



<b>Evento</b>	Salão UFRGS 2018: SIC - XXX SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
<b>Ano</b>	2018
<b>Local</b>	Campus do Vale - UFRGS
<b>Título</b>	A Caminho do Entendimento das Dinâmicas Ocultas das Interconexões de IXPs Sobre a Infraestrutura da Internet
<b>Autor</b>	LAURIEN SANTIN
<b>Orientador</b>	ANTONIO MARINHO PILLA BARCELLOS

UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL  
**A Caminho do Entendimento das Dinâmicas Ocultas das Interconexões de IXPs Sobre a  
Infraestrutura da Internet**

Autor: Laurien Santin  
Barcellos

Orientador: Marinho P.

A topologia da Internet se transformou bastante nos últimos anos, se tornando atualmente fortemente conectada e plana. Essa transformação se deve em grande parte à popularização dos pontos de troca de tráfego (IXPs, de Internet eXchange Points), que servem como ponto central de interligação entre dezenas ou centenas de sistemas autônomos (ASes, de Autonomous Systems). Há mais de 800 IXPs espalhados pelo mundo, e os maiores transportam vários Terabits de tráfego por segundo. Apesar de sua relevância para o ecossistema da Internet, os estudos anteriores deixaram de considerar a estrutura interna de IXPs, estudando os mesmos como caixas-preta. As relações entre IXPs, suas *colocation facilities* e os ASes interligados são altamente dinâmicas. O tráfego interno presencia mudanças bruscas com certa frequência, devido às alterações nesses vínculos. Oscilações repentinas podem afetar o desempenho observado externamente ao IXP. Nesse contexto, dois temas fundamentais foram explorados: estabilidade e segurança.

No primeiro tema, foram estudados os detalhes da infraestrutura física básica dos IXPs. Denominada *switching fabric*, é composta por um conjunto de *Colocation Facilities* e interconexões com ASes. Ela é propícia como ponto de observação de ataques, congestionamento e outros aspectos da rede. Entretanto, essas informações não são normalmente divulgadas para o público. Por isso, vários métodos, com diferentes níveis de sucesso, existem para fazer uma estimativa das *coordenadas geográficas de interconexões*. Um exemplo recente que apresenta boa acurácia na inferência das interconexões de ASes e Colocation Facilities é o *Constrained Facility Search* [2]. Um trabalho foi desenvolvido sobre essa metodologia, para torná-la funcional para execuções periódicas e formar uma base histórica.

No segundo tema, com foco em segurança, foi abordado o problema da existência de tráfego ilegítimo na Internet. A diversidade de ASes participantes e, portanto, de tráfego que passa pela malha de IXPs também faz deles bons lugares para estudo de certos padrões de tráfego. O protocolo IP, enquanto funciona como uma boa abstração para encaminhamento de pacotes a nível de roteador, não fornece nenhuma garantia da identidade da origem do pacote. Assim, a falsificação do IP de origem (*spoofing*) viabiliza uma série de ameaças, como ataques de negação de serviço. Uma avaliação preliminar foi realizada com um método baseado no desenvolvido por Lichtblau et al. em [3]. Para tanto, análises estão sendo realizadas sobre fluxos de tráfego coletados em um IXP de médio porte. Um conjunto de categorias e subcategorias foi definido como parte de uma nova metodologia que está sendo proposta para avaliar o comportamento do tráfego e compreender o comportamento observado em cada uma dessas categorias.

**Referências:**

- [1] B. Ager, N. Chatzis, A. Feldmann, N. Sarrar, S. Uhlig, and W. Willinger, “Anatomy of a large european ixp,” in Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, ser. SIGCOMM ’12, Helsinki, Finland: ACM, 2012, pp. 163–174, isbn: 978-1-4503-1419-0.
- [2] V. Giotsas, G. Smaragdakis, B. Huffaker, M. Luckie, and k. claffy k., “Mapping Peering Interconnections to a Facility,” in ACM SIGCOMM Conference on emerging Networking EXperiments and Technologies (CoNEXT), Dec. 2015.

[3] F. Lichtblau, F. Streibelt, T. Krüger, P. Richter, and A. Feldmann, “Detection, classification, and analysis of inter-domain traffic with spoofed source ip addresses,” in Proceedings of the 2017 Internet Measurement Conference, ser. IMC ’17, London, United Kingdom: ACM, 2017, pp. 86–99, isbn: 978-1-4503-5118-8.