About this document

This document constitutes the result of research conducted by WG6 members of WWRF, with respect to Network Architecture and Support Services for Reconfigurability.

Network Architecture and Support Services for Reconfigurability

Joint Editor Group:

Markus Dillinger, Siemens GE, Germany

Panagiotis Demestichas, University of Piraeus, Greece

Nikolas Olaziregi, King's College London, UK

George Dimitrakopoulos, University of Piraeus, Greece

Nancy Alonistioti, University of Athens, Greece

Abstract:

Reconfigurable technologies enable efficient access management for terminals, in addition to flexibility in operating the radio network. Reconfigurability is expected to realize the main requirements for adaptability in 4G systems, where a significant advance is the expectation of improved capabilities. Such capabilities include support for smaller cells, self-planning dynamic topologies, full integration with IP, more flexible use of the spectrum and other resources, as well as user location-dependent usage. In this white paper, an End-to-End Reconfiguration system architecture is presented, detailing the reconfiguration management plane that implements protocols and mechanisms supporting efficient context, policy and profile management, service provisioning, software download, secure reconfiguration, and dynamic network planning. Specific mechanisms such as one-to-many software download facilitators are also introduced.

LIST OF FIGURES

1. Introduction

Software Defined Radio (SDR) has recently been the subject of much research activity within industrial consortia and publicly funded projects. The work presented in this paper has been partly carried out within the IST End-to-End Reconfigurability (E^2R) [1] project, motivated by results from the SDR Forum [2], in addition to those of the IST TRUST [3] and IST SCOUT [4] projects. In particular, under the perspective of TRUST and SCOUT, SDR is not restricted to terminal but also takes network aspects into account. An overview over SDR from a technical, market and regulatory perspective is given in [5] and [6].

Today's state-of-the-art multi-band terminals usually consist of several dedicated transceivers (i.e. hardware components restricted to a single radio access technology), and a general purpose processor that runs higher level functions such as applications and graphics/sound etc. The usage of various TDMA and CDMA technologies in different regions of the world leads to a fragmentation of the global market for mobile devices, thus making it difficult for equipment manufacturers to leverage the economy of scale expected from the growing global market for their products. SDR terminals, with generic transceivers that can be reconfigured to different radio standards through software, promise to allow such economy of scale thus to reduce manufacturing costs for terminals as a common platform for all kinds of radio access technologies.

The development of configurable hardware devices and fast DSPs for digital base-band processing has already begun (see [7], for example). However, the full exploitation of the possible benefits of the SDR concept requires far more than shier processing power in terminals. In order to allow for maximum flexibility, terminals should be able to download new radio-software via the mobile network. Through this downloaded software, the terminal can be reconfigured to new radio access technologies that have not been considered by the manufacturer. Moreover, bug fixes to software can be delivered quickly, thus minimising the effects of known bugs on the operation of the terminal and the network. Unfortunately, such software download requires a sophisticated network infrastructure to be performed efficiently and securely; furthermore, there will be a gradual evolution towards SDR terminals from today's devices.

Key requirements for network infrastructure should be identified through use-cases [8]. Terminal reconfiguration affects a wide range of network entities, protocol layers and operational schemes. Among the different management aspects for reconfiguration, we consider the following important cases which cover the essential network support required for terminal reconfiguration: Software Download Management, Profile Management, Connection Management, and Programmable Network Element Management. Related work has already been carried out in IST-FP5 projects (e.g. TRUST, SCOUT, and MOBIVAS [9]), which serves as basis for the research of E^2R.

The delivery of seamless mobile multimedia services, enabled by the interoperation of heterogeneous radio access networks, poses new requirements and invokes new challenges in radio network planning. Inevitably, the concise definition, development, and integration of novel methods and mechanisms for network planning and deployment in a reconfigurability context are vital. Operators should coordinate their heterogeneous wireless access systems, a process which could materialise through agreements to absorb traffic from other networks with predefined coupling structures. This would assist in the handling of changing circumstances (e.g., hot-spots, traffic demand alterations, etc.), or service management requests.

The support of advanced services requires the engagement of additional management intelligence and associated modules, for the realisation of a Management Plane spanning all layers. Moreover, the support of application and service adaptation, in conjunction to network reconfiguration, is very important.

Taking Software Download as example, scenarios can be classified into either Terminal-Initiated Software Downloads, Mass Upgrade Software Downloads, or Delayed/Rejected Software Upgrades. These three key classes of software downloads require functional components to be defined in networks, such as reconfiguration managers at different hierarchy levels.

Network planning is considered an important research working area, offering challenges for detailed Radio Resource Management (RRM), including parameter fine-tuning. The essential inputs to network planning consist of propagation modelling, traffic modelling, traffic forecasting and RRM performance modelling. A number of IST projects have considered network planning for particular RATs, in the sphere of geographical deployments and multimedia services offering [10][11][12][13]. In the reconfiguration environment, the optimisation of radio resource deployment through cost-effective RAT selection, with different coupling structures and traffic splitting policies [14], is presently under investigation within the IST E^2R project.

1.1. SYSTEM ARCHITECTURES SUPPORTING RECONFIGURABILITY

The system architecture providing reconfigurability incorporates the concept of a Reconfiguration Management Plane (RMP), interacting with users, services, networks, and terminals. This enables reconfiguration signalling between Reconfigurable Equipment and Reconfiguration Managers in the network, providing interworking with the legacy planes (i.e. Control, User, and Operation, Administration and Maintenance (OAM) planes) by means of Reconfiguration Supporting Functions (RSFs).

Currently, this system architecture is bringing together the evolution of cellular radio access networks, IP-based mobile networks (e.g., network reconfiguration functions/proxies), and network planning concepts, yielding network functions which are able to support reconfigurable entities, and potential architectures for appropriate network deployment. It describes a functional split between multi-standard reconfigurable entities and other network nodes and signalling concepts for network reconfiguration, developed for optimising the inter-working of coupled networks and reconfigurable terminals, capable of simultaneous connections both on the uplink and downlink (adaptive radio multi-homing). As a result, concepts for optimal traffic splitting amongst the involved access networks (i.e. UMTS, WLAN, DVB) are anticipated.

Emerging networks, equipped with scalable and reconfigurable network elements, should be capable of optimally allocating resources to radio links, for cost effective network management. This implies the following objectives:-

- Definition of reconfiguration architecture and dynamic network management mechanisms, with the required levels of network interworking/coupling.
- Creation of functional elements supporting software download, service calibration, profile management, and connection management.
- Specification of an operational interface between mobile industry players, including regulators, service provider, operators, manufactures, and end users.
- Infrastructure sharing, as can be assisted by network reconfigurability.
- Functional partitioning, supporting dynamic network management.
- Fault tolerance and reversible processes.
- Solutions for secure software download and reconfiguration service provisioning
- Mobility management in the software download process.

1.2. RECONFIGURATION SERVICES FOR CONTEXT, POLICY AND PROFILE MANAGEMENT

A primary objective of E²R is the design and specification of a reconfigurable protocol framework that enables the implementation of mechanisms supporting reconfiguration in a dynamic fashion.

Mechanisms supporting reconfiguration of protocols may be classified into: control of protocol components, including reconfiguration actions decision and selection, and discovery of protocol component services, including monitoring of their features. These areas address context management (encompassing profile definition and management), policy management, service management (encompassing service discovery, provision, and adaptation), and reconfiguration management (encompassing functions for reconfiguration operations and maintenance).

The RMP can be viewed as another control plane that operates on all OSI layers and runs in conjunction with the network control plane. Its main task is to provide layer abstractions to the applications and services on one hand, and to the terminals and network devices on the other. Furthermore, the RMP is responsible for the coordination of the reconfiguration process, as well as the provision of required resources.

As part of a new *plane*, the RMP functional entities reside both in network elements and in the terminal. Within E²R, a systematic effort to define, specify, verify, and validate these functional entities is being undertaken.

1.3. ENABLING PROCEDURES - *e.g.*, DOWNLOAD MECHANISMS, *etc.*

Independently of the type of software involved, the scenarios related to Software Download can be classified as Terminal-initiated, Delayed/Rejected Software Upgrades or Mass Software Upgrades. In the first of these scenarios, the choice to perform the software download is dominated by user-specified criteria. For instance, the trade-off between performance and cost restrictions may result in choosing an individual (fast) or a collective (slower) download mechanism. In the former case, the software download is performed as quickly as possible via an individual channel to the terminal. The user has to pay the full cost of the download, which might be considerable if the software is not stored in the software download infrastructure and has to be downloaded from an external source (e.g. an Equipment Manufacturer, or a Service Provider). For the collective download mechanism, the download request is registered at a software download support entity in the RAN, and a confirmation of the request is returned to the terminal. In contrast to the instantaneous download scenario, this software download support entity does not send the requested software modules immediately via an individual channel to the terminal, but instead waits for a certain period of time to collect a number of terminal requests for the same software. After this collection period is over, the software download support function sends the software modules to all associated terminals via a cell broadcast channel. Hence considerable wireless capacity can be saved. Of course, the use of a broadcast channel only makes sense if a threshold minimum number of users have requested the download, otherwise an individual download channel for each terminal should be used.

The delayed/rejected upgrade scenario is explained as follows. Compulsory downloads, not initiated by the terminal, which may result in negative effects on the performance of user services, are rejected. However, they can also be logged and performed at a later date (i.e. delayed). Possible reasons for delaying/rejecting the download include the terminal being busy with user applications that would be impaired by a software download, or the cost of the download exceeding the cost limitations specified by the user preferences (e.g. users on expensive low-bandwidth connections, or roaming in a foreign country). A particular download/upgrade might not required as the air interface implemented by the software might currently not be being used or is not available at all in this connecting area. The introduction of a network element can avoid unnecessary downloading: a central software repository can provide persistent long-term storage for software and profiles that have been downloaded from, or uploaded by, external software suppliers. The software download box is responsible for filtering and delaying software upgrades on behalf of the user’s terminal. It manages the download to the terminal of software upgrades that have been stored in the central repository in an asynchronous and situation-aware manner. One software download box per user is maintained by the network operator, hence each box has the capability to keep track of the states of several terminals belonging to one user.

Mass software upgrades are usually initiated by suppliers, such as equipment manufacturers, service providers, or 3rd party software vendors; they may also be performed in the operator’s own interests. The motivation of suppliers to perform a mass software upgrade depends on the kind of software they offer. Equipment manufacturers often want to perform critical bug fixes for a large number of terminals in a fast and efficient way. Service providers offer upgrades to a new version of an application, as a free service to a large number of users. In both cases, the software supplier has to pay for the upgrade, and therefore, it is essential that the network operator offers mass upgrade methods that use bandwidth efficiently and reach a large number of terminals within a short period of time. One-to-many download mechanisms are of particular interest to meet these requirements, hence some research topics and novel solutions in this area are extensively covered in this paper.

1.4. SECURITY

Reconfiguration allows properties of communication equipment that have previously been fixed in the design phase to be changed. This increased flexibility poses the threat that changes contradicting the interests and expectation of end users, network operators, service providers, equipment manufacturers and also regulatory authorities might be made to the configuration of mobile terminals. Security in a reconfigurability context utilises important security services, cryptographic primitives, and building blocks. Reconfiguration safety for secure software download, installation, verification, and fault management is addressed in satisfying regulatory demands for radio software.

1.5. FLEXIBLE NETWORK ELEMENTS

The ITU categorizes two types of network management platforms, namely the *hierarchy distributed data management*, and the *object oriented* platforms. The 3GPP has adopted *hierarchy distributed data management* for the operator-based management architecture and some interfaces. For the data management, the 3GPP has used the *object oriented* method, e.g., the OAM data definition is given in terms of the CMIP or CORBA languages.

The core management architecture for different platforms is very similar; however, the management infrastructure belonging to different PLMNs might be different. The similarity results from the common demands on the general purpose of the mobile communication operations. These are: service provisioning, service creation/advertising, the provisioning of the network infrastructure to fulfil service demands, assurance of the reliability, fault management, and the guarantee of the grade of services, security control, and accounting, etc

The overall Telecommunication Management Network (TMN) concept for 3G networks comprises an integrated solution for service management, network management, and network element managers. The element managers are considered as technology- and vendor-specific entities. This concept ensures multi-vendor management, between network element managers and the network and service management systems. The management system is considered as an important subsystem to save costs during network operation, to accelerate the operational procedures and to improve the overall data consistency. Management for UMTS comprises element management, network management and service management, according to the layered TMN-architecture standardized by ITU-T.

2. APPROACHES AND RESEARCH IDEAS

2.1. *INTRODUCTION*

Reconfigurable radio can be used together with traditional network infrastructures, which do not provide any support for network reconfiguration. However, the full benefits of SDR only become apparent if the utilised network infrastructure takes into account the specifics of a particular terminal, and provides support for it.

In order to sufficiently support SDR, network infrastructure has to be carefully reconsidered. In particular, the following issues have to be taken into account in the design of network elements for future mobile networks:-

- The distribution pattern of terminal and user-related information (profiles) is different compared to conventional networks.
- Software download support has to be integrated into network infrastructure.
- Integrated usage of different radio technologies available in the same area should be allowed.
- Focus on fixed radio standards is likely to be reduced in favour of greater flexibility.
- Greater openness of network infrastructure must allow device sharing, RAT sharing and resource sharing amongst network operators.
- Full usage of reconfigurable network elements to support optimal working points for tuning of RRM parameters.

Technical solutions for these issues attain to aspects of reconfiguration platforms, stretching over reconfigurable network entities and terminals. The interfaces between the entities participating in reconfiguration procedures have to be considered, and their required functionalities have to be identified. Above all, an environment has to be defined to enable the deployment, download, installation and initialisation of network services for reconfiguration. The objectives here are:-

- The definition and outlining of requirements and strategies of end-to-end reconfiguration policies within the reconfigurability management framework. Also, the specification of Reconfiguration management plane concepts.
- The definition of discovery mechanisms for available reconfiguration services and downloadable reconfiguration software.
- Specification of reconfiguration and download services, as well as their respective triggering interfaces and mechanisms.
- The definition of management procedures and APIs for reconfiguration negotiation and initiation, between adaptable end-user services and the reconfigurability management framework.
- The design of reconfiguration platforms, over reconfigurable entities and their respective interfaces.

2.2. *SYSTEM ARCHITECTURES SUPPORTING RECONFIGURABILITY*

The network architecture supporting end-to-end reconfiguration [15] aims to define functional entities for deployment in physical infrastructures, along with interworking with legacy control, management, user-data planes. This architecture is based on the RMP, a management functionality conceived for the flexibility to reconfigure all the layers of the protocol stack.

The overall E^2R system architecture in Figure 1 depicts the logical functions relating to layering principles for protocol modelling. These principles separate protocol structure into three layered subsystems, namely Transport, Radio Network and System Network layers (see [6] for more detail). A layer encompasses elements of similar functionality. Protocols within each of the layers operate across multiple interfaces; they are interworking entities that belong together because of the nature of the mechanisms they provide. These logical elements also extend across multiple network nodes, thus they comprise a set of protocols contributing to the distributed execution of a common system-wide function.

The RMP architecture facilitates inter-operator negotiations, involving the exchange of information that is required for terminal reconfiguration and advanced Radio Resource Management (RRM) and to provide mechanisms for the dynamic planning and management of heterogeneous, coupled, and multi-standard radio access networks. In the Mobile Terminal, RSFs access reconfigurable layers through the Local Reconfiguration Manager. From the Application layer, through the Radio Network layers and down to modem baseband and HW, RSF in the Mobile Terminal control the reconfiguration process of the complete communication chain. They also process all reconfiguration process related information for reconfigurable terminals, originating in any of the layers.

Following the design principles of IP-based networks, the functions related to wireless connectivity are logically and physically separated. The concept of a common IP-based core network, serving multiple heterogeneous radio access networks, requires the encapsulation of access-specific functions in order to allow for the definition of an abstract set of functions which common apply for all access networks.

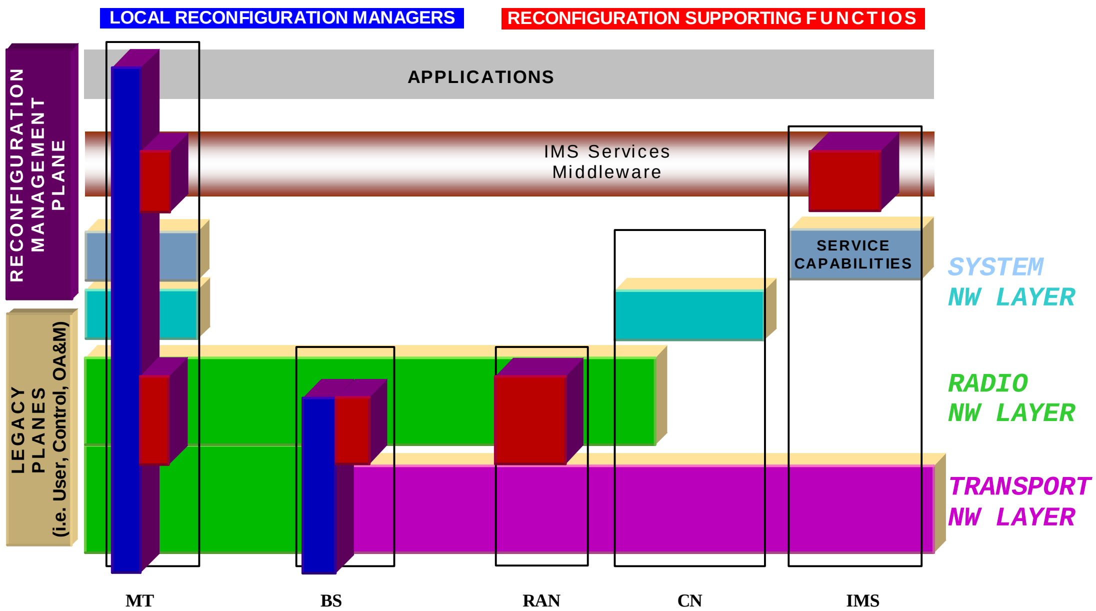

Figure 1: E^2R System Architecture

On this rationale, Radio RSF have been defined to fulfil the requirements identified in the introduction section, spanning the RMP down to the composite RAN, in order to habilitate faster environment scanning when managing the context of the heterogeneous wireless access to support seamless services.

The terminal communicates with the network for assistance when a reconfiguration trigger provokes a state change in the terminal, and launches the reconfiguration process. The Radio RSF assist the terminal by interacting with Radio Network layer elements of available RANs, implementing interworking functions where needed [8].

Interworking refers to interactions that occur in the access stratum between entities of different systems—these entities may reside in domains belonging to different operators. To assist interworking, the terminal reconfiguration process benefits from the rapid detection, identification and selection of the most suitable RAN [16]. In deploying these functions in the RAN, the reconfiguration process also benefits from locality, thereby performing acceptably in time-constrained scenarios such as vertical handovers in delay and jitter sensitive sessions (i.e. Conversational and Streaming in UMTS); furthermore, interactions between Control plane functions are kept within the radio access system domain. Traffic management for spectrally efficient downloads is enhanced, because interactions are closer to radio resource controlling servers. Moreover, the accuracy of time sensitive information, such as radio channel conditions, is improved by shortening paths in retrieving context information. Locality consequently reduces traffic in the network as well.

Radio RSF for Base Stations (BS) also fall within the access stratum. RSF for BS implement DNPM mechanisms, that inter-work with Operation System Functions local to Radio Network Subsystems OAM plane.

2.3. RECONFIGURATION SERVICES FOR CONTEXT, POLICY AND PROFILE MANAGEMENT

The main task of the RMP is to provide layer abstractions to applications and services on one hand, and to terminal equipment and network devices on the other. The RMP also comprises RSF responsible for coordination of the reconfiguration process and for the provision of the required resources [17].

The RMP aims to provide the basis for integrated plane management and layer management support functions. Traditional plane management embraces configuration control, resource management, performance management, fault management, access and security management, and accounting management [8]. Traditional layer management necessitates the existence of interfaces to all protocol layers, both in the control and in the user plane. Layer management handles Operation and Management (O&A) functions on a per-layer basis.

The additional functional entities required to cater for reconfigurable environments, specify a new plane (e.g. RMP) that streches across both network elements and terminal equipment. The modular entities describing the RMP functional architecture and comprising the core reconfiguration services, are shown in Figure 2, and are described as follows.

2.3.1. Plane Management Functions

- *Context Management*: This functional entity monitors, retrieves, processes, and transforms contextual information. Contextual information includes profile information as well as resource-specific information, regarding the reconfiguration progress, the current operational mode, state information, congestion indications, etc. Contextual information affects the service provision phase, and provides inputs to policy decisions and reconfiguration strategies.
- *Profile Management*: The profile management entity handles profile definition and provision, managing and combining the different profiles. This profile information originates in different parts of the system, and includes user profiles, network profiles, application/service/content profiles, terminal profiles (i.e. so-called Reconfiguration Classmarks), charging profiles, security profiles, and so on. The collection of profile repositories in a reconfigurable beyond 3G system should be viewed as a composite Profile Provision System (PPS). The PPS should apply to an *n*-tier platform capable of disseminating profile management policies to an *n*-layered architecture. This multi-tier architecture can be constructed based on topological and/or semantic considerations. Segmentation and distribution of profile data representation via profile staging, and a two-dimensional (topology-based) multi-tier (semantic-oriented) hierarchical organization of profile managers, should offer performance and flexibility benefits.
- *Reconfiguration Classmarking*: This entity keeps track of the different network nodes and their states regarding reconfiguration (e.g., the protocol versions that are installed). Each terminal is assigned a Reconfiguration Classmark, which specifies its level of dynamism

and capabilities regarding reconfiguration (e.g., enhanced MExE classmark). The calculated value of the classmark depends on the type of reconfiguration requested and negotiated, on the type of software to be downloaded, on business incentives, and on individual or operational chains of stakeholders involved in the reconfiguration process.

- *Policy Provision*: This functional entity is the main decision-making entity for reconfiguration, comprising the entry point for reconfiguration-related system policies. Furthermore, it exploits contextual information and redefines policy rules and reconfiguration strategies. This functional entity makes up-to-date decisions about the feasibility of reconfigurations, as well as the respective actions required to be triggered. Additionally, the Policy Provision function caters for inter-domain issues, interacts with Policy Enforcement Points, and facilitates the mechanics for end-to-end reconfiguration differentiation.
- *Reconfiguration Management*: The reconfiguration management function initiates network-originated and coordinates device-initiated configuration commands, by communicating with peer Configuration Control Modules in the terminal equipment. In order to supervise end-to-end reconfiguration, it incorporates the necessary signalling logic, including trading and negotiation services. In the case of scheduled software download, the Reconfiguration Control function hands-over control of the residual reconfiguration steps to the Software Download Management function.
- *Software Download Management*: This function is responsible for identifying, locating, and triggering the suitable protocol for software for download, as well as for controlling the steps prior to, during, and after the download. The target software is fetched from the appropriate repository under the control of a RSF.
- *Service Provision*: This entity is responsible for interaction between the RMP and the application/service. It accepts and processes reconfiguration requests for the network, in order to provide the necessary environment for an application and service to execute. Additionally, it provides feedback to the application about the feasibility of the request, and can also initiate a reconfiguration command on behalf of the application; for example, it can initiate network configuration changes or selection of different settings by the users, or it can initiate mobility-related actions. Furthermore, the Service Provision function can 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 Service Provision functional entity.

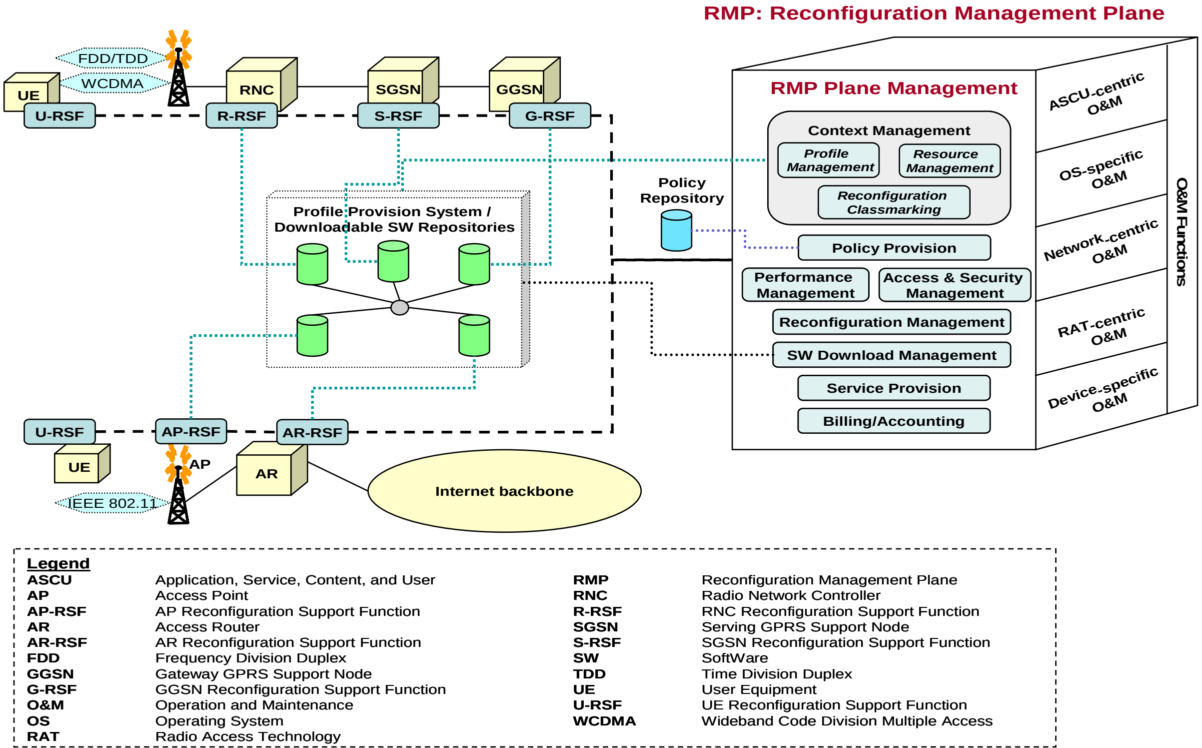

Figure 2: RMP Architecture

2.3.2. Layer Management Functions

In order to accomplish end-to-end reconfiguration, traditional layer management functions must be enhanced to collaborate with the RMP plane management functions. For example, functions for O&M may be exploited for the service provision stage, thus should be adapted based on input related to the definition and enforcement of reconfiguration policies. End-to-end differentiation of reconfiguration services should also take into account the outcome of reconfiguration functions for O&M, such as monitoring the reports and capabilities of network elements.

O&M functions can be classified to five categories: Application, Service, Content, and User-centric (ASCU) functions; OS-specific; Network-centric; RAT-centric; Device-specific. The provision of customer care information is a typical example of an ASCU-centric O&M function. Logging is an important feature, offering the history of reconfiguration actions (e.g., recent OTA upgrades), statistical information on the latest faults, and alarms reported to the user, etc. The other four categories of O&M functions are described as follows.

- *OS-specific O&M functions*: These coordinate the auditing, testing, and validation procedures at the Reconfigurable User Equipment.

- *Network-centric O&M functions*: Address the impact of mobility and QoS on the software download process, also dynamic network planning and its impact on traffic split, which comprise important O&M functions for reconfigurable network elements.
- *RAT-centric O&M functions*: Manage RAT-specific issues for a single Radio Access Technology, or guarantee efficient collaboration of multiple RATs. The *Composite Radio Environment Management function* handles stability, conflict resolution, and certification issues, and ensures proper collaboration between network infrastructure manufacturers and terminal providers in the reconfiguration process. The Radio Element Management functional entity cooperates with the Performance Management RMP plane management entity. Analysis of RAT-specific performance data is an example of performance management, which may in turn affect real-time reconfiguration. The Function Partitioning and Reallocation entity coordinates coupling issues, as well as the distribution of functional entities for multi-RAT environments owned by a single administrative authority. Finally, the Interworking function verifies the correct operation of control plane functionality between radio elements owned by different operators, as well as in network sharing scenarios.
- *Device-specific O&M functions*: These include, for example, functions for User Equipment Management. Although security hazards exist, remote equipment diagnosis assists in the remote identification of equipment faults. Coordination with HAL configuration modules can also be accomplished through device-specific RMP O&M functions.

2.3.3. Radio Reconfiguration Supporting Functions

The work on the definition of a general reconfiguration procedure started in the TRUST project [3], in which high-level system schematic descriptions were provided. The following phases were identified as taking part of the reconfiguration process:

- 1st phase: Available Mode Lookup.
- 2nd phase: Negotiation.
- 3rd phase: Decision Making.
- 4th phase: Software Download.
- 5th phase: Location Update.

In addition, a number of reconfiguration management strategies were identified for the negotiation and decision making stages. To develop all of these phases, a modular approach was used in TRUST [18].

The SCOUT project continued the detailing of each stage. Work was focused on the definition of the functions needed to address each step, the network elements involved, and the signalling flows between them. Figure 3 introduces the functional architecture of the Radio RSF, instantiated in the Proxy Reconfiguration Manager (PRM) located in the RAN; this is further grained in the C-Plane (SDRC) and User-Plane (SPRE).

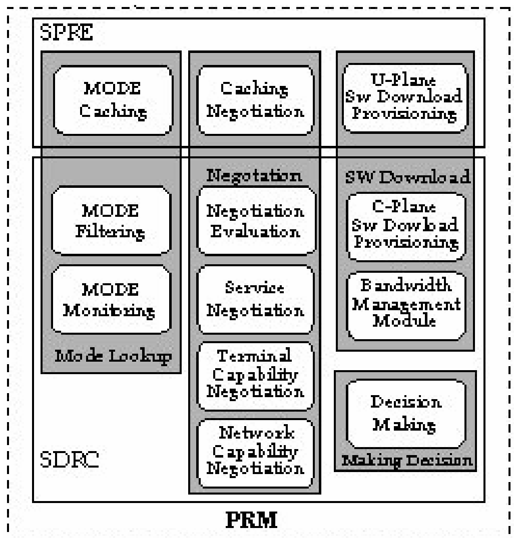

Figure 3: Radio RSF architecture

Interworking covers the necessary requirements needed for providing interoperability between different RATs. A high degree of integration between different RATs should be supported, improving network efficiency for important functionalities such as inter-system vertical handovers. The SCOUT project analyzed Tight and Very Tight Coupling approaches, in terms of their impacts on the reconfiguration process of a terminal, as well as the consequent distribution of functions in network elements [19].

Figure 4 is a composite illustration showing the proposed message exchange process between the Radio RSF entities involved in the different steps of the reconfiguration process.

2.3.3.1. Available Mode Lookup

The identification of alternative modes *can be network assisted or not*, depending on the status of the terminal. This means that if the terminal has insufficient resources to autonomously scan the spectrum, the network can provide this kind of information. The module specified to address this task is the Mode Identification and Monitoring Module (MIMM).

The MIMM consists of three functional blocks mapped into the user (U-) and control (C-) planes of the PRM Proxy Reconfiguration Manager, located in the RAN. These are the Mode Monitoring and Mode Filtering functions in the SDRC, and Mode Caching function in SPRE.

- *Mode Monitoring*: This function is able to discover, identify, and monitor existing alternative modes. It is also able to perform measurements, and it provides a list of available modes to the Mode Filtering process.
- *Mode Filtering*: When the reconfiguration process is ongoing, this function interacts with the Mode Caching function in order to retrieve the list of alternative modes, and then

filters them according to the criteria specified both by user and the terminal constraints. Mode Filtering provides a list of modes with the minimum requirements to address, to the Negotiation phase.

- *Mode Caching*: This function manages the information obtained from Mode Monitoring, and stores it in a Repository. This function interacts with the database where profiles are stored. The role of this repository is to share, with all the terminals, a list of available modes.

Figure 4 illustrates the locations of the functionalities in the PRM and their role in the "Available Mode Lookup" mechanism in detail.

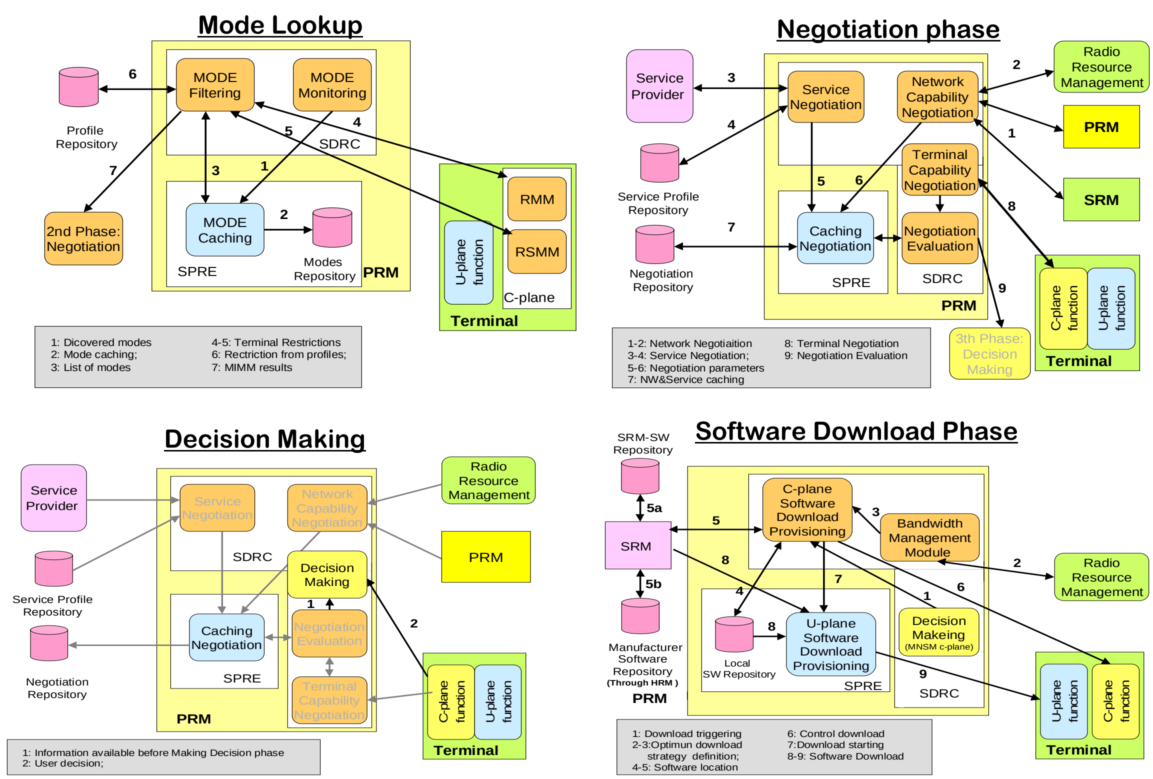

Figure 4: Reconfiguration process phases

2.3.3.2. Negotiation

The Available Mode Lookup phase has the goal of providing a list of available RATs to the Negotiation phase, addressing mainly user- and terminal-specific criteria. The Negotiation phase then executes a filter based on Service, Network, and Terminal capability negotiations. Networks should report information that could be reused for future reconfiguration processes.

Service negotiation has the aim of retrieving service capabilities related to services offered by a particular Service Provider, while the Network capability negotiation has the main goal of identifying the QoS that will be offered to the user by a particular RAT.

A further filter to the RAT mode list is provided based on Service and Network negotiation, and results are cached in the network near the terminal (i.e. in the PRM).

Finally, if the reconfiguration is ongoing, the terminal interacts with the network and negotiates the Terminal capability, matching the status of the terminal resources with the requirements of the RATs acquired in the previous phases—this is in order to find the best solution for a possible switching mode. Results of this evaluation are sent to the Making Decision phase. The module specified to address the Negotiation phase is the Mode Negotiation and Switching Module (MNMS). It is composed of the following functionalities:

- *Network Capability Negotiation Function (NCN)*: Gathers information about the network resources available for new modes (i.e. for QoS reasons).
- *Service Negotiation Function (SN)*: Retrieves the service requirements needed to support the service provisioning.
- *Terminal Capability Negotiation Function (TCN)*: Interacts with the terminal C-plane in order to gather information on dynamic terminal parameters (i.e. remaining power, available memory, etc.)
- *Cache Negotiation Function (CN)*: Results from the NCN and SN functions are stored in Negotiation Repositories by the Cache Negotiation Function.
- *Negotiation Evaluation (NE)*: Collects information from the Negotiation Repository and TCN function, and matches this information to find the best solution for a possible mode switch.

2.3.3.3. Decision-Making

Information collected in the previous phase is input to the "Decision Making" algorithm, which aims to understand whether the reconfiguration is feasible or not.

- The *Decision-Making function* is located in the MNSM module, is mapped in the C-plane of the PRM and interacts with the caching negotiation module and the terminal.

2.3.3.4. Software Download

This phase consists of the requested software module’s download to the device. The module to support this process is the SDM (Software Download Module) located in the U-plane. The C-plane also participates in the download, providing control functions and signalling.

After the definition of the optimal download strategy, the SDM is in charge of downloading the software from a certain entity in the network, for example a software cache situated within the PRM or the HRM. It is composed of the following functions:

- *Bandwidth Management Module (BMM)*: Depending on several important variables, this calculates the optimum download strategy. It interacts with the Radio Resource Management in the network.
- *SW Download Provisioning (SDP) function*: The SDM also interacts with a local software Repository. The SW Download Provisioning function is able to download the software from the network to the terminal.

2.3.3.5. Location Update

This phase has the goal of supporting terminal mobility during the reconfiguration process. This task is supported by the LUM (Location Update Module). In micro-mobility situations, the functionalities supporting terminal mobility should be located in the PRM (C-Plane), while in macro-mobility situations the management of mobility should be done within the core network.

2.3.3.6. Base Station RSF

RSF for BSs implement BS Service Profile Management, describing the Hardware, Software and Functional (e.g. Air-interface) capabilities; SW Download Management of additional/ new software modules required for a specific configuration; Load/ Traffic Management to control the allocation of resources to a specific standard; and Performance/ Load Monitoring to observe the hardware and software resources within a Base Station.

2.4. ENABLING PROCEDURES - e.g., DOWNLOAD MECHANISMS, etc.

2.4.1. One-to-Many Software Download Protocol for End-to-End Mass-upgrade Downloads

Mass-upgrades are a particularly important area of research at present. To provide software, firmware, or other information to mobile terminals for mass-upgrades, Over-the-Air (OTA) downloads ultimately offer a *panacea*, as is the case for single-user downloads [20]. Through OTA downloads, no prerequisites are needed to create channels for the software download as it is assumed that wireless channels, or an automated means to create them, already exist ubiquitously. Hence no effort from the user is needed to perform the software download, and it is ensured for security purposes that the download can be enforced if the terminal is to be allowed to use the resources of the system.

2.4.1.1. One-to-Many Downloads at the Network Layer

At the network layer, there are three basic methods for one-to-many software downloads: *n*-times unicast (where *n* is the number of receivers of the software download), which we will refer to as *n*-unicast, reliable multicast and reliable broadcast. Practically, mass upgrades over the Internet are usually performed using *n*-unicast connections to receivers, because receivers are likely to initiate the upgrade at different points in time. This is very inefficient, as the same information is sent repeatedly, particularly on links close to a source. Future one-to-many software downloads should be achieved using reliable multicast for improved efficiency, and a range of reliable multicast protocols have been envisaged for this purpose [21][22] (see [23] for some further examples). However, many reliable multicast solutions suffer from operational difficulties, which cannot easily be overcome.

Given the challenges introduced by the use of reliable multicast, TCP *n*-unicast would be advisable if there were only a small number of receivers of the download. TCP is far superior to reliable multicast in congestion control and flow control performance, and it is also able to offer a separate data rate to each receiver of the download (i.e. it is multi-rate), whereas many reliable multicast protocols only offer the download at the rate that the worst performing receiver in the group can sustain (they are single-rate). Alternatively, given a very high proportion of receivers of the download in the network, multicast routing and state requirements in the source and intermediate nodes might be excessive and unnecessary, so broadcasting of packets might be a better option.

For a range of reasons in mobile communication scenarios, it is unlikely that all receivers would be able to, or wish to, receive the download starting from the same point in time. Hence a mechanism should be incorporated allowing receivers to join the download after it has been initiated. Furthermore, at some point in the download receivers might forsake participation, due to leaving a radio resource coverage area or the loss of terminal power for example. For these reasons amongst others, the number of download receivers hence the optimum form of one-to-many download method might change during the download, and consequently, a switching scheme between one-to-many download methods would be beneficial [24].

2.4.1.2. Unified Protocol

From a high-level perspective, there are two basic approaches for the implementation of dynamic switching between one-to-many download methods [24]. Bridging schemes may be applied between existing protocols, which are relatively simple to achieve but exhibit bad performances. However, a unified protocol, merging elements of *n*-unicast and multicast/broadcast techniques, would provide far better computational and operational efficiency than bridging. A unified protocol at receiver and source sides is depicted in Figure 5 and Figure 6 respectively.

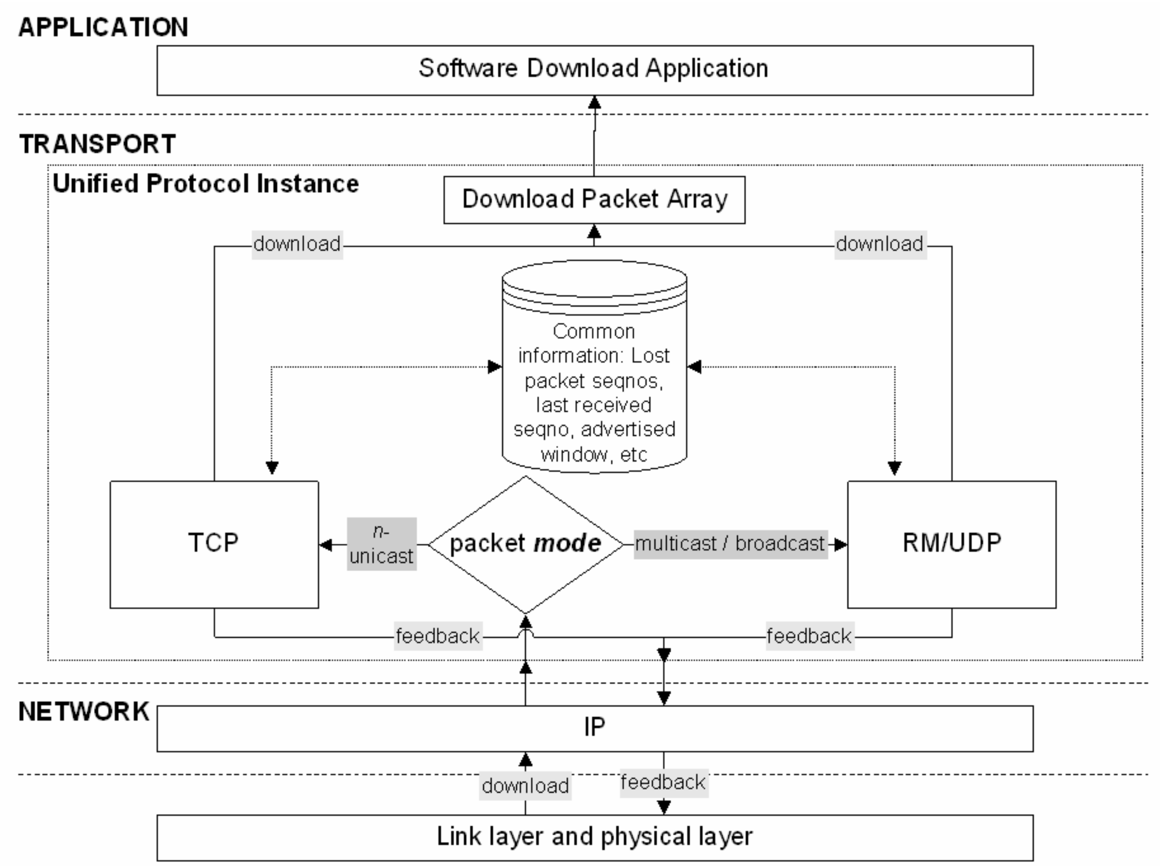

Figure 5: Unified protocol at a receiver

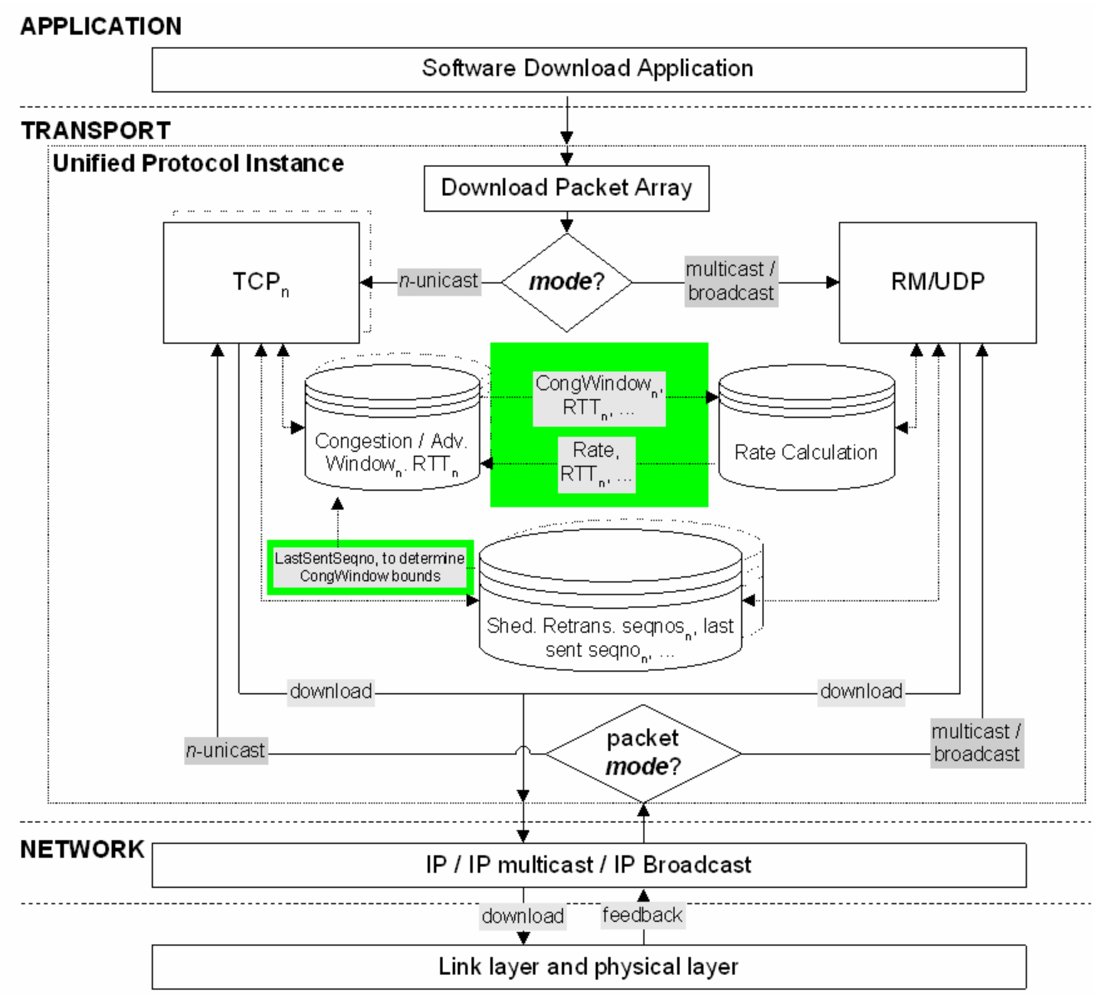

Figure 6: Unified protocol at the source

To trigger the switching process, we define four threshold values:

Tu = Threshold for switch from multicast to *n*-unicast

*Tm*1 = Threshold for switch from *n*-unicast to multicast

*Tm*2 = Threshold for switch from broadcast to multicast

Tb = Threshold for switch from multicast to broadcast

where $Tu < Tm1 < Tm2 < Tb$. We have introduced a form of hysteresis in return switches to improve the stability, e.g., switches from multicast to *n*-unicast occur at a lower value of the considered metric than associated switches from *n*-unicast to multicast. This averts unnecessary switching as a result of small fluctuations in the metric.

2.5. SECURITY

In using a reference model for the reconfiguration system, threats and security objectives related to reconfiguration need to be thoroughly understood. To achieve the overall objective of providing a reliable service that fulfils the expectations of all involved stakeholders, the following points have to be addressed:

- The provision of a secure software download and execution environment to protect against malicious (or non-operational) software.
- Specification of a secure reconfiguration process to ensure that the configuration matches the preferences and expectations of the end user, service provider, and network operators.
- The control of radio emissions to ensure that, irrespective of the possibility to reconfigure a terminal's radio part, specified conformance parameters cannot be invalidated.

Suitable splits of responsibility between the control the reconfiguration processes, as well as different approaches regarding the responsibility and technical means to ensure conformance must all be investigated. The most suitable chosen approach depends on the required flexibility, end user, and/or service provider preferences, as well as the economic/business environment.

For reconfiguration control, the following scenarios need to be investigated:

- *Centralised Reconfiguration Control*: A single, central entity is responsible for deciding on and performing the reconfiguration. This means that the entity decides on which software (configuration) must be downloaded and installed on a reconfigurable device, and on when to do the reconfiguration. The reconfiguration control can lie in a network-based entity, or be controlled directly by the end user. Candidate stakeholders controlling the reconfiguration must be identified; in particular, possible stakeholders are the user's (communication) service provider, the network operator (in case this is different from the service provider), or an independent reconfiguration service provider (which must in any case be certified and approved by the service provider). Some form of distributed control for the reconfiguration can be achieved by using a central reconfiguration decision authority (RDA), that acts as an arbiter or mediator to solve possible conflicts of interest between the involved administrative domains. While the final decision is still taken by a central entity, several stakeholders can signal status information and proposals to perform a reconfiguration, and therefore can influence the reconfiguration.
- *Decentralised Reconfiguration Control*: This is the more challenging approach where control of the reconfiguration is distributed between administrative domains. This means that possible conflicts of interest have to be solved directly by the involved administrative domains and the reconfigured device, without relying on a central entity to take the final decision. In particular, the split between a currently used visited network and the user's service provider needs to be investigated. While the current network has detailed information about local radio link properties and current network conditions, it is the user's service provider who is responsible to ensure reliable provision of subscribed services.

Conformance for radio emissions can be ensured based on the following approaches:

- Reliance on a trusted provider for radio software (a manufacturer or independent third party)
- Network-based configuration validation
- Terminal and/or network-based radio-emission monitoring to identify and deactivate incorrectly configured radio equipment.

While using a network-based server to validate an intended radio configuration has been discussed in literature, it has been left open as to which properties can actually be verified, as well as whether the properties that can be verified are sufficient to ensure conformance of radio emissions and / or standard compliance. However, network-based tests and checks can be used to ensure reliability, thereby reconfiguration attempts can be prevented that would be rejected later-on by the terminal in any case.

In TRUST, an approach has been developed to monitor radio emissions, either terminal-based or network based, and to detect and deactivate terminals with a rogue radio configuration. From the regulatory perspective, it needs to be clarified as to which properties are sufficient to monitor, in order to ensure conformance of radio emissions acceptably. Furthermore, instead of deactivating the terminal, a more user-friendly approach has been developed that deactivates the “Rogue” radio configuration, and activates a fixed failure-mode configuration instead, that allows the terminal to contact a network-based repair function. The terminal may contacts this repair function to obtain a working configuration, without being required to be brought to a service point or returned to the manufacturer. This fixed failure-mode configuration can also be used to ensure that, irrespectively of the currently-used configuration, emergency-calls can be set-up. However, since this issue deals with service deactivation, non-authorised terminal modifications should be carefully analysed.

2.6. FLEXIBLE NETWORK ELEMENTS

The Dynamic Network Planning and Flexible Network Management (DNPM) [25] concept investigates network planning issues for coupled networks, based on reconfigurable network elements such as the BS and RNC. It aims to deliver the principles of network reconfiguration, and to show the advantages of reconfigurable networks for capacity enhancement In order to deliver reasonable results, both analytical and simulation approaches should be carried out by means of task-splitting amongst work packages and activities. The demanded dynamic network simulations, taking into account multi-standard radio network elements, must be performed, and recommendations for network planning must be derived. Automatic network planning is another use-case for reconfigurable, multi-standard network elements (e.g. autonomous selection of carrier frequencies, etc). Mechanisms and signalling for such “self-tuning” RAN’s must be developed.

Compared to conventional situations, additional capabilities that arise from composite radio infrastructures include the abilities for alternate RATs to be activated in network segments, and for available resources (spectrum) to be assigned to RATs taking into consideration of varying temporal and spatial spectrum needs in reconfigurable communications. There are several key tasks that are covered by network planning:

The modelling task is a logistic task for fulfilling network reconfiguration, in order to design the system signalling supporting reconfigurability. This task delivers time-variant and site-variant traffic intensities, with detailed models for Busy Hours (BH) in different service types, as well as combinations of models for different traffic splitting policies. The reason to model time-variant and site-variant traffic types and user behaviours, is to test the performance of advanced network management schemes, including network reconfiguration working in an outer-loop and joint radio resource management and spectrum sharing schemes being modelled as an inner-loop.

Theoretical work to test the requirements of the radio interface, can be compared to trials from snap-shot simulation in typical scenarios; different network configurations can be tested, where the network configurations include: Feasibility of setting radio interfaces; Location of Base stations of available air interfaces; Propagation parameters; Antenna patterns; Coupling structures and depth among sub-networks; Policy of JRRM; Statistical values of required spectrum in different scenarios with available RATs. In the optimisation campaign, algorithms like Greedy, Taboo Search, and Simulated Annealing can be considered.

During network performance evaluation procedure, the following policies from reconfiguration feasibility viewpoints are taken into consideration: Joint admission control and adaptive radio multi-homing policy (e.g., whether alternative access is allowed, whether simultaneous connections are allowed); maximum delay, mean delay for sub-streams if traffic has been split.

The output of a problem that handles such network planning instances includes the network elements (base stations) that will be deployed and their locations, the selection and configuration of multiple RATs in certain elements of the network, the partitioning of traffic to various RATs and networks (e.g., from UMTS to 4G or vice versa, from UMTS to BRAN, etc.) as well as the resources per BS/RAT.

New functions required to exploit the benefits flexible network management are as follows:

- *Real time network reconfiguration*: The interworking between performance management and the radio element manager can be reused for the purpose of observing, triggering and evaluating the changes of the radio network. However, the existing architecture and signalling only support the changes of the selected implementation parameters.
- *Optimal radio environment setting*: Different levels of radio entities will be supported. The end to end reconfiguration aims at optimal reconfiguration with the involvement of reconfigurable mobile terminal and the radio network. The network management architecture is designed to optimally schedule the network reconfiguration and terminal reconfiguration.
- *Function partitioning and reallocation*: A very important character of the reconfigurable radio elements is the changing of functions and changing of associations. A typical example can be given based on the hotel BTS/RNC concept. The signal from one RF set can be processed by one node B or another from time to time which allows the enhancement of the system reliability, availability and room for the design of advanced radio resource management.
- *Flexible network management*: The statically behaviour of the user traffic shows the features of the traffic as temporal-spatial variant with short coherence time. It requires that the data base management to be efficient targeting at the optimal selection of the

effective parameters which triggers the network reconfiguration. For instance, a local jitter/variance of the traffic can be amended by a local implementation parameter change, whereas, statistical thorough traffic change with confidence of long term analysis will result in a big change of the radio network, e.g., RF reconfiguration and function reallocation.

- *Distributed intelligence*: From the nature of the hierarchy architecture defined by 3GPP, indirect interworking between radio elements in different levels becomes inefficient, e.g., between node B and the extension points, between the neighbouring node Bs, etc. are envisaged to be included in the emerging reconfigurable system. In addition, the operators might operate the same radio network (network sharing scenario) or allow coupling the network architecture with each other. In this case, strategies implicating the signalling design must be developed, which supports efficient reconfiguration. The possibilities of establishing common databases being accessed by different operators are under investigations, which targets at a shared network infrastructure.
- *Network reliability*: Sudden changes of the radio network resulting in degradation of the availability should be avoided, whereas, the lost of availability is measured by the dramatic drop of on going calls or the high probability of the high rate of call blocking for the admission control functions. Therefore, steps ensuring the reliable network reconfiguration and the levels of network reliability should be reached. Decision making process enhances the network reliability based on accurate traffic estimation.

2.7. OTHER RECONFIGURATION APPROACHES

2.7.1. The User-Centric Personal Area Network Approach to Reconfiguration

The concept of a reconfigurable Personal Area Network (PAN) might be seen as an alternative approach to providing a user with multiple local services in a distributed manner. This approach might also be seen as more generic in nature; the all-in-one terminal could in fact be a part of a Personal Area Network.

Networks can save hardware resources by permitting multiple users use of the same supporting network. To date however, resource sharing is mainly available on a large scale and is designed to serve the global population at large. It might be seen as highly desirable to have a user-centric network, linked to a single user, whereby a number of electronic devices are controlled in such a fashion as to enable the user access to all of his own devices as well as those which are in his immediate surroundings.

Bluetooth technology has gone some way to addressing this issue, and allows for short-range radio communications between electronic devices that are equipped with the blue-tooth “chip”. Moreover, the pico-net and scatter-net concepts might be seen as forerunners in the quest for complete Personal Area Network automation (i.e. reconfiguration) where the aim is to develop a system that is transparent and user-friendly (simple to use). Bluetooth networks can be seen to be comprised of master and slave devices. One device is nominated as the master for the purposes of network initialization and the rest of the devices become slaves. This requires a set-up procedure: when setting up a Bluetooth network care must be taken that the correct configurations are implemented and that the correct device has been selected to control the device. Such set-up procedures can take time and can prove inconvenient, and the loss of the Master device, for whatever reason, can mean the complete network fails. Hence research is on-going into the seamless set-up of such small, local, radio networks; furthermore, examination of how these PANs might subsequently be linked to other PANs to form a complete Personal Network (PN) with a single user as the centre of such a network is an active area of investigation.

The following subsections outline a possible PAN/PN connectivity architecture. We start by considering device and component definitions, and progress through to a core-PAN, extended PAN and PN architecture. A possible topology is derived and defined in enough detail to allow self-organising PAN algorithms to be deduced.

The topology is based around the concept of having master devices controlling appropriate slaves and relayed slaves—the topology can be seen on the PAN level and when extending the PAN through to the PN level. Current ideas, with respect to linking PANs to each other, come conceptually from making use of existing infrastructure such as Cellular, Satellite, WLAN/LAN, Internet and Wireline access networks (with appropriate connectivity to the Core Network).

The (Over-the-air) Control Channel possibility, in relation to the Core PAN Link Topology along with Dynamic Master Reconfiguration is considered, as is the PAN interconnectivity towards the formation of a PN. Finally, a way forward is proposed relating the architecture for PAN Device Admission, PAN control, and link formation.

2.7.1.1. PN/PAN Terminology and Definitions

The PAN/PN concept is a new idea in the world of mobile communications. This top-level idea originates from the expectation of a user possessing multiple devices for his personal use, in addition to there possibly being other devices in the immediately surrounding area which under the right circumstances he could have access to.

The most important step before any system definition is to ensure the architecture is coherently presented and that the nomenclature is well understood. The following definitions address those issues.

Definitions:

User Core-PAN (also referred to as Personal Bubble/Subnetwork): A User Core-PAN consists of the user's own devices, which are within short range (e.g. Bluetooth) communication distance of the user. The User Core-PAN is an essential component of a User Personal Network (PN).

User Extended Core-PAN: The User Extended Core-PAN is the Core-PAN as defined above plus additional devices which are linked to the Core-PAN by means of relaying.

PAN_MASTER: A device in a Core-PAN that is responsible for controlling the Core-PAN (e.g. for device synchronization).

PAN_SLAVE: A device in a Core-PAN that is under the control of the PAN_MASTER.

RELAYED_SLAVE: A device which is part of the Extended Core-PAN, through means of relaying.

Local Foreign Agents: Devices that are also within communication distance of the User, which can be accessed by that User using interconnected structures.

User Remote Network: A network which is currently out of (short) range, but which the User has access to via interconnecting structures. Remote Networks can be a:

Home Network: Consisting of a User's devices at home.

Corporate Network: Consisting of a User's devices at work.

Vehicular Area Network: Consisting of a User's devices in that User's vehicle.

Interconnecting Structure: Structures that enable communications between a User's Core-PAN, Local Foreign Agents and User Remote Networks. An interconnecting Structure can be fixed.

User Personal Network (PN): A User Personal Network is a Network constructed from a User's Core-PAN, Local Foreign Agents and User Remote Networks. These are linked through the use of interconnecting structures.

2.7.1.2. Personal Network (PN) Concept

The previous definitions lead to the first visual concept of a PN. This has been well captured by the MAGNET proposal itself, as seen in Figure 7.

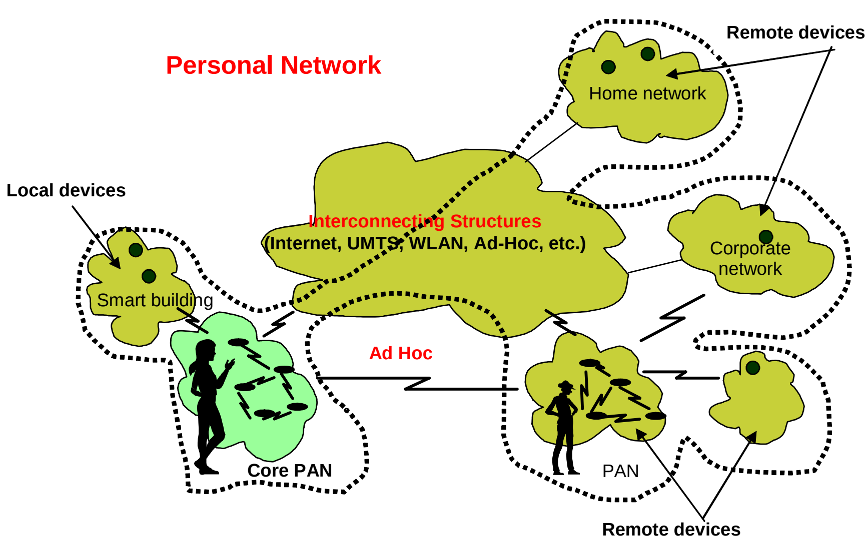

Figure 7: PN Conceptual Visualization (taken from MAGNET Integrated Project proposal FP6/2002/IST/1)

Figure 7 shows in diagrammatic form a User Personal Network (PN) as being a Network constructed of the User's Core-PAN, Local Foreign Agents and User Remote Networks. As per the previous definitions, these are linked through the use of interconnecting structures.

The PN might be seen as a network routing structure terminating at and designed to work in unison with the Core-PAN technology (which is limited by short transmission-range and low power requirements).

2.7.1.3. Core-PAN Concept

Focusing on the Core-PAN component of Figure 7, this area can be expanded in more detail to show User devices that exist in a Core-PAN, as is seen in Figure 8.

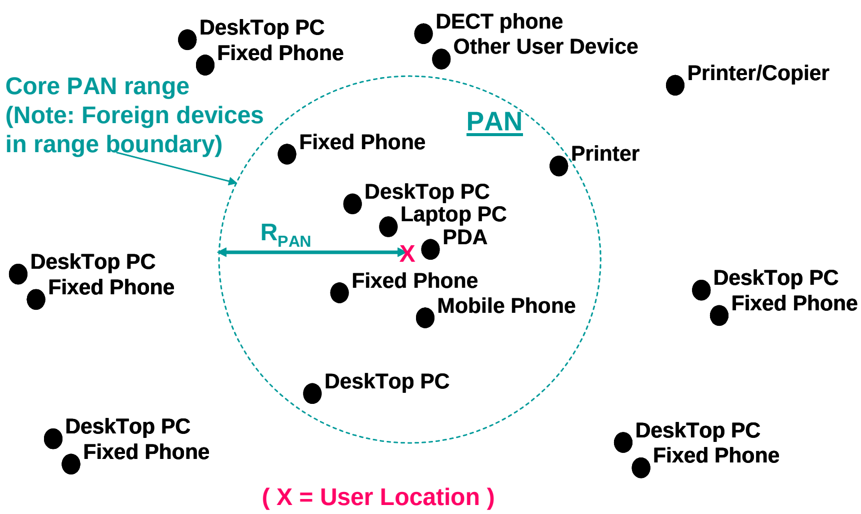

Figure 8: Core-PAN Conceptual Visualization

Figure 8 indicates a particular isolated User, surrounded by devices that form part of that User's core-PAN. However, Figure 7 and Figure 8 simply show devices and grouping of devices, without addressing fundamental communications and link formation strategies that will ensure the system design will work. Definition of exactly how the PAN/PN concept will operate is required, and this requires looking closer at the Design and System Requirements.

Current thinking in this field is that the Core-PAN might be thought of as either a distributed super-terminal, or as a small network. This concept thus brings together ideas that until now have been traditionally regarded as separate entities (namely terminals and networks). The Core-PAN might therefore be seen as a routing structure, with relaying capability, designed to overcome the limitations of the underlying short-range link technology.

With many devices in a Core-PAN operating through battery power, links should be connection-oriented; this has a large impact when considering control information exchange in terms of appropriate protocols and protocol layering. Indeed the question of using a layered approach itself arises.

The OSI seven-layer reference model was conceived to enable protocols to operate fairly independently of each other (i.e. without having to have a knowledge of each other). However, this approach may not be efficient when considering networks which contain nodes (devices) which are battery powered and which need to conserve their energy. An alternative approach may be needed, and this implies so-called cross-layer considerations (which may ultimately result in a Single Layer Protocol, within the scope of the Core-PAN). This will be one of the focus areas for the Core-PAN (i.e. explicitly when looking at keeping links active ONLY when required, minimizing Core-PAN flooding link activation etc).

With this in mind, Link Formation of a Core-PAN is addressed, with the intention of aiming towards a Protocol responsible for creating the subsequently defined the core-PAN topology.

In the Core-PAN concept, to be outlined here, proximity of devices does not mean the existence of a direct link between the two devices (nodes). There is to be an explicit Link Formation Stage.

2.7.1.4. Core- and Extended-PAN Link Consideration (towards an over-the-air Common Control Channel)

As indicated in Figure 9, one important design requirement is to know whether or not the PAN/PN devices are to communicate using a homogeneous or heterogeneous control channel (over the air).

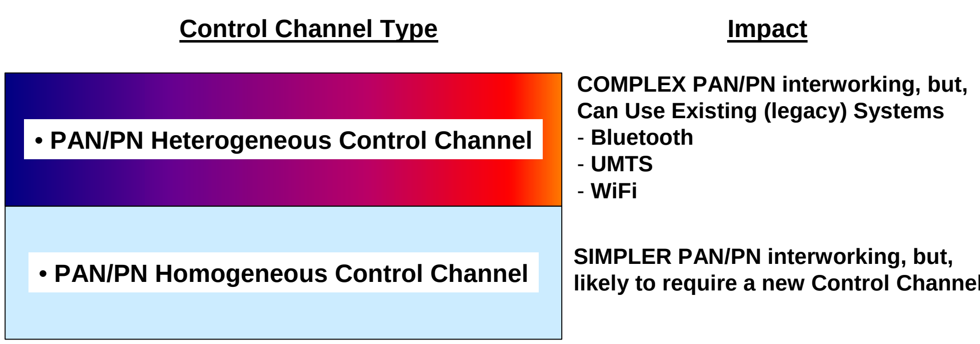

Figure 9: Control Channel Considerations

If the design is to be such that only existing air interfaces can be used in the PAN/PN design, then this automatically drives the requirement to that of a heterogeneous control channel. With heterogeneous control it is likely that an interworking design will be relatively more complex (and PAN requirements will be harder to achieve) than a corresponding design using a new PAN/PN control channel concept. It is also thought that, even with the absence of a new control channel, changes will still be necessary to legacy systems (when working with the PAN/PN concept) and that these changes will not be simple in nature. Hence recommended requirement is the use of a (new) PAN/PN over-the-air control channel.

2.7.1.5. Core-PAN Link Topology

The question of the topology within the Core-PAN also needs to be considered. As seen in Figure 10, three basic kinds of control flow connectivity (not traffic flow connectivity) might be considered: (1) Ad-hoc Mesh Based, (2) Ad-hoc Star Based, and (3) a Star/Mesh Hybrid.

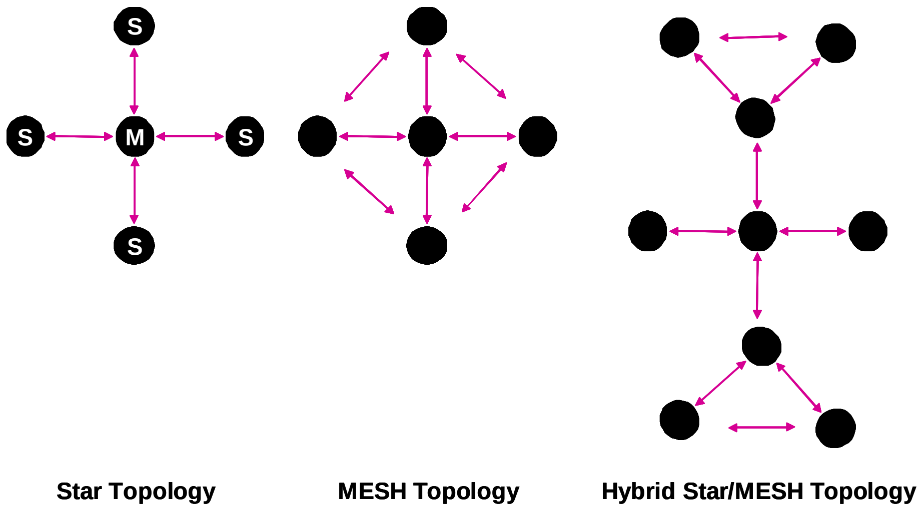

Figure 10: Star/Mesh/Hybrid Based (over-the-air) Control Channel

Both Mesh Based control flow and Hybrid control flow connectivity raise questions about how to ensure that the distributed management of devices is efficiently performed. Distributed management using a Mesh Topology for a PAN is conceptually possible, but control and management issues can be more easily addressed if the Star Based topology of a PAN is adopted. Unlike the other topologies, with a Star Based configuration there is one device that might be easily seen as the MASTER device. The MASTER might be a single device, without which the core PAN cannot be activated; however, a better concept might be to have a single MASTER which is elected at core-PAN setup time, with re-elections occurring should a MASTER be lost for some reason or should a more capably device enter the PAN. In this way the Core-PAN might be said to be in a continuing state of reconfiguration, making particular use of a Dynamic Master selection algorithm.

The choice of which device to use as the MASTER at any particular time might be made in a pre-determined hierarchical way based on device capability; for example, the mobile phone might be set as the default MASTER, but control might be later given to a Laptop PC that is connected to a fixed power supply when the core PAN moves to encompass the Laptop PC. The decision to move MASTER control to another device might be based on criteria such as: (1) device availability, (2) the power source (including knowledge of remaining battery power), (3) the traffic bandwidth capability, and (4) the device processing capability. This is indicated in Figure 11.

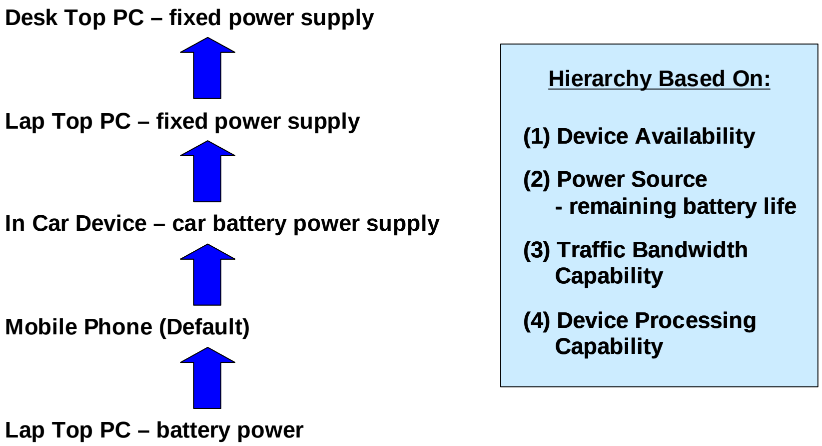

Figure 11: MASTER selection Hierarchy Indication

Further issues arise if multiple users are in close proximity of each other. The possibility of PAN mergers and the resulting topology then needs to be considered. It is thought that each PAN should retain a unique identity, with its own MASTER. In line with this is the concept of allowing devices to join a core-PAN through relaying, thus forming an extended core-PAN.

2.7.1.6. PAN interconnectivity to form a PN

From the foregoing sections, a User's Core PAN, is a result of the (close) proximity of devices to the User, although, as mentioned before, in order to become part of the PAN there is to be an explicit Link Formation process. With the addition of the PAN common control channel, legacy devices can be included in a PAN architecture. In order to link PANs together, there should be, within each PAN, a device capable of accessing the core network. This might be referred to as a **PAN Access Point** (PAP) or **Gateway**, as seen in Figure 12

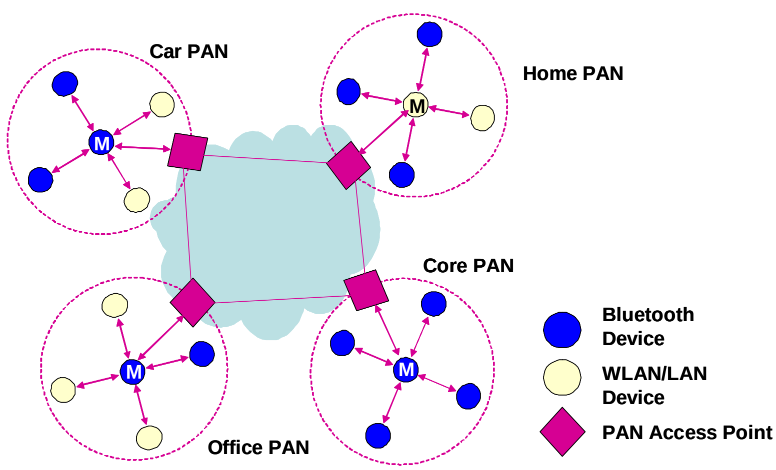

Figure 12**:** PAN Access Points/Gateways

The PAN Access Point (PAP)/Gateway might be one of a number of devices having connectivity to a further, external, system. Depending on device capability these systems might be:

- Mobile Radio Access (e.g. UMTS Access)
- Intranet Access (corporate/private)
- LAN/WLAN Access (e.g. IEEE802.11)
- Satellite Access
- Internet Access (public)

The connectivity would therefore be, as shown in Figure 13;

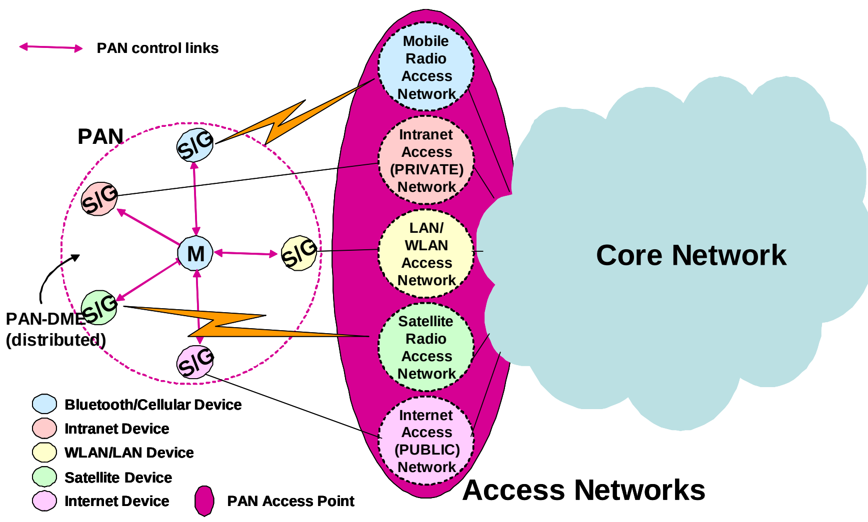

Figure 13: PAN Access to External Systems via PAP/Gateways

Connection to other PANs might be undertaken using the access networks, and their associated structures.

Figure 13 also indicates some Gateway air interface connectivity between the core PAN and the Access Networks (which feed into the Core Network). The air interface connectivity to the access network (i.e. radio access networks) indicated in Figure 13 is;

- Mobile Radio (cellular)
- Satellite

Inside the core PAN air interface connectivity may also utilize Mobile Radio and Satellite systems, although the concept of the PAN is to utilize a local (core-PAN) radio system. The two legacy systems shown in Figure 13 which could be used for the local air interfaces are:

- Bluetooth
- WLAN

These two (local) air interface technologies are the natural fore-runners of the MAGNET PAN concept.

Also shown in Figure 13 is the fact that each SLAVE device is (in the diagram) functioning as a Gateway (hence the S/G nomenclature).

The basic architectures pertaining to possible core-PAN, extended PANs and PNs have been shown. Their derivation leads to consideration of other aspects such as;

- Usage of, and possible Services for, the PN/PAN concept.
- Types of PAN devices and associated capabilities;
- Legacy Local Systems: Bluetooth, WLAN (might be seen as pre-system PANs) – existing Air Interfaces/Control Channels
- New Systems: (new) PAN Air Interface/Control Channel

Core and Extended-PAN Control Channel basic service requirements and scenarios can be deduced from the architecture, e.g. the requirement for, say 10Mbps may come from having a SLAVE device that also acts as a Gateway to an enhanced UMTS (>2Mbps) system, or through having a local video connection as part of the Core-PAN, or alternatively having a SLAVE device that also acts as a Gateway to a broadcast HDTV system.

The topologies can be used to address issues of Link Formation (+Device Discovery, Device Admission Control), routing and service discovery.

2.7.2. Relaying and Reconfiguration

As already seen, reconfiguration is a multi-dimensional problem concerning all parts of the system and all players in the field (business as well as technical).

Concepts related to system and device reconfiguration have evolved due to the perceived need to deliver to the user a fully ubiquitous service, anytime, anyplace, anywhere, any device, any service. All areas of a mobile system can be seen as important, including that of ensuring the coverage to a user is adequate. Relaying can be seen as a way to increase coverage. When considering mobile relaying once might imagine coverage that is “tuned“ to coverage requirements and which might be reconfigured dependent on needed deployment.

2.7.2.1. Dynamic Relay Management

Relays are network elements that are used in order to provide additional coverage in cellular/wireless networks. Some of the main reasons for identifying a need for increased coverage are:

- Bad coverage due to inability of cell planning to give adequate solutions.
- Unexpected concentration of UEs (User Equipment) e.g. accidents (unpredictable).
- Advanced knowledge that an event will occur e.g. football match (predictable).

Two main reasons why Fixed Relays (FRs) (in the form of repeaters – amplify and forward network elements) have been traditionally used for network deployment are:

- To provide coverage in “black” spots (shadowed areas within the coverage area of an AP).
- To provide coverage outside the borders of the AP (Access Point) coverage area.

Alternatively relays can be used to provide higher bit rates, better QoS or cheap infrastructure (sacrificing coverage for these other criteria).

Design and deployment of fixed relays is quite a complex task and many issues need to be investigated. Mobile Relays (MRs) take this a step further. The main problem with mobile relays is the mobility aspect itself and all the associated implications this has e.g. none guaranteed coverage of an area for a fast moving MR. In general, the issue is the dynamic system that mobile relays form and the consequential higher demand for “real-time” management of such a system.

2.7.2.2. Types of Relays

Within a reconfigurable system architecture, several types of Mobile Relays (MRs) could exist. An initial classification could be the following:

Mobile Relays type A (MRtA):→Terminals acting as relays

Mobile Relays type B (MRtB):→Dedicated Relays (built for this prime purpose)

MRtA might be expected to have built-in functionality for relaying, which can be used by the network for the appropriate relay functions. On the other hand, MRtB are relays that need to be designed and as such, any appropriate relay mechanism might be designed, depending on what requirements are given. Additionally, different processes should/could be taken by the network depending on the use of either MRtA or MRtB.

Another classification of relays is based on the functionalities incorporated into them. The simplest fixed relay could be a repeater (an amplify-and-forward element). The most complex and sophisticated fixed relay is similar to an Access Point (AP), although the most complex mobile relay could be even more complicated than an AP, since it would be required to perform additional tasks, i.e. those that a terminal would perform – due to its mobility. For instance, in the case of handover, a MRtB would probably be required to monitor different APs, thus acting like a UE (for the AP) while at the same time acting as an AP for the terminals. In parallel to the above, we expect to have different types of terminals acting as Mobile Relays (MRtA).

The above indicates that in future network deployments, in order to cover different user/network needs, deployment concepts etc., a large number of each of these relays will be present within a cell. Table 1 lists some possibilities. In such a case, it might be beneficial to use just some of those relays and not all of them. There are two main reasons for doing so.

Choosing the correct type based on only what suits our needs best.

Not wasting resources or inducing interference by using relays that don’t “add value”.

Relay	Type	Complexity	Example	% of population
FIXED		High	AP-like relay	70
		Low	Repeater	30
MOBILE	MRtA	High	Laptop	10
		Medium	PDA	30
		Low	Terminal	60
	MRtB	High	Layer1/2 functionalities	30
		Medium	L1 functionalities	50
		Low	"Mobile" Repeater	20

Table 1 : Types of Relays and percentage of total population

The following hypothetical scenario, depicted in Figure 14, might be considered. An AP cell has 5 Fixed Relays (FRs), 60 MRtA(40/15/5→low/medium/high end) and 10 MRtB(7/3→low/high end). Additionally, every e.g. 10/60 secs a new MRtA/MRtB registers or deregisters with the AP. A management and coordination mechanism for this relay population would be necessary - to effectively provide a decision in terms of making the best selection of relays to cover the hypothetical user needs.

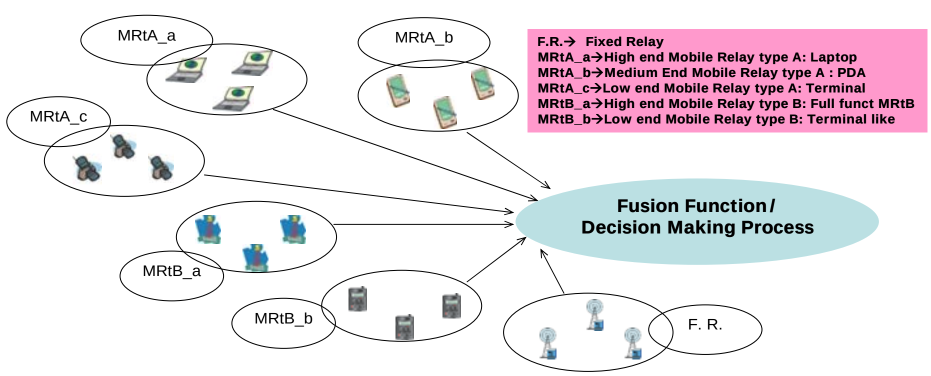

Figure 14 **:** Types of relays Scenario

2.7.2.3. Relay Selection – Management and Coordination Mechanism

A decision making process will be required to manage a dynamic system incorporating relays of various types; managing the relay population. A plethora of parameters (not only related to the relays) need to be taken into account. These could be grouped in the following categories:

- Relay Capabilities/Classes
- Static needs (e.g. area in m^2 to cover, characteristics of area)
- Dynamic Needs (UE population, data rates-applications etc)
- "Real-time" measurements (e.g. interference induced)
- "Real-time" information (e.g. location of UEs/Relays)
- Weighting factors

All the above will be taken into account into one "fusion" function as part of the selection process. This fusion function will yield the optimum relay(s) to cover specific needs. The outcome of the fusion function could be

A number of best-of-all relays to be used. The relays are valued/ranked from e.g. 1-10 and the best e.g. 4 are used. The other 6 are discarded. Effectively we have two groups of relays. A more sophisticated approach would be to not discard all the remaining ones, but keep some of them under "monitoring status" with the possibility of them becoming favourable in the "future". In this case we have 3 groups of relays. In the same way we could have 4 or 5 groups of relays.

A number of optimum relays for each of the identified scenarios. Assume that we have two (or more) scenarios to cover within a cell, with different priorities and needs. Thus, instead (as in the above point) of having one list of relays for both (all) the scenarios, the selection process could yield one group of relays for each of those scenarios. Of course one relay could as well be in both (or more) scenarios.

In parallel to the above we also have to consider how often this "reconfigurability" of the network resources on a cell level occurs. If it is repeated very often then it will consume resources, but will be quite accurate for a fast-changing system. However, with a slow-changing system this might not be required – resources would be wasted. On the other hand, we could introduce some triggers in order to initiate this process. In general, this process could be occurring;

- Periodically e.g. every X seconds.
- Upon registration/de-registration of a relay in the cell or in the APC area. (Access Point Control).
- Upon shift of a relay from the "Active" to the "Monitoring" group and vice versa.
- Upon request from the network for more resources.

2.7.2.4. Relay Selection – Parameters and Capabilities

Based on the previous discussion, a number of parameters/capabilities need to be monitored/taken into account. Some of these could be the following:

- Presence and location of relays
- Velocity of relays and/or UEs
- Power availability/constraints
- Supported data rates
- Priority issues
- Layer 1 supported techniques e.g. power control
- Higher Layer supported techniques
- Induced Interference

- Channel quality
- Transmitted Power/Coverage
- Handover

This list could be as large as necessary for, for example, accurate mapping of relay capabilities to reduce uncertainties in the decision process. However, at the same time it should be as small as possible so that it does not induce delays, signalling problems and generally require large network resources to perform the selection process.

Those parameters, combined with the different scenarios can also give rise to a number of weighting factors. It is expected that different needs will arise for different deployment concepts/scenarios within each cell. Thus, based on each scenario, different priorities will need to be assigned to different criteria e.g. coverage versus bit rates. This is the reason for introducing the weighting factors.

Relays would be required to signal their capabilities to the AP/APC. Another approach would be to set up classes of relays. Thus, instead of each relay signalling its capabilities, (which would induce delay and signalling requirements) it could signal its class. For example, instead of using 20 bits for mapping 20 capabilities, we can use 5 bits to define the class of each relay.

The level at which this management could be done could be either the AP or the APC level. However, before a decision is taken we should take into account the following:

- Complexity of the decision making algorithm/management function
- Delays induced
- Signalling requirements (delay & resources)
- Availability of computational power

2.7.2.5. Relays – Concluding Remarks

The mobility of non-static relays results in a dynamic topology within a cell with a plethora of categories of mobile relays and several, diverse, needs/scenarios to cover. In addition, this status is constantly changing in terms of capabilities and requirements. Thus, in order to make efficient use of the available resources, without at the same time wasting resources or causing additional problems, a dynamic relay management/coordination function should be in place. This management function, part of RRM, will effectively reconfigure the network resources by taking into account a number of parameters (some of them highlighted above) and decide on the optimum relay(s) to serve our needs. Although complex, it seems highly desirable and necessary if we want to take into account the full potential of mobile relays. A detailed study would be required to address the issues of the necessary parameters to take into account and the detailed design of the related algorithms without at the same time introducing highly complex schemes.

3. PROOF OF CONCEPT

3.1. ONE-TO-MANY SOFTWARE DOWNLOAD: UNIFIED PROTOCOL CONCEPT

The performance advantages of using a unified one-to-many software download protocol, able to dynamically switch between one-to-many download methods, are wide-ranging. For example, consider a switch from *n*-unicast to multicast. Given a bridging scheme between protocols, it is likely that congestion control in multicast mode would have to start from a transmission rate of zero, taking time to converge and causing considerable packet loss in the process (see Figure 15, [24]). A unified protocol, as illustrated in section 2.4.1.2, would be able to share information more easily between one-to-many download instances, hence could inherit/transform congestion control measurements into the target mode and in many cases would maintain the transmission rate throughout a switch.

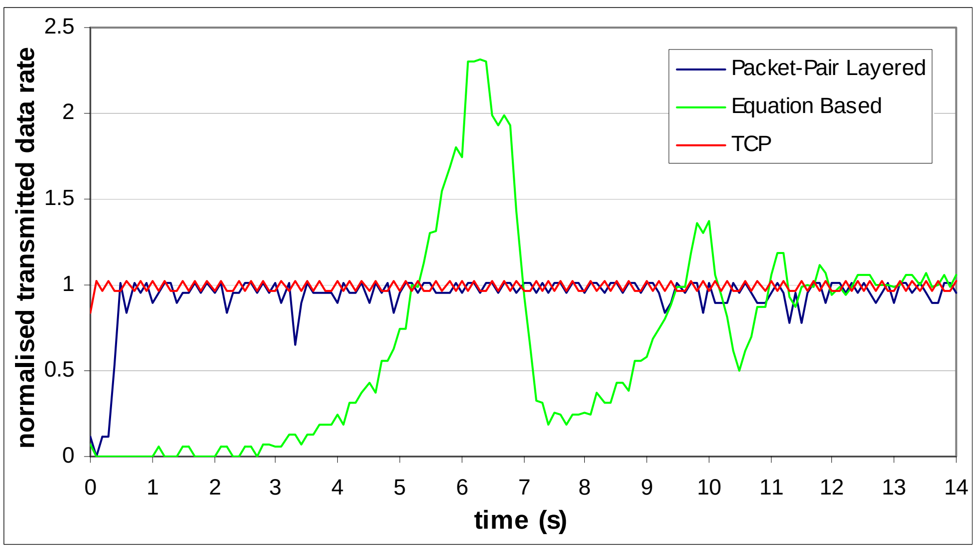

Figure 15: Plot of convergence to available bottleneck data rate of layered and equation based multicast, compared to TCP

Further advantages of using a unified protocol are compelling: drastically reduced memory consumption (see

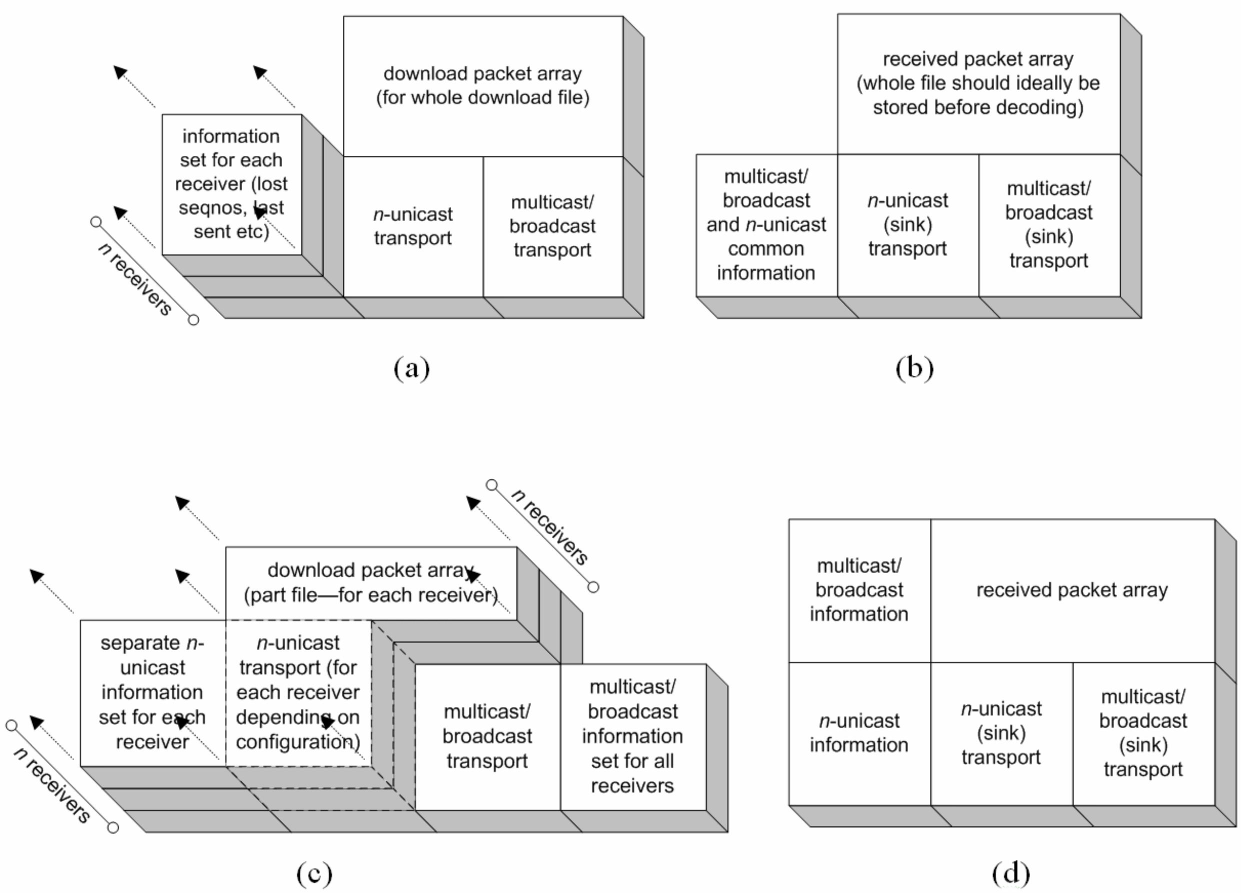

Figure 16, [24]), improved processing efficiency across the transport layer, and the flawless continuation of the download throughout the switching process amongst many others.

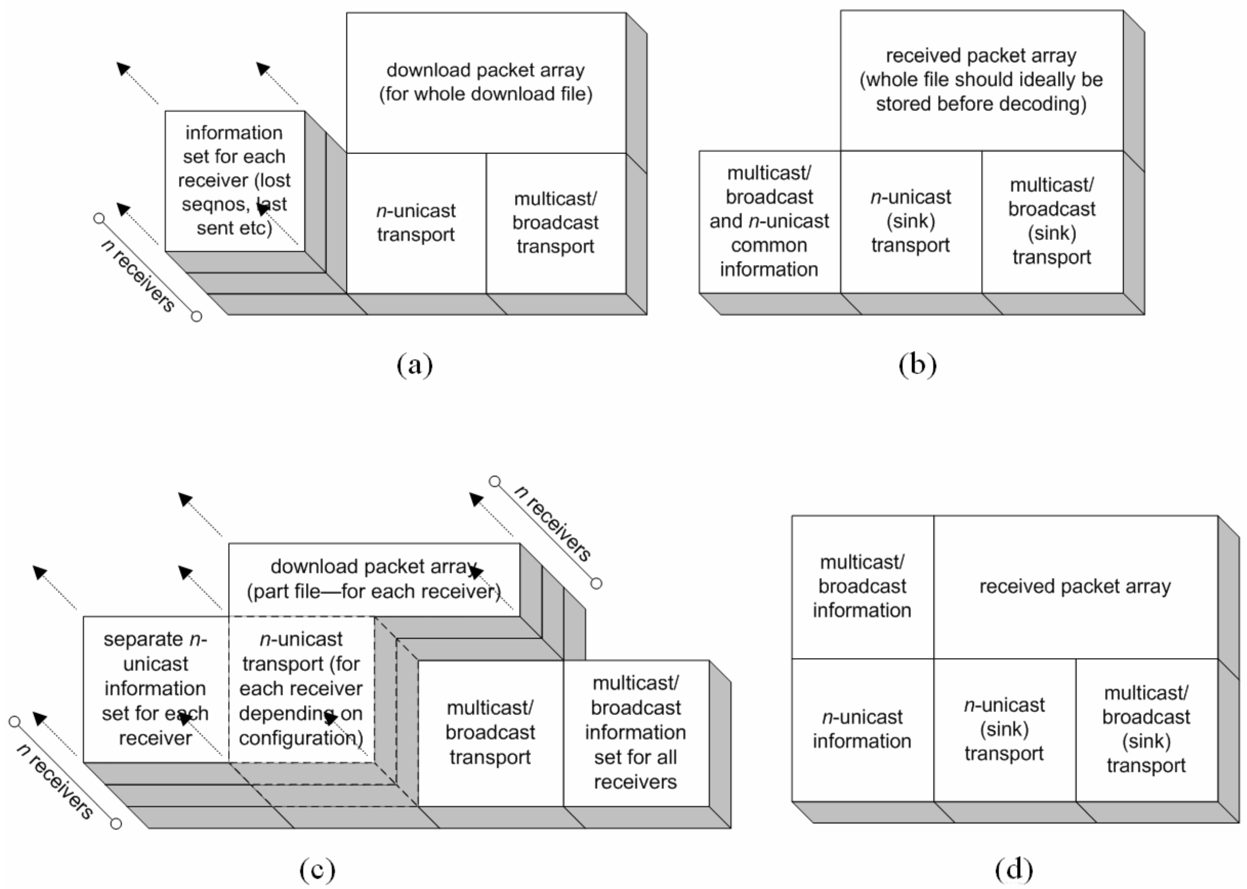

Figure 16: Volumetric depiction of memory usage for the unified protocol approach (a) at the source, (b) at a receiver; alternatively, for a form of bridging between protocols (c) at the source, (d) at a receiver

3.1.1. Realisation of the Unified Protocol Concept

Much work is being undertaken to extend the logical implications of the unified protocol architecture for dynamic switching, as well as considering its incorporation into a range of systems in more depth. We hope to achieve an actual implementation of a unified switching protocol in the medium-long term, but in the short-term we are improving some of the finer details of the protocol's architecture.

Particular areas of research interest for the unified protocol concept include:

- ***Packet mode marking:*** *n*-unicast or multicast/broadcast mode must be marked on each packet. How is this achieved?
- ***Progression of congestion window edges immediately after switching from multicast to n-unicast:*** This is problematic because of the lack of in-flight positive feedback immediately after a switch to many-unicast

- ***Further refinement of parity transmission approaches:*** To further optimise dynamic switching (particularly between *n*-unicast and multicast) and late receiver joining, in addition to providing improved recovery from wireless losses
- ***Incorporation of layered multicast into the dynamic switching protocol:*** Requires in-depth consideration of the benefits

3.1.1.1. Packet Mode Marking

The mode to which they apply must be marked on packets in order for them to travel to the correct part of the unified transport protocol upon reception. This applies for both the source and receivers, hence download and feedback packets must be marked.

For reliability and congestion control purposes, there are two approaches used in the unified protocol: TCP-like unicast, and reliable multicast. Only one bit is therefore required to mark packets, in order to select which of these parts packets are destined for. This bit could be taken from common free space in the transport headers for the constituent parts of the protocol, or alternatively two ports could be used, which both would apply to the protocol. Clearly, the former option is preferable, so an area of research is to look for a way of using that approach with some likely combinations of unicast and reliable multicast over UDP transports.

3.1.1.2. Switching to n-unicast Mode from Multicast Mode

In *n*-unicast mode, positive feedback (using a sliding-window mechanism similar to TCP) is assumed. In reliable multicast/broadcast modes, negative feedback applies in order to limit the risk of a feedback implosion; alternatively, other mechanisms in which feedback traffic load is sparse might also be used. Hence switching back from multicast to *n*-unicast mode, should such a switch be required, is problematic because of the lack of in-flight positive feedback at the time of the switch. Given no such positive feedback, the sliding window edges would not proceed after the switch, and transmission would abruptly halt.

The solution suggested by us in [24] simply involves the automated transmission of packets, at the correct transmission rate, for an approximate period of one round-trip time. However, we are working on a range of alternative approaches to maintain transmission after the switch, using an interim measure. The important considerations here are that congestion control performance shouldn't be impeded, and acceptable fairness and reactivity must be maintained.

3.1.1.3. Parity Transmissions

We are working on a range of analyses and simulations of parity coding performance in general, particularly with a view to coding parity over the whole file as one, instead of coding in blocks. Coding over the file as one offers several performance advantages. Namely, each received parity packet is able to correct any original data packet from the whole file, instead of just a subsection (block) of the file; furthermore, a scheme can be employed allowing receivers to automatically leave the download once they have received enough packets to reconstruct the download. In recent papers, we have quantified these benefits both through analysis and simulation. Figure 17 shows the transmission efficiency performance gains that can be achieved by such an approach. We plan to significantly expand on this work in the context of our unified protocol.

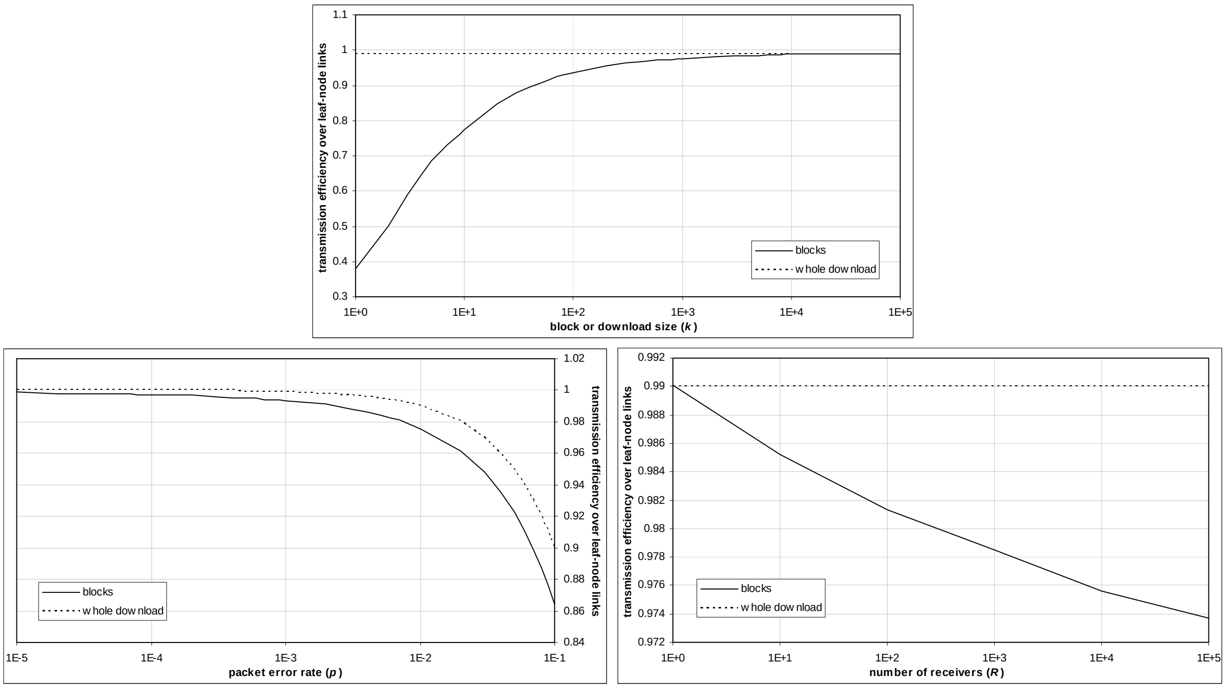

Figure 17: Transmission efficiency over leaf-node links for the 'whole download' and 'block' parity coding approaches. k=1000, p=0.01, and R=10,000, although these are varied in turn in the plots

This work is relevant because, further to the above advantages, parity transmission if coded over the whole file as one assists our unified dynamic switching transport protocol in the following ways.

Late Receiver Joining

Parity transmission helps recover the download at late-joining receivers. This is important in accounting for the temporary lack of availability of some receivers at the start of a download, where such a requirement is particularly relevant in large one-to-many downloads to mobile terminals.

Switching Between *n*-unicast and Multicast

If a download were in *n*-unicast mode for a period of time before a switch to multicast, receivers would have obtained different numbers of packets of the download at the time of the switch. This is because a different transmission rate to each receiver is allowed in *n*-unicast mode.

Given conventional retransmissions, after a switch from multi-rate *n*-unicast to single-rate multicast, the source would have the option of either continuing transmitting from min{lastSentSeqno$_n$}, max{lastSentSeqno$_n$} or a point in between. Continuing from min{lastSentSeqno$_n$} is the simplest choice, but would erode many of the advantages of the prior n-unicast mode through data repetition to many receivers. Continuing from max{lastSentSeqno$_n$} avoids repetition, but requires the later retransmission of sequence numbers min{lastSentSeqno$_n$} through to max{lastSentSeqno$_n$}. In a subsequent retransmissions pass, these packets could probabilistically be a cause of inefficiency to those receivers not requiring them.

Alternatively, the transmission of parity packets in the subsequent pass ensures optimum transmission efficiency, as each transmitted parity packet is useful to every receiver.

3.1.1.4. Parity Transmission Orders

In our unified protocol [24], and in related work we are performing, we suggest possible approaches for parity transmission ordering (see Figure 18). Further work is being undertaken to analyse and simulate such approaches. Particular areas of interest include parity processing loads at receivers for the transmission orders, and the overall transmission efficiency implied by these respective approaches.

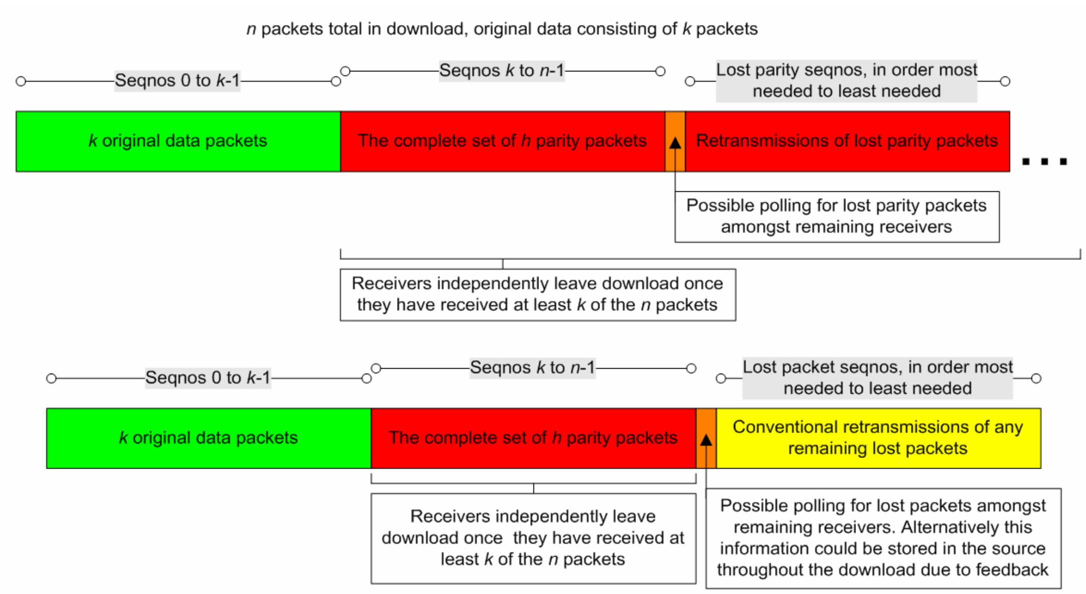

Figure 18: Two parity transmission approaches for our unified protocol (these also apply for reliable multicast downloads in general)

3.1.1.5. Layered Multicast

We also are working on schemes for incorporating layered multicast into the switching protocol concept. Clearly, the use of broadcast in conjunction with layered multicast is not an option, because it would require flooding the network with the information in all layers of the multicast. Hence in such a scenario the dynamic switching scheme would only operate between *n*-unicast and multicast. Furthermore, such are the performance gains of using layered multicast in preference to equation-based multicast congestion control, that layered multicast may indeed be sufficient as a stand-alone solution in place of dynamic switching, should sufficient technologies exist to achieve layered multicast in an acceptable fashion. In the light of this, the benefits of using layered multicast for the scheme require further investigation.

Figure 19 shows a basic transmission order for original data and parity packets using layered multicast [24]. Given the use of layered multicast, we particularly plan to look at performances of various distributions of parity and transmission rates amongst layers. It is unclear how different our conclusions would be from other established layered multicast mechanisms—this is to be found upon deeper consideration of the implications of our requirements.

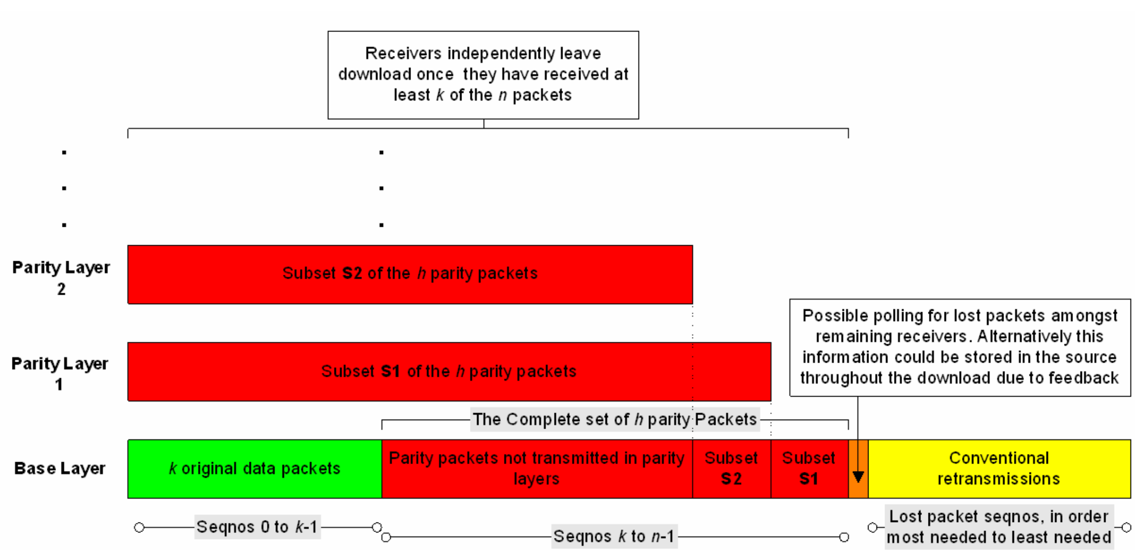

Figure 19: Packet transmission order for the layered multicast

4. Conclusion

This paper has presented many areas of research undertaken by WWRF members that fall into the realm of reconfigurable networks. Since reconfigurability is envisaged to prevail in the world of telecommunications in the coming years, it is mandatory to embrace the overall system's characteristics from the network point of view in order to support reconfigurability at all levels. Hence starting from an appropriate system architecture, this paper has presented the key issues that need be addressed; these issues are topics of ongoing research particularly within the IST-E2R project. In addition to this, it has presented a novel concept for an end-to-end download transport protocol, which potentially offers many performance advantages over currently assumed one-to-many download techniques. This novel protocol offers an approach for dynamic switching between one-to-many download methods many-unicast, reliable multicast and reliable broadcast. Moreover, the architecture for this approach has been introduced, highlighting the way in which elements of reliable unicast and reliable multicast transports can be merged into a single one-to-many download transport layer. As a proof of concept, this paper has considered gains to congestion control performance and protocol memory usage that can be achieved through the use of a unified transport protocol. It has also shown the benefits of some of the facilitating technologies for the unified protocol; furthermore, it has discussed some of the implementation complexities that should ideally be overcome to smooth the incorporation of the protocol into a range of systems.

5. References

[1] End to End Reconfigurability (E^2R), IST-2003-507995 E²R, http://www.e2r.motlabs.com/

[2] Software Defined Radio Forum (SDRF), http://www.sdrforum.org

[3] Transparently Reconfigurable Ubiquitous Terminal, IST-1999-12070 TRUST, http://www.ist-trust.org

[4] Smart User Centric Communication Environment, IST-2001-34091 SCOUT, http://www.ist-scout.org

[5] W. Tuttlebee (Editor). Software Defined Radio. Origins, Drivers and International Perspectives, Wiley Series in Software Radio, John Wiley and Sons, Ltd., 2002.

[6] D. Bourse et al, "WWRF WG3 White Paper: 'Reference model for end-to-end reconfigurable mobile communication systems'," WWRF6 Meeting in London, UK, June 25-26 2002

[7] SandBlaster™ DSP, Sandbridge Technologies, Inc., http://www.sandbridgetech.com

[8] M. Dillinger, K. Madani, N. Alonistioti, *Software Defined Radio: Architectures, Systems and Functions*, John Wiley & Sons, ISBN: 0-470-85164-3, April 2003

[9] IST Project MOBIVAS, http://mobivas.cnl.di.uoa.gr

[10] IST Project CREDO, http://credo.nal.motlabs.com

[11] IST Project Nr. 2000-28088, Models and Simulations for Network Planning and Control of UMTS (Momentum), web: http://momentum.zib.de

[12] IST Project Nr. 18863, System for management of quality of service in 3G networks, (SOQUET)

[13] IST Project Nr. 20275, Simulation of Enhanced UMTS Access and Core Networks (SEACORN)

[14] Jijun Luo, R. Mukerjee, Markus Dillinger, Eiman Mohyeldin and E. Schulz, “Investigation on Radio Resource Scheduling in WLAN Coupled with 3G Cellular Network”, IEEE Communication Magazine, June, 2003.

[15] M. Dillinger, G. Ravasio, N. Olaziregi, N. Alonistioti, K. Kawamura, R. Garcia, T. Wiebke, “Network architecture supporting the End to End Reconfiguration (E2R)”, WWRF8bis Meeting, Beijing, China, February 2004

[16] N. Olaziregi, H. Aghvami, "A Novel Approach for Reconfigurable Systems at RAN Level," ICT'2003 Proceedings, Tahiti, Papeete, French Polynesia, February 2003

[17] Z. Boufidis, M. Stamatelatos, N. Alonistioti, A. Delautre, M. Dillinger, "Actors, Management Plane, and Policy Provision Challenges for End-to-End Reconfiguration", E^2R Workshop, Barcelona, Spain, September 2004

[18] N. Olaziregi, C. Niedermeier, R. Schmid, D. Bourse, T. Farnham, R. Haines, F. Berzosa, “Overall System Architecture for Reconfigurable Terminals”, IST Summit 2001, Sitges, Spain, September 2001

[19] S. Micocci, N. Olaziregi, G. Ravasio, J. Bachmann, F. Berzosa, "Architecture of IP based Network Elements Supporting Reconfigurable Terminals", IST Summit 2003, Proceedings, Aveiro, Portugal, June 2003

[20] W. H. W. Tuttlebee, "Software-Defined Radio: Facets of a Developing Technology," IEEE Personal Communications Magazine, Vol. 6, No. 2, April 1999, pp. 38-44

[21] Multicast Dissemination Protocol version 2 (MDPv2) homepage: http://cs.itd.nrl.navy.mil/5522/mdp/mdp_index.html

[22] L. Rizzo and L. Vicisano, "RMDP: An FEC-based Reliable Multicast Protocol for Wireless Environments," ACM Mobile Computing and Communications Review, Vol. 2, No. 2, April 1998

[23] K. Obraczka, "Multicast transport protocols: a survey and taxonomy," IEEE Communications Magazine, Vol. 36, No. 1, January 1998, pp. 94-102

[24] O. Holland and A. H. Aghvami, "Dynamic Switching Between One-to-Many Download Methods in 'All-IP' Cellular Networks," to appear in IEEE Transactions on Mobile Computing.

[25] M. Dillinger, E. Mohyeldin, P. Demestichas, G. Dimitrakopoulos, J. Luo, N. Olaziregi, N. Alonistioti, "Dynamic Network Planning and Functional Components supporting End to End Reconfiguration (E^2R)", WWRF10 Meeting, New York, USA, October 2003

6. CONTRIBUTING AUTHORS

Fernando Berzosa, Panasonic European Laboratories GE, Germany, (berzosa@panasonic.de)

Eiman Mohyeldin, Siemens GE, Germany, (eiman.mohyeldin@siemens.com)

Jijun Luo, Siemens GE, Germany, (Jesse.luo@siemens.com)

Rainer Falk, Siemens GE, Germany, (rainer.falk@siemens.com)

Gianluca Ravasio, Siemens IT, Italy, (Gianluca.ravasio@siemens.com)

Oliver Holland, King's College London, UK (oliver.holland@kcl.ac.uk)

Hamid Aghvami, King's College London, UK (hamid.aghvami@kcl.ac.uk)

Zachos Boufidis, University of Athens, (boufidis@di.uoa.gr)

Thomas Wiebke, Panasonic European Laboratories GE, Germany, (wiebke@panasonic.de)

Terence Dodgson, Samsung Electronics Ltd., UK (terry.dodgson@samsung.com)