PEERING: Um sistema autônomo para nós*

Bruno Vinícius[1], Fábio Dayrell Rosa[1], Brandon Schlinker[2], Kyriakos Zarifis[2], Ítalo Cunha[1], Nick Feamster[3] e Ethan Katz-Bassett[2]

[1] Universidade Federal de Minas Gerais – Belo Horizonte – Brazil

[2]University of Southern California – Los Angeles – EUA

[3]Princeton University – Princeton – EUA

{bruno.avila, dayrell, cunha}@dcc.ufmg.br
{bschlink, kyriakos, ethan.kb}@usc.edu, feamster@cs.princeton.edu

Abstract. *Internet routing suffers from persistent and transient failures, circuitous routes, oscillations, and prefix hijacks. A major impediment to progress is the lack of ways to conduct impactful interdomain research. Most research is based either on passive observation of existing routes, keeping researchers from assessing how the Internet will respond to route or policy changes; or simulations, which are restricted by limitations in our understanding of topology and policy. We propose a new class of interdomain research: researchers can instantiate an AS of their choice, including its intradomain topology and interdomain interconnectivity, and connect it with the "live" Internet to exchange routes and traffic with real interdomain neighbors. Instead of being observers of the Internet ecosystem, researchers become members. Towards this end, we present the* PEERING *testbed. In its nascent stage, the testbed has proven extremely useful, resulting in a series of studies that were nearly impossible for researchers to conduct in the past. In this paper, we present a vision of what the testbed can provide. We sketch how to extend the testbed to enable future innovation, taking advantage of the rise of IXPs to expand our testbed.*

Resumo. *Roteamento na Internet sofre de falhas transitórias e persistentes, rotas tortuosas, oscilações e sequestros de prefixos. O maior obstáculo ao progresso é a falta de meios para conduzir pesquisa impactante sobre roteamento interdomínios. A maior parte dos trabalhos existentes utiliza observações passivas, o que não permite pesquisadores analisarem como a Internet responde a mudanças de políticas de roteamento. Outros trabalhos utilizam simulações que são imprecisas devido ao nosso entendimento limitado da topologia da Internet. Neste artigo apresentamos PEERING, uma nova plataforma para pesquisa em roteamento na qual pesquisadores podem instanciar um sistema autônomo, definindo sua topologia intradomínio e conectividade interdomínios. PEERING conecta o sistema autônomo com a Internet e permite troca de rotas e tráfego com redes vizinhas. Em vez de serem observadores do ecossistema da Internet, pesquisadores passam a ser participantes ativos. Em seu estágio inicial, a plataforma PEERING já se mostrou útil, resultando em uma serie de estudos que eram quase impossíveis para pesquisadores conduzirem no passado. Neste artigo, apresentaremos as funcionalidades da plataforma e como ela pode ser utilizada. Mostramos também como estender e utilizar o PEERING para avaliar novos mecanismos de roteamento.*

PEERING (http://peering.usc.edu) foi originalmente apresentado no XIII ACM Hot Topics in Networks (HotNets), em novembro de 2014. Este artigo resume o original e adiciona uma discussão sobre como utilizar *PEERING* para experimentos.

1. Introdução

Roteamento interdomínios tem muitos problemas. Mecanismos de coordenação e configuração de rotas usados por provedores em suas fronteiras são ineficientes, levando frequentemente a rotas congestionadas ou geograficamente tortuosas [15]. Os provedores de Internet não têm visibilidade para resolver problemas efetivamente, contribuindo para interrupções de longa duração [8]. O protocolo de roteamento interdomínios (BGP) tem convergência lenta e pode apresentar oscilações persistentes [17]. Apesar destes problemas conhecidos, pouco tem mudado em roteamento interdomínios e houve poucas pesquisas impactantes nesta área nos últimos anos.

O progresso é impedido porque os mecanismos para realizar pesquisas em roteamento interdomínios são muito limitados e o caminho para implantar novas soluções, mesmo que de forma incremental, é árduo. A maioria das pesquisas em roteamento interdomínios é baseada em medições de rotas existentes ou em simulações cujo realismo é severamente restrito por limitações em nosso entendimento sobre a topologia [11]. Nós temos uma visibilidade tão limitada em roteamento na Internet que vários trabalhos recentes apenas relatam os detalhes de conjuntos de dados privilegiados ou mostram como fazer medições escaláveis de toda a Internet [4, 11].

Para contornar a falta de controle em medições passivas e a falta de realismo em simulações, argumentamos que precisamos deixar de realizar pesquisas fundamentalmente de forma passiva e externa ao roteamento interdomínios, para sermos participantes ativos no ecossistema de roteamento interdomínios. Exemplos de pesquisadores que participaram ativamente do roteamento interdomínios se provaram úteis [9], mas estes pesquisadores interagiram diretamente com um ou poucos provedores de Internet (ISPs). Esta interconectividade limitada é adequada apenas para certos tipos de experimentos, mas não corresponde à capilaridade de parcerias de troca de tráfego na Internet de hoje. Mesmo esta interconectividade limitada é praticamente impossível de alcançar para a maioria dos pesquisadores mesmo que tenham um prefixo IP e pares (*peers*) BGP para quem anunciá-los. Podemos habilitar uma nova classe de pesquisa, permitindo à cada pesquisador operar seu próprio sistema autônomo (AS) na Internet.

Para este fim, nós apresentamos *PEERING*, uma plataforma de experimentação em roteamento interdomínios. A plataforma tem facilitado muitos estudos que não eram possíveis para pesquisadores acadêmicos no passado [7, 8]. Para encorajar outros a aproveitar as vantagens das capacidades únicas do *PEERING*, nós apresentamos uma visão do que *PEERING* pode prover, como um passo para encorajar a inovação que acreditamos que o *PEERING* pode fomentar. Descreveremos também como utilizar o *PEERING*, além de detalhar as atividades de nossa apresentação no salão de ferramentas.

2. Metas e Requisitos

Nossa abordagem é deixar pesquisadores projetarem seus próprios sistemas autônomos (ASes) experimentais, conectá-los à Internet real, fazer anúncio de prefixos e observar suas rotas na Internet. Apesar deste modelo não permitir atualizar todos os roteadores da Internet com um novo protocolo, esta funcionalidade modela a compatibilidade retroativa que novas soluções precisarão prover para serem implantadas incrementalmente. Esta seção descreve os recursos que a plataforma deve oferecer.

Conectividade realista e rica: Transit Portal [16] e BGP beacons [9] deixaram pesquisadores anunciar rotas, mas conectados a poucos ASes. Transit Portal teve apenas universidades como provedores, o que impedia a execução de experimentos que requeriam conectividade à Internet comercial. Dirigido pelo aumento dos pontos de troca de tráfego (PTTs) com politicas abertas de troca de tráfego e servidores de rotas (route servers) [5], bem como o aumento do consumo de vídeo e necessidade de reduzir custos de trânsito, a Internet mudou de uma hierarquia simples para uma malha rica em parcerias de trocas de tráfego [1]. Para representar de forma realista este cenário, o *PEERING* precisa prover interconectividade difundida em torno do mundo, permitindo pesquisadores realizarem experimentos emulando grandes ASes com milhares de pares, não apenas um pequeno AS.

Controle da topologia e roteamento interdomínios. Pesquisadores devem ter flexibilidade para decidir com quais ASes trocar tráfego bem como onde e quais anúncios fazer. A habilidade de injetar rotas permite observar como ASes reagem a diferentes mudanças de roteamento.

Controle de roteamento e topologia intradomínio. Além do controle de roteamento e tráfego interdomínios, pesquisadores devem ser capazes de definir a topologia, protocolos de roteamento e políticas de roteamento dos ASes que eles projetarem. Plataformas de experimentação existentes geralmente focam somente no controle de domínios inteiros [3] ou somente na interação com outros ASes [9, 16].

Controle de tráfego. Além de anúncios de rotas, pesquisadores devem poder trocar tráfego entre seu experimento e a Internet real.

Habilidade de implantar serviços reais. O *PEERING* deve permitir que pesquisadores executem (protótipos de) serviços que recebem e enviam tráfego. A comunidade de pesquisadores de redes tem aprendido muito a partir de sistemas implantados, tais como CDNs baseadas no PlanetLab [12].

Suporte à pesquisa segura. Além de prover aos pesquisadores estes vários aspectos de realismo e controle, o *PEERING* deve fazer tudo de forma que seja fácil para pesquisadores implantarem seus experimentos, deve suportar múltiplos experimentos simultâneos e deve prover segurança. *PEERING* deve isolar experimentos para que cada um possa fazer decisões de roteamento independentes bem como enviar e receber tráfego sem interferir com os outros experimentos. A plataforma deve proteger a Internet dos experimentos impondo melhores praticas (por exemplo, prevenindo sequestro de prefixos e controlando cuidadosamente a falsificação de endereços de origem [7, 8]). *PEERING* deve prover estabilidade para o resto da Internet, sem reiniciar sessões BGP para reconfigurar o início e término de experimentos. Considerações cuidadosas de segurança vão encorajar operadores de redes, que vão nos ajudar a atingir a conectividade rica necessária para experimentos realistas.

Capacitação do pesquisador. Apesar de sistemas anteriores terem alcançado alguns destes objetivos [13, 16], nossa contribuição é combinar todos eles em uma plataforma aberta. Esta combinação pode melhorar trabalhos existentes e habilitar novas pesquisas.

3. Arquitetura e design

O *PEERING* permite pesquisadores realizarem experimentos com roteamento interdomínios em escala global, executando seus próprios ASes que se conectam com

centenas—eventualmente milhares—de ASes reais em torno do mundo. Nossa abordagem é (1) implantar um AS na Internet; (2) confiar nas tendências em direção a parcerias abertas de troca de tráfego para ajudar a conectar o *PEERING* a milhares de outros ASes ao redor do mundo; (3) permitir aos pesquisadores usarem ferramentas existentes para emular redes intradomínios e serviços de sua escolha; (4) conectar estas redes emuladas ao nosso AS global, permitindo aos pesquisadores trocar rotas e tráfego entre suas redes emuladas e a Internet real. *PEERING* compreende dois tipos de dispositivos: *servidores PEERING* trocam rotas com ASes reais, e clientes *PEERING* se conectam aos servidores para executarem experimentos. A equipe do *PEERING* opera os servidores. Pesquisadores operam os clientes. A figura 1 mostra uma visão global do *PEERING*. Abaixo descrevemos os componentes focando em como eles alcançam as metas acima.

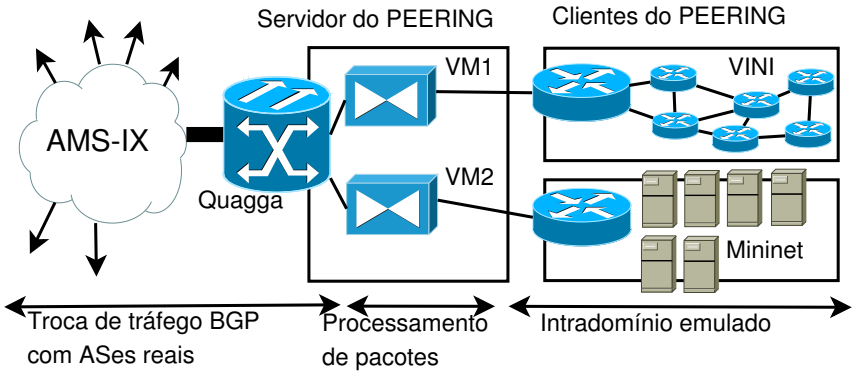

Figura 1. Visão geral da arquitetura do *PEERING*

Alcançando conectividade rica. Nós tiramos vantagem do aumento do papel dos PTTs [1] para prover aos clientes do *PEERING* uma conectividade rica. Muitos PTTs agora oferecem servidores de rotas, que oferecem um ponto central para formação de parcerias multilaterais de troca de tráfego, contornando a necessidade de estabelecer acordos e configurações bilaterais. Através da conexão com o servidor de rota do AMS-IX (Amsterdam Internet Exchange), o *PEERING* instantaneamente estabeleceu conexão com centenas de ASes. Mesmo entre ASes que não se conectam a servidores de rotas, ou em PTTs que não oferecem servidores de rotas, muitos ASes têm políticas abertas de estabelecimento de parcerias, significando que eles estão dispostos a se conectarem com qualquer outro AS sem restrições. Esta política aberta contradiz a visão comum de muitos pesquisadores que para manter essas parcerias de troca de tráfego é necessário troca de tráfego balanceada, dentre outros requisitos. Provedores de conteúdo em particular tendem a utilizar política aberta para estabelecimento de parcerias. Com o crescente número de PTTs e ASes presentes nos PTTs, bem como a prevalência de trocas de tráfego abertas e multilaterais, nós podemos implantar roteadores do *PEERING* em PTTs com expectativa de conseguir atingir conexões com vários ASes comerciais.

Entretanto, manter uma plataforma de experimentação globalmente distribuída requer de atenção operacional. Convenientemente, o crescimento do papel dos provedores de troca remota de tráfego (*remote peering*) implica que nós não precisamos manter uma implantação física grande.

PEERING tem nove servidores em três continentes, duzias de provedores indiretos através de universidades e centenas de pares no AMS-IX e no Phoenix-IX. Outros PTTs

europeus também proveem servidores de rotas com troca de tráfego aberta e a maioria de PTTs tem instalações abertas nos Estados Unidos e na Ásia. Nós estamos expandindo o nosso alcance implantando servidores em grandes PTTs e nos conectando remotamente com PTTs menores.

Controlando o roteamento e topologia interdomínios. *PEERING* é uma extensão do sistema Transit Portal [16] para prover controle sobre o roteamento interdomínios. *PEERING* opera com um numero de AS e prefixos IPv4 próprios. Servidores do *PEERING* executam o software de roteamento Quagga para estabelecer sessões BGP com pares, mas provê experimentos hospedados com controle completo sobre anúncios de prefixos. Um roteador BGP normal com múltiplos pares rodam o processo de seleção de rota BGP, escolhe a melhor rota e exporta esta rota para outros pares. Para prover controle aos pesquisadores, os servidores do *PEERING* não rodam o processo de seleção de rota BGP; em vez disto, eles redistribuem todas as rotas de todos os pares (em vez de apenas a melhor rota) para cada cliente; segundo, clientes podem controlar quais dos seus anúncios vão para cada provedor ou parceiro; terceiro, clientes podem descartar pares para emular uma topologia particular. Combinando tudo isto, é como se os clientes se conectassem diretamente aos pares.

Embora não provenhamos trânsito para destinos que não sejam do espaço de endereçamento do *PEERING*, clientes podem emular múltiplos domínios. Cada domínio emulado usa um número de AS privado "por trás" do *PEERING*. Números de AS privados são retirados dos anúncios BGP repassados para o resto da Internet. Os domínios emulados podem trocar rotas e tráfego entre si diretamente ou através da Internet real. Com apenas um número de AS atualmente, as configurações para certos cenários é complexa. No futuro, nós planejamos adquirir números de AS públicos adicionais para facilitar a implantação e melhorar a flexibilidade de experimentos.

Nossa configuração atual utiliza o Quagga e requer uma conexão entre cliente e servidor para cada par *upstream*, o que não escala para grandes PTTs [16]. Nós planejamos substituir o Quagga por uma solução mais simples capaz de multiplexar sessões *upstream* usando o software de roteamento BIRD.

Controlando roteamento e topologia intradomínio. Uma vez que nós não implantamos uma rede de longa distância com roteadores e enlaces dedicados, nós trabalhamos para oferecer opções flexíveis para que pesquisadores possam encontrar uma que satisfaça suas necessidades. Pesquisadores podem usar plataformas existentes para experimentos intradomínios que podemos combinar com a conectividade interdomínios do *PEERING*. A rede intradomínio pode ser emulada ou real e poderia ser, por exemplo, uma rede definida por software, um data center, ou uma rede de longa distancia. Pode incluir protocolos de roteamento customizados e middleboxes. Alguns experimentos podem usar VINI para realizar experimentos com uma WAN virtualizada geodistribuída [3] interconectando PoPs *PEERING*.

Para outros experimentos, o ambiente Mininet de emulação baseado em contêiner leve pode ser apropriado, permitindo um controle fino de topologias arbitrárias com pouca sobrecarga. Nós desenvolvemos um conjunto de extensões Mininet para habilitar experimentos com topologias intradomínio virtuais no *PEERING* [14].

Controlando o tráfego. Servidores do *PEERING* encaminham tráfego enviado de clientes para provedores por enlaces locais e encaminham tráfego de provedores para clientes

via túneis OpenVPN. Uma vez que o tráfego chega aos clientes, eles podem, por exemplo, encaminhá-lo através de comutadores dentro de uma emulação MinineXt [14] ou através de uma WAN VINI. Estamos estendendo *PEERING* para permitir que pesquisadores executem processamento (leve) de pacotes em máquinas virtuais em nossos servidores. Pretendemos suportar funcionalidades como reescrever campos do cabeçalho, limitar taxas de transmissão, inspecionar o conteúdo de pacotes, ou coordenar com um controlador SDN.

Existem limites para o tráfego que o *PEERING* suporta. Primeiro, nós não assumimos a responsabilidade de transportar tráfego de redes operacionais, por isso apenas transportamos tráfego experimental. Segundo, nós suportamos pequenos volumes de tráfego, pois todo o nosso trafego atravessa a Internet em túneis OpenVPN e algumas universidades têm restrição ao volume de tráfego do *PEERING*. Esta segunda limitação não é fundamental; no futuro, nós planejamos interconectar alguns locais dos servidores com banda dedicada via VINI [3], CloudLab e Internet2.

Desenvolvimento de serviços reais. *PEERING* delega controle de seus prefixos a clientes. Com acesso a estes recursos, pesquisadores podem disponibilizar serviços em endereços IP globais e atrair tráfego. Por exemplo, é possível fazer um anúncio *anycast* de um prefixo a partir de todos os provedores do *PEERING*. Máquinas virtuais em servidores *PEERING* também deixam os serviços processarem tráfego arbitrariamente. As máquinas virtuais permitem flexibilidade, mas causam alta sobrecarga. Pretendemos expor a pesquisadores uma API de processamento de pacotes com menor sobrecarga (por exemplo executando um comutador OpenFlow ou estendendo o iptables do Linux) para cobrir casos comuns de processamento de pacotes. Isto liberaria poder de processamento e permitiria a execução de mais serviços no servidor.

Garantindo segurança. Como servidores estão interpostos entre clientes (de pesquisadores) e a Internet em ambos planos de controle e dados, servidores *PEERING* estão na posição ideal para garantir segurança [16]. Da perspetiva de cada cliente, é essencial ter conexões diretas com provedores. Da perspetiva dos provedores, ele apenas se conecta ao *PEERING*, que mantém uma sessão BGP estável a medida que experimentos são realizados. O *PEERING* impede que experimentos impactem o roteamento de prefixos fora de seu controle aplicando filtros aos anúncios e implantando amortecimento de oscilações (*route-flap dampening*). Clientes não podem sequestrar ou vazar prefixos, nem podem falsificar tráfego de forma incontrolável.

Suportando múltiplos experimentos simultâneos. Cada experimento recebe seu próprio prefixo fornecido pelo *PEERING*, isolando-o dos outros experimentos. A escalabilidade do *PEERING* depende do número de prefixos disponíveis. Alguns pesquisadores ofereceram doações de prefixos IPv4 para o *PEERING* e nós também temos um plano de adicionar suporte a IPv6.

Facilitando a administração e implantação de experimentos. O *PEERING* retira dos pesquisadores o fardo de registrar um AS, de pagar pela alocação de um prefixo IP e de estabelecer parcerias de troca de tráfego ao redor do mundo. O *PEERING* remove obstáculos que poderiam impedir avaliações ou implantações de novas técnicas e serviços em cenários realistas. Estamos implementando um serviço Web para permitir que usuários programem anúncios sem configurar um cliente *PEERING*. O sistema vai notificar os pesquisadores quando seus anúncios serão executados para que eles possam

	PlanetLab	VINI	EmuLab	MiniNet	Route Collectors	Beacons	TransitPortal	**PEERING**
Interdomínio	✗	✗	✗	✗	✗	≈	✓	✓
Conec. rica	✓	✗	✗	✗	✓	✗	✗	✓
Serviços reais	✓	✓	✗	✗	✗	✗	✓	✓
Intradomínio	✗	✓	✓	✓	✗	✗	✗	✓

Tabela 1. Comparação do *PEERING* com outras plataformas.

agendar qualquer medição necessária em seu estudo. Nós também coletamos periodicamente medições no plano de dados e plano de controle para prefixos do *PEERING*. Este serviço tornará mais fácil a realização de experimentos simples.

4. Plataformas de experimentação relacionadas

Experiências bem sucedidas anteriores demonstraram o potencial de novas capacidades do *PEERING*. RON e PlanetLab levaram à uma enxurrada de trabalhos em redes sobrepostas, Emulab possibilitou o trabalho em protocolos e ferramentas de medição, DETER criou um meio para avaliação de segurança e Mininet inspirou trabalhos em SDN [6, 2, 10], os sistemas existentes não alcançaram todos os nossos objetivos, como resumido na tabela 1 e discutido abaixo.

Controle sobre rotas interdomínios. A maioria das plataformas de pesquisas não podem interagir com o plano de controle da Internet. Apenas o Transit Portal [16] e, até certo ponto, faróis BGP [9] fornecem controle sobre as rotas interdomínios.

Conectividade rica. Apenas plataformas que executam em hospedeiros finais, como o PlanetLab [13] ou o RIPE Atlas, têm conectividade rica e geograficamente distribuída. Outras plataformas como VINI, Emulab e Mininet podem trocar tráfego com a Internet apenas em seus pontos de presença.

Suporte para serviços reais. Serviços possuem necessidades específicas, mas exigem no mínimo a execução de código e recursos computacionais. Plataformas que não permitem ao usuário executar código não podem suportar serviços reais.

Controle sobre as rotas intradomínio. Plataformas que são executadas em hospedeiros finais como o Planetlab e RIPE Atlas não podem controlar rotas intradomínio.

5. Salão de ferramentas

Para usar o *PEERING*, um pesquisador precisa entrar em contrato com os administradores do projeto ou submeter uma proposta na página (http://peering.usc.edu). Os administradores alocam prefixos IPs ao pesquisador e configuram os servidores para que o pesquisador consiga anunciar prefixos. O pesquisador deverá configurar um cliente *PEERING* e conectá-lo aos servidores. Após realizar estes passos, o pesquisador já estará apto a fazer anúncios a partir de qualquer servidor do *PEERING*. Para realizar um anúncio, o pesquisador deverá utilizar o Quagga ou executar um *script* que criamos para isto. O anúncio é feito imediatamente e precisamos esperar apenas os anúncios serem repassados para o restante da Internet.

No salão de ferramentas, pretendemos demonstrar o uso de um cliente do *PEERING*, realizando anúncios reais. Iremos verificar a propagação das rotas na Internet usando programas como ping e traceroute bem como servidores de rotas BGP.

6. Conclusão

Apesar dos problemas de longa data com roteamento interdomínios, as soluções tem chegado lentamente, pois são dificultadas pela incapacidade de implementar e testar mecanismos alternativos em um ambiente que é realista o suficiente para ser confiável, controlável o suficiente para ser interessante e seguro o suficiente para realizar experimentos. *PEERING* permite pesquisadores executarem experimentos como parte do ecossistema de roteamento interdomínios da Internet, em vez de serem apenas observadores passivos ou participantes externos.

Agradecimentos. O *PEERING* não seria possível sem cooperação dos administradores de redes que hospedam nossos servidores. Google, NSF (CNS-1351100, CNS-1405754) e CNPq financiaram parcialmente esse trabalho. Nós somos gratos por esse apoio.

Referências

[1] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger. Anatomy of a Large European IXP. In *SIGCOMM*, 2012.

[2] D. G. Andersen, H. Balakrishnan, M. F. Kaashoek, and R. Morris. Resilient Overlay Networks. In *SOSP*, 2001.

[3] A. C. Bavier, N. Feamster, M. Huang, L. L. Peterson, and J. Rexford. In VINI Veritas: Realistic and Controlled Network Experimentation. In *SIGCOMM*, 2006.

[4] X. Cai and J. S. Heidemann. Understanding Block-level Address Usage in the Visible Internet. In *SIGCOMM*, 2010.

[5] N. Chatzis, G. Smaragdakis, A. Feldmann, and W. Willinger. There is More to IXPs than Meets the Eye. *CCR*, 2013.

[6] B. Heller, C. Scott, N. McKeown, S. Shenker, A. Wundsam, H. Zeng, S. Whitlock, V. Jeyakumar, N. Handigol, J. McCauley, K. Zarifis, and P. Kazemian. Leveraging SDN Layering to Systematically Troubleshoot Networks. In *HotSDN*, 2013.

[7] E. Katz-Bassett, H. V. Madhyastha, V. K. Adhikari, C. Scott, J. Sherry, P. van Wesep, T. E. Anderson, and A. Krishnamurthy. Reverse Traceroute. In *NSDI*, 2010.

[8] E. Katz-Bassett, C. Scott, D. R. Choffnes, I. Cunha, V. Valancius, N. Feamster, H. V. Madhyastha, T. E. Anderson, and A. Krishnamurthy. LIFEGUARD: Practical Repair of Persistent Route Failures. In *SIGCOMM*, 2012.

[9] Z. M. Mao, R. Bush, T. Griffin, and M. Roughan. BGP Beacons. In *IMC*, 2003.

[10] J. Mirkovic, H. Shi, and A. Hussain. Reducing Allocation Errors in Network Testbeds. In *IMC*, 2012.

[11] R. V. Oliveira, D. Pei, W. Willinger, B. Zhang, and L. Zhang. The (In)completeness of the Observed Internet AS-level Structure. *IEEE/ACM Trans. Netw.*, 2010.

[12] V. S. Pai, L. Wang, K. Park, R. Pang, and L. L. Peterson. The Dark Side of the Web: An Open Proxy's View. *CCR*, 2004.

[13] L. Peterson, A. Bavier, M. Fiuczynski, and S. Muir. Experiences Building PlanetLab. In *OSDI*, 2006.

[14] B. Schlinker, K. Zarifis, I. Cunha, N. Feamster, E. Katz-Bassett, and M. Yu. Try before you buy: Sdn emulation with (real) interdomain routing. In *Open Networking Summit*, 2014.

[15] N. T. Spring, R. Mahajan, and T. E. Anderson. The Causes of Path Inflation. In *SIGCOMM*, 2003.

[16] V. Valancius, N. Feamster, J. Rexford, and A. Nakao. Wide-Area Route Control for Distributed Services. In *USENIX ATC*, 2010.

[17] K. Varadhan, R. Govindan, and D. Estrin. Persistent Route Oscillations in Inter-domain Routing. *Computer Networks*, 2000.