THE RESPONSIBILITY CHAIN CONCEPT

Klaus Moessner[1], Didier Bourse[2], Karim El-Khazen[2], David Grandblaise[2]
[1] *CCSR, The University of Surrey, Guildford, UK*
[2] *Motorola Labs, ECR, France*
k.moessner@surrey.ac.uk, {didier.bourse, karim, david.grandblaise}@motorola.com

Abstract

Reconfigurability introduces, together with all the flexibility it provides, also the problem of having to ensure that each of the reconfigurable elements has been configured in a way which does not interfere with the overall system/application environment. This paper outlines and initially describes the concept of building a 'responsibility chain' in which each of the players involved can be made accountable for any misbehaviour a failed configuration can cause. The paper explains the concept and its applicability to the Spectrum sharing scenarios developed in E²R project.

Keywords: Reconfiguration Policies, Responsibility, Regulation, Efficient Spectrum Usage.

1. INTRODUCTION

The possibility that equipment may be configured to practically any setting and may potentially implement any radio interface (a RAT standard or a rogue scheme), opens way for any type of intended as well as unintended faulty system implementation.

Reconfigurable terminals in particular, are easily circulated, thus they may appear in administrative areas where regulation or law prohibits the use of a reconfiguration capability or, in very strict cases, even the mere possession of such equipment. The problem of how to stop the unintentional incrimination of users arises.

The capabilities of reconfigurable terminals will facilitate cross air interface technology roaming, the ability to adapt to any (legacy and public standard) air interface available and to download and install new system software in both the home but also when being in the foreign environment. The question of "what happens when a user wants to install software, obtained from a third party provider, on their terminal, which should operate in the network of another operator" can become a question of 'does the user act as a criminal when doing the reconfiguration or is he still within the rules'.

Furthermore, with a focus on security, mechanisms are required to verify the source of system program code, and this has to happen well before a piece of system software becomes integrated into a reconfigurable device. Regarding reliability, techniques, mechanisms and procedures are needed to ensure that a reconfiguration action will not be able to make a running system stop working correctly. This means that some entity has to validate any configuration before it may go 'live'. This means that mechanisms for validation, fault diagnosing as well as error recovery procedures have to be in place.

In particular when reconfiguring in heterogeneous environments, when reconfigurability aims to support the increased efficient use of the radio resources, the question of responsibility gains particular importance. The implications of end-to-end reconfigurability [1], in spectrum sharing scenarios can range from very positive (i.e. efficiency) to rather negative (distortion of the radio environment due to misconfigurations).

One of the key questions, which the responsibility chain concept aims to answer, lies in the accountability for fault free functioning of reconfigurable equipment when reconfigured in (foreign) environments or (foreign) administrative domains.

2. THE RESPONSIBILITY CHAIN

In the past, the responsibilities for equipment in the mobile arena were clearly distributed; equipment was manufactured implementing all layers according to the given standards, it was verified through an independent type approval process in test houses and the configurations could not, or only in a long lasting and tedious procedure, be changed. With introduction of the R&TTE directive [2], the scheme evolved, and now even manufacturers can approve, or certify that their equipment complies with the relevant standards. Again, responsibilities in this case were rather clear; they and the liability were shifted to the manufacturer. For reconfigurable equipment however, this becomes even more of a problem, as the three radio regions also follow different approaches to the problem [3].

Assuming an indicative End-to-End Reconfigurable system, and focusing on the administrative roles of its actors [4], such situation is depicted in Figure 1. Following introduction of the problem of responsibility assignment, this figure shows, in the context of an end-to end-system, the main points of interference identifying where actors would have to take responsibility for the system state. There are a number of sensitive areas (indicated by the stars in the figure) in a reconfiguration procedure. *Problematic issue 1* highlights the question of the actor who takes the responsibility for third party software and who vouches that such software can be used to implement a radio protocol on the platform built by a specific manufacturer. *Problematic issues 2* and *3* tackle the same situation but in these cases the software would be provided by the equipment

manufacturer or operator, respectively, and the configurations would be used in a different administrative domain. *Problematic issue 4* tackles the matter about permitting (reconfigured) terminals to access/use an operator's Radio Access Technology (RAT), while *Problematic issue 5* deals with the biggest problem of who can (and will) take the responsibility if a terminal is being

Main assumption in this model is that regulation defines for the RATs the policies and the limits that are to be applied in defined geographical area and timeframe. The second assumption is that equipment can not be altered without consent from the controller of the reconfiguration space (as depicted in Figure 1).

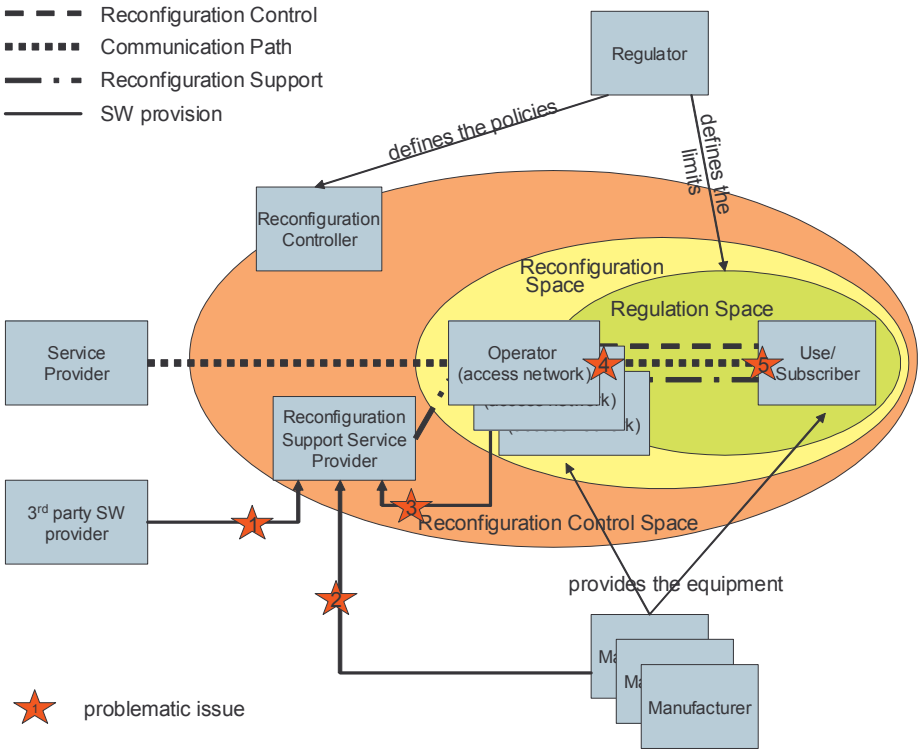

Figure 1: Actors of the Administrative Dimension and their Involvement

reconfigured. *Problematic issues 4* and *5* include the prevention of misuse of spectrum (e.g. in the Cognitive Radio Approach, when a user does not release the spectrum) as well as the spectrum control.

To tackle these problems, a clear understanding of the relationships between the actors in end-to-end reconfigurable environment has to be established. The introduced responsibility chain concept will provide an overview of the different responsibilities and aim to show their relationships. This chain will also be related to the value chain of mobile telecoms, with the aim to outline possible approaches for the assignment of responsibilities in reconfigurable radio systems. The responsibility chain defines a model where the accountability for reconfigurations can be assigned to the different actors within end-to-end reconfigurable systems. Connected to the concept of value chain in the definition of the business models for end-to-end reconfigurable systems, the responsibility chain will identify the dynamic interactions between actors encompassing information data, control data and money flow. Moreover, the money flow of the responsibility chain will include the penalty payments to recover damages created by faulty reconfiguration.

3. RESPONSIBILITY AND SPECTRUM SHARING

E^{2}R considers the concept of the responsibility chain as affecting the complete stack as well as all actors that are involved in the different reconfiguration/spectrum sharing scenarios. Looking into the Flexible Spectrum Playground. Four main E^{2}R spectrum scenarios have been identified:

- Scenario # 1 *"Spectrum Sharing between Heterogeneous Systems*" and Scenario # 2 *"Spectrum Pooling for Time Varying Hot Spot Location"* deal both with Flexible Spectrum Management (FSM) but from two different perspectives. For these both scenarios, there is no Joint Radio Resource Management (JRRM), i.e. the inter-system handover is not allowed,
- Scenario #3 *"Joint Radio Resources Management in Heterogeneous Systems"* considers JRRM (inter-system handover is enabled) but without FSM,
- Scenario #4 *"Dynamic Network Reconfiguration Facilitating Spatial-Temporal Traffic Changes"* includes both JRRM and FSM capabilities. This scenario is the combination of Scenario #1 and #3,
- A reference scenario has been defined as a basic scenario with which the scenarios from #1 to #4 are compared.

Depending on the scenario, one or several services can be delivered by a same radio access technology (services delivery flexibility), or a Dynamic Network Planning and Management (DNPM) capability is enabled in support of the FSM or JRRM functionalities.

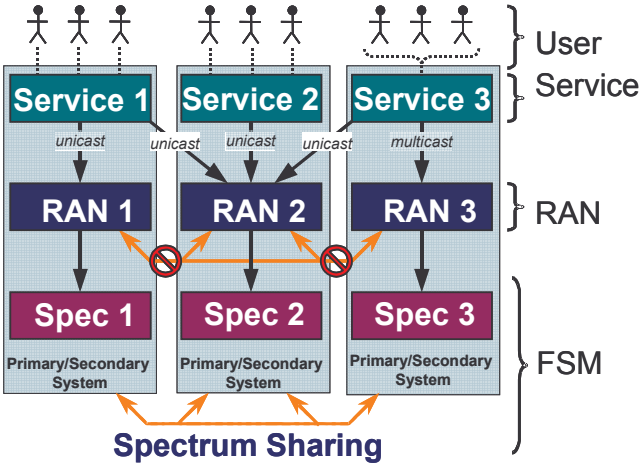

Figure 2: Scenario #1 description

As example, in scenario #1 (see Figure 2), each radio access technology can potentially deliver more than one service ("services delivery flexibility" functionality can be enabled), and the underlying support of the radio network management is considered ("DNPM" functionality is enabled) within the spectrum sharing management.

Taking this simple scene as example, the responsibility problem becomes more apparent; a service can be provided via different underlying transport mechanisms (i.e. radio access technologies), yet those will be chosen to facilitate the most efficient use of the spectrum these three RATs had been given.

This means, equipment may be reconfigured to use service 1 by accessing RAN 2 (rather than RAN1). If however, some part of the reconfiguration procedure should fail, the gains anticipated (i.e. spectrum efficiency gain) may not materialize or even result in efficiency losses.

4. CONCLUSION

Reconfigurability potentially offers, not only flexibility and adaptability, but it also provides the potential to support technologies like dynamic or flexible spectrum assignment, hence the prospective for considerable gains in spectrum efficiency. However, if the configurations necessary to implement the FSA assignment fail, considerable system distortions may occur. The responsibility concept described provides a framework in which, for each different source of failure, the responsibility can be assigned to one of the actors involved, thus making someone accountable for failures of reconfigurations.

REFERENCES

[1] IST-2003-507995 FP6 Project E²R, http://www.e2r.motlabs.com

[2] R&TTE Directive, http://europa.eu.int/comm/enterprise/rtte/

[3] Walter Tuttlebee, "Software Defined Radio: Origins, Drivers and International Perspectives", Wiley, March 2002

[4] S. Hope, F. Marx, M. Arndt, A. Delautre, E. Buracchini, P. Goria, A. Trogolo, M. Stamatelatos, N. Alonistioti, A. Kaloxylos, G. Vivier, K. El-Khazen, M. Alvarez, "End-to-End Reconfigurability System Scenarios", Wireless World Research Forum, June 2004