Adaptive Network Control and Management for Beyond 3G End-to-End Reconfiguration

Zachos Boufidis[1], Nancy Alonistioti[1], and Markus Dillinger[2]
[1] The University of Athens, Athens, Greece
[2] Siemens AG, Munich, Germany
E-mail: boufidis@di.uoa.gr, nancy@di.uoa.gr, markus.dillinger@siemens.com

Abstract— **Reconfiguration is the action of modifying the operation or behaviour of a system, a network node, or functional entity. The end-to-end notion dictates that, in certain cases, control and management plane interactions may occur from source to destination in order to adapt the system, the equipment, the application, the service, or the content. This paper describes an integrated control and management plane framework for end-to-end reconfiguration, and maps this model to a Beyond 3G mobile network architecture. Policy control aspects for end-to-end reconfiguration differentiation are also described, aiming at diverse service offering.**

Index Terms— **All-IP Network, Reconfiguration Management Plane, plane management, layer management, policy control.**

I. Introduction

Evolution of 3G cellular mobile systems and interworking with off-the-shelf products (e.g., WLAN cards and access points) in conjunction with the progress on broadband wireless IP-based networks (e.g., IEEE 802.16 series, IEEE 802.20) and digital broadcasting (e.g., DVB-T, DAB) raises new research challenges for the control and management of such Composite Radio Access Networks (RANs). On the other hand, the trend towards All-IP mobile networks, with IP routing, mobility, and Quality of Service (QoS) mechanisms in addition to recently adopted bare IP transport, necessitates further research on the efficient application of IT temperament in evolving telecom world networking [1].

Reconfiguration spans across end-user devices, network equipment, software, and services. Target reconfigurable elements include, in the mid-term, the User Equipment (UE) and Base Stations or Access Points. Signal-processing modules in the UE as well as firmware enhancing the Hardware Abstraction Layer (HAL) can be upgraded. Operational and non-operational software can be downloaded [2]. Service and content adaptation have already gained attention in the mobile world, promising on-the-fly playout adaptation via, for example, download of upgraded codecs. In the long-term, interior network nodes such as routers and switches or even (parts of) the network itself could be reconfigured, especially for large user groups requesting specialized treatment.

In order to accomplish flexible service offering and to cope with complex systems, the need for end-to-end reconfigurable architectures, systems, and functions raises [3]. Within this context, the EU FP6 Integrated Project IST-E²R (End-to-End Reconfigurability) [4] aims to devise, develop and trial architectural design of reconfigurable devices and supporting system functions to offer an expanded set of operational choices to the users, application and service providers, operators, and regulators in the context of heterogeneous mobile radio systems.

End-to-end reconfiguration dictates the design and specification of an integrated control and management plane for coordinating the interactions between the involved entities, and for enabling the decision-making and enforcement of mechanisms supporting reconfiguration in a dynamic fashion. In [5], the Reconfiguration Management Plane (RMP) was introduced, whose main task is to provide layer abstractions to applications and services on one hand, and to terminal equipment and network devices on the other. Furthermore, the RMP is responsible for the coordination of the reconfiguration process and for the provision of the required resources. In this paper, we augment the identified plane management modules with layer management functions and identify key challenges for policy-based reconfiguration differentiation.

The rest of the paper is organized as follows: the design goals of modelling control and management functions for end-to-end reconfiguration are sketched in Section 2. The constituent RMP modules and the mapping of the RMP logical model to evolved physical configurations are described in Section 3. The challenge for end-to-end reconfiguration differentiation is elaborated in Section 4. We conclude and describe future work on accomplishing the differentiation of reconfiguration services in Section 5.

II. Design Goals

End-to-end reconfigurability necessitates an integrated framework to address all management aspects related to composite reconfigurable environments. The ITU FCAPS topics, i.e., Faults, Configuration, Accounting, Performance, and Security, comprise traditional management areas, along with resource management and access and security management. The 3GPP has introduced additional management areas tailored to the management domains and areas of a 3G PLMN, including roaming management, fraud management, software management, User Equipment Management (UEM), QoS Management, Subscription Management, and Subscriber and Equipment Trace Management [6].

The Reconfiguration Management Plane comprises a network-agnostic protocol-independent model for specifying operations and notifications. The RMP comprises a logical model, i.e., an expression of an abstract view of a network element or subnet by means of functional entities incorporating specific functionality to realize physical implementation independent control and management tasks. The Reconfiguration Management Plane can be considered either as extension to existing control and management planes or as a new intermediary plane between legacy control and management planes for dedicated reconfiguration-related tasks, such as context management, policy and profile definition and provision, service management, and native reconfiguration and download management. In addition, the RMP incorporates layer management functions tailored to the O&M needs of reconfigurable network elements and subnets (e.g., Composite RANs). The above design considerations are fulfilled by the RMP modules described in the following section.

The proposal of physical configurations based on concrete network architectures is achieved by mapping the RMP model to a horizontal, two-tier organization of reconfiguration managers within a single administrative domain. These managers are hereafter called the ReConfiguration Manager (RCM) and the Radio Reconfiguration Support Function (R-RSF). This pair of network elements is capable of interworking with systems not offering all areas of traditional management and control, such as Wi-Fi islands. This design decision is further elaborated in the following section, which sketches the network support architecture for end-to-end reconfiguration.

III. Reconfiguration Management Plane

The Reconfiguration Management Plane accommodates the following plane management and layer management modules (Fig. 1).

A. Plane Management Modules

The RMP plane management consists of the Context Management, Policy Provision, Performance Management, Access and Security Management, Reconfiguration Management, Software Download Management, Service Provision, and Billing and Accounting Management modules.

The *Context Management Module (CMM)* monitors, retrieves, processes, and transforms contextual information. Contextual information affects the service provision phase, and provides input to policy decisions and reconfiguration strategies. Contextual information includes profile information as well as resource-specific information. Profile composition and provision is handled by the CMM *Profile Management Module (PrMM)*, which manages and combines the different profiles. Profile information originates from different parts of the system, and includes user profile, network profile, application/service/content profile, terminal profile (the so-called Reconfigurability Classmark), charging profile, and security profile. The CMM *ReSource Management Module (RSMM)* handles resource-specific data regarding the reconfiguration progress, such as the operational mode, state information, and congestion indication. In addition, the CMM *Reconfigurability ClassMarking Module (RCMM)* assigns and retrieves the *Reconfigurability Classmark*, which characterizes any mobile terminal and specifies the level of dynamism regarding reconfiguration, as well as the capabilities of the terminal (e.g., enhanced MExE/WAP classmark). The calculated value of the classmark depends on the type of reconfiguration requested and negotiated, on the type of software to be downloaded, on business incentives, and on individual or operational chains of stakeholders involved in the reconfiguration process.

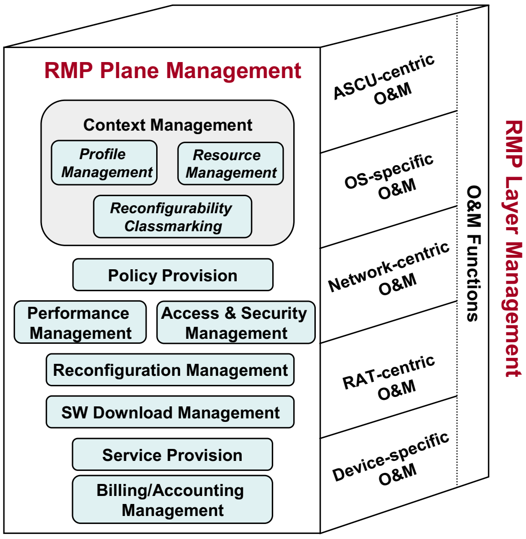

Figure 1. The Reconfiguration Management Plane.

The *Policy Provision Module (PPM)* is the main decision-making entity for reconfiguration, by comprising the entry point for reconfiguration-related system policies. Furthermore, it exploits contextual information and redefines policy rules and reconfiguration strategies. This module produces an up-to-date decision about the feasibility of a reconfiguration as well as respective actions to be triggered. In addition, the PPM caters for inter-domain issues, interacts with Policy Enforcement Points (e.g., in the GGSN), and facilitates the mechanics for the differentiation of end-to-end reconfiguration services.

The *Performance Management Module (PMM)* collects performance measures, usage data, and traffic data, and estimates performance and cost constraints, which can be exploited for network-initiated element reconfiguration.

The *Access and Security Management Module (ASMM)* participates in the mutual authentication of the user reconfigurable terminal, verifies the authorization to download, and determines the security control mechanisms (e.g., agreement on security keys) prior to download transfer.

The *Reconfiguration Management Module (RMM)* initiates network-originated and coordinates device-initiated configuration commands, by communicating with Reconfiguration Support Functions at the User Equipment (U-RSF), as well as at interior network nodes (e.g., the R-RSF handling a Composite RAN). In order to accomplish the supervision of end-to-end reconfiguration, the RMM incorporates the signaling logic, including negotiation and capability exchange services. In the case of scheduled software download, the Reconfiguration Management Module hands-over the control of the residual reconfiguration steps to the Software Download Management Module. Finally, the RMM undertakes the necessary session management and Mobility Management (MM) context transfer and translation in cases of inter-domain handover, e.g., from a 3GPP System to a WLAN/Wi-Fi access network.

The *Software Download Management Module (SDMM)* is responsible for identifying, locating, and triggering the suitable protocol or software for download, as well as for controlling the steps during, and after download.

The *Service Provision Module (SPM)* is responsible for the interaction between the RMP and the application/service. This entity accepts and processes service improvement requests from the service providers. In addition, the SPM can initiate a reconfiguration command on behalf of the application. For example, it can initiate network configuration changes or selection of different settings by the users, or it can launch mobility-induced events. In addition, the Service Provision Module may trigger service adaptation actions based on network or device capability modifications, or based on updated policy conditions. Finally, roaming issues for service provisioning are also tackled by the SPM.

Finally, the *Billing and Accounting Management Module (BAMM)* collects charging records from the additional network elements supporting reconfiguration (i.e., the R-RSFs), processes these records, and apportions the reconfiguration-induced revenues to the involved business players.

B. Layer Management Functions

Layer management functions handle Operation and Maintenance (O&M) tasks per protocol layer. The number and scope of these layers depends on the managed environment. In environments supporting end-to-end reconfiguration, layer management functions can be introduced in order to support the service provision stage, and should be adapted based on input related to the definition and enforcement of reconfiguration policies. End-to-end differentiation of reconfiguration services should also take into account the outcome of reconfiguration functions for O&M, such as monitoring reports and capabilities of network elements.

Reconfiguration-oriented O&M functions can be classified to five categories: Application-, Service-, Content- and User-centric (ASCU) functions; Operating-System-specific; Network-centric; RAT-centric; and Device-specific.

Provision of customer care information is a typical example of *ASCU-centric O&M* function. Logging is an important feature, offering the history of reconfiguration actions (e.g., recent over-the-air upgrades), statistical information on the latest faults and alarms reported to the user, etc.

OS-specific O&M functions should coordinate the auditing, testing, and validation procedures at the reconfigurable terminal. *Network-centric O&M* functions estimate the impact of mobility and QoS on the software download process. In addition, dynamic network planning and its impact on traffic split comprise important O&M functions for reconfigurable network elements.

RAT-centric O&M functions manage RAT-specific issues for a single Radio Access Technology or guarantee efficient collaboration of multiple RATs. The Composite Radio Environment Management function handles stability, conflict resolution, and certification issues, and ensures proper collaboration between network infrastructure manufacturers and terminal providers. The Radio Element Management function cooperates with the RMP Performance Management Module. Analysis of RAT-specific performance data is an example of performance management, which may in turn affect real-time reconfiguration. The Function Partitioning and Reallocation entity coordinates coupling issues as well as distribution of functional entities for multi-RAT environments owned by a single administrative authority. Finally, the Interworking function verifies the correct operation of control plane functionality between radio elements owned by different operators, as well as network sharing scenarios. RMP RAT-centric O&M functions communicate with the R-RSF for efficient management of composite multi-RAN environments.

Device-specific O&M functions include, for example, functions for User Equipment Management. Remote equipment diagnosis assists in the remote identification of equipment faults, taking into account security threats. Finally, coordination with Hardware Abstraction Layer configuration modules can also be accomplished through device-specific RMP O&M functions.

C. The RMP in a Beyond 3G Mobile Network

The provision of end-to-end reconfiguration services and reconfiguration management in Composite RAN environments, coupled with scenarios of evolved core network architectures [7], should be accommodated via the two-tier control and management architecture depicted in Fig. 2. From a high-level perspective, the architecture consists of two managers, i.e., the ReConfiguration Manager and the Radio Reconfiguration Support Function.

The RCM comprises a realization of the RMP logical model to the heterogeneous network architecture. In order to cope with complex and interleaved scenarios, the RCM is located at the highest network hierarchy, i.e., either in the core network domain (e.g., attached to the Gi and/or the Gp interface in a 3GPP System) or in a Trusted Third Party (TTP) domain. Alternatively, the RCM would be distributed in the core network, with its functionality apportioned to the SGSN and GGSN. The first option facilitates future architectural scenarios. For example, apart from intra-domain connection of RAN nodes to multiple CN nodes currently supported in a

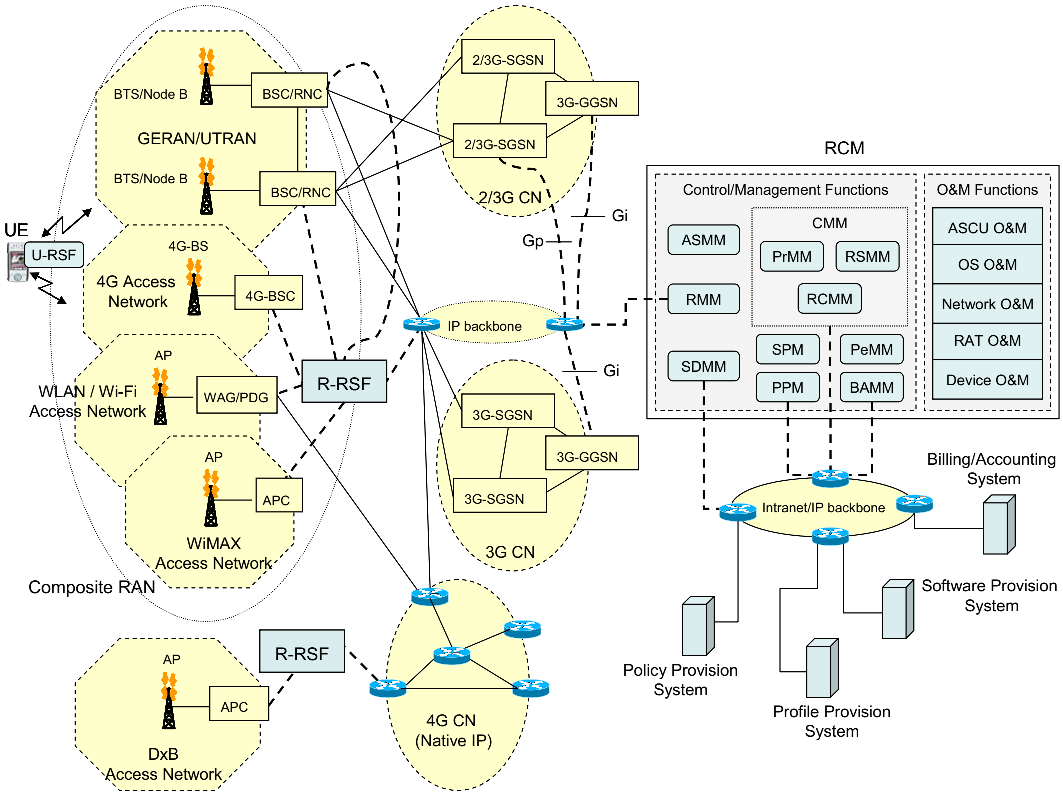

Figure 2. The RMP in a Beyond 3G mobile network architecture.

3GPP Release 6 System inter-domain connection as well as network sharing scenarios dictate the presence of the RCM as a separate network element beyond the GGSN in the network hierarchy. This decision also facilitates independent evolution paths for future all-IP core networks, i.e., with IP routing and IP mobility except IP transport [1]. The second option is more efficient for mobility management purposes; when a User Equipment abruptly de-attaches from a 3GPP System and attaches to a WLAN or Wi-Fi hot-spot, the RCM Reconfiguration Management Module should undertake the transfer of the necessary Mobility Management (MM) context from the source SGSN to the target WLAN or Wi-Fi Access Gateway / Packet Data Gateway (WAG/PDG). Mapping the MM context to the target MM information elements should be performed by the RCM-RMM as well, thus achieving hard and soft handover scenarios.

The R-RSF manages a single or a Composite RAN, thus being responsible for functions such as Joint or Common Radio Resource Management, Network Planning, and Spectrum Management [7].

Fig. 2 also depicts a collection of repositories in the form of four integrated systems. The collection of profile repositories in reconfigurable Beyond 3G systems should be viewed as a composite *Profile Provision System (PPS)*. The PPS should apply to an n-tier system capable of disseminating profile management policies into an n-layered architecture. Such multi-tier architecture can be constructed based on topological considerations and/or on semantic aspects. Segmentation and distribution of profile data representation via *profile staging,* and a two-dimensional (topology-based) multi-tier (semantic-oriented) hierarchical organization of profile managers should offer performance and flexibility benefits.

Accordingly, the download servers are organized into a *Software Provision System*, whilst the *Policy Provision System* holds reconfiguration policies and strategies. Finally, the *Billing and Accounting System* calculates the revenues induced by reconfiguration operations, both due to signaling and user traffic.

IV. END-TO-END RECONFIGURATION INITIATION

Realization of end-to-end reconfiguration is expected to be a slowly evolving process. As the reconfiguration capabilities of network nodes and terminal equipment will be gradually enhanced, the issue of transparent operation over *Reconfiguration-Ignorant Nodes or Networks (RINs)* should be investigated. In general, network nodes and network domains are expected to fall into three categories:

- *Reconfiguration-enabled*: A node or domain (e.g., autonomous system, routing area) with full reconfiguration capabilities.
- *Reconfiguration-aware RIN*: A node or domain being aware that it can or cannot support reconfiguration signalling and procedures.

- *Reconfiguration-unaware RIN*: A node or domain which has no capabilities to interpret any reconfiguration commands. Signalling traverses such node/domain transparently.

Within this context, the scope, definition, retrieval, and associated signalling exchange to exploit a new identifier that characterizes spatially and temporally an end-to-end reconfiguration service should be explored. Such an *End-to-end Reconfiguration Label (ERL)* comprises an expression of end-to-end reconfiguration capabilities piggybacked onto the data and/or control path in order to assist in the initiation, negotiation, and enforcement (classification and filtering) of end-to-end reconfiguration. The ERL should be a globally unique identifier incorporating legacy parameters when software download and reconfiguration signalling traverses 3G networks (e.g., MS Class A, B, C; IMEISV (IMEI Software Version); NMO (Network Mode of Operation) I, II, III; RAN mode A/Gb, Iu; RAT type GERAN, UTRAN; MS classmark; CN classmark; Radio access classmark; Network Identity and Time Zone [8]), as well as new identifiers for Beyond 3G networks. These fields should accommodate evolving capabilities of the terminal equipment (expressed via the Reconfigurability Classmark), the user profile, the service and content profile (e.g., Circuit Switched IMS [IP Multimedia Subsystem] Combinational Service), the charging profile, the security profile, and the runtime profile. In addition, the reconfiguration capabilities of network elements on the end-to-end data path (based on the above categorization), and the network/subnet profile should be taken into account. The network profile can be expressed via high-level system identities (e.g., 3GPP Release 5 with HSDPA vs. 3GPP Release 6 with network sharing and IMS Phase 2; interior MPLS subnet employing LDP vs. MPLS with RSVP-TE). Finally, presence and roaming issues as well as inter-operator agreements should affect the end-to-end reconfiguration procedure and, consequently, the ERL.

V. Conclusion

We presented an integrated plane management and layer management framework for the support of end-to-end reconfiguration, and elaborated on the constituent modules for control and management operations. The introduced Reconfiguration Management Plane comprises a network-agnostic protocol-independent model for specifying operations and notifications, viewed as extension to existing control and management planes or as a new intermediary plane for dedicated reconfiguration-induced tasks.

Envisaging the major challenges for end-to-end reconfiguration differentiation, we identified the requirement of communication between reconfiguration-aware and unaware nodes, and the necessity to offer transparent reconfiguration services in the form of "service pipes". In order to accomplish operation over reconfiguration-ignorant nodes or domains, we proposed the End-to-end Reconfiguration Label for packet classification and filtering. We plan to further investigate design issues pertaining to the granularity of such label, and to incorporate various reconfiguration classes. It is our conjecture that such tagging should assist in the initiation, negotiation, and enforcement of end-to-end reconfiguration.

Future work on the differentiation of policy-based reconfiguration services includes a target switching mechanism between pure Service-Based Local Policy (SBLP), native IP QoS signalling, and IP QoS signalling tailored to SBLP [9]. SBLP enables IMS and non-IMS Application Functions to control the QoS provided by the GPRS bearer service based on the requirements of the negotiated application services, exploiting the COPS protocol and PDP context modification procedures. Finally, since the IETF Policy Framework [10] does not address inter-domain or end-to-end policy control, our next steps include research on collaboration of clusters of Policy Decision Points (PDPs) via a supervising entity that interfaces with the RMP Policy Provision Module of multiple administrative domains. An alternative distributed solution through a coordination protocol between multiple PDPs should work as well. We will analyse the pros and cons of these inter-domain policy provision options from the required business incentives viewpoint, the network management aspect, and the associated technical implications.

Acknowledgment

This work has been performed in the framework of the EU funded project E²R. The authors would like to acknowledge the contributions of their colleagues from E²R consortium.

References

[1] 3GPP TR 22.978, "All-IP Network (AIPN) Feasibility Study (Release 7)", V1.0.0, Oct. 2004.

[2] The Software Defined Radio (SDR) Forum, http://www.sdrforum.org/.

[3] M. Dillinger, K. Madami, and N. Alonistioti (Editors), *Software Defined Radio: Architectures, Systems and Functions*, John Wiley & Sons Ltd, 2003

[4] IST-2003-507995 Project E²R (End-to-End Reconfigurability), http://e2r.motlabs.com/

[5] N. Alonistioti, Z. Boufidis, A. Kaloxylos, and M. Dillinger, "Integrated Management Plane for Policy-based End-to-End Reconfiguration Services", 13th IST Mobile and Wireless Communications Summit, Lyon, France, June 2004.

[6] 3GPP TS 32.101, "Telecommunication management; Principles and high-level requirements".

[7] S. Uskela, "Key concepts for evolution toward Beyond 3G Networks", *IEEE Wireless Communications*, vol. 10, no. 1, Feb. 2003..

[8] 3GPP TS 23.060, "General Packet Radio Service (GPRS); Service description; Stage 2".

[9] 3GPP TS 23.207, "End-to-end Quality of Service (QoS) concept and architecture".

[10] The IETF Policy Framework Working Group, http://www.ietf.org/html.charters/policy-charter.html