AS-Path Prepending: there is no rose without a thorn

Pedro Marcos

Joint work with:

Lars Prehn

Lucas Leal

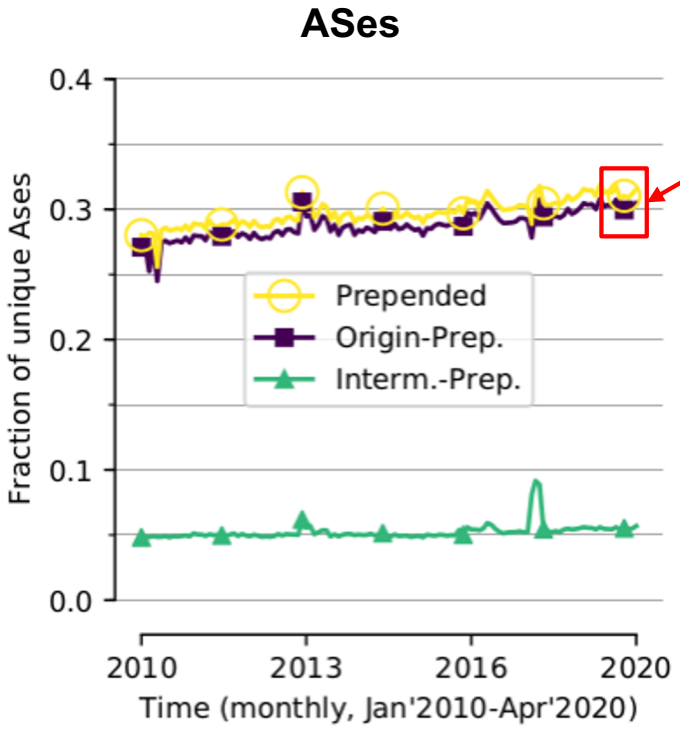
Alberto Dainotti

Anja Feldmann

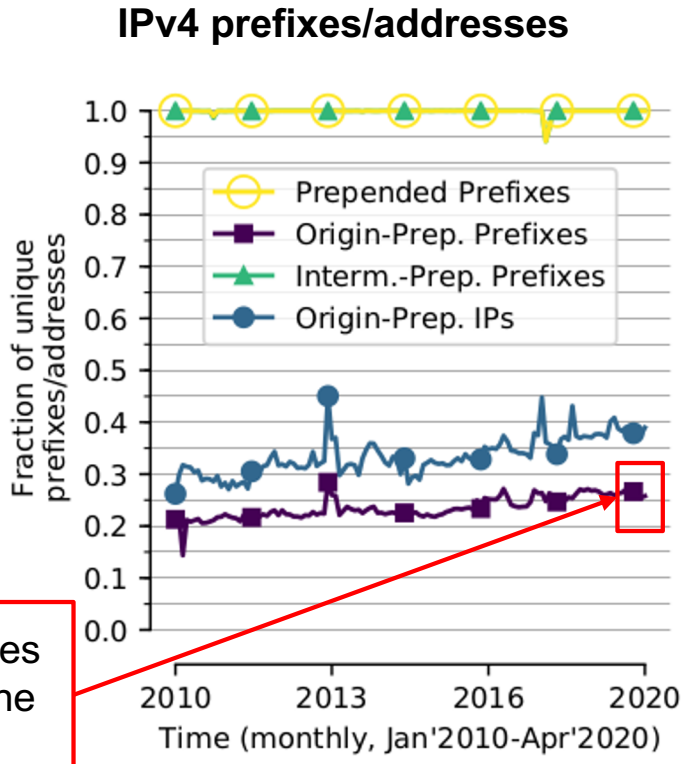
Marinho Barcellos

October, 2020

AS Path Prepending is a largely deployed technique for inbound traffic engineering…



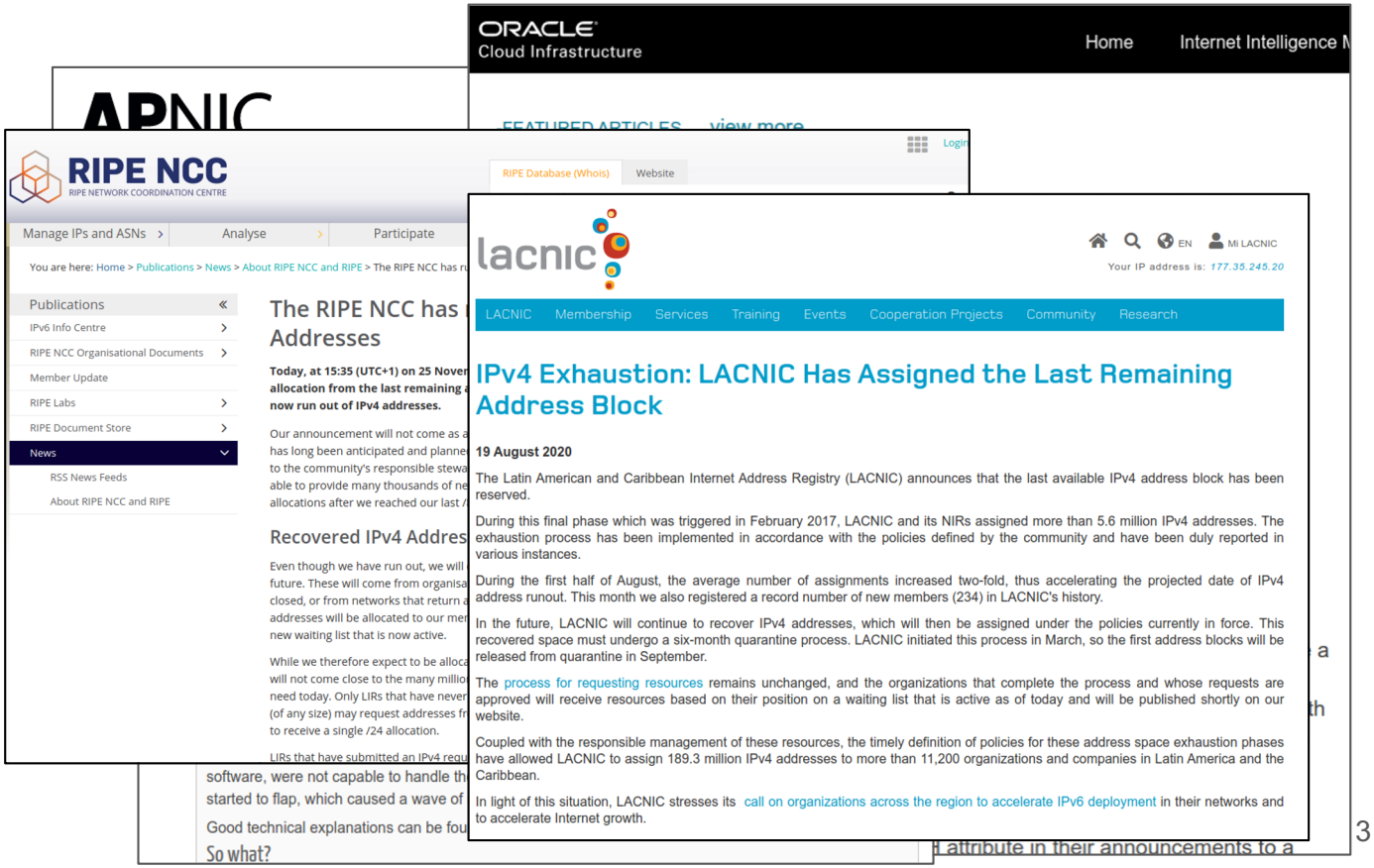
~30% of ASes use ASPP



~25% of IPv4 prefixes are prepended by the originator AS

… however, there has been some “controversy” regarding its utilization

“More specifics. That's the way to steer your traffic. Not prepeding! At all!” (RIPE 79)



Our goal is to contribute to an informed discussion without taking sides

Deployment

Effectiveness

Security Implications

ROUTE VIEWS 6447

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Isolario Project

PEERING
The BGP Testbed

Contributing to an informed discussion

Deployment

Effectiveness

Security Implications

ROUTE VIEWS 6447

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Isolario Project

PEERING
The BGP Testbed

How prefixes have been prepended?

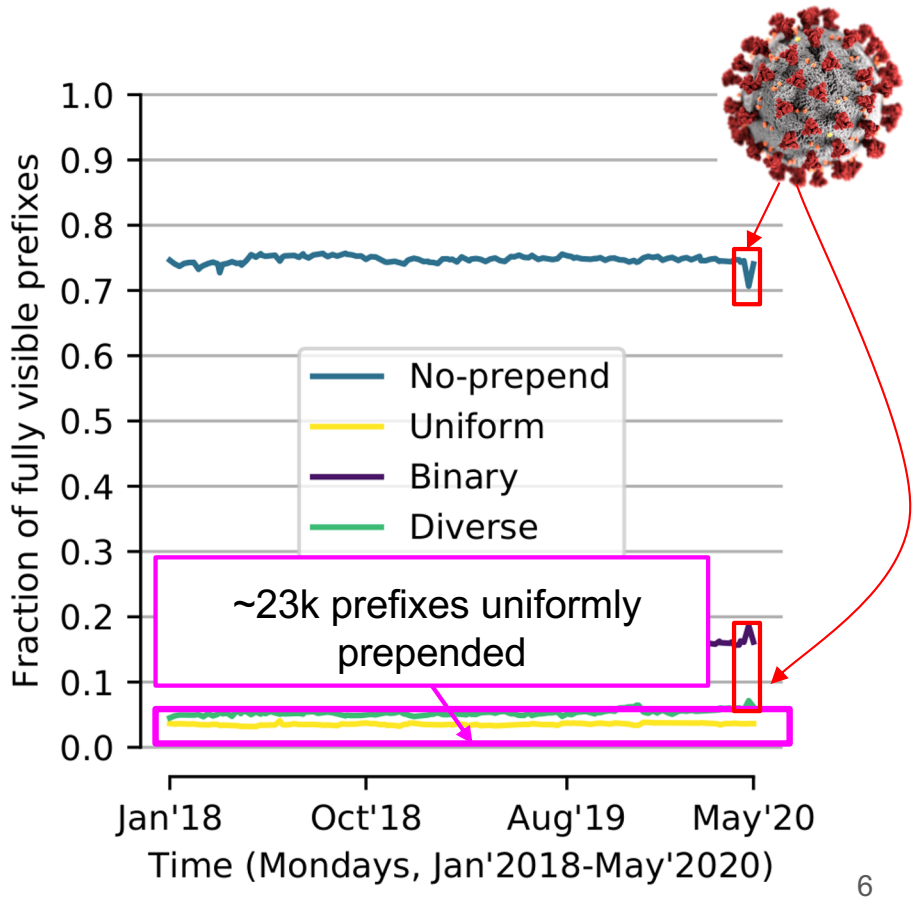
Prefix Policy Taxonomy

No. Prefix is not prepended

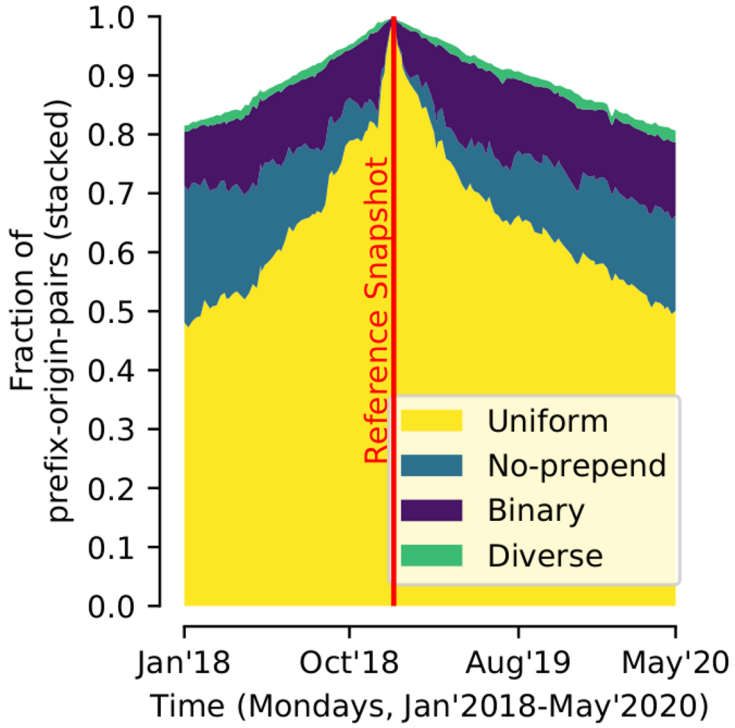
Uniform. Prefix is uniformly prepended to everyone

Binary. Prefix is announced with two different prepend lengths (e.g., 0, 2)

Diverse. Prefix is announced with at least three different prepend lengths (e.g., 1, 2, 5)



A deeper look into uniform prepending policies



Reasons for uniformly prepending a prefix

1) Loss of a neighbor
2) Lack of knowledge about BGP
3) Procrastination for stability
4) Good news travel fast, bad news slowly
5) Sibling artifacts
6) Other ASes ignoring prepending

For some prefixes, uniform prepending is a transitory state
~12k prefixes were uniformly prepended for at least one year

Contributing to an informed discussion

Deployment

Effectiveness

Security Implications

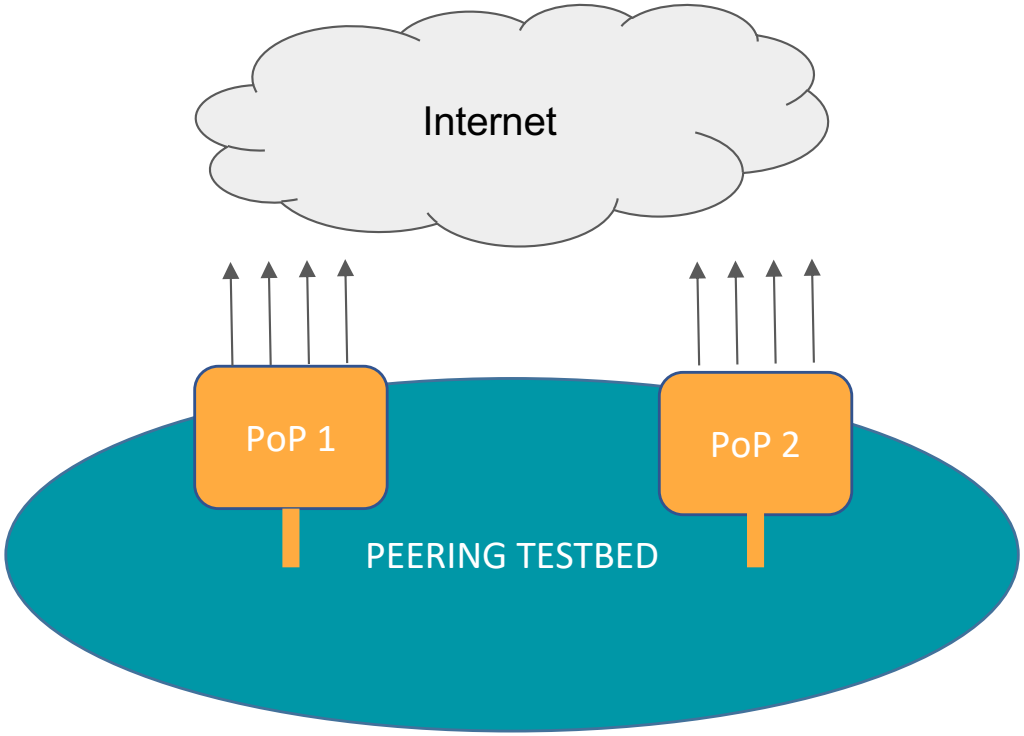
ROUTE VIEWS 6447

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Isolario Project

PEERING
The BGP Testbed

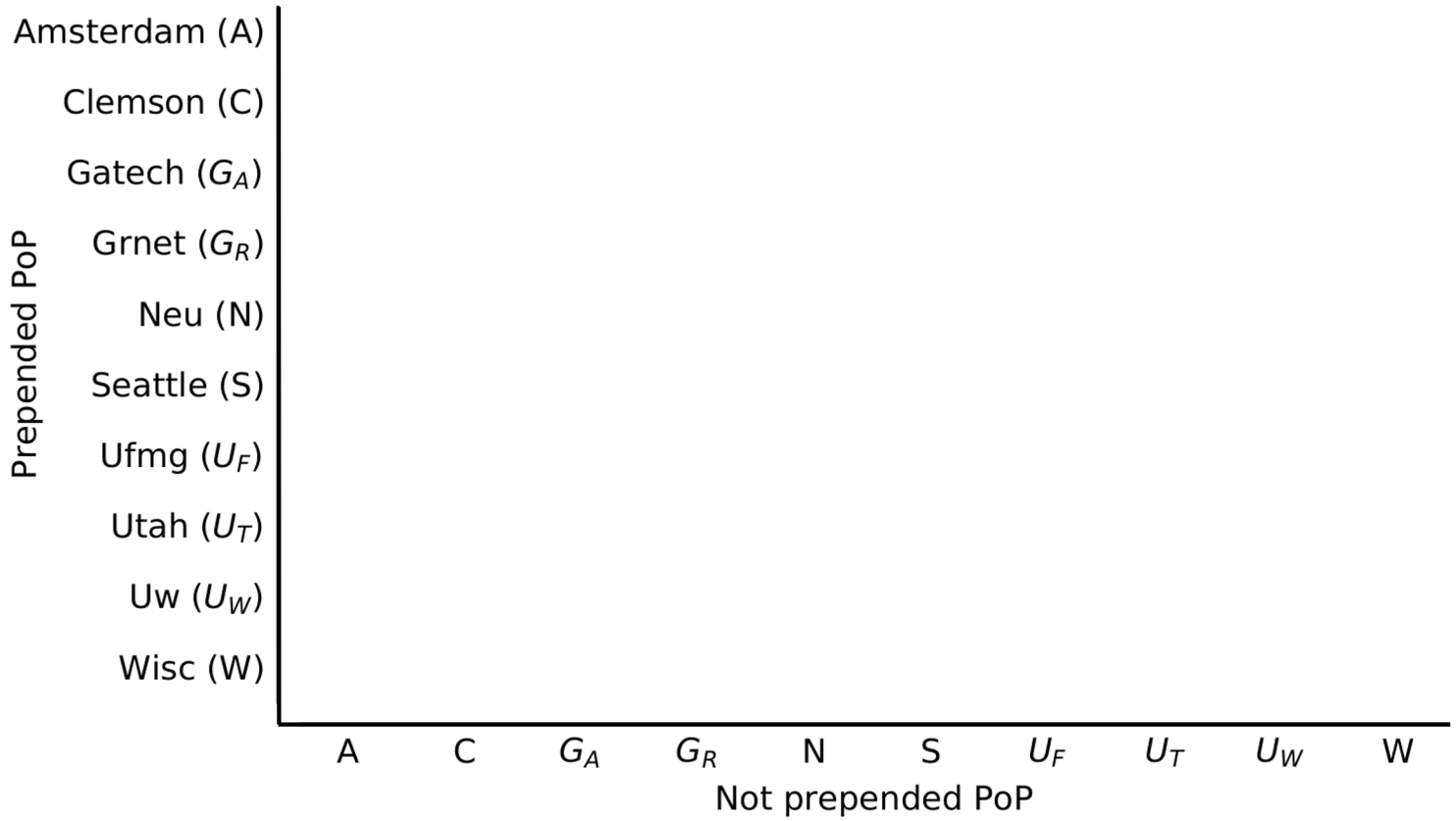
How effective is ASPP?



Methodology

1. For each pair (PoP1, PoP2), announce our prefix without prepended
2. Perform pings towards a set of targets (e.g., CDNs, tier-1s)
3. Measure in which PoP the response packets arrived
4. Prepend our prefix in one of the PoPs and repeat steps 2 and 3

Effectiveness for upstreams into different locations



Contributing to an informed discussion

Deployment

Effectiveness

Security Implications

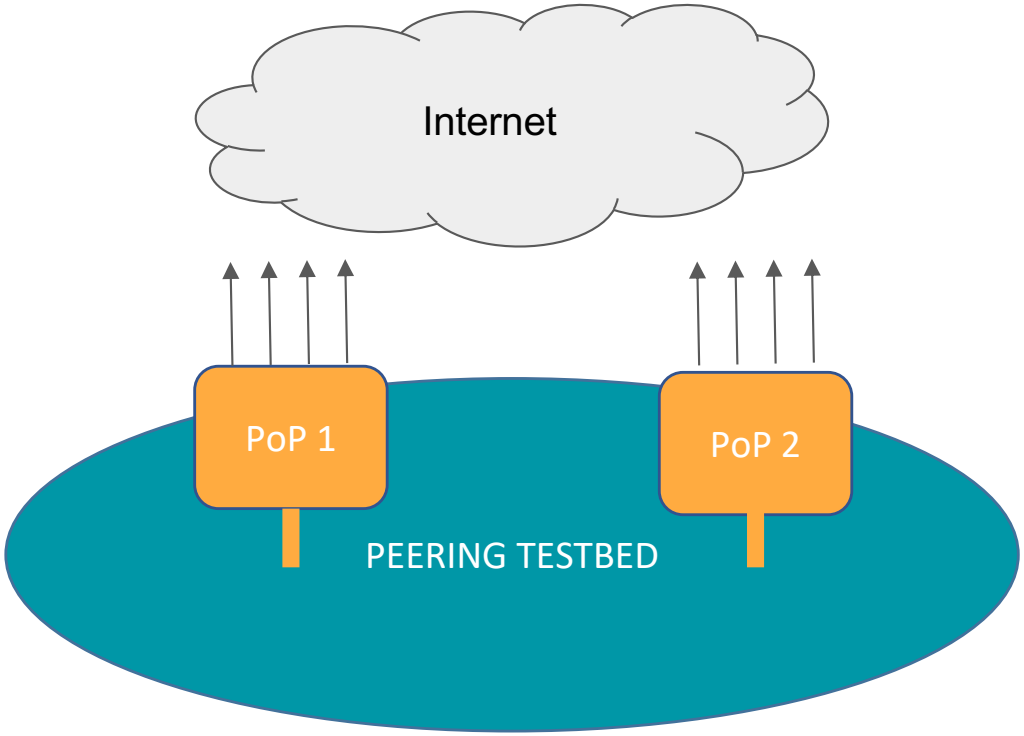
ROUTE VIEWS 6447

RIPE NCC
RIPE NETWORK COORDINATION CENTRE

Isolario Project

PEERING
The BGP Testbed

Measuring ASPP security implications



Methodology

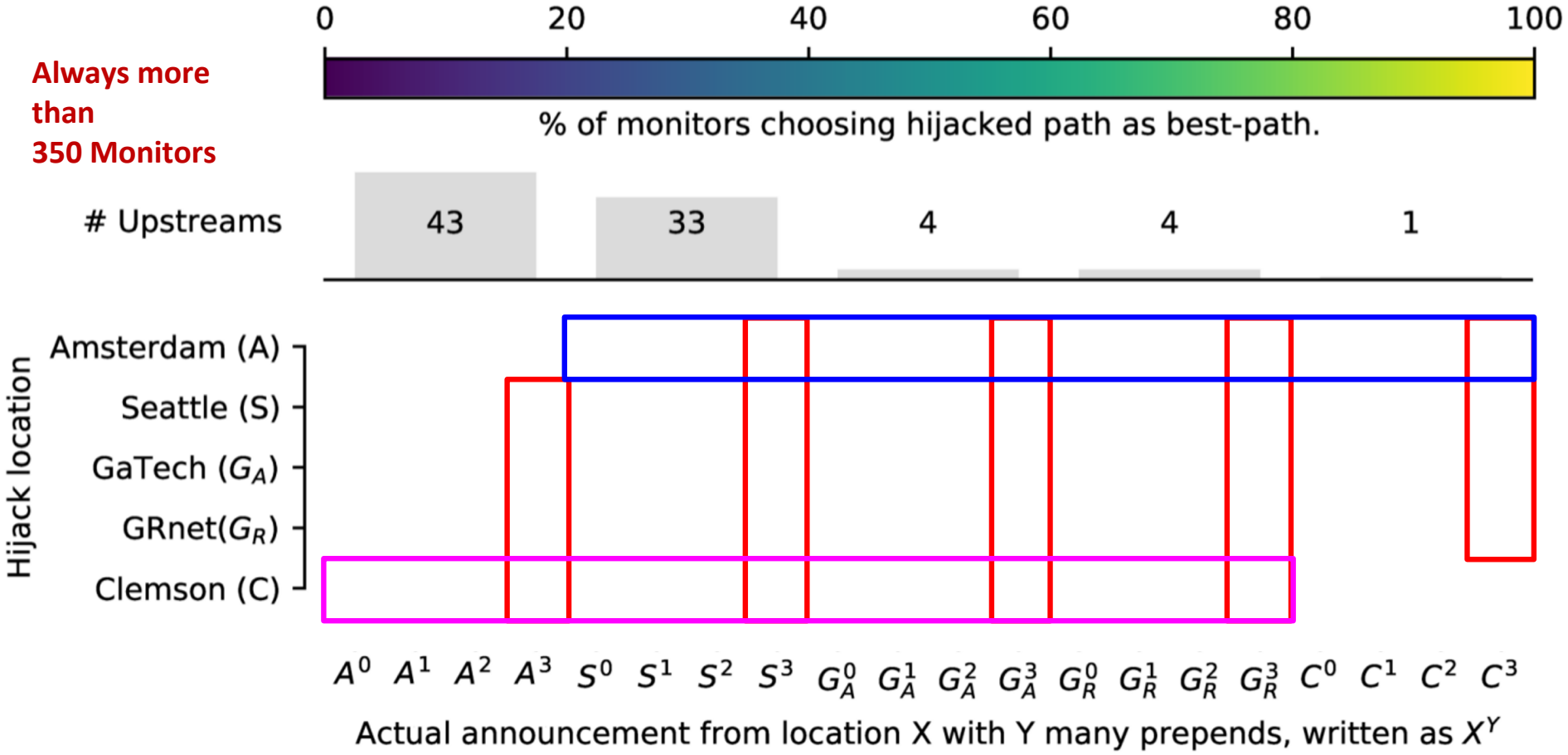
1. For each pair (PoP1, PoP2), announce our prefix with 0, 1, 2 or 3 prepends using one origin ASN

2. Wait 15 minutes and then announce the same prefix without prepend from a different POP using a different ASN as origin

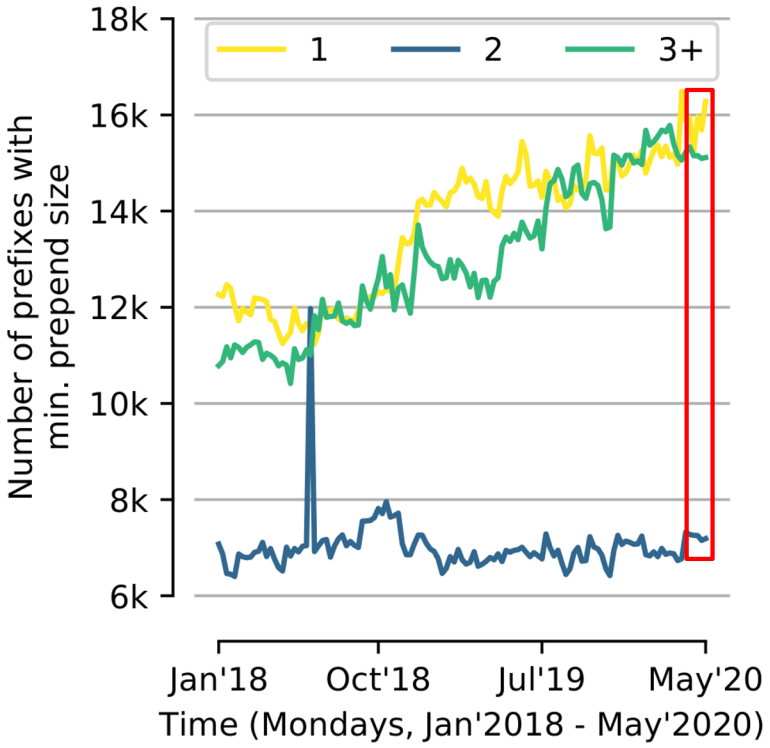
3. Measure the number of BGP monitor adopting the second announcement

Can we exploit ASPP?

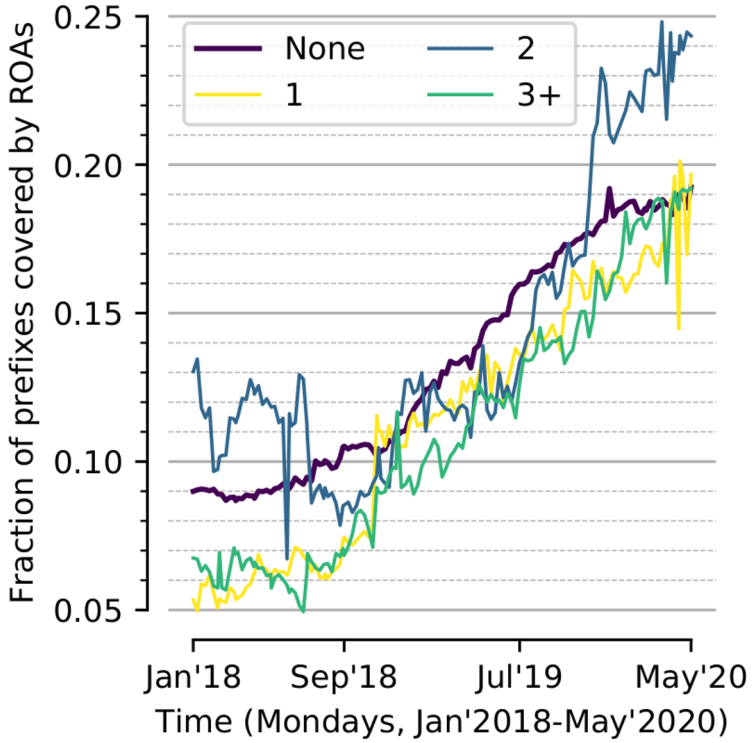
Always more than 350 Monitors



Considerations about ASPP and Security



38K prefixes being originated with at least one prepend



Prepended prefixes are not more protected by ROAs than non-prepended ones

Fir

AS-Path Prepending: there is no rose without a thorn

Pedro Marcos* — FURG — pbmarcos@furg.br
Lars Prehn* — MPI for Informatics — lprehn@mpi-inf.mpg.de
Lucas Leal — UFRGS — lsleal@inf.ufrgs.br
Alberto Dainotti — CAIDA, UC San Diego — alberto@caida.org
Anja Feldmann — MPI for Informatics — anja@mpi-inf.mpg.de
Marinho Barcellos — University of Waikato — marinho.barcellos@waikato.ac.nz

ABSTRACT

Inbound traffic engineering (ITE)—the process of announcing routes to, e.g., maximize revenue or minimize congestion—is an essential task for Autonomous Systems (ASes). AS Path Prepending (ASPP) is an easy to use and well-known ITE technique that routing manuals show as one of the first alternatives to influence other ASes' routing decisions. We observe that origin ASes currently prepend more than 25% of all IPv4 prefixes.

ASPP consists of inflating the BGP AS path. Since the length of the AS path is the second tie-breaker in the BGP best path selection, ASPP can steer traffic to other routes. Despite being simple and easy to use, the appreciation of ASPP among operators and researchers is diverse. Some have questioned its need, effectiveness, and predictability, as well as voiced security concerns. Motivated by these mixed views, we revisit ASPP. Our longitudinal study shows that ASes widely deploy ASPP, and its utilization has slightly increased despite public statements against it. We surprisingly spot roughly 6k ASes originating at least one prefix with prepends that achieve no ITE goal. With active measurements, we show that ASPP effectiveness as an ITE tool depends on the AS location and the number of available upstreams; that ASPP security implications are practical; identify that more than 18% of the prepended prefixes contain unnecessary prepends that achieve no apparent goal other than amplifying existing routing security risks. We validate our findings in interviews with 20 network operators.

CCS CONCEPTS

• **Networks → Network measurement**.

ACM Reference Format:

Pedro Marcos, Lars Prehn, Lucas Leal, Alberto Dainotti, Anja Feldmann, and Marinho Barcellos. 2020. AS-Path Prepending: there is no rose without a thorn. In *ACM Internet Measurement Conference (IMC '20), October 27–29, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3419394.3423642

*Both authors have contributed equally to the paper.

IMC '20, October 27–29, 2020, Virtual Event, USA

ACM ISBN 978-1-4503-8138-3/20/10…$15.00
https://doi.org/10.1145/3419394.3423642

1 INTRODUCTION

Many Internet Autonomous Systems (ASes) receive significantly more traffic than they send. They often use inbound traffic engineering (ITE) to influence the link through which they receive traffic based on economic considerations (e.g., transit cost) or operational demands (e.g., latency, packet loss, capacity). ITE has become even more important, as there are more options for inter-AS connectivity due to, e.g., IXPs (Internet eXchange Points), PNIs (Private Network Interconnects), and an overall increase of peering [9, 58, 71, 74, 75]. Border Gateway Protocol (BGP)-enabled ITE techniques include AS-Path Prepending (ASPP) [15, 22, 76], selective or more-specific prefix announcements [27], BGP communities [23, 63], or Multi Exit Discriminator (MED) values [25, 41].

In this paper, we focus on understanding ASPP deployment and the potential issues associated with it. ASPP is a straightforward, easy-to-use technique that is often mentioned among the first ITE techniques by router vendors [19, 21, 26, 35, 43]. It is a technique where an AS artificially inflates the BGP AS path by inserting (subsequent) duplicate entries of its ASN. Since the length of an AS path is the second most important tie-breaker in BGP best path selection, ASPP may steer traffic from one route to another. However, its effect depends on route propagation and the routing decisions made by other ASes. Despite (or because of) its simplicity and its inherent limitations, the appreciation of ASPP among operators and researchers is mixed. On the one hand, ASPP—unlike other ITE techniques—does not need any support from other ASes, nor deaggregatable prefixes. On the other hand, its need, effectiveness, and predictability have been questioned [37, 50, 65]. In addition, there have been concerns about the extent to which ASPP can amplify existing routing insecurities [38, 39, 64], and reports of improper ASPP configurations triggering bugs in router software [79, 80].

Motivated by the mixed views about the ASPP method, we investigate the current use of ASPP and find that more than 30% of ASes use it. Thus, to contribute to an informed discussion, we address three fundamental questions:

(i) **How do ASes use prepending?** To put effectiveness and risk into context, we first identify and characterize the *policies* ASes apply (i.e., the number of prepends used for each prefix) when using ASPP. Even when using data from all route collectors over the last decade, limited route visibility [16, 29, 47] poses a significant challenge. We deal with it by conducting interviews with more than 20 operators and by cross-checking our results with private data sources from large Internet players.

(ii) **How effective is prepending?** Among both operators and academics, the opinion on whether ASPP is effective as an ITE

Questions?

Pedro Marcos - pbmarcos@furg.br
Lars Prehn - lprehn@mpi-inf.mpg.de

…tiveness

…lependent for …eams

…with multiple …s

Security Implications

Prepending 3+ times is a risk

38k prefixes with possibly unnecessary prepends

Tak… …unity to review their prepending policies, …and using small prepend sizes for ITE