Seamless Connectivity System for Intelligent Public Transportation Systems: Architecture and Mechanism Design

Zsuzsanna Ilona Kiss, Andrei Ciprian Hosu, Gabriel Lazar,
Andrei Bogdan Rus, Virgil Dobrota, and Zsolt Alfred Polgar

Abstract—**Providing ubiquitous connectivity to the passengers of public transportation vehicles is an important goal of the communication system designers in the context of fast development of the intelligent transportation systems and of the Future Internet communication technologies. This paper proposes the architecture of a connectivity system for public transportation communication services, the architecture design being considered on three distinct levels: system, functional and platform level. The proposed system architecture specifies a minimal set of entities required to implement the envisaged connectivity solution and based on a functional analysis the subsystems and modules are derived. By mapping the functional architecture on the hardware components intended to be used the platform architecture is developed. The paper proposes also the design of the mechanisms which implement the inter-process communications, perform the acquisition and handling of the context information and implement a distributed information system characterizing the heterogeneous networking environment. For other mechanisms, like decision and mobility management, the design principles are described. In order to validate the proposed architecture design and to check the correct functioning of the various subsystems and modules a few experimental tests are presented.**

Keywords*—*heterogeneous networks, mechanisms design, network monitoring, system architecture, ubiquitous connectivity.

I. Introduction

The users of Next Generation Networks (NGN) have to be Always Best Connected with the best possible quality anywhere and anytime using different access technologies. In order to satisfy this requirement NGNs have to make use of multiple broadband technologies and have to support generalized mobility.

An important characteristic of the NGNs will be the integration of heterogeneous access technologies in order to increase the system efficiency and improve the users experience. However, achieving seamless service continuity in heterogeneous networks is not yet a completely solved task [1].

To provide ubiquitous connectivity in a heterogeneous wireless network new architecture elements have to be defined. The solution has to fulfill strict Quality of Service (QoS) requirements. Coordination and interoperability between the networks to which the mobile device is connected are required.

In [2] a new architecture integrating different access technologies into an IP core infrastructure based heterogeneous network is proposed. A network selection scheme that takes into account the resource usage and the QoS requirements is also proposed in [2]. A similar architecture is presented in [3], but the network selection problem is considered only for IEEE 802.11a/g and WiMAX networks. An UMTS/WiMAX interworking architecture based on 3GPP standards is proposed in [4].

The challenges related to the inter-working and handover management architecture for WLAN/UMTS systems are identified in [5]. A policy based architecture for multi-service vertical handover is proposed in [6]. The authors in [7] propose a cross-layer architecture which provides handover and mobility control in a WWAN/WLAN environment.

A survey of emerging protocols and architectures aiming to support inter-system handover can be found in [8]. In that paper an optimized handover framework built around the IEEE 802.21 standard is also presented. Another survey discussing the existing vertical handover methods, requirements and technologies is presented in [9]. In [10] a mobile-assisted vertical handover mechanism which exploits the IEEE 802.21 framework and provides service continuity is proposed. An efficient yet flexible handover decision mechanism based on multiple criteria decision algorithms is proposed in [11].

Several international research projects and initiatives are also dedicated to the development of communications technologies intended for heterogeneous networks. The HURRICANE project [12] investigated the optimized handover operation performed between two cooperative RATs (Radio Access Technology). The SMART-Net project [13] aims at developing heterogeneous access network solutions which incorporate smart antennas and offer advanced wireless broadband solutions. The WWRF Initiative (Wireless World Research Forum) [14] studies algorithms and mechanisms dealing with ubiquitous connectivity and service continuity in heterogeneous wireless networks.

The UCONNECT [15] project develops an architecture provisioning ubiquitous connectivity for public transportation communication services.

In this paper we propose the architecture of a system capable to offer ubiquitous connectivity over open coupled heterogeneous networks for the passengers of public transportation vehicles. The architectural design of this system is done at system, functional and platform level. The functional architectures of the entities are developed based on the analysis of the operations which have to be performed by the connectivity system. The platform architecture is derived based on the projection of the functional architecture on the hardware foreseen to be used.

The issue of subsystems and functional modules integration is also considered and a dedicated interoperability mechanism is proposed. This mechanism allows easy upgrading of the con-

Manuscript received May 13, 2014; revised July 8, 2014.

Authors are with the Technical University of Cluj-Napoca, Communications Department, Cluj-Napoca, Romania.

Z. Kiss is the corresponding author (e-mail: zsuzsanna.kiss@com.utcluj.ro).

1845-6421/09/8354 © 2014 CCIS

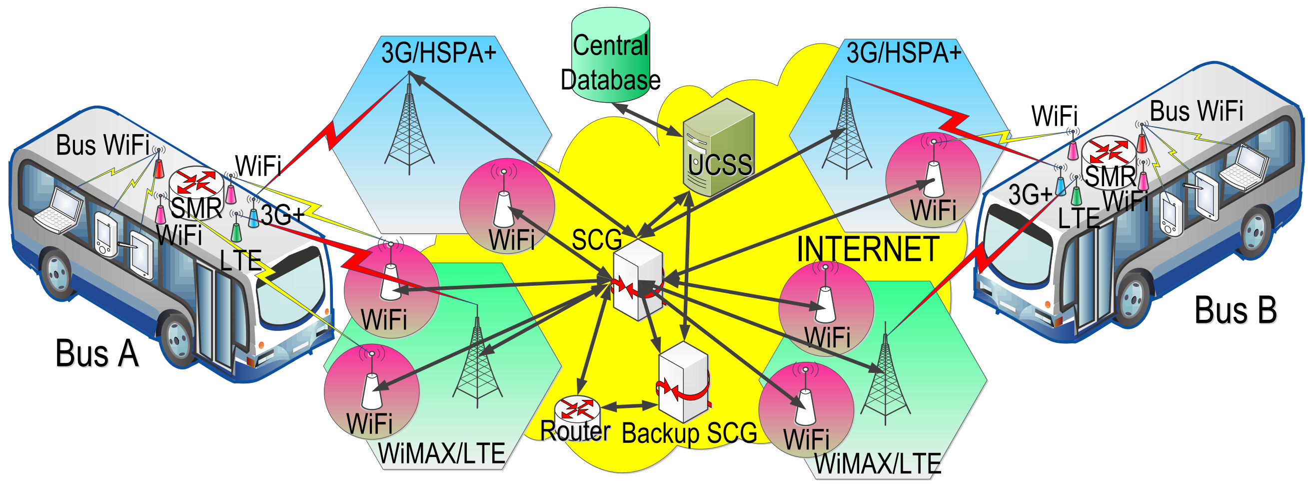

Fig. 1. System architecture.

nectivity platform. The design and implementation principles of the main mechanisms are also discussed within the paper.

This paper is structured as follows: Section II proposes the system architecture providing ubiquitous connectivity for the passengers of the public transport. Section III presents the functional architecture the of the connectivity system entities. Section IV discusses the platform architecture of the connectivity system and the integration issue of the software modules composing this architecture. Section V presents the design and implementation of the main mechanisms necessary for the seamless connectivity provisioning while Section VI presents several experimental tests performed to validate the proposed platform architecture. Finally, Section VII concludes the paper.

II. System Architecture

The design of the system architecture has followed the principles used in designing the architecture of NGN wireless networks, like the LTE-SAE networks. Shortly these principles are [16] [17]: flat architecture with a reduced set of entities, high level of scalability, simple QoS model, efficient usage of the radio resources, cost efficient deployment.

The system architecture presented in Figure 1 is composed of three main entities: the Smart Mobile Router (SMR), the Service Continuity Gateway (SCG) and the Ubiquitous Connectivity Support Server (UCSS). The last two entities form the Application Server Platform (ASP) which is a fixed infrastructure offering support for the implementation of the ubiquitous connectivity system. Open coupling between the networks composing the heterogeneous networking environment is considered, which allows fast and cost effective deployment.

The SMR installed in the public transportation vehicle offers Internet access to the devices located in the vehicle. The WLAN access allows the passengers of the vehicle to connect to the SMR and further on to the Internet. Access control and authentication functions are integrated into the SMR. The SMR is equipped with several wireless interfaces being capable of connecting in the same time to several wireless networks in order to make use of the transmission resources offered by all these networks and to implement the ubiquitous connectivity concept.

The SMR integrates the intelligence necessary for selecting the target network for handover and load balancing operations, i.e. for switching the service flows on the IP tunnels instantiated in different wireless networks in the condition of fulfilling the QoS requirements of the services. The SMR has also integrated the capabilities for acquiring, measuring and processing the network and service flow parameters and for reporting this information to the central database.

The ASP assists the SMRs in providing ubiquitous connectivity and load balancing over several wireless networks using the same or different transmission technologies. The UCSS entity gathers, processes and stores the context information (CI) received from the SMRs. The information stored in the central database, accessible for all SMRs, allows each SMR to have a global picture on the networking environment. Based on this information each SMR will be able to take better, i.e. more efficient, handover and load balancing decisions. Distribution of the centralized and processed context information to the SMRs is controlled also by UCSS, by using protocols which communicate continuously with the SMRs. The intelligence incorporated in the SMR also allows the execution of the handover and load balancing operations based only on local measurements if the UCSS cannot offer the context information.

The ASP also implements the service continuity by managing and switching the IP tunnels opened by the SMRs. The SCG entity is working closely with the SMRs and assists these entities in offering ubiquitous connectivity in a heterogeneous wireless network. A second role of the SCG consists in assisting the SMRs in performing active measurements of some parameters like available transfer rate (ATR), delay, latency, etc. Some measurements of the service flow parameters could be performed also by the SCG entity.

The proposed system architecture allows to combine into one single process the handover and load balancing operations in heterogeneous networks owned by the same or different operators and using the same or different wireless access technologies. This leads to a better connectivity and implicitly an improved user experience in a vehicular scenario.

III. Functional Architecture

Based on the analysis of technical and non-technical requirements which have to be fulfilled by the SMR in order to provide seamless connectivity to the passengers of the public transport two high level sets can be identified:

- Functional requirements: connectivity and mobility, interoperability, security, authentication and accounting, scalability, portability.
- Non-functional requirements: health effects, usability.

In order to fulfill the enumerated functional requirements, the architecture depicted in Figure 2 is proposed for the SMR, called hereafter functional architecture. The subsystems of this architecture can be organized into seven categories as follows: decision, execution, operation support, data storage, communication, authentication and configuration subsystems. Each of these subsystems includes one or several functional modules and sub-modules.

The decision entity of the functional architecture is the Handover and Load Balancing Manager Subsystem which includes the Handover (HO) Decision Module and the Load Balancing (LB) Decision Module. The first one controls the vertical handover process between different wireless technologies. It decides about the handover initiation moment and selects the target network. The second module controls the load balancing operations in heterogeneous wireless networks, having as target the increase of the wireless resources usage efficiency and the user satisfaction. This module selects the networks which are involved in load balancing and identifies the data flows that have to be sent to each network. The HO and the LB Decision modules are inter-related, the load balancing operations representing a particular case of handover, when only some data flows are handed over from one network to another and not the entire aggregated flow. The HO and LB decision modules use as input the acquired network state information (NSI) and traffic related information.

The execution entity is the Connection and Mobility Manager (CMM) Subsystem, which performs the handover and load balancing operations by rerouting data flows from one operator/wireless interface to another one. This subsystem is represented by the Handover and Load Balancing Execution Module and the NAT Control Module (NAT-CM). The first module selects and switches data flows between IP tunnels using various wireless Internet Service Providers (ISP), based on the commands issued by the HO & LB Manager Subsystems. The second module is in charge with creating new logical IP tunnels using available operators as carriers. This action supposes that a set of signaling messages has to be exchanged between the SMR and the SCG.

The operation support entity is the Context Information Manager Subsystem, which includes all the modules which are dealing with the acquisition of the network state and service related information and the storage of this data. The communication entity is the Information Forwarding Subsystem, which acts as a communication switch and allows the modularization of the SMR architecture and an easy integration of subsystems performing different operations.

The configuration entity is the Configuration Interface Subsystem, which allows the system administrator to specify the policies controlling the HO and LB operations and the QoS requirements of the services offered to the passengers of the bus. The data storage entity is the Local Database (LD) Subsystem which has the role of storing the NSI and service related information acquired by local measurements, as well as the communication context information downloaded from the Central Database (CD) Subsystem.

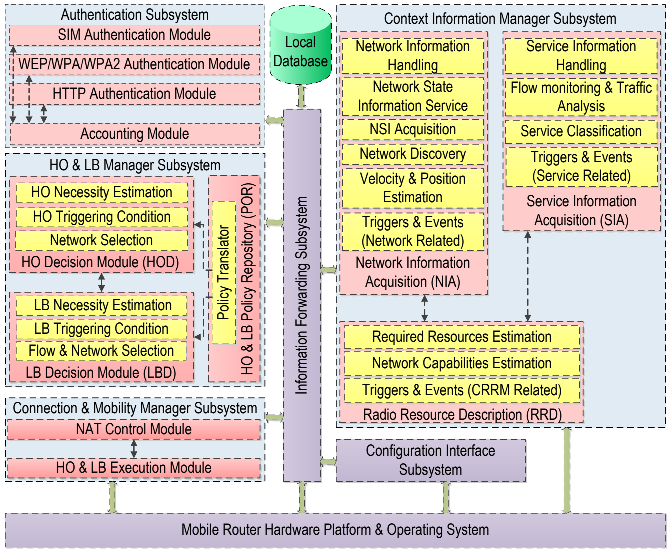

Fig. 2. Functional architecture of the SMR.

The Authentication Subsystem allows the SMR to get authenticated and authorized in different operator's networks which are used to connect to the Internet. As such, it implements the authentication clients needed for every envisaged type of network (2G/3G/4G/WiFi).

The functional architecture of the SCG is similar to that of the SMR's architecture, the main differences consisting in the lack of the HO & LB Manager Subsystem and of the Authentication Subsystem. No decision is taken by the SCG concerning the HO and LB operations and the Context Information Manager Subsystem has a simplified structure, it only offering support to the SMR in performing active measurements.

The functional architecture of the UCSS has a simpler structure and includes only the Context Information Manager Subsystem and the Authentication Subsystem. This entity has only two roles: to authenticate the SMRs and the users of the SMRs and to offer support for the SMRs in taking their routing decisions, but this decisions also can be taken without the intervention of the UCSS.

IV. Platform Architecture

A. *Smart Mobile Router Platform Architecture*

The SMR can be implemented on an embedded microcomputer, which has the processing and storage capabilities necessary for performing the operations requested by the ubiquitous connectivity system. The microcomputer must have interfacing capabilities with a high number of wireless network cards as well as low energy consumption. The hardware design of the microcomputer has to provide robustness to mechanical vibrations. The operating system (OS) running on the microcomputer is a minimal Linux OS including only the libraries necessary for the operations performed by the SMR.

The platform architecture is represented by the software architecture of the SMR shown in Figure 3. The software modules are running in the OS user space and are requesting various operations from the OS. The mapping of the SMR's functional architecture subsystems and modules, see Figure 2, on the software architecture is also presented in Figure 3.

The HO & LB Manager Subsystem, the Connection & Mobility Manager Subsystem, the Authentication Subsystem and the Configuration Interface Subsystem map on individual software modules. In the case of these subsystems no functional sub-modules exist or if they exist, e.g. the Handover Decision Module and the Load Balancing Decision Module of the HO & LB Manager Subsystem, they are strongly correlated and integrated into a single software module.

Differently from the previously mentioned functional subsystems, the Context Information Manager Subsystem maps on several software modules of the platform architecture. Four monitoring software modules can be identified, which are dedicated to the monitoring of the wireless (WiFi and 2G/3G/4G) interfaces, the GPS receiver and the data flows. Besides these modules a Local Database & Context Information Handler module and a Database module exist.

Each of the network monitoring software modules performs NSI acquisition, network discovery and network resource measurement and estimation. Each of them integrates sub-modules of the Network Information Acquisition & Radio Resource Description functional modules of the Context Information Manager Subsystem. The Velocity & Position Estimation functional sub-module maps on the GPS Module, while the Service Information Acquisition functional module maps on the Traffic Monitoring Module of the software architecture.

The Network Information Handling, the Service Information Handling and the Network State Information Service submodules of the Context Information Manager Subsystem are mapped on the Local Database & CI Handler software module of the platform architecture. This software module handles and stores the NSI and traffic information in the Local Database (LD) and controls the information exchange between the LD and the Central Database of the system.

The hardware monitoring module allows the identification of potential operational issues or malfunctioning.

The interaction between the modules is controlled by the Interoperability Module which is the instantiation of the Information Forwarding Subsystem of the functional architecture.

The design of the SMR's software architecture and the proposed mapping of the functional architecture on the software architecture is based both on functional and non-functional criteria. By identifying the functionality of different software modules a more efficient usage of the hardware resources is possible. Different priorities and execution time constraints could be identified for software modules executing different tasks. The monitoring modules have to be able to quickly detect any changes in the network state or in the functioning of the hardware. The software modules implementing the routing operations in heterogeneous networks have to react promptly to the commands generated by the decision blocks in order to avoid supplementary delays of the data packets or packet losses due to the handover operation. The software modules implementing decision operations have to be proactive, i.e. capable of predicting changes in the network or system state what makes them less time dependent. The same is the situation with the software modules performing the context information handling and storage, these operations having less stringent time constraints.

The non-functional criteria are related to the portability of the SMR platform. The software modules performing decision and context information handling are independent of the OS and the hardware used. The modules performing the routing depend on the OS while the modules performing monitoring operations depend both on the OS and the hardware used.

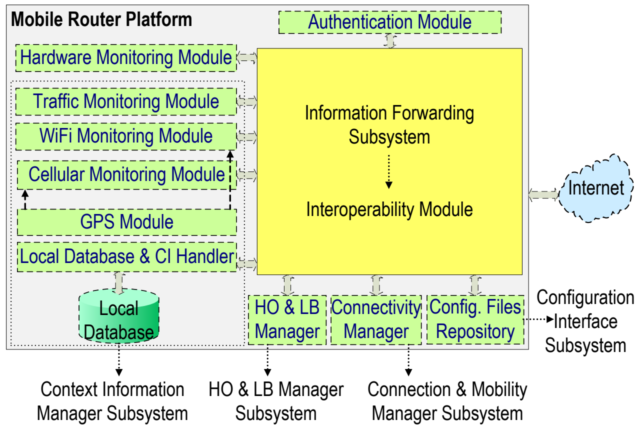

Fig. 3. Smart Mobile Router platform architecture.

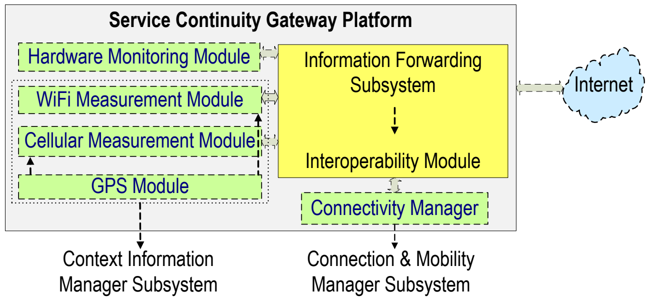

Fig. 4. Service Continuity Gateway platform architecture.

B. Service Continuity Gateway Platform Architecture

The SCG is implemented on a high performance computer, which has the processing and storage capabilities necessary for ensuring the service continuity to a large number of SMRs moving in a heterogeneous networking environment and performing HO and LB operations. The SCG is connected to the Internet through several Gigabit Ethernet links.

The platform architecture of the SCG, presented in Figure 4, includes the following software modules:

- The Connectivity Manager Module which implements the routing operation necessary to maintain the connectivity when the traffic is switched from one wireless connection to another. It is controlled by the SMR.
- The WiFi and the 2G/3G/4G Measurement modules which works together with the WiFi and 2G/3G/4G Monitoring modules of the SMR in order to perform active measurements of the wireless links parameters.
- The GPS Module used for synchronization purposes.
- The Hardware Monitoring Module which performs monitoring of the SCG hardware functioning.
- The Interoperability Module which implements the communication between local and remote modules.

In what concerns the mapping of the SCG's functional architecture on the software architecture we have a situation similar to that of the SMR.

C. Ubiquitous Connectivity Support Server Platform Architecture

The platform architecture of the UCSS is presented in Figure 5, and it includes besides the Interoperability Module the following modules:

- The Central Database and CI Handler Module which implement the protocols used to gather the information from the SMRs and to distribute this centralized information to all SMRs which need it.
- The Central Database (CD) which stores the CI acquired from all SMRs
- The Authentication Module which represents an Extended - Radius Server. This Radius Server is in charge of maintaining the whole authentication system for users public access, as well as the accounting necessary for SMRs to be controlled on their foreign access to different operator's networks.

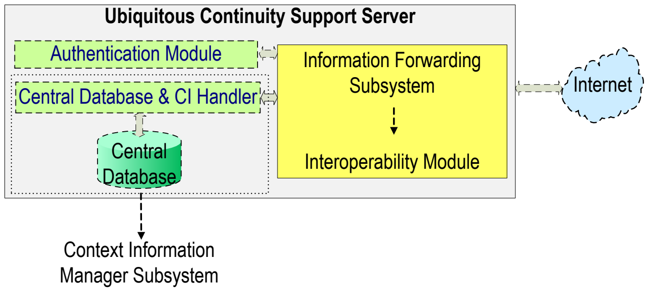

Fig. 5. Ubiquitous Connectivity Support Server platform architecture.

D. *Software Modules Integration*

The principles of the proposed integration methodology are the following:

- Identify the software modules which run distinctive processes.
- Identify the interaction between the software modules and the data structures exchanged.
- Define and develop a flexible and reliable inter-module communication mechanism, capable to implement data communication between modules running both on local and remote machines or devices.

The rules governing the data exchange between the local and remote modules of the platform are the following:

- All NSI and traffic monitoring data (i.e. CI data) are stored in the Local Database of the SMR. These data are continuously refreshed by the monitoring processes. The acquired CI data are not sent directly to the decision algorithms, being simplified the communication and the synchronization between the monitoring and decision modules.
- The Local and the Central Database are exchanging CI based on algorithms implemented by the CI Handler module. The CI exchange takes place in both directions, i.e. each SMR uploads it's new measurements in the CD and the CI Handler distributes the new CI to all SMRs. This process runs in parallel with the local monitoring and measurement of the NSI and traffic parameters. All CI exchange and acquisition processes are synchronized in order to avoid conflicts in accessing the Local Database.
- The monitoring modules generate specific triggers which are sent to the HO & LB Manager. In this way the decision algorithms are aware of important events. In such moments the decision algorithms must analyze the new data available in the Local Database and take decisions accordingly.
- The active measurement modules running on the SMR and SCG are exchanging active probes and the results of these measurement processes are stored in the Local Database of the SMR.
- The HO & LB Manager takes decisions on the network to be used for each data flow and these decisions are communicated to the Connectivity Manager. The Connectivity Manager maintains the routing of a given flow until this flow exists or the HO & LB Manager does not take another decision.
- The HO & LB Manager sends to the Network Monitoring Module information concerning the preferred / default networks and the connection setup/release commands based on the analysis of the NSI.
- The modules implementing the Connectivity Manager on the SMR and the SCG are exchanging signaling messages in order to maintain the virtual tunnels over the heterogeneous wireless network and to route each flow on the tunnel decided by the HO & LB Manager.

A map of the data exchange between the local and remote modules is presented in Figure 6, being identified the different types of messages exchanged.

V. Mechanism Design and Implementation

This section presents the design and implementation of the main mechanisms integrated in the presented platform architecture, but it is beyond the scope of this paper to go into all the details concerning the design and implementation of particular mechanisms. Only the mechanisms which represent a basic component of the platform will be discussed.

A. *The Interoperability Mechanism*

This mechanism is needed to permit flexible message exchanging between multiple modules that are working together to achieve the ubiquitous connectivity. As it is depicted in Figure 6 this module forwards messages destined for both local modules connected to it and remote modules connected to a similar Interoperability Module on a different device that has network connectivity. This mechanism allows fully exploiting the modular design of the platform architecture. It also allows replacement or upgrading of the existing mechanisms without being necessary changing the mechanisms which are interacting with the ones being upgraded.

Each software module that needs to communicate with other ones must have a unique ID within the platform. Same software module types that are running on different devices can have the same ID.

After a software module connects to the Interoperability Module, the first step that must be performed is to send its unique ID. From that moment any other module can exchange messages with the current one. Exchanged messages between modules must have the following format:

<dest_IP>,<dest_ID>,<src_IP>,<src_ID>,<Message>

If the message is destined to a local module (running on the same device), the <dest_IP> and <src_IP> fields must have the value: "local". Otherwise, the values should be set according to specific IP addresses on both source and destination hosts. After receiving a message a confirmation code will be sent back from the Interoperability Module to the source module.

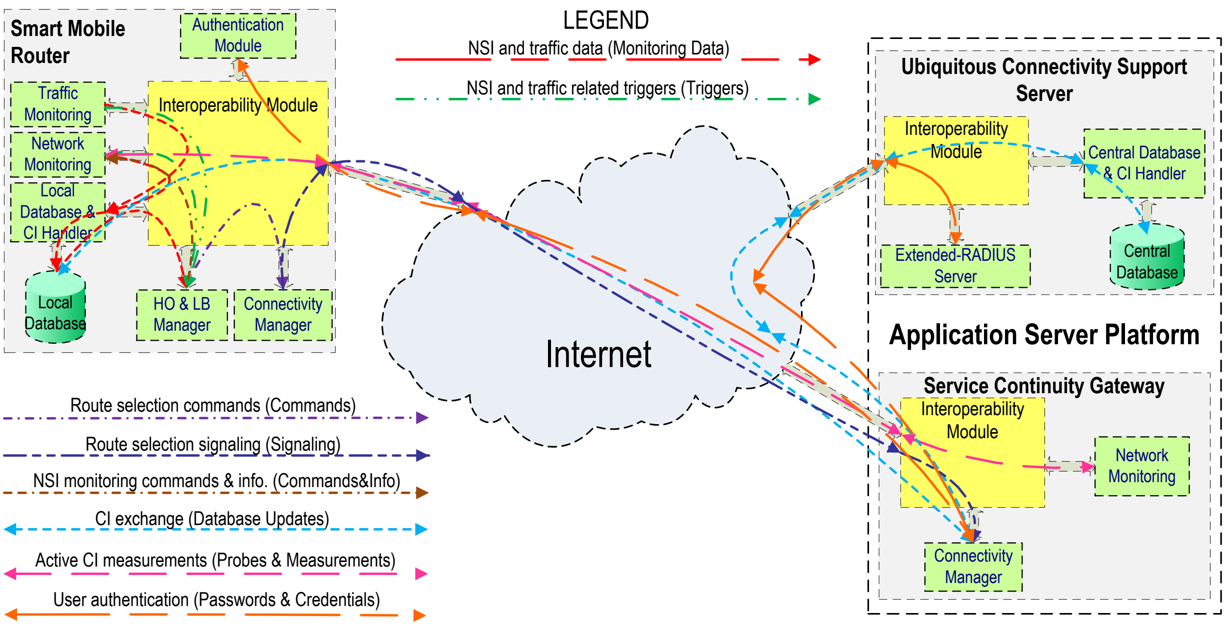

Fig. 6. Data exchange between local and remote software modules of the platform architecture.

For optimization reasons the Interoperability Module is composed of multiple threads (see Figure 7), each one with its own functionality. For each connected module a dedicated thread (Port Thread) is created in order to handle the communication. Thus, within this thread messages will be received, processed and sent to the corresponding destination. If the received message must be sent to another device on the Internet a Network Send Thread, that connects to the remote Interoperability Module in order to forward the message, will be automatically created. For receiving messages from the Internet the Network Receive Thread, that acts as a TCP server, is enabled. For each connected software module a separate handling thread (Peer Thread) is created only for the time the connection is active. The Menu Thread is responsible with the user interaction.

B. Network State Information and Flow Parameter Acquisition

This mechanism gathers the network and traffic parameters by passive and active monitoring operations, pre-processes this information and finally stores it in the local database of the SMR according to the process flow presented in Figure 8.

The NSI acquired from the wireless interfaces, WiFi and cellular, can be grouped in three main categories: link parameters (e.g. signal strength, SINR, etc.), traffic parameters (e.g.

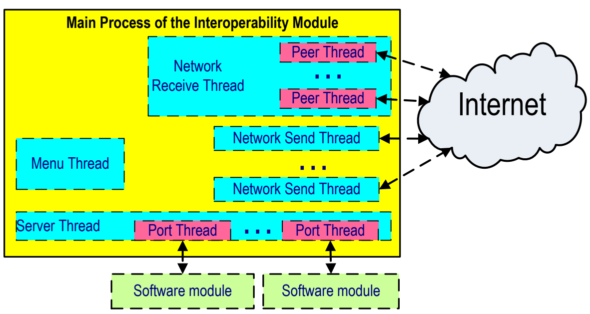

Fig. 7. Architecture of the Interoperability Module.

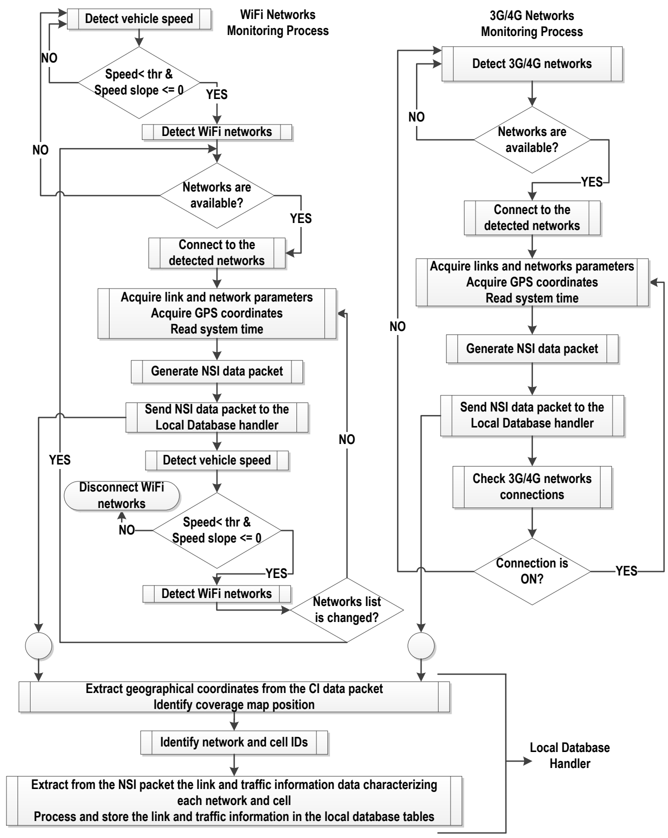

Fig. 8. WiFi and 2G/3G/4G network state information acquisition and handling.

transmitted/received packets, traffic class, etc.) and network parameters (e.g. Service Set Identifier, operator name, etc).

The WiFi networks are used for providing connectivity only if the speed of the vehicle carrying the SMR is smaller than a given threshold (e.g. 2 - 3 m/s) due to the lower coverage and slower link adaptation capabilities of these networks. Establishing connectivity with these networks is also a more complex process because a larger and variable number of access points could be available in a given geographical area.

It can be seen from Figure 8 that the LD stores practically a coverage map of the geographical areas visited by the SMR.

Monitoring of the WiFi network's parameters is based on the functions offered by the *iw* tool integrated in Linux operating system, which is running on the connectivity platform. This tool includes specific commands for monitoring and interacting with the WiFi interfaces. The Linux OS offers also a virtual file system, */proc/net/wireless*, which stores several parameters of the active WiFi links. The data stored in this virtual file can be accessed with standard Linux commands. Using a specific set of functions offered by Daemon programs, like the *wpa supplicant*, represents another alternative.

Monitoring of the cellular interfaces can be achieved by using specific AT commands sent to the interface and by analyzing the standard output replies generated by the OS as a response to these commands. Another solution to monitor the cellular interfaces is the use of the QMI (Qualcomm Mobile Station Modem Interface) protocol which is designed for interfacing between the Mobile Station Modem and the attached Terminal Equipment. The QMI protocol defines multiple services, each action requested from the modem being part of a service.

C. Flow Monitoring and Traffic Analysis Mechanisms

The data traffic which has to be routed through the SMR is first differentiated into individual application flows by a specific mechanism and the parameters of these flows are measured. The main operations performed are the following:

- Flow recognition: An application flow is classified based on the 5-tuplet IP header of each packet arriving at the SMR. The 5-tuplet IP header is built from the following IPv4 fields: IP source address, IP destination address, Layer 4 protocol number, source port and destination port.
- Real-time traffic accounting: Every flow is split into two simplex flows and each direction is registered to a combined byte/packet accounting infrastructure. Both upload and download rates of each flow are computed periodically by reading the per-flow accumulated bytes and the monitoring inter-read duration.
- Flow selection and exporting: The majority of the flows which travel through a router are short-lived, bursty flows (i.e. web traffic, DNS queries, ARP requests etc.). Because the flow recognition method is very accurate, the number of such detected flows grows very fast and in general is very dynamic. While it is perhaps possible to export and use the statistics collected from every such flow, it is more practical to consider only relevant flows for HO & LB decisions. In order to achieve this goal, the bursty and short-lived traffic will be grouped as one single flow (the default flow) and only flows which live longer than a certain minimum amount of time (e.g. a few seconds) and which use a minimum defined quantum of the capacity of the link will be exported as individual flows. This limits the number of the exported flows (and their associated rate statistics) which will be sent to the LD Module. Thus, the Flow Capture & Traffic Analysis module keeps track of every individual flow at a fine-grained level, but it selects only relevant flows to be exported and subsequently used by various policy-based routing algorithms. This process takes place both in uplink and downlink.
- Flow management: If a TCP connection ends or if, for a specific flow, no packets are received for a certain period of time that flow will be deleted automatically from the connection tracking system. The Flow Monitoring Module is able to react instantly to NEW and DELETE flow events and updates the local database flow entries accordingly.

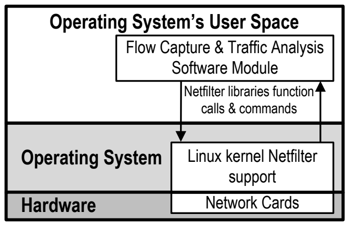

Fig. 9. Application flow monitoring. Implementation details.

The implementation of the Flow Monitoring and Traffic Analysis Mechanisms is based on the *libnetfilter_conntrack* library. This code is built on top of the Netfilter framework and extends the information provided by the packet header by providing and maintaining a connection state. The latter enables a software application to define intelligent filtering policies which take into account the state of a connection or its related packets. By hooking the Flow Monitoring Module to the connection tracking system, each NEW or DELETE flow event is received in real-time, together with additional relevant information (the 5-tuple IP header, connection state and so on).

Flow accounting (i.e. keeping track of per-flow accumulated bytes and packets) is implemented using the *libnetfilter_acct* library. The accounting framework works at the kernel level and can register unique flow names as objects associated with bytes and packet counters. Some implementation details of this mechanism are presented in Figure 9.

D. Local and Central Database Update Mechanism

The Ubiquitous Connectivity Support Server has the role of gathering the communication context information from a large number of SMRs. This information is generated in different geographical positions at unsynchronized moments in time and characterizes several wireless networks using different technologies and owned by different operators. The context information exchange process between the SMR and the UCSS is presented in Figure 10 and has 4 main steps, as follows:

Step 1. At the starting point of the route the SMR downloads from the central database the context information (network and traffic parameters) related to the route which will be followed. This information includes the coordinates of the points which are going to be visited, the data about the available operators and different measurement results.

Step 2 . The measurement reports generated by the SMR must be centralized on the UCSS. In order to make the signaling operations more efficient and avoid sending continuously management information, the SMR checks if the local measurements are different than the ones stored in the local database and if the difference is above a given threshold. If so, the SMR will send the new data to the UCSS to be stored into the central database.

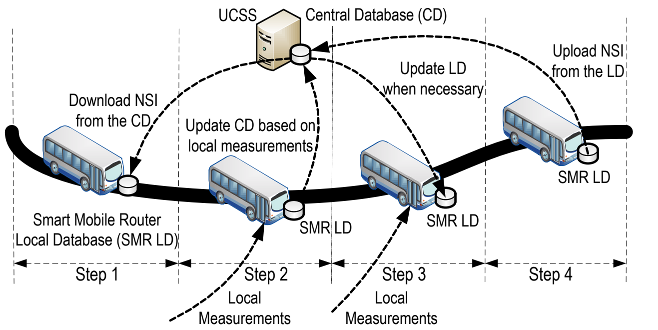

Fig. 10. Context information exchange mechanisms between SMR and UCSS.

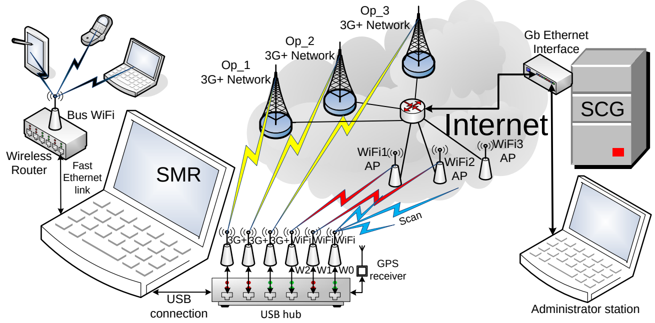

Fig. 11. Architecture of test connectivity platform.

Step 3. The UCSS analyzes the information received from all the SMRs connected to it. If an important change is detected, which affects some SMRs that are going to visit the affected map positions, updates of that SMRs LD will be performed based on the data stored in the CD.

Step 4. At the end of the route the SMR updates the central database of the system with the results of the measurements performed during its journey.

The parameters of the above presented mechanism for context information exchange have to be tuned to reduce as much as possible the signaling traffic and the usage of the network resources needed to transport the CI data. It has to be underlined that the local - central database updates take place in parallel with the VHO & LB decision process and the previously described phases of this CI management process are initiated by triggers generated by the CI Handler Module.

E. The Decision Mechanism Design

The platform architecture described allows the integration of decision mechanisms having different capabilities, complexities and performances. Depending also on the computation capabilities and available memory of the hardware implementing the SMR the decision mechanisms used can implement only "simple" VHO operations, i.e. selection at a given moment of the best network, or more complex load balancing, i.e. bandwidth aggregation, operations capable to exploit the transmission resources available in a heterogeneous networking environment. In order to offer this flexibility the decision mechanism has to be separated from the monitoring and switching/routing functionalities of the platform. The decision mechanism acts based on a limited but carefully selected network and traffic parameters stored in the local database. In this way changes of the wireless interfaces or of the APIs permitting the access to these interfaces have no effect on the decision process and the upgrading of the decision process doesn't require the alteration of the network and flow monitoring processes. Also, the decision mechanism is an event based one, meaning that it reacts to triggers generated by the network and traffic monitoring modules or by dedicated timers. The commands generated by the decision process establishes for each 4 tuple of source & destination IP address and source & destination port which is the operator network to be used and this information is sent to the Connectivity Manager which performs the routing.

F. The Mobility Management Mechanism Design

Depending on the complexity of the decision process, i.e. only VHO or LB operations are performed, and on the coupling between the heterogeneous networks different mobility management mechanisms can be used, like Mobile IP [18], SIP [19] or *iproute* tool based [20] mechanisms. The proposed mechanism receives from the decision mechanism the list of flows and the wireless networks and takes appropriate actions in order to route each flow on the selected network.

An alternative solution, integrated in the described platform architecture and tested, is represented by the use of Virtual Private Network (VPN) tunnels created between each SMR and the SCG, through all available operators and access networks. This mechanism forwards through these VPN tunnels, based on the decisions taken by the HO & LB Manager Mechanism, the flows detected by the Flow Monitoring Mechanism. These tunnels are created using the *OpenVPN* software.

To forward data packets to any destination on the Internet, appropriate default route must be inserted into the routing table. Because multiple operators are used at the same time (i.e. different data flows might use separate ISPs) if LB operations are implemented multiple default routes need to be inserted into the routing table, but this requirement is impossible to address. The solution is to create multiple virtual routing tables, one for each available connection, having as default route the route through the tunnel deployed over the corresponding operator network.

The last step is to specify what virtual routing table to be used for each flow that is arriving at the SMR. This can be achieved with the *iptables* tool available in Linux that can attach a mark to any packet that has a specific set of properties (i.e. source and destination IP address, source and destination port and transport protocol used). The whole process must be performed both on the SMR and the SCG, so that the settings are consistent on both devices.

VI. Architecture and Mechanisms Design Evaluation

This section presents a few experimental tests performed to check the functionality of the developed architecture and the correct functioning of the subsystems and modules of the platform. The tests were performed both in low and high speed conditions and the complexity of the decision algorithms used is a medium one, the goal being the validation of the architecture and not the development and testing of complex decision algorithms. The architecture of the test platform, presented in Figure 11, is in line with the proposed system architecture.

The SMR is represented by a laptop computer running Fedora Core 18 OS. A wireless router (Bus WiFi) attached to the SMR through a Fast Ethernet connection represents the local WiFi access point of the bus. A GPS receiver, three WiFi and three 3G+ wireless interfaces are connected to the USB ports of the SMR. The SCG and the UCSS run on a server connected to the internet through a Gb Ethernet connection. Another laptop computer connected to the server is used to remotely control the SCG and the UCSS.

The heterogeneous networking environment is represented by three 3G networks and by three WiFi networks. Each of the 3G+ interfaces connects to a separate 3G operator network. One WiFi interfaces (W0) is used only for scanning operations, while the other two WiFi interfaces (W1 and W2) can connect to any of the WiFi networks (see Figure 11).

A. The Low Speed Test

The low speed test involves only the WiFi networks (802.11g) and can be shortly described as follows:

1. The WiFi Access Points (AP) were installed in two buildings in a university campus and the SMR, installed on a pushcart, was slowly moving in the area covered by the WiFi APs.
2. The W1 and W2 WiFi interfaces used for data transmissions connect to the WiFi APs which generate the strongest signals. The Received Signal Strength (RSS) parameter is obtained by the scanning operation performed by the WiFi interface (W0) dedicated to network scanning.
3. If the normalized Link Quality Indicator (LQI) of any active link goes below an imposed threshold (0.4 in our test) then go to Step 2, and reselect the WiFi networks used.
4. If only vertical handover (VHO) operations are performed all data flows are handed over to the network having the link with the largest LQI.
5. If LB operations are performed the link with the largest LQI is selected as default link and all the new flows are initially routed through this link. Data flows which exceed some imposed rate (64kbps) and duration (30s) thresholds are handed over to the link or links having smaller LQI. In this way the default link will transport the short-lived flows, Web browsing and SMR - UCSS signaling flows, while flows with longer duration are routed on the other link or links.

In Table I the network (AP, RSS, LQI) and traffic (Available Transfer Rate-ATR, Speed Test Rate-STR) parameters measured in 10 test points (TP) by interfaces W1 and W2 when only VHO operations were performed are presented. In test points 1-4 and 9-10 interface W1 connects to AP1, while in test points 5-8 it connects to AP3. Interface W2 connects only to AP2 and since it has in all test points the largest LQI it is selected as VHO target in all points and the speed test traffic goes through it.

A second test involves LB operations as it was previously described. The SMR travels on the same route and passes through (approximately) the same test points. The values of the measured network and traffic parameters are similar to the ones presented in Table I and the WiFi interfaces connect to the APs in the same way. The test flows are represented by 10 video streams having an average rate of 780kbps. These flows were generated by two laptop computers connected to the SMR. As in the previous experiment the W2 interface is selected the default one and the systems tries to switch the data flows on the other connection, allowing to use the default interface for Web browsing (one of the most popular application) and SMR-SCG signaling. The usage ratios of the W1 and W2 WiFi links (defined as data traffic/link capacity) measured in the test points are given in Table II.

TABLE I. NETWORK AND TRAFFIC PARAMETERS ACQUIRED DURING THE LOW SPEED TEST

	W1 interface				W2 interface			
TP	AP	RSS [dBm]	LQI [%]	ATR/STR [Mbps]	AP	RSS [dBm]	LQI [%]	ATR/STR [Mbps]
1	1	-73	52	7.4/NA	2	-65	64	9.5/8.7
2	1	-78	45	6.0/NA	2	-80	46	6.1/5.6
3	1	-77	47	6.2/NA	2	-78	51	6.6/5.7
4	1	-70	55	8.1/NA	2	-66	61	8.9/8.1
5	3	-69	58	5.0/NA	2	-65	64	9.2/8.2
6	3	-69	58	5.2/NA	2	-61	72	10.1/9.3
7	3	-63	67	6.2/NA	2	-61	71	9.8/9.1
8	3	-79	44	2.7/NA	2	-67	61	9.1/8.2
9	1	-69	61	8.2/NA	2	-67	61	9.3/8.5
10	1	-77	47	6.0/NA	2	-75	50	7.1/6.4

The performed tests show that: monitoring of WiFi networks and handling of the context information, handling of the WiFi interfaces and switching of flows from one connection to another one according to the commands issued by the decision algorithm are working; the monitoring, decision and mobility management modules are interacting as expected. In conclusion the proposed architecture is fully functional in low mobility conditions.

B. The High Speed Test

The high speed test involved only 3G networks and it took place in a hilly area where the 3G coverage is discontinuous for all operators. Figure 12 presents the geographical area where the test took place and also gives the coverage for one of the 3G operator which took part in the experiment. During this test only VHO was operations were performed and the steps taken can be shortly described as follows:

1. Each 3G interface connects to a different network.
2. VHO operations are initiated only if the value of the normalized RSCP (Received Signal Code Power) and/or the EcIo (Energy of CPICH pilot over Interference; CPICH Common Pilot Channel) parameter goes below an imposed threshold (0.4 in our test). This has the effect of reducing the number of handovers and the signaling traffic required.
3. The preferred/target network is selected based on a simple utility function, U, given by:

$$U = w_{RSCP} * RSCP_{norm} + w_{EcIo} * EcIo_{norm}$$

where $w_{RSCP} = w_{EcIo} = 1$. The network which has the largest utility function is selected as the preferred one.

The network and traffic parameters measurement results are presented in Table III. More exactly it is about the normalized RSCP and EcIo parameters of the 3G networks measured in some test points. These points (placed approximately on the coverage map see Figure 12) identify the areas where around 90% of the time one of the operator network was selected as preferred one. For normalization of the network parameters, P, the max-min method was used: $P_{norm} = \frac{P - P_{min}}{P_{max} - P_{min}}$.

TABLE II. WIFI LINKS USAGE RATIO OBTAINED IN THE LB TEST

TP	1	2	3	4	5	6	7	8	9	10
W1 [%]	94	91	88	96	93	90	88	86	95	91
W2 [%]	8	39	35	0	33	30	31	60	0	32

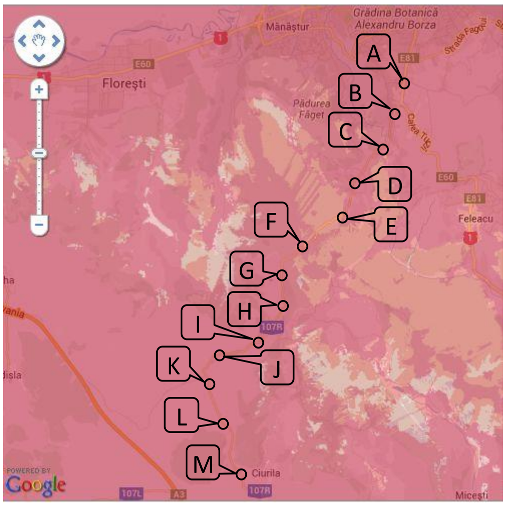

Fig. 12. High speed test geographical area and 3G network coverage.

TABLE III. NETWORK AND TRAFFIC PARAMETERS ACQUIRED DURING THE HIGH SPEED TEST

TP	3G-1 interface		3G-2 interface		3G-3 interface		STR [Mbps]
	RSCP	EcIo	RSCP	EcIo	RSCP	EcIo	
1	**0.774**	**0.666**	0.849	0.666	1	0.833	2.26
2	0.749	0.366	**1**	**0.9**	0.737	0.733	2.11
3	0.499	0.266	0.787	0.2	**0.749**	**0.866**	3.13
4	0.849	0.666	0.899	0.833	**0.724**	**0.666**	3.66
5	1	0.733	**0.912**	**0.866**	0.587	0.4	4.12
6	0	0	0.624	0.566	**0.799**	**0.833**	3.55
7	0.549	0.333	**0.65**	**0.733**	0.461	0.4	4.09
8	0	0.033	0.374	0.833	**0.399**	**0.866**	3.42
9	0	0	**0.449**	**0.866**	0.362	0.833	3.95
10	0	0	0.336	0.766	**0.362**	**0.766**	1.14
11	0	0	**0.374**	**0.833**	0.399	0.766	0.38
12	0	0.233	**0.814**	**0.9**	0.646	0	0.56
13	0	0	**0.762**	**0.833**	0.929	0	1.65

The text with boldface identifies in each test point the preferred network used fort transmission. Zero value RSCP means that no coverage was detected for a given 3G network.

The performed tests show that: monitoring of 3G networks and handing of the context information, handling of the 3G interfaces and switching of flows from one 3G connection to another one according to the commands issued by the decision algorithm are working; the monitoring, decision and mobility management modules are interacting as expected. In conclusion the proposed architecture is fully functional in high mobility conditions as well.

VII. Conclusion

The paper proposes an architectural design of a seamless connectivity system for public transportation. The connectivity system has as main characteristics the joint usage of vertical handover and load balancing operations in heterogeneous networks and the open coupling between the networks, which allows fast and cost effective deployment. The proposed system and functional architecture designs are adapted to the mentioned characteristics of the connectivity system. By mapping the subsystems and modules of the functional architecture on the hardware components envisaged to be used the platform architecture of the connectivity system is developed.

The proposed platform architecture offers a modular design capable to integrate easily changes in the algorithms and in the operation mode of the functional modules. In order to fully exploit this modularity and flexibility a dedicated Interoperability Module was designed. This module manages the communication between the software modules of the platform architecture and allows hiding the internal operations of the interacting modules. In this way replacement or upgrading of the existing mechanisms/algorithms can be achieved without being necessary changing the mechanisms which are interacting with the ones being upgraded.

The paper also presents some design and implementation details of the main mechanisms integrated in the platform. The principles of the mechanisms dealing with context information acquisition and handling, implementation of the centralized information system, HO & LB decision respectively with mobility management are discussed.

Tests performed both in low speed and high speed conditions show without any doubts that the developed and implemented architecture is fully functional and that the subsystems and modules are interacting and exchanging data as it is expected. These tests validate also the functional decomposition of the system architecture which is a valid one allowing the correct functioning of the entire system.

Acknowledgment

The research leading to these results has received funding from the European Union's Seventh Framework Programme managed by REA-Research Executive Agency under grant agreement no. FP7-SME-2012-315161.

References

[1] Z.I. Kiss, A.B. Rus, V. Dobrota, A. Consoli, M. Egido, Z.A. Polgar, "Seamless Connectivity Platform Architecture for Public Transportation Software," *Proc. of 21st International Conference on Telecommunications and Computer Networks*, Primosten, 2013.

[2] F. Zarai, I. Smaoui, J-M. Bonnin, L. Kamoun, "Seamless Mobility in Heterogeneous Networks, " *International Journal of Next-Generation Networks*, vol. 2, no. 4, pp. 12–31, 2010.

[3] M. Garcia, J. Lloret, M. Edo, R. Lacuesta, "IPTV Distribution Network Access System Using WiMAX and WLAN Technologies, " in *Proc. 4th Edition of the UPGRADE-CN Workshop on Use of P2P, GRID and Agents for the Development of Content Networks*, pp. 35–44, Garching, 2009.

[4] Q.-T. Nguyen-Voung, L. Fiat, N. Agoulmine, "An Architecture for UMTS-WIMAX Interworking, " in *Proc. of 1st International Workshop Broadband Convergence Networks*, Vancouver, 2006.

[5] G. Lampropoulos, A. Kaloxylos, N. Passas, L. Merakos, "Handover Management Architectures in Integrated WLAN/Cellular Networks, " *IEEE Communications Surveys and Tutorials*, vol. 7, no. 4, pp. 30–44, 2006.

[6] F. Zhu, J. McNair, "Multiservice Vertical Handoff Decision Algorithms, " *EURASIP Journal on Wireless Communications and Networking*, vol. 2006, pp. 1-13, 2006.

[7] A. Hasswa, N. Nasser, H. Hassanein, "Tramcar: A Context Aware Cross-Layer Architecture for Next Generation Heterogeneous Wireless Networks, " in *Proc. of IEEE International Conference on Communications*, vol. 1, pp. 240245, Istanbul, 2006.

[8] L. Sarakis, G. Kormentzas, F. M. Guirao, "Seamless Service Provision for Multi Heterogeneous Access, " *IEEE Wireless Communications*, vol. 16, no. 5, pp. 32-40, 2009.

[9] A. Macriga, A. Kumar, "Mobility Management for Seamless Information flow in Heterogeneous Networks Using Hybrid Handover, " *IJCSNS International Journal of Computer Science and Network Security*, vol. 10, no. 2, pp. 61–70, 2010.

[10] A. Makris. (2008, August). An IEEE 802.21 based mobile assisted vertical handover algorithm. *KTH* [Online]. Available: http://www.ict.kth.se/courses/IK2555/ExamplePapers/A.Makris-WMNA-20080618.pdf

[11] M. Kassar, B. Kervella, G. Pujolle, “An Intelligent Handover Management System for Future Generation Wireless Networks, ” *EURASIP Journal on Wireless Communications and Networking*, vol. 2008, pp. 1-12,2008.

[12] ***, “*Handovers for Ubiquitous and Optimal Broadband Connectivity among Cooperative Networking Environments*, ”[Online], Available: http://www.ict-hurricane.eu/

[13] ***, “*Smart-Antenna Multimode Wireless Mesh Networks*, ”[Online], Available: http://www.ict-smartnet.eu/

[14] ***, “*Wireless World Research Forum*, ”[Online], Available: www.wireless-world-research.org/

[15] ***, “*Implementation of Ubiquitous Connectivity for Public Transport*, ”[Online], Available: http://idi.gowex.com/uconnect/index.html

[16] P. Beming, L. Frid, G. Hall, P. Malm, T. Noren, M. Olsson, G. Rune, “LTE-SAE architecture and performance,” *Ericsson Review*, no. 3, pp. 98–104, 2007.

[17] G. Fritze, “*SAEThe Core Network for LTE*, ”[Online], Available: www.3g4g.co.uk/Lte/SAE_Pres_0804_Ericsson.pdf

[18] C.E. Perkins, “Mobile IP,” *IEEE Communications Magazine*, vol. 40, no. 5, pp. 66–82, 2002.

[19] H. Schulzrinne, E. Wedlund, “Application - layer mobility using SIP,” *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 4, no. 3, pp. 47–57, 2000.

[20] B. Hubert, “Linux Advanced Routing & Traffic Control HOWTO, ”[Online]. Available: http://lartc.org/howto/index.html

Zsuzsanna Ilona Kiss is with the Communications Department of the Technical University of Cluj-Napoca, Faculty of Electronics, Telecommunications and Information Technology. She finished her bachelor, master and PhD studies at the same institution in 2008, 2010 and 2012. Her research interests include networking, heterogeneous networks, inteligent transportation systems and network coding techniques.

Andrei Ciprian Hosu is a PhD student in Telecommunications at the Technical University of Cluj-Napoca. He received his BSc. diploma in Electronics and Telecommunications in 2011 from the Technical University of Cluj-Napoca and a MSc. diploma in Telecommunications in 2013 from the same institution. He has been involved in the FP7 research project UCONNECT and his research interests include wireless heterogeneous networks and handover and load balancing algorithms.

Gabriel Lazar is with Technical University of Cluj-Napoca (Communications Department) since 2001, working on QoS in IP networks and Linux network administration. His current research program in networking includes work in the areas of real-time video streaming in heterogeneous IP networks, TCP-friendly applications and development of Linux traffic control mechanisms.

Andrei Bogdan Rus is Assistant Professor at the Technical University of Cluj-Napoca, Faculty of Electronics, Telecommunications and Information Technology since 2012, where he is involved in both didactic and research activities in the area of Communications Technologies. Dr. Rus received his Ph.D in 2011 in the field of Electronics and Telecommunications Engineering.

Virgil Dobrota holds Dipl.Eng. in Telecommunications (1987) and Ph.D. in Electronics and Telecommunications (1995) from Technical University of Cluj-Napoca. He is currently professor at TU Cluj-Napoca and Head of Communications Department, teaching switching and routing systems, Internet protocols and unified communications. Professor Dobrota was involved in RACE-MAGIC, INCO-COPERNICUS 1529, ACTS AC235, COST 290, FP7-4WARD, FP7-UCONNECT. Member of IEEE Communications Society, ACM SIGCOMM, he served as TPC Co-Chair at IEEE LANMAN 2007 and General Co-Chair at IEEE LANMAN 2008.

Zsolt Alfréd Polgár received Dipl.Eng. degree, M.Sc. and Ph.D. degrees in Telecommunications Engineering from the Technical University of Cluj-Napoca in 1995, 1996 and 2002, respectively. Since 1996 he is with the Communication Department of Technical University of Cluj-Napoca, where currently he is Associate Professor. His research interests involve error correcting codes, wireless networks, network coding and cooperative communications. He was involved in several COST actions and FP7 projects as team member and as local coordinator.