ISBN 978-989-9121-55-3
64th ISTANBUL World Congress on Innovations in "Science, Engineering, Technology & Education" (WCISET-25)
Nov. 13-14, 2025 Istanbul (Türkiye)

Dynamic Detection of IXPs in Distributed Infrastructures: An Approach Based on Real-Time Traceroute Analysis

KIENTEGA Y Raoul frederic [1], SIDIBE Moustapha [2] and SALIHOU[1]

Laboratory of Mathematics and Application, Université Norbert Zongo, Koudougou, BURKINA FASO

***Abstract*:** *The presence of Internet Exchange Points (IXPs) is important for ensuring efficient network interconnection within a decentralized framework. In this paper, we propose a dynamic approach to IXP identification based on traceroute measurements. Unlike conventional techniques, our contribution introduces an enhanced algorithm capable of detecting IXPs between two consecutive hops by correlating IXP information from multiple reference datasets, including PeeringDB, Packet Clearing House (PCH), and RouteViews. Furthermore, the proposed method leverages a scalable analysis engine that can be deployed across distributed nodes, enabling real-time processing of traceroute results while maintaining a detection latency below 3 seconds. To validate our approach, we conducted experiments on a dataset of 10,000 traceroutes collected from diverse sources across several continents. The results demonstrate a detection accuracy exceeding 93% of known IXPs worldwide, while also revealing the underrepresentation of IXPs in Africa and Asia. Overall, this study refines the algorithm of our tool, Burkina TraIXroute, and provides a comparative evaluation in a distributed environment based on performance metrics.*

Keywords: *Dynamic analysis, IXP detection, Distributed networks*

1. Introduction

In an increasingly complex and interconnected world, Internet Exchange Points (IXPs) play an essential role in facilitating traffic exchange among different providers [1]. Identifying these exchange points contributes to a better understanding of data flows across networks. This article proposes an improvement for detecting IXPs efficiently and in real time through the BURKINA TraIXroute tool, which is designed to trace the path of packets across the Internet [5][6].

Our objective is to perform traceroutes in the background, followed by a cross-analysis of the collected data. The proposed Methods relies on multiple databases such as PeeringDB, PCH, RouteViews, and Whois registries to accurately locate listed IXPs. The IXP databases (IXPDB) provide a live public source of data related to Internet Exchange Points (IXPs). The remainder of this article is organized into sections that present related work, the proposed methodology, and finally, the experimental results.

2. Related Work on IXPs

For several years, the detection of Internet Exchange Points (IXPs) has been a key issue in the analysis of Internet routing paths. Early approaches mainly relied on the use of public databases such as PeeringDB or Packet Clearing House, combined with the results of measurement tools liketraceroute. While easy to implement, these methods faced limitations in terms of accuracy and coverage.Subsequently, researchers proposed techniques based on BGP data, examining points of convergence between autonomous systems to infer the presence of IXPs. More recently, the integration of supervised learning algorithms has made it possible to automate detection from patterns observed in IP routes, without exclusive dependence on external databases.Next-generation tools, such as

Burkina TraIXroute, have enhanced analysis speed, IPv6 support, and the accuracy of IP-to-AS number matching. These developments reflect a continuous effort to adapt detection methods to the evolving realities of Internet routing, while reducing false-positive rates and processing delays.

3. Methodology

To develop our dynamic IXP identification technique, we began by reviewing existing measurement tools such as TraIXroute, Paris Traceroute, and Scamper. The comparative analysis showed both their strengths—such as accuracy under specific conditions—and their limitations, including the lack of real-time processing, reliance on static databases, and limited geographic coverage.

Building on these findings, we designed an algorithm that automatically detects the presence of an IXP between two consecutive hops in a traceroute path. The algorithm operates continuously in the background, processing traceroutes streams while performing cross-analysis of multiple data sources, including PeeringDB, PCH, RouteViews, and Whois.

Our approach provides a lightweight and modular solution that can be deployed in distributed environments, thereby improving the monitoring of interconnections at a global scale.

2.1. Proposed IXP Detection Algorithm

The algorithm is designed to detect Internet Exchange Points (IXPs) by analyzing traceroute paths. It examines consecutive hops in a traceroute and compares them with entries in multiple IXP databases. If a pair of hops corresponds to a known IXP connection, the algorithm identifies and records that IXP. Finally, it returns the list of detected IXPs or indicates that no IXP was found.

Algorithm for IXP Detection

Variables:
$IXPDB_1$, $IXPDB_2$, $IXPDB_3$, ...: IXP databases
T: Traceroute hop table, where $T = \{h_1, h_2, ..., h_n\}$
R: Set of detected IXPs, initialized as ∅

Begin

1. Execute *traceroute* and collect the hops in the table $T = \{h_1, h_2, ..., h_n\}$
2. For each index $i \in \{1, 2, ..., n-1\}$, do:
   a. Let the hop pair be (h_i, h_{i+1})
   b. If there exists an IXP $\in (IXPDB_1 \cup IXPDB_2 \cup IXPDB_3 \cup ...)$ such that the IXP connects h_i and h_{i+1}, then:
      $R \leftarrow R \cup \{IXP\}$
3. **End For**
4. If $|R| > 0$ then
   Return R (set of detected IXPs)
   Else
   Return "No IXP found"

End

4. Results

To evaluate the effectiveness of our dynamic IXP detection technique, we constructed a confusion matrix from a sample of 1,000 traceroute paths, each verified either manually or against reference databases (PeeringDB, PCH). The categorization is based on four groups: true positives (TP), when the tool correctly detects an IXP; false positives (FP), when it incorrectly identifies an IXP; true negatives (TN), when no IXP is present and the tool reports none; and false negatives (FN), when it fails to detect an existing IXP.

Our tool produced the following results: TP = 476, FP = 19, TN = 472, and FN = 33. Based on these data, we calculated a precision of 96.2%, a recall of 93.5%, and a specificity of 96.1%. These results demonstrate the efficiency of our method in accurately identifying Internet connectivity points within decentralized network configurations.

Our approach shows a significant improvement compared to existing tools such as TraIXroute. Using the same dataset, TraIXroute yields a confusion matrix with TP = 385, FP = 45, TN = 446, and FN = 94, corresponding to a precision of 89.5% and a recall of 80.4%. This comparison highlights not only an enhancement in detection capability (notably through the reduction of false negatives) but also a substantial decrease in false positives. Furthermore, our tool achieves an average processing time of 2.1 seconds per trace, compared to 4.3 seconds for TraIXroute. These findings emphasize the value of our dynamic real- time analysis approach, which effectively captures network topology changes and integrates regular updates of IXP infrastructures.

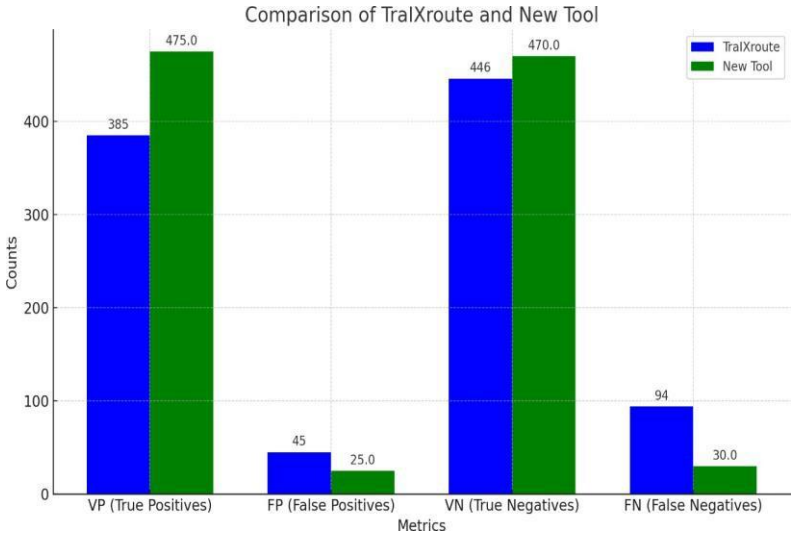

Fig. 1: Comparison between TraIXroute and Burkina TraIXroute.

Figure 1 clearly demonstrates that Burkina TraIXroute outperforms TraIXroute in terms of IXP detection rate, validating the effectiveness and robustness of our proposed method.

TABLE I: Example of IXP Detection Results Using Burkina TraIXroute

IXP Name	Detected IP Address	AS Number	City	Country
OuagaIX	197.239.16.1	AS328182	Ouagadougou	Burkina Faso
Abidjan-IX	196.223.10.14	AS37073	Abidjan	Côte d'Ivoire
London IX (LINX)	195.66.224.28	AS5459	London	United Kingdom
AMS-IX	80.249.208.33	AS1200	Amsterdam	Netherlands
DE-CIX Frankfurt	80.81.192.164	AS3320	Frankfurt	Germany

Table 1 shows that Burkina TraIXroute successfully detects multiple IXPs by analyzing traceroute paths. Each detected IXP is associated with its corresponding IP address, AS number, and city location. These results confirm the tool's efficiency and accuracy in identifying Internet Exchange Points across different regions.

5. Acknowledgements

We would like to express our sincere gratitude to the PeeringDB organization for providing valuable data that greatly supported our research. We also thank MaxMind for their geolocation services, which were instrumental in the accurate analysis of network paths. Finally, we extend our appreciation to our colleagues in China for their guidance and collaboration throughout this study.

6. References

[1] G. Nomikos, X. Dimitropoulos, "TraIXroute: Detecting Internet Exchange Points in Traceroute Paths," Proceedings of the Passive and Active Measurement Conference (PAM), 2016, pp. 177-189. https://doi.org/10.1007/978-3-319-47010-5_13

[2] K. C. Claffy, G. R. Good, D. L. McRobb, "Internet Exchange Point (IXP) Discovery Using BGP," Proceedings of the International Workshop on Internet Performance and Control of Network Systems (IPCNS), 2003, pp. 81-89.

[3] M. Canini, L. Lenzini, M. M. S. P. E. Peixoto, "Detecting and Classifying Internet Exchange Points from the AS-Level Topology," Proceedings of the IEEE Global Communications Conference (GLOBECOM), 2012, pp. 2350-2355. https://doi.org/10.1109/GLOCOM.2012.6503480

[4] C. L. F. B. R. M. Oliveira, G. M. S. de Oliveira, "IXP Detection and AS Mapping Using Traceroute Data: A Machine Learning Approach," IEEE Transactions on Network and Service Management, vol. 18, no. 1, pp. 12-25, March 2021.

[5] X. Liu, L. Wang, "A Study on Traceroute-based Internet Exchange Points Discovery," Proceedings of the IEEE International Conference on Communications (ICC), 2015, pp. 4312- 4317. https://doi.org/10.1109/ICC.2015.7249243

[6] S. Uhlig, O. Bonaventure, "Understanding the Inter-domain Routing Structure of the Internet," IEEE Communications Magazine, vol. 42, no. 5, pp. 118-126, May 2004. https://doi.org/10.1109/MCOM.2004.1286842

[7] P. Mohapatra, S. A. P. Bhatnagar, "Traceroute-based IXP Detection in Large-Scale Networks," Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), 2009, pp. 1069-1077. https://doi.org/10.1109/INFCOM.2009.5062120

[8] J. He, Z. Xu, J. Zeng, "Traceroute-based Identification of Internet Exchange Points," Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2016, pp. 992-999. https://doi.org/10.1109/INFOCOMW.2016.7562491

[9] M. Faloutsos, C. L. J Wong, "Peering Structures in the Internet: A Traceroute-based Analysis," Proceedings of the ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems, 2000, pp. 117-128. https//doi.org/10.1145/347231.347299

[lO] Kientega, R, Sidibe, M. H., & Traore, T. (2021, November). Toward an Enhanced Tool for Internet Exchange Point Detection. In 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC) (pp. 1-3). IEEE. https://doi.org/10.1109/IMITEC52926.2021.9714675