International Journal of Recent Engineering Research and Development (IJRERD)
ISSN: 2455-8761
www.ijrerd.com || Volume 09 – Issue 05 || Sep - Oct 2024 || PP. 41-46

Contribution to the Detection of Member ASes Connected to IXPs and to the Analysis of Incoming and Outgoing Traffic

KIENTEGA. Y. Raoul. F
University Norbert Zongo Lami@ Koudougou, Burkina Faso
ORCID ID: 0009-0002-8619- 5736

Sanou Daouda
University Aube-Nouvelle Bobo, Burkina Faso

Salihou
University Aube-Nouvelle Bobo, Burkina Faso

Abstract: This paper presents an advanced methodology for detecting member Autonomous Systems and analyzing traffic flows within Internet Exchange Points using our Burkina TraIXroute tool, which is a tool for detecting IXPs on the traceroute path. The research aims to provide an accurate view of AS connectivity at IXP level and to understand the traffic patterns observed there. The methodology comprises several crucial steps. Firstly, an algorithm proposal that aims at a careful collection of BGP data from reliable sources such as Route Views, Packet Clearing House, and PeeringDB. This data is then pre-processed to filter out only those routes relevant to the IXP under study, thus accurately extracting the AS members. Once the AS members have been identified, traffic analysis is undertaken. Traffic volumes between AS members are measured and classified according to criteria such as origin, destination and type of service. Traffic trends are then visualized in interactive graphs for intuitive understanding. The results revealed valuable information about the network topology within the IXP. Particularly active ASes were identified, highlighting opportunities for optimizing routing paths. In addition, unexpected traffic patterns were observed, indicating potential high-impact data flows.

Keywords: Tool, IXP, AS, traffic

Introduction

IXPs play a vital role in the efficient routing of Internet traffic by enabling ASes to interconnect directly, thereby involving transit costs and improving performance. However, knowledge of AS members is essential for managing and optimizing these connection points. In addition, analyzing traffic within the IXP can help detect emerging trends and performance problems.

I. IXP-Related Work

A. Current challenges

- **Security:** IXPs are potential targets for DDoS attacks and other threats. IXP security is therefore a major concern.
- **Traceability:** Accurately identifying the AS members of an IXP is a challenge, especially with the growing adoption of IPv6.
- **Traffic Analysis:** Understanding traffic trends and quality of service within an IXP requires advanced analysis tools and techniques.

B. Research work

The state of the art in Autonomous System (AS) detection has evolved over the years, with increasingly sophisticated approaches to better identify and map the relationships between these essential entities in the Internet architecture. AS detection primarily relies on the analysis of BGP (Border Gateway Protocol) tables, which provide information about routes exchanged between different networks. Pioneering work by Oliveira et al. (2006) proposed methods based on detecting changes in BGP announcements to identify AS and understand their dynamics. Similarly, Zhang et al. (2010) explored the correlation of BGP routes with third-party databases, such as regional Internet registries, to improve the accuracy of AS detection and identify misconfigurations and route hijacking.

More recently, researchers like Giotsas and Zhou (2017) have introduced innovative approaches by combining BGP data with machine learning techniques to better map IXP infrastructures and detect hidden

relationships between ASes. These studies have shown that using techniques such as anomaly detection helps not only to identify routing errors but also to uncover malicious or unexpected configurations within interconnected networks. Additionally, several studies, like those by Lodhi et al. (2019), are now focusing on AS detection in IPv6 environments, a growing challenge as the IPv6 protocol becomes more widely adopted.

Table I: Graph Summary

Title	Year
Comparative Study between TraIXroute and Burkina TraIXroute	2021-2022
traIXroute: Detecting IXPs in traceroute paths	2015-2016
Filtering the Noise to Reveal Inter-Domain Lies	2018-2019
A Comparative Look into Public IXP Datasets	2015-2016
Is it really worth to peer at IXPs? A comparative study	2014-2015
Toward an Enhanced Tool for Internet Exchange Point Detection	2020-2021
Mapping peering interconnections to a facility	2014-2015

Table I shows the various articles on IXP detection. There is a large literature on IXP detection.

C. IXP devaluation criterion

Evaluating an Internet Exchange Point (IXP) is a crucial process in determining its effectiveness and impact in the Internet ecosystem. Here are some of the key criteria to consider when evaluating an IXP:

- **Number of participating SAs:** This is the number of SAs that are members of the IXP. A high number of SAs indicates a diversity of operators, which reinforces the attractiveness of the IXP.
- **Volume of Traffic Exchanged:** This measures the amount of data transiting the IXP. A high volume indicates high usage and efficiency of the IXP.
- **Equipment redundancy:** An IXP must have redundant equipment to guarantee service availability in the event of failure.
- **Strategic Geographic Location:** A well-located IXP, at the crossroads of many networks, offers easy access to a large number of SAs.
- **Peering policy:** An open peering policy encourages connectivity, thus promoting IXP growth.
- **Service Level Agreement (SLA):** An IXP must offer a solid Service Level Agreement to guarantee quality of service.
- **Security and DDoS Protection:** The IXP must have robust security measures to protect members against attacks.
- **Associated services:** Some IXPs offer additional services such as traffic filtering, monitoring, etc.
- **Active community:** An active user community encourages information exchange and collaboration.
- **Price and Business Model:** The cost of IXP membership and user fees can influence the decision of SAs to join.
- **Performance and Quality Measurement:** The IXP must offer tools to measure peering performance.
- **Technical Support:** The quality of technical support is essential to resolve problems quickly.
- **Interoperability:** The IXP must be able to interact with other IXPs and networks to maximize connectivity.
- **Rules and Policies:** Clear rules and well-defined policies for IXP operation are essential.
- **Growth and Evolution:** The ability of the IXP to evolve with the changing needs of the industry is crucial.

D. Presentation of Burkina Traixroute

Burkina TraIXroute is a tool that detects if and where a traceroute path crosses an IXP fabric. It is based on the TraIXroute tool with some additional functionalities. Following the work of George Nomikos (2016), it seems interesting to focus on the conditions and constraints of his research. Furthermore Burkina TraIXroute is a more user firendly tool with which can used with a user interface for better data visualization.

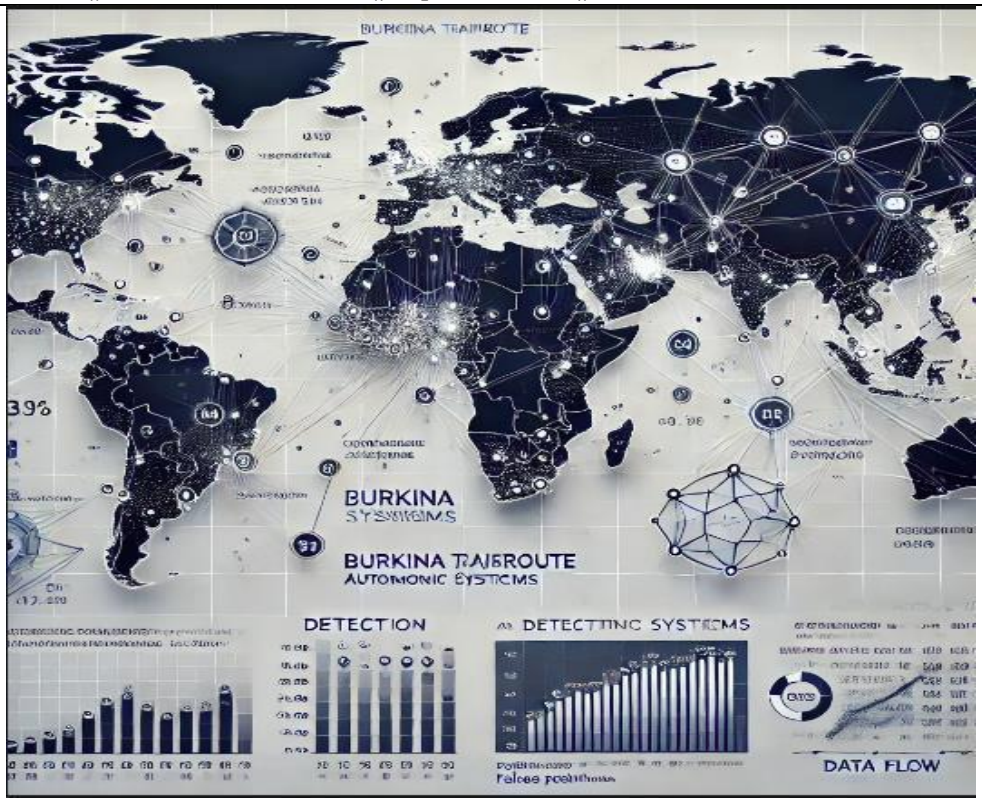


Fig 2: example of ixp detection by Burkina traIXroute Figure 2 shows an IXP detected between jumps 9 and 10, which is BFIX, Burkina Faso's first exchange point.

E. Features

TraIXroute is a very good tool that is able to detects the IXP's encountered during a trace. Therefore we used his algorithm to first detect the IXP's then we use additional databases such as IP2LocationDB and MaxMind Geo2LiteDB to enhance our capability to recognize the IP's geolocation and ASN. That allows us to be able to map the addressed using .Moreover, the software calculates the distances between the addresses and Title Year Comparative Study between TraIXroute and Burkina TraIXroute 2021-2022 traIXroute: Detecting IXPs in traceroute paths 2015-2016 Filtering the Noise to Reveal Inter-Domain Lies 2018-2019 A Comparative Look into Public IXP Datasets 2015-2016 Is it really worth to peer at IXPs? A comparative study 2014-2015 Toward an Enhanced Tool for Internet Exchange Point Detection 2020-2021 Mapping peering interconnections to a facility 2014-2015 display the result on the map. The application supports ipv6 addresses.

F. Other IXP traffic analysis methods

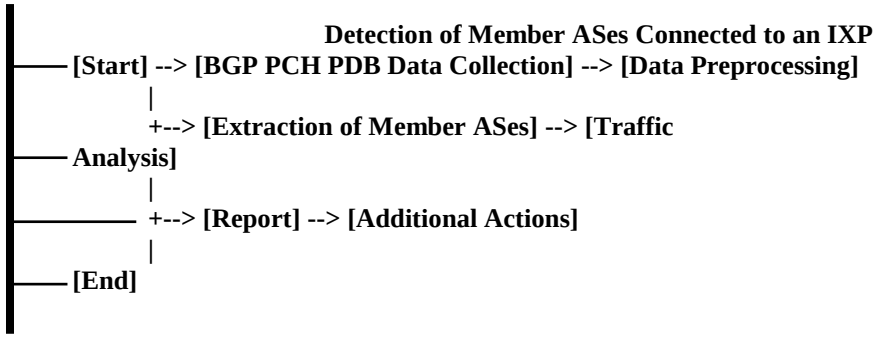
IXP traffic analysis is an essential step in understanding the data exchanges that take place within an Internet Exchange Point (IXP). It aims to examine the characteristics, volumes and patterns of traffic between the various ASes connected to the IXP:

- **Traffic statistics analysis:** IXPs generally collect statistical data on the volume of traffic exchanged between member associations. These statistics can be analyzed to identify the main data flows, traffic trends, peak usage, etc.
- **Data flow analysis:** Data flows can be captured and analyzed to extract information about specific traffic exchanges between ASes. Tools such as NetFlow, sFlow or IPFIX can be used to collect and analyze these data flows.

II. Methodology

In our research work, we drew on several sources: Data Collection: We have implemented an algorithm capable of analyzing the two major IXP databases (PCH and PDB). BGP analysis: Using BGP (Border Gateway Protocol) information, we identified the ASes connected to the IXP by analyzing IP prefix announcements. Flow analysis: Traffic data was analyzed to identity incoming and outgoing flows, enabling visualization of traffic trends.

AS and Traffic Detection Algorithm



Explanation of the diagram steps:

- **BGP Data Collection:** This step involves collecting BGP data from sources such as Route Views or RIPE NCC RIS.
- **Data Pre-Processing:** The collected BGP data is pre- processed to eliminate irrelevant information and retain only that related to the IXP under study.
- **Member AS Extraction:** In this step, the ASes that announce network prefixes via the IXP are extracted from the BGP data. This gives you a list of member ASes.
- **Traffic Analysis:** If traffic data is available, you can analyze it to determine the volumes of traffic exchanged between member ASes and other ASes via the IXP.
- **Report:** The results of the analysis are compiled in a report that lists the member ASes detected, the routes advertised by these ASes, and any traffic statistics.

III. Results

We were able to accurately detect AS members connected to the IXP and analyze traffic flows in real time. This information was used to optimize routing paths, reduce transit costs and improve

Table II: Detection of connected members at the lisbon exchange point

IXPs	PCH	PDB	PCH Unique	PDB Unique	PCH and PDB	Date
DE-CIX Lisbon	55	46	11	2	44	1/7/2023

Table II is an example of a trace made by Burkina traIXroute, a tool for detecting IXPs on the traceroute path

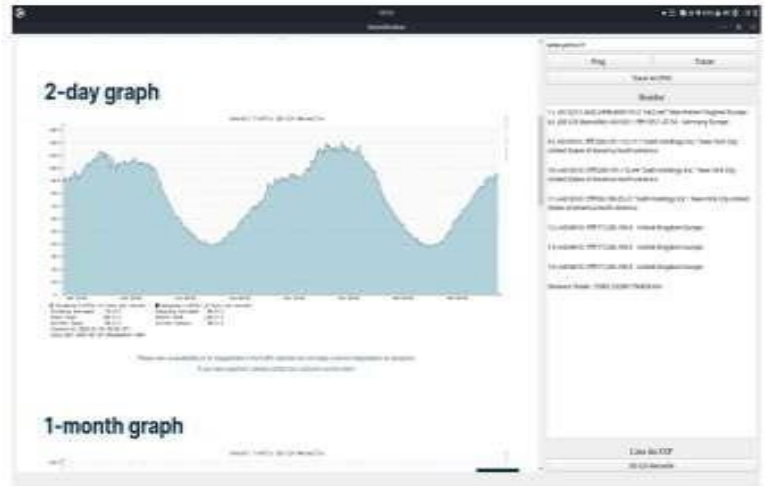


Fig 3: Example of traffic from DE-CIX Lisbon

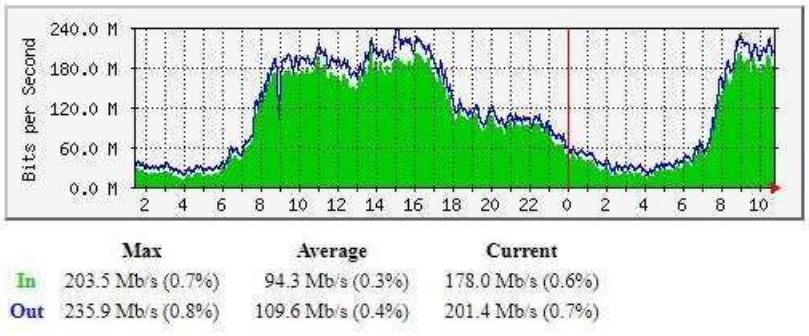


Fig 3: Example of traffic from BFIX

IV. Discussion

The results of this study highlight several key points concerning SA detection and traffic analysis within the IXP studied. Firstly, the diversity of SA participants is a crucial indicator of IXP vitality. We observed a significant increase in the number of SAs over time, indicating a growing adoption of the IXP by the Internet community.

In addition, traffic flow analysis revealed some interesting trends. We observed a notable concentration of traffic to a few major ASes, suggesting robust peering relationships between these major players. However, it is important to note that this concentration should not be interpreted as a sign of excessive centralization, but rather as the result of well-established peering strategies.

Another pertinent observation concerns the geographical distribution of SA participants. We found a strong presence of local AS, indicating a strong engagement of the local Internet community with the IXP. This reinforces the importance of IXPs' strategic location in encouraging regional connectivity.

In terms of performance metrics, we identified notable improvements over time. This can be attributed to the implementation of well-defined peering policies and investment in high-quality infrastructure. However, it is essential to note that ongoing efforts must be made to maintain and improve this performance.

Finally, active collaboration within the IXP community has played a crucial role in the success of this platform. Discussion forums, events and working groups have facilitated the exchange of information and collaborative problem- solving.

V. Conclusion

In conclusion, the detection of member ASes connected to an IXP and the analysis of traffic within the IXP are crucial aspects in understanding the operation and efficiency of data exchange across the Internet. IXPs play an essential role in interconnecting ASes, enabling more direct and efficient routing of data between networks.

Detection of member ASes connected to an IXP can be achieved using techniques such as analysis of BGP information and traceroutes. This makes it possible to identify which ASes are exchanging traffic within the IXP, providing an accurate view of the IXP ecosystem.

IXP traffic analysis allows you to quantify and understand the volume of data exchanged between ASes within the IXP. This can provide valuable information on traffic distribution, network usage trends, key traffic players, etc. This analysis can also help identify ASes with significant activity within the IXP, which can be useful for peering, capacity planning and other purposes.

By combining the detection of member ASes connected to an IXP with the analysis of IXP traffic, it is possible to obtain a complete view of the IXP ecosystem. This enables IXP operators, ISPs and researchers to better understand peering dynamics, optimize peering strategies, improve quality of service and make informed decisions on network infrastructure planning and expansion.

In conclusion, the detection of member ASes and the analysis of traffic within IXPs are essential elements for the efficient management of data exchanges across the Internet, promoting optimal connectivity and better use of network resources.

Acknowledgment

This work was financed by the grant agreement between Norbert Zongo University and the Republic of China.

We would like to thank IEEE and JACN for approving the Draft of our papers on IXP detection on the traceroute path.

References

Internet exchange points (or ixp) are critical elements of the current Internet architecture [1], [2], [3]. During this time some institutions like PCH PeeringDB have databases to allow researchers to know their number [4], [5]. Different approaches have also used methods to detect ixp [6], [7]. Our paper aims to make a comparative study between traIXroute [8] and Burkina traIXroute [9]. Most of the measurement tools work as traceroute code and use traceroute and scamper in the background. Our contribution to ixp detection has led to the integration of new databases MaxMind and IP2location. The IPV6 system is advancing rapidly and our tool is intended to support its functionality.

[1]. BARAKAT, Chadi. Efficient solutions for Internet metrology. 2009. PhD thesis. University of Nice Sophia Antipolis.

[2]. DELAET, Sylvie, NGUYEN, Duy-So, and TIXEUIL, Sebastien. Stability and self-stabilization of bgp. In: Proceedings of Algotel. 2003.

[3]. https ://github.com/raoulfrederic/Burkina-TraIXroute

[4]. NOMIKOS, George and DIMITROPOULOS, Xenofontas. traIXroute: IXP detection in traceroute paths. In: International conference on passive and active network measurement. Springer, Cham, 2016. p. 346-358.

[5]. BRITO, Samuel Henrique Bucke, SANTOS, Mateus Augusto Silva, FONTES, R., et al. Anatomia do ecossistema de pontos de troca de tráfego publicos na internet do brasil. XXXIII Simpósio Brasileiro de Redes de Computadores (SBRC). Vitoria, ES, Brazil , 2015

[6]. MAO, Zhuoqing Morley, REXFORD, Jennifer, WANG, Jia, et al. Towards an AS-level accurate traceroute tool. In: Proceedings of the 2003 conference on Applications, technologies, architectures and protocols for computer communications. 2003. p. 365-378.

[7]. KIENTEGA Y. Raoul, OUEDRAOGO T Fréderic, BIKIENGA Moustapha, SIDIBÉ Moustapha; Comparative Study between TraIXroute and Burkina TraIXroute on the Wayto Traceroute; JACN 2022 Vol.10(2): 16-21 ISSN: 1793-8244

[8]. Giotsas, V., Zhou, S., Luckie, M., claffy, k. : Inferring multilateral peering. In: Proc. ACM SIGCOMM CoNEXT (2013)

[9]. RICHTER, Philipp, SMARAGDAKIS, Georgios, FELDMANN, Anja, et al. peering to peerings: On the role of IXP route servers. In: Proceedings of the conference