SEVENTH FRAMEWORK PROGRAMME
THEME ICT-1-1.1
"Network of the future"

Project acronym: EFIPSANS

Project full title: Exposing the Features in IP version Six protocols that can be exploited/extended for the purposes of designing/building Autonomic Networks and Services

Proposal/Contract no.: INFSO-ICT-215549

Appendix to D3.2: "Advanced Network Services in Autonomic IPv6 Networking: Performance Analysis and Evaluation"

Project Document Number: EFIPSANS/D3.2_Appendix I CO[1] v1.0
Project Document Date: 31/12/2009
Workpackage Contributing to the Project Document: WP3
Deliverable Type and Security: PU
Editors: Symeon Papavassiliou (ICCS) and Timotheos Kastrinogiannis (ICCS)

Abstract: This document serves as a supplement to Deliverable D3.2 by providing a brief description and status of the autonomic emerging architectures within WP3. A detailed evaluation of the integrated architectures and corresponding features will be included in D3.6 (M30).

Keywords: Advanced Network Services, Autonomics, GANA, EFIPSANS, performance evaluation.

[1] Security Class: PU- Public, PP – Restricted to other programme participants (including the Commission), RE – Restricted to a group defined by the consortium (including the Commission), CO – Confidential, only for members of the consortium (including the Commission)

Project Number	**INFSO-ICT-215549**
Project Name	**E**xposing the **F**eatures in **IP** version **S**ix protocols that can be exploited/extended for the purposes of designing/building **A**utonomic **N**etworks and **S**ervices
Document Number	**INFSO-ICT-215549**/WP3/D.3.2_Appendix I v0.1
Document Title	Appendix to D3.2: "Advanced Network Services in Autonomic IPv6 Networking: Performance Analysis and Evaluation"
Workpackage	WP3
Editors	Symeon Papavassiliou (ICCS) Timotheos Kastrinogiannis (ICCS)
Authors	Symeon Papavassiliou (ICCS) Timotheos Kastrinogiannis (ICCS) Juan M. González (TID) Zhaojun (Alice) Li (FLE) Ranganai Chaparadza (Fraunhofer FOKUS) Petre Razvan (Fraunhofer FOKUS) Nikolay Tcholtchev (Fraunhofer FOKUS) Michal Wodczak (TARC-PL) Grzeda, Monika(TARC-PL) Yuhong Li (BUPT) Sheila Becker (UL) Thorsten Ries (UL) Xiangyang Gong (BUPT) Yan Shi (BUPT) Xin Li (BUPT) Wang Wendong (BUPT) John Ronan (TSSG) Tasos Zafeiropoulos (GRNET) Athanassios Liakopoulos (GRNET) Vassilios Kaldanis (Velti) Rolland Vida (BME) Gabor Vincze (BME) Bruno Vidalenc (ALF) Pierre Peloso (ALF) Giorgos Aristomenopoulos (ICCS) Eirini –Eleni Tsiropoulou (ICCS)
Reviewers	John Ronan (TSSG) Symeon Papavassiliou (ICCS) Maria Striki (TARC-USA)
Contractual delivery date	31st December 2009
Delivery Date	31st December 2009
Version	1.0

Copyright

Contact authors: Symeon Papavassiliou (papavass@mail.ntua.gr), Timotheos Kastrinogiannis (timothe@netmode.ntua.gr)

APPENDIX I: TOWARDS INTRODUCING AUTONOMIC-FLAVOURED IPV6 ENABLED ARCHITECTURES

A. Autonomic QoS Managements in over Wired Core Environment

Due to the heterogeneous environment and diverse services and applications today, it is difficult to guarantee the satisfaction of various services' QoS requirements. With the dramatically changing environment, the human input is often required when aiming at efficient QoS support, which increases significantly the cost and the complexity of management and configuration. DiffServ is considered the preferred way of implementing QoS in the Internet, but it is still hard to provide satisfactory quality of service. In recent years, the concept of autonomicity has been proposed in the autonomic computing and autonomic communications to solve the complexity issues of the management and reduce the manual intervention. As a consequence there is lack of adaptability to the changing environment, and therefore, autonomicity is envisioned as an enabler to address these issues. Within the framework of EFIPSANS we propose a novel architecture for QoS management in wired core networks on the basis of traditional Diffserv QoS architecture, which is shown in detail in section 2.2.1 of [D3.2].

The architecture is characterised by several QoS-aware autonomic functions and mechanisms in IPv6 networks, through which we aim at introducing several autonomic attributes, such as self-optimisation, self-configuration, self-organisation, and self-adaptation. In addition, the proposed architecture takes advantage of effective service-aware functions to improve the autonomic service control. The main objective of this novel architecture is to enable the QoS management systems in wired core networks to automatically adapt to the changing context, optimise network resources management, thus improving users' QoS experience and reducing the manual intervention.

At the network level, NET_LEVEL_QoS_M_DE is the (optimisation) decision maker which collects QoS requirements and performance parameters from users and the network, analyses them, and makes decisions according to certain policies. Self-adaptation could be achieved by enabling autonomic nodes to select proper mechanisms for each type (or functionality) and thus, by efficiently aggregating protocol level DEs together to achieve a suitable QoS function in an autonomic node. Protocol level DEs automatically adjust appropriate mechanisms and parameters adapting to the changing context in order to achieve better performance. With all the functionalities that the various DEs do together, the architecture could finally achieve the autonomic functionalities.

B. Autonomic Mobility and QoS Management over a Heterogeneous wireless environment

Introduction

Among the core problems that has been extensively investigated within the context of EFIPSANS is the following.

The problem of seamless mobility and proficient joint radio resource management in an all-IP internetworked WLAN/Cellular (CDMA, OFDMA) heterogeneous wireless environment

Towards addressing this issue of high importance, both from academic and industrial point of view, within the framework of EFIPSANS GANA architecture, the autonomicity of nodes/networks has been envisioned as the enabler to devise a QoS-centric architecture for supporting various services within the broadband wireless networks. Moreover, resource allocation within the interworking environment has been investigated, taking into account the access networks' diverse characteristics, vertical handoff, user mobility, and service types, via introducing a distributed node-networks assignment mechanism aiming at QoS provisioning and efficient resource utilisation.

The proposed autonomic mobility and QoS management architecture for heterogeneous wireless networks is a collaborative work among Task3.1 and Task3.2 in WP3 and involves several research topics addressed and presented respectively in deliverable [D3.2].The various individual novel autonomic functionalities concerning either autonomic mobility or autonomic QoS and resource allocation functionalities that have been developed in the project have all been guided and steered by three common principles:

- GANA architecture,
- 3GPP LTE/SAE architectures and their key drivers towards enabling "Self-Organising / Self-Optimising Network", i.e. SON functionalities,
- Generic design principles of the overall envisioned autonomic architecture (reported in [D3.1, Chapter 6] and in M3.2).

Therefore, complementary autonomic sub-architectures have already been developed, the integration of which will lead us to our ultimate goal of an **"Autonomic Mobility and QoS Management over a Heterogeneous Wireless Environment in line with 3GPP/LTE".** This section serves the purpose of outlining our overall achievements towards the previous directions and thus, reveals our methodology towards unifying the various developed autonomic mechanisms. Specifically, the following issues will be addressed: a) motivations and architecture's goals identification, b) initial description and justifications of the overall architecture and the introduced novelties, c) description of the sub-architectures that will be integrated, d) our integration approach (both at theoretic/conceptual level and DEs level) and the integrated Function Level DEs. The outcome of this work will be extensively presented in D3.6 while remaining open problems and future steps are reported in M3.4.

The Vision of 3GPP & Autonomicity

Reduction of operational efforts and complexity are key drivers for 3GPP LTE. One of the important ways towards minimising operational efforts is to introduce SON mechanisms (Self-Organising / Self-Optimising Network). Automation of some network planning, configuration and optimisation processes via the use of SON functions can help the network operator reduce OPEX by reducing manual involvement, as well as increase network performance and quality reacting to dynamic processes in the network. Several SON use cases have been captured in 3GPP, TR36.902.

Among these use cases, **Mobility Load Balancing Optimisation** is closely related to our work in both Task3.1 and Task3.2. The objectives of Mobility Load Balancing Optimisation include:

- Optimisation of cell reselection/handover parameters to cope with the unequal traffic load and minimise the number of handovers and redirections needed to achieve the load balancing.
- Self-optimisation of the intra-LTE and inter-RAT mobility parameters to the current load in the cell and in the adjacent cells can improve the system capacity and can minimise human intervention in the network management and optimisation tasks.

In accordance with the previous analysis, what is currently missing is (are) the algorithm(s) or mechanism(s) that will determine how to distribute the UEs camping and/or delay or advance handing over the UEs between cells and thus, to balance the traffic load between cells. Our research aims at filling these gaps.

Motivation & Key Novelties

The integration of broadband Wireless Local Area Networks (WLANs) and cellular networks (i.e. Code Division Multiple Access (CDMA) or Orthogonal Frequency-Division Multiplexing (OFDM)) has recently attracted significant attention as a promising direction to facilitate and realise seamless broadband Internet access for mobile users with multimode access capabilities. However, when aiming at satisfying various QoS constraints within the integrated system, separate and independent studies on optimal resource allocation and QoS provisioning in either cellular networks only or WLANs only, may prove inadequate. Our approach tries to overcome such inefficiency via exploiting in a fully integrated manner (i.e. common resource management) both types of access technologies advantages.

Moreover, due to the heterogeneity of the wireless environment, in most cases only the mobile node has the complete view of its own environment, in terms of available access networks in its locality, the corresponding available resources and QoS support mechanisms. This becomes even more critical when the available networks belong to different operators. Therefore, contrary to traditional architectures where network/nodes' performance is controlled in a centralised way, future wireless networking envisions as its foundation element an autonomic self-optimised wireless node with enhanced capabilities in terms of acting/re-acting to mobility, connectivity or even QoS- performance related events. Such a vision and evolution, makes the design of a flexible autonomic user-centric mobility and QoS-aware joint network selection mechanism, a promising alternative service oriented paradigm that allows to fully exploiting the proliferation of wireless networks, as opposed to the more conventional existing access oriented designs.

With respect to the previous discussions, within the framework of EFIPSANS we have envisioned and designed an autonomic seamless mobility and QoS-aware joint resource allocation architecture for integrated WLAN/CDMA-cellular systems that aims at maximising the overall integrated network's revenue, while enabling users to efficiently self-adapt at the event of QoS-triggered occurrences towards self-optimising their services' performance. The distinct novel features of the proposed architecture are summarised as follows:

- Autonomic mobility management in tune with current 3GPP/SAE interworking vision. MIPv6 and PMIPv6 are the key protocols of the proposed architecture.
- Optimal utility-based resource allocation and QoS provisioning within each system's cell (WLAN or CDMA (currently expending our approach to OFDMA)). Thus, an Autonomic Radio Recourse Management (ARRM) mechanism is introduced to achieve the above goal.
- Efficient joint resource management via a flexible network selection mechanism, which determines whether or not to admit and to which network cell (WLAN or CDMA network) a new or vertical/horizontal handoff service arrival. Towards enabling that, an Autonomic JOint Network Selection (AJONS) decentralised mechanism is introduced.

An Overview of the Complementary Sub-Architectures

Figure 1 illustrates an overview of the proposed architecture from an autonomic mobile node's point of view, in terms of introduced DEs in various levels of GANA's hierarchy as well as their main interactions. Initially, the two main autonomic sub-architectures that constitute the overall architecture can be observed: namely, autonomic mobility management (green) and autonomic resource allocation and QoS provisioning (black) architectures. Key components of these architectures are their corresponding function level DE (i.e., FUNC_LEVEL_MM_DE and FUNC_LEVEL_QoS_M_DE) that are responsible for steering all the mobility and QoS related functionalities either of the autonomic mobile nodes or the autonomic base stations/access points. Their communication and collaboration allows us to exploit information from mobility related protocols (e.g., events and measurements) in order to enhance the performance of resource allocation related protocols and vice versa. Thus, towards achieving their goals they are steering their

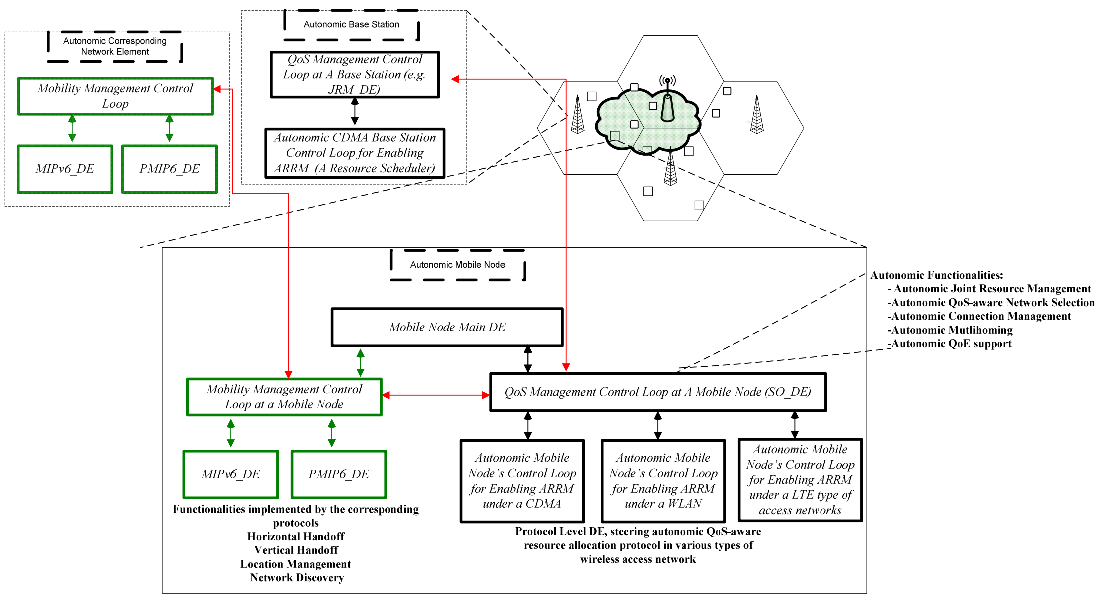

Figure 1. Autonomic Mobility & QoS Management with Control Loops over a Heterogeneous Wireless Environment

corresponding managed entities (i.e. protocol level DEs) and harmonise their operation i.e., PROTO_LEVEL_MIP6_DE and PROTO_LEVEL_PMIP6_DE in the case of FUNC_LEVEL_MM_DE and PROTO_LEVEL_NODE_R&Q_WLAN_DE, _AP_R&Q_WLAN_DE, _NODE_R&Q_CDMA_DE and PROTO_LEVEL_BS_R&Q_CDMA_DE, in the case of FUNC_LEVEL_QoS_M _DE. Each one of the latter DEs introduces autonomic attributes into specific parts of the overall architecture like autonomic resource allocation in CDMA type of networks or Proxy MIPv6 protocol. Finally, these two vital function level DEs are complying their operation in accordance to policies (e.g., imposed by network operations) via their communication and collaboration with corresponding introduced network level DEs (i.e., NET_LEVEL_MOM_DE and NET_LEVEL_QoS_M_DE). Table 1 summarises all the DEs that participate in the proposed architecture. Moreover, for each DE a pointer to the corresponding sections of this deliverable that analyse its operation, its control loop as well as an analytical (theoretic) justification of its operation is provided (last column). Moreover, detailed tables analyzing the operation of these DEs can be found in D1.5. It should be noted here that a detailed description of the communication and co-operation of the various involved DEs will be provided in [D3.6] (M30).

Table 1. DEs Related to the Autonomic Mobility & QoS Management Architecture

GANA-aware Decision Elements of the Autonomic Mobility & QoS Management Architecture		
DE's Acronym	**DE's Name**	**Task / Section in D3.2**
Mobility Related Functionalities		
NET_LEVEL_MOM_DE	Network-Level-Mobility-Management Decision-Element	Task3.1/ 3.2
FUNC_LEVEL_MM_DE	Function-Level-Mobility-Management Decision-Element (at the mobile node)	Task3.1/ 3.2
PROTO_LEVEL_MIP6_DE	Protocol-Level-Mobile-IPv6 Decision-Element (at the mobile node)	Task3.1/ 3.2.1
PROTO_LEVEL_PMIP6_DE	Protocol-Level-Network-Based-Mobility-Management Decision-Element	Task3.1/ 3.2.2
QoS and Resource Allocation Related Functionalities		
NET_LEVEL_QoS_M_DE	Network-Level-Quality-Of-Service-Management - (Wireless-Network) Decision-Element	Task3.2 / 2.3.1
FUNC_LEVEL_QoS_M_DE	Function-Level Quality-Of-Service Management (Wireless) (at the mobile node)	Task3.2 / 3.3.1, 2.3.3, 2.4
PROTO_LEVEL_NODE_R&Q_WLAN_DE	Protocol-Level Node's-Resource-Allocation-And-Quality-Of-Service-Management-In-WLAN-Networks Decision-Element	Task3.2 / 2.3.1
PROTO_LEVEL_AP_R&Q_WLAN_DE,	Protocol-Level Access-Point-Resource-Allocation-And-Quality-Of-Service-Management-In-WLAN-Networks Decision-Element	Task3.2 / 2.3.1
PROTO_LEVEL_NODE_R&Q_CDMA_DE	Protocol-Level Node's-Resource-Allocation-And-Quality-Of-service-Management-In-CDMA-Cellular-Networks Decision-Element	Task3.2 / 2.3.2
PROTO_LEVEL_BS_R&Q_CDMA_DE	**Protocol-Level-Base-Station-(eNodeB)-Resource-Allocation-And-Quality-Of-Service-Management-In-CDMA-Cellular-Networks Decision-Element**	Task3.2 / 2.3.2

- ***Key Novelties and Designing Principles of the proposed Autonomic Mobility Management Architecture***

Compared with traditional mobility management mechanisms in homogeneous networks, there are several additional challenges in designing mobility management systems for heterogeneous networks, such as the handoff decision making among access points of multiple technologies, and the execution of handoff methods that depend on context, though not all methods apply in every scenario. By means of control loops that steer and manage to date IP enabled mobility protocols, a flexible autonomic architecture has be devised which adds flexibility and adaptability to the mobility management system. EFIPSANS autonomic solution is enabled by two control loops residing at the mobile nodes and network nodes respectively. As illustrated in Figure 2, the Mobility Management (FUNC_LEVEL_MM_DE) control loop at a mobile node controls a mobile node's mobility related behaviours, while the one at a network node manages the mobility management at network level.

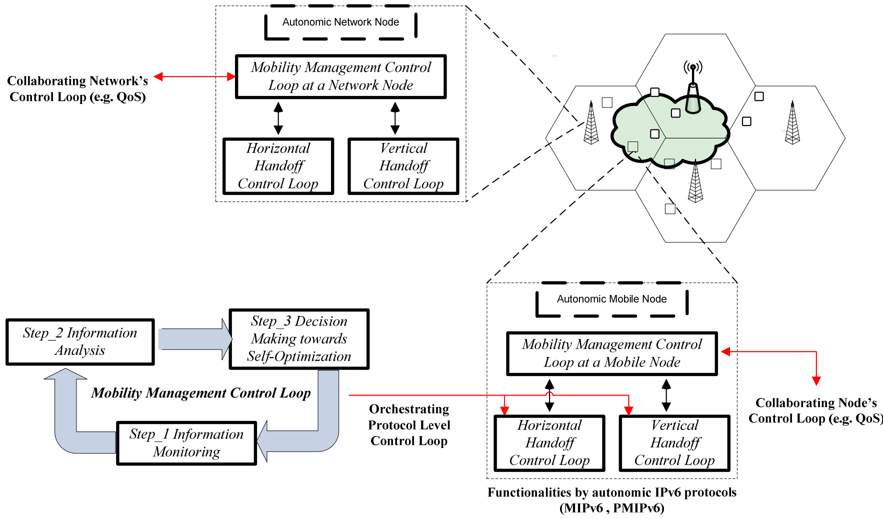

Figure 2. Autonomic Mobility Management with Control Loops

In general, a mobility management control loop consists of three basic steps based on the autonomicity requirements.

Mobility Management Control Loop

Step_1: Information Monitoring

For a network node, it needs the knowledge of its own components, current status, and ultimate capacity, as well as the possible connections with other systems (for example to discover neighbors as potential "target base station" in the case of handoff).

For a mobile node, it needs the knowledge of its own capability and of this of the network, such as if it has multiple interfaces and if the multiple interfaces can be used simultaneously, as well as the supported mobility management protocols. It constantly monitors the status of the wireless links and the available access networks.

Step_2: Information Analysis

Analyzes the performance changes of node's current communication paths and more importantly senses the handoff triggering events.

Step_3: Decision Making towards Self-Optimization

Evaluates policies to look for the best possible relation between terminal activity and connectivity resources. Thus, in collaboration with AJONS they together realise QoS-aware self-optimization

In order to perform such self-adapting mobility operations, the Mobility Management (FUNC_LEVEL_MM_DE) control loop must orchestrate the necessary protocols and other functions that carry out handoff procedures, namely vertical or horizontal handoffs (i.e., handoff between heterogeneous or homogenous access technologies, respectively). It is widely agreed that IP based mobility management protocols can provide vertical handoff support, including network-based mobility management mechanism (e.g.. Proxy Mobile IP – PMIPv6) and host-based mobility management mechanism (e.g., Mobile IP – MIPv6). In fact, both MIPv6 and PMIPv6 are the supported IP based mobility management mechanisms in 3GPP SAE/LTE system, which are used to support mobility management between 3GPP and non 3GPP accesses. Therefore, towards creating the foundation stones of our overall proposed autonomic mobility management architecture, as well as various QoS, resilience and survivability related autonomic mechanisms, we introduce autonomicity into these two basic mobility support protocols. For details concerning the novelties and autonomic functionalities introduced into MIPv6 and PMIPv6 the reader may refer to sections 3.2.1 and 3.2.2, respectively, of deliverable [D3.2].

❖ *Key Novelties and Designing Principles of the proposed Autonomic QoS & Resource Management Architecture*

In the proposed integrated WLAN/cellular (CDMA or OFDM) architecture, a proper Autonomic Radio Resource Management mechanism (ARRM) residing at the base station of each cell in the network is responsible for optimally and independently allocating cell's available radio resources among all active users already attached to the specific network. Moreover, a new user entering the network or an already attached user willing to perform vertical or horizontal handoff due to connectivity, mobility or QoS-triggered events, is accountable for selecting the most appropriate access network type to be attached to, as well as the corresponding base station (cell) from the ones available in his locality using only locally available information. We use the term QoS-triggered events to refer to the occurrences of a user's service degradation due to (a) connectivity issues (e.g. low signal strength), (b) congestion in the serving cell, (c) potential bad channel conditions, or (d) the existence of lightly loaded (less congested) cells in his locality that could potentially support better his service QoS prerequisites.

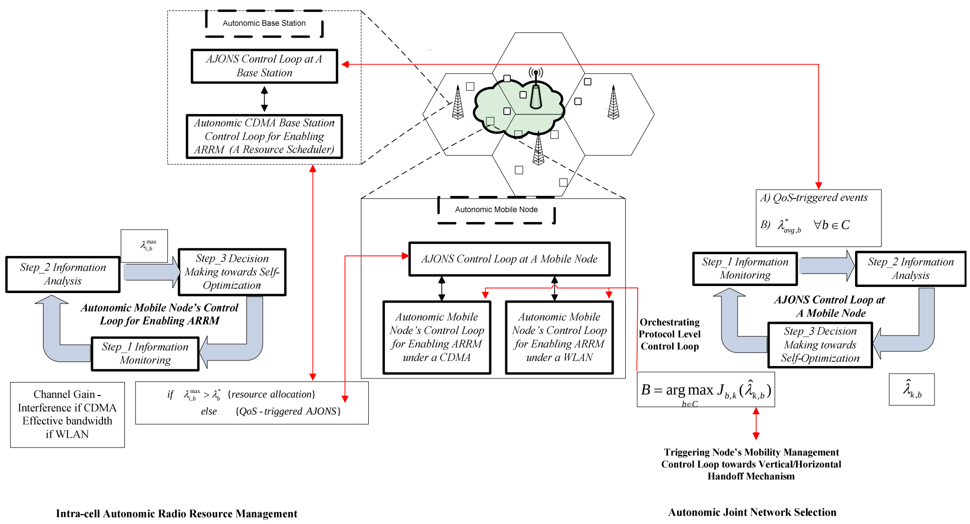

Figure 3. Autonomic intra-cell QoS-aware radio resource management & Autonomic Joint Network Selection Mechanism (AJONS).

In line with GANA architecture, two levels of DEs along with the corresponding autonomic functionalities are introduced, as shown in Figure 3. At protocol level, a DE for steering the radio resource management and QoS provisioning protocol for each of the various access types of networks, namely, CDMA and OFDM cellular networks and WLANs have been introduced (i.e., PROTO_LEVEL_NODE_R&Q_WLAN_DE, and PROTO_LEVEL_NODE_R&Q_CDMA_DE). Moreover, such protocol level DEs aim at exploiting autonomic functionalities and behaviours of current resource management mechanisms towards improving users' and network performance. For details we refer to sections 2.3.1 and 2.3.2, of deliverable [D3.2]. Furthermore, in order to operate and thus, create overall radio resource management mechanisms per wireless network type, corresponding DEs at various network components are introduced (i.e., base station, access point, RANs) (i.e., PROTO_LEVEL_AP_R&Q_WLAN_DE and PROTO_LEVEL_BS_R&Q_CDMA_DE).

All these efforts will be controlled and orchestrated, either at the mobile node level or the network level (e.g., at each base station) by function level DEs that will control the overall QoS-related functionalities of the node or the network. Within an autonomic mobile node, such a functional level is referred as FUNC_LEVEL_QoS_M_DE. The FUNC_LEVEL_QoS_M_DE via its collaboration with other DEs (DEs at same level in GANA's hierarchy such as FUNC_LEVEL_MM_DE, FUNC_LEVEL_QoS_M_DE at base stations, access points, RANs e.t.c., or MEs in terms of protocol level DEs with reference to Figure 1), is envisioned to enable the following enhanced functionalities:

- Autonomic Joint Resource Management over Heterogeneous Network (section 3.2.1 of [D3.2])
- Autonomic QoS-aware Network Selection (section 3.2.1 of [D3.2])
- Autonomic Connection Management (section 3.2.2 of [D3.2])
- Autonomic QoE support (section 2.4 of [D3.2])

Currently, individual DEs towards implementing the previous enhanced functionalities have been implemented and tested. Thus, their efficient and seamless integration into a common FUNC_LEVEL_QoS_M_DE (which will be analysed in D3.6) is reassured not only due to GANA principles that all DEs follow, but also due to the common theoretic framework (utility-based optimisation framework) that has been adopted during their design. Specifically, all the developed autonomic QoS-aware resource allocation mechanisms have adopted a common utility-based framework. Moreover, though the process of designing and theoretically analysing our envisioned approaches a generic methodology via which theoretically-sound autonomic architectures can be derived. This methodology extends NUM theory (Network Utility Maximisation theory) in the field of autonomics. NUM theory has been widely adopted over the last years by the scientific community as one of the basic theoretic frameworks for designing network architectures and protocols [S95], [MZH05], [XLCC08], [C08]. Figure 4 outlines the basic steps of the proposed methodology, which we call ANUM (Autonomic NUM).

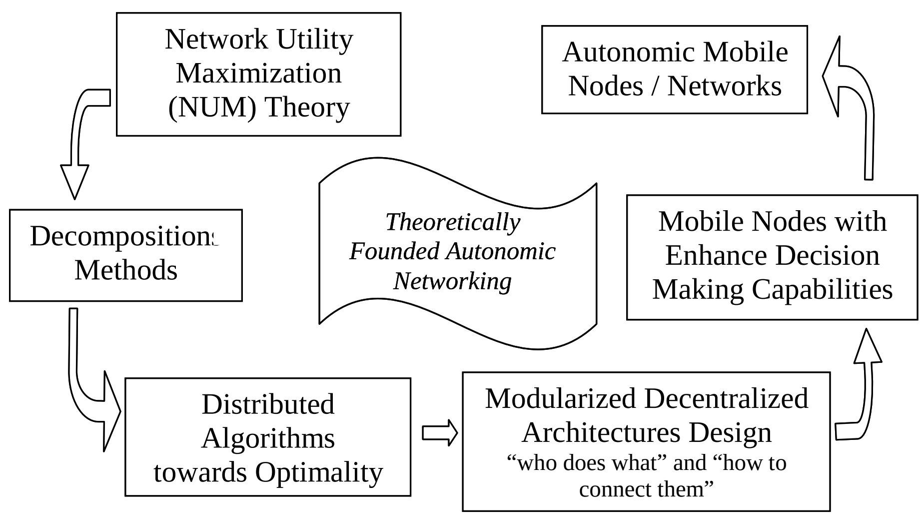

Figure 4. From Describing to Deriving Autonomic Architectures - A Unified Methodology

Designing In Line with 3GPP

The evolution or migration of the 3GPP system aims to develop a higher-data-rate, lower-latency, packet-optimised system that supports multiple Radio Access Technologies (RATs). Meanwhile, reduction of operational efforts and complexity is a key driver for 3GPP LTE, which results in the introduction of the SON functions. Autonomic solutions become essential that support mobility management (especially inter-RAT handover) and QoS, which are expected to increase network performance and quality reacting to dynamic processes in the network with the reduced operational efforts and complexity.

Figure 5 illustrates the reference model of the 3GPP heterogeneous network architecture [RFC5213] [3GPP TS 23.402], where different radio access technologies co-exist in this network including 3GPP LTE, WiMAX, WLAN, etc. As one alternative, Proxy Mobile IPv6 (PMIPv6) [RFC5213] is used as a network-based solution to handle the mobility management between 3GPP and non 3GPP accesses. The LTE radio access network consists of eNodeBs (eNBs), providing services to the User Equipments (UEs). The eNBs interfaces Mobility Management Entity (MME) and Serving Gateways via S1 interface. The PDN Gateway is the gateway which terminates towards the packet data network. Packet data networks may be an external public or private network or an operator's internal network, e.g., for provision of IP multimedia services. The Policy Control and Charging Rules Function (PCRF) encompasses policy control decision and flow based charging control functionalities, which allows the operators to control the overall network through specific policies and rules, for example the authorisation and enforcement of the maximum QoS allocated to the network service.

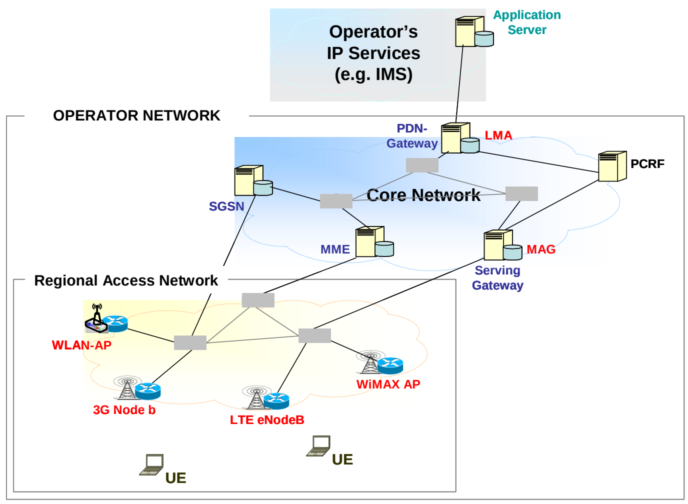

Figure 5. 3GPP Heterogeneous Network Architecture Reference Model

The eNB hosts the functions, such as scheduling, dynamic radio resource allocation, handover decision making and radio admission control, etc. which are closely associated with QoS and MM. The Serving Gateway acts as a Mobile Access Gateway (MAG) [RFC5213] while PDN Gateway includes the functionality of a Local Mobility Anchor (LMA) [RFC5213].

There are several drivers for mobility/QoS control in 3GPP networks.

1. Best radio condition: The primary purpose of cell reselection (for idle mode UEs) and handover (for active mode UEs) is to ensure that the UE camps on/connects to the best cell in terms of radio condition, e.g., path loss, received reference symbol power. The UE should support measurements to suffice this aspect.
2. Camp load balancing: This is to distribute idle state UEs among the available bands/carriers/RATs, such that upon activation, the traffic loading of the bands/carriers/RATs would be balanced. A deliberate mechanism would be necessary to avoid UEs concentrating to a certain RAT.
3. Traffic load balancing: This is to balance the loading of active state UEs. A solution is desired that causes minimum impact on the user perception.
4. UE capability: UEs having different band capabilities may coexist within a network. The mobility solution should cope with the coexistence of various UE capabilities in an efficient manner.
5. Service based mobility control: An operator may have different policies in allocating frequencies to certain services. UEs requiring higher data rates may better be served on a

frequency layer or RAT having a larger bandwidth. This driver is essential for inter-RAT, due to the different QoS levels provided by different RATs. The nature of the service being requested (e.g., QoS and traffic behaviour) should be considered in controlling mobility, so that services are accommodated in the best suitable RAT.

In this work, we have examined the existing mechanisms and protocols and exploiting the autonomic features, which are not only based on the research papers and results, but also on the current specifications and the ongoing discussions in 3GPP. Thus the proposed algorithms and mechanisms well fit into the 3GPP system. Both MIP and PMIP are supported in 3GPP for inter-RAT mobility, and in this work we introduced the autonomic functionalities into these protocols. Mobility control and admission control mechanisms are always the most important features in 3GPP and the proposed mechanism well serve these purposes: 1) Autonomic Joint Resource Management over Heterogeneous Network and Autonomic QoS-aware Network Selection (see section 3.2.1 in [D3.2]); 2) Autonomic Connection Management (section 3.2.2 in [D3.2]) and 3) Autonomic QoE support (section 2.4 in [D3.2]).

C. Resilience – Survivability

The architectural framework proposed here addresses the converging aspects of Resilience, Survivability and Autonomic Fault Management in self-managing networks – UAFAReS (Unified Architecture for Autonomic Fault-Management, Resilience, and Survivability in self-managing networks). The main structure of the architecture was presented in [D3.1]. To recall the goal and the functionality, the architecture is designed to combine some of the research results related to Autonomic Fault-Management with the diversity of the network resilience mechanisms. As a consequence, a unified architectural framework takes the challenge to integrate the diverse existing intrinsic resilient mechanisms into a framework that is able to observe the network and handle properly the occurring erroneous states, thereby taking into consideration the inbuilt resilient mechanisms inside the node functional entities. The emerging architecture is expected to increase the dependability, the reliability and the robustness of the network layer and to provide better conditions to the services and applications running on top of it [TGV10].

During the course of EFIPSANS, the components comprising the architecture have been proposed and the internal structure of the NODE_LEVEL_FM_DE and the NODE_LEVEL_RS_DE as well as their functionality and interactions were specified. The overall architecture is presented in Figure 6. Given the nature of the architecture incorporating the aspects of Resilience and Survivability (targeted in T3.3), and Autonomic Fault-Management (investigated in T4.5), we decided to focus on the components related to Resilience and Survivability in this deliverable. The other components and their interactions are described extensively in D4.5.

A number of factors should be taken into account while designing UAFAReS framework architecture. All of these factors are presented in D4.5. Here, however, we give a short discussion with a focus on the requirements which are closely related to Resilience and Survivability. First and foremost, it is necessary that the proposed architecture takes into account the intrinsic resilient mechanisms implemented inside the network components [TGV10], as it is responsible for choosing the appropriate solution from the set of available ones. This is especially crucial to address *reactive resilience*. In order to be aware of the influence of undertaken actions, the framework should be equipped with a repository storing the knowledge about dynamic dependencies among protocols and services in the network. This knowledge would help to investigate which entities are controlled in order to mask the fault and which are the other ones directly influenced by a Fault-Masking actions. This way the framework will be self-aware and could avoid undertaking contradicting or not effective decisions. In order to realise *proactive resilience* it is necessary to provide *risk assessment* capabilities, so that it is possible to estimate proactively the risk that various components and functional entities will cause further failures in the future. Such a module would help the framework to prepare for future incidents and possibly also avoid future fault activations by proactively sustaining the network functionalities in challenging conditions. Also the architecture needs to be application/service aware and thus provide facilities for implementing the concept of *Survivability Requirements (SR)*. By means of SR the framework will provide the possibility for applications to express their needs for obtaining vital information regarding incidents/alarms in the network [TGV10]. Thus the application layer could be prepared to react accordingly and survive in the presence of faulty conditions [TGV10].

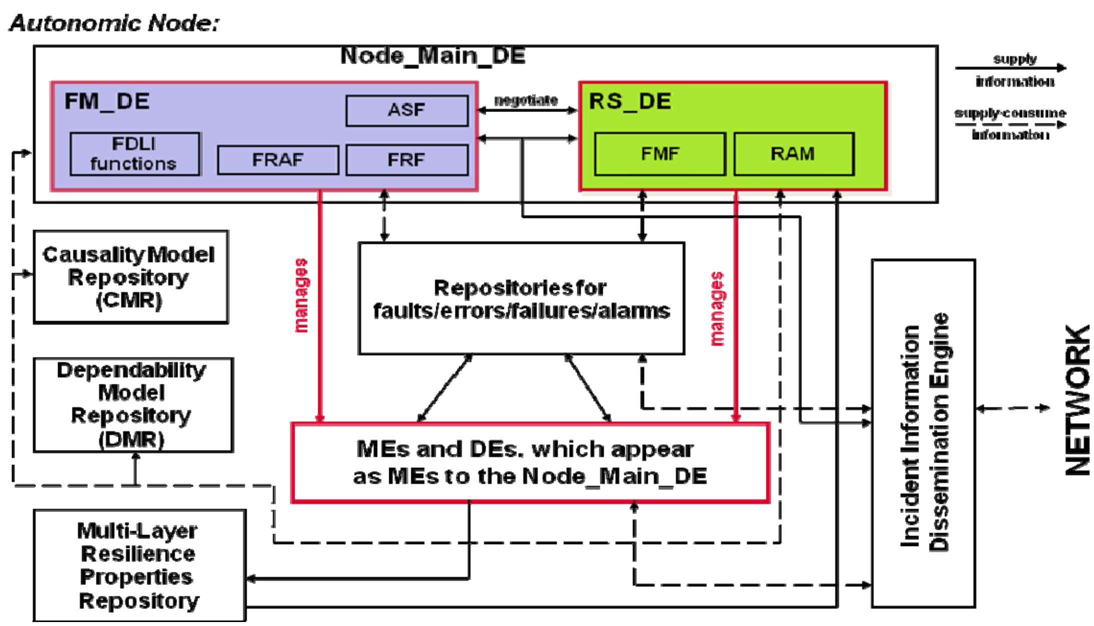

Figure 6. The unified node architecture for Resilience, Survivability and Autonomic Fault-Management for self-managing networks [TGV10]

Based on these requirements and the control loop structures of GANA, a number of components and inter-working mechanisms are defined. In this document the NODE_LEVEL_RS_DE component will be presented. Figure 7 shows the relations between NODE_LEVEL_RS_DE and other components that interact with it in order to introduce resilient behaviours inside a node.

The NODE_LEVEL_RS_DE is responsible for an immediate reaction to failures and faults aimed at sustaining an acceptable QoS level by employing diverse fault-tolerant mechanisms, i.e. it performs Fault-Masking. Additionally, the NODE_LEVEL_RS_DE implements proactive mechanisms based on the estimated fitness of the network components [TGV10].

In a GANA autonomic node/device, the NODE_LEVEL_RS_DE is required to have exclusive access to all other entities (MEs and DEs) inside the node. That is why we introduce the NODE_LEVEL_RS_DE at the node level inside the GANA reference model.

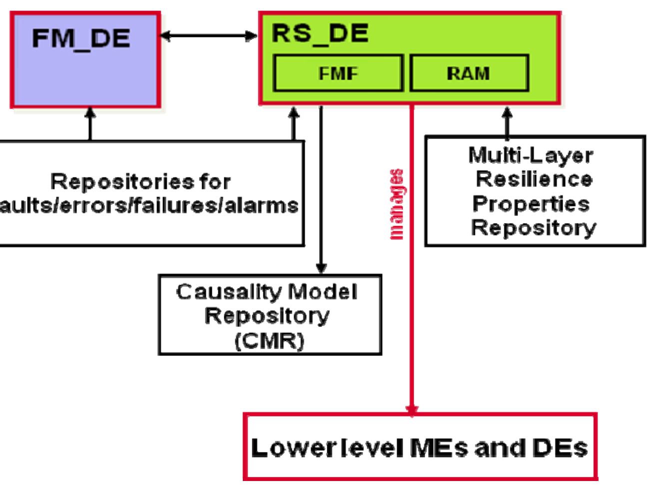

Figure 7. NODE_LEVEL_RS_DE and related components of the architecture

The operation of the NODE_LEVEL_RS_DE is based on information from the NODE_LEVEL_FM_DE and from other diverse functional entities that supply information to the fault/error/failure/alarm repositories of an autonomic node. The Monitoring Components, supported by the node repositories, provide data related to the directly detected faults, errors and failures or generated alarms. The direct connection to the NODE_LEVEL_FM_DE ensures that the NODE_LEVEL_RS_DE has the up-to-date knowledge about isolated faults and the Fault-Removal process [TGV10].

Having information from the NODE_LEVEL_FM_DE and dedicated repositories, the NODE_LEVEL_RS_DE triggers diverse reactive Fault-Masking mechanisms depending on the situation in the network. This process is controlled by the *Fault Masking Functions* (FMF) module realising *Reactive Resilience* functionalities. Thus, the NODE_LEVEL_RS_DE acts in a fault-tolerant manner and orchestrates resilient mechanisms of the selected node entities (MEs of this DE) to ensure acceptable QoS and sustain network functionality. In order to select appropriate solutions and to manage the resilient behaviour of a node, the NODE_LEVEL_RS_DE must be aware of the resilient mechanisms implemented intrinsically inside the MEs which are under its control (protocol modules and other lower-level DEs). This knowledge is stored and retrieved from a dedicated repository – *Multi-Layer Resilience Properties Repository*. Moreover, before imposing its own decisions, the NODE_LEVEL_RS_DE is required to give the low level MEs a chance to recover based on their own intrinsic resilient mechanisms. However, managerial responsibilities belong to the NODE_LEVEL_RS_DE and thus it has the right to intercept the intrinsic actions undertaken by the autonomic entities if they are contradicting [TGV10].

Below the two main components of NODE_LEVEL_RS_DE are presented in more details:

Fault Masking Functions

The FMF module of the NODE_LEVEL_RS_DE is being immediately informed about an incident in the network that the node is aware of and about the isolated fault(s) (once this information is available). NODE_LEVEL_RS_DE can be used to perform both – fast reactions upon just detecting an incident and fault masking while the isolated fault is being removed. As a consequence, in both cases the NODE_LEVEL_RS_DE triggers a *Fault-Masking* procedure as described in Figure 8. After being informed about an incident or a fault, the NODE_LEVEL_RS_DE synchronises, i.e., negotiates, its tentative action with the NODE_LEVEL_FM_DE (see details in D4.5, chapter 2), in case a preconfigured policy does not allow it to execute the intended activity autonomously. Based on the negotiation result, the NODE_LEVEL_RS_DE discards or performs the Fault-Masking action on the corresponding MEs.

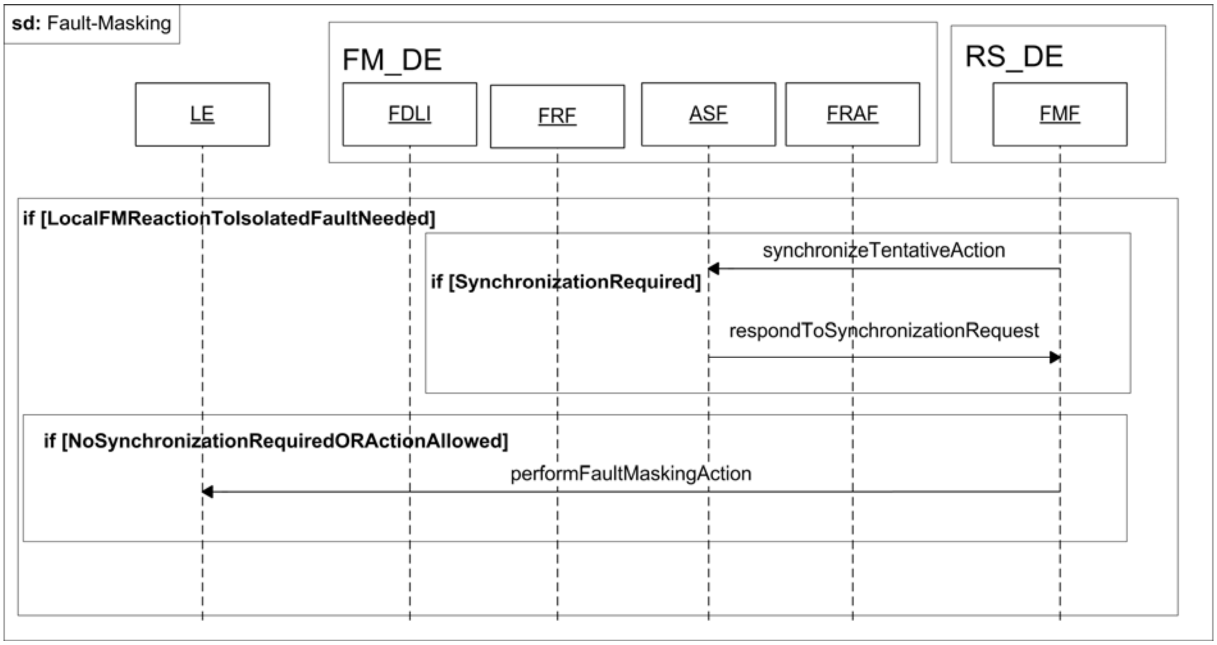

Figure 8. The interaction flow required for realising fault-masking

Risk Assessment Module

While the FMF module of the NODE_LEVEL_RS_DE takes reactive actions upon detected incidents, the *Risk Assessment Module* (RAM) is in charge of spreading real-time risk assessment information within the network. This module intends to deal with the fluctuating nature of the failure occurrence probabilities by multicasting risk level information that contains the origin of the prediction, the probability of occurrence, the potential impact of the failure as well as its severity, the failure extent and the impacted services. The failure prediction is based on the monitoring of internal state and behaviour of a node involving specific parameters, which are significant enough to predict a future failure, such as the hardware temperature, the internal fan status, the hard drive status, the voltage instability, the signal quality, etc. We also need to take into account software parameters including the load, anomalies (memory leaking, unreleased file locks, file descriptor leaking, data corruption), the virus and hacker attacks, and the maintenance activities since such interventions account for 20% of all failures. The primary benefits expected from the RAM relate to the NODE_LEVEL_RS_DE, and more precisely to adapt the GMPLS level of recovery [section 4.4 in [D3.2]] with regards to the incurred risk. Finally, as means of *proactive resilience*, the risk information can be exploited by any candidate DE such as the Routing-Management-DE, that tune OSPFv3 link weights in order to dynamically adapt to Risk-levels in the network [D2.4]. As a result of all its functionalities, the NODE_LEVEL_RS_DE is able to proactively steer the node entities such that the node and/or network can prepare for the problems that are likely to manifest in the future. In a consequence, it is possible to avoid future fault activations [TGV10].