Birdf meeting task 10

March 20 2023

Ron Insler – Rad Data Communication

Project 3 tasks 10– Multilayer anomaly detection sub task Communications network features

Your Network's Edge®

- Focus on efficient measurement, detection, and reporting of networking features
- Problems addressed:
  - Partners will define needed networking parameters
  - RAD has extensive expertise in OAM and fault isolation
- Research directions:
  - Adaptation of conventional mechanisms
  - Big data collection
  - Edge aggregation, thresholding/triggering, reporting
- Feature extraction in pluggable devices (MiSec)
- Define the KPI's to collect
  Define the algorithm for anomaly
  Focus on efficient measurement, detection, and reporting of networking features
- Deliverable –product on SFP and product running on compute

Task 10 current activities in progress until March 2023

Your Network's Edge®

- Define network KPIs to be used as features for ML anomaly detection mechanism: RTT, packet rate, % loss, packet delay variations, time of day – Completed
- Exploratory data analysis of the KPIs – graphical representation of real network traffic to understand the underlying statistics – univariable/bivariable analysis – Completed
- Evaluate various unsupervised anomaly detection algorithms: local outlier factor, isolation forest, robust random cut forest, neural network-based methods and clustering (OPTICS). – completed
  - Calculate feature importance score
  - Automatic anomaly score threshold mechanism
  - Distinguish between "bad anomalies" and "good anomalies"
  - Identify anomalies and divide for outliers and clusters with different levels
  - Ensemble algorithm for final decision
  - Validation - In progress

- A plan for commercialization of the ideas / work plan proposed in the Task. - *the system was presented to some major customers or RAD we plan POC during this year.*
- **Collaboration** with industrial partner(s) in realizing the commercialization plan. - *Talks will start with Delek US for this solution when we will get to the LAB*
- ***Demonstration*** *: once installed in Delek US Lab the system can be demonstrated alternatively it can be demonstrated in RADs lab*
- ***Impact*** *: Detect in the OT network volumetric attack of DDOS as well as any other anomaly that observed in the network transport layer .*

ML-based network anomaly detection via 3-step approach

Your Network's Edge®

Samples of Network's features

RTT

Loss rate

Detect all anomalies ("good" and "bad")

Using Robust Random Cut Forest Algorithm
Threshold for anomaly is the x-quantile of the sample's RRCF score

Filter out "good" anomalies

A good anomaly is determined when all features are below a threshold defined by the median of each feature plus an overhead defined by a constant and a factor over the median value

Detect dense "bad" anomalies

Find dense "bad" anomalies in a short timeframe of ~1 hour
Dense bad anomalies are bad anomalies with high density in a short timeframe. Probability for dense bad anomalies are calculated by cumulative binomial distribution

Cluster data to separate anomalies

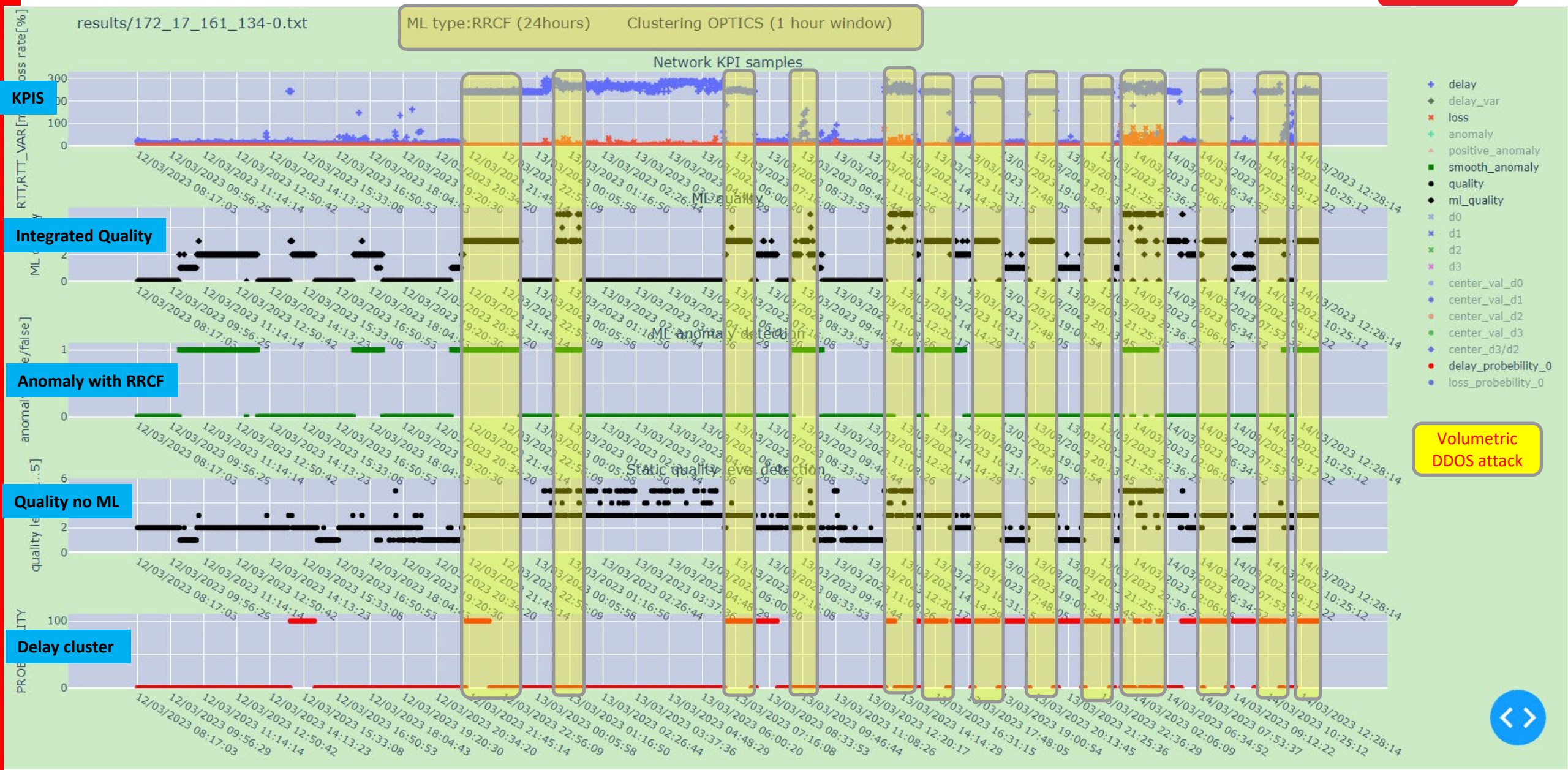
Using OPTICS algorithm to find clusters and outliers in a short timeframe of ~1 hour. The algorithm finds one cluster if there is no anomaly and two or more clusters in case of anomalies. OPTICS parameters dynamically calculated to be optimized.

Final decision of anomaly by ensemble of methods

Network degradation

Detect dense "bad" anomalies and clustering are use as ensemble methods to improve our ML results.

Simulation with Real data on the algorithm



RAD

Your Network's Edge®

Thank you

For your attention