An Architecture for a Network Anomaly Detection Framework

draft-ietf-nmop-network-anomaly-architecture-01

Motivation and architecture of a Network Anomaly Detection Framework
and the relationships to other documents describing
network symptom semantics and network incident lifecycle

wanting.du@swisscom.com
pierre.francois@insa-lyon.fr
thomas.graf@swisscom.com
vincenzo.riccobene@huawei-partners.com
alex.huang-feng@insa-lyon.fr

26. October 2024

Problem Statement and Motivation

How it is being addressed in which document

Network Anomaly Detection

When operational or configurational changes in connectivity services are happening, the objective is to detect interruption at network operation faster than the users using those connectivity services

In order to achieve this objective, automation in network monitoring is required. This automation needs to monitor network changes holistically by monitoring all 3 network planes simultaneously and detect whether that change is service disruptive.

Through network incidents postmortems we network operators learn and improve so does network anomaly detection and supervised and semi-supervised machine learning. With more and more incidents the postmortem process demands automation and with the standardization of labeled network incident collaboration among network operators, vendors and academia is facilitated.

- draft-ietf-nmop-network-anomaly-architecture describes the motivation and architecture and the relationship to other two documents.
- draft-netana-nmop-network-anomaly-semantics defines Symptom semantics to enable standardized data exchange to validate results with network engineers and improve supervised and semi-supervised machine learning systems.
- draft-netana-nmop-network-anomaly-lifecycle describes on managing the lifecycle process, in order to facilitate network engineers to interact with the network anomaly detection system to refine the detection abilities over time.

An Architecture for a Network Anomaly Detection Framework

Status and Next steps

Deployment Status

- Cosmos Bright Lights streaming based implementation deployed in Swisscom production environment. Service auto profiling successfully deployed. Monitoring >12'000 L3 VPN's.
- Bell Canada data processing chain is operational. Preparations for deployment started.

Deployment Next Steps

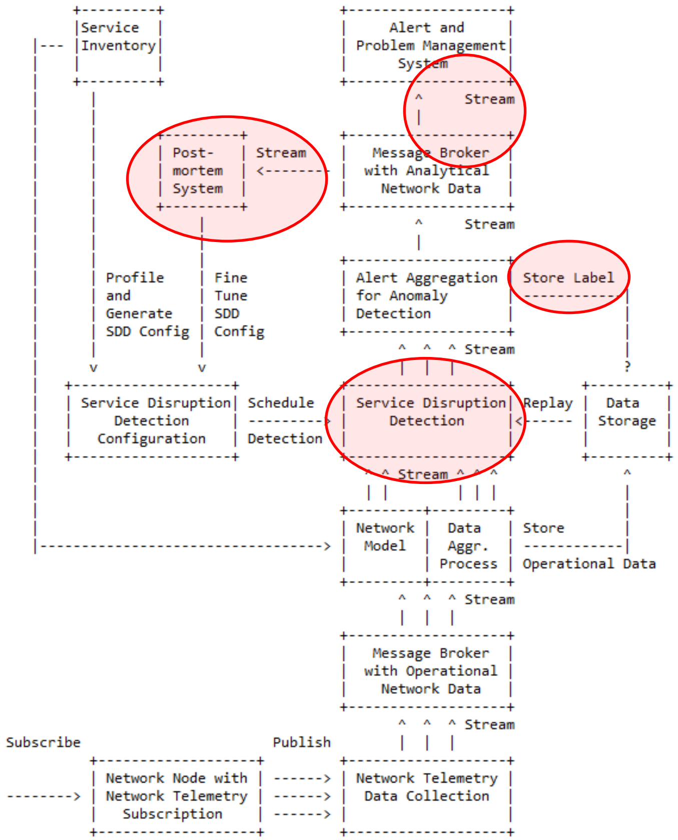
- Preparing code for Bell Canada deployment. Code refactoring according to latest annotation and notification semantics.
- Continue search for other network operators interested in collaboration and co-development.

Document Status

- Knowledge Graph references for rule in section 2.3 and symptom definitions in section 2.4.2 were added as per request from Nacho.
- Merged editorial updates from Qin in section 1.2.
- Merged terminology input from Adrian in regard to "network topology state" vs. "network state", "alert" vs. "alarm" and "component" vs. "resource" to be aligned with draft-ietf-nmop-terminology.

Document Next Steps

- **-> Incorporate already received feedback from Michael and look forward for feedback from Nacho on Knowledge Graph related changes.**



Semantic Metadata Annotation and Anomaly Lifecycle

Status and Next steps

Deployment Status

- Antagonist PoC at IETF 121 hackathon, https://github.com/vriccobene/antagonist
  -> See NMOP presentation in the afternoon.

Deployment Next Steps

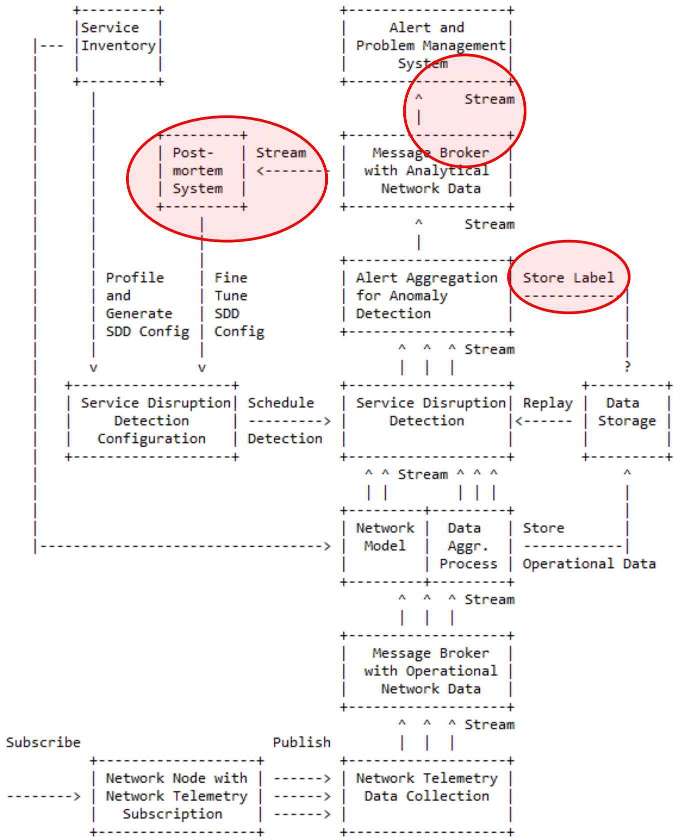
- Antagonist code refactoring according to latest annotation and notification semantics and deployment in Swisscom lab environment.

Document Status

- Merged terminology input from Adrian "alert" vs. "alarm" and "occurrence"
- Updated YANG module with relevant-state container and notification augmentations to enable a structured and extensible YANG module tree.
  -> See next slides for details.

Document Next Steps

- -> Conversation with draft-ietf-nmop-network-incident-yang authors on "incident-info grouping" and "incident-notification notification" in relation to draft-ietf-nmop-terminology-05#figure-3 workflow diagram to **align on a generic "Occurrence" and "Relevant State" container notification structure.** See relevant-state-notification notification and relevant-state container in ietf-relevant-state YANG module of draft-netana-nmop-network-anomaly-lifecycle for reference.
- Conversation with draft-havel-nmop-digital-map authors on currently defined YANG nodes in "ietf-network-anomaly-service-topology" where to augment to.
  -> See next slides for details.



Semantic Metadata Annotation for Network Anomaly Detection

draft-netana-nmop-network-anomaly-semantics

Goal: Enable the exchange of labelled dataset between operators, vendors and academia

- **Augments symptom-grouping in ietf-relevant-state** used in relevant-state-notification notification and relevant-state container defined in [draft-netana-nmop-network-anomaly-lifecycle]().
- **Observed Symptoms** as in Action, Reason, Cause semantic triplet described in Section 3 of [draft-netana-nmop-network-anomaly-semantics]().
- **Network Plane relation** as described in Section 2.4.1 of [draft-ietf-nmop-network-anomaly-architecture]().

```
module: ietf-network-anomaly-symptom-cbl

  augment /rsn:relevant-state/rsn:anomalies/rsn:symptom:
    +--rw action?              string
    +--rw reason?              string
    +--rw cause?               string
    +--rw (plane)?
       +--:(forwarding)
       |  +--rw forwarding?    empty
       +--:(control)
       |  +--rw control?       empty
       +--:(management)
          +--rw management?    empty
  augment /rsn:relevant-state-notification/rsn:anomalies/rsn:symptom:
    +-- action?              string
    +-- reason?              string
    +-- cause?               string
    +-- (plane)?
       +--:(forwarding)
       |  +-- forwarding?    empty
       +--:(control)
       |  +-- control?       empty
       +--:(management)
          +-- management?    empty
```

Semantic Metadata Annotation for Network Anomaly Detection

draft-netana-nmop-network-anomaly-semantics

Goal: Should relate to existing service and network topology YANG modules to enable topology visualization.
Repository: [ietf-network-anomaly-service-topology%402024-10-18.yang]()

- **Augments service-grouping in ietf-relevant-state** used in relevant-state-notification notification and relevant-state container defined in draft-netana-nmop-network-anomaly-lifecycle.
- **Observed Service connectivity** service. Relate to connectivity service topology YANG nodes.
- **Observed network topology**. Relate to peer and next-hop IP address and node and interface id YANG nodes.

```
module: ietf-network-anomaly-service-topology

  +--ro service!
     +--ro id
     |       yang:uuid
     +--ro smtopology:vpn-service-container
     |  +--ro smtopology:vpn-service* [vpn-id]
     |     +--ro smtopology:vpn-id        string
     |     +--ro smtopology:vpn-name?     string
     |     +--ro smtopology:site-ids*     string
     +--ro smtopology:vpn-node-termination-container
        +--ro smtopology:vpn-node-termination*
      [hostname route-distinguisher]
           +--ro smtopology:hostname       inet:host
           +--ro smtopology:route-distinguisher     string
           +--ro smtopology:peer-ip*
           |       inet:ip-address
           +--ro smtopology:next-hop*
           |       inet:ip-address
           +--ro smtopology:interface-id*int32
```

Experiment: Network Anomaly Lifecycle

draft-netana-nmop-network-anomaly-lifecycle

« Network Anomaly Detection is an iterative process that requires continuous improvement »

```
4.  Lifecycle of a Network Anomaly

   The lifecycle of a network anomaly can be articulated in three
   phases, structured as a loop: Detection, Validation, Refinement.

                                  +-------------+
                     +---------> |  Detection  | ---------+
           Adjustments |          +-------------+          | Symptoms
                       |                                   |
                       |                                   v
               +------------+                       +------------+
               | Refinement |<--------------------- | Validation |
               +------------+        Incident       +------------+
                                   Confirmation

                 Figure 1: Anomaly Detection Refinement Lifecycle

   Each of these phases can either be performed by a network expert or
   an algorithm or complementing each other.
```

Detection: The Network Anomaly Detection stage is about the continuous monitoring of the network through Network Telemetry [RFC9232] and the identification of symptoms.

Validation: Decides if the detected symptoms are signaling a real incident or if they are to be treated as false positives.

Refinement: Network operator performs detailed postmortem analysis of the network incident, collected Network Telemetry data and detected anomaly with the objective to identify useful adjustments in the Network Telemetry data collection and Anomaly Detection system.

Experiment: Network Anomaly Lifecycle

draft-netana-nmop-network-anomaly-lifecycle

Goal: A generic relevant-state container, anomaly and annotator groupings.

- **Defines** relevant-state-notification notification and relevant-state container with unique id and start and end time of relevant-state.
- **Anomalies** provides unique id and start and end time of the anomaly with a confidence score. **Pattern** describes the identified pattern of the anomaly.
- **Annotator** describes wherever the anomaly was detected by a human or algorithm and uniquely identifies the entity who/which detected.
- **Symptoms and Service** provides unique id and a concern score.

```
module: ietf-relevant-state
+--rw relevant-state
  +--rw id  yang:uuid
  +--rw description?    string
  +--rw start-time      yang:date-and-time
  +--rw end-time?       yang:date-and-time
  +--rw anomalies* [id version]
      +--rw id        yang:uuid
      +--rw version      yang:counter32
      +--rw state        identityref
      +--rw description?  string
      +--rw start-time     yang:date-and-time
      +--rw end-time?      yang:date-and-time
      +--rw confidence-score            score
      +--rw (pattern)?
      |  +--:(drop)
      |  |  +--rw drop?   empty
      |  +--:(spike)
      |  |  +--rw spike?  empty
      |  +--:(mean-shift)
      |  |  +--rw mean-shift?          empty
      |  +--:(seasonality-shift)
      |  |  +--rw seasonality-shift?         empty
      |  +--:(trend)
      |  |  +--rw trend?  empty
      |  +--:(other)
      |     +--rw other?  string
      +--rw annotator!
      |  +--rw name      string
      |  +--rw (annotator-type)?
      |     +--:(human)
      |     |  +--rw human?          empty
      |     +--:(algorithm)
      |        +--rw algorithm?     empty
      +--rw symptom!
      |  +--rw id           yang:uuid
      |  +--rw concern-score            score
      +--rw service!
        +--rw id         yang:uuid
```

Relevant Papers for more Details

Practical Anomaly Detection in Internet Services: An ISP centric approach

Alex Huang Feng*, Pierre Francois*, Kensuke Fukuda‡, Wanting Du†, Thomas Graf†, Paolo Lucente§, Stéphane Frénot*

*INSA Lyon, Inria, CITI, UR3720, Villeurbanne, France
alex.huang-feng@insa-lyon.fr, pierre.francois@insa-lyon.fr, stephane.frenot@insa-lyon.fr
‡National Institute of Informatics, Tokyo, Japan
kensuke@nii.ac.jp
†Swisscom, Zurich, Switzerland
wanting.du@swisscom.com, thomas.graf@swisscom.com
§pmacct.net, Barcelona, Spain
paolo@pmacct.net

***Abstract*—Identifying anomalies in a network is a crutial endeavor for Internet Service Providers (ISPs). Anomalies that impact the traffic of the ISP customers can lead to a degradation in the reputation of the company. Moreover, silent anomalies that do not break connectivity can impact the revenue and business of ISPs. Therefore, monitoring and anomaly detection has become essential for ISPs. In this paper, we present an ongoing research project aimed at identifying anomalies in Internet services provided by an ISP. We aim at detecting anomalies within the domain managed by the ISP that impact the customers and the business of the ISP. We propose a rule-based approach designed to promptly detect and provide reporting for such anomalies in near real time, giving information that allows the operator to identify whether a solution can be brought. In this paper, we describe the collected network telemetry metrics and illustrate how they are processed using open-source solutions. We introduce a set of use cases showing that an ISP can monitor Internet services using IETF standard metrics.**

I. Introduction

Internet services include providing global Internet reachability for customer Autonomous Systems (ASes) connected to an Internet Service Provider (ISP) and serving private customers within the ISP (e.g. FTTH). Disruptions in the network that affect the connectivity of an ISP not only significantly degrade the organization's reputation but also have implications on the company's revenue. Customers subscribed to Internet services depend on the ISP peerings to reach the Internet and an incident between them and the Internet can have detrimental implications for their business.

Today, routing between different ASes is established using BGP [1]. ISPs managing an AS configure policies in their routers based on the business relationship they have with their neighboring ASes. Generally, ISPs classify their BGP neighbors into Customers, Settlement-free Peers and Transit Providers. Customer ASes compensate the ISP to reach the Internet, Settlement-free peers are mutual arrangements between two ISPs to exchange Internet traffic without any financial compensation and Transit Providers provide access to the global Internet.

ISPs rely on collected BGP messages and traffic counters to monitor peerings and detect anomalies that could impact their customers. They closely supervise network traffic to identify unexpected patterns or potential abuses by peers. This underscores the importance for ISPs to receive prompt alerts when anomalous or unwanted traffic behaviors occur, enabling network operators to rapidly implement solutions and address the detected issues.

Anomaly detection (AD) has been a hot topic in the last decade where researchers have proposed new ways to detect irregularities in the data. Most research projects aiming at detecting anomalies in BGP networks use public repositories such as Routeviews and RIPE NCC archives [2, 3], allowing researchers to identify problems in Internet from a global point of view. In conjunction with publicly known incidents, researchers have been able to develop methods to detect anomalies in data from the public domain, with a focus on detecting anomalies in the global Internet topology [4, 5].

Simulated environments mimicking the deployed network and manually generated anomalies have also been used to test anomaly detection [6]. Very few projects use production data coming from an ISP to detect anomalies and root cause analysis within a single domain. AD within an AS have only been investigated by very few researchers having access to production data [7]–[9].

In this paper, we focus on detecting anomalies within a single AS to potentially help them fixing their configuration and find unwanted traffic flows impacting their business. We describe the target use cases in Section II. Instead of solely using BGP activity as a source of data, as done in [7], we use a larger set of monitoring information, allowing us to cover a broader set of service anomalies (Sec. III-A). The authors in [8] focus on detecting performance issues from end-to-end users, while the work presented in this paper also covers anomalies impacting the traffic from peerings. In [9], anomaly detection is based on traffic information with a focus on network intrusion detection, while the project presented

Paper "**Practical Anomaly Detection in Internet Services: An ISP centric approach**"
Published at AnNet Workshop (In conjunction with IEEE NOMS)
Seoul, South Korea (6–10 May 2024)
Open access: https://hal.science/hal-04655324

Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks

Alex Huang Feng
alex.huang-feng@insa-lyon.fr
Univ Lyon, INSA Lyon, Inria, CITI, EA3720
Villeurbanne, France

Pierre Francois
pierre.francois@insa-lyon.fr
Univ Lyon, INSA Lyon, Inria, CITI, EA3720
Villeurbanne, France

Stéphane Frenot
stephane.frenot@insa-lyon.fr
Univ Lyon, INSA Lyon, Inria, CITI, EA3720
Villeurbanne, France

Thomas Graf
thomas.graf@swisscom.com
Swisscom
Zurich, Switzerland

Wanting Du
wanting.du@swisscom.com
Swisscom
Zurich, Switzerland

Paolo Lucente
paolo@pmacct.net
pmacct.net
Barcelona, Spain

ABSTRACT

We present an architecture aimed at performing Anomaly Detection for BGP/MPLS VPN services, at scale. We describe the challenges associated with real time anomaly detection in modern, large BGP/MPLS VPN and BGP/IPv6 Segment Routing VPN deployments. We describe an architecture required to collect the necessary routing information at scale. We discuss the various dimensions which can be used to detect anomalies, and the caveats of the real world impacting the level of difficulty of such anomaly detection and network modeling. We argue that a rule-based anomaly detection approach, defined for each customer type, is best suited given the current state of the art. Finally, we review the current IETF contributions which are required to benefit from a fully open, standard, architecture.

ACM Reference Format:
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 *Applied Networking Research Workshop (ANRW '23), July 24, 2023, San Francisco, CA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3606464.3606470

ANRW '23, July 24, 2023, San Francisco, CA, USA

ACM ISBN 979-8-4007-0274-7/23/07…$15.00
https://doi.org/10.1145/3606464.3606470

1 INTRODUCTION

Customers subscribing to BGP/MPLS VPN services usually come along with stringent Service Level Agreements. Consequently, Service Providers must be capable of detecting anomalies in their services in a timely fashion, while accommodating for scale. Around 10 thousand L3 VPNs in our Swisscom use case. Long-lasting outages, detected by the customer before the service provider, are detrimental to the perception of service quality, and may dramatically impact the customer business.

The goal of the presented architecture is to provide an anomaly detection solution that scales while being flexible on the following aspects: (i) the dimensions that must be used to detect anomalies are multiple; (ii) VPN customers wear different profiles in terms of normal and abnormal values for such dimensions; (iii) the amount of information collected to produce values for such dimensions is extremely large in such deployments: around 175 thousand messages/second in our use case; (iv) the operating costs for managing an anomaly detection solution must be kept low; and (v) the networking platforms providing the service may come from different vendors and have different monitoring capabilities.

The remainder paper is structured as follows. In section 2, we define what is considered a network anomaly and present the associated challenges behind its detection. In Section 3, we describe the Daisy architecture. In Section 4, we review the ongoing IETF efforts aimed at filling the gaps for a fully open, standard, Anomaly Detection (AD) implementation. And finally, in section 5, we present the first results of Daisy deployment at Swisscom.

2 PROBLEM STATEMENT

We describe some of the challenges associated with customer diversity, and a non-exhaustive list of anomalies targeted by the base recipes from our limited proof of concept deployment setup.

1

Paper "**Daisy: Practical Anomaly Detection in large BGP/MPLS and BGP/SRv6 VPN Networks**" published at ACM/IRTF ANRW'23
San Francisco, USA (24 July 2023)
Open access: http://hal.science/hal-04307611