Network Support Modeling, Architecture, and Security Considerations for Composite Reconfigurable Environments

Zachos Boufidis, University of Athens, Greece
Rainer Falk, Siemens AG, Corporate Technology, Germany
Nancy Alonistioti, University of Athens, Greece
Eiman Mohyeldin, Siemens AG, Germany
Nikolas Olaziregi, King's College London, UK
Bertrand Souville, DoCoMo Communications Laboratories Europe GmbH, Germany

ABSTRACT

Emerging radio access technologies such as wireless personal and metropolitan area networks and digital broadcasting are a new era for wireless communications. These standards aim at complementing existing cellular/Wi-Fi networks in order to offer a wide range of available access modes to mobile terminals. Multiradio wireless systems referred to as composite radio access networks, bear diverse capabilities, with the optimal radio being invoked to perform a specific set of functions. Composite reconfigurable radio networks support the collaboration of a wide range of heterogeneous radio access technologies under a single or multiple administrative boundaries, adding further intelligence to the way devices attach to and switch between networks spatially and temporally. The EU End-to-End Reconfigurability (E²R) research project envisages composite reconfigurable radio networks coupled with legacy as well as evolved core network architectures, yielding simpler and flexible configurations for reduced latencies, autonomic operation, and adaptive functionality. This article presents a cohesive model for controlling and managing such networks, elaborates on the constituent functional entities, and maps this model to two-tier network support architecture. Finally, key security issues for software download over reconfigurable radios and systems are identified and solutions for software certification and authorization as well as for the authentication of roaming terminals are proposed.

INTRODUCTION

One of the trends in the wireless commercial market is to modify over-the-air certain functionalities of the mobile terminals and base stations [1]. The possibility to upgrade the firmware of user equipment due to glitches is already a reality, whereas the first software radio GSM base station has been deployed using an Internet connection to download new releases of the base station software [2]. Composite reconfigurable radio networks exploit the Software-Defined Radio (SDR) concept [3,4], leading to heterogeneous multiradio platforms offering a wide range of access modes to reconfigurable terminals. Examples of Radio Access Technologies (RATs) include legacy cellular (2G/3G TDMA/CDMA), beyond 3G cellular (e.g., High-Speed Downlink Packet Access, Enhanced Uplink, Multimedia Broadcast/Multicast Service, Super 3G), wireless personal (e.g., Ultra-WideBand, ZigBee), local (e.g., IEEE 802.11 series), and metropolitan access (e.g., IEEE 802.16 series, IEEE 802.20), as well as digital broadcasting (e.g., DVB-H). On the other hand, convergence of the Internet with 3G mobile communication systems, and increasing user needs for seamless pervasive services and for ubiquitous access at higher bit rates and processing capacity, lead to the Next Generation Internet based on Grid infrastructures over ultrahigh-speed optical backbones.

In order to accomplish flexible service offering and to couple composite reconfigurable radio networks with evolved Core Networks (CNs), the need for end-to-end architectures, systems, and functions raises. In this context, the European IST FP6 Integrated Project E²R [5] 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. E²R project explores solutions for the control and management of increasingly complex networks that facilitate self-configuration (i.e., the ability to adapt to system changes), self-healing (i.e., the ability to recover from detected errors), self-optimization (i.e., the ability to improve the use of resources), and self-protection capabilities (i.e., the ability to anticipate and cure intrusions).

This article analyzes the standardization status and related EU R&D efforts, and outlines the major design decisions when modeling network support architectures for composite reconfigurable radio networks. An innovative network-agnostic protocol-independent model for specifying operations and notifications in such systems is presented, the hereafter called Reconfiguration Management Plane (RMP). The way the RMP logical model is mapped to two-tier physical control/management architecture is elaborated and important security issues for software download over reconfigurable radios and systems are highlighted.

Standardization and Research Initiatives

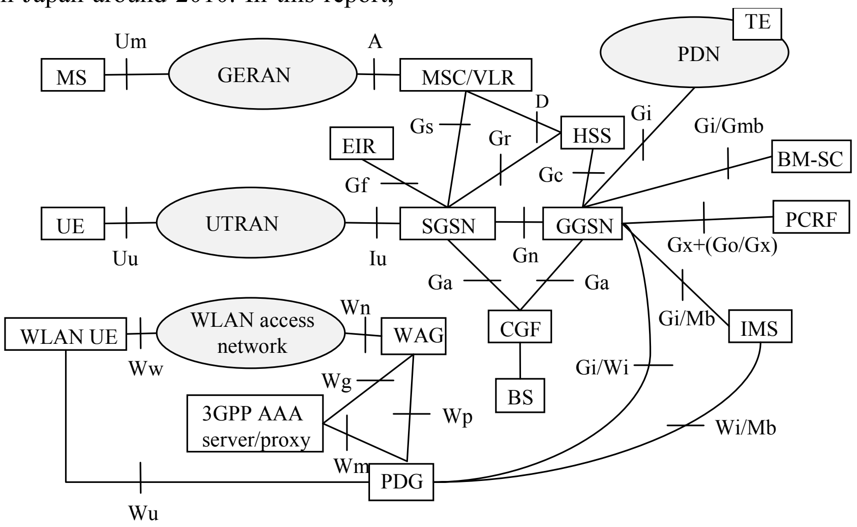
Analysis of Standardization Status

Various studies on software defined, reconfigurable and composite radios have been undertaken by fora and research consortia since the beginning of the 1990s. The SDR Forum [6] defined an open architecture for software radios applicable to military and commercial applications in 1997 and reached a broad audience through liaison activities with European research programs (e.g., TRUST/SCOUT, E^{2}R), with Asian activities (e.g., IEICE), and with standardization bodies (e.g., ITU, OMG). Currently, the SDR Forum aims to harmonize the regulations for software radios worldwide and continues to survey market opportunities and enabling technologies for software radios. The Wireless World Research Forum (WWRF) has established a working group dedicated to Reconfigurability [7], which has been producing a series of white papers on reference models and architectures for reconfigurable equipment and supporting networks. The Mobile IT Forum published a report entitled "Flying Carpet" describing the vision and requirements for future mobile communication services in Japan around 2010. In this report, terminal reconfigurability is one of the identified functions required for 4G mobile systems enabling reconfigurable user equipment to be adaptive to service and user environment.

End-to-end composite reconfigurable environments necessitate an integrated framework to cover all management aspects. The ITU-T TMN FCAPS functions (faults, configuration, accounting, performance, and security) comprise traditional management topics [8], 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, quality of service (QoS) management, subscription management, and subscriber and equipment trace management [9]. The basic configuration of a 3GPP Release 7 System is depicted in Fig. 1 [10].

The above management procedures are activated during network-initiated scenarios, e.g., following the assessment of offline performance measures. However, network initiation may not always be the case; for example, fault management is usually device-initiated, as network elements incorporate self-healing capabilities. These management areas are usually served by management plane functions.

This article enhances and extends these areas in the form of the so-called *reconfiguration plane*, which includes control and management functions tailored to composite reconfigurable environments. In addition, *reconfiguration*



Legend

AAA	Authentication, authorization, and accounting	PCRF	Policy and charging rule function
BM-SC	Broadcast/multicast service centre	PDG	Packet data gateway
BS	Billing system	PDN	Packet data network
CGF	Charging gateway functionality	SGSN	Serving GPRS support node
EIR	Equipment identity register	TE	Terminal equipment
HSS	Home subscriber server	UE	User equipment
IMS	IP multimedia subsystem	UTRAN	UMTS terrestrial radio access network
GERAN	GSM enhanced radio access network	VLR	Visitor location registry
GGSN	Gateway GPRS support node	WAG	WLAN access gateway
MS	Mobile station	WLAN	Wireless local area network
MSC	Mobile services switching centre		

Figure 1. Basic configuration of a 3GPP Release 7 system.

layer management functions are proposed for handling Operation and Maintenance (O&M) tasks. These functions maintain interfaces to all protocol layers both in the control and management planes and administer parameters and resources specific to three generic layers that offer reconfiguration capabilities.

Satisfaction of security concerns of the stakeholders involved in the reconfigurability lifecycle (network operators, service providers, and equipment manufacturers) comprises an important prerequisite for the successful introduction of reconfigurable devices in the market. Secure reconfiguration involves the secure download to defend against potentially malicious software and to prevent the manipulation of the reconfiguration process. Communication between involved nodes has to be protected ensuring authenticity, integrity, and confidentiality with the use of existing protocols such as IPsec or SSL/TLS (Secure Sockets Layer / Transport Layer Security). Many commercially available mobile terminals already support the download of Java MIDlets, i.e., small Java applications executed in a restricted runtime environment referred to as "sandbox". The advent of Mobile Information Device Profile (MIDP) version 2.0 led to the distinction of untrusted and trusted MIDlet suites. The recommended security policy for GSM/UMTS compliant devices defines four protection domains, namely the manufacturer, the operator, the third party, and the untrusted domain. A digital signature (signed content) is used to bind a MIDlet suite to its protection domain, thus receiving permissions depending on its domain (e.g., granting access to restricted functions allowing sending short messages with or without requiring prompting the user for confirmation). Finally, it is worth charting the 3GPP Mobile Execution Environment (MExE) standard, which defines core software download allowed only under the control of the manufacturer.

EUROPEAN RESEARCH EFFORTS

Within the EU IST FP5 program, a number of projects have addressed terminal and network reconfiguration from different perspectives.

IST project SCOUT developed models for supporting reconfigurable mobile equipment in IP-based mobile networks, and provided concepts for intelligently customizing and managing terminal reconfiguration within a wide range of wireless access technologies [11]. In particular, reconfiguration of all layers while supporting QoS was set as a key premise during system design. The analysis of the process led to architectural specifications in areas such as the distribution of software to download and communication profiles in the network, the description of the reconfiguration process with focus on the identification of the functions involved in each step, and the definition of interfaces. The hierarchical topology of reconfiguration managers followed delayering principles of IP-based networks, presenting a logical separation of radio and core network functions, further distributed in user and control planes.

The IST project MOBIVAS developed concepts and design features for the realization of end-to-end reconfiguration services [12]. The architectural and implementation effort led to the specification and development of a prototype consisting of a reconfiguration control and service provision manager, which is responsible for service discovery and provision, network-level reconfiguration, download of operational and non-operational software (i.e., value-added services (VAS) programs), and profile management. In addition, an access network component has been designed to accelerate the download process and to cater for performance boosting. Security considerations for user registration and for the protection of downloaded software, as well as an integrated charging, billing, and accounting system for the apportionment of revenues to incumbent operators and to VAS providers comprise salient features of the MOBIVAS prototype.

IST project CREDO defined a management architecture designed to optimize the traffic load distribution and service delivery in a composite radio environment [13]. A network-access coordination protocol was proposed, with a network-assisted mechanism supporting the "always best connected" principle, in terms of the most appropriate access network for the terminal to attach. The project also showed through prototyping the benefits of integrating broadcasting technologies such as DVB-T in the composite radio environment.

Current EU initiatives include the IST FP6 projects Ambient Networks, WINNER, and E^2R. The Ambient Networks project aims at enabling scalable and affordable wireless networking, and rich and easy to use communication services [14]. Ambient Networks considers multiaccess connectivity, resource management, security, context awareness, and content handling in the form of cross-domain media flow routing, as inherent services of the so-called "ambient control space". This also comprises mechanisms for self-composition, reconfiguration, and management of mobile network components, thus reducing planning, deployment, configuration, and network maintenance costs. In particular, multi-radio resource management (RRM) functions handle inter-RAT and interadministrative collaboration, facilitating load balancing in the composite network. Finally, the cooperation between multiple network domains and with service platforms and applications relies on scalable and secure interfaces.

IST project WINNER focuses on the realization of a high bit-rate radio technology (from 100 Mbps to 1Gbps) [15]. In addition, WINNER sets its requirements in the provision of co-operation mechanisms at radio access level in the form of the "ubiquitous radio system" concept. The ubiquitous notion aims at providing user- and network-centric schemes for network selection, as well as seamless change of radio access system. The WINNER paradigm reorders the functional protocol structure of user and control planes, and extends the Radio Access Layer management plane with convergence protocols.

The following sections elaborate on the effort within IST project E^2R [5] on modeling and defining network support architecture for composite reconfigurable networks. Within

E^{2}R project, reconfigurability research is conducted in the following topics:

- Over-the-air software download aiming at equipment reconfiguration
- Dynamic selection and adaptation of access technologies and networks in order to improve the user perception
- Dynamic spectrum allocation and access for increasing the available bandwidth for user plane sessions
- Reconfiguration of hardware resources aiming at the optimization of physical layer performance (e.g., reduced power consumption).

This paper focuses on network support modeling and architecture for addressing the first two areas, thereby fulfilling security requirements as well.

MODELING AND DESIGN ASSUMPTIONS

Composite reconfigurable radio networks are designed to adapt the use of radio resources of complementary radio access technologies in an optimal way such that an expanded set of services is proposed to end users while moving/roaming between networks. In E^{2}R project, adaptation and reconfiguration of the underlying radio access technologies is performed through functional allocation and modification (adding/replacing) of the radio, terminal and network equipment functionalities. Therefore, new network support functions have to be defined for the management and control of the terminal and network equipment reconfiguration processes.

This article presents the Reconfiguration Management Plane (RMP), which comprises a network-agnostic protocol-independent model for specifying operations and notifications. The RMP is 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, management, and O&M tasks. The RMP modules support dedicated reconfigurability tasks such as reconfiguration session signaling, secure administration of the software download process, and policy-based context management. These modules belong to a logically separated reconfiguration plane, which can be considered either as a new plane or as extension to the existing control and management planes. In addition, the RMP incorporates layer management functions tailored to the O&M needs of composite reconfigurable network elements and subnets.

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. This pair of network elements is capable of interworking with systems not offering all areas of legacy management and control functions, such as Wi-Fi islands.

Apart from horizontal mapping, vertical distribution of reconfiguration intelligence across multiple administrative domains should offer flexibility and well-defined interfaces between these domains. In general, the reconfiguration procedure is governed by the serving network or by the reconfigurable terminal. Centralized network-controlled reconfiguration is advantageous in various occasions. The use of a single, central reconfiguration manager should lead to clear responsibilities in the case when the nature of a reconfiguration is not understandable to end-users, when required information is not available to them, or when reconfigurations occur so often that it would be inconvenient for end users to be directly involved (e.g., dynamic radio reconfiguration to adapt to local network conditions). However, distribution of reconfiguration control to several managers — with each one handling a single administrative domain — should prove an efficient design decision for roaming scenarios. For example, decentralization in visited networks allows for local adaptations to be implemented by the visited reconfiguration manager itself, as well as for the coordinated reconfiguration of end-user and infrastructure equipment. In such architectures, the user's service provider (operator) could be at the top of the hierarchy, delegating control on terminal reconfiguration partly to roaming partners. The visited network would perform reconfiguration actions on terminals belonging to roaming users, but only as far as allowed by the users' service provider. Using several, temporally valid configuration profiles associated with specific networks allows that the changes made by a specific network are in effect only as long as that network is actually used.

THE RECONFIGURATION MANAGEMENT PLANE

The RMP accommodates reconfiguration plane modules and reconfiguration layer management functions (Fig. 2). An overview of these modules and functions follows.

RECONFIGURATION PLANE MODULES

The reconfiguration plane consists of the reconfiguration management, software download management, context management, policy provision, service provision, performance management, access and security management, and billing and accounting management modules.

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 Radio Reconfiguration Support Function, 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 RMM hands-over the administration of the reconfiguration steps after capability exchange 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 WiMAX 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 the transfer of the downloaded software.

The Context Management Module (CtxMM) 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 CtxMM Profile Management Module (PrMM), which manages and combines the different profiles (network, terminal, user, application, service, and content profile). The CtxMM 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 CtxMM Reconfigurability ClassMarking Module (RCMM) assigns and retrieves the Reconfigurability Classmark, which characterizes reconfigurable terminals and specifies the level of dynamism regarding reconfiguration, as well as the dynamic capabilities of the terminal. The calculated value of this classmark depends on the type of reconfiguration requested and negotiated, the type of software to be downloaded, on business incentives, and individual or operational chains of stakeholders involved in the reconfiguration process.

The Policy Provision Module (PPM) is the main decision-making entity, 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 interdomain issues and interacts with policy enforcement points (e.g., in the GGSN).

The Service Provision Module (SPM) is responsible for the interaction between the reconfiguration plane and the application/service. This entity accepts and processes service improvement requests from service providers. In addition, the SPM may initiate a reconfiguration command on behalf of the application. For example, it initiates network configuration changes and the selection of different settings by the users. In addition, the SPM 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.

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 device reconfiguration.

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

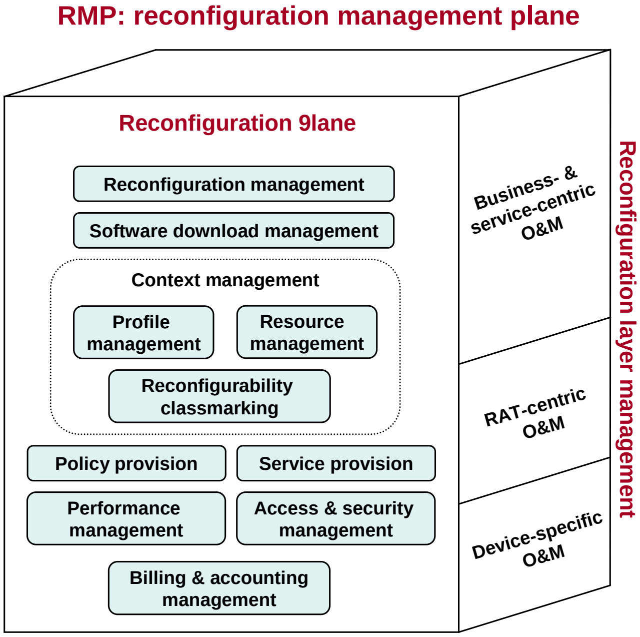

RMP: reconfiguration management plane
Reconfiguration 9lane
Reconfiguration management
Software download management
Context management
Profile management
Resource management
Reconfigurability classmarking
Policy provision
Service provision
Performance management
Access & security management
Billing & accounting management
Business- & service-centric O&M
RAT-centric O&M
Device-specific O&M
Reconfiguration layer management

Figure 2. The reconfiguration management plane.

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 induced revenues to the involved business players. These revenues are only due to reconfiguration operations, e.g., signaling and user traffic generated due to software download.

RECONFIGURATION LAYER MANAGEMENT

In environments supporting end-to-end reconfiguration, layer management functions are 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. This article classifies reconfiguration-oriented O&M functions to three generic categories: business- and service-centric functions, RAT-centric ones, and device-specific ones. The provision of customer care information is a typical example of the first category. Logging is an important feature, offering the history of reconfiguration actions (e.g., recent over-the-air upgrades) and statistical information on the latest faults and alarms reported to the user. RAT-centric functions manage parameters and resources specific to a single radio access technology, such as intelligent resource management within a single RAT (e.g., power control, allocation of RAT resources, load control). Device-specific O&M functions handle remote user equipment management, whereas remote equipment diagnosis assists in the remote identification of equipment faults, taking into account security threats. Finally, coordination with hardware abstraction layer configuration modules is also accomplished through device-specific O&M functions.

ARCHITECTURE FOR COMPOSITE RECONFIGURABLE RADIO NETWORKS

The two-tier control and management architecture depicted in Fig. 3 should accommodate the provision of end-to-end reconfiguration services and supporting management facilities in composite RAN environments, coupled with scenarios of evolved core network architectures. From a high-level perspective, the architecture consists of two managers, the Reconfiguration Manager (RCM) and the Radio Reconfiguration Support Function (R-RSF).

The RCM comprises a realization of the RMP logical model in heterogeneous network architectures. In order to cope with complex and interleaved scenarios, the RCM is located at the highest network hierarchy, i.e., either in a Trusted Third Party (TTP) domain or in the core network domain (e.g., attached to the Gi and/or the Gp interface in a 3GPP system; see Fig. 4). Alternatively, the RCM is 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 intradomain connection of RAN nodes to multiple CN nodes currently supported in a 3GPP system, interdomain connection as well as network sharing scenarios dictate the presence of the RCM as a separate network element beyond the network attachment server. This decision also facilitates independent evolution paths for future all-IP core networks, that is, with IP routing and IP mobility except IP transport. The second option is more efficient for mobility management purposes; when the user equipment abruptly detaches from a 3GPP system and attaches to a WLAN hot-spot, the RCM-RMM transfers the MM context from the source SGSN to the target WLAN Access Gateway / Packet Data Gateway (WAG/PDG). The mapping of MM context to the target MM information elements should be performed by the RCM-RMM as well, thus achieving hard and soft handover scenarios.

Following design principles of IP-based networks, the functions related to wireless connectivity are separated logically and physically. The concept of a common next-generation (i.e., 4G) IP-based core network serving multiple, heterogeneous radio access networks requires the encapsulation of access-specific functions into the R-RSF to allow for the definition of an abstract set of functions being common for all access networks [16]. The R-RSF establishes a separated modular entity lying within a domain of multi-RAN scope. This concept fits well in a system incorporating Joint Radio Resource Management (JRRM) and Dynamic Network Planning and flexible network Management (DNPM), which are investigated in the context of E^{2}R project [17]. The R-RSF implements interfaces to a variety of radio access protocol suites, depending on the composition of the heterogeneous RAN.

Radio RSF for terminals span RMP down to the composite RAN to support fast environment scanning when managing the context of the multiaccess network. Radio RSF assist the

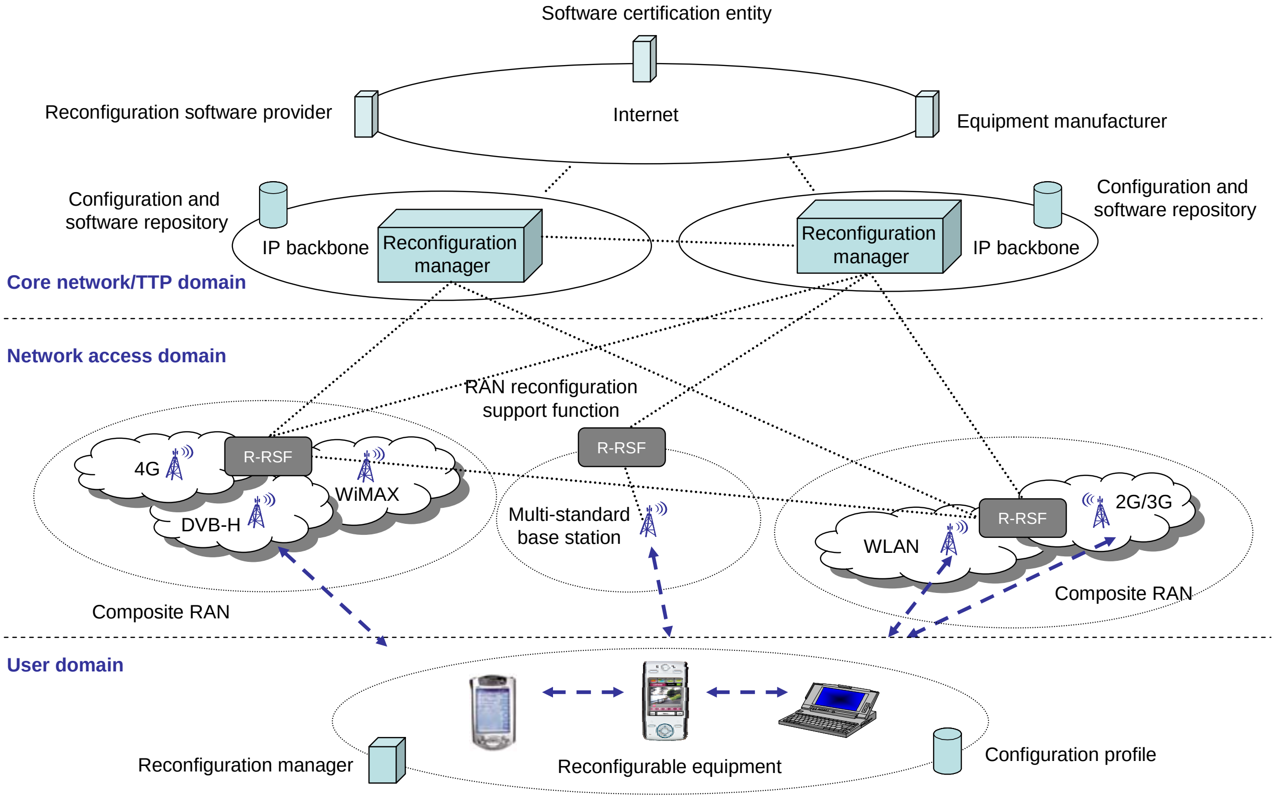


Figure 3. High-level architecture for composite reconfigurable radio networks.

terminal by interacting with radio network layer elements of available RANs, implementing interworking functions where needed. The translation mechanisms occur in the access stratum towards radio elements in different RANs and/or operators domains. Subsequently, the terminal reconfiguration process benefits from rapid detection, identification, monitoring, negotiation, and selection of the most suitable access network. Furthermore, traffic management for spectral efficient downloads is enhanced in that interworking is closer to the radio resource controlling servers.

Radio RSF for Base Stations (BS) also fall within the access stratum sphere. The DNPM mechanisms [17] interwork with RMP layer management functions local to radio network subsystems (i.e., with RAT-centric O&M functions). BS service-profile management describes the hardware, software, and functional (e.g., air-interface) capabilities, software download management manages the download of additional or new software modules required for a specific configuration, load/traffic management controls the allocation of resources to a specific standard, and performance/load monitoring monitors the hardware and software resources within a base station.

The optimization of network resources in a composite reconfigurable network is rather challenging since the operational costs associated with these optimizations should be kept at a minimum. Therefore, the interactions between the R-RSF and the RCM RAT-centric O&M functions should be automated for the implementation of the required reconfigurations after the analysis of RAT-specific performance data. In addition, the R-RSF and the RCM RAT-centric O&M should collaborate for the definition of JRRM policy rules (e.g., RSSI thresholds, OFDM code generation, admission control, traffic distribution), which are stored in the Policy Provision System. Then the RCM-PPM retrieves and delivers these conditions to the R-RSF for policing the JRRM procedures.

Fig. 4 also depicts a collection of repositories and servers in the form of four integrated systems. The Profile Provision System is the collection of profile repositories and front-end managers capable of disseminating profile information into the network support architecture. Accordingly, the download servers are organized into a Software Provision System, whereas the Policy Provision System holds reconfiguration policies and strategies. Finally, the Billing and Accounting System receives reports from the RCM-BAMM on the apportionment of revenues induced by reconfiguration operations, which are communicated to the various business players.

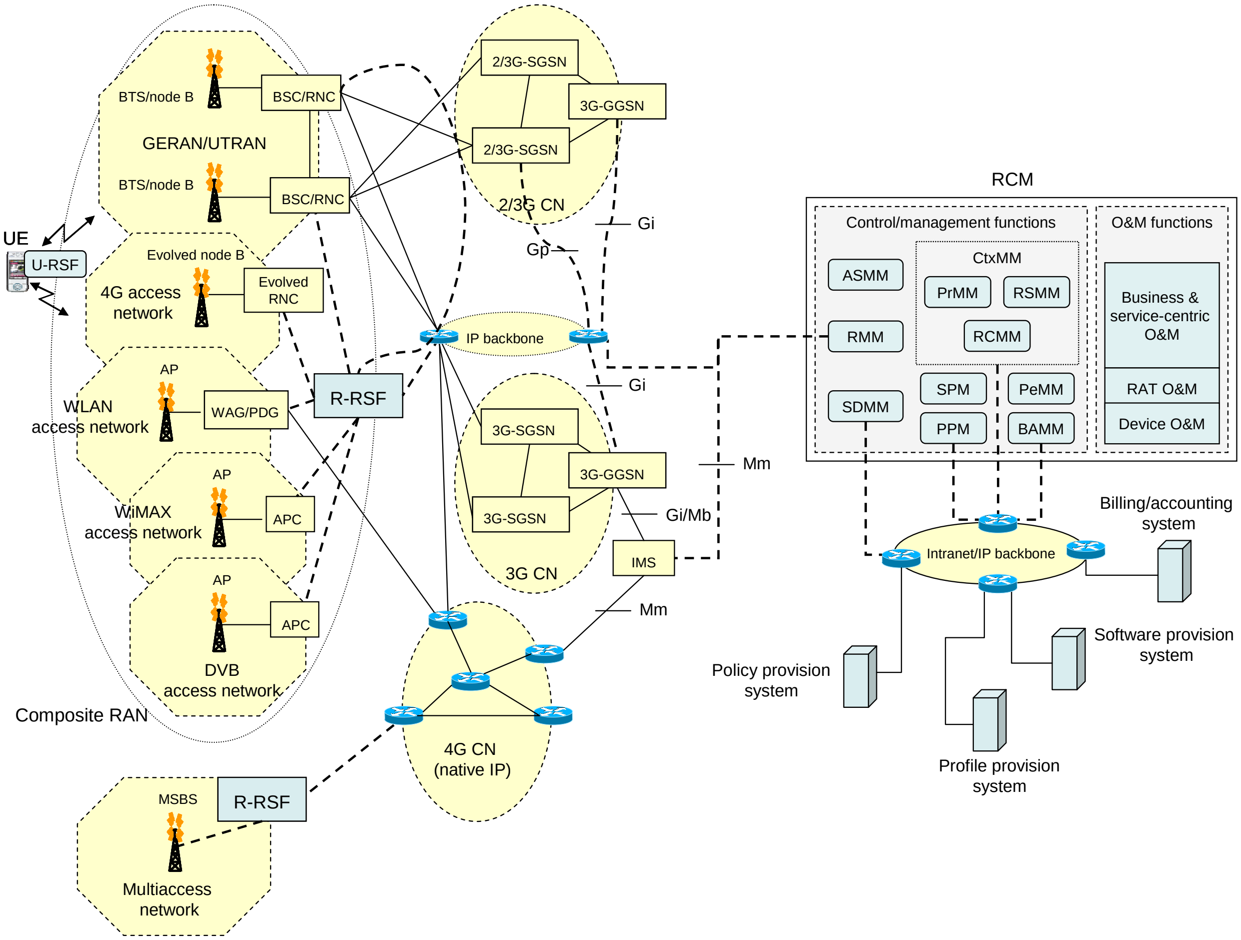


Figure 4. Detailed architecture for composite reconfigurable radio networks.

SOFTWARE DOWNLOAD AND SECURITY CONSIDERATIONS

Adaptation and reconfiguration of the radio access technologies are performed through software component replacement at the terminal and base station. The previous sections described required network support functions for the management and control of processes for reconfigurable terminal and network equipment. Ref. [18] describes the signaling between the terminal and network elements in the course of an exemplary staged process for terminal reconfiguration through over-the-air software download.

Reconfiguration allows changing the properties of communication equipment that have previously been fixed by their mere design. Such flexible configuration changes pose the threat that they contradict to the interests and expectation of end users, network operators, service providers, equipment manufacturers, and regulatory authorities. Malicious configurations and radio software could invalidate essential conformance properties. Without suitable protection mechanisms, other functionality not being directly related to reconfiguration could be negatively affected; employed mechanisms for secure network access could be circumvented, a user's private data could be accessed and sent to unauthorized parties, or premium rate numbers could be called in the background.

This section describes certification (authorization) of a reconfiguration software module, authorizing it for installation on a certain target device type, and the authorization to perform the actual software download.

SOFTWARE CERTIFICATION AND AUTHORIZATION

Basic approaches for secure software download are to verify that the software a) originates form a trusted source, and b) is executed in a restricted, managed execution environment (sandbox), controlling which actions the software performs. While a) limits from which software providers a software module is accepted before installing and executing it, b) limits the damage that an accepted piece of software could potentially cause when executing.

A well-known and widely used security mechanism to protect software download is signed content [19]. The software provider attaches a digital signature to the module that is verified by the receiving device. The digital signature ensures integrity, i.e., that the module has not been modified, and authentication of origin, i.e., that it attests its provider. The receiving device validates the signature of a received software module ensuring that it has not been tampered with and it checks whether it originates from a trusted provider. Correct root keys of authorized software providers have to be available. The kind of the provider determines where the root keys can be stored, that is, on the device itself or on a pluggable user module (e.g. the user's SIM card), and who may update them. For a managed execution environment, also the granted permissions are determined.

A central issue for secure download of radio software is the underlying policy that determines the certifying party, that is, the entity that is in the position to approve and authorize a reconfiguration software module for installation and execution on certain target device types. This entity generates the signature, thereby indicating to a mobile terminal that the software module may be accepted (authorization, approval), hence assuring that conformance properties are not invalidated. Accessibility to the radio download security solution needs to be limited to ensure that its required restrictions cannot be overridden. Even when a radio software module is authorized for downloading on a certain reconfigurable device, there may be further restrictions concerning the conditions under which it may be activated. In particular, different regulations depending on the region/location have to be respected, or a radio software module may even require dynamic authorization by the serving network.

In a vertical market model, only radio-related software authorized by the device manufacturer is accepted. In this model, the device manufacturer is still in control on what radio software is accepted on its devices. Consequently, the manufacturer can ensure that conformance properties are met, as well as ensure a proper operation. Alternative approaches suitable for horizontal market models are a current research topic. Examples include either combined or separate approval for radio hardware and radio software, moving the responsibility to check a radio configuration to a network-based validation function, the supervision of radio emissions, and applying reactive measures if a malfunction is detected. Signed content can enforce different policies in which different entities act as authorized approval authority; it can be used for a vertical market model where only software authorized by the device manufacturer is accepted, as well as for a horizontal market model, with each hardware-software combination requiring authorization from a separate trusted approval authority (Fig. 5).

Should independent approval of radio hardware and radio software be deemed acceptable, it could be realized in a similar way: Meta-information encodes the type of the authorized target devices, whereas a change history allows identifying the responsible party in case of malfunctioning configurations.

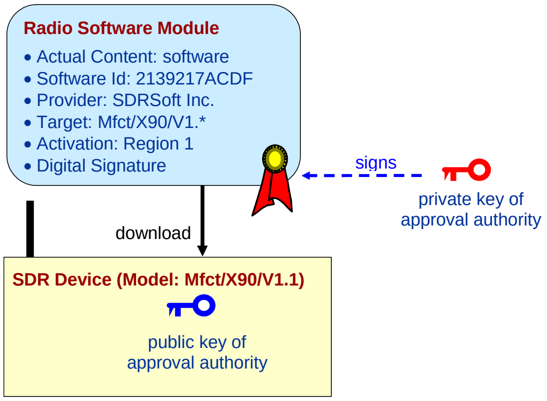

Radio Software Module
• Actual Content: software
• Software Id: 2139217ACDF
• Provider: SDRSoft Inc.
• Target: Mfct/X90/V1.*
• Activation: Region 1
• Digital Signature
signs
private key of approval authority
download
SDR Device (Model: Mfct/X90/V1.1)
public key of approval authority

Figure 5. Software certification by approval authority.

Secure software download can be complemented with a restricted radio execution environment. Control parameters driving reconfigurable radio hardware as frequency, output power, bandwidth can be validated to lie within an authorized range. Actual radio emissions can be monitored and compared with reference data such as a spectral power density mask. Reference data could be fixed or changeable only with special restrictions. These would relate to the conformance constraints that the device enforces independently of the currently executed radio software. The device itself or a communication network can monitor correct protocol behavior, e.g., obeying power control commands. The reconfiguration software of a rogue device would be terminated, and either the last correctly working software or a fixed failure mode configuration would be activated when a malfunction is detected.

AUTHENTICATION PROCEDURE FOR SOFTWARE DOWNLOAD

The previous section described solutions for the authorization of radio software for download and installation and enforcing restrictions during runtime. This section describes an authorization procedure to download reconfiguration software.

Network access is limited and constrained to specific services, following successful authentication of the mobile terminal. An authentication procedure for roaming terminals can exploit service-specific certificates, hereafter called service vouchers [20], which encode identification/permission information. In contrast to the use of the SIM card, the service voucher is not bound to a user, network operator, or service provider and is thus universally applicable. Nevertheless, its validity is temporally bound, and restricted to certain services to be consumed via specific equipment. These restrictions aim at preventing the abuse of the service voucher, for instance alleviating the repeated use on different devices by duplicating the vouchers.

A service voucher is composed of the following attributes:

- The International Vendor Identity Number (IVIN) identifies the origin/vendor of the service voucher.
- The Service Voucher Identity (SVI) can be used to distinguish service vouchers issued from the same vendor.
- The International Service Identity Number (ISIN) is a world-wide number identifying the possible type of the services associated or valid to the voucher.
- The Service Level specifies the type of service covered by the service voucher.
- The International Mobile Equipment Identity (IMEI) is the globally unique identifier of the mobile equipment.
- The expiration date specifies the time validity of the service voucher.
- Integrity and verification data, e.g., vendor private key.

The service voucher vendor possesses an IVIN as well as private/public key for asserting its validity. The user of a service voucher specifies the desired service (in the view of the ISIN), the desired validity period, and the IMEI of the equipment to be used for the specific service. Based on the above information, the vendor produces the SVI number protected using the vendor's private key.

The service voucher can be delivered to the mobile terminal during, for example, the UMTS mutual authentication procedure or as a feature of a prepaid card. The validity of the voucher is examined when the user requests the utilization of a specific service.

Figure 6 depicts the signaling exchange for the authentication procedure. As part of the Service Request message, the mobile terminal sends the service description field and the authentication attributes, i.e., the IMEI and the service voucher, to the RCM Access and Security Management Module. The service data and service voucher fields are sent to the vendor's Authentication Server that determines the vendor's public key certificate and delivers it to the RCM-ASMM. Next, the RCM-ASMM decodes the vendor's certificate and verifies the validity of the service voucher: a) certificate validity; b) comparison of the IMEI with the one indicated in the voucher; c) validity check (e.g., of the expiration date); and d) service validity check based on the ISIN. As a fallback solution for test d), redirection to another network will break the tie. Other validity tests can be optionally run to check SVI/IMEI presence in black lists or terminal compatibility for the designated services.

In case all the above authentication and certification tests are positive, a service provider is identified and a connection to that provider via the network operator is established. Finally, the RCM-ASMM sends as authentication response a Service Response message to the mobile terminal.

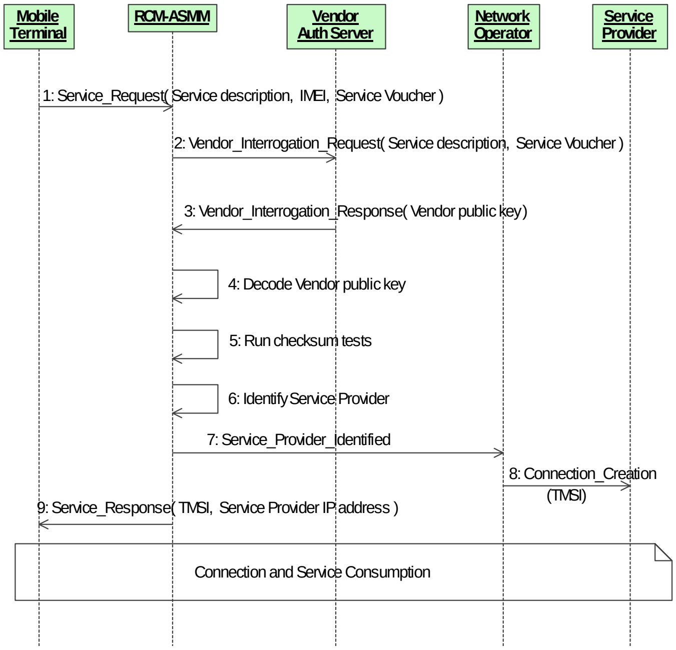

Mobile Terminal
RCM-ASMM
Vendor Auth Server
Network Operator
Service Provider
1: Service_Request(Service description, IMEI, Service Voucher)
2: Vendor_Interrogation_Request(Service description, Service Voucher)
3: Vendor_Interrogation_Response(Vendor public key)
4: Decode Vendor public key
5: Run checksum tests
6: Identify Service Provider
7: Service_Provider_Identified
8: Connection_Creation (TMSI)
9: Service_Response(TMSI, Service Provider IP address)
Connection and Service Consumption

Figure 6. Authentication procedure for software download.

CONCLUSION

Composite reconfigurable radio networks exploit the availability of diverse radio access technologies, bearing inherent capabilities to download new radio software, and to discover and select the most suitable access scheme according to spatial and temporal conditions. This article has envisaged a cohesive control, management, and O&M framework in which composite reconfigurable RANs are coupled with evolved core network architectures. The presented Reconfiguration Management Plane (RMP) comprises a network-agnostic protocol-independent model for specifying operations and notifications, with the reconfiguration plane part viewed either as an extension to existing control and management planes or as a new intermediary plane for dedicated reconfiguration-induced tasks.

From the deployment perspective, the RMP logical model is horizontally mapped to two-tier architecture. The anchor reconfiguration manager lies in the core network, in a TTP domain, or is distributed in core network elements, and addresses reconfiguration session management, secure software-download management, and policy-based context management. The radio reconfiguration support function lies within a domain of multi-RAN scope for joint radio resource management, and dynamic network planning and management. In addition, vertical distribution of reconfiguration control intelligence in the physical configurations allows local adaptations to be implemented by the visited network itself, thus yielding coordinated reconfiguration of end-user and infrastructure equipment.

The proposal of service vouchers as authentication scheme for software download alleviates complex administrative effort resulting from the use of the SIM card and exploits locality, as signaling is carried out in the roaming network alone. Reconfigurable radio environments can accommodate legacy security technologies, such as digital certificates and security standards built on top of them, provided concrete guidelines for designating the approval authority and for the definition of the target signed fields be derived, adhering to regulatory rules, market peculiarities, and business model principles.

The E^{2}R project has introduced the RMP model to research fora and pre-standards bodies such as the SDR Forum [18], the Object Management Group [21], and the TeleManagement Forum. A prototype implementation of the Reconfiguration Management Plane functionality is a major objective of E^{2}R II consortium, aiming to validate the RMP rationale and to introduce a subset of the modules to the 3GPP.

ACKNOWLEDGMENT

This work has been performed in the framework of the EU funded projects E²R and E²R II. The authors would like to acknowledge the contributions of their colleagues from E²R and E²R II consortia.

REFERENCES

[1] J. Hoffmeyer, Il-Pyung Park, M. Majmundar, and S. Blust, “Radio Software Download for Commercial Wireless Reconfigurable Devices”, *IEEE Radio Commun.*, Mar. 2004.

[2] J. Steinheider, “Field Trials of an All-Software GSM Base Station”, *RF Design*, Mar. 2004.

[3] P.Demestichas, G.Vivier, K.El-Khazen, and M.Theologou, "Evolution in Wireless Systems Management Concepts: From Composite Radio to Reconfigurability", *IEEE Commun. Mag.*, vol. 42, no. 5, May 2004.

[4] M. Dillinger, K. Madami, and N. Alonistioti, Eds., *Software Defined Radio: Architectures, Systems and Functions*, Wiley, 2003.

[5] EU IST Project E²R (End-to-End Reconfigurability), http://www.e2r.motlabs.com/

[6] SDR Forum, http://www.sdrforum.org/

[7] WWRF Working Group 6, “Reconfigurability”, http://wg6.ww-rf.org/

[8] ITU-T Rec. M.3400, “TMN Management Functions”, Feb. 2000.

[9] 3GPP TS 32.101, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Telecommunication management; Principles and high level requirements”, http://www.3gpp.org/

[10] 3GPP TS 23.002, “3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture”, http://www.3gpp.org/

[11] J. Luo, C. Niedermeier, R. Schmid, and M. Dillinger, “Network Components for Enhanced Software Download and Connection Management”, SDR Forum input doc. SDRF-2003-I-0036, Sept. 2003.

[12] S. Panagiotakis, N. Alonistioti, and L. Merakos, "An Advanced Location Information Management Scheme for Supporting Flexible Service Provisioning in Reconfigurable Mobile Networks", *IEEE Commun. Mag.*, vol. 41, no. 2, Feb. 2003.

[13] A. Koutsorodi *et al.*, “A Management Architecture for Enabling Wireless System Operation in the B3G Context and Exploitation of the ABC Concept”, *Proc. 5th Euro. Wireless Conf. Mobile and Wireless Sys. beyond 3G*, Barcelona, Spain, Feb. 2004.

[14] N. Niebert *et al.*, “Ambient Networks: an Architecture for Communication Networks beyond 3G”, *IEEE Wireless Commun.*, vol. 11, no. 2, Apr. 2004.

[15] B. Walke, R. Pabst, L. Berlemann, and D. Schultz, “Architecture Proposal for the WINNER Radio Access Network and Protocol”, *WWRF11*, Oslo, Norway, June 2004.

[16] S. Uskela, “Key Concepts for Evolution toward Beyond 3G Networks”, *IEEE Wireless Commun.*, vol. 10, no. 1, Feb. 2003.

[17] K. Moessner *et al.*, “Functional Architecture of End-to-End Reconfigurable Systems”, *Proc. IEEE 63rd VTC*, Melbourne, Australia, May 2006.

[18] Z. Boufidis, N. Alonistioti, and E. Mohyeldin, “Generic Process for Terminal Reconfiguration through Software Download”, SDR Forum input doc. SDRF-04-I-0081, Nov. 2004.

[19] R. Falk and M. Dillinger, “Approaches for Secure SDR Software Download”, *SDR Forum Tech. Conf.*, Phoenix, AZ, Nov. 2004.

[20] E. Mohyeldin, M. Dillinger, C. Niedermeier, and R. Schmid, “Advanced Mechanisms for Software Download Management”, SDR Forum input doc. SDRF-04-I-0082, Nov. 2004.

[21] N. Alonistioti, C. Anagnostopoulos, and M. Stamatelatos, “Reconfiguration Management Metamodel”, *OMG 1st Annual Software-Based Commun. Wksp.: From Mobile to Agile Communications*, Arlington, VA, Sept. 2004.