Network Automation and Data Analytics in 3GPP 5G Systems

Miguel A. Garcia-Martin*, Marco Gramaglia†, and Pablo Serrano†.
*Ericsson, Spain
†University Carlos III of Madrid, Spain

***Abstract*—We are witnessing an "automation revolution" in mobile networking, thanks to the development of Artificial Intelligence (AI) techniques. These require vast amounts of data, which for the case of mobile networking are typically collected and stored using proprietary procedures, a methodology that precludes a faster development of AI and its adoption by network operators. The first release (Release 15) of the 5th generation of mobile networks (5G) addressed this challenge by introducing a novel standards framework for data analytics. Its cornerstone is the *Network Data Analytics Function (NWDAF)*, whose main purpose is to issue network analytic reports, which can be used by Network Function (NF)s to take automated decisions. While in Release 15 the use of NWDAF was limited to a single use case, in Release 16 more functionalities are added, extending the number of use cases and confirming that 5G is embracing automation. This paper provides an overview of the ecosystem, empowered by the data analytics architecture, discussing its functionality, and use cases enabled by the NWDAF and the other enablers for network automation in Release 16, highlighting the extensions recently added in Releases 17 and 18.**

I. Introduction

The operation of mobile networks is embracing automation, which supports the efficient operation of multi-service and multi-tenant 5G networks. A key requirement of automation is the availability of data to support Artificial Intelligence (AI) operations, e.g., model training and forecasting.

Although monitoring tools have been required in networks since day one, the analysis of the monitoring data has been traditionally *detached* from the operation and performed *a posteriori*, in an offline manner (e.g., billing). In contrast to this approach, 5G envisions that the analysis is done in *real-time* as part of the network operation procedures. The softwarization of the network, and the associated increased complexity, motivates the use of a centralized and standardized view of the analytics to scale for the large number of heterogeneous use cases envisioned in 5G and beyond [1].

The architecture of 5G automation is specified in 3GPP TS 23.288 [2], which defines the modules, interfaces, and semantics of the data analytics. The cornerstone of this ecosystem is the Network Data Analytics Function (NWDAF), firstly specified in Release 15 (R15), which is the hub for all the agents that produce and consume data analytics: the analytic services are specified in 3GPP TS 29.520 [3], while the specific messages sequences for a full data-driven operation of the network are specified in TS 29.552 [4]. This analytics framework is not *exhaustive*, i.e., it can be complemented and integrated with additional proprietary functionality (outside the scope of this paper).

TABLE I: Acronym list

Acronym	Definition
5GC	5G Core Network
5QI	5G QoS Identifier
AF	Application Function
AMF	Access and Mobility management Function
ADRF	Analytics Data Repository Function
AnLF	Analytics Logical Function
DNAI	Data Network Access Identifier
DNN	Data Network Name
LADN	Local Area Data Network
LCS	Location Services
MDAF	Management Data Analytics Function
MFAF	Messaging Framework Adaptor Function
MTLF	Messaging Framework Adaptor Function
NEF	Network Exposure Function
NRF	Network Repository Function
NS	Network Slice
NSACF	NS Access Control Function
NSI	NS Instance
NSSF	NS Selection Function
NWDAF	Network Data Analytics Function
OAM	Operations, Administration and Maintenance
PCF	Policy Control Function
PFD	Packet Flow Description
PLMN	Public Land Mobile Network
RAN	Radio Access Network
RAT	Radio Access Technology
SBI	Service Based Interface
SMF	Session Management Function
S-NSSAI	Single Network Slice Selection Assistance Information
SUPI	Subscription Permanent Identifier
TAI	Tracking Area Identity
UDM	Unified Data Management
UE	User Equipment
UPF	User Plane Function

In this paper, we overview the 3GPP standardization work on Network Automation and Data Analytics, from Release 15 (R15) up to R18. First, we present the overall framework in Section II, reviewing the role of Data Analytics and explaining the design assumptions. Then, in Section III we detail the analytics production and consumption strategies specified by 3GPP. In Section IV we specify the different kinds of analytics specified by 3GPP, along with some examples. Finally, we conclude the paper by summarizing the novelties introduced in R17 and R18 in Section V.

II. Network Automation Framework

The need for network automation guided the design of the 3GPP system standardized in R15. Before this release, the generation of data and analytics from the network typically

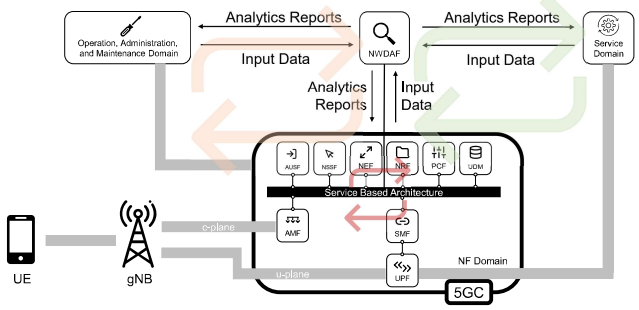

Fig. 1: Feedback loops enabled by the NWDAF analytics

consisted of exchanges between network elements and their corresponding managers using proprietary interfaces. With R15 and the further consolidations in the subsequent releases, the architecture has been re-designed to natively support the collection of analytics that can be eventually leveraged, as we explain in the following, to provide feedback loops either by standard or proprietary solutions. The cornerstone of this system is the NWDAF, that (i) gathers data (i.e., metrics related to the current status of the network), coming from other producer NFs; (ii) computes analytics, i.e., refined statistics based on the gathered data; and (iii) shares them with other consumer functions in the network.

These analytic reports provide as output either statistics based on past data or a prediction for a certain metric, depending on whether the requested period of time is in the past or in the future, respectively. Both outcomes are used to optimize the operation of NFs. The output may also include a `confidence` parameter (between 0 and 100) which conveys information about the certainty of the prediction made, and may be based on the amount of data used to generate the prediction, the AI model age, etc.

A. Automation domains and loops

The overall framework for network automation is illustrated in Figure 1. NWDAF is the hub for different spokes that connect several analytics in the system, which is split into three different domains (top of the figure).

The first reference domain is **5GC**, where the NWDAF resides. The main producers and consumers of data and analytics are the other NFs of the core, that use them to operate the network in a data-driven way. Thanks to the NWDAF, consumer NFs do not contact all the possible producers to compute analytics, effectively re-using information.

The second domain is **OAM**, performed by modules such as the Element Managers or the Network Elements in pre-5G networks. From R15 onward, OAM effectively enforces network slicing through SBMA [5]. The OAM domain can also feed the NWDAF with data obtained from the RAN and from 5G NFs (e.g., resource consumption), since the pre-5G 3GPP RAN architecture does not have an analytics hub such as NWDAF (other architectures such as O-RAN [6] feature analytics-specific modules). The module in charge of the interaction with the NWDAF is the Management Data Analytics Function (MDAF) which provides the Management Data Analytics Services (MDAS). As discussed, the MDAF interacts with the NWDAF and other core NFs to produce management analytics information that, in turn, are consumed by other NFs or by other management procedures such as the SON.

Finally, the third domain is the **service domain**, via the Application Function (AF). These functions (outside the 3GPP trust domain) are critical for the envisioned tight interaction between the service provider and the network operator by means of enriched *service layers*, that help to *commoditize* the network and enhance the interaction between the service and the network intelligence. Clearly, authorization and security are critical, to check whether AFs are duly authorized to interact with the NWDAF and can hence exchange data with third parties.

Overall, any NF deployed within the 5GC, the OAM system, or any AF, can provide input to the NWDAF and can request analytic reports from the NWDAF. As a result, a feedback loop is created, where any NF, OAM, or AF provide input data to the NWDAF and can receive analytic reports created from all the data obtained by the NWDAF. Through these loops, most of the automated operations on the network can be performed, leveraging on the analytics we present in Section IV, through the services detailed next.

III. NWDAF Services and Analytic IDs

NWDAF exposes two SBIs, which are specified in 3GPP TS 29.520 [3]. These services allow any NF, OAM, or AF to subscribe to or receive analytic reports:

- The `Nnwdaf_AnalyticsInfo` service provides a one-shot request/response operation that is useful when the consumer of the service wants to retrieve a single analytics report.
- The `Nnwdaf_AnalyticsSubscription` service provides a subscribe/notify set of operations that are useful for a longer-term timescale, i.e., a periodic reception of analytic reports.

A. Data gathering

To generate the analytics reports the NWDAF collects data from other elements in the network. The first and most common source is the other 5GC NFs, that provide information about core-related metrics. The second source is OAM, which can provide resource-related data for 5GC NFs as well as RAN related data. Finally, the NWDAF can gather data from the AF operated by the service provider to collect application-related metrics.

The way in which the NWDAF collects the data depends on the source of the information:

- If the data is collected from other 5GC NFs or AF, an SBI Event Exposure interface is used. This is the case when the data is collected from AMF, SMF, UDM, and AF. Data collection from AF may need to traverse a NEF when the AF is located outside the 5GC trusted domain.

TABLE II: Possible Targets of analytics services

Target	Identifiers
UEs	UE ID SUPI, Internal Group ID, or any UE
Areas	A set of TAI
Services	DNN
Network Functions	NF type of NF ID, or All NFs serving a SUPI

- If the data is collected from the NRF, the existing `Nnrf_NFDiscovery` and `Nnrf_NFManagement` services are used.
- If the data is collected from the UPF, 3GPP does not standardize the interface in R15, R16 or R17.
- The NWDAF collects performance measurements or 5G end-to-end KPIs from OAM using standardized performance management services and fault supervision services (e.g., utilization traces from the RAN).

B. Analytics request syntax

When a consumer NF requests analytic reports from the NWDAF, it must identify the type of requested report. This is done by supplying an `Analytics ID` to the request, an information element to uniquely identify them. R16 has standardized nine different analytics, such as "Network Performance" or "Abnormal UE Behavior" —they will be presented below in Section IV. The `Analytic ID` acts as a (de)multiplexer in the SBI service as it determines the type of information that NWDAF collects from data sources and the type of information provided in an analytics report.

The analytics consumer must also identify the `Target` of the report which, in turn, depends on the `Analytics ID`. Possible targets, as reported in Table II may be related to UEs, geographical areas of interest, or NFs. The latter category is usually built with data coming from NRF.

The consumer may also include analytics `filter information`, which contains a collection of parameters and values of interest (to filter out those of no interest), such as specific network slices, applications, areas, radio frequencies, etc. The consumer may also include analytics `reporting information`, indicating additional conditions to fulfill when producing notification reports, e.g., the maximum number of reports to be received, the maximum number of objects within a report, or threshold values to trigger a report when exceeded.

IV. Analytics

In this section, we introduce the different analytics considered in R16 and beyond, along with the data used for their generation, and potential use cases. Their interactions are summarized in Fig. 2.

A. Slice Load level

1) Definition and data gathering: The Slice Load level analytics provide information about the overall load of a NS, a NSI, or both. The NWDAF produces analytic reports including the average (and variance) of the number of UE registrations and number of PDU sessions in the slice, the resource usage belonging to the slice, the resource usage crossing thresholds, the load level of their NFs, and the crossed load level thresholds that are met or exceeded.

To produce these analytics, the NWDAF gathers data related to the NS identifiers from OAM and the resource utilization from the NFs that constitute the NS. Additionally, the NWDAF collects data, for each target S-NSSAI or NSI ID depending on the final consumer of the analytics (another NF or the management), from AMF (number of registered/de-registered/served UEs at that AMF), SMF (number of established or released PDU sessions at that SMF), NSACF (number of registered UEs and established PDU sessions), and NRF (load of the NFs that are serving the network slice or instance).

2) Use cases: These analytics deal with the most resource-consuming factors in the network, allowing operators to take decisions on resource provisioning. NSACF is a common subscriber for these analytics, as one of the possible actions is the throttling of the UEs or PDU session for a given network slice, to avoid exceeding the available resources. Alternatively, OAM (in particular the network orchestration) can also consume these analytics to scale the virtual infrastructure accordingly. Finally, the AF may also consume these analytics to monitor the current Service Level Agreement (SLA) and determine whether the SLA is enough to keep the desired QoS quality or it should be changed.

B. Observed Service Experience

1) Definition and data gathering: The Observed Service Experience analytics provide statistics or predictions of the service experienced by the user. Although the service was initially intended for streaming services (e.g., video conference calls), it has been recently extended to include other type of services, such as Vehicle to Everything (V2X) or web browsing.

These analytics can target either one or a set of UEs, or an area of interest, and for this purpose, the NWDAF collects data mostly from the AF itself, including the Mean Opinion Score (MOS) of the perceived quality of the service. The NWDAF also collects performance data from the AF, e.g., average delay, average loss rate, and average throughput. From SMF and AMF, the NWDAF collects the location of the UE, its UPF ID, IP related information, etc. From UPF, the NWDAF collects the uplink and downlink bitrates, uplink and downlink packet delays, and the number of packet transmissions and re-transmissions. Finally, the NWDAF collects from OAM radio-related aspects, such as the Reference Signal Received Power, Reference Signal Received Quality, Signal-to-Noise and Interference Ratio, and the mapping between Cell-ID and Frequency.

Figure 3 reports the so-called `experiences` defined by 3GPP, that are used by the NWDAF as a secondary de-multiplexer for reporting about the quality of experience observed by different groups of UEs according to the kind of context (e.g., Network Slice or Applications). Whenever the target includes a group of UEs, these analytics report the

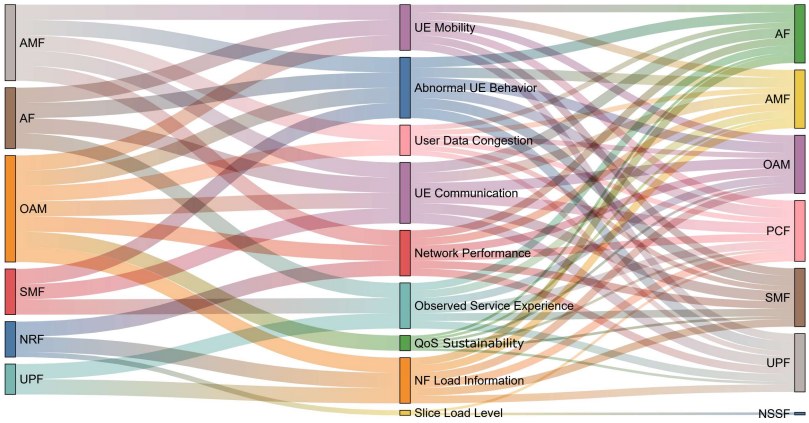

Fig. 2: Analytic IDs

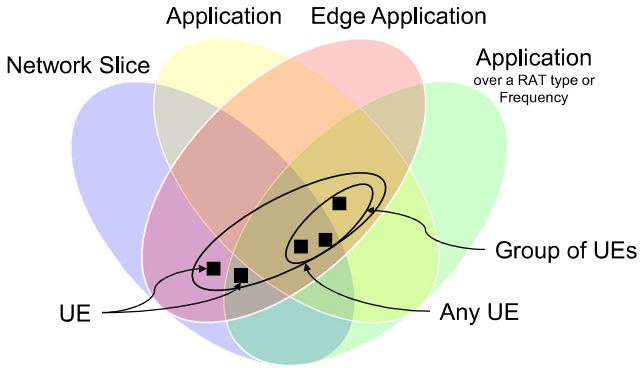

Fig. 3: The experiences defined by the Observed Service Experience analytics

percentage of UE that share the same experience (e.g., average delay below a certain threshold).

2) Use cases: As exemplary use cases, the PCF may use the Observed Service Experience analytics to modify the 5QI of one or more flows. The SMF may also use this information for selecting an appropriate UPF that is able to handle high-QoS demands from QoS flows.

C. Network Function Load

1) Definition and data gathering: These analytics refer to the load of one or more NFs. Once the target NFs are identified, the NWDAF collects their loads from the NRF, which is continuously receiving heartbeat messages from NFs. Another source of data is OAM, which provides resource-related data such as CPU, memory, and disk usage. Finally, the UPF also provides data for these analytics, including data volume and duration measurement, UE IP address, or UE Ethernet information, and the timestamp of the first and the last packets.

With the gathered load status, the NWDAF produces an analytics report that includes either statistics from the past or predictions for the future, including a list of resource status, each one identifying the NF type, NF instance ID, NF status, NF resource usage, NF load, and NF peak load. This provides detailed information of the past or predicted load of the relevant NFs for the UE.

2) Use cases: The load information can be very useful for an operator for, e.g., capacity planning. Additionally, some NFs, such as AMF or SMF can use it to select less-loaded NFs, e.g., when AMF selects an SMF or when SMF selects a UPF.

D. Network Performance

1) Definition and data gathering: This analytics processes the performance information coming from a specific area of interest, including RAN performance, communication performance (e.g., radio throughput and latency), and mobility performance. For the RAN part, the analytics include gNBs status and resource (CPU, memory, and disk) usage. Other metrics of interest include the average ratio of successful PDU Sessions and successful handovers, as well as the number of UEs in a given area of interest. RAN-related information is provided by OAM, while the number of UEs in the target area of interest is retrieved by the NWDAF by first contacting the NRF, and then polling all the AMFs serving the area. From the AMF, the NWDAF also retrieves UE-related information, such as the location, the Type Allocation Code, or behavioral trends related to the UE access and UE location.

2) Use cases: The Network Performance Analytics is consumed to make decisions based on the "health" of the network in the given area. This information can be leveraged by e.g., an AF, to select the most adequate time and area to deliver premium content to a group of UEs, by an AF to negotiate background data transfer policies, or by OAM to re-configure or scale NFs serving a certain area.

E. UE Mobility Analytics

1) Definition and data gathering: The UE mobility analytics provide consumer NFs with statistics or predictions related to the mobility of a UE or a group of UEs, i.e., network locations and timestamps. To generate this analytics report, NWDAF collects data from OAM, AMFs, and AF.

The AMF constitutes the most relevant source of information for these analytics, since the AMF is able to report the UE location, in the format of tracking areas or cell identifiers.

NWDAF produces analytics reports that include the location of the UE at certain time intervals, or the percentage of UEs included in the report (in case the target of the prediction is a group of UEs rather than a single one). As mentioned in Section III-B, the analytics can be further filtered by Area of Interest (as the consumer of these analytics is usually interested on the UEs related to the areas that the consumer is covering).

2) Use cases: UEs location analytics can be leveraged in a number of ways. AMF can use the UEs predicted location to adjust (e.g., enlarge) their registration area, in order to minimize registrations due to UE mobility. Another relevant use case for the AMF is the adjustment of the paging strategy for a given set of UEs. The SMF is another consumer of the analytics, that can handle PDU sessions related to UEs that are expected to enter the coverage area of a LADN.

Besides simple and short-term predictions, more complex analytics over larger time scales are also possible. These types of predictions can support e.g. the optimization of resource consumption (e.g., switching on and off base stations to track demand), or the analysis of UE trajectories, to discover and characterize the behavior of crowded areas over time.

F. UE Communication Analytics

1) Definition and data gathering: The UE Communication Analytics provides statistics or predictions for a UE or group of UEs, related to their communication patterns and user plane traffic. For these analytics, NWDAF collects data from AMF, SMF, AF, and UPF. The most relevant data is produced by SMF and UPF, as they deal with data plane flows. The consumer may filter the data for S-NSSAI, DNN, certain applications, and areas of interest.

The NWDAF produces statistics or predictions including the start time, duration, and periodicity of UE communications, the recurring time of day and day of week of the communication, the uplink and downlink data rate, and the traffic volume of the communication. Wherever possible, average and variance may be indicated. Traffic characterization, such as DNN, S-NSSAI, ports, etc. may also be included. The NWDAF also includes the percentage of UEs to which the analytic report applies, in case the request target is a group of UEs.

2) Use cases: These analytics are extremely useful for massive Machine-Type Communication (mMTC) services, where a very large number of devices may access the network and generate a large amount of control traffic. Hence, leveraging on short-term predictions of UE patterns, the network can optimize the access accordingly. For instance, the AMF may apply Mobile-Initiated Connection Only (MICO) mode parameters to the UE optimizing the control channel usage. An SMF may use these analytics for determining the value of the inactivity timer for the PDU session provided to the UPF. Also, an AF in a vertical domain may also subscribe to the analytics to receive statistics or predictions of the PDU sessions from to their supervised UEs.

G. Abnormal UE Behaviour Analytics

1) Definition and data gathering: The Abnormal UE Behaviour analytics targets Internet of Things (IoT) and unattended devices, allowing monitoring UE suspicious behavior, indicating a faulty or compromised device that requires further attention. The target of these analytics is a UE, a group of UEs, or "any UE." In this context, 3GPP defines a list of standardized exceptions, which we list in Table III.

To create this analytics report, the NWDAF collects data from AMF, SMF, and AF. In particular, the NWDAF collects from AMF and SMF the same data as in the UE Mobility Analytics (see Sec. IV-E) and the UE Communication Analytics (see Sec. IV-F). The analytics consumer may set filters on the Expected UE Behaviour parameters of interest, the expected analytics type, or a list of exception IDs, along with thresholds for the exception levels.

An Abnormal UE Behaviour analytics report includes a list of exceptions, each one comprising an Exception ID, an Exception Level, an Exception Trend (up, down, stable, unknown), a Type Allocation Code (TAC) identifying the type of affected device, the list of Subscription Permanent Identifier (SUPIs) of the affected UEs, a Ratio describing the percentage of UEs for the Target of Analytics affected by the exception and, in case the target was "any UE," the estimated number of UEs affected by the exception, plus additional specific information that depends on the actual exception. For instance: if the exception indicates that the UE was at an unexpected location, the additional information may include the tracking area or cell ID; if the exception detected unexpected radio link failures, the additional information may include frequency, time, location, or assumptions about the possible circumstances.

2) Use cases: As the target of these analytics is IoT and unattended devices, most of the use cases so far are related to mMTC, which have quite predictable communication patterns (other use cases are under study). Typical consumers of these analytics are PCF, AMF, and AF, which can react to the anomaly reports. For instance: if the ping pong exception is triggered, the AMF may consider a larger registration area to avoid the frequent re-registration of the UE; if an unexpectedly large data rate flow is detected, the PCF may restrict the PDU session or reduce its Quality of Service; if there are unexpected radio failure reports, the AMF may apply coverage enhancements for devices in the edge of the coverage.

H. User Data Congestion

1) Definition and data gathering: These analytics provide statistics or predictions related to the congestion of the control plane, user plane, or both, related to either a UE or "any UE" in the area of interest. Consumers can filter the results by requesting a list of the applications that contributed more to the congestion and set a threshold upon which congestion levels are indicated. The NWDAF produces reports with statistics including the congestion level of the user plane, control plane, or both, applicable to a UE o any UE per time window. The report may also include the list of top applications contributing

TABLE III: The exceptions defined by the Abnormal UE Behaviour Analytics analytics

Exception	Description
Unexpected UE Location	The UE has been detected in an atypical or unexpected location. This may indicate a stolen or fraudulent re-location of the device.
Ping-ponging across neighbouring cells	The UE is frequently re-registering in the AMF from different cells.
Unexpected long-live/large rate flows	The UE keeps an atypically long or data-hungry flow compared to short and periodically data transfers performed in the past.
Unexpected wake-up	The UE has woken up at an abnormal time. This Exception is only valid if the UE is configured to send data periodically.
Suspicion of Distributed Denial of Service∼(DDoS) attack	There is the suspect that the UE is being hijacked and being used as the source or target of a DDoS attack.
Wrong or unusual destination address	The UE is trying to send data to an atypical or wrong destination address.
Too frequent Service Access	The UE is establishing PDU sessions and sending data atypically.
Unexpected radio link failures	The UE is experiencing disruption on the radio connectivity.

to the uplink or downlink, identified by an Application ID or by its IP packet filter.

The data producers for these analytics are: the AMF instances that are polled to fetch the information about the UEs in the target areas, and OAM, which provides RAN-related information, such as performance measurements that NWDAF translates into congestion levels, including UE throughput, Data Radio Bearers setup management, Radio Resource Connection number, Radio Resource utilization or PDU Session management. Finally, the UPF or AF provide related measurements, such as the application ID of the PDU session, IP packet filter set, measurement periods, throughput in uplink and downlink, peak throughput in uplink and downlink, and timestamps where the measurements were taken.

2) Use cases: An external AF receives statistics, about a given application. as a percentage of the total throughput in the area of interest. This information helps the AF to determine areas where, e.g., a video should be served with lower resolution and/or frame rate, to preserve video quality. These reports may also be helpful for operators to determine bottlenecks in the network and, e.g., instantiate additional NFs to alleviate congestion.

I. QoS Sustainability

1) Definition and data gathering: These analytics provide information about QoS changes in a given area of interest for a number of QoS flows. These QoS changes may be statistics from the past or the likelihood of a QoS change, if they refer to predictions for the future. More specifically, the consumers specify a set of standardized or pre-configured 5QI, along with their thresholds, to receive alerts when any QoS flow crosses the corresponding threshold. As these analytics relate to a given area of interest, the input data is provided by OAM, as it can export RAN related metrics. Among these metrics, it is worth highlighting RAN UE throughput (average UE bitrate in the cell, per timeslot, per cell, per 5QI and per S-NSSAI) and QoS flow Retainability (number of abnormally released QoS flows during the time the QoS flows were used per timeslot, per cell, per 5QI and per S-NSSAI.).

With this information, the NWDAF produces an analytic report that includes a list of QoS sustainability analytics, each one detailing the area to which the analytics applies, the applicable time period, and the corresponding information about the thresholds, i.e., the reporting thresholds that are met, exceeded, or crossed.

2) Use cases: These analytics are useful to adapt the QoS parameters of flows generated by users belonging to a given area, and it is consumed mostly by AFs through the NEF. One exemplary use case is a V2X AF receiving predictions of the immediate QoS sustainability, where the V2X AF determines whether a vehicle may sustain the QoS flows to support autonomous driving. Another example is an AF processing the 5QIs information to understand the achievable QoS for audio/video streams, in locations where the 5QI might not cope with the expectations. The AF could then dynamically adjust the QoS requirements of multimedia flows, or defer the streaming to a most suitable time.

V. Outlook to Release 17 and Release 18

As we have seen, R16 lays the foundations for network automation, focusing on the operation of NWDAF and detailing a number of use cases. Next, we summarize the major enhancements introduced by R17 and R18.

A. Release 17

R17 follows the architectural de-composition trends and splits the NWDAF functionality in a provider and a generator:

- The Analytics Logical Function AnLF: responsible for inference, reporting, and exposing analytics services.
- The Model Training Logical Function MTLF: responsible for training ML models and exposing them to the AnLF.

R17 also introduces new capabilities, supporting features such as: aggregation from multiple NWDAFs, so analytics can be composed e.g. across network slices; bulk data collection, and data collection from the UE through a specific flavor of the AF application function; transfer of analytics contexts or subscriptions, e.g., due to UE mobility; or managing user consent for analytics.

To this aim, R17 introduces new functions: (1) Data Collection Coordination Function DCCF that orchestrates the collection of data from 5GC NFs, avoiding that multiple NWDAFs access the same data in 5GC NFs; (2) Analytics Data Repository Function ADRF, to store and collect data and analytics; and (3) Message Framework Adaptation Function MFAF, which exposes the services implemented by the NWDAF over a Messaging Framework employing a pub-sub pattern, such as e.g. Apache Kafka.

Finally, R17 introduces five new types of analytics: Dispersion Analytics, WLAN performance analytics, Session Management Congestion Control Experience Analytics, Redundant Transmission Experience related analytics, and Data Network Performance Analytics.

B. Release 18

R18 improves the operation of NWDAF in several ways: first, by including mechanisms for the AnLF to compute the accuracy of ML models and report it to the MTLF and the service consumers; second, by a similar mechanism in the MTLF for computing the accuracy of ML models and receive the accuracy reports from AnLFs, which can determine if an ML model needs retraining; third, by receiving feedback from service consumers regarding the actions taken by the service consumer that could have had an impact on the results of analytics predictions; fourth, on the capability for the MTLF to generate and deliver to the AnLF multiple ML models for the same Analytics ID, so that the AnLF could select the most appropriate one; fifth, by supporting NWDAF Federated learning, i.e., training an ML Model across multiple decentralized entities without exchanging/sharing local data set; sixth, by supporting NWDAF reallocation, as well as DCCF, and MFAF reallocation.

R18 also introduces new functionality, such as supporting roaming scenarios, e.g., when the UE is roaming, including data collection by a Home NWDAF from a Visited NWDAF for outbound roaming users as well as data collection by a Visited NWDAF from a Home NWDAF for inbound roaming users. The functionality of the ADRF is extended to also store of ML models. A new SBI in the UPF provides a standard interface for collecting data from UPF. Finer UE location information granularity is provided by collecting data from Location Services LCS systems.

Finally, R18 also introduces five new analytics (summing up to 18): for the determination of Packet Flow Descriptions PFD, Location Accuracy Analytics, End-to-end volume transfer time, Relative Proximity Analytics, and UE-Route Selection Policies URSP enforcement Analytics

C. Other standards

In the same way 3GPP natively integrated data analytics into its architecture, other SDOs started similar efforts. One of the most notable cases is O-RAN [7], which relies on an ecosystem of 3rd party applications (xApps) leveraging both quasi-real time data coming from the gNB and orchestration to perform e.g., Machine Learning based analytics and reconfigurations. Another case is ETSI ENI [8], which is currently paving the way for the Autonomous Network Management [9] by integrating different data sources, especially from the management domain.

VI. Summary

This paper has introduced and summarized the work carried out by 3GPP around network automation and analytics that started with Release 15 and continues towards Release 18. Many standardization bodies besides 3GPP are targeting the concept of autonomous [9] or zero touch [10] networks.

Acknowledgement

The work of University Carlos III of Madrid has been funded by European Union's Horizon-JU-SNS-2022 Research and Innovation Programme Project TrialsNet (Grant Agreement No. 101095871) and H2020 DAEMON (Grant Agreement No. 101017109). This work is also partially supported by the Spanish Ministry of Economic Affairs and Digital Transformation and the European Union-NextGenerationEU through the UNICO 5G I+D 6G-CLARION and 6G-SORUS projects.

References

[1] V. Sciancalepore, C. Mannweiler, F. Z. Yousaf, P. Serrano, M. Gramaglia, J. Bradford, and I. Labrador Pavón, "A Future-Proof Architecture for Management and Orchestration of Multi-Domain NextGen Networks," *IEEE Access*, vol. 7, pp. 79 216–79 232, 2019.

[2] 3GPP, "Architecture enhancements for 5G System (5GS) to support network data analytics services," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 23.288, March 2023, version 18.1.0. [Online]. Available: https://www.3gpp.org/DynaReport/23288.htm

[3] ——, "5G System; Network Data Analytics Services; Stage 3," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 29.520, March 2023, version 18.1.0. [Online]. Available: https://www.3gpp.org/DynaReport/29520.htm

[4] ——, "5G System; Network Data Analytics signalling flows; Stage 3," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 29.552, December 2022, version 18.0.0. [Online]. Available: https://www.3gpp.org/DynaReport/29552.htm

[5] ——, "Management and orchestration; Concepts, use cases and requirements," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 29.520, March 2023, version 17.4.0. [Online]. Available: https://www.3gpp.org/DynaReport/28530.htm

[6] A. Garcia-Saavedra and X. Costa-Perez, "O-RAN: Disrupting the Virtualized RAN Ecosystem," *IEEE Communications Standards Magazine*, pp. 1–8, 2021.

[7] L. Bonati, S. D'Oro, M. Polese, S. Basagni, and T. Melodia, "Intelligence and learning in o-ran for data-driven nextg cellular networks," *IEEE Communications Magazine*, vol. 59, no. 10, pp. 21–27, 2021.

[8] Y. Wang, R. Forbes, C. Cavigioli, H. Wang, A. Gamelas, A. Wade, J. Strassner, S. Cai, and S. Liu, "Network management and orchestration using artificial intelligence: Overview of etsi eni," *IEEE Communications Standards Magazine*, vol. 2, no. 4, pp. 58–65, 2018.

[9] ETSI ENI, "Unlocking Digital Transformation with Autonomous Networks; ETSI perspectives and major achievements," Tech. Rep., March 2023. [Online]. Available: https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP56_Unlocking-Digital-Transformation-with-Autonomous-Networks.pdf

[10] ETSI, "Zero-touch network and Service Management (ZSM); Reference Architecture," ETSI, Tech. Rep. GS ZSM 002, August 2019. [Online]. Available: https://www.etsi.org/deliver/etsi_gs/ZSM/001_099/002/01.01.01_60/gs_ZSM002v010101p.pdf

Miguel-Angel Garcia-Martin is a Senior Engineer at the Technology unit of the Product Development Unit Communications, UDM and Exposure at Ericsson. Miguel-Angel received his B.Eng in Telecommunications Engineering (1993) from the University of Valladolid and his M.Sc degree in NFV and SDN for 5G Networks (2020) from University Carlos III of Madrid. He co-authored the book *The IP Multimedia Subsystem (IMS): Merging the Internet and the cellular worlds*.

Marco Gramaglia is a Visiting Professor at University Carlos III of Madrid, where he received M.Sc (2009) and Ph.D (2012) degrees in Telematics Engineering.

Pablo Serrano (M'09, SM'16) is an Associate Professor at the University Carlos III de Madrid. He has over 100 scientific papers in peer-reviewed international journals and conferences. He currently serves as Editor for IEEE Open Journal of the Communication Society