Understanding how does AS-PATH prepending can compromise the security of Internet routing

Pedro Marcos[1] [2], Marinho Barcellos[1]

{pbmarcos, marinho}@inf.ufrgs.br

[1]Informatics Institute - Federal University of Rio Grande do Sul - UFRGS, Brazil

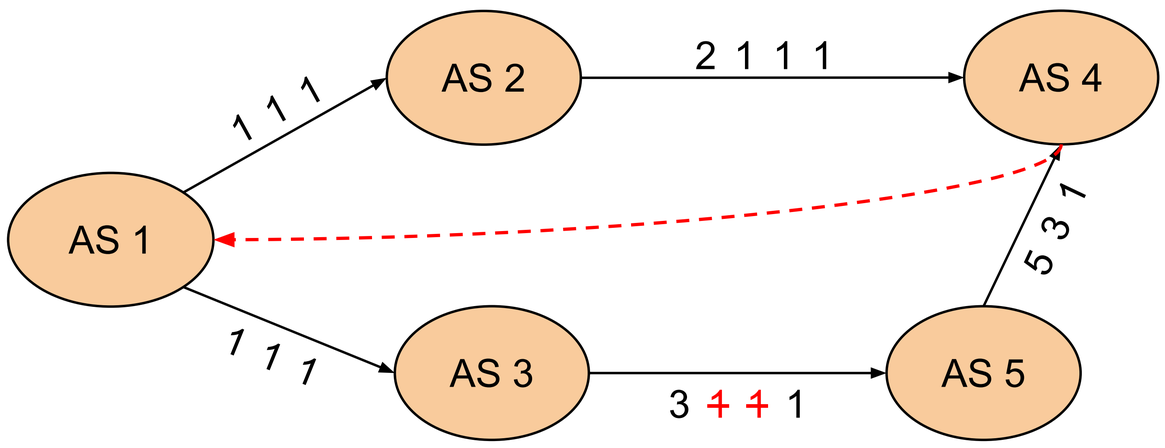
[2]Center for Computational Science - Federal University of Rio Grande - FURG, Brazil

Motivation and Problem

AS-PATH Prepending (ASPP) is commonly used to perform traffic engineering by **artificially inflating path length**

While intended to enhance traffic delivery, ASPP can increase the **risk of prefix hijacking** attacks such as the one reported by Cloudflare [1]

RPKI is not suitable for preventing such types of attacks while **BGPSec** is not widely deployed due to its requirements

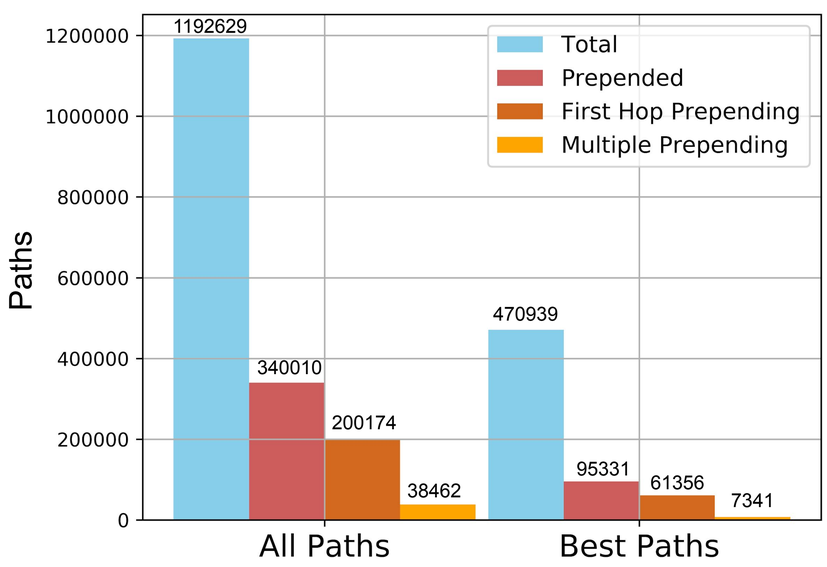


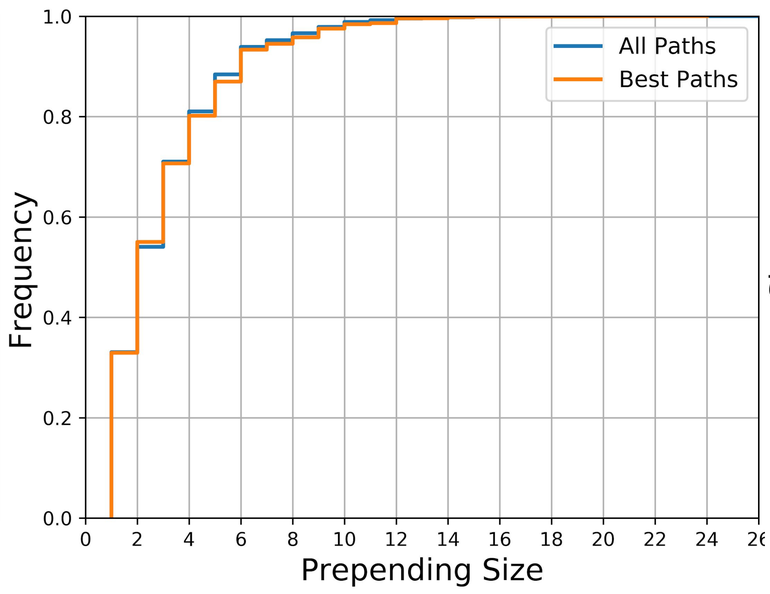
Previous work investigated hijacking likelihood related to **topology aspects** [2], and proposed algorithms to **detect hijackings** due to ASPP [3]

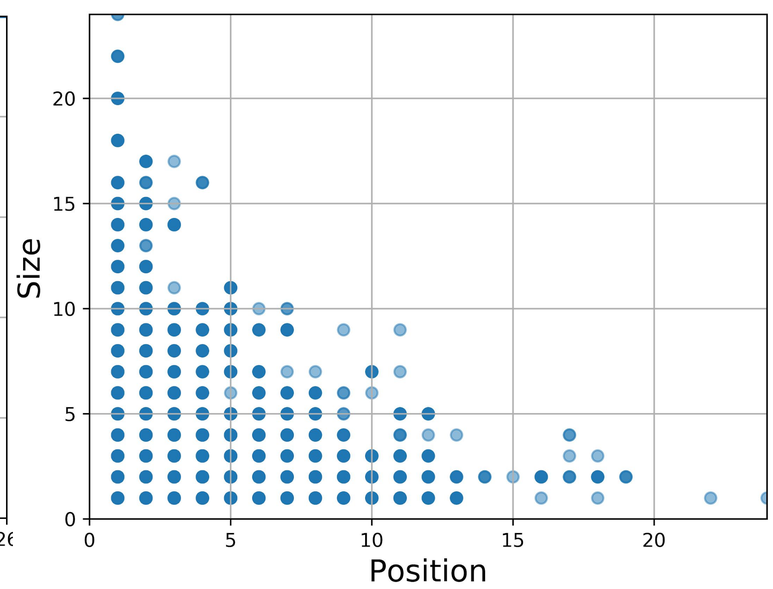
Research Goals

1. **Understand** how network operators are using ASPP and its evolution over time
2. Identify **routing vulnerabilities** caused by the use of ASPP on today's Internet
3. Propose a **methodology** to allow operators to make **informed decisions** when using ASPP
4. Define a **set of best practices** to be followed by network operators when using ASPP

Preliminary Analysis of ASPP Utilization







PCH AMS Route Collector - IPv4 Table - January 15th 2019

Summary

ASPP is present in approximately **one-third of the analyzed paths**

There are **paths where multiple ASes perform prepending**, which contributes to increasing the prefix hijacking likelihood

Informed decisions can help operators to **reduce the vulnerabilities**

References

[1] T. Strickx. "Technical Debt: an Anycast Story", In RIPE 77, 2018

[2] H. Ballani, P. Francis, and X. Zhang. "A study of prefix hijacking and interception in the internet", In ACM SIGCOMM, 2007

[3] Y. Zhang and M. Pourzandi, "Studying Impacts of Prefix Interception Attack by Exploring BGP AS-PATH Prepending", In IEEE ICDCS, 2012

UFRGS UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

INSTITUTO DE INFORMÁTICA UFRGS

FURG

C3 centro de ciências computacionais

PAM 2019