MOBILE NETWORKS ASSURANCE: A SEA OF DATA – HOW TO NAVIGATE IT?

bwtech

Network engineers who are tasked to monitor, assure and optimize mobile networks need to have visibility over a complex and diverse set of analytics, which are generated in a continuous form by mobile network elements, or collected via different kinds of external probes.

WHICH ANALYTICS SHOULD BE ANALYZED?

Performance Management (PM)
Network counters and derived performance indicators.

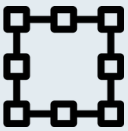
Configuration Management (CM)
Network parameters and resources.

Fault Management (FM)
Alarms generates by network elements.

Call Detailed Records (C/XDR)
Detailed records of voice or analytics call sessions.

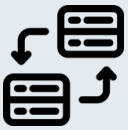
Call Traces
Detailed call logs with layer 3 messages.

Minimization of Drive Tests (MDT)
Specific call traces enriched with GPS location.



Network Probes
Hardware or software external probes aimed at collecting the signaling flow.

Drive Tests
Detailed call logs collected in the streets using dedicated software and scanners.



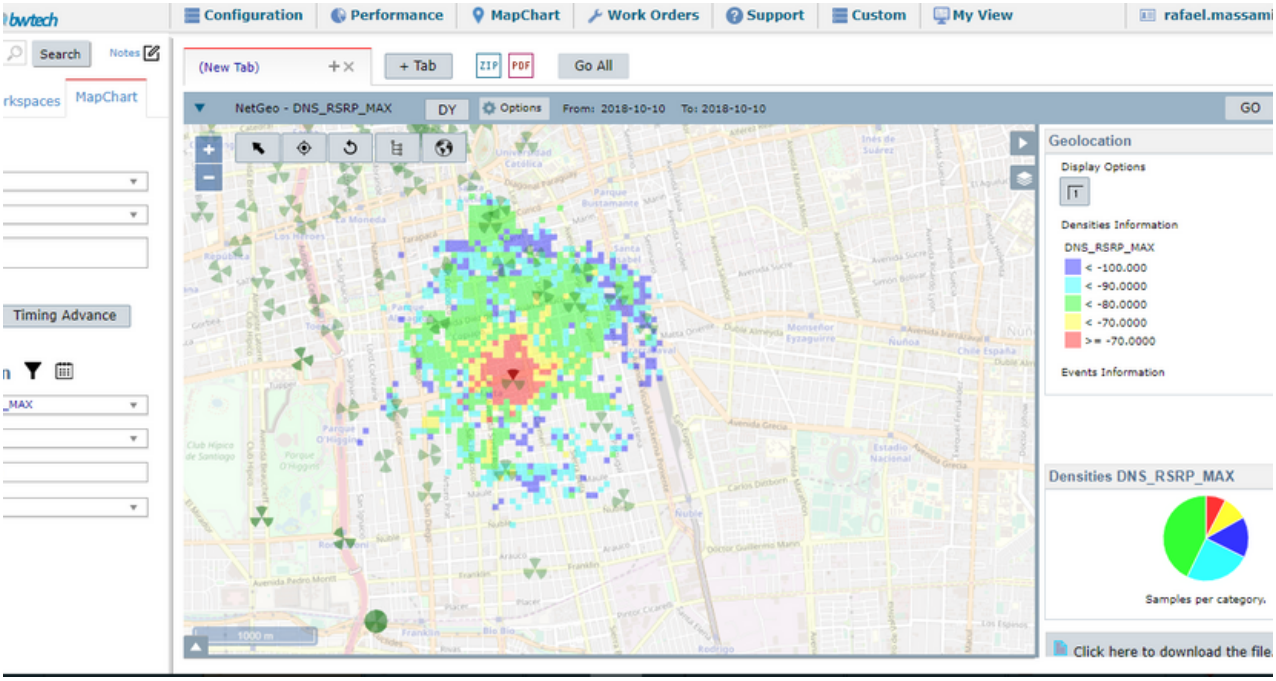
Crowdsourcing
Basic network information collected from millions of UEs via agents.

Network engineers, depending on the specific tasks and goal they have in the organization, can give different importance to a specific sets of analytics, being Performance Management and related Service Quality Management KPIs/KQIs usually a starting point for an effective network and service monitoring.

Fault Management data should also be collected in real time, then filtered and organized in order to identify alarms that are relevant for service monitoring and assurance.

Drive Test analytics have been widely used in the past to monitor users experience, however they are expensive to collect and non-comprehensive; in addition, they do not capture the main traffic of current mobile networks, that are indoor users.

Geolocation data based on Call Traces are used as a valid replacement of Drive Tests, recently enhanced by MDT and crowdsourcing analytics. These data provide in a cost effective manner a comprehensive view of network and subscribers analytics.



Configuration Management is a set of essential data, not always properly collected and effectively used by network engineers.

Proper monitoring of network parameters, as well as license management control are of paramount importance, as the incident involving Ericsson Core network license expiration that happened in O2 UK in December 2018[1] has shown.

A major reason for the outage has been related with the expiration of license certificates in the SGSN-MME (Serving GPRS Support Node - Mobility Management Entity), which triggers an automatic shutdown of the equipments for security purposes.

Even though operators have legal and SLA agreements with equipment providers that should assure full functioning and license renewal of critical network elements, mobile operators themselves should take an active approach in setting up an internal monitoring and warning system to prevent license expiration issues.

Finally, X/CDR data can also be collected and analyzed by network assurance engineers, enhancing the network analytics provided by PM/CM/SQM data, with the subscribers performance and behaviors provided by the XDR data.

[1] https://www.bbc.com/news/business-46499366

AUTOMATING DATA GATHERING

Not only the potential sources of analytics are so diverse in nature, but on top of this different equipment vendors generate row data in different formats (XML, binary, etc), with different granularity (hourly, 15 mins) using different network protocols (SNMP, CORBA, etc).

A first and foremost priority is therefore to automate the network data gathering, processing and storing to avoid engineers spending most of their time in data handling, while they should be focusing on analysis and insights.

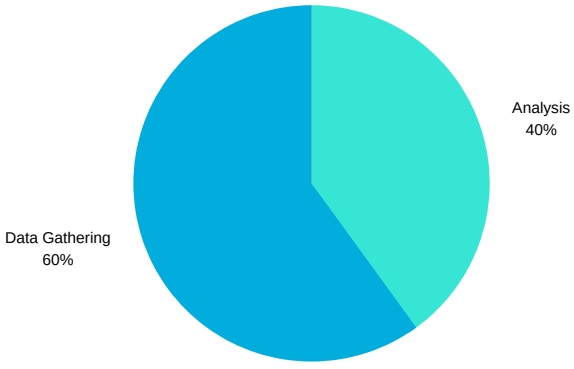
This can only be achieved using multi-vendor network data collection platforms, that are continuously adapted and updated to different vendors formats, and that continuously improve the process of data handling, through efficient parsing and streaming technologies.

This update process should happen in the background, engineers should not be involved at all in the process.

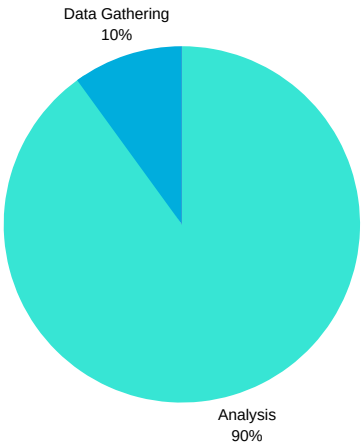
Not enough emphasis is given to this aspect when network engineering teams select their tools for network assurance, troubleshooting and optimization. A lot of focus and interest is given to tools features and functionalities, but what if engineers need to spend most of their day in the administration of the tools? Features are great, but the whole data gathering and processing should be considered as one of the key attributes in the selection of the best tool.

AMOUNT OF TIME SPENT ON EACH TASK:

Without automation tools:



With automation tools:



ANALYTICS CORRELATION

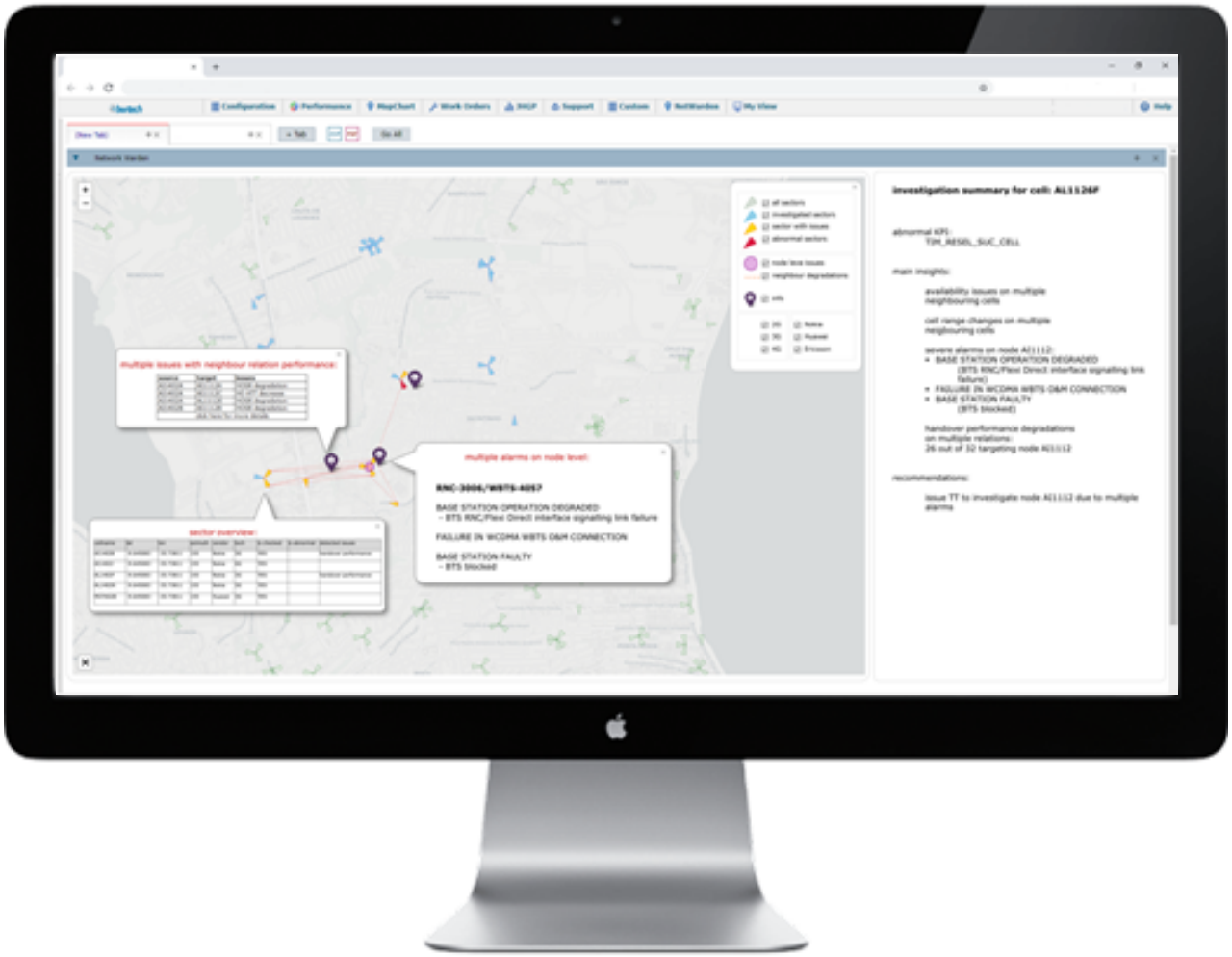
Once data are collected and stored, it is paramount for network engineers to have the capability to correlate all these network analytics, in order to gain real insights on possible root causes of network issues, correlate network issues with subscriber experience and eventually be able to take meaningful actions for QoE improvement.

This can be achieved only if all the analytics are centralized in just one consolidated platform, that is today a major challenge for mobile service providers who have been implementing along the years separated tools for different analytics type or even for different vendors.

Once data collection is automated, all analytics are consolidated in one platform and therefore can be correlated, engineers need smart ways to navigate through the sea of analytics.

BASIC CORRELATIONS OF NETWORK DATA MAY INCLUDE:

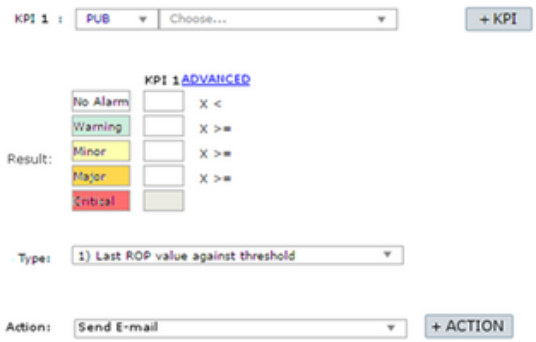
- Performance degradation/improvement and alarms increase/decrease
- Performance degradation/improvement and parameters changes
- Correlations between different KQIs and KPIs, for instance performance degradation/improvement and traffic increase/decrease
- Correlation between network KPIs and QoE measured via XDRs
- Network performance degradation/increase and subscribers analytics measured via crowdsourcing
- Geographical correlation of network performance and alarms



SMART WAYS TO MAKE USE OF ANALYTICS

One common way to facilitate the monitoring and assurance tasks is through the implementation of soft alarms, which are triggered with a key indicator reaches a pre-defined threshold. Ideally, this action should trigger automatically the correlation of the key indicator with other network analytics, such as physical alarms (FM) or parameter changes.

However, soft alarms are complex to set up and manage, given the high complexity of current networks, where different domains, vendors and even geographical areas would request different threshold settings. In addition, thresholds should be dynamic, in order to accommodate for the always changing network configuration.

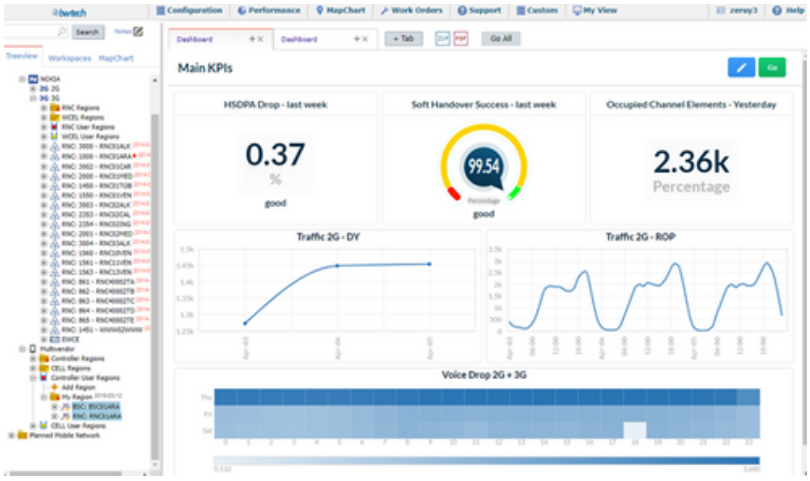


A new, smarter way of facilitating network monitoring is making use of Anomaly Detection algorithms based on Machine Learning. Instead of setting specific thresholds, the algorithms automatically learn what is a normal behavior for a given Key Performance Indicator and automatically reports when the behavior becomes abnormal.

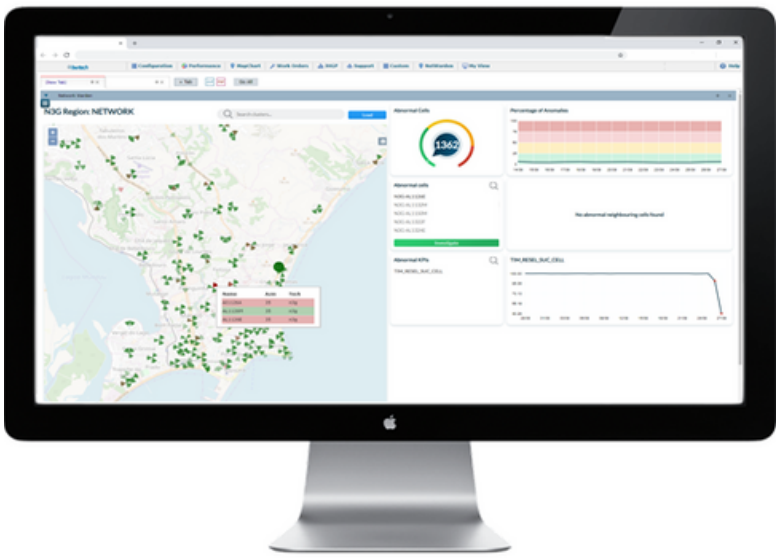
Once the Anomaly is spotted, an automatic correlation with other indicators or analytics sources should be generated, to support the engineer providing the proper information for problem resolution. Machine Learning techniques should be used at this stage to enhance the correlation algorithms and to provide novel and useful insights to network engineers.

Finally, it is very important for network engineers to implement a smart way to visualize all his analytics.

One option is to pre-define correlation dashboards based on the priorities, in terms of KQIs/KPIs and monitored services of each network engineer.



Another option is to visualize anomalies and correlated analytics in a map, or a combination of dashboard and map.



Analytics dashboards should be working in almost real time, in order to solve the network and service issues before their impact becomes significant for the subscribers experience.

HOW BWTECH SOLVES THE NETWORK ANALYTICS CHALLENGES

Bwtech is the global expert in gathering, processing and visualizing network analytics for network assurance.
Our monitoring and optimization platform, NetChart, is a single user interface, cloud-based, multi-vendor and multi-technology, real-time, monitoring and optimization system.

NetChart addresses the challenge of dealing with modern and hugely complex mobile networks that generate vast and diverse volumes of data, providing advanced network analytics and the correlation of various network data sources, such as counters, parameters, inventory, alarms, CDRs, traces and drive test with each other.

For more information, feel free to contact our marketing and sales team at hello@bwtech.com

https://www.bwtech.com/