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

Advanced Network Services in Autonomic IPv6 Networking: Performance Analysis and Evaluation

Project Document Number: EFIPSANS/D3.2 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 presents a concrete and comprehensive analysis of the autonomic functionalities, behaviours and mechanisms regarding advanced network services in autonomic IPv6 enabled networking environments, studied and devised within EFIPSANS Work Package 3. Specifically, it covers the areas of mobility management, QoS provisioning, resilience and survivability, security and cross layering. The purpose of this deliverable is twofold. It aims at illustrating the novelties achieved within the framework of WP3 as well as revealing the efficacy of the proposed approaches via simulation and analysis, in terms of performance evaluation. Furthermore, it presents in a concrete and comprehensible way WP3 progress and methodology towards integrating various autonomic functionalities (sub-architectures) that have been devised into overall emerging architectures, leading to the fulfilment of EFIPSANS goals and objectives.
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.3.2v1.0
Document Title	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) 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)

Executive Summary

This deliverable summarizes the work performed in WP3 "Advanced Network Services and Applications Support" up to M24 of the EFIPSANS project. The focus of WP3 is on introducing autonomicity in advanced network functionalities e.g. mobility, QoS, Resilience, Security, etc. Specifically, the main objectives are: to develop advanced seamless mobility mechanisms that efficiently support multihoming over an IPv6 heterogeneous wireless environment; develop novel mechanisms that enable regional collaboration of various autonomic wireless networks under a common utility based integrated framework; develop mechanisms that will provide QoS guarantees for users' applications in autonomic IPv6 networks; design a novel QoS architecture based on the identification of the interaction between autonomicity and the current QoS mechanisms; develop mechanisms, concepts, components and protocols that will improve the resilience and survivability in autonomic IPv6 networks; address security (i.e. trust models (in sense of architectural components relations) and vulnerability) in autonomic IPv6 enabled networks; research autonomic mechanisms that will take advantage of cross layered information exchange. It is within these objectives that the contributions of this deliverable lie. This is a final deliverable due in month M24 (Dec '09) and focuses on the development of Frameworks F6 – F12**.**

For each of the topics studied here a two-layer analysis is performed and illustrated:

I. Analysis and Assessment of the proposed autonomic functionalities/behaviours/mechanisms.
Towards fulfilling this goal, for each of the topics (WP3) covered within this deliverable, the following key objectives have been set: a) clear problem statement (beyond state-of-the-art necessity), b) concrete proposed autonomic solution presentation, c) analytic description of the corresponding DEs and the algorithms (i.e. control loops) that steer them, d) illustration of numerical results (produced via simulations) that clearly reveal the operation and the benefits of the proposed autonomic mechanism, and finally, e) discussion of scalability and stability issues.

II. Autonomic mechanisms integration and autonomic architectures analysis.
For each of the topics presented and analysed in an individual manner, a justified methodology is presented that has been followed towards integrating them (i.e. multiple autonomic functionalities/mechanisms, either in node's or network's scope) in a seamless, efficient and flexible way in overall emerging architectures. Thus, it is revealed how the overall followed approach facilitates the creation of autonomic, proficient, flexible and scalable architectures via GANA, which encapsulate and thus define, in a concrete way, the orchestration and collaboration of multiple Decision Elements (DEs) at various network components or within a node. A detailed analysis and evaluation of the integrated architectures will be presented in D3.6 (M30).

Table of Contents

Table of Figures

Table of Tables

1 INTRODUCTION

The vast increment of Internet and Mobile users during the preceding years, their corresponding services' growing demands on resources and firm QoS expectations, as well as the existence of various available fixed or mobile access network types, assemble the view of current networking environment, which is mainly characterized by its heterogeneity, multiplicity and complexity. Therefore, the introduction of various self-* functionalities to the end-users or various network components towards enabling autonomic network architectures, is considered as one of the most promising future network design paradigms, that will allow to overcome the previous drawbacks and to enhance users' experience, in terms of improved service performance, perceived Quality of Service (QoS) and reduced costs. As its foundation, EFIPSANS project envisions autonomicity as the enabler to achieve and realize this vision.

With respect to the previous vision, WP3 focuses on introducing autonomic attributes to advanced functionalities that a network could in principle operate without e.g. mobility, QoS, resilience, security, etc, as opposed to the basic networking services (functions) addressed by WP2 "Basic Networking Services". To be more precise, the main objectives of WP3, as summarized in Annex I - "Description of Work", are the following:

(i) To develop advanced seamless mobility mechanisms that efficiently support multihoming over an IPv6 heterogeneous wireless environment;

(ii) To develop novel mechanisms that enable regional collaboration of various autonomic wireless networks under a common utility based integrated framework;

(iii) To develop mechanisms that will provide QoS guarantees for users' applications in autonomic IPv6 networks;

(iv) To design novel QoS architectures based on the identification of the interaction between autonomicity and the current QoS mechanisms;

(v) To develop mechanisms and protocols that will improve the resilience and survivability in autonomic IPv6 networks;

(vi) To investigate and address security issues, concerning trust models (in sense of architectural components relations) and vulnerability in autonomic IPv6 enabled networks;

(vii) To develop autonomic mechanisms that will take advantage of the cross layered information exchange.

Towards accomplishing the previous objectives, during project's second year, WP3 placed emphasis on achieving the following: **a)** ***assessing*** all the various autonomic functionalities and mechanisms that have been developed within its framework via simulation and experimentation, towards *i)* revealing the benefits of the proposed autonomicity-driven approaches compared to current state-of-the-art ones and *ii)* assessing the scalability/stability attributes of the proposed autonomic approaches either via analysis or simulation in specific use cases; **b)** ***finalizing the design*** and development of concrete DEs for all the previous introduced autonomic functionalities; **c)** ***incorporating*** individually developed components in WP3 into emerging concrete architectures via the integration of various produced autonomic mechanisms, in terms of integrated function level DEs, towards enabling the following emerging architectures: *i)* autonomic QoS management over a wired environment, *ii)* autonomic mobility and QoS management over a heterogeneous wireless environment, *iii)* autonomic resilience & survivability; **d)** ***specifying concrete scenarios*** that allow the identification and demonstration of the key features and novelties of the emerging architectures within WP3 and thus, will be partially implemented in project's testbeds.

1.1 Scope of the Deliverable

This deliverable serves two main goals. Its principal goal is to present in a concrete way the various autonomic functionalities that have been devised within WP3 and to assess their efficacy through illustrating numerical results. Such demonstration and assessment refers to all topics covered within WP3 in an individual manner.

It is noted that, the previous goal mainly concerns WP3 objectives regarding mobility management (*Task3.1*), QoS provisioning (*Task3.2*) and cross layering (*Task3.5*), i.e. WP3 objectives (i)-(iv) and (vii). Security aspects (*Task 3.4 - WP3 objective (vi)*) are specifically addressed in D3.5 (a new added deliverable – M24). With respect to resilience and survivability issues (*Task 3.3 - WP3 objective (v)*) initial only achievement are highlighted in this deliverable, while according to the Technical Annex a detailed description and evaluation is planned to be covered in the upcoming deliverable D3.4 (M36).

Towards fulfilling the previous objectives and in order to improve illustration's efficacy, each topic's analysis follows the same pattern that includes: i) problem statement, ii) proposed autonomic solution, iii) corresponding GANA compatible mechanism(s), iv) scalability, stability and complexity issues and then v) performance evaluation and numerical results.

The second main goal is to outline the methodology, current achievements and future plan towards fulfilling the ultimate goal of integrating most of the previous individually studied topics in concrete integrated autonomic architectures.

In order to efficiently achieve the previous goal, each topic's treatment contains a concrete analysis of the corresponding devised autonomic mechanism integration status within WP3 emerging architectures, in terms of goals, methodology and key designing principles. For completeness purposes, this deliverable is also supplemented by Appendix I [D3.2_Appendix I] that provides a brief description and status of the respective emerging architectures. A detailed evaluation of the integrated architectures and corresponding features will be included in D3.6 (M30).

1.2 Structure of the Document

The rest of this document is organized as follows.

Chapter 2, presents and validates WP3 efforts towards introducing autonomic attributes in QoS management mechanisms in various networking environments.

Chapter 3, illustrates a comprehensive analysis and assessment of the issues concerning autonomicity and mobility management.

Chapter 4, gives a comprehensive analysis of the key achievements in the area of resilience-survivability and/for autonomicity.

Chapter 5, provides an explicit analysis of the proposed autonomic mechanisms devised within the framework of cross layering and autonomicity.

Chapter 6, concludes this deliverable and discusses the next research and development steps.

2 AUTONOMIC BEHAVIOURAL CHARACTERISTICS IN QOS MANAGEMENT

2.1 Introduction

Chapter 2 studies QoS management and autonomicity in various networking environments. Initially, two basic sections that address the issues of efficient autonomic QoS provisioning over wired (section 2.2) and wireless (section 2.3) networking paradigms are included.

While considering an enhanced autonomic solution to QoS management in core wired networks sections 2.2.1 and 2.2.2 outline our overall research effort towards introducing autonomic attributes into traditional DiffServ QoS architectures. Thus, in both sections inherent drawbacks of a DiffServ architecture are identified (e.g., its inability to set and/or distinguish packets priorities when belonging to the same flow) and then, autonomicity-driven mechanisms are devised in order to overcome them. Moreover, even if both sections address the same problem, from a different point of view, complementary approaches are presented. Specifically, an overall concrete autonomic GANA-aware architecture is presented which enables the QoS management systems in wired core networks to automatically adapt to the changing context and optimise network resources management, as presented in section 2.2.1 and section 2.2.2 EFIPSANS exploits a dynamic QoS framework over autonomic networks. Afterwards, section 2.3 emphasises QoS management over an autonomic wireless environment. Specifically, proficient QoS-aware radio resource management in CDMA cellular (both downlink and uplink) and WLAN networks under a common utility-based framework is addressed and then, based on the aforementioned integrated framework, autonomicity in QoS management over 3GPP systems is studied. This is dealt within sections 2.3.1, 2.3.2 and 2.3.3, respectively. Finally, tackling the issue of autonomicity from services perspective, section 2.4 explores the interrelation between QoE & QoS in autonomic environments.

All of the above developments which are presented in an individual manner is this chapter are presented (along with individual efforts from other tasks) within the framework the emerging integrated architectures that are described in [D3.2_Appendix_I].

2.2 QoS Managements and Autonomicity in Wired Core Networks

2.2.1 Autonomicity in traditional DiffServ QoS architectures

Introduction. A new architecture for QoS management in wired core networks is proposed based on the traditional Diffserv QoS architecture, through which we aim at enhancing the efficacy of currently existing approaches via the introduction of autonomic attributes, such as self-optimisation, self-configuration, self-organisation, and self-adaptation. In addition, the proposed architecture takes also advantage of effective service-aware functions to improve the autonomic service control, which enables the QoS management systems in wired core networks to automatically adapt to the changing context, optimise network resources management and thus, improve users' QoS experience and reduce manual intervention.

Problem's statement and its autonomic solution

The existing Internet is facing great challenges in many aspects such as address assignment, routing scalability, management and configuration, QoS, security, trust, etc. These problems are restricting the evolution of the current Internet. Recently more and more researchers are paying increased attention to research on future Internet architecture, and new Internet architecture models are proposed. Autonomic networking is an important research field in future network architecture. In an autonomic network, a series of autonomic attributes (such as context-aware, self-configuration, self-management, self-organisation, self-optimising, self-adjustment and self-protection) are introduced into network entities. The objective is to solve the increasingly complexity of network control and management in heterogeneous network environments, and minimise the burden of manual operation.

QoS management in core networks is one of the most important research topics focusing on end-to-end QoS provisioning. Due to its simplicity and scalability, the DiffServ framework is a widely accepted QoS solution. In a DiffServ domain, edge nodes implement the most complex functionalities, such as packet classifying, marking and shaping; core nodes only provide simple mechanisms such as queue management and scheduling.

However, the traditional DiffServ architecture lacks flexibility and self-adaptability. Take the packet marking mechanism as an example. In the edge nodes of a domain, a packet marker is employed to mark arriving packets into different priorities according to their service type and traffic conditions. Other network components will use special per hop behaviors (PHB) to process marked packet flows based on the priorities of each packet. Therefore, selecting different marking schemes will directly affect the overall performance of QoS provision. However, traditional marking algorithms lack self-adaptability i.e., packets are marked on the basis of the traffic parameters in accordance to traffic specifications which are generally extracted from SLA/SLS (Service Level Agreement/Specification). Before the arrival of a service packet flow, the marker parameters in the edge node must be configured for this flow in advance; and this requires manual configuration or a complex QoS control and management system in the network. Following the previous analysis, we can identify a number of other techniques in DiffServ network that are also facing with the same problem.

In addition to these drawbacks, traditional DiffServ mechanisms do not distinguish packets with different higher-layer semantics. In practice, a flow of the same service may consist of packets with different semantic priorities i.e., some critical packets may require much more protections than other packets when they are transferred through the network. Therefore, recognising higher-level semantics and context will help the network to select suitable behaviours to improve users' QoS experience.

While studying and providing solutions for the above critical problems, we introduce context-aware and autonomic features into DiffServ architecture, and enhance QoS mechanisms to support autonomicity. The goal is to enable the autonomic DiffServ network to adaptively guarantee better QoS performance according to diversified user requirements and dynamically network environments. Actually, all kinds of DiffServ mechanisms can be enhanced to support autonomic attributes. The proposed architecture of QoS management in a core network is shown in **Figure 1**.

The QoS Manager is in charge of the QoS management of the entire network. It coordinates the behaviours of QoS mechanisms in autonomic nodes (AN) and the interactions among them. In this architecture, several components (and their corresponding DEs) are introduced [details can be found in D3.1, Section 5.2.1.1.1 & 5.2.1.1.2] to support autonomic attributes in the DiffServ QoS architecture including:

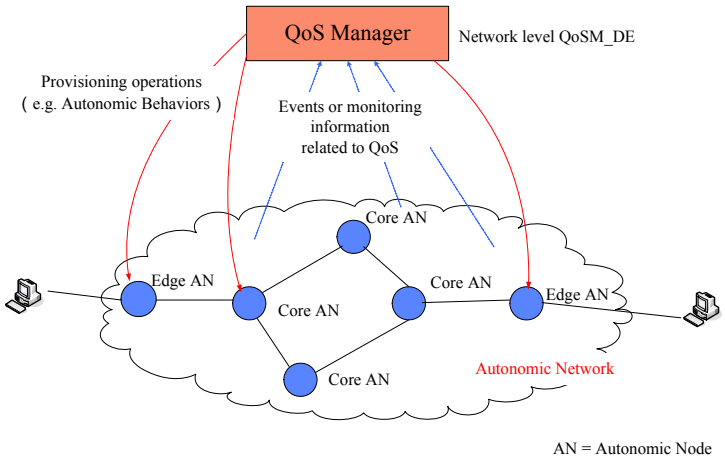


Figure 1. Wired Network Architecture

1. Self-adaptation and self-organisation

In the dynamically changing network environment, self-adaptation abilities are required in QoS management. For each special type of QoS functionality, e.g., the packet marking mechanism, a network node may support different marking mechanisms or algorithms. A protocol level packet marking DE (PROTO_LEVEL_PM_DE) is introduced to dynamically control, organise and configure behaviours of these packet-marking mechanisms. This enables the autonomic nodes to select the proper mechanisms for packet marking according to network environment and conditions. Therefore, self-adaptation and self-organisation are achieved.

2. Self-configuration

In the autonomic QoS framework, network elements are capable of supporting various QoS mechanisms for different application scenarios. These QoS mechanisms are usually configurable and adjustable to adapting to the changing network context.

3. Self-optimisation

At the network level, NET_LEVEL_QoS_M_DE is the decision maker for optimisation. It collects QoS requirements and performance parameters from users and the network, analyses them, and makes decisions according to certain policies. For instance, when the traffic of a service flow is high, NET_LEVEL_QoS_M_DE may decide to adjust the bandwidth allocation scheme of the entire network. If NET_LEVEL_QoS_M_DE detects congestion in the network, it may generate new admission control policies and disseminate them to autonomic edge nodes control some low priority traffic flows' coming into the network.

Proposed Algorithm. To address the above issues we have proposed a context-aware autonomic packet marking algorithm and queue management mechanism.

A. The Context-aware autonomic packet marking algorithm

The proposed autonomic packet marking algorithm (CAPM--a novel context-aware autonomic packet marker) is capable of collecting various QoS related service contexts and network contexts. CAPM is capable of recognising semantic priorities in application traffic flows and then, adaptively adjust its marking behaviour accordingly. We introduce autonomic and context-awareness into the packet marker, which exploits service application and semantic priorities as service context information. Specifically, it uses the network packet loss rate feedback from the destination terminal as network context information to decide the marking distribution. Thus, the packet marker adjusts its marking behaviour according to the collected context information.

The autonomic features are realised in the form of an autonomic control loop. The CAPM is a multimedia-friendly marking mechanism, which provides 2 context-aware features: (1) adaptively selecting suitable marking scheme according to different service type; (2) recognising different

semantic priorities of packets in a same service flow, and differentially mark them with different profiles. The CAPM is an extended version of srTCM (Single Rate Three Colour Marker). Packets are divided into critical packets and non-critical packets according to their semantic importance. CAPM adds a dark green bucket to increase the probability of critical packet marked as green. The packets of different semantic priorities are marked following different marking processes. Moreover, we introduce two concepts, such as token reserve and token borrowing to adjust the marking distribution of non-critical packets.

B. The autonomic queue management algorithm

We also introduce autonomic mechanisms to our queue management mechanism design. Autonomic attributes such as self-configuration and self-adaptation are realised based on a feedback loop. And the feedback loop is based on context information collected through the collecting step. We use the context information to dynamically configure and adjust the packet dropping operation. Firstly, the source terminal records the service context information (video codec characteristics information) into each IP packet header. It defines several fields in the IP header to record the corresponding video compression characteristics information. The source will map packets to five priority classes according to their context information, and pre-mark the priority index into each video packet header. The autonomic queue management algorithm is capable of collecting service context and network context information. The autonomic queue management mechanism obtains the service context information by reading the IP header fields. The packets of different priority classes are mapped to corresponding virtual queues in the intermediate nodes output queue. When the network congestion occurs, the node always chose the lowest priority packets to drop. The queue management parameter can be adjusted adaptively according to the service context information. In our algorithm, maximum drop probability Maxp is adjustable. It can be adjusted by the P frame index and B frame size. Maxp is relatively high for packet with higher semantic importance, so that it is not easy to drop. Therefore, the queue management algorithm tries to decrease the dropping of important video packets and decrease the loss of perceived video quality caused by packet loss.

Scalability, Stability and Validation Issues. DiffServ itself is proposed by IETF as a scalable solution to provide quality of service in IP networks. Depending on the DSCP it classifies IP packets located in the IPv6 header, and delivers them according to the PHB. Unlike IntServ, DiffServ is course-grained, (i.e., no need for routers to maintain state on every flow passing through them) and deals with the aggregate flow and not the single one. The architecture we proposed is the extension of DiffServ, so it also has good scalability properties (similar to existing standards). We use simulation to evaluate the efficiency of the proposed mechanisms and algorithms. At present, we have completed the simulation and validations of the proposed autonomic packet marking mechanism. The following section describes some initial results of our simulation. Currently, simulations concerning the proposed queue management algorithms are underway.

Numerical Results. We simulate the performance of proposed CAPM under NS-2. The network topology is shown as **Figure 2**. We assume the link between the two core autonomic nodes (CAN) is the bottleneck, the capacity of which is 10Mbps. Multimedia traffic is sent from source *S1, S2, ..., Sn* to destination terminal *D*. The multimedia traffic from source terminals is mapped to standard DiffServ AF1 class. Two classes of background traffics (respectively mapped to AF2 and BE) are transferred from CAN1 to CAN2 via the bottleneck link. In core nodes, three queues (AF1, AF2 and BE) are configured. In all nodes the packet dropping algorithm for AF queues are configured to WRED (Weighted Random Early Detection), and the queue scheduling algorithm is WRR (Weighted Round Robin). Through adjusting weights of AF1/AF2 queues and increasing the AF2 background traffic volume (BE will not affect AF1), congestion can arise on the AF1 queue. In this situation, the performances of CAPM and srTCM are compared.

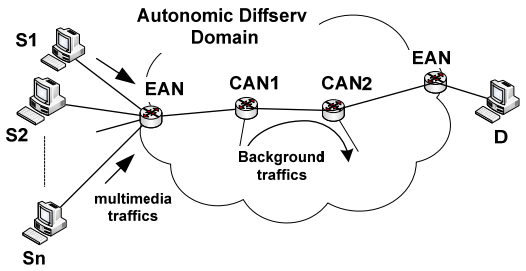


Figure 2. The simulation topology.

Table 1. Traffic attributes of four H.264 encoded video streams.

Stream Name	Frames	AR [1]	AR_{cri} [2]	MBS [3]
Foreman_cif	300	34.2	14.1	20.1
Tempete_cif	260	74.3	29.0	24.2
hall_monitor_qcif	329	6.84	4.47	9.8
news_qcif	299	8.45	5.24	11.9

Note: 1. *AR* - the average information rate of the stream (KB/s).
2. AR_{cri} - the average information rate of critical packets (KB/s).
3. *MBS* - the maximum bust size (KB).

Encoded video streams are used as input source traffics, and a method similar to Chih-Heng Ke's method [GLCW09], [XWY] is adopted. We use 4 different H.264 encoded video clips. In the receiver terminal, the received packet flow is re-assembled and decoded to a sequence of video frames. Then the decoded video is compared to the original video source. In this paper, we use PSNR (Peak Signal to Noise Ratio) to evaluate the end users' QoS experience of video services. The attributes of the encoded video clips are summarised in **Table 1**.

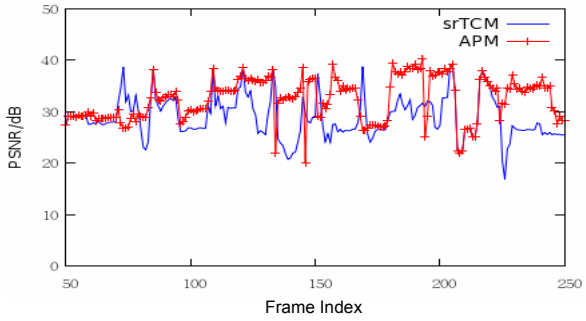


Figure 3. PSNR results of srTCM and APM in simulation scenario 1.

Figure 4. Screen snapshots of srTCM (left) and CAPM (right) in the simulation scenario 1.

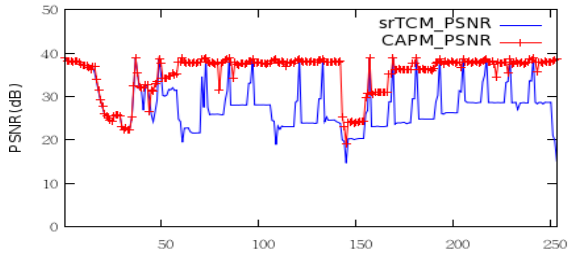
In the first simulation scenario, a single video traffic flow is transferred from terminal S1 to terminal D. The clip forman_cif is used as source stream. **Figure 3** compares the PSNR results of CAPM and srTCM, and **Figure 4** shows the comparison of screen snapshot of two algorithms. In the second simulation scenario, four video streams are simultaneously transferred from terminal S1, S2, S3, S4 respectively to terminal D. **Figure 5**A presents the comparison among two marking algorithms with respect the achieved PSNR values of 2 video streams (hall_monitor_qcif and news_qcif) in all 4 streams. Thus, **Figure 5**B compares the screen snapshot of CAPM and srTCM, in which the video stream is news_qcif.

Table 2 summarises the average values of PSNR results in the simulation scenario 1 and scenario 2. Obviously, the simulation results reveal that the proposed CAPM provides a distinct improvement in users' QoS experience and performance for multimedia applications.

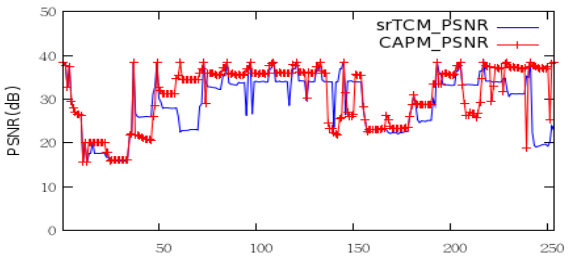
Table 2. The summary of average PSNR (db) in the simulation scenario 1 and 2.

Stream Name	Scenario	PSNR (srTCM)	PSNR (CAPM)
Foreman_cif	1	28.46	31.36
	2	23.35	25.65
Tempete_cif	2	20.28	22.12
hall_monitor_qcif	2	27.79	35.47
News_qcif	2	29.08	30.87

From the simulation results, we can see that CAPM is capable of recognising semantic priorities in application traffic flows and adaptively adjust its marking behavior accordingly, making it suitable for multimedia services. The previous work has been published in [GLCW09] and [XWY].



(a) Video stream: *hall_monitor_qcif*



(b) Video stream: *news_qcif*

(a) Video stream: *hall_monitor_qcif.*

(b) Video stream: news_*qcif.*

Figure 5. A) PSNR results of srTCM and CAPM, B) Screen snapshots of srTCM (left) and CAPM (right).

2.2.2 Dynamic QoS framework over Autonomic Networks

Introduction. As mentioned above, provisioning of inter-domain QoS is not widely realised in today's networks. Functional and operational limitations of proposed frameworks present

technical challenges in implementing scalable solutions that satisfy end-to-end QoS user requirements on a per flow basis across multiple domains.

As IP networks are dynamic with frequent topology changes, resource management becomes cumbersome for network operators. This is particularly acute when multiple domains are involved for the provision of a QoS service and time-consuming off-line arrangements are necessary between operators in different domains. Unexpected network topology changes due to link or node failures cause traffic to be rerouted leading (Figure 6) to service degradation to most of the flows passing through congested links with network operators unable to take immediate actions.

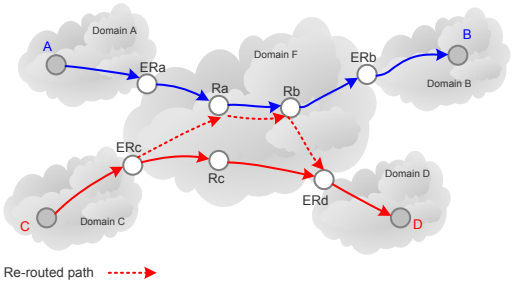


Figure 6. Congestion problems in Ra-Rb link due to rerouting of red flow.

Autonomic QoS Provisioning in DiffServ Networks

The following figure Figure 7 shows an ideal situation for supporting end-to-end QoS guarantees in a multi-domain environment based on DiffServ framework. The first router across the path, called in this document as *Designated Source Router (DSR)*, enables per flow traffic conditioning for the flows initiated in the router's local network. At the administrative domains borders, the edge routers (ER) perform policing to traffic aggregates.

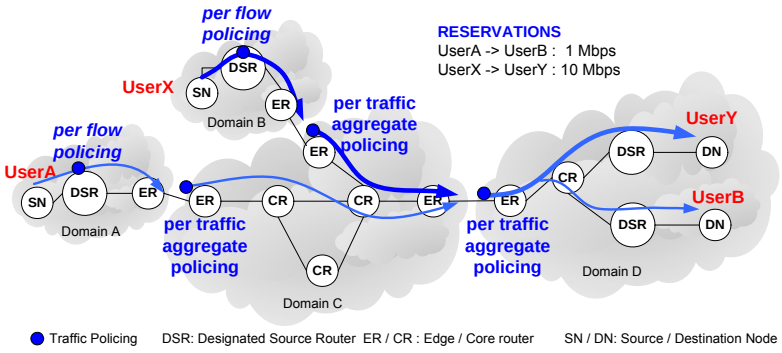


Figure 7. Traffic control in DiffServ network (inter-domain scenario)

There are multiple challenges to be addressed for the provision of QoS in multi-domain environments, as follows:

1. Resource management of scarce resources, i.e., allocate resources along the end-to-end path
2. Control inter-domain traffic policing, i.e., how to set and maintain the traffic police's at the administrative domains edges.
3. Monitor traffic guarantees on per flow basis, i.e., assess whether performance guarantees is provided to transported traffic
4. Handle rerouted traffic caused by network failures, especially in order to sustain performance guarantees to existing flows

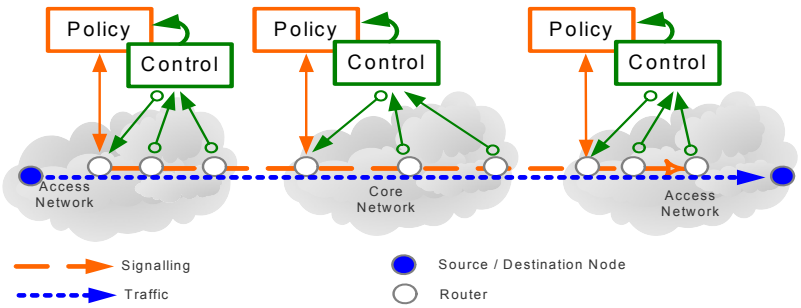


Figure 8. Control mechanisms in routers for autonomic control of flows and traffic policies

We aim to address –to some extent- all the above challenges taking into consideration basic autonomic principles, especially focusing on *self-management* and *self-optimisation*. In a multi-domain environment, we assume that there are no centralised entities that have a general view of the network topology, of the available resources and the active flows. Such entities, e.g., *bandwidth brokers*, are able to perform efficient resource allocation. However, the collection and updating of required data is a laborious and complex task. We propose a fully distributed technique, where resource allocation is handled with end-to-end signalling. Node-local mechanisms will assess the availability of local resources in routers along the end-to-end paths. As explained later, routers are enabled to independently control the establishment of new flows and police their traffic at the domain boundaries according to administrators' policies (Figure 8). Routers capabilities exhibit autonomic *self-management* behaviour.

Data communication between two random nodes in the network is not interrupted when network topology is changed. However, as discussed previously, traffic guarantees are usually violated in case of network topology change, as rerouting traffic may causes congestion along the new network path. We propose an end-to-end technique where monitoring packets -exchanged between traffic source nodes and consuming nodes- is used for identifying rerouted flows. Mechanisms activated by monitoring packets allow reducing the impact of network congestion to the minimum number of flows. This is also considered as autonomic *self-optimisation* behaviour.

Challenge 1: Resource Management in the end-to-end path

We propose that the routers across the end-to-end path verify that there are available network resources and thus, the admittance of another flow will not impact the performance guarantees already provided to other users. Admission control decisions are based on *Measurement-based Admission Control (MBAC)* mechanisms [BJS00]. MBAC mechanisms are attractive for management of network resources as they do not require per-flow state information and a prior knowledge of traffic specifications.

In our proposal, a signalling packet is sent towards the destination (using standard IP routing protocols) and allocate bandwidth according to the flow specifications prior a new (QoS-) flow is established. We will refer to signalling packets as *Path Resource Estimation Packets (PREP)*.
The exact signalling mechanism is as follows:

1. The Designated Source Router (DSR) creates a PREP REQ (request packet), which contains the traffic profile parameters of the flow upon an initial request from the end-user (source node).
2. The PREP REQ is routed based on the destination address (path-coupled signalling) in order to trigger routers across the path to estimate if there are enough resources. If there are adequate resources locally, a router will further forward the message to the next hop and will temporarily store flow information in its local Q-FLIB. Otherwise, it will discard the message and return a negative response to the sender's DSR.

3. If eventually the PREP REQ arrives to the destination DSR, the latter can conclude that the new flow can be established and, thus, returns a positive response PREP RESP to the sender's DSR. Routers along the return path will initially verify that the corresponding flow information is stored in their local Q-FIB database. If true, they will remove the entry and further forward them towards the source. Upon reception of the PREP RESP, the sender's DSR will update the flow state information in the Q-FLIB.

All the steps in the above flow establishment process are shown in Figure 9. This process can be extended for arbitrary number of domains.

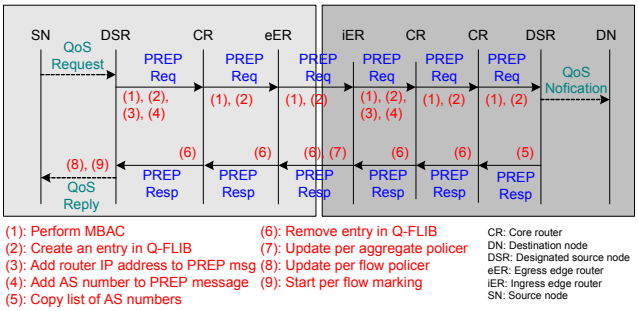


Figure 9. End-to-end Signaling.

Challenge 2: Inter-domain traffic policing

A source that violates its agreed traffic contract can negatively affect other flows. To avoid this, IQPM (Inter-domain QoS Provisioning Model) enables traffic conditioners at the domain boundaries to control incoming traffic. PREP signalling is used to update and maintain the traffic conditioners at the domain ingress routers. A PREP REQ packet, in addition to the flow traffic profile, registers Autonomous System (AS) numbers in its the path between the source and the destination. This information is copied to PREP RESP packets in the opposite direction. Edge routers use the list with the AS numbers to identify the incoming and outgoing administrative domains of the path. Based on this information, edge routers update the traffic conditioners (Figure 9). For scalability reasons, traffic conditioning is performed on a per-traffic aggregate. Traffic profile information is stored in the local Q-FLIB but it is not used for data forwarding.

Challenge 3: Monitor traffic guarantees

After receiving a positive PREP RESP message, the sender's DSR indicates to the end-user via signalling to start injecting traffic into the network. In addition, the DSR enables a traffic conditioner that controls incoming traffic and, in case of profile violation, packets are discarded. Internal core routers do not perform any policing. Edge routers monitor the aggregate traffic that crosses the domain boundaries and perform per aggregate and per AS policing. Traffic guarantees are not expected to be violated, as appropriate resources are allocated and misbehaving sources are controlled at the edge of the network.

The sender node (or a delegated router) interleaves monitoring packets within data packets of each flow. Each ingress router in the multi-domain path inserts its IP address in the source DSR. In addition, each internal core router just copies monitoring packets into its local memory, called monitoring cache (MC), and then forwards them.

Challenge 4: Handling rerouted traffic

In case of a network or node failure, portion of the traffic is rerouted causing congestion to some links. The following paragraphs explain how to protect legitimate (non-rerouted) traffic from rerouted traffic. In case of congestions, our target is to minimise the number of flows experiencing service degradation.

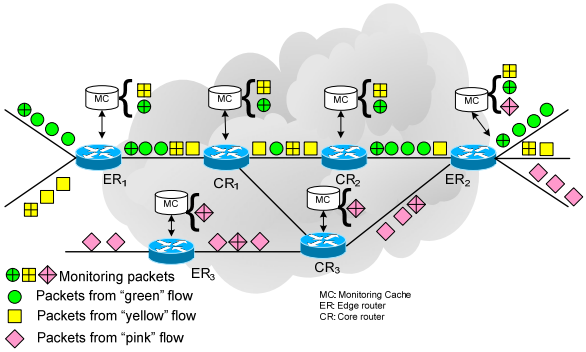


Figure 10. Handling monitoring packets by ingress and internal routers in a domain.

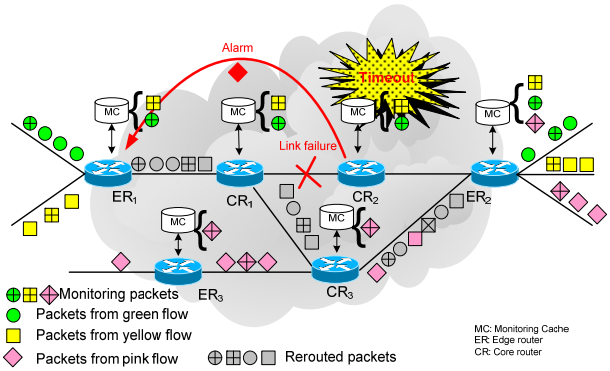
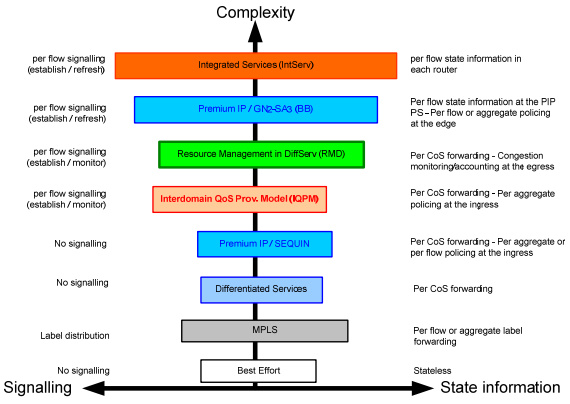


Figure 11. Generating alarms after a traffic reroute.

The entries in the monitoring cache continuously expire. If the corresponding validity timer of an entry expires, an alarm message towards the ingress edge router is generated. As long as the flow is active and the forwarding path is not changed, the reception of consecutive monitoring packets will reset the validity timer and no alarms will be generated.

Assume that a link failure causes flows paths to change, as shown the previous figure. Any router that does not belong in the new path will not receive any more monitor packets. The validity period for entries involved in the failed path will expire and ALARM packets will be generated. The edge router upon reception of these alarms identifies the rerouted flows and starts remarking their packets to a lower forwarding priority. This procedure protects original traffic (i.e., on the links prior to congestion being experienced) in congested links against any rerouted traffic inside the current domain. Note that the egress router restores the DSCP value of re-routed packets prior to forwarding them to the next domain.

Scalability, Stability and Complexity Issues



The proposed approach for QoS provision in DiffServ networks is scalable, since it follows fully distributed techniques and does not assume the existence of centralised entities. End-to-end mechanisms are used for admission control while node-local mechanisms are used for resource management. The approach is also stable since, for any new flow in the network, information regarding available resources in the end-to-end path is collected prior to acceptance of the flow. Furthermore the established signalling, monitoring and management mechanisms that are developed assure the stable operation of the network. The following diagram compares the IQPM approach with similar frameworks or architectures in term of complexity, signalling and state information overhead, such as IntServ, DiffServ, Premium IP/Sequin [R03], RMD [W02].

Validation of the proper functionality of the described QoS provision mechanisms is provided through an extended set of simulations. A part of this set is presented in the following section. Finally, focus is given on the reduction of the overall network complexity through the design of specific autonomic behaviours. Self-management is achieved, since routers are enabled to independently control the establishment of new flows and police their traffic at the domain boundaries according to administrators' policies. Self-optimisation is also provided in case of failures in the network or violations of performance guarantees.

Numerical Results

Simulation experiments using network simulator-2 (NS-2) [BJS00] were performed to estimate the performance of IQPM in failure conditions, in terms of the number of high priority flows affected after a link failure. We used the network topology, as shown in Figure 12, which is a simplified topology of GÉANT network. In each core node, ten end-systems were attached (not shown), each of them generating sequentially multiple UDP flows of 150Kbps at constant bit rate (CBR). The link capacity was set to 1 Mbps and, thus, it could sustain up to 6 concurrent flows without over-subscription. We considered three traffic services; a *high priority service* such as Premium IP - PIP, a *middle priority service* used only for rerouted high priority traffic, and a *best effort (BE)* service. Weighted Round Robin (WRR) queue scheduling was used to isolate traffic from different classes and to provide diverse packet loss guarantees to each class. Admission control mechanisms rejected flow establishment whenever link utilisation exceeded 85% of the link capacity. Therefore, under normal conditions core links were never oversubscribed, which avoided packet losses due to buffer overflows.

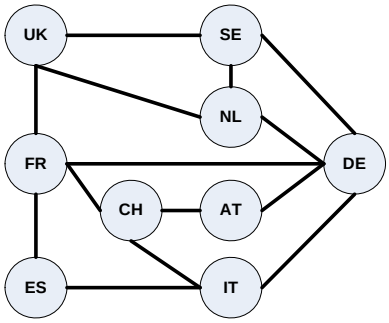


Figure 12. Planar graph of simulated topology

Two sets of simulations were performed; one with mean link availability of 99% and one with 99.8%, respectively. During our tests, each link failed only once and never did two links fail simultaneously. Failures caused traffic to be rerouted in the core network and, therefore, some links were temporally congested. The portion of rerouted flows as compared to the active flows varied from 10% to 40%, as shown in Figure 13. Congestion caused buffer overflow, thus high priority flows experienced some packet loss. Congestion was gradually reduced as admission control mechanism rejected the establishment of new flows. Still, multiple high priority flows were impacted after each link failure.

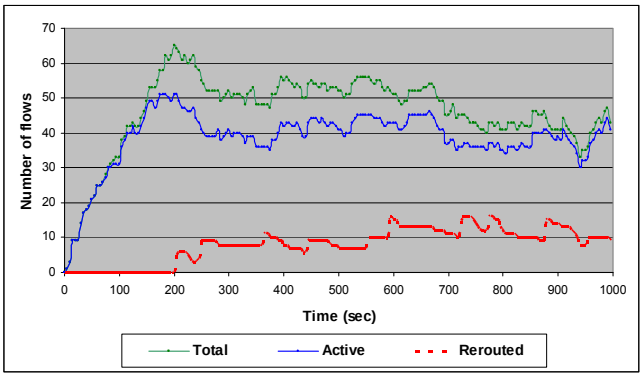


Figure 13. Typical diagram of rerouted flows during a simulation iteration

The performance parameter measured was the percentage of high priority flows that experienced negligible packet loss. In all simulation tests, flows were categorised into three groups according to the achieved performance; Excellent (with packet loss <0.1%), Limited, and Unacceptable (with packet loss >3%). Therefore, all the high priority flows that achieved the target performance guarantees were categorised in the "Excellent" group. We compared four cases, employing different admission control and monitoring mechanisms: In the first, no admission control was enabled and end-systems could inject traffic to the network without any restriction. The second case involved the IntServ framework, where admission control is required prior to a new flow establishment. The third case was based on IQPM with both admission control and monitoring mechanisms being activated. Timeout period for the monitoring cache entries was set to 3 seconds and rerouted flows were (re)marked to middle priority class. The last case simulates a situation, where an ideal "bandwidth broker" remarks, instantaneously, all the traffic that was rerouted.

In Figure 14 and Figure 15, we show performance guarantees for high priority traffic for link availability 99% and 99.8%. When no admission control was enabled, approximately 60% of the flows did not achieve the target performance. When admission control was enabled (IntServ case), the number of flows achieving the target performance significantly increased to approximately 70%, as shown in Figure 16. The admission control mechanisms cannot alleviate the side effects caused by the rerouted traffic and, thus, 3/10 of the flows achieved medium or low performance guarantees. When supplementary monitoring mechanisms were activated (IQPM case), the number of flows within target further increased by 8,8%-10,7%, up to 75,55%-81,22% for link availability 99% and 99.8%, respectively. As rerouted traffic was remarked to lower priority, non-rerouted flows in target reached 85,25%-86,59% (see Figure 17). In the BB case, the non-rerouted flows within target reached 85,71%-87,91% (see Figure 17). It should be noted that a link failure reduces the network resource and, thus, it is impossible to avoid service degradation for some of the high priority flows.

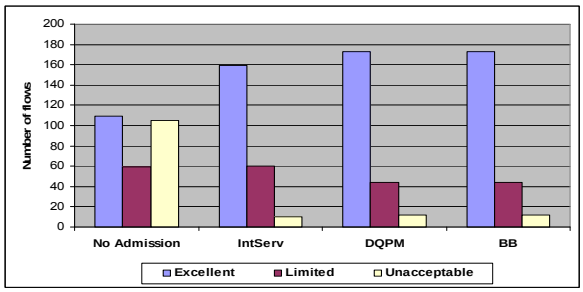


Figure 14. Flow performance for link availability 99%

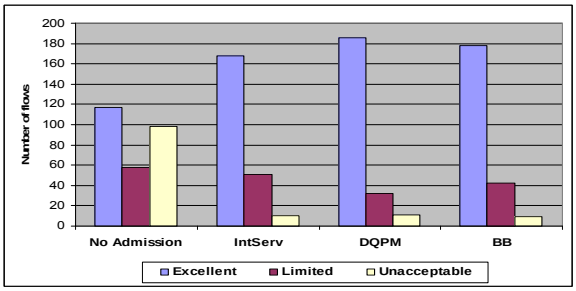


Figure 15. Flow performance for link availability 99.8%

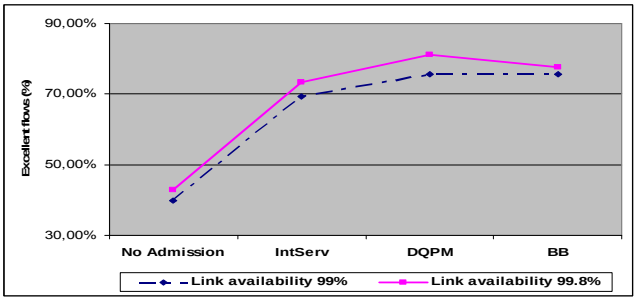


Figure 16. Percentage of flows achieved target performance guarantees (packet loss < 0.1%)

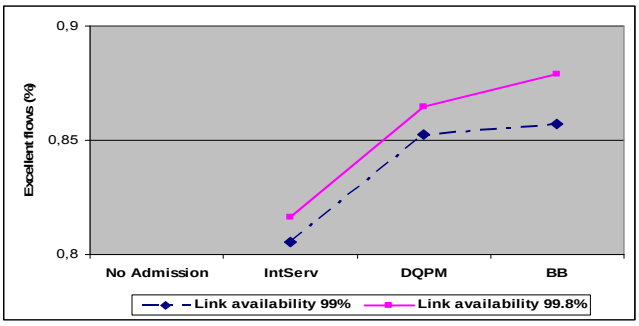


Figure 17. Percentage of non rerouted flows achieved target performance guarantees (packet loss < 0.1%)

2.3 QoS-aware Resource Management over Integrated Heterogeneous Wireless Networks

2.3.1 QoS provisioning in autonomic CDMA networks through a Common Utility-Based Framework

Introduction. With the growing demand for high data rate and support of multiple services with various quality of service (QoS) requirements, the scheduling policy plays a key role in the efficient resource allocation process in future wireless networks. Due to the inherent characteristics of wireless communications, users experience time-and-location dependent channel conditions, which limit system's available resources and its ability in satisfying their QoS requirements. Therefore, a flexible power and rate allocation scheme is essential for optimising system's performance. Our goal is to study and devise autonomic mechanisms towards achieving optimal radio resource utilisation over a heterogeneous CDMA cellular network subject to various services' QoS requirements. In order to accomplish our goals, we initially analysed basic users'

services QoS prerequisites and mapped them to appropriate utility functions. The utility function reflects a user's degree of satisfaction with respect to his service performance, and therefore services with assorted QoS prerequisites can be represented by forming appropriate utility functions. In this way, we adopted and exploited a common utility based framework in order to reflect in a unified normalised way various and often diverse users' QoS prerequisites, under common optimisation problems. Afterwards, we set appropriate QoS-aware resource allocation utility-based non-convex optimisation problems, both for the downlink and the uplink of a CDMA cell. Moreover, appropriate mathematical techniques in order to solve the corresponding problems have been proposed, leading to appropriate downlink/uplink power control algorithms that will obtain the solution of the proposed resource allocation and QoS management problems. Finally, issues of stability, scalability and complexity of the proposed scheme is discussed and then the proposed autonomic approaches are validated via analysis and simulation.

Problem's Statement

A. System Model

We consider the downlink and the uplink of a single cell time-slotted CDMA wireless network with N continuously backlogged users at time slot t respectively, where S denotes their corresponding set. The corresponding path gain of each user at time slot t is denoted by $G_i(t)$. In the following, assuming fixed users' channel conditions within the duration of each time slot, we omit the notation of the specific slot t in the notations and definitions we introduce. At the beginning of each time slot, system's (i.e., a cell's) resource scheduler, residing at the base station, in collaboration with attached mobile nodes' QoS support mechanisms, are responsible of making decisions on nodes' transmission power and resulting rate in a distributed manner.

We consider two types of users in accordance to requested services, namely non-real-time *(NRT)* users requesting delay-tolerant high-throughput services (i.e., data users) and real-time *(RT)* users with strict short-term QoS constraints (i.e., voice/video conference users). The number of NRT users (*RT* users) is denoted by N_{NRT} (N_{RT}) and by S_{NRT} (S_{RT}) we denote their corresponding set. Furthermore, due to the need for supporting multiple services with various QoS requirements, each user i is associated with a proper utility function U_i which reflects in a normalised way his degree of satisfaction with respect to his service performance. A user's utility function U_i differs in the case of downlink and uplink, even if his service type is the same, due to the diverse power and rate physical limitations imposed in each case [KP08_1], [KP08_2]. In the uplink [[KP08_2], users have individual transmission power and rate upper bounds (i.e. $P_i \le P_i^{Max}$ and $R_i \le R_i^{Max}$), while in the case of downlink only base station's transmission power limitation P_{max} affects system's capabilities [KP08_1].

We denote by R_i the transmission rate and by P_i the transmission power of user i in the slot under consideration. Moreover, we denote by $\gamma_i = E_b/I_o$ the bit energy to interference density ratio of user i, by θ the orthogonality factor and by W the system's spreading bandwidth.

B. The Downlink Case

Regarding the downlink of the CDMA cell, in order to efficiently reflect various services QoS prerequisites at the scheduling policy, we define users' utility functions as follows [KPKD07]:

$$U_i\left(R_i,\bar{P},a_i,b_i\right) = R_i f_i\left(\gamma_i,a_i,b_i\right) \quad i=1,..,N \tag{1}$$

expressing their degree of satisfaction in accordance to their actual expected downlink throughput [KPKD07], [KP08_1]. Function f_i represents a function for the probability of a successful packet transmission for user i and is an increasing function of his bit energy to interference ratio γ_i at any time slot, and can be represented by a sigmoidal-like function of his power allocation for various modulation schemes. Parameters a_i and b_i are variables that define utility function's shape [KPKD07]. With respect to delay-tolerant non-real time users, utility (1) properly expresses their desired actual throughput (i.e., goodput) maximisation. On the other hand, the QoS requirements

of real-time users consist mainly of a constant downlink rate and short-term throughput guaranties. Therefore, we consider as a real-time user's performance indicator the achieved probability of receiving an amount of service, in terms of data units, smaller than a predefined threshold within successive observation time intervals [KPKD07], i.e.

$$\Pr[\hat{\beta}_{RT,i}(t) \le B_{RT,i}]_{W_i} \quad \forall t \ (slot) \ \ \forall i \in S_{RT} \tag{2}$$

where W_i denotes a RT user's i observation time interval in terms of slots, $B_{RT,i} = R_{RT,i} \cdot W_i \cdot t_s$ denotes his predefined data units threshold and $\hat{\beta}_{RT,i}(t)$ the amount of data he received within a specific time interval from slot *(t-W_i+1)* to slot *t*. The smaller the achieved value of a RT user's short-term throughput probability (2), the greater is his degree of satisfaction. To achieve this goal, dynamically adapted real-time users utilities, based on (1), via the introduction of tunable b_i parameters have been proposed in [KPKD07]. As to reflecting the scheduling policy, the previous short-term requirement, we allow RT users to dynamically adopt their utility functions in accordance to the fulfilment of their QoS prerequisites. This adaptation mechanism enables these enhanced autonomic functionalities towards self-optimising their service performance.

In order to optimise the overall system performance as well as users' QoS-aware degree of satisfaction, the following utility-based power and rate allocation optimisation problem must be solved at the scheduler at every time slot [KPKD07], [KP08_1]:

$$\begin{aligned} &\max_{\bar{R},\bar{P}} \sum_{i=1}^{N} U_i^*(R_i, \bar{P}, a, b_i(t)) \\ &s.t. \ \ \sum_{i=1}^{N} P_i \le P_{\max} \\ &\quad 0 \le P_i \le P_{\max} \quad i = 1,2,...,N \\ &\quad 0 \le R_i \le R_i^{\max} \quad i = 1,2,...,N \end{aligned} \tag{3}$$

It can be shown that the optimal solution of problem (3) is achieved when the base station allocates all of its resources X_{max} to the users. Therefore, optimality is achieved when the following equality holds:

$$\sum_{i=1}^{N} P_i = P_{\max} \ . \tag{4}$$

Initially, the scheduler selects users to which non-zero resources will be allocated by using the information of their parameters' $\lambda_i^{\max}$ values. Parameter $\lambda_i^{\max}$ represents user's i maximum willingness to pay per unit of resource and is defined as the solution of the following users' independently solvable problems:

$$\lambda_i^{\max} = \min\left\{\lambda \ge 0 \,|\, \max_{0 \le X \le X_{\max}} \{U_i(P_i) - \lambda P_i\} = 0\right\} \tag{5}$$

In other words $\lambda_i^{\max}$ is the price λ that maximises user's i net utility $P(\lambda) = \arg\max_{0 \le X \le X_{\max}} \{U_i(P) - \lambda P\}$, i.e.

$$\lambda_i^{\max} = \begin{cases} \left.\dfrac{\partial U_i(P_i)}{\partial P_i}\right|_{P=0} & \text{if } U_i \text{ is concave} \\ \left.\dfrac{\partial U_i(P_i)}{\partial P_i}\right|_{P=P^*} & \text{if } U_i \text{ is a sigmoidal function and } P^* \text{ exists} \\ \dfrac{U_i(P_{\max})}{P_{\max}} & \text{otherwise} \end{cases} \tag{6}$$

where P_i^* is the unique positive solution of: $U_i(P_i) - P_i \dfrac{\partial U_i(P_i)}{\partial P_i} = 0$ *for* $0 \le P_i \le P_{\max}$.

C. The Uplink Case

For the uplink case, in order to express, in a common utility-based framework, a user's degree

of satisfaction in accordance to their service performance we define their utilities as follows [KP08_2], [KTP08]:

$$U(R_i^*, P_i, \bar{P}_{-i}) = \frac{T_i(R_i^*, P_i, \bar{P}_{-i})}{P_i} = \frac{T_i(R_i^F \cdot f_i(\gamma_i), P_i, \bar{P}_{-i})}{P_i} \quad (7)$$

where $R_i^* \equiv R_i^F \cdot f_i(\gamma_i)$ denotes user's i actual uplink transmission rate (i.e. *goodput*) during the time slot under consideration and R_i^F denotes the user's fixed designed transmission rate. User's i actual throughput utility T_i is employed to reflect, within the resource allocation algorithm, his degree of satisfaction. This satisfaction level is expressed in terms of service performance expectations and achieved QoS requirements for a given achieved goodput. In this way, in the uplink case, due to their limited power resources a user's utility expresses the expected trade-off between his utility-based actual uplink QoS-aware throughput performance, and the corresponding energy consumption per time slot t.

In general, a user's i actual throughput utility $T_i(R_i^*, P_i, \bar{P}_{-i}) \equiv T_i(R_i^*)$ is a nested (due to the existence of f_i), non-convex function of his achieved goodput R_i^*. Specifically, T_i is an increasing twice continuously differentiable function of R_i^* and with respect to user's service type, can be a sigmoidal-like, a strictly concave, or a strictly convex function of R_i^* within his corresponding definition set $[0, R_{Max,i}^*]$, where denotes user's i maximum goodput.

As the system evolves, at every timeslot each user aims at the maximisation of the expectation of his utility U_i, therefore the corresponding goal of user's i uplink power control algorithm in the uplink case can be defined as the following maximisation [TKP09_1], [TKP09_2]:

$$\max_{P_i} U_i = \max_{P_i} U_i(P_i, \bar{P}_{-i}) \quad \text{for } i=1,\ldots,N$$
$$s.t.\ \ 0 \le P_i \le P_i^{Max} \quad (8)$$

Let $G = [S, \{A_i\}, \{U_i\}]$ denote the corresponding non-convex non-cooperative game, where S is the set of all users and $A_i = [0, P_i^{Max}] \times \Re^N$ is the strategy set of the i^{th} user. Each player-user in game G picks a transmission power from his strategy set A_i and receives a payoff U_i in accordance to his best response policy $B_i(\bar{P}_{-i}) = \max_{P_i \in A_i} U_i(P_i, \bar{P}_{-i})$. The Nash equilibrium approach is adopted towards seeking the solution of the non-convex non-cooperative uplink power control game G and its existence and uniqueness are proved. The Nash equilibrium of the non-cooperative game (8) is given by $\bar{P}^* = \left(P_1^*, \ldots, P_N^*\right)$, where P_i^* is the unique global maximisation point of the overall user's i utility function, given by [TKP09_3]:

$$P_i^* = \min\{\frac{\gamma_i^*(R_{T,i}^* + MF_i) I_{-i}(\bar{P}_{-i})}{WG_i}, P_i^{Max}\} \quad \text{if } i \in S_{RT},$$

and by:

$$P_i^* = \min\{\frac{\gamma_i^* R_i^{Max} I_{-i}(\bar{P}_{-i})}{WG_i}, P_i^{Max}\} \quad \text{if } i \in S_{NRT}.$$

Furthermore, γ_i^* results from the unique positive solution of equation $(\partial T_i(\gamma_i)/\partial \gamma_i) \cdot \gamma_i - T_i(\gamma_i) = 0$.

Devising a QoS-Aware Autonomic Architecture via DEs

In this section, iterative and distributed power control algorithms for obtaining the optimal solutions of the proposed downlink/uplink resource optimisation problems at every time slot t are introduced and then mapped to their corresponding DEs (i.e., PROTO_LEVEL_NODE_R&Q_CDMA_DE and PROTO_LEVEL_BS_R&Q_CDMA_DE). Concerning the downlink of a CDMA wireless network a power and rate allocation scheme is presented, which is realised by the efficient collaboration of two low complexity algorithms residing at each mobile node and the base station, respectively. From mobile nodes' perspective,

the proposed algorithm introduces a control loop towards enabling their QoS-aware self-optimisation, while at the base station realises a flexible algorithm to obtain optimal users' power and rate vectors for the subsequent time slot.

Downlink Power and Rate Control Algorithm

At Base Station (A Resource Scheduler)

Step_1: The scheduler requests users' utility functions.

Step_2: The non-convex power and rate optimisation problem (3) is re-defined with respect to the current users' utilities.

Step_3: Users selection is performed for the current optimisation problem.

Step_4: Users' allocated downlink power and rate are estimated for both non-real-time and real time users.

At Mobile Nodes (A Control Loop)

Step_1: Information Monitoring: A user computes the actual amount of data units that has received within his current observation time interval.

Step_2: Information Analysis: Determines his need for accessing system resources with respect to his QoS prerequisites.

Step_3: Decision Making towards Self-Optimisation: Reflects his QoS requirements and resources expectation at the scheduler by adjusting his utility function and then, disseminates this information at the base station.

The second part of the previous algorithm is developed on each node's PROTO_LEVEL_NODE_R&Q_CDMA_DE while the first part is developed on PROTO_LEVEL_BS_R&Q_CDMA_DE.

Explicitly, PROTO_LEVEL_NODE_R&Q_CDMA_DE dynamically adapts mobile user's utilities by constantly monitoring users' service performance, analysing their current status with respect to QoS requirements, and reacting on QoS triggering events via the dynamic alteration of the users' utilities. Moreover, PROTO_LEVEL_BS_R&Q_CDMA_DE enables QoS-aware resource allocation mechanisms, by realising optimal self-adapting radio-resource (e.g., power and rate) allocation procedures. These procedures simultaneously satisfy various, and often diverse, users' service QoS prerequisites, residing at autonomic wireless network cell's base stations.

Concerning the uplink of a CDMA wireless network, an iterative and decentralised uplink power control algorithm is presented for reaching the Nash equilibrium of the proposed non-cooperative game *G* in [TKP09_3].

Uplink Power Control Algorithm

At Base Station (A Resource Scheduler)

Step_1: At the beginning of time slot *t*, all the users transmit with an arbitrary initial power.

Step_2: The base station collects the transmission power of the mobile users, calculates overall cell's interference and broadcasts this information back to the users.

At Mobile Nodes (A Control Loop)

Step_1: At the beginning of time slot *t*, user *i*, $i \in S$ transmits with an arbitrary initial power.

Step_2: Given the uplink transmission powers of other users, which is implicitly reported by the base station when broadcasts its overall received interference, the user computes his interference at the base station and then refines his transmission power.

Step_3: If the powers converge, then stop.

Step_4: Otherwise, go to step 2.

The first part of the proposed decentralised uplink power control algorithm resides at PROTO_LEVEL_BS_R&Q_CDMA_DE and the second part resides at PROTO_LEVEL_NODE_R&Q_CDMA_DE. Specifically, as it is illustrated in Figure 18 PROTO_LEVEL_BS_R&Q_CDMA_DE is responsible to gather the information of users' transmission power, compute the overall interference in the network and broadcast this information to the users. On the other hand, a mobile node's PROTO_LEVEL_NODE_R&Q_CDMA_DE realises a self-adaptation mechanism – with respect to QoS-aware self-optimisation – in terms of a node's local control loop that: a) constantly monitors a user's service performance as well as the corresponding environment changes, b) analyses his current status with respect to QoS requirements and, c), reacts to QoS triggering events towards optimising his service performance. In addition, PROTO_LEVEL_BS_R&Q_CDMA_DE can exploit users' satisfaction of their QoS requirements, combined with their modulation and coding schemes, as a call admission control criteria, in order to accept serving a user with fixed QoS prerequisites ([TKP09_3]).

The importance of such a decentralised autonomic approach relies on the enhanced self-adaptation capabilities attributed to the wireless nodes. Such an architectural design approach favours the exploitation of future wireless environment's heterogeneity by users with multimode capabilities, since in most cases only the mobile nodes have the complete view of their own environment, in terms of available access networks in their locality, corresponding available resources and QoS supporting mechanisms.

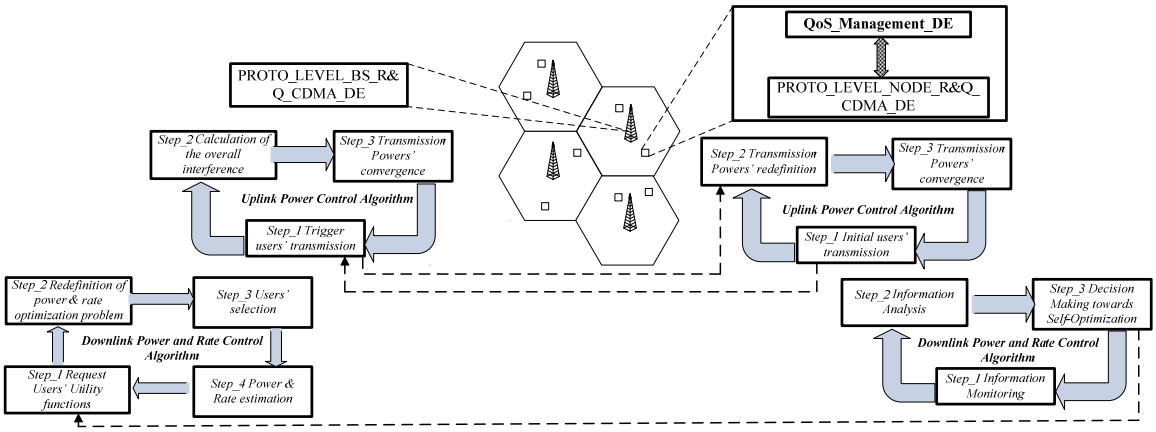


Figure 18. Proposed autonomic architecture PROTO_LEVEL_BS_R&Q_CDMA_DE and PROTO_LEVEL_NODE_R&Q_CDMA_DE and corresponding control loops

Scalability, Stability, Validation and Complexity Issues

The proposed iterative and distributed power control algorithms for obtaining the optimal solutions of the proposed downlink/uplink resource optimisation problems is designed and built under common principles, not only regarding their autonomic attributes (i.e., GANA), but also harmonise and cooperate with 3GPP, adding minimum overhead and monitoring information exchange. Specifically, as discussed in the previous section each part of each algorithm resides either at the base station or at the node, operates autonomically and both algorithms concerning the downlink and the uplink are of low complexity, (i.e., *O(N)*). Concerning the algorithms' as well as the corresponding optimisation problems' stability, the convergence of each algorithm, concerning the uplink and the downlink has been proven in [TKP09_3] and [KPKD07], [KP08_1], respectively. Finally the performance and effectiveness of proposed approaches is evaluated in the next section.

Numerical Results

In this section we provide some initial numerical results illustrating the operation and performance of the proposed autonomic architecture, concerning both the downlink and uplink. Throughout our study we consider a single cell time- slotted CDMA system, supporting *N=30* continuously backlogged users. Each simulation lasts *10.000* time slots.

Figure 19 illustrates the total actual average throughput as a function of the number of RT users in the system, concerning the downlink and the uplink for both NRT and RT users, while Figure 20 presents their corresponding average utility performance. The results shows that for both NRT and RT users, their QoS expectations are fulfilled in terms of high throughput performance and fixed transmission rates (i.e., *512 Kbps*), respectively. We can observe that concerning the downlink a RT user's average received throughput is almost fixed, independent of their number in the system, due to their self-adaptation attribute that steers them to request system resources to RT users up to the point where their required streaming throughput is satisfied. Moreover, a NRT user's average received throughput increases as the number of NRT users in the system decreases because the degree of competition among them for the excess system resources decreases as well, which is an inherent characteristic of any opportunistic scheduler. Similar observations are made for the case of the uplink as well. Finally, the results reveal that via the proposed autonomic architecture the system maintains high performance, in terms of overall utility maximisation. This implies user's QoS prerequisites fulfilment, while avoiding scalability vulnerability issues by providing users enhances self-adaptation flexibilities.

The presented novel autonomic QoS-aware resource allocation architecture aims to jointly and proficiently support multiple services in both the downlink and the uplink of a CDMA wireless network. While working towards achieving our goal, we adopted the analytic solutions of the above resource allocation optimisation problems developed in our works [KPKD07]-[KP08_1], within the framework of an autonomic architecture.

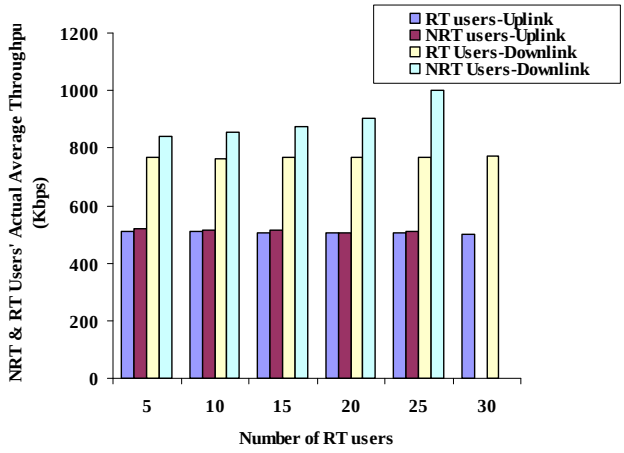


Figure 19. NRT and RT users' actual average received throughput

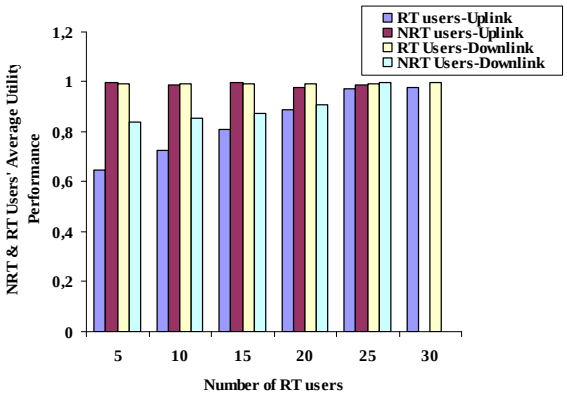


Figure 20. NRT and RT users' average utility performance

2.3.2 QoS provisioning in autonomic WLANs under a Common Utility-Based Framework

With the growing requirement to support various applications, including multimedia applications, efficient QoS provisioning has become an important research topic in WLAN. However, due to the intrinsic features of WLAN and the heterogeneous wireless access network environment, QoS provisioning quickly becomes a complex task. Specifically, in order to optimise the resource utilisation of the whole system, QoS provisioning may not only relate with the resource utilisation in WLAN, but also affect the resource allocation in other wireless access networks, such as CDMA, in case where both access technologies co-exist. In this section, we discuss QoS provisioning in WLAN based on a utility-function framework. Our goal is to study and devise autonomic mechanisms towards achieving optimal resource utilisation in WLAN and thus, set the foundations of the autonomic joint resource allocation and network selection mechanisms over integrated CDMA/WLAN systems (an architecture emerging within EFIPSANS, [D3.2_Appendix I]).

QoS Provisioning under a Common Utility-based Framework

A. Applications and Utilities

The utility of an application is defined as a metric for users to measure the general degree of satisfaction of a user with respect to his applications' performance. It can also be defined as the degree of resources allocated to him, when the application executes in a certain environment, i.e., under certain resource conditions.

Because of the complexity of applications and their algorithms, as well as the control parameters for each algorithm, it is difficult to give a general form of utility function to all applications in terms of different resource dimensions. However, according to the above assumptions, some common properties of the utility functions associated with each resource dimension can be summarised as follows:

- Non-decreasing: typically, the increase of a type of resource does not decrease the application performance. This makes the utility function a non-decreasing function of each resource type.
- With maximum extreme value: basically, the utility of an application will rise with the increase of the amount of resources consumed by the application. However, when the amount reaches a definite value, the performance will not increase.
- Always have definition in the bounded interval $[r_{min}, r_{max}]$. The utility function of an application may not be continuous in the range $[r_{min}, r_{max}]$, however, it can be piecewise continuous.

For simplicity, in this section, we consider only one resource dimension, namely network bandwidth. Note that we use the variable R (data rate of an application) to denote the network bandwidth resource that the application obtains (is allocated to the user). In addition, we suppose that the utility function is twice continuous differentiable in the range $[r_{min}, r_{max}]$.

B. QoS and Resource Allocation in WLAN based on Utility

Consider a modification of the IEEE 802.11e standard, presented in [BPO03] which allows for the provisioning of throughput guarantees in WLANs. The dominant media access control (MAC) protocol in IEEE 802.11e is Enhanced Distributed Channel Access (EDCA), a carrier sense multiple access control protocol with a collision avoidance mechanism (CSMA/CA). EDCA controls the access to the wireless channel on the basis of the channel access functions (CAFs). Each CAF executes an independent back off process to determine the time of transmission of its frames. A mobile user that intends to transmit a new packet has to sense the channel as idle for a minimum duration, called Arbitration InterFrame Space ($AIFS_i$). Once the channel is sensed idle for $AIFS_i$ the user generates a backoff interval before transmitting, which is randomly selected from the range $(0,CW_i)$, where CW_i is the contention window, in order to minimise the probability of collision with other packets transmitted by other stations. At the first transmitting attempt, CW_i is assigned a value CW_{min}. If the transmission is not successful due to collision, the value of CW is doubled up to a maximum value CW_{max}. After a successful transmission, the CAF is allowed to transmit several consecutive frames, the only restriction being that it cannot occupy the channel for a period of time longer than the transmission opportunity limit parameter ($TXOPlimit_i$).

IEEE 802.11e allows specific parameters that affect the performance of a user j, including minimum contention window $CW_{min,j}$, maximum contention window $CW_{max,j}$, Arbitration InterFrame Space ($AIFS_j$) and $TXOPlimit_j$, to be altered by the access point and communicated to the user. Furthermore, a plethora of QoS-aware resource allocation mechanisms proposed for WLANs in the literature initially set a system's bandwidth optimisation problem, identify the interrelation between users' bandwidth and one of the above tuneable parameters, and then propose heuristics for computing them [BPO03], [F07], [JK07] and [YWK07].

Therefore, given a system's maximum effective capacity C_{max} [YWK07], according to the common utility-based framework the corresponding non-convex optimisation problem for WLAN can be formally defined as:

$$\begin{aligned} &\max_{\bar{R}} \sum_{j=1}^{N_{WLAN}} U_j(R_j) \\ &s.t.\ \sum_{j=1}^{N_{WLAN}} R_j \le C_{\max},\ 0 \le R_j \le C_{\max}\ \ j \in S_{WLAN} \end{aligned} \tag{9}$$

where S_{WLAN} is a set of N_{WLAN} continuously backlogged users attached to a specific WLAN. Problem (9) can be solved by applying the same methodology followed in section 2.3.1, in the downlink case of a CDMA network, towards solving the corresponding non-convex optimisation problem. Subsequent to the computation of users' optimal rate vector $\bar{R}^* = \{R_1^*,...,R_i^*,...,R_{N_{WLAN}}^*\}$, resulting from (9), we can derive a proper unique contention window set $CW^* = \{CW_1^*,...,CW_i^*,...,CW_{N_{WLAN}}^*\}$ that meets the throughput requirements for the N_{WLAN} users, i.e.

$$\begin{aligned} &CW_j^* : R_j \ge R_j^*\ \ \forall j \in S_{WLAN} \\ &s.t.\ \sum_{j=1}^{N_{WLAN}} R_j \le C_{\max}, \\ &0 \le R_j \le C_{\max}\ \ j \in S_{WLAN} \end{aligned} \tag{10}$$

via the proposed algorithm in [BPO03] that aims at a) providing the committed throughput guarantees; and b) accepting as many requests as possible (i.e., derives the solution of problem (10)). Intuitively, optimality in terms of accepted number of users is achieved only when the equality in (10) holds, leading users to attain the desired optimal transmission rate derived in problem (9). Moreover, due to the imposed constraint $\sum_{j=1}^{N_{WLAN}} R_j \le C_{\max}$ in (9) which ensures that $\sum_{j=1}^{N_{WLAN}} R_j^* \le C_{\max}$, the contention window set CW^* is always feasible. To make use of (9) and (10), we assume that each user j may alter his contention window after the network reaches a steady state, i.e., a quasi-stationarity assumption about the network state, as in [JK07]. We refer to the latter short-term time period as WLAN's time-frame (T_f).
Note that the above algorithm is about a single WLAN. The algorithm can also be extended to the case when multiple WLANs exist.

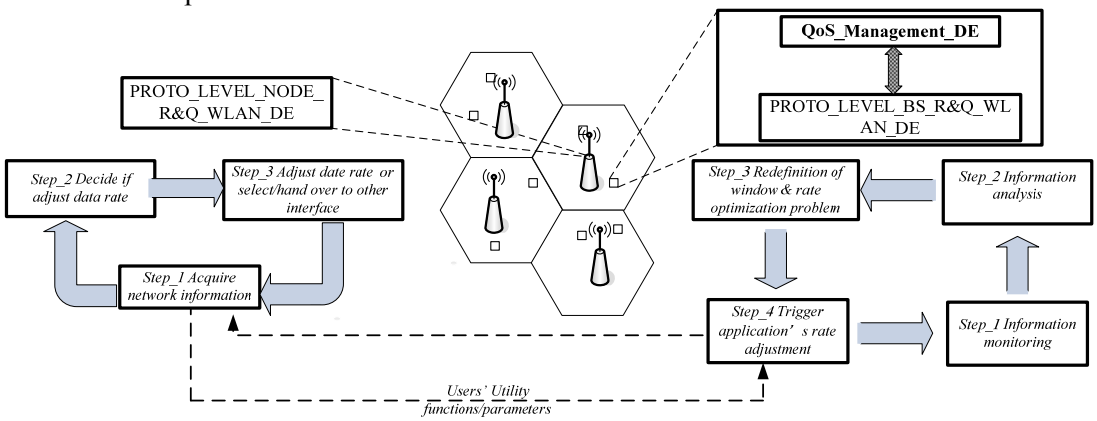


Figure 21. WLAN QoS related decision elements (DEs) and control loops in GANA

C. Autonomic QoS Management in GANA

Via adopting the above utility-based framework and solving the corresponding optimisation problems (9) and (10), distributed QoS provisioning mechanism where derived towards enabling autonomic resource management in WiFi networks. Thus, in accordance to GANA the previous mechanism were mapped into the corresponding decision making elements, namely PROTO_LEVEL_NODE_R&Q_WLAN_DE and PROTO_ LEVEL_BS_R&Q_WLAN_DE.

As shown in Figure 21, at the access point, the PROTO_LEVEL_BS_R&Q_WLAN_DE realises the self-adaption and self-optimisation logic through a control loop, that (1) monitors the network status information, e.g., the total number of applications and their utility functions in the system, and (2) analyses if the system resources need to be re-allocated when new (including handover) applications come in. If yes, it (3) redefines the rate optimisation problem (9)-(10) and (4) triggers the adjustment of the application's data rate through adjusting their contention windows. Note that the PROTO_LEVEL_BS_R&Q_WLAN_DE may exchange some information with QoS_Management_ DE for the optimisation of the whole heterogeneous wireless system (for details we refer to Appendix I [D3.2_Appendix I]).

At the mobile node side, the PROTO_LEVEL_BS_R&Q_WLAN_DE realises the self-adaptation logic through (1) acquiring the current network status, (2) deciding if it should adjust the data rate of the corresponding application (3) triggering the adjustment of the data rate or selecting/handing over to other network interfaces.

Scalability, Stability, Validation and Complexity Issues

The proposed autonomic mechanisms are implemented in the mobile nodes and the access points of WLAN. Regarding the optimisation algorithm, we borrow some mature and low complex algorithms from [BPO03], [F07], [JK07] which also will not affect the stability of the

system. In addition, we use the "in-band" method to transfer applications' utility function to each access point, and the utility functions are denoted using several parameters, which introduce only minimum network overhead. This will not cause any scalability problem.

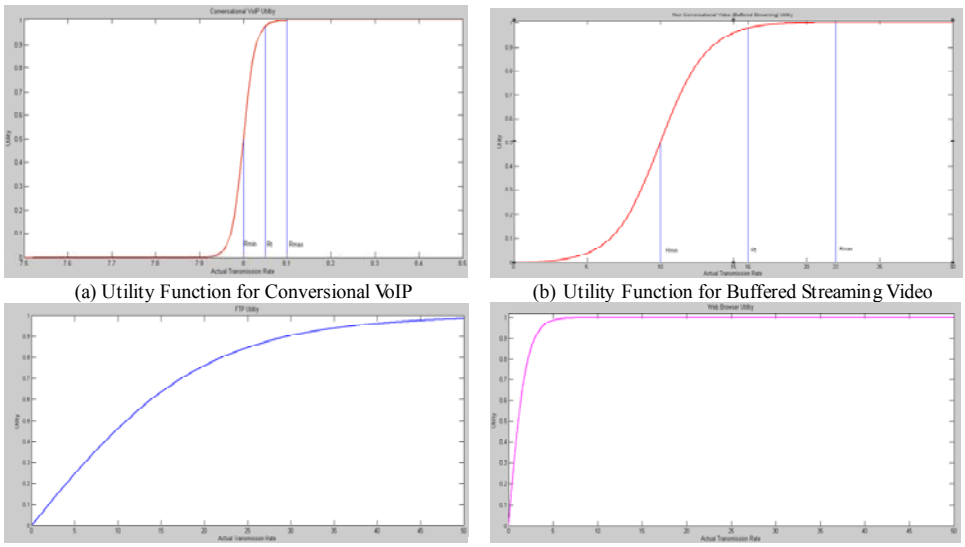
Numerical Results via Simulations

We use a common definition of the utility function based on the sigmoid function, as shown in Eq. (11).

$$U(r) = \alpha\{\frac{1}{1+e^{-a(r-b)}} - \beta\} \quad \text{where} \quad \alpha = (1+e^{ab})/e^{ab},\ \beta = 1/(1+e^{ab}) \tag{11}$$

In Eq. (11), a and b reflect the type and the intrinsic resource requirements of the application. α and β are constants that normalise the utility's value. If an application is a real-time or streaming application that has fixed QoS requirements, r_{min} decides the parameter b, and $b>0$; while r_{max} decides the parameter a. In others words, once the flow's QoS requirements are fixed, the corresponding utility function can be obtained by converting r_{min} and r_{max} into a and b. Similarly, given an application's utility function, the corresponding r_{min}, and r_{max} of the application can be obtained.

In case of the best-effort flows or elastic flows that do not have fixed QoS requirements, b should be equal to zero, and the flows' intrinsic features and relative priority decide the value of a. E.g., if a user prefer web browsing (WWW service) to file transfer (FTP service), the value of a for the web browsing flow will be larger than that of the file transfer flow.



(a) Utility Function for Conversional VoIP

(b) Utility Function for Buffered Streaming Video

(c)Utility Function for FTP Service

(d) Utility Function for Web Browsing Service

Figure 22. Utility function of typical applications

Figure 22 illustrates the utility functions of some typical applications. From this figure we can see that the utility function can clearly reflect not only the features of an application, but also the resource requirements of the application as well as the adaptability of the applications. This builds a solid base for devising autonomic mechanisms towards achieving optimal resource utilisation in WLAN. Moreover, an application can decide how much network resources it may require, given a certain price of the resource, according to its utility function. On the other hand, the network can determine the price of the resource dynamically, according to the utility functions of the applications that are using the resources and the total resource capacity in the network.

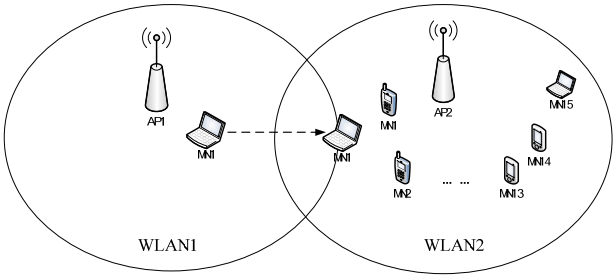
Simulations have been performed to evaluate the proposed algorithms using Network Simulator-2 (NS-2). As shown in **Figure 23**-(a), two WLANs were formed by using two access

points (APs). We selected IEEE 802.11e for the WLANs on account of its QoS support. In the first experiment, we concentrated on one WLAN (i.e., WLAN2 in **Figure 23-**(a)). Forty five flows of VoIP, Video and FTP/HTTP (background) run on *15* mobile nodes at time point *t=0s*. The bandwidth requirement, the utility function of each flow, and their corresponding QoS category (i.e. min, max. contention window size in 802.11e) are summarized in **Table 3**.

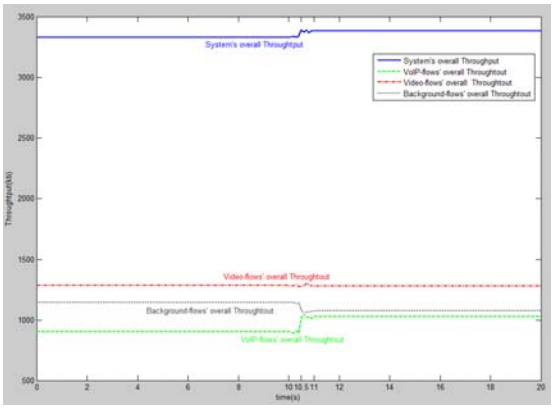
Table 3. Basic setting of flows in the simulation

Flow type	*Number of flows*	*Bandwidth requirement of each flow*	*Parameters of utility function*	*QoS category*	*Min CW*	*Max CW*
VoIP	13	64kbps	a = 76.005, b = 8	AC3	16	64
Video	10	128kpbs	a = 0.6034, b = 10	AC2	16	256
Background	22	52kpbs	a = 0.5,b = 0	AC0	32	1024

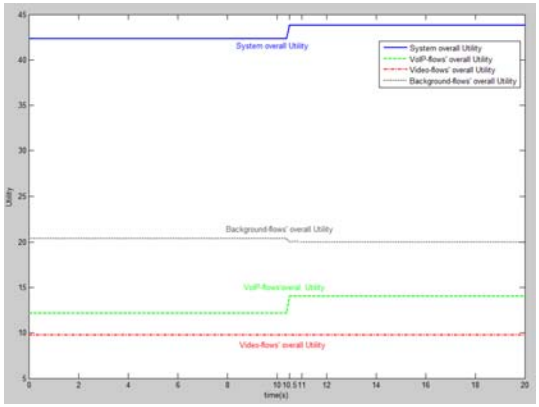
At time point *t=10s*, two new flows are requiring to be serves, which triggered the optimization algorithms. **Figure 23-**(b) and (c) illustrates the system throughput and utility before and after the operation of the proposed optimization algorithm. The results show that both the utility and the throughput of the existing background flows decreased, whereas new flows with higher priority can still be accepted in case of resource scarceness. That means that the system can satisfy the needs of as much applications as possible.



(a) Simulation Topology



(b) System throughput



(c) System utility

Figure 23. WLANs Scenario, simulation topology, system throughput and overall utility

In the second experiment, we consider the case where two WLANs that partially overlap each other. We assume that the mobile node (MN1) stays in WLAN1 at the beginning, and then moves towards WLAN2 at time point *10s*. Then, at time *35s*, the mobile node enters WLAN2, whereas still in the coverage area of WLAN1 simultaneously. Finally, the mobile node stops moving, till

simulation ends at time *50s*. In this simulation, two applications run on top of the mobile node from beginning to the end. One is voice over IP (VoIP) with utility function parameters (*a=1.0860, b=72*), and the other is FTP with the utility function parameters (*a=0.1, b=0*).

Figure 24a and Figure 24b illustrate the throughput and utility of two applications using the proposed mechanism. If the self-adaptation and optimisation algorithm is not used, both the VoIP and FTP applications will always stay in WLAN1, and the throughput of VoIP and FTP application is about 80kb and 150kb, respectively. When the algorithm with bandwidth optimisation consideration is applied, the VoIP application decides to attach to WLAN2 due to the heavy traffic in WLAN1. However, this makes WLAN2 become more crowed after the attachment of the VoIP application, whereas the traffic in WLAN1 becomes more lighter at the same time, so the FTP application select WLAN1 finally. From the result we can see that the throughput of VoIP and FTP application is up to 116.7 and 215.4, respectively.

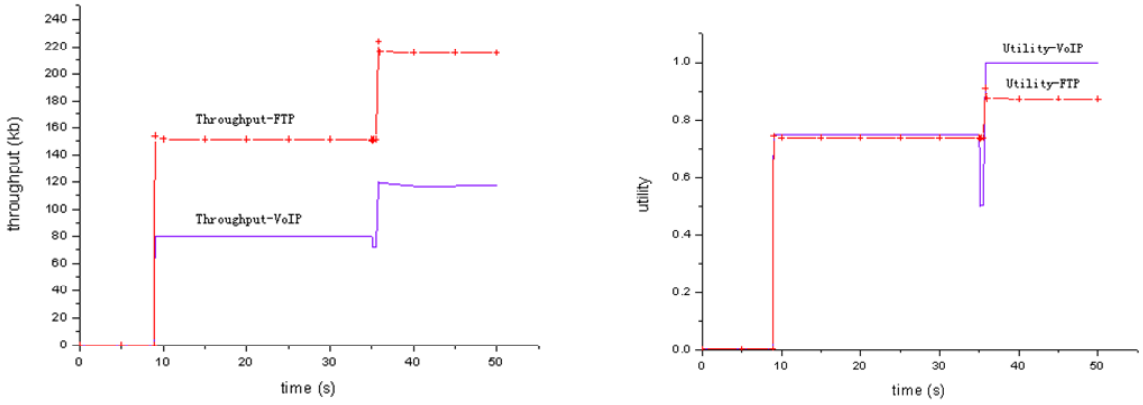


Figure 24. **a)The thr. of the two aps.** **b)The utility of the two aps.**

2.3.3 Introducing autonomicity in QoS management over 3GPP systems

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). Important parts of such a long-term evolution (LTE) include reduced latency, higher user data rates, improved system capacity and coverage, and reduced cost for the operator. In order to achieve this, an evolution of the radio interface as well as the radio network architecture has been considered. In particular, QoS guarantee in the radio access network is one of the critical issues during this evolution.

Meanwhile, reduction of operational efforts and complexity are key drivers for 3GPP Long Term Evolution (LTE). One of the important aspects is to minimise operational effort by introducing self configuring and self optimising mechanisms, which is the so-called self organising network (SON) functions. A self-optimising function shall increase network performance and quality, reacting to dynamic processes in the network. It is thus essential to introduce the autonomicity into 3GPP LTE. In this section we focus on the SON related functions which aim to improve the QoS support in the radio access network by introducing the autonomic mechanisms.

B. Autonomic Hierarchical QoS-MM (Mobility Management) Scheme

Integration of mobility with QoS support is a difficult challenge because of specific radio channel characteristics and complexity of mobility management. In this work we attempt to propose an autonomic hierarchical QoS-MM scheme based on the 3GPP networks.

B1. Introduction

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. Figure 25 gives an overview of an LTE network.

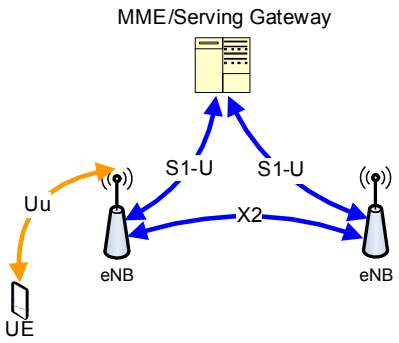


Figure 25. LTE Network Architecture

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.

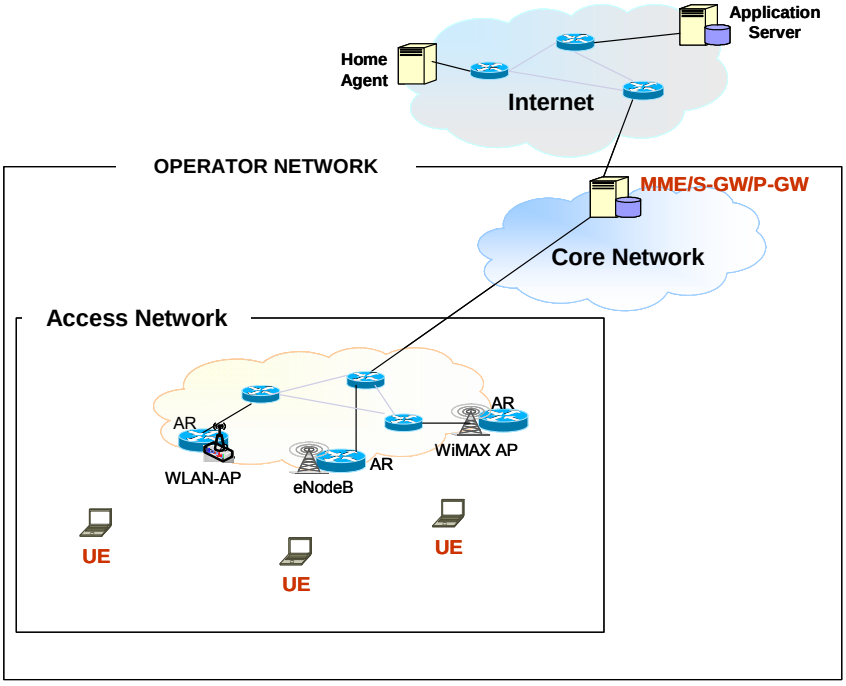


Figure 26. Heterogeneous Network Scenario

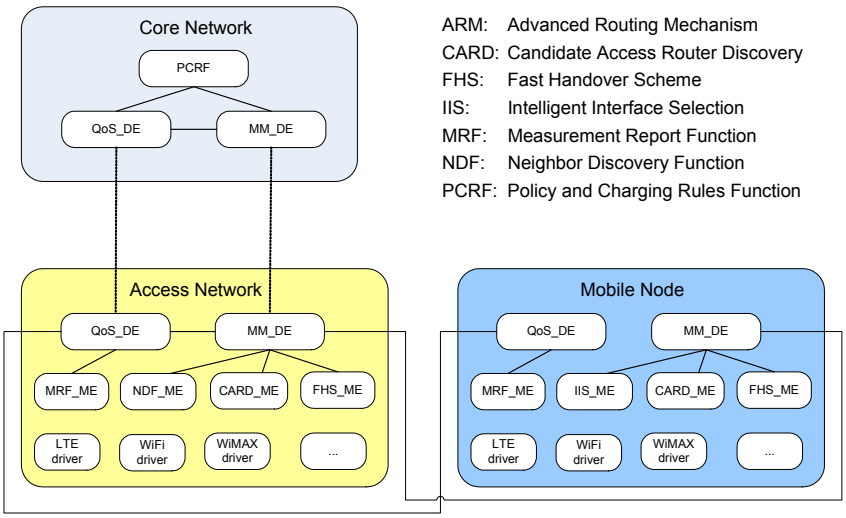


Figure 27. Hierarchical Mobility Management Scheme

B2. Autonomic Hierarchical QoS-MM Framework

The heterogeneous network scenario is considered in this work, where different radio access technologies co-exist in this network including 3GPP LTE, WiMAX, WiFi, etc. (as shown in **Figure 26**). The proposed autonomic hierarchical QoS-MM scheme is illustrated in **Figure 27**, where the node level decision elements FUNC_LEVEL_QoS_M_DE and FUNC_LEVEL_MM_DE are located in Core Network, Access Network and Mobile Node respectively. Especially the 3GPP specific functions (defined as MEs) are also included in this scheme.

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.

The Measurement Report Function (MRF) is the one of main supporting functions (or ME) that enable the autonomic features in this scheme. MRF consists of UE measurement report and eNB measurement report. UE measurements are mainly physical layer measurements to support mobility and scheduling, including **1)** within LTE radio access network (intra-frequency, inter-frequency); **2)** Inter radio access technology; **3)** Inter 3GPP access system mobility. The information supplied by this function includes:

- QoS related information about the current connection, including data rate, packet delay, data loss, etc.
- Potential connections with other access points in the same network or other surrounding networks

The eNB measurements are mainly for load management among the neighbouring eNBs. This function is used by eNBs to indicate resource status, overload and traffic load to each other. The exchanged measurements information includes:

- Hardware Load Indicator, including uplink hardware load information and downlink hardware information;
- Radio Resource Status, including both uplink and downlink radio resource usage information.

These measurements may trigger handover procedure with causes such as “Handover Desirable for Radio Reasons”, “Time Critical Handover”, “Resource Optimisation Handover”, “Reduce Load in Serving Cell”. Thus the overall QoS guarantee can be achieved in a 3GPP network.

C. Use Case: Load Balancing Optimisation

Load balancing is one of the radio resource management functions that are located in the eNB. The main task of load balancing is to handle uneven distribution of the traffic load over multiple cells. The load balancing thus influences the load distribution in such a manner that radio resources remain highly utilised and the QoS of in-progress sessions are maintained to the extent possible and call dropping probabilities are kept sufficiently small. Load balancing algorithms may result in hand-over or cell reselection decisions with the purpose of redistribute traffic from highly loaded cells to underutilised cells.

Depending on the mode of the UEs, there are two types of load balancing. For the idle mode UEs (with which there are no active sessions associated), the task of camp load balancing is to distribute the idle state UEs among the available bands/carriers/RATs, such that upon activation, the traffic loading of the bands/carriers/RATs would be balanced. For the active mode UEs (which are engaged in active sessions), the traffic load balancing functions/mechanisms distribute the UEs/traffic among the available and suitable cells by using redirection for example. In LTE, traffic load balancing is essential because of the shared channel nature. That is, the user throughput decreases as the number of active UEs in the cell increases, and the loading directly impacts on the user perception.

Load balancing directly affects not only the QoS and QoE of the end users, but also the overall network’s radio resource usage efficiency. Optimisation of cell reselection/handover parameters is desirable in order to cope with the unequal traffic load and to minimise the number of handovers and redirections needed to achieve the load balancing. Self-optimisation of the intra LTE and inter radio access technology mobility parameters to the current load in the cell and in the adjacent cells can improve the system capacity. Such optimisation can also minimise human intervention in the network management and optimisation tasks. Besides the general self-* features, the specific autonomic features are highly desirable during the load balancing optimisation, which are summarised as follows:

- **Monitoring functions**
  - UE measurements: UEs monitor the neighbouring cells and measure at least “reference symbol received power” and “received signal strength indicator”. UEs report the measurements to eNBs through event triggered reporting or periodic reporting.
  - An eNB monitors the load in the controlled cell and exchanges related information over X2 or S1 with neighbouring node(s).
  - Load information exchange: The neighbour load can be provided through information exchange – 1) the current radio resource usage; 2) the current hardware load indicator; 3) the current transport network layer load indicator and 4) a composite available capacity indicator.
- **Auto-adaptation**
  - Through the measurements information, an eNB identifies the need to distribute the load of the cell towards either adjacent or co-located cells, including cells from other radio access technologies, e.g., by comparing the load among the cells, the type of ongoing services, the cell configuration, etc.
  - An eNB also estimates if the handover parameter settings need to be modified; if so, communication between involved eNBs takes place to change the handover parameter settings to the neighbour eNB.

For further information concerning the above autonomic sub-architecture integration within WP3 emerging architecture, the interested reader may refer to [D3.2_Appendix I].

2.4 Interrelation between QoE & QoS in autonomic environments (a pervasive service approach)

Introduction. The rising demand for multimedia services in today's broadband networks is highlighting the importance of efficient use of the available resources aiming at satisfying services' requirements. In recent years, considerable efforts have been done towards this goal, resulting in the evolution from a best effort Internet packet forwarder to a Quality of Service-aware framework for real-time services. Nevertheless, despite the deployment of QoS mechanisms that try to fulfil various network metrics such as latency, jitter and packet loss with acceptable values, the final judge of the received stream quality still remains the user/human. A human's actual needs and requirements cannot be defined or mapped in strict values and thresholds, but rather depend on psychological metrics, such as mood, background noise as well as the importance of the multimedia content to the viewer. In [SP54], for instance, it has been shown that if visual factors supplementary to the oral speech are utilised, humans can tolerate higher noise interference levels than if no visual factors are utilised.

The latter highlights the importance and significance of Quality of Experience (QoE), defined as "a measure of the overall acceptability of an application or service, as perceived subjectively by the end-user" [ITU-D197]. Various research efforts are concentrating in correlating QoE with specific QoS metrics. The QoE of multimedia services is mainly affected by the original quality of the multimedia service (i.e., bitrate encoding) and the quality of the transmission (i.e., packet loss, latency, etc). While there is an obvious relationship between packet loss and QoE [LAG08, RP07], as well as delay and jitter and QoE [GG07], the authors argue that despite of that relation between these parameters and QoE, no clear mapping can be made due to the complexity of the compression and delivery of the services. Moreover, in [LSV09] specific full-reference metrics are utilised, comparing the original video with the transmitted one using two different objective video quality metrics: the Peak Signal to Noise Ratio (PSNR) and the Structural Similarity Index (SSIM), and calculate a corresponding QoE value. The authors claim that this value has a strong correlation with the results obtained through subjective testing which is typically given in terms of a Mean Opinion Score (MOS) [ITU-P800].

In the literature, as discussed before, most efforts concentrate on offline methods that try to clearly map the perceived QoE with specific network metrics and then use those patterns relying in QoS mechanisms to satisfy the user. However, to the best of our knowledge there is no complete QoE architecture that allows the users to express their perceived QoS and urge the network to adapt in real time to their choices towards satisfying their QoE. Thus, within the framework of EFIPSANS we propose an online autonomic mechanism that allows users to express their (dis)satisfaction with respect to their service's quality of service. Consequently, it operates in conjunction with Service Management DE and Quality of Service Management entities (FUNC_LEVEL_QoS_M_DE), based on a common Utility Based Framework (Section 2.3). Moreover, a pricing scheme is introduced to dynamically adapt users' service towards embracing high values of QoE in terms of allocated resources and service cost. The rest of this section includes the reasoning behind introducing the proposed QoE mechanism, the detailed operation of the mechanism as well as a few indicative results providing a proof of concept of our autonomic proposal.

Enabling Autonomic Quality of Experience with Control loops

Quality of Experience is envisioned as a cross-layer mechanism, jointly interworking between the medium access control and the application layer. This is reasonable considering the definition of QoE as stated before (i.e., user's satisfaction) and the factors responsible for determining its value (i.e., network metrics like latency, jitter etc).

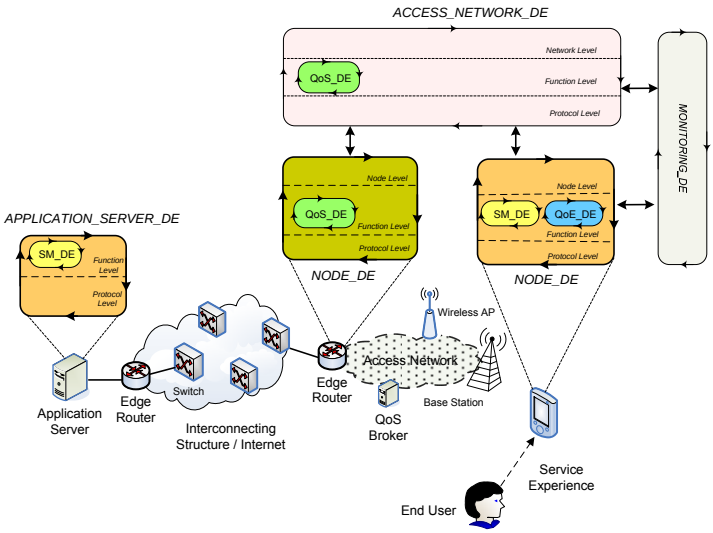


Figure 28. Quality of Experience – An overall architecture

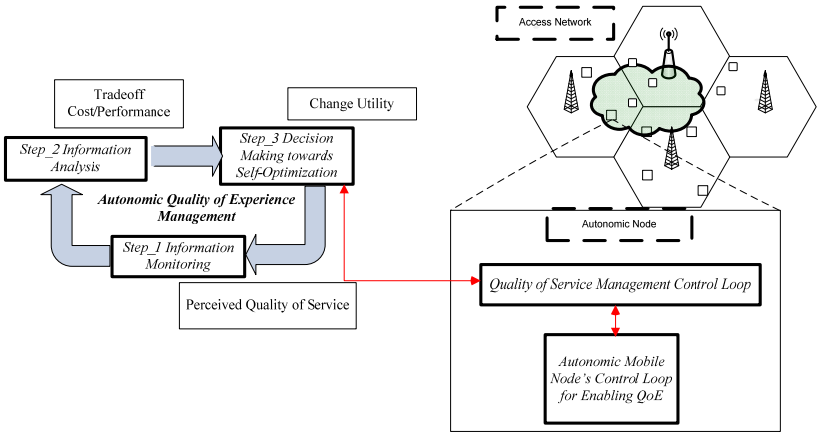


Figure 29. Quality of Experience Management in line with GANA

Therefore, by using existing autonomic elements in line with GANA in an overall autonomic architecture as described in **Figure 28**, we are able to seamlessly integrate the Quality of Experience DE as follows: Quality of Experience Decision Element (PROTO_LEVEL_QoE_DE) constantly monitors service's perceived QoS performance (i.e. QoE) at the application layer and informs accordingly the Service Management DE (SM_DE). SM_DE is in turn responsible for disseminating all necessary information to the Function Level QoS Management DE towards autonomically adjusting MAC layer parameters, satisfying eventually user's prerequisites.

Within the framework of EFIPSANS, Service Management DE is defined as an intermediate between the service the user is currently experiencing and function level DEs responsible for providing that service, managing all the required information exchanged between them. Thus, in order to better illustrate the operation of the proposed Quality of Experience mechanism we eliminate the "overhead" of the SM_DE and consider that all required information is directly disseminated between the PROTO_LEVEL_QoE_DE and function level DEs. Therefore, aiming towards enabling users' autonomicity in Quality of Experience, we introduce a control loop residing at the node. The control loop constantly monitors service's perceived QoS performance (i.e., QoE) and informs the respective cell's resource control mechanisms. These in turn respond providing, or not, the requisite resources towards satisfying the user and thus, maximising his QoE. Specifically, as depicted in **Figure 29**, the perceived services' quality of service is

monitored by the user, allowing him to take action. Next, the user acts towards maximising his Quality of Experience, choosing whether or not to alter his service performance and/or quality, in terms of requesting more or less resources, taking in mind psychological metrics, such as background noise, importance of the service content, mood, as well as the billing policy for the current service. Thus, a billing mechanism is introduced for the purposes of indicating to the user the cost of his service in accordance to the quality of the service he intends to select. The billing mechanism could be quite generic, so as to allow the service cost to vary according to the type of service, network congestion, time of day etc., in line with the providers' revenue policies. The purpose of such a billing mechanism is to prevent users from always selecting the maximum quality for the services within their overall duration. Moreover, analytical results on applying billing policies and how this influences users, or maximises the providers' revenue will be presented in Deliverable 3.6. Finally user's utility function is (dynamically) altered by the Function Level QoS Management DE towards complying with user's desires and is passed to the Protocol Level Node R&Q CDMA DE which in turn realises the resource allocation or informs the user in case of infeasibility.

Quality of Experience Management at a Node

- *Step_1* The user constantly monitors service's performance and reacts to towards maximizing his QoE
- *Step_2* Obtains service's billing policies and autonomically decides the necessary actions to be taken, in terms of requesting more or less resources
- *Step_3* Calculates the new service's utility, triggering at the same time FUNC_LEVEL_QoS_M_DE
- *Step_4* The FUNC_LEVEL_QoS_M_DE informs about the feasibility of the user's request.

In **Figure 30**, a possible Graphical User Interface realising the described Quality of Experience mechanism is presented. Consider a user watching a streaming action movie from a remote video server. The picture on the left is a frame of the streaming video. The user, considering the content of the video and his willingness to pay, decides to request increased quality for a higher cost towards maximising his QoE. The picture on the right is a frame of the stream in increased quality as resulted after realising the QoE control loop.

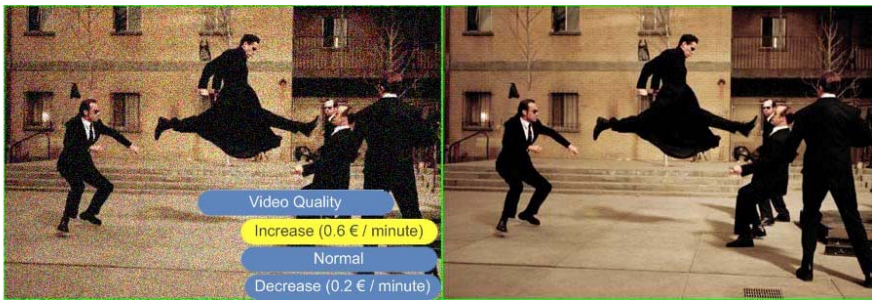


Figure 30. Quality of Experience in Application Layer

Note that the operation of the QoE control loop relies on the adaptation of a Common Utility Based Framework that is able to optimally distribute available resources to all attached users to a cell. As mentioned in Section 2.3 each user is associated with a proper utility function U_i which represents his degree of satisfaction in accordance to his expected actual downlink transmission rate R_i. Intuitively, the utility function also characterises a user's superiority among others, therefore by properly altering a user's utility function and thus user's priority, the Autonomic Radio Resource Mechanism responsible for allocating available resources to user's cell, increases or decreases the user's allocated resources accordingly, finally providing the requested QoE.

Scalability, Stability, Validation and Complexity Issues. The proposed Quality of Experience Management mechanism is designed and built under common principles, not only regarding its

autonomic attributes (i.e., GANA), but also harmonises and cooperates with the Common Utility Function that is adopted to support the QoS mechanisms within the EFIPSANS project. Specifically, given the operation of the ARRM in each cell as described in Section 2.3, the QoE mechanism relies only on the perceived quality of the service the node acquires. The outcome produced, which comprises of just one floating point number, can be easily piggybacked in any control or data packet. Moreover, the QoE mechanism acts and reacts on demand, while its decisions will only be evaluated by the ARRM in the next time slot, thus requiring no synchronisation. The fully autonomic nature of the Quality of Experience mechanism implies no dependencies on the size and type of the integrated system, thus implying it is completely scalable. Furthermore, as noted in the previous paragraph, the QoE control loop only suggests to Function-Level Quality-Of-Service Management and does not require or provide increased/reduced QoS thus eliminating time scaling issues and conflicts between DEs. Finally the performance and effectiveness of proposed approaches is evaluated in the next section.

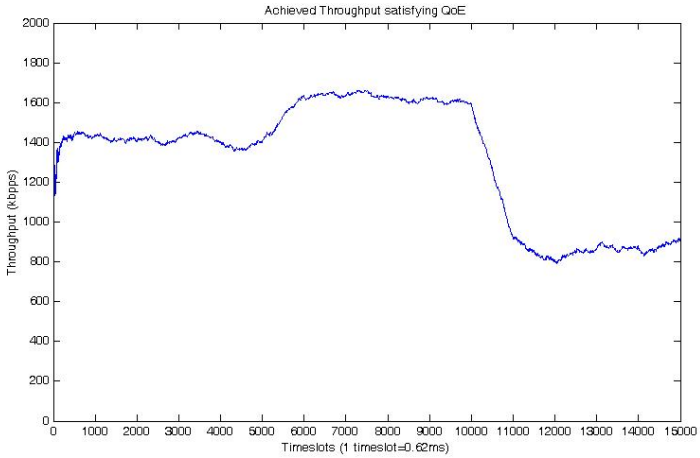


Figure 31. User's 15 Achieved Throughput

Initial Numerical Results. In this section we present some indicative numerical results providing a proof of concept of the proposed QoE mechanism. We consider a CDMA cellular network integrating the ARRM control loops described in Section responsible for optimally allocating the available resources to all active nodes in cells locality. We use the following sigmoidal function to represent users' utility $U_i(R_i)$, i.e $U_i(R_i) = \mathrm{m}\{1/1+e^{-a(R_i-p)} - d\}$, where we set for normalisation purposes $m = \left(1+e^{ap}\right)/e^{ap}$, $d = 1/\left(1+e^{ap}\right)$ (i.e. $U(0)=0$ and $U(\infty)=1$), a=3 and p=3 [LMS05]. We consider 15 users already attached to the cell requesting Real Time services and we rum our simulation for 15000 timeslots (i.e. *1 timeslot=0,62ms*). The following scenario demonstrates the efficacy of our proposed mechanism. Specifically, consider a user travelling by train while watching a streaming movie, finally achieving the average throughput illustrated in **Figure 31**. At timeslot 5000 the user enters a tunnel resulting in increased values of BER, thus reducing video's quality of service, finally reducing his QoE. Thereupon, the user decides that the perceived quality of service he is currently experiencing is not sufficient, and requests for increased QoS in return of increased cost (**Figure 30**). The Function-Level Quality-Of-Service Management DE grants his request triggering the Protocol-Level Node R&Q CDMA DE accordingly. As illustrated in **Figure 31** in just 1000 timeslots (i.e., *0,62 sec*) user's acquired throughput is increased by 15% thus improving his QoE. In a short time the train exits the tunnel and the user again decides that since the reception is now considerably better and the content of the video (pause for commercials) does not require high quality, there is no point in paying extra money, thus requesting for lower quality. Likewise the Protocol-Level Node R&Q CDMA DE acts accordingly towards reducing achieved throughput (**Figure 31**) and satisfying the user.

3 AUTONOMIC BEHAVIOURAL CHARACTERISTICS IN MOBILITY MANAGEMENT

3.1 Introduction

This chapter provides a detailed description of the proposed autonomic mobility management framework and the associated autonomic mechanisms and protocols, developed within the framework of Task 3.1, as well as their performance analysis and evaluation.

Section 3.2 presents the proposed approaches that exploit the autonomicity in the IPv6 protocols. Specifically,

1) An approach that facilitates proper integration of MIPv6 protocol within the overall autonomic mobility management architecture emerging within the framework of WP3 [D3.2_Appendix I], allowing the exploitation of several network and nodes autonomic features and behaviours.

2) An enhanced PMIPv6 scheme is presented that improves the efficiency of PMIPv6 in terms of inter-system handover support in order to meet the critical QoS requirements.

The proposed autonomic mechanisms for mobility & resource management in integrated heterogeneous networks are described in Section 3.3. Specifically,

1) An autonomic QoS-aware joint resource allocation architecture is proposed for integrated systems that aims at maximising the overall integrated network's revenue, while enabling users to self-adapt at QoS-triggered occurrences towards self-optimising their services' performance.

2) An autonomic connection management mechanism is proposed with a finer granularity, with a connection based handoff algorithm as one of its core functions.

3) Also an extension to Shim6 is presented in order to allow pre-emptive failover under user control of network connections.

Finally, two special cases regarding autonomic mobility management in Wireless Sensor Networks and Vehicular Networks are presented in Section 3.4.

Most of the aforementioned efforts, presented in an individual manner is this chapter have been integrated into the emerging architecture of WP3 (along with individual efforts from other tasks), concerning "Autonomic Mobility and QoS Management over a Heterogeneous Wireless Environment", presented with more detail in [D3.2_Appendix I].

3.1.1 Mobile IPv6 (MIPv6)

Mobility Support in IPv6 (MIPv6) specifies a protocol which allows nodes to remain reachable while roaming across different IPv6 networks. Each mobile node is always identified by its home address, regardless of its current point of attachment to the network. While situated away from its home network, a mobile node is also associated with a care-of address, which provides information about the mobile nodes current location. IPv6 packets addressed to a mobile node's home address are transparently routed to its care-of address. All IPv6 nodes, whether mobile or stationary, can communicate with mobile nodes. The goal is to improve the performance of MIPv6 protocol by exploiting or adding autonomic characteristics within specific aspects of its operation. Through the specification of a MIPv6 DE, more autonomic features can be achieved via coordinated decisions taken by several DEs at the decision plane.

The objective is to design a mechanism in line with the principles of the GANA architecture; specifying its interfaces, identifying the information that it requires for proper operation, as well as the information that it can provide to other Decision Elements. The final step is to design a proper control loop that will allow us to manage this protocol. Such an approach will facilitate proper integration of MIPv6 protocol within the overall autonomic mobility management

architecture designed in WP3, and most importantly, will make the protocol and its features available to other DEs, either at node or network level. This will allow the exploitation of several network and nodes autonomic features and behaviours, such as:

- **Self-configuration**: when the mobile node is attached to a foreign link, the mobile node acquires a care-of address through stateless or stateful auto-configuration procedures.
- **Self-advertisement**: when the mobile node is attached to a foreign link and acquires a care-of address, the mobile node self-advertises this address to the home agent and correspondent node through binding update messages.
- **Self-optimisation**: when the correspondent node knows the care-of address of the mobile node (thanks to a binding update message sent by the mobile node), it can send packets directly to the mobile node without going through the home agent. It enables faster and more reliable transmission within the network.
- **Self-healing**: the correspondent node sends a binding error message to the mobile node in order to report errors in a binding update. The mobile node is notified by these errors related to mobility in order to repair them.
- **Self-protection**: The MIPv6 protocol, expected to be deployed in most nodes of the IPv6 network (among others the mobile node), protects itself against threats, such as man-in-the-middle, hijacking, confidentiality and impersonation attacks.

Therefore, this DE will enable other DEs to take advantage of the mobility self* properties shown by the Mobile IPv6 protocol.

Problem's statement and its autonomic solution

Mobile IPv6 protocols show a number of autonomic characteristics. How IP addresses are configured and disseminated, some security aspects through the use of IPSec, etc, are examples of the autonomic behaviour described above. Nevertheless, there are some drawbacks. The operation of the protocol is only network-based and therefore, the actions may conflict with the real needs of services. The use of the GANA architecture will provide a way to enable and thus, exploit MIPv6 characteristics from a service point of view. The protocol will be "open" to let other DEs to capture information that can be useful for their decision making process (for example allowing FUNC_LEVEL_MOB_M_DE or FUNC_LEVEL_QoS_M_DE to know other available networks, whether a hand-off is going to occur) and provide a control interface to force the desired behaviour. This way if it is required to perform a hand-off to assure any service, it can be done even though MIPv6 network based hand-off procedures do not indicate it is necessary from a network point of view. On the other hand when the PROTO_LEVEL_MIP_DE decides to perform a hand-off for network reasons it can be communicated to upper DEs, then they can analyse the impact of such hand-off in running services.

In brief PROTO_LEVEL_MIP_DE will enable the following behaviour on top of the already existing MIPv6 protocol. In general, two basic kinds of behaviours can be expected from this DE:

- **Periodic operation**: monitoring the network components, current status and network conditions
- **Reactive operation**: This DE performs a hand-off when another DE requires the node to perform a hand off. MEs can enable fast hand-off if necessary.

A mobility trigger indication is the main required input to perform a hand-off, which is the main functionality of the DE. So PROTO_LEVEL_MIP6_DE will allow other DEs to force a hand-off based on service level information. Moreover, PROTO_LEVEL_MIP6_DE can export information about current working parameters of the MIPv6 protocol. PROTO_LEVEL_MIP6_DE may internally decide whether to trigger a hand-off. In this case it is possible to ask for authorisation, if needed through communication with security DEs.

Proposed Autonomic Algorithm

PROTO_LEVEL_MIP6_DE is a wrapper for the existing Mobile IPv6 protocol to act in coordination with other DEs, thus allowing the possibility to extend the autonomic functions of the protocol by interacting with such other DEs. The algorithm that rules the behaviour of the DE is summarised in the following steps:

1. The DE gathers information about the network where the mobile node is attached. In addition, the protocol captures the new access point and the associated subnet prefix information when the mobile node is still connected to its current subnet. This information is available to any other DE through its sensor interface.
2. The information is processed internally at the protocol level. If necessary a hand-off will be made. This situation can be informed through the DE sensor interface for other DEs like QoS DE or Mobility Management DE to analyse the impact that the hand-off may have on services.
3. The hand-off is performed. Using the information about available networks, the latency in the hand-off process is reduced.
4. Apart from this periodic operation to perform a hand-off, the design of the PROTO_LEVEL_MIP6_DE will allow other DEs to decide whether a hand-off is necessary for service performance or security reasons, even though it is not necessary from the network performance perspective. Therefore an effector [EFIPSANS – D1.5] interface to force a hand-off is offered.

The PROTO_LEVEL_MIP6_DE will provide information on the current network where it is attached, but also information on available networks. The MIPv6 protocol uses this information in order to reduce configuration and binding latencies towards performing fast hand-off. The designed DE will enable the use of this information from a service perspective, thus it is offered through the DE sensor interface.

Other DEs that may interface with the PROTO_LEVEL_MIP6_DE are:

- NET_LEVEL_MOM_DE
- FUNC_LEVEL_QoS_M_DE
- PROTO_LEVEL_PMIP_DE

Scalability, Stability and Validation Issues

Scalability issues are actually those associated to Mobile IPv6 itself. Two main concerns are:

- Scalability in terms of number of mobile nodes which can be supported by a home agent
- Scalability in terms of time to effect a handover in terms of distance from the home agent

In order to face these issues the DE gathers and offers information not only about the current attached network, but also about available networks, so that hand-off latencies are decreased.

Towards addressing the issue of stability of the proposed autonomic architecture devised we aim at providing mechanism for conflicts resolution (not only between DEs belonging to different network components but among DEs with the same node), which is done through the sensor interfaces for other DEs to learn what can affect their decision and effectors interfaces.

Numerical Results

For simulation purposes we considered a case where the mobile node moves from its home to a foreign network. As the mobile node goes away from its home access point it will remain attached to it until some internal network parameters indicate that the handoff has to be made (internal MIPv6 algorithms). This procedure is made independently of the running application or services and based solely on network based information. As the MN moves away from the access point the delay increases, if the MN was running a VoIP conference, delay may impact the service before performing the hand-off. However, other applications like IPTV (thanks to buffering) or file transfer will work properly. Therefore the network based hand-off will have a different impact on QoE depending on the service in use (Figure 32).

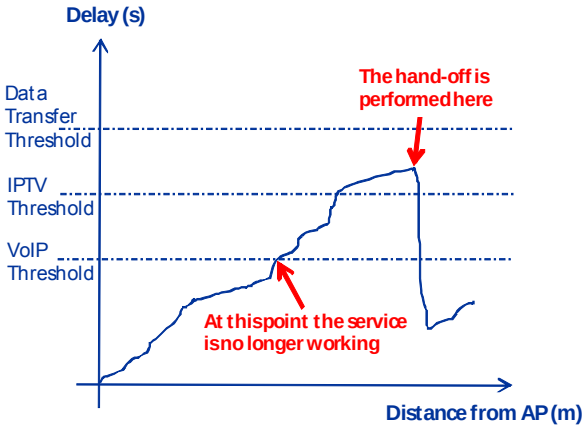


Figure 32. MIPv6 hand-off behavior

In a GANA compliant environment the MIPv6 is empowered with a control loop (the PROTO_LEVEL_MIP6_DE) that opens the MIPv6 operation to be autonomously adapted according to what the user desires. The difference now is that different DEs are responsible for different purposes (for example a FUNC_LEVEL_QoS_M_DE may monitor service performance). When the mobile node delay is about to impact the VoIP service it can communicate with the NET_LEVEL_MOM_DE to force a hand-off to a network with better characteristics. This hand-off enforcement is decided following service level policies and communicated through the NET_LEVEL_MOM_DE and finally the PROTO_LEVEL_MIP6_DE to realise it. As a result the behaviour of the node regarding hand-off is different depending on different situations where different services are running. The GANA based node shows adaptability that is not currently observed.

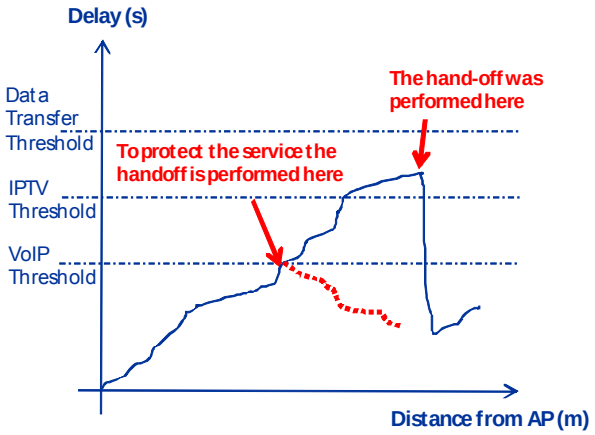


Figure 33. MIPv6_DE hand-off behaviour

The PROTO_LEVEL_MIP6_DE potentially opens a number of possible improvements to the mobility protocol operation. It is possible to add new hand-off functionalities in the DE that takes into account information gathered by other DEs. Moreover it is possible to coordinate different mobility protocols, such as Proxy Mobile IPv6 protocol. From an architecture perspective the DE offers a sensor interface for other DEs to ask for information and a control interface that enable external entities to force a hand-off.

3.1.2 Proxy Mobile IPv6 (PMIPv6)

A. Background

As one of the supported IP based mobility management mechanisms in 3GPP Evolved Packet Systems [3GPP TS 23.402], Proxy Mobile IPv6 (PMIPv6) [RFC5213] is used as a network-based solution to handle the mobility management between 3GPP and non 3GPP access networks.

PMIPv6 enables IP mobility for a mobile node (MN) without requiring its participation in any mobility related signalling. Figure 34 illustrates the main features of a PMIPv6 domain, where two mobility entities are involved in the mobility management - Mobile Access Gateway (MAG) and Local Mobility Anchor (LMA). MAG detects the MN's movement and initiates the signalling with the MN's LMA for updating the route to the MN's home address, sets up the data path for enabling the MN to use its home address for communication from the access link and emulates the MN's home link on the access link. LMA has the functional capabilities of a home agent as defined in Mobile IPv6 (MIPv6) based specification [RFC3775] and with the additional required capabilities for supporting PMIPv6 as defined in the specification [RFC5213].

As illustrated in Figure 35, in the architecture for 3GPP accesses within EPS using PMIP-based S5 Serving Gateway acts as an MAG while PDN Gateway includes the functionality of a LMA [3GPP TS 23.402]. In practice, the Serving Gateway is located in the core network and has little information about the mobility status of the mobile nodes (i.e. UEs). Thus, MAG (collocated in the Serving Gateway) cannot detect the MN's movement and initiate the network level handover in an efficient manner. Therefore the enhancement is required to improve the efficiency of PMIPv6 in terms of inter-system handover support in order to meet the critical QoS requirements.

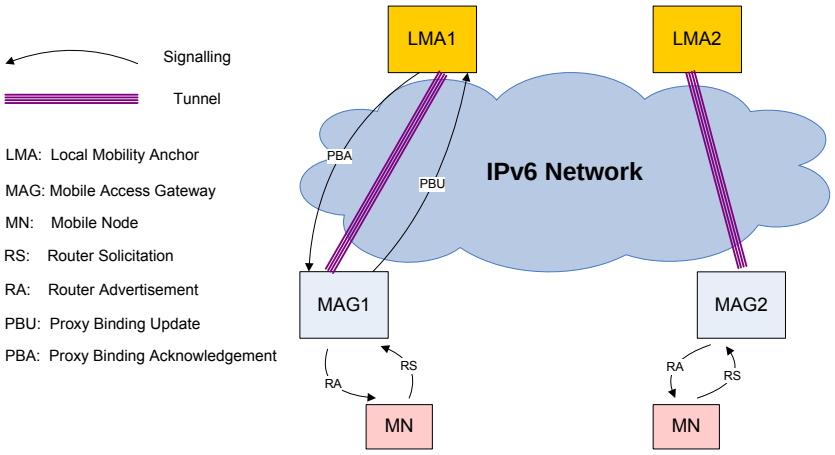


Figure 34. Proxy Mobile IPv6 Domain

B. Enhanced PMIPv6 Mechanism

In this project, one of our main focal points is to introduce extensions to PMIPv6 for performance enhancement when handling local mobility. This solution is independent of the underlying access technology, allowing mobility within or between different types of access networks. Figure 36 depicts the architecture of a Hierarchical PMIPv6 (HPMIPv6) domain. Besides the core functional entities of LMA and MAG, a new functional entity, Mobility Access Router (MAR), is introduced in this architecture, which can also be used to further improve the performance of PMIPv6 by supporting fast handover.

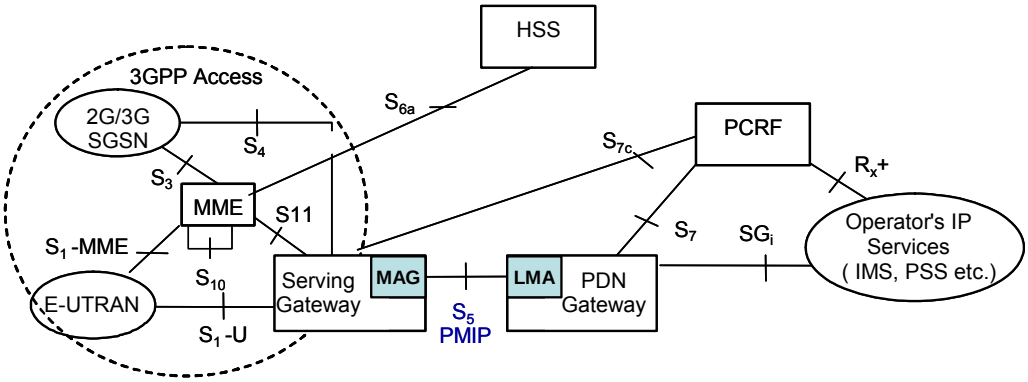


Figure 35. Architecture for 3GPP Accesses within EPS using PMIP-based S5

The MAR acts as an immediate access router, which provides MNs IP mobility support. It can be located in the radio access network when it is deployed in a wide area wireless communication system, such as 3GPP networks, WiMAX, etc. Generally the MAR is located close to the MNs, which allows it promptly detect the MNs' movements and thus provide fast handover support.

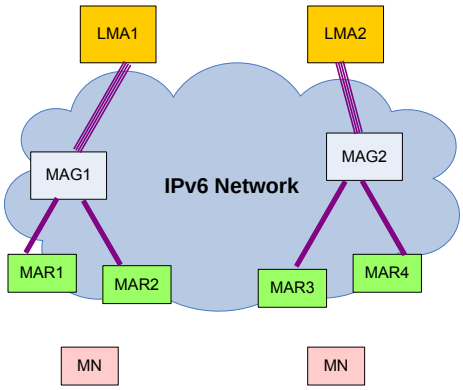


Figure 36. Hierarchical PMIPv6 Domain

MN Attachment

Figure 37 shows the signalling flow when the MN enters the HPMIPv6 domain. The Router Solicitation (RA) message from the MN may arrive at any time after the MN's attachment. For updating the MAG with the current location of the MN, the MAR sends a Local Binding Update (LBU) message to the MN's MAG. The MAG then sends a Proxy Binding Update (PBU) message to the MN's LMA. Upon accepting the PBU, the LMA sends a Proxy Binding Acknowledgement (PBA) message back to the MAG. By then a bi-directional tunnel is set up between the LMA and the MAG. The MAG then accepts the LBU, and replies to the MAR with a Local Binding Acknowledgement. A bi-directional tunnel is set up between the MAG and the MAR. At this point the MAR sends Router Advertisement messages to the MN. The MN now is ready to configure its interface with one or more addresses.

Handover Procedures in HPMIPv6 Domain

Figure 38 and Figure 39 show the signalling sequences for the MN's handover from previously attached MAR (p-MAR) to the newly attached MAR (n-MAR) in case of intra-MAG and inter-MAG respectively. The proxy binding update with the LMA is required only when inter-MAG handover takes place.

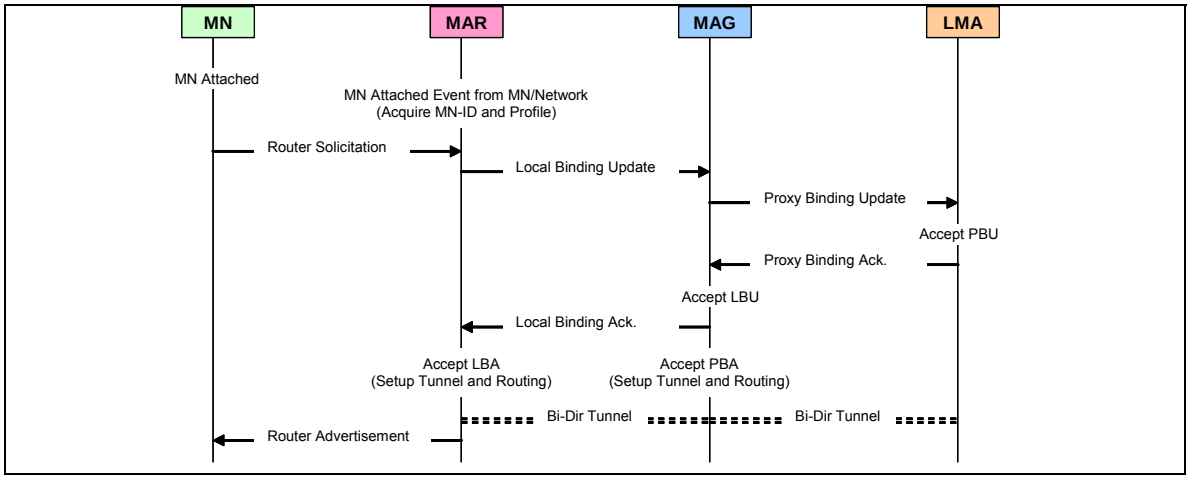


Figure 37. MN Attach – Signalling Sequence

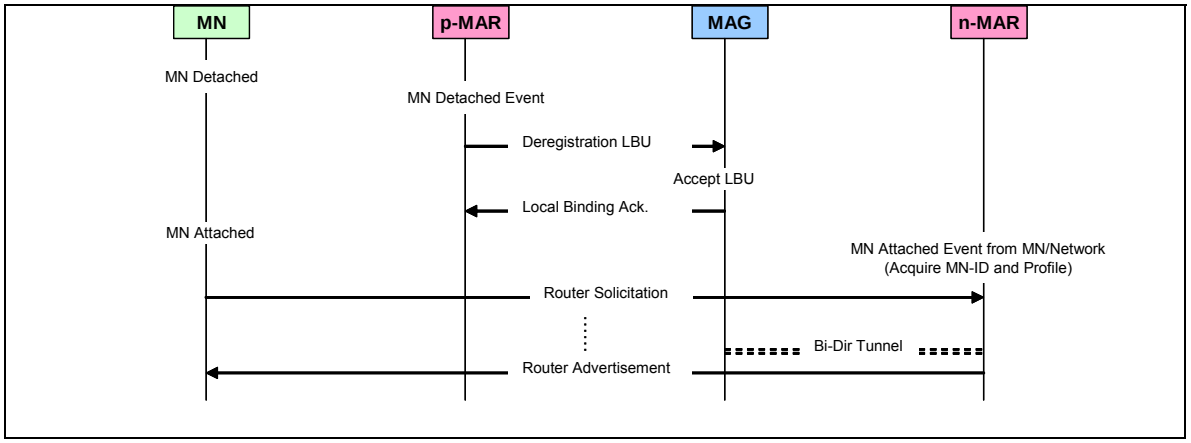


Figure 38. Intra MAG Handover – Signalling Sequence

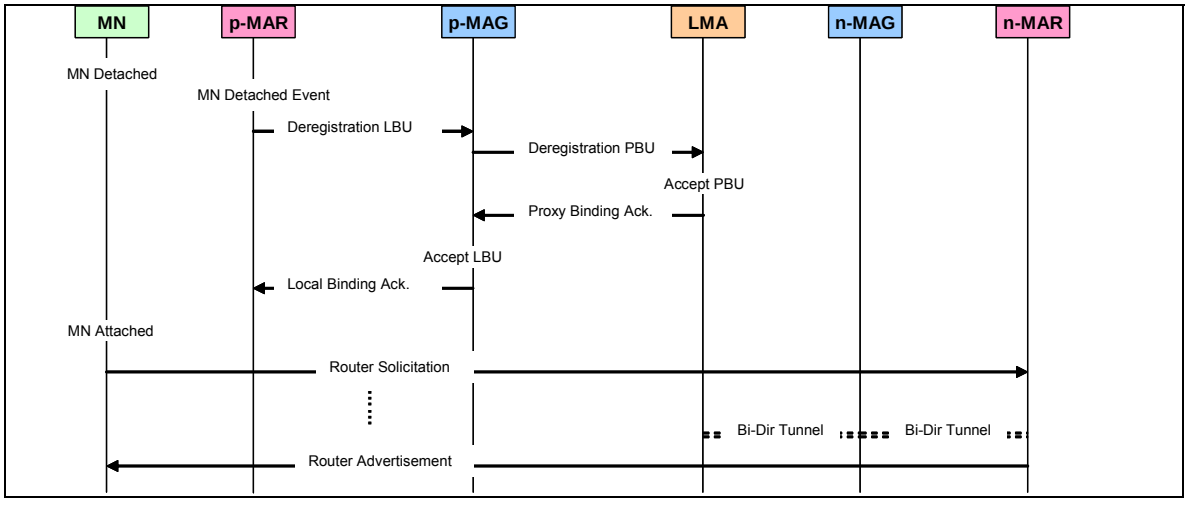


Figure 39. Inter MAG Handover – Signalling Sequence

Fast Handover Support in HPMIPv6 Domain

In order to further improve the performance of PMIPv6, the fast handover support in HPMIPv6 (F-HPMIPv6) is also proposed. Unlike Fast Handovers for Mobile IPv6 (FMIPv6) [RFC 4068], the proposed F-HPMIPv6 is a network-based solution without requiring MNs' participation in any mobility related signalling. This allows a MN to send packets as soon as it detects a new subnet link and allows the new access router to deliver packets as soon as it detects the MN's attachment. Figure 40 illustrates the fast handover signalling flow in an HPMIPv6 domain.

- After discovering one or more nearby access points, the MN sends out a Router Solicitation for Proxy Advertisement (RtSolPr) message to the p-MAR requesting information for a potential handover.
  In some wireless technologies, such as 3GPP UMTS, LTE or mWiMAX, the handover control may reside in the network, a MAR has good knowledge of the attached MNs' movements. In these networks, the p-MAR can send an unsolicited Proxy Router Advertisement (PrRtAdv) containing the link layer address, IP address, and subnet prefixes of the n-MAR when the network decides that a handover is imminent.
- As a response to RtSolPr, p-MAR sends a Proxy Router Advertisement (PrRtAdv) to the MN that provides information about neighbouring links facilitating expedited movement detection. The message also acts as a trigger for network-initiated handover.
- p-MAR sends an Handover Initiate (HI) message to n-MAR, and receives Handover Acknowledgement in response.
- The MN is disconnected from the p-MAR and p-MAR starts deregistration procedures with MAG and/or LMA as shown in Figure 38 and Figure 39. The packets for the detached MN will be forwarded from p-MAR to the n-MAR.
- Meanwhile, the MN attaches to the n-MAR and the n-MAR starts registration procedures with MAG and/or LMA as shown in Figure 38 and Figure 39.

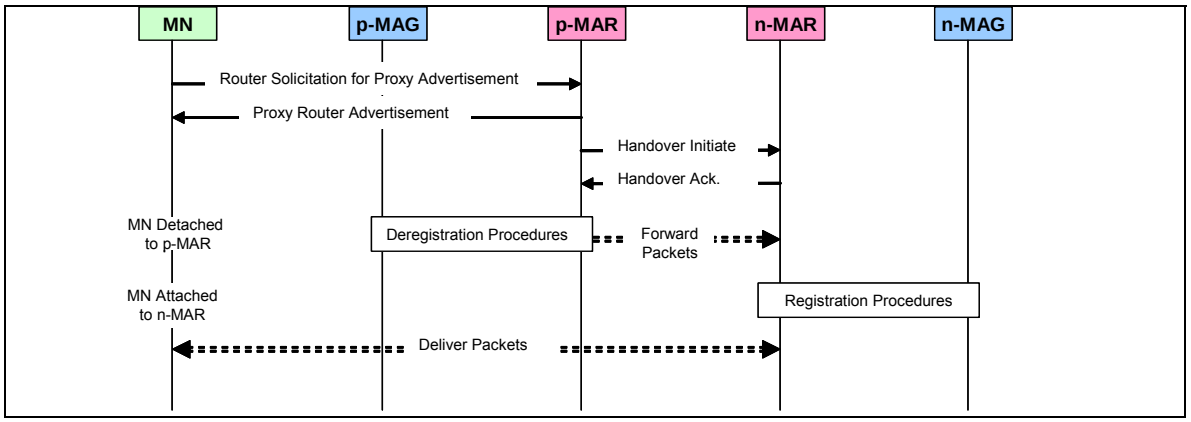


Figure 40. Fast Handover in HPMIPv6 Domain

Table 4. Handover Signalling Overhead

Protocol	Overhead (air)	Overhead (network)	Number of Messages
FMIPv6	72 bytes	86 bytes	5
PMIPv6	0	72 bytes	2
E-PMIPv6	0	116 bytes	4

C. Observations

The proposed enhanced PMIPv6 mechanism can potentially, provide the fast handover support to further enhance the performance by reducing the handover latency. Moreover, because of the collaboration between p-MAR and n-MAR prior to the handover execution, lossless handover for downlink data can be provided.

1) The proposed scheme inherits the main benefits of PMIPv6:
   - Reduction in handover-related signalling overhead, especially the tunnelling overhead over the air. This is particularly important for wireless networks with scarce radio resources. The signalling overhead caused by FMIPv6, PMIPv6 and the proposed enhanced PMIPv6 is summarised in Table 4.
   - Location privacy. The mobile node's home address remains unchanged over the PMIPv6 domain, which reduces the chance that an attacker can deduce the precise location of the mobile node. This is crucial for MNs to access public networks, e.g., Internet.
   - No requirement for MN to support IP mobility. This is especially attractive for various devices in HNB access networks that are not necessarily equipped with mobility support functionalities.
2) The proposed mechanism introduces MAR function in a hierarchical architecture, which can be located in the radio access network when it is deployed in a wide area wireless communication system, such as 3GPP networks, WiMAX, etc. Generally the MAR is located close to the MNs, which allows it to promptly detect the MNs' movements thus providing fast handover support. Therefore, the proposed mechanism improves mobility support performance by reducing the handover latency and providing the lossless handover for downlink data.
   - Compared with the handover procedure under the original PMIPv6 scheme, the E-PMIPv6 enables the collaboration between p-MAR and n-MAR and the downlink data can be forwarded from p-MAR to n-MAR, thus lossless handover for downlink data delivery can be provided.
   - Under the original PMIPv6 scheme, during handover the MN detaches from the p-MAG by performing the de-registration procedure, then attaches to the n-MAG by performing the registration procedure. Several round-trip delays occur during the handover. In case of E-PMIPv6, information is exchanged between p-MAR and n-MAR before MN detaches to the p-MAR. Pre-registration can take place before MN attaches to the n-MAR. Therefore handover delay can be significantly reduced (as shown in Figure 41).

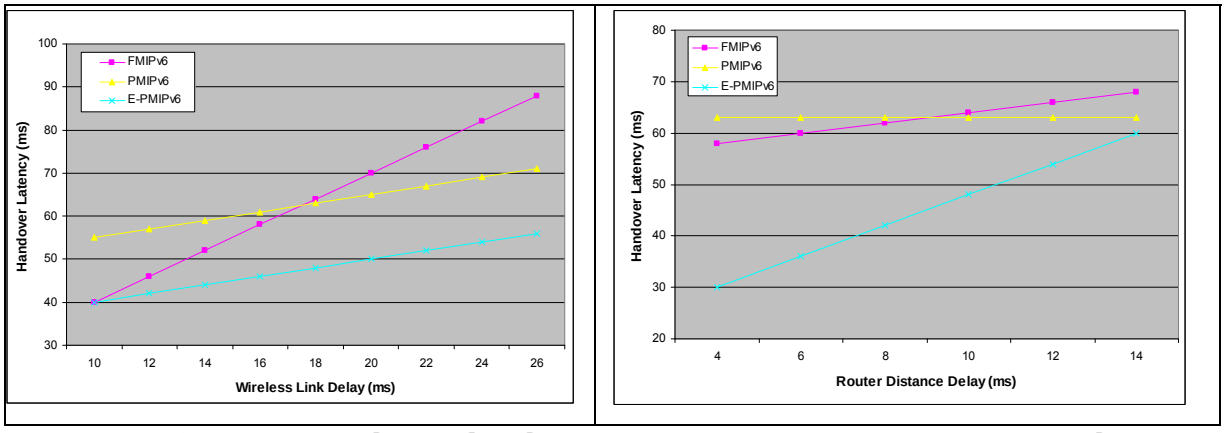


Figure 41. a) Varying Wireless Link Delay **b) Varying Router Distance Delay**

Specifically, Figure 41 illustrates a comparison analysis between the proposed autonomic E-PMIPv6 (blue lines) scheme and the original PMIPv6 (yellow lines) and FMIPv6 (pink lines) schemes, with respect to the achieved handover latency in *msec*. Thus, towards improving illustration's efficacy, two types of results are demonstrated. Figure 41a presents the handover latency achieved by all the previous schemes only as a function of increasing wireless link delay (*msec*), since this factor affects most the overall delay (i.e. end-to-end delay within the 3GPP/SAE architecture) due to the inherent characteristics of the wireless link, while Figure 41b shows the handover latency as a function of increasing router distance delay (i.e. core 3GPP/SAE network delay). The results reveal that the proposed autonomic scheme E-PMIPv6 outperforms both other schemes in all cases, in terms of achieving lower handover latency. Thus, as the wireless link delay increases the better the performance of our scheme (Figure 41a), since due to its desirable design attributes it requires less wireless link signalling messages (i.e. among the base station and the mobile node) than the others. Thus, the required singling in the core network involves closer entities, due to the introduced MAR function in the hierarchical architecture, which also reduces the corresponding handoff delay (Figure 41b).

D. Protocol Level Decision Element: PROTO_LEVEL_PMIP_DE

A Protocol Level Decision Element based on the proposed enhanced PMIPv6 mechanism is designed to provide the network based mobility support. The protocol level decision element PROTO_LEVEL_PMIP_DE belongs to Decision Plane. Its associated MEs include:

- PMIP_CN_ME (Proxy-Mobile-IP_Core-Network_Managed-Entity)
  This ME locates in the Core Network nodes (e.g., Serving Gateway in a 3GPP LTE network), and provides the specific PMIPv6 functionality (e.g., MAG function). This ME also provides system level information, such as system policies about charging, authentication, QoS or security.
- PMIP_AN_ME (Proxy-Mobile-IP_Access-Network_Managed-Entity)
  This ME locates in the Access Network nodes (e.g., eNode B in a 3GPP LTE network), and provides the specific PMIPv6 functionality based on the proposed extension to PMIPv6. The information supplied by this ME and associated other MEs (e.g., CARD_ME) includes:
  - neighbouring access routers, and their current status and capabilities
  - candidate target access routers in case of handover
- MM_UE_ME (Mobility-Management_User-Equipment_Managed-Entity)
  This ME is located in the mobile nodes (e.g., UE in a 3GPP LTE network), and provides the specific mobility related functionality.
- MRF_ME (Measurement-Report-Funtion_Managed-Entity)
  This ME is located in the mobile nodes (e.g., UE in a 3GPP LTE network), and provides 3GPP LTE based Layer 2 measurements function [3GPP TS 36.314]. The information supplied by this ME includes:
  - QoS related information about the current connection, including data rate, packet delay, etc.
  - Potential connections with other access points in the same network or other surrounding networks
- CARD_ME (Candidate-Access-Router-Discovery_Managed-Entity)
  This ME is located in the access router (e.g., eNode B in a 3GPP LTE network), and provides candidate access router discovery function [RFC4066].
- FHS_ME (Fast-Handover-Scheme_Managed-Entity)
  This ME is located in the access router (e.g., eNode B in a 3GPP LTE network), and provides a fast handover function [RFC 4068].

In general, the proposed PMIP based DE and its associated MEs implement the following autonomic features:

- Auto-discovery:
  - "Self-discovery": this DE and its associated MEs (e.g., MM_UE_ME) enable the discovery of a Mobile Node's components, current status, and ultimate capacity, as well as the possible connections with other systems.
  - "Network / neighbour discovery": this DE and its associated MEs (e.g., CARD_ME, MRF_ME) discover all possible access routers, and the access routers to discover neighbours as potential "target access routers" in the case of handover
- Self-optimisation: this DE and its associated MEs always sense the environment and look for the best possible relation between terminal activity and connectivity resources
- Auto-adaptation: When the handover is executed, this DE and the associated MEs enable the self-adaptation behaviours to handle the difference in a heterogeneous access networks.
- Auto-configuration/re-configuration: When a node handovers to a new access network, this DE and the associated MEs enable the self-configuration and re-configuration behaviour.

3.2 Mobility & Resource Management in Integrated Heterogeneous Networks

3.2.1 Autonomic Joint Resource Allocation and Network Selection over Integrated CDMA/WLAN Systems

Introduction. Separate and independent studies on optimal resource allocation and QoS provisioning in specific network types, may prove inadequate when aiming at satisfying various Quality of Service (QoS) constraints within a heterogeneous integrated system. 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. Therefore, future wireless networking [3GPP TS 23.402] envisions, as a founding 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. Within the framework of EFIPSANS, we propose an autonomic QoS-aware joint resource allocation architecture for integrated systems that aims at maximising the overall integrated network's revenue, while enabling users to efficiently self-adapt to QoS-triggered occurrences towards self-optimising their services' performance. The generic nature of the proposed architecture allows it to be integrated in any unified networking environment that a Common Utility Based Framework [LMS05] can be applied. In this context, an integrated WLAN/CDMA-cellular system is used towards providing a proof of concept and validation of our proposed mechanism.

The proposed integrated architecture requires a proper Autonomic Radio Resource Management (ARRM) mechanism, residing at the base station of each cell in the network. This is responsible for optimally and independently allocating a cell's available radio resources among all active users already attached to the specific network (see Sections 2.3.1, 2.3.2). 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 responsible for selecting the most appropriate access network type to be attached to. This includes the current base station the user is attached to (cell), as well as all the ones available in their locality.

Henceforth, 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 poor channel conditions, or (d) the existence of lightly loaded (less congested) cells in his locality that could potentially support better service QoS prerequisites. The following section summarises the ARRM mechanism extendedly reported in Sections 2.3.1 and 2.3.2 towards providing a complete view of the proposed Autonomic JOint Network Selection Mechanism (AJONS).

Autonomic Intra-cell QoS -Aware Joint Resource Management with Control Loops

In order to enable intra-cell mobile nodes'/network autonomicity we introduce two control loops residing at mobile nodes and base stations. The first manages a node's QoS performance and the second one manages a cell's resource control mechanism, while their collaboration realises autonomic QoS radio resource management within the cells of an integrated WLAN/CDMA system (ARRM), as depicted in Figure 42.

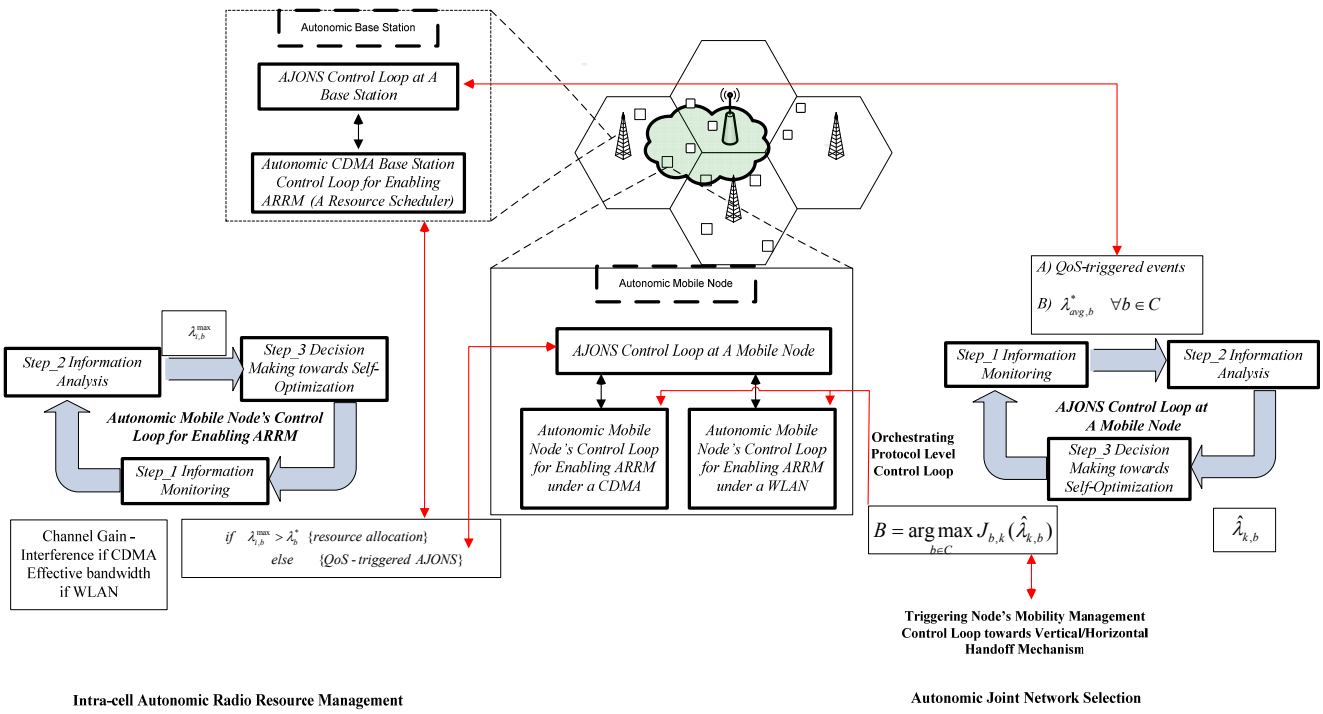


Figure 42. Autonomic intra-cell QoS-aware radio resource management & Autonomic Joint Network Selection Mechanism (AJONS).

Autonomic Base Station Control Loop for Enabling ARRM

Periodically (i.e. on a time-slot basis regarding a CDMA cell (T_s) and every time-frame concerning a WLAN (T_f)), a control loop residing at a base station performs the following steps:

- *Step_1* Monitors its environment and gathers QoS related information concerning: a) active mobile users' services' QoS requirements (i.e. users' utilities) b) active mobile nodes' channel conditions and overall interference (CDMA cell) or current cells' maximum effective capacity (WLAN).
- *Step_2* Sets the corresponding, constrained, non-convex, utility-based optimization problem and obtains its solution.
- *Step_3* Disseminates the acquired optimal resource allocation vectors to the cell's active autonomic nodes.

Autonomic Mobile Node's Control Loop for Enabling ARRM

Mobile node i is already attached to cell $b \in \{CDMA, WLAN\}$

- *Step_1 Information Monitoring:* Constantly monitors a user's service performance and networking environment conditions (i.e. user's channel quality and overall attached cell interference or effective capacity).
- *Step_2 Information Analysis:* Analyses its current status with respect to QoS requirements and computes its current willingness to pay $\lambda_{i,b}^{\max}$.
- *Step_3 Decision Making towards Self-Optimization:* Interacts with the cell's b base station towards determining cell's equilibrium price per unit of resource λ_b^* .Thus:
  - If $\lambda_{i,b}^{\max} < \lambda_b^*$, and the user is currently not selected to access system's resources and thus triggers user's network selection algorithm towards performing a QoS-triggered handoff
  - Otherwise, determines its allocated resources.

Establishing control loops that steer nodes' and base stations' QoS resource allocation mechanisms allows us to further enhance them with self-optimisation and manageability attributes. The necessity of the latter emerges by the heterogeneity of the wireless environment where multiple network access mechanisms regarding a node's service QoS functionalities must simultaneously coexist and/or collaborate. To effectively accomplish that, an orchestrator is required. Such an orchestrator should also be a control loop, acting at a higher level, with advanced accountabilities that manages lower level control loops within a mobile node. The operation, the liabilities, the goals and the algorithms that enable such higher level control loop, and thus an autonomic mobile node, to make QoS-aware, self-optimising decisions are studied in the following sections.

Autonomic Joint Network Selection Mechanism (AJONS)

The goal of Autonomic JOint Network Selection mechanism (AJONS) is to enable autonomic mobile nodes to exploit locally available information from the base stations of the existing cells in their locality. This is done in order to dynamically determine which network to be attached to if needed at all, either when entering the system or at the event of a QoS-triggered handoff. Such a procedure mainly aims at guarantying the services' QoS constraints in both WLANs and CDMA networks as well as maximising the average network revenue via endorsing cell's load balancing.

As the system evolves, periodically, every T_{AJONS}, each base station solves the corresponding QoS-driven resource allocation optimisation problem individually for a CDMA cell (see Section 2.3.1) or WLAN (see Section 2.3.2), regarding its already attached users and considering exponentially averaged values for nodes' and cells' characteristics respectively. Subsequently, each cell's b averaged equilibrium price per unit of resource, $\lambda_{avg,b}^*$ (Lagranzean multiplier) is disseminated via broadcasting to the mobile nodes. Each autonomous node k, either entering the integrated system or reacting to QoS-triggered events, computes its maximum willingness to pay per resource unit $\lambda_{k,b}^{\max}$ that she would acquire if she selected cell b to attach to, for each of the

corresponding existing cells in her locality. In the following, we assume a set C of N_C network cells, belonging to either of the considered access technologies, to be available for the user to receive service from. In this way the user possesses all the necessary required information to compute for each cell $b \in C$ the normalised indicator $\hat{\lambda}_{k,b}$, defined as follows:

$$\hat{\lambda}_{k,b} = \begin{cases} \dfrac{\lambda_{k,b}^{\max} - \lambda_{avg,b}^{*}}{\lambda_{avg,b}^{*}} & if\ \lambda_{k,b}^{\max} \geq \lambda_{avg,b}^{*} \\ 0 & otherwise \end{cases} \quad (12)$$

Since $\lambda_{k,b}^{\max}$ can be interpreted as the maximum value of resource unit of user k at cell b and $\lambda_{avg,b}^{*}$ as the long-term price of resource unit at cell b, then $\hat{\lambda}_{k,b}$ can be interpreted as the normalised profit per resource unit that user k can acquire once selecting cell b to attach to. Afterwards, the node selects the cell $B \in C$ at which he will be finally attached to, in accordance to the following policy:

$$c^{*} = \arg\max_{c \in C} \left\{ \max_{c \in C_{-b}} \{ e \cdot J_{c,k}(\hat{\lambda}_{k,c}) \}, J_{b,k}(\hat{\lambda}_{k,b}) \right\} \quad (13)$$

where b is user *k's* current point of attachment and $J_{c,k}$, is an non-negative, increasing, concave function of $\hat{\lambda}_{k,c}$ and is employed to reflect (a user's network selection strategy) several network type related parameters or in order to allow network's operator to impose policies regarding billing, services' and users' access priorities, as well as congestion avoidance policies. Moreover e $(0 \leq e \leq 1)$ is the sensitivity factor employed to deal with the undesirable QoS-driven ping-pong handoff effect and thus address stability issues.

The intuition behind the proposed network selection strategy is twofold. From network's perspective, the higher the congestion of a cell, the higher its equilibrium price per unit $\lambda_{avg,b}^{*}$ will be in the event that a user selects to attach to the cell, thus discouraging or preventing the user from being attached to that cell. Such an approach will eventually lead towards a load balanced integrated network [LMS05], From a users' perspective, the higher his utility-based satisfaction is, from being attached to a cell is (i.e. his service QoS-aware performance), the higher his maximum willingness to pay will be for the specific offered service quality. This then will guide him to select the most profitable cell and network type. In the rest of this section we outline two control loops (illustrated in Figure 42) for accomplishing the above described distributed asynchronous QoS-triggered joint network selection.

AJONS Control Loop at a Base Station

- *Step_1* Periodically, every T_{AJONS}, sets and obtains the solution of cell's b constrained non-convex utility-based resource allocation optimization problem using exponential averaging, within a T_{AJONS} time interval, for the parameters: users' channel quality regarding all users already attached to cell b when b is a CDMA cell, or effective capacity when b is a WLAN, respectively.
- *Step_2* Disseminates the acquired equilibrium price per unit of resource $\lambda_{avg,b}^{*}$ to the autonomous mobile nodes/users in the cell.

AJONS Control Loop at a Mobile Node

- *Step_1* Constantly monitors user's services performance and reacts to QoS-triggered events (i.e. Step_3 of Autonomic Mobile Node's Control Loop for Enabling ARRM) or mobility triggered events (i.e. Step_3 of Mobility Management Control Loop).
- *Step_2* Obtains locally available networks' average equilibrium price per unit of resource $\lambda_{avg,b}^{*}$, disseminated from all network's cells in his locality (i.e. $b \in C$).
- *Step_3* Computes the normalised profit per resource unit $\hat{\lambda}_{k,b}$ for each $b \in C$ and selects the most profitable network to handover/attach.
- *Step_4* Disseminates this decision to lower level control loops that execute the attachment/handoff.

Scalability, Stability, Validation and Complexity Issues

The proposed Autonomic Joint Network Selection mechanism (AJONS) is designed and built under common principles, not only regarding its autonomic attributes (i.e. GANA), but also harmonises and cooperates with 3GPP, adding minimum overhead and monitoring information exchange. Specifically given the operation of the ARRM in each cell, AJONS requires only globally broadcasted messages by the Base Stations, while the results produced, which comprise of just one floating point number, can be easily piggybacked in any control or data packet. Moreover, synchronisation between BS and mobile node control loop is not required since, both control loops operate and cooperate in an complete asynchronous manner. Specifically the AJONS control loop at a Base Station operates in large intervals (i.e. 5 sec), while the AJONS control loop at a mobile node runs only on demand, (i.e. QoS-triggered).

The fully distributed proposed solution makes the AJONS mechanism completely scalable and independent of the size and type of the integrated system. Furthermore, AJONS is a complete autonomous mechanism that can be modified to act as a "consulting" agent, providing to both Function-Level Quality-Of-Service Management and Mobility-Management Decision Elements, a prioritised list of networks to handoff. Thus, this way we are eliminating time scaling issues and conflicts between DEs. Concerning the stability of the algorithm as well as this of the corresponding optimisation problem, the convergence of the BS control loop has been proven in [LMS05]. Moreover towards reassuring a stable system, we have identified the problem of ping-pong (i.e. mobile nodes continuously swapping between neighbouring cells), and addressed it, by adopting 3GPP solutions and mechanisms and using thresholds. Specifically, we use the parameter *e* in expression (13) and forbid nodes performing handoff until a minimum time period has elapsed since the last handoff. Extended stability and scalability results with relative discussion will be presented in Deliverable D3.6 in which the AJONS mechanism will be integrated to the overall architecture. Finally the performance and effectiveness of proposed approaches is evaluated in the next section.

Numerical Results

In this section we present some indicative numerical results considering an integrated CDMA/WLAN (IEEE 802.11e) system with one CDMA cell, and one WLAN network overlapping with the CDMA cell. We assume that the CDMA network's base station is located at the cell's center and that its maximum transmission power is $P_{max}=10$. Moreover, we assume that CDMA system's spreading bandwidth is $W = 10^8$ and all users' maximum downlink rate is $R_i^{\max} = 2 \cdot 10^3\ kbps$. Regarding the WLAN, the system's access point is also located at the centre of its coverage area and operates in *5GHz* band with maximum network data rate of *54Mbit/s*.

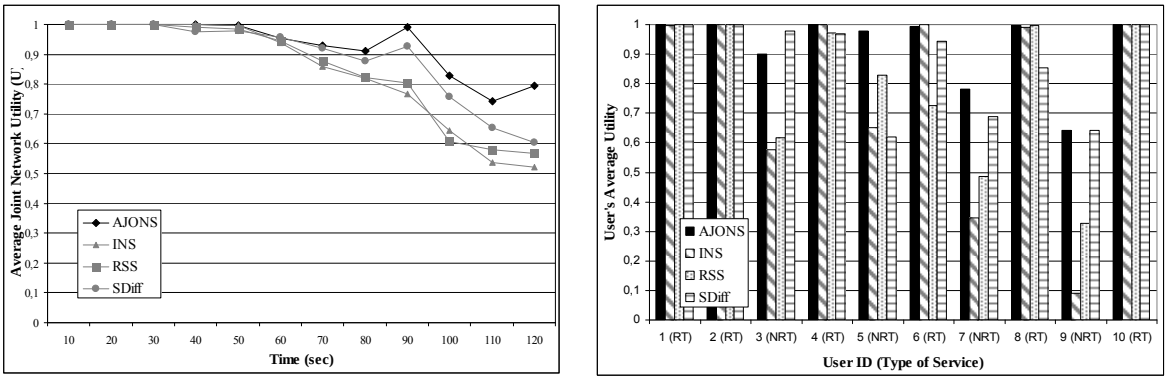


Figure 43. a) Overall system utility and b) Users' average utility based performance.

WLAN effective capacity, C_{max} is dynamically calculated using a simulator that incorporates the IEEE 802.11e scheme. We model the path gain from the CDMA base station to user *i* as $G_i = K_i / s_i^n$ where s_i is the distance of user *i* from the base station and *n* is the path loss exponent (*n=4*) and K_i is a log-normal distributed random variable with mean *0* and variance σ^2 = *8(dB)*. New users periodically enter the system (i.e. every T_{AJONS}) requesting Real Time (RT) and Non-Real Time (NRT) services in a random manner while moving in arbitrary patterns. We use the following sigmoidal function to represent real-time users' $U_i(R_i)$, i.e $U_i(R_i) = \mathrm{m}\{1/1+e^{-a(R_i-p)} - d\}$, where we set $m = \left(1+e^{ap}\right)/e^{ap}$ and $d = 1/\left(1+e^{ap}\right)$ for normalisation purposes (i.e. $U(0) = 0$ and $U(\infty) = 1$), while regarding non-real-time services, a concave function $U_i(R_i)=1-exp(-gR_i)$ is applied, with *g=0.8*. For demonstration only purposes we set *a=3* and *p=3* [LMS05].

We compare the performance of ARRM/AJONS architecture against three other network selection schemes. This is done in order to better illustrate the efficacy of the proposed autonomic joint network selection and QoS-triggered handoff mechanism in terms of achieved overall integrated network utility-based performance. The first one makes use of Radio Signal Strength quality for determining the cell that a user should be attached to (referred as RSS) [LWZ07]. The second approach applies a Service Differentiation scheme (SDiff), where RT users are served by the CDMA cellular network while NRT are served by the WLAN [SJZS05]. Finally, INS scheme performs only Initial Network Selection at the time of a new user's arrival adopting AJONS mechanism, while vertical handovers are not permitted over the duration of its service. Let us underline that under all examined schemes optimal intra-cells' radio resource management is achieved by ARRM scheme. Finally, for demonstration purposes we set $J_{b,k}(\hat{\lambda}_{k,b}) = \hat{\lambda}_{k,b}$ and *M=1*.

Figure 43a illustrates average joint integrated network's utility performance achieved under ARRM/AJONS, INS, RSS and SDiff schemes. The results reveal the superiority of the proposed autonomic scheme in terms of overall system performance, even more so as the system evolves and the overall load increases. Moreover, the normalised profit per resource unit ($\hat{\lambda}$) exploited by ARRM/AJONS scheme reflects not only performance parameters regarding both types of networks (i.e., congestion level, available resources and channel conditions), but more importantly user's service QoS-aware metrics, thus steering users towards making appropriate attachment decisions. On the other hand, myopic network selection criteria (i.e., RSS, SDiff) or even static network attachment schemes where no vertical handoffs are allowed (i.e., INS) are not capable of responding to networking environment variation (e.g., network cells' load and/or users' channels time-varying nature) resulting to low overall system performance, and thus to users' service QoS degradation. The latter behaviour is revealed in Figure 43b where users' average utility based performance is illustrated as a function of their ID and requested type of service.

In summary the presented autonomic architecture, which allows mobile nodes to self-adapt to QoS-triggered events by dynamically determining in an asynchronous manner which network to be attached to if needed, outperforms simplistic and myopic network selection schemes while at the same time utilises the overall available radio resources optimally. Nodes' and network autonomicity is employed as an enabler towards devising a flexible and proficient QoS-aware service orientated wireless interworking architecture, while various autonomic functionalities were developed and studied. The proposed scheme can maximise the network revenue, under given QoS constraints, in both WLANs and CDMA cellular networks, while aiming at the overall system's utility-based load balancing.

The proposed mechanism will be part of the Autonomic Mobility and QoS Management Scenario Testbed that will be realised within WP5 and will provide us with useful results demonstrating the efficacy and effectiveness of our mechanism. The previous work has led to the following publications [AKP09_1], [AKP09_2], [AKP09_3] και [AKP09_4].

3.2.2 Autonomic Connection Management

Introduction. In heterogeneous wireless access networks, seamless handoff for a mobile node is a key issue. Even more so for a multi-homed mobile node that runs multiple applications or services simultaneously. Traditional handoff algorithms are no longer able to make optimal handoff decisions due to the complexity and the heterogeneity of the network. In our work, an autonomic connection management mechanism is proposed. A finer granularity, connection based handoff algorithm is one of its core functions. Furthermore, some autonomic attributes, such as self-configuration and self-adaptation, are embodied in the mechanism. Self-configuration will be used for configurations of mobile nodes' IPv6 addresses and the entries of Connection Information Lists (CIL). Given the complex networks environment, self-adaptation handoff decisions, which take network related factors, device related factors, service requirement and user preferences into account, will be made.

Problem's statement and its autonomic solution

There are two main problems that should be addressed in the proposed connection management mechanism:

- how to achieve connection-granularity, seamless handoff, for different applications running on multi-homed mobile terminals?
- how to use integrated network resources effectively in heterogeneous wireless access networks?

To solve the aforementioned problems, we proposed an autonomic connection management mechanism based on mobile terminals. As shown in Figure 44, there are two types of nodes in the mechanism. The first type is autonomic mobile nodes, and the second type is autonomic network nodes, such as base stations or access points. Each node has one control loop for connection-based mobility management.

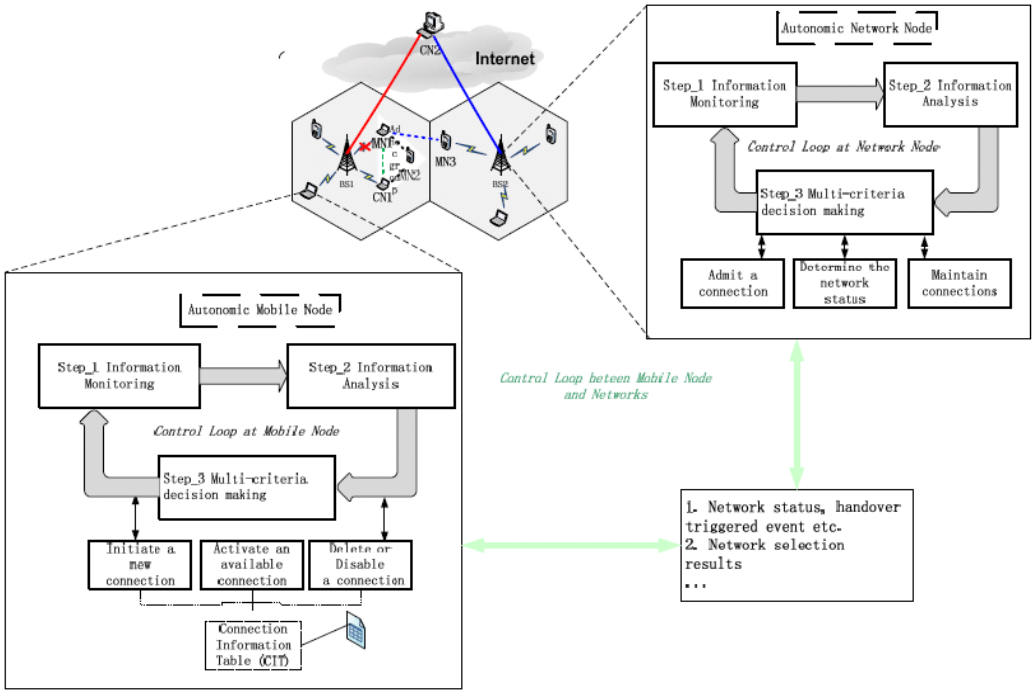


Figure 44. Connection Management Mechanism with Control Loops of GANA

Autonomic Base Station/Access Points Control Loop for Mobility Management

Periodically, a control loop residing at a base station/ access points performs the following steps:

- *Step_1* Monitors its environment and gathers mobility management related information, including: a) network status or available resource; b) statistic features of connections attached to it; c) numbers and features of new connections tending to attach to it.
- *Step_2* Analyse the lowest requirements of both existed connections and new connections with respect to the current network status.
- *Step_3* Given the networks' resource as a whole, disseminate the acquired optimal resource allocation to the connections of active autonomic nodes.

Autonomic Mobile Node's Control Loop for Mobility Management

Mobile node is already under the coverage of both CDMA and WLAN.

- *Step_1 Information Monitoring:* Monitors its environment and gathers mobility management related information, including: a) network related factor (e.g., available broadband, RRS); b) device capability(e.g. battery life, processor speed, velocity); c) application requirements(e.g., delay, jitter, bandwidth, reliability) d) user preference(e.g., monetary cost and interface preference)
- *Step_2 Information Analysis:* Analyzes current status of all available access networks and the capability of mobile node with respect to applications' requirements along with the user preference, and then network ranking for each application will be computed in Section 3.
- *Step_3 Decision Making towards Self-Adaptation:* The multi-criteria handoff decision algorithm takes advantages of both AHP and SAW. Based on inputs collected in *Step_1*, it computes network ranking for each connection. Thus:
  - For a connection serving an application f, which is attached to CDMA network, if the final network ranking is $Fo_{f-WLAN} > Fo_{f-CDMA}$, then this connection will be attached to WLAN.
  - Otherwise, handoff will not happen.

As shown in Figure 44, there are interactions between control loops residing on mobile nodes and network nodes, respectively. The interaction information contains network status, handoff trigger events, network selection result, and so on.

The concrete algorithm for multi-criteria handoff decision algorithm is described in the following section.

Proposed Multi-Criteria Handoff Decision Algorithm

The connection management mechanism in our research is an autonomic system, which has four steps forming a feedback loop as shown in Figure 45. The system collects information from a variety of sources, which is analysed in order to construct a case model of the evolving situation faced by mobile terminals. This includes outputs by this model, i.e., a solution, which is used as a basis for intelligent decisions. The decisions are propagated through network and mobile terminals. The impact of decisions can then be collected to inform the next control cycle.

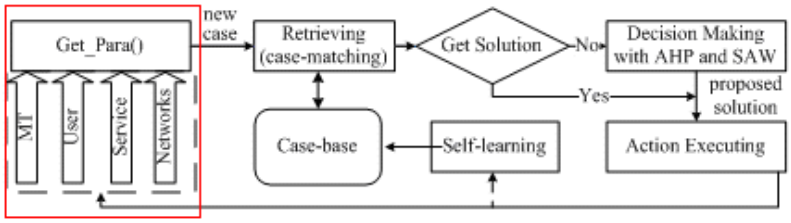


Figure 45. Autonomic connection management

`Step1 Context Collected by Get_Para()`

Context information, including network and device related factors along with service requirements and user preferences, needs to be collected for handoff trigger reorganisation. This allows for case matching in step 2 and multi-criteria handoff decision in step 3. In order to make best use of integrated network resources, performance information of each available access network should be collected, which contains types of network, availability of a network, limited available resources, their access mechanisms and characteristics, etc. One result of Get_para() is a new case or problem description, which is used for the case matching in step 2.

Given the Generic Autonomic Network Architecture (GANA), our proposed mechanism is mapped into the elements in GANA, either DEs or MEs.

Functions achieved in the red box labelled in Figure 45, which collect various information for handoff triggering or decision making, should be supplied by the PROT_LEVEL_ ND_DE or/and FUNC_LEVEL_Monitoring_DE.

Step2 Retrieving Similar Cases

Retrieving a case starts with a problem description and ends with either a "best matching" case being found or not. We adopt case based reasoning (CBR) techniques to implement the knowledge repository (KR). A case represents specific knowledge in a particular context. Case base (CB) is a cases library. Cases stored in the case base should be described clearly by "which service" using "which network" under "what conditions".

Fuzzy matching is used to match the new case and cases stored in the CB. If a similar case is found, its solution can be directly reused to solve the current problem, going to step 4. If not, go to step 3 to generate a new solution.

Step3 Decision Making Algorithm Combined with AHP and SAW

Step3.1 Velocity Judgment

As shown in Figure 45, after all the necessary context information has been collected, the velocity of the MT is firstly analysed to decide whether it is in the threshold scope. If it exceeds the threshold scope, just go to step 4. Nothing has to be done and CIL will be barely maintained. Otherwise, go to step 3.2.

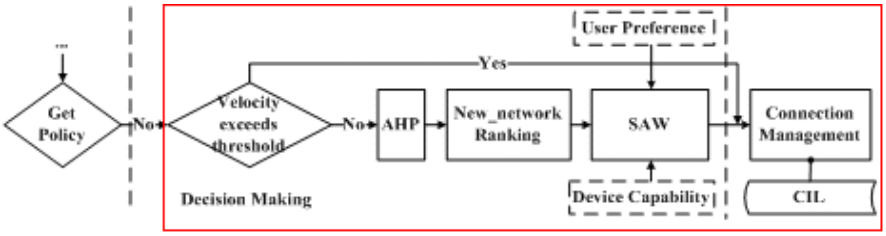


Figure 46. Decision making with AHP and SAW

Step3.2 Analytic Hierarchy Process (AHP) and Simple Additive Weight(SAW)

In this section, AHP is used to get network ranking for each service type, and its result is part of input to SAW which finally makes handoff decision for each connection. Functions achieved in red box labeled in Figure 46, which combine AHP and SAW to charge for multi-criteria handoff decision of connection management, should be one core function of FUNC_LEVEL_MM_DE in GANA.

Communications between FUNC_LEVEL_MM_DEs in mobile nodes and its peering DEs residing at other network nodes are planned to be achieved by extending the ICMPv6 protocol.

Step4 Action Executing

After the handoff decision has been made for each connection as an outcome from step 3, corresponding operations will be enforced on BSs/APs and the MT. With regard to BSs/APs, authorisation for the MT to use their resources needs to be processed. For the MT, some connection entries in its CIL need to be modified.

The proposed solution is under observation. If the new case is efficiently dealt with, the solution will be added to the CB. This is a self-learning procedure, a key step to achieve autonomicity in connection management. As more cases are experienced by MT, the CB will get more plentiful. When the CB gets sufficiently populated, new cases should be closely matched with cases already stored and solutions can be directly retrieved rather than calculated by step 3.

Scalability and Validation. The proposed algorithm is based on mobile terminals, and contributes to the scalability of the network. As already defined, each terminal or network node has a mobility management control loops at all nodes. This distributed mobility management mechanism could be independently implemented in various access networks. Therefore, if a new terminal attaches to a specific access network, it will not have significant impact on the network-level mobility management control loop, which can be just regarded as an information supplier to the FUNC_LEVEL_MM_DE.

Numerical Results & Discussions. In the following we present some numerical results obtained by simulations that reveal the autonomicity feature of the proposed management mechanism thought the property of self-adaptation.

1. Simulation Scenario

The simulation was carried out in ns-2+802.21 protocol to evaluate the performance of our approach. The simulation scenario is shown in Figure 47. We assume that UMTS has full coverage while WLAN exists with access point located at coordinates (100,100), which has 50 meters coverage radius. The MT moves from (40, 100) to (160, 50) from 5s with a certain constant velocity ($v_{\min} = 1m/s$, $v_{\max} = 30m/s$ and $v_{threshold} = 20m/s$). A CT initiated two TCP connections with MT, which last from 10s to 130s.

2. Self-Adaptation Handoff Decision

Scenario 1: The MT moved with a velocity of 2m/s. Once it discovered WLAN existed, the proposed mechanism would analyse current handoff related factors collected from the network, the device, user preference and application requirements, and make handoff decisions. In this simulation scenario, FUNC_LEVEL_MM_DE made the decision that moving to the WLAN (offered by PROT_LEVEL_ND_DE) was more appropriate than remaining on UMTS with regard to data downloading. Then, the data traffic of this service was redirected from the former connection on UMTS to a new connection on WLAN. As shown in Figure 48, we can see that the data download application received a higher download speed than it did in the UMTS, and the user got a better quality of experience.

Scenario 2: The MT moved with a velocity of 25m/s, which had exceeded the predefined threshold. In this scenario, we will compare two different handoff decision mechanisms, one of which took velocity as one handoff decision factor while the other did not.

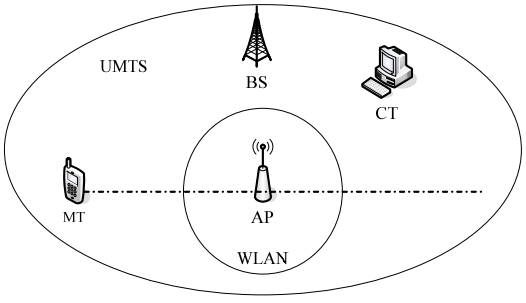


Figure 47. Simulation scenario

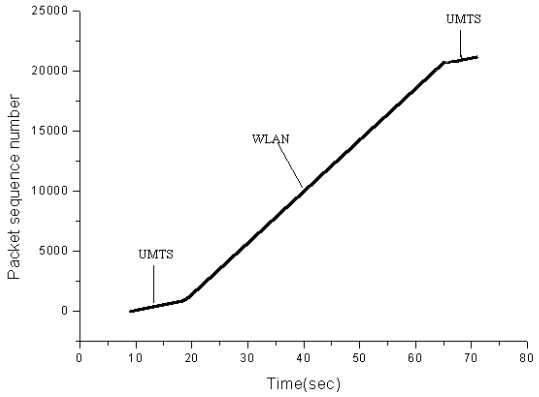


Figure 48. Packet sequence number of data downloading with two handoffs

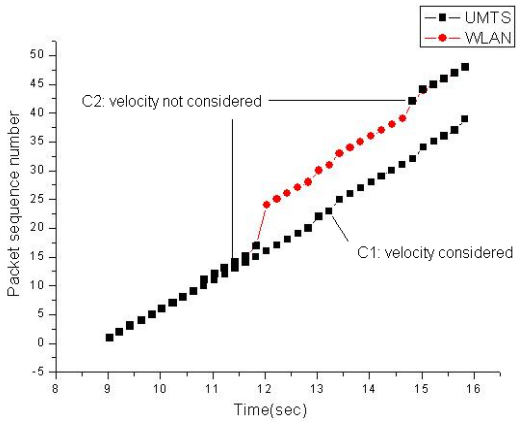


Figure 49. Impact on packet lost rate of velocity

As shown in Figure 49, Curve 1 (red dots) represents the packet loss performance of the data downloading when velocity was not considered in the a handoff making procedure. We can see that when WLAN was detected and once handoff decision that the performance of WLAN was more suitable for data downloading was made, the connection serving for the application had a vertical handoff occurring and started to run in WLAN. When the MT moved out of coverage of WLAN, the connection experienced another handoff and then ran in UMTS again. During 9s and 16s, two handoffs occurred. 15 packets were lost while 53 packets were transmitted, so the packet loss rate was 0.28.

Relatively, velocity was taken into account for handoff decision by FUNC_LEVEL_MM_DE. When velocity exceeded the threshold, irrespective of whether the status of WLAN was good or not, the handoff would never happen. The MT just kept on using UMTS. Curve 2 (black dots) represents the packet lost performance when our algorithm was carried out. Only 4 packets were lost while 44 packet were transmitted, so the packet loss rate was 0.09.

Therefore, it is demonstrated that our algorithm integrated within FUNC_LEVEL_MM_DE performs considerably well on low packet loss rate based on considering the metric of velocity in the whole decision making procedure.

In short, the proposed connection management mechanism can automatically distribute different applications to its most appropriate networks. This is to say that applications can be self-adapting to changes of their context environment while users could be gaining better experience. The previous work has led to the following publications [Z09], [G09], [X09_1] and [X09_2].

3.3 Sensor Networks and Vehicular Networks

3.3.1 Autonomicity and Vehicular Networks

Introduction. The primary goal of Intelligent Transportation Systems (ITS) is to increase road safety by detecting emergency situations in advance and notifying the drivers about the traffic events. The sensors of the vehicle, however, can only provide limited information to the driver -- they can monitor the status of the various parts of the car, but not all the external conditions that affect the driving. Information sharing among the vehicles leads to increased efficiency of a collision warning system and enables the implementation of an advanced traffic optimising service as well.

The seamless operation of an automated traffic control requires all vehicles to be equipped with on-board navigational systems. Nowadays this is possible with no significant additional cost, and in the near future it might even become a default feature like ABS is today. The traffic could become much more efficient if the navigational system could provide the driver up-to-date information about vehicle density, speeds, possible accidents and other unforeseen or temporary restrictions. Some sort of communication is necessary to achieve the latter. Then, the vehicles should disseminate the relevant information through a decentralised wireless network.

Problem statement and its autonomic solution

A decentralised vehicular network is similar to a traditional wireless ad hoc network; however, mobility and communication patterns are entirely different. The vehicles have high speeds, but predictable paths, and the nature of the information exchange is not one-to-one, but one-to-many (multicast). Therefore, traditional ad hoc routing algorithms are in general not appropriate, or should be significantly re-designed to decrease the required signalling traffic spent on route maintenance. More efficient information spreading techniques have to be applied, which support the multicast communication scheme and take advantage of the position information that is expected to be available to all vehicles by using a GPS receiver. These techniques include directed and restricted flooding and location based multicasting (geocasting).

The “Localized Urban Dissemination (LoUD)” emergency message propagation protocol proposed in [MV08] statistically restricts the message flood into the vicinity of the originator by randomly dropping packets. This probabilistic dropping scheme is called gossiping in the literature, and its original purpose was to decrease the network load caused by flooding (e.g., in the path discovery phase of reactive ad hoc routing protocols). When the network nodes are placed along a line (like cars on the road), gossiping effectively limits the distance a message can reach if the p rebroadcast probability is less than 1. To be more precise, the chain of message passing consists of independent, identically distributed Bernoulli-trials, and it is known that the sum of such events follows a geometric distribution. The expected value of the hop count is the mean of the resulting distribution, $h=1/1-p$, which is not infinite if $p<1$.

The size of the coverage area is determined by the value of the p rebroadcast probability. On a highway, for example, it might be set according to the priority of the message. In an urban environment, like in downtown, the buildings block the propagation of the radio signals, so the road segments are similar to highways, only their lengths are shorter. The big difference between the two scenarios is that junctions are frequent in the latter, and in those junctions the messages are not required to be forwarded equally in all directions. Some roads are one-way, some are rarely used, and turning left is prohibited in larger intersections in some countries. This information should also be considered in the junctions in order to limit the flooding into areas it is believed to be useful.

The coverage area defined by the LoUD protocol not only depends on the usual traffic conditions, but it can also adapt to the actual traffic situation. The rebroadcast probability set by the dissemination control algorithm depends both on static data read from the digital map and

dynamic data from online measurements. This self-configuration is believed to be beneficial to the distributed traffic control system that uses the LoUD protocol as a message dissemination subsystem.

Proposed Algorithm

The LoUD protocol doesn't require all nodes to reconsider the rebroadcast probability of the forwarded packets. The nodes that are in a junction become Deciders, and only these nodes change the rebroadcast probability of the packets, according to the previous path of the message and information about the next road segment the message will be flooded into. The computation is based on two probabilities:

1. the probability that the message reaches a certain junction;
2. the probability that vehicles go to the source from that junction.

The basic dissemination control of the protocol sets the p rebroadcast probability so that these two probabilities are equal. The traffic model used in the calculation consists of q turning probabilities in the junctions and s stop probabilities on the road segments. This results in a non-persistent dissemination, because in reality the Deciders consider the probability of the event of ``the message reaches the next junction if it reached the current one'', and it is known that $P(X > x+y \mid X > y) = P(X > x)$ if X follows a geometric distribution.

The resulting formula reported in [MV08] for computing the rebroadcast probability for the next road segment is

$$p = \sqrt[h]{q(1-s)}. \tag{14}$$

This is the formula the RPR_DE (Protocol-Level Inter-Vehicle-Communication-Rebroadcast-Probability-Recalculation Decision-Element) evaluates. It is possible to derive the turning and stop probabilities from the digital map, but there are several factors that influence the route of the vehicles without being represented on the map. These include popular places, e.g., parking lots, popular detours, and of course temporarily closed roads. A network management service might be able to monitor the traffic and supply a Traffic Conditions Database (TCDB) that contains the q and s values describing the usual traffic conditions. The actual traffic almost always differs from the usual one of course, but if we assume that the traffic control system built upon this message dissemination eliminates some of the traffic jams, then the difference might decrease significantly, and the usual conditions converge to the optimal one.

The length of the previous road segment measured in hop count must also be available when recomputing p. The RLE DE (Protocol-Level Inter-Vehicle-Communication-Road-Length-Estimation Decision-Element) supplies this information to the RPR DE. The segment length in meters is supplied by the digital map, and the average hop length should be measured by the media access protocol while the vehicle travels that road segment. Using this locally collected information the calculation might be more precise, than an estimation done by the source node.

The computations so far have been quite simple, and the result is also promising, as the packet does not have to carry any information about its past, other than its rebroadcast probability. There is a price for this simplicity, though; the distance a packet travels follows a geometric distribution, which has an enormous variation. It means the size and shape of the coverage area is very fuzzy, and thus the message delivery is not reliable. The solution is to change the message passing scheme in order to produce a different path length distribution with smaller variance. The modified protocol, called Carefully Localised Urban Dissemination (CLoUD), uses a voting process instead of the instant packet drop in case a Bernoulli trial fails [MV09]. The packet is only dropped if it collected K votes, where K is a predefined averaging factor.

The resulting path length distribution is a Negative Binomial Distribution, and its mean and variance can be tuned with the K parameter. If we keep the mean value the same as the original

mean of the simple gossiping, then the variance becomes: $\sigma' = \sigma(1 - p + p/K)$. The mean is kept constant by decreasing the rebroadcast probability:

$$p' = \frac{p}{k + p(1-k)} \tag{15}$$

Although the original formula (14) for the rebroadcast probability does not contain any information related to the mean of the distribution, the modified gossiping scheme with the modified p' rebroadcast probability does not deviate significantly from the original path length distribution, while being noticeably more reliable.

Scalability, Stability and Complexity Issues

a. Scalability is achieved through a mostly stateless operation in LoUD; the only state a packet carries in its header is its actual rebroadcast probability. In CLoUD, however, there is a counter, the number of votes, that causes the packets to retain information about their past, but this should not decrease the scalability of the dissemination; there is still no need for any signalling messages, as the nodes know all information they need when forwarding packets – they have the digital map, and the header of the data packet.

b. If $p<1$, the area is finite; thus, the number of active messages in the network is also finite. The stability of the traffic control is the responsibility of the application that uses CLoUD as a message dissemination protocol, but the application itself that analyses the traffic situation and suggests actions to the driver is out of our scope.

c. The message dissemination is validated through simulations; both the size of the coverage area and its reliability can be measured easily with the toolset we developed.

d. The algorithmic complexity of the calculations is considered low. The n^{th} root calculations might look complex, but they can be computed quite easily via Newton's method; thus, this does not prevent a possible implementation of the protocol on an embedded hardware. The random number generation is much more resource demanding though, especially in the modified gossiping scheme, which requires significant amounts of random numbers to be generated. This issue still needs some verification before the protocol is deployed.

Numerical Results

The fairness equation (14) includes the standard gossiping scheme as the message passing probability, and theoretically the change to the modified gossiping scheme ruins its nice non-persistent solution. Keeping the rebroadcast probability recalculation scheme while changing the packet-forwarding scheme is not an appropriate approach. However, the proper solution would require the Deciders to make complicated calculations, and additional stored states would be needed in the packet header, which is not desirable. The engineering solution is to keep the calculation and treat the deviation from the fairness as a systematic error. This error is shown in **Figure 50**. Only small *K* values cause dramatic changes in the error, while above *30* it is almost constant. Therefore, this does not present any limitation for the averaging factor.

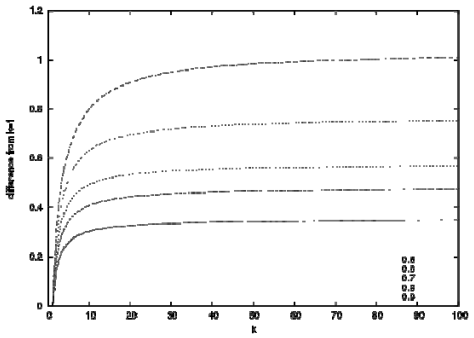


Figure 50. Difference between the standard and the reliable gossiping scheme

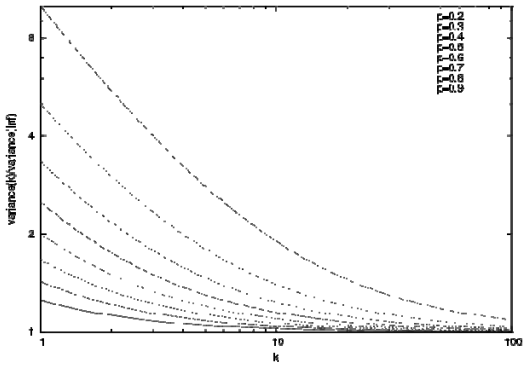


Figure 51. Variance of the path length distribution

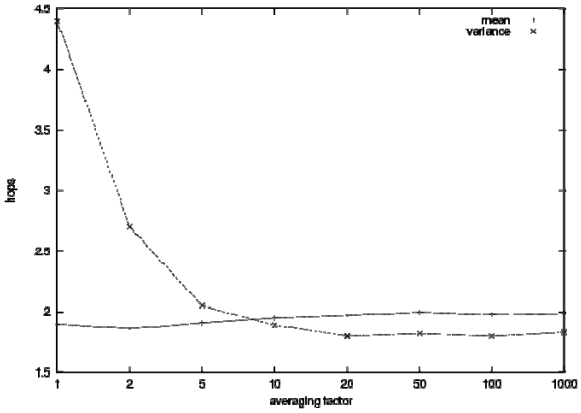


Figure 52. Simulation result for the variance decrease

The higher *K* is the better the reliability, but above a certain threshold the decrease of variance is negligible. The theoretical variance is shown in **Figure 51**. At small K values the variance decreases rapidly, but the lines quickly become nearly horizontal, and a K much larger than *100* does not make a difference anymore. The calculations presented so far only focused on a single propagation path. In an urban environment, however, there are several possible routes between two points, and the messages are broadcasted in every direction in the junctions. Thus, it is possible that multiple instances of a message arrive at a vehicle. The number of arriving instances and their delay are best examined through simulations. Therefore, we implemented the CLoUD protocol using Network Simulator 3, an event-based simulation environment designed for packet level simulations of wired and wireless networks hooked up with our road topology and vehicle placement managing tool. This tool is able to generate a TCDB for the road topology, visualise the results, and calculate the spread on road topology level with a modified breadth-first search algorithm. The behaviour of the protocol may be analysed though the event traces created during the simulation, and by examining the graphical representation of the results. The triangles on the roads represent the vehicles, while their colour reflects the number of received messages; the warmer the colour is, the more messages the vehicle received. The numerical results of a simulation run are shown in **Figure 52**. The variance of the coverage area decreases as expected, but the mean is small, due to the traffic conditions. The following papers have been produced based on these results [MV08] and [MV09].

3.3.2 Autonomic Sampling for Mobility Management in Wireless Sensor Networks

Introduction. Studying distributed sensor networks has been an area of interest among researchers since early 1990s. There was a trend to move from the centralised, extremely reliable, powerful and expensive platform to large number of cheap, decentralised and potentially unreliable components that as a group are capable of far more complex tasks than any individual super-node. Wireless sensor networks (WSN) are formed by one or more base stations (sinks), where the collected information or data is sent, and a large number of sensors distributed geographically over an environment and connected through a radio network. Sensors are low-cost and low-power tiny nodes equipped with limited sensing, computing, power, memory and radio communication capabilities. They typically have an irreplaceable power source, designed for single usage, and are deployed in an unplanned manner. In this section we study and evaluate the adaptive regression DE for distributed dynamic clustering in wireless sensor networks.

There is an essential difference in our terminology, as compared to the usual one, related to cluster definition. By cluster we indicate a subset of entities that could be potentially monitored (e.g., a set of coordinates where sensors could be placed), and not a subset of sensor nodes; thus, in our terms, cluster formation mainly depends on the environment, the physical phenomena in which we would like to find the redundancy. In order to better understand our model, we introduce some basic definitions. Let F be a set of entities that could be potentially monitored.

Then, $f_i \in F$ is the *i-th* cluster, i.e., a subset of F in which each of the entities can be mutually described based on another arbitrary entity in the same set, within a user specified error bound. Thus, we need to sample only one of the entities in the cluster, and can then compute any other entity in the same set. When cluster f_i is monitored using k nodes, we call it k-coverage, where the redundancy is $1{:}k$; thus, $k-1$ nodes can be sent to sleep mode. The number and topology of the clusters f are unknown, and they are dynamically changing depending on the physical phenomena, error bound and the goal and technology of the sensor network. For instance let's have two clusters f_i and f_j. If we have the technology to predict any of the entities in f_i based on the readings of any entity in f_j, the two abstract clusters will merge.

Problem's statement and its autonomic solution

A. Problem's Statement

The main function of this DE (Adaptive Regression DE) is to cope with the mobility issues in an event driven wireless sensor network. The problem can be formulated as follows. There are several mobile nodes in a sensor network, each one is moving, and the correlation structure of the measurements is changing as well. The main problem is to decide which node will extrapolate which one in the network, so as to minimise the extrapolation error and the overhead, while maximising the power savings and balancing the residual power after each sleeping cycle.

B. Autonomic Solution

First we assume that $\forall j \exists! i : n_i \rightarrow f_j$ (the coverage is perfect). Then, we try to merge clusters together as follows. Every sensor n_i tries to describe every other node n_j it has information about (e.g., by grabbing packets from the air). If n_i approximates successfully (beyond a user specified error bound) the measurements of another node n_j , it declares that the approximated sensor is in the same cluster and sends a message to it, containing its own battery capacity B_i and the inverse

parameters of the linear regression ($[a_{inv}, b_{inv}]$) that n_i calculated. Since node n_j has the inverse regressor parameters as well, each of the nodes can approximate the other. After node n_j sends back its own B_j to n_i, the node that has less energy left will go to sleep for a predetermined time n_p. In the course of performance evaluation we will consider this scenario as well.

Proposed Algorithm

In this section we propose the adaptive regression algorithm that can dynamically determine if two different clusters *fi* and *fj* can be merged together, switch off the redundant node and therefore prolong the global lifetime (GL) of the network. In the beginning, we assume that $\forall j \exists! i : n_i \rightarrow f_j$; the coverage is perfect, $N \geq |f|$ is satisfied. Let *x[t]* be a sample from one of the entities in cluster *fi* , sampled by node *ni* at moment *t*. Similarly, let *y[t]* be a sample from one of the entities in cluster *fj* , sampled by node *nj* at the same moment. Two clusters *fi* and *fj* can be merged at moment *tk* , for a period *tp* , if $\exists a(tk), b(tk)$ so that:

$$\frac{1}{t_p}\int_{t=t_k}^{t_k+t_p}\{y(t)-a(t_k)x(t)-b(t_k)\}^2dt \leq U_{err} \tag{16}$$

In our algorithm (for discrete time) this means that $\exists a(tk), b(tk)$ so that:

$$\frac{1}{t_p}\sum_{t=t_k}^{t_k+t_p}\{y[t]-a[t_k]x[t]-b[t_k]\}^2 \leq U_{err} \tag{17}$$

where *Uerr* is the user specified mean square error (MSE). Naturally, we have to know the MSE of our model before we send nodes *ni* or *nj* to sleep mode for a *tp* time interval. We have little choice here but to continuously measure the mean square error of our model, and if (17) is satisfied, presume that the process is stationary for another *tp* interval. Then, we send one of the nodes to sleep mode for *tp*, while the awaken node will regress the sleeping node's measurements and send them to the sink, on behalf of the sleeping node. The parameter estimation (line 10) in case of linear regression is well known, so we only summarise the equations. Let $\{x[t_k], y[t_k]\}$, $\{x[t_k+1], y[t_k+1]\}$, .., $\{x[t_k+t_p], y[t_k+t_p]\}$ be the discrete samples from clusters f_i and f_j, sampled by nodes n_i and n_j. If

$$a[t_k] := \frac{cov(\underline{x},\underline{y})}{\sigma^2(\underline{x})}; \qquad b[t_k] := E(\underline{y}) - a[t_k].E(\underline{x}) \tag{18}$$

the sum specified in (17) will be minimal; thus, the linear model is optimally set. In our algorithm we are continuously pushing the *[x, y]* pairs to a FIFO queue, and with each new learning pair we update the latest *a, b* parameters. For all of the monitored clusters ***f***, node *ni* can have separate and independent FIFO queues, so the algorithm can be fully distributed.

The adaptive regression is a continuous algorithm. After the initialisation (lines 1-3), in each iteration we are waiting for a sample from the monitored node *nj*. However, before we receive it, *ni* tries to forecast it in order to test the model's accuracy (lines 5-7). In order to compute the latest cumulated error, *ni* stores the forecast error in a FIFO queue, along with the samples for regression (lines 8-10). If the latest cumulated error is lower than a user specified error rate, *ni* will either go to sleep (lines 12-15) or send the approximated node *nj* to sleep (lines 16-21) depending on which node has more energy left. After the sleeping period, we increment all the elements in the error vector by a value depending on the sleeping time, in order to avoid multiple sleep cycles without the model's accuracy test (line 23). The process events procedure (line 25) processes the interrupts by other nodes that are monitoring us (answering others' go to sleep requests).

Algorithm 1 Adaptive Regression on n_i

Require: $EFifoSize$, $SFifoSize$, U_{err}, t_p
$n_i, n_j : (n_i \mapsto f_i \wedge n_j \mapsto f_j) \vee (n_i \mapsto f_i \wedge n_j \mapsto f_i)$
Ensure: *Perfect coverage of* $f_i \cup f_j$ and *power balancing*

```
1: init set ErrFIFO's size to EFifoSize;
2: init set SampleFIFO's size to SFifoSize;
3: init a ⇐ 1; b ⇐ 0; %first forecast is the same x
4: while (true) do
5:    x ⇐ sample(); %local node n_i sampling the env.
6:    y' ⇐ ax + b; %try to forecast n_j's measurements
7:    y ⇐ receive('y', n_j); %receiving n_j's y sample
8:    push(ErrFIFO, (y' − y)^2); %stores the forecast error
9:    push(SampleFIFO, [x, y]); %stores the data pairs
10:   [a, b] ⇐ LinReg(SampleFIFO); %updating params.
11:   if (mean(ErrFIFO) ≤ U_err) then
12:      send(n_i to n_j, GoSleep[B_i, a_inv, b_inv]);
13:      if (B_i < receive('B', n_j)) then
14:         SetSleepMode(t_p); %Sleeping for t_p
15:      else
16:         for i = 1 to t_p do
17:            x ⇐ sample(); %n_i samples the environment
18:            send(n_i to bts, x); %n_i sends its sample to bts
19:            y ⇐ ax + b; %n_i approximating the sleeping n_j
20:            send(n_j to bts, y); %sample in behalf of n_j
21:         end for
22:      end if
23:      inc(ErrFIFO, h(t_p)); %increment error vector
24:   end if
25:   ProcessEvents(); %Process outside events
26: end while
```

Figure 53. – The proposed algorithm

Scalability, Stability and Complexity Issues

The proposed solution is scalable, since all the DEs are monitoring a constant number of nodes in the vicinity and choosing one of them for the participation in the adaptive regression. Due to the fully distributed functioning and the continuous error monitoring the proposed model is stable, because if a particular DE detects extreme deviations in measurements, the user specified error will increase and the node disables the adaptive prediction. We validated the operation of our proposed model through simulations, which we present in the next section. The most computationally expensive phase is when the DE has to update the parameters of the linear regression, which is not more complex than O(n^2), where n is the length of the Sample FIFO.

Numerical Results. In this section we present two sets of simulations in order to evaluate the proposed scheme. The first pack evaluates the speed and accuracy of the adaptation, while the second pack evaluates the sleep scheduling process and different error rates in contrast to deterministic clustering solutions.

A. Evaluation of accuracy and adaptation speed

In **Figure 54** we can see the adaptation speed of our proposed scheme. The parameters of our algorithm are *[EF if oSize=3, SFif oSize=20,* U_{err} *=0.5,* t_p *=10]*. The a_{sim} and b_{sim} parameters are the simulation coefficients, showing how the relation between the two generated set of samples changes. We have chosen sinusoid shapes, with some inflection points, for these parameters, just as an illustration that would enable us to show how

adaptable the regression method is. On the other hand, a_{est} and b_{est} represent the parameters estimated by our algorithm. If we would decrease the size of the sample buffer (SF *if*oSize), the adaptation would be quicker, but the noise sensitivity would get higher as well. The minimal value of SF *if*oSize is 2, because this is the minimal number of points that can describe a linear relation.

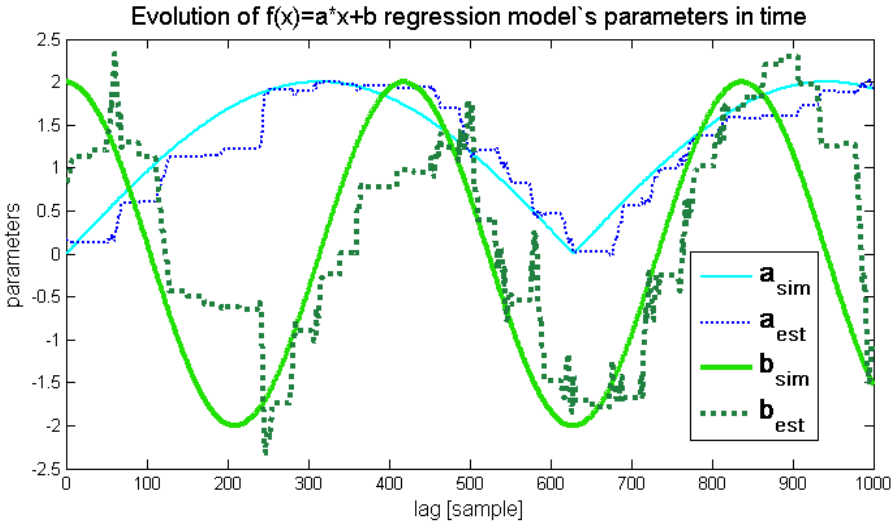


Figure 54. – Adaptation Speed

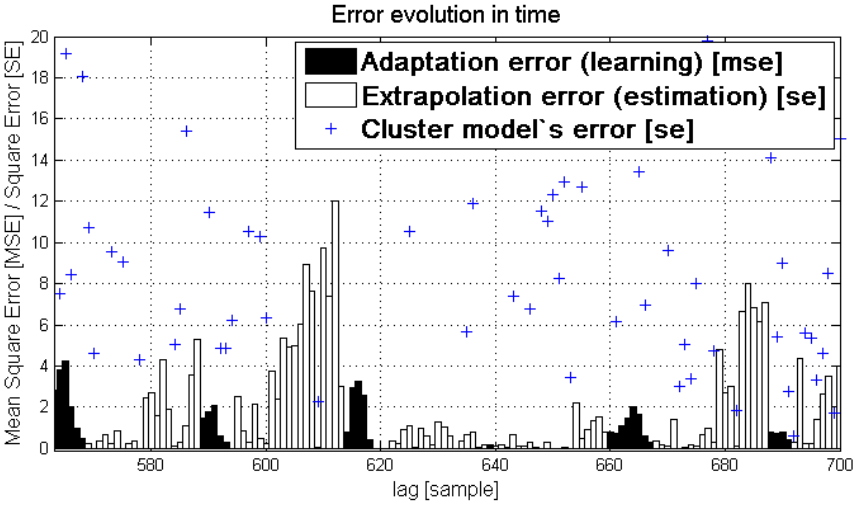


Figure 55. Sleep Scheduling Process

B. The Sleep Scheduling Process

In **Figure 55** we can see the sleep scheduling process of our proposed scheme. The parameters of our algorithm are *[EFifoSize=3, SFifoSize=6,*U_{err}*=0.5,* t_p *=20].* The black bars in the histogram indicate the adaptation error, which is the MSE error mean **(***ErrFIFO***)** in each iteration (algorithm 1, line 8), during the learning phase. The white bars in the histogram indicate the squared estimation error of the sleeping node. The black and white bars are alternating; when on one of the nodes the adaptation error decreases below U_{err}, the node which has less energy left goes to sleep mode. Then, after a sleeping period, a new

learning phase starts. In **Figure 55**, the sleeping period is $t_p = 20$, what corresponds to the number of white bars in each sleep stage. The crosses represent the error made by the traditional deterministic cluster based technique, in which there are two nodes as well, but one of them is always sleeping and the method assumes that the sleeping node would be measuring the same values as the awaken one. Thus, the error made by such a traditional approach is $Clust_{err}=(x-y)^2$ in each step. As it can be seen, the extrapolation error of our regression technique is significantly smaller, but the power consumption is slightly higher. If the sleeping period t_p would be smaller, the extrapolation error would be smaller as well, since the model is more frequently updated. Generally, the adaptation error is decreasing until it reaches the user specified error rate. The extrapolation error increases because the learned model's parameters are becoming more and more outdated. Note that there is a noise factor as well in the linear relation used by our model, which explains the jumps in the consecutive error bars [OV09].

4 RESILIENCE, SURVIVABILITY AND/FOR AUTONOMICITY

4.1 Introduction

In this chapter a detailed EFIPSANS vision on the topic of autonomic resilience and survivability is presented. First, resilience is discussed in relation to fault-management in self-managing networks, where the Unified Architecture for Resilience, Survivability and Fault-Management and its specific components are described. Following that, resilience in the context of auto-configuration and autonomic routing is analysed. This is done for MANETs where specific components of the platform for *Multi-path routing, Auto-configuration, Resilience and Survivability In context of fault-management for mobile Ad-hoc Networks* (MARSIAN), are detailed and the particular focus is laid on the interactions between auto-configuration and autonomic routing entities when triggered by the resilience module. More specific investigations on autonomic routing in fixed networks are given in the section that follows which elaborates on routing resilience for OSPF protocol. The chapter concludes with analysis of the adaptive level of recovery by indicating that the fluctuating nature of the failure probability, together with the static nature of existing fault-management systems, implies unused network resources for the operator. This might be addressed by providing real-time risk level assessment information adapting the level of recovery to the probability of failure.

4.2 Resilience in Relation to Fault-Management in Self-managing Networks

Introduction. The EFIPSANS research regarding Resilience addresses issues related to the *"node-resilience in the long term operation of an autonomic node"*. In particular, the role of automated Incident-Detection, Fault-Isolation, and Fault-Removal is being investigated with respect to its Resilience and Survivability aspects. This results in a number of synergies with the topic of Autonomic Fault-Management and requires components and mechanisms that exploit the relations between Resilience, Survivability and Autonomic Fault-Management. Therefore, the EFIPSANS project is coming up with *Unified Architecture for Resilience, Survivability and Autonomic Fault-Management* [TGV10] - UAFAReS. The architectural framework defines a number of components that should be implemented in the nodes of a network designed to exploit the converging aspects of Resilience and Fault-Management in the emerging autonomic networks. The architecture and its Resilience related components are presented in the further chapters of this deliverable. The aspects of Autonomic Fault-Management are elaborated in [D4.5].

Problem statement and its autonomic solution

We present our on-going work on Resilience related components of the *UAFAReS* architecture. The problem statement in that context is constituted by the need to design algorithms and mechanisms that fulfil the functions which have been assigned to the corresponding architectural parts. However, we want to emphasise that due to the converging character of Resilience, Survivability, and Fault-Management (now becoming *"autonomic"*) in self-managing networks, and due to the fact that we work on a unified node architecture for those functions, it is sometimes difficult to identify a particular component as realising only Resilience or only Fault-Management aspects.

Specific components that are being implemented are the so-called *Node Resilience Functions (NRF)* of a node, which can be further subdivided in *Fault-Removal Functions (FRF)* and *Fault-Masking Functions (FMF)*. The FRF functions are realised by the FM_DE[2] [D4.5] and the FMF functions by the RS_DE [D3.1]. Furthermore, detected (observed) incidents need to be disseminated to the relevant functional entities inside an autonomic node and across the network (area), which is realised by a component denoted as Incident Information Dissemination Engine (IDE). Such incident dissemination provides opportunities for diverse functional entities, e.g., protocol modules, applications and services, to implement intrinsic resilient mechanisms as to self-adapt to the challenging conditions in the network.

Proposed Algorithm

The first aspect pertains to Node Resilience Functions implementing in general an **"if *condition* then *action*"** logic. The condition is the occurrence of a particular symptom (failure/alarm) in case of the FMF functions. In case of the FRF functions, the condition is constituted by the result of the process of automated Fault-Isolation, i.e. the reaction is specific to the isolated fault. However, some of the actions issued by the FRF and the FMF can be contradictory or even harmful for the network. This depends on its current state, and the actions undertaken as a result of the isolation of multiple faults or the fault-tolerant reaction to multiple reported symptoms (failures/alarms). Hence the actions issued by the FMF and FRF must be synchronised towards a global goal for the FM_DE and RS_DE control loops running in parallel. Therefore, a component called **Action Synchronisation Functions (ASF)** was defined, which is the architectural module that ensures the **stability** of the RS_DE and FM_DE control loops running in parallel. The ASF is currently considered as part of the FM_DE. The component optimises a utility function based on the actions that are about to be issued by the FRF and FMF, and on the values of different metrics reflecting the state of the network and their corresponding importance. The ASF should be referred for all actions that are considered requiring synchronisation. The component was implemented, and evaluated in terms of its scalability. The results were published in [TCP09]. For further information regarding the ASF we refer the reader to [D4.5] , [D1.5b], [TCP09].

The existence of the ASF influences the FRF and FMF in the sense that the Event-Condition-Action logic must be extended as follows:

```
1.  if a particular fault isolated, or failure detected
2.      if  reaction to the event requires synchronization
3.          refer to ASF:
4.          if  action allowed
5.              execute action;
6.      else
7.          execute action:
8.      end if;
9.  end if;
```

Scalability, Stability and Complexity Issues

The critical part of this procedure is the referring to the ASF, since the synchronisation includes the optimisation of a binary-linear program, which is known to be NP-hard. However, the use of numerical optimisation algorithms provided by solvers such as Coin-OR [Coin-OR] proved to give reasonable results in terms of **scalability**. The corresponding results are presented in the next section.

The second aspect is the Incident Information Dissemination Engine employing diverse algorithms like gossiping, flooding, and multicast on top of the network layer or on top of the link

[2] In this chapter, for simplicity in the presentation, due to the large number of references in various DEs, in their corresponding acronyms their position within GANA's hierarchy is omitted.

layer when the protocol modules of the upper layers are in a faulty condition. In order to improve the **scalability** of the incident dissemination, we hold that the scope of the dissemination should be limited to an area of the network, e.g. OSPF area, which means that the flooding of the area will scale similarly as the LSA flooding inside an OSPF area. Additionally, the IDE must intelligently select the type of dissemination algorithm to use. For more details on the algorithm for the selection, we refer the reader to [D4.1 summary].

The **validation** of the Node Resilience Functions and the IDE will be performed in the course of the scenario *"Autonomic Fault-Management and Reactive Resilience for selected types of Black Holes in Fixed Networks"*, which is the goal of the current implementation activities.

Initial Numerical Results

In this section we present the results of the **scalability** evaluations related to the issue of stability and synchronisation of tentative actions in the context of Fault-Masking and Fault-Removal. We implemented such an ASF component and tested its response times to the limit. Our goal was to examine the performance of the overall processes implemented by the ASF component - 1) accepting synchronisation requests, 2) extracting the information about the requested actions, 3) preparing the requests in the form required by the native solver interface [Coin-OR], 4) solving the optimisation problem presented in [D4.5], 5) extracting the results of the optimisation and encoding them in response messages, and eventually, 6) responding back to the client DEs. The evaluations were conducted on a single Linux machine - Intel(R) Pentium(R) M processor 1.60GH, 509.2 MB RAM. Several experiments were carried out with different numbers of metrics and actions, different numbers of client DEs simultaneously requesting for synchronisation, and different number of requests issued by every client. **Figure 56** presents the results of our performance evaluations. The time measurements that are plotted on the Z-axis correspond to the maximum response time of an ASF component, after each of the simultaneously started ASF clients (DE mockups) have issued a number of requests (shown on the X-axis). In the environment described above it was impossible to complete the experiments with more than 70 client DEs started simultaneously. This could be due to the prototype design or an overload of the operating system. However, this is not relevant for the issue of Resilience, since it requires the synchronisation of tentative actions coming from only two DEs – the FM_DE and the RS_DE. Despite this, one can observe (**Figure 56**) that for 70 and fewer clients the response times were quite reasonable. Hence, we deduce that our ASF prototype can be used for fast synchronisation of tentative actions as required by the Node Resilience Functions.

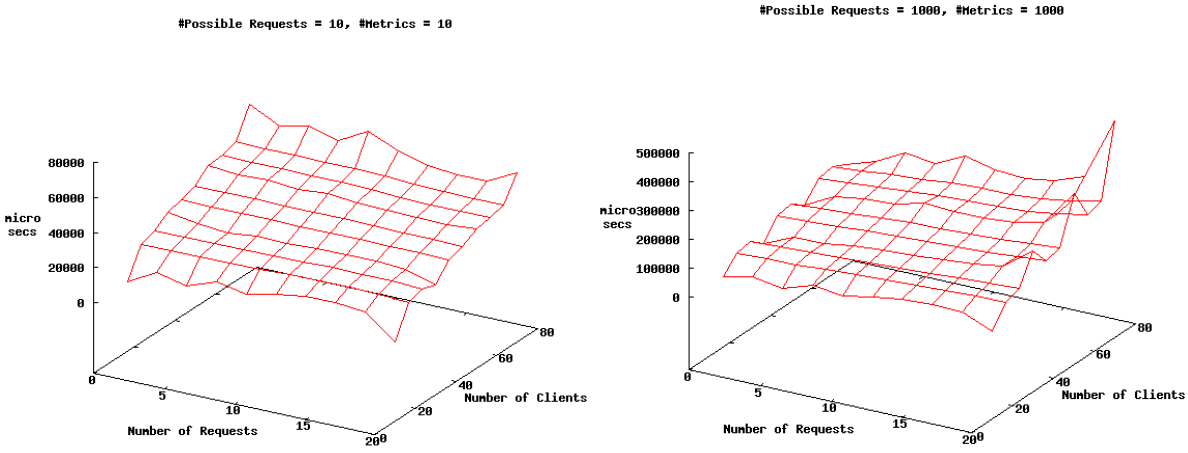


Figure 56: Performance evaluations of the proposed approach

Till now the following publications have been produced towards supporting the previous work [TCP09] and [TGV10].

4.3 Resilience in context of Auto-configuration and Autonomic Routing in MANETs

Introduction. During the course of EFIPSANS the MARSIAN platform [D2.1], [D2.4] has been proposed as a platform addressing the converging aspects of Multi-path routing, Auto-configuration, Resilience and Survivability In context of fault-management for mobile Ad-hoc Networks (MARSIAN). In fact, the aspects brought up during the development of the MARSIAN platform pertain to resilience, survivability and autonomic routing in IPv6 networks (in context of fault-management).

Problem's statement and its autonomic solution. In today's communications systems different diversified mechanisms intrinsic to some protocols or integrated with several node functional elements are not interacting with each other which may result in reduced network level self-healing capabilities. This especially holds true for MANETs where mobility of the nodes results in a constantly changing topology. To target this kind of scenarios MARSIAN platform was integrated with GANA as depicted in Figure 57. The work on resilience, survivability and fault-management in the context of auto-configuration and autonomic routing aims at defining the functionality of each element so that the mechanisms and actions performed to ensure resilience of a node and network are coordinated in such a way that the resilient behaviours orchestrated in each specific situation are not contradicting and stay in line with the predefined policies.

The proposed architecture being a part of the MARSIAN platform enables to take into consideration the information about the current state of the node and choose the best solution with regard to Resilience and Survivability from the plethora of possible methods that are implemented inside diversified functional entities of a node. This increases the self-healing capabilities of a node and a network as a whole. Especially resilient mechanisms in the components for Auto-configuration and Routing are taken into consideration.

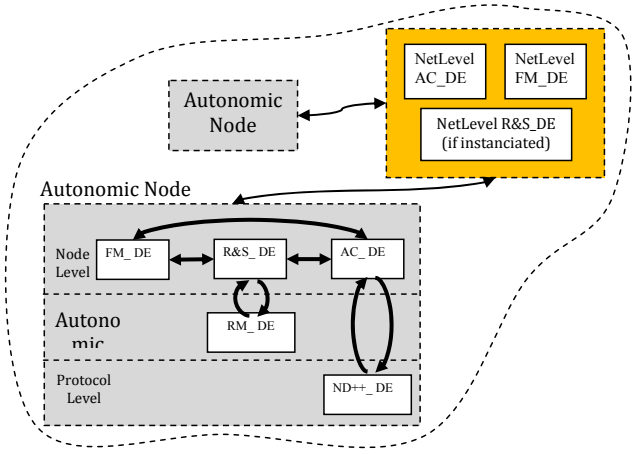


Figure 57. GANA overview for MARSIAN platform

Proposed Algorithm. The performed work concentrates on interactions between the Fault Masking Functions block of Resilience & Survivability DE [TGV10] and the Auto-configuration DE as well as the Routing Management DE. In the investigated scenario nodes create a multi-domain MANET network, where domains can merge or split. As such, when the lack of connectivity with one of the nodes occurs (e.g., due to the lost link or node failure) the node and/or network should undertake resilient actions in order to mask the occurrence of the fault. The RS_DE performs the action by activating resilient mechanisms intrinsic to other entities within the node. In the investigated case one of the actions can be to reroute the traffic and use the Routing Management DE to adjust routing protocol actions to the current situation. In particular, assuming

OLSR (Optimized Link State Routing) protocol primary, secondary and lower order MPR (multipoint relay) nodes can be identified which can be then used to instantiate multiple-path routing as well as provide re-routing in case of failure. According to the policies a node might need to merge with other sub-domain that appeared in the neighbourhood. In this case, it would be better to re-configure the network first and then potentially modify routing schemes if the problem still occurs. In the proposed scenario RS_DE is responsible for analyzing the policies and behaviours of a node as well as capabilities of AC_DE and RM_DE, as well as undertake decisions about which resilient mechanisms to use in the current situation that would best enable to reach the goal defined by specific policies. The proposed algorithm is still subject to further research, however, the basic functionality and the process of interactions between RS_DE, AC_DE and RM_DE can be specified by the following high level algorithmic description:

```
1.  if the failure related to topology occurred (e.g. the connection with node y is
        lost):
2.      execute:  FM_DE action to isolate the root cause (fault) and invoke
                  RS_DE - mask the failure/fault;
3.          do:
4.              get information from MLRP Repository about DEs with
                    resilient mechanisms applicable in this case;
5.              if AC_DE is identified and RM_DE is identified:
6.                  if AC_DE is about to reconfigure the group of nodes:
7.                      if new routes to the destination will be established or
                            new node will join a network or misbehaving node
                            will join another sub-network:
8.                          refer to ASF:
9.                              if action allowed
10.                                 execute: run AC_DE action to mask the
                                        fault;
11.                         if RM_DE action required by RS_DE
12.                             execute: RM_DE routine;
13.                     else
14.                         execute: RM_DE routine;
15.                 else
16.                     execute: RM_DE routine;
17.             end if;
18.         while failure/fault is still to be masked;
19. end if;
20.
21. RM_DE routine:
22.     refer to ASF:
23.         if action allowed
24.             execute: IP fast re-routing;
```

Scalability, Stability, Complexity and Validation Issues. Multi-domain setups are investigated to ensure scalability whereas stability is to be verified at the test-bed (with regard to auto-configuration) and with the aid of OPNET simulations (for autonomic routing). Both platforms will be used for validation of the work performed in WP2 as well so indirect results will be available for WP3 as well. Complexity of the solution is kept at a reasonable level through the encapsulation of each of the analysed items into a building block of the MARSIAN platform.

So far the architecture [TGV10], [D3.1] supporting the envisioned functionality has been developed as a joint effort in T3.3. Further work will concentrate on the interactions between AC_DE, RS_DE and RM_DE and specification of functionality of FMF block, so that the resilience of the autonomic node in a MANET network is supported in the best possible way. Although no direct validation of this concept is envisioned, as work in T3.3 concentrates mainly on the architecture development, the aspect of resilience is an important part of scenario dedicated for Telcordia's testbed with the goal to demonstrate selected features of the MARSIAN platform. The aspect of resilience will be also included in the simulations regarding autonomic routing.

4.4 Routing Resilience

Introduction. Open Shortest Path First (OSPF) is a routing protocol used to determine the correct route for packets within IP networks, it can satisfy most types of networks. Despite the wide-spread use, OSPF is not efficient in some specific customised networks. These networks contain some key links which plenty of shortest path pass through (we called key links as important links). The network needs to react quickly on the important links' state changes (e.g., link failure), while react normally on the unimportant links' state changes.

Simply changing the OSPF timer faster (e.g. using subsecond HELLO timers) may detect the link state changes quickly, but this may react too sensitive to all the links and may introduce network flap. Therefore, only changing the OSPF timer could not solve the above problems properly.

Problem statement and the corresponding autonomic solution. We introduce a controller to OSPF, called RR_DE, which may monitor the network and select different policies to control OSPF when different link state changes happen. RR_DE works like OSPF but using a faster HELLO interval, each router running RR_DE generate "Link State Advertisements" (RR_DE type LSAs) to create and maintain a view of the topology of the entire network. After the computation of SPF in OSPF, RR_DE starts to compute its own SPF using Floyd Algorithm that can compute all node's shortest path to the destination. Through this method, RR_DE can compute every link's important value (the total shortest path passing through this link).

For different link's important value, RR_DE adopts different policy to trigger OSPF changing its timer. For instance, if a link has a low important value, that stands for a low number of flows on this link. The RR_DE does not control the OSPF. A normal convergence of OSPF will be efficient. If a link has a high important value, that stands for a high number of flows on this link. This link's state change will trigger RR_DE to notice OSPF changing its Hello timer. Totally, RR_DE is just a controller of OSPF, without intervening with the network flow.

Proposed Algorithm. RR_DE is composed of five main components: LSDB (Link-State Database), destroy database, communication process, policy selection and the interface with OSPF:

- LSDB database is a fundamental component of RR_DE. It is responsible for storing all the link state information used for computing the shortest path of all nodes.
- Destroy database is the core of RR_DE, RR_DE uses the LSA data from LSDB compute the shortest path. Destroy database contains all link's important value and the shortest path through these links.
- RR_DE has three communication protocols, the main functions of which are the following:
  - The RR_DE Hello protocol is used for establishing and maintaining neighbor relationships. It also ensures that communication between neighbors is bidirectional. The hello packets are sent by the router every "hello interval" seconds from all router interfaces. RR_DE uses the "interface state machine" to establish and maintain the neighbor relationship.
  - When two routers have established the neighbor relationship on a point-to-point link, they begin to synchronise their topological databases. The initial synchronisation is performed through the exchange protocol. The RR_DE exchange protocol uses "database packets" to describe its database. Thus, it is using the following steps that describe the exchange process between two routers.

    (1) Set Master and Slave. The fist step of the protocol is to select the master and slave. This step needs the two routers to negotiate with each other to determine which router is the master router through sending exchange packets. The router with larger node ID would take the role of master router.

(2) Exchange Process. Once the roles of the router have been distributed, the asymmetric exchange begins. The master router will send its database in a sequence exchange packet. The packets will be sent in sequence and should be sent one at a time. After each packet is sent, the slave router will send an acknowledge packet (An exchange packet with the same sequence number). When the master transmits its last database record, it will set the more bit to 0. At this point, the master begins to send its database. The end of exchange process occurs at the point when the two routers send exchange packet setting *M* bit to *0*.

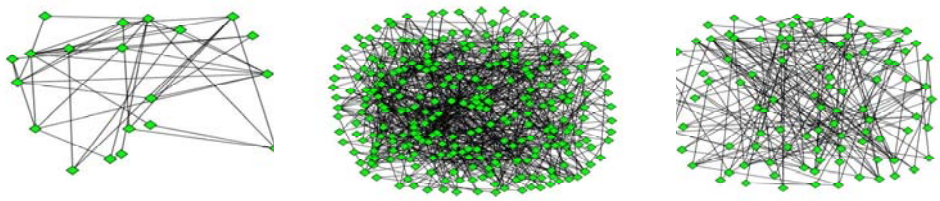
- A flooding packet may contain several distinct advertisements, and floods each advertisement one hop further from its point of origination. To make the flooding procedure reliable, each advertisement must be acknowledged separately. When a link state is changed (e.g., link failure), a router will send a flooding packet to its neighbors. The flooding process starts when a flooding packet has been received by one of its neighbors. For each advertisement in the flooding packet, the sequence number is compared to the value in the local database. If the sequence number is a new value, the neighbor floods the new advertisement on all other interfaces.

On observing or receiving any information that indicates a change in the network state, the RR_DE will decide whether and to what degree the network state has changed. Using the evolution result as an index, RR_DE could find corresponding timer configuration policy in the policy database and use it to control the timers of OSPFV3. The knowledge base of RR_DE stores established policies and each policy matches one kind of environment.

Scalability, Stability and Complexity Issues. The scalability of RR_DE is a least as good as that of OSPF and even better in many cases, since RR_DE is not bundled with route computation and it needs not to worry about the negative effects of small hello interval and timely computation when detecting failures. This also guarantees the stability of RR_DE. The basic functions of RR_DE are going to be validated through simulations after we finish the development of RR_DE simulation software and will be included D3.4 (M36).

Initial numerical results. There is no central control in our RR_DE framework. Therefore, we tested its function and compared its efficiency with OSPF through simulations based on SSFNET concerning three different scenarios. The first scenario is a *20* nodes network. Results show that when 30% of the using path were destroyed simultaneously (correspond to 30% damage degree) RR_DE reacted swiftly in evaluating damage degree, searching for policy and enforcing the policy. Network with RR_DE outperforms pure OSPF network dramatically in convergence time. In the second scenario the number of nodes increased to *100*. After 30% routing paths were broken we found that RR_DE still outperformed pure OSPF a lot. But compared with the *20* nodes scenario the convergence time is rather long. This is mainly because increased network diameter prolonged the LSA dissemination time of RR_DE. In a *300* nodes scenario (i.e. scenario 3) both the convergence time of OSPF and OSPF+RR_DE were increased accordingly with the network diameter. But OSPF+RR_DE proposed scheme still work much better than pure OSPF.

All the simulation results above demonstrate that RR_DE has good scalability. It could work well in networks with diverse scale in a distributed way.



Scenario 1 *Scenario2* *Scenario3*

	20 nodes	*100 nodes*	*300 nodes*
OSPF convergence time	*45.350s*	*60.056s*	*61.822s*
OSPF+RR_DE convergence time	*0.497s*	*11.614s*	*13.934s*

Concerning the previous analysis and results the following publications have been achieved [XCLL] and [WCLL08].

4.5 Adaptive level of Recovery

Introduction. Since today's operators provide guaranteed reliability to their end-users, they need to handle any failure within their networks, by using various fault management systems. The fluctuating nature of the failure probability and the static nature of the fault-management systems imply unused network resources for the operator. We propose to improve fault management functions by providing real-time risk level assessment information in order to adapt the GMPLS level of recovery to the probability of failure.

Problem statement and its autonomic solution. The static nature of fault management systems compels operators to design their infrastructure to be capable of handling the worst situation. Such strategies based on over-provisioning provide reliable services with elements dedicated to failure management most of time unused. We propose to improve fault management functions by providing real-time risk level assessment information in order to reduce operator's costs by avoiding useless redundancy.

A Risk Assessment Modules (RAM), placed in the node level RS_DE, is in charge of spreading real-time risk assessment information in the network. The risk assessment description needs details to be relevant for candidate DEs, and incorporate 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. This prediction is based on the monitoring of internal state and behavior of a node involving specific parameters, which are significant enough to predict a future failure, such as the hardware temperature, the signal quality, anomalies, etc…

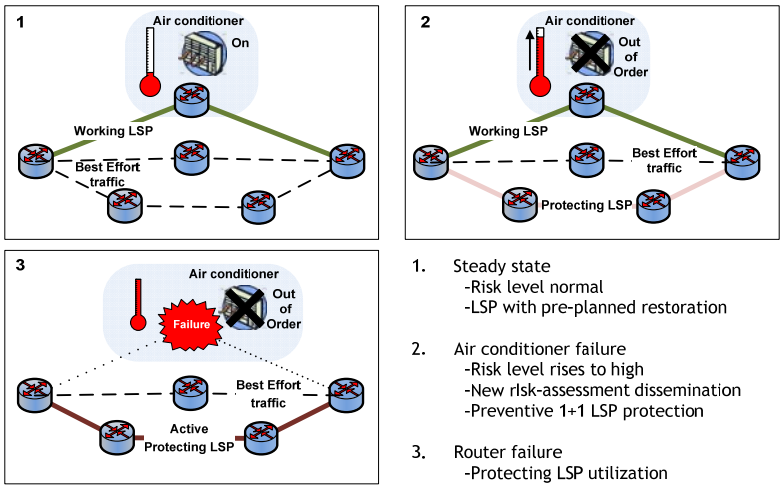


Figure 58. GMPLS Adaptive level of recovery

The node level RS_DE can exploit the failure predictions to anticipate failures by temporary raising the recovery level of GMPLS Label Switch Paths (LSP). GMPLS standards provide different level of recovery starting from the pre-planned restoration and ending with the 1+1 protection, where the resulting availability performances are proportional to the consumed network resources. A proactive strategy would exploit a light recovery level, like a pre-planned restoration, in normal time in order to preserve network resources and would switch toward a 1+1 protection during all the critical periods, thanks to risk level warnings. In order to execute this process without disturbing the end user's services, we need to create new LSP with new recovery level using Make-before-break tools, such as the Shared Explicit option. The benefits of such measures are network resources saving, by finely fitting the recovery resources to the risk incurred, with a direct cost economy for operators.

Proposed Algorithm

```
1.  for all node in Network do
2.
3.    if  node->risk_Level_Assessment > node->old_Risk_Level_Assessment
4.      for all lsp in node-> LSPs do
5.            create new_Working_LSP with SharedExplicit option
                    (Make-before-break)
6.            create new_Protection&Restoration_Path
                    with higher Recovery level
7.             execute Associate(new_Working_LSP,
                          new_Protection&Restoration_Path)
8.             execute   Switch traffic From lsp->working to
                          new_Working_LSP
9.             delete lsp-> protection&Restoration_Resources
10.            delete lsp->working
11.         end for;
12.
13.     else if node->risk_Level_Assessment <node->old_Risk_Level_Assessment
14.        for all lsp in node-> LSPs do
15.           create new_Working_LSP with SharedExplicit option
                    (Make-before-break)
16.           create new_Protection&Restoration_Path
                    with lower Recovery level
17.            execute Associate(new_Working_LSP,
                          new_Protection&Restoration_Path)
18.            execute   Switch traffic From lsp->working to new_Working_LSP
19.            delete lsp-> protection&Restoration_Resources
20.            delete lsp->working
21.     end for;
22.   end if;
```

Scalability, Stability, Complexity and Validation Issues. The scalability performance will be measured by simulation on different size of networks, with different number of LSPs, while the stability of such solution depends on the failure prediction accuracy and the occurrence of failure in the network. We will evaluate the stability issues by measuring the impacts of errors in the prediction function and the limit of the solution with regards to the amount of failure. Validation of the solution will focus on comparing the solution with the actual mechanism to show the benefit in term of average available bandwidth while keeping the same level of availability. Additionally, the solution involves well known algorithms such as path calculations that do not need additional complexity evaluation.

Validation and specific numerical results are not available yet, but an integration work has been done with other resilience and survivability issues to build a coherent Resilience and Autonomic Fault Management architecture composed of two DEs. Moreover, a scenario using the concept proposed in this issue but applied for routing purposes has been defined in the WP2 and will demonstrate the feasibility of the risk assessment module. Validation and results are expected in the near future, first for the next délivrable D3.6 and most of all for the délivrable D3.4 dedicated to resilience and survivability. Expected results will intend to demonstrate the benefit of such a solution on the average available bandwidth while keeping the same level of availability [TGV09].

5 CROSS LAYERING AND AUTONOMICITY

5.1 Introduction

Breaking with the approach of separating the different layers in the OSI model, cross-layer usage allows information exchange over several layers and enables direct communication between e.g., network- and application layer. Cross-layer technology thus allows the usage of parameters, which are difficult to 'use' otherwise. In Task 3.5, we use cross-layer technologies and autonomicity mainly in two areas:

1. Improvement of Quality of Service (QoS) in wireless networks (*Section 5.2*).
2. Improvement of performance and security in peer-to-peer (p2p) networks (*Section 5.3*).

Cross-layer technologies are widely used in wireless networks in order to adjust QoS by using information that is available on the network layer. In the context of this project, we consider QoS-aware power and rate control in autonomic CDMA networks and we also propose techniques to increase QoS mechanisms in WMNs (wireless mesh networks) using a time and frequency division approach.

The aim of the first approach is to minimise power consumption and interference by assigning power and rate to maximise overall goodput by self-adaptation of transmission power in each node. Results show that nodes using the higher power levels receive the lowest utility, where nodes with the lowest power receive the highest utility.

Besides the power-aspect, wireless networks often face bandwidth issues. Especially in Wireless Mesh Networks studies show that (if uncoordinated) the service bandwidth degrades exponentially to 0.5^n at n-hop distance to the hot-spot. First results using a time scheduling approach were further improved by as an improvement, a frequency division algorithm is proposed that will be integrated in a Decision Element (DE) to set-up and maintain the topology of a WMN. An algorithm is already proposed and the simulation results will be available in the next deliverable [D3.6].

In P2P networks, cross-layer usage is not very common, however could be one possibility for further improvements. By taking into account the physical network, improvement of P2P routing tables for faster downloads and more efficient resource utilisation is envisaged, by which both participants, users and network operators, will benefit.

Another approach of using cross-layer technologies is the exchange of data, initiated from higher layers, whereas usually information is pushed up the OSI model for further processing. The main idea here is to use information that is available on the overlay to improve routing and by this increasing the security of the system. We do this by improving disjoint data routing, not exclusively on the overlay but also on the underlying network.

5.2 Autonomic Multihop Networks

5.2.1 Utility-based distributed QoS-aware power and rate control in autonomic CDMA ad-hoc networks

Introduction. Wireless ad hoc networks have become very popular due to their capabilities to provide effective services to mobile and nomadic users. With the framework of EFIPSANS project, a generic autonomicity-driven framework for efficiently assigning power and rate in autonomic CDMA ad-hoc networks is proposed, in order to minimise power consumption and

interference, and maximise overall goodput under the imposed physical limitations. The corresponding problem is formulated as a non-cooperative game where users selfishly aim at maximising their performance by means of a utility function. Moreover, a distribute Autonomic Power & Rate Control (APRC) algorithm for CDMA ad-hoc networks is devised, aiming at enabling each node to *self-adapt* its transmission power and rate towards *self-optimising* its average utility performance. The proposed mechanism operates in each node, requires locally exchanged information between neighboring nodes and takes decisions on node's power and rate in time-slotted bases. Finally, a PROTO_LEVEL_CDMA_AHN_R&Q_DE has been developed towards realising the proposed autonomic mechanism in line with GANA architecture.

Problem's statement, solution and an autonomic mechanism

A. System Model & Assumptions

We consider a wireless CDMA ad-hoc network that consists of a set S of N nodes and a set of links L. A link from node i to node j, denoted as (i, j), is an abstract representation of communication and/or imposed interference between them. The channel conditions of each link are affected by long-time scale variations due to users' low mobility, shadow fading and fast fading and therefore, can be modelled as stationary time-varying stochastic processes. Thus, let as denote as $G_{i,j}$ the random variable of the instantaneous path gain from transmitter i to receiver j. Time is divided in fixed length time slots. At the beginning of every time slot t each node $i \in S$ determines its transmission power $P_i(t)$, its transmission rate $R_i(t)$ and selects its destination nodes, under the assumption that network link's channel conditions are fixed within the duration of a time slot. The set of node's i destinations at time slot t, $S_i(t) \subseteq S$ is determined not only by the network's routing protocol but also from its proposed Autonomic Power and Rate Control (APRC) mechanism. Each of these nodes will receive complete or partial information transmitted by user i at the corresponding time slot. In order to exploit the advantages of the CDMA multiple access scheme towards maximising the overall network performance, we allow simultaneous transmissions of one node to many, as well as simultaneous reception at a node from many. In addition, each node can receive data wile it transmits data (i.e., full duplex scheme). Node's i transmission power is upper bounded due to hardware limitations and lower bounded due to network's connectivity issues (i.e., $P_i(t) \in [P_i^c, P_i^{\max}]\ \forall i \in S$). In our analysis we assume that $P_i^c << P_i^{\max}\ \ \forall i \in S$, therefore there exists a fixed set of neighbors for node i denoted by S_i^c, which contains exactly those nodes determined by P_i^c. Moreover, we assume that a user's destination set is always a subset of his neighbor set (i.e. $S_i(t) \subseteq S_i^c$), due to the routing operation. For a given node i, $R_i^{\max}$ is the maximum achievable rate at which he can transmit data. Further, considering the transmission of node i, let us denote by $\gamma_{i,j} = E_b / I_o$, $j \in S_i(t)$ the bit energy to interference density function at the receiver j which regarding conventional matched filters can be expressed as:

$$\gamma_{i,j}\left(R_i(t), P_i(t), \bar{P}_{-i}(t)\right) = \frac{W}{R_i(t)} \frac{G_{i,j}(t)P_i(t)}{\theta \sum_{\substack{k=1 \\ k \neq j}}^{N} G_{k,j}(t)P_k - \theta G_{i,j}(t)P_i(t) + I_o} = \frac{W}{R_i(t)} \frac{G_{i,j}(t)P_i(t)}{I_{j/i}(\bar{P}_{-i}(t))} \quad j \in S_i(t), \tag{19}$$

where, W is system's spreading bandwidth, θ is the orthogonality factor ($0 \le \theta \le 1$), $\bar{P}_{-i}(t)$ is node's power vector excluding node i; $G_{i,j}(t)$ is the path gain from transmitter i to receiver j at time slot t, I_0 is the background noise and thus,

$$I_{j/i}(\bar{P}_{-i}(t)) = \theta \sum_{k=1, k \neq j}^{N} G_{k,j}(t)P_k - \theta G_{i,j}(t)P_i(t) + I_o . \tag{20}$$

Each node has a proper utility function U_i which represents his degree of satisfaction in relation to the expected tradeoff among the actual amount of data received correctly by its receivers per unit of energy consumption at time slot t, defined as:

$$U_i\left(R_i(t),P_i(t),\bar{P}_{-i}(t)\right)=\frac{\sum_{j\in S_i(t)} a_{i,j}(t)R_i(t)f_i\left(\gamma_{i,j}\left(R_i(t),P_i(t),\bar{P}_{-i}(t)\right)\right)}{P_i(t)} \quad (21)$$

where $a_{i,j}(t)$ is 1 when node j is selected to receive part of the total amount of information transmitted by node i at time slot t and 0 otherwise. The values of $\bar{a}_i(t)=(a_{i,1}(t),...,a_{i,j}(t),...,a_{i,|S_i(t)|}(t))$ are determined by the node's i APRC mechanism and its information is biggypacked at the transmitted packets. Further, f_i represents a function for the probability of a successful packet transmission from node i to node j with respect to the instantaneous signal to interference and noise per bit ratio at j and depends on the transmission schemes (modulation and coding) being used. We assume that f_i function has the following properties: (a) f_i is an increasing function of $\gamma_{i,j}$. (b) f_i is twice continuously differentiable sigmoidal function. (c) $f_i(0)=0$ to ensure that $U_i = 0$ when $P_i = 0$. (d) $f_i(\infty)=1$. These are valid assumptions for many practical scenarios when packets size M is reasonably large (i.e., $M = 100$ bits) [MCPS06].

B. Problem Formulation and Solution

Each node's i *A*PRC mechanism determines its minimum power level P_i^c that reassures network's 1-conectivity ([LH05]). Moreover, it determines neighboring nodes (i.e., set $S_i^c \subseteq S$). We assume infinite backlogs for each node in the connectivity set S_i^c of node i and hence, $S_i^c \equiv S_i(t) \equiv S_i$. At the beginning of its time slot the APRC is executed individually in each node in the network to obtain its power and rate levels for that time slot, as well as to specify the nodes from its destination set that will receive data (i.e. determine the values of the $a_{i,j}(t)$ indicators $\forall j \in S_i$). Each node in the network aims at the maximisation of the expectation of her utility U_i, therefore the corresponding goal of his APRC mechanisms can be expressed as the maximisation of the objective function:

$$\max_{\bar{a}_i(t),R_i(t),P_i(t)} E\left(U_i\left(R_i(t),P_i(t),\bar{P}_{-i}(t)\right)\right) \quad (22)$$

Consider the Power and Rate Control Game (PRCG) $G=[S,\{A_i\},\{U_i\}]$ where S is the set of nodes-players and $A_i=[0,R_i^{\max}]\times[P_i^c,P_i^{\max}]$ is the strategy set for the i^{th} user. Each strategy in A_i can be analytically written as follows

$$\{\bar{R}_i,\bar{P}_i\}=\{(a_{i,1},...,a_{i,j},...,a_{i,|S_i(t)|})\cdot(R_i,...,R_i,...,R_i),(a_{i,1},...,a_{i,j},...,a_{i,|S_i(t)|})\cdot(P_i,...,P_i,...,P_i)\} \quad (23)$$

incorporating the ability of the node to select those nodes from their destinations set that will receive data. Fixing the other nodes' transmission powers and rates (i.e., the corresponding interference at its destinations) and permitting only point to point transmissions in the game, which is quite realistic due to node's hardware limitations, the utility-maximising strategy for user i can be obtained by solving the following constrained maximisation problem:

$$\begin{aligned} &\max_{\bar{a}_i,R_i,P_i} U_i\left(R_i,P_i,\bar{P}_{-i}\right) \\ &s.t. \quad 0\le R_i \le R_i^{\max},\ P_i^c \le P_i \le P_i^{\max} \\ &\sum_{j\in S_i} a_{i,j}=1,\ \ a_{i,j}=0 \text{ or } 1 \ \ \forall j\in S_i \end{aligned} \quad (24)$$

We adopt *Nash equilibrium* to solve PRCG which is most widely used for game theoretic problems. At equilibrium no node has the incentive to change its power and rate levels since its utility can not be further improved by making any individual changes on their values, given the power and rate vectors of other nodes. For presentation purposes, in the rest of this section let us denote as $\{\bar{R}_i,\bar{P}_i\}\equiv\{R_i,P_i\}$ node's i strategy space due to allowance of unique node transmission.

Definition 1: The power and rate vectors $P^*=\left(P_1^*,...,P_N^*\right)$, $R^*=\left(R^*_1,...,R_N^*\right)$ are a Nash equilibrium of the PRCG, if for every $i\in S$, $U_i\left(R_i^*,P_i^*,P_{-i}^*(t)\right)\ge U_i\left(R_i,P_i,P_{-i}^*(t)\right)$ for all $(R_i^*,P_i^*)\in A_i$.

Initially, we characterise single node's utility maximisation when other users' transmission powers and rates are fixed. The following proposition asserts the existence and the uniqueness of a Nash equilibrium point of the above reduced power control game and hence, determines nodes' transmission power vector at equilibrium when all nodes has determined the optimal destination nodes ant their corresponding optimal transmission rates.

Proposition 3 The Nash equilibrium of the non-cooperative game (24) is given by P_i^*, where $P_i^* = \max\left\{P_i^c, \min\left\{\frac{\gamma_i^* R_i^{\max} I_{j/i}^*}{WG_{i,j}^*}, P_i^{\max}\right\}\right\}$. Here, γ_i^* results from the unique positive solution of equation $f_i'(\gamma)\gamma - f_i(\gamma) = 0$. Furthermore, the equilibrium exists and is unique.

Proof: The proof can be found in [TKP08].

Proposed Autonomic Algorithm and corresponding DE

In this section, we present an iterative and distributed opportunistic power and rate control algorithm for reaching the Nash equilibrium for the PRCG game *G* at every time slot *t*.

A. APRC Algorithm

Initially: Node's *i* power level, P_i^c, is determined along with its destination node set S_i.

(I) At time slot *t*: Node *i* transmits with maximum power $P_i^{\max}$. Set $k = 0$.

(II) Broadcasts its interference $I_i^{(k)}(t)$, receives its destination nodes interference $I_j^{(k)}(t) \forall j \in S_i$ and computes $I_{j/i}^{(k)}(t), \forall j \in S_i$. $I_j^{(k)}(t)$ is the total interference at node *j*.

(III) Determines its optimal destination node $j^{*(k)}$, its optimal transmission rate $R_i^{*(k)}$ and transmission power $P_i^{*(k)}$, according to Propositions 1-3.

(IV) If powers converge then stop, and at the beginning of the next time slot go to step (I)

(V) Transmits with $P_i^{*(k)}$.

(VI) $k = k + 1$, go to step (II).

It is clear that when the algorithm converges, it converges to the Nash equilibrium of the PRCG, which always exists as explained in the previous section. That also asserts the **stability** of the proposed autonomic approach. On the other hand, since multiple equilibrium points exist, the above algorithm converges to one of the equilibria. However, the Pareto optimality of the solution is not asserted. At equilibrium, the maximisation of user utilities is achieved while throughput maximisation is obtained. Finally, the **complexity** of the proposed algorithm is very low since one division and one comparison has to be made by each user per iteration.

B. Towards Autonomic CDMA Ad-hoc Network – A GANA Oriented Approach

To accomplish the above goals, i.e. realise APRC algorithm in line with GANA, a new Protocol Level DE is introduced, namely, Protocol-Level CDMA-Based-Ad-Hoc-Node's-Resource-Allocation-And-Quality-Of-Service-Management Decision-Element (PROTO_LEVEL_CDMA_AHN_R&Q_DE). The basic operational steps of the control loop enabled by PROTO_LEVEL_CDMA_AHN_R&Q_DE are outlined as follows:

On a time slotted basis, the DE (introduced above) residing at each CDMA Ad-Hoc node, will realise a control loop, in line with APRC algorithm, which:

Step 1. Constantly monitors a user's service performance and its wireless environment ((I) and (V)),

Step 2. Analyses its current status with respect to QoS requirements (II) and,

Step 3. Reacts to QoS triggering events via the dynamic alteration of user's transmission power and transmission rate. Furthermore, it specifies the nodes from its destination set that will receive

data. All the above are achieved by formulating and participating in a distributed, utility non-cooperative game (III).

Moreover, the information required for the operation of the introduced DE, will be obtained via periodically "listening" to its closest neighbors broadcasts. The information contained within these broadcasts will include, a) neighbors overall received interference, b) point to point link status and c) connectivity. Finally, the node itself will monitor its current services' QoS status. For details concerning PROTO_LEVEL_CDMA_AHN_R&Q_DE we refer to D1.5.

Evaluation Results

In this section, we provide some numerical results illustrating the operation and features of the proposed framework and the distributed APRC algorithm. Initially, for demonstration purposes we consider an example scenario of ten nodes, where the algorithm's convergence and opportunistic nature is exhibited. Then, the APRC algorithm's performance and **scaling properties** are demonstrated for an increasing number of nodes. Henceforth, we consider the following values of system parameters, as shown in Table 5.

Table 5. Simulation Parameter Values

Value	Parameter
$P^c = 1$	min. trans. power of a node (mW)
$P_{\max} = 800$	max. trans. power of a node (mW)
$R^{\max} = 100$	max. trans. rate of a node (kbits)
$W = 10^6$	spread spectrum bandwidth (Hz)
$\sigma = 5 \cdot 10^{-16}$	AWGN noise power at receiver
$\gamma^* = 8.1$	target SINR
$\alpha = 4$	path loss gain

A. Evaluating Network's & Nodes' Performance under the Proposed Autonomic Approach

The generated topology that was studied for a network with $N = 10$ nodes is shown in Figure 59a. Node locations were uniformly and randomly selected. The behavior of the system is presented for a single time slot, in order to study the corresponding properties of the game's equilibria. In Figure 59b, the selected destination of each node within an arbitrary time slot is shown as the games evolves. Each curve corresponds to a network user, as denoted in the legend, and the vertical axis represents the corresponding destinations. The curves depict the selected target nodes in each iteration of APRC algorithm until the latter determines the final destinations. It is noted that user destinations fluctuate within the duration of the game due to the opportunistic nature of the APRC algorithm. Specifically, some users do not change their initial selection, while others change it (particularly in the early iterations of the algorithm). User pairs that select each other, i.e. 9-10, 3-6 and 4-5, do not change their initial choices for the duration of the iterative process. By inspection of the corresponding topology (Figure 59a), these pairs seem the most appropriate with respect to the geometric distances and number of neighbors in their neighborhood locality. Moreover, nodes 7, 8 are not selected at all for receivers by other nodes and as far as their destinations are concerned, user 7 oscillates between 1 and 2, ending up with the first one, while user 8, starts with 3 but ends up with 5, both due to distance and interference reasons.

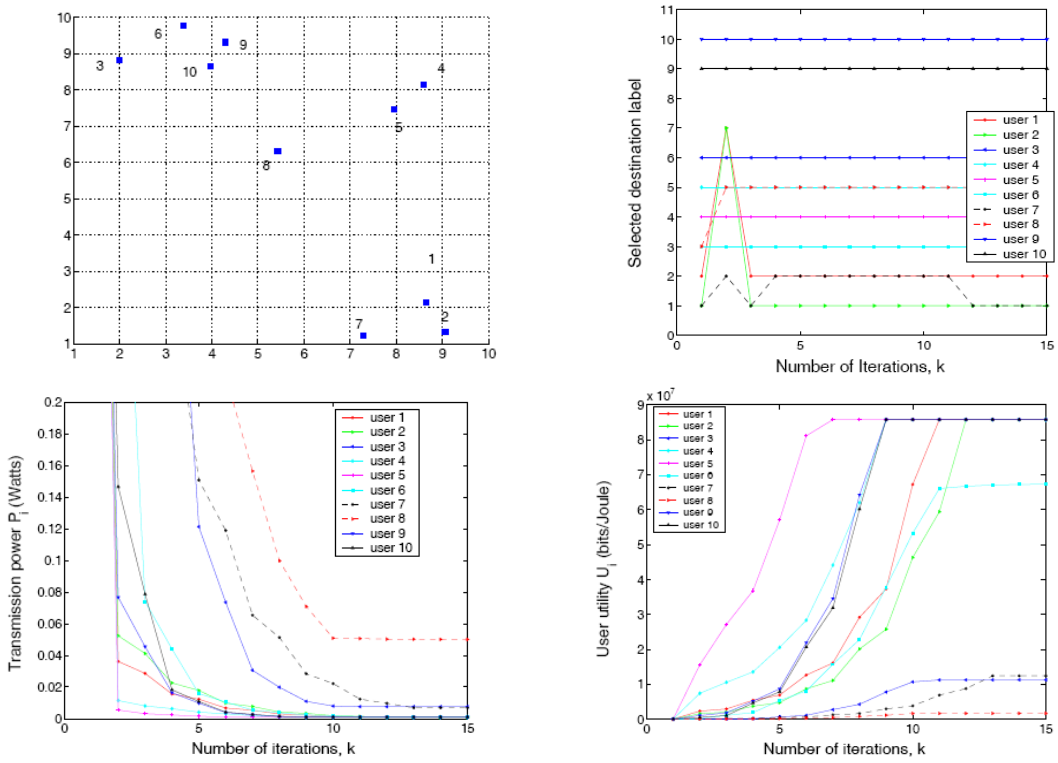


Figure 59. a) Network topology for 10 nodes; b) Users' destinations selection; c) Users utilities; d) User's transmission powers.

Users 1, 2 initially pick 7 for receiver, but finally they select each other. We emphasise that the aforementioned destination choices are made within the repeated process of the game. Figure 59c, presents the decrease in transmission powers until convergence is achieved. Final transmission powers differ significantly at the end, as a result of the specific topology. Node pairs 3-6, 4-5 and 1-2 have lower transmission powers, while the rest have greater levels, with user 8 having the greatest. Furthermore, we observe that user 9 is finally allocated a large transmission power, despite the fact that its destination is geometrically close, due to the specific bad channel condition of its neighboring links. Figure 59d, shows the corresponding utilities of the ten users for the same time slot. In general, nodes allocated the higher power levels, receive at the end the lowest satisfaction (utility), where nodes with the lowest power levels receive the highest utility. However, there are cases like user 6, that even though the user is allocated low power levels, its utility is not large enough, because in its neighborhood interference levels are relatively high (user 6 has nodes 9, 10 in its neighborhood transmitting to each other).

B. Assessing the Scalability Attributes of the Proposed Autonomic Solution

In this section, APRC algorithm is studied for increasing network sizes and constant user densities. The proposed algorithm was run for 500 iterations and the results were averaged over 10 different scenario topologies for every different network size. Figure 60a, presents the average number of iterations per time slot for increasing network sizes, where a constant density of 100=3002 users/m2 has been considered. As the number of nodes increases, so does the number of iterations needed for the iterative process of the APRC algorithm to converge to the final values of the transmission power, rates and destination nodes. This is due to the fact that as the number of nodes increases, the interactions of the non-cooperative game increase as well, which in turn takes more time for the game to reach a Nash equilibrium.

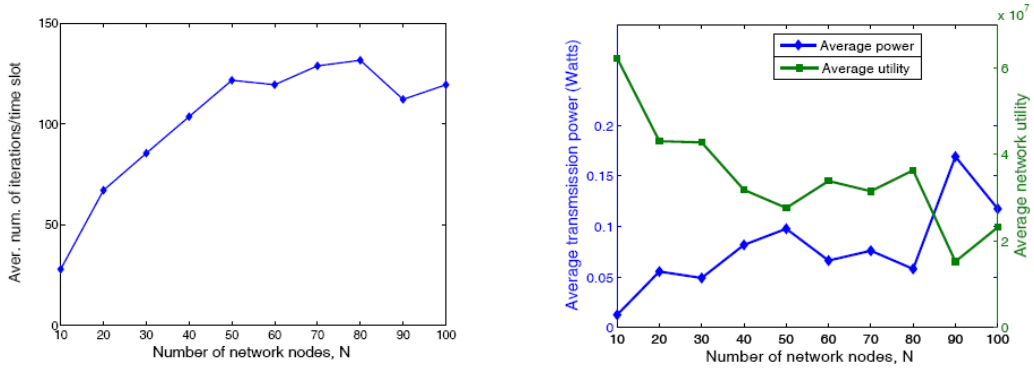


Figure 60: a) Average number of iterations per time slot; b) Average user transmission power and utility.

Moreover, it can be observed that the average number of iterations tends to **stabilise** around a fixed value as the network size increases, indicating a good scaling property of the APRC algorithm. It should be underlined that the previous property has been confirmed under a fixed node density. A similar trend holds for the rest of the system quantities, as it is shown in the sequence. Specifically, Figure 60b presents the average consumed power of a user under APRC algorithm for increasing network sizes. It is shown that as the network size increases, so does the average allocated power, as a consequence of the increased interference imposed by the larger number of users in the network. The corresponding average node utility is also shown in Figure 60b, following an inverse trend as opposed to that of the average power level. The average utility decreases as the network size increases, which can be attributed to the increased number of neighbors in the locality of a user. Therefore, as the interactions of nodes increase a user's satisfaction (expressed by the utility function) decreases, due to increase in the system-wide interference.

5.2.2 QoS in wireless mesh networks

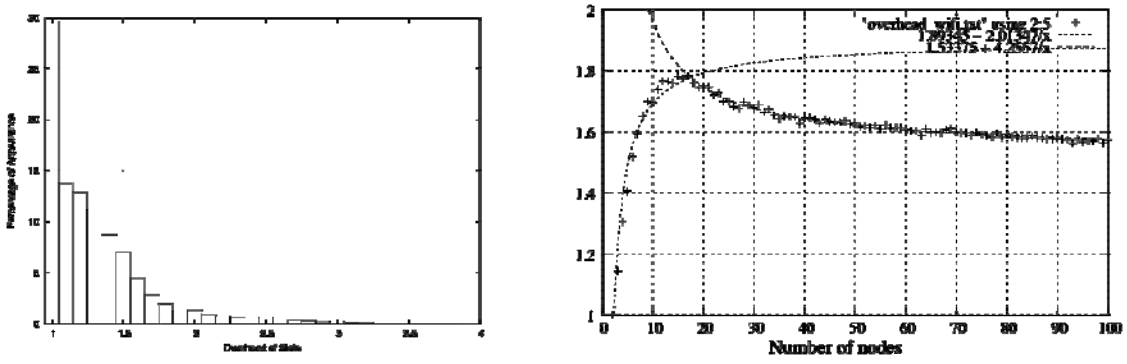
Introduction. It is often doubted that wireless mesh networks (WMNs) are scalable in terms of service provision. It is claimed that the bandwidth decreases strongly with multi-hop communications. Their data frames are sent several times over the same physical channel, which consumes bandwidth. Wireless nodes cannot send and receive at the same time, because own signals overpower those of other stations. They have to alternate between sending and receiving. Therefore, mesh nodes can only provide one-half of their available service bandwidth to neighbouring mesh nodes. If completely uncoordinated the service bandwidth degrades exponentially to 0.5^n at n-hop distance to the hot spot (HS).

There are several approaches that can be used to enhance overall performance of WMNs. In a first step, we provide a capacity study that shows that for most random mesh network topologies there exists a time scheduling which allows to exploit the entire service bandwidth [SE06].

Based on this analysis, we propose an autonomic solution making use of frequency division rather than time division. This method is more suitable for practical implementations and increases the overall service bandwidth. In such a scenario, the HS is used as central coordinator to assign frequency channels to the different participating mesh nodes. To do this, the HS needs to be aware of the WMN topology as well as the quality of the different communication links. Using this information, a communication tree to reach all the nodes is centrally computed by the HS. Cross layer information can this way be used to assign the appropriate channel to the different links. A Decision Element will be responsible to periodically evaluate the quality of neighbouring communication links and communicate this information to the HS, which keep an

up-to-date database of the network (ONIX). This way, corrective step can be taken in case of changing network conditions.

Problem statement. In this study, we consider mesh networks where all mesh nodes store a packet to be sent to one HS. These packets represent a share of service bandwidth, which is assigned to the originating mesh node. The minimum duration to deliver all packets to the HS corresponds to a maximisation of service bandwidth. Time is measured in time slots. One time slot allows the transmission of a packet over one hop. Transmissions in 3-hop distance on a multi-hop path can be assigned to the same time slot. Slotted transmissions are commonly denoted as Spatial Time Division Multiple Access (STDMA) in the wireless domain. For some multi-hop mesh networks this is sufficient to deliver all packets in as many time slots as mesh nodes exist. Then the HS receives a packet in every time slot and its available service bandwidth is completely used. As every mesh node originates one packet the bandwidth is uniformly shared. For random network topologies it is known that it is NP hard to maximise the service bandwidth [TS06]. Still, *30%* of arbitrary chosen network topologies operate without losing service bandwidth by the usage of a best effort algorithm. Most network topologies do only suffer minor bandwidth sacrifices. In worst case, mesh network topologies can always use one third of the service bandwidth. This is, if every multi-hop path is treated solely by the hot spot. Then the hot spot has to alternate between all multi-hop paths to achieve a uniformly shared access. The results depicted in Figure 61 (a) and (b) were already presented in [SE06']. The produced overhead is measured as the ratio of needed slots to (#Slots / #Nodes). Figure 61 (a) shows percentages of appeared overhead values in the simulations. As already stated, almost *30%* of the simulations have been solved without losing bandwidth. More than 4 of 5 simulations did not need more than *50%* more slots than mesh nodes. This shows how good bandwidth loss due to multi-hop transmissions is compensated by parallelism in the WMN. Figure 61 (b) shows the simulation result as a function of the number of nodes in the WMN using standard WiFi. The y-axis is the average achieved slot to node number ratio (#Slots / #Nodes) for every node number. The two curves in the graph represent approximations of the measured values. The measured worst-case overhead is represented by the intersection of both curves, which is about *1.8* (*44%* overhead) with *17* nodes. For an increasing number of nodes the overhead seems to converge against *1.5* (*33%*). This means that about *33%* more slots than nodes on average are needed, therefore *33%* of the bandwidth is lost. In this calculation WiFi is encapsulated by STDMA. Therefore, the overhead arising due to random access and the related back-off procedures is not visible. This additional overhead is measured in [LBDLM01] and will further affect the performance of the WMN when WiFi is used on its own.



(a) (b)

Figure 61. Time Slot Overhead

Instead of separating mutual excluding transmissions in time we assign them to non-interfering channels. The STDMA approach is a suitable tool to determine capacity bounds but a practical realisation is difficult due to time slot provision and allocation. Mesh nodes need to agree on time slot boundaries throughout the WMN. This can be defined by some external signaling or implicitly by internal frame exchanges. The external signaling needs to be precise enough to allow short inter-slot spaces and time slots. The internal signaling needs to be integrated into the normal frame exchange procedures, which puts further complexity into the protocol. Not only the provision but also the use of time slots is difficult. It is a non-trivial task to assign transmissions to time slots in real-time. The link-layer protocol tends to become un-adaptable when the scheduling is predefined and needs not to be solved in real-time. Load adaption and rerouting are difficult to implement.

From a theoretical point of view the capacity utilisation is independent from the approach to resolve collisions. If we subdivide the single communication channel into multiple communication channels we are able to avoid interferences, as well, but it needs to be ensured that no resources are unnecessarily wasted. As it is possible to fully utilise the resources for a single channel it is possible to achieve this with multiple channels, too. Therefore, we will transform the situation to a multi-channel approach to obtain an easier to realise setup.

Proposed solution

In order to deploy scalable WMNs in practice using WiFi, the STDMA approach has to be transformed into a multi-channel approach where transmissions are not separated in time but by channel allocation. In a result every transmission is always allowed and is not deferred to dedicated time slots. Mutually excluding transmissions have to be assigned to different orthogonal channels to allow simultaneous transfers. As described earlier, for nodes on a line every third node is allowed to send at a time using the same channel. Let $(S_i)_{i=1}^{n}$ be a sequence of nodes in a line, where S_1 is a neighbor of the HS. Further, we have $C_{1 \le k \le 3}$ orthogonal channels. Then we can assign links $(S_i, S_{i-1}), i = 2,\ldots,n$ to the channels in such way that all transmissions can be done without interference by assigning (S_i, S_{i-1}) to channel $C_{(i\%k)+1}$. Every *k*-th link is then assigned to the same channel. All transmissions can be done in parallel as long as *k* is bigger than 3. To do this every node needs to have at least two wireless interfaces, a third wireless interface for mobile clients. S_i operates one interface on channel $C_{(i\%k)+1}$ and the other on channel $C_{((i+1)\%k)+1}$. As every node is able to send at the same time it is possible to utilise the entire data-rate of a single channel. This means one *k*-th of the overall capacity is utilised. In previous studies, we showed that single path capacity holds for arbitrary mesh networks. So, if only one path at a time is treated in the mesh network we obtain an overall service capacity of one *k*-th. To completely avoid multi-hop scheduling one needs to consider mutual interferences between adjacent routing paths. Suppose *(A, B)* is a link in the mesh network that is used for routing packets, where *A* is at hop-distance *t* to the HS. Then, utilisation of one *k*-th can be achieved by assigning *(A, B)* to channel $C_{(t\%k)+1}$. So, all client mesh nodes may send to the same wireless interface of the parent node. Therefore, 2 wireless interfaces per node are still sufficient for this setup. One wireless interface is used to transmit and receive frames from and to the parent node the other one is used to provide a wireless interface to the client node.

Up to now one *k*-th of the capacity is utilised, but this is for arbitrary mesh networks. It is possible to obtain a full utilisation by creating sub-networks, which are connected by single links to the HS using directional antennas. The HS needs to be able to always send or receive over all wireless channels to achieve a full utilisation. This is not possible if the HS is designed like an ordinary mesh node with one single wireless interface for all client nodes. Then, only one node is able to send at a time and one can only obtain one *k*-th of the global capacity. To fully utilise the

capacity the HS needs to have for every channel in use a wireless interface to be able to send and receive at the same time in every channel. It is now possible to provide *k* sub-networks. All of them are connected to the HS using a dedicated wireless interface operating on a dedicated wireless channel. So, the first client node of each sub-network is connected via a different channel to the HS. Channels in the sub-networks are again assigned in the same manner as before to provide one *k*-th bandwidth to the HS-neighbor. So, if a HS-neighbor uses channel C_i to communicate with the HS it will allocate channel C_{i+1} on the second interface to communicate with its client node and so on. Figure 62 shows a sample Mesh Network for $k = 3$, which is especially suitable for WiFi (3 non-overlapping channels). The channels are represented by different colors. The colors are alternated along routing paths, while the initial colour is different for every sub-network due to the channel assignment of the HS. This setup is now able to fully utilise the entire capacity with a reduced complexity compared to the single channel approach.

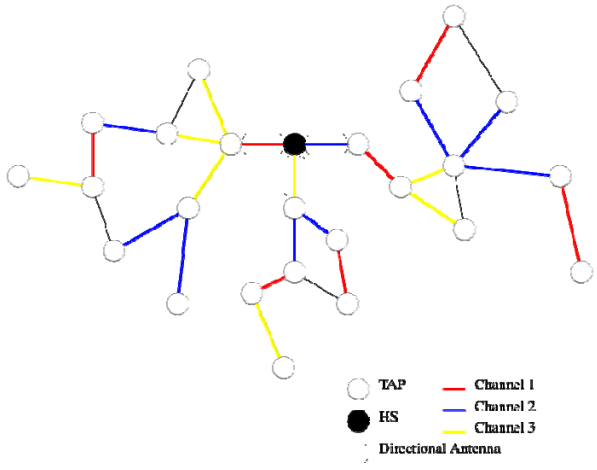


Figure 62. Multi-Channel WMN

The procedure described previously can easily be automated and used within the GANA framework. Assume a set of mesh nodes is placed in a certain environment. The initialisation of then network is done in two phases. In the first phase, links have to be identified that can operate at an acceptable quality. A link is acceptable if it supports a given bit rate. As a mesh network is considered that shall operate under a high service bandwidth it is vivid to avoid the usage of weak links. Therefore links should be further rated by their signal quality at the receiving stations. The HS can trigger the identification of links. To do this, the hot spot broadcasts a beacon. Stations receiving this beacon in an acceptable strength confirm the reception to the HS. This has to be done with a random access collision avoidance strategy to ensure that the HS receives the feedback. Recursively this is repeated for every new mesh node. A dedicated DE is used to perform those operations. The HS, which is the central coordinator, triggers every mesh node one after another to send a beacon, which is confirmed by overhearing mesh nodes. The requests to send beacons as well as the list of new neighbors will be delivered via the newly found links to the HS.

After this initial step, the second phase starts. Now, the HS is aware of the network topology and computes the adequate routing paths. Further, The HS determines the channel allocation to be used. The channel assignment may for example follow the methodology described previously where one multi-hop path is treated at a time. All the newly collected information should be stored in a dedicated ONIX database to allow further analysis. As a next step, the new configuration needs to be tested to ensure a reasonable QoS. For that, the HS tests the channels one after another. It sends transmission requests to every sender that has been chosen to operate on the same channel. The transmission is scheduled to be performed at a given period of time.

During this period the senders starts transmitting data frames to one neighbor. Afterwards, the HS requests feedback from the receivers. The feedback provides information on how many data frames have been successfully received. If these values are high enough the channel can be used for this configuration. If not, one may change to alternative routing paths that avoid links that caused failures. It may turn out that some nodes can only be reached via weak links. To also support these nodes one may reduce the bit rate of weak links to support better robustness against interferences. This technique is already supported in the state-of-the-art link layer protocol of WiFi, which supports transmissions in various bit rates. It chooses bit rates between 54Mbps to 1Mbps depending on the quality of links. Also, this allows an adaptation to dynamic changes in noise and interferences. A maintenance procedure is scheduled periodically to ensure continuous service. The DE of the participating nodes periodically triggers test messages to check the quality of active communication links and transfers this information to the HS. Based on this information, the DE of the HS decides if the frequencies need to be re-allocation or remain the same.

5.3 Cross-Layer optimisation in Peer-to-Peer networks

5.3.1 Cross-layer peer-to-peer topology optimisation

Introduction. Traffic generated by peer-to-peer applications is estimated to account for 30-70% of all Internet traffic. Peer-to-peer applications implement an overlay network: a virtual network on top of the underlying layers, with nodes in the overlay network connected by virtual links. The structure of the overlay network shows virtually no correlation with the structure of the physical network.

This approach allows for rapid deployment of p2p applications, and resilience to correlated failures of nodes in the physical network (as it will translate to random failures in the overlay). However, it also results in poor locality of data transfers, which is undesirable both for network operators and users of p2p applications. For network operators, it results in ineffective utilisation of network resources, overloading of links in the core network, and high cross-ISP traffic. For users, it results in slower than optimal downloads.

Network operators tried to mitigate consequences of traffic generated by p2p applications by throttling p2p traffic. However, this approach was only moderately effective, as developers of p2p applications responded with protocol modifications that made identification of p2p traffic difficult; furthermore, throttling traffic generated by users also raises concerns from the network neutrality point of view.

An alternative approach is cooperation between network operators and p2p applications. Peers use cross-layer topology information to configure their routing tables, which results in the overlay network self-organising by taking into consideration the topology of the physical network. This approach decreases redundant data transfer in the core network, benefiting both the users of the p2p application in the form of faster downloads, and the network operators in the form of more efficient resource utilisation.

Problem's statement and its autonomic solution

The objective of the topology-aware peer-to-peer applications part of task 3.5 is to explore how GANA can be used to optimise the overlay topology to localise data transfer, the advantages this localisation brings to users and network operators, and the effects of this localisation on the robustness of the overlay structure.

The problem of topology-aware p2p applications has been mainly explored for BitTorrent, a widespread p2p file sharing application. In task 3.5, we explore the possibilities of using topology

information to optimise the structure of the Kad network, which is the largest deployed, completely decentralised p2p network. By incorporating results from previous work on the BitTorrent protocol, and developing a topology-aware version of a client for the Kad network, we hope to gain a more complete view on the general approach of topology-aware peer-to-peer applications. Optimising the structure of a p2p overlay to mirror the physical network with information on topology can be broken down into two major sub-tasks: 1. gather topology information and 2. use this topology information to configure the overlay. For the BitTorrent protocol, different information-gathering approaches have been explored: topology information can come from a server operated by ISPs (as in Proactive Provider Participation for Peer-to-Peer – P4P), from reusing topology information gathered by another entity (as in the Ono project, where the Akamai content delivery network is probed to infer network topology), or from autonomous measurements by the peer-to-peer application (as in TopBT, where nodes try to deduce proximity by pinging other nodes).

In task 3.5, we implement a client for the Kad network which uses these information-gathering approaches, and adapts the overlay structure to the physical network. The fundamental difference between the BitTorrent protocol and the Kad network is that in the case of the Kad network, there is no central entity indexing content and controlling connections between nodes; thus, adapting the overlay structure to the physical network requires a different approach.

Topology information can be used at the system level (such as the tracker in the case of a BitTorrent swarm, or the distributed hash table in the case of a decentralised peer-to-peer application like the Kad network), or at the node level (choice of connections for each node based on topology information).

Our first goal is to investigate the possibilities of using topology information in the Kad network at the node level: nodes take into account distance in the physical network when choosing connections for data transfer. Our second goal is to investigate the possibilities of modifying the distributed hash table of the Kad network for topology-aware operation.

Autonomic topology-aware operation is made possible by self-configuration of nodes: nodes choose connections for data transfer based on topology information. At the network level, this translates to the self-organisation of the overlay based on topology information, to adapt to the structure of the physical network and localise data transfers.

Proposed Algorithm

The download process in the original Kad client works as follows:

1. The downloading node contacts the Kad DHT for nodes which possess the desired part of the file to be downloaded (called a PartFile in the Kad terminology)
2. The downloading node contacts each node whose address it retrieved from the Kad DHT, in the order it received them
3. The downloading node is inserted into an upload queue at each node it contacted. The upload queue is ordered according to a priority, which is calculated based on the time a node has been waiting to download, and credits resulting from previous uploads from each node.
4. When the downloading node becomes the first in the upload queue of one of the uploading nodes, data transfer starts.

We modified this download process at two levels to enhance locality of data transfers: the downloading node contacts nearby nodes first, and the uploading node takes into account network proximity when calculating priority for nodes in the upload queue.

- in step 2., the downloading node gets topology information for each node received from the DHT; depending on the source of topology information (an ISP-operated server, probing of a content-delivery network, or autonomous measurements), this corresponds to the information gathering part of the control loop of PROTO_LEVEL_ISX_DE, PROTO_LEVEL_CDNX_DE or PROTO_LEVEL_MSRX_DE. The downloading node then

orders the list of the nodes to be contacted according to network distance, so that nearest nodes are contacted first; This corresponds to the second part of the control loop of the decision elements.

- in step 3., the uploading node orders the upload queue based on waiting time, previous uploads, but also network proximity, so that nearby nodes get a higher priority, and reach the top of the list faster. This also corresponds to the second half of the control loop of the decision elements.

Scalability, Stability and Complexity Issues

Peer-to-peer protocols, and thus the Kad protocol have been designed with scalability as one of the primary objectives in mind; the application can scale to millions of nodes.

Topology awareness introduces a new network message for each node whose address is retrieved from the Kad DHT, for each downloaded part of a file. However, the number of nodes returned by the Kad DHT for each request is limited by the Kad protocol; thus, the number of necessary network messages has an upper bound, and does not increase linearly with the number of nodes. Caching of previous answers can further reduce the number of new network messages introduced by topology awareness.

With large networks, the information server operated by the ISP could also become a bottleneck; however, as the network grows, we expect nodes to be distributed across more ISPs, with each ISP operating an independent topology information server for his network. Therefore, the number of servers should also scale with the number of nodes. The CDN or Autonomous measurement based approach has no centralised element which could become a scalability bottleneck.

The Kad protocol has been designed to tolerate large scale correlated failures. This is made possible by the overlay approach, which distributes correlated failures in the physical network randomly in the overlay layer. The extent to which topology awareness makes the Kad network more vulnerable to correlated failures has to be investigated; however, as only the order of nodes in the download and upload queues is changed, our intuition is that in the case of correlated failures, distant nodes can still be reached by downloading nodes.

As part of the evaluation process we will compare the number of data packets which do not cross AS boundaries in the modified client against the original client. Furthermore, we will investigate the number of network messages generated by the topology-aware approach, as well as the extra delay introduced, as a function of the download swarm size. We will also investigate the effect of correlated failures on the original, and the modified client.

Initial Evaluation

To test our modified application, we have installed it on 3 workstations with 7, 7 and 10 clients, running on different user accounts and different ports each. Nodes were assigned virtual network coordinates, each of the nodes being assigned to one of 3 different virtual ASes.

Five different files, with sizes varying between 10 and 12 megabytes, were shared between the clients; each client seeded only one file, and downloaded the remaining four from the other clients. Results were unconclusive, as the number of clients in the swarm was very limited compared to the number of virtual ASes involved, and the size of the downloaded file size. Unfortunately, we could not observe any significant improvement in the locality of data transfers with the modified client. This was probably due to the fact that we tested the application with small number of clients, as we were limited by the number of available workstations.

Also, each client only accepts three clients with the same IP address in its upload queue, which may also have decreased the amount of useful data.

To acquire better interpretable data, we will deploy the application on the PlanetLab network. We will investigate the effect of download swarm size and downloaded file size on locality.

5.3.2 Security and Privacy in Peer-to-Peer networks using Cross-Layer optimisation

Introduction. In today's networks, P2P systems become an essential tool for the exchange of data. In GANA, the secure exchange of information is a very important challenge in regard to availability, confidentiality, integrity, authenticity and privacy. Especially due to the autonomic and distributed architecture, where nodes and routers must be considered as untrusted, security is difficult to establish and faces multiple threats. Also, P2P security heavily depends on the underlying network infrastructure. Especially the flexibility of IPv6 may be feasible to overcome parts of this limitation, e.g. by using available IPv6 Extension Headers for improvement by shifting P2P protocol information to lower OSI layers.

Within this task, we try to improve the idea of achieving confidentiality and anonymity with the help of information slicing, a technique proposed by [KCK07], in exploiting IPv6 capabilities.

There are many approaches to distribute data in an anonymised manner, mainly requiring public key cryptography. The proposal in [KCK07] describes a solution by chopping the information to be sent into several pieces that are worthless without the other pieces, and creating an overlay topology using disjoint paths to forward these pieces and thus enables confidential data transfer from A to B. This solution has several advantages:

- No public key cryptography is needed
- Higher throughput than onion routing is achieved
- Adaptive to the highly dynamic behaviour of autonomic networks. Consequently, aspects like churn and network changes are better supported

The problem we face is the untrusted underlay network, on which the overlay has no influence and where malicious nodes on the underlay may be able to reveal nodes in the overlay, or even sender and/or receiver.

Problem's statement and its autonomic solution

The main idea is to use overlay information in order to optimise underlay routing and data transfer in general. In the context of GANA, several OSI layers may be connected to ONIX in order to get up-to-date network status information, etc.

The problem of the initial approach is that the underlay network is not considered. This implies that underlay nodes (most times routers) need to be trusted. Thus, what could happen, if exclusively underlay nodes are malicious? Messages sent from overlay node A to B can be sniffed by underlay nodes.

This counts even more, if messages are sliced to achieve confidentiality and anonymity, as in this case, the information pieces travelling in the network are *not* encrypted in the usual way. If one node gets all slices belonging to one message, it knows at least parts of the overlay network, even if the receiver may not be unveiled. More specifically, a node that receives all slices of a message intended to an overlay node gets information about the overlay node's routing table, and also may also discover the parents of the overlay node.

The usual metrics for measuring the anonymity in a system are *source anonymity* and *destination anonymity*. Source anonymity is a function of the probability of the attacker identifying the source of a message, while destination anonymity is a function of the probability the attacker assigns to each node being the destination of a message [KCK07]. Nodes in the underlay, which can unintentionally or maliciously receive several messages intended to overlay nodes can have a substantial impact on these measures.

To analyse this problem, we set up a simulation environment on top of SciLab [SCI09]. Specifically, we created an underlay topology based on the Barabasi-Albert model that reflects the current Internet topology plus -based on this model- we constructed a typical disjoint-path overlay model (Figure 63, right).

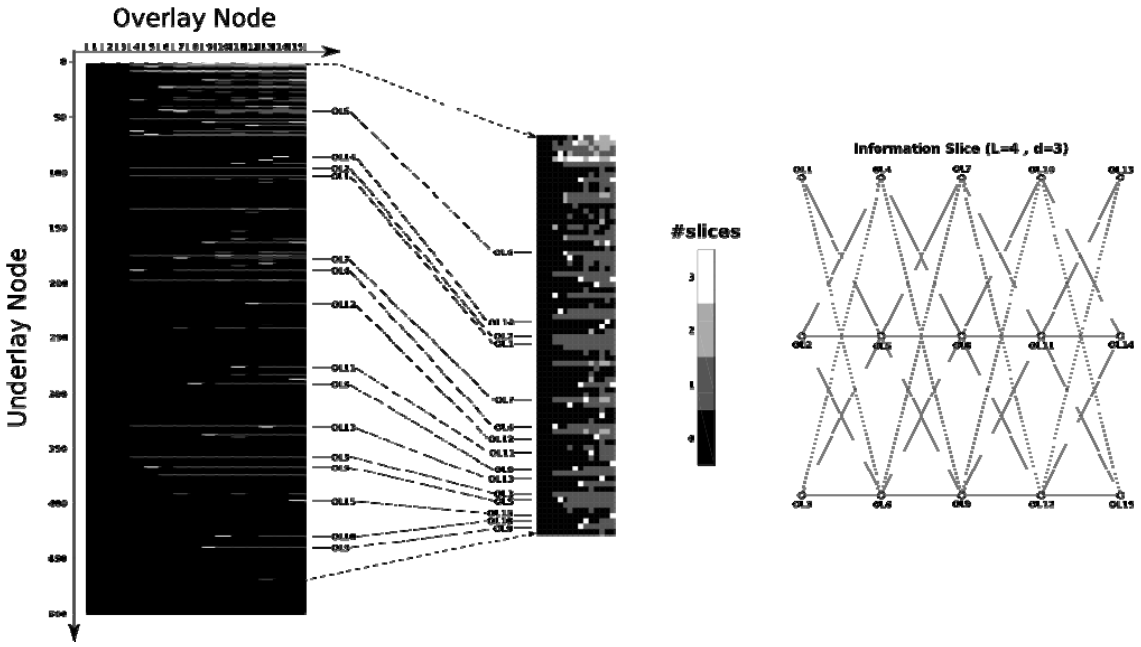


Figure 63. Left: Revealed overlay information from underlay nodes. The illustration on the right shows a sample overlay configuration with 3 slices per message.

In Figure 63, the left part shows all underlay nodes and the number of slices they received. The extract aside presents all underlay nodes that receive at least one slide (dark grey). The simulation showed that in a network of 500 nodes, in average 76 nodes including 15 overlay nodes receive at least one slice and 29 nodes receive a complete set of slices (shown as white dots; here: 3), highlighted with white dots (extract in Figure 63). Thus, there are 14 more underlay nodes that receive information unintended about other involved overlay nodes, which may reveal also source and destination nodes. Particularly underlay nodes in the beginning of the transmission path receive more slides. This shows clearly the limitation of this approach: the availability of underlay nodes close to the sender is limited and it is difficult to ensure pure underlay disjoint paths, especially on the first stage of the forward scheme.

Finally, we see that both source anonymity and destination anonymity are subject to this kind of information leaking: considering only the overlay network when evaluating these metrics leads to unduly optimistic results.

Proposed Autonomic Solution

The work on the solution of this problem is still in progress. One planned solution to improve overall security and performance is the usage of Multi-Path routing approaches, extending them to force disjoint path routing on the underlay and using the 'knowledge' of ONIX.

To support the overall GANA security model, we also plan to use the Security-DE (SECURITY_MANAGEMENT_DE, [D3.5]) to set security level inside a node. This communication between SECURITY_MANAGEMENT_DE and overlay application will apply the security threat level [D3.5] directly into the application and thus improves overall security. A consequence could be the additional usage of encryption for instance.

On the other side, performance will be additionally improved, using values like *filesize* and a *slicing-bit* in the IPv6 Hop-by-Hop extension header to improve packet routing. Here, every underlay router may be able to react immediately in the case of congestion or link failure.

Consequently, the high-level algorithm of a router involved in anonymous data transfer (indicated by an IPv6 Hop-by-Hop flag) may look like the following (Figure 64):

```
if (slicing-bit == 1)
      if (outgoing-link == ok)
            send packet
      else
            contact ONIX to find alternative disjoint route
      end if;
end if;
```

Figure 64. Simple high-level algorithm using ONIX as 'central' repository to improve routing

Obviously, we face an issue concerning the extra 'slicing' bit in the protocol header as it reveals that the forwarded packet belongs to a confidential and anonymous message. Even though the overlay nodes get this information as well, the visibility of such an additional bit should be reduced. This issue will be subject of further research.

Scalability, Stability and Complexity Issues

The current approach uses ONIX as an information repository and the question is whether this system can handle numerous requests in the case of a large-scale 'problem', which could arise if many node failures occur at the same time. Our initial approach to get further routing information from ONIX may result in a denial of service attack.

We are currently working on this issue, trying to minimise ONIX requests and to find alternative disjoint paths autonomously. In the context of our work, stability is considered within several aspects. First of all: how does the developed approach handle attacks against confidentiality and anonymity on both layers (overlay and underlay)? Sybil attacks for instance could target on the underlying network as well as the overlay and cause the complete de-anonymisation of the traffic. Secondly, we have to ensure that design and implementation of the cross-layer information exchange will not have influence on other layered communication.

In addition, we need to consider packet delays to ensure network stability, as there is no consistent packet numbering yet. Currently, we assume that packets from A to B are sent at the same time and arrive at the same time within one stage. This problem may become serious due to different packet propagation travel time from the source until the end of the created overlay topology.

Planned Results. Due to the fact that our solution is not completely elaborated, only initial indicative results have been obtained, which, however, already highlight the necessity of considering the multi-layered nature of nowadays communication networks. The comprehensive investigation of this issue, which is our immediate future work, will precisely characterise the loss in terms of anonymity considering [KCK07] as a benchmark, and we will propose cross-layered solutions to overcome this problem. The reason for being behind schedule was mainly due to the limitation of resources we experienced during the first year of the project. However, we put emphasis on this task and plan to finalise the proposed solution during the first half of 2010. Consequently, we will present our results in deliverable [D3.6] at M30.

6 CONCLUSIONS

6.1 Progress so far

This deliverable presented in concrete and proficient way overall WP3 progress and key achievements. Specifically, within the reported period WP3 placed emphasis on **a)** finalizing the design and assessment of the various autonomic functionalities and mechanisms (as well as the corresponding DEs) that have been developed within its framework, via simulation and experimentation towards *i)* revealing the benefits of the proposed autonomicity-driven approaches compared to current state-of-the-art ones and *ii)* assessing the scalability/stability attributes of the proposed autonomic approaches (in specific use cases) in the areas of QoS provisioning (*Chapter 2*), mobility management (*Chapter 3*), resilience and survivability (*Chapter 4*) and cross layering (*Chapter 5*); **b)** incorporating individually developed components in WP3 into emerging concrete architectures via the integration of various produced autonomic mechanisms, in terms of integrated function level DEs, concerning the following networking paradigms: *i)* autonomic QoS management over a wired environment, *ii)* autonomic mobility and QoS management over a heterogeneous wireless environment, *iii)* autonomic resilience & survivability; **c)** specifying concrete scenarios that allow the identification and demonstration of the key features and novelties of the emerging architectures within WP3.

6.2 Next Steps

In accordance to the previous discussions and analysis, the following key steps will be followed (details on WP3 future work plan are provided in Milestones M3.3 and M3.4 (Month 24)).

- Enhancing, refining and evaluating developed autonomic functionalities, mechanisms and behaviours, concerning security *(Deliverable D3.3, M36)* and resilience and survivability *(Deliverable D3.4, M36)*.
- WP3 Integrated architectures final design and evaluation. *(Deliverable D3.6, M30)*
- Enhancing and analyzing the proposed scenarios.(*Collaboration with WP5)*

The realization of all the previous activities will reassure the fulfilment of WP3 frameworks (F6-F12). Each framework is actually describing in a formal way the goals of each of the proposed architectures in WP3 and vice versa. Thus, the development of the prototypes defined in each framework will be achieved:

- Either by the specification, implementation and evaluation via simulation of all the algorithms and autonomic mechanism developed within WP3,
- Or, by implementing and testing part of them into EFIPSANS testbeds, especially those that are parts of the overall architectures designed within WP3.

7 REFERENCES

[3GPP TS 23.402] 3GPP TSG SA, 3GPP TS 23.402 "Architecture enhancements for non-3GPP accesses (Release 8)"

[3GPP TS 36.314] 3GPP TSG RAN, 3GPP TS 36.314 "Evolved Universal Terrestrial Radio Access (E-UTRA); Layer 2 - Measurements (Release 8)"

[AKP09_1] G. Aristomenopoulos, T. Kastrinogiannis, and S. Papavassiliou, "A Unified Approach for Efficient Network Selection in Multi-Service Integrated CDMA/WLAN Systems," *in Proc. of 5th International Wireless Communications and Mobile Computing Conference (IWCMC 2009)*, June, 2009.

[AKP09_2] G. Aristomenopoulos, T. Kastrinogiannis, and S. Papavassiliou, "Efficient QoS-Driven Resource Allocation in Integrated CDMA/WLAN Networks - An Autonomic Architecture", *in Proc. of 1st Int. Conf. on Mobile Lightweight Wireless Systems (MOBILIGHT 2009), LNICST Springer*, May 2009.

[AKP09_3] G. Aristomenopoulos, T. Kastrinogiannis, and S. Papavassiliou, "Enabling Efficient QoS-Driven Resource Management in Heterogeneous Wireless Networks via Autonomicity" *submitted to Computer Com.*.

[AKP09_4] G. Aristomenopoulos, T. Kastrinogiannis, Zhaojun Li and S. Papavassiliou, "An Autonomic QoS-centric Architecture for Integrated Heterogeneous Wireless Networks", *subm. to IEEE Wireless Com. Mag*.

[BJS00] L.Breslau, S. Jamin, S. Shenker, "Comment on the Performance of Measurement-Based Admission Control Algorithms", *IEEE Journal on Selected Areas in Com*, 2000.

[BPO03] Banchs, X. Pérez-Costa, and D. Qiao, "Providing Throughput Guarantees in IEEE 802.11e Wireless LANs," *in Proc. of the 18th Inter. Teletraffic Congress* (ITC18), Berlin, Germany, Sept.2003.

[C08] M. Chiang, "Nonconvex optimization of communication systems," *Advances in Mechanics and Mathematics*, *Special volume on Strang's 70th Birthday,* Ed., D. Gao and H. Sherali, Springer, 2008.

[Coin-OR] Coin-OR: http://www.coin-or.org/ as of date 01.10.2009

[D1.5] INFSO-ICT-215549-EFIPSANS-FP7-IP Project, Deliverable D1.5: "Third Draft of Autonomic Behaviours Specifications (ABs) for the Diverse Networking Environments".

[D1.5B] INFSO-ICT-215549-EFIPSANS-FP7-IP Project, Deliverable D1.5: "Third Draft of Autonomic Behaviours Specifications (ABs) for the Diverse Networking Environments".

[D3.1] INFSO-ICT-215549-EFIPSANS-FP7-IP Project, Deliverable D3.1: "Advanced Network Services in Autonomic IPv6 Networking: Methods, Services and Architectures".

[D3.5] INFSO-ICT-215549-EFIPSANS-FP7-IP Project, Deliverable D3.5: "GANA threat and trust models".

[F07] Z. Fan, "Throughput and QoS Optimization for EDCA-based IEEE 802.11 WLANs," *Wireless Personal Communications,* vol. 43, no.4, pp. 1279-1290, Dec. 2007 .

[G09] X. Guo, "An Autonomic Flow based Path selection Method for Multi-homed Nodes", a*ccepted to be published in the 2nd IEEE international Conf. on Broadband Network and Multimedia Technology* (IC-BN-MT), October 2009.

[GLCW09] Xiangyang Gong, Yan Li, Jieyao Chen, and Wendong Wang, "A Context-aware Packet Marking Algorithm in Autonomic Networks". *In Proc. of 2009 Int. Conf. on Broadband Network and Multimedia Technology (ICBNMT 2009).* (The paper has obtained the Best Paper Award in ICBNMT 2009).

[HBH05] J. Huang, R. A. Berry and M. L. Honig, "A Game Theoretic Analysis of Distributed Power Control for Spread Spectrum Ad Hoc Networks", *in Proc. of Int'l Symp. on Inf. Th. (ISIT),* pp. 685-689, Australia, Sept. 2005.

[JK07] Y. Jin, and G. Kesidis, "Distributed Contention Window Control for Selfish Users in IEEE 802.11 Wireless LANs," *IEEE Journal on Selected Areas in Comm.*, vol. 25, no. 6, pp. 1113 – 1123, Aug. 2007.

[KCK07] S. Katti, J. Cohen, and D. Katabi, "Information slicing: Anonymity using unreliable overlays," Usenix NSDI 2007, Usenix, 2007.

[KP08_1] T. Kastrinogiannis, and S. Papavassiliou, "Game Theoretic Distributed Uplink Power Control in CDMA Networks with Real-Time Services," *Com. Com., Elsevier,* (Published online: 20 November 2008).

[KP08_2] T. Kastrinogiannis, and S. Papavassiliou, "Utility based Short-term Throughput Driven Scheduling Approach for Efficient Resource Allocation in CDMA Wireless Networks", *in Wireless Personal Comm. Journal, Springer*, (Published online: 13 November 2008).

[KPKD07] T. Kastrinogiannis, S. Papavassiliou, K. Kastrinogiannis, and D. Soulios, "A Utility-based Resource Allocation Approach for the Downlink in CDMA Wireless networks with Multimedia Services", *in proc. of IEEE PIMRC 2007*, pp.1-5, Sept. 2007.

[KTP08] T. Kastrinogiannis, E. E. Tsiropoulou, and S. Papavassiliou, "Utility-Based Uplink Power Control in CDMA Wireless Networks with Real-Time Services," *in Proc. of Ad-hoc, Mob.and Wireless Net*., vol. 5198, p.p. 307-320, Sept. 2008.

[LBDLM01] Jinyang Li, Charles Blake, Douglas S.J. DeCouto, Hu Imm Lee, and Robert Morris, "Capacity of ad-hoc wireless networks. *In ACM Mobicom 2001*, Rome, Italy, July 2001.

[LH05] N. Li and J. C. Hou, "Localized Topology Control Algorithms for Heterogenous Wireless Networks", *IEEE Trans. Netw.*, vol.13, no.6, pp. 1313-1324, Dec. 2005.

[LinShim6] LinShim6, http://inl.info.ucl.ac.be/LinShim6

[LMS05]. J.-W. Lee, R. Mazumdar and N. B. Shroff, "Downlink power allocation for multi-class wireless systems," *in IEEE/ACM Trans. on Networking*, vol. 13, no. 4, pp. 854-867, Aug. 2005.

[LMS07] J.-W. Lee, R. Mazumdar and N. B. Shroff, "Joint Opportunistic Power Scheduling and End-to-End Rate Control for Wireless Ad Hoc Networks", *IEEE Trans. Veh. Tec*, vol.56, no.2, pp.801-809, Mar. 2007.

[LWZ07] L. Liang, H. Wang, and P. Zhang, "Net Utility-Based Network Selection Scheme in CDMA Cellular/WLAN Integrated Networks," *In Proc. of WCNC 2007*, p.p. 3313-3317, Mar. 2007.

[LZLYG07] C. Long, Q. Zhang, B. Li, H. Yang and X. Guan, "Non-Cooperative Power Control for Wireless Ad Hoc Networks with Repeated Games", *IEEE J. Sel. Areas Com*., vol.25, no.6, pp.1101-1112, Aug. 2007.

[MCPS06] F. Meshkati, M. Chiang, H. V. Poor and S. C. Schwartz, "A Game- Theoretic Approach to Energy-Efficient Power Control in Multicarrier CDMA Systems", *IEEE JSAC*, vol. 24,no. 6,pp.1115- 1129, June 2006.

[MV08] M. Máté, R. Vida, "Probability-based information dissemination in urban environments", *in Proceedings of Eunice 2008,* Brest, France, September 2008.

[MV09]M. Máté, R. Vida, "Reliable Gossiping in Urban Environments", *sub. to IFIP Wireless Days 2009.*

[MZH05] M. Chiang, S. Zhang, and P. Hande, "Distributed rate allocation for inelastic flows: Optimization framework, optimality conditions, and optimal algorithms," *in IEEE Infocom'05*, March 2005.

[OBMS07] A. de la Oliva, M. Bagnulo, A. Garcia-Martinez and I. Soto, "Performance Analysis of the REAchability Protocol for IPv6 Multihoming," *Conference on Next Generation Teletraffic and Wired/Wireless Advanced Networking (NEW2AN 2007*), September 2007.

[OV09] Gergely O¨ llos, Rolland VIDA, "Adaptive Regression Algorithm for Distributed Dynamic Clustering in Wireless Sensor Networks", *in Proc of 2nd. IFIP Wireless Days*, France, Paris, 15-17 Dec. 2009.

[R03] R. Roth et al., "IP QoS Across Multiple Management Domains: Practical Experiences for the Pan-European Experiments", *IEEE Communications Magazine*, Vol. 41, No 1, January 2003.

[RFB01] K. Ramakrishnan, S. Floyd and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP," http://tools.ietf.org/html/rfc3168, September 2001.

[RFC 4068] R. Koodli, "Fast Handover for Mobile IPv6," RFC 4068, IETF Net. Working Group, 2005.

[RFC 5533] E. Nordmark, M. Bagnulo RFC 5533 Shim6: Level 3 Multihoming Shim Protocol for IPv6, http://tools.ietf.org/html/rfc5533

[RFC3775] D. Johnson, C. Perkins, and J. Arkko, RFC3775: "Mobility Support in IPv6," RFC3775, IETF Network Working Group, 2004.

[RFC4066] M. Liebsch, A. Singh, H. Chaskar, D. Funato, E. Shim "Candidate Access Router Discovery (CARD)," RFC4066, IETF Network Working Group, 2005.

[RFC5213] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC5213, IETF Network Working Group, August 2008.

[S95] S. Shenker, “Fundamental design issues for the future Internet,” *IEEE JSAC*, vol. 13, no. 7, pp. 1176-1188, Sept. 1995.
[SCI08] SciLab project website. Available from: http://www.scilab.org [Accessed: 15 November 2009].
[SE06'] Thomas Scherer and Thomas Engel, “Bandwidth Consumption for Providing Fair Internet Access in Wireless Mesh Networks,” *in Proc. of the 2006 IEEE Int. Work. on Wireless Ad-hoc and Sensor Net*. (IWWAN 2006), June 2006.
[SE06] Thomas Scherer and Thomas Engel, “Bandwidth overhead in WiFi mesh networks for providing fair Internet access,” *in Proc. of PM2HW2N '06: Proc. of the ACM int. workshop on Performance monitoring, measurement, and evaluation of heterogeneous wireless and wired networks,* New York, USA, 2006.
[Shim6] Shim6 Implementation Report : LinShim6, draft-barre-shim6-impl-03, http://tools.ietf.org/html/draft-barre-shim6-impl-03
[SJZS05]. W. Song, H. Jiang, W. Zhuang, and X. Shen, “Resource management for QoS support in cellular/WLAN interworking,” *in IEEE Network Mag*., vol.19, no.5, pp. 12-18, Oct. 2005.
[TCP09] Nikolay Tcholtchev, Ranganai Chaparadza, and Arun Prakash, “Addressing Stability of Control-Loops in the context of the GANA architecture Synchronization of Actions and Policies,” *acc. to IWSOS 2009.*
[TGV10] Nikolay Tcholtchev, Monika Grajzer and Bruno Vidalenc, “Towards a Unified Architecture for Resilience, Survivability and Autonomic Fault-Management for Self-Managing Networks,” *accepted in proc. s of the 2nd Work. on Monitoring, Adapt. and Beyond (MONA+), 2009.*
[TKP08]T. Kastrinogiannis, V. Karyotis, and S. Papavassiliou, “An Opportunistic Combined Power and Rate Allocation Approach in CDMA Ad Hoc Networks,” *in Proc.of 2008 IEEE Sarnoff Symposium on Advances in Wired and Wireless Communications*, p.p.1-5, April 2008.
[TKP08’] T. Kastrinogiannis, V. Karyotis, and S. Papavassiliou, “On the Problem of Joint Power and Rate Control in CDMA Ad Hoc Networks”, *in Proc of 3rd Int. Symp. on Wireless Pervasive Comp., 2008. (ISWPC 2008)*. p.p.78-82, May 2008.
[TKP09_1] E. E. Tsiropoulou, T. Kastrinogiannis, and S. Papavassiliou, “Realization of QoS Provisioning in Autonomic CDMA Networks under Common Utility-Based Framework” *in Proc. of IEEE WoWMoM workshop on Autonomic and Opportunistic Comm.*, AOC’09, June, 2009.
[TKP09_2] E. E. Tsiropoulou, T. Kastrinogiannis, and S. Papavassiliou, “A Utility-based Power Allocation Non-cooperative Game for the Uplink in Multi-Service CDMA Wireless Networks,” *in Proc. of 5th Int. Wireless Com. and Mobile Computing Conference*, June, 2009.
[TKP09_3] E. E. Tsiropoulou, T. Kastrinogiannis and S. Papavassiliou, “QoS-Driven Uplink Power Control in Multi-Service CDMA Wireless Networks - A Game Theoretic Framework”, *Journal of Com., Academy Publisher*, Oct. 2009.
[TS06] Thomas Scherer. Mbsp is NP complete. (http://wiki.uni.lu/secan-lab/docs/mbsp.pdf), May 2006.
[W02] L. Westberg, , et al., "Resource Management in Diffserv (RMD): A Functionality and Performance Behavior Overview", IFIP PFHSN'02.
[WCLL08] Fang Wang, Shanzhi Chen, Xin Li, Yuhong Li, "A Route Flap Suppression Mechanism Based on Dynamic Timers in OSPF Network," *icycs,pp.2154-2159, 2008 The 9th Inte. Conf. for Young Computer Scientists,* 2008.
[X09_1] Y. Xiao, "Calculating the reliability of communication networks using an enhanced OBDD algorithm", *accepted to the Journal of China Universities of Posts and Telecom.*, 2009.
[X09_2] Y. Xiao, "Evaluate Reliability of wireless sensor networks with n enhanced OBDD Algorithm", a*ccepted to the Journal of China Universities of Posts and Telecommunications*, 2009.
[XCLL] Yufeng Xiao, Shanzhi Chen, Xin Li, Yuhong Li, “The Adaptive Loopback Mechanism for LSP Failure Detection,” *Journal of Beijing University of Posts and Telecom. (accepted)*.
[XLCC08] Dahai Xu, Ying Li, M. Chiang, and A. Calderbank, “Elastic service availability: utility framework and optimal provisioning,” *IEEE JSAC,* vol.26, no.6, pp.55-65, Aug. 2008.
[XWY] Gong Xiangyang, Wang Wendong, Li Yan, “A Novel Packet Marking Algorithm in Context-aware Autonomic QoS Framework”, *submitted to Journal of China Communication*.
[YWK07] Y. Yang, J. Wang, and R. Kravets, “Distributed Optimal Contention Window Control for Elastic Traffic in Single Cell Wireless LANs,” *IEEE/ACM Trans. on Networking*, vol. 15, no. 6, pp. 1373 – 1386, Dec. 2007.
[Z09] X. Zheng, "An autonomic connection management mechanism based on mobile terminal", *in proc. of the 1st In. ICST conf.on Mobile Networks and Management*, October 2009.