Identificação de Políticas de Validação de Rotas no RPKI

Marcel Mendes,[1] **Leonardo Oliveira,**[1] **Ítalo Cunha,**[1] **Ethan Katz-Bassett**[2]

[1]Departamento de Ciência da Computação
Universidade Federal de Minas Gerais
{marcelmendes, leonardooliveira, cunha}@dcc.ufmg.br

[2]Department of Electrical Engineering
Columbia University
ethan@ee.columbia.edu

Abstract. *BGP, the routing protocol used to interconnect networks in the Internet, lacks the ability to authenticate routes, leading to vulnerabilities like prefix hijacks and route leaks. RPKI is a growing technology that alleviates this problem by allowing operators to specify which networks can announce their prefixes. Quantifying RPKI's impact on routing security requires monitoring which networks deploy RPKI route validation. This monitoring is challenging due to limited route visibility and opaque routing policies. In this work we propose a new algorithm that combines targeted announcement configurations to extract more detailed information about a network's routing decisions with careful reasoning to make precise inferences about how a network uses the RPKI. Our experiments on the Internet unveils different RPKI policies, and indicates that RPKI adoption is increasing.*

Resumo. *O BGP, protocolo de roteamento usado para interconectar redes na Internet, não suporta a autenticação de rotas, levando a vulnerabilidades como sequestros de prefixos e vazamentos de rotas. O RPKI é uma tecnologia em adoção que alivia esse problema, permitindo que os operadores especifiquem quais redes podem anunciar seus prefixos. Quantificar o impacto do RPKI na segurança de roteamento requer monitorar quais redes implementam validação de rotas usando o RPKI. Esse monitoramento é desafiador devido à visibilidade limitada sobre rotas na Internet e à opacidade de políticas de roteamento. Neste trabalho propomos um novo algoritmo que combina configurações de anúncios direcionadas para extrair informações mais detalhadas sobre decisões de roteamento com um processamento judicioso das observações para fazer inferências precisas sobre como uma rede utiliza o RPKI. Nossos experimentos na Internet revelam diferentes políticas de RPKI utilizadas na prática e apontam um aumento da adoção RPKI.*

1. Introdução

O *Border Gateway Protocol* (BGP) é o protocolo usado para a troca de anúncios entre sistemas autônomos na Internet. O BGP provê escalabilidade e permite operadores de rede expressarem políticas de roteamento complexas [Quoitin et al. 2003]. Porém, o BGP não provê mecanismos de autenticação, resultando em sérios problemas de segurança. Em particular, o BGP é incapaz de verificar a validade ou legitimidade de um anúncio de rota recebido de uma rede vizinha, tornando-o vulnerável a ataques ou até mesmo erros

de configuração acidentais. Problemas como sequestros de prefixos (*prefix hijack*) ou vazamento de rotas (*route leak*) estão entre falhas de segurança recorrentes e de grande impacto [Testart et al. 2019] resultantes da falta de autenticação no BGP.

Diferentes mecanismos de autenticação foram propostos para estender o BGP ao longo dos anos. Recentemente, o *Resource Public Key Infrastructure* (RPKI) [Bush and Austein 2013] vem ganhando tração e sendo adotado por operadores de rede. O RPKI adiciona uma camada de segurança no compartilhamento de rotas entre sistemas autônomos na Internet. O RPKI usa uma infraestrutura distribuída de chaves públicas, onde é possível emitir certificados de autorização de rotas (*Route Origin Authorization*, ROA) e adicioná-los a repositórios públicos. Estes repositórios públicos podem ser consultados por sistemas autônomos interessados em realizar a validação de rotas propagadas na Internet utilizando os certificados de autorização (ROAs). Um ROA é criado pelo controlador de um prefixo IP P e especifica quais sistemas autônomos podem anunciar quais sub-prefixos de P. O processo de validação (*Route Origin Validation*, ROV) é realizado comparando rotas recebidas em um anúncio BGP com os ROAs armazenados no RPKI.

Diversos trabalhos anteriores se propuseram a quantificar a adoção e o impacto de ROV. Alguns trabalhos utilizam apenas rotas observadas na Internet por coletores BGP, comparando a propagação de rotas válidas e inválidas para inferir se sistemas autônomos realizam ROV [Gilad et al. 2017, Testart et al. 2020]. Outros realizam experimentos controlados e coletam dados de medições ativas [Reuter et al. 2018, Rodday et al. 2021, Li et al. 2023], o que permite estabelecer com maior precisão se uma rota sofre mudanças devido ao estado do ROA ou devido a outros fatores externos.

Apesar do progresso realizado na caracterização da adoção ROV, estudos anteriores se limitam a uma classificação binária para determinar se um sistema autônomo implanta ROV ou não. No entanto, alguns sistemas autônomos de trânsito implantam ROV de forma parcial, (i) descartando rotas inválidas recebidas de provedores e parceiros, mas não quando recebidas de clientes, ou (ii) utilizam o ROV como um passo adicional no processo de seleção de rotas, preferindo rotas válidas quando disponíveis mas tolerando rotas inválidas quando nenhuma rota válida existe. O estado da arte, limitado à classificação binária da implantação de ROV, é inadequado para sistemas autônomos realizando implantação parcial.

Neste trabalho apresentamos um algoritmo para inferência do comportamento ROV de um sistema autônomo de forma mais detalhada do que em trabalhos anteriores. Nosso algoritmo combina observações de rota para cinco configurações distintas (trabalhos anteriores utilizam no máximo duas configurações), coletando um conjunto rico e complementar de informações que permitem ir além da classificação binária e caracterizar *como* um sistema autônomo implanta ROV. Em particular, nosso algoritmo consegue identificar se um sistema autônomo (i) descarta rotas inválidas, (ii) prefere rotas válidas mas utiliza rotas inválidas como *backup*, ou (iii) ignora ROAs.

Avaliamos nosso algoritmo realizando experimentos reais na Internet usando a plataforma PEERING. A caracterização dos resultados mostra que o algoritmo faz inferências consistentes para diferentes configurações de experimentos. Mostramos ainda que alguns sistemas autônomos na Internet de fato utilizam a política de preferir rotas válidas e utilizam rotas inválidas como *backup*; política esta não considerada em traba-

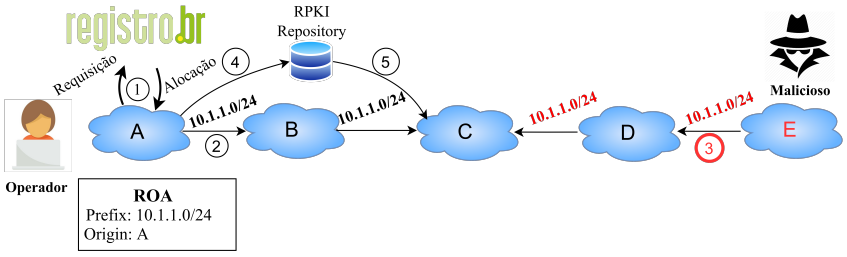

Figura 1. Anúncio de rotas

lhos anteriores. Por último, nossas medições indicam um aumento da fração de sistemas autônomos que implantam ROV e, consequentemente, da segurança do sistema de roteamento interdomínio da Internet.

O monitoramento da adoção de RPKI é importante e desafiador. Nosso trabalho avança o estado da arte e provê informações mais precisas sobre esse complexo sistema. Os resultados das nossas inferências estão disponíveis para as comunidades de pesquisadores e operadores de rede. Acreditamos que nossas contribuições impulsionarão, indiretamente, a adoção do RPKI.

2. Roteamento Interdomínio e Validação de Rotas

A figura 1 mostra o processo de anúncio de rotas por um operador de rede. Antes de anunciar um prefixo, um operador de rede precisa obter uma alocação de recursos (endereços IP e número de sistema autônomo) de um registro de numeração como o Registro.br ①. Um operador de rede pode então anunciar seus prefixos para outras redes, em geral provedores de trânsito e parceiros em pontos de troca de tráfego, utilizando o protocolo BGP ②. Um grave problema de segurança do BGP é a falta de autenticação de rotas, o que permite um operador de rede anunciar, maliciosamente ou acidentalmente, um prefixo que não foi alocado a ele ③.

Neste cenário, um anúncio legítimo compete com um anúncio ilegítimo durante o processo de propagação de rotas no BGP. O primeiro critério de escolha de rotas no protocolo BGP é o LocalPref, um valor numérico associado a cada rota pelo sistema autônomo para implementar sua política de roteamento. Geralmente, o LocalPref é configurado para que rotas de clientes (que geram receita) sejam preferidas sobre rotas de parceiros (que não geram receita nem custo) e para que rotas de parceiros sejam preferidas sobre rotas de provedores (que geram custo). Caso duas rotas tenham o mesmo LocalPref (e.g., duas rotas recebidas de clientes), o segundo critério de escolha de rota do protocolo BGP é o comprimento das rotas, que conta o número de sistemas autônomos atravessados pela rota. No exemplo da figura 1, o sistema autônomo D escolheria a rota ilegítima de E em vez da rota legítima de A pois a rota de E é mais curta (considerando que o LocalPref é o mesmo).

Para aliviar este problema, o RPKI provê mecanismos que permitem a autenticação de rotas na Internet. Primeiro, um operador de rede precisa publicar certificados de autorização de rota (ROA) descrevendo quais sistemas autônomos podem anunciar prefixos sob seu controle ④. Um ROA especifica um prefixo IP P, o subprefixo mais específico de P que pode ser anunciado (*maxLength*), e o conjunto de sistemas autônomos que podem anunciar P e os subprefixos de P inclusos. Qualquer sistema

autônomo pode acessar os repositórios armazenando ROAs e verificá-los através de uma cadeia de certificados cuja raiz é o registro de numeração responsável pela alocação do prefixo ⑤. Na figura 1, o sistema autônomo C pode utilizar as informações do RPKI para realizar ROV e escolher a rota legítima anunciada pelo sistema autônomo A. A validação de rotas tem precedência sobre o LocalPref e o comprimento das rotas no processo de decisão do BGP.

3. Inferência de Políticas de Validação de Rotas

Neste trabalho propomos um novo algoritmo para caracterização da política de sistemas autônomos em relação à validação de rotas (ROV) na Internet. Nosso algoritmo diferencia entre três políticas possíveis:

Ignora-ROA. Um sistema autônomo *ignora-ROA* quando ele não realiza validação de rotas. Estes sistemas autônomos utilizam o processo padrão de escolha de rotas do BGP, e escolhem rotas inválidas quando elas têm LocalPref maior ou são mais curtas que as rotas válidas. Este é o comportamento padrão do protocolo BGP quando um sistema autônomo não realiza ROV.

Descarta-inválida. Um sistema autônomo que implanta ROV pode configurar seus roteadores para *descartar* rotas *inválidas*. Estes sistemas autônomos ficam sem rota para um prefixo quando apenas rotas inválidas estão disponíveis.

Prefere-válida. Um sistema autônomo que implanta ROV pode configurar seus roteadores para *preferir* rotas *válidas*. Estes sistemas autônomos utilizam rotas válidas sempre que disponíveis, mas utilizam rotas inválidas como uma alternativa caso nenhuma rota válida esteja disponível. Essa configuração evita a perda de conectividade em casos de erro de configuração, do ROA ou do anúncio, que podem causar uma rota legítima ficar inválida no RPKI [Iamartino et al. 2015]. Por outro lado, essa configuração permite a utilização de prefixos não utilizados para atividades maliciosas como envio de spam [Testart et al. 2019].

Até onde sabemos, o nosso é o primeiro trabalho capaz de inferir a implantação parcial de ROV através da política *prefere-válida*. A identificação das políticas *ignora-ROA* e *descarta-inválida* já foi estudada anteriormente na literatura; a classificação binária, porém, leva a erros ao ignorar a política *prefere-válida*.

3.1. Configuração de Anúncios

Para identificar a política de segurança de sistemas autônomos, nosso algoritmo manipula certificados de autorização de rota (ROAs) e anúncios BGP para cinco prefixos distintos. As informações complementares obtidas de rotas para cinco prefixos permitem (i) identificar quais rotas estão disponíveis para um sistema autônomo em diferentes cenários e (ii) identificar a rota escolhida por um sistema autônomo em cenários onde múltiplas rotas estão disponíveis. Estes dois fatores permitem nosso algoritmo diferenciar entre possíveis explicações para as escolhas de rota observadas e obter informações complementares para fazer inferências mais precisas. Trabalhos anteriores comparam apenas rotas válidas e rotas inválidas para dois prefixos, focando apenas em identificar a rota escolhida, e não em obter informações completas para determinar as rotas disponíveis [Reuter et al. 2018, Hlavacek et al. 2018, Rodday et al. 2021]. Consequentemente, os trabalhos anteriores não coletam informações suficientes para diferenciar a política *prefere-válida* da política *ignora-ROA*, classificando ambas como *ignora-ROA*.

Tabela 1. Configurações dos Anúncios dos Prefixos

PREFIXO	VIZINHOS	ROA	COMPRIMENTO
P_1	V_{good} e V_{bad}	Nenhum	Curta de V_{bad}, longa de V_{good}
P_2	V_{bad}	Nenhum	Curta
P_3	V_{good}	Nenhum	Longa
P_4	V_{bad}	Inválida	Curta
P_5	V_{good} e V_{bad}	Inválida de V_{bad}, válida de V_{good}	Curta de V_{bad}, longa de V_{good}

Nosso algoritmo anuncia cinco prefixos, denotados de P_1 a P_5. A configuração do anúncio de cada prefixo é mostrada na Tabela 1. Os prefixos são anunciados para um par de sistemas autônomos vizinhos. Um dos vizinhos anuncia apenas prefixos válidos no RPKI e é denotado V_{good}, enquanto o outro vizinho faz anúncios de prefixos inválidos no RPKI e é denotado V_{bad}. Os prefixos P_2, P_3 e P_4 são anunciados apenas para um vizinho para permitir a identificação de rotas disponíveis para sistemas autônomos na Internet em diferentes cenários, enquanto os prefixos P_1 e P_5 são anunciados pelos dois vizinhos para permitir a propagação de duas rotas com propriedades distintas e identificarmos qual rota os sistemas autônomos escolhem quando múltiplas estão disponíveis.

Além disso, fazemos anúncios de prefixos sem ROA e com ROA, para identificar as escolhas realizadas por sistemas autônomos quando o RPKI não é utilizado, quando a rota recebida é válida e quando a rota recebida é inválida.

Por último, utilizamos *BGP prepending*, adicionando artificialmente o número de sistema autônomo da origem múltiplas vezes ao anúncio realizado, tornando a rota artificialmente mais longa. O *prepending* é uma prática comum no roteamento interdomínio e utilizado para tornar rotas menos atrativas, especialmente útil para rotas de *backup* ou que têm capacidade reduzida [Marcos et al. 2020]. Em geral, utilizamos *prepending* para tornar as rotas válidas mais longas que as rotas inválidas. O comprimento de uma rota é o segundo fator de desempate de rotas no BGP e afeta as escolhas realizadas por sistemas autônomos na Internet. Sem controlar o comprimento das rotas, seria impossível diferenciar se um sistema autônomo escolhe uma rota em função da utilização de ROV ou em função do comprimento da rota. Ao tornar as rotas válidas artificialmente mais longas, removemos este fator de confusão de nossas análises e garantimos que a rota válida, longa, só é escolhida sobre a rota inválida, curta, em função da aplicação de ROV.

A intuição por trás da configuração de cada prefixo é a seguinte:

P_1: Permite identificar o vizinho preferido na ausência de ROA.
P_2 e P_3: Permitem identificar a rota preferida por sistemas autônomos para V_{good} e V_{bad}.
P_4: Permite identificar quais sistemas autônomos utilizam uma rota inválida na ausência de alternativas. Se um sistema autônomo escolhe uma rota para P_4, sabemos que ele não utiliza a política *descarta-inválida*.
P_5: Permite identificar a preferência de sistemas autônomos entre uma rota válida longa e uma rota inválida curta. Utilizamos esta informação para tentar inferir se um sistema autônomo utiliza a política *prefere-válida*.

Apesar das informações complementares obtidas pelos anúncios acima e utilizadas como entrada por nosso algoritmo, frequentemente é impossível identificar com exatidão a política de ROV de um sistema autônomo. Três casos comuns impossibilitam

Tabela 2. Perfis de Comportamento e Inferências na Fase 1

ROTA OBSERVADA			
P_1	P_4	P_5	INFERÊNCIA
Qualquer rota	Inválida curta para V_{bad}	Inválida curta para V_{bad}	*ignora-ROA*
Curta para V_{bad}	Inválida curta para V_{bad}	Válida longa para V_{good}	*prefere-válida*
Curta para V_{bad}	Sem rota	Válida longa para V_{good}	*descarta-inválida*

a identificação de políticas de ROV, gerando ambiguidades: (i) falta de visibilidade sobre as rotas utilizadas por um sistema autônomo, (ii) ambiguidade na inferência de ROV de algum sistema autônomo na rota escolhida, e (iii) escolhas de rotas por um sistema autônomo que contradizem expectativas ou modelos conhecidos.

Apresentamos nosso algoritmo em duas fases. A fase 1 realiza uma inferência inicial para as três políticas descritas acima (*descarta-inválida*, *prefere-válida* e *ignora-ROA*) considerando falta de visibilidade e escolhas de rota contraditórias. A fase 2 faz verificações adicionais para refinar inferências realizadas na fase 1 em função de possíveis ambiguidades decorrentes das rotas observadas.

3.2. Fase 1: Classificação Inicial por Perfis de Comportamento

Na fase 1 realizamos uma classificação inicial em função das rotas escolhidas por sistemas autônomos na Internet para os prefixos P_1, P_4 e P_5. A tabela 2 apresenta três perfis de rotas observadas (um perfil por linha). Para cada perfil inferimos uma política de ROV distinta na fase 1, que será refinada na fase 2.

Uma restrição importante dos perfis apresentados na tabela 2 para as políticas *prefere-válida* e *descarta-inválida* é o requisito de que a rota curta para V_{bad} seja escolhida para o prefixo P_1. Esta restrição garante que a escolha entre a rota curta e a rota longa para P_1 é feita em função do comprimento das rotas, e não em função do LocalPref. Quando essa restrição é violada e o LocalPref de um sistema autônomo leva à escolha da rota longa para P_1, é impossível diferenciar se a escolha da rota válida longa sobre a rota inválida curta para P_5 é feita em função da aplicação de ROV ou LocalPref.

Os perfis apresentados na tabela 2 são os perfis esperados. Porém, às vezes sistemas autônomos fazem escolhas de rota contraditórias, por exemplo descartando a rota para o prefixo P_4 ao mesmo tempo que utiliza a rota inválida para o prefixo P_5. Caso a escolha de rotas de um sistema autônomo não se encaixe em nenhum perfil, classificamos sua política de segurança como *oculta*. Também é possível que as rotas observadas estejam incompletas ou que alguma anomalia de roteamento tenha ocorrido. Em particular, rotas para os prefixos P_1, P_2 e P_3 devem sempre propagar para todos os sistemas autônomos devido à ausência de ROA. Caso alguma destas rotas não sejam observadas, também classificamos a política de segurança de um sistema autônomo como *oculta*.

3.3. Fase 2: Tratando Casos Especiais e Ambiguidades

A fase 2 implementa verificações adicionais para diferenciar entre as possíveis explicações possíveis para as observações utilizadas para inferência na fase 1. Para cada uma das inferências realizadas na fase 1, aplicamos verificações adicionais:

***Ignora-ROA*.** Antes de inferir que um sistema autônomo A utiliza a política *ignora-ROA*, na fase 2 verificamos se A recebe a rota válida longa para o prefixo P_5. Caso o

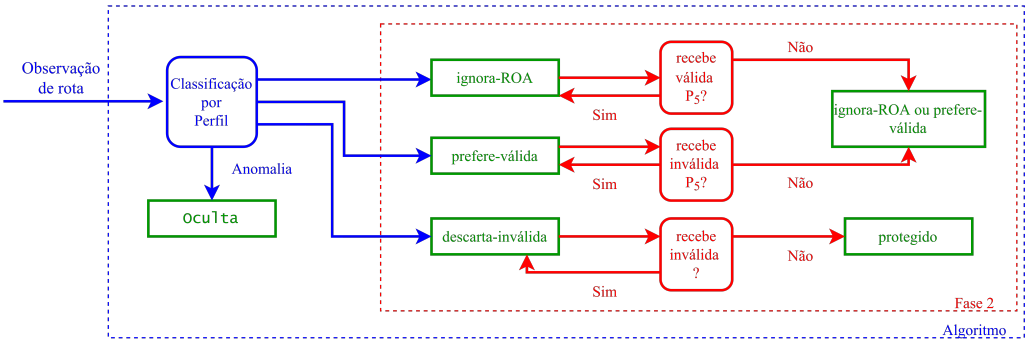

Figura 2. Diagrama simplificado do Algoritmo

sistema autônomo A não receba a rota válida longa para o prefiro P_5, a escolha da rota inválida curta para o prefixo P_5 é consequência direta da indisponibilidade da rota válida longa e não podemos tirar nenhuma conclusão sobre a política de ROV utilizada por A.

Concretamente, analisamos a rota R escolhida pelo sistema autônomo A para o prefixo P_3 e verificamos se todos os sistemas autônomos em R utilizam a política *descarta-inválida* ou *prefere-válida*. Também verificamos se existe algum vizinho conhecido[1] de A utilizando uma rota válida longa para P_5. Caso uma destas condições sejam satisfeitas, consideramos que A recebe a rota válida longa e é responsável por escolher a rota inválida curta, confirmando a política *ignora-ROA*.

Caso nenhuma das condições seja satisfeita, tornamos a inferência para A menos precisa. Em particular, como observamos A utilizando a rota inválida curta para P_4, conseguimos excluir a possibilidade de A utilizar a política *descarta-inválida* e inferimos sua política como *prefere-válida* $\vee$ *ignora-ROA*.

Descarta-inválida. Antes de inferir que um sistema autônomo A utiliza a política *descarta-inválida*, na fase 2 verificamos se A recebe a rota inválida curta para os prefixos P_4 e P_5. Caso o sistema autônomo A não receba a rota inválida curta para estes prefixos, a ausência de rota para o prefixo P_4 e a utilização da rota válida longa para o prefixo P_5 são consequências diretas da indisponibilidade da rota inválida curta e não podemos tirar nenhuma conclusão sobre a política de ROV utilizada por A.

Concretamente, analisamos a rota R escolhida pelo sistema autônomo A para o prefixo P_2, que tem anúncio equivalente ao prefixo P_4 exceto pela configuração de ROA. Se todos os sistemas autônomos em R utilizarem a política *ignora-ROA*, então consideramos que A recebe a rota inválida curta para P_4 e P_5 através dos sistemas autônomos em R. Neste caso, concluímos que A é responsável por descartar a rota inválida curta e confirmamos a inferência *descarta-inválida*.

Se algum sistema autônomo $X \in R$ utiliza a política *descarta-inválida* ou *prefere-válida*, então consideramos que X é responsável por descartar a rota inválida e impedir que ela propague até o sistema autônomo A. Neste caso não conseguimos inferir a política de ROA utilizada por A. Porém, em vez de classificar sua política como *oculta*, dizemos

[1]Identificamos o conjunto de vizinhos de A a partir da base de relacionamentos entre sistemas autônomos da CAIDA [Luckie et al. 2013].

que A está *protegido*, pois as rotas observadas indicam que ele não recebe rotas inválidas, beneficiando das políticas de segurança *descarta-inválida* de outros sistemas autônomos na topologia.

Prefere-válida. Antes de inferir que um sistema autônomo A utiliza a política *prefere-válida*, na fase 2 verificamos se A recebe a rota inválida curta para o prefixo P_5. De forma similar, caso A não receba a rota inválida curta para P_5, a escolha da rota válida longa para P_5 é consequência direta da indisponibilidade da rota inválida curta e não podemos tirar nenhuma conclusão sobre a política de ROV utilizada por A.

Concretamente, analisamos a rota R escolhida pelo sistema autônomo A para o prefixo P_4 e verificamos se todos os sistemas autônomos em R utilizam a política *ignora-ROA* ou se existe algum vizinho conhecido de A que recebe a rota curta inválida para P_5. Caso uma das condições seja satisfeita, consideramos que A recebe a rota inválida curta mas escolhe a rota válida longa devido à aplicação de ROV, confirmando a inferência *prefere-válida*.

Se algum sistema autônomo $X \in R$ utiliza a política *descarta-inválida* ou *prefere-válida*, então tornamos a inferência para A menos precisa. Como no caso *ignora-ROA*, como observamos A utilizando a rota inválida curta para P_4, conseguimos excluir a possibilidade de A utilizar *descarta-inválida* e inferimos sua política como *prefere-válida* $\vee$ *ignora-ROA*.

Refinamentos Complementares. Além do refinamento da política *descarta-inválida* para *protegido* descrito acima, também aplicamos um refinamento para sistemas autônomos com política *prefere-válida* $\vee$ *ignora-ROA*.

Identificamos que um subconjunto dos sistemas autônomos com inferência *prefere-válida* $\vee$ *ignora-ROA* sempre escolhem rotas através de um vizinho X específico, inclusive para P_5, exceto no caso da rota inválida para o prefixo P_4. Estas observações podem ser resultado da aplicação (i) de uma política de segurança *prefere-válida* ou (ii) de uma política de engenharia de tráfego que configura um LocalPref maior para rotas recebidas de X (e.g., por razões de custo ou desempenho). Para estes casos, refinamos a inferência de *prefere-válida* $\vee$ *ignora-ROA* para *prefere-válida* $\vee$ *prefere-vizinho* para capturar a propriedade de que estes sistema autônomos evitam rotas inválidas por preferirem rotas através de redes que utilizam *descarta-inválida*.

3.4. Inferência por Busca em Largura

A inferência para um sistema autônomo A depende das políticas de outros sistemas autônomos X atravessados pelas rotas escolhidas por A para o prefixo P_2. Para permitir a inferência das políticas utilizadas por sistemas autônomos distantes, o algoritmo deve ser executado para cada sistema autônomo individualmente, ordenados de acordo com uma busca em largura no grafo formado pelos sistemas autônomos (vértices) e enlaces das rotas observadas para o prefixo P_2.

4. Experimento e Coleta de Dados

Nesta seção descrevemos os experimentos que executamos para caracterizar o comportamento de ASes na Internet quanto à RPKI. Descrevemos os experimentos realizados (seção 4.1) e os dados utilizados no estudo (seção 4.2).

4.1. Experimentos no PEERING

Executamos experimentos reais na Internet através da plataforma PEERING [Schlinker et al. 2019]. Entre 15 e 30 de dezembro de 2023 realizamos 8 experimentos, totalizando 40 anúncios de rota, utilizando os prefixos 138.185.228.0/22 e 204.9.170.0/24.

A plataforma PEERING recebe trânsito de redes de pesquisa (Internet2, RNP e Gèant) e de provedores que suportam atividades de pesquisa. Devido ao perfil dos provedores, a maioria dos PoPs do PEERING têm provedores que utilizam a política *descarta-inválida*, o que limita as opções de PoPs que podem ser utilizados como V_{bad}. Especificamente, utilizamos o PoP do PEERING no Amsterdam Internet Exchange (AMS-IX) como V_{bad}, o único PoP do PEERING com um provedor que atualmente permite a propagação de anúncios e rota inválidos.[2] Utilizamos quatro PoPs do PEERING hospedados no Vultr[3] como V_{good}: Londres, Madri, Estocolmo e Varsóvia. Para cada par (V_{good}, V_{bad}), realizamos dois experimentos repetidos para verificar a consistência das inferências.

Cada prefixo é anunciado por um período de 90 minutos, o que é suficiente para convergência do protocolo BGP [Anwar et al. 2015] e, mais importante, para evitar mudanças de rota frequentes e a ativação do mecanismo de prevenção de oscilações (*route-flap damping*) [Villamizar et al. 1998]. Para evitar utilizar rotas transientes durante o período de convergência que segue um anúncio, esperamos a estabilização das rotas e consideramos apenas a primeira rota estável por pelo menos 5 minutos após o anúncio do prefixo [Feldmann et al. 2004].

De forma similar, retiramos (*withdraw*) o anúncio dos prefixos por um período de 90 minutos antes de realizar outro anúncio. A retirada no anúncio garante que cada experimento realizado parte de um único estado conhecido, no qual nenhum sistema autônomo na Internet tem rotas para os prefixos. Considerando o período de anúncio e a retirada, cada experimento leva 180 minutos.

Para realização deste trabalho, integramos o PEERING à cadeia certificadora do RPKI do NIC.br. Esta integração está em produção e é atualmente utilizada por múltiplos grupos de pesquisa em projetos sobre RPKI. A implementação utiliza o servidor Krill e delega a hospedagem dos ROAs para o repositório do NIC.br.

4.2. Conjuntos de Dados

Utilizamos tabelas e atualizações (RIBs e *updates*) dos coletores BGP das plataformas RIPE RIS[4] e RouteViews[5] para a observação das rotas durante nossos experimentos. Coletores BGP recebem e catalogam anúncios de rotas de sistemas autônomos parceiros, fornecendo uma visão do roteamento interdomínio na Internet.

Inferimos as rotas de um AS X que não faz parceria com os coletores quando o AS X faz parte da rota de outro AS P parceiro de algum coletor. Por exemplo, se

[2]Discutimos esta limitação com os operadores do PEERING, que não estavam cientes dela. Os operadores informaram que pretendem conversar com os provedores para pedir que dêem tratamento especial aos prefixos do PEERING e propaguem anúncios inválidos, aumentando a flexibilidade da plataforma para suportar experimentos sobre RPKI.

[3]Vultr, https://vultr.com

[4]RIPE Routing Information Service, https://ris.ripe.net

[5]University of Oregon RouteViews Project, https://routeviews.org

Tabela 3. Distribuição das Inferências de Políticas de Segurança

CLASSIFICAÇÃO	MADRI		ESTOCOLMO		LONDRES		VARSÓVIA		TODOS	
Descarta-inválida	39	8,11%	37	7,66%	34	7,01%	35	7,22%	41	8,10%
Ignora-ROA	21	4,37%	30	6,21%	34	7,01%	20	4,12%	33	6,52%
Prefere-Válida	5	1,04%	3	0,62%	5	1,03%	5	1,03%	7	1,38%
" ∨ ignora-ROA	43	8,94%	31	6,41%	32	6,59%	41	8,45%	36	7,11%
" ∨ prefere-vizinho	7	1,46%	11	2,28%	2	0,41%	7	1,44%	5	0,99%
Oculto	94	19,54%	85	17,60%	129	26,60%	99	20,41%	104	20,55%
Protegido	272	56,55%	286	59,21%	249	51,34%	278	57,32%	280	55,34%
# ASes	481		483		485		485		506	

observarmos a rota $\langle P, X, Y, Z, O\rangle$, onde P é o AS parceiro do coletor e O é o AS que originou o anúncio, consideramos que a rota de X é $\langle X, Y, Z, O\rangle$.

5. Avaliação

Nesta seção apresentamos os resultados dos experimentos realizados e das políticas de segurança identificadas por nosso algoritmo na Internet. Disponibilizamos nossos resultados publicamente através de uma interface Web que facilita a visualização das rotas observadas e verificação das inferências realizadas pelo algoritmo bem como através de um arquivo JSON para uso por pesquisadores e operadores de rede[6]. O código fonte também se encontra disponível publicamente para consulta[7].

Consistência das inferências. As medições coletadas cobrem 507 sistemas autônomos distintos, a grande maioria observados em todos os experimentos. Para verificar a consistência das inferências realizadas pelo nosso algoritmo, comparamos as políticas de segurança inferidas para os 8 experimentos realizados a partir dos quatro pares de (V_{good}, V_{bad}) de origens utilizados.

Observamos que 65,08% (330) dos sistemas autônomos possuem 8 inferências idênticas, e que 34,71% (176) sistemas autônomos possuem 8 inferências consistentes. Definimos inferências como consistentes se elas têm interseção, por exemplo, quando um sistema autônomo é inferido *prefere-válida* em um experimento e *prefere-válida* ∨ *ignora-ROA* em outro experimento. Para estes casos, consideramos a inferência mais específica como a inferência correta. Observamos apenas 1 caso de inconsistência para o AS 51185, que apresentou uma inferência *ignora-ROA* para um experimento, *prefere-válida* para 4 experimentos e *prefere-válida* ∨ *ignora-ROA* para o restante.

Políticas de segurança na Internet. Na tabela 3 mostramos a distribuição das inferências realizadas para os sistemas autônomos cobertos por nossas medições, com exceção do AS 51185. Apresentamos os resultados por PoP do Vultr utilizado para originar as rotas válidas (V_{good}) e também os valores agregados em todos os experimentos.

Aproximadamente metade dos sistemas autônomos em cada localidade foram classificados como *protegidos*. Não conseguimos inferir a política de segurança desses sistemas autônomos pois eles estão "atrás" de outros sistemas autônomos utilizando políticas *descarta-inválida* ou *prefere-válida*, e provavelmente não recebem rotas

[6]Resultados: https://homepages.dcc.ufmg.br/~marcelmendes/medicao_1
[7]Código fonte: https://github.com/MarcelHMendes/rov-inference

Tabela 4. Distribuição de Inferências por Distância da Origem das Rotas Inválidas

DISTÂNCIA	1		2		3		4		5+	
Descarta-inválida	0		32	31,07%	7	3,68%	0		0	
Ignora-ROA	1	25,00%	16	15,53%	4	2,11%	0		0	
Prefere-válida	0		5	4,85%	0		0		0	
" ∨ ignora-ROA	2	50,00%	20	19,42%	15	7,89%	5	3,73%	1	2,00%
" ∨ prefere-vizinho	0		2	1,94%	1	0,53%	3	2,24%	1	2,00%
Protegido	0		1	0,97%	142	74,74%	102	76,12%	27	54,00%
Oculto	1	25,00%	27	26,21%	21	11,05%	24	17,91%	21	42,00%
# ASes	4		103		190		134		50	

Tabela 5. Mudança de Classificação Entre as Fases do Algoritmo

FASE 1	FASE 2	MADRI		ESTOCOLMO		LONDRES		VARSÓVIA	
Descarta-inválida	Protegido	272	87,45%	286	88,27%	249	87,67%	278	88,53%
Prefere-válida	Prefere-válida ∨ ignora-ROA	5	29,41%	4	22,22%	9	56,25%	4	25,00%
Ignora-ROA	Prefere-válida ∨ ignora-ROA	38	62,29%	27	45,76%	23	38,98%	37	62,71%
Prefere-válida	Prefere-válida ∨ prefere-vizinho	7	41,17%	11	61,11%	2	12,50%	7	43,75%

inválidas. Apesar do nosso algoritmo não conseguir fazer inferências para estes sistemas autônomos, notamos que esta limitação é intrínseca a qualquer algoritmo. É fundamentalmente impossível observar os efeitos e inferir a política de segurança de um sistema autônomo se ele nunca recebe rotas inválidas.

A tabela 3 também mostra que entre 12,17% e 14,28% dos sistemas autônomos têm inferências exatas de suas políticas de segurança (*descarta-inválida*, *ignora-ROA* e *prefere-válida*). Para uma fração entre 17,6% e 26,6% dos sistemas autônomos, não conseguimos fazer uma inferência (*oculta*) devido à falta de visibilidade de rotas pelos coletores utilizados. Em muitos casos não conseguimos observar as rotas de um sistema autônomo para os prefixos P_1, P_2 e P_3 que não possuem ROA.

A tabela 4 mostra a distribuição das políticas inferidas em função da distância de um sistema autônomo para a origem das rotas inválidas (V_{bad}). Uma abordagem para aumentar a cobertura das inferências seria realizar anúncios de mais PoPs, visto que conseguimos inferir de forma mais exata as políticas de sistemas autônomos próximos à origem. Podemos ver que a fração de sistemas autônomos com política *protegido* ou *oculta* cresce com o aumento da distância da origem. De qualquer forma, notamos que o aumento de inferências *protegido* é decorrente do aumento da adoção de ROV, o que demonstra a melhoria de segurança do roteamento interdomínio na Internet.

Tratamento de ambiguidades. A tabela 5 mostra a quantidade e fração de sistemas autônomos que mudaram de classificação durante a fase 2 do algoritmo. De forma geral, vemos que a fase 2 impacta significativamente os resultados e é essencial para a acurácia das inferências. Por exemplo, vemos que 272 dos sistemas autônomos inferidos como *descarta-inválida* mudaram a classificação para *protegido* no experimento, utilizando Madri como V_{good}; estes sistemas autônomos representam 87,45% dos sistemas

autônomos classificados como *descarta-inválida* na fase 1. Notamos que uma quantidade considerável de inferências *prefere-válida* mudaram para *prefere-válida* $\vee$ *prefere-vizinho*, mostrando que políticas de engenharia de tráfego e preferências de rota podem impactar inferências de políticas de segurança, especialmente em algoritmos anteriores que não levam estes fatores em consideração.

Evolução do uso de RPKI. Observamos um aumento na proporção de ASes que adotam o ROV. Comparando estudos anteriores [Rodday et al. 2021, Reuter et al. 2018] com os resultados obtidos, observamos um aumento da fração de ASes inferidos como *descarta-inválida* e *prefere-válida* em relação ao total de ASes analisados. Também observamos como a adoção do RPKI por um AS pode ter um efeito em cascata na propagação de rotas válidas para os ASes vizinhos, evidenciado pela proporção de ASes classificados como *protegidos*.

6. Trabalhos Relacionados

Utilização de ROA. Uma série de trabalhos caracteriza o agregado de ROAs criados no RPKI. O serviço de monitoramento do RPKI mantido pelo NIST (*National Institute for Standards and Technology*) é um dos derivados desta frente de pesquisa. Segundo o NIST, 47,71% dos prefixos anunciados são válidos, 0,92% são inválidos e 51,37% não possuem ROA em 15 de Janeiro de 2024.[8]

Resiliência e desempenho do RPKI. Como explicado na seção 2, a utilização do RPKI requer vários passos envolvendo diversos componentes distribuídos. Trabalhos anteriores realizaram estudos para testar a resiliência do RPKI contra ataques ou aumento de carga. [Hlavacek et al. 2022] explora a dependência do RPKI sobre seus componentes DNS. Neste trabalho eles argumentam que e o DNS é um ponto de preocupação na infraestrutura do RPKI. Os resultados mostram que o componente DNS pode levar a problemas de falta de redundância e ser um elo fraco, vulnerável a ataques, na infraestrutura do RPKI. De forma complementar, outros trabalhos caracterizaram o desempenho de componentes do RPKI. Por exemplo, [Fontugne et al. 2023] decompõe o processo de publicação de um ROA em múltiplos passos e caracteriza o tempo gasto pelos componentes envolvidos em cada etapa, fornecendo informações valiosas sobre o tempo de publicação de um ROA em diferentes registros de numeração e repositórios de armazenamento.

Adoção de ROV. Mais próximos ao nosso trabalho estão os que visam identificar quais sistemas autônomos implantam ROV [Reuter et al. 2018, Rodday et al. 2021, Gilad et al. 2017, Testart et al. 2020, Hlavacek et al. 2018]. Estas técnicas apresentam melhorias incrementais, por exemplo melhorando a precisão das inferências através do processamento judicioso das rotas observadas. [Reuter et al. 2018] mostra que o uso de experimentos BGP não controlados não é suficiente para determinar a adoção de ROV por um AS, apresentando uma metodologia rigorosa que permite a identificação de adoção de ROV por ASes vizinhos. [Hlavacek et al. 2018] e [Rodday et al. 2021] também usam experimentos BGP controlados em conjunto com medições de plano de dados, permitindo a inferência precisa da política de ROV para sistemas autônomos distantes da origem. Nosso trabalho pode ser visto como mais um elo nessa cadeia de técnicas de inferência. Nossa contribuição está em uma inferência mais precisa que vai além da classificação

[8]NIST Monitor, https://rpki-monitor.antd.nist.gov

binária, onde as inferências se limitam à implantação ou não implantação de ROV, utilizada em todos os trabalhos anteriores. Como mostramos neste trabalho, a classificação binária é simplista e não considera implantações parciais de ROV.

Mais recentemente, [Li et al. 2023] propôs uma técnica para identificar o nível de proteção provido pelo RPKI para cada sistema autônomo na Internet, quantificada como a porcentagem de anúncios inválidos que um sistema autônomo utiliza. Apesar da técnica não identificar quais sistemas autônomos implantam ROV, a abordagem combina técnicas avançadas de sondagem no plano de controle (*spoofing* e IP ID *side-channels*), não dependendo de pontos de medição distribuídos, e provê cobertura global de todos os sistemas autônomos na Internet.

7. Conclusão

Neste trabalho apresentamos um novo algoritmo para inferência de políticas de segurança utilizando ROV na Internet. Nosso algoritmo combina diversos anúncios de rota para obter informações complementares e assim inferir com maior precisão não apenas *se* um sistema autônomo utiliza validação de rotas, mas também detalhes de *como* a utiliza. Mais precisamente, nosso algoritmo identifica se um sistema autônomo *ignora-ROA* (não utiliza ROV), se prefere rotas válidas mas tolera rotas inválidas caso nenhuma rota válida esteja disponível (*prefere-válida*), ou se descarta todas rotas inválidas. Em casos ambíguos, nosso algoritmo ajusta as inferências para restringir a política *descarta-inválida* utilizada por um sistema autônomo em função das informações disponíveis.

Nossa avaliação utilizando experimentos e medições na Internet mostra que, de fato, alguns sistemas autônomos na Internet utilizam a política *prefere-válida*, e que algoritmos mais precisos como o proposto são necessários para caracterização de políticas de segurança na Internet. Além disso, nossos resultados indicam um aumento da implantação de ROV por sistemas autônomos na Internet, um evento positivo que torna o roteamento interdomínio da Internet mais seguro.

Como trabalho futuro, pretendemos melhorar a cobertura dos sistemas autônomos na Internet. Para aumentar a diversidade de rotas e a quantidade de sistemas autônomos observáveis, pretendemos (i) contactar operadores de redes que provêm trânsito ao PEERING para obter permissão para realizar anúncios inválidos de um número maior de PoPs e (ii) utilizar comunidades BGP para engenharia de tráfego para controlar de forma precisa anúncios realizados através do Vultr. Por último, pretendemos utilizar medições ativas de traceroute para complementar as rotas observadas de coletores BGP.

Referências

[Anwar et al. 2015] Anwar, R., Niaz, H., Choffnes, D. R., Cunha, I., Gill, P., and Katz-Bassett, E. (2015). Investigating Interdomain Routing Policies in the Wild. In *Proc. ACM IMC*.

[Bush and Austein 2013] Bush, R. and Austein, R. (2013). The Resource Public Key Infrastructure (RPKI) to Router Protocol. RFC 6810, RFC Editor.

[Feldmann et al. 2004] Feldmann, A., Maennel, O., Mao, Z. M., Berger, A., and Maggs, B. (2004). Locating Internet Routing Instabilities. In *Proc. ACM SIGCOMM*.

[Fontugne et al. 2023] Fontugne, R., Phokeer, A., Pelsser, C., Vermeulen, K., and Bush, R. (2023). RPKI Time-of-Flight: Tracking Delays in the Management, Control, and Data Planes. In *Proc. PAM*.

[Gilad et al. 2017] Gilad, Y., Cohen, A., Herzberg, A., Schapira, M., and Shulman, H. (2017). Are We There Yet? On RPKI's Deployment and Security. In *Proc. ISOC NDSS*.

[Hlavacek et al. 2018] Hlavacek, T., Herzberg, A., Shulman, H., and Waidner, M. (2018). Practical Experience: Methodologies for Measuring Route Origin Validation. In *IEEE International Conf. on Dependable Systems and Networks*.

[Hlavacek et al. 2022] Hlavacek, T., Jeitner, P., Mirdita, D., Shulman, H., and Waidner, M. (2022). Behind the Scenes of RPKI. In *Proc. ACM SIGSAC Conf. on Computer and Communications Security*.

[Iamartino et al. 2015] Iamartino, D., Pelsser, C., and Bush, R. (2015). Measuring BGP Route Origin Registration and Validation. In *Proc. PAM*.

[Li et al. 2023] Li, W., Lin, Z., Ashiq, M. I., Aben, E., Fontugne, R., Phokeer, A., and Chung, T. (2023). RoVista: Measuring and Analyzing the Route Origin Validation (ROV) in RPKI. In *Proc. ACM IMC*.

[Luckie et al. 2013] Luckie, M., Huffaker, B., Claffy, K., Dhamdhere, A., and Giotsas, V. (2013). AS Relationships, Customer Cones, and Validation. In *Proc. ACM IMC*.

[Marcos et al. 2020] Marcos, P., Prehn, L., Leal, L., Dainotti, A., Feldmann, A., and Barcellos, M. (2020). AS-Path Prepending: There is no Rose Without a Thorn. In *Proc. ACM IMC*.

[Quoitin et al. 2003] Quoitin, B., Pelsser, C., Swinnen, L., Bonaventure, O., and Uhlig, S. (2003). Interdomain Traffic Engineering with BGP. *IEEE Communications Magazine*, 41(5):122–128.

[Reuter et al. 2018] Reuter, A., Bush, R., Cunha, I., Katz-Bassett, E., Schmidt, T. C., and Wahlisch, M. (2018). Towards a Rigorous Methodology for Measuring Adoption of RPKI Route Validation and Filtering. *SIGCOMM Comput. Commun. Rev.*, 48(1):19–27.

[Rodday et al. 2021] Rodday, N., Cunha, I., Bush, R., Katz-Bassett, E., Rodosek, G. D., Schmidt, T. C., and Wahlisch, M. (2021). Revisiting RPKI Route Origin Validation on the Data Plane. In *Proc. PAM*.

[Schlinker et al. 2019] Schlinker, B., Arnold, T., Cunha, I., and Katz-Bassett, E. (2019). PEERING: Virtualizing BGP at the Edge for Research. In *Proc. ACM CoNEXT*.

[Testart et al. 2019] Testart, C., Richter, P., King, A., Dainotti, A., and Clark, D. (2019). Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. In *Proc. ACM IMC*.

[Testart et al. 2020] Testart, C., Richter, P., King, A., Dainotti, A., and Clark, D. (2020). To Filter or not to Filter: Measuring the Benefits of Registering in the RPKI Today. In *Proc. PAM*.

[Villamizar et al. 1998] Villamizar, C., Chandra, R., and Govindan, R. (1998). RFC 2439: BGP Route Flap Damping. http://www.ietf.org/rfc/rfc2439.txt.