ver 1.0

traIXroute

NAME

traIXroute [1] — A tool that detects if and where a traceroute path crosses an IXP fabric.

SYNOPSIS

traIXroute [-h] [-u] [-m] [-asn] [-rule] [-i IP] [-d input file] [-o output file] [-s [options]] [-t [options]]

DESCRIPTION

traIXroute is a python 3 tool that infers IXP hops on traceroute paths by applying IXP detection rules using data provided by PeeringDB (PDB) [6], Packet Clearing House (PCH) [5] and CAIDA [7]. The user can specify either a single destination IP address or a list of addresses in an input file (*batch execution)* to probe. **traIXroute** can be configured to use in the background either the well-known traceroute tool [4] or scamper [2], a more sophisticated tool provided by CAIDA, which implements the Paris traceroute technique [3]. **traIXroute** first probes a paths using traceroute or scamper. Next, it seeks for an IXP IP address in the path and applies the IXP detection rules in a sliding window fashion to deduce, if possible, the exact hop (i.e. before or after the IXP IP address) where the IXP was crossed. **traIXroute** does not support yet IPv6.

Available **traIXroute** options:

-h

Prints a list of the command line options with a synopsis for each one.

-u

Downloads all the necessary files for the IXP detection rules (see section Datasets). The tool automatically enables this option in case the files are missing.

-m

Exports the database to the files *ixp_membership.txt* and *ixp_prefixes.txt.* For further information see the Datasets section.

-asn

Enables printing the ASN for each IP hop in the traIXroute output (see section Output).

-rule

Enables printing the hitted IXP detection rule in the *IXP Hops* output (see section Output).

-i IP/FQDN

Specifies the destination IP address or the fully qualified domain name (FQDN) to probe.

-d input file

As an alternative way to send probes to multiple IPs, the user can create a .txt file with a list of IP addresses or FQDNs, following the format shown below. **traIXroute** will probe all the destinations.

IP1/FQDN1
IP2/FQDN2
IP3/FQDN3

-o output file

Specifies the name of the output file. Otherwise, the default output file name (i.e. *output_Y_M_D-h_m_s.txt*) will be used.

traIXroute can send probes either using the scamper or traceroute tools. To use one of these, one of the following arguments should be used:

-s (optional) **[options]**

traIXroute will use the scamper tool. traIXroute is configured to use scamper with the **-trace** option only. All the available **-trace** options can only be used in brackets after **-s** argument. For further information about the available options see the documentation of scamper [8].

-t (optional) **[options]**

traIXroute will use the traceroute tool. All the traceroute options can only be used in brackets after **-t** argument. For further information about the available options see traceroute's documentation [9].

EXAMPLES

Some examples on how to use the tool are described below. Depending on the configuration of the operating system, "sudo" might not be required.

- traIXroute uses scamper with the option max ttl 12 towards the destination inspire.edu.gr:
  $ sudo python3 traIXroute.py -i inspire.edu.gr -s [-m 12]

- traIXroute uses scamper towards the destination 8.8.8.8:
  $ sudo python3 traIXroute.py -i 8.8.8.8 -s

- traIXroute uses traceroute with ICMP ECHO probes towards destinations read from an input file *input.txt*.
  $ sudo python3 traIXroute.py -d input.txt -t [-I]

- traIXroute rebuilds the database with fresh data (if available), uses traceroute towards the destination 192.198.10.10, and writes the output to a file.
  $ sudo python3 traIXroute.py -i 192.198.10.10 -o myoutput.txt -u -t

OUTPUT

A sample of **traIXroute**'s output is shown below running the following command:

sudo python3 traIXroute.py -i inspire.edu.gr -asn -rule -s

→ The first time **traIXroute** runs, it initializes its database with the IXP detection rules and with the downloaded IXP Membership Data and IXP Prefix Data.

Imported 8 IXP Detection Rules from rules.txt.
Imported 16 Reserved Subnets.
Extracted 0 IXP IPs from additional_info.txt.
Extracted 1 IXP Subnets from additional_info.txt.
Extracted 14040 IXP IPs from PDB.
Extracted 9984 IXP IPs from PCH.
Extracted 377 IXP Subnets from PDB.
Extracted 368 IXP Subnets from PCH.
Extracted 14449 not dirty IXP IPs after merging PDB, PCH and additional_info.txt.
Extracted 1516 dirty IXP IPs after merging PDB, PCH and additional_info.txt.
Extracted 587 IXP Subnets after merging PDB, PCH and additional_info.txt.

→ Prints all the configuration parameters.

traIXrouting using scamper with default options.

→ Prints the traceroute path enriched with AS and IXP information for each hop, resolving the domain name for every IP address.

traIXroute to inspire.edu.gr (139.91.152.72)
1) AS 192.168.1.1 (192.168.1.1) 0.482 ms*
2) AS1241 bbras-llu-her-01L500.forthnet.gr (213.16.246.[redacted]) 30.750 ms
3) AS1241 213.16.247.[redacted] (213.16.247.X) 30.683 ms
4) AS1241 te0-4-0-11.core-kln-13.forthnet.gr (194.219.199.[redacted]) 41.178 ms
5) AS1241 distr-kln-02Be2.forthnet.gr (213.16.247.[redacted]) 37.480 ms
6) AS1241 core-kln-12Be3.forthnet.gr (213.16.247.[redacted]) 40.440 ms
7) GR-IX->AS5408 grnet.gr-ix.gr (176.126.38.1) 39.864 ms
8) AS5408 forth-her-4.eier.access-link.grnet.gr (62.217.98.[redacted]) 45.995 ms
9) AS * (*) -*
10) AS * (*) -*
11) AS * (*) -*
12) AS * (*) -*
13) AS * (*) -*

→ Prints the IXP hop(s), if there exist, following the format: *IXP detection rule number --- Hop number) IP Address (AS number) - IXP Name - Hop number) IP Address (AS number)*. For instance, in the output below, Rule 1 of the IXP detection rules infers an IXP crossing (GR-IX) between hops 6 and 7 (AS1241 and AS5408, respectively).

IXP Hops:
Rule: 1 --- 6) 213.16.247.[redacted] (AS1241) <--- GR-IX ---> 7) 176.126.38.1 (AS5408)

DATASETS

traIXroute utilizes three types of data to detect IXPs, which can be updated from the command line automatically (see available options and [1]):

1. IXP Membership Data
2. IXP Prefix Data
3. Routeviews Prefix to AS mappings

The first two datasets are retrieved from the PDB and PCH to detect IXP IP addresses in an IP path. The two datasets are merged by matching IXP IP addresses, prefixes and names since they do not use consistent identifiers for IXPs. The third dataset is used to map IP addresses to ASes. Such mappings might be wrong [11], therefore **traIXroute** does not consider this evidence alone conclusive to infer IXP crossings.

During the merging process, the tool finds and filters out inconsistencies between the two datasets, i.e., IXP IP addresses that are assigned to multiple ASes and IXP prefixes that belong to different IXPs between PDB and PCH.

After merging, **traIXroute** conducts further sanity checks in the database. **traIXroute** excludes the IXP IP addresses and Prefixes that belong to the Reserved IP Subnets [10]. However, when IXP IP addresses that do not belong to any of the available IXP prefixes or their corresponding IXP prefix maps to a different IXP from the IXP of the IXP IP address, are not filtered, but are kept and marked as **"dirty"** information. Hence, for each IP hop the tool utilizes dirty information, the **"?"** notation is used at the beginning of the row in the traIXroute output.

For convenience, when the first two datasets have been finalized and sanitized, all the IXP Membership and Prefix Data are exported into two files, *ixp_membership.txt* and *ixp_prefixes.txt*, respectively. Note that in the second column in the *ixp_membership.txt* file, the **"?"** is used for the dirty data while the **"+"** for the data coming from the *additional_info.txt* file.

ADDITIONAL FILES

traIXroute uses additionally the *additional_info.txt* file which contains user-specified IXP data. The user can add IXP Membership and Prefix Data or overwrite the PDB and PCH data in the *additional_info.txt* file (check the file for an example of the format). The file includes one IXP Membership or IXP Prefix Data entry per line. If an entry in the file does not exist in the PDB and PCH data, then it is added to the final dataset. Otherwise, it overwrites the corresponding entry in the database of **traIXroute**.

IXP DETECTION RULES

To detect an IXP crossing in the traceroute path, **traIXroute** applies various heuristic rules over the IP path in a sliding window fashion. The length of the window is set to two or three IP addresses depending on the rule. IXP detection rules can be appended in the *rules.txt* file (one rule per line). If detection rules have not been specified in the file, the tool cannot infer an IXP crossing. They are applied in the order they appear in the file. This means that the first rule in the file has the highest priority, etc.

IXP detection rules can be defined with a specified grammar, which allows to compose new rules. However, the tool is pre-configured with the rules proposed and evaluated in [1]. Each rule consists of the left (condition) and the right (assessment) part. The left part includes the conditions of the rule hops under which an IXP crossing is detected in a path, and the right assesses between which hops the IXP crossing takes place. The available keywords for defining IXP detection rules are the following:

- **IXP_IP :** denotes that the rule in the condition part requires an IXP IP address at the certain hop. This keyword is only used with **AS_M** and **!AS_M** notations, i.e., **IXP_IP and AS_M** to detect an IXP IP address in the trace based on the IXP Membership data while **IXP_IP and !AS_M** based on IXP Prefixes data respectively.
- **AS_M :** denotes that the rule in the condition part requires an AS to be IXP member. If the **AS_M** is used with the **IXP_IP** keyword (e.g., *IXP_IP and AS_M0*), then the AS should be member to the respective IXP at the certain hop. Otherwise, when the **AS_M** keyword is used as the only condition in a rule hop (i.e., without an **IXP_IP**), then the rule expects the AS, mapped from an IP based on Prefix-to-AS mappings, to be member to the candidate IXPs of the previous/next hops in the rule (e.g. rule example 7).
- **'!' :** is used as a 'not' operator to reverse the condition. This can be used only with the **AS_M** keyword. When the notation **!AS_M** is used with the **IXP_IP** (e.g., *IXP_IP and !AS_M*, as described earlier) denotes an IXP IP, detected based on IXP Prefixes data, while if it is used as the only condition in a certain rule hop, it determines an AS as a not IXP member.
- **a :** specifies that the IXP crossing link is located between the first two hops of the sliding window.
- **b :** specifies that the IXP crossing link is located between the last two hops of the sliding window. This can only be used with the rules of window size 3.
- **and :** can be used either in the condition or the assessment part of the rule. In the condition part, it is used to build a condition set for a certain hop (e.g., *IXP_IP and !AS_M*). If used in the assessment part, the rule must have window size 3 and it specifies that there exist IXP crossings between the first and the last two hops (e.g., *a and b*).
- **or :** can only be used in the assessment part of the rule to specify the IXP crossing link.
- **'-' :** separates the conditions of each hop in the condition part of the rule (e.g., *condition - condition - condition : assessment*).
- **'( )' :** determines a condition set (e.g., *condition - (IXP_IP and !AS_M) - condition : assessment*) in the condition part of the rule.
- **':' :** separates the condition from the assessment part of the rule (e.g., *rule_conditions: rule assessment*).

- To formulate rules that require more than one (different) IXPs and/or (different) AS members in the condition part, the user can concatenate to the keywords **IXP_IP** and **AS_M**, same or different numbers (i.e., **0, and/or 1, and/or 2**) that allows to differentiate between IXPs (e.g., *(IXP_IP0 and AS_M) - (IXP_IP1 - AS_M)*) and AS members (*AS_M0 - AS_M1 - (IXP_IP and !AS_M)*) (see rule examples 4 and 5).

RULE EXAMPLES

Examples of IXP detection rules are proposed below. Some of the following rules are only used for demonstrating all the possible ways to syntax the rule keywords. This means that their assessment does not necessarily infer a valid IXP crossing.

1. **AS_M0 - (IXP_IP and AS_M1) - AS_M1: *a***

This rule examines a window of size three. (1) It requires one IXP IP in the middle hop and (2) AS based information for all the three hops, for the middle one based on IXP Membership data while for the border ASNs based on Prefix-to-AS mappings. (3) The ASN in the first hop should be different from the next two ASNs, since the first concatenated keyword number, *'0'*, differs from the one in the next two hops (i.e., *'1'*). (4) All the three ASes are required to be members of the candidate IXP in the middle hop. Its assessment is an IXP crossing in link *a*, i.e., in the first hop.

2. **AS_M0 - (IXP_IP and !AS_M) - !AS_M1: *a***

This rule examines a window of size three. (1) It requires one IXP IP in the middle hop based on IXP Prefixes data, (2) AS information only for the border IPs and (3) the two border ASNs must be different. (4) In contrast with the previous rule, only the first AS must be member of the candidate IXP of the middle hop. Its assessment is an IXP crossing in link *a*, i.e., in the first hop.

3. **AS_M0 - (IXP_IP and AS_M1) - AS_M2: *a or b***

This rule examines a window of size three. (1) It requires one IXP IP in the middle hop, (2) AS information with (3) different ASNs for all the three hops and (4) all the three ASes to be members of the candidate IXP of the middle hop. Its assessment is an IXP crossing in hops *a* or *b*.

4. **(IXP_IP0 and AS_M0) - (IXP_IP0 and AS_M1): *a***

This rule examines a window of size two. (1) It requires two different IXP IPs (2) from the same IXP subnet (3) with AS information based on IXP Membership data. (4) The rule specifies different ASNs between the two hops since there are different numbers (i.e., *0 and 1*) concatenated with the AS_M keywords. Its assessment is an IXP crossing in link *a*, i.e., in the first hop.

5. **(IXP_IP0 and AS_M) - (IXP_IP1 and AS_M): *a***

This rule examines a window of size two. (1) It requires two different IXP IPs for both IPs (2) from different IXPs (3) with AS information based on IXP Membership data. (4) The rule does not compare the ASNs of the two IPs, in contrast to the previous rule. This means that both ASes might be the same. Its assessment is an IXP crossing in link *a*, i.e., in the first hop.

6. **(IXP_IP0 and AS_M0) - (IXP_IP1 and AS_M1) - (IXP_IP2 and AS_M2): *a and b***

This rule examines a window of size three. (1) It requires IXP IPs for all the three hops (2) coming from three different IXPs (3) with AS information based on IXP Membership data, and (4) different ASNs for all the ASes. Its assessment is two consecutive IXP crossings in hops *a* and *b*.

7. **(IXP_IP0 and AS_M0) - AS_M - (IXP_IP1 and AS_M1): *a or b***

This rule examines a window of size three. (1) It requires two IXP IPs in the border IPs based on IXP Membership data (2) from different IXP subnets and (3) AS information for all the three hops. However (4) the ASN in the middle hop is not compared with the rest ASNs (i.e., it can be either the same or different; this would not affect the rule assessment). (5) Also, the AS in the middle hop has to be member in both IXPs. Its assessment is an IXP crossing in hops *a* or *b*.

MODULES

A detailed representation of the modules of **traIXroute** is shown in Figure 1.

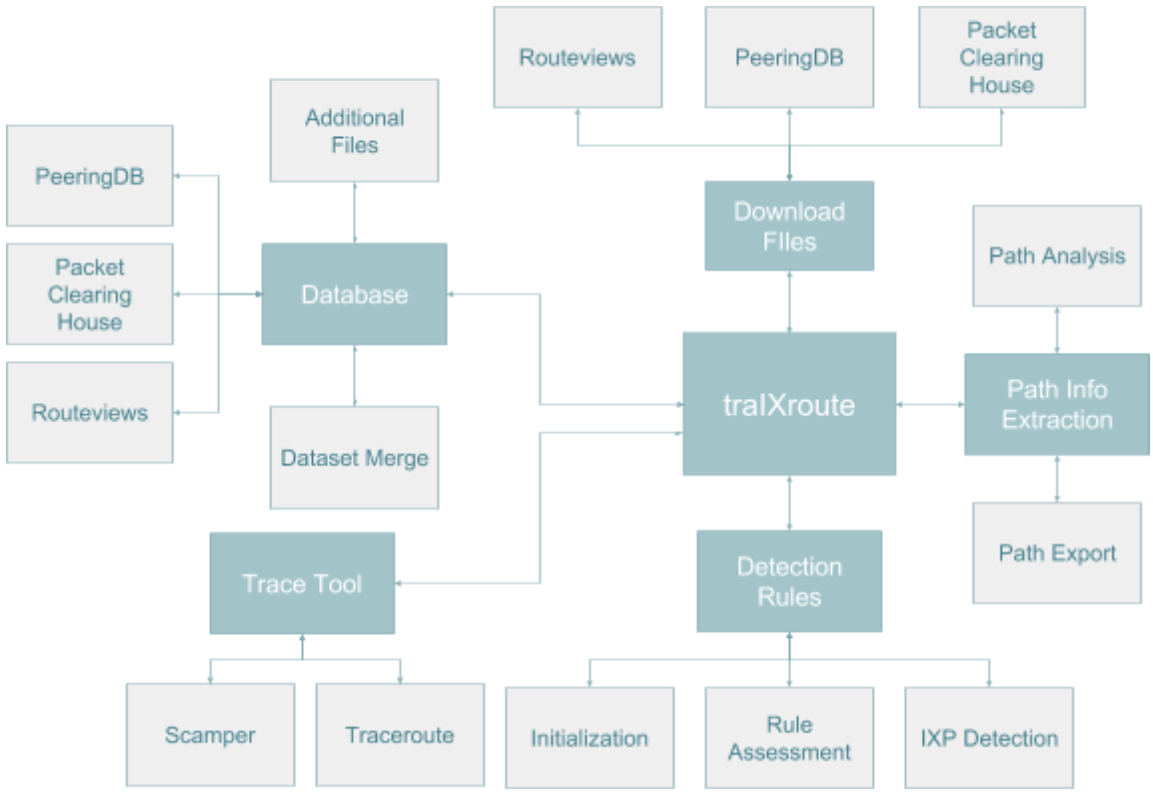

Figure 1: Overview of **traIXroute** modules.

A brief description of each module is given below. The modules' Class names are shown in parenthesis:

traIXroute (*traIXroute*): This is the core module that orchestrates all the modules to detect and identify if and at which hops an IXP is crossed.

Download Files (*download_files*): It is responsible for downloading the PDB and PCH datasets and the Routeviews AS-to-Prefix mappings.

Database (*database*): This module is responsible for managing the database of **traIXroute**. It uses the downloaded data, imports the files with the user-defined data (Reserved IP addresses, IXP Membership and Prefixes data), and finally merges the datasets.

Trace Tool (*trace_tool*): It configures and runs the selected traceroute tool.

Path Info Extraction (*path_info_extraction*): It enriches the traceroute path with AS and IXP information, and prints the output.

Detection Rules (*detection_rules*): It loads the IXP detection rules, applies the rules on the enriched traceroute path, and prints the detected IXP hops.

AUTHORS

traIXroute was written by Michalis Bamiedakis (mbam [at] ics [dot] forth [dot] gr) and George Nomikos (gnomikos [at] ics [dot] forth [dot] gr) from the **IN**ternet **S**ecurity, **P**rivacy, and **I**ntelligence **RE**search (INSPIRE) Group in the Institute of Computer Science of the Foundation for Research and Technology - Hellas (FORTH). The research was supervised by Prof. Xenofontas Dimitropoulos (fontas [at] ics [dot] forth [dot] gr).

ACKNOWLEDGEMENTS

The research that led to **traIXroute** was supported by the European Research Council (ERC) Grant 338402 - The NetVolution Project (www.netvolution.eu).

REFERENCES

[1] Nomikos, G. and Dimitropoulos, X., "traIXroute: Detecting IXPs in traceroute paths." In *Passive and Active Measurement Conference*, pp. 346-358. Springer International Publishing, 2016.

[2] Luckie, M., "Scamper: a scalable and extensible packet prober for active measurement of the internet." In *Proceedings of the 10th ACM SIGCOMM Conference on Internet Measurement*, pp. 239-245. ACM, 2010.

[3] Augustin, B., Friedman, T. and Teixeira, R., "Multipath tracing with Paris traceroute." In *End-to-End Monitoring Techniques and Services, 2007. Workshop on*, pp. 1-8. IEEE, 2007.

[4] Traceroute. (https://en.wikipedia.org/wiki/Traceroute)

[5] Packet Clearing House - Internet Exchange Directory. (https://prefix.pch.net/applications/ixpdir/menu_download.php)

[6] PeeringDB. (http://www.peeringdb.com)

[7] Routeviews Prefix to AS mappings Dataset (pfx2as) for IPv4. (http://www.caida.org/data/routing/routeviews-prefix2as.xml)

[8] Scamper Documentation. https://www.caida.org/tools/measurement/scamper/man/scamper.1.pdf

[9] Traceroute Documentation. (http://linux.die.net/man/8/traceroute)

[10] Reserved IP addresses. (https://en.wikipedia.org/wiki/Reserved_IP_addresses)

[11] Mao, Z.M., Rexford, J., Wang, J. and Katz, R.H., 2003, "Towards an accurate AS-level traceroute tool." In *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pp. 365-378. ACM, 2003.