Wireless World Research Forum
(WWRF)

Concept of the Responsibility Chain in an End-to-End Reconfigurable Framework

Klaus Moessner, Didier Bourse, Karim El-Khazen, David Grandblaise

***Abstract*— Together with reconfigurability comes the problem of 'what happens if any intended configuration goes wrong?'. This paper introduces the concept of the responsibility chain in end to end reconfigurable systems; it outlines the relationships between the different actors in reconfigurable environments and defines how the responsibilities between them are distributed. The aim of the approach is to clearly define which actor is liable if a reconfiguration causes system failure or other system inconsistencies/disturbances. Eventually a scheme will be developed to enforce regulation in reconfigurable systems and to penalize possible violations.**

***Index Terms*— Actors in reconfigurable environments, responsibility distribution, failure liability.**

Introduction

THE feature that equipment may be set to theoretically any configuration and may, at least potentially, implement any radio interface (a RAT standard or a rogue scheme), opens the path for both intended as well as unintended non-conformant system implementation.

Reconfigurable terminals in particular, can be easily circulated, thus they may appear in global 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 prevent 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 while being in a foreign environment. Questions like "what happens if 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'.

With a focus on security, mechanisms to verify the source of system program code are required. The verification of where a piece of system software comes from has to happen well before the software becomes integrated into a reconfigurable device. Regarding reliability, techniques, mechanisms and procedures are needed to ensure that a reconfiguration action will not stop a correctly working system and will not replace the current settings with a non-operational configuration. This means that any configuration has to be validated before it may be used. Mechanisms for validation, fault diagnosis as well as error recovery procedures have to be put in place.

In particular reconfigurations in heterogeneous environments, when the reconfiguration capability is being exploited increase the efficiency of use of the radio resources, the question of 'who is responsible' gains particular importance. The implications of end-to-end reconfigurability [1], in spectrum sharing scenarios can range from increased spectral efficiency to distortion of the radio environment due to mis-configurations.

The key question, which the responsibility chain concept aims to answer, concerns the accountability for the functioning of reconfigurable equipment, in particular when equipment becomes reconfigured in (foreign) environments or (foreign) administrative domains. The question of 'who (i.e. which actor) will be accountable for what' needs to be answered.

Reconfigurable Systems and their Players and Actors

Reconfigurability opens the possibility for third party software vendors to provide high-level as well as low level system software. It also allows different actors to trigger changes, like upgrades, to the HW/SW combination of the equipment, even after the equipment has entered the market. In such scenarios, the assignment of responsibility becomes quite crucial.

The settings and software combinations of equipment, already for non-reconfigurable technologies, are rather complex. The manufacturer installs the firmware, operating system and basic applications while the operator may include some tailored platform software and applications. All of these installations may be correct or they may have bugs which potentially require patching. While this, in recent terminals can be done, to a certain extend, rather easily, such patching will become rather problematic when system configuration software may be procured and installed even from/by third parties.

Much of the flexibility and the value that is added through reconfigurability are based on software download and controlled installation/ activation. This however relies on sufficiently secure mechanisms for download and trust into origin, download path, suitability and authenticity of the software.

For operators there are two main problem areas; in case reconfigurations cause any problems, the operator will be the main point of contact (and blame) for the user, thus failed reconfigurations can potentially harm the operators reputation. The second problem is in the efficiency of use of an operators’ spectrum. Reconfigurations may lead to inefficiencies or misuses and consequently resulting in revenue loss. There may be many other potential problems, yet the shared theme of all problems identified is the need for a common scheme to assign the responsibilities for reconfiguration.

As aforementioned, there are many actors involved in reconfiguration procedures, and their interests and dealings may be rather complex; these actors, their tasks and their relations need to be identified and the roles they play in reconfiguration processes needs to be evaluated.

A distinction of two dimensions in which actors may operate can be made: the first being the operational and the second the administrative dimension. In E^2R [1], fifteen actors have been identified for end-to-end reconfigurable systems [2]: User, subscriber, network operator, equipment manufacturer, (value-added) service provider, content provider, software provider, service aggregator, regulator, reconfigurable equipment, reconfiguration manager, certification entity, security entity, pilot channel provider and spectrum manager.

Focusing on some of these actors, their roles in the operational dimension include:

- Equipment Manufacturer: provides the reconfigurable platform, firmware and software updates/new versions,
- Network Operator: owns the spectrum as well as the infrastructure, can also act as service provider,
- Software Provider: third party providing application software, but also low level configuration relevant software,
- Service Provider: provides the required/requested services, this may also imply the possibility that an end user may act as service provider,
- Reconfiguration Support Service Provider (e.g. Reconfiguration Manager): provides the basic services necessary for reconfiguration, including for example secure software download,
- User/Subscriber: uses the equipment and infrastructure, may request installation of new configuration of application software.

While in the administrative dimension, the same actors may assume different roles:

- Regulator: sets the framework for use of reconfigurable equipment, allocates the spectrum to lease holders and governs (using policies) the usage of the spectrum and the circulation of reconfigurable equipment,

- Reconfiguration Controller (e.g. Certification Entity, Security Entity, Spectrum Manager): verifies that intended reconfigurations will comply with given standard or that the equipment is prevented from implementing an intended configuration. This controller also implements functions like spectrum management according to given policies and certifies the intended configurations of the reconfigurable equipment,
- Equipment Manufacturer: arranges and initiates (performs) software (firmware) updates and patch installation,
- Software Provider: provides third party system, protocol and application software,
- Service Provider: may request the reconfiguration of equipments to enable the provision of its services,
- Reconfiguration Support Service Provider (e.g. Reconfiguration Manager): provides the control and security features for the reconfiguration procedure, independent of who may have initiated the reconfiguration process,
- Network Operator: provides the radio resources, mobility management and fixed capabilities to switch, route and handle the traffic associated with the services offered to users,
- User/Subscriber: may initiate, allow or decline a reconfiguration.

The Responsibility Chain Concept

Looking into a complete end-to-end reconfigurable system, and focusing on the administrative roles of the various actors involved (see figure 1). The figure outlines, in the context of the end-to end-system, the main points of where actors (and their activities) may interfere with the system functions and where they will have to take responsibility for the system state.

There are a number of rather sensitive areas (indicated by the stars in the figure) that may be affected during a reconfiguration procedure.

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.

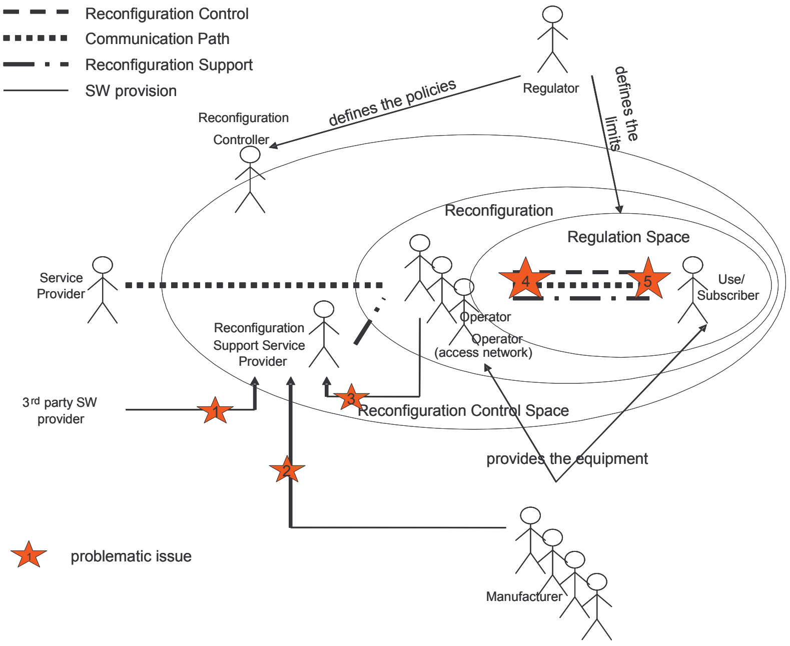

Figure 1: Actors in End-to-End reconfigurable Systems

Issues 2 and **Issue 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.

Issue 4 tackles the matter about permitting (reconfigured) terminals to access/use an operator's Radio Access Technology (RAT).

Issue 5 deals with the problem of who can (and will) take the responsibility if a terminal is being reconfigured.

Issues 4 and 5 include the prevention of misuse of spectrum (e.g. in the Cognitive Radio Approach, when a user does not releases the spectrum) as well as the spectrum control.

To approach these problems, the relationships between the actors in end-to-end reconfigurable environment have to be defined and established.

The responsibility chain concept provides an initial overview of the different responsibilities and aims to do this definition of these relationships. The chain needs also be connected to the value chain of mobile telecoms, with the aim to outline possible sanctions if the assigned responsibilities are violated. 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 need to identify the dynamic interactions between actors encompassing information data, control data and money flow and will need to define a penalty scheme to penalize violations or infringements with actors rights as result of reconfiguration procedures.

Conclusions

Questions regarding the actors' responsibilities in an end-to-end reconfigurable environment arise when addressing security, reliability and privacy issues. In order to ensure compliance and fault-free functioning of reconfigurable equipments in this heterogeneous environment, it is necessary to clearly describe the chain and relations of the actors involved in reconfiguration, identifying the possible threats and associated responsibilities.

Taking the responsibility for reconfiguration of radio equipment may appear to be a burden, but it also opens new commercial possibilities. The classical communications value chain remains being in place, but, on top of this, a scheme to charge for violations of reconfiguration policies is being introduced. The responsibility chain enables the provisioning of security and reliability in the reconfiguration procedures, which is of crucial importance in order for end-to-end reconfigurability technology to gain market acceptance.

ACKNOWLEDGMENT

This work is being performed in the framework of the EU funded project E^{2}R. The authors would like to acknowledge the contributions of their colleagues from E^{2}R consortium.

REFERENCES

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

[2] Walter Tuttlebee, “Software Defined Radio: Origins, Drivers and International Perspectives”, Wiley, March 2002

[3] 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

AUTHORS

Klaus Moessner, CCSR, The University of Surrey, Guildford, United Kingdom.

Didier Bourse, Karim El-Khazen, David Grandblaise, European Communications Research Lab (ECRL), Paris, France.