Deliverable D3.3

Identification of suitable classes of methods for learning and operations

Grant Agreement	257513
Date of Annex I	25-07-2011
Dissemination Level	Public
Nature	Report
Work package	WP3 – Network Empowerment
Due delivery date	01 September 2011
Actual delivery date	14 September 2011
Lead beneficiary	INRIA Eric Fabre (fabre@irisa.fr)

SEVENTH FRAMEWORK PROGRAMME

FUTURE NETWORKS

Authors	INRIA, Martin Barrere, Remi Badonnel, Olivier Festor, Eric Fabre (Editor) ALBLF, Leila Benacer ALBLI, Rouzbeh Razavi ALUD, Ingo Karla, Markus Gruber NEC, Johannes Lessmann, Paulo Loureiro, Zarrar Yousaf FT, Zwi Altman, Richard Combes TIS, Antonio Manzalini TID, Alfonso Castro, Beatriz Fuentes Fraunhofer, Mikhail Smirnov UNIS, Majid Ghader, Stylianos Georgoulas NKUA, Panagiotis Spapis, George Katsikas UPRC, Kostas Tsagkaris, Vera Stavroulaki, Aimilia Bantouna, Giorgos Poulios, Yiouli Kritikou, Panagiotis Vlacheas, George Athanasiou, Nikos Koutsouris, Dimitris Karvounas, Evagelia Tzifa, Assimina Sarli, Evangelos Thomatos, Marios Logothetis, Andreas Georgakopoulos, Louiza Papadopoulou, Panagiotis Demestichas UT, Ramin Sadre

Executive summary

As per the Description of Work, deliverables D3.2/D3.3 identifies learning methods that are suitable to given problems. Furthermore, it presents cooperative network/service operations and introduces distributed cross-layer and cross-domain methods including observation, correlation, decision-making, and control.

More concretely, this document examines different problems that have been selected in the various use-cases of the project (see deliverable D4.1), and that are 1/ exemplary of important features one can expect from self-management methods, and 2/ of practical importance to network operators, as sources of OPEX/CAPEX reductions, 3/ instructive about the design of a Unified Management Framework (UMF). Two other main deliverable series are attached to WP3 on network empowerment. Deliverable D3.1 focuses on all aspects of parameter optimization in networks, whereas deliverable D3.4 addresses the cooperation strategies between different management functions and/or modules. The idea is that modern networks are intrinsically distributed systems, with diverse technologies, vendors, managed domains and objectives. Their management is also distributed, both for scalability issues, and to account for different managed domains and various objectives of the management functions. Therefore one must address issues like the cooperation to achieve a global objective, compatibility of local objectives, trustability, etc. In contrast, deliverable D3.2 and deliverable D3.3 address all the remaining aspects of network empowerment, which covers the design of algorithms for all parts of control loops: observation, knowledge extraction, decision, action, as well as stability issues. The selected problems cover fault diagnosis, healing, information dissemination, optimal content delivery, early detection of congestion, vulnerability detection and management, stability issues of control loops, and more.

The document is structured according to use-cases, in which several specific problems are extracted. These problems have different degrees of ambition and of maturity, and this version of the deliverable tries to capture the work achieved so far to address them. There will be future releases of this work, at the second and third year of the project, where the algorithmic solutions will be given with more details. The work described here will support both the demonstrations and validations scheduled in the life cycle of the use-cases, and will serve as a basis to design and challenge the concepts of UMF.

This document (D3.3) is the public part of the technical report D3.2 which is restricted to internal use to the UniverSelf project.

Table of Content

1 Introduction 5

2 Problems in use case 1 Self-diagnosis and self-healing for IMS VoIP and VPN Services 6

2.1 Joint failure management in network and IMS services: a framework for active diagnosis 6

2.2 Improvement of fault diagnosis based on the combination of Bayesian network and case-based reasoning 6

2.3 Vulnerability management in autonomic networks and services 7

2.4 QoS-based fault management in IP networks and IMS services: framework for active diagnosis and reasoning adjustment 7

2.5 Autonomic management of intrusion detection systems 7

2.6 Traffic trace analysis of free WiFi hotspots, as a preliminary to network optimization 8

2.7 Proactive diagnosis of congestion 8

3 Problems in use case 2 Networks' Stability and Performance 9

3.1 Controlling the stability of a complex network 9

3.2 Vulnerability management in autonomic networks 9

4 Problems in use case 3 Dynamic virtualization and migration of contents and servers 10

4.1 Identification and acquisition of user, network and service context for dynamic migration of network entities 10

4.2 Optimization of context acquisition and dissemination using a distributed data mining framework 10

4.3 Resource and service discovery and rule-based reasoning from contextual data 11

5 Problems in use case 4 SON and SON collaboration according to operator policies 12

5.1 Robust learning using policy gradient reinforcement learning 12

5.2 Observation and action in orchestration of SON LTE control loops 12

5.3 Optimization of femtocell networks using fuzzy logic assisted reinforcement learning 12

6 Problems in use case 6 Deployment of new services and accommodation of new traffic on heterogeneous networks 14

6.1 A fuzzy reinforcement learning approach to pre-congestion notification (PCN) - based admission control14

6.2 Bandwidth estimation 14

7 Problems in use case 7 Network and service governance for IPTV over fixed and mobile networks 16

7.1 Providing FTTH network elements with self-* feature 16

8 Conclusion 17

Acronyms 18

Definitions 20

1 Introduction

This deliverable has been developed in the work package 3 “Network Empowerment” that aims at developing algorithms to address a selection of typical network management problems for which autonomic solutions are desirable. Within the project, the long-range objective is twofold:

1. to demonstrate on concrete use-cases how self-management can be implemented, and thus propose methodologies to existing or emerging management issues of operators,
2. to identify the essential features of self-management functions, and help define the characteristics of a Unified Management Framework (UMF), that would allow a soft embedding of such autonomic functionalities. The work about the UMF is essentially covered by the WP2.

Within WP3, deliverable D3.1 focuses on optimization issues that arise in network management, while deliverable D3.4 is concerned by the cooperation strategies that must take place in self-management functions that address large heterogeneous systems. The idea is that the management of large systems must necessarily be distributed in order to cope with scalability issues, and thus the various management modules have to cooperate in order to guarantee that global management objectives are met. Deliverable D3.2 and its public part D3.3 are concerned with some remaining aspects of network management, typically those related to observing the network behaviour, building knowledge about it and extracting aggregated information about events of interest, in order to drive control actions over the network. A central difficulty being that one has to manage essentially a distributed system, so distributed management solutions seem natural, which makes the link with deliverable D3.4.

The ultimate objective of deliverables D3.2/D3.3 is to identify the suitable classes of methods to progress towards self-managed networks. There will be follow-ups to this document within the project, as deliverables D3.6 (end of year 2) and D3.9 (end of year 3). For the initial step, it was considered that the most productive way of addressing the question would be to make sure that all the management problems that have been identified in the various use-cases of the project were correctly handled. Concretely, this means that each problem is correctly described and understood, that the state-of-the-art on the topic is well covered, and mostly that the formalisation has started: i.e. mathematical expression of the problem, and identification of the algorithmic solution(s) that will be used/designed to address it. This is a little below the objective of a nice synthesis of the best self-management methods and concepts, but probably more in phase with the project developments, given all the effort that was dedicated to the definition of use-cases and problems during year 1. The next version of this document, at the end of year 2, will provide a more synthetic view about the most appropriate algorithmic solutions, and about their influence on the definition of a UMF. An important element will be the identification of common features to all these methods: what kind of information is required from the managed network, what are the shapes of the main algorithmic solutions, how the feedback is performed, how results are displayed (human-machine interaction), stability and robustness issues, distributed vs. centralized solutions, etc.

The problems presented here cover a wide range of issues appearing all along the network management control loop, and address either the observation part (knowledge building, sensitivity to context), or the information dissemination aspects, or the decision functions, or cover issues of the full control loop. Not all use-cases have the same breadth, and within each one, the selected problems have different levels of maturity, scope and ambition. Some problems focus on well-known existing issues (for example on. congestion prediction and avoidance). Others have a broader scope (for example on proactive diagnosis and repair of network and service) for which off-the-shelf solutions do not exist, and thus requires rethinking how these issues must be addressed. Others again address fundamental issues that inevitably will appear in tomorrow’s networks (for example, the stability of large scale control loops, or the coexistence of multiple control loops with possibly conflicting objectives). This diversity is of course reflected by the document, and should be considered as instrumental, and not detrimental, to the synthesis work that will take place along the project.

The document is organized according with main sections corresponding to the identified use-cases of the project (see Deliverable D4.1), and subsections correspond to the identified management issues related to these use-cases. The follow-ups of this document will account for the progress made in solving each problem, will incorporate new problems that may emerge (see the use-case life-cycle), and will progress towards a more unified vision of self-management methodologies.

2 Problems in use case 1
Self-diagnosis and self-healing for IMS VoIP and VPN Services

2.1 Joint failure management in network and IMS services: a framework for active diagnosis

We consider here both a large-scale physical (wireline) network, capturing DSL subscribers, access and core networks, on top of which IMS services are deployed, typically VoIP. The objective is to develop methods to help diagnose malfunctions that can take the form of symptoms observed on the user side. Diagnosis here means isolating the root causes of symptoms, whether they are located in the service layer or in the physical layer. The existing management solutions handle separately the service layer, the access networks and the core network, which prevents a smart and automatic analysis of the network situation, and blocks any correlation of observed events in these domains. By contrast with most settings in this domain, we aim at active diagnosis procedures, which consist in questioning the network to collect the observations necessary to identify malfunctions, and possibly to run some probes that will help resolve conflicts between possible explanations.

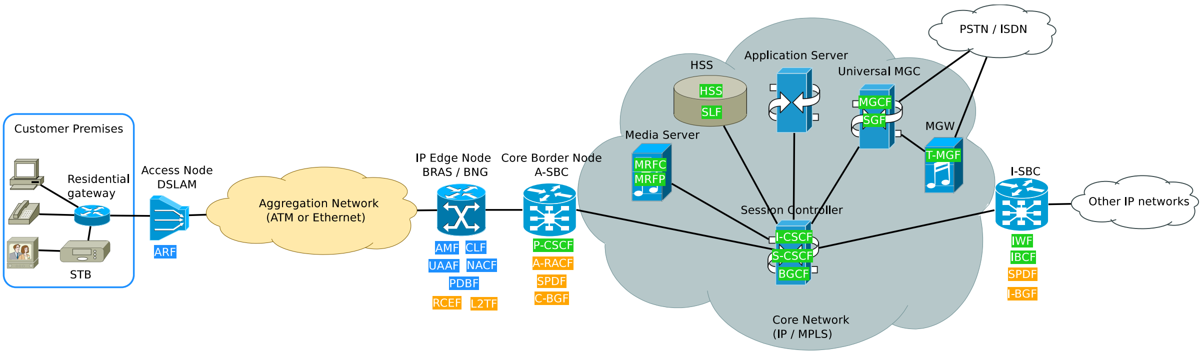

Fig.1 : Functions of the NASS are depicted in blue, those of the RACS in orange, and the functions of the core IMS are in green. Their communication links (at the functional level) are not represented for clarity

Beyond this objective of developing cross-layer, and possibly cross-domain, autonomic active diagnosis procedures, we further aim at providing a framework for proactive action. In particular, we aim at providing tools for estimating the impact on services of failures occurring at the physical level. For example, in order to determine the availability of some services in the network (e.g. the ability to make calls), the number of impacted users, etc. If some protection mechanisms are available in the network, this approach could also make a step towards self-healing procedures. For example by estimating how much service impact can be reduced by the various corrective actions that are possible.

2.2 Improvement of fault diagnosis based on the combination of Bayesian network and case-based reasoning

Fault diagnosis, a central aspect of network fault management, is a process of deducing the exact source of a failure from a set of observed failure indications.

In this context, we propose to design a method to optimize network and service diagnosis process by detecting, rapidly and with minimal human intervention, the source of an observed problem that occur at the service or network level, and avoiding detrimental effect(s) on other equipment of the infrastructure. The objective is also to reduce the complexity of the diagnosis process and analysis (as a function of the network "size"), and propose a generic approach that is not technology/service specific.

Instead of solving a problem when it occurs at the level of a device, it would be more appropriate to identify the source of the failure and solve the problem at the source so that this problem does not impact other network devices. Root cause analysis is a topic that has been considered previously but so far the problem still exists and new techniques to solve this problem efficiently are arguably needed.

In our idea, we are particularly focused on identifying the source of a fault by reducing the human intervention (avoid processing all the received alarms and avoid checking equipment per equipment), by reducing the time to complete the diagnosis process, and by reducing the complexity of the process (use of artificial intelligence and probabilistic techniques).

2.3 Vulnerability management in autonomic networks and services

[This problem is also related to UC2.]

Vulnerability awareness is a key challenge for increasing the security and safety of autonomic networks and services. When self-management related tasks are performed, the autonomic environment is modified in order to achieve specific objectives defined through high-level policies. However, these changes may lead the environment to potential vulnerable configurations and increase its exposure to risks. An autonomic network must be able to manage its own state and to perform the required activities to achieve safe configurations. If it is unable to support this capability, it will age with time, becoming more vulnerable, insecure and useless. In that context, we propose to support the self-configuration activities of autonomic networks with vulnerability management mechanisms. In particular, we consider that they should exploit the knowledge provided by configuration vulnerability repositories in order to detect and prevent vulnerable configurations. Strong standardization efforts have been done for uniformly describing vulnerabilities and exchanging related information. We argue in favour of using policy-based management methods and techniques for integrating these vulnerability descriptions into the management plane. For that purpose, we are formalizing how these descriptions can be mapped and translated into policy rules that can be directly interpreted by an autonomic configuration system. We are also developing and evaluating a first prototype based on the Cfengine configuration tool, which covers a subset of OVAL definitions and permits to generate vulnerability alerts during the self-configuration activity. As future work, we are interested in investigating further the treatments to be considered when a vulnerable configuration is observed, and also in increasing the coupling of our vulnerability management methods with the anomaly detection mechanisms developed by the University of Twente, in order to elaborate an integrated anomaly/vulnerability management strategy within the unified management framework.

2.4 QoS-based fault management in IP networks and IMS services: framework for active diagnosis and reasoning adjustment

In order to meet the objectives posed by the evolution of the networks and the services, the proposed solution is related to an event identification scheme; it moves towards two directions event identification on the one hand and adjustment of the reasoning scheme based on feedback from the previews decisions on the other. The framework could be applied both in core and access network simply by modifying the event identification component of the framework.

The developed scheme is applied in an IP network for IMS services. More specifically a QoS-based fault management framework in IP networks and IMS services is developed. The fault identification is based on network and service information whereas the evolution scheme aims at evolving the way a network element interprets its environment. The QoS degradation identification procedure is related to VoIP services; the solution concerns end-to-end QoS degradation diagnosis in a distributed scheme, where every network element in the session route identifies QoS issues in a specific link.

2.5 Autonomic management of intrusion detection systems

The proliferation of networks and services (heterogeneity of networks and increasing number of services, vulnerabilities), highlights the crucial role of assurance processes. Fault and Performance Management as defined before are critical functions towards ensuring the quality of the provisioned services or network capabilities, especially in an end-to-end way.

The goal of UC1 is to improve reactive management by reducing the delay between incident occurrence and detection reparation delay, and to enable a proactive management to prevent incident impact. In this context, we focus our attention to the problem of autonomic management of intrusion detection system in the core networks. We propose an autonomic approach to the problem or tuning the parameters of an intrusion detection system such that is behaviour is optimal according to a specific goal function.

2.6 Traffic trace analysis of free WiFi hotspots, as a preliminary to network optimization

A detailed analysis was performed of the traffic data traces from the free WiFi hotspot project "Île Sans Fil (ISF)" in Montreal, which are provided by Crawdad. These data reveal a very large variation of the amount and distribution of the traffic between different days and it seems that the network is most of the time only using a small amount of its actual capacity, because it is able to transport sometimes a much larger amount of data than in average.

These hotspot data allow to characterize user traffic behaviour and to derive useful information for realistic traffic models in heterogeneous mobile networks with small cells and with an increasing amount of data traffic. This leads to developing realistic assumptions about future networks, which are needed as an input for algorithms to optimize the network from a system performance and from an energy efficiency point of view.

2.7 Proactive diagnosis of congestion

A problem that Network Operators (NOs) need often enough to handle is congestion. NOs become aware of such situations only after the latter have occurred. Our proposal is to develop a mechanism according to which the network will be able to predict the possibility of congestion (how far from or close to congestion the link is or even if it is already congested). The application of the above mechanism is based on an unsupervised learning mechanism. The proposed learning procedure will take into account the traffic load of the area, the delays and the packet losses so as to train the system how to predict the possibility of congestion. Finally, the proactivity of the mechanism will enable the system to make decisions according to both NO's business goals and the predicted possibility of congestion so as to avoid congested links and enhance Quality of Experience (QoE) of the users.

3 Problems in use case 2 Networks' Stability and Performance

3.1 Controlling the stability of a complex network

Several trends are announcing that, in the next decade, future networks will become more and more ubiquitous and dynamic. Communications capabilities will be embedded in any device, object and things around the Users.

At the edges of the networks (i.e. in the access segment), nodes will create network of networks of heterogeneous and highly interconnected (real/virtual) entities (e.g. from sensors to smart things, from Users' devices to access/metro nodes). In this context, it is likely that we'll the emergence of dynamic games of (sub-) networks (belonging to the same, or different Operators), supporting any sort of services by using local processing and storage resources. This evolution will transform future networks (at the edges) into large-scale complex systems, characterized by the coexistence of dynamic games of various methods and systems.

This level of complexity will make networks design and management highly challenging: network should have capability to self-adapt and self-configure itself (with limited human intervention) to satisfy dynamically changing services demand.

This will imply the existence of multiple phases in network behaviours (i.e. identical local dynamic can give rise to widely different global dynamics) and state/phase transitions might occur (and maybe also due to self-organized criticalities).

In this evolution, it will be strategic for Network Operators to be able: 1) to validate (off-line, during planning) self-* features deployed into the network; 2) to monitor, predict and control (in-line during operations) the stability the stability of the network in its domains (Use-Case 2); 3) to actuate self-stabilization policies or human de-activation of self-* features (in case of persistent instabilities). This is the area of study of use-case 2.

3.2 Vulnerability management in autonomic networks

This work is a follow-up of the work related to vulnerability detection; both topics are jointly detailed in section 2.3.

4 Problems in use case 3 Dynamic virtualization and migration of contents and servers

4.1 Identification and acquisition of user, network and service context for dynamic migration of network entities

Presently most of the network/content/application service hosting and management is being concentrated at the core. As a result most of the user/control-plane traffic has to go through the core over the backbone and hence a lot of resources (bandwidth and processing wise) are consumed. This centralized organization of networks imposes serious operational and performance demerits, especially in case of mobile users using bandwidth intensive real time applications (such as streaming video content etc.). Because of mobility and variations in traffic patterns, such a centralized system poses several issues due to the constant re-routing of user data to its new point of attachment or resulting load imbalances. This would imply dynamic management of resources such as bi-directional tunnels maintained between the UE and the Core (more specifically the PDN-GW). Such a scenario thus imposes extra burden on the backbone and the access links and can significantly impact QoS delivery to mobile users. Besides, such a centralized approach increases the CAPEX/OPEX as the operator has to keep up with the total user demand to provide newer and better services.

To address this issue it is proposed to dynamically and autonomically migrate services/functions/resources, traditionally offered/accessed from the core, in the backhaul and access network by leveraging virtualization and cloud networking techniques and strategies. Such an approach would merit efficient and autonomic load balancing strategies to ensure continued dispensation of network services to the mobile users with the required QoS.

However, as a pre-requisite for achieving effective and efficient migration and balanced distribution of resources, it is imperative that high quality context information is made available and processed in a timely fashion that will dictate the decision logic to perform migration functions for achieving balanced distribution of resources.

Within the framework of this task group, we will jointly work with our partners towards developing sophisticated context correlation functions that will jointly take into account multiple context information, as opposed to relying on single context data, which will be utilized by the load balancing decision algorithms. Learning mechanism such as SOM or Fuzzy Logic will be considered to filter the various relevant context data and jointly process them in order to get some meaningful and actionable information.

NEC is closely collaborating with partners such as UPRC and UniS for developing effective context correlation functions that will then be used by NEC and partners like VTT, NKUA and UPRC in Task 3.2 developing load balancing strategies with reference to UC3 objectives. It may be noted that the proposed work will be carried out with reference to the Context Management framework proposed in WP2 as part of UMF and will also be available to other tasks and task forces for achieving their respective objectives.

4.2 Optimization of context acquisition and dissemination using a distributed data mining framework

One of the most challenging tasks of network management is to reduce the huge amount of network data while also to exploit the subject context, comprised on this volume. For this reason, modern network management approaches shall be fuelled with a variety of sophisticated techniques such as machine learning and data mining. To this end, this contribution shall focus on the “Optimization of Context Acquisition and Dissemination using a Distributed Data Mining Framework”, addressing the problems identified in Use Case 3 (Dynamic Virtualization and Migration of Contents and Servers).

The context acquisition and dissemination mechanism is formalized based on a data pre-processing and data-mining framework using transformation and clustering techniques. The former techniques are based on mathematical dimensionality models while the latter on a minimum distance grouping of data records. The challenge of this work is to apply this framework in a distributed way such that each network element should be able to extract context and deliver it to the neighbouring devices with the most resource efficient way. Such problem is also related with QoS degradation mechanism based on Fuzzy Logic, which is part of Use Case 1, since the correlations identified by the proposed clustering mechanism can be used as enablers for machine learning event identification mechanisms.

In order to realize the importance of such a mechanism, it would be valuable to mention the major advantages of its application on modern network systems. First of all, it can achieve significant information reduction, since massive raw data is translated to context while the requested bandwidth resources for the exchanged context are minimized. Secondly, there is an important processing gain at each network element because context requires fewer CPU, Memory, Disk and battery/energy usage comparing to the initial dataset. Finally, since this mechanism is fully distributed, it could collect and exploit the context of many network elements, either in a local environment or globally; thus it can be further elaborated by more advanced Learning techniques, in order to enable Self-X capabilities.

4.3 Resource and service discovery and rule-based reasoning from contextual data

The reference problem of resource, service and context discovery in use case 3 is that how the (User, network, environment, resource, service) context can be discovered, based on the data collected from different sources within the system. Data can be collected by discovery protocols, sensors, monitoring probes, statistics, or measured metrics of the system.

Knowledge is being developed through different sources. The network domain is a collection of resources and services interacting with each other. Discovering available resources and services within the network can be achieved by appropriate discovery protocols. Resources include nodes (and their capabilities, including memory, processor, clock speed, etc.) and links (specified by their properties such as capacity, BER, etc.). Services include Operator provided services (such as telecomm and internet access services), those offered by Service Providers (Content, web services) and corporate/local services (e.g. printers, FAX machines, etc.).

Beside knowledge on the ***entities*** of the network (resources and services), the ***status*** of the network resources and services contributes to the development of the knowledge. The status of the resources and services, added to the status of users and environment, is classified as ***context***.

Within UniverSelf, we focus on two major problems and propose solutions for them:

- Resource and service discovery, through service discovery protocols
- Rule-based reasoning from contextual data

5 Problems in use case 4 SON and SON collaboration according to operator policies

5.1 Robust learning using policy gradient reinforcement learning

UC4 has identified three key research axes for future evolutions of SON enabled radio access networks:

1. Design of novel SON functionalities for future radio access networks (such as SON in LTE-Advanced HetNets or home networks, coverage capacity optimization, or network topology control),
2. Design solutions for coordinated operation of SON functionalities,
3. Integrate SON operation in a Unified Management Framework developed in the UniverSelf project

Self-optimizing functionality is a control function or control loop that maps the system state into actions. In the learning vocabulary, a state to action mapping can be viewed as a rule, and the set of rules constitute a controller. The controller should allow to autonomously adapting the network to variations in traffic or in propagation conditions. Designing (near) optimal rules can be done using a learning process that is a part of the self-optimizing functionality, e.g. Reinforcement Learning. In the learning (or exploration) phase, new actions are tested which may temporarily deteriorate the network performance or the perceived quality of service (QoS).

According to the UMF requirements, the self-optimization process should be *scalable* (i.e. the self-optimization process should operate in a large scale deployment of the SUN functionality in network nodes); *stable* (i.e. a system is considered as unstable if certain quality indicators vary strongly as a result of parameter modifications of the self-optimizing functionality) and *robust* (i.e. a learning process is robust if during the learning phase, performance/QoS degradation is limited to a pre-defined threshold).

The purpose of this contribution is to adapt a robust learning solution, namely the Policy Gradient Reinforcement Learning to a SON use case of a heterogeneous LTE-Advanced network with eNode B and relay stations. The learning algorithm aims at optimizing resource allocation between to the backhaul link and to the direct station (eNode B and relay) to mobile links in order to increase the network capacity while minimizing performance deterioration during the learning phase.

5.2 Observation and action in orchestration of SON LTE control loops

UniverSelf Use Case 4 studies interaction of SON LTE use cases (3GPP) in the attempt to orchestrate their co-existing control loops in a conflict-free manner, so that the optimization of different LTE parameters performed by the respective control loops is mutually beneficial. The main finding of this section is: contrary to a conventional opinion potentially conflicting mechanisms can be orchestrated to operate not only in a conflict free manner, but even provide mutual benefits. In the studied case of two control loops the required orchestration is facilitated by a hierarchical relation between the two and by creation of two dynamic and disjoint policy domains.

5.3 Optimization of femtocell networks using fuzzy logic assisted reinforcement learning

With the ever-increasing data traffic demand in today's mobile networks, the operators seek immediate solutions for capacity improvement. With up to 80 per cent of the traffic being originated from the indoor where the current mobile networks are least effective due to high penetration losses of buildings, indoor data offloading has become a focus of the industry in the recent years. Femtocells are low-power, short-range data access points that can provide improved indoor coverage and increased throughput to home users while offloading traffic from expensive macro radio access networks on to the low-cost public Internet. While deployment of femtocell base-stations can provide significant capacity improvement due to the increased spatial re-use, interference is considered to be a significant issue to be considered. Considering most femtocell base-stations being equipped with simple omni-directional antennas, an effective way to control the interference is through optimization of the transmission power. This is a two-dimensional optimization task where from one hand the femtocell base-station needs to allocate an optimized portion of its total transmission budget for the pilot channel and from the other hand the transmission power is to be optimally set. This problem is related to the radio network optimization (UC4) and is in fact an optimization task with contradicting objectives. The proposed solution to mitigate the interference in femtocell networks in a distributed fashion consists of using reinforcement learning combined with fuzzy logic such that to prevent the curse of dimensionality problem of the classical reinforcement learning solutions.

6 Problems in use case 6 Deployment of new services and accommodation of new traffic on heterogeneous networks

Note: The use case 5 and use case 6 have been merged in July 2011. The use case numbering has been kept unchanged and the content of use case 5 has been progressively incorporated in the definition of the use case 6.

6.1 A fuzzy reinforcement learning approach to pre-congestion notification (PCN) - based admission control

The dynamicity of future Internet networks, where applications with different service requirements can appear, makes Quality of Service (QoS) provisioning and service continuity a challenging issue. Traditional traffic engineering approaches, usually based on offline optimizations (bandwidth provisioning), may not be able to address this efficiently. Towards this end, dynamic service management functions such as admission control can play a significant role with respect to supporting QoS for application flows during the service delivery time, helping to overcome the inability of slow-changing network configurations to react rapidly enough to load fluctuations in order to prevent QoS degradation. Such functions can be therefore seen as means of dynamic corrective actions aiming to guarantee QoS at time scales significantly shorter than the time scales of traffic engineering optimizations. Admission control in particular attempts to guarantee QoS at time scales comparable and shorter than the duration of individual application flows.

Even though admission control is a well-studied subject, most of the existing schemes suffer from the fact that they are based on some very rigid assumptions about the per-flow and aggregate underlying traffic models and network characteristics. They require, therefore, manual configuration of some tuning parameters to perform well in the intended conditions and manual reconfiguration of their tuning parameters in a “trial and error” fashion as soon as these original assumptions stop being valid, in order to keep performing well. The idea of mechanisms able to self-adapt as the flow and network conditions change has been around for quite some time under the generic term *autonomic management* and towards this end in this work we propose a novel, autonomic admission control scheme based on the increasingly popular Pre-Congestion Notification (PCN) framework put forward to the IETF.

PCN, which targets core/fixed network segments, defines a new traffic class that receives preferred treatment by PCN-enabled nodes, similar to the expedited and assured forwarding per-hop behaviours in Differentiated Services. PCN assumes that some signalling protocol (e.g. RSVP or SIP) requests admission for a new flow and supports two distinct mechanisms; admission control (AC) and flow termination (FT). AC is a control function that decides on whether new flow requests should be admitted or rejected based on the current network conditions. FT is a control function that tears down already admitted flows in case of overload that can occur, in spite of AC, due to rerouted traffic in case of link failures and other unexpected events.

Our approach employs fuzzy logic and reinforcement learning in order to improve the original PCN AC mechanism. The aim is to induce autonomic behaviour in order to minimize the need for manual reconfigurations, as well as to enhance the robustness and adaptability of the mechanism to changing flow and network conditions.

6.2 Bandwidth estimation

Even for a single Internet application, the number, types, locations, and usage patterns of devices, as well as the condition of the communication environment, and traffic characteristics may dynamically change considerably every moment. In such an environment, a network would often face unexpected or unpredictable user behaviour, usage of network, and traffic patterns, which were not anticipated at the time the network was designed or built.

The so-called “Network Morphing” consists in the capability of dynamically reconfiguring the network when networking conditions change, while constantly optimizing network resources, in response to unexpected changes in traffic demand or on the detection of degraded performance, such as the current configuration is far away from the “ideal” configuration.

Bandwidth estimation, in particular for the purpose of link dimensioning and network configuration, plays an important role in Network Morphing. Usually, network operators make manual provisioning decisions based on empirical rules and on rough traffic measurements. The goal of this activity is to identify and validate suitable methods to achieve an autonomic and efficient estimation of bandwidth requirements in high-speed networks.

7 Problems in use case 7 Network and service governance for IPTV over fixed and mobile networks

7.1 Providing FTTH network elements with self-* feature

FTTH rollout is today one of the main drivers of telecom business transformation, encompassing high investments in equipment and systems. In traditional copper-based DSL services, the network structure was relatively simple, with a relation one-to-one between the ports at the Central Office (CO) and at the customer premises. But Passive Optical Network (PON) has a tree layout, with different levels of splitting. Failures in the branches of this tree cannot be located easily even with sophisticated optical testing techniques, such as reflectometric procedures. In addition, new equipment is located on both sides (OLT at Central Office, ONTs, routers, set top boxes or IP phones at home).

These devices provide useful information, of heterogeneous nature and format, through different interfaces and using a variety of protocols, information that need to be evaluated in order to find the root cause of a failure. We aim to research a service assurance solution for FTTH environments, providing the network elements with self-monitoring, self-diagnosis and self-healing possibilities. These functionalities will enable the early detection and resolution of network, QoS, and QoE problems with limited or no customer impact.

Traditional telecom networks management relied on big inventory systems where all the network elements were stored, and on the assumption that the state of every entity was precisely known at any instant. Classical Operating Support Systems were therefore built as large centralized systems, able to deal with huge amounts of information and find the root cause of failure, but unable to provide a solution when only partial data were available.

Today the introduction of new technologies and the popularity of broadband-based services have produced an important growth in the number of managed entities, which complicates the labour of centralized solutions. Topology and inventory data are scattered among multiple systems and it is not always complete neither consistent. The complexity of the network environment makes very difficult to observe certain aspects of the domain, and moreover, the relationships between domain events are not always deterministic. Besides, it is often impractical to model and analyse explicitly all the dependencies.

The explosion of new devices makes it difficult the gathering of all the needed monitoring information, and when it is feasible to get it, sometimes is inaccurate or vague. Even more, due to efficiency reasons it may be convenient to collect only a subset of the raw data, from which the state of the network and the service need to be extracted. Therefore, uncertainty in data has become a main source of problems for network operators.

Our approach, based on Bayesian Networks for the diagnosis of failures, and Belief-Desire-Intention model for the decisions that supports self-healing processes, aims to build a solution for the automatic diagnosis and healing procedures in FTTH deployments.

8 Conclusion

This document has presented a first set of concrete management problems that need to be made autonomic in order to empower future networks and services, and has presented the research directions that are currently followed to solve them. They will form the solid ground on which the central concepts of a Unified Management Framework (UMF) will be tested and validated. According to the life cycle of the use cases, these problems will now be addressed and solved individually, and it is expected that some of them will quickly lead to prototypes and demonstrations for validation. In any case, all problems mentioned in this document will be confronted against the already proposed concepts of the UMF, and reversely they will challenge the definition of the UMF, as the adequate framework where all these management algorithms can be embedded.

This document will evolve along the project. Future versions will account for the progress made on the resolution of the selected problems, and will present as well new problems that may appear in relation to the use-cases of the project. The relations of the selected problems and their solutions to the UMF will be enhanced, in order to progress towards a unified vision of the central concepts of self-management methods.

Acronyms

A	Authorisation (Policy)
AC	Admission Control
ADSL	Asymmetric Digital Subscriber Line
AR	Admissible Rate
BDI	Belief-Desire-Intention
BMU	Best Matching Unit
BN	Bayesian Network
BS	Base Station
CB	Context Broker
CBR	Case-Based Reasoning
CDF	Cumulative Distribution Function
CC	Context Client
CLE	Congestion Level Estimate
CMF	Context Management Framework
CMI	Context Management Infrastructure
CO	Central Office
CP	Context Provider
CPr	Context Profile
CS	Context Source
DAG	Directed Acyclic Graph
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
FQL	Fuzzy Q-Learning
FT	Flow Termination
FTTH	Fiber To The Home
HetNet	Heterogeneous Network
HO	Handover
IDS	Intrusion Detection System
IMS	IP Multimedia Subsystem
IPTV	Internet Protocol television
KPI	Key Performance Indicator
LB	Load balancing
LTE	Long Term Evolution
MF	Member Function
MRO	Mobility Robustness Optimization
MT	Mobile Terminal
NASS	Network Attachment Sub-System
NO	Network Operator
O	Obligation (Policy)
OLT	Optical Line Termination
ONT	Optical Network Terminal

OPEX	Operational Expenditure
OSS	Operations Support Systems
OWL	Web Ontology Language
P-CSCF	Proxy Call Session Control Function
PAN	Personal Area Network
PCN	Pre-Congestion Notification
PLGSOM	ParameterLess Growing Self-Organizing Maps
PLR	Packet Loss Rate
PON	Passive Optical Network
QoE	Quality of Experience
QoS	Quality of Service
OVAL	Open Vulnerability and Assessment Language
RACH	Random Access CHannel
RACS	Resource and Admission Control Sub-System
RDF	Resource Description Framework
RL	Reinforcement Learning
RS	Relay Station
RSSI	Received Signal Strength Indication
RSVP	Resource Reservation Protocol
SAP	Situation Awareness Pyramid
SINR	Signal to Interference plus Noise Ratio
SIP	Session Initiation Protocol
SLP	Service Location Protocol
SOM	Self-Organizing Map
SON	Self-Organizing Network
SR	Supportable Rate
SWRL	Semantic Web Rule Language
TD	Temporal Difference
TTT	Time to Trigger
UE	User Equipment
UMF	Unified Management Framework
VDSL	Very high bitrate Digital Subscriber Line
VoIP	Voice over IP

Definitions

Algorithm – *A concrete step-by-step procedure for calculation. It is an effective method expressed as a finite list of well-defined instructions for calculating a function. Algorithms are used for calculation, data management, and automated reasoning.*

Capability – *The ability to perform actions. It is the sum of know-how and capacity.*

Governance – *A high level mechanism which involves all functionalities necessary to address the gap between high-level specification of human operators' objectives and existing resource management infrastructures towards the achievement of global goals. It relates to decisions that define network expectations, grant control, or verify performance. It consists of either a separate process or part of management processes. These processes and systems are typically administered by a governing function.*

Method – *A general procedure for solving a problem. It is a series of steps or acts for performing a function.*

Model – *A system and/or a representation of postulates, data, behaviour, and inferences presented as a description of an entity or state of affairs. An example of an optimization with a model would be the optimization of the channel capacity in a wireless access network by changing the transmission power of the base station. The Shannon-Hartley theorem tells us that the increase of channel capacity monotonically increases with increasing total received signal power over the bandwidth; and the total received signal power is directly related to the transmission power. Hence the model tells us that if we increase the transmission power of the base station, the channel capacity can be assumed to increase. In this case the model is reflected in a formula, namely the Shannon-Hartley theorem. Furthermore, thanks to the autonomic increase, the described problem also belongs to the class of convex optimization problems where solutions can be found in a straightforward way without getting trapped in local optima. For the class of non-convex optimization problems with models, however, the situation is slightly more complex as there need to be ways to avoid local optima, but the model can still be used to check new parameter configurations before they are actually tried in the network.*

Network empowerment – *Embedded network ability and authority to access and manage information, resources for decision-making and execution elements for changes of network behaviour. It is an approach where management and control functions are distributed and located in or close to the managed network and service elements. The potential benefits are the inherent support for self-management features, higher automation and autonomicity capabilities, easier use of management tools and empowering the network with inbuilt cognition and intelligence. Additional benefits include reduction and optimization in the amount of external management interactions, which is key to the minimization of manual interaction and the sustaining of manageability of large networked systems and moving from a managed object paradigm to one of management by objective.*

Self-optimization – *Selection and adjusting best (network and/or service parameters or behaviours from some set of available alternatives and/or minimize or maximize a utility function by systematically choosing the values of the parameters from within an allowed set in an autonomous way. Self-Optimization is a process in which the system's settings are autonomously and continuously adapted to the traffic profile and the network environment in terms of topology, propagation and interference. Together with Self-Planning and Self-Healing, Self-Optimization is one of the key pillars of the Self-Organizing Networks (SON) management paradigm.*

Management Tool – *Means to produce a management function or to achieve a management task, but that is not consumed in the process. Informally the word is also used to describe a management procedure or process with a specific purpose.*

Use case – *A descriptor of a set of precise problems to be solved. It describes steps and actions between stakeholders and/or actors and a system, which leads the user towards an added value or a useful goal. A use case describes what the system shall do for the actor and/or stakeholder to achieve a particular goal. Use-cases are a system modelling technique that helps developers determine which features to implement and how to gracefully resolve errors.*