

Brief description of the SCOUT project, its objective and its organization structure

The SCOUT project is affiliated to the IST action line IV.5.1 “Reconfigurable radio systems & networks”. It supports the priorities for the workprogramme 2001 and the key goals of this action line and will actively contribute to the concertation and cluster activities in the “reconfigurability” cluster.

Project results from TRUST, BRAIN and MIND will be one of the key sources, but also findings from the projects in the “reconfigurability” cluster will be incorporated. Further, current outcomes of the WWRF, ITU-R WP8F, 3GPP, IETF and SDR-F will play a major role to advance the state-of-the art in this IST action line IV.5.1.

The findings in SCOUT will improve natural and personalized interactions with applications and services, which will be offered by reconfigurable user equipment. This includes multimodal interaction systems that are adaptable to the user’s preferences and lifestyle. But also the operator needs and regulatory requirements will have an impact on the adaptation process in reconfigurable terminals.

Reconfigurable equipment will foster the development and convergence of networking infrastructures and architectures based on IP transport mechanisms. The second pillar in SCOUT is to provide the basis in access and backbone systems supporting reconfigurable terminals in the reconfiguration process.

Key goals of the development within SCOUT will be the definition of open architectures providing service and mode adaptation across heterogeneous wireless networks. Aspects of particular relevance are those related to self-adaptation to traffic load and characteristics, including multi-streaming, dynamic bandwidth allocation, and spectrum sharing.

Following are the main objectives of the SCOUT project:

- Achievement of accurate SDR vision from user/operator/regulator points of view
- Definition of potential system architecture supporting terminal re-configuration
- Definition of networks protocols and procedures for terminal re-configuration in hierarchical and decentralised networks. Interactions with IETF
- Progress in research on enabling technologies and definition of solutions for the main bottlenecks,
- Validation of concepts and demonstration of services.
- Disseminating the results

Sixteen partners including manufacturers, network provider, regulatory, universities and research and development companies are contributing to this project.

The SCOUT project is structured into 5 workpackages, where 3 of them work technically (WP2, WP3 and WP4). WP1 is the project management and WP5 organises the dissemination activities. Following describes the activity area of these workpackages:

WP2 (Vision on Reconfigurability for User, Operator and Regulator):

The introduction of reconfigurable terminals will increase the flexibility of the development and applications of adaptive user profiles. The following objectives are defined to tackle this challenge: To develop and validate algorithmic and theoretical framework for adaptive user profiles based on the user, operator and regulator requirements; to investigate user interactions on user profile and eventually on the behaviour of the reconfigurable terminal; to refine user, operator and regulator requirements in cellular and ad-hoc networks; to investigate new business models with reconfigurable equipment.

WP3 (Terminal Reconfiguration Management):

Terminal-centric procedures interacting with the network must take into account: The interface between wireless middleware services as broker- or trading service to support P2P applications and reconfiguration; to develop spontaneous interworking between software modules needed for reconfiguration; to define procedures for managing the downloaded software on reconfigurable terminals; to define and demonstrate flexible transceiver front-end for reconfigurable terminals.

WP4 (Architectures and Radio Resource Management in All-IP Networks Supporting Reconfigurable Terminals):

Reconfigurable terminals and their local procedures must be supported by new network architectures and functions. Reconfiguration concepts will be validated by hardware and software.

List of Security threat for the reconfigurable systems

The possibility to reconfigure mobile equipment introduces also new threats as – without suitable protection mechanisms – the reconfigurable equipment could be reconfigured in undesirable ways. Therefore it has to be ensured that only desired reconfigurations can in fact take place, as the operation of a communication system relies on reconfiguration.

Reconfiguration allows changing the properties of communication equipment that have previously been fixed by their mere design. This improved flexibility poses the threat that changes are made to the

configuration of communication equipment that contradict the interests and expectation of end users, network operators and service providers, equipment manufacturers and regulatory authorities. The overall objective is to provide a reliable service that fulfils the expectations of all involved stakeholders.

The following reconfiguration-specific security threats could occur by accident or by intention. They motivate the need to investigate and understand the security issues involved with reconfiguration and to derive the security objectives and to develop suitable protection mechanisms.

- ◆ *Download and Execution of Malicious Software*
Software download is a key technology for reconfiguration. It poses the threat that malicious software is downloaded that causes harm by accident or by intention. The software could simply not work properly or not implement the expected functionality and thereby pose a threat to reliability and availability, but it could as well implement malicious functionality as for example dialling premium rate numbers in the background, launching denial of service attacks on specific web sites or telephone numbers or any other of the threats described below.
- ◆ *Modification of Other Functionality*
The purpose of a reconfiguration is to modify certain properties or functions of reconfigurable equipment. Other functionality not intended or authorized to be reconfigured could be affected by a reconfiguration.
- ◆ *Circumvention of Security Functions*
Security functions, for example for secure network access to a cellular system or an Intranet or for m-commerce, have to be trustworthy themselves, but rely furthermore on secure storage of and protected access to cryptographic material and policy information. Unprotected reconfiguration could help to circumvent security functions not related to reconfiguration and thereby make them useless.
- ◆ *Easier Attacks*
Reconfiguration could also make attacks against the wireless communication system easier and bring it in the range of a greater base of potential attackers. Attackers do not have to rely anymore on expensive equipment as signal generators or spectrum and protocol analysers, or have to build own special equipment involving e.g. reverse engineering and modification of proprietary, highly integrated devices. Instead they get easy access to open interfaces and could simply reconfigure off-the-shelf equipment according to their intentions.
- ◆ *Invalidation of Regulatory Requirements*
Regulatory bodies pose requirements on radio equipment concerning user safety, electromagnetic compatibility (EMC immunity), and radio spectrum use (EMC emission). Conformance with these requirements can either be tested by an authorized testing house or by self-approval using a declaration of conformity by the manufacturer. Reconfiguration poses the threat that radio equipment may be brought into market where properties required from a regulatory perspective are violated during the operation of the equipment.
- ◆ *User Safety*
Reconfiguration of radio equipment could, when the hardware allows, even endanger the health and safety of the user, for example when radiated power is too high.
- ◆ *Disturbing Other Users or Other Radio Systems*
Reconfiguration could lead to emissions that harm other users and radio systems. Besides emitting in wrong frequency bands, using too high power, or wrong modulation schemes, also access to the radio medium could be modified in ways that have a negative impact on other users. As a single user or a small set of users could have an advantage in using “improved” configurations that do implement unfair behaviour, this threat shows that the user cannot given full control over his reconfigurable equipment. This threat is obviously related to regulatory requirements, but its scope is broader than regulatory compliance as certain properties could be required by operators or non-regulatory standards who want to use their spectrum efficiently and provide good service to all customers.
- ◆ *Disregard of Preferences*
Communication services could be used that do not match the preferences and expectations of the end user concerning available services, provided quality of service, and the involved cost. Also the preferences of service providers and network operators could be disregarded. As the

intentions and preferences of users, different network operators and service providers could contradict, this point is not easy to solve. An examples for possibly contradicting preferences is the selection of the radio access technology and network. While a user would probably prefer the cheapest technology that suits his service requirements, operators have obviously an interest in the usage of the most profitable service and network and especially that a service and network offered by themselves and not by a competitor is used.

- ◆ *Manipulated Reconfiguration*
The reconfiguration of terminal equipment will be supported by functions in the network, for example to assist mode monitoring or the mode switching decision. The reconfiguration process will be distributed between several entities in the fixed part and the mobile part of the communication system. Information used or even required for the reconfiguration or any other information exchanged between the involved nodes can be manipulated and therefore the reconfiguration process could be influenced in illegitimate ways..
- ◆ *Unreliable Operation*
Unstable, non-working configuration. A configuration is activated that does not work at all or not properly. The consequence would be unsatisfied users, and high costs for customer care for the service provider. Unavailability of required reconfiguration services; software
- ◆ *Protection of Intellectual Property*
Both hardware and software manufacturers have an intention to protect their development effort and to receive a fair compensation. Reconfiguration could make reverse engineering easier, and software could be used or copied illegally. When the user or the service provider can freely add desired features, differentiation of products by supported features will not work in the same way as for current equipment.
- ◆ *Illegitimate Access to Private Information*
Sensitive information is required for the reconfiguration. Access to information about the preferences, used services, or the current location and configuration has be controlled to protect the private sphere of a user. But also information related to a service provider or a network provider can be required to be kept confidential when the involved companies do not want to share data about their customers or network internals with competitors.