parâmetros, como protocolo de aplicação, porta, hora do dia, origem, destino, entre outros.

O Packsen utiliza dois fluxos de dados: um fluxo de medição, referente a aplicações específicas, e um fluxo base, o qual se assume não sofrer nenhuma discriminação. Estes fluxos são enviados entre *hosts* finais de forma intercalada e mantendo a mesma largura de banda para os dois fluxos. Se no recebimento dos fluxos for observada uma diferença significativa entre a largura de banda de cada um, então houve DT no caminho entre os dois *hosts*. A métrica utilizada pelo Packsen é, portanto, os tempos de chegada dos pacotes de cada fluxo.

A detecção do Packsen utiliza três métodos. O primeiro método apenas detecta se houve discriminação de um fluxo em relação a outro. Esta detecção é feita comparando-se as distribuições dos tempos de chegada dos pacotes dos dois fluxos. Se a diferença entre as distribuições for estocasticamente significativa, então houve DT. A comparação é feita utilizando o teste U de Mann-Whitney [H. B. Mann 1947]. O segundo método infere qual o tipo de manipulação de tráfego utilizada e quais os parâmetros empregados, como o peso atribuído a cada fluxo, por exemplo. Esta inferência é feita comparando-se a largura de banda dos fluxos no envio com a largura de banda observada no recebimento. Segundo os autores, este método não é robusto na presença de tráfego de fundo (*cross-traffic*). Quando outras aplicações estão gerando uma quantidade significativa de tráfego simultaneamente aos fluxos do Packsen, as larguras de banda dos fluxos podem ser alteradas de forma diferente. É possível que um processador de tráfego classifique o tráfego de fundo e o fluxo de medição como pertencentes à mesma classe, priorizando o fluxo base. Assim, o tráfego de fundo pode influenciar apenas o fluxo de medição e não o fluxo base. O terceiro método trata o tráfego de fundo, sendo capaz de medi-lo, ajustando o monitoramento efetuado. Neste método, as medições do Packsen precisam ser repetidas até que a variação dos resultados seja significativamente baixa.

A implementação do Packsen é dividida em três partes, ilustradas na Figura 4.8: o cliente, o servidor de experimentos e os servidores de medição. O cliente conecta-se ao servidor de experimentos, solicitando um experimento para ser executado (1). O servidor de experimentos escolhe um experimento em seu repositório e retorna-o ao cliente. O

cliente então escolhe um servidor de medição disponível (com baixa carga), informando o experimento que deve ser executado (2). O servidor de medição executa então o experimento, coletando os dados dos fluxos gerados. Os dados são enviados para o servidor de experimento que os armazena para posterior análise (3).

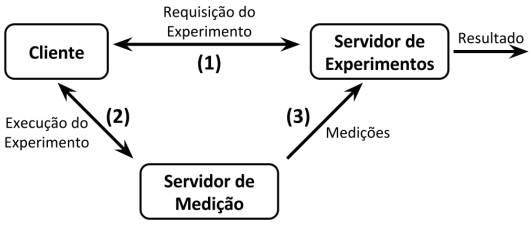


Figura 4.8: Funcionamento do Packsen.

Os autores avaliaram o Packsen primeiramente em um ambiente controlado, utilizando um *testbed* local. Este ambiente permitiu a emulação de diversos tipos de processadores de tráfego, com diferentes parâmetros, assim como diferentes combinações de tráfego de fundo. Após os experimentos no *testbed* local, foram conduzidos experimentos em cerca de 1000 *hosts* do PlanetLab, com o objetivo de melhor avaliar o Packsen em um ambiente real e de maior escala.

Os resultados obtidos no *testbed* local mostraram que o Packsen detectou, com baixa margem de erro, tanto a ocorrência de DT, quanto os parâmetros empregados nos processadores de tráfego, mesmo na presença de tráfego de fundo. Apenas um falso-negativo foi registrado nesses experimentos, no qual houve DT mas o Packsen não a detectou. Já nos experimentos conduzidos no PlanetLab, foi detectada DT em apenas 0.7% dos pares de *hosts* testados (4 de 518).

4.5.8. ChkDiff

ChkDiff [Ravaioli et al. 2012, Ravaioli et al. 2015] é uma ferramenta para a detecção de DT praticada por ISPs que atendem o mercado doméstico (*Tier* 3). O funcionamento da ferramenta consiste em reproduzir o tráfego real do usuário (previamente capturado e preparado) de forma que este tráfego atinja apenas os roteadores a poucos *hops* de distância – o ISP do cliente. São efetuadas medições de atraso e perda de pacotes para cada fluxo de dados presente neste tráfego. A partir destas medições, a ChkDiff é capaz de inferir se houve DT e também identificar a partir de qual roteador a DT aconteceu. Os autores afirmam que a estratégia de medição e detecção da ChkDiff é independente de aplicações específicas e dos mecanismos de DT utilizados pelo ISP. Quaisquer que sejam as aplicações discriminadas ou as técnicas utilizadas para tal, uma DT tipicamente resultará, para o *host* cliente, em maiores atrasos e perdas de pacotes.

O tráfego de dados utilizado pela ChkDiff é obtido capturando-se o tráfego real de um usuário durante uma sessão normal de uso (*trace*). Assim, os resultados produzidos pela ferramenta serão referentes ao conjunto de aplicações executadas pelo usuário durante a captura do *trace*. O *trace* capturado é utilizado com o mínimo de alterações: isto garante que os processadores de tráfego (*traffic shapers*) atravessados pelo *trace* terão o mesmo comportamento que teriam caso os pacotes estivessem sendo gerados pelas res-

pectivas aplicações. As únicas modificações feitas nos pacotes de um *trace* são no campo TTL, para alcançar apenas o *hop* desejado, e nos dados da aplicação, para que todos os pacotes tenham o mesmo tamanho, evitando assim diferentes tempos de transmissão.

A ChkDiff efetua suas medições reproduzindo o *trace* capturado diversas vezes, a partir do *host* cliente. Utiliza-se um valor incremental para o TTL dos pacotes, de forma que cada reprodução do *trace* alcance o roteador seguinte à reprodução anterior. Quando um pacote chega ao roteador ao qual foi destinado (TTL decrementado para zero), o roteador envia uma mensagem ICMP de tempo excedido (*ICMP Time Exceeded*) de volta ao *host* cliente. As medições de atraso e perda de pacotes utilizadas pela ChkDiff são referentes a estas respostas ICMP: o atraso é o RTT entre o envio do pacote e o recebimento da resposta ICMP. A perda de pacotes corresponde à taxa de respostas ICMP não recebidas. O objetivo é avaliar apenas os primeiros roteadores após o *host* do cliente, identificando a partir de qual roteador a DT acontece: assume-se a existência de um processador de tráfego logo antes deste roteador.

A ChkDiff faz uma análise estatística para inferir se um fluxo de dados sofreu DT ou não até o roteador destino (para o qual as medições foram obtidas). Compara-se o atraso e perda de pacotes medidos para este fluxo/roteador com os medidos para todo o resto do tráfego até o mesmo roteador. Se estas medições forem significativamente maiores do que as medições do resto do tráfego, então o fluxo sofreu discriminação a partir daquele roteador. Assim, a base para comparação (*baseline*) utilizada pela ChkDiff é o tráfego todo: a NR estabelece que um fluxo não discriminado é tratado da mesma forma que todo o resto do tráfego, ou seja, as medições obtidas para um fluxo discriminado irão se sobressair em relação ao resto do tráfego. Em um exemplo simplificado, caso a perda de pacotes medida para um fluxo for em torno de 50%, enquanto a perda medida para os demais fluxos for em torno de 10%, é possível que o ISP esteja violando a NR.

O funcionamento da ChkDiff pode ser dividido em 4 etapas, ilustradas na Figura 4.9. Na primeira etapa (1) o tráfego real do usuário é capturado resultando em um *trace*. Na segunda etapa (2) este *trace* é pré-processado, gerando-se um conjunto de *traces* modificados. Na terceira etapa (3), o conjunto de *traces* modificados é reproduzido e as medições são obtidas. Na quarta etapa (4) é feita a análise estatística para inferir se houve discriminação de algum fluxo e identificar a posição do processador de tráfego, relativa ao *host* cliente. Cada etapa é descrita em maiores detalhes abaixo.

Na primeira etapa, a ferramenta captura o tráfego real do *host* cliente. Esta captura é feita durante a atividade regular do usuário na Internet. Como a ChkDiff utiliza o tráfego de envio do usuário (*upstream*), espera-se que durante a captura sejam utilizadas aplicações com envio intenso de dados, como compartilhamento de arquivos, VoIP e mensagens instantâneas, por exemplo.

Na segunda etapa, a ChkDiff processa o *trace* capturado. Este pré-processamento gera um conjunto de *traces* que serão reproduzidos na etapa seguinte. O *trace* é separado em fluxos, agrupando os pacotes segundo 5 itens: endereço de origem e destino, porta de origem e destino e protocolo de transporte. O tamanho de todos os pacotes é padronizado, para evitar que os pacotes tenham tempos de transmissão diferentes, o que geraria erro na análise, já que os atrasos medidos para os pacotes devem ser comparáveis entre si. Com os pacotes padronizados em tamanhos iguais e separados em fluxos, são gerados diversos

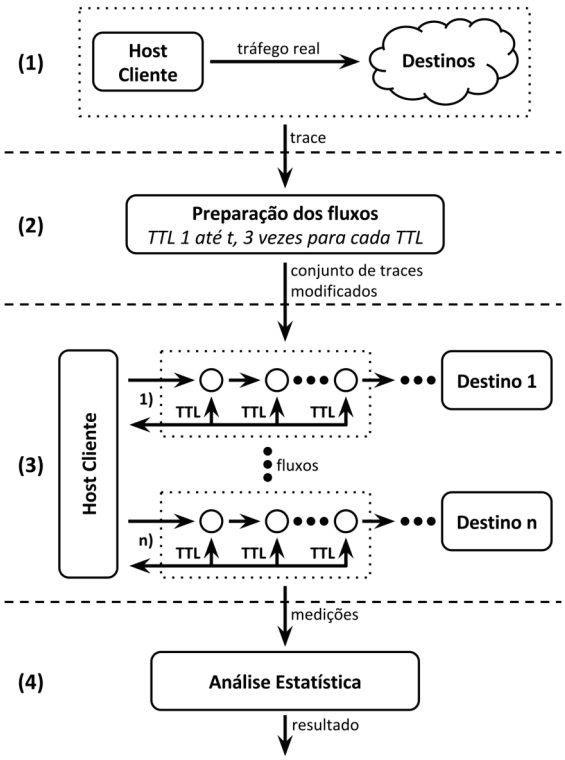


Figura 4.9: Funcionamento da ferramenta ChkDiff.

novos *traces*. Em cada um destes novos *traces*, os pacotes são reordenados e um valor específico de TTL é atribuído. O TTL varia de 1 a t e são criados 3 *traces* para cada valor de TTL. Assim, tem-se um conjunto de $3t$ *traces*, contendo os mesmos pacotes mas em ordem diferente e com valores diferentes de TTL. Os autores afirmam que um valor de 3 ou 4 para t deve ser suficiente para atravessar os roteadores do ISP do cliente.

A reordenação dos pacotes em cada *trace* criado na etapa 2 é feita de forma aleatória, mas sempre mantendo a ordem global dos pacotes do mesmo fluxo. Esta reordenação é necessária para evitar que os fluxos sejam afetados por possíveis vícios (*bias*) nas condições da rede. Segundo os autores, esta técnica também é útil para minimizar problemas como tráfego de fundo e limitação na taxa máxima de respostas ICMP de alguns roteadores. Ao final desta etapa, tem-se então um conjunto de *traces* modificados, prontos para serem reproduzidos.

Na terceira etapa, cada *trace* do conjunto resultante da etapa anterior é reproduzido. Seja h o TTL dos pacotes de um destes *traces*. Cada pacote do *trace* sendo reproduzido é enviado para seu destino e porta originais. Quando um destes pacotes alcança o h-ésimo *hop* a partir do *host* cliente, o roteador presente neste *hop* envia uma mensagem ICMP de tempo excedido para o *host* cliente. Duas medições são efetuadas pela ChkDiff baseadas nestas respostas ICMP: atraso e perda de pacotes, descritas acima. Esta estratégia de medição pode ser prejudicada caso os roteadores do ISP tenham uma taxa limitada de respostas ICMP. Os autores afirmam que, nestes casos, a reordenação dos pacotes em cada *trace* gerado faz com que as respostas ICMP não recebidas fiquem

razoavelmente bem distribuídas entre todos os fluxos do *trace*.

A quarta etapa consiste na análise estatística para inferir se houve discriminação de algum fluxo e identificar a posição do processador de tráfego, relativa ao *host* cliente. A ChkDiff considera nesta análise apenas os fluxos que tiveram pelo menos 20 respostas ICMP recebidas. Como descrito anteriormente, para cada valor h de TTL são reproduzidos e medidos 3 *traces*. Estas 3 repetições diminuem consideravelmente os falso-positivos, conforme os autores concluíram nos experimentos, descritos abaixo. Assim, se para os 3 *traces* o mesmo fluxo falhar no teste estatístico, é considerado que este fluxo sofreu discriminação em relação aos demais. Para as medições de atraso, a ChkDiff compara a distribuição de atraso de cada fluxo com a distribuição de atraso do restante do *trace*. O teste de hipótese utilizado é o Kolmogorov-Smirnov. No caso de uma rede neutra, espera-se que este teste indique que as duas distribuições são iguais. Assim, se um fluxo apresentou atrasos maiores do que o resto do trace, o teste para este fluxo falhou. Para as medições de perda de pacotes, a ChkDiff verifica se a perda de pacotes de cada fluxo é significativamente diferente da perda de pacotes do restante do *trace*. Utiliza-se um teste probabilístico inspirado em uma distribuição binomial. Se um fluxo teve uma perda de pacotes maior do que deveria, o teste probabilístico para este fluxo falhou, isto é a hipótese é falsa. Quando uma DT é detectada para um *hop* h, esta mesma DT será observável para todos os *hops* depois de h. Assim, se a DT não foi detectada para o *hop* anterior, a ChkDiff assume a existência de um processador de tráfego entre o *hop* $h-1$ e h.

A ChkDiff foi avaliada primeiramente em um ambiente neutro, sem nenhuma DT, e posteriormente em um ambiente não-neutro. Em ambos, o *trace* do usuário foi capturado durante um período de 3 minutos de uso típico da Internet. Durante este período foram feitos: envios de imagens em uma rede social, navegação em páginas de notícias e envio de mensagens em aplicativos de *chat*.

No ambiente neutro, a ChkDiff foi executada 100 vezes em uma configuração de rede controlada, em que o roteador no segundo *hop* garantidamente não discriminava nenhum dos fluxos presentes no *trace*. Analisando os resultados com apenas 1 reprodução para cada valor de TTL, cerca de 30% das execuções apresentaram de 1 a 3 falso-positivos. Os autores refizeram o experimento, mas com dois *traces* para cada valor de TTL: não houve nenhum falso-positivo. Com base nesta avaliação preliminar, os autores fixaram em 3 a quantidade de *traces* gerados para cada valor de TTL, como descrito anteriormente.

A avaliação em ambiente não-neutro foi feita primeiramente com apenas um fluxo discriminado. Posteriormente foram utilizados múltiplos fluxos discriminados, com diferentes frações do *trace* contendo fluxos discriminados. Em ambas as avaliações foi utilizada uma configuração de rede controlada. O *host* do usuário foi conectado a um *host* intermediário (*middlebox*), o qual fornecia acesso à Internet para o *host* cliente e também operava como um processador de tráfego (*traffic shaper*). Este *host* intermediário foi conectado a um roteador, no qual o TTL dos pacotes expirava. Foi utilizada a ferramenta Dummynet [Carbone and Rizzo 2010] no *host* intermediário para emular as práticas de DT. A DT foi implementada de duas formas diferentes: limitando a largura de banda dos fluxos selecionados e descartando pacotes dos fluxos selecionados de forma mais frequente.

Nos experimentos com apenas um fluxo discriminado, a ChkDiff foi capaz de detectar corretamente 100% dos fluxos discriminados por limitação de banda. Já quando a DT foi por descarte de pacotes, foram observados alguns falso-negativos (uma discriminação ocorreu mas não foi detectada). Nos experimentos com múltiplos fluxos discriminados, a análise estatística da ChkDiff deixou de funcionar corretamente quando a fração de fluxos discriminados é grande (cerca de 80% ou mais). A ChkDiff também foi avaliada na presença de um limite na taxa de envio de respostas ICMP do roteador. Os resultados mostraram que a ChkDiff manteve bons resultados na presença de tal limitação.

4.5.9. POPI

A POPI [Lu et al. 2010] é uma ferramenta que utiliza medições fim-a-fim para inferir se existe priorização no encaminhamento de pacotes de tipos diferentes (*packet forwarding prioritization*). A métrica utilizada pela POPI é a taxa de perda de pacotes, medida para tráfegos e diferentes tipos. O POPI considera que a priorização no encaminhamento de pacotes é feita seguindo alguma das estratégias de escalonamento da engenharia de tráfego, descritos anteriormente. A ideia central da POPI é que em uma rede neutra, todos os pacotes são encaminhados pelos roteadores conforme a ordem de chegada. Assim, caso a rede esteja congestionada e o descarte de pacotes seja necessário, tráfegos de tipos diferentes sofrerão uma taxa de perda similar. Porém, caso os pacotes de um tipo sejam encaminhados pelos roteadores com uma maior prioridade em relação aos pacotes de outros tipos, a taxa de perda de pacotes será diferente, configurando assim uma DT.

O funcionamento da POPI consiste em 3 etapas, ilustradas na Figura 4.10. A primeira etapa (1) consiste nas medições, que são obtidas em uma série de rajadas de mensagens. Na segunda etapa (2) as medições são computadas a fim de obter-se uma ordenação dos tipos de tráfego que sofreram maiores perdas de pacotes, para cada rajada. A terceira etapa (3) consiste em uma análise estatística para verificar se houve priorização de tipos específicos de tráfego ao longo das rajadas. Cada uma destas etapas é descrita abaixo.

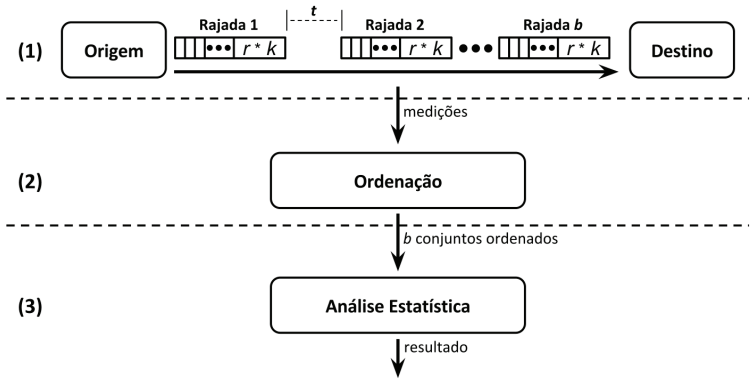


Figura 4.10: Funcionamento da ferramenta POPI.

Na primeira etapa (1), a POPI efetua as medições de perda de pacotes para k tipos de tráfego. As medições são feitas em b rajadas de pacotes, enviados entre um *host* origem e um *host* destino. As rajadas são separadas por intervalos de t segundos. Cada rajada é composta de r rodadas e em cada rodada são enviados k pacotes – um para cada tipo

de tráfego sendo avaliado, em ordem aleatória. Assim, em cada rajada são enviados $r * k$ pacotes em sequência. Segundo os autores, o valor de t não pode ser muito baixo, para que uma rajada não interfira na próxima, mas também não pode ser muito alto para que a medição toda termine dentro de um período curto de tempo, tornando-a menos suscetível a flutuações no tráfego de fundo. Os autores afirmam também que é necessário enviar uma quantidade grande de mensagens para garantir que os roteadores entre a origem e o destino fiquem congestionados e comecem a descartar pacotes, não dependendo assim do tráfego de fundo para tal.

Na segunda etapa (2), as taxas de perda de pacotes para todos os tipos de tráfego em cada rajada são computadas e ordenadas. Nesta ordenação, o tipo de tráfego com a maior taxa de perda de pacotes em uma dada rajada, por exemplo, fica na primeira posição, o tipo com a segunda maior taxa fica na segunda posição e assim por diante. Segundo os autores, se os pacotes de todos os tipos forem tratados de forma neutra, as posições de tipos diferentes formarão arranjos aleatórios ao longo de todas as rajadas, já que a ordem de envio dos pacotes de tipos diferentes em cada rodada é aleatória. Porém, caso alguns tipos de tráfego tenham baixa prioridade, estes tipos estarão sempre nas primeiras posições da ordenação. Assim, ao fim desta etapa, tem-se b conjuntos de tipos de tráfego – um para cada rajada – ordenados conforme as taxas de perda de pacotes observadas em cada rajada.

Na terceira etapa (3), é feita uma análise estatística para verificar se houve priorização de tipos específicos de tráfego ao longo das rajadas. Segundos os autores, se a POPI comparasse apenas dois tipos de tráfego diferentes, bastaria determinar se estes tipos foram tratados de forma diferente comparando as medições obtidas para cada um. Porém, para analisar mais de dois tipos de tráfegos é necessário agrupá-los conforme suas prioridades. Verificar se as posições relativas de k valores repetem-se de forma consistente ao longo de b observações é um problema estatístico conhecido como *"Problem of N Rankings"* [Noether 2012]. A solução adotada na POPI foi calcular uma média das posições de cada tipo de tráfego em todas as rajadas (*Average Normalized Ranks*) e agrupar os tipos cujas médias não apresentam diferença significativa. Este agrupamento é feito utilizando um método hierárquico divisivo. Ao fim deste processo, tem-se grupos de tipos de tráfego ordenados conforme suas prioridades. Em uma rede neutra, esta análise resulta em apenas um grupo, já que todos os tipos de tráfego apresentam a mesma taxa média de perda de pacotes e, portanto, têm a mesma prioridade.

Para avaliar a POPI, os autores primeiramente realizaram simulações utilizando o simulador de rede NS2. Nestas simulações foram utilizados dois pares de *hosts* origem/destino. Um destes pares foi responsável por simular o tráfego de fundo, enquanto o outro par simulou a execução da POPI. Na topologia usada nas simulações, a comunicação entre ambos os pares atravessa os mesmos dois roteadores, responsáveis por simular a priorização de determinados tipos de tráfego, com uma largura de banda máxima de 100 Mbps. O valor utilizado nas simulações para k e b foi 32, ou seja, 32 tipos de tráfego e 32 rajadas. Foram utilizados valores incrementais para r – a quantidade de rodadas por rajada. A taxa de envio do tráfego de fundo também variou de 10 a 90 Mbps. Os resultados obtidos nestas simulações mostraram que a POPI foi capaz de obter bons resultados mesmo na presença de uma grande quantidade de tráfego de fundo: os pacotes de baixa prioridade foram sempre descartados antes dos de alta prioridade. Outro resultado obtido

foi quanto ao valor de r. Para $r < 18$ o tráfego de medição não foi capaz de congestionar as filas dos roteadores, não gerando nenhuma perda de pacotes, impossibilitando assim a inferência. Conforme o valor de r aumenta, a perda de pacotes começa a ser observada de forma mais frequente para os tipos de tráfego de baixa prioridade. Com base nos resultados, os autores afirmam que $r > 30$ é suficiente para obter resultados confiáveis. Assim, foi utilizado $r = 40$ nos experimentos conduzidos no PlanetLab, descritos abaixo.

Foram conduzidos experimentos no PlanetLab para avaliar a POPI em um ambiente real e encontrar possíveis casos reais de priorização. Nestes experimentos foram utilizados 162 nodos do *testbed*, espalhados em diversos continentes. A POPI foi executada em todos os pares de nodos e em ambos os sentidos para cada par. Os valores utilizados das variáveis foram: $k = 26$, $b = 32$, $r = 40$ e $t = 10s$. O tamanho dos pacotes enviados foi de 1500 *bytes* cada, o que gerou um consumo de banda médio de 1.04 Mbps. Os resultados obtidos indicaram que houve algum tipo de priorização de pacotes para 15 pares de nodos. Os autores também executaram a POPI utilizando outras métricas com menor sobrecarga de medição, descritas acima. Os resultados para estas outras métricas mostraram que estas não foram capazes de detectar muitos dos casos de priorização detectados nos experimentos que utilizaram a taxa de perda de pacotes como métrica.

4.5.10. Resumo Comparativo das Soluções

Um resumo comparativo das soluções é mostrado na Tabela 4.1. Para cada solução, a Tabela mostra a topologia de medição utilizada, a(s) métrica(s) empregada(s), que tipo de comparação é feita (tráfegos de tipos diferentes, por exemplo), resultados obtidos e observações específicas sobre a solução e suas limitações.

4.5.11. Outras Soluções Relacionadas

Esta subseção descreve outros trabalhos relacionados à NR que não se referem diretamente à detecção de DT. Estes outros trabalhos tratam de outras práticas que também podem ser consideradas como violações da NR, por exemplo censura ou qualidade de serviço inferior à contratada, além de outras soluções que podem ser utilizadas no contexto da NR.

Soluções que medem a **qualidade do serviço de ISPs** efetivamente entregue ao usuário e/ou monitoram a conformidade do serviço fornecido com acordos de nível de serviço (SLA – *Service-Level Agreement*), também têm relação com a NR, já que a normatização da NR de alguns países incluem estes temas. É importante destacar que algumas destas soluções surgiram devido à preocupação de governos em garantir o cumprimento da NR em relação a estes quesitos. Existem diversos trabalhos [Bischof et al. 2012, Sánchez et al. 2011, Aida et al. 2003, SamKnows , Ookla , TestMy.net , Broadband Speed Checker , NIC.br , Sommers et al. 2007, Sommers et al. 2010, Ta and Mao 2006, Serral-Gracia et al. 2009, Qiu et al. 2008, Serral-Gracià et al. 2010, Yuksel et al. 2010, Hourton et al. 2012] focados em resolver estas questões, não necessariamente motivados pelo debate da NR.

A HAKOMetar [Weber et al. 2013] é uma ferramenta que permite a um usuário final verificar a qualidade de serviço que seu ISP está lhe fornecendo. Esta ferramenta foi desenvolvida pela HAKOM, a agência reguladora das telecomunicações da Croá-

Tabela 4.1: Comparação das características principais das soluções.

Solução	Medição	Métrica	Comparação	Resultados	Observações
Glasnost	Entre um *host* final e um servidor de medição	Taxa de transferência	Aplicação **X** Dados aleatórios	10% dos usuários sofreram DT de BitTorrent e 6% relataram possíveis falso-negativos	Detecta apenas DT baseada em porta e protocolo de aplicação
NetPolice	A partir de diversos *hosts* finais	Perda de pacotes (das respostas ICMP)	Diversos protocolos **X** HTTP	4 dos 18 ISPs avaliados realizaram DT em 4 aplicações e 10 ISPs realizaram DT baseada no AS anterior dos pacotes	Requer acesso a múltiplos *hosts* e a medição depende de respostas ICMP, que nem sempre são suportadas
DiffProbe	Entre um *host* final e um servidor de medição	Atraso e perda de pacotes	Skype/Vonage **X** Dados aleatórios	Simulações e experimentos em ambiente emulado mostraram que a detecção foi precisa.	Primeiramente congestiona a rede, inserindo uma grande quantidade de tráfego artifical na rede
Tomografia	Fim-a-fim entre diversos pares de *hosts*	Qualquer métrica aditiva	Técnica de tomografia de redes	Em ambiente emulado, o algoritmo inferiu corretamente a presença e localização da DT	É necessário conhecer a topologia da rede e ter acesso a uma grande quantidade de *hosts*
NANO	Captura passivamente o tráfego real de aplicações	Depende da aplicação	Mesma aplicação em ISPs diferentes	Em ambiente emulado, a NANO foi capaz de detectar DT praticada de diferentes formas e para diferentes tipos de aplicação	Caso as variáveis de confusão não forem todas conhecidas, a inferência pode ser efetuada erroneamente.
Gnutella RSP	Induz clientes Gnutella a tentarem se conectar a um servidor de medição	Bloqueio de portas	Diversos protocolos (número das portas)	Houve bloqueio de pelo menos 1 porta em 256 de 31 mil prefixos e as portas mais bloqueadas foram a 136 e as referentes aos serviços FTP, SSH, Bittorrent e VPNs	Explora o procedimento de ingresso de novos clientes na rede Gnutella, detectando DT baseada em bloqueio de portas
Packsen	Entre um *host* final e um servidor de medição	Tempos de chegada dos pacotes	Aplicação **X** Não-discriminado	Em um *testbed* local, a Packsen detectou com baixa margem de erro tanto a presença e parâmetros da DT, mesmo na presença de tráfego de fundo	Assume a presença de um modelador de tráfego e envia uma grande quantidade de dados para forçar este modelador a enfileirar os pacotes
ChkDiff	Reproduz tráfego real (previamente capturado) a partir de um *host* final	Atraso e perda de pacotes (das respostas ICMP)	Cada fluxo **X** Restante do tráfego	Em ambiente emulado, a ChkDiff detectou com baixa margem de erro os casos de DT por limitação de banda e por descarte de pacotes	A medição depende de respostas ICMP, que nem sempre são suportadas
POPI	Entre dois *hosts* finais	Perda de pacotes	Diversas aplicações são agrupadas conforme similaridade das medições	Experimentos com 162 nodos espalhados em diversos continentes mostraram que houve DT em 15 pares de nodos.	Congestiona a rede antes de efetuar medições enviando grande quantidade de dados

cia. A estratégia da agência em relação à NR é utilizar a HAKOMetar para aumentar a transparência e competitividade no mercado de banda larga do país. O desenvolvimento da ferramenta baseou-se em resultados anteriores acerca de práticas de gestão de tráfego, obtidos em experimentos conduzidos em ambientes de teste na Croácia [Jukic et al. 2011]. A medição da HAKOMetar é feita em três etapas. Na primeira etapa são recolhidos dados sobre o *host* em que a HAKOMetar está sendo executado e sobre sua rede local. Na segunda etapa, mede-se a taxa de envio e recebimento de dados entre o cliente e o servidor, assim como outras propriedades como latência. Na última etapa, a HAKOMetar cria uma grande quantidade de conexões em paralelo com diversos destinos

diferentes, transferindo uma grande quantidade de dados entre o cliente e estes destinos (usando HTTP e/ou FTP). A partir dos resultados da medição, o usuário pode comparar se a largura de banda medida é a mesma que a contratada. Segundo os autores, os resultados reais obtidos com a HAKOMetar indicam que a ferramenta efetivamente aumentou a transparência do mercado de banda larga na Croácia, já que os consumidores passaram a poder verificar se a qualidade do serviço fornecido pelos ISPs estava de acordo com a contratada. Os autores também afirmam que ainda é necessário incluir mais medições na ferramenta para que ela possa ser usada para detectar violações da NR.

A Adkintun [Bustos-Jiménez et al. 2013] é uma solução para monitoramento da qualidade do serviço de banda larga no Chile. A solução foi desenvolvida pelo *NIC Chile Research Labs* à pedido da Secretaria Nacional de Telecomunicações do Chile (SUBTEL), com o objetivo de monitorar o cumprimento da Lei de NR vigente no país. As medições da Adkintun são efetuadas periodicamente por um *software* cliente instalado nos *hosts* dos usuários finais ou embarcado em roteadores residenciais fornecidos a alguns usuários selecionados. Um servidor central informa periodicamente aos *softwares* cliente quais medições devem ser feitas e quais *hosts* destino devem ser utilizados nestas medições. As medições da Adkintun incluem disponibilidade, taxa de transferência, latência, perda de pacotes, bloqueio de portas, entre outras. Os *hosts* destino utilizados nas medições podem estar localizados dentro da infraestrutura do ISP do cliente, em outro ISP chileno ou ainda em uma localização internacional, dependendo da medição. Todas as medições são coletadas por um servidor central, que disponibiliza todos os resultados publicamente em uma página Web. Assim, é possível consultar dados históricos da qualidade de serviço de cada ISP chileno monitorado pela Adkintun. Os autores afirmam que a Adkintun tem proporcionado aos cidadãos meios para proteger seus direitos, já que os resultados obtidos pela ferramenta estão sendo utilizados como base para reclamações de usuários contra a má qualidade dos serviços prestados por ISPs e até mesmo como evidência em processos judiciais envolvendo a SUBTEL e ISPs. Também foi desenvolvida uma versão da ferramenta para redes móveis, a Adkintun Mobile [Bustos-Jiménez et al. 2013, Lalanne et al. 2015]. Esta versão utiliza uma combinação de medições passivas com algumas medições ativas efetuadas em dispositivos móveis, com o objetivo de monitorar a qualidade do serviço de Internet móvel no Chile.

Além da qualidade de serviço, a liberdade de escolha dos usuários quanto ao conteúdo que desejam acessar também está inserida no contexto da NR. Assim, trabalhos sobre **detecção de censura na Internet** também têm relação com o tema. A censura na Internet ocorre, por exemplo, quando usuários têm seu acesso bloqueado a determinadas páginas Web ou serviços. Existem diversas soluções para detecção de censura [Sfakianakis et al. 2011, Net Neutrality Monitor , Hwang 2007, Network of Excellence in InterNet Science , Filasto and Appelbaum 2012]. Estas soluções monitoram a rede efetuando medições periodicamente, criando assim um "censo" sobre assuntos, serviços e páginas Web bloqueados e/ou filtrados. Um *survey* bastante completo sobre detecção de censura na Internet foi publicado recentemente [Aceto and Pescapé 2015].

Um tema relacionado à censura é a **modificação de conteúdo**. Exemplos desta prática incluem: alterar o conteúdo de uma página Web (inserindo anúncios, por exemplo), injetar pacotes forjados em um fluxo de comunicação ou ainda modificar o conteúdo dos pacotes (prejudicando a integridade dos dados transferidos por BitTorrent, por exem-

plo). Existem algumas soluções para detectar estes tipos de práticas. A Switzerland [Electronic Frontier Foundation] é uma ferramenta para a detecção de modificação e injeção de pacotes de dados trafegando na Internet. Já em [Reis et al. 2008] os autores apresentam uma solução para detectar modificações feitas em páginas Web no caminho entre o servidor e o usuário final, como inserção de anúncios e códigos maliciosos, por exemplo.

Diversos trabalhos sobre **medições de rede** podem ser utilizados no contexto de NR. Os dados coletados por plataformas e serviços de medição [Dhawan et al. 2012, Dischinger et al. 2007, Mahajan et al. 2008, Bischof et al. 2011, Sánchez et al. 2013, Dovrolis et al. 2010, Trestian et al. 2009, Antoniades et al. 2010, Miorandi et al. 2013, Molavi Kakhki et al. 2015] podem ser utilizados para detecção de violações da NR. Estas soluções monitoram continuamente diversas propriedades da rede de diversos ISPs, possibilitando também uma comparação de desempenho entre ISPs distintos. Um *survey* completo sobre plataformas de medição na Internet foi publicado recentemente [Bajpai and Schönwälder 2015]. Diversas técnicas para medição de rede e geração de tráfego [Vishwanath and Vahdat 2009, Michaut and Lepage 2005, Basso et al. 2013, Kanuparthy and Dovrolis 2011, Cheng et al. 2004, Botta et al. 2012, Detal et al. 2013] também podem ser utilizadas na detecção de DT (empregando tipos diferentes de tráfego) e para medir qualidade de serviço de ISPs. São descritos abaixo alguns trabalhos sobre medição de rede diretamente voltados para a obtenção de dados que podem ser utilizados na detecção de algum tipo de violação da NR.

A Neubot (*Network Neutrality Bot*) [Martin and Glorioso 2008, Basso et al. 2011] é uma plataforma de *software* para a obtenção contínua de medições distribuídas na Internet. A Neubot permite a implementação de ferramentas e estratégias para verificar a qualidade do serviço oferecido por ISPs, conforme diferentes protocolos e/ou aplicações são utilizados nas medições. As medições implementadas na Neubot são executadas periodicamente em *hosts* finais e todos os dados obtidos são disponibilizados publicamente. As medições de rede já implementadas pela Neubot incluem os protocolos HTTP, BitTorrent, RTP, VoIP, entre outros. Destaca-se que a Neubot não implementa a detecção de violações da NR propriamente dita, servindo para obtenção de medições que poderão ser utilizadas para tal. Desde fevereiro de 2012 a Neubot efetua suas medições dentro da plataforma de medição Measurement Lab [Dovrolis et al. 2010], utilizando os diversos servidores de medição disponibilizados pela plataforma. Os autores afirmam que a grande quantidade de dados de medição referentes à qualidade da Internet de usuário finais permite uma análise sistemática dos serviços de Internet sendo oferecidos pelos ISPs. Os autores afirmam ainda que os os dados coletados pela Neubot podem trazer um melhor entendimento da NR baseado em dados reais, contribuindo assim com o atual debate mundial.

O Netalyzr [Kreibich et al. 2010] é um serviço de medição de rede proposto no contexto da NR. O objetivo deste serviço é avaliar a conexão de Internet de usuários finais, coletando dados que podem ser utilizados para identificar violações da NR e problemas de rede. O projeto do Netalyzr visa abranger a maior quantidade possível de métricas e ser de fácil utilização por usuários sem conhecimento técnico. O Netalyzr é implementado como um *applet* Java (executado em um navegador) que se comunica com diversos servidores de medição. São efetuadas diversas medições referentes a diversos protocolos (como TCP,

UDP, HTTP e DNS), à rede local do usuário (como NAT e *buffers*), ao ISP de acesso (como suporte IPv6, modificação de conteúdo, filtragem de portas, largura de banda e latência), entre outras. Além de informar as medições ao usuário, a ferramenta também funciona como um serviço de monitoramento contínuo de *hosts* na borda da Internet, já que armazena todas as medições feitas pelos diversos usuários finais na Internet. Assim, tem-se uma grande base de dados que pode ser utilizada para a detecção de diversas características da rede, inclusive para estudos referentes à NR. Os autores apresentam uma análise sobre 130.000 medições registradas pelo Netalyzr, as quais foram disponibilizadas publicamente.

A NNMA (*NNSquad Network Measurement Agent*) [Network Neutrality Squad] é uma ferramenta que monitora a atividade de rede dos *hosts* em que está instalada. Este monitoramento tem como objetivo obter diversas medições de rede que possam posteriormente auxiliar na detecção de violações da NR e problemas na rede. No contexto de NR, a principal medição feita pela NNMA é a identificação de pacotes forjados do tipo RST (*reset*) do protocolo TCP. Um pacote RST indica que um dos *hosts* encerrou a conexão e não irá mais enviar ou receber pacotes. ISPs podem injetar pacotes RST forjados para encerrar conexões referentes à algum tipo de tráfego específico [Weaver et al. 2009]. A NNMA não efetua nenhuma comparação sobre a quantidade de pacotes RST forjados para o tráfego de diferentes aplicações. Porém, é uma métrica que pode ser utilizada para inferir se um ISP está efetuando DT utilizando tal prática.

4.6. Conclusão

A Neutralidade da Rede é um tema em crescente discussão ao redor do mundo. Conforme crescem a quantidade de usuários e os serviços oferecidos na Internet, práticas de DT tornam-se cada vez mais comuns. É mais barato para os ISPs bloquearem ou degradarem conteúdos que demandem alto desempenho da rede do que investir em melhorias de infraestrutura ou em soluções não discriminatórias. Além do aumento da demanda, muitos ISPs empregam a DT por interesses comerciais, priorizando seus próprios serviços em detrimento dos serviços concorrentes, por exemplo.

Apesar de diversos países já terem criado regulamentações, Leis, entre outros, que exigem redes neutras por parte dos ISPs, fiscalizar se a NR está sendo cumprida pelas operadoras ainda é um desafio. Este minicurso apresentou diversas soluções para a detecção de DT. As soluções apresentadas baseiam-se, em geral, em medições de rede e métodos estatísticos para inferir se um ISP está discriminando um tipo de tráfego de dados em relação a outros. Estas soluções diferem, principalmente, na topologia utilizada para medição, nas métricas empregadas, no tipo de comparação estatística realizada e nos requisitos e limitações das estratégias adotadas.

Também foi apresentada neste minicurso uma introdução sobre o debate da NR e os conceitos relacionados, assim como um panorama da normatização da NR ao redor do mundo. Uma linha do tempo com diversos incidentes relacionados à NR que ocorreram durante o período do debate também foi apresentada, destacando a importância e atualidade do tema.

Espera-se que este minicurso fomente o debate sobre a NR no Brasil, em especial na comunidade de pesquisa em redes de computadores e sistemas distribuídos.

Referências

[Aceto and Pescapé 2015] Aceto, G. and Pescapé, A. (2015). Internet Censorship detection: A survey. *Computer Networks*, 83.

[Aida et al. 2003] Aida, M., Miyoshi, N., and Ishibashi, K. (2003). A scalable and lightweight QoS monitoring technique combining passive and active approaches. In *IEEE INFOCOM*, volume 1.

[American Cable Association 2016] American Cable Association (2016). ACA Statement On Netflix's Throttling Of Wireless Video Streaming Traffic. `http://www.americancable.org/node/5668`. Acessado em 25/01/2017.

[Anderson 2013] Anderson, C. (2013). Dimming the Internet: Detecting Throttling as a Mechanism of Censorship in Iran. `http://arxiv.org/abs/1306.4361`. Acessado em 25/01/2017.

[Antoniades et al. 2010] Antoniades, D., Markatos, E. P., and Dovrolis, C. (2010). *MOR: Monitoring and Measurements through the Onion Router*, pages 131–140. Springer Berlin Heidelberg.

[Austen 2005] Austen, I. (2005). A Canadian Telecom's Labor Dispute Leads to Blocked Web Sites and Questions of Censorship. `http://www.nytimes.com/2005/08/01/business/worldbusiness/a-canadian-telecoms-labor-dispute-leads-to-blocked.html`. Acessado em 25/01/2017.

[Bajpai and Schönwälder 2015] Bajpai, V. and Schönwälder, J. (2015). A Survey on Internet Performance Measurement Platforms and Related Standardization Efforts. *IEEE Communications Surveys Tutorials*, 17(3).

[Bashko et al. 2013] Bashko, V., Melnikov, N., Sehgal, A., and Schönwälder, J. (2013). Bonafide: A traffic shaping detection tool for mobile networks. In *IFIP/IEEE International Symposium on Integrated Network Management (IM)*.

[Basso et al. 2013] Basso, S., Meo, M., and De Martin, J. C. (2013). Strengthening Measurements from the Edges: Application-level Packet Loss Rate Estimation. *SIGCOMM Computer Communication Review*, 43(3).

[Basso et al. 2011] Basso, S., Servetti, A., and Martin, J. C. D. (2011). The network neutrality bot architecture: A preliminary approach for self-monitoring of Internet access QoS. In *Computers and Communications (ISCC), 2011 IEEE Symposium on*.

[Berners-Lee 2010] Berners-Lee, T. (2010). Long Live the Web. *Scientific American*, 303(6).

[Beverly et al. 2007] Beverly, R., Bauer, S., and Berger, A. (2007). The Internet is Not a Big Truck: Toward Quantifying Network Neutrality. In *International Conference on Passive and Active Network Measurement (PAM)*. Springer-Verlag.

[Bischof et al. 2012] Bischof, Z. S., Otto, J. S., and Bustamante, F. E. (2012). Up, Down and Around the Stack: ISP Characterization from Network Intensive Applications. *SIGCOMM Computer Communication Review*, 42(4).

[Bischof et al. 2011] Bischof, Z. S., Otto, J. S., Sánchez, M. A., Rula, J. P., Choffnes, D. R., and Bustamante, F. E. (2011). Crowdsourcing ISP Characterization to the Network Edge. In *SIGCOMM Workshop on Measurements Up the Stack (W-MUST)*. ACM.

[Body of European Regulators for Electronic Communications] Body of European Regulators for Electronic Communications. All you need to know about Net Neutrality rules in the EU. `http://berec.europa.eu/eng/net/introduction`. Acessado em 25/01/2017.

[Body of European Regulators for Electronic Communications 2012a] Body of European Regulators for Electronic Communications (2012a). BEREC Guidelines for quality of service in the scope of net neutrality. `http://berec.europa.eu/eng/document_register/subject_matter/berec/regulatory_best_practices/guidelines/1101-berec-guidelines-for-quality-of-service-in-the-scope-of-net-neutrality`. Acessado em 25/01/2017.

[Body of European Regulators for Electronic Communications 2012b] Body of European Regulators for Electronic Communications (2012b). Summary of BEREC positions on net neutrality. http://berec.europa.eu/eng/document_register/subject_matter/berec/opinions/1128-summary-of-berec-positions-on-net-neutrality. Acessado em 25/01/2017.

[Botta et al. 2012] Botta, A., Dainotti, A., and Pescapé, A. (2012). A Tool for the Generation of Realistic Network Workload for Emerging Networking Scenarios. *Computer Networks*, 56(15).

[Broadband Speed Checker] Broadband Speed Checker. The UK's No.1 Broadband Speed Test. http://www.broadbandspeedchecker.co.uk. Acessado em 25/01/2017.

[Brodkin 2014] Brodkin, J. (2014). Netflix performance on Verizon and Comcast has been dropping for months. *http://arstechnica.com/information-technology/2014/02/netflix-performance-on-verizon-and-comcast-has-been-dropping-for-months*. Accessed in October 19, 2016.

[Bustos-Jiménez et al. 2013] Bustos-Jiménez, J., Del Canto, G., Pereira, S., Lalanne, F., Piquer, J., Hourton, G., Cádiz, A., and Ramiro, V. (2013). How AdkintunMobile Measured the World. In *ACM Conference on Pervasive and Ubiquitous Computing Adjunct Publication (UbiComp)*. ACM.

[Bustos-Jiménez and Fuenzalida 2014] Bustos-Jiménez, J. and Fuenzalida, C. (2014). All Packets Are Equal, but Some Are More Equal Than Others. In *Latin America Networking Conference (LANC)*. ACM.

[Bustos-Jiménez et al. 2013] Bustos-Jiménez, J., Ramiro, V., Lalanne, F., and Barros, T. (2013). Adkintun: SLA Monitoring of ISP Broadband Offerings. In *International Conference on Advanced Information Networking and Applications Workshops (WAINA)*.

[Campbell 2016] Campbell, P. S. (2016). Public Interest Groups Urge FCC Action Against Zero-Rating. http://www.lexology.com/library/detail.aspx?g=e4fbf6ad-03f4-4a04-83c9-f4220c6dea26. Acessado em 25/01/2017.

[Canadian Radio-television and Telecommunications Commission 2009] Canadian Radio-television and Telecommunications Commission (2009). Review of the Internet traffic management practices of Internet service providers. http://www.crtc.gc.ca/eng/archive/2009/2009-657.htm. Acessado em 25/01/2017.

[Carbone and Rizzo 2010] Carbone, M. and Rizzo, L. (2010). Dummynet Revisited. *SIGCOMM Computer Communication Review*, 40(2).

[Cellan-Jones 2009] Cellan-Jones, R. (2009). BT accused of iPlayer throttling. http://news.bbc.co.uk/2/hi/technology/8077839.stm. Acessado em 25/01/2017.

[Cheng et al. 2004] Cheng, Y.-C., Hölzle, U., Cardwell, N., Savage, S., and Voelker, G. M. (2004). Monkey See, Monkey Do: A Tool for TCP Tracing and Replaying. In *USENIX Annual Technical Conference (ATEC)*.

[Coates et al. 2002] Coates, A., III, A. O. H., Nowak, R., and Yu, B. (2002). Internet tomography. *IEEE Signal Processing Magazine*, 19(3).

[Comisión de Regulación de Comunicaciones 2011] Comisión de Regulación de Comunicaciones (2011). Condiciones regulatorias relativas a la neutralidad en Internet. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=45061. Acessado em 25/01/2017.

[Comitê Gestor da Internet no Brasil 2009] Comitê Gestor da Internet no Brasil (2009). Princípios para a Governança e Uso da Internet no Brasil. http://www.cgi.br/resolucoes/documento/2009/003. Acessado em 25/01/2017.

[Cooper and Brown 2015] Cooper, A. and Brown, I. (2015). Net Neutrality: Discrimination, Competition, and Innovation in the UK and US. *ACM Transactions on Internet Technology*, 15(1).

[Crowcroft 2007] Crowcroft, J. (2007). Net Neutrality: The Technical Side of the Debate: a White Paper. *SIGCOMM Computer Communication Review*, 37(1).

[Detal et al. 2013] Detal, G., Hesmans, B., Bonaventure, O., Vanaubel, Y., and Donnet, B. (2013). Revealing Middlebox Interference with Tracebox. In *Internet Measurement Conference*, pages 1–8. ACM.

[Dhawan et al. 2012] Dhawan, M., Samuel, J., Teixeira, R., Kreibich, C., Allman, M., Weaver, N., and Paxson, V. (2012). Fathom: A Browser-based Network Measurement Platform. In *ACM Conference on Internet Measurement Conference (IMC)*. ACM.

[Dischinger et al. 2007] Dischinger, M., Haeberlen, A., Gummadi, K. P., and Saroiu, S. (2007). Characterizing Residential Broadband Networks. In *SIGCOMM Conference on Internet Measurement (IMC)*. ACM.

[Dischinger et al. 2010] Dischinger, M., Marcon, M., Guha, S., Gummadi, K. P., Mahajan, R., and Saroiu, S. (2010). Glasnost: Enabling End Users to Detect Traffic Differentiation. In *USENIX Conference on Networked Systems Design and Implementation (NSDI)*.

[Dischinger et al. 2008] Dischinger, M., Mislove, A., Haeberlen, A., and Gummadi, K. P. (2008). Detecting Bittorrent Blocking. In *SIGCOMM Conference on Internet Measurement*. ACM.

[Dovrolis et al. 2010] Dovrolis, C., Gummadi, K., Kuzmanovic, A., and Meinrath, S. D. (2010). Measurement Lab: Overview and an Invitation to the Research Community. *SIGCOMM Computer Communication Review*, 40(3).

[Dreier 2016] Dreier, T. (2016). Comcast Hit With FCC Complaint Over Net Neutrality Violations. `http://www.streamingmedia.com/Articles/News/Online-Video-News/Comcast-Hit-With-FCC-Complaint-Over-Net-Neutrality-Violations-109609.aspx`. Acessado em 25/01/2017.

[El Congreso de Colombia 2011] El Congreso de Colombia (2011). Plan Nacional de Desarrollo, 2010-2014. `http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101`. Acessado em 25/01/2017.

[Electronic Frontier Foundation] Electronic Frontier Foundation. Switzerland Network Testing Tool. `https://www.eff.org/pages/switzerland-network-testing-tool`. Acessado em 25/01/2017.

[Esnaashari 2014] Esnaashari, S. (2014). Invisible Barriers: Identifying restrictions affecting New Zealanders' access to the Internet. Master's thesis, Victoria University of Wellington. `http://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/3263/thesis.pdf`.

[European Commission 2009] European Commission (2009). EU Telecoms Reform: 12 reforms to pave way for stronger consumer rights, an open internet, a single European telecoms market and high-speed internet connections for all citizens. `http://europa.eu/rapid/press-release_MEMO-09-513_en.htm`. Acessado em 25/01/2017.

[European Commission 2010] European Commission (2010). Digital Agenda: Commission launches consultation on net neutrality. `http://europa.eu/rapid/press-release_IP-10-860_en.htm`. Acessado em 25/01/2017.

[European Commission 2014] European Commission (2014). 2014 Report on Implementation of the EU regulatory framework for electronic communications. `https://ec.europa.eu/digital-single-market/en/news/2014-report-implementation-eu-regulatory-framework-electronic-communications`. Acessado em 25/01/2017.

[European Commission 2015] European Commission (2015). Commission welcomes agreement to end roaming charges and to guarantee an open Internet. `http://europa.eu/rapid/press-release_IP-15-5265_en.htm`. Acessado em 25/01/2017.

[European Parliament and Council of the European Union 2009] European Parliament and Council of the European Union (2009). Regulation 1211/2009 establishing the Body of European Regulators for Electronic Communications. `http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2009.337.01.0001.01.ENG`. Acessado em 25/01/2017.

[Federal Antimonopoly Service 2016] Federal Antimonopoly Service (2016). Creating equal conditions on the market of Internet services. http://en.fas.gov.ru/press-center/news/detail.html?id=44823. Acessado em 25/01/2017.

[Federal Communications Commission 2002] Federal Communications Commission (2002). FCC Classifies Cable Modem Service as "Information Service": Initiates Proceeding to Promote Broadband Deployment and Examine Regulatory Implications of Classification. http://transition.fcc.gov/Bureaus/Cable/News_Releases/2002/nrcb0201.html. Acessado em 25/01/2017.

[Federal Communications Commission 2005] Federal Communications Commission (2005). FCC 05-150. Report and order and notice of proposed rulemaking. https://apps.fcc.gov/edocs_public/attachmatch/FCC-05-150A1.pdf. Acessado em 25/01/2017.

[Federal Communications Commission 2010] Federal Communications Commission (2010). FCC 10-201. Report And Order. https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf. Acessado em 25/01/2017.

[Federal Communications Commission 2014] Federal Communications Commission (2014). Public Notice.DA 14-211.New docket established to address open internet remand GN Docket No. 14-28. https://apps.fcc.gov/edocs_public/attachmatch/DA-14-211A1.pdf. Acessado em 25/01/2017.

[Federal Communications Commission 2015] Federal Communications Commission (2015). Open Internet. https://www.fcc.gov/general/open-internet. Acessado em 25/01/2017.

[Federal Communications Commission 2016] Federal Communications Commission (2016). Remarks of FCC Chairman Tom Wheeler. http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0411/DOC-338806A1.pdf. Acessado em 25/01/2017.

[Filasto and Appelbaum 2012] Filasto, A. and Appelbaum, J. (2012). OONI: Open Observatory of Network Interference. In *USENIX Workshop on Free and Open Communications on the Internet*.

[Flach et al. 2016] Flach, T., Papageorge, P., Terzis, A., Pedrosa, L., Cheng, Y., Karim, T., Katz-Bassett, E., and Govindan, R. (2016). An Internet-Wide Analysis of Traffic Policing. In *ACM SIGCOMM*. ACM.

[Ganley and Allgrove 2006] Ganley, P. and Allgrove, B. (2006). Net neutrality: A user's guide. *Computer Law & Security Review*, 22(6).

[GreatFire.org] GreatFire.org. Expanding Online Freedom of Speech in China and Beyond. https://en.greatfire.org. Acessado em 25/01/2017.

[Guo and Easley 2016] Guo, H. and Easley, R. F. (2016). Network Neutrality Versus Paid Prioritization: Analyzing the Impact on Content Innovation. *Production and Operations Management*, 25(7):1261–1273.

[H. B. Mann 1947] H. B. Mann, D. R. W. (1947). On a Test of Whether one of Two Random Variables is Stochastically Larger than the Other. *The Annals of Mathematical Statistics*, 18(1).

[Habibi Gharakheili et al. 2016] Habibi Gharakheili, H., Vishwanath, A., and Sivaraman, V. (2016). Perspectives on Net Neutrality and Internet Fast-Lanes. *SIGCOMM Computer Communication Review*, 46(1):64–69.

[Hahn and Wallsten 2006] Hahn, R. W. and Wallsten, S. (2006). The Economics of Net Neutrality. *The Economists' Voice*, 3(6).

[Hourton et al. 2012] Hourton, G., Canto, G. D., Bustos, J., and Lalanne, F. (2012). Crowd-measuring: Assessing the quality of mobile Internet from end-terminals. In *International Conference on Network Games, Control and Optimization (NetGCooP)*, pages 145–148.

[Hwang 2007] Hwang, T. (2007). Threat Modeling: Herdict: A Distributed Model for Threats Online. *Network Security*, 2007(8).

[Internet Society] Internet Society. Net Neutrality. http://www.internetsociety.org/net-neutrality. Acessado em 25/01/2017.

[InternetNZ 2015] InternetNZ (2015). Network Neutrality. https://internetnz.nz/content/network-neutrality-discussion-document. Acessado em 25/01/2017.

[Joch 2009] Joch, A. (2009). Debating net neutrality. *Communications of the ACM*, 52(10):14–15.

[Jordan 2009a] Jordan, S. (2009a). Four questions that determine whether traffic management is reasonable. In *IFIP/IEEE International Symposium on Integrated Network Management*.

[Jordan 2009b] Jordan, S. (2009b). Some Traffic Management Practices Are Unreasonable. In *International Conference on Computer Communications and Networks (ICCCN)*.

[Jukic et al. 2011] Jukic, Z., Weber, M., Svedek, V., Vukovic, M., Katusic, D., and Jezic, G. (2011). Technical aspects of network neutrality. In *International Conference on Telecommunications (ConTEL)*.

[Kanuparthy and Dovrolis 2010] Kanuparthy, P. and Dovrolis, C. (2010). DiffProbe: Detecting ISP Service Discrimination. In *IEEE INFOCOM*.

[Kanuparthy and Dovrolis 2011] Kanuparthy, P. and Dovrolis, C. (2011). ShaperProbe: End-to-end Detection of ISP Traffic Shaping Using Active Methods. In *SIGCOMM Conference on Internet Measurement Conference (IM)*. ACM.

[Kendrick 2009] Kendrick, J. (2009). T-Mobile Germany Blocks iPhone Skype Over 3G and WiFi. https://gigaom.com/2009/04/06/t-mobile-germany-blocks-iphone-skype-over-3g-too. Acessado em 25/01/2017.

[K.G. Coffman 2002] K.G. Coffman, A. O. (2002). *Internet Growth: Is There a "Moore's Law" for Data Traffic?* Springer US.

[Kinzinger 2016] Kinzinger, A. (2016). H.R. 2666 - No Rate Regulation of Broadband Internet Access Act. http://www.gop.gov/bill/h-r-2666-no-rate-regulation-of-broadband-internet-access-act. Acessado em 25/01/2017.

[Knutson and Ramachandran 2016] Knutson, R. and Ramachandran, S. (2016). Netflix Throttles Its Videos on AT&T, Verizon Networks. http://www.wsj.com/articles/netflix-throttles-its-videos-on-at-t-verizon-phones-1458857424. Accessed in October 19, 2016.

[Korea Communications Commission 2012] Korea Communications Commission (2012). Annual Report 2011. http://eng.kcc.go.kr/download.do?fileSeq=35215. Acessado em 25/01/2017.

[Kreibich et al. 2010] Kreibich, C., Weaver, N., Nechaev, B., and Paxson, V. (2010). Netalyzr: Illuminating the Edge Network. In *SIGCOMM Conference on Internet Measurement (IMC)*. ACM.

[Krämer et al. 2013] Krämer, J., Wiewiorra, L., and Weinhardt, C. (2013). Net neutrality: A progress report. *Telecommunications Policy*, 37(9).

[Lalanne et al. 2015] Lalanne, F., Aguilera, N., Graves, A., and Bustos, J. (2015). Adkintun Mobile: Towards using personal and device context in assessing mobile QoS. In *International Wireless Communications and Mobile Computing Conference (IWCMC)*.

[Lee 2016] Lee, M. (2016). S.2602 - Restoring Internet Freedom Act. https://www.congress.gov/bill/114th-congress/senate-bill/2602/text. Acessado em 25/01/2017.

[Lessig 2001] Lessig, L. (2001). *The Future of Ideas: The Fate of the Commons in a Connected World*. The Future of Ideas: The Fate of the Commons in a Connected World. Random House.

[Ling et al. 2010] Ling, F.-Y., Tang, S.-L., Wu, M., Li, Y.-X., and Du, H.-Y. (2010). Research on the net neutrality: The case of Comcast blocking. In *International Conference on Advanced Computer Theory and Engineering (ICACTE)*, volume 5.

[Lomas 2016] Lomas, N. (2016). Verizon Accused Of Net Neutrality Foul By Zero-Rating Its Go90 Mobile Video Service. https://techcrunch.com/2016/02/07/verizon-accused-of-net-neutrality-foul-by-zero-rating-its-go90-mobile-video-service. Acessado em 25/01/2017.

[Lu et al. 2010] Lu, G., Chen, Y., Birrer, S., Bustamante, F. E., and Li, X. (2010). POPI: A User-Level Tool for Inferring Router Packet Forwarding Priority. *IEEE/ACM Transactions on Networking (TON)*, 18(1).

[Mahajan et al. 2008] Mahajan, R., Zhang, M., Poole, L., and Pai, V. (2008). Uncovering Performance Differences Among Backbone ISPs with Netdiff. In *USENIX Symposium on Networked Systems Design and Implementation (NSDI)*.

[Maille et al. 2016] Maille, P., Simon, G., and Tuffin, B. (2016). Toward a net neutrality debate that conforms to the 2010s. *IEEE Communications Magazine*, 54(3):94–99.

[Martin and Glorioso 2008] Martin, J. C. D. and Glorioso, A. (2008). The Neubot project: A collaborative approach to measuring internet neutrality. In *IEEE International Symposium on Technology and Society*.

[Michaut and Lepage 2005] Michaut, F. and Lepage, F. (2005). Application-oriented network metrology: metrics and active measurement tools. *IEEE Communications Surveys Tutorials*, 7(2).

[Ministry of Internal Affairs and Communications 2006] Ministry of Internal Affairs and Communications (2006). New Competition Promotion Program 2010. `http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/060928_1.pdf`. Acessado em 25/01/2017.

[Ministry of Internal Affairs and Communications 2007] Ministry of Internal Affairs and Communications (2007). Report on Network Neutrality. `http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/pdf/070900_1.pdf`. Acessado em 25/01/2017.

[Ministry of Internal Affairs and Communications 2008] Ministry of Internal Affairs and Communications (2008). Report from Panel on Neutrality of Networks. `http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/NewsLetter/Vol18/Vol18_23/Vol18_23.html`. Acessado em 25/01/2017.

[Ministério da Justiça] Ministério da Justiça. Marco Civil da Internet. `http://pensando.mj.gov.br/marcocivil/`. Acessado em 25/01/2017.

[Miorandi et al. 2013] Miorandi, D., Carreras, I., Gregori, E., Graham, I., and Stewart, J. (2013). Measuring net neutrality in mobile Internet: Towards a crowdsensing-based citizen observatory. In *IEEE International Conference on Communications Workshops (ICC)*, pages 199–203.

[Molavi Kakhki et al. 2015] Molavi Kakhki, A., Razaghpanah, A., Li, A., Koo, H., Golani, R., Choffnes, D., Gill, P., and Mislove, A. (2015). Identifying Traffic Differentiation in Mobile Networks. In *ACM Conference on Internet Measurement Conference*, pages 239–251. ACM.

[Mr T. 2013] Mr T. (2013). Zambia, a country under Deep Packet Inspection. `https://ooni.torproject.org/post/zambia`. Acessado em 25/01/2017.

[Mueller and Asghari 2012] Mueller, M. L. and Asghari, H. (2012). Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States. *Telecommunications Policy*, 36(6).

[Net Neutrality Monitor] Net Neutrality Monitor. `http://www.neumon.org`. Acessado em 25/01/2017.

[Network Neutrality Squad] Network Neutrality Squad. NNSquad Network Measurement Agent (NNMA). `https://www.nnsquad.org/agent.html`. Acessado em 25/01/2017.

[Network of Excellence in InterNet Science] Network of Excellence in InterNet Science. MorFEO: MOnitoRing network connections to assess Freedom of Expression Online. `http://www.internet-science.eu/open-call-projects/morfeo`. Acessado em 25/01/2017.

[NIC.br] NIC.br. Sistema de Medição de Tráfego Internet (SIMET). `http://simet.nic.br`. Acessado em 25/01/2017.

[Noether 2012] Noether, G. E. (2012). *Introduction to statistics: the nonparametric way*. Springer Science & Business Media.

[Norwegian Communications Authority a] Norwegian Communications Authority. Net neutrality. http://eng.nkom.no/technical/internet/net-neutrality/net-neutrality. Acessado em 25/01/2017.

[Norwegian Communications Authority b] Norwegian Communications Authority. The Norwegian model. http://eng.nkom.no/technical/internet/net-neutrality/the-norwegian-model. Acessado em 25/01/2017.

[Ookla] Ookla. The world standard in Internet metrics. https://www.ookla.com. Acessado em 25/01/2017.

[O'Rielly 2016] O'Rielly, M. (2016). Shining the Spotlight: How FCC Rules Impact Consumers and Industries. https://apps.fcc.gov/edocs_public/attachmatch/DOC-338600A1.pdf. Acessado em 25/01/2017.

[Poder Executivo 2011] Poder Executivo (2011). PL 2126/2011. http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=517255. Acessado em 25/01/2017.

[Presidência da República 2014] Presidência da República (2014). Lei 12965. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acessado em 25/01/2017.

[Presidência da República 2016] Presidência da República (2016). Decreto 8771. http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acessado em 25/01/2017.

[Press Trust of India 2015] Press Trust of India (2015). Net Neutrality debate: TRAI aims to resolve some issues by early 2016. http://indianexpress.com/article/technology/tech-news-technology/trai-aims-to-resolve-some-net-neutrality-issues-by-early-2016. Acessado em 25/01/2017.

[Public Knowledge 2016] Public Knowledge (2016). Petition for the Federal Communications Commission to Enforce Merger Conditions and its Policies. https://ecfsapi.fcc.gov/file/60001526808.pdf. Acessado em 25/01/2017.

[Qazi et al. 2013] Qazi, Z. A., Lee, J., Jin, T., Bellala, G., Arndt, M., and Noubir, G. (2013). Application-awareness in SDN. *SIGCOMM Computer Communication Review*, 43(4).

[Qiu et al. 2008] Qiu, T., Ni, J., Wang, H., Hua, N., Yang, Y. R., and Xu, J. J. (2008). Packet Doppler: Network Monitoring Using Packet Shift Detection. In *ACM CoNEXT Conference*. ACM.

[Ravaioli et al. 2012] Ravaioli, R., Barakat, C., and Urvoy-Keller, G. (2012). Chkdiff: Checking Traffic Differentiation at Internet Access. In *ACM Conference on CoNEXT Student Workshop*. ACM.

[Ravaioli et al. 2015] Ravaioli, R., Urvoy-Keller, G., and Barakat, C. (2015). Towards a General Solution for Detecting Traffic Differentiation at the Internet Access. In *Teletraffic Congress (ITC)*.

[reddit 2014] reddit (2014). I just doubled my PIA VPN throughput that I am getting on my router by switching from UDP:1194 to TCP:443. https://www.reddit.com/r/VPN/comments/1xkbca/i_just_doubled_my_pia_vpn_throughput_that_i_am. Acessado em 25/01/2017.

[Reis et al. 2008] Reis, C., Gribble, S. D., Kohno, T., and Weaver, N. C. (2008). Detecting In-flight Page Changes with Web Tripwires. In *USENIX Symposium on Networked Systems Design and Implementation (NDSI)*.

[Respect My Net] Respect My Net. Report cases of Net Neutrality violations. https://respectmynet.eu. Acessado em 25/01/2017.

[SamKnows] SamKnows. The global platform for internet measurement. https://www.samknows.com. Acessado em 25/01/2017.

[Sánchez et al. 2011] Sánchez, M. A., Otto, J. S., Bischof, Z. S., and Bustamante, F. E. (2011). Dasu - ISP Characterization from the Edge: A BitTorrent Implementation. *SIGCOMM Computer Communication Review*, 41(4).

[Sánchez et al. 2013] Sánchez, M. A., Otto, J. S., Bischof, Z. S., Choffnes, D. R., Bustamante, F. E., Krishnamurthy, B., and Willinger, W. (2013). Dasu: Pushing Experiments to the Internet's Edge. In *USENIX Conference on Networked Systems Design and Implementation*, pages 487–500. USENIX Association.

[Sander Greenland 1999] Sander Greenland, James M. Robins, J. P. (1999). Confounding and Collapsibility in Causal Inference. *Statistical Science*, 14(1).

[Sandvine] Sandvine. Intelligent Broadband Networks. `https://www.sandvine.com`. Acessado em 25/01/2017.

[Scott 2014] Scott, M. (2014). Tim Berners-Lee, Web Creator, Defends Net Neutrality. `http://bits.blogs.nytimes.com/2014/10/08/tim-berners-lee-web-creator-defends-net-neutrality`. Acessado em 25/01/2017.

[Secretaria de Comunicaciones y Transportes 2014] Secretaria de Comunicaciones y Transportes (2014). Ley Federal de Telecomunicaciones y Radiodifusión. `http://www.sct.gob.mx/fileadmin/Comunicaciones/LFTR.pdf`. Acessado em 25/01/2017.

[Serral-Gracia et al. 2009] Serral-Gracia, R., Labit, Y., Domingo-Pascual, J., and Owezarski, P. (2009). Towards an Efficient Service Level Agreement Assessment. In *IEEE INFOCOM*.

[Serral-Gracià et al. 2010] Serral-Gracià, R., Yannuzzi, M., Labit, Y., Owezarski, P., and Masip-Bruin, X. (2010). An efficient and lightweight method for Service Level Agreement assessment. *Computer Networks*, 54(17).

[Sfakianakis et al. 2011] Sfakianakis, A., Athanasopoulos, E., and Ioannidis, S. (2011). CensMon: A Web censorship monitor. In *USENIX Workshop on Free and Open Communications on the Internet*.

[Shankesi 2013] Shankesi, R. (2013). *Friendsourcing to detect network manipulation*. PhD thesis, University of Illinois. `https://www.ideals.illinois.edu/bitstream/handle/2142/45321/Ravinder_Shankesi.pdf`.

[Sommers et al. 2007] Sommers, J., Barford, P., Duffield, N., and Ron, A. (2007). Accurate and Efficient SLA Compliance Monitoring. *SIGCOMM Computer Communication Review*, 37(4).

[Sommers et al. 2010] Sommers, J., Barford, P., Duffield, N., and Ron, A. (2010). Multiobjective Monitoring for SLA Compliance. *IEEE/ACM Transactions on Networking (TON)*, 18(2).

[Subsecretaría de Telecomunicaciones 2010] Subsecretaría de Telecomunicaciones (2010). Consagra el Principio de Neutralidad en la Red para los Consumidores y Usuarios de Internet. `http://www.leychile.cl/Navegar?idNorma=1016570`. Acessado em 25/01/2017.

[Subsecretaría de Telecomunicaciones 2011] Subsecretaría de Telecomunicaciones (2011). SUBTEL instruye y exige a empresas de internet mayor transparencia en planes de banda ancha por Ley de Neutralidad de Red. `http://www.subtel.gob.cl/subtel-instruye-y-exige-a-empresas-de-internet-mayor-transparencia-en-planes-de-banda-ancha-por-ley-de-neutralidad-de-red/`. Acessado em 25/01/2017.

[Subsecretaría de Telecomunicaciones 2014] Subsecretaría de Telecomunicaciones (2014). Ley de Neutralidad y Redes Sociales Gratis. `http://www.subtel.gob.cl/ley-de-neutralidad-y-redes-sociales-gratis/`. Acessado em 25/01/2017.

[Sørensen 2014] Sørensen, F. (2014). Net neutrality and charging models. `http://eng.nkom.no/topical-issues/news/net-neutrality-and-charging-models`. Acessado em 25/01/2017.

[Ta and Mao 2006] Ta, X. and Mao, G. (2006). Online End-to-End Quality of Service Monitoring for Service Level Agreement Verification. In *IEEE International Conference on Networks*, volume 2.

[Tariq et al. 2009] Tariq, M. B., Motiwala, M., Feamster, N., and Ammar, M. (2009). Detecting Network Neutrality Violations with Causal Inference. In *International Conference on Emerging Networking Experiments and Technologies (CoNEXT)*. ACM.

[Telecom Regulatory Authority of India 2016] Telecom Regulatory Authority of India (2016). Prohibition of Discriminatory Tariffs for Data Services. http://www.trai.gov.in/WriteReadData/WhatsNew/Documents/Regulation_Data_Service.pdf. Acessado em 25/01/2017.

[TestMy.net] TestMy.net. Broadband Internet Speed Test. http://testmy.net. Acessado em 25/01/2017.

[Topolski 2007] Topolski, R. (2007). Comcast is using Sandvine to manage P2P Connections. http://www.dslreports.com/forum/r18323368-Comcast-is-using-Sandvine-to-manage-P2P-Connections. Acessado em 25/01/2017.

[Trestian et al. 2009] Trestian, I., Potharaju, R., and Kuzmanovic, A. (2009). Closing the Loop: Feedback at Your Fingertips. http://www.cs.northwestern.edu/~ict992/docs/draft.pdf.

[van Schewick 2016] van Schewick, B. (2016). T-Mobile's Binge On Video Streaming Program. https://prodnet.www.neca.org/publicationsdocs/wwpdf/2216she.pdf. Acessado em 25/01/2017.

[van Schewick and Farber 2009] van Schewick, B. and Farber, D. (2009). Point/Counterpoint: Network Neutrality Nuances. *Communications of the ACM*, 52(2).

[Vishwanath and Vahdat 2009] Vishwanath, K. V. and Vahdat, A. (2009). Swing: Realistic and Responsive Network Traffic Generation. *IEEE/ACM Transactions on Networking*, 17(3).

[Weaver et al. 2009] Weaver, N., Sommer, R., and Paxson, V. (2009). Detecting Forged TCP Reset Packets. In *Network and Distributed System Security Symposium (NDSS)*.

[Weber et al. 2013] Weber, M., Svedek, V., Jukic, Z., Golub, I., and Zuljevic, T. (2013). Can HAKOMetar be used to increase transparency in the context of network neutrality? In *International Conference on Telecommunications (ConTEL)*.

[Weinsberg et al. 2011] Weinsberg, U., Soule, A., and Massoulie, L. (2011). Inferring traffic shaping and policy parameters using end host measurements. In *IEEE INFOCOM*.

[Weitzner 2008] Weitzner, D. J. (2008). Net Neutrality... Seriously this Time. *IEEE Internet Computing*, 12(3):86–89.

[Wu 2002] Wu, T. (2002). A Proposal for Network Neutrality. http://www.timwu.org/OriginalNNProposal.pdf. Acessado em 25/01/2017.

[Wu and Lessig 2003] Wu, T. and Lessig, L. (2003). Ex Parte Submission in CS Docket No. 02-52. http://www.savetheinternet.com/sites/default/files/resources/wu_lessig_fcc.pdf. Acessado em 25/01/2017.

[Yuksel et al. 2010] Yuksel, M., Ramakrishnan, K. K., Kalyanaraman, S., Houle, J. D., and Sadhvani, R. (2010). Quantifying Overprovisioning vs. Class-of-Service: Informing the Net Neutrality Debate. In *International Conference on Computer Communications and Networks*, pages 1–8.

[Zhang et al. 2009] Zhang, Y., Mao, Z. M., and Zhang, M. (2009). Detecting Traffic Differentiation in Backbone ISPs with NetPolice. In *SIGCOMM Conference on Internet Measurement Conference*. ACM.

[Zhang et al. 2008] Zhang, Y., Morley, Z., and Zhang, M. M. (2008). Ascertaining the Reality of Network Neutrality Violation in Backbone ISPs. In *ACM Workshop on Hot Topics in Networks*.

[Zhang et al. 2014] Zhang, Z., Mara, O., and Argyraki, K. (2014). Network Neutrality Inference. *SIGCOMM Computer Communication Review*, 44(4).