Practical Anomaly Detection in Internet Services: An ISP centric approach

Alex HUANG FENG - INSA Lyon

Pierre FRANCOIS - INSA Lyon

Kensuke FUKUDA - NII Tokyo

Wanting DU - Swisscom

Thomas GRAF - Swisscom

Paolo LUCENTE - pmacct.net

Stéphane FRENOT - INSA Lyon

Interim Anomaly Detection - NMOP WG

11th September 2024

Index

Introduction

- Monitoring in ISP is important to avoid anomalies
  - Issues happen to all networks
  - Service interruptions
    - Cost you money
    - Make you look bad

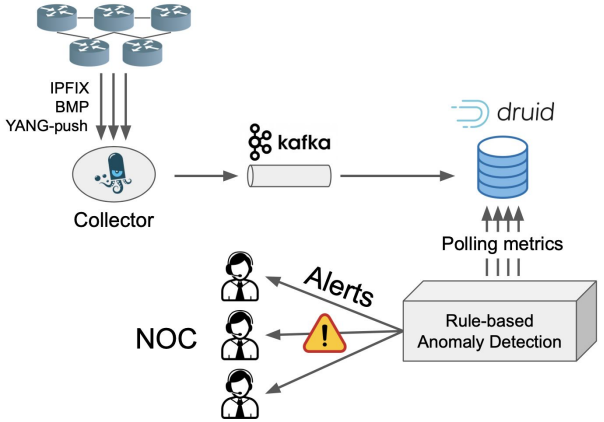
→ How can we detect anomalies in real world Internet Service Providers?

→ Which data can we use to detect these anomalies? Standards?

→ Can a rule-based approach be effective in detecting such anomalies?

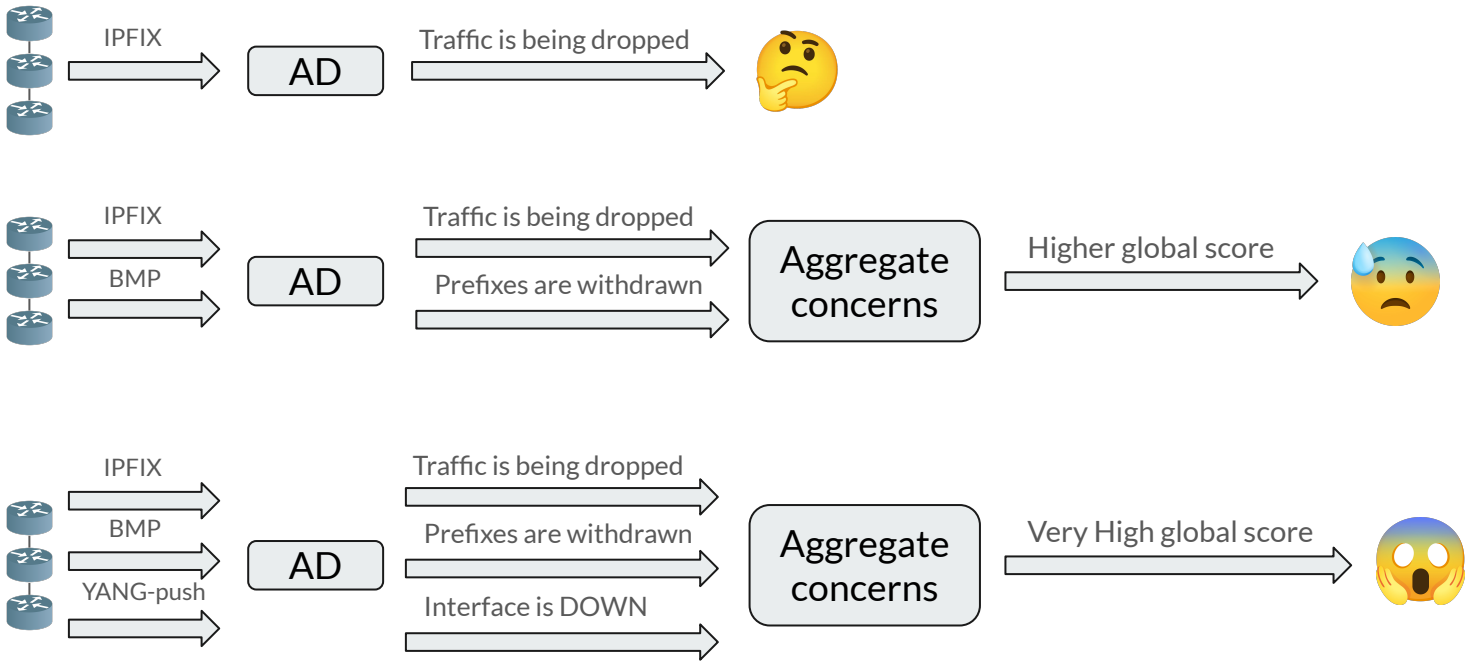
Use case: Anomaly Detection in BGP/MPLS VPN environments

- ***Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks ****
- Work presented at **IRTF 117/ANRW'23** San Francisco
- Anomaly Detection based on *Customer profiles*
  - Set of Strategies assigned to each profile
  - Set of Rule-based Checks assigned to each Strategy
  - Execution of these Checks in Real-time in polling mode
    - Comparing traffic to last week
    - Spikes in control-plane (BGP Updates & BGP Withdraws)
    - Interface status gone DOWN
    - …
- Currently deployed in Swisscom VPN Customers



* *Alex Huang Feng, Pierre Francois, Stéphane Frenot, Thomas Graf, Wanting Du, and Paolo Lucente. 2023. Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks. In Proceedings of the Applied Networking Research Workshop (ANRW '23). Association for Computing Machinery, New York, NY, USA, 8–14.* https://doi.org/10.1145/3606464.3606470 (Open access: https://hal.science/hal-04307611)

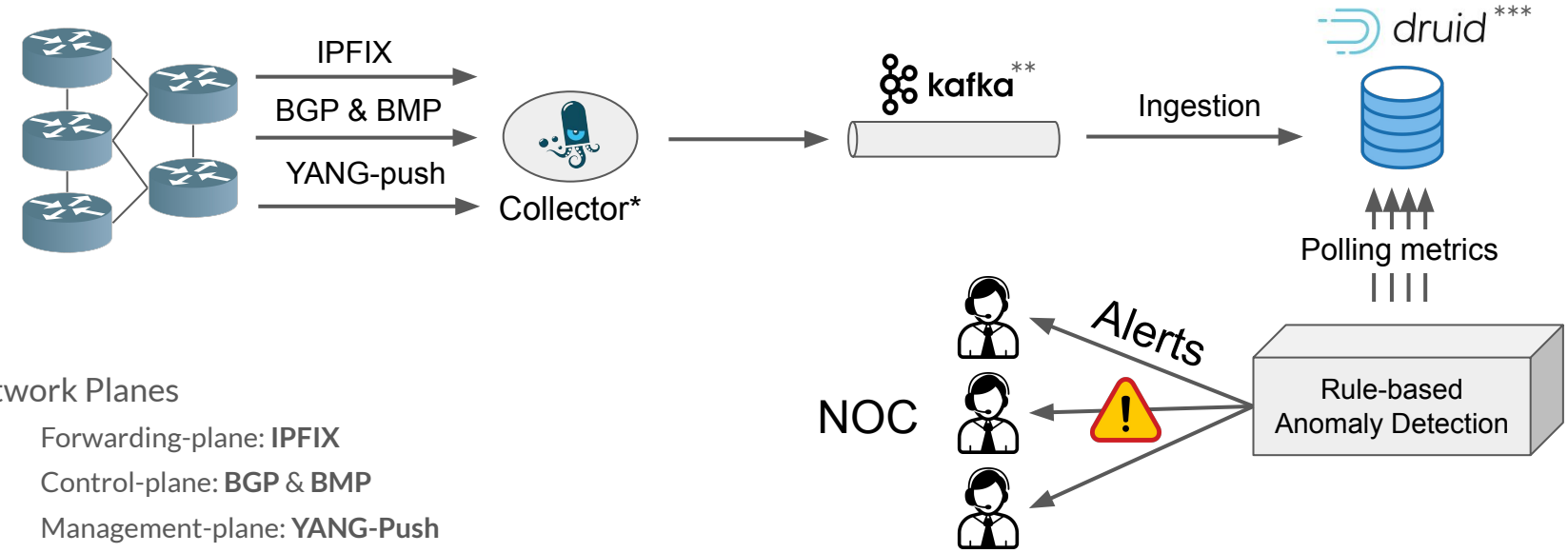
Daisy: Anomaly Detection (AD)



Current work: Anomaly Detection in Internet Services

- Plan: use same Framework to detect anomalies in services providing Internet Connectivity
- Customer Profiles: BGP Communities vs AS Number
- Implement specific Strategies for monitoring ASN traversing an ISP
- **Disruptions Detection**
  - Losing a Top talker
  - Neighbour AS has been disconnected from the Internet
  - Trending analysis: Saturating a neighbour peer link
- **Anomaly Detection**
  - Traffic from a Settlement-free peer has moved to a Transit provider
  - Monitor traffic ratios on Settlement-free peers
  - The traffic from an AS is traversing my whole network instead of rapidly being forwarded to the shortest path
  - Prefix for which RPKI was valid is not anymore
- **Security related anomalies** (low priority)
  - Prefix hijacks
  - DDoS

Architecture - High level view



Network Planes

- Forwarding-plane: **IPFIX**
- Control-plane: **BGP** & **BMP**
- Management-plane: **YANG-Push**

* *pmacct* collector: http://www.pmacct.net
** Apache Kafka: https://kafka.apache.org
*** Apache Druid https://druid.apache.org

Rule-based checks

- IPFIX
  - Comparing total bytes to one week before
  - Comparing the slope to one week before
  - Spike in flow count
  - Spike drop counters
- BGP / BMP
  - Spike in BGP withdraw messages
  - Spike in BGP update messages
  - Spike in peer down messages
- YANG-Push
  - Interfaces changed status to DOWN

Based on what operators do when looking at the data

More to come based on post-mortem analysis!

Use case: Losing a top talker (Disruption)

Top talkers = ASN sending the most traffic to you

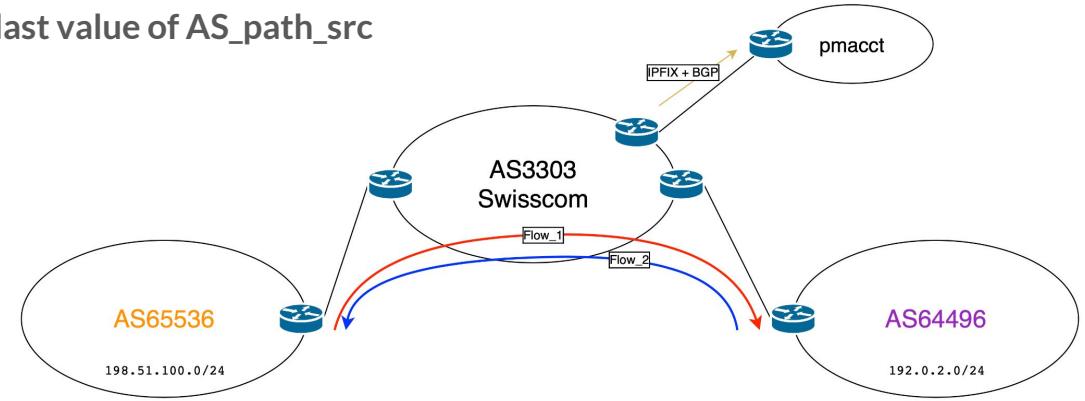
Flow_ 1:

- src:198.51.100.1; dst:192.0.2.1; Bytes: 10 bytes; AS_path: <AS3303,AS64496>; AS_path_src: <AS3303,AS65536>

Flow_2:

- src:192.0.2.1; dst:198.51.100.1; Bytes: 10 bytes; AS_path: <AS3303,AS65536>; AS_path_src: <AS3303,AS64496>

Top talkers: **Aggregation of flows based on last value of AS_path_src**



Use case: Losing a top talker (Disruption)

Monitor ASN on a ASN basis:

- Compare ingress* traffic to last week
- Compare ingress* slope to last week
- Spike in egress** flow count
- BGP Withdraws spike from the Origin ASN
- BGP Update spike from the Origin ASN

* ingress traffic: Traffic going from the Origin ASN to the local ASN
** egress traffic: Traffic going from the local ASN to the Destination ASN

Use case: Losing a top talker (Disruption)

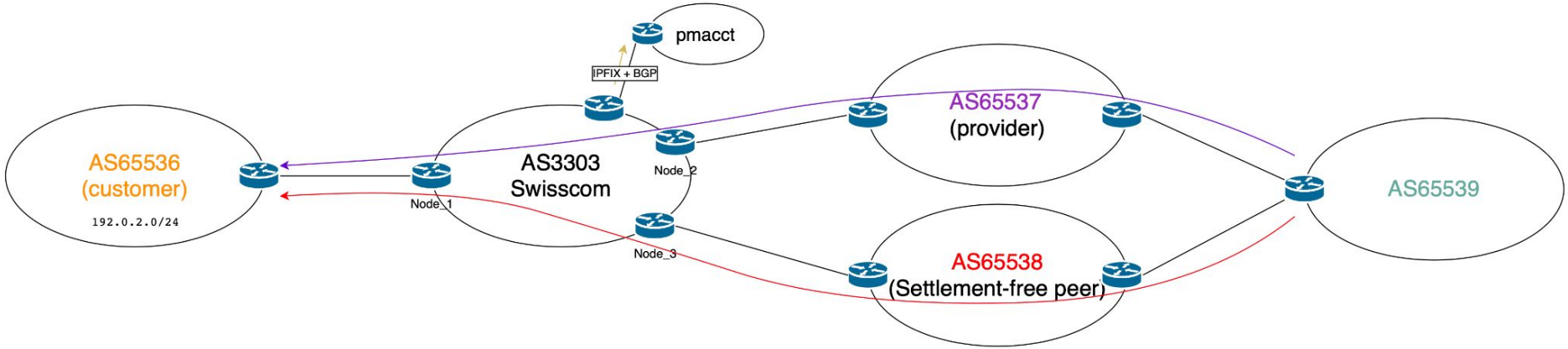
Use case: Settlement-free peer traffic shifted to transit provider (Anomaly)

Flow_1 (aggregated from 2 nodes):

- src:198.51.100.1; dst:192.0.2.1; Bytes: 10 bytes; AS_path: <AS3303,AS65536>; AS_path_src: <AS3303,AS65537,AS65539>; comms: [3303:1000] (customer); comms_src: [3303:XXXX] (Upstream)

Flow_2 (aggregated from 2 nodes):

- src:198.51.100.2; dst:192.0.2.2; Bytes: 10 bytes; AS_path: <AS3303,AS65536>; AS_path_src: <AS3303,AS65537,AS65538>; comms: [3303:1000] (customer); comms_src: [3303:YYYY] (Peer)

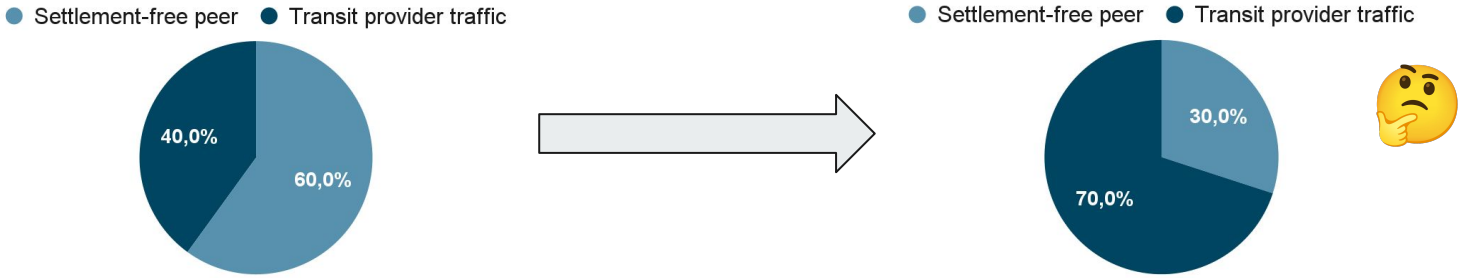


Use case: Settlement-free peer traffic shifted to transit provider (Anomaly)

1. Track for selected ASN:
   - sum of traffic coming from settlement-free peers
   - sum of traffic coming from transit providers
2. Track ratio over time and alert

How ?

- Leveraging **BGP communities** identifying where the prefixes **were learned from**



Project Status

- Current Network Telemetry data:
  - IPFIX (Internet flows)
  - BGP (Internet BGP messages)
  - YANG-Push (Lab only)
- AD Strategies implemented in Python (pulling based mode)
- Checks implemented
  - VPN environments (currently deployed in prod)
  - **Internet Services (WIP)**
- Conducting tests in Swisscom lab
- Analysis of Swisscom Production
- Goal: deployment on a subset of ASNs based on the different use cases

Conclusion

- Network Operators want to be alerted when there are issues in their network but **also want to understand why these alerts were generated**
- We provide a solution based on IETF Standards to collect the data and Open-source solutions
- What's next?
  - Complete use cases on Internet Services
  - Analysis using production use cases
  - Detect missing Standard gaps to support the anomaly detection
  - For some use cases, external views (outside of the ISP) would be needed (RouteViews*)
  - Root cause analysis?

* RouteViews: https://www.routeviews.org/routeviews/

Reference Papers

- Alex Huang Feng, Pierre Francois, Kensuke Fukuda, Wanting Du, Thomas Graf, et al.. **Practical Anomaly Detection in Internet Services: An ISP centric** approach. *NOMS 2024-2024 IEEE Network Operations and Management Symposium*, May 2024, Seoul, South Korea. pp.1-4, ⟨10.1109/NOMS59830.2024.10575071⟩. ⟨hal-04655324⟩

- Alex Huang Feng, Pierre Francois, Stéphane Frenot, Thomas Graf, Wanting Du, et al.. **Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks**. *ANRW 2023 : Applied Networking Research Workshop*, Jul 2023, San Francisco, United States. pp.8-14, ⟨10.1145/3606464.3606470⟩. ⟨hal-04307611⟩

Thanks for listening

Contacts

- Alex Huang Feng (INSA Lyon): alex.huang-feng@insa-lyon.fr
- Pierre Francois (INSA Lyon): pierre.francois@insa-lyon.fr
- Kensuke Fukuda (NII Tokyo): kensuke@nii.ac.jp
- Wanting Du (Swisscom): wanting.du@swisscom.com
- Thomas Graf (Swisscom): thomas.graf@swisscom.com
- Paolo Lucente (NTT, pmacct.net): paolo@pmacct.net
- Stéphane Frénot (INSA Lyon): stephane.frenot@insa-lyon.fr