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

FELIPE MÜLLER IZAGUIRRE

CONFPEERING-IX: Preservando confidencialidade em acordos de interconexão no ambiente de IXP

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

Orientador: Prof. Dr. Marinho Barcellos
Co-orientador: Prof. Me. Pedro Marcos

Porto Alegre
2018

AGRADECIMENTOS

Agradeço a minha família pelo suporte e apoio ao longo de toda graduação. Agradeço aos professores orientadores pela paciência e disposição durante toda a orientação do trabalho. Aos demais amigos, colegas de trabalho e de curso agradeço por sugestões e esclarecimentos de dúvidas técnicas que foram de essencial contribuição para o resultado do trabalho.

RESUMO

Pontos de troca de tráfego (IXP, do inglês *Internet Exchange Point*) desempenham um papel importante no contexto de interconexão de Sistemas Autônomos (AS, do inglês *Autonomous Systems*), comportando até 20% do tráfego inter-domínio na Internet. Por outro lado, o processo de fechamento de acordos é quase arcaico, tipicamente baseado em relacionamentos interpessoais e reputação. Além disso, a maioria dos acordos são estabelecidos de maneira informal apenas. Uma pesquisa recente mostra que garantir a privacidade das políticas de interconexão é um fator importante para operadores de Provedores de Serviços de Internet (ISP, do inglês *Internet Service Providers*). Nesse contexto, o presente trabalho propõe uma plataforma a ser implantada por um IXP para que ASes membros possam fechar acordos de interconexão de forma confidencial, ágil e dinâmica. A plataforma foi implementada como um protótipo, sendo o mesmo usado para uma avaliação de desempenho em condições controladas. Os resultados indicam para uma amostra de 20 ASes que é possível consultar ofertas de interconexão em menos de um segundo e fechar acordos em 40 segundos para 80% do casos.

Palavras-chave: IXP. Peering.

CONFPEERING-IX: Providing privacy on interconnection agreements in an IXP environment

ABSTRACT

Internet Exchange Points (IXPs) play an important role in the Autonomous Systems (ASes) interconnection context on Internet, carrying up to 20% of the inter-domain traffic. On the other hand, the process of establishing interconnection agreements is typically based on archaic ways: interpersonal relationships and reputation. Moreover, most of the agreements are established without a formal contract. A recent survey has shown that keep the privacy of interconnection agreements is important for Internet Service Providers (ISPs) operators. In this context, we propose a platform to be deployed at an IXP for its member ASes to establish interconnection agreements in a private, fast and dynamic way. The proposed platform was implemented as a prototype, which was used in a performance evaluation using a controlled environment. Numerical results for an evaluation with 20 ASes indicate that it is possible to query interconnection offers in less than a second and make agreements in 40 seconds in 80% of the cases.

Keywords: IXP. Peering.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

AS	*Autonomous System*
IDP	*Identity Provider*
ISP	*Internet Service Provider*
IXP	*Internet Exchange Point*
RIR	*Regional Internet Registry*
SLA	*Service Level Agreement*

SUMÁRIO

1 INTRODUÇÃO

A Internet é composta pela interconexão de diversos Sistemas Autônomos (AS, do inglês *Autonomous Systems*) através de acordos de troca de tráfego firmados entre essas entidades. As interconexões podem acontecer de forma direta, interconectando dois ASes através de uma infraestrutura própria, ou através de Pontos de Troca de tráfego (IXP, do inglês *Internet Exchange Points*) (MARCOS et al., 2018a; AUGUSTIN; KRISHNAMURTHY; WILLINGER, 2009). Essas infraestruturas desempenham um papel importante no contexto da Internet fornecendo infraestrutura de conectividade física para ASes. Dados (THE. . . , 2018) do PeerindgDB (PEERINGDB, 2018) de Março de 2016 compilados pelo CAIDA (CAIDA. . . , 2018) mostram que ISPs conectados a portas de até 1Gbps representam 47,4% dos membros conectados a IXPs públicos. No Brasil, 69,6% dos ISPs estão conectados a portas de até 1Gbps em IXPs públicos. Isto mostra que ISPs de menor porte são maioria em ambientes de IXPs públicos.

Nas últimas décadas, percebeu-se o crescimento do número de IXPs e da quantidade de tráfego que passa por eles diariamente, com estimativas mostrando que IXPs carregam de 15% a 20% do tráfego inter-domínio da Internet (RESTREPO; STANOJEVIC, 2012). Apesar disso, em muitos momentos, a concretização de um acordo de troca de tráfego é um processo lento. Estudos mostram que acordos podem levar de dias a semanas para serem fechados, são realizados para durar um longo período de tempo e muitas vezes não são formalizados via contrato (WOODCOCK; FRIGINO, 2016). Com isso, Provedores de Serviço de Internet (ISP, do inglês *Internet Service Providers*) vem buscando alternativas para aprimorar a entrega de tráfego através de *peering* utilizando IXPs ou soluções como Google Espresso (YAP et al., 2017) e Facebook Edge Fabric (SCHLINKER et al., 2017).

Nos últimos anos, o perfil de tráfego na Internet tem mostrado que conteúdos como vídeo sobre demanda, voz sobre IP e video-conferência virão a ocupar grande parte do volume de dados trafegado na rede (VALANCIUS et al., 2008). Esses tipos de aplicações normalmente demandam melhor qualidade de serviço, por exemplo com valores de latência e *jitter* reduzidos, a fim de proporcionar uma boa experiência ao usuário. Por outro lado, estudos mostram que em grande parte do tempo IXPs possuem clientes com portas com capacidade sobrando (MARCOS et al., 2018a), recurso que poderia ser utilizado via engenharia de tráfego para melhorar serviços oferecidos por ISPs. Visto que o processo de fechar um acordo de troca de tráfego com outro ISP é um processo que pode levar

até mesmo semanas, ISPs nem sempre podem contar com o fechamento de um acordo rápido para responder a incidentes repentinos como sobrecarga ou ruptura de um enlace para uma rota existente. Além disso, pesquisas com operadores de ISP mostraram que os mesmos gostariam de poder adaptar suas parcerias e rotas de forma mais ágil e dinâmica (MARCOS et al., 2018b; CHIESA et al., 2017).

Trabalhos como MINT (VALANCIUS et al., 2008) e ChoiceNET (WOLF et al., 2014) propõem melhorar a entrega de tráfego na Internet através de uma plataforma para oferta de troca de tráfego. Entretanto, ambas soluções não se preocupam em garantir a privacidade das informações armazenadas e trocadas entre as entidades participantes, algo que pesquisas recentes (CHIESA et al., 2017; MARCOS et al., 2018b) demostraram ser um fator pertinente para administradores de ISPs. Route Bazaar (CASTRO et al., 2015) é uma proposta para oferta de troca de tráfego com acordos de troca de tráfego e roteamento abordados em uma mesma solução, se inspirando no modelo descentralizado do registro público (do inglês, *public ledger*) para fornecer uma maneira automatizada para ASes estabelecerem e verificarem acordos de troca de tráfego. A proposta entretanto também não garante confidencialidade das informações das rotas disponibilizadas por determinado AS, visto que as ofertas são cadastradas no ledger público e ficam disponíveis para visualização por qualquer membro. Além disso, a proposta tem uma maior complexidade para sua implementação e utilização pelo ISP, necessitando o provisionamento de um equipamento para operações no ledger público demandando consideráveis custos de armazenamento em disco. No mesmo contexto há o Dynam-IX (MARCOS et al., 2018a), um protocolo distribuído para a oferta de rotas e acordos de troca de tráfego em IXPs. Diferente das outras soluções, o Dynam-IX garante a privacidade das informações trocadas entre as entidades, armazenando as políticas de interconexão localmente em cada AS. Por outro lado a complexidade demandada para executar o protocolo pode ser um fator que limite a adesão por ISPs de menor porte que tendem a ser a maioria no IXP (THE..., 2018), e por vez podem não possuir a infraestrutura ou funcionários suficientes para gerir a solução.

Tendo em vista os problemas relacionados ao processo para fechamento de acordos de interconexão em IXPs, no presente trabalho estudamos uma forma de como o IXP pode prover um serviço que facilite a interconexão e acordos de troca de tráfego entre os ASes em seu ambiente, sem comprometer a confidencialidade das informações armazenadas e trocadas entre os membros da infraestrutura. Visto que o IXP seria responsável pela solução, ASes de menor porte que por ventura não possuem recursos disponíveis para

usar uma solução mais complexa poderiam ser beneficiar de um ambiente que facilite o acesso a ofertas de interconexão.

Propondo uma solução para o problema apresentado, este trabalho define uma plataforma centralizada fornecida pelo IXP para oferta e realização de acordos de interconexão. Para garantir a confidencialidade dos dados armazenados e compartilhados foram utilizadas técnicas de criptografia para consulta e armazenamento das informações criadas pelos ASes. ISPs podem utilizar o serviço para buscar e fechar acordos de troca de tráfego. As informações armazenadas pela plataforma são confidenciais e apenas as partes envolvidas possuem acesso.

As contribuições deste trabalho são:

1. Proposta de uma arquitetura de solução centralizada para compartilhamento de ofertas e realização de acordos de interconexão.
2. Implementação de um protótipo da arquitetura proposta que permite que operadores de ISPs cadastrem ofertas de troca de tráfego e realizem acordos. Ao final do acordo uma nota pode ser registrada por ambas as partes a fim de demonstrar o nível de satisfação com o serviço.
3. Avaliação do protótipo implementado com experimentos simulando diferentes números de ASes interagindo com a plataforma, analisando tempo de consulta por ofertas de interconexão, tempo para estabelecimento de acordos de interconexão, espaço de armazenamento necessário pela solução e quantidade de recursos de rede que a solução demanda.

Organizamos o restante deste trabalho da seguinte forma. No Capítulo 2, revisamos fundamentos de interconexão na Internet, bem como técnicas de criptografia para consulta em dados criptografados, conceitos chave para o entendimento deste trabalho. No Capítulo 3, discutimos os principais trabalhos relacionados, diferenciando de nossa proposta. No Capítulo 4, propomos uma plataforma centralizada, adequada a uma implantação em um IXP, para oferta e realização de acordos de interconexão de forma confidencial. No Capítulo 5, apresentamos a metodologia de avaliação e os resultados de experimentos realizados. Por fim, no Capítulo 6, resumimos as principais conclusões do trabalho e discutimos possibilidades de trabalhos futuros.

2 CONCEITOS

Este capítulo aborda conceitos relacionados a proposta do trabalho. Nós discutimos formas e modelos de interconexão entre ASes e conceitos de criptografia de dados, apresentando técnicas que foram estudas e serviram para a construção da proposta.

2.1 Interconexão

ISPs buscam formar acordos de interconexão com outros provedores com o objetivo de ter acesso a diferentes rotas para poder ofertar seus serviços a potenciais clientes. Esta seção apresenta os diferentes tipos e formas de fechar esses acordos.

2.1.1 IXPs

Pontos de troca de tráfego (IXPs) são infraestruturas de interconexão que operam abaixo da camada de rede (nível 3 da pilha da Internet) e tem como propósito facilitar a interconexão e troca de tráfego entre diferentes ASes. Essas infraestruturas devem ter ao menos três ASes presentes e uma clara política para que novos possam se integrar ao IXP (EURO-IX, 2012; CHATZIS; SMARAGDAKIS; FELDMANN, 2013). Em termos de modelos econômicos, estas infraestruturas podem ser separadas em duas categorias: sem fim lucrativos e com fins lucrativos (CHATZIS; SMARAGDAKIS; FELDMANN, 2013). O primeiro modelo é mais comum em países da América Latina, Africa e Europa enquanto que o segundo, na América do Norte (CHATZIS; SMARAGDAKIS; FELDMANN, 2013). Após conectados ao IXP, ASes podem buscar parceiros para firmar acordos de troca de tráfego.

2.1.2 Acordos de troca de tráfego

São relacionamentos de interconexão de redes firmados por dois ASes com o objetivo de trocar tráfego de forma mútua ou prover a um AS acesso a determinadas redes. Acordos podem ser categorizados da seguinte maneira:

- Trânsito: Acordo onde um ISP provê acesso a toda Internet, cobrando pelo serviço

normalmente através da taxa de utilização (MARCOS et al., 2018a), tendo como referência o pico de tráfego em 95% do tempo (DIMITROPOULOS et al., 2009), por exemplo.

- Trânsito parcial: Semelhante ao acordo de Trânsito, porém com acesso limitado a determinadas redes (MARCOS et al., 2018a).
- *Peering*: Acordo onde ambas as partes concordam em dar acesso mútuo às suas redes e trocar tráfego entre si (LUCKIE et al., 2013). O acesso pode ser cobrado ou não, dependendo de quem mais se beneficia do acordo, entre outros fatores (MARCOS et al., 2018a).

2.1.3 Processo de estabelecimento de acordos

Em busca de estabelecer um acordo de interconexão, normalmente as pessoas responsáveis pelos ISPs buscam parceiros através de reconhecimento de marca, contato interpessoal, ou informações obtidas junto a plataformas como PeeringDB (PEERINGDB, 2018) (MARCOS et al., 2018a). Com o intuito de agilizar estes encontros, IXPs e Registros Regionais da Internet (RIR, do inglês *Regional Internet Registry*) organizam reuniões periódicas para promover a interação entre ASes. Após contato inicial e a vontade manifestada de fechar um acordo de interconexão, ASes passam a discutir detalhes do acordo como preço e SLA, por exemplo. Dependendo do modelo é feito um processo de acordo legal, entretanto em outros casos apenas um acordo informal é realizado entre as partes e o acordo segue para a implementação técnica, configurando os roteadores em ambas as partes envolvidas (MARCOS et al., 2018a; MARCOS et al., 2018b).

2.2 Criptografia

No contexto deste trabalho, técnicas criptográficas são necessárias para que informações sobre acordos possam ser armazenadas em uma entidade centralizada, o IXP, permitindo consultas de ASes mas ao mesmo tempo mantendo a confidencialidade de informações que não deveriam ser expostas. A pesquisa nesta área refere-se a consulta em dados criptografados. Nesta seção apresentamos as técnicas de criptografia utilizadas no presente trabalho, com ênfase nas ferramentas e a funcionalidade que as mesmas prestam.

2.2.1 Consulta em dados criptografados

O armazenamento e operação em dados criptografados é objeto de estudo de diversos trabalhos (ARASU et al., 2014; POPA et al., 2014; POPA et al., 2012). Uma forma de manter as informações de acordos armazenadas no IXP é através de um banco de dados, existindo soluções comerciais para armazenar dados de forma criptografada. Entretanto, na maioria das soluções, uma chave privada é utilizada pelo sistema gerenciador do banco de dados para manipular estas informações, mantendo os dados criptografados em disco mas em texto claro quando trabalhando em memória. Uma área de pesquisa bastante atual, a *consulta em dados criptografados*, ou do inglês *query over encrypted data*, estuda uma forma de armazenar e realizar operações em dados em formato criptografado, evitando assim revelar informações para o ambiente em que o sistema de banco de dados opera (POPA et al., 2012).

2.2.2 Consulta por múltiplas palavras-chave em dados criptografados

Uma técnica, em específico, é de interesse a este trabalho: realizar consultas por palavras-chave em dados criptografados, ou do termo em inglês *Keyword search over encrypted data*. Nos trabalhos de (POPA et al., 2012; KAMARA; PAPAMANTHOU; ROEDER, 2012; SONG; WAGNER; PERRIG, 2000), a busca é limitada a uma chave por vez, o que incorre em demasiado custo computacional para uma aplicação de uso real. Alternativamente, a técnica chamada Consulta por multi-palavra-chave em dados criptografados (POPA et al., 2014), ou do inglês *Multi-keyworld search over encrypted data*, foi desenvolvida e possibilita realizar consultas em dados criptografados com menor custo computacional.

A técnica utilizada para compartilhar registros criptografados e realizar consulta nos mesmos funciona da seguinte maneira. Ao passo que os documentos armazenados no servidor estão criptografados com chaves k_1 a k_n, o usuário que for fazer uma busca precisa computar um token *tk* (que representa a palavra a ser buscada em modo cifrado) para a palavra *w* utilizando sua chave privada *uk*, denominando isto por ${tk_{uk}}^{w}$ (POPA et al., 2014). Se o servidor tivesse os tokens ${tk_{uk1}}^{w}$ a ${tk_{ukn}}^{w}$, poderia fazer a comparação com múltiplos documentos criptografados com diferentes chaves (POPA et al., 2014). Dessa forma a ideia é adaptar o token recebido pelo servidor para os diferentes formatos de dados criptografados. Este procedimento é feito através de um delta $\Delta_{\mathrm{uk}\rightarrow\mathrm{ki}}$, que é

um valor criptográfico gerado por usuários que escolheram compartilhar dados com um determinado usuário (POPA et al., 2014). Ao combinar os diferentes deltas gerados por outros usuários com o token de consulta do usuário que esta fazendo a busca no servidor, podemos fazer comparações com dados cifrados por outros usuários.

Portanto, a consulta é feita através da comparação de palavras cifradas com outras palavras cifradas. Ao adaptar uma palavra cifrada por um usuário A para um formato de cifragem de outro usuário B é possível encontrar registros da palavra buscada pelo usuário A nos documentos do usuário B. Esta adaptação é feita pelos valores criptográficos, deltas, gerados pelos usuários que escolheram compartilhar registros com determinado usuário.

3 TRABALHOS RELACIONADOS

Neste capítulo apresentamos trabalhos da área de interconexão de ASes e criptografia que se relacionam à proposta deste trabalho. Discutiremos brevemente o objetivo de cada trabalho e seus principais pontos.

3.1 Interconexão de ASes

Diversos esforços tem buscado melhorar o processo de interconexão de ASes. Para o presente trabalho, estudamos as diferentes abordagens propostas na literatura. Considerando o foco deste trabalho, nos concentramos nas seguintes propostas: MINT (VALANCIUS et al., 2008), ChoiceNet (WOLF et al., 2014), Route Bazaar (CASTRO et al., 2015) e Dynam-IX (MARCOS et al., 2018a). Nesta seção apresentamos esses trabalhos e suas características.

3.1.1 MINT

Os autores em MINT (VALANCIUS et al., 2008) propõem uma suíte de protocolos de roteamento e uma estrutura de mercado para realização de acordos de interconexão de rotas fim-a-fim com certas garantias de qualidade. Os autores argumentam que o roteamento atual na Internet é ineficiente e operadores de ISPs não tem informações suficientes no momento de escolher os melhores parceiros para fechar acordos de interconexão. Com isso, ao contrário de adquirir apenas acesso a redes em um modelo de melhor esforço, MINT introduz um mercado para oferta de rotas fim-a-fim com garantias específicas de qualidade, além de um conjunto de procolos de roteamento, auxiliando na implementação de acordos e provendo informação de métricas aos operadores a fim de ajudar na escolha dos melhores parceiros. Sua estrutura é composta por compradores, vendedores e um mediador. Vendedores oferecem caminhos de rede com determinadas características e preço ao mercado através da plataforma. Compradores por sua vez podem fazer lances por determinados caminhos e características definidas. O mediador tem o papel de casar ofertas de acordos com o melhor preço possível. Após o fechamento do acordo, é feita a configuração dos equipamentos de rede para interligação do segmento proposto.

3.1.2 ChoiceNet

Os autores em ChoiceNet (WOLF et al., 2014) propõem, de forma mais genérica, um plano econômico para serviços na Internet. De acordo com os autores, atualmente consumidores de serviços de Internet não tem outra alternativa a não ser escolher por um provedor de acesso à Internet e pagar pela banda disponibilizada. Dessa forma ao, por exemplo, contratar um serviço de *streaming* de video, consumidores não tem controle sobre a qualidade da rota a ser disponibilizada na utilização do serviço. Nem mesmo o provedor do serviço de streaming tem este controle, restando apenas torcer para que a rota de melhor esforço seja suficiente para oferecer o serviço com qualidade satisfatória (WOLF et al., 2014). Assim, os autores propõem um mercado de serviços de Internet onde consumidores possam escolher determinados serviços em específico, como rotas com certa qualidade, armazenamento de discos em rede, serviço de localização, etc, aumentando com isso a competição dos provedores de serviços na Internet e a qualidade dos serviços disponibilizados a usuários finais. Neste modelo, um consumidor pode também ser um provedor de serviço. Contratos são registrados para cada serviço contratado e o provedor deve fornecer uma prova de que os termos do acordo foram respeitados ao final do contrato.

3.1.3 Route Bazaar

Route Bazaar (CASTRO et al., 2015) é uma plataforma para busca e fechamento de acordos de interconexão com controle de rotas fim-a-fim e uma dada garantia de qualidade de serviço. Os autores do referido trabalho argumentam que os acordos bilaterais de BGP não fornecem as condições necessárias para que ASes firmem acordos de interconexão com controle e qualidade de serviço para rotas fim-a-fim. A solução usa um *ledger* público, uma forma de livro contábil utilizado pelo protocolo *Blockchain*, onde ASes podem ofertar rotas com certa qualidade de serviço e fechar acordos multilaterais. Como o registro de ofertas e acordos fica no ledger público, ASes que não confiem entre si poderiam utilizar esta informação como um mecanismo auxiliar de decisão em busca de parceiros.

3.1.4 Dynam-IX

Os autores em Dynam-IX (MARCOS et al., 2018a) propõem um framework para promoção de acordos de interconexão entre ISPs em um ambiente de IXP. A solução opera de forma distribuída e as informações sobre políticas de interconexão dos ASes são mantidas confidenciais. Através de um mecanismo chamado *Intent Abstraction*, ASes podem buscar por ofertas de interconexão que atendam determinados critérios de qualidade. A proposta utiliza o ledger público para que ASes envolvidos em um acordo registrem uma nota avaliando a experiência que tiveram. Esta avaliação pode ser utilizada como mecanismo de construção de confiança para futuros ASes que busquem por acordos.

3.1.5 Discussão sobre os trabalhos relacionados da área de interconexão

Todos trabalhos relacionados tem como objetivo propor maneiras de melhorar o processo de interconexão de ASes na Internet. As propostas MINT e ChoiceNET focam em aspectos de mercado e procedimento para fechamento de acordos ou contratação de serviços de Internet, por outro lado não se preocupam em garantir confidencialidade das informações armazenadas pelo responsável por administrar a plataforma, critério relevante para operadores de ISPs segundo recentes pesquisas (MARCOS et al., 2018b; CHIESA et al., 2017).

Route Bazaar e Dynam-IX são propostas que focam em acordos de interconexão e atuam de forma distribuída. Ambas as propostas se preocupam em criar um mecanismo de geração de confiança entre ASes que não se conhecem poderem fechar acordos de interconexão, baseando sua escolha em históricos e avaliações de contratos anteriores fornecidos por ASes que mantiveram um acordo. Porém Route Bazaar não fornece mecanismos suficientes para garantir a confidencialidade das políticas de acordos de interconexão de ASes, algo que o Dynam-IX atinge ao armazenar estas informações localmente em cada AS. Estas duas soluções demandam certo esforço em seu provisionamento e uso necessitando de consideráveis recursos computacionais e de pessoal para administrar a ferramenta, algo que ISPs de menor porte, que tendem a ser a maioria em IXPs (THE. . . , 2018), podem não ter disponíveis, o que desestimularia seu uso por estas entidades.

Levando em consideração os fatores relacionados a complexidade de operação e confidencialidade, a presente proposta tem o objetivo de possibilitar que o IXP ofereça um serviço para realização de acordos de interconexão sem revelar informações relativas

a políticas de interconexão ao ambiente em que a solução é administrada. Sendo o IXP o provedor da solução, ISPs de menor porte que por ventura não tenham recursos disponíveis para operar uma solução que demande maiores esforços podem utilizar a plataforma central com pouco esforço operacional. Além disso IXPs poderiam utilizar o serviço como recurso para atrair novos participantes. A tabela 3.1 resume os critérios atingido pelos trabalhos avaliados e a solução aqui proposta.

Tabela 3.1: Tabela com critérios atingidos pelas propostas.

Proposta	**Privacidade**	**Complexidade**
MINT	✗	✓
ChoiceNet	✗	✓
Route Bazaar	✗	✗
Dynam-IX	✓	✗
CONFPEERING-IX	✓	✓

Fonte: Os Autores

3.2 Criptografia

Nesta sessão discutimos trabalhos da área de criptografia que buscam manipular e realizar consulta em dados criptografados, tecnologia habilitadora ao presente trabalho. Nos focamos em duas propostas, mais estreitamente relacionadas: CryptDB (POPA et al., 2012) e Mylar (POPA et al., 2014).

3.2.1 CryptDB

CryptDB (POPA et al., 2012) é uma proposta de sistema gerenciador de banco de dados que garante privacidade nas informações armazenadas, realizando operações em dados criptografados. Através de um mecanismo entre o cliente e o servidor de banco de dados, a solução intercepta consultas SQL e as altera para que possam ser executas nos dados criptografados. Para isto, a solução usa três técnicas: (a) *Estratégia de criptografia levando em consideração SQL*: encriptar os dados em um esquema que seja possível ao servidor executar consultas neles; (b) *Criptografia baseada em consulta ajustável*: os dados são dinamicamente ajustados para o nível de criptografia ideal para realizar a consulta solicitada; e (c) *Consulta ajustável baseado na criptografia*: criptografa os dados em diversas camadas de criptografia que podem ser posteriormente removidas para que

possam ser executadas certos tipos de consultas.

O mecanismo que intercepta as consultas reside entre a aplicação e o sistema de banco de dados. O administrador onde o componente reside poderia ter acesso à chave mestra e assim descriptografar registros armazenados na base de dados; um administrador malicioso poderia ter acesso a informações confidenciais, violando os requisitos estabelecidos no presente trabalho.

3.2.2 Mylar

Mylar (POPA et al., 2014) utiliza a técnica de consulta por multi-palavras-chave em dados criptografados para armazenar e realizar buscas por texto em dados cifrados. Além disso, os registros criptografados criados por um usuário podem ser compartilhados com outros usuários sem comprometer a privacidade das informações armazenadas no sistema de banco de dados. Um mecanismo de encadeamento de chaves é utilizado para compartilhar registros com múltiplos usuários.

A proposta funciona no modelo cliente-servidor, sendo o cliente responsável por criptografar e descriptografar os dados enviados e recuperados do servidor. O servidor executa as consultas nos dados criptografados através do mecanismo de adaptação do token descrito na Seção 2.2.2.

Criptografia assimétrica é utilizada para cifrar as informações armazenadas na base de dados. No momento em que um usuário se registra no sistema, um par de chaves pública e privada é gerado. A chave privada é armazenada no servidor criptografada com a senha que o usuário utiliza para se autenticar na plataforma, enquanto que a chave pública é armazenada em texto claro no servidor e utilizada por outros usuários para compartilhar registros com este.

Mylar necessita de um provedor de identidade (IDP, do inglês *Identity Provider*) para validar a autenticidade das chaves públicas apresentadas pelos usuários. Caso um IDP não seja utilizado, a plataforma gerencia os pares de chave e garante apenas proteção contra ataques passivos. O IDP ou a plataforma também gerenciam *principles* (pares de chave pública e privada) que são utilizados pelos usuários para compartilhar dados entre si.

O compartilhamento de dados criptografados ocorre através da criação e compartilhamento de um principle, que permite acesso a determinados registros para um certo conjunto de usuários. Podemos exemplificar um caso base para o compartilhamento de

um registro da seguinte maneira. O usuário A cria um novo principle P, compartilha este principle com o usuário B cifrando a chave privada do principle P com a chave pública do usuário B. O usuário A armazena um registro na base da dados cifrado com a chave privada do principle P. Como o usuário B tem acesso à chave privada de P, o usuário B pode descriptografar os registros cifrados com a chave privada de P e acessar as informações.

Mylar prove garantias de segurança para ataques passivos (aqueles em que um atacante intercepta o tráfego mas não compromete componentes do sistema) e ataques ativos (onde há invasão de componentes do sistema). Para isso Mylar assume que o desenvolvedor utilizará corretamente a API de programação, que não irá vazar chaves privadas do usuário e não será persuadido a vazar essas chaves através de exploração de bugs. Caso a chave privada de um usuário seja compartilhada indevidamente, registros deste usuários estarão comprometidos e podem ser descriptografados.

O desenvolvedor deve marcar os campos que devem ser criptografados, a serem cifrados com algoritmos de criptografia padrão. Para que possam ser feitas pesquisas por palavras-chave, determinados campos devem ser marcados como *pesquisáveis*, para este tipo de campo as garantias de criptografia são mais fracas e é utilizado o algoritmo de criptografia IND-CPA (Criptografia Randômica).

Dadas estas características, consideramos que a solução satisfaz o requisito de armazenamento confidencial de informações. Assim, adotamos o Mylar para o armazenamento e consulta de ofertas de interconexão de forma confidencial.

4 PROPOSTA

Estudos mostram que IXPs carregam uma significativa fatia do volume de dados trafegado na Internet (RESTREPO; STANOJEVIC, 2012). Percebe-se também que a crescente demanda por serviços que exigem maior qualidade das rotas e interconexões é uma tendência na rede (VALANCIUS et al., 2008). Visto que IXPs possuem recursos ociosos por certa parte do tempo (MARCOS et al., 2018a), seria benéfico que ISPs conectados a estas infraestruturas utilizassem desses recursos para melhorar sua engenharia de tráfego, elevando a qualidade dos serviços prestados aos consumidores.

Neste trabalho, propomos uma plataforma para oferta e consulta de intenções de troca de tráfego com base em um IXP, que permita ISPs fechar acordos de interconexão após a identificação de ofertas que melhor se adéquem a seus critérios.

Primeiramente, apresentamos os requisitos e as premissas da plataforma (Seção 4.1). Após, discutimos as decisões de projeto mais importantes (Seção 4.3), seguida pela descrição dos componentes da arquitetura e os objetos que eles manipulam (Seção 4.4). Encerramos a seção descrevendo o fluxo operacional, passo a passo, mostrando o funcionamento da plataforma proposta (Seção 4.5).

4.1 Requisitos

Há dois requisitos principais a satisfazer. Primeiro, a confidencialidade: pesquisas (MARCOS et al., 2018b; CHIESA et al., 2017) com operadores de ISP mostram que garantir a privacidade das políticas de interconexão é um fator relevante para os ASes, pois tais políticas influenciam em questões de mercado e ASes tem interesse em manter estas informações de forma privada. O segundo é a baixa complexidade operacional para os ASes, que neste caso definimos como o custo de equipamentos e pessoal para o provisionamento e operação de determinada solução, visto que ISPs de pequeno porte compõem uma parte significativa no contexto de IXPs (THE..., 2018) e podem não ter recursos operacionais e financeiros suficientes para despender em uma solução que demande maior esforço para seu provisionamento e operação.

4.2 Premissas

Como premissa, assumimos que o administrador do IXP não entrará em conluio com algum ISP usuário da plataforma a fim de tentar ter acesso a dados criptografados por meio de um ataque ativo à plataforma. Também empregamos estratégias de implementação na solução que armazenam meta dados a respeito de acordos e de ASes na base de dados central. Estas informações podem inferir possíveis acordos entre ISPs, entretanto nenhuma informação confidencial dos documentos de ofertas, propostas ou acordos é revelada.

4.3 Escolhas de Projeto

A solução aqui apresentada é definida em termos de uma arquitetura cliente-servidor. Uma base de dados central é utilizada para armazenar as ofertas de interconexão e registros de acordos firmados. O servidor tem a função de realizar consultas em dados criptografados e armazenar as informações de forma confidencial. ISPs interagem com o servidor através de um cliente executado localmente, necessitando de apenas um navegador web para acessar a plataforma.

Optamos pelo uso de uma base de dados central para armazenamento de dados relativos a ofertas e acordos. Para garantir a confidencialidade das informações armazenadas, selecionamos técnicas de consulta em dados criptografados para o armazenamento e realização de consultas. Os dados ficam protegidos tanto do gerente do serviço, neste caso o IXP, quanto de outros ASes e possíveis agentes maliciosos que por ventura tentem descobrir informações confidenciais a respeito das políticas de interconexão dos ASes membros da infraestrutura através de ataques passivos.

Com o intuito de garantir a confidencialidade também no trânsito das informações que passam pela rede, utilizamos o protocolo HTTPS para cifragem da comunicação entre o cliente e servidor da plataforma.

4.4 Componentes

A arquitetura é formada por três componentes básicos:

- Base de dados: Uma base de dados é utilizada para armazenar registros de ofertas,

propostas, acordos de troca de tráfego e informações gerais sobre ASes.

- Servidor: Componente responsável por armazenar e realizar consulta nos dados criptografados. Apenas entes que escolham compartilhar um registro, como uma oferta ou acordo de interconexão, podem ter acesso a estes dados. O servidor também garante que as informações estão disponíveis apenas para as partes envolvidas em um acordo ou oferta.
- Cliente: Para ter acesso aos serviços oferecidos pelo servidor, uma aplicação cliente deve ser utilizada pelo ISP usuário para comunicação com o servidor e execução das operações relativas a consulta e acordos de interconexão. É apresentado ao usuário uma interface para consulta de ofertas, avaliações de acordos previamente realizados, envio de propostas e fechamento de acordos de interconexão.

Os elementos mencionados acima são mais especificamente definidos como:

- Oferta: o trabalho do Dynam-IX (MARCOS et al., 2018a) apresenta um conceito chamado *Intent Abstraction* que tem como objetivo descrever intenções de políticas de interconexão. Aplicamos o mesmo conceito ao definir este componente da proposta. Dentre os campos que compõem a Intent Abstratction, os mais importantes para esta proposta são descritos na Tabela 4.4.
- Proposta: documento que descreve a intenção de fechar um acordo de troca de tráfego relacionado a uma oferta contendo a identificação da oferta e o tempo do contrato.
- Acordo: documento definindo termos legais do serviço prestado.

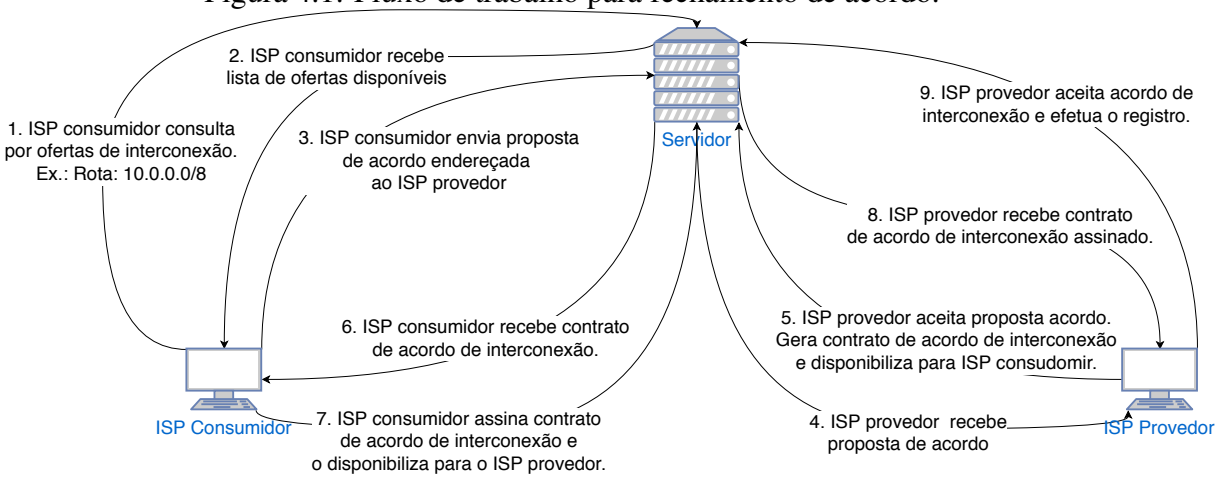
Tabela 4.1: Tabela com atributos da Intent Abstraction para registro de ofertas.

Atributo	**Descrição**
aspath	Define a rota que esta sendo ofertada.
bwidth	Largura de banda disponibilizada pela oferta.
latency	Latência do enlace para a rota especificada.
pkt_loss	Porcentagem de perda de pacote para o destino ofertado.
jitter	Variação da latência do enlace para o destino ofertado.
repair	Tempo de reparo em caso de indisponibilidade da rota ofertada.
guarantee	Porcentagem de garantia de qualidade de serviço.
availability	Porcentagem do tempo de disponibilidade mínimo do serviço.
billing	Forma de cálculo do preço.

Fonte: Dynam-IX (MARCOS et al., 2018a)

4.5 Fluxo Operacional

Figura 4.1: Fluxo de trabalho para fechamento de acordo.



Fonte: Os Autores

Explicamos o fluxo de trabalho através de um passo-a-passo, como exemplificado na Figura 4.1. Para efeito de clareza, não exploraremos todas as situações, apenas o caso típico. Primeiro, os ASes se registram na plataforma e após isto cadastram suas ofertas de interconexão. A busca por uma oferta de interconexão é feita pelo cliente, informando uma rota que se tem interesse em ter acesso. A consulta é enviada então ao servidor, que retorna ofertas que atendem a rota requisitada. Após receber o resultado das ofertas disponíveis, o ISP consumidor pode enviar uma proposta de interconexão para o ISP ofertante. Ao receber uma oferta de interconexão, o ISP que irá prover o serviço pode escolher aceitar a proposta ou rejeitá-la.

Supondo que aceite a proposta, este ISP gera um contrato, assina o documento digitalmente e disponibiliza para o ISP que irá atuar como consumidor o documento contendo os termos do acordo. Neste ponto, o ISP consumidor pode rejeitar o acordo proposto ou aceitá-lo. Assumindo que aceite, o ISP cliente deve assiná-lo digitalmente e então disponibilizá-lo para o ISP provedor. Este, por sua vez, recebendo a confirmação do ISP consumidor, pode rejeitar o acordo assinado, devido a uma assinatura inválida por exemplo, ou registrá-lo. Apondo que seja registrado, o acordo entra em efeito e os ASes podem passar para fase de implementar tecnicamente o acordo firmado.

Ao final do acordo, ambas as partes do contrato podem registrar uma nota, em uma escala de 0 a 5, onde 0 definiria uma péssima experiência com a parceria firmada e 5 uma ótima experiência. As notas referentes a parcerias anteriores ficam disponíveis

para consulta por outros ASes e podem ser utilizadas como mecanismo de construção de confiança, auxiliando na tomada de decisão no momento de fechar um acordo de interconexão.

5 AVALIAÇÃO

Com o objetivo de avaliar a proposta descrita neste trabalho, realizamos uma série de experimentos a partir da implementação de um protótipo. Estes experimentos visam responder três perguntas sobre o design proposto: (i) é possível estabelecer acordos de interconexão intermediados pelo IXP de forma confidencial? (ii) quais os requisitos de armazenamento e de rede da solução proposta? e (iii) é possível escalar a solução para o tamanho atual dos IXPs?

Neste capítulo comentaremos sobre a metodologia utilizada no protótipo, o ambiente de experimentos utilizado e as métricas coletadas. Ao final da avaliação, faremos uma discussão a partir das respostas apresentadas.

5.1 Metodologia

A metodologia utilizada para avaliar a proposta parte da implementação de um protótipo da solução. Montamos um ambiente de experimentos na nuvem com o objetivo de avaliar se os objetivos foram atingidos e quais os requisitos necessários para o uso do protótipo. Para esta avaliação coletamos métricas de tempo de consulta por ofertas de interconexão, tempo para fechamento de acordos e quantidade de recursos de rede e armazenamento utilizados.

5.1.1 Implementação

Construímos o protótipo utilizando técnicas de consulta por multi-palavras-chave em dados criptografados. Buscamos implementações desta técnica e que estivessem publicamente disponíveis. A única opção disponível foi o Mylar (POPA et al., 2014), que adotamos como principal componente do protótipo.

Mylar foi implementado utilizando como base o Meteor (METEOR, 2018), plataforma para desenvolvimento de aplicações web em JavaScript. Dessa maneira, foi conveniente estruturar a solução aqui proposta usando toda a plataforma. Existe uma discussão (RESPONSE..., 2018; GRUBBS et al., 2016; MYLAR..., 2018) em relação às garantias de segurança do Mylar, que podem ser consultadas na página dos autores de Mylar (POPA et al., 2014), e em Breaking Web Applications Built On Top of Encrypted Data

(GRUBBS et al., 2016). Não há um consenso dentro da comunidade sobre quem está certo referente a esses pontos. De qualquer maneira, essas possíveis falhas de projeto não são relevantes para impedir o uso do recurso neste trabalho. Para um ataque, o servidor precisaria ser comprometido, e um esquema de ataque elaborado precisaria ser posto em prática, algo que assumimos não corresponder ao perfil de membros de IXPs.

Por fim, o Meteor está baseado no MongoDB. Trata-se de um banco de dados NoSQL, normalmente utilizado para o desenvolvimento de aplicações que não precisam de uma estrutura rígida de um banco de dados relacional. Este banco de dados foi utilizado para o armazenamento dos registros criptografados.

5.1.1.1 Servidor

A aplicação que executa no servidor é responsável por controlar o acesso aos dados armazenados na base de dados, além de executar funções relativas ao fluxo de trabalho do fechamento de acordos. O servidor recebe e processa consultas por ofertas de interconexão nele registradas.

No servidor fica também a base de dados dos registros (MongoDB). Ao longo deste capítulo, mencionaremos elementos desta tecnologia, conforme a Tabela 5.1.

Tabela 5.1: Descrição de elementos do MongoDB.

Elemento	**Descrição**
Documento	Registro BSON, composto por campos e valores para armazenamento de dados.
Coleção	Um agrupamento de documentos. Análogo a tabelas em bancos de dados relacionais.
Base de dados	Armazena um conjunto de coleções de documentos.

Fonte: Documentação MongoDB (MONGODB..., 2018)

Desenvolvemos o servidor da solução em JavaScript, linguagem necessária para desenvolver aplicações utilizando Meteor. O componente Mylar é responsável por realizar consultas de multi-palavras-chave em dados criptografados. É através deste componente que é possível fazer consulta nas ofertas registradas em formato criptografado.

No desenvolvimento do protótipo do servidor definimos coleções para armazenamento dos registros de ofertas, propostas, acordos e avaliações. Ao definir estas coleções, campos que devessem ser protegidos por criptografia precisaram ser marcados com um modificador especial. A lógica do servidor é composta por funções que definem quais coleções serão expostas para o cliente, funções que alteram estados de propostas e acordos de interconexão no fluxo de trabalho e consultas em dados criptografados.

5.1.1.2 Cliente

O cliente da solução é executado utilizando-se um navegador web. Ao acessar o servidor web que hospeda a plataforma, uma série de arquivos JavaScript são carregados no navegador do cliente. Estes arquivos possuem funções que definem a lógica de funcionamento do cliente.

O cliente possui funções para registrar, compartilhar e consultar ofertas de interconexão, além de funções para enviar propostas e fechar acordos de interconexão. Como principal função, o cliente é responsável por criptografar e descriptografar registros utilizando chaves privadas ou compartilhadas do usuário. Através do cliente, o AS informa quais outros usuários da plataforma poderão consultar suas ofertas de interconexão.

5.1.2 Desafios da implementação

Enfrentamos desafios de implementação na utilização do Mylar. Funções descritas no artigo não seguiam a mesma semântica na implementação do protótipo do Mylar, além dos parâmetros das funções definidas no artigo em muitos dos casos não condizer com os implementados no protótipo. Isto demandou esforços para entender como utilizar as funções que foram definidas no artigo do Mylar no protótipo disponibilizado.

Tentamos também utilizar WebSockets para obter um melhor desempenho da comunicação entre o cliente e servidor. Porém, ao habilitar tal tecnologia, funções do Mylar passaram a lançar exceções, e tais erros impossibilitavam a comunicação do cliente com o servidor. A própria solução verifica se é possível realizar a comunicação utilizando WebSockets; caso isso não seja possível, mecanismos alternativos como AJAX ou Long Pooling são utilizados. Visto que não era objetivo deste trabalho alterar componentes internos do Mylar, preferimos utilizar a plataforma com o mecanismo alternativo de comunicação a WebSockets.

Para simulação dos ASes nos experimentos, adotamos o Selenium (SELENIUM, 2018). Tivemos algumas dificuldades para programar os scripts do Selenium que interagiam com os elementos JavaScript, visto que em muitos casos erros de elementos obsoletos eram retornados. Cada interação com elementos que disparavam troca de dados com o servidor geravam atualizações dos elementos JavaScript da página, porém não da página em si. Como a página não atualizava por completo o script tentava utilizar elementos capturados anteriormente, que neste momento eram obsoletos, disparando então

uma exceção no script. Contornamos este problema adicionado pausas forçadas entre as interações do script Selenium na página do cliente.

5.1.3 Ambiente de experimentos

Buscando avaliar a solução proposta, utilizamos instâncias EC2 (AMAZON..., 2018b) no ambiente de nuvem da AWS (AMAZON..., 2018c), simulando ASes interagindo com a plataforma. Para automação da tarefa, usamos Selenium (SELENIUM, 2018). Trata-se de uma plataforma para realização de testes automatizados em aplicações web. Scripts Selenium foram criados para realizar trinta consultas e acordos de interconexão contra um AS.

O servidor da solução foi provisionado em uma instância EC2 de tamanho c4.4xlarge, assim como o AS que atuou como ISP provedor oferecendo ofertas de interconexão. Os demais ASes simulando ISPs consumidores utilizaram instâncias EC2 t2.micro.

5.1.4 Métricas

Um conjunto de métricas foi utilizado a fim de avaliar a solução e responder os questionamentos elencados no início deste capítulo. Os seguintes dados relativos a estas métricas coletados são:

- Tempo para consulta de ofertas de interconexão.
- Tempo para fechamento de um acordo de interconexão.
- Espaço em disco consumido pelos registros na base de dados.
- Banda de rede consumida.

Estas informações indicam como a solução escala a medida que o número de ASes interagindo é incrementado e quais os recursos mínimos necessários para que a solução opere.

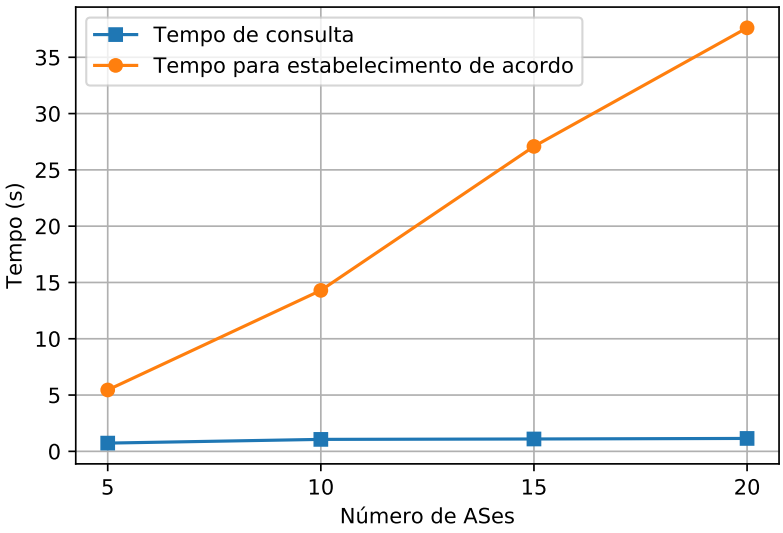
5.2 Experimentos

Realizamos os experimentos utilizando 5, 10, 15 e 20 ASes tentando fechar acordos de interconexão contra 1 AS. Escolhemos estes conjuntos para serem avaliados pois

tivemos problemas ao executar os experimentos com mais de 20 ASes, conforme será comentado em detalhes na Seção 5.3. O objetivo dos experimentos com um conjunto reduzido de ASes é observar como o protótipo se comporta a medida que o número de ASes interagindo com o servidor aumenta, avaliando desta maneira o desempenho do protótipo e possíveis gargalos.

Os gráficos 5.1, 5.2 e 5.3 apresentam a evolução do tempo de consulta de ofertas e fechamento de acordos de interconexão.

Figura 5.1: Tempo de resposta para consultas e fechamento de acordos.



Fonte: Os Autores

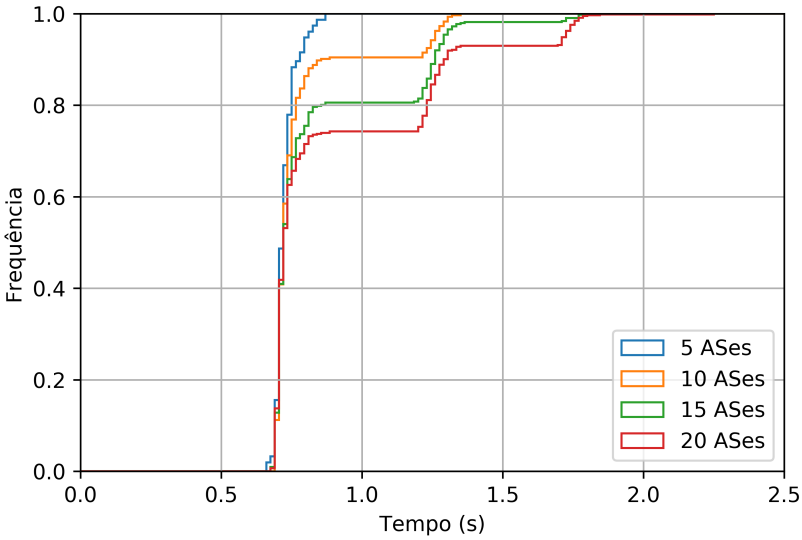
Na Figura 5.1, podemos perceber que o tempo para consulta de ofertas de interconexão se manteve praticamente constante, enquanto que o tempo para fechamento de acordos cresceu de forma linear.

Analisando o gráfico da Figura 5.2, concluímos que para 80% das métricas coletadas, o tempo de resposta foi inferior a 1,5 segundo para consultas, com o restante não ultrapassando 2,5 segundos.

As informações das Figuras 5.1 e 5.2 demonstram que não há sobrecarga para realização de consultas de ofertas de interconexão para os conjuntos avaliados. Entretanto, podemos perceber que o tempo para estabelecimento de acordos de interconexão cresce linearmente, indicando um problema de desempenho ao passo que o número de ASes interagindo com o protótipo aumenta.

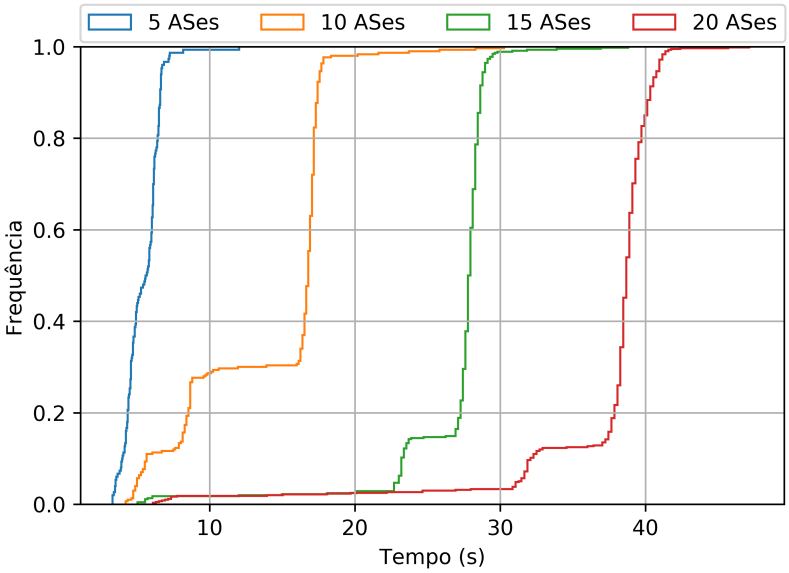
Observando o gráfico da Figura 5.3, percebemos que o tempo para o estabelecimento de um acordo de interconexão aumenta consideravelmente, ao passo que o número de ASes tentando fechar acordos é elevado. Isto demonstra que a solução não escala tão

Figura 5.2: CDF - Tempo de resposta para consultas.



Fonte: Os Autores

Figura 5.3: CDF - Tempo de resposta para fechamento de acordos.



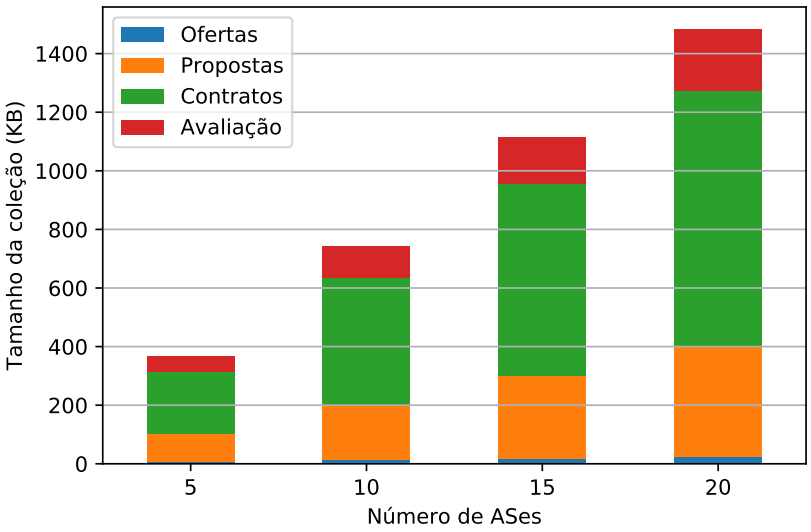
Fonte: Os Autores

bem neste critério. Na Seção 5.3, discutiremos as possíveis razões para isto.

O gráfico da Figura 5.4 apresenta a quantidade de espaço necessário ao armazenamento dos registros relativos a ofertas e acordos de interconexão. Percebe-se um crescimento quase linear no espaço de armazenamento utilizado ao passo que o número de ASes tentando fechar acordos de interconexão aumenta.

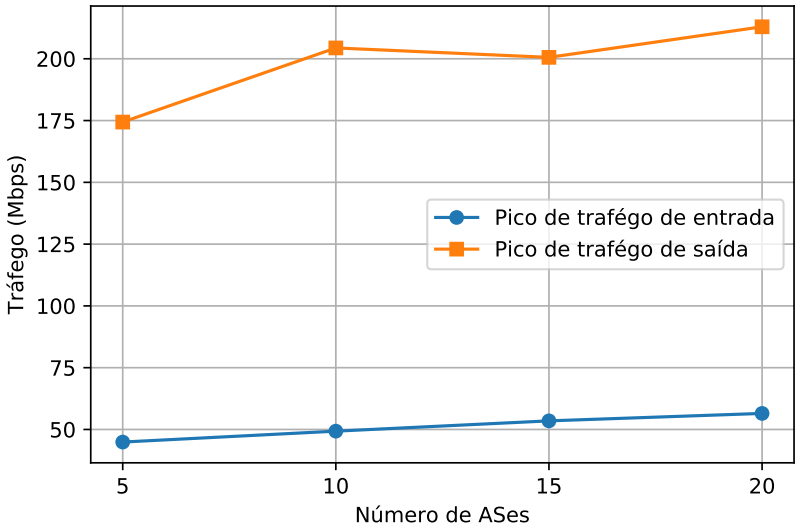
Os gráficos das Figuras 5.5 e 5.6 apresentam ruído na informação apresentada. Isto ocorreu pois utilizamos o plano básico do CloudWatch (AMAZON. . . , 2018a) que fornece métricas com precisão de 5 minutos. Levando isto em consideração, o gráfico

Figura 5.4: Espaço de armazenamento utilizado pelos registros.



Fonte: Os Autores

Figura 5.5: Tráfego de rede no servidor.

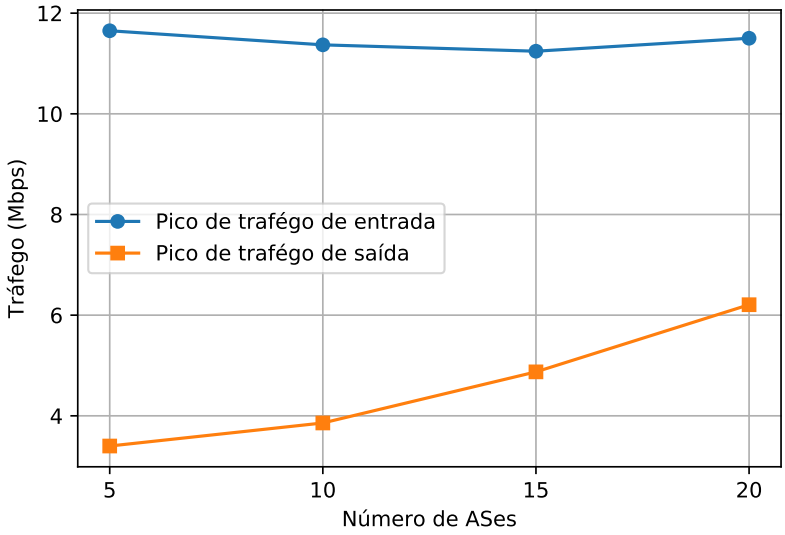


Fonte: Os Autores

apresentado fornece apenas uma estimativa para o tráfego de rede gerado. Uma forma de melhor avaliar este especto seria executar os experimentos um maior número de vezes e calcular um intervalo de confiança para o tráfego gerado.

De qualquer forma observamos pelos gráficos das Figuras 5.5 e 5.6 que o tráfego de rede se concentra no servidor. Isto faz sentido, visto que a solução é centralizada e os ASes devem usar o servidor para trocar informações.

Figura 5.6: Tráfego de rede no AS provedor.



Fonte: Os Autores

5.3 Discussão

Esta seção apresenta uma discussão sobre os resultados dos experimentos e a resposta para as perguntas feitas no início do capítulo.

É possível estabelecer acordos de interconexão intermediados pelo IXP de forma confidencial? Observando os resultados apresentados na Seção 5.2, concluímos que a solução é viável para ser utilizada pelo IXP a fim de intermediar acordos de interconexão de forma confidencial. Pelo gráfico da Figura 5.1, é possível perceber que o tempo para consultas por ofertas de interconexão se manteve constante para os conjuntos avaliados, enquanto que o tempo para o fechamento de acordos cresce quase que de forma linear. Apesar do desempenho não ser satisfatório no tempo para fechamento de acordos ao passo que o número de ASes aumenta, a solução se mostrou funcional para a tarefa de intermediar os acordos de interconexão.

Quais os requisitos de armazenamento e de rede da solução proposta? A solução foi avaliada com conjuntos de 5 a 20 ASes fechando 30 acordos de interconexão. Utilizamos como base para os experimentos o artigo do Dynam-IX. (MARCOS et al., 2018a). Dessa forma escolhemos simular cada AS fechando 30 acordos de interconexão, porém utilizamos uma escala menor no número de ASes interagindo com o protótipo devido a problemas de desempenho encontrados no momento da realização dos experimentos. Devido à arquitetura centralizada da solução proposta, foram medidos o pico de tráfego de entrada e saída no servidor e no AS provedor de ofertas de interconexão. Os

resultados apresentados na Seção 5.2 mostram que para 5 ASes foi gerado no máximo 174,38Mbps de tráfego de entrada no servidor, enquanto que para 20 ASes este valor é de 212,94Mbps. O AS atuando como provedor de ofertas de interconexão registrou pico de tráfego de entrada de 11.65Mbps enquanto que o pico de tráfego de saída foi de 6.2Mbps.

Ainda com o mesmo conjunto avaliado, foram gerados de 150 a 600 contratos de interconexão e de 300 a 1200 registros de notas avaliando acordos de interconexão (cada parte no acordo fornece uma nota avaliando o contrato firmado). Para o menor conjunto avaliado, foram consumidos 367,72KB para armazenar os registros de ofertas, notas, propostas e acordos de interconexão e 1,48MB para o maior conjunto avaliado.

É possível escalar a solução para o tamanho atual dos IXPs? Os experimentos foram realizados com um conjunto de ASes reduzido a fim de identificar a tendencia de crescimento dos tempos de consulta e fechamento de acordos.

Analisando o resultado da avaliação, percebemos que o tempo para estabelecimento de acordos de interconexão cresceu de forma linear. Para 20 ASes o tempo médio para fechamento de acordos chega próximo de 40s. Dessa maneira, a tendencia é que ao passo que o número de ASes tentando fechar acordos de interconexão aumente, e este valor cresça proporcionalmente. O alto tempo para estabelecimento dos acordos de interconexão está relacionado a dois fatores: (i) uso do Selenium para automação da simulação dos ASes e (ii) cliente da solução implementado em uma página web com componentes controlados por JavaScript.

O cliente da solução é executado em uma página web que tem seus elementos gerados e atualizados de forma dinâmica. O controle dessas alterações é feito pela plataforma de desenvolvimento utilizada (Meteor). Determinadas ações geram a atualização de objetos na página, embora não atualize a página por completo. Um exemplo disso seria quando o ISP que esta provendo o serviço de interconexão gera um novo contrato, implicando a criação de uma nova linha na tabela para exibir os contratos na tela do cliente, atualizando alguns componentes da página dinamicamente.

A plataforma de automação Selenium captura elementos na página e executa ações programadas. Caso um elemento capturado tenha sido atualizado, uma exceção é lançada informando que o elemento é obsoleto, sendo descartado logo após. Com o intuito de evitar exceções desse tipo, foram adicionadas pausas a cada interação com um elemento, a fim de aguardar a atualização dos elementos da página e não capturar elementos obsoletos.

Visto que a implementação do cliente foi feita em uma página web, ao passo que o número de elementos na página aumenta, como propostas e acordos de interconexão,

percebemos maior lentidão para o processamento e carregamento dos elementos. Este fator implica nos problemas de desempenho relativos a grande quantidade de elementos sendo exibidos na página web do cliente.

Utilizamos o protocolo HTTPS para garantir a cifragem das informações em trânsito. Este protocolo é também obrigatório para o uso da Web Cryptography API (WEB..., 2018), mecanismo disponibilizado nos navegadores web modernos para executar funções criptográficas. As funções da Web Cryptography API foram uteis no nosso caso para assinar e verificar assinaturas de registros de ofertas e acordos de interconexão.

Meteor utiliza como principal componente para comunicação entre cliente e servidor *WebSockets*. Caso este recurso não esteja disponível no servidor web técnicas alternativas como *XHR* (AJAX..., 2018) ou *Pooling* (ARTICLE..., 2016) são utilizadas. Estes mecanismos alternativos possuem desempenho inferior em relação a WebSockets (LUBBERS, 2018; ARTICLE..., 2016; APPELQVIST; ÖRNMYR, 2017).

Para o uso do protocolo HTTPS, um servidor web foi provisionado no mesmo ambiente que o Meteor. Este servidor é responsável por prover a terminação HTTPS entre o cliente e servidor da solução e encaminhar o tráfego internamente para o Meteor, atuando dessa maneira como um intermediador.

O protótipo do Mylar foi implementado adicionando e modificando pacotes da plataforma de desenvolvimento de aplicações web em JavaScript Meteor. Ao habilitar WebSockets no servidor web, importantes funções do Mylar pararam de funcionar devido provavelmente as modificações realizadas em pacotes relacionados a comunicação entre o cliente e servidor e que não foram testadas para trabalhar com WebSockets intermediado por um servidor web HTTPS, impossibilitando o uso deste recurso. O uso de um mecanismo alternativo a WebSockets pode ter contribuído para a performance reduzida da solução ao passo que maior carga foi adicionada nos experimentos.

Devido aos problemas de sobrecarga e escalabilidade, podemos afirmar que protótipo não atingiu ao critério de escalar ao tamanho dos IXPs. Uma possível solução para este problema seria implementar um servidor que atuasse como uma API REST (REST, 2018), e o cliente como uma aplicação de linha de comando, por exemplo, isto demandaria conhecimento mais profundo do funcionamento do Mylar e modificações tanto no cliente como no servidor.

6 CONCLUSÃO

Com o objetivo de melhorar a dinâmica de acordos de interconexão na Internet, propusemos uma plataforma centralizada em IXP para facilitar a busca e estabelecimento de acordos de interconexão. Apresentamos uma proposta detalhada da solução, assim como a escolha das melhores técnicas para alcançar os objetivos propostos. Além disso, fizemos uma avaliação da proposta através da implementação de um protótipo da solução. A avaliação demonstrou que a solução é viável, porém requer alguns ajustes para se tornar escalável considerando o número de ASes membros dos maiores IXPs.

6.1 Trabalhos futuros

A partir da experiência adquirida com este trabalho, apresentamos nesta seção os trabalhos futuros com o objetivo de trazer melhorias para a proposta.

6.1.1 Alterar modelo de comunicação com o servidor

A partir da experiência deste trabalho e de acordo com a avaliação da solução apresentada percebemos que alterar a arquitetura do servidor para atuar como API REST poderia trazer melhorias de desempenho, visto que o cliente poderia ser refatorado para utilizar componentes que não causem tanto atraso no seu uso. Isto demandaria estudo aprofundado sobre um dos componentes utilizados, Mylar, ou a mudança do mesmo por outro que atenda as mesmas propriedades e tenha melhor desempenho para escalar ao tamanho dos IXPs.

6.1.2 Modificação do cliente

Devido ao uso de toda plataforma de desenvolvimento web Meteor, o qual o Mylar foi construído em cima, o cliente foi implementado em uma página web. Conforme relatado no Capítulo 5 isto trouxe alguns problemas de desempenho para a solução. Sugerimos como trabalho futuro alterar o cliente para funcionar como um aplicativo de linha de comando, dessa forma removendo os atrasos causados por componentes web e facilitando possíveis processos de automação para operação.

REFERÊNCIAS

AJAX - The XMLHttpRequest Object. 2018. Disponível em: <https://www.w3schools.com/js/js_ajax_http.asp>. Acesso em: 10 dez. 2018.

AMAZON CloudWatch. 2018. Disponível em: <https://aws.amazon.com/cloudwatch/>. Acesso em: 09 dez. 2018.

AMAZON EC2. 2018. Disponível em: <https://aws.amazon.com/ec2/>. Acesso em: 09 dez. 2018.

AMAZON Web Services. 2018. Disponível em: <https://aws.amazon.com/>. Acesso em: 09 dez. 2018.

APPELQVIST, R.; ÖRNMYR, O. Performance comparison of XHR polling, Long polling, Server sent events and Websockets. In: . SE-371 79 Karlskrona, Sweden: [s.n.], 2017. Disponível em: <http://www.diva-portal.se/smash/get/diva2:1133465/FULLTEXT01.pdf>.

ARASU, A. et al. Querying Encrypted Data. In: **Proceedings of the 2014 ACM SIGMOD International Conference on Management of Data**. New York, NY, USA: ACM, 2014. (SIGMOD '14), p. 1259–1261. ISBN 978-1-4503-2376-5. Disponível em: <http://doi.acm.org/10.1145/2588555.2588893>.

ARTICLE SockJS: WebSocket emulation done right. 2016. Disponível em: <https://github.com/sockjs/sockjs-client/wiki/%5BArticle%5D-SockJS:-WebSocket-emulation-done-right>. Acesso em: 02 dez. 2018.

AUGUSTIN, B.; KRISHNAMURTHY, B.; WILLINGER, W. IXPs: Mapped? In: **Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement**. New York, NY, USA: ACM, 2009. (IMC '09), p. 336–349. ISBN 978-1-60558-771-4. Disponível em: <http://doi.acm.org/10.1145/1644893.1644934>.

CAIDA: Center for Applied Internet Data Analysis. 2018. Disponível em: <http://www.caida.org/home/>. Acesso em: 09 dez. 2018.

CASTRO, I. et al. Route Bazaar: Automatic Interdomain Contract Negotiation. In: **Proceedings of the 15th USENIX Conference on Hot Topics in Operating Systems**. Berkeley, CA, USA: USENIX Association, 2015. (HOTOS'15), p. 9–9. Disponível em: <http://dl.acm.org/citation.cfm?id=2831090.2831099>.

CHATZIS, N.; SMARAGDAKIS, G.; FELDMANN, A. On the importance of Internet eXchange Points for today's Internet ecosystem. In: . [S.l.: s.n.], 2013.

CHIESA, M. et al. Internet Routing Privacy Survey. In: . [s.n.], 2017. Disponível em: <http://bit.ly/2rjT7Nj>.

DIMITROPOULOS, X. et al. On the 95-percentile billing method. In: **Proceedings of the 10th International Conference on Passive and Active Network Measurement**. Berlin, Heidelberg: Springer-Verlag, 2009. (PAM '09), p. 207–216. ISBN 978-3-642-00974-7. Disponível em: <https://doi.org/10.1007/978-3-642-00975-4_21>.

EURO-IX. European Internet Exchange Association 2012 Report on European IXPs. In: . [s.n.], 2012. Disponível em: <https://www.euro-ix.net/media/filer_public/79/76/7976b7ab-2620-4f62-9f57-5ab0d81be4d7/euro-ix_ixp_report_2012.pdf>. Acesso em: 04 dez. 2018.

GRUBBS, P. et al. Breaking Web Applications Built On Top of Encrypted Data. In: **Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security**. New York, NY, USA: ACM, 2016. (CCS '16), p. 1353–1364. ISBN 978-1-4503-4139-4. Disponível em: <http://doi.acm.org/10.1145/2976749.2978351>.

KAMARA, S.; PAPAMANTHOU, C.; ROEDER, T. Dynamic Searchable Symmetric Encryption. In: **Proceedings of the 2012 ACM Conference on Computer and Communications Security**. New York, NY, USA: ACM, 2012. (CCS '12), p. 965–976. ISBN 978-1-4503-1651-4. Disponível em: <http://doi.acm.org/10.1145/2382196.2382298>.

LUBBERS, F. G. P. **HTML5 WebSocket: A Quantum Leap in Scalability for the Web**. 2018. Disponível em: <https://www.websocket.org/quantum.html>. Acesso em: 02 dez. 2018.

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

MARCOS, P. et al. Dynam-IX: a Dynamic Interconnection eXchange. In: **ACM CoNEXT 2018**. [S.l.: s.n.], 2018.

MARCOS, P. et al. Internet Interconnection Ecosystem Survey. In: . [s.n.], 2018. Disponível em: <https://dynam-ix.github.io/docs/internet_interconnection_ecosystem_survey.pdf>.

METEOR. 2018. Disponível em: <https://www.meteor.com/>. Acesso em: 29 nov. 2018.

MONGODB Documentation. 2018. Disponível em: <https://docs.mongodb.com/manual/core/document/>. Acesso em: 12 out. 2018.

MYLAR: The Guide for the Perplexed. 2018. Disponível em: <https://docs.google.com/document/d/1NJHodio0UHs4fLhbLrbpoQJYriOEuUPNmB1e8cPRXfY/pub>. Acesso em: 09 dez. 2018.

PEERINGDB. 2018. Disponível em: <https://www.peeringdb.com/>. Acesso em: 07 out. 2018.

POPA, R. A. et al. CryptDB: Processing Queries on an Encrypted Database. **Commun. ACM**, ACM, New York, NY, USA, v. 55, n. 9, p. 103–111, sep. 2012. ISSN 0001-0782. Disponível em: <http://doi.acm.org/10.1145/2330667.2330691>.

POPA, R. A. et al. Building Web Applications on Top of Encrypted Data Using Mylar. In: **Proceedings of the 11th USENIX Conference on Networked Systems Design and Implementation**. Berkeley, CA, USA: USENIX Association,

2014. (NSDI'14), p. 157–172. ISBN 978-1-931971-09-6. Disponível em: <http://dl.acm.org/citation.cfm?id=2616448.2616464>.

RESPONSE to "Breaking web applications built on top of encrypted data"(CCS 2016) by P. Grubbs, R. McPherson, M. Naveed, T. Ristenpart and V. Shmatikov. 2018. Disponível em: <https://css.csail.mit.edu/mylar/security.html>. Acesso em: 09 dez. 2018.

REST. 2018. Disponível em: <https://www.w3.org/2001/sw/wiki/REST>. Acesso em: 11 dez. 2018.

RESTREPO, J. C. C.; STANOJEVIC, R. IXP Traffic: A Macroscopic View. In: **Proceedings of the 7th Latin American Networking Conference**. New York, NY, USA: ACM, 2012. (LANC '12), p. 1–8. ISBN 978-1-4503-1750-4. Disponível em: <http://doi.acm.org/10.1145/2382016.2382018>.

SCHLINKER, B. et al. Engineering Egress with Edge Fabric: Steering Oceans of Content to the World. In: **Proceedings of the Conference of the ACM Special Interest Group on Data Communication**. New York, NY, USA: ACM, 2017. (SIGCOMM '17), p. 418–431. ISBN 978-1-4503-4653-5. Disponível em: <http://doi.acm.org/10.1145/3098822.3098853>.

SELENIUM. 2018. Disponível em: <https://www.seleniumhq.org/>. Acesso em: 15 out. 2018.

SONG, D. X.; WAGNER, D.; PERRIG, A. Practical techniques for searches on encrypted data. In: **Proceeding 2000 IEEE Symposium on Security and Privacy. S P 2000**. [S.l.: s.n.], 2000. p. 44–55. ISSN 1081-6011.

THE CAIDA UCSD PeeringDB Dataset, March-2016. 2018. Disponível em: <http://www.caida.org/data/peeringdb.xml>. Acesso em: 09 dez. 2018.

VALANCIUS, V. et al. MINT: A Market for INternet Transit. In: **Proceedings of the 2008 ACM CoNEXT Conference**. New York, NY, USA: ACM, 2008. (CoNEXT '08), p. 70:1–70:6. ISBN 978-1-60558-210-8. Disponível em: <http://doi.acm.org/10.1145/1544012.1544082>.

WEB Cryptography API. 2018. Disponível em: <https://www.w3.org/TR/WebCryptoAPI/>. Acesso em: 17 out. 2018.

WOLF, T. et al. ChoiceNet: Toward an Economy Plane for the Internet. **SIGCOMM Comput. Commun. Rev.**, ACM, New York, NY, USA, v. 44, n. 3, p. 58–65, jul. 2014. ISSN 0146-4833. Disponível em: <http://doi.acm.org/10.1145/2656877.2656886>.

WOODCOCK, B.; FRIGINO, M. Survey of Internet carrier interconnection agreements. In: **Packet Clearing House**. [S.l.: s.n.], 2016.

YAP, K. et al. Taking the Edge off with Espresso: Scale, Reliability and Programmability for Global Internet Peering. In: . [s.n.], 2017. Disponível em: <http://dl.acm.org/ft_gateway.cfm?id=3098854&ftid=1898911&dwn=1&CFID=776908660&CFTOKEN=29525737>.