RouteWatcher: Monitorando e Verificando Rotas na Internet

Lucas Barsand* **Giovanni Tagliaferri** **Ítalo Cunha**

Universidade Federal de Minas Gerais

{lucas.barsand, giovannitgl, cunha}@dcc.ufmg.br

Abstract. *BGP, the Internet's interdomain routing protocol, lacks native mechanisms to prevent errors like route leaks and attacks like prefix hijacks. This limitation can compromise robustness against link failures, degrade performance of distributed systems, and lead to unreachability. To aid researchers and network operators overcome these challenges, we present RouteWatcher: a tool that monitors and validates Internet routes according to inferences based on a routing model. RouteWatcher integrates multiple data sources into a Web interface that allows researchers and operators to identify and analyze routing anomalies.*

Resumo. *O BGP, protocolo de roteamento interdomínio na Internet, não possui funcionalidades nativas de prevenção de erros como vazamento de rotas ou ataques como sequestro de prefixos. Esta limitação pode comprometer a robustez da Internet contra falhas de enlace, deteriorar o desempenho de sistemas distribuídos, e levar a perda de conectividade. Para auxiliar pesquisadores e operadores de rede a superarem estes desafios, apresentamos o RouteWatcher: uma ferramenta que monitora e valida rotas na Internet de acordo com inferências baseadas em um modelo de roteamento. O RouteWatcher integra múltiplas fontes de dados em uma interface Web que permite pesquisadores e operadores identificarem e analisarem anomalias de roteamento.*

1. Introdução

A Internet é composta por diversas redes independentes, chamadas de sistemas autônomos (ASes). ASes estabelecem parcerias de troca de tráfego, conduzindo tráfego entre outros ASes que não estão diretamente conectados. Duas classes comuns de parcerias de troca de tráfego são *cliente-provedor*, onde o cliente paga ao provedor por conectividade ao resto da Internet, e *peer-to-peer*, onde duas redes trocam tráfego sem custo.

O protocolo para distribuição de rotas entre ASes na Internet é o BGP (*Border Gateway Protocol*). O BGP suporta políticas de roteamento que implementam objetivos de negócio decorrentes de acordos (frequentemente sigilosos) de parcerias de troca de tráfego. Por exemplo, políticas de roteamento no BGP ignoram desempenho e priorizam a rota com parceria de troca de tráfego mais atrativa (i.e., com o menor custo). Para cada prefixo IP na Internet, o protocolo BGP escolhe e distribui apenas uma (a "melhor") rota. Este comportamento reduz a quantidade de rotas distribuídas e provê escalabilidade ao protocolo, mas oculta informações sobre quais rotas estão disponíveis. O sigilo sobre

*Parte deste trabalho foi desenvolvido como pesquisador convidado na Columbia University.

parcerias de troca de tráfego combinado à falta de visibilidade sobre rotas disponíveis na Internet dificultam a identificação de falhas e anomalias de roteamento.

Além disso, o BGP não possui mecanismos nativos para prevenir erros de configuração ou impedir a realização de ataques. Essas limitações permitem a ocorrência de acidentes como vazamento de rotas [Siddiqui et al. 2014], que podem causar indisponibilidade de serviços para milhões de usuários [Strickx 2019], e ataques como sequestro de prefixos [Lad et al. 2006, Zheng et al. 2007], que podem expor dados sensíveis a terceiros [Goodin 2017, Memoria 2019]. Estes problemas podem comprometer o funcionamento da Internet e, consequentemente, a segurança e confiabilidade de sistemas distribuídos que operam sobre sua infraestrutura, criando uma demanda por monitoramento de rotas para permitir a identificação de falhas e anomalias de roteamento.

Trabalhos anteriores propuseram métodos para identificação de problemas específicos no roteamento interdomínio, como vazamento de rotas [Siddiqui et al. 2014] e sequestro de prefixos [Lad et al. 2006, Zheng et al. 2007, Zhang et al. 2010]. Infelizmente estas soluções requerem informações sobre os prefixos monitorados (e.g., controle do AS que anuncia o prefixo ou conhecimento sobre quais rotas são válidas), e não podem ser aplicados na Internet em geral. A comunidade de pesquisa propôs mecanismos para autenticação de anúncios do protocolo BGP, como o RPKI e o BGPSec, mas estas soluções requerem modificações nos roteadores e possuem adoção lenta. Existem serviços comerciais de identificação e remediação de problemas como ataques de negação de serviço, como o Google Cloud Armor[1], mas em geral, suas aplicações são desenvolvidas especificamente para um determinado problema, e por motivações comerciais, não são oferecidos detalhes de suas metodologias.

Serviços de código aberto, tal como o BGPlay[2] por exemplo, oferecem ferramentas de visualização da topologia no nível de AS, baseados na informação de rotas observadas obtidas de projetos como RIPE RIS [RIPE NCC 2019], Route Views [Route Views 2019] e Isolario [IIT-CNR 2019], que oferecem dados de rotas observadas, mas oferecem funcionalidades analíticas, sem explorar métodos robustos de verificação. Desconhecemos soluções que unificam a comparação de rotas observadas com expectativas de melhores rotas possíveis para classificar eventuais anomalias para proporcionar um ambiente centralizado que viabilize o monitoramento e identificação de problemas de segurança no plano de controle da Internet.

Para auxiliar operadores de rede a identificar anomalias de roteamento na Internet, apresentamos o RouteWatcher: um sistema que compara rotas observadas por monitores BGP dos projetos RIPE RIS e RouteViews, e rotas inferidas a partir de bases de dados sobre parcerias de troca de tráfego entre ASes [Luckie et al. 2013, Giotsas et al. 2014]. O RouteWatcher infere rotas usando o modelo de roteamento sem vale (*valley-free*) proposto por [Gao 2001], e classifica cada rota observada de acordo com sua conformidade ou não-conformidade ao modelo. O RouteWatcher possui um módulo de visualização Web que permite aos seus usuários inspecionarem observações, inferências e classificações. Particularmente, RouteWatcher auxilia seus usuários na identificação de problemas de propagação de rotas, vazamento de rotas, e sequestros de prefixo.

[1] `https://cloud.google.com/armor`
[2] `https://bgplay.massimocandela.com/`

Neste trabalho descrevemos a arquitetura desta ferramenta, e demonstramos sua aplicação ao realizar uma análise da conformidade de rotas para prefixos IP operados pelos maiores bancos do mundo com o modelo de roteamento sem vale.

2. Fundamentos

Nesta seção descrevemos os trabalhos relacionados que fundamentam os mecanismos e o desenvolvimento do RouteWatcher. Em particular, descrevemos o modelo de roteamento utilizado para inferências de rotas, a base de dados utilizada para parametrização do modelo e os pontos de medição utilizados pela ferramenta.

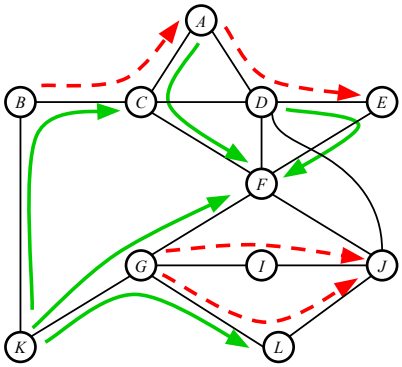
Coletores BGP e monitoramento de rotas. Projetos como RouteViews e RIPE RIS operam roteadores BGP (chamados *coletores*) que estabelecem sessões BGP com outros roteadores BGP (chamados *monitores*) de redes voluntárias. O coletor recebe informações sobre rotas observadas por monitores e disponibilizam os dados publicamente. Monitores de rotas podem exportar rotas para todos os prefixos da Internet (monitores completos) ou apenas para prefixos recebidos de clientes (monitores parciais). Como esta configuração impacta significativamente o conjunto de rotas observadas a partir de um monitor, neste trabalho classificamos monitores como completos se eles exportam rotas para mais de 775 mil prefixos IPv4 distintos e como parciais caso contrário.[3] Em 24 de junho de 2019, o RouteViews opera 25 coletores conectados a 583 monitores, e o RIPE RIS opera 24 coletores conectados a 967 monitores. Estes projetos disponibilizam grandes quantidades de dados sobre rotas na Internet e são amplamente usados por pesquisadores e operadores de rede para análise do roteamento entre ASes.

Modelo de roteamento na Internet. A Internet pode ser abstraída como um grafo direcionado $G = (V, E)$, onde V é o conjunto de ASes e E é o conjunto de interconexões entre ASes. Cada aresta $e \in E$ é anotada com relacionamento de troca de tráfego entre os ASes. Mais precisamente, uma aresta e interconectando os ASes i e j é uma tripla $\langle i, j, p \rangle$, em que $p \in \{p2p, c2p, p2c\}$ denota o relacionamento entre i e j. Dentre os tipos de relacionamentos entre ASes, destacamos os de (i) parceria ($p2p$), determinados por acordos de benefício mútuo onde a troca de tráfego ocorre de forma bilateral e sem custo entre dois ASes; e (ii) comerciais, onde um cliente paga pela conectividade oferecida por seus provedores, denotados cliente-provedor ($c2p$) ou provedor-cliente ($p2c$) dependendo da direção da aresta. Neste modelo, uma *rota* é uma sequência de ASes (vértices) utilizada por um AS para encaminhar tráfego para um prefixo IP de destino.

Um modelo clássico para roteamento interdomínio na Internet é o de políticas de roteamento sem vale (*valley-free*) proposto por Gao [Gao 2001], que baseia-se nos três tipos de relacionamento acima para determinar regras de preferência e propagação de rotas alinhadas com objetivos de negócio (considerando que um cliente paga a um provedor pelo trânsito de dados):

1. Rotas recebidas de clientes são preferidas a rotas recebidas de parceiros, que por sua vez são preferidas a rotas recebidas de provedores.
2. Rotas recebidas de clientes podem ser exportadas para todos os vizinhos, e rotas recebidas de parceiros ou provedores são exportadas apenas para clientes.

[3] A tabela de roteamentos atual da Internet tem aproximadamente 800 mil prefixos IPv4.



Exemplo de caminho	Relacionamento entre saltos	Conformidade com política GR
$K \rightarrow G \rightarrow F$	c2p, c2p	✓
$K \rightarrow B \rightarrow C$	c2p, p2p	✓
$K \rightarrow G \rightarrow L$	c2p, p2c	✓
$B \rightarrow C \rightarrow A$	p2p, c2p	✗
$G \rightarrow I \rightarrow J$	p2p, p2p	✗
$D \rightarrow E \rightarrow F$	p2p, p2c	✓
$G \rightarrow L \rightarrow J$	p2c, c2p	✗
$A \rightarrow D \rightarrow E$	p2c, p2p	✗
$A \rightarrow C \rightarrow F$	p2c, p2c	✓

Figura 1. Exemplo de verificação do modelo do roteamento sem vale aplicado a caminhos de dois saltos.

A figura 1 ilustra a aplicação deste modelo para validação de rotas BGP interconectando dois ASes por um AS intermediário (i.e., caminhos com 3 ASes). À esquerda mostramos um grafo representando ASes e interconexões; denotamos interconexões de parceria com linhas na horizontal e interconexões comerciais com linhas diagonais e verticais onde o provedor está acima do cliente. Dentre os nove possíveis caminhos de dois saltos mostrados na figura (listados à direita), setas em verde (continuas) exemplificam trechos que respeitam o modelo de roteamento sem vale, enquanto as setas em vermelho (tracejadas) não estão em conformidade. Um caminho válido de A para J, por exemplo, é $A \longrightarrow C \longrightarrow F \longrightarrow J$, já que todos os trechos dois-a-dois (i.e., $A \longrightarrow C \longrightarrow F$ e $C \longrightarrow F \longrightarrow J$) deste caminho respeitam a política GR. Por outro lado, a rota $A \longrightarrow D \longrightarrow E \longrightarrow F \longrightarrow J$ desrespeita a política GR, uma vez que o trecho $A \longrightarrow D \longrightarrow E$ é inválido já que D não exporta rotas de parceiros (como E) para provedores (como A).

Classificação do relacionamento entre ASes na Internet. Em [Luckie et al. 2013], dados de coletores BGP são processados para inferir relacionamentos entre ASes. Validação usando múltiplas fontes de dados de verificação (*ground truth*) indica que as inferências atingem precisão de 96.5% para relacionamentos comerciais ($p2c$ e $c2p$) e 82.8% para parcerias ($p2p$). O algoritmo de inferência foi extendido posteriormente por [Giotsas et al. 2014] e [Jin et al. 2019], e bases de dados contento as inferências são disponibilizados periodicamente pela CAIDA.

3. Arquitetura

A verificação de roteamento interdomínio implementada pelo RouteWatcher baseia-se em duas funcionalidades principais como fonte de dados: coleta e inferência de rotas. A primeira é encapsulada no módulo DumpParser, que opera a interação com fontes diversas para obter e organizar dados de *rotas observadas*, enquanto a segunda é implementada pelo módulo RouteModel, que processa dados de inferência de relacionamentos entre ASes para gerar *rotas inferidas*.

O módulo WebView compara os resultados de DumpParser e RouteModel para gerar informação refinada sobre roteamento interdomínio por meio de uma página web. Esta seção descreve a arquitetura destes módulos, bem como sua integração para realizar a verificação de rotas.

3.1. DumpParser

O módulo DumpParser implementa a coleta de rotas para um conjunto $\mathcal{P}$ de prefixos especificados pelo usuário observadas pelo conjunto $\mathcal{M}$ composto por todos os 1550 monitores conectados aos projetos RouteViews e RIPE RIS. Ambos projetos disponibilizam dois tipos de registros de dados (*dumps*), que contém (i) tabelas de roteamento, que listam todas as rotas atualmente conhecidas por cada monitor, e (ii) atualizações de rotas, listando mudanças recentes de rota recebidas por monitores.

Para permitir análises em instantes arbitrários t, o DumpParser recupera o registro de tabela de roteamento do instante t_T mais recente anterior a t. O DumpParser recupera também todos os registros de atualizações de rota entre t_T e t para aplicar quaisquer atualizações de rotas para os prefixos em $\mathcal{P}$ deste o último registro de tabela de roteamento. Assim, é possível utilizar o DumpParser para obter fotografias instantâneas de tabelas de roteamento em qualquer instante de tempo.

Organizamos informações de rotas em um banco de dados, reconstruindo a tabela de roteamento de cada monitor. Mais especificamente, para cada monitor $m \in \mathcal{M}$ armazenamos a rota (sequência de ASes) observada de m para cada prefixo $p \in \mathcal{P}$. Denotamos $\mathcal{R}_{\text{obs}}(m, p, t)$ a rota de m para o prefixo p no instante t. Quando m não possui rota para p no instante t, denotamos $\mathcal{R}_{\text{obs}}(m, p, t) = \emptyset$.

3.2. RouteModel

Para gerar inferências de rotas, o módulo RouteModel utiliza dados de relacionamento entre ASes disponibilizado pela CAIDA [Luckie et al. 2013] para emular o processo de propagação de rotas de acordo com o modelo de roteamento sem vale. Em particular, utilizamos a base dados de relacionamento entre ASes da CAIDA para construir o grafo G de ASes e relacionamentos na Internet.

Dado um AS de origem o, o RouteModel emula a propagação de anúncios e construção de rotas para prefixos IP controlados por o. O algoritmo inicia propagando o anúncio do prefixo para todos os vizinhos de o. Quando um AS a recebe um anúncio de um provedor ou de um parceiro, o algoritmo propaga o anúncio os clientes de a; e quando um AS a recebe um anúncio de um cliente, o algoritmo propaga o anúncio para todos os vizinhos de a (exceto o cliente do qual o anúncio foi recebido). Um dos desafios da inferência de rotas na Internet é que ASes podem receber diversas rotas para um anúncio; a escolha da melhor rota pelo protocolo BGP depende das políticas de roteamento sigilosas ou, na ausência de políticas explicitas, de configurações internas de cada AS. Para contornar este desafio, o RouteModel infere a propagação de *todas* as *rotas ótimas* possíveis para um prefixo, onde uma rota ótima é uma rota em que (i) todos os ASes obedecem as regras 1 e 2 do modelo de roteamento sem vale (seção 2) e que (ii) está entre as rotas mais curtas possíveis para o prefixo de destino.

Ao final da execução do algoritmo para um AS de origem o, é gerada uma lista de rotas inferidas para cada AS $a \in V$. Denotamos $\mathcal{R}_{\text{inf}}(p, m)$ o conjunto de rotas para o prefixo $p \in \mathcal{P}$ que inferimos propagar até o AS m. Para fins de avaliação, em geral estamos interessados nos conjuntos de rotas inferidas para ASes que hospedam um monitor BGP m conectado ao RIPE RIS ou RouteViews.

Cor	Descrição
Preto	Não há rotas observadas e não há rotas inferidas: $\mathcal{R}_{\text{obs}}(p, m, t) = \mathcal{R}_{\text{inf}}(p, m) = \emptyset$. Este cenário acontece quando o monitor m é parcial (só exporta rotas recebidas de clientes) e todas as rotas inferidas para o AS que hospeda m são via parceiros ou provedores.
Vermelho	Não existem rotas observadas e existem rotas inferidas: $\mathcal{R}_{\text{obs}}(p, m, t) = \emptyset$ e $\mathcal{R}_{\text{inf}}(p, m) \neq \emptyset$. Este cenário pode indicar um problema de propagação de rotas na Internet, o que pode comprometer conectividade e a robustez em caso de falhas.
Laranja	A rota observada viola o modelo de roteamento sem vale: $\mathcal{R}_{\text{obs}}(p, m, t) \notin \mathcal{R}_{\text{inf}}(p, m)$ e $\mathcal{R}_{\text{obs}}(p, m, t)$ contém uma aresta $p2p/c2p$ após uma aresta $p2c/p2p$ (i.e., o caminho observado possui um par de saltos ilustrado em linhas pontilhadas em vemelho na figura 1). Este cenário pode indicar algum erro de configuração de roteamento (e.g., vazamento de rotas) ou erros na base de dados da CAIDA (e.g., devido à mudança do tipo de relacionamento entre dois ASes na Internet).
Azul	A rota observada contém um enlace ausente na base da CAIDA: $\mathcal{R}_{\text{obs}}(p, m, t) \notin \mathcal{R}_{\text{inf}}(p, m)$ e existe uma aresta $(i, j) \in \mathcal{R}_{\text{obs}}(p, m, t)$ tal que $(i, j) \notin E$. Este cenário pode indicar atividade maliciosa (e.g., sequestro de rotas), ou erro na base de dados da CAIDA (e.g., devido ao estabelecimento de um novo relacionamento de troca de tráfego).
Amarelo	A rota observada não foi inferida: $\mathcal{R}_{\text{obs}}(p, m, t) \notin \mathcal{R}_{\text{inf}}(p, m)$. Este cenário pode indicar engenharia de tráfego (e.g., escolha proposital de rotas mais longas ou mais caras para fins de melhorar desempenho).
Verde	A rota observada foi inferida: $\mathcal{R}_{\text{obs}}(p, m, t) \in \mathcal{R}_{\text{inf}}(p, m)$.

Tabela 1. Sistema de coloração utilizado pelo WebView para classificar resultados comparativos de dados de prefixos monitorados pelo RouteWatcher. Regras são verificadas na ordem apresentada, da mais específica à menos específica.

3.3. WebView

Uma vez gerados os conjuntos $\mathcal{R}_{\text{obs}}$ e $\mathcal{R}_{\text{inf}}$, a verificação de roteamento interdomínio oferecida pelo RouteWatcher se dá conforme descrito a seguir: primeiro, é gerado o produto cartesiano $\mathcal{M} \times \mathcal{P}$. Em seguida, para cada par (m, p) comparamos os valores de $\mathcal{R}_{\text{obs}}(p, m, t)$ e $\mathcal{R}_{\text{inf}}(p, m)$ para classificar as rotas para p observadas em m. O módulo WebView organiza os resultados da análise em uma matriz onde cada posição apresenta utiliza um código de cores para denotar a classificação, aplicando as regras na tabela 3.3, em ordem da classificação mais específica para a menos específica.

3.4. Detalhes de implementação

O RouteWatcher é modularizado utilizando contêineres do Docker, facilitando a configuração do ambiente de execução, modularizando os serviços de banco de dados, e a integração dos módulos DumpParser e o RouteModel para servir o WebView.

4. Avaliação

O propósito do desenvolvimento do RouteWatcher foi de implementar um sistema para monitoramento e verificação de rotas na Internet. Para evidenciar esta contribuição, demonstramos o funcionamento desta ferramenta realizando uma analise pontual de diversos prefixos em um instante de tempo. Nesta seção descrevemos as configurações do RouteWatcher realizada ao longo do experimento, bem os resultados obtidos.

Prefixos alvo. Monitoramos prefixos IP de grandes bancos por que estes prefixos (i) hospedam serviços críticos e precisam de alta robustez, e por que (ii) são visados por

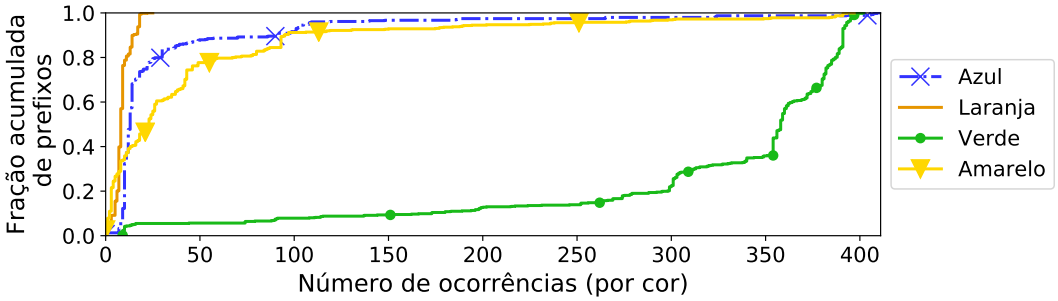


Figura 2. Distribuição de prefixos de acordo com a classificação de cores utilizada na visualização de resultados do experimento para análise pontual do RouteWatcher.

agentes maliciosos e sequestros de prefixos para realização de ataques de *phishing*. Obtemos uma lista de bancos candidatos da lista de 100 maiores bancos do mundo segundo pesquisa da Standard & Poor's.[4]

Convertemos o nome de cada banco para uma lista de ASes usando a base de dados da Hurricane Electric.[5] Dentre os 100 bancos, selecionamos um subconjunto de 25 bancos operando 60 ASes presentes na base de dados de relacionamento entre ASes disponibilizado pela CAIDA [Luckie et al. 2013]. Consideramos como alvo todos os prefixos IP originados pelos 60 ASes, removendo prefixos pequenos cobertos por outros prefixos maiores. Nossa lista de prefixos alvo $\mathcal{P}$ possui 547 prefixos.

Rotas para os prefixos alvo. Em nossa análise usamos o RouteWatcher para análise estática de rotas em tabelas BGP coletadas de um conjunto $\mathcal{M}$ de 565 monitores BGP [RIPE NCC 2019, Route Views 2019] para os prefixos em $\mathcal{P}$. Em particular, utilizamos um registro de rotas de tabelas BGP coletado às 00:00 do dia 8 de Junho de 2019. O registro de rotas contém 20.941 rotas para os 547 prefixos monitorados, dos quais 130 possuem 90% de classificações pretas ou vermelhas. Estes monitores foram ignorados nesta análise já que este valor indica falha ou comportamento anômalo do monitor.

Resultados. Para o conjunto de dados resultante do processo de coleta e processamento descrito na seção anterior, calculamos $\mathcal{R}_{\text{inf}}$ (seção 3.2) e comparamos com $\mathcal{R}_{\text{obs}}$ (seção 3.1). A figura 2 mostra a distribuição, para todos os prefixos $p \in \mathcal{P}$ alvo, a fração de monitores com para cada tipo de resultado comparativo classificado de acordo com o sistema de coloração utilizado pelo módulo WebView (seção 3.3). Nossos resultados indicam que a maior parte dos pares (prefixo, monitor) possuem rota compatível com o modelo, mas que alguns casos fogem do esperado (linhas laranja e azul), que podem ser causadas por erros na base da CAIDA ou anomalia de roteamento.

5. Descrição da demonstração planejada para o Salão de Ferramentas

O código-fonte, documentação e tutorial de instalação do RouteWatcher estão disponíveis em `http://dcc.ufmg.br/~lucas.barsand/routewatcher` . O plano para demonstração do RouteWatcher no salão de ferramentas é proporcionar aos conferencistas uma interação com dados recentes de tabelas de roteamento. Para fins de demonstração, iremos utilizar o RouteWatcher para verificar rotas para prefixos analisados na seção 4.

[4]https://www.spglobal.com
[5]https://bgp.he.net

6. Conclusão

Embora seja imprescindível para o atual funcionamento da Internet, o roteamento entre ASes realizado pelo BGP possui diversas limitações que o tornam vulnerável sob diversos aspectos, demandando monitoramento constante de rotas para fins de identificação e análise de anomalias. Para auxiliar pesquisadores e operadores de rede, apresentamos o RouteWatcher: um sistema que compara rotas observadas em coletores BGP com inferências a partir de um modelo para facilitar identificação e análise de anomalias de roteamento interdomínio. Demonstramos sua eficácia utilizando-o na verificação de rotas para prefixos de 25 dos 100 maiores bancos do mundo.

Agradecimentos Este trabalho foi financiado por: RIPE NCC, RNP, FAPEMIG, CAPES e CNPq.

Referências

[Gao 2001] Gao, L. (2001). On inferring autonomous system relationships in the internet. *IEEE/ACM Trans. Netw.*, 9(6):733–745.

[Giotsas et al. 2014] Giotsas, V., Luckie, M., Huffaker, B., and claffy, k. (2014). Inferring complex as relationships. In *IMC 2014*.

[Goodin 2017] Goodin, D. (2017). Russian-controlled telecom hijacks financial services' Internet traffic. ARS Technica, `bit.ly/2JqRZCe`.

[IIT-CNR 2019] IIT-CNR (2019). Isolario Project. `www.isolario.it`.

[Jin et al. 2019] Jin, Y., Scott, C., Dhamdhere, A., Giotsas, V., Krishnamurthy, A., and Shenker, S. (2019). Stable and practical AS relationship inference with ProbLink. In *NSDI*.

[Lad et al. 2006] Lad, M., Massey, D., Pei, D., Wu, Y., Zhang, B., and Zhang, L. (2006). Phas: A prefix hijack alert system. In *USENIX Security Symposium 2006*.

[Luckie et al. 2013] Luckie, M., Huffaker, B., Dhamdhere, A., Giotsas, V., and claffy, k. (2013). As relationships, customer cones, and validation. In *IMC 2013*.

[Memoria 2019] Memoria, F. (2019). Hackers Hijack Major UK Supermarket's Twitter Account to Promote Bitcoin Scam. Crypto Globe, `bit.ly/2G7qagb`.

[RIPE NCC 2019] RIPE NCC (2019). Routing Information Service. `bit.ly/2NNZbwn`.

[Route Views 2019] Route Views (2019). University of Oregon Route Views Project. `www.routeviews.org`.

[Siddiqui et al. 2014] Siddiqui, M. S., Montero, D., Yannuzzi, M., Serral-Gracià, R., and Masip-Bruin, X. (2014). Route leak identification: A step toward making inter-domain routing more reliable. In *DRCN 2014*.

[Strickx 2019] Strickx, T. (2019). How Verizon and a BGP Optimizer Knocked Large Parts of the Internet Offline Today. Cloudflare blog, `bit.ly/2SbZbFc`.

[Zhang et al. 2010] Zhang, Z., Zhang, Y., Hu, Y. C., Mao, Z. M., and Bush, R. (2010). iSPY: Detecting ip prefix hijacking on my own. *IEEE/ACM Trans. Netw.*, 18(6):1815–1828.

[Zheng et al. 2007] Zheng, C., Ji, L., Pei, D., Wang, J., and Francis, P. (2007). A light-weight distributed scheme for detecting ip prefix hijacks in real-time. In *SIGCOMM 2007*.