RECONFIGURATION SIGNALLING

Stoytcho Gultchev, Klaus Moessner, Rahim Tafazolli (Mobile VCE Research Team,
Centre for Communication Systems Research, University of Surrey, Guildford, UK
{K.Moessner, S.Gultchev, R.Tafazolli}@eim.surrey.ac.uk)

ABSTRACT

Roaming across different air interface standards and the necessary reconfiguration of terminals requires the download of radio implementation software. However, such download to reconfigurable SDR terminals and the management of reconfiguration sequences within such terminals requires additional signalling and security capabilities. This paper uses the Reconfiguration Management Architecture (RMA) as example and describes the sequence during a reconfiguration process as well as the triggering mechanisms to initiate reconfiguration procedures.

1. INTRODUCTION

Increasing digitisation and software definability of functions and functional modules within SDR equipment moves the complexity of radio implementations away from the hardware towards the software structures. Exactly this shift of complexity provides the opportunity for truly flexible reconfiguration of radios, in contrast to the well used classical switching between different waveforms or radio access technologies (e.g. GSM 900/1800, IS-95/AMPS and GSM1900/AMPS). Eventually, on-the-fly reconfigurability will allow and facilitate seamless roaming through the coverage areas of different radio access technologies and in the long-term, it will even support service and application specific configurations of the radio interface (providing the establishment of a suitable regulatory framework) [1].

To implement a configuration scenario in which the user may roam in vertical (within cellular systems) and horizontal directions (between different wireless technologies e.g. satellite/cellular), a number of requirements have to be met:

a) suitable reconfiguration control mechanisms need to be developed/employed,
b) the infrastructure to ensure security and adherence to radio regulation needs to be specified and developed, and
c) the means to facilitate user and terminal mobility between different systems (i.e. to support vertical roaming) will have to be provided.

Several proposals have already been brought forward defining a 'Global Connectivity Channel' to support basic connectivity for SDR terminals and also to provide an infrastructure for OTA software download. Apart from ubiquitous connectivity for SDR terminals, such a channel may also be used to inter-connect the various legacy PLMNs and therein facilitate cross-system (vertical) mobility. Beside connectivity and mobility support, such a channel may be used as transport infrastructure for the signalling between the different parts of a reconfiguration management architecture, i.e. to connect terminal and network resident control authority facilitating secure software download and controlled reconfiguration of SDR terminals.

Signalling mechanisms for software download, for the establishment of secure connections between network and reconfigurable terminals, for the support of reconfiguration control mechanisms, as well as for inter-system roaming are required. Whereby the aspects from the different Radio Access Networks (RAN) have to be considered and signalling connections between the nodes of different networks have to be defined. The following sections of this paper deal with the question how un-authorised, fraudulent, non-standard conformant and unwanted configuration and reconfiguration of a terminal can be prevented. The paper presents a set of signalling sequences and algorithms used in the MVCE Reconfiguration Management Architecture (RMA). Mechanisms and messages for establishment of a secure download and signalling connection between the different parts of the RMA are described whereby particular focus is set on the local and remote triggers for reconfiguration procedures. This includes the description of security functions necessary to authenticate the entity (user/application, network operator, etc.) which/who requests reconfiguration and to authorise or reject the reconfiguration request.

2. RECONFIGURATION CONTROL: FRAMEWORK AND MECHANISMS

Adaptation and reconfigurability to different cellular communication Radio Access Technologies (RATs) is likely to be one of the initial uses for Software Radios in the commercial sector, whilst the future may even see a move away from the current rigid frequency allocation towards a dynamic, application-specific allocation of bandwidth (with customisable QoS levels etc.). This type of reconfigurability introduces a number of challenges towards the actual process of reconfiguring the mobile terminal: A framework to support SW download and signalling scheme to facilitate the whole reconfiguration process are required. The RMA, as presented in [2] and [3], provides such a framework as well as the mechanisms necessary; it defines a distributed framework divided in three major sections: including the Configuration Control (CCP), Configuration Management (CMP) and Radio Module (RMP) parts and a set of signalling sequences to:

- To enable full or partial reconfiguration of all protocol stack layers;
- Control and monitor the configurations of network nodes;
- Control and manage reconfiguration processes at both terminal and network side.

2.1 The Architectural Framework

The RMA is a distributed framework, whereby a part of the architecture is located within the network (i.e. the 'Configuration Control Part' (CCP)), it is responsible for the coordination of the configurations of network nodes and also provides the mechanisms for the approval of anticipated terminal configurations. The tasks of the CCP include:

- reconfiguration software provision, negotiation and download,
- evaluation and approval of intended configurations, using a virtual configuration process,
- assurance of standard compliance,
- monitoring of configurations throughout the network,
- provision of configuration rules for different reconfigurable radio platforms,
- registration of the current/new configuration.

To perform these tasks, there are a number of functional modules within the CCP: the AcA-Server performs most of the aforementioned tasks, it monitors the configurations of the network neighbourhood, manages the registration of terminal configurations, handles the software download, validates new configurations and ensures the

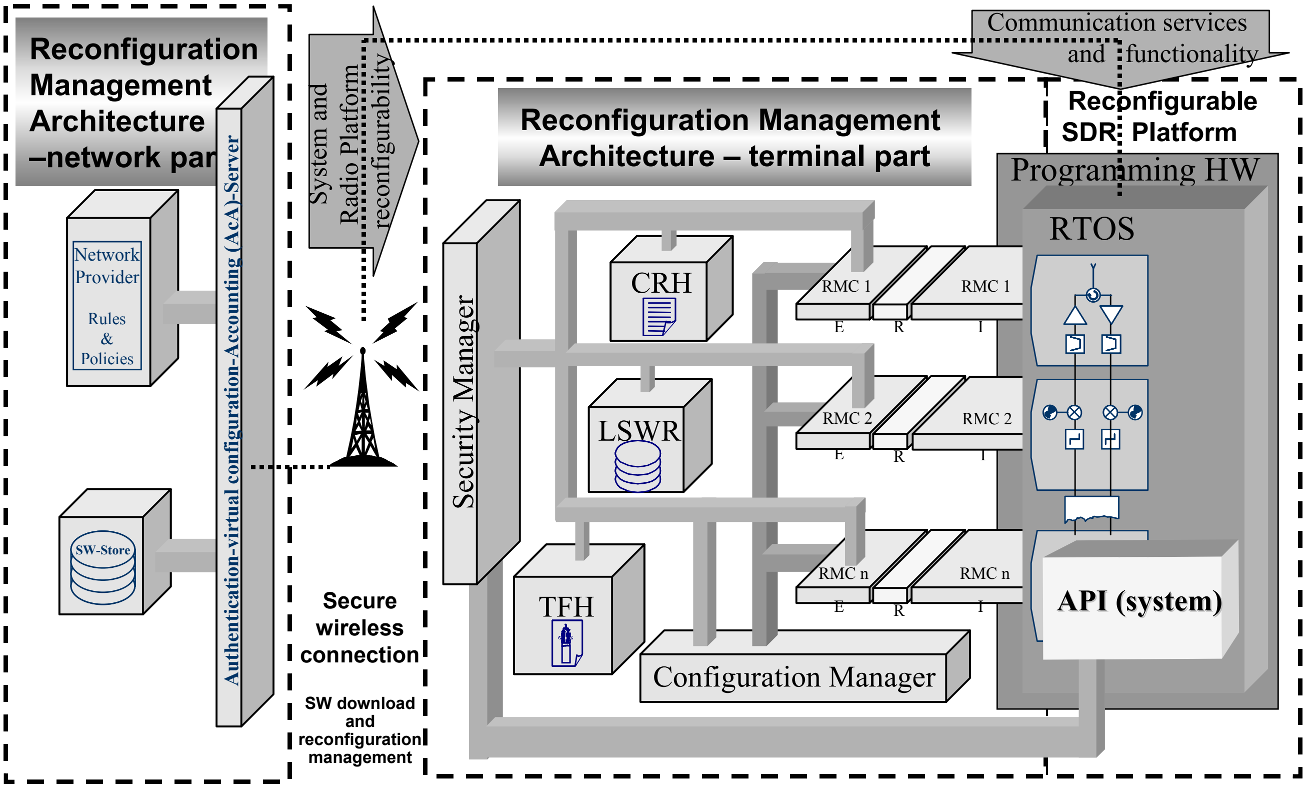
Reconfiguration Management Architecture –network par
Authentication-virtual configuration-Accounting (AcA)-Server
Network Provider Rules & Policies
SW-Store
System and Radio Platform reconfigurability
Secure wireless connection
SW download and reconfiguration management
Communication services and functionality
Reconfiguration Management Architecture – terminal part
Reconfigurable SDR Platform
Programming HW
RTOS
Security Manager
CRH
LSWR
TFH
RMC 1
E
R
RMC 1
T
RMC 2
E
R
RMC 2
T
RMC n
E
R
RMC n
T
API (system)
Configuration Manager

Fig1 RMA - reconfiguration management and control planes

adherence to given standards. The CCP may be located either within the access or even the core network. The ‘Rules&Policies’ Module is a tool to be used by the network provider to specify certain platform dependent parameters and reconfiguration policies. The ‘SW-Store’ is a database hosting approved configuration software and the terminal configuration register.

Across the air interface, the two parts within the reconfigurable terminal are the CMP, which coordinates the configuration and reconfiguration processes of the configurable RMP.

Tasks of the CMP include the procurement of configuration software, handling of configuration rules, generation and compilation of tag-files, implementation of new configurations and finally execution and control of reconfiguration related signalling. [3], [4].

The CMP contains a number of functional modules, including the ‘Configuration Manager’, which manages the communication between the modules within the CMP and also the signalling between CMP and CCP. A variable number (dynamically created) of ’Reconfiguration Management Controllers’ (RMC) acts as interfaces between the managing domain (i.e. the CMP) and the radio execution domain (i.e. the RMP). The RMCs implement the actual configuration of radio modules within the RMP (i.e. they install the software modules and establish the connections between the various objects), whilst the Configuration Manager (CM) controls and coordinates the whole of the reconfiguration process. Other modules within the CMP are a Local SoftWare Repository (LSWR) (to store radio configuration software), a Configuration Rule Handler (CRH) (this unit maintains the list of rules for reconfiguration, these rules depend on policies set by the network provider and also on the terminal type), a Tag-File Handler (TFH) (to store, interpret, generate and alter tag-files) and a Security Manager (SM) (responsible for establishment, maintenance and termination of secure connections between the different management and control units and to prevent malicious reconfiguration requests and tampering during the download of reconfiguration software). A configuration software bus, based on CORBA facilitates the transport between the modules within elements; it carries the signalling traffic between the distributed reconfiguration management and control parts. The functionality of the ‘security manager’ is required to ensure secure, trusted and authorised exchange/download of reconfiguration information and of configuration software between different parts of the architecture.

2.2 Reconfiguration Mechanisms

A reconfiguration process, in general, (i.e. reconfiguration of the RMP, controlled by the CMP) consists of three major steps that need to be completed before a terminal is able to apply its new configuration. These stages are:

- Download of rules and software – respectively CRH and LSWR;
- The creation of a tag-file (n.b. a tag-file contains the ‘blueprint’ of the terminal created by the Tag-File Handler (TFH) module);
- The validation of the intended terminal configuration by the CCP (i.e. the verification, within the network/AcA server, of the configuration described in the tag-file);

The implementation of the radio modules in the RMP is performed by the Reconfiguration Module Controllers (RMC). It relies on the SW structure (i.e. radio blueprint) defined within the tag-file..

The signalling scheme to facilitate and implement these procedures relies on support from the network, and has to provide secure transport of software-, terminal-, user-, operator-, and regulation-related reconfiguration information. Transactions take place between network support node (AcA) and terminal. The complexity of such a system requires an additional, purely reconfiguration related functional plane, in addition to the existing user-, control- and management planes (e.g. in GSM). The relationships between network and reconfigurable terminal are becoming exceedingly complex and that the need of reconfiguration control and management mechanisms with strong security enforcement is crucial.

2.3 Signalling issues for download

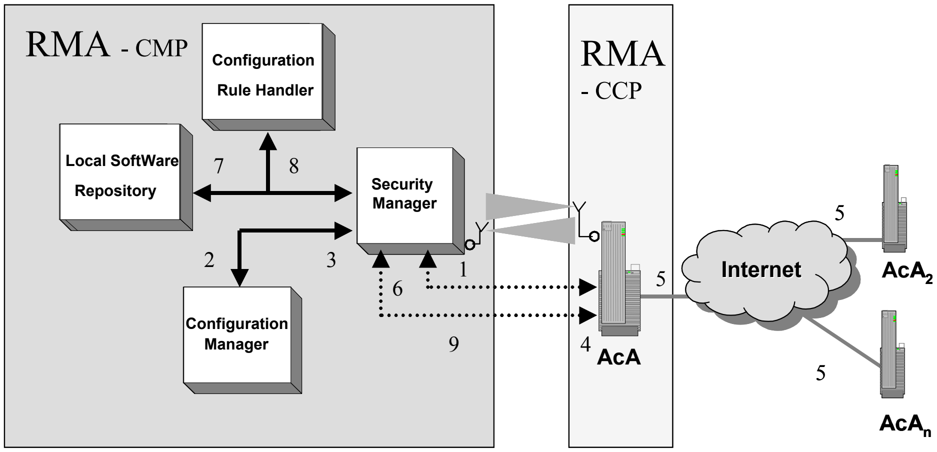

Fig 2 Reconfiguration Download Signalling

Installing a new configuration in a SDR terminal necessitates the availability of the required software. This software may be negotiated and downloaded via different channels (including dedicated traffic channels of the currently active RAT or a possible global control channel [5]).
Independent of the download channel, there are signalling requirements to be met during a download sequence (as described in [6]):

- Authorisation and authentication (i.e. in a mutual manner) and establishment of a secure connection between terminal and network fig 2 (1÷4);
- Checking the availability of the required software within the network and procurement from other sources fig 2 (5), if the SW is not locally available (in the local SW store of AcA);
- Acknowledgement and control of the download of software between network and network node - fig 2 (6) and.
- Download confirmation fig 2 (7 & 8) and termination of the secure connection fig 2 (9).

A) Establishing a secure connection

After receiving a trigger, the first step of any reconfiguration sequence is to establish a secure connection between terminal and network. Thereby, the network entity and terminal involved ensure that only authorised access to the reconfiguration management system takes place and that code downloaded and signalling messages exchanged will have not been corrupted during the download. After establishing the secure connection, the reconfiguration requesting entity (either network or terminal) requests its counterpart the details about the actual reconfiguration procedure, thereby specifying the type of the reconfiguration and providing additional details (e.g. software to be downloaded, specific directions about the flow of the reconfiguration procedure (i.e. ready modules' instructions will be supplied by the network for the installations radio part)). Due to the distributed nature and the multiple parties involved in reconfigurations, there are a number of security threats to be solved. The mechanisms provided in the RMA are capable to cope with - unauthorised interception of data, malicious modification to data, impersonation of terminal or network [5]. To meet and tackle these security threats, a number of security services are required: - confidentiality, integrity, and origin authentication. The appropriate encryption and decryption mechanisms have to be defined and a secure authentication procedure has to be performed using a scheme like PKI (Public Key Infrastructure). The PKI scheme has the advantage that it ensures secure exchange of data even if there is no prior 'security context' (i.e. assuming that all terminals and servers are equipped with an asymmetric key pair and a certificate for their public key); an additional advantage of a PKI is that there is no immediate need for on-line communications with third parties.

B) Software availability

An initial assumption for a reconfiguration process would be to have the required software module available within a software repository attached to the AcA, however if the software is not available in the repository an extended search needs to be performed querying other AcAs and their repositories and download the SW module from the remote location. If a specific software module would be required but is not available, the reconfiguration process will have to be terminated. .

C) Trigger and support for a reconfiguration procedure, SW download and termination of the secure connection

By requesting a terminal to reconfigure to another RAT, the network (i.e. the operator or an standard authority) may issue an initial trigger for reconfiguration (i.e. including all three possible reconfiguration types ranging from sub-module, module to complete reconfiguration). The procedure requires support from the terminal, which has to install the radio modules, generates the 'blueprint' (i.e. a tag-file) of the new terminal configuration (the network may also provide a tag-file for the intended configuration) as well as software and configuration standard compliance confirmation. This type of request is issued in case that the network provider made alterations or requires module updates (e.g. new software releases) or bug fixes. In case the terminal requests/triggers a reconfiguration, there are two possible procedures, which depend on the policies and security policy files used. These policy files are derived from the initial terminal (hardware) and personal/user information (i.e. the user profile), changes to policy files require the confirmation from the user. In case, the user has agreed to an 'open policy', the management entity responsible for the reconfiguration procedure becomes automatically authorised to proceed with the reconfiguration procedure without user intervention (see Fig 3). If, as second case, user affirmation is required, the management entity will dispatch a message to the user for authorisation of the intended reconfiguration.

Independent which approach is followed, once a reconfiguration is mutually authorised, the management entity (within the terminal) sends a notification message to the network and starts the actual reconfiguration sequence.
If a reconfiguration has been triggered and authorised, and the terminal has ascertained that a SW download is

required, it will use a secure connection (SC) to pursue the download.

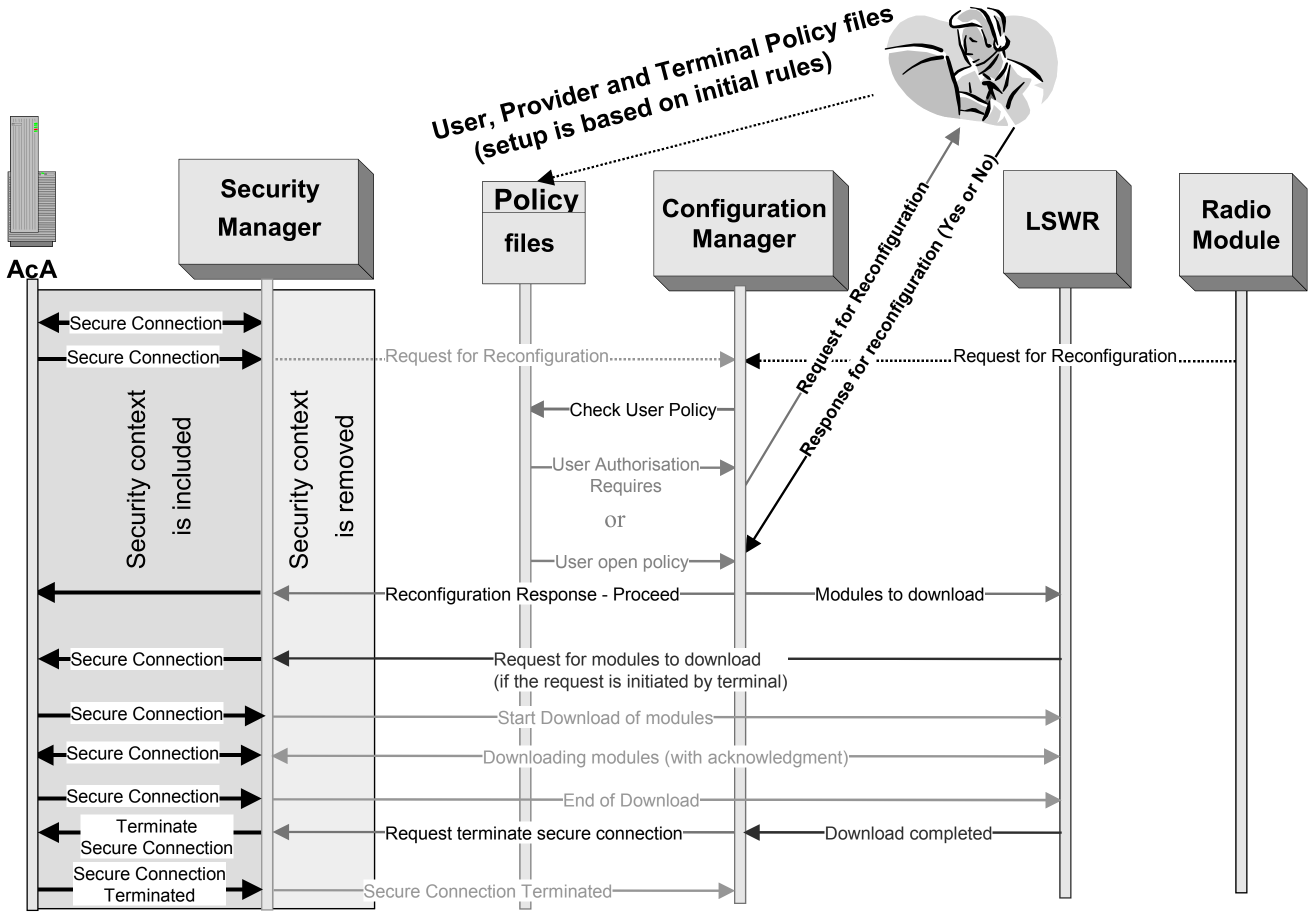
User, Provider and Terminal Policy files
(setup is based on initial rules)
AcA
Security Manager
Policy files
Configuration Manager
LSWR
Radio Module
Request for Reconfiguration
Response for reconfiguration (Yes or No)
Security context is included
Security context is removed
Secure Connection
Secure Connection
Request for Reconfiguration
Request for Reconfiguration
Check User Policy
User Authorisation Requires
or
User open policy
Reconfiguration Response - Proceed
Modules to download
Secure Connection
Request for modules to download
(if the request is initiated by terminal)
Secure Connection
Start Download of modules
Secure Connection
Downloading modules (with acknowledgment)
Secure Connection
End of Download
Terminate Secure Connection
Request terminate secure connection
Download completed
Secure Connection Terminated
Secure Connection Terminated

Fig 3 Reconfiguration signalling messages for software download in RMA

Assuming the availability of the required software (local or obtained from other repositories), the next step is to forward the module to the terminal. During the complete download, the SW module becomes wrapped with security information (i.e. this takes place within the AcA) and then forwarded to the terminal where the security context is stripped off (in the Security Manager Module). The first packet(s) (i.e. an object or piece of information) received will contain the required index data and also the size of the expected data/software to be downloaded (n.b. it would be also possible to apply an end-packet with an identifier stating the number of bytes and packets sent). After reception of the first packet(s), the remaining packets (i.e. containing the requested software entity itself) are transmitted. A download procedure continues until the final packets have arrived and the data is completely processed (i.e. un-wrapped and stored in the LSWR). In case of any loss of data, the LSWR can request the re-transmission of the missing packet(s). After completion of the download and confirmation to the management entity (the Configuration Manager Module) the secure connection becomes terminated.

3. SUMMARY

Signalling for reconfiguration sequences is a non-trivial task; there are both various threats to security as well as additional complexity. This paper aimed to outline the mechanisms necessary to perform a reconfiguration procedure; it uses the RMA as example for a reconfiguration management framework and described the signalling exchanges necessary to pursue secure and trustworthy download and reconfiguration of mobile radio equipment. Main focus has been set on the signalling messages passed between the terminal resident reconfiguration management part and the AcA server located within the network. It tries to identify the necessary reconfiguration protocols for signalling, network communication and data download.

ACKNOWLEDGEMENTS

The work reported in this paper has formed part of the Core 2 Research Programme of the Virtual Centre of Excellence in Mobile & Personal Communications, Mobile VCE, www.mobilevce.com, whose funding support, including that of EPSRC, is gratefully acknowledged. More detailed technical reports on this research are available to Industrial Members of Mobile VCE.

4. REFERENCES

[1] W. Tuttlebee (ed.), *Software Defined Radio: Enabling Technologies*, Wiley, ISBN 0470843187, 2002.

[2] N. Jefferies, et. al., *A Solution for Regulatory Issues with SDR*, XIV. General Assembly of the International Union of Radio Science, Mastricht, The Netherlands, 17-24th August 2002.

[3] S. Gultchev, et. al., *Securing Reconfigurable Terminals-mechanisms and protocols*, 13th International Symposium on Personal, Indoor and Mobile Communication, Lisboa, Portugal, 15-18th September 2002.

[4] S. Gultchev, et. al., *Management and Control of Reconfiguration Procedures in Software Radio Terminals.* 2nd Karlsruhe Workshop on Software Radios, Karlsruhe, Germany, 20-21 March 2002.

[5] K. Moessner, et. al., *Software Download Enabling Terminal Reconfigurability*, Annales des telecommunications, 57, no.5-6, 2002.

[6] M. Cummings, et. al., *MMITS Standard Focusses On APIs And Download Features*, Wireless Systems Design, April 1998.