Identifying Legitimate Route Changes

We identify legitimate route changes via a heuristic rule derived from the multi-homing settings [1], which is a common route engineering practice. We label an origin change as legitimate if it satisfies two conditions: (i) Two different origin ASes (*i.e.,* on the changed and the original routing paths, respectively) belong to the same organization; (ii) There is no duplicate AS numbers in its routing paths. The first condition ensures the legitimacy of this route change since the actual ownership of the corresponding prefix is not changed, and the second one filters out the potential noises caused by routing paths manipulations, *e.g.,* AS prepending. Note that we use the CAIDA AS organization dataset [2] to obtain the organization name of each AS. These rules can not identify all legitimate route changes in the Internet. We only utilize them to find out changes with high confidence.

References

[1] X. Zhao, D. Pei, L. Wang, D. Massey, A. Mankin, S. F. Wu, and L. Zhang, "An analysis of bgp multiple origin as (moas) conflicts," in *SIGCOMM WS*, 2001, pp. 31–35.

[2] CAIDA. AS Organizations Dataset. Accessed Dec. 10, 2021. [Online]. Available: https://www.caida.org/catalog/datasets/as-organizations/