ONTIC D5.1: Use case requirements

Alejandro Bascuñana, Patricia Sánchez, Miguel-Ángel Monjas, Ericsson Spain, José-Maria Ocon, José-Ignacio Laureano, Miguel-Angel Lopez, Bruno ; Ordozgoiti, Alberto Mozo, Daniele Apiletti, et al.

Online Network Traffic Characterization

Deliverable
Use Cases Requirements

ONTIC Project
(GA number 619633)

Deliverable D5.1
Dissemination Level: PUBLIC

Authors
Alejandro Bascuñana, Patricia Sánchez, Miguel-Ángel Monjas (Ericsson Spain); José-María Ocón, José-Ignacio Laureano, Miguel-Angel López (SATEC Spain); Bruno Ordozgoiti, Alberto Mozo (UPM); Daniele Apiletti, Fabio Pulverenti (POLITO); Philippe Owezarski (CNRS)

Version
ONTIC_D5.1.2015-01-30.1.00

Version History

Version	Modification date	Modified by	Summary
0.01	2014-11-28	Ericsson	Structure proposal
0.1	2014-12-10	Ericsson	First draft version
0.2	2014-12-12	UPM	SoTA on use cases 9.2 and 9.3
0.3	2014-12-16	SATEC	SoTA on Big Data
0.4	2014-12-18	CNRS	SoTA User Case 1 / Use case 1 description
0.5	2014-12-23	SATEC	New version SoTA on Big Data
0.6	2014-12-23	POLITO	Introduction to Big Data SoTA
0.7	2015-01-14	Ericsson	First full review
0.8	2015-01-22	Ericsson, CNRS, UPM	Contributions from partners after first full review
0.9	2015-01-26	SATEC	SoTA on Network Management
1.0	2015-01-30	Ericsson, UPM,	Final review

		SATEC, EMC	

Quality Assurance:

Role	Name
Quality Assurance Manager	Miguel Ángel Lopez Peña (SATEC Spain)
Reviewer #1	Alberto Mozo (UPM)
Reviewer #2	Fernando Arias (EMC Spain)

Table of Contents

List of figures

List of tables

1. Acronyms and Definitions

1.1 Acronyms

Acronym	Defined as
3GPP	3rd Generation Partnership Project
AF	Analytics Function Application Function
ANDSF	Access Network Discovery and Selection Function
API	Application Programming Interface
APN	Access Point Name
AQM	Active Queue Management
AQoE	Adaptive Quality of Experience
ASA	Adaptive Security Appliance
ATM	Asynchronous Transfer Mode
AVQ	Adaptive Virtual Queue
BBERF	Bearer-Binding And Event-Reporting Function
BSS	Business Support System
CN	Core Network
CoS	Class of Service
CSP	Communication Service Provider
CSS	Context Sensing Software
DoW	Description of Work
DPI	Deep-Packet Inspection
DoD	Definition of Done
DSCP	Differentiated Services Code Point
ECN	Explicit Congestion Notification
EERC	Explicit End-to-end Rate-based Congestion Control
EP	Enforcement Point
EPC	Evolved Packet Core
EPS	Evolved Packet Systems
ESM	Experience Sampling Method
GSM	Global System for Mobile Communications
HTML	HyperText Markup Language
ICT	Information and Communications Technology
IDC	International Data Corporation
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
ISP	Internet Service Provider
IW	Initial Congestion Window Size
KPI	Key Performance Indicator
ME	Mobile Equipment
MME	Mobility Management Entity
MOS	Mean Opinion Score
MT	Mobile Termination
OCS	Online Charging System
OD	Origin-Destination

OSS	Operation Support System
PC	Policy Controller
PCA	Principal Component Analysis
PCC	Policy and Charging Control
PCEF	Policy and Charging Rule Enforcement Function
PCRF	Policy and Charging Rules Function
PDN	Packet Data Network
PDP	Policy Decision Point
PEP	Policy Enforcement Point
PGF	Policy Governance Function
QCI	QoS Class Indicator
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Network
RCAF	RAN Congestion Awareness Function
RCP	Rate Control Protocol
RED	Random Early Detection
REM	Random Exponential Marking
RFC	Request For Comment
RUCI	RAN User Plane Congestion Information
SAE	System Architecture Evolution
SDF	Service Data Flow
SDN	Software-Defined Networks
SLA	Service Level Agreement
SLS	Service Level Specification
SMPP	Short Message Peer-to-Peer
SMS-C	Short Message Service Center
SNMP	Simple Network Management Protocol
SoTA	State of The Art
SPR	Subscription Profile Repository
SVM	Support Vector Machine
TCA	Traffic Conditioning Agreement
TCS	Traffic Conditioning Specification
TE	Terminal Equipment
TFO	TCP Fast Open
TCP	Transmission Control Protocol
TFRC	TCP-Friendly Rate Control
UC	Use Case
UE	User Equipment
UI	User Interface
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunications System
UNADA	Unsupervised Network Anomaly Detection Algorithm
URCA	Unsupervised Root Cause Analysis
VCP	Variable-Structure Congestion Control Protocol
XCP	Explicit Congestion-Control Protocol

2. Purpose of the Document

As described in the ONTIC DoW: “This deliverable will contain the requirements for the following Use Cases: (a) Network Intrusion Detection, (b) Dynamic QoS management and (c) Proactive Congestion Detection and Control Systems. These requirements will be implemented in the corresponding prototypes. It must be observed that only a basic set of requirements will be described initially, and then, applying some kind of Agile methodology (e.g. SCRUM) they will be augmented along the WP duration.”

ONTIC work package WP5 follows a customized version of the Scrum Agile methodology; therefore the requirements are written down as user stories. In addition to what has been described as initial goals for D5.1, this deliverable provides the background the reader needs to understand the overall context of the project and its relationship with the three proposed use cases. The different sections along the document provide information about:

- High level view of the Agile methodology that is being followed in the project.
- State of the Art for the provided use cases.
- First detailed description of the use cases and the initial user stories (requirements).

This is a live document that will describe in following versions the evolution of the scenarios and the related user stories.

It must be noted that the definition of the user requirements for these use cases requires the previous specification of the underlying architectural models. However, the application of advanced machine learning techniques to the specific scenarios to be addressed by the ONTIC project is not sufficiently widespread in the industry, which means that such models do not exist yet. This absence prevents the corresponding user requirements to be fully specified in the early stages of the project. Once the consortium has completed the mentioned architectural models, a complete specification of the use cases and the corresponding requirements will be described in Deliverable D5.2 [3].

3. Scope

This document provides the definition of the three use cases in the first year of ONTIC. It is a live deliverable, which means that, the progress in ONTIC on the user requirements during the second year will be held in Deliverable 5.2 [3], as a continuation of the current deliverable. In this way, as a live deliverable, the use case requirements will be updated along the duration of the ONTIC project with new and evolved user stories, as well as the progress on design and implementation of the corresponding prototypes. The third and last year will generate three deliverables, one per use case, containing the final set of requirements, as well as the design, implementation and validation of its corresponding prototype.

Once explained the whole context of the use cases requirements-deliverables association, this document provides a general overview about the user stories that will drive the development of the use cases (already defined in the DoW) and the background that is needed to understand them.

4. Intended Audience

The intended audience includes every partner within ONTIC project, especially those involved in gathering requirements, and in designing, implementing and validating the prototypes. It also includes any reader interested in knowing the ONTIC use cases in order to understand the business principles that guide the research within the project.

The readers of this document will receive information about the state or the art beyond the use cases, and a basic set of requirements for each use case. The requirements extraction methodology is also included in this deliverable, which is the intended methodology to be used also in the next deliverables.

5. Suggested Previous Readings

It is expected that a basic background on Information and Communications Technology (ICT) is sufficient to address the contents of this document; however, some previous reading are suggested:

- ONTIC. “Deliverable D2.1. Requirement Strategy” [1].
- ONTIC. “Deliverable D6.4. Progress on Exploitation and Dissemination Plans – Part I” [4].

6. Executive Summary

Modern networks have to face an increasing growth of traffic, which does not seem to stop in the near future. The resilience of packet networks is currently not high, especially when considering how difficult is to detect and even predict anomalies in real-time and therefore to actuate in order to alleviate network incidents or issues.

Terabytes of data are being transferred through the core network of a typical Communication Service Provider (CSP) every day. Moreover, an exponential growth with more than 50 billion devices connected to Internet is expected in the near future. Therefore, this scenario hampers network data capture and analysis.

In the context of network management and engineering, ONTIC has identified in the DoW the following three scenarios as key to address the network transformation:

1. Proactive and dynamic QoS Management
2. Network intrusion detection
3. Early detection of network congestion situations

The value in those scenarios lays in the implementation of an accurate and scalable mechanism for online characterization of the evolution of network traffic patterns so that appropriate actuation mechanisms are used to alleviate said situations.

Within ONTIC, scenarios #2 and #3 address a network optimization scenario, providing analytics capabilities to network elements in charge of enforcing the corresponding policies. On the other hand, scenario #1 addresses the problem of network anomaly detection.

Currently, CSPs address congestion management in a reactive way:

- Congestion management follows a manual approach. Planning is done in advance.
- It only solves programmed congestion situations.
- Only a very basic set of rules is supported: those being configured by PC operator. Thus, only ad-hoc optimization solutions can be provided.

ONTIC aims to provide an architecture to enable enhanced congestion management, taking advantage of analytics-enabled functionalities, thus showing proactive features:

- Congestion management is automatic. No need of previous planning.
- It is possible to solve unexpected congestion situations.
- An advanced set of rules enhanced by a so-called Analytics Function is supported. Thus a generic and continuous network optimization procedure will be implemented and included within the Ericsson Policy and Charging Control (PCC) offering.

In the ONTIC project, it is also proposed to experiment a disruptive technology on anomaly detection. It is then proposed to make the anomaly detection system take advantage of unsupervised learning in order to make it autonomous. The idea is then to make possible detecting, classifying, and applying counter measures autonomously without the intervention of a human expert. In our idea, the system does not need any previous acquired knowledge, i.e. no need for known anomaly, intrusion, or attack signatures, and no need for previously labeled traffic for classification (or system validation). The system will then run with limited cost as producing signature and labeling traffic traces can only be hand made by a human expert, and is then slow, costly, and is lacking reactivity. We then aim at designing a proactive anomaly detection system as opposed to the current reactive ones.

7. WP5 Methodology

7.1 Ways of working

This section describes the methodology followed by work package WP5 in ONTIC. It will drive the development of the final proofs of concept as well, taking into account the priorities that will be followed in WP5 (years 2 and 3) in order to have a proper coordination among already proposed use cases #1 #2 and #3. ONTIC is a use case driven research project that aims to show the power of a new generation of online/offline distributed and scalable big data algorithms, developed throughout the project. This section is an updated version of the one provided in deliverable D2.1 “Requirements Strategy” [1].

To have a clear picture of how to manage priorities and requirements taking the market needs into account, it is quite important to implement a clear and simple coordination process. This process will help to manage the end-to-end process, to set priorities on which research field should be addressed first, to select and specify scenarios close to the market needs, and to eventually validate them. It is inspired by the Agile methodology [12], adapted to the specific constraints of an international and collaborative research and innovation project such as ONTIC.

The Agile methodology is a lightweight project management framework with broad applicability to all types of iterative and incremental projects. Several roles are defined. Product Owners are in charge of identifying and prioritizing user stories (requirements) and updating and prioritizing the so-called “Backlog” following the Actors (customer) needs. As said, the prioritized requirements to be implemented are identified by the Actors (the market) and described as “User Stories”. The priorities in the Backlog are set-up by the use case leaders (Product Owners) and implemented during “Sprints”, which will be flexible enough to be adapted to the required pace of the project.

By using agile methodologies within the ONTIC Project the market requirements are introduced within the research and development process. Furthermore, agile methodologies provide a general framework to coordinate the partner’s effort. ONTIC will take as the base Agile principles the ones provided within SCRUM [76].

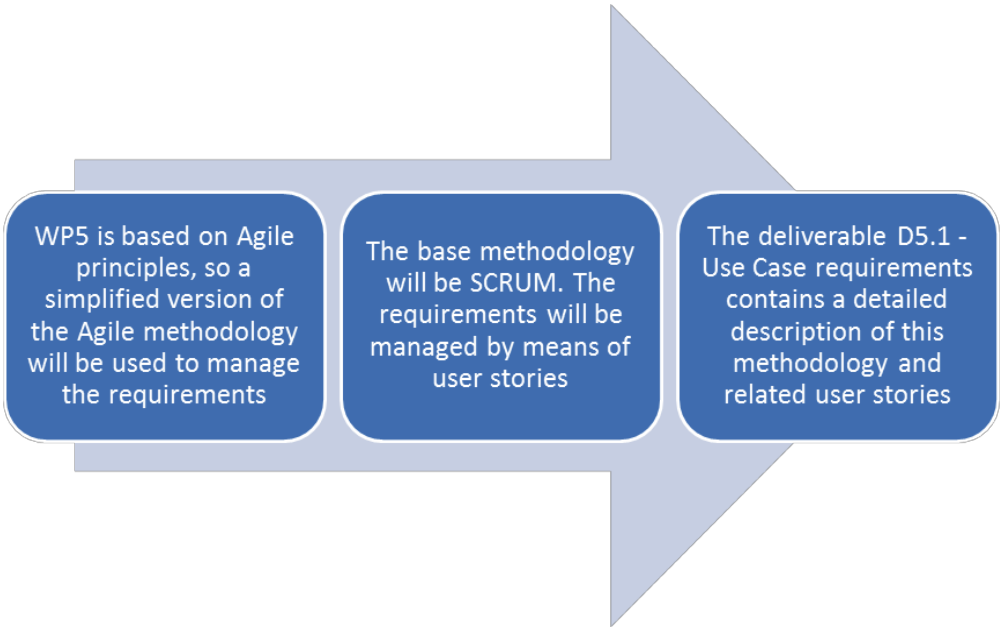

Figure 1: The agile flow within ONTIC WP5

The following sections provide a more detailed description of the different roles and tools involved in the Agile methodology.

7.2 Product Owner

The role of the "Product Owner", in our case played by the leaders of use cases #1 #2 and #3, is to identify Actors and related market needs, and to translate said needs into a prioritized list of User Stories that later on will be "implemented" in the project.

Product Owner → Use-Case #1, #2 and #3 drivers.

7.3 Actors

The first action to be carried out in the project is to identify the different actors; they are the potential customers of the outputs of the project. Once actors are identified, a prioritized list of user stories is generated.

Actors will define their priorities and therefore will drive the research and development of the big data components.

Actors → Identified receivers of the project's output.

7.4 User Stories

As said, Actors will define, via Product Owners, the User Stories that, later on, will be prioritized in the WP5. A User Story is the proposed tool used to summarize the requirements coming from the different WPs. A "Definition of Done" (DoD) will be also linked to each User Story to assure that WP Leader/ Task Leaders will work on it, knowing in advance what it is expected to be shown as a result. Once each Sprint ends, WP5 Leader/ Task leaders will show to the rest of the consortium the outputs, which should be aligned with the User Story definition and its DoD.

The standardized way to define a user story is as follows:

As <user>

I want <what>

So that <why>

User Stories → Summarizes requirements from the Actors (Customers).

7.5 Task

Once the User Stories have been prioritized, the WP5 Leader/Task Leaders select those ones that will be worked. Once the User Stories are selected, the WP5 Leader/ Task Leaders split them in tasks for their internal work. In the end, the WP5 Leader/ Task Leaders will present to the rest of the consortium the outputs of the ongoing sprint.

Tasks → Internal work modules to achieve a User Story

7.6 Backlogs

There will be two backlogs:

- A prioritized backlog of user stories (Product Backlog) for use cases #1 #2 and #3.

- A per-Sprint backlog (Sprint Backlog), created at the beginning of each Sprint as part of the Sprint Planning. It will consider the new needs identified in every Sprint Review.

The WP5 Leader/ Task Leaders are responsible for selecting the User Stories to work in based on the prioritization and will do the same process in the following sprints.

Backlogs → prioritized list (Product Owner) of user stories for the whole use case (Product Backlog) or for the Sprint (Sprint Backlog)

7.7 Tools

A MS Excel file stored in the common repository is proposed as a way to manage the prioritized Product Backlog and the related definitions of done, tasks, etc. This simple tool has the advantage of providing an easy way of accessing the information without administrative overloads.

Section 10 will provide a summary of the different backlogs already proposed for the different scenarios.

8. State-of-the-Art (general)

8.1 Introduction

The ONTIC project comprises three use cases that aim to face the challenging scenarios that Communication Service Providers (ISPs, Telco operators, etc.) currently have on their radar in the context of network management [62] [63]:

- Personalization of services in dynamic complex scenarios
- Self-optimization
- Self-configuration
- Automatic intrusion detection
- OPEX and CAPEX pressure
- Network optimization
- High growth rate of connected devices
- Heterogeneity in the user side
- Dynamic scenarios management, etc.
- …

The baseline scenario: Reactive Network Control and Management scenario

The needs listed in the section above describe how future networks should be. However, it not actually possible to address all the new functionalities that will come out of such needs. Instead, ONTIC will address a survey of three use cases that characterize some of the most important features of future networks. Use Case #1 (Network Anomaly Detection), Use Case #2 (Proactive Congestion Detection and Control Systems) and Use Case #3 (Dynamic QoS Management) cover a wide spectrum whose solutions would create the foundations of future networks.

In order to understand the step forward the ONTIC use cases provide, we need to briefly depict the current status of Network Management and Control. Figure 2 provides a high level view summarizing the current state of the art.

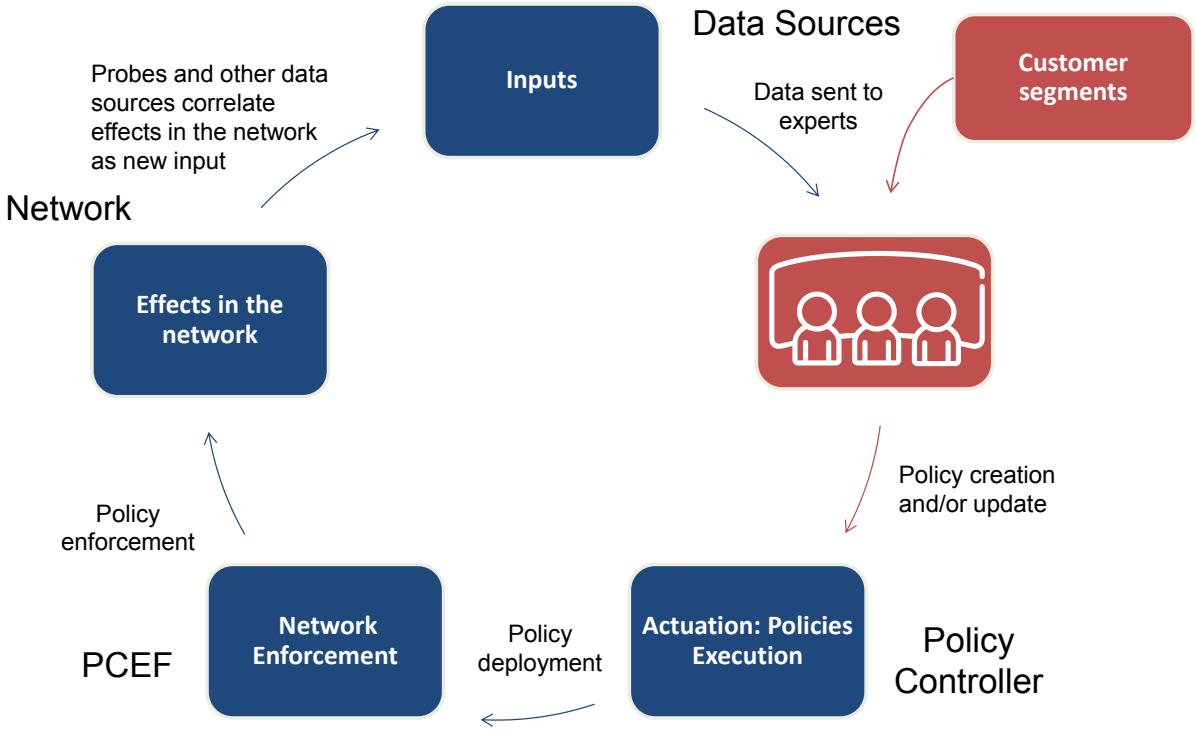

Figure 2: The current "reactive" network monitoring and control loop

The network is constantly generating signaling information. Said information may be collected and aggregated by OSS/BSS systems (inputs) and then provided to experts; based on this information, the experts will set-up policies that improve the network performance, that prevent attacks, etc. Such new policies are managed by a Policy Controller, and applied in Network Enforcement points.

So, in this case the network is working in a "reactive" mode, as it reacts to new events once they occur, with policies based on "historical" information and past experience. The network is able to react to unexpected events in a limited way and cannot anticipate such events, as only receives information about what is currently going on or about what happened some time ago.

The ONTIC proposal: from reactive to proactive network control and management

The target ONTIC scenario must be automated and intelligent, moving from a "classical" reactive scenario to a "disruptive" proactive one. Nowadays, networks are managed and controlled following a reactive paradigm (left-hand side of Figure 3). ONTIC aims, by implementing the already defined use cases, to provide the building blocks to enable the transformation from the left side (reactive) to the right side (proactive) of the picture. Thus, the ONTIC outcomes will help networks to implement self-configuration and self-optimization features, so that they evolve to a scenario where they are capable to react in real time to changes in the network.

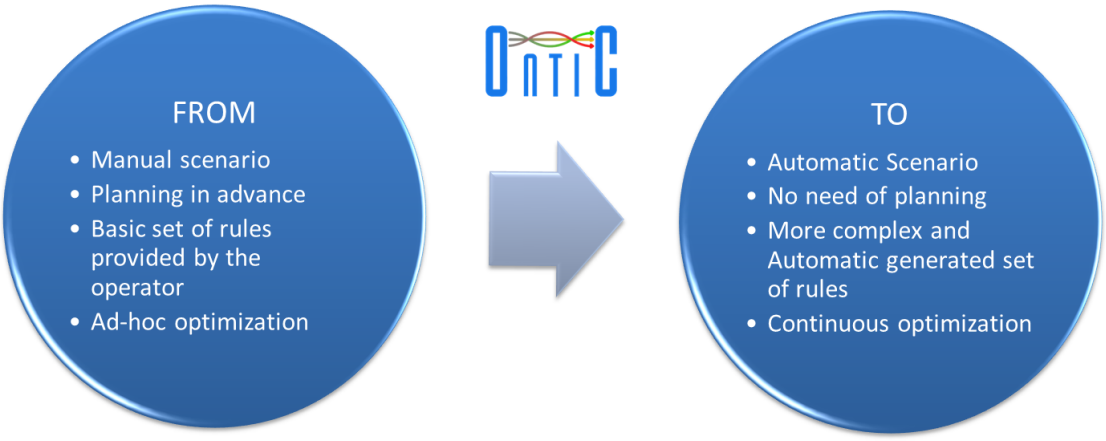

Figure 3: Network management transformation

The target scenario: Proactive Network Control and Management

To enable this new proactive scenario the network monitoring and control loop described in Figure 2 is evolved to the one shown in Figure 4. Such figure shows how the human experts' analysis and policies configuration is automated by means a so-called **Analytics Function** that is introduced by the ONTIC project.

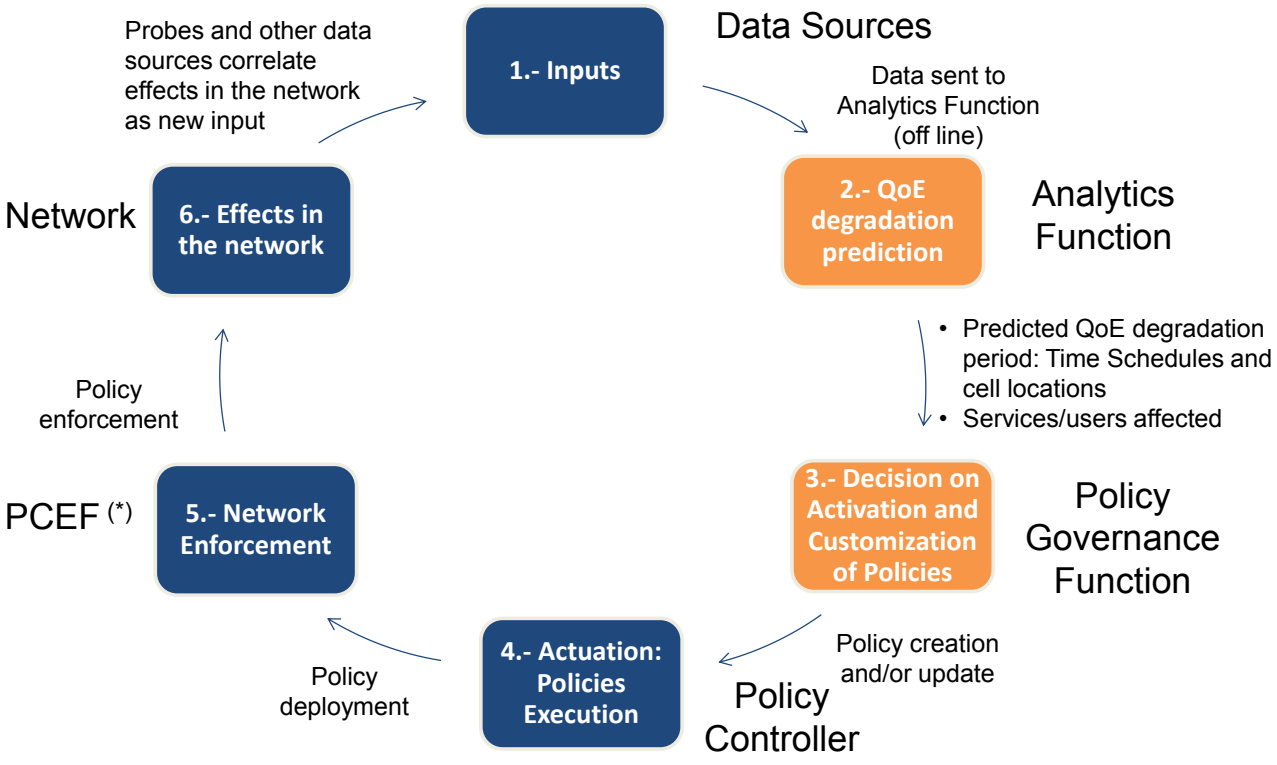

Figure 4: The new analytics virtuous circle

The Analytics Function is the entity where ONTIC will provide their main contributions. The Analytics Function will provide predictions to a Policy Governance Function that will be in charge or managing the actuation on the network so that alleviation measures are carried out. By closing the Network Management and Control loop the network will be able to make autonomous decisions and

provide online actuation. This closed loop will be the key to enable a solution for the described use cases, especially UC#2 and UC#3.

8.2 ONTIC Challenges, Values and Opportunities

Figure 5 provides a summary of the foreseen challenges, values and opportunities in the Network Management and Control that ONTIC can address:

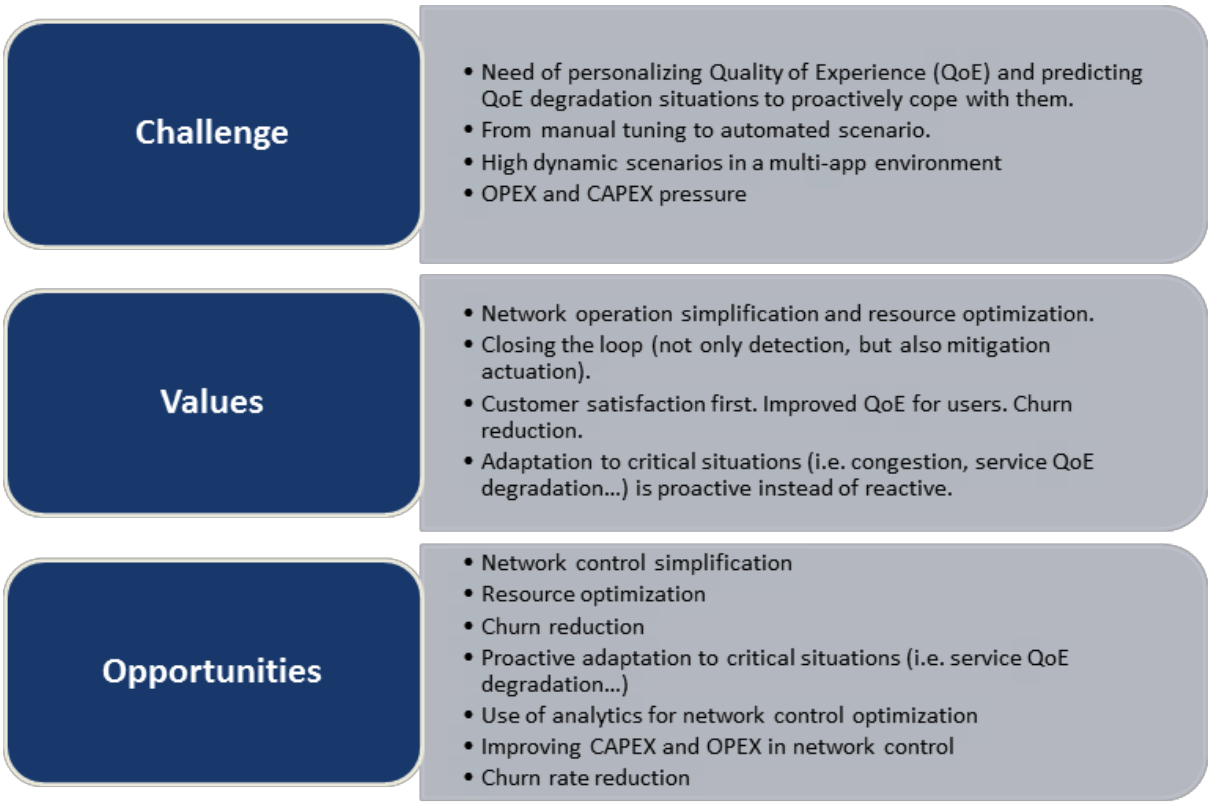

Figure 5: Challenges, Values and Opportunities

8.3 Network Management & Control SoTA

OSI has a well-defined network management reference model that breaks its functions into the following functional fields:

- Fault management
- Configuration management
- Accounting management
- Performance management
- Security management

Since early 1990's, policy-based network management is the norm as network management paradigm [138] [141]. The notion of policy turns out to be quite obvious to any large management systems, up to the point of all medium-to-large size companies nowadays arrange policies derived from their own objectives [143] [144]. In policy-based network management, policies are settled as rules that administer the states and behaviors of the network.

The management logic deals with:

1. The conversion from human-friendly directives (at a high level of abstraction) to syntactical device-independent rules governing the role and status of the network.
2. The translation of such rules to device-dependent configurations, hiding the complexity of such process and therefore bridging the business objectives to network configurations. When the state of a network varies, policies would be automatically updated to ensure consistency without any human intervention.
3. Lastly, the distribution of these configurations to enforcement entities.

The relevant policy-based network management architectural model is extensively a manager-agent model [142], where some nodes —called Policy Decision Points (PDPs)— handle the first two tasks, and other nodes —called Policy Enforcement Points (PEPs)— handle the last one (Figure 6). The way these points exchange information is through SNMP, or Simple Network Management Protocol, and although other alternatives are also available [139], it is by far the most spread protocol.

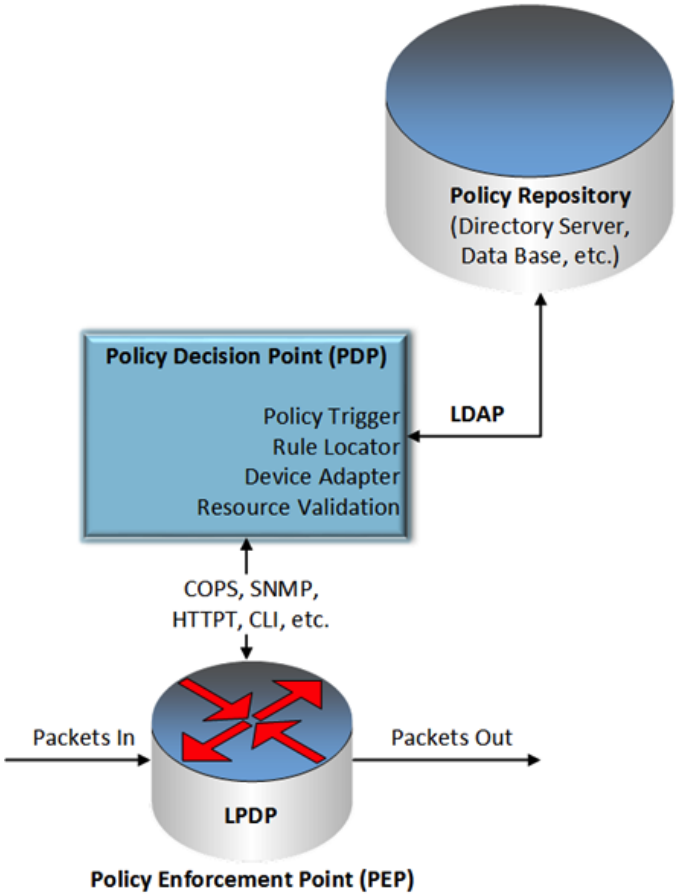

Figure 6: Policy-based network management architectural model

Bearing in mind both architectural and functional fields, the participants responsible for network management may fall into one of these five categories:

1. SNMP agents: switches, routers, etc. Basically PEP's.
2. Data presenters: with the only intent of recollecting data from SNMP agents to illustrate the results in HTML format, hence any web browser can easily retrieve and display the data.
3. Network mappers: for recognizing and showing the topology of the network, for example, based in IP or MAC addresses.

4. Network protocol analysts: for security matters like intrusion detection. Since inspecting at network or application protocol level requires more CPU-intensive data analysis, specialized nodes for this purpose come into play: IDS (intrusion detection system) and IPS (intrusion prevention system), explained below.
5. Network and system monitors: responsible for determining the state of the network, administering events and sending notifications, i.e. the so-called PDP's. HP OpenView [145] is a well-known solution for monitoring and administering network systems, as well as Network Supervisor (3Com) or CA Unicenter (TNG).

An intrusion detection system (IDS) examines all input and output network traffic to recognize not-trustworthy patterns that could point out any kind of network/system attack from a malicious entity trying to break into the system. IDS diverge from firewalls in that a firewall attempts to avoid intrusions from happening by restricting the access between networks so that they can be blocked, but it never notifies an attack from inside the network. An IDS reckons a doubtful intrusion just when it has taken place to do nothing else but signaling an alarm.

An IPS (intrusion prevention system) procures policies for network activity along with a detection system for sending alerts to network administrators when any suspicious irregularity occurs, but also lets the administrator to define the action upon being warned [140]. Some note the similarities between an IPS and a combination of IDS plus a firewall for safeguard. Cisco ASA [147] or FortiGate [148] are renowned examples of firewall with IDS integration. Figure 7 outlines the intrusion management model.

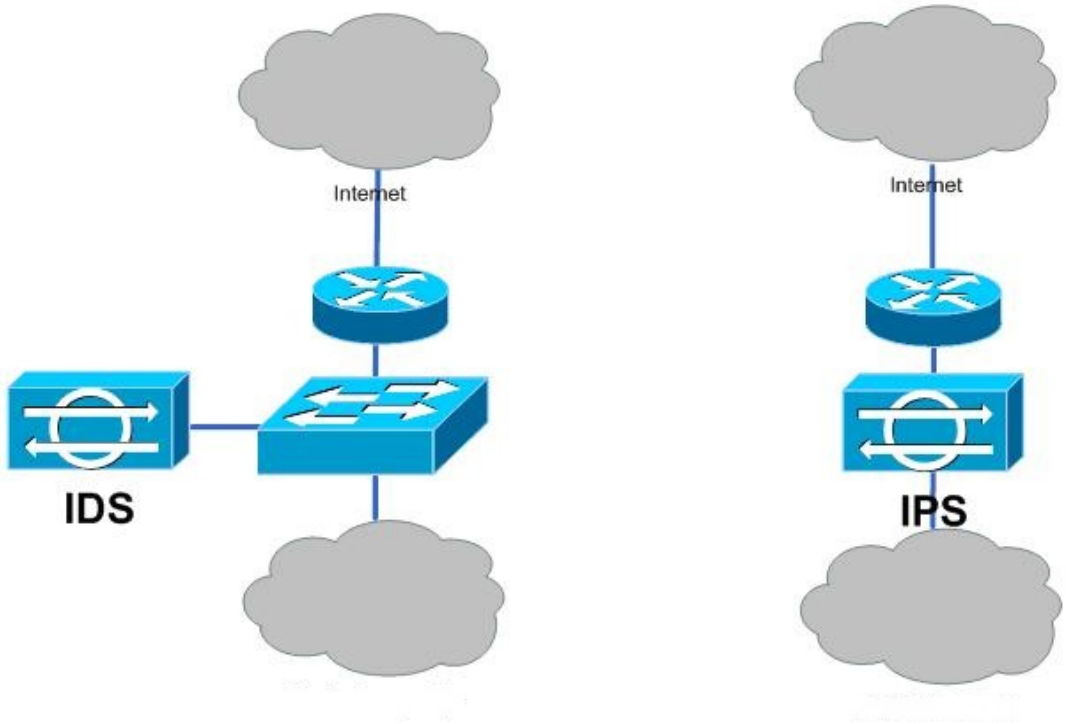

Figure 7: Intrusion management model

As the size of networks has been continuously growing since 1990's till current date, more network devices have been needed to be managed efficiently, exposing a trend in network management that moves from a centralized architecture to an everyday more and more distributed one. Not only there is no reason to think this trend will stop, but it will burst even more intensely in years to come due to the increasing size, management complexity, and real-time service requirements of today's networks. Concerning to an Internet Service Provider, voice, data, and multimedia services at this time converge onto a single network with increasing heterogeneity of underlying wireless and optical networking systems, while these services should be cost-and-resource-efficiently

delivered with ensured user satisfaction. To this end, an ISP is forced to switch the focus from traditional network Quality of Service (QoS) parameter to user Quality of Experience (QoE), which describes the overall network's performance from the user perspective. High network QoS may, in many cases, result in high QoE, but not always. Optimizing end-to-end QoE must consider other contributing factors such as the application-level QoS, the capability of terminal equipment and customer premises or subjective user factors. Therefore, new challenges appear demanding better scalability on network management designs as current paradigms do not suffice. In regards to this need, a node for analytics has been implemented recently: such device would supply highly precise analysis and detailed information about the transient performance of the network determined directly by the hardware in real time (since inherently experiences from scalability challenges in distributed deployments) with the purpose of predicting any undesirable anomaly in the network at a specific future's moment (congestion, QoS degradation…). Once the prediction is made, the PDP's are able to choose some particular policies, as mentioned before, aiming to prevent the unwanted situation. For example, cPacket Networks has developed a software solution integrated in its hardware, called SPIFEE [146], which offers such predictive characteristics.

8.4 Big Data technologies

The main challenge to address the proactive paradigm outlined in previous sections lies in the big amount of data that have to be managed in real or almost real-time by the Analytics Function. Therefore, Big Data technologies are a cornerstone for the paradigm:

- Big data has been a much discussed subject over the last five years or so. It has gone from being an expertise area surrounded by considerable hype and confusion, to a foundation for businesses and even industries.
- Google and Amazon are examples of "Internet companies" that would not exist if it was not for big data, but many other companies do leverage the power of big data techniques and analytics.
- The market for big data is really taking off at the moment. In comparison with the ICT market as a whole, big data connected services grow 6 times as fast.
- Estimates from IDC (2013) say that the market will amount to $32.4 billion in 2017 [36]. McKinsey estimates that it has a potential value in US Health Care, of $300 billion of annual savings (12% of total US health care cost) [35].

The real challenge that Big Data poses is not only related to storing large volumes of information but to how to manage large volumes of information and how to subsequently treat said information. Big Data makes reference to data sets with sizes unmanageable by commonly used software tools, at least within a bearable elapsed time. The sizes we are talking about vary across time; what today is considered Big Data it could not be in five years from now. As of 2014, data sets from few terabytes to many petabytes qualify. Today much of the industry describes big data following the "3Vs" model, defined by the Gartner Group: "Big Data is high volume, high velocity, and/or high variety information assets that require new forms of processing to enable enhanced decision making, insight discovery and process optimization" [64].

Nowadays the volume of data generated, stored, and mined has become relevant to businesses, governments, and consumers, even to the point of transforming everyday's lives. Furthermore, the real-time and high-frequency nature of the data (the *velocity* in "3Vs") must be also taken into account, so the ability to estimate metrics immediately is adding considerable power to prediction to a level never seen before. The use of vast amounts of separate data sets for analysis to make better decisions and enhancing productivity, i.e. combining different kinds of data sets (variety), will become the basis for companies by reducing waste and increasing the quality of products. Increasingly, companies will need to access third-party data to integrate it with their own.

Nowadays the use of Big Data is widespread in many both public and private sectors and is used in many applications [65]. Examples of sectors and applications which are using Big Data technology include:

- Scientific Research:
  - Physics: The Large Hadron Collider (150 million sensors delivering data 40 million times per second, the data flow represents 25 Petabytes annually) [66] [67] [68].
  - Astronomy: The Sloan Digital Sky Survey (at a rate of 200 GB per night, it has amassed more than 140 terabytes of information) [69].
- Weather Forecast: NASA Center for Climate Simulation (32 Petabytes from observations and simulations) [70].
- Politics and Society: Barack Obama's successful re-election campaign in 2012 [71].
- ICT in Merchandising:
  - eBay.com Data Warehouse (7.5 Petabytes) and Hadoop Cluster for search, consumer recommendations and merchandising (40PB) [72].
  - Walmart databases (1 million customer transactions per hour, more than 2.5 Petabytes of data) [69].
- Social Networking: Facebook users generate 50 billion photos [73].
- Internet Search: In 2012, Google handled 100 billion searches per month [74]. Google stores each and every search a user makes into its databases.
- IoT: In 2012, Intel introduced the terms “brontobyte” (1 followed by 27 zeroes), and “gegobyte” (10 to the power of 30). A “brontobyte” could be used to describe the order of magnitude of the sensor data generated by the Internet of Things [75].

It is unquestionable the fast growth of data generation in the last years and this trend will continue in the future, specially bearing in mind our everyday more connected society; with smartphones and wearable products becoming present in our lives it will not be surprising to soon reach a moment where there are more of these gadgets –connected and generating data– than people in the Earth. Being able not just to collect but to analyze it will be of huge value from both an economic and a social point of view.

But a controversial issue arises: Privacy. The magnificent benefits of Big Data are moderated by concerns over data protection. Privacy defenders fear that Big Data will lead to some kind of profiling, as racial discrimination. Finding the right balance between privacy risks and Big Data rewards may be one of the biggest public policy challenges of our time.

8.4.1 Tools

Beyond the already-mentioned 3Vs model, there are actually many Big Data definitions in literature, and all of them are also important because any of them stresses some relevant characteristics that have to be taken into account and translate into different technologies and tools. In [33] for example, the authors focus on its characteristic attributes, like very large volumes of a wide variety of data, growing at a very high velocity. In [36] they simply define Big Data as datasets whose size is beyond the ability of typical database tools. Even if the latter is a subjective definition, it includes an across-sector definition of what a dataset must be to be intended as Big Data. Other important differences among Traditional Data and Big Data are in the structure and the source: Big Data repositories are often semi-structured or un-structured. Data source is likely to be distributed in opposite to the centralized collection manner of the traditional datasets. Literature is full of Big Data state-of-the-art surveys, [37] being, probably, the most exhaustive.

In general, most of the technologies involved in Big Data analytics have to be redesigned: often, it is not enough to simply adapt these tools to the new magnitude of the problems. Even the Data Storage had to be adapted because Relational Database Management Systems proved to be not effective anymore: hence, in the last years we have witnessed the introduction of Distributed File Systems like Google File System [38] and its open source derivative HDFS [39].

For its schema-free feature, but also for the easy replication, eventual consistency, and large amount of data support, NoSQL databases have become among the most adopted in Big Data environment. In particular, among the column oriented databases, the ones storing data by column instead of by rows, we should mention Bigtable [40] by Google (and its open source derivative HBase [41]), and Cassandra [42] by Facebook. Document databases, instead, are able to support more complex structures: the most popular are MongoDB [43] and SimpleDB by Amazon [44].

Since NoSQL databases lack of support of declarative expression or query and analysis operation, it is difficult for traditional parallel models such as MPI [45] or OpenMP [46] to implement parallel programs in Big Data environment. Thus, many programming models have been introduced to solve specific environment applications.

Programming models, as Big Data analytics, are divided in two categories, according to processing time requirements: Streaming or Batch Processing.

Streaming processes assume that potential value of data depends on data freshness. Only a portion of the data stream is stored in memory. Batch processing, instead, assume that all data is stored and then processed. This kind of processes typically assumes complex data storage and management systems, while streaming ones do not.

MapReduce [47] is probably the most popular example of generic, batch-based, processing model: it enables automatic parallelizing and distribution of work-intensive application over clusters of devices. MapReduce is based on two main phases, called Map and Reduce; between the two phases, the framework groups together the intermediate results according to a key value and delivers them to a user-defined Reduce function. Hadoop MapReduce, built over Google's MapReduce, is the most spread MapReduce distribution for data analysis. Many companies have built their own SQL framework on the top of MapReduce in order to use it for traditional database process: Pig Latin [48] by Yahoo and Hive by Facebook [49] are only two among other numerous frameworks. Hadoop is a tool which fit ideally for the vast majority of Big Data problems, but it fails dramatically when the typical low-latency requirement of real-time services is needed. To address this limitation, other technologies been developed. Apache Spark [50], a new distributed framework, is spreading around the world: like Hadoop, Spark can be used to examine data that are too large to fit into a tradition dataset, but with a 100x performance increase in respect to Hadoop. Furthermore, it can deal with data streams and interactive processes thanks to its Resilied Distributed Datasets (RDD) architecture. This feature allows it to support both interactive and iterative jobs. Storm [51] and S4 [52], instead, are the most spread distributed stream programming platforms. They share some features, like the graph representation of the jobs and the event handling. S4 architecture is strictly decentralized and symmetric while Storm adopts a master-slave fashion.

Finally, another family of models, the Graph Processing Model, can be introduced: they have been developed as the results of new types of applications/domains which are better expressed using graph models, e.g. social network connections. The most important are Google Pregel [53], Giraph [55] (open source counterpart to Pregel), GraphX [54] (Apache Spark API for graph-parallel computation) and GraphLab [56].

As mentioned previously, Big Data environment should provide its entirety hardware, infrastructure software, operating software, management software, APIs (Application Programming Interface) properly defined and even specific development tools software. The architecture, in short, must be

able to meet the basic requirements, somehow, we can say that are the classics of all data processing architecture: Capture, Integration, Organization, Analysis and Actions.

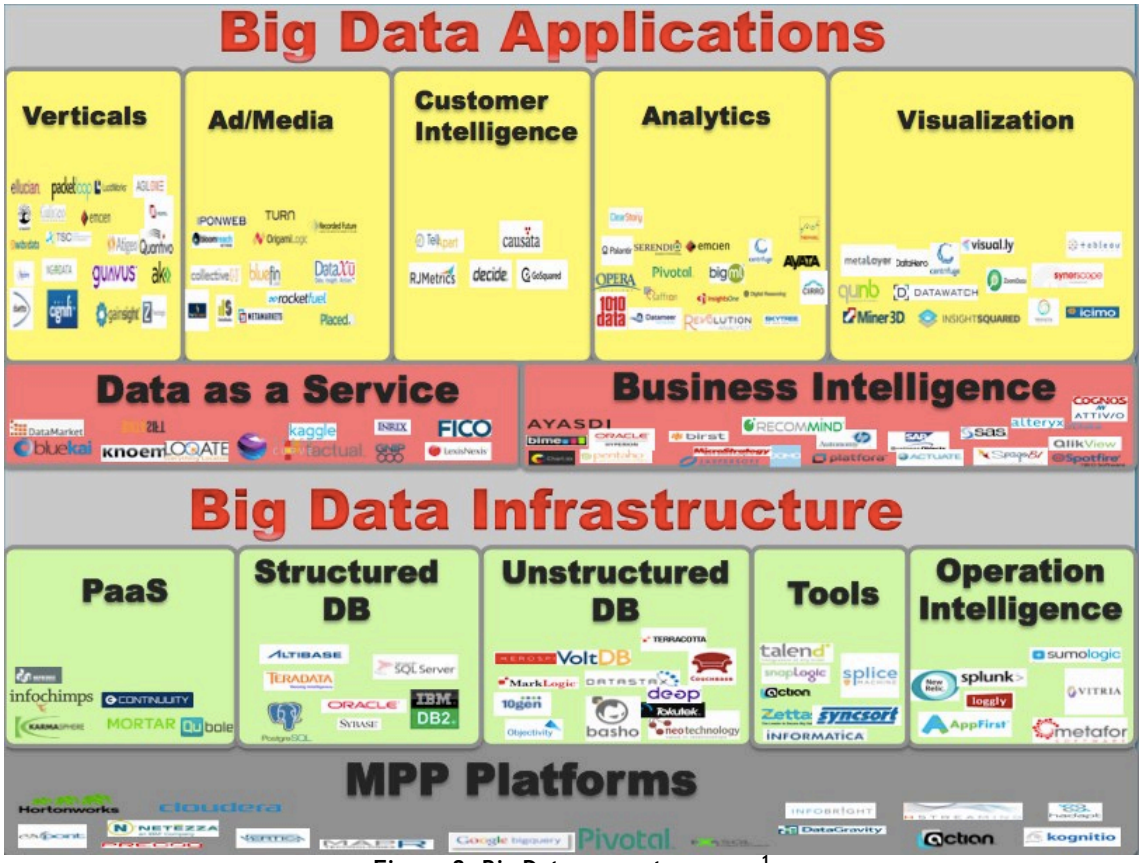

Figure 8: Big Data ecosystem map.[1]

Some of the most relevant components that have become part of the Big Data ecosystem can be summarized by the categories shown below:

- **Getting Data**: Most of the Big Data originates outside the MapReduce cluster. These tools will help to get data:

Tool	Remarks
Flume	Gathers data from multiple sources
Sqoop ("Sql-to-Hadoop")	Transfers data between Hadoop and Relational Databases
Kafka	Distributed publish-subscribe system.
Scribe	Distributed log gatherer, originally developed by Facebook.
Chukwa	Data collection system.

- **NoSQL stores**:

Tool	Remarks
HDFS	Storage system based on a distributed file system
HBase	NoSQL built on top of Hadoop.
Cassandra	NoSQL store (does not use Hadoop).
MongoDB	NoSQL database System document oriented. It is an

[1] Luke Lam. "Big Data Ecosystem". Internet: http://datacenter.opentray.com/2013/07/big-data-ecosystem/, Jul. 11, 2013.

	open source project.
Redis	Key value store.
Amazon	SimpleDB Offered by Amazon on their environment.
Voldermort	Distributed key value store developed by LinkedIn.
Hypertable	Data base model highly scalable, high performance data. Distributed as open source.
Accumulo	A NoSQL store developed by NSA.

- **Querying Data:**

Tool	Remarks
Hive	The data can be queried using SQL rather than writing Java MapReduce code.
Impala	Provides real time queries over Big Data
Pig	Pig provides a higher level data flow language to process data. Pig scripts are much more compact than Java MapReduce code.
Apache Drill	that allows interactive analysis of massive data clusters
Presto	Developed by Facebook, provides fast SQL querying over Hadoop
Apache Solr	platform for natural language searches

- **Work-Cluster Management:**

Tool	Remarks
Google MapReduce	Batch process created for distributed data processing
Yarn	Evolution of the concept of Apache Hadoop
Mesos	Cluster management system that provides an efficient proposal for load balancing and resource management for distributed applications

- **Real Time Processing:**

Tool	Remarks
Storm	Platform for real time data streams processing. It is scalable, fault-tolerant and ensures that the data are processed.
Spark	Cluster computing system designed to process information quickly
S4	Distributed Stream Computing Platform

- **Data Analysis:**

Tool	Remarks
Mahout	Machine Learning library on top of Hadoop.
MLlib	Machine Learning library on top of Spark.
Giraph	Fast graph processing on top of Hadoop.
GraphX	Analytics for graph structures over Spark.
Dato	Formerly GraphLab. Machine Learning framework for graph structures integrated with Spark, Hadoop and others.
SimSQL	Relational database system that compiles SQL queries on top of Hadoop

Samoa	Framework for Scalable Advanced Massive Online Analysis on top of S4, STORM and SAMZA
Weka	Collection of machine learning algorithms for data mining tasks

- **Coordination**:

Tool	Remarks
ZooKeeper	ZooKeeper is a centralized service for maintaining configuration information, naming, and providing distributed synchronization.
Book keeper	Distributed logging service based on ZooKeeper.

- **Administration:**

Tool	Remarks
Apache Ambari	Hadoop Management
Cloudera Manager	Cloudera framework Management

- **Monitoring Systems:**

Tool	Remarks
Hue	Developed by Cloudera
Ganglia	Overall host monitoring system. Hadoop can publish metrics to Ganglia.
Open TSDB	Metrics collector and visualizer.
Nagios	IT infrastructure monitoring.

- **Work flow Tools / Schedulers:**

Tool	Remarks
Oozie	Orchestrates MapReduce jobs.
Cascading	Application framework for Java developers to develop robust Data Analytics and Data Management applications on Apache Hadoop.
Scalding	Scala library that makes it easy to specify Hadoop MapReduce jobs. Scalding is built on top of Cascading.
Lipstick	Pig work flow visualization

- **MapReduce in the Cloud:**

Tool	Remarks
Amazon Elastic MapReduce (EMR)	On demand Hadoop on Amazon Cloud.
Hadoop on	Rackspace On demand and managed Hadoop at Rackspace
Hadoop on Google Cloud	Hadoop runs on Google Cloud
Hadoop Streaming	MapReduce in other languages (Ruby, Python)

- **Analytics:**

Tool	Remarks
Pentaho	Business Intelligence tool developed under the philosophy of Open Source
Tableau	Tools for instant access to data and visual analytics

QlikView	Business Intelligence tool
Talend	ETL (Extract, Transform and Load) tool
Jaspersoft	Advanced BI platform.

9. State-of-the-Art (applied to use cases)

9.1 Use Case # 1. Network Anomaly Detection

The problem of network anomaly detection has been extensively studied during the last decade. Most of the approaches analyze statistical variations of traffic volume (e.g. number of packets, bytes or new flows) and/or traffic features (e.g. IP addresses and ports), using either single-link measurements or network-wide data. A non-exhaustive list of standard methods includes the use of signal processing techniques (e.g. ARIMA –Autoregressive Integrated Moving Average– modeling, wavelets-based filtering) on single-link traffic measurements [13][14], PCA (Principal Component Analysis) for network-wide anomaly detection [16] [17] [18], and Sketches applied to IP-flows [15] [19].

The simultaneous detection and characterization of traffic anomalies has also received quite a lot of attention in the past, but results are few and present important limitations, either because they rely on some kind of training data and/or anomaly signatures, or because they do not provide meaningful and tractable information to a human network operator, who has to take the final decision about the nature of the detected problem. Authors in [16] characterize network-wide anomalies in highly aggregated traffic (Origin-Destination flows or OD flows for short), using PCA and the sub-space approach [18]. An important limitation of this approach is that the information obtained from OD flow data is too coarse-grained to provide meaningful information to the network operator. Papers like those of Lakhina et al. [17] or Biang et al.[19] detect and characterize anomalies using finer-grained traffic information, basically applying the same PCA approach to the sample entropy of the empirical distribution of specific traffic features. One clear limitation of these approaches is that the information they provide is not immediately usable and easy-to-understand by the network operator, who may not even be familiar with concepts distant from his tasks such as sample entropy. Besides, the PCA approach is highly sensitive to noise when used for anomaly detection [20] [21], requiring in practice a fine-tuning and data-dependent calibration step to work.

UNADA (Unsupervised Network Anomaly Detection Algorithm) [22] falls within the unsupervised anomaly detection domain, a novel research area that has drawn quite a lot of interest in the research community, but that still represents a rather immature field. Most work on unsupervised network anomaly detection has been devoted to the Intrusion Detection System (IDS) field, generally targeting the detection of network intrusions in the very well-known KDD'99 dataset. The great majority of the detection schemes proposed in the literature are based on clustering techniques and outliers detection, being [23] [24] [25] some examples. The objective of clustering is to partition a set of unlabeled patterns into homogeneous groups of “similar’” characteristics, based on some similarity measure. Outliers detection consists in identifying those patterns that do not belong to any of these clusters. In [25], authors use a simple single-linkage hierarchical clustering method to cluster data from the KDD'99 dataset, based on the standard Euclidean distance for inter-pattern similarity. Eskin et al. [23] reports improved results in the same dataset, using three different clustering algorithms: the Fixed-Width clustering algorithm, an optimized version of the k-NN algorithm, and the one class Support Vector Machine (SVM) algorithm. Leung and Leckie [24] present a combined density-based and grid-based clustering algorithm to improve computational complexity, obtaining similar detection results.

Previous work of some ONTIC partners permits to automatically characterize network traffic anomalies [26], but using a-priori well-defined anomaly signatures. Closer to our current work, authors in [27] present URCA (Unsupervised Root Cause Analysis), a two-steps algorithm to characterize network anomalies in an unsupervised fashion. URCA uses as input the traffic in the anomalous time slots detected by any generic time-slot-based detection algorithm [28]. In the first

step, it identifies the anomaly by iteratively removing from the anomalous time slots those flows that seem normal. In the second step, the algorithm uses a hierarchical clustering method to characterize the particular flows identified as anomalous. We identify some serious drawbacks and omissions in URCA: authors claim that the approach is unsupervised, which is not true, simply because it uses previously labeled anomalous events for the characterization. As in previous works, the algorithm uses difficult-to-interpret traffic descriptors for the clustering step (e.g. sample entropy of the distribution of IP addresses, aggregated at different levels), obscuring the comprehension of the network operator. Finally, the algorithm removes those flows that seem normal before the characterization step, which drags possible errors to the clustering step.

The Unsupervised Anomaly Detection and Characterization algorithm [29] from some ONTIC partners presents several advantages w.r.t. current state of the art. First and most important, it works in a completely unsupervised fashion, which means that it can be directly plugged into any monitoring system and start to work from scratch. Secondly, we perform anomaly detection based not only on outliers detection, but also by identifying small-clusters. This is achieved by using different levels of traffic aggregation, both at the source and destination of the traffic; this additionally permits to discover low-intensity and distributed anomalies. Thirdly, we avoid the lack of robustness of general clustering approaches, by combining the notions of Sub-Space Clustering [30] and multiple Evidence Accumulation [31]. In particular, this algorithm is immune to general clustering problems like sensitivity to initialization, specification of number of clusters, or structure-masking by irrelevant features. Fourthly, the algorithm performs clustering in low-dimensional feature spaces, using simple traffic descriptors like number of source IP addresses or fraction of SYN packets. This simplifies the characterization of the anomaly, and avoids well-known clustering problems when working with high-dimensional data [32]. This algorithm ranks the multiple evidence of an anomaly detected in different sub-spaces, combining the most relevant traffic descriptors into a compact and easy-to-interpret signature that characterizes the problem. This permits to reduce the time spent by the network operator to understand the nature of the anomaly. Finally, this algorithm is designed to work in an on-line fashion, analyzing traffic from consecutive time slots in near real time. This is possible even when working with large number of traffic descriptors, because the sub-space clustering and the evidence accumulation algorithms are perfectly adapted for parallelization (see [29]).

9.2 Use Case # 2. Proactive Congestion Detection and Control System

Internet Service Providers

The growth of the Internet has increased the need for scalable congestion control mechanisms in high speed networks. The protocols currently deployed suffer from performance degradation as the bandwidth-delay product increases. The proposals to face this issue have mainly followed two paths. First, modified versions of TCP, which rely on packet drops or ECN bits, were proposed to improve performance while maintaining scalability. Second, new explicit congestion control approaches, based on closed-control loops, were proposed. These latter approaches provide the sources with explicit feedback about the congestion level of the network. The feedback sent by the routers to the sources is usually an explicit window size or an explicit sending rate. These approaches are claimed to achieve fast convergence and fair distribution of network resources among sessions. However, in the big data scenario that dominates nowadays Internet, the variety of technologies in use and the volume and velocity of the data traversing them severely hampers the performance and the applicability of the existing techniques for congestion control.

Mobile Communication Service Providers

In a typical mobile scenario, when a user terminal (i.e. a smartphone) starts a Packet Data Network (PDN) connection, a default bearer is established. Said bearer is characterized by the user terminal (UE) IP address and certain Quality of Service (QoS), meaning that all the traffic running over the

same bearer will obtain the same treatment in the Radio Access Network (RAN) and in the transport network in terms of QoS and priority. More than one bearer can be established in order to give different treatment in the radio network to different services. Upon a congestion situation, the RAN may apply admission control and even tear down established bearers based on the bearers' priority. This solution based on dedicated bearers provides service and subscriber differentiation. However the majority of mobile data traffic (e.g. Internet or over-the-top services traffic) is currently delivered over default bearers.

Certain alternatives have been explored. For example, congestion-awareness, based on statistics regarding what locations are prone to be congested at certain periods of time, is a more advanced solution provided by vendors like Ericsson. With such an approach, a Policy and Charging Rules Function (PCRF, see section 9.3.2.3) can make policy decisions based on these statistics and also considering the current UE location information and time. In order to prevent congestion the PCRF can decide to limit the bandwidth assigned to certain users for the total traffic or for specific services. Statistic data is populated in a database accessible by the PCRF. This data is mainly a table containing locations and congested time periods.

The main handicaps with this type of solution are that operator must maintain this information as much updated as possible and that location information received in the PCRF is not always accurate due to the signaling penalty that may cause to propagate to the PCRF all the location changes of all the users. Besides, the congestion decisions are based on historical preconfigured data, and this means that the PCRF decision is purely a prediction. Depending on accuracy of this prediction the goodness of this solution can vary, meaning that it can be decided to throttle traffic unnecessarily.

Next Steps in Congestion Control

The scenarios described above clearly show that problem of congestion control in the Internet and mobile networks still presents many open issues, and is undoubtedly in need of new research and engineering solutions. The current state of the art in the fields of big data, data analytics and machine learning open up a whole landscape of opportunities to try to address this problem from new perspectives.

9.2.1 Bandwidth Allocation and Congestion Control Protocols

There exists in the literature a wealth of protocols that aim to maximize bandwidth utilization while preventing congestion events from happening. Many of these protocols are conceived over a distributed computing model, which allows generalization to most network implementations. In order to gain a full understanding of recent proposals, it is convenient to have an overview of the evolution of these techniques from the very first ones. Some of these protocols are described below.

In his seminal work, Jacobson mentioned the possibility of equipping routers with mechanisms to notify congestion to sources [79]. This idea took shape in several proposals such as Random Drop gateways [82] and Drop Tail gateways, which deliberately drop packets in order to raise the alert in sources. Early Random Drop adds a slight sophistication to this notion by attempting to predict the growth of queues based on their behavior patterns. When the average queue length surpasses a specific threshold the congestion control mechanisms is activated.

9.2.1.1 Active Queue Management (AQM)

Many of the most relevant protocols for congestion control available in the literature can be classified as belonging to the AQM class. In AQM protocols, sources receive congestion information from the network implicitly via packet drops or explicitly using the ECN field of the IP packets. ECN [58] [81] is a mechanism that allows links to explicitly notify congestion to sources using a flag in

the IP header. This is an alternative to packet discarding, which can be ambiguous to interpret. ECN was finally added to the standard IP header years after this initial proposal [83]. Some of the most relevant AQM protocols are described below.

Random Early Detection is a congestion control system that computes the probability of a congestion event happening based on information stored in links [80]. Depending on the congestion level, which is calculated based on the evolution of the buffers, sources can be instructed to adapt their transmission rate accordingly. This system was inspired by the need to stop sources from sending packets between the moment congestion happens and the time at which they receive the corresponding notification. The main drawback of RED is that its success depends heavily on its adequate tuning, which can be challenging [84] [97].

Random Exponential Marking (REM) [78] shows two distinctive characteristics:

1. It tries both to determine the correct transmission rate for each source and to keep buffers clear at the same time.
2. The estimated probability of losing a packet is calculated as a function of the congestion levels of all the links in the path.

In REM, the probability of marking a packet as a herald for congestion depends on a variable called price, present at each link, which is updated periodically. Other notable AQM protocols are Adaptive Virtual Queue, Blue [98] and Stochastic Fair Blue [99].

9.2.1.2 Control Theory

The model of Control Theory consists in periodically acting upon a signal in order to adjust it to the desired levels. The modified signal is permanently fed back to the controller to minimize the error between the output and the expected values. This model has been used to maximize router utilization while retaining a fair share of the resources between sessions [86].

Explicit Congestion Control Protocol (XCP) [77] was conceived to address some of the problems of TCP. It maintains three values in the packet headers: H_cwnd and H_rtt represent the corresponding TCP values. H_feedback represents the rate demanded by the source. When a packet crosses a link, the value of H_feedback is modified according to the current circumstances. When the source receives an ACK carrying the modified feedback variable, it recomputes it as H_feedback = max(cwnd + H_feedback, s), where s is the packet size.

An XCP link uses two different controllers:

- An efficiency controller, responsible for maximizing utilization.
- An equal share controller, responsible for calculating the feedback value with the aim of keeping a fair share.

In [85], a proportional integrator controller was proposed to address some of the issues present in RED. This controller relies on the assumption that the derivative of queue size converges to zero if the transference function stabilizes. In [59] and [87], Rate Control Protocol (RCP) is described. RCP is a congestion control and transmission rate allocation protocol based on one basic principle: flows must complete as quickly as possible. It was designed based on the assumption that TCP and XCP do not honor this requirement, which makes them perform poorly on real-world scenarios where a majority of flows are short-lived.

RCP proposes to explicitly calculate the transmission rate for each session instead of progressively increasing or reducing the congestion window. RCP favors simplicity over accuracy.

The transmission rate is calculated as follows:

- Every link keeps and periodically updated a value R(t) that represents the bandwidth allocation to all of its sessions
- Every packet header has a value R_p that represents the desired transmission rate. When a link receives a packet, it changes $R_p$to R(t) if R_p > R(t).
- The source ends up transmitting at R_p, the minimum rate encountered in its path.
- Links update R(t) according to a specific equation.

This approach was later improved by RCP-AC, which addresses the weakness of RCP when facing sudden changes in traffic [60] and PIQI-RCP [88] which recalculates the rate using a Proportional-Integral controller.

9.2.2 Other proposals

Various different techniques have been proposed for better bandwidth allocation and enhanced congestion control. Variable-Structure Congestion Control Protocol (VCP) claims to achieve a bandwidth distribution equal to that of XCP using the ECN bits only [89]. In contrast to XCP, VCP routers are only responsible for the calculation of the congestion level. The authors of MPCP [91] conclude that using 2 packets to notify congestion provides an optimal performance. BMCC [92] claims that a performance equal to that of RCP can be achieved using an ADPM approach –packets are marked if the hash function of some constant header field is less than the current link load. UNO [90] encodes a 3-bit long congestion notice using just one bit in several packets. In [134], Salamatian et al. posit that network congestion can be perceived as the probability that a packet will be lost. Consequently, they understand loss as a Hidden Markov Model in which the observed process consists of the losses experienced at the source, while the process itself is the sequence of discretized packet loss probabilities. This article states that the process can be effectively modeled using a 4-state Markov chain. In order to estimate the correct number of states, the authors use the concept of entropy from Information Theory.

9.2.2.1 EERC Congestion Control and max-min fair allocation

EERC protocols (Explicit End-to-End Rate-Based Flow Control) address congestion by explicitly telling hosts their corresponding transmission rate. An optimal bandwidth allocation criterion for these protocols is max-min fairness. Intuitively, this criterion consists in sharing the network resources equally while maximizing usage if possible. If a session suffers stronger restrictions than others, the resources that it cannot use will be allocated to others.

9.2.2.2 Distributed max-min fair protocols

Max-min fairness is easily achieved using a centralized algorithm. In a computer networks context, however, it is necessary to attain it in a distributed fashion in order to maintain scalability. There exist certain protocols in the literature that achieve a max-min fair distribution, but they are not scalable. The techniques described in [93] and [94] do it using only one queue per session in every link and a round-robin scheduler. In [95], Bartal et al. proposed a protocol that used ATM cells in order to calculate and store information about each session on every link. In [96], Cao et al. described a similar method and introduced the concept of Utility max-min fairness, based on the needs of each application. Unfortunately, all of these methods suffer from poor scalability. More recently, a protocol that tackles this problem was proposed in [57] . The max-min fair allocation is achieved without storing information per-session at the links, and the process converges in linear time.

9.2.3 Congestion Control Protocols today

The problem of bandwidth usage maximization and congestion control in generalized network environments is still an active topic of research today, as shown by the constant trickle of new protocols and proposals. Some of the current research focuses on designing mechanisms that get along well with the current standards (namely TCP CUBIC [103]), while others try to design new protocols from scratch. Some of the most relevant publications from the last few years are discussed below.

In [103], ATRED is proposed. This mechanism attempts to overcome the difficulty of tuning RED by adding an adaptive mechanism for its dynamic adjustment. In [104], the authors introduce a framework of Markov Decision Processes for queue management in a bottleneck. They also propose a heuristic that manages to desynchronize the flows, which results in better utilization of the network resources, even beyond classical successful DropTail-based approaches and RED. In [105] TCP-FIT is proposed. This method makes changes to the congestion window dynamically according to an estimation of the packets that are currently queued in network buffers. In [106] [105], CUBIC-FIT is described. It attempts to remain robust to wireless loss via a delay-based approach while staying friendly to CUBIC dominated environments.

The explosion of multimedia and streaming content on the Internet has spurred specific research and engineering efforts. One of the first proposals to take this transformation into account was TCP-Friendly Rate Control (TFRC), described in [107]. In [108], the revised version of TFRC, which was designed to cope with the variable rate of modern streaming applications, is analyzed. In addition, a new method (Faster Restart) is proposed. In [109], the authors claim that delay-based algorithms are a good choice to manage multimedia traffic. They propose a method to determine if a TCP flow obtained from an Internet traffic capture behaves as though the generating source were employing a delay-based algorithm, and use this technique to infer the amount of traffic that is governed by this type of congestion control scheme.

The authors of [110] argue that the handshake process inflicts significant penalties on short-lived flows, which constitute the majority of TCP connections in nowadays' Internet. In order to address the problem, they propose TCP Fast Open (TFO), a mechanism that allows for the exchange of data during the handshake. TFO was merged into the Linux kernel from version 3.6 for clients and version 3.7 for servers. It is also supported by Google Chrome. In [111], a delay-based congestion control mechanism is proposed. Techniques of this family try to infer if loss is due to congestion based on delay measurements. Unlike previous proposals along those lines, the approach presented in this paper is not dependent on path-specific knowledge in order to reach meaningful conclusions.

In [112] the authors focus on an approach that has been extensively studied during the last decade. This strategy consists in regarding the issue congestion control as an optimization problem which they solve using a primal-dual algorithm. The resulting equations reveal a stability condition that can be used to choose the parameters for TCP and AQM schemes and even to design new protocols.

In the last few years, a new family of congestion control protocols providing what is called a *Less-that-best-effort* service has gained momentum. These protocols aim to minimize their impact on the network by using only residual resources so that delay-sensitive connections can achieve a better performance. This approach, thus, is adequate for applications that do not have strong time-related constraints. Even though they could yield some improvements, there are unresolved issues regarding their deployment [113].

The initial size of the congestion window of TCP (IW) remains a controversial issue. Researchers at Google made an argument for increasing this value a few years ago [114]. They propose an increase to at least ten segments, which according to them yields improvements of approximately 10% in HTTP response times, especially in high RTT and bandwidth-delay product (BDP) networks. In [115],

a game-theoretic approach for choosing this value is proposed. The initial size of the window is chosen using a function that depends on the size of the flow and that has two parameters. The authors claim that a fixed value for one of these parameters, which results in an IW four times as large as the standard one for small flows, yields significant improvements with respect to the constant size currently in use.

9.2.4 The Role of Big Data Analytics

After reviewing available methods for distributed bandwidth allocation and congestion control, it becomes evident that there is a variety of open issues. No single protocol is able to cope with the diversity and unpredictability of actual networks, in part because of the difficulty of developing deterministic models for traffic behavior. These difficulties suggest that new approaches must be explored in order to achieve sufficiently flexible and effective techniques. Knowledgeable analysis of vast records of network traffic can provide the grounds for the design of better-performing algorithms. In turn, online Machine Learning techniques can ensure an optimal tuning of these algorithms for an increased effectiveness in any environment.

In RFC 6077 [116], an outline of the most important challenges in Internet Congestion Control was provided. They key elements to describe the open issues are (1) heterogeneity: the variety of deployed technologies in terms of capacity, latency, topologies and algorithms is enormous; (2) stability: the stability of computer networks has been extensively analyzed from a control-theoretic point of view. However, the complexity of today's networks makes it impossible to accurately model traffic behavior. Moreover, the impact of such a primitive mechanism as Slow-Start on stability is still not clear; and (3) fairness: the definition of this concept in the context of Internet traffic is not yet agreed upon, even though its importance in determining the research goals of the future is unquestionable.

The plethora of existing congestion control protocols and schemes along with the scarcity of real-world deployments and the continuance of age-old open issues reveal that this scenario could immensely benefit from innovative approaches. Due to the heterogeneity of the Internet pointed out in RFC 6077, it is unlikely that a single protocol tested on simplified simulated environments can actually make a significant impact on congestion-related problems. The analysis of vast amounts of actual network traces can provide insights on the behavior of Internet traffic, which can in turn allow for the design of generalized, dynamic and scalable methods for congestion control.

One of the main challenges that network service providers face when it comes to deploying new congestion control protocols is the adequate tuning of its parameters. An algorithm might perform well on a given scenario but poorly on a slightly different one if it is not adequately retuned, which can be extremely difficult [84] [117]. The use of machine learning techniques along with real data collected from the Internet (such as the ONTS being gathered by the ONTIC project) can help infer those parameters as a function of the current network conditions. Hence, it is undoubtedly desirable to develop new scalable algorithms that can (1) be periodically retrained offline with sufficient frequency so as to reflect up-to-date trends in traffic dynamics and (2) analyze big enough amounts of data in real time so that inference can be performed with significant traffic samples.

Scalable algorithms with the ability to extract relevant information on big amounts of traffic traces can also help to detect long-term regularities. This can help design holistic approaches able to cope with the varying needs of a seemingly unpredictable environment.

Several research directions hint at the possibility of leveraging big data sets and statistical methods for the improvement of congestion-related performance issues on computer networks. In [118], the potential of using statistical models for estimating the likelihood of a congested buffer is shown. In [124], Support Vector Regression is used in order to predict TCP throughput based on a small set of

features. The authors claim that quite accurate results were obtained. Other examples of prediction techniques for network traffic and similar scenarios can be found in [119], [120], [121] and [122], and are further discussed in Deliverable D4.1 [2]. In [123], several AQM methods based on Artificial Neural Networks are evaluated in terms of performance, and are shown to outperform traditional techniques such as Adaptive RED, a Proportional-Integrator controller and REM.

It is therefore clear that different network scenarios could benefit from the use of Big Data Analytics and machine learning techniques to tackle congestion-related problems. Research in this field, however, is hampered by a series of limiting factors: (1) access to large-scale real-world traffic traces is very difficult, and it is essential for model fitting and technique validation; (2) many existing machine learning algorithms do not scale sufficiently well for the volumes of data that are generated in the Internet every second; (3) deployment of new techniques without sufficient testing on realistic data sets is generally not feasible.

The role of ONTIC in addressing problems related to congestion control is hence invaluable, and its position as holder of the ONTS data set extremely advantageous.

9.3 Use Case # 3. Dynamic QoS Management

9.3.1 Terminology

The term **Quality of Service** (QoS) is used to characterize different aspects ranging from the user's perception of the service (more tied to actual QoE) to a set of connection parameters necessary to achieve a particular service quality. Intrinsic QoS in packet networks is expressed by at least the following set of parameters that are meaningful for most IP-based services [100]:

- **Bit rate** of ongoing user data transfers available for the service or target throughput that may be achieved.
- **Delay** experienced by packets while passing through the network. It may be considered either in an end-to-end relation or with regard to a particular network element.
- **Jitter**: variations in the IP packet transfer delay. Again, it can be applied to an end-to-end relation or a single network element.
- **Packet loss rate**, usually defined as the ratio of the number of undelivered packets to the sent ones.

Class of Service (CoS) is defined by IETF as "The definitions of the semantics and parameters of a specific type of QoS" [101]. Services belonging to the same class are described by the same set of parameters, which can have qualitative or quantitative values. In network devices terminology, it refers to three bits that are used to indicate the priority of the Ethernet frame as it passes through a switched network. Different network protocols define in different ways the CoS attributes. Currently, concrete service classes are defined within IP-QoS architectures proposed by IETF, such as IntServ and DiffServ.

Differentiated Services Code Point (DSCP) is the first six bits of the ToS byte in the IP header. DSCP is only present in an IP packet. It contains the IP precedence bits: they are the three most significant bits of the ToS byte in the IP header.

Service Level Agreement (SLA). In [135], a SLA is defined as a negotiated agreement between a customer and the service provider on levels of service characteristics and the associated set of metrics. The content of SLA varies depending on the service offering and includes the attributes required for the negotiated agreement. It also must consist of responsibility rules for breaking the contract by the service provider as well as by the customer. An SLA should be expressed in a way intelligible to a customer.

In [136], the following additional concepts are defined:

- **Service Level Specification** (SLS) was introduced to separate a technical part of the contract from SLA. It specifies a set of values of network parameters related to a particular service.
- **Traffic Conditioning Agreement** (TCA) is an agreement specifying packet classification rules and traffic profiles as a description of the temporal properties of a traffic stream, such as the rate and burst size. In order to force a customer's traffic conformance to the profile particular metering, marking, discarding, and shaping rules are defined.
- **Traffic Conditioning Specification** (TCS). It is a set of parameters with assigned values that unambiguously specify a set of classifier rules and a traffic profile. A TCS is a technical part of both TCA and SLS

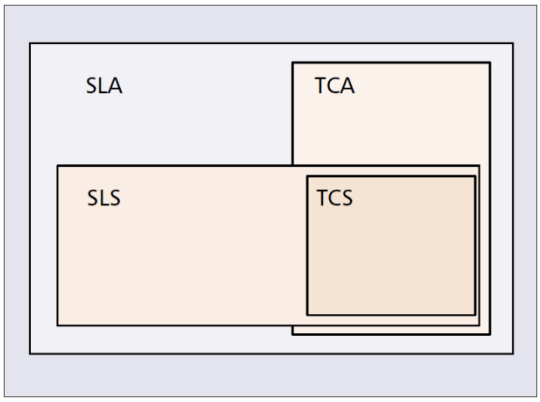

Figure 9: Relationship between SLA, SLS, TCA and TCS

9.3.2 Network-related elements

9.3.2.1 QoS on UMTS

9.3.2.1.1 UMTS QoS Classes

The Universal Mobile Telecommunications System (UMTS) is a third generation mobile cellular system for networks based on the GSM standard. Its specifications are developed and maintained by the 3GPP (3rd Generation Partnership Project). In [137], the UMTS QoS classes are defined based on how delay-sensitive each traffic type is:

- Conversational class.

  This scheme applies to telephony speech, as well as certain Internet such as voice over IP or video conferencing. Since real time conversation is always performed between peers of live end-users, the required characteristics for this scheme are strictly given by human perception. The preservation of time relation (variation) between information entities of the stream and conversational pattern (stringent and low delay) are fundamental for QoS.
- Streaming class.

  This scheme applies to the now highly prevalent one-way streaming media services. The time relations (variation) between information entities (i.e. samples, packets) within a flow must be preserved.
- Interactive class.

This scheme applies when the end-user requests data from remote equipment, e.g. web browsing, data base retrieval, server access, polling for measurement records and automatic data base enquiries (tele-machines).

Interactive traffic is characterized by the request response pattern of the end-user. At the message destination there is an entity expecting the message (response) within a certain time. Round trip delay time is therefore one of the key attributes. Another characteristic is that the content of the packets shall be transparently transferred (with low bit error rate).

- Background class.

  This scheme applies when the end-user sends and receives data files in the background. Examples are background delivery of E-mails, SMS, download of databases, and reception of measurement records. The destination does not expect the data within a certain time. The scheme is thus more or less delivery time insensitive.

9.3.2.2 QoS Architecture on UMTS

The Quality of Service Architecture on UMTS is defined in [137]. Network Services are considered end-to-end. It is the user that decides whether he is satisfied with the provided QoS or not.

A bearer service includes all aspects necessary to enable the provision of an agreed-upon QoS. These aspects are, among others, control signaling, user plane transport and QoS management functionality. Each bearer service offers its individual services using services provided by the layers below.

- End-to-End Service

  A Terminal Equipment (TE, the UE hardware equipment) is connected to the UMTS network by means of a Mobile Termination (MT, which controls the radio link; MT and TE are the elements of the Mobile Equipment, ME; ME and the SIM card –UICC, Universal Integrated Circuit Card– are the components of the UE). End-to-End Bearer Service consists of the various services offered by the UMTS Bearer Service that the UMTS operator provides. It is this bearer service that provides the UMTS QoS.

- TE/MT Local Bearer Service

  The TE/MT Local Bearer Service is outside the scope of the UMTS network.

- UMTS Bearer Service

  The UMTS Bearer Service provides the UMTS QoS. The UMTS Bearer Service consists of two parts, the Radio Access Bearer Service and the Core Network Bearer Service.

- Radio Access Bearer Service

  The Radio Access Bearer Service provides confidential transport of signaling and user data between MT and Core Network (CN) Edge Node with the QoS adequate to the negotiated UMTS Bearer Service or with the default QoS for signaling. This service is based on the characteristics of the radio interface and is maintained for a moving MT.

- Radio Bearer Service + Physical Radio Bearer Service

  The Radio Bearer Service covers all the aspects of the radio interface transport. This bearer service is provided by the UTRAN FDD/TDD or the GERAN, which are not discussed further in the present document.

- RAN Access Bearer Service + Physical Bearer Service

  The RAN Access Bearer Service together with the Physical Bearer Service manages the transport between RAN and CN. RAN Access bearer services for packet traffic shall provide different bearer services for QoS variety.

- Core Network (CN) Bearer Service + Backbone Bearer Service

  The Core Network Bearer Service of the UMTS core network connects the UMTS CN Edge Node with the CN Gateway to the external network. The role of this service is to efficiently control and utilize the backbone network in order to provide the UMTS bearer service that has been agreed upon. The UMTS packet core network shall support different backbone bearer services for variety of QoS.

- External Bearer Service

  The External Bearer Service is not further discussed here as this bearer may be using several network services, e.g. another UMTS Bearer Service from a different operator.

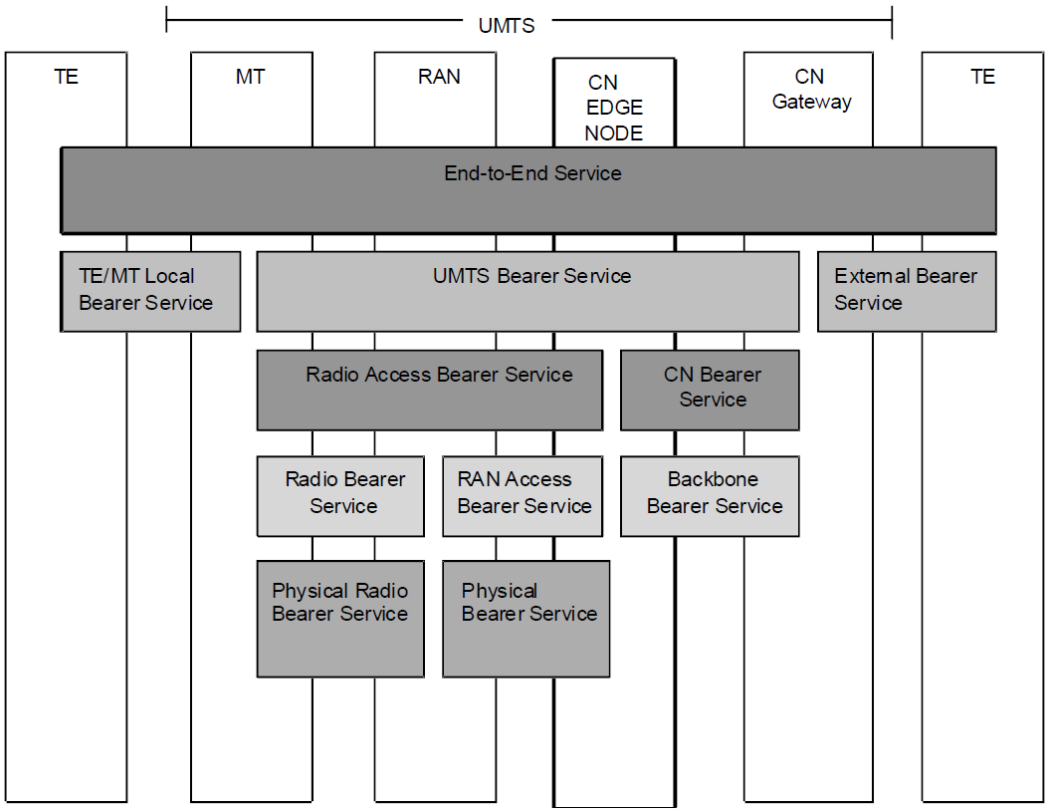

Figure 10: QoS Architecture in UMTS

9.3.2.2.1 QoS attributes

The UMTS bearer service attributes describe the service provided by the UMTS network to the user of the UMTS bearer service. A set of QoS attributes (QoS profile) specifies this service. At UMTS bearer service establishment or modification different QoS profiles have to be taken into account.

The sources of these QoS parameters come from different elements:

- The UE capabilities form a QoS profile which may limit the UMTS bearer service which can be provided.
- The UE or the terminal equipment (TE) within the terminating network may request a QoS profile at UMTS bearer establishment or modification
- A QoS profile in the UMTS subscription describes the upper limits for the provided service if the service user requests specific values.

- If the UE requests or modifies a UMTS bearer and one or more of the QoS attributes are not specified by the UE by setting the attributes to 'subscribed', the SGSN shall assume a request as specified in the QoS profile in the UMTS subscription.

9.3.2.3 Policy and Charging Control (PCC) for Evolved Packet System (EPS)

In [102], the reference network architecture for Policy and Charging Control (PCC) in Evolved Packet Systems (EPS) is described. The AF (Application Function) obtains information from applications susceptible in order to enact the corresponding dynamic policy and charging control. The extracted information is passed on to the Policy and Charging Rules Function (PCRF) over the Rx reference point. The AF also can audit traffic plane events, such as IP session termination or access technology-type change. The PCRF is in charge of notifying these events to the AF.

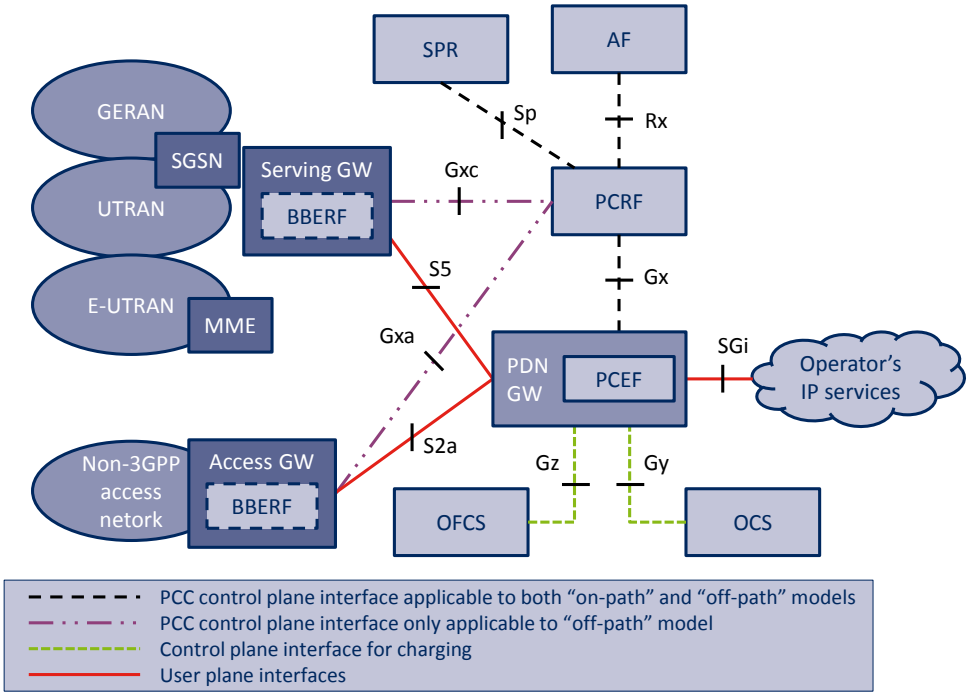

Figure 11: 3GPP PCC Architecture

The decision-making process carried out by the PCRF relies on a combination of the information coming from the Rx, Gx and Gxa/Gxc reference points and user-specific policies and data from the Subscription Profile Repository (SPR). The resulting policy decisions are relayed to the PCEF and the BBERF (if present). In addition, the PCRF performs event forwarding actions between the BBERF, the PCEF, and the AF.

The enforcement of the previously mentioned decisions is carried out by the PCEF, which also provides the PCRF with user- and access-specific information over the Gx reference point and interacts with the online charging system (OCS).

The PCEF and the BBERF classify packets using the packet filters of PCC and QoS rules, in a process referred to as Service Data-Flow (SDF) detection. Dynamically provisioned rules are based on IP five-tuple filters. The definition of filters for predefined rules is not standardized.

9.3.2.4 3GPP ANDSF

The Access Network Discovery and Selection Function (ANDSF) is an entity introduced by 3GPP as part of their Release 8 set of specifications, within an Evolved Packet Core (EPC) of the System Architecture Evolution (SAE) for 3GPP compliant mobile networks. It purpose is to assist a User

Equipment (UE) to discover non-3GPP access networks –such as WLAN or WIMAX– that can be used for data communications in addition to 3GPP access networks (such as HSPA or LTE) and to provide the UE with rules policing the connection to these networks. Details about a node implementing the ANDSF functionality are specified in 3GPP specifications TS 23.402 [126] and TS 24.302 [127]. Offloading to non-3GPP, i.e. to WiFi, can be an effective way to alleviate congestion situations in a mobile packet core network. The figure below shows a typical layout of a network where an ANDSF Server is integrated. It implements the logical S14 interface, as per 3GPP TS 24.312 [130], to an UE with and ANDSF Client. The ANDSF Server usually implements also an SMPP interface towards a SMS-C to push a notification to one or more UEs to instruct them to fetch access network policy rules from the ANDSF Server.

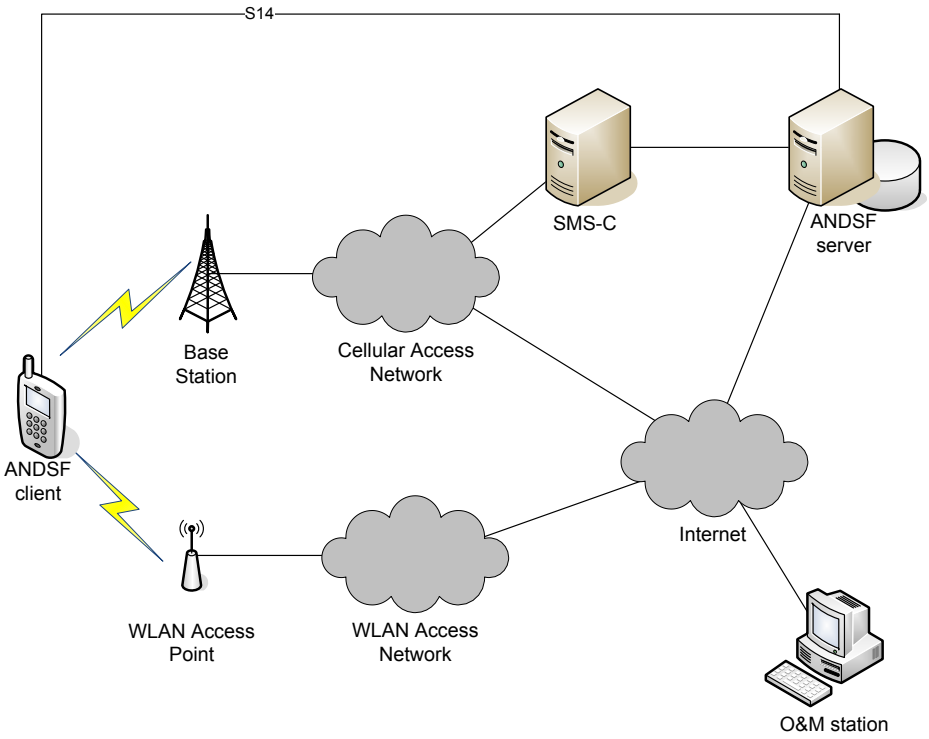

Figure 12: General architecture of the ANDSF interworking

It is relevant to mention that, according to the standards, the ANDSF Server is somehow an isolated network entity, without any other reference point but the S14. No integration with other network entity has been specified.

9.3.2.4.1 ANDSF operation modes

The dialogue between the ANDSF Server and the ANDSF Client at the UE is implemented by means of the S14 reference point. The 3GPP standards specify two modes of operation:

1. **Pull mode:** According to internal configuration, the UE decides that it needs new policies. The ANDSF client requests policy rules to the ANDSF Server. This message includes its location. The ANDSF Server validates the request and sends and answers with access network policy rules, identified as ISMP in Figure 13. Said figure shows a **logical** diagram flow of the pull mode of operation when the UE is identified by its IMEI over the S14 interface.

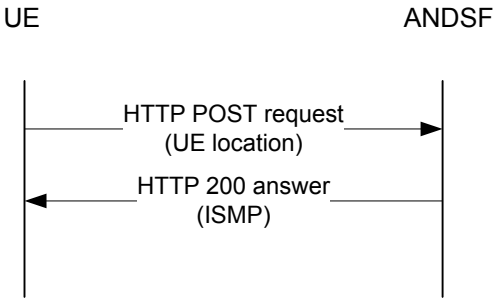

Figure 13: ANDSF PoC. Pull mode of operation

2. **Push mode:** It is very similar to the pull mode, but with a preliminary step in which the ANDSF Server asks the UE to start the policy download process. Thus, the ANDSF server sends a WAP-Push SMS to selected ANDSF Clients, indicating the URL where they should fetch policy rules. Then UEs request policy rules from the ANDSF Server, which answers with access network policy rules. Figure 14 shows a logical diagram flow of the push mode of operation when the UE is identified by its IMEI over the S14 interface.

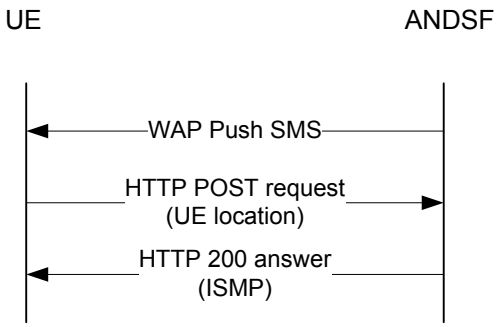

Figure 14: ANDSF PoC. Push mode of operation

9.3.2.4.2 Relationship between PCRF and ANDSF Server

The patent application “Policy Decisions for Data Communications in Constrained Resource Networks” [128], by García-Martín et al., introduces a new reference point between the ANDSF Server and the PCRF with the following functionality:

- Upon reception of an indication of a failure when opening a new flow by a UE, the PCRF can asks the ANDSF Server, using a UE identifier, whether there is an alternative access network for the UE.
- The ANDSF Server answers with a list of available alternative access networks for the UE in its current location.
- With such information the PCRF decides which access network is suitable and sends a prioritized list of alternative access networks to the ANDSF Server. Said list also includes the UE identifier the list refers to.
- Upon reception, the ANDSF Server starts a regular procedure to make the UE to switch access network.

The network architecture is described in the figure below:

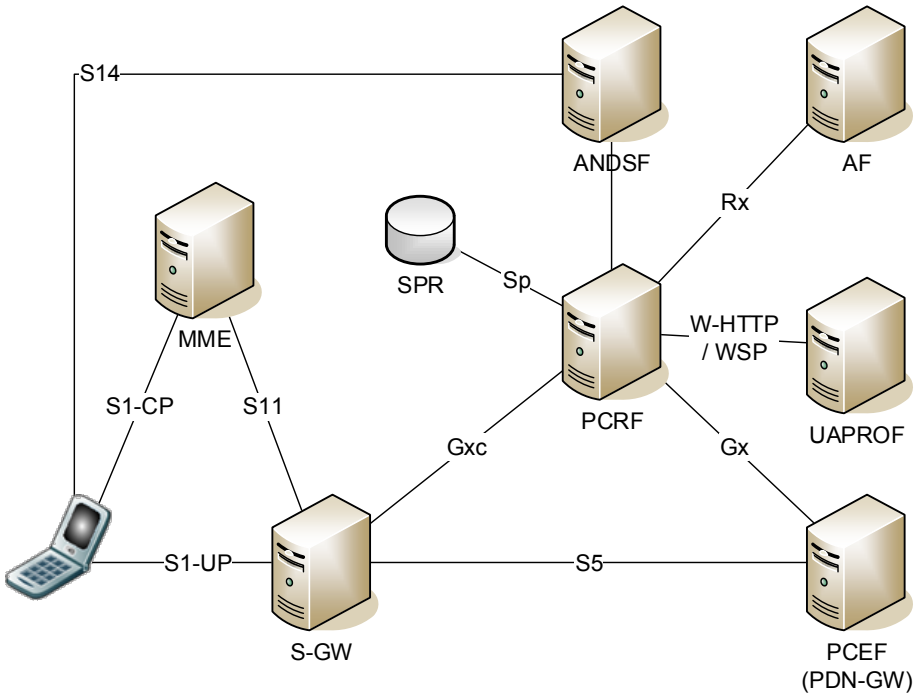

Figure 15: Interworking between PCRF and ANDSF proposed by García-Martín et al.

9.3.2.5 Use of congestion status in PCC

Some patent applications by LM Ericsson suggest the introduction of access network congestion status information as part of PCC decisions at a PCRF and also the possibility of predicting such congestion status in advance, so that the limitations of actual status determination are overcome.

In "Technique for Introducing a Real-Time Congestion Status in a Policy Decision for a Cellular Network", Ávila-González et al. [132], the authors describe the possibility of taking into account the congestion status of a given cell to assign a QoS class upon establishment or modification of an IP Connectivity Access Network (IP-CAN) session for a user. The patent application defines a so-called Performance Manager able to determine the congestion status of the radio network and store the congestion status in a database. It can be queried by the PCFR in order to assign a QoS class (identified by a QoS Class Indicator, QCI).

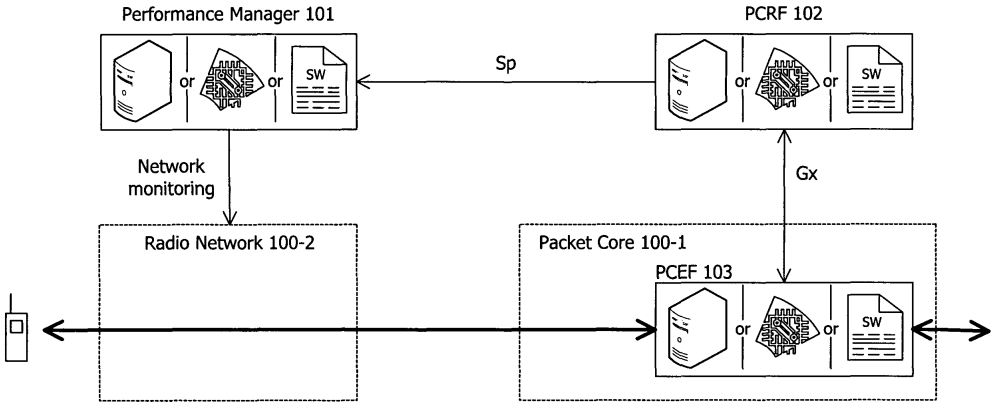

Figure 16: Consideration of the congestion status when the PCRF makes a decision

In “Method For Introducing Network Congestion Predictions in Policy Decisions,” [131] Carnero-Ros et al. propose to introduce a so-called Congestion Prediction Engine (CPE) in charge of making predictions by means of “machine-learning techniques” so that the PCRF can use said predictions when making a decision. The CPE periodically uploads predictions to a generic database that is actually queried by the PCRF when making a decision upon establishment or modification of an IP-CAN session for a user. The patent application states that supervised machine-learning techniques are used and mentions two types of regression trees: ID3 and J48. WEKA is also mentioned as the toolkit used to make decisions. However, no further details (data inputs, considered features, training space…) are provided.

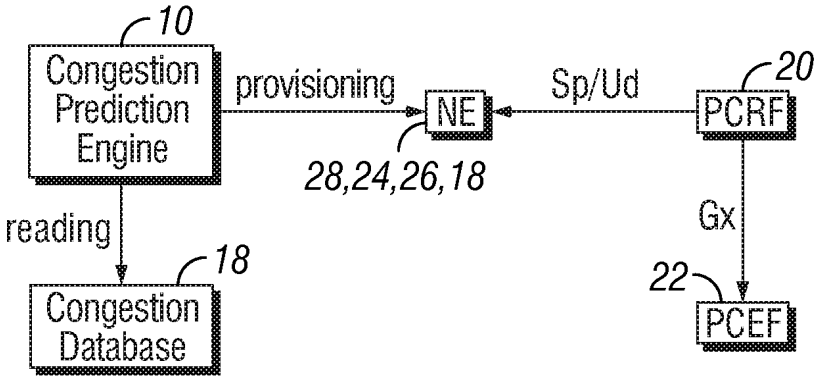

Figure 17: Introduction of a Congestion Prediction Engine according to Carnero Ros et al.

9.3.2.6 RAN User Plane Congestion

RAN user plane congestion occurs when the demand for RAN resources exceeds the available RAN capacity to deliver the user data for a period of time. RAN user plane congestion leads, for example, to packet drops or delays, and may or may not result in degraded end-user experience.

In order to cope with RAN User Plane Congestion, different issues must be addressed. One of them is the application of congestion mitigation measures. Such measures may include traffic prioritization, traffic reduction and limitation of traffic, and shall be able to manage user plane traffic across a range of variables including the user's subscription, the type of application, and the type of content.

9.3.2.6.1 3GPP UPCON architecture

3GPP has discussed several options to cope with UPCON [129] and has finally agreed on the architecture described in the figure below. It relies on the Policy and Charging Control architecture (see section 9.3.2.3) to implement the aforementioned alleviation measures:

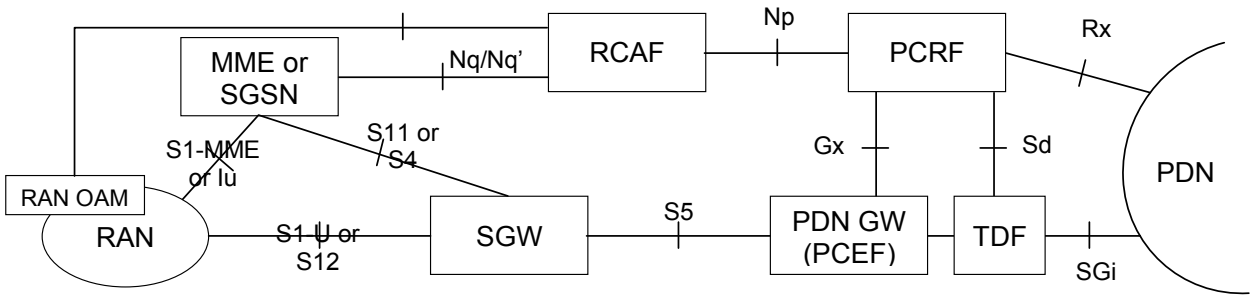

Figure 18: 3GPP UPCON Architecture

According to the 3GPP specifications, a new logical function entity, RAN Congestion Awareness Function (RCAF), is added to report RAN User Plane Congestion Information (RUCI) to a PCRF for the purpose of congestion mitigation. For this purpose the RCAF:

- Collects raw user plane congestion information from the RAN OAM. The RAN OAM corresponds to OSS level features of the RAN operator;
- Determines the list of impacted UEs;
- Integrates the RAN congestion status with an integration time fitting with Core Network mitigation tools (e.g. to provide the PCRF only information on sustained congestion);
- Provides "spatial" integration of the RAN congestion information, if the RUCI associated with a cell should depend on the congestion status in the neighboring cells (e.g., in case intra-eNB mobility reporting is not activated);

Upon reception of said reports, the PCRF will make the PCEF, or any other enforcement point, apply actions for congestion mitigation.

The introduction of the RCAF involves the addition of the following reference points to the PPC architecture:

- Np: Between RCAF and PCRF. Over Np, RAN User Plane Congestion Information (RUCI) is sent from RCAF to PCRF.
- Nq/Nq': Via Nq, the MME provides the RCAF with the list of UEs (IMSIs) in a given eNB ID/ECGI and for each of these IMSI(s) the APNs of the active PDN connections. The Nq' reference point between RCAF and SGSN is used, for a set of IMSI(s), to provide the RCAF with the list of APNs of the active PDN connections of each of these IMSIs.

RAN User Plane Congestion Information (RUCI) is defined over Np and includes following information:

- Congestion/abatement location information (e.g. eNB ID or Cell ID or 3G Service Area ID);
- Congestion level;
- The validity time of the information. When this time has elapsed and no further congestion information has been received, the congestion is assumed to be over.
- List of affected IMSI.

9.3.3 Quality of Experience

A key concept that has been analyzed along this first year and quite related with the proposed use cases, especially use cases #2 and #3, is the Quality of Experience (QoE) definition.

Quality of Service (QoS) is a measure of performance at the packet level from the network perspective and performance of other devices involved in the service. QoS also refers to a of technologies (QoS mechanisms) that enable the network administrator to manage the effects of congestion on application performance as well as providing differentiated service to selected network traffic flows or to selected users [5].

However, no unambiguous definition of **Quality of Experience** (QoE) exists. A basic definition has been provided by Ofcom [11] relative to the quality of mobile services (that is, including not only data services but classical voice and short message-related services). According to Ofcom, QoE is *the technical performance of the services delivered to consumers*. When referring to technical performance, it is understood as *the operation of the network and services (i.e. the coverage,*

speed, capacity and reliability) rather than customer service related aspects of a mobile service such as billing, call centres and sales.

The DSL Forum establishes that Quality of Experience (QoE) *reflects the collective effect of service performances that determines the degree of satisfaction of a user with a service e.g. what a user really perceives in terms of usability, accessibility, retainability and integrity of the service. QoE is a measure of the end-to-end performance at the service level from the user perspective and an indication of how well the system meets the user's needs* [5].

From an industrial point of view, it has been acknowledged *that subscribers make subjective assessments of their mobile QoE based on a combination of factors that affect their applications: speed, smoothness, latency, and clarity* [6]. Subscriber QoE is thus based on factors such as:

- The amount of stalling in the video being viewed
- The time required to download a webpage
- The resolution of the video content being viewed
- The responsiveness of a mobile app

QoE reflects the collective effect of service performances that determines the degree of satisfaction of a user with a service e.g. what a user really perceives in terms of usability, accessibility, retainability and integrity of the service. Thus QoE is a measure of the end-to-end performance at the service level from the user perspective and an indication of how well the system meets the user's needs [7].

With regard to the relationship between QoS and QoE, QoE can be regarded as *a concept comprising all the elements of a subscriber's perception of the network and its performance and how they meet expectations*. On the other hand, QoS *is intrinsically a technical concept [that] is measured, expressed and understood in terms of networks and network elements. QoS is a subset of the overall QoE scope* [10].

9.3.3.1 Quality of Experience Metrics

Measurement of quality in voice services has been standardized by means of so-called MOS (Mean Opinion Score). MOS is a subjective measurement where listeners sit in a "quiet room" and score call quality as they perceived it. Afterwards, the average of the results of a set of tests is obtained [8].

However, there is no equivalent measure of quality for mobile data services. They show a wide variety of content types and usage patterns with different features [6].

If we assume the MOS approach as valid, the best way to measure QoE would be to get users' feedback. However, this approach poses a number of drawbacks that make it unfeasible: the variety of data services and users' expectations; the dependability of the quality on the users' situation (time of the day, whereabouts…); and last but not least, the "forensics" approach MOS involves, that is, trying to measure the quality after the service has been accessed.

Other approaches are intrusive and require the installation of specific clients or apps in the user equipment (Ickin et al. [9]) propose to use a Context Sensing Software (CSS) app installed in the users' mobile phone; the execution of an Experience Sampling Method, ESM, where participants are provided stopwatches so that they make notes of their experience in real time; and weekly interviews). That's unfeasible.

Therefore, we will adopt a network-based model, with meaningful KPIs with predefined thresholds.

9.3.3.2 Quality of Experience – Service Classification

Ickin et al. [9] have identified 13 different categories of mobile applications used by the participants:

- Communication: talk, skype, gmail, email, gtalk
- Web: default browser, dolphin
- Social network applications: okcupid, cooliris, foursquare, facebook, twitter, foursquared, tumblr, touiteur
- Productivity tools: astrid, sandbox, calendar, shuffle, callmeter, outofmilk
- Weather apps: weather, weatherservice, weathercachingprovider
- News: espn, sports, news, penguinsmobile, foxnews, penguinsMob, reddit, newsfox, pittFight
- Multimedia streaming: listen, youtube, pandora, lastfm
- Games: worldwar, WoW, games, poker, zyngawords, words, touchdown
- Lifestyle apps: horoscope, sparkpeople, diet
- Finance: stock
- Shopping: ebay, coupons, starbuckscard, craigslist, starbucks
- Travel: navigator, maps
- Other applications

9.3.3.3 Quality of Experience – Proposed Cycle

ONTIC will follow the following approach to deal with QoE degradation in order to detect it and properly actuate in order to provide alleviation actions.

- Selection of one type of service (see service classification in section 9.3.3.2). Video services will be selected as it is one of the more fast growing types of traffic.
- Analysis of how feasible is its online detection (by URL, such as netflix, YouTube, Hulu…; by type of protocol, such as HTTP-based protocols –there are proprietary specifications, like Adobe Dynamic Streaming, Apple HLS, Microsoft Smooth Streaming; and standards, like Dynamic Adaptive Streaming over HTTP, DASH [133]–).

Figure 19: HTTP Adaptive Streaming Protocols

- Definition of Key Performance Indicators (KPI). For instance, Ericsson CEA (Customer Experience Assurance) [125] define its per-service KPI's in the following way:

Type of Service	KPI	Meaning
Web	Web page Accessibility	Measured as the ratio between the number of successful HTTP request-responses pairs and the total number of web page access attempts
	Web Download Success	Measured as the ratio between the successful resource downloads and the total web page resource download attempts
	Web Page Access Time	Measured as the latency between HTTP request and respones when the user starts downloading a web page
	Web Download Time	Measured as the download time of resources belonging to the same web page-multiple overlapping TCP connections can be used for transferring the same web page
	Web Speed	Measured with the throughput calculation algorithm that uses heuristics to detect active periods on a TCP connection and calculates the throughput for these periods only
Video	Video Accessibility	Measured as ratio between the number of HTTP requests and successful responses when the user starts downloading a video
	Video Freeze Rate	Measured by comparing the media timestamp to the actual transport packet timestamp. It is possible to estimate the amount of media buffered an missing from the client playback buffer. Assuming a certain playback buffer size, the number and duration of media freezes can be estimated.
File Transfer	File Transfer Accesibility	Measured as the ratio between the number of requests and successful responeses when the user starts a file transfer (FTP).
	File Transfer Success	Measured as the ratio of successfully finished TCP connections of file transfers and the number of attempts
	File Transfer Access Time	Measured as the latency between the number of TCP requests and responeses when the user starts a file transfer (FTP)
	File Transfer Speed	Measured with the throughput calculation algorithm that uses heuristics to detect active periods on a TCP connection and calculates the throughput for theses periods only

Table 1: KPI's per service

- Determine whether per-user video KPI's can be computed on line.
- Determine thresholds for video KPI's.
- Detection of degradation of video services (KPI sustainably below the threshold) for a given user or area
- Prediction of degradation of video services for a given user or area

9.3.4 Next Steps

Effective QoE policy enforcement relies strongly on the accurate characterization of traffic packets. Recent advances in unsupervised classification using machine learning lay out a promising landscape for the significant improvement of QoS and QoE in diverse network scenarios. It is therefore desirable to conduct further research in this domain in order to enhance network QoE.

10. Use Cases Description. First Year Summary

10.1 Introduction

This section provides a more detailed view of the different scenarios addressed by ONTIC. It details how the use cases, originally described in the DoW, have been landed into the work stream of the project.

In the DOW it can be found three high level use cases descriptions that are the core business driver for the whole ONTIC research and development initiatives. These are:

1. Use Case # 1. Network Anomaly Detection
2. Use Case #2 Proactive Congestion Detection and Control Systems
3. Use Case #3.Dynamic QoS management

As a result of the Agile methodology chosen to drive the activities in the project, these Use Cases has been converted into Epics (High level user stories). In addition to this change, and due to the high dependency between them, partners have decided to group UC#2 and UC#3 into a common Epic (High level User Story description). So as a summary, and in order to ease the reading of this section, it is provided a table that matches Use Cases, as described in the Dow, Epics as provided in the project and User Stories.

Use Case (As provided in the DoW)	Epic (As translated in project execution time)	User Stories (As working items)
UC#1 - Network Anomaly Detection	User Story #2 US#2: As a network administrator, I want an autonomous way for detecting and characterizing traffic anomalies, so that it makes possible to autonomously and efficiently manage them	US#2.1 As a network administrator, I want a mining mechanism, so that traffic classes can be autonomously distinguished
		US#2.2 As a network administrator, I want a discrimination mechanism so that anomalies signatures can be autonomously issued
		US#2.3 As a network administrator, I want a ranking score for assessing the abnormality and dangerousness of anomalies, so that an autonomous process can discriminate between discarding attacks vs. Coping with legitimate anomalies management
UC#2 :Proactive Congestion Detection and Control Systems	User Story #1 US#1 As an ISP, I want to deliver to my users the best user experience by making an efficient use of my current network resources, so that I can provide more value with	US#1.2 (UC#2) As an ISP, I want to have an early detection System for congestion, so that I can make decisions in advance to mitigate it

UC#3 Dynamic QoS management	less OPEX and same resources	US#1.1 (UC#3): As an ISP, I want to have an efficient way of managing QoS, so that I can make decisions about what applications and services must be prioritized

Table 2: Use Cases (DoW) – Epics and User Stories correlation

Along the project it will be used the words "Scenario" and "Use Case" as synonyms, always referring to the original use cases described in the DoW.

Following sections follow the User Story numbering schema.

10.2 User Story #1: Proactive Congestion Detection and Control Systems/Dynamic QoS management

10.2.1 User Story #1 Epic

This section describes the high level user stories (epics) for the DoW UC#2 and UC#3. As described previously, UC#2 is related to the User Story#1.2 and UC#3 to the User Story#1.1. The root User Story for UC #2 and UC#3 is the so called User Story 1:

*"**As an ISP**, **I want** to deliver to my users the best user experience by making an efficient use of my current network resources, **so that** I can provide more value with both less OPEX and same resources"*

10.2.1.1 Scenario description

Early detection of potential quality of experience (QoE) degradation patterns which could end up in congestion situations is currently a hot topic for CSPs, especially for Mobile Operators [61]. However, detection of said patterns is not a trivial task, as Mobile Networks are evolving towards scenarios of exponential mobile data traffic growth, where heterogeneous users, with different needs and profiles, demand the best QoE according to their expectations and personal preferences. Although it could be argued that CSPs could cope with the growth of congestions situations simply with higher investments in capacity, a more intelligent and adaptive approach is required, as network resources are always limited and finite and there is a tremendous pressure over the CSPs to improve their OPEX and CAPEX [62].

Today Mobile Operators are able to classify users and apply congestion mitigation policies depending on the customer segment they belong to. Segmentation can be done in different and even highly flexible ways (i.e. there are operators which build their segments based on user's own tailored service offering, while others have a more schematic segmentation based on generic rules for all the users with the same subscription profile –typically Gold, Silver and Bronze segments–, etc.) with different bandwidth limits, different congestion mitigation measures and even different customer care strategies depending on the customer segment. However, no Mobile Operator CSP is going a step further by giving their users the necessary procedures so that their QoS meet their different expectations, profiles, and use of mobile devices (professional, leisure time, etc.) in QoE degradation scenarios. Fine tuning of the networks is done currently by human experts that typically set up static optimization rules which get applied in case of QoE degradation scenarios, in a reactive, or at least planned, manner.

Telco operators are looking for a simplification in their operations having churn reduction as one of their main goals, by distributing their limited re-sources in the best way to their users and allowing them to have the best Quality of Experience in such critical situations.

As shown in Figure 20, data traffic is expected to grow about 50 percent each year until 2018. This implies a very high growth rate of the data going through telecom networks. In addition to that, from an economics point of view, there is an increasing CAPEX and OPEX pressure in the communication service providers (CSP) operation activities [62]. Among all the options that could be taken to reduce such pressure, the one we are focusing on in our current work is operation management optimization, by proposing investments in network optimization tools to decrease the CAPEX, making a better use of current network resources; OPEX will be reduced by automating these activities. All these actions will lead to a better use of the resources and therefore to reach the goals of CAPEX and OPEX optimization.

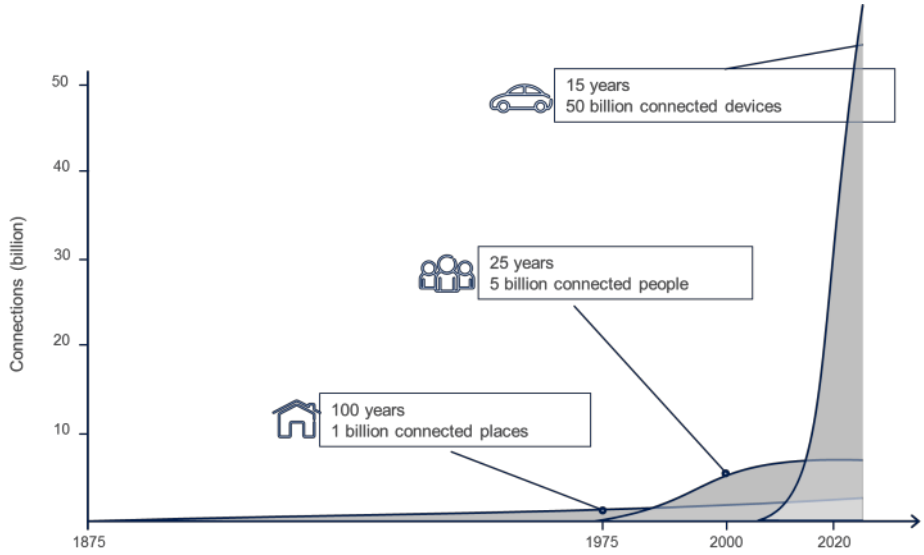

Figure 20: Pace of change in network traffic

Another key trend is the adoption of Big Data technologies [63] in the telecom industry with the introduction of new products and tools in the market such as Ericsson CEA [125], which allows telecom companies to make complex analysis about their customer needs, problems, etc. by means of analytic tools.

10.2.1.2 Proposed way forward

In this high data growth scenario, CSPs are looking for automatic procedures to improve the provided Quality of Experience levels (QoE) for each of the applications and services used by the users. This can be done by making an optimized use of available network resources. QoE (see section 9.3.3 “Quality of Experience”) provides a subjective measure about the experience of the user with an application or service and therefore is different from the current way of managing the user experience via QoS levels. On the other hand the automatic procedures will help CSPs to reduce their churn rates and to improve their customer satisfaction index differentiating their offering from others. The optimization of the perceived quality of experience (QoE) when using different applications, services, etc. is becoming more and more a cornerstone to CSPs. The QoE optimization is later on done via the configuration of QoS parameters.

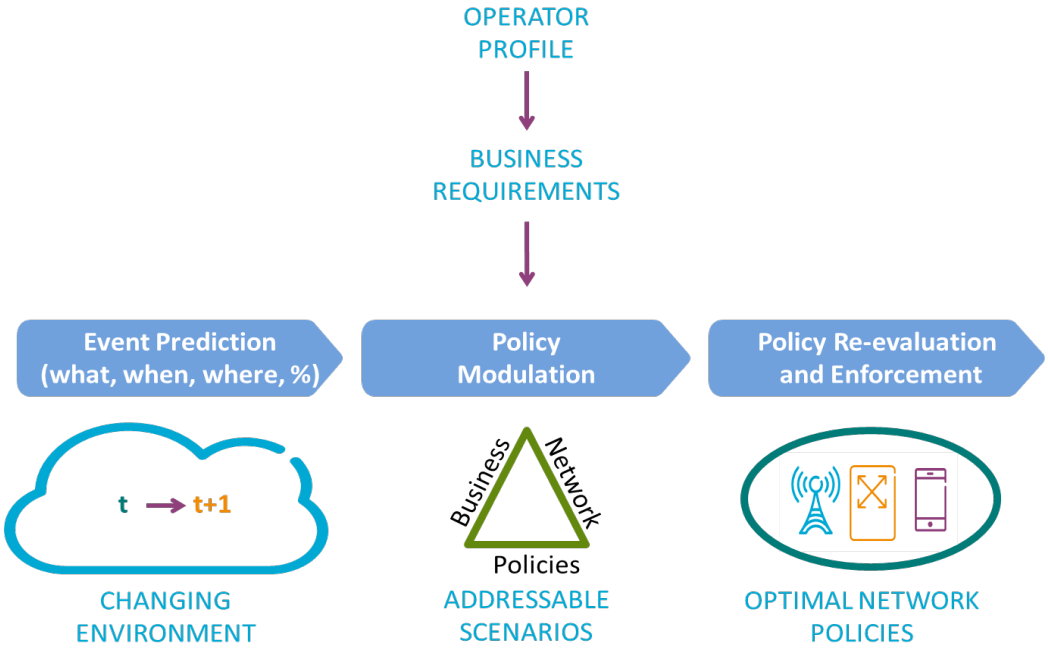

Figure 21: Use cases #2 and #3 framework

Figure 21 provides an end to end view of the proposed whole Adaptive Quality of Experience (AQoE) process, providing a general framework to manage QoS and congestion Use Cases. On the left side of the figure it is shown the prediction/Analytics module. This analytics module provides in time t, an estimation about the status of the network in time t+1 (what event, where, probability, etc.). The policy modulation function receives that prediction. This entity has to be configured in a flexible way, by i.e. following the operator profile policies and therefore the concrete business requirements, etc. The policy modulation function (also called the Policy Governance module) will modulate the policies following the Operator's business requirements. Once the process has predicted and built policies to actuate, the enforcement points will enforce them in the network side. This action will launch a new reevaluation process to follow up the provided actions.

Therefore there is a higher pressure on the CSPs to give their end users the best QoE even in potential QoE degradation scenarios. Different network situations can lead to such scenarios. Planned or unplanned crowded events with thousands of people attending them on the same location are, among others, the typical scenarios that can trigger a "QoE degradation" pattern in the network. Once these QoE degradation scenarios are detected, the main goal of mobile operators should be to enable the best use of their resources, assuring that network resources are distributed properly among their customers -i.e. matching available bandwidth with expected QoE, minimizing denial of service, and accommodating the different priorities dynamically, etc. Figure 22 summarizes the evolution from the current QoE control scenario to one based on analytics and on user personalization:

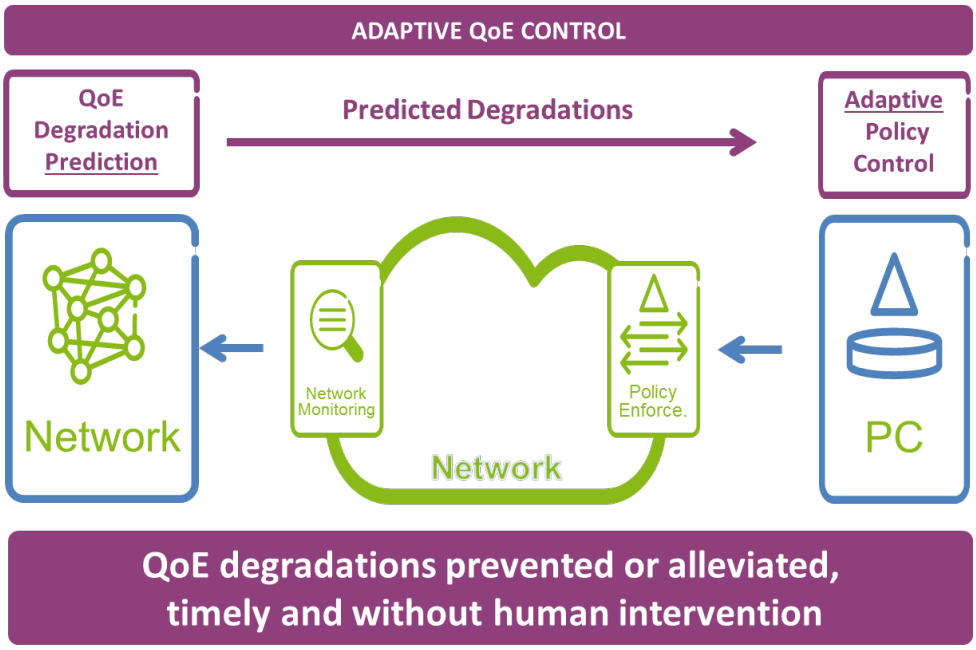

Figure 22: AQoE End to End flow

It is foreseen new ways of optimizing networks in QoE degradation scenarios. First of all, network QoS control will evolve from manual to automatic. Policies will be automatically defined taking into account operator policies, user preferences and network parameters. One advantage of this QoE automation scenario is the transition from planned-in-advance QoE degradation mitigation actions to scenarios where no actions have to be explicitly planned or deployed, from the manual set-up of optimization rules to the automatic generation of rules carried out by analytics systems; and last but not least, from a scenario where network optimization is carried out in an ad-hoc way in critical situation to scenarios where network optimization is done continuously.

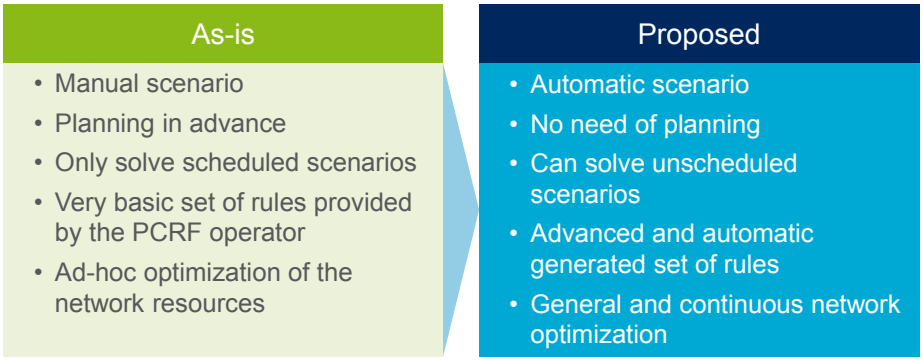

Figure 23: New scenarios for enhancing user's QoE

The proposal is to close the management and control loop by including two new functionalities:

- An Analytics Function.
- A Policy Governance Function.

The Analytics Function provides predictions, classifications, etc. Anticipating the network status based on historical and current information coming from both, the network side and external data sources. On the other hand the Policy Governance Function translates these prediction and classifications into concrete rules within the PC. We could say that the Policy Governance Function is equivalent to the human expert that set-up the information in the network side, and the analytics function provide the information to configure the rules.

Analytics can also be used to know more about subscribers, not only about the network. Making a dynamic clustering of subscribers/Service Usage trends are examples of analytics focused on subscribers.

Figure 24 shows the “closed” virtuous analytics circle:

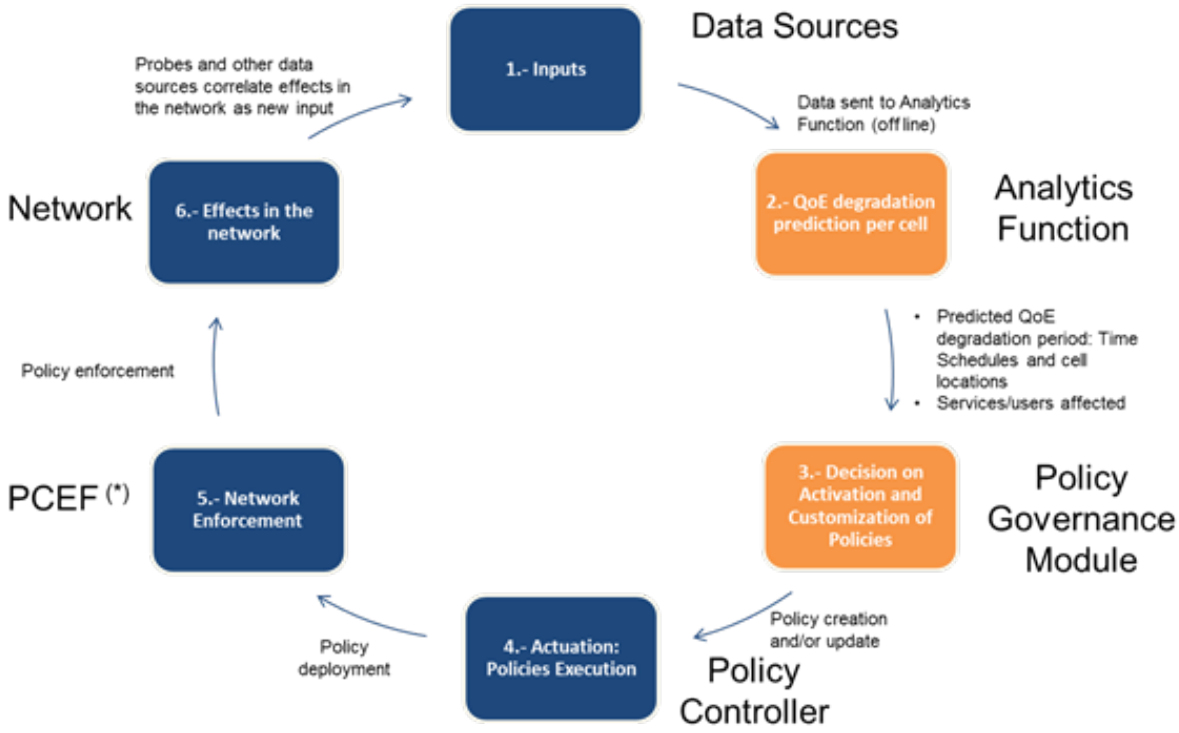

Figure 24: The expanded analytics virtuous circle

10.2.1.3 Draft System model

A network operator wants to detect congestion problems in its network, as the traffic is growing more and more. In order to avoid service delivery to be compromised, the network operator needs to incorporate a new function to control and analyze the traffic of its own network. As efficiency is a must for a network operator, the new function is enhanced with an analytic subsystem. With this new integrated subsystem, the network operator will proactively detect congestion situations. When congestion is detected, the system will inform an expert to analyze the situation or take self-managed corrective actions.

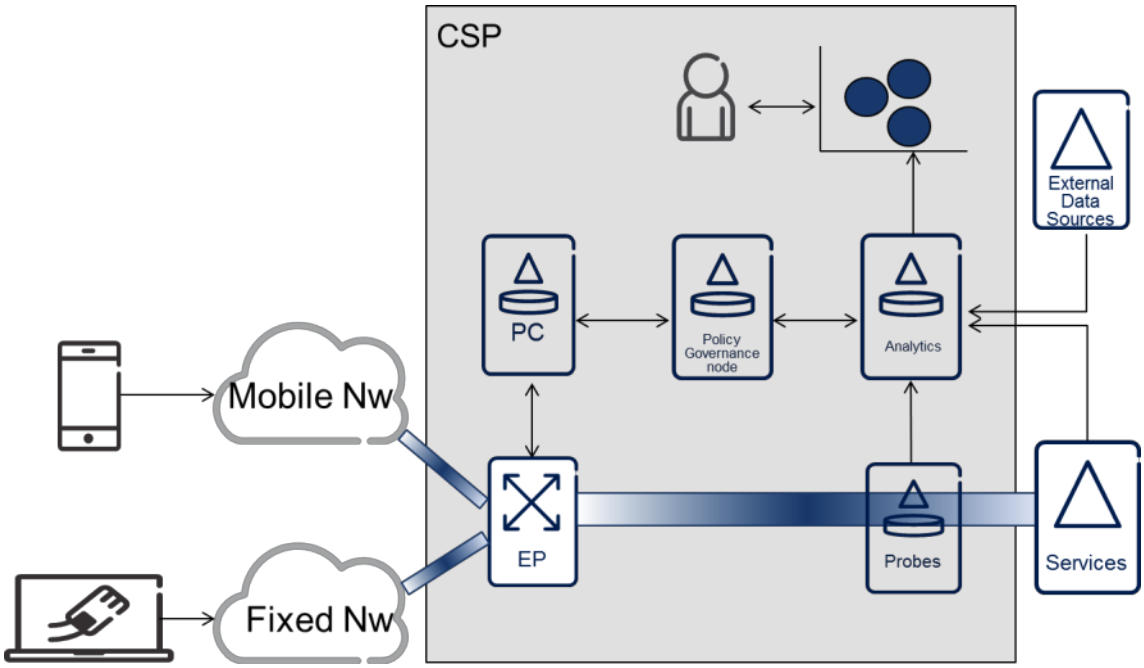

Figure 25: Architecture for Use Case 2

Figure 25 shows a high-level description of the architecture. According to this figure the network operator receives traffic from fixed and mobile networks through the Enforcement Point (EP), an entity that (a) interconnects fixed and mobile networks with ISP's internal services, and (b) applies congestion control and prevention policies to the traffic that crosses it. A high level view of the flow is provided below:

1. **Analytics Function** (AF)

    a. Main target for the ONTIC activities. This entity takes as **input information** coming from several **internal and external** sources and performs **classifications and predictions tasks.**

    b. **Processes the information** and makes predictions about potential QoE degradation situations in a time t+x. The Analytics Function can also provide a user/service classification to know better which the important services for the user are.

    c. The result of the analysis will be shown in a UI (User Interface), represented by a chart in Figure 25. Therefore, the UI will present analytics results in nearly real-time related with the congestion situation of the ISP and the characterization of the network traffic that is crossing the EP.

    d. **Sends the predictions to the Policy Governance Function** (PGF).

2. **Policy Governance Function** (PGF)

    a. This entity is responsible for building the policies that helps to alleviate the QoE degradation scenarios and will improve the user's QoE.

    b. Based on the predictions provided by the Analytics Function the Policy Governance Function builds/composes/selects policies to alleviate the predicted situations.

3. **Policy Controller** (PC)

a. Process events coming from the network side and deploy specific traffic rules on the Enforcement Point. This deployment is done based on the policies already set-up by the Policy Governance Function. 3GPP PCRF and 3GPP ANDSF may play this role

4. **Enforcement Point** (EP)

a. This entity is the responsible of applying the rules already set-up by the Policy Controller based on the predictions provided by the Analytics Function and the policies composition did by the Policy Governance Function.

Due to the complexity of deploying the described QoE degradation control system described in Figure 25 in a real production network, a simulated scenario will be used instead, and synthetic traffic (based on the ONTIC dataset) will be generated and injected in the simulated network.

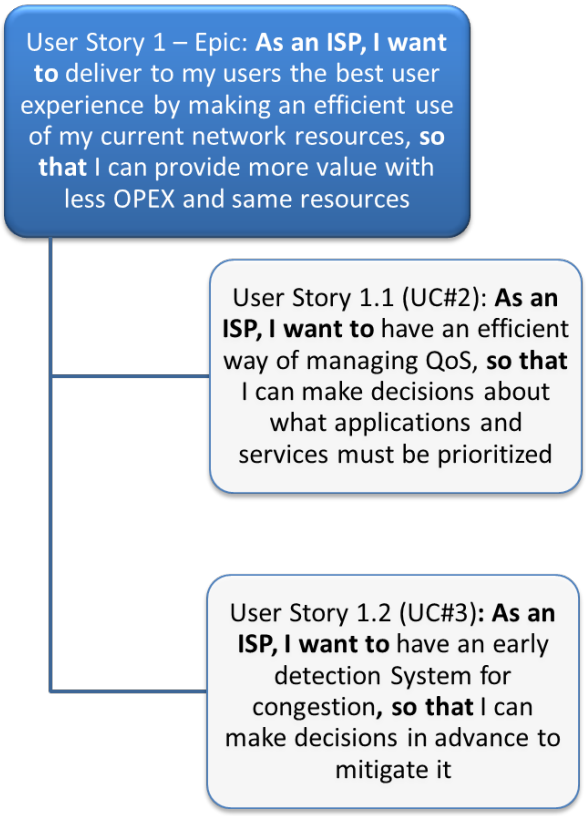

Figure 26: User Story 1 (UC#2 and UC#3)

10.2.1.4 User Story#1.1. Dynamic QoS Management

10.2.1.4.1 Initial description from DoW

The past few years have witnessed a dramatic increase in the number and variety of applications running over the Internet and over enterprise IP networks. The spectrum includes interactive (e.g., telnet, instant messaging, games etc.), bulk data transfer (e.g. ftp, P2P file downloads), corporate (e.g., database transactions), and real time applications (voice, video streaming, etc.), to name just a few. Network operators (particularly in enterprise networks) are actively seeking the ability to support different levels of Quality of Service (QoS) for different types of applications. The need is driven by (i) the inherently different QoS requirements of different types of applications (e.g. high throughput for file transfer applications etc.); (ii) the different relative importance of different applications to the enterprise: e.g., database transactions may be considered critical and therefore high priority, while traffic associated with browsing external web sites is generally less

important; and (iii) the desire to optimize the usage of their existing network infrastructures under finite capacity and cost constraints, while ensuring good performance for important applications.

In spite of a clear perceived need, and the fact that various mechanisms (traffic prioritization, etc.) have been developed for providing different service quality guarantees in the network, their adoption has not been widespread. A pertinent question then is: what ails QoS?

Realization of service differentiation capabilities requires association of the traffic with the different applications, determination of the QoS to be provided to each, and finally, mechanisms in the underlying network for providing the QoS. Based on interactions with large enterprise network operators, we believe that a key issue behind the slow spread of QoS use is not the lack of interest or need, but rather, the absence of suitable classification techniques that can aid operators in classifying the network traffic mix among the different QoS classes. We refer to this as the mapping/classification problem, and hypothesize that solving this would go a long way in making the use of QoS more accessible to operators.

Network mapping and classification inside the network is a non-trivial task. Ideally, a network system administrator would possess precise information on the applications running inside their network, along with simple, unambiguous mappings from easily obtained traffic measurements to applications (e.g. by port numbers, or source and destination IP addresses). This information is vital not just for the implementation of classification rules, but also in planning the capacity required for each class, and balancing trade-offs between cost and performance that might occur in choosing class allocations. For instance, one might have an application whose inclusion in a higher priority class is desirable, but not cost effective (based on traffic volumes and pricing), and so some difficult choices must be made. Good data is required for these to be informed choices. However, in general, the required information is rarely up-to date or complete, if it is available at all. The traditional ad-hoc growth of IP networks, the continuing rapid proliferation of new applications, the merger of companies with different networks, and the relative ease with which almost any user can add a new application to the traffic mix with no centralized registration are some factors contributing to this “knowledge gap”. Furthermore, over recent years it has become harder to identify network applications within IP traffic. Traditional techniques such as port-based classification of applications have become much less accurate The state-of-the-art & actual limitations: Different approaches have been proposed in the industry during last years in order to both, classify and map the traffic patterns to specific applications, services and groups of users. All those approaches are based on the assumption that the normal traffic pattern and load are well known and studied and then, apply such knowledge to tasks like dimensioning or traffic prioritization.

10.2.1.4.2 Description included in D2.1

The use case related to the QoS scenario will be implemented in two phases, as part of an incremental process. Phase 1 is focused on big data analysis. Once completed, the second phase will be focus on the actuation of the big data algorithms developed in phase 1. Next subsections describe each phase.

10.2.1.4.3 User Story 1.1

- **As an ISP, I want to** deliver to my users the best user experience by making an efficient use of my **current** network resources, **so that** I can provide more value with both less OPEX and same resources
    - User Story 1.1 UC#3**: As an ISP, I want to** have an efficient way of managing QoS, **so that** I can make decisions about what applications and services prioritize
        - Detailed user stories (Development level)

- **As an ISP, I want to** be able of automatically detect new applications and services already running in my network, **so that** I can make a decision about what prioritize
- **As an ISP, I want to** know more in deep what means QoE for my customers**, so that** I can adjust the network parameters in consequence
- **As an ISP, I want to** know how QoE parameters are linked to the QoS ones, **so that** I can provide the best QoE to my customers
- **As an ISP**, I **want to** know better my customers, **so that** I can provide them the best QoE

10.2.1.4.4 The actors

Communication Service Providers

10.2.1.5 User Story # 1.2. Proactive Congestion Detection and Control System

10.2.1.5.1 Initial description from DoW

The objective of this use case deals with trying to detect congestion problems in the network of an ISP before they become harmful, and to take some corrective actions to correct and eliminate the problem. ONTIC online network traffic characterization can be used as a building block in such a proactive system. The idea is to detect in real time the beginning of a sequence of a network traffic pattern that has been previously identified as harmful because it generates severe congestion problems. Therefore, if the beginning of a harmful sequence is detected at an early stage, corrective measures can be adopted to diminish the problem. In the case a new pattern sequence appears, and then, if it is not registered in the database, an alarm subsystem implemented on top of this system will trigger a warning to an expert, informing him about this potentially harmful new situation.

10.2.1.5.2 Description included in D2.1

The congestion detection Use Case will be implemented in two phases, as part of an incremental process. In phase 1, a new control system will detect congestion in real time, showing analytics results in a basic user interface (UI). In that way an expert can take the proper corrective actions. In phase 2 the solution evolves, and the control system is able to apply in a self-managed way corrective actions, always in real time.

Summarizing, the implementation of use case 2 is conceived within an incremental process with two phases: phase 1 is focused on big data analysis, and phase 2 is focused in the actuation of the big data algorithms.

10.2.1.5.3 User Story 1.2 (UC#2)

- **As an ISP, I want to** deliver to my users the best user experience by making an efficient use of my current network resources, **so that** I can provide more value with both less OPEX and same resources
    - User Story 1.2 (UC#2): **As an ISP, I want to** have an early detection system for potential congestion patterns**, so that** I can make decisions in advance to mitigate it
        - Detailed user stories (Development level)

- **As an ISP, I want to** have an efficient way to set-up policies on the network, **so that** I can make decisions about how to use my resources
- **As an ISP, I want to** have my own set of preferences about the services I want to keep on going, in case of a bandwidth limitation, **so that** I can make decisions about how to use my resources

10.2.1.5.4 The actors

Communication Service Providers.

10.3 User Story #2 (previous use case #1): Network Anomaly Detection

10.3.1 Introduction

This section provides a general overview about the first year's status of the "Network Anomaly Detection" scenario.

10.3.2 Scenario description

Network anomaly detection has become a vital component of any network in today's Internet. Ranging from non-malicious unexpected events such as flash-crowds and failures, to network attacks such as denials-of-service and network scans, network traffic anomalies can have serious detrimental effects on the performance and integrity of the network. The principal challenge in automatically detecting and characterizing traffic anomalies is that these are moving targets. It is difficult to precisely and permanently define the set of possible anomalies that may arise, especially in the case of network attacks, because new attacks as well as new variants to already known attacks are continuously emerging. A general anomaly detection system should therefore be able to detect a wide range of anomalies with diverse structures, using the least amount of previous knowledge and information, ideally none.

The problem of network anomaly detection has been extensively studied during the last decade. Two different approaches are by far dominant in current research literature and commercial detection systems: signature-based detection and supervised-learning-based detection. Both approaches require some kind of guidance to work; hence they are generally referred to as supervised-detection approaches. Signature-based detection systems are highly effective to detect those anomalies that are programmed to alert on. When a new anomaly is discovered, generally after its occurrence, the associated signature is coded by human experts, which is then used to detect a new occurrence of the same anomaly. Such a detection approach is powerful and very easy to understand, because the operator can directly relate the detected anomaly to its specific signature. However, these systems cannot defend the network against new attacks, simply because they cannot recognize what they do not know. Furthermore, building new signatures is expensive, as it involves manual inspection by human experts.

On the other hand, supervised-learning-based detection uses labeled traffic data to train a baseline model for normal-operation traffic, detecting anomalies as patterns that deviate from this model. Such methods can detect new kinds of anomalies and network attacks not seen before, because they will naturally deviate from the baseline. Nevertheless, supervised-learning requires training, which is time-consuming and depends on the availability of purely anomaly-free traffic data-sets. Labeling traffic as anomaly-free is expensive and hard to achieve in the practice, since it is difficult to guarantee that no anomalies are hidden inside the collected traffic. Additionally, it is not easy to maintain an accurate and up-to-date model for anomaly-free traffic, particularly when new services and applications are constantly emerging.

Apart from detection, operators need to analyze and characterize network anomalies, in order to take accurate countermeasures. The characterization of an anomaly can be a hard and time-consuming task. The analysis may become a particular bottleneck when new anomalies are detected, because the network operator has to manually dig into many traffic descriptors to understand its nature. In current traffic scenario, even expert operators can be quickly overwhelmed if further information is not provided to prioritize the time spent in the analysis.

10.3.2.1 Proposed way forward

Based on the problematic exposed right above, the objective of this use case deals with designing an autonomous anomaly detection system that does not rely on previous acquired knowledge, i.e. that does not need known attack signature, labeled traffic, training, etc. It also aims at autonomously triggering suited countermeasures when attacks are detected among the legitimate traffic classes.

The result of this use case cannot be stated at this point of the project. However, we rely on previous work to draw the line of what we expect this use case to be at the end of the project.

As indicated previously, it is well admitted now, that network anomaly detection is a critical aspect of network management for instance for QoS, security, etc. The continuous arising of new anomalies and attacks create a continuous challenge to cope with events that put the network integrity at risk. Most network anomaly detection systems proposed so far, employ a supervised strategy to accomplish the task, using either signature-based detection methods or supervised-learning techniques. Yet, both approaches present major limitations: the former fails to detect and characterize unknown anomalies (letting the network unprotected for long periods); the latter requires training and labeled traffic, which is difficult and expensive to produce. Such limitations impose a serious bottleneck to the previously presented problem.

At this stage the directions we will follow for this use case are:

- To take advantage of an unsupervised clustering approach to detect and characterize network anomalies, without relying on signatures, statistical training, or labeled traffic, which represents a significant step towards the autonomy of networks;
- To propose for accomplishing unsupervised detection some robust data-clustering techniques to avoid general clustering lacks as sensitivity to initial conditions, course of dimensionality, cluster correlation, etc.
- To use the clustering results for issuing traffic characteristics and especially the rules characterizing the anomalies, and that could be used as filtering rules in security devices, for instance.

10.3.2.1.1 Draft system model

Autonomously detecting anomalies in network traffic is a complex process that consists in several tasks: (1) a monitoring and pre-processing task able to draw the traffic analysis space according to a full set of traffic features and attributes, (2) an unsupervised data mining technique (based on clustering here) that aims at solving the main problems related to noise agnosticism or curse of dimensionality for example, and (3) the analysis of the clustering results for characterizing classes and distinguishing legitimate from illegitimate ones, and triggering suited countermeasures. Figure 27 exhibits the draft general architecture for the anomaly detection process as it is currently defined.

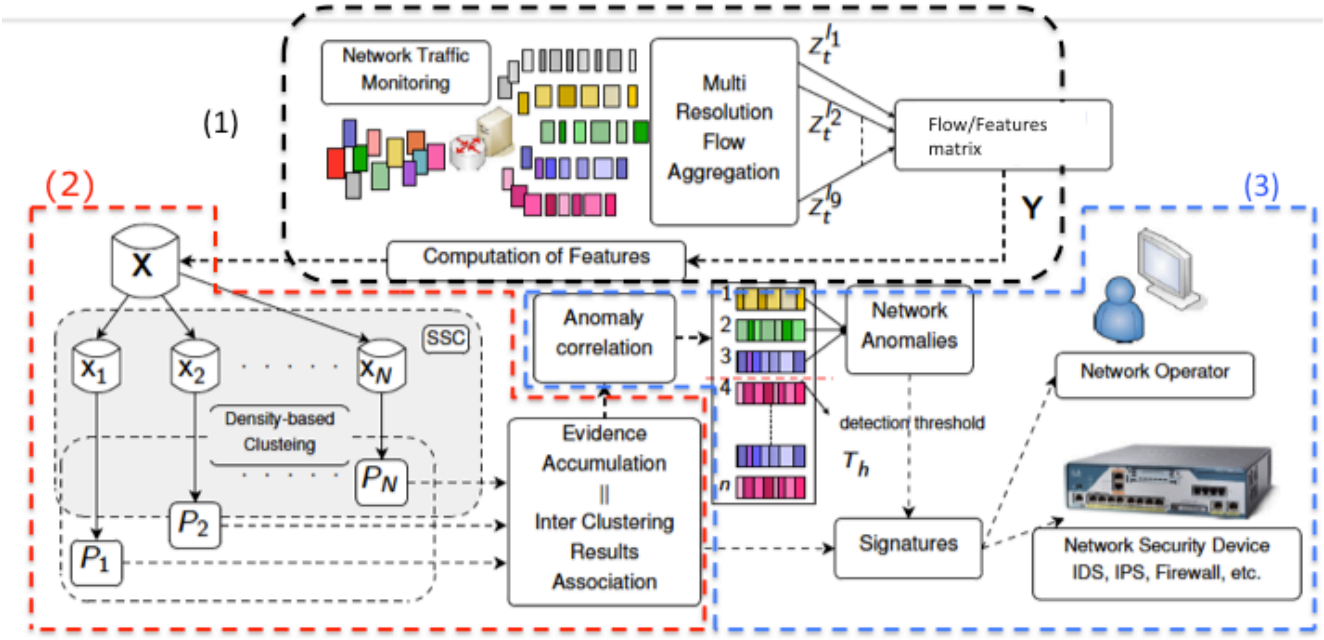

Figure 27: Functional three stages architecture for anomaly detection system

10.3.2.2 User Stories view

- **As a network administrator, I want** an autonomous way for detecting and characterizing traffic anomalies, **so that** it makes possible to autonomously and efficiently manage them
  - User Story 2.1 UC#1: **As a network administrator, I want** a mining mechanism, **so that** traffic classes can be autonomously distinguished
    - Detailed user stories (Development level)
      - **As a network administrator, I want to** have efficient monitoring and unsupervised clustering techniques, **so that** I can autonomous classify the network traffic
  - User Story 2.2 UC#1: **As a network administrator, I want** a discrimination mechanism, **so that** anomalies signatures can be autonomously issued
    - Detailed user stories (Development level)
      - **As a network administrator, I want to** have mechanisms for identifying the most significant traffic attributes, **so that** It becomes possible to issue traffic classes discrimination rules
  - User Story 2.3 UC#1: **As a network administrator, I want** a ranking score for assessing the abnormality and dangerousness of anomalies, **so that** an autonomous process can discriminate between discarding attacks vs. Coping with legitimate anomalies management
    - Detailed user stories (Development level)
      - **As a network administrator, I want to** have accurate abnormality score, **so that** It becomes possible to autonomously discriminate between legitimate and illegitimate traffic classes

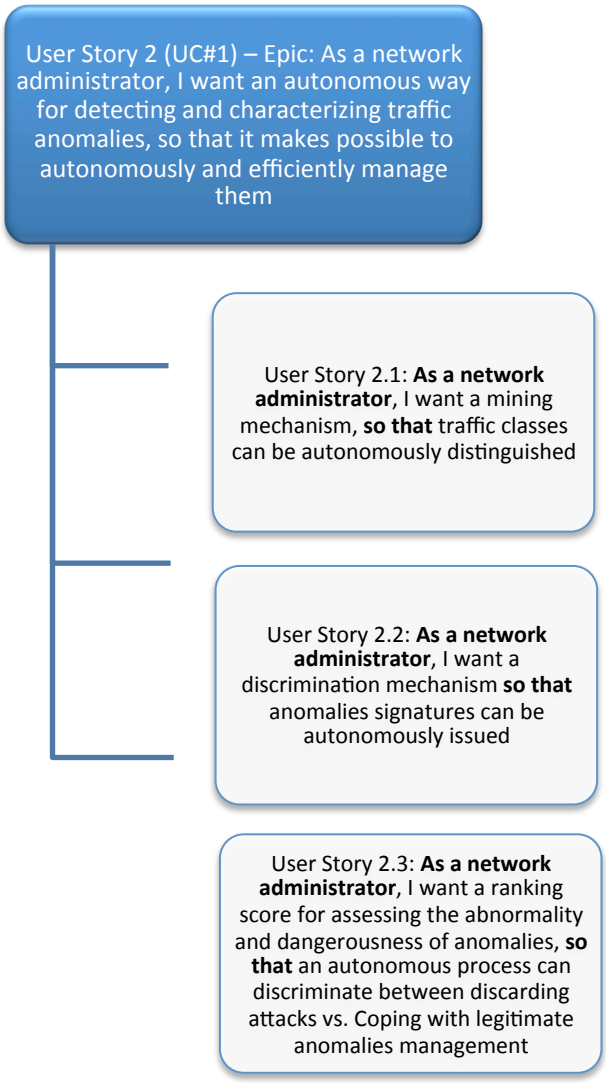

Figure 28: User Story 2 (UC#1)

10.3.3 The actors

The actors for this use case are network and security administrators / managers wherever they work. The unsupervised anomaly detection algorithm could be integrated on the residential communication boxes (be they based on ADSL, fiber…).

11. Initial User Requirements

11.1 Introduction

ONTIC follows a customized version of SCRUM methodology. The project team has worked along the first year collecting inputs from potential "customers" and refining accordingly the original use cases.

As said above, use cases have been adapted to the Agile User Stories format, and by using them the project will manage the requirements within the project.

The aim of this section is to provide an initial set of high level user stories (Epics) and different levels of details, ready to be used as a guide for the implementation along the second year. The implementation will be done by prioritizing and splitting these detailed user stories into affordable tasks.

User Stories will be continuously refined along the second and third years of the project incorporating new inputs from the market. This principle is key in Agile methodologies. The changes will be incorporated on the User Stories as the whole project executes the so called "sprints", and provides as an output outputs to be checked with potential stakeholders.

Summing up, the backlogs provided in this chapter are the ones coming from the first year analysis, but will change in the following years according to the market inputs. The outputs generated along the different sprints will be used as tools to engage with potential receivers of the said solutions.

11.2 Product Backlog – Epics

The root epic user stories (high level view) for the different scenarios are shown in Table 3:

Status	Sprint	ID	User Stories	Comments
		1	**As an ISP**, **I want to** deliver to my users the best user experience by making an efficient use of my current network resources, **so that** I can provide more value with both less OPEX and same resources	
		1.1	User Story 1.1 (UC#3): **As an ISP**, **I want** to have an efficient way of managing QoS, so that I can make decisions about what applications and services prioritize	
		1.2	User Story 1.2 (UC#2): **As an ISP**, **I want to** have an early detection system for the QoE degradation, **so that** I can make decisions in advance to mitigate it	
		2	As a network administrator, I want an autonomous way for	

		detecting and characterizing traffic anomalies, so that it makes possible to autonomously and efficiently manage them
	2.1	As a network administrator, I want a mining mechanism, so that traffic classes can be autonomously distinguished
	2.2	As a network administrator, I want a discrimination mechanism so that anomalies signatures can be autonomously issued
	2.3	As a network administrator, I want a ranking score for assessing the abnormality and dangerousness of anomalies, so that an autonomous process can discriminate between discarding attacks vs. Coping with legitimate anomalies management

Table 3: Epics Product Backlog

11.3 Use Case # 1. Network Anomaly Detection

11.3.1 Product Backlog

Third detailed user stories' level for User Story #1.2 (UC#2) is shown in Table 4:

Status	Sprint	ID	User Stories	Comments
		2.1.1	**As a network administrator, I want to** have efficient monitoring and unsupervised clustering techniques, **so that** I can autonomous classify the network traffic	
		2.1.2	**As a network administrator, I want to** have mechanisms for identifying the most significant traffic attributes, **so that** It becomes possible to issue traffic classes discrimination rules	
		2.1.3	**As a network administrator, I want to** have accurate abnormality score, **so that** It becomes possible to autonomously discriminate between legitimate and illegitimate traffic classes	

Table 4: Use Case 1 Product Backlog

11.4 Use Case # 2. Proactive Congestion Detection and Control System

11.4.1 Product Backlog

The user stories for User Story #1.2 (UC#2) are shown in Table 5:

Status	Sprint	ID	User Stories	Comments
		1.2.1	**As an ISP, I want to** have a way to detect congestion patterns by locations and link them with related access points, **so that** I can customize already existing policies in the policy node	
		1.2.2	**As an ISP, I want to** have an efficient way to set-up policies on the network, **so that** I can make decisions about how to use my resources	
		1.2.3	**As an ISP, I want to** have my own set of preferences about the services I want to keep on going in case of a bandwidth limitation, **so that** I can make decisions about how to use my resources	

Table 5: Use Case 2 Product Backlog

11.5 Use Case # 3. Dynamic QoS Management

11.5.1 Product Backlog

The user stories for User Story 1.1 (UC#2) are shown in Table 6:

Status	Sprint	ID	User Stories	Comments
		1.1.1	**As an ISP, I want to** be able of automatically detect new applications and services already running in my network, **so that** I can make a decision about what prioritize	
		1.1.2	**As an ISP, I want to** know more in deep what means QoE for my customers, **so that** I can adjust the network parameters in consequence	
		1.1.3	**As an ISP, I want to** know how QoE parameters are linked to the QoS ones, **so that** I can provide the best QoE to my	

		customers
	1.1.4	**As an ISP**, I **want to** know better my customers, **so that** I can provide the best QoE to my them

Table 6: Use Case 3 Product Backlog

12. References

[1] ONTIC. “Deliverable D2.1. Requirement Strategy.” Internet: http://www.ict-ontic.eu/, Feb. 2014 [Jan. 1, 2015].

[2] ONTIC. “Deliverable D4.1. Infrastructure Description.” Internet: http://www.ict-ontic.eu/, Feb. 2015 [Feb. 1, 2015].

[3] ONTIC. “Deliverable D5.2: Progress on Use Cases.” Feb. 2016 (due date).

[4] ONTIC. “Deliverable D6.4. Progress on Exploitation and Dissemination Plans – Part I.” Internet: http://www.ict-ontic.eu/, Feb. 2015 [Feb. 1, 2015]

[5] DSL Forum Architecture & Transport Working Group. “DSL Forum Technical Report TR-126: Triple-play Services Quality of Experience (QoE) Requirements.” Internet: https://www.broadband-forum.org/technical/download/TR-126.pdf, Dec. 2006 [Nov. 23, 2014].

[6] Citrix. “Quality of Experience for Mobile Data Networks. White Paper.” Internet: https://www.citrix.se/content/dam/citrix/en_us/documents/products-solutions/quality-of-experience-for-mobile-data-networks.pdf [Nov. 22, 2014].

[7] Eileen Dillon et al. “PERIMETER: a quality of experience framework,” 2009 [Nov. 22, 2014].

[8] Wikipedia contributors. “Mean opinion score.” Internet: http://en.wikipedia.org/w/index.php?title=Mean_opinion_score&oldid=627638924, Nov. 30, 2014 [Dec. 4, 2014].

[9] Selim Ickin et al. (2012). “Factors influencing quality of experience of commonly used mobile applications.” *Communications Magazine, IEEE*, vol. 50, no 4, p. 48-56. Available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6178833&isnumber=6178822 [Nov. 27, 2014].

[10] Nokia. “Telecom Services White Papers: Quality of Experience (QoE) of mobile services: can it be measured and improved?” Internet: http://www.afutt.org/Qostic/qostic1/MOB-GD-MGQ-NOKIA-040129-Nokia-whitepaper_qoe_net-final.pdf, 2004 [Nov. 23, 2014].

[11] Ofcom. “Measuring mobile voice and data quality of experience.” Internet: http://stakeholders.ofcom.org.uk/binaries/consultations/mobile-voice-data-experience/summary/condoc.pdf, Jan. 23, 2013 [Nov. 23, 2014].

[12] K. Beck, M. Beedle, A. Van Bennekum, A. Cockburn, W. Cunningham, M. Fowler... & D. Thomas. “Manifesto for agile software development.” Internet: http://agilemanifesto.org/principles.html, 2001 [Dec. 16, 2014].

[13] P. Barford, J. Kline, D. Plonka, and A. Ron, “A signal analysis of network traffic anomalies,” in *Proc. ACM IMW*, 2002.

[14] J. Brutlag, “Aberrant behavior detection in time series for network monitoring,” in *Proc. 14th Systems Administration Conference*, 2000.

[15] B. Krishnamurthy, S. Sen, Y. Zhang, and Y. Chen, “Sketch-based change detection: Methods, evaluation, and applications,” in *Proc. ACM IMC*, 2003.

[16] A. Lakhina, M. Crovella, and C. Diot, “Characterization of network-wide anomalies in traffic flows,” in *Proc. ACM IMC*, 2004.

[17] A. Lakhina, M. Crovella, and C. Diot, “Mining anomalies using traffic feature distributions,” in *Proc. ACM SIGCOMM*, 2005.

[18] A. Lakhina, C. Diot, and M. Crovella, “Diagnosing network-wide traffic anomalies,” in *Proc. ACM SIGCOMM*, 2004.

[19] X. Li, F. Biang, M. Crovella, C. Diot, R. Govindan, G. Iannaccone, and A. Lakhina, “Detection and identification of network anomalies using sketch subspaces,” in *Proc. ACM IMC*, 2006.

[20] P. Casas, S. Vaton, L. Fillatre, and I. Nikiforov, “Optimal volume anomaly detection and isolation in large-scale ip networks using coarse-grained measurements,” *Computer Networks*, vol. 54, pp. 1750-1766, 2010.

[21] H. Ringberg, A. Soule, J. Rexford, and C. Diot, “Sensitivity of PCA for traffic anomaly detection,” in *Proc. ACM SIGMETRICS*, 2007.

[22] P. Casas, J. Mazel, and P. Owezarski, “Unada: Unsupervised network anomaly detection using sub-space outliers ranking,” presented at IFIP Networking conference, 2011.

[23] E. Eskin, A. Arnold, M. Prerau, L. Portnoy, and S. Stolfo, “A geometric framework for unsupervised anomaly detection: Detecting intrusions in unlabeled data,” in *Applications of Data Mining in Computer Security*, Kluwer Publisher, 2002.

[24] K. Leung and C. Leckie, “Unsupervised anomaly detection in network intrusion detection using clustering,” in *Proc. ACSC05*, 2005.

[25] L. Portnoy, E. Eskin, and S. Stolfo, “Intrusion detection with unlabeled data using clustering,” in *Proc. ACM DMSA Workshop*, 2001.

[26] G. Fernandes and P. Owezarski, “Automated classification of network traffic anomalies,” in *Proc. SecureComm’09*, 2009.

[27] F. Silveira and C. Diot, “RCA: Pulling anomalies by their root causes,” in *Proc. IEEE INFOCOM*, 2010.

[28] G. Cormode and S. Muthukrishnan, “What’s new: Finding significant differences in network data streams,” *IEEE Trans. on Networking*, vol. 13 (6), pp. 1219-1232, 2005.

[29] J. Mazel, P. Casas, Y. Labit, and P. Owezarski, “Sub-space clustering, interclustering results association & anomaly correlation for unsupervised network anomaly detection,” presented at the 7th International Conference on Network and Service Management (CNSM 2011), CNSM’11, October 2011.

[30] L. Parsons, E. Haque, and H. Liu, “Subspace clustering for high dimensional data: a review,” *ACM SIGKDD Expl. Newsletter*, vol. 6 (1), pp. 90-105, 2004.

[31] A. Fred and A. K. Jain, “Combining multiple clusterings using evidence accumulation,” *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. 27 (6), pp. 835-850, 2005.

[32] A. K. Jain, “Data clustering: 50 years beyond k-means,” *Pattern Recognition Letters*, vol. 31 (8), pp. 651-666, 2010.

[33] J. Gantz and D. Reinsel. “Extracting value from chaos,” in *Proc. IDC iView*, 2011, pp. 1-12. Available: http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf [Aug. 31, 2014]

[34] Ashish Nadkarni, Dan Vesset. “Worldwide Big Data Technology and Services 2014-2018 Forecast.” Internet: http://www.idc.com/getdoc.jsp?containerId=250458, Sep. 2014 [Nov. 21, 2014].

[35] Peter Groves, Basel Kayyali, David Knot, and Steve Van Kuiken. “The ‘big data’ revolution in healthcare: accelerating value and innovation.” Internet: http://www.mckinsey.com/~/media/mckinsey/dotcom/client_service/healthcare%20systems%20and%20services/pdfs/the_big_data_revolution_in_healthcare.ashx, Jan. 2013.

[36] J. Manyika et al. (2011). *Big data: The Next Frontier for Innovation, Competition, and Productivity*. [Online]. Pp. 1–137. Available:

http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights%20and%20pubs/MGI/Research/Technology%20and%20Innovation/Big%20Data/MGI_big_data_full_report.ashx [Jan. 12, 2015]

[37] Han Hu, Yonggang Wen, Tat-Seng Chua, Xuelong Li, "Toward Scalable Systems for Big Data Analytics: A Technology Tutorial," *IEEE Access*, vol. 2, pp. 652, 687, 2014.

[38] S. Ghemawat, H. Gobioff, and S.-T. Leung, "The Google file system," in *ACM SIGOPS Operating Systems Review*, 2003, pp. 29–43.

[39] "Hadoop Distributed File System." Internet: http://hadoop.apache.org/docs/r1.0.4/hdfsdesign.html

[40] F. Chang et al., "Bigtable: A distributed storage system for structured data," in *ACM Transactions on Computer Systems (TOCS)*, vol. 26, no. 2, Jun. 2008, pp. 4:1–4:26.

[41] "HBase." Internet: http://hbase.apache.org/

[42] A. Lakshman and P. Malik, "Cassandra: Structured storage system on a p2p network," in *Proceedings of the 28th ACM symposium on Principles of distributed computing*, 2009, p. 5.

[43] "MongoDB." Internet: http://www.mongodb.org/

[44] "SimpleDB by Amazon." Internet: http://aws.amazon.com/simpledb/

[45] D. W. Walker and J. J. Dongarra, "MPI: A standard message passing interface," *Supercomputer*, vol. 12, 1996, pp. 56–68.

[46] "OpenMP." Internet: http://openmp.org/wp/

[47] J. Dean and S. Ghemawat, "MapReduce: Simplified data processing on large clusters," *Communications of the ACM*, vol. 51, no. 1, 2008, pp. 107–113.

[48] A. F. Gates et al., "Building a high-level dataflow system on top of Map-Reduce: The Pig experience," in *Proceedings of the VLDB Endowment*, vol. 2, no. 2, Aug. 2009. pp. 1414-1425.

[49] A. Thusoo et al., "Hive: A warehousing solution over a Map-Reduce framework," in *Proceedings of the VLDB Endowment*, vol. 2, no. 2, 2009, pp. 1626–1629.

[50] Matei Zaharia, Mosharaf Chowdhury, Michael J. Franklin, Scott Shenker, and Ion Stoica. 2010. "Spark: cluster computing with working sets," in *Proceedings of the 2nd USENIX conference on Hot topics in cloud computing*, p. 10-10.

[51] "Storm." Internet: http://storm-project.net/

[52] L. Neumeyer, B. Robbins, A. Nair, and A. Kesari, "S4: Distributed stream computing platform," in *Proceedings of the IEEE International Conference on Data Mining Workshops (ICDMW)*, 2010, pp. 170–177.

[53] G. Malewicz et al., "Pregel: A system for large-scale graph processing," in *Proceedings of the 2010 ACM SIGMOD International Conference on Management of data*, 2010, pp. 135–146.

[54] "GraphX. Apache Spark API for graph-parallel computation". Internet: https://spark.apache.org/graphx

[55] "Apache Giraph". Internet http://giraph.apache.org/

[56] Y. Low, D. Bickson, J. Gonzalez, C. Guestrin, A. Kyrola, and J. M. Hellerstein, "Distributed graphlab: A framework for machine learning and data mining in the cloud," in *Proceedings of the VLDB Endowment*, vol. 5, no. 8, 2009, pp. 716–727.

[57] A. Mozo, J. L. Lopez-Presa, and A. Fernández Anta, "Slbn: A scalable max-min fair algorithm for rate-based explicit congestion control," in *Network Computing and Applications (NCA),2012 11th IEEE International Symposium* on. IEEE, 2012, pp. 212–219.

[58] S. Floyd, “Tcp and explicit congestion notification,” *ACM SIGCOMM Computer Communication Review*, vol. 24, no. 5, pp. 8–23, 1994.

[59] N. Dukkipati and N. McKeown, “Why flow-completion time is the right metric for congestion control,” *ACM SIGCOMM Computer Communication Review*, vol. 36, no. 1, pp. 59–62, 2006.

[60] N. Dukkipati, N. McKeown, and A. G. Fraser, “Rcp-ac: Congestion control to make flows complete quickly in any environment,” in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications*. Proceedings. IEEE, 2006, pp. 1–5.

[61] A. Bascuñana, F. Castro, D. Espadas, P. Sánchez, M.A. Monjas (2014). “Adaptive Quality of Experience (AQoE) control for Telecom Networks.” *Proceedings First international Workshop BigDAP ‘14*, Sept. 11-12, 2014.

[62] Arthur D. Little. “Cost Reduction in the Telecom Industry.” Internet: http://www.adlittle.com/downloads/tx_adlreports/ADL_Cost_Reduction_Telecom_Industry.pdf, 2010 [Jul. 1, 2014]

[63] Frost&Sullivan. “How Real-Time Convergent Billing, Policy, Self-Service, and Analytics Are Changing the Future.” Internet: https://www.asiainfo.com/Portals/0/pdfs/products/2014%20June_Stratecast_AsiaInfo_SPIE_RealTime%20Convergence.pdf, Jun. 13, 2014 [Jul. 2, 2014]

[64] “Gartner IT Glossary.” Internet: http://www.gartner.com/it-glossary/big-data/

[65] Wikipedia contributors. “Big data.” Internet: https://en.wikipedia.org/w/index.php?title=Big_data&oldid=642117737, Jan. 12, 2015

[66] Christiane Lefevre. “LHC Brochure.” Internet: https://cds.cern.ch/record/1278169?ln=en, 2010 [Jan. 2013].

[67] Christiane Lefevre. “LHC: the guide.” Internet: http://cds.cern.ch/record/1092437?ln=en, 2008 [Jan. 20, 2013].

[68] Geoff Brumfiel (Jan. 2011).”High-energy physics: Down the petabyte highway.” *Nature* 469, pp. 282–83, doi:10.1038/469282a.

[69] “Data, data everywhere.” *The Economist* (Feb. 25, 2010). Internet: https://www.emc.com/collateral/analyst-reports/ar-the-economist-data-data-everywhere.pdf

[70] “Supercomputing the Climate: NASA's Big Data Mission.” *CSC World Magazine* (Spring 2012). Internet: http://www.csc.com/cscworld/publications/81769/81773-supercomputing_the_climate_nasa_s_big_data_mission

[71] Andrew Lampitt. “The real story of how big data analytics helped Obama win.” *Infoworld* (Feb. 14, 2013). Internet: http://www.infoworld.com/article/2613587/big-data/the-real-story-of-how-big-data-analytics-helped-obama-win.html [May 31, 2014].

[72] Liz Tay, “Inside eBay’s 90PB data warehouse.” Internet: http://www.itnews.com.au/News/342615,inside-ebay8217s-90pb-data-warehouse.aspx, May 10, 2013

[73] Robert Johnson. “Scaling Facebook to 500 Million Users and Beyond.” Internet: https://www.facebook.com/notes/facebook-engineering/scaling-facebook-to-500-million-users-and-beyond/409881258919, Jul. 21, 2010.

[74] Danny Sullivan. “Google: 100 Billion Searches Per Month, Search To Integrate Gmail, Launching Enhanced Search App For iOS.” Internet: http://searchengineland.com/google-search-press-129925, Aug. 8, 2012.

[75] Stacey Higginbotham. “As data gets bigger, what comes after a yottabyte?” Internet: https://gigaom.com/2012/10/30/as-data-gets-bigger-what-comes-after-a-yottabyte/, Oct. 30, 2012

[76] Scrum Alliance. “Getting Started with Scrum.” Internet: https://www.scrumalliance.org/why-scrum/getting-started-with-scrum [Jun. 12, 2014]

[77] D. Katabi, M. Handley, and C. Rohrs, “Congestion control for high bandwidth-delay product networks,” *ACM SIGCOMM Computer Communication Review*, vol. 32, no. 4, pp. 89–102, 2002.

[78] S. Athuraliya, S. H. Low, V. H. Li, and Q. Yin, “REM: active queue management,” *Network, IEEE*, vol. 15, no. 3, pp. 48–53, 2001.

[79] V. Jacobson, “Congestion avoidance and control,” in *ACM SIGCOMM Computer Communication Review*, vol. 18, no. 4. ACM, 1988, pp. 314–329.

[80] S. Floyd and V. Jacobson, “Random early detection gateways for congestion avoidance,” *Networking, IEEE/ACM Transactions on*, vol. 1, no. 4, pp. 397–413, 1993.

[81] K. Ramakrishnan and R. Jain, “A binary feedback scheme for congestion avoidance in computer networks,” *ACM Transactions on Computer Systems (TOCS)*, vol. 8, no. 2, pp. 158–181, 1990.

[82] E. S. Hashem, “Analysis of random drop for gateway congestion control,” DTIC Document, Tech. Rep., 1989.

[83] K. Ramakrishnan, S. Floyd, D. Black et al., “The addition of explicit congestion notification (ECN) to IP,” 2001.

[84] S. H. Low, F. Paganini, J. Wang, S. Adlakha, and J. C. Doyle, “Dynamics of TCP/RED and a scalable control,” in *INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 1. IEEE, 2002, pp. 239–248.

[85] C. V. Hollot, V. Misra, D. Towsley, and W.-B. Gong, “On designing improved controllers for AQM routers supporting TCP flows,” in *INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 3. IEEE, 2001, pp. 1726–1734.

[86] C. V. Hollot, V. Misra, D. Towsley, and W. Gong, “Analysis and design of controllers for AQM routers supporting TCP flows,” *Automatic Control, IEEE Transactions* on, vol. 47, no. 6, pp. 945–959, 2002.

[87] N. Dukkipati, M. Kobayashi, R. Zhang-Shen, and N. McKeown, “Processor sharing flows in the internet,” in *Quality of Service-IWQoS 2005*. Springer, 2005, pp. 271–285.

[88] S. Jain and D. Loguinov, “PIQI-RCP: Design and Analysis of Rate-Based Explicit Congestion Control,” in *Quality of Service, 2007 Fifteenth IEEE International Workshop on*. IEEE, 2007, pp. 10–20.

[89] Y. Xia, L. Subramanian, I. Stoica, and S. Kalyanaraman, “One more bit is enough,” in *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 4. ACM, 2005, pp. 37–48.

[90] N. Vasic, S. Kuntimaddi, and D. Kostic, “One bit is enough: a framework for deploying explicit feedback congestion control protocols,” in *Communication Systems and Networks and Workshops, 2009. COMSNETS 2009. First International*. IEEE, 2009, pp. 1–9.

[91] X. Li and H. Yousefi’zadeh, “MPCP: multi packet congestion-control protocol,” *ACM SIGCOMM Computer Communication Review*, vol. 39, no. 5, pp. 5–11, 2009.

[92] I. A. Qazi, L. L. Andrew, and T. Znati, “Congestion control using efficient explicit feedback,” in *INFOCOM 2009, IEEE*. IEEE, 2009, pp. 10–18.

[93] E. L. Hahne and R. G. Gallager, “Round robin scheduling for fair flow control in data communication networks,” DTIC Document, Tech. Rep., 1986.
[94] M. Katevenis, “Fast switching and fair control of congested flow in broadband networks,” *Selected Areas in Communications, IEEE Journal on*, vol. 5, no. 8, pp. 1315–1326, 1987.
[95] Y. Bartal, M. Farach-Colton, S. Yooseph, and L. Zhang, “Fast, fair, and frugal bandwidth allocation in ATM networks,” in *Proceedings of the tenth annual ACM-SIAM symposium on Discrete algorithms*. Society for Industrial and Applied Mathematics, 1999, pp. 92–101.
[96] Z. Cao and E. W. Zegura, “Utility max-min: An application-oriented bandwidth allocation scheme,” in *INFOCOM’99. Eighteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE*, vol. 2. IEEE, 1999, pp. 793–801.
[97] V. Jacobson, K. Nichols, K. Poduri et al., “RED in a different light,” 1999.
[98] W.-c. Feng, D. Kandlur, D. Saha, and K. Shin, “BLUE: A new class of active queue management algorithms,” *Ann Arbor*, vol. 1001, p. 48105, 1999.
[99] W.-c. Feng, D. D. Kandlur, D. Saha, and K. G. Shin, “Stochastic fair blue: A queue management algorithm for enforcing fairness,” in INFOCOM 2001. Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, vol. 3. IEEE, 2001, pp. 1520–1529.
[100] J. Gozdecki, A. Jajszczyk, and R. Stankiewicz, “Quality of service terminology in IP networks,” Communications Magazine, IEEE, vol. 41, no. 3, pp. 153–159, 2003.
[101] E. Crawley, H. Sandick, R. Nair, and B. Rajagopalan, “RFC 2386: A framework for QoS-based routing in the Internet,” 1998.
[102] Javier Pastor-Balbás, Stefan Rommer, and John Stenfelt, “Policy and Charging Control in the Evolved Packet System.” Communications Magazine, vol. 47, no 2, pp. 68-74, Feb. 2009.
[103] S. Ha, I. Rhee, and L. Xu, “CUBIC: a new TCP-friendly high-speed TCP variant,” ACM SIGOPS Operating Systems Review, vol. 42, no. 5, pp. 64–74, 2008. Z. Liu, Y. Zhang, and C. Philip Chen, “Adaptive mechanism-based congestion control for networked systems,” International Journal of Systems Science, vol. 44, no. 3, pp. 533–544, 2013.
[104] K. Avrachenkov, U. Ayesta, J. Doncel, and P. Jacko, “Congestion control of TCP flows in internet routers by means of index policy,” Computer Networks, vol. 57, no. 17, pp. 3463–3478, 2013.
[105] J. Wang, J. Wen, J. Zhang, and Y. Han, “TCP-FIT: An improved TCP congestion control algorithm and its performance,” in INFOCOM, 2011 Proceedings IEEE. 2894–2902. IEEE, 2011, pp. 2894-2902
[106] J. Wang, J. Wen, Y. Han, J. Zhang, C. Li, and Z. Xiong, “CUBIC-FIT: A high performance and TCP CUBIC friendly congestion control algorithm,” *Communications Letters*, IEEE, vol. 17, no. 8, pp. 1664–1667, 2013.
[107] M. Handley, S. Floyd, J. Padhye, and J. Widmer, “RFC 3448. TCP Friendly Rate Control (TFRC): Protocol Specification,” Jan. 2003.
[108] A. Sathiaseelan and G. Fairhurst, “TCP-Friendly Rate Control (TFRC) for bursty media flows,” *Computer Communications*, vol. 34, no. 15, pp. 1836–1847, 2011.
[109] P. Yang and L. Xu, “A survey of deployment information of delay-based TCP congestion avoidance algorithm for transmitting multimedia data,” in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*. IEEE, 2011, pp. 18–23.

[110] S. Radhakrishnan, Y. Cheng, J. Chu, A. Jain, and B. Raghavan, "TCP fast open," in *Proceedings of the Seventh COnference on emerging Networking EXperiments and Technologies*. ACM, 2011, p. 21.

[111] D. A. Hayes and G. Armitage, "Revisiting TCP congestion control using delay gradients," in *NETWORKING 2011*. Springer, 2011, pp. 328–341.

[112] W. Zhang, L. Tan, C. Yuan, G. Chen, and F. Ge, "Internet primal-dual congestion control: Stability and applications," *Control Engineering Practice*, vol. 21, no. 1, pp. 87–95, 2013.

[113] D. Ros and M. Welzl, "Less-than-best-effort service: a survey of end-to-end approaches," *Communications Surveys & Tutorials, IEEE*, vol. 15, no. 2, pp. 898–908, 2013.

[114] N. Dukkipati, T. Refice, Y. Cheng, J. Chu, T. Herbert, A. Agarwal, A. Jain, and N. Sutin, "An argument for increasing TCP's initial congestion window." *Computer Communication Review*, vol. 40, no. 3, pp. 26–33, 2010.

[115] R. Barik and D. M. Divakaran, "Evolution of TCP's initial window size," in *Local Computer Networks (LCN), 2013 IEEE 38th Conference on*. IEEE, 2013, pp. 500–508.

[116] D. Papadimitriou, M. Welzl, M. Scharf, and B. Briscoe, "RFC 6077. Open research issues in internet congestion control," Feb. 2011.

[117] S. H. Low, F. Paganini, J. Wang, and J. C. Doyle, "Linear stability of TCP/RED and a scalable control," *Computer Networks*, vol. 43, no. 5, pp. 633–647, 2003.

[118] I. D. Barrera, S. Bohacek, and G. R. Arce, "*Statistical detection of congestion in routers*," Signal Processing, IEEE Transactions on, vol. 58, no. 3, pp. 957–968, 2010.

[119] V. Alarcon-Aquino and J. A. Barria, "Multiresolution FIR neural-network-based learning algorithm applied to network traffic prediction," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol. 36, no. 2, pp. 208–220, 2006.

[120] D.-C. Park, "Structure optimization of BiLinear Recurrent Neural Networks and its application to Ethernet network traffic prediction," *Information Sciences*, vol. 237, pp. 18–28, 2013.

[121] P. Bermolen and D. Rossi, "Support vector regression for link load prediction," *Computer Networks*, vol. 53, no. 2, pp. 191–201, 2009.

[122] G. Gursun, M. Crovella, and I. Matta, "Describing and forecasting video access patterns," in *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, pp. 16–20.

[123] F. Li, J. Sun, M. Zukerman, Z. Liu, Q. Xu, S. Chan, G. Chen, and K.-T. Ko, "A comparative simulation study of TCP/AQM systems for evaluating the potential of neuron-based AQM schemes," *Journal of Network and Computer Applications*, vol. 41, pp. 274–299, 2014.

[124] M. Mirza, J. Sommers, P. Barford, and X. Zhu, "A machine learning approach to TCP throughput prediction," in *ACM SIGMETRICS Performance Evaluation Review*, vol. 35, no. 1. ACM, 2007, pp. 97–108.

[125] LM Ericsson. "Ericsson Customer Experience Assurance." Internet: http://www.ericsson.com/ourportfolio/products/customer-experience-assurance [Jan. 9, 2015]

[126] "3GPP TS 23.402 V12.4.0 (2014-03): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses (Release 12)," pp. 49-59. Internet:

http://www.3gpp.org/ftp/Specs/archive/23_series/23.402/23402-c40.zip, Mar. 2014 See section 4.8.2.1

[127] "3GPP TS 24.302 V12.4.0 (2014-03): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks; Stage 3 (Release 12)." Internet: http://www.3gpp.org/ftp/Specs/archive/24_series/24.302/24302-c40.zip, Mar. 2014.

[128] Miguel-Ángel García-Martín, Pablo Martínez de la Cruz. "Policy Decisions for Data Communications in Constrained Resource Networks." PCT Patent Application. PCT/EP10/66337, Oct. 28, 2010.

[129] "3GPP TR 23.705 V0.10.0 (2014-04): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on system enhancements for user plane congestion management (Release 13)," pp. 39-44. Internet: http://www.3gpp.org/ftp/Specs/archive/23_series/23.705/23705-0a0.zip, Apr. 2014.

[130] "3GPP TS 24.312 V12.3.0 (2013-12): 3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Access Network Discovery and Selection Function (ANDSF) Management Object (MO) (Release 12)" Internet: http://www.3gpp.org/ftp/Specs/archive/24_series/24.312/24312-c30.zip, Dec. 2013.

[131] Roberto Carnero-Ros, Beatriz Pérez-Laínez. "Method For Introducing Network Congestion Predictions in Policy Decision." PCT Patent Application. PCT/IB2011/050823, Feb. 25, 2011.

[132] Víctor-Manuel Ávila-González, Roberto Carnero-Ros and Zsolt Kenesi. "Technique for Introducing a Real-Time Congestion Status in a Policy Decision for a Cellular Network." PCT Patent Application. PCT/EP2010/003905, Jun. 25, 2010.

[133] "Overview of MPEG-DASH Standard." Internet: http://dashif.org/mpeg-dash/

[134] K. Salamatian and S. Vaton, "Hidden Markov modeling for network communication channels," in *ACM SIGMETRICS Performance Evaluation Review*, vol. 29, no. 1. ACM, 2001, pp. 92–101.

[135] B.-Y. Lee and G.-H. Lee, "Service Oriented Architecture for SLA Management System." *The 9th International Conference on Advanced Communication Technology*, vol. 2, 2007, pp. 1415–1418.

[136] D. Grossman, "RFC 3260: New Terminology and Clarifications for Diffserv." Internet: https://tools.ietf.org/html/rfc3260, April 2002.

[137] "3GPP TS 23.107 V12.0.0 (2014-09): 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Quality of Service (QoS) concept and architecture (Release 12)." Internet: http://www.3gpp.org/ftp/Specs/archive/23_series/23.107/23107-c00.zip, Sep. 2014.

[138] Erick Hans Klijn. "Analyzing and Managing Policy Processes in Complex Networks. A Theoretical Examination of the Concept Policy Network and Its Problems." *Administration & Society*, vol. 28, no. 1, 1996, pp. 90-119.

[139] Jim Boyle, David Durham, and Shai Herzog. "RFC2749. COPS usage for RSVP." (2000)

[140] Stefano Zanero. "Flaws and frauds in the evaluation of IDS/IPS technologies." In *Proc. of FIRST*, 2007.

[141] H. Hegering, S. Abeck, B. Neumair. *Integrated management of networked systems: concepts, architectures, and their operational application*, Morgan Kaufmann Publishers, Inc. 1999, pp.121-152.

[142] J. P. Martin-Flatin, S. Znaty, J. P. Hubaux. “A Survey of Distributed Enterprise Network and Systems Management Paradigms,” *Journal of Network and Systems Management*, vol.7, no.1, 1999

[143] M. Stevens et al. “IETF Internet Draft: Policy Framework,” work in progress. Internet: https://tools.ietf.org/html/draft-ietf-policy-framework-00, Sep. 1999.

[144] A. Westerinen et al. “IETF Internet Draft: Policy Terminology,” work in progress. Internet: https://tools.ietf.org/html/draft-ietf-policy-terminology-00, July 2000.

[145] Wikipedia contributors. “HP OpenView.” Internet: https://en.wikipedia.org/w/index.php?title=HP_OpenView&oldid=619684855, Aug. 3, 2014 [Dec. 22, 2014].

[146] “CPacket Networks: Spifee”. Internet: http://cpacket.com/products/spifee, 2015

[147] “Cisco Systems Inc.: Security Products.” Internet: http://www.cisco.com/c/en/us/products/security/firewalls/index.html, 2015

[148] Fortinet. “High Performance Next-Generation Firewall and UTM FortiGate Platform.” Internet: http://www.fortinet.com/products/fortigate/