# Detecting External Disruptions in Internet Services Provider Networks

***Alex HUANG FENG*** - INSA Lyon
Pierre FRANCOIS - INSA Lyon
Kensuke FUKUDA - NII Tokyo
Wanting DU - Swisscom
Thomas GRAF - Swisscom
Paolo LUCENTE - pmacct.net
Maxence YOUNSI - INSA Lyon
Stéphane FRENOT - INSA Lyon

IETF IEPG / NMOP WG

20th July 2025

# Context

- ISPs offer multiple IP-based connectivity services
  - BGP / MPLS VPNs
  - Internet Connectivity
  - ...
- Network disruptions affect the reputation and business of the ISP
- Network operators want to detect these anomalies
  - Promptly: to provide a resolution as soon as possible
  - Comprehensively: to understand the issue when they are alerted

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

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

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


Media & Telecom

2 minute read · July 14, 2021 7:57 AM GMT+2 · Last Updated 2 years ago

**Swisscom boss apologises for massive network outage - newspaper**

Reuters

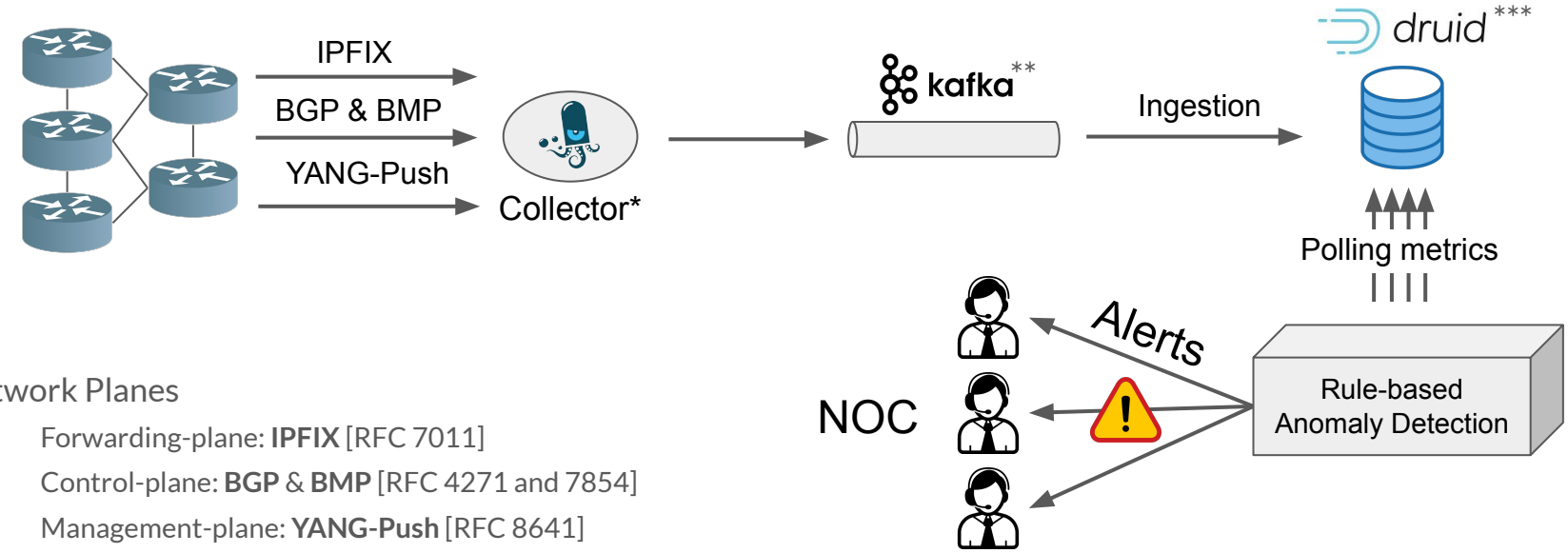


[1/2] Chief Executive Urs Schaeppi of Swiss internet, mobile phone and digital television provider Swisscom addresses the company's annual news conference in Zurich, Switzerland February 7, 2019. ... Read more

# Issues with State of the Art approaches

- Common approaches
  - Data-centric approaches: let the ML system learn and trigger alerts based on outliers
  - Output from data-centric systems not entirely interpretable by network engineers
  - Usually focused on Anomaly Detection in the Internet Topology rather than from an ISP perspective
- Usually results in:
  - Loss of trust in the system by network engineers
  - Lacks a defined starting point for troubleshooting
- We need a network-centric solution!
  - Use Standards when possible
    → Avoid reinventing the wheel when the ISP changes to a new vendor
  - Implement Open-source solutions
    → Avoid the need of buying vendor specific products
  - Use of scalable network telemetry protocols
    → Aggregation at different stages: Node, Collector, Anomaly Detection System

# High Level Architecture

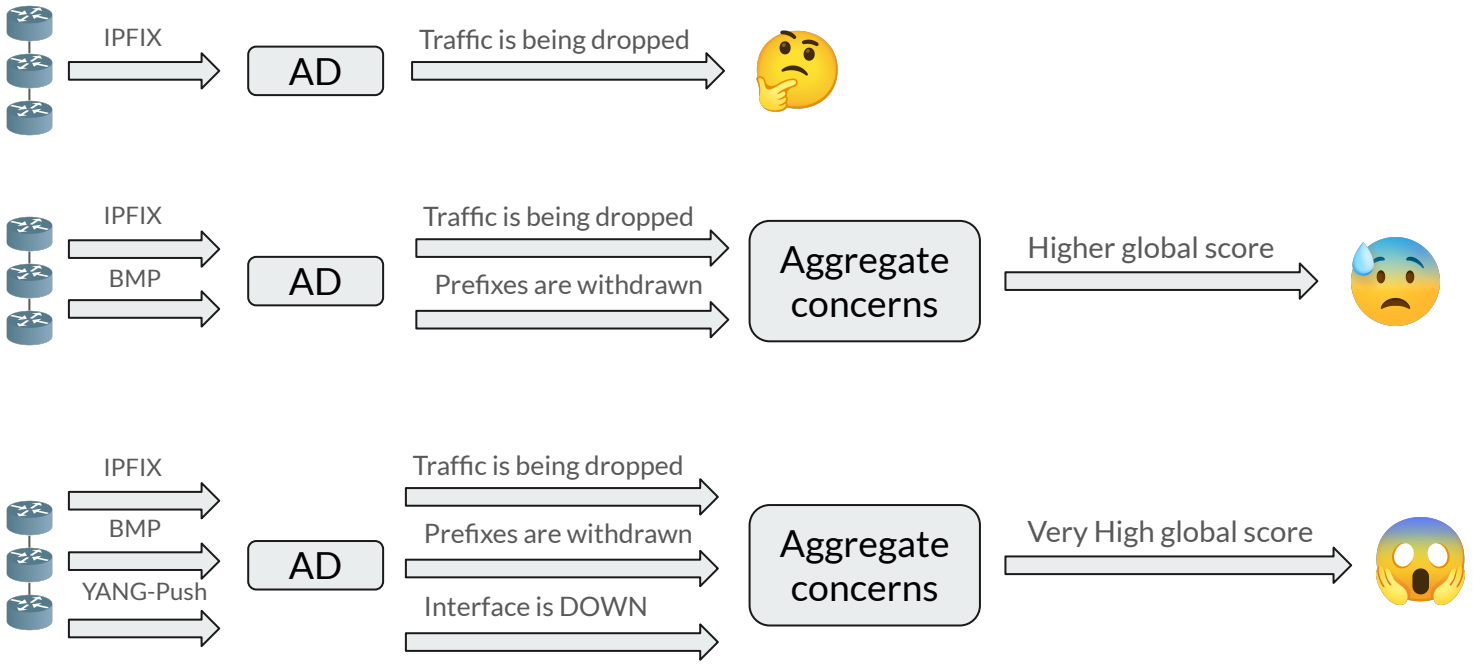



Network Planes

- Forwarding-plane: **IPFIX** [RFC 7011]
- Control-plane: **BGP** & **BMP** [RFC 4271 and 7854]
- Management-plane: **YANG-Push** [RFC 8641]

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

# Our Approach: Mimic network engineers



# Scope: Anomaly Detection in Internet Services

- Framework [1] already fully deployed in Swisscom L3 VPN network [2]
- Focus: Internet Connectivity Services
- **Disruptions Detection**
  - Losing a Top talker / Top receiver
  - 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
  - Impact of BGP Filtering on Inter-Domain Routing Policies [RFC7789]
  - The traffic from an AS is traversing my whole network instead of rapidly being forwarded to the shortest path
- **Security related anomalies** (further works)
  - Prefix hijacks
  - DDoS

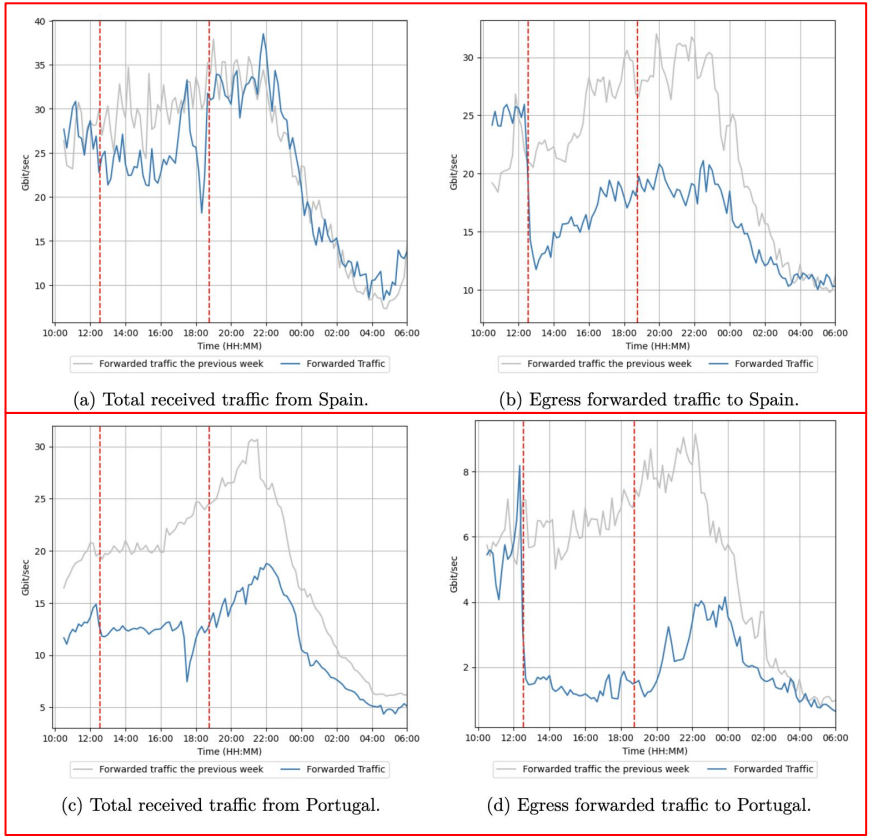
[1] https://datatracker.ietf.org/doc/draft-ietf-nmop-network-anomaly-architecture/
[2] https://datatracker.ietf.org/meeting/122/materials/slides-122-nmop-sessb-swisscom-network-incident-network-analytics-postmortem-00

# First Case Studies (in collaboration with Swisscom)

- Chile power Blackout
  - The 25 February 2025, Chile had a nationwide blackout that impacted all critical infrastructure including its network infrastructure [1]
- Bouygues Telecom nationwide disruption
  - On March 11, 2025, the French ISP Bouygues Telecom experienced an outage that disrupted Internet connectivity across France [2]
- **Iberian Peninsula power Blackout**
  - On April 28, 2025, Spain and Portugal, a massive power outage impacted critical infrastructure, including telecommunications services [3]


[1] https://www.barrons.com/news/chile-suffers-extensive-electricity-blackout-authority-f9bac89d
[2] https://www.lemonde.fr/pixels/article/2025/03/11/bouygues-telecom-subit-une-panne-de-grande-ampleur_6578598_4408996.html
[3] https://www.euronews.com/my-europe/2025/04/28/spain-portugal-and-parts-of-france-hit-by-massive-power-outage

# Case Study: Iberian Peninsula power Blackout




(a) Total received traffic from Spain.

(b) Egress forwarded traffic to Spain.

(c) Total received traffic from Portugal.

(d) Egress forwarded traffic to Portugal.

Timeline

- Power outage started at 12:33 pm CEST April 28th
- Restoration efforts began in the afternoon, with peripheral areas regaining power around 5:00 PM CEST.
- By 8:35 pm, 35% of the energy demand was met
- Full restoration at 11:00 am the next day

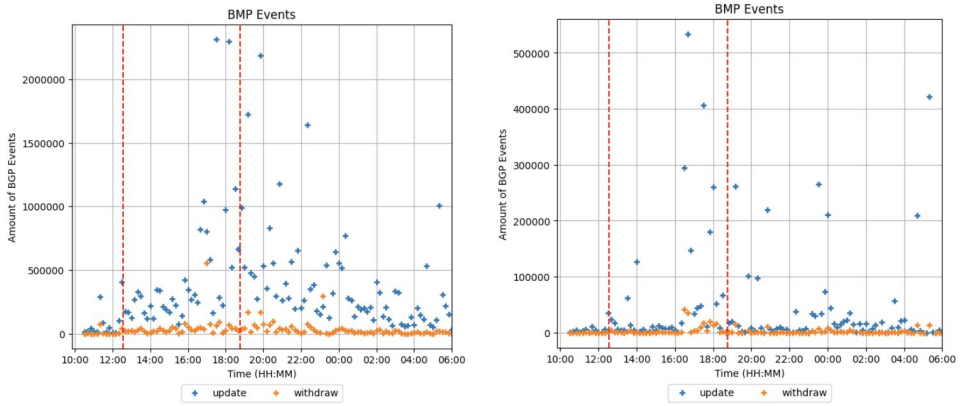
Impacts on the Internet:

- Spain traffic dropped to 20% of typical levels
- Portugal traffic dropped to 10% of typical levels

Traffic at Swisscom:

- Inbound Spain traffic dropped 20%
- Outbound Spain traffic dropped 50%
- Inbound Portuguese traffic dropped 50%
- Outbound Portuguese traffic dropped 80%

# Case Study: Iberian Peninsula power Blackout




(a) Received BGP events from Spain. (b) Received BGP events from Portugal.

Figure 2.24: Observed BGP topology changes at Swisscom associated to Spanish and Portuguese ASes.

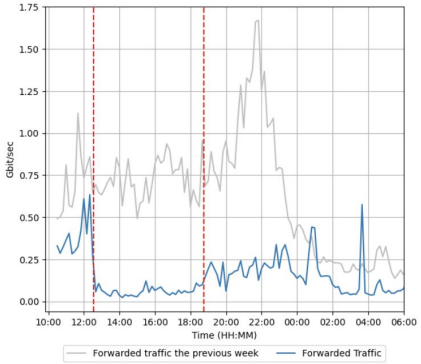
Timeline

- Power outage started at 12:33 pm CEST April 28th
- Restoration efforts began in the afternoon, with peripheral areas regaining power around 5:00 PM CEST.
- By 8:35 pm, 35% of the energy demand was met
- Full restoration at 11:00 am the next day

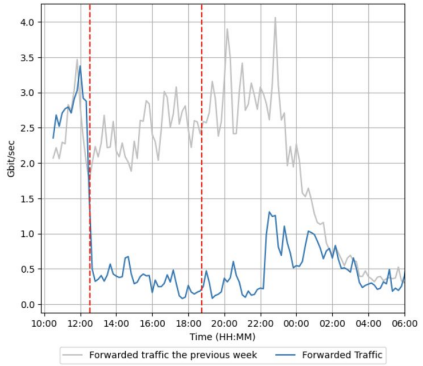
BGP events from Spain and Portuguese ASes at Swisscom:

- Sudden **spikes** in BGP updates and BGP withdraw events

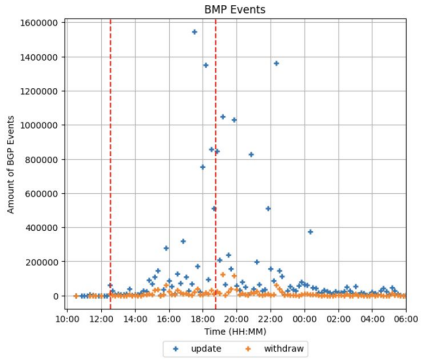
# Detailed Case Study: Orange Spain (AS12479)




(a) Total received ingress traffic.




(b) Total forwarded egress traffic.




(c) Received BGP events.

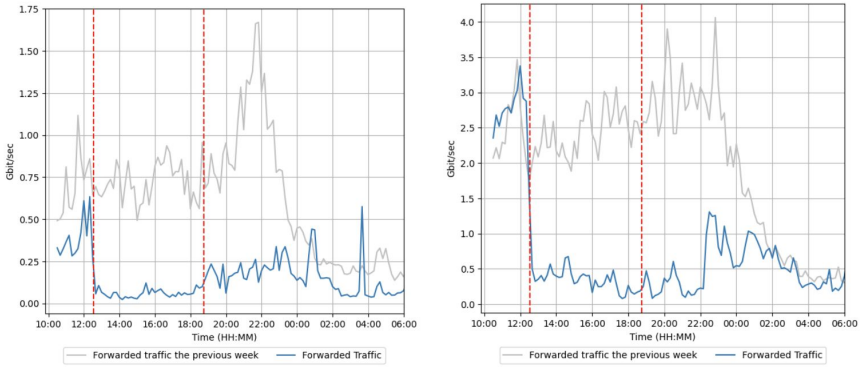
Key observations:

- **Sharp decrease** in inbound and outbound traffic when the power blackout started
- **Increase** in BGP update and withdraw events

→ Anomaly Detection Strategy:

- Comparison of inbound traffic to a week before (0.3)
- Comparison of outbound traffic to the week before (0.3)
- Spikes in BGP updates (0.1)
- Spikes in BGP withdraws (0.3)

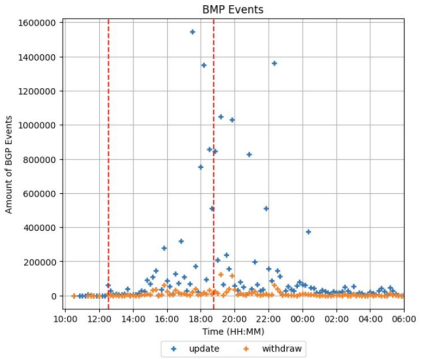
# Detailed Case Study: Orange Spain (AS12479)



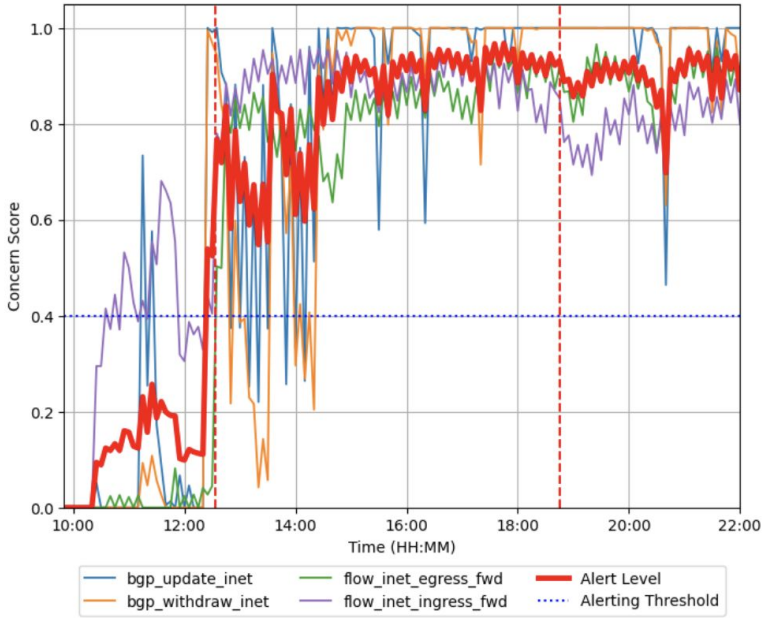

(a) Total received ingress traffic.



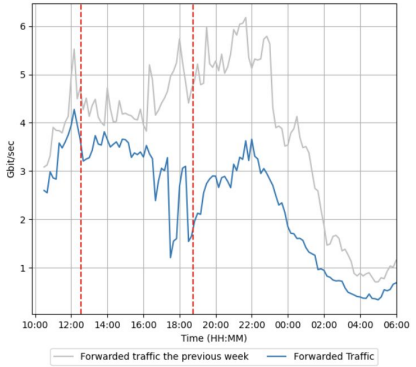

(b) Total forwarded egress traffic.



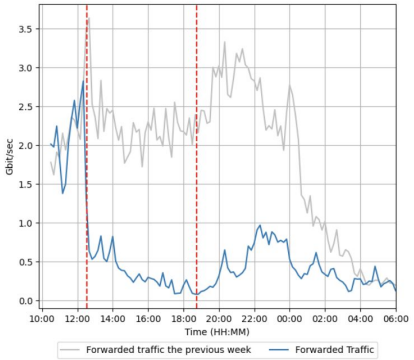

(c) Received BGP events.



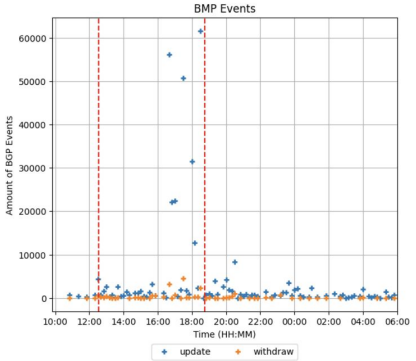
# Detailed Case Study: NOS Portugal (AS2860)



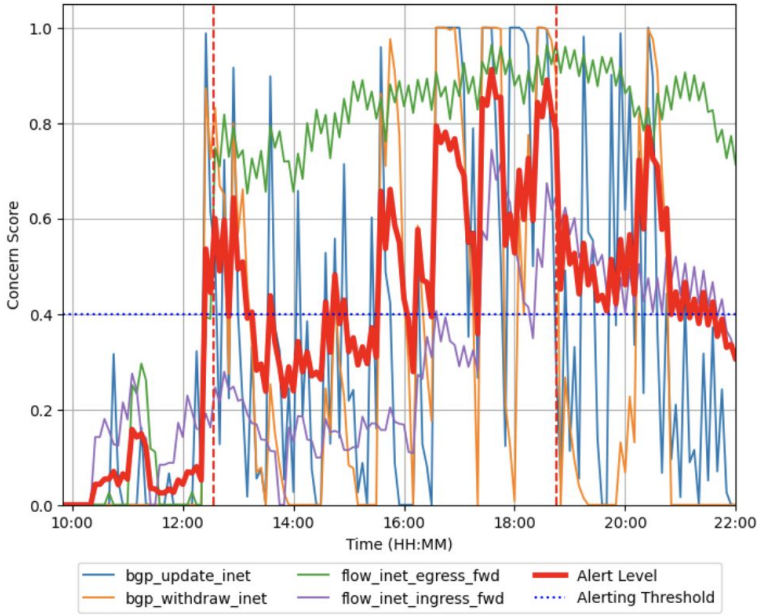

(a) Total received ingress traffic.




(b) Total forwarded egress traffic.




(c) Received BGP events.



# Conclusion

- Anomaly Detection systems for service provider networks need to be tailored to their daily processes
- Mimicking data inspections performed by network engineers can effectively detect disruptions, while also providing alerts that are comprehensible by network engineers.
- Strategies can be tailored to targeted anomaly use cases
- Future works
  - Integrate YANG-Push data (device status, configuration)
  - For some use cases, external views (outside of the ISP) would be needed (RouteViews*)
  - Root cause analysis?

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

# What's next?

- Interested in more Network Incident Postmortems?
  - Join **NMOP working group session on Wednesday 23th 16:00 – 17:00**
  - 2 incident postmortem presentations are scheduled
- Interested in contributing to requirements and anomaly detection?
  - Join **NMOP working group session on Monday 21st 9:30 – 11:30**
  - 4 documents related to Anomaly Detection and Incident management
    - draft-ietf-nmop-network-anomaly-architecture-04
    - draft-ietf-nmop-network-anomaly-lifecycle-03
    - draft-ietf-nmop-network-anomaly-semantics-03
    - draft-ietf-nmop-network-incident-yang-05

# Related Papers & Internet-Drafts


- 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
- Alex Huang Feng, Pierre Francois, Kensuke Fukuda, Wanting Du, Thomas Graf, Paolo Lucente and Stéphane Frenot. 2024. **Practical Anomaly Detection in Internet Services: An ISP centric approach**. In Proceedings of IEEE/IFIP INTERNATIONAL Workshop on Analytics for Network and Service Management (AnNet'24). NOMS 2024 IEEE/IFIP Network Operations and Management Symposium, Seoul, Korea, 2024. https://doi.org/10.1109/NOMS59830.2024.10575071
- Alex Huang Feng, Pierre Francois, Maxence Younsi, Stéphane Frenot, Thomas Graf, Wanting Du, Paolo Lucente and Ahmed Elhassani. 2025. **Detecting Service Disruptions in Large BGP/MPLS VPN Networks**. In Proceedings of IEEE Transactions on Network and Service Management (TNSM) Special Issue "Resilient Communication Networks for an Hyper-Connected World". https://doi.org/10.1109/TNSM.2025.3588314
- draft-ietf-nmop-network-anomaly-architecture-04
- draft-ietf-nmop-network-anomaly-lifecycle-03
- draft-ietf-nmop-network-anomaly-semantics-03

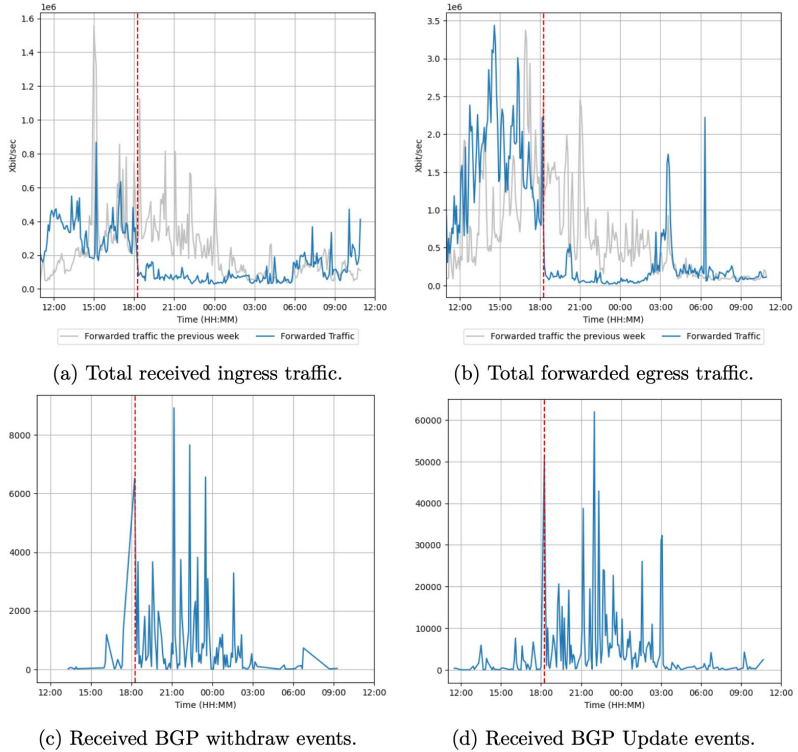
# Thanks for your attention!

Contacts

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

# Other Case Studies

# Case Study: Chile Blackout




(a) Total received ingress traffic.

(b) Total forwarded egress traffic.

(c) Received BGP withdraw events.

(d) Received BGP Update events.

Figure 3.12: Operational metrics at Swisscom during the Chile blackout.

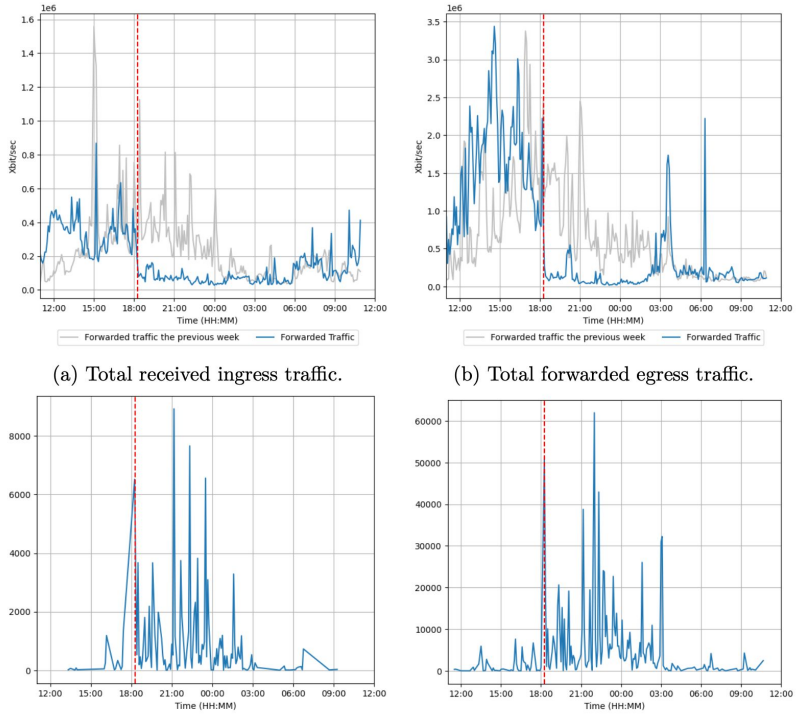
Timeline

- Power blackout started at 15:16 Chile Local Time (18:16 UTC) on 25 February 2025
- Outage solved by early morning the next day (03:00–06:00 UTC)

Observations:

- Not great amount of forwarded towards Swisscom, however, outage noticeable
- Spikes in BGP events (both updates and withdrawals)

# Case Study: Chili Blackout



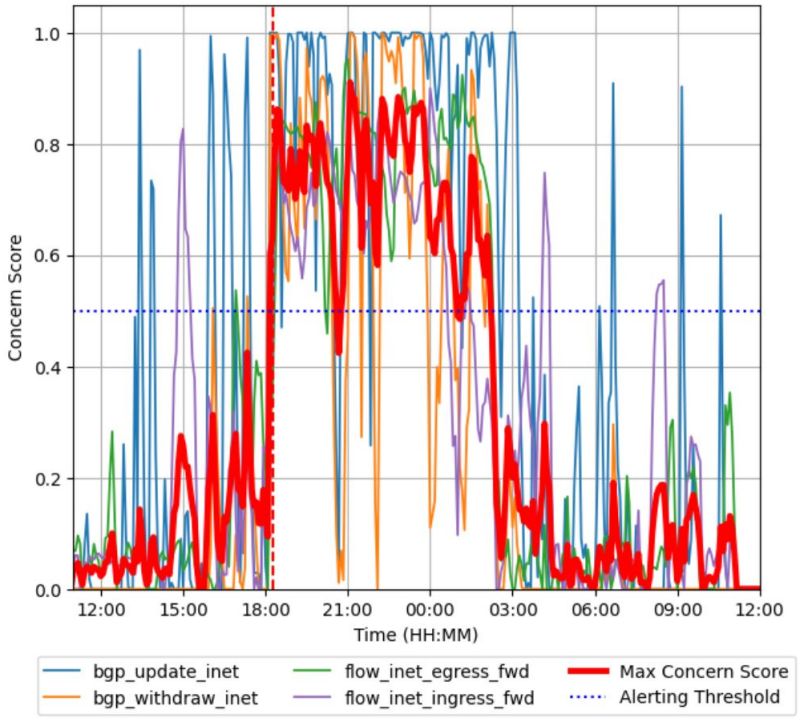

(a) Total received ingress traffic.

(b) Total forwarded egress traffic.

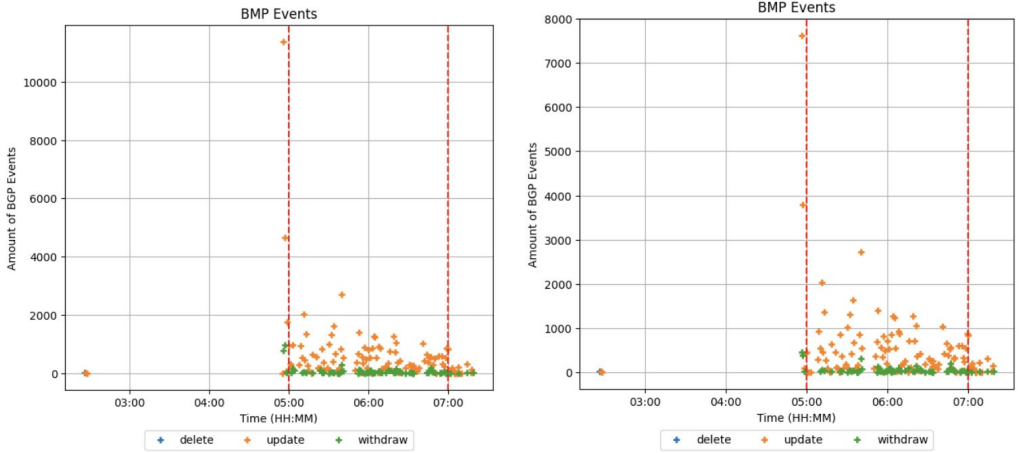
(c) Received BGP withdraw events.

(d) Received BGP Update events.

Figure 3.12: Operational metrics at Swisscom during the Chile blackout.



# Case Study: Bouygues Telecom disruption




(a) BGP events received from AS 5410.



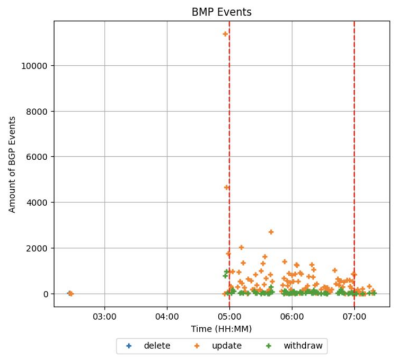

(b) BGP events received from AS 12844.

- On March 11th, between 5am–7am, Bouygues experimented a major service disruption impacting mobile and Internet nationwide

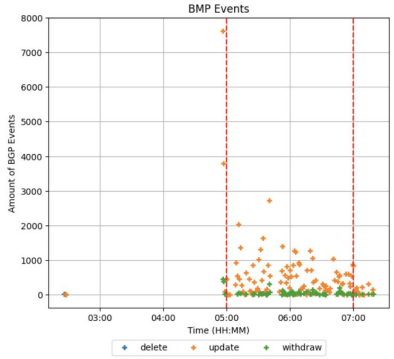
Observations:

- Swisscom does not have representative IPFIX flows (not a lot of flows between Swisscom and Bouygues)
- BGP control plane activity visible during the disruption (5am–7am)

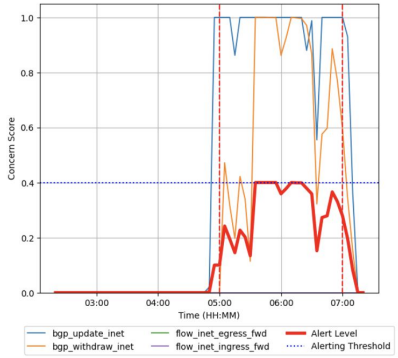
# Case Study: Bouygues Telecom Disruption



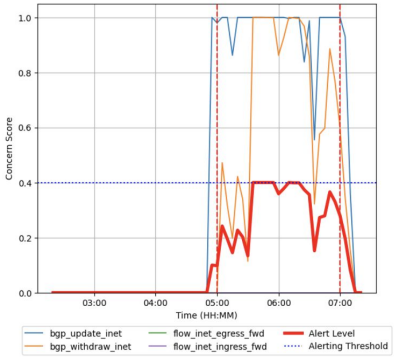

(a) BGP events received from AS 5410.




(b) BGP events received from AS 12844.




(a) Concern Scores for AS 5410.




(b) Concern Scores for AS 12844.

- On March 11th, between 5am–7am, Bouygues experimented a major service disruption impacting mobile and Internet nationwide

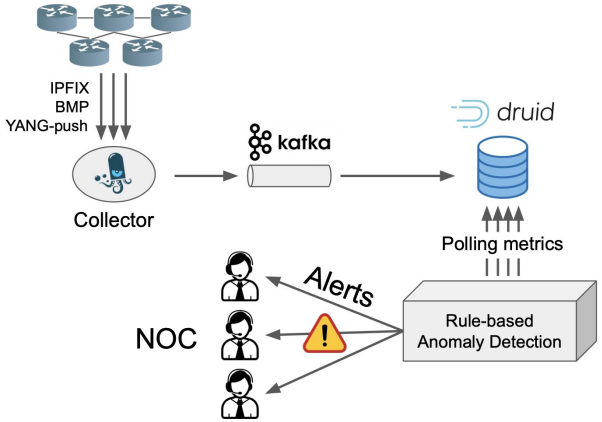
Observations:

- As there are only BGP events and no representative forwarded traffic, the resulting concern score does not increase as much as other disruptions

# Back up

# 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 for a subset of Swisscom VPN Customers
- Currently migrating to Streaming mode




** 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)