Monograph: New Trends in Network Management (published jointly with Novática*)
Guest Editors: Ramon Puigjaner-Trepat, Raouf Boutaba

2 Presentation. Network Management and Quality of Service — Ramon Puigjaner-Trepat and Raouf Boutaba

5 Application Oriented Network Management — Miquel Bordoy-Marcó, Jaume Prohens-Vadell, and Antonio Solana-Venteo

12 E2E Service Delivery through User Mobile Session Management — Noëmie Simoni, Chunyaing Yin, and Ken Chen

22 Secure Management of SCADA Networks — Cristina Alcaraz-Tello, Gerardo Fernández-Navarrete, Rodrigo Roman-Castro, Angel Balastegui-Velasco, and Javier López-Muñoz

29 Converting Computer Network Malicious Activity into Digital Footprints Based on a Notional Representation — Grigorios Fragkos

36 An Autonomic Architecture for Network Management and Control — Guy Pujolle


49 Users and Network Management for Secure Interworking and Roaming in WiMAX, 3G and Wi-Fi Networks Using RRI Architecture — Vamsi-Krishna Gondi and Nazim Agoulmine

59 A Life Devoted to Innovation in IT — Press Conference with Radia Perlman

UPEND (UPGRADE European NETwork)

65 From Informatik Spektrum (GI, Germany, and SI, Switzerland)
Software Engineering Model-Driven Development - Piecing together the MDA Jigsaw Puzzle — Oscar Pastor, Sergio España, José Ignacio Panach, and Nathalie Aquino

CEPIS NEWS

77 Selected CEPIS News — Fiona Fanning

* This monograph will be also published in Spanish (full version printed; summary, abstracts, and some articles online) by Novática, journal of the Spanish CEPIS society ATI (Asociación de Técnicos de Informática) at <http://www.ati.es/novatica/>.

UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

Publisher

UPGRADE monographs are also published in Spanish (full version printed; summary, abstracts and some articles online) by Novática

UPGRADE was created in October 2000 by CEPIS and was first published by Novática and INFORMATIQUE. Bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifs.org/>)

UPGRADE is the anchor point for UPNET (UPGRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:

• Informatica, journal from the Slovenian CEPIS society SI
• Informatik-Spektrum, journal published by Springer Verlag on behalf of the CEPIS societies GI, Germany, and SI, Switzerland
• ITNOW, magazine published by Oxford University Press on behalf of the British CEPIS society BCS
• Mondodigitale, digital journal from the Italian CEPIS society AICA
• Novática, journal from the Spanish CEPIS society ATI
• OCG Jurnal, journal from the Austrian CEPIS society OCG
• Pliroforiki, journal from the Cyprus CEPIS society CCS
• Pro Dialog, journal from the Polish CEPIS society PTI-PIPS
• Tölvumál, journal from the Icelandic CEPIS society ISIP

UPEND Advisory Board
Matjaž Gams (Informatica, Slovenia)
Hermann Engesser (Informatik-Spektrum, Germany and Switzerland)
Brian Runciman (ITNOW, United Kingdom)
Fernando Fierro Gómez and Llorenç Pagés-Casas, ATI (Spain)
Francois Louis Nicollet, SI (Switzerland)
Roberto Carriel, ALSI – Tecnoteca (Italy)

Editorial Team
Chief Editor: Llorenç Pagés-Casas
Deputy Chief Editor: Francisco-Javier Cantais-Sánchez
Associate Editors: Fiona Fanning, Rafael Fernández Calvo

Editorial Board
Prof. Wolfram Stucki, CEPIS Former President
Prof. Nello Scarabottolo, CEPIS Vice President
Fernando Fierro Gómez and Llorenç Pagés-Casas, ATI (Spain)
Francois Louis Nicollet, SI (Switzerland)
Roberto Carriel, ALSI – Tecnoteca (Italy)

English Language Editors: Mike Andersson, David Cash, Arthur Cook, Tracey Darch, Laura Davies, Nick Dunn, Rodney Fennemore, Hilary Green, Roger Harris, Jim Holder, Pat Moody, Brian Robson

Cover page designed by Concha Arias-Pérez
"The Dome of Gods" / © CEPIS 2008

Layout Design: François Louis Nicollet

Composition: Jorge Lázaro Gil de Ramalhes

Editorial correspondence: Llorenç Pagés-Casas <pages@ati.es>
Advertising correspondence: novatica@ati.es

UPGRADE Newslist available at <http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

Copyright © 2008 (for the monograph) CEPIS 2008 (for the sections UPEND and CEPIS News)
All rights reserved under otherwise stated. Abstracting is permitted with credit to the source. For copying, reprint, or republication permission, contact the Editorial Team

The opinions expressed by the authors are their exclusive responsibility

ISSN 1684-5285
Users and Network Management for Secure Interworking and Roaming in WiMAX, 3G and Wi-Fi Networks Using RII Architecture

Vamsi-Krishna Gondi and Nazim Agoulmine

The increase in the usage of different access technologies has led to a need for new mechanisms to manage interworking and roaming between different network technologies. To provide secure and seamless roaming capability for mobile users across different access network domains, belonging to the same or different operators, we propose a roaming and interworking solution using an intermediary entity, called Roaming Interworking Intermediary (RII). A generic RII-based interworking and roaming architecture between WiMAX, 3GPP (third Generation Partnership Project) and WLAN networks is presented. This paper describes the operational practices, technical architectures, authentications and mobility mechanisms to enable a subscriber of one operator to roam securely into the access networks of another operator. Using ontology based network management the operator and subscribers are handled efficiently. We provided details of network management for operators and subscriber management in the proposed architecture. A test-bed has been set up, using real pre-WiMAX and Wi-Fi equipment and a real operational cellular network, to demonstrate and evaluate the proposed solutions. The robustness, feasibility and efficiency of the proposed architecture are proven through different user scenarios.

Keywords: EDGE, Interworking, Multi-Operator, Network Management, Roaming, Subscribers Management, Wi-Fi, WiMAX.

1 Introduction

With IEEE 802.11 having been adopted in the early 2000s operators are intended to provide services through the WLAN hotspots, but due to its limited range (about 200 meters), a single operator cannot provide the services in all places: instead different operators can have agreements between the different service providers to provide a global connectivity to their users. WI-FI alliance [1] is formed to facilitate the internetwork and inter-operator roaming among different service providers and vendors. WiMAX (Worldwide Interoperability for Microwave Access), the user-friendly name associated with the IEEE 802.16 [2] standard, is an emerging wireless communication system that can provide broadband access with large-scale coverage. From the operator perspective, WiMAX roaming will increase the attractiveness to subscribers and generate additional revenues. From an end user’s point of view, WiMAX roaming will allow them to access different networks using the same subscription. The global interworking and roaming solution of WiMAX with cellular/Wi-Fi allows end-users to roam securely among these access networks while ensuring the continuity of their ongoing sessions. However, such a solution has not been covered sufficiently in the standards and in research publications.

Real-world interworking/roaming can encompass a large number of possible scenarios and network configurations. In general, a roaming agreement is required to allow subscribers of one operator to gain access to networks of other operators. The agreement deals with technical and commercial aspects related to the roaming procedure, particularly how costs and earnings are divided. Regardless of roaming relationship, the interworking between cellular and WiMAX/WLAN networks can be categorized into two
main approaches: tight-coupling and loose-coupling [1-2]. Initial work on the interworking between WiMAX and 3GPP networks has been done by the WiMAX Forum in [3]. The 3GPP-WiLAN interworking models proposed in [1] have then been reused for the 3GPP-WiMAX interworking. In addition to this proposed model there are different interworking models proposed for seamless secured roaming in heterogeneous networks, Seamless converged communications across networks (SCCAN) [4], Unlicensed Mobile Access (UMA) [5], I-WLAN [6] and Media Independent Handover (MIH) IEEE 802.21 [7].

To enable the roaming between different networks, a third party roaming intermediary has been introduced [8-11]. The intermediary can enable the roaming between two networks without any direct agreements between operators of these networks. As the number of hotspot operators has rapidly increased, the roaming capability without direct agreement has become crucial. Besides the roaming intermediaries among hotspot operators, the roaming broker facilitating the roaming between mobile and hotspot operators is also proposed [11]. It is responsible for providing the information about a user’s home services to the visited domain, taking care of the dynamical relationship and determining signalling and accounting procedures. Unlike a broker, clearinghouse [9] does not reslease the WLAN access, instead it provides a trusted intermediary for implementing roaming agreements. Most of the current solutions are proprietary ones. Furthermore, the mobility between the home and visited networks has not been addressed in any of the above solutions. Therefore they could not maintain on-going communication sessions while users roam between home and visited networks. In our work, we extend the roaming intermediary concept to deal with not only the roaming but also the interworking issue, called Roaming Interworking Intermediary (RII). Importantly, the proposed RII will enable the secure handover across different access systems and different operator domains without service interruption.

In this paper we present a generic interworking and roaming architecture between different access technologies using the RII entity. Using RII architecture we have managed to achieve secure authentication and re-authentication during roaming and handover procedures. The proposed authentication procedure using RII provides low latency and compatibility with the existing interworking architectures and procedures. While an RII architecture greatly simplifies service delivery for nomadic users, the complexity of managing and exchanging profiles, SLAs, and configurations between heterogeneous networks and the RII, becomes very complex for network administrators and systems integrators. The operators management models encompass a set of profiles (User, Content, Context, Configs, etc.) which must be aligned with the RII to allow interoperability. The user and operators are managed in an efficient manner using a network management tool proposed for this specific architecture. Arguably, the first step toward simplifying data integration is to choose a single, yet powerful language in order to maintain a coherent knowledge base. This language, or specification, will then be translated into platform specific formats. Our investigations resulted in the choice of the W3C Web Ontology Language (OWL) [13] as the RII specification language. Using Protégé [14], a tool for manipulating OWL-based ontologies, we have designed a set of concepts and properties based on our previous work in [15]. Also, to reduce the visual complexity of designing the system and to enable a fast prototyping and deployment of our broker, we have developed a tool for loading and manipulating ontologies. This tool implements our platform transformation pattern and automatically generates specific configuration files from the ontology instances (individuals). These configurations are then deployed in different areas of the access network.

Most importantly, we present our testbed implementation where the interworking & roaming of WiMAX with Enhanced Data Rates for GSM Evolution (EDGE) and WLAN is built. The RII implementation including the security management and the mobility management is detailed. Some experimental results are also presented. Section 2 defines RII architecture, components, functionalities and signaling exchanges in the architecture. Security and mobility management in WLAN, WiMAX and 3G networks is proposed in section 3. Section 4 defines network and user management in RII architecture. Section 5 provides information of the testbed for validating RII architecture, and future works and conclusion is in Section 6.

2 Roaming Interworking Intermediary Concept

2.1 Generic Roaming Interworking Architecture

We introduce a novel RII entity to facilitate the interworking/roaming among different access technologies and to enable the intersystem handover with uninterrupted services. Our proposed architecture will take into consideration different contractual relationships between operators. If the operators have a close Service Level Agreement (SLA) the roaming can be done directly between two involved networks. In this case, the RII will ease the roaming management and enhance the service continuity. On the other hand, if the operators have no agreement, the roaming will be handled with help of the RII. The interworking and roaming architecture among the 3GPP, WiMAX and WLAN networks is illustrated in Figure 1. The 3GPP network architecture used in this generic case is the 3GPP LTE architecture [8]. Though our solution is aligned with the 3GPP LTE architecture, this does not preclude the implementation of RIIs in the current cellular 2G/3G systems.

Specifically, in order to support different interworking/roaming scenarios, we introduce three kinds of RII: local RII, core RII and global RII:

- **Local RII** is a control agent and a signalling gateway of a non-3GPP access system in the interworking/roaming architecture. The local RII can be implemented as a separate entity or integrated with an access gateway, e.g. Access Service Network gateway (ASN GW) or WLAN Access Controller (WAC).
Core RII is located in the 3GPP core network and serves as a control agent and a signalling gateway between 3GPP and non-3GPP systems. The core RII performs as a local RII in respect of the global RII and as a global RII for different local RIIs under its control.

Global RII is an intermediary for interconnecting the access network of different independent operators. It is an independent entity located outside the 3GPP core network and can be deployed by a Mobile Virtual Network Operator (MVNO). The global RII is a higher-tier RII that interconnects different core RIIs and local RIIs. Functionalities of the different RII entities will be detailed in the following Section.

2.2 RII Functionalities

The RII consists of four components: mobility management (MM), security management (SM), network selection (NS) and presence management (PM). Within an RII, the MM is a centralized component that interworks with the others. We can distinguish three kinds of information exchanged between RIIs: provisioning information between NS components, security context transfer and roaming information between SM components, and all information related to handover between MM components.

Mobility Management: The MM is responsible for preparing the handover by starting the network selection (i.e., interaction between MM and NS), routing the handover preparation request based on the information from PM component, checking the Quality of Service (QoS) support in candidate target access networks and assigning the connection setup information for imminent handover terminals. It also makes the handover decision and notifies the handover to the data plane anchor for handover execution preparation. The security context transfer between two networks involved will also be triggered by the MM (i.e., interaction between MM and SM). Once the handover is complete, the MM will initiate the presence update (i.e., interaction between MM and PM) and the resource release in the old access network.

Security Management: The SM is responsible for handling authentication, authorization and billing issues for intersystem roaming users. The SM encompasses the Authentication, Authorization and Accounting (AAA) functionalities defined in [1]. In addition, the SM can manage and communicate the user’s security context (i.e., authentication identity, user identity, certificates, authorization and encryption keys) for roaming and vertical handover preparation. It is in charge of authenticating and authorizing users based on the subscriber profile retrieved from the Home Location Register (HLR) or from security context transferred by users serving/home network. The SM in the global RII plays the role of a mediator for roaming contract establishment and context transfer between serving and target access networks to optimize handover latency caused by re-authentication procedures.

Network Selection: The NS provides the provisioning information from the home/serving network to the subscribed/roaming users. Once the MM receives a list of candidate target networks from the user equipment (UE) during handover preparation, the MM communicates with the NS to eliminate the undesirable access networks.

2.3 Signalling Exchanges

The proposed architecture allows users to roam among different access systems while maintaining on-going communication sessions: the roaming and mobility management should be done simultaneously. The hierarchical mobility concept (i.e., localized and global
Figure 2: Generic Handover and Roaming Signalling Exchanges.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>During the communication on the serving RAN, the UE receives the provisioning information (e.g. neighbouring cells information, preferable access network list) from the NS component of the serving/home RII.</td>
</tr>
<tr>
<td>2</td>
<td>The UE measures the link quality of serving cell and neighbouring cells and sends measurement reports to the network either periodically or event-based.</td>
</tr>
<tr>
<td>3</td>
<td>Once the vertical handover is initiated, the serving RAN will perform the handover preparation: checking whether candidate target access networks can support the imminent handover and performing the resource reservation in advance. The handover preparation request will be routed to the indicated target RAN via the global RII if needed.</td>
</tr>
<tr>
<td>4</td>
<td>The serving RII sends the UE a handover command including recommended target cells associated with the connection setup information. The UE selects the most suitable cell among the recommended ones and sends a handover indication to notify its choice to the serving RII for handover execution preparation.</td>
</tr>
<tr>
<td>5</td>
<td>The UE performs attachment and re-authentication with the target RAN. If the security context transfer mechanism is used, the target RII authenticates the UE without need to communicate with its home network.</td>
</tr>
<tr>
<td>6</td>
<td>Once the connection to the target RAN is successfully achieved, the UE sends the MIP registration to the HA to update the data plane path. The data tunnel will be then established to route packets to the UE.</td>
</tr>
<tr>
<td>7</td>
<td>After the handover completion is notified, the resources in the old access network will be released and the presence information will be updated in the RIIs involved.</td>
</tr>
</tbody>
</table>

Table 1: Generic Inter-Operator Domain Handover Steps Description.
mobility management) [10] is used in our proposed architecture. If the handover occurs between two indirectly interconnected access networks, the handover signalling will go through intermediaries. For example, if the handover occurs between the MNO’s 3GPP access network and the WISP A’s WiMAX in Figure 1, the core RII will play the role of a mediator. If the handover occurs between two access systems that have no direct roaming agreement, WISP A and WISP B networks in Figure 1 for instance, the roaming and handover is achieved with help of the global RII. Note that the service continuity during roaming between two operators that have no existing agreement is one of the key advantages of our proposed solution. A generic signalling exchange is illustrated in Figure 2.

3 Security Management in RII Architecture

In this section we will deal with security access mechanisms for user clients accessing networks when they are in same domain or in different domains. RII architecture provides high level security architecture where the access networks are independent of another access network, whereas global RII mediating with all the networks reduces the complexity of routing, security with every individual operator networks, configurations and maintenance tends to ease. We have used these two approaches to solve the long-standing issue of user identity and routing of user authentication information from visiting access networks with or without a direct SLA with the home network.

In the first method (Figure 3a) the Users are informed to use the Network Access Identifier (NAI) of the home access network when they are in vicinity of local networks, and use NAI of global RII when they are in the visiting network using the same user ID. When the user terminal is at the home network the local RII and the Authentication, Authorisation, Accounting (AAA) server of the access network identify the authentication request from the user which is relayed by a Network Access Server (NAS) or Access Point (AP). After identifying the NAI of the user access request, the AAA server of Local RII initiates the authentication. Once authentication is done the user terminal is provided with the access. If ever the user terminal is in the visiting network, the terminal sends an authentication request to NAS or AP with the NAI of the global RII with its own user ID. Once the local RII of the visiting network identifies the global RII NAI it proxies the authentication request to the global RII. Once the global RII identifies the user ID and which network it belongs to, it forwards the authentication the local RII with the stripped user ID. Once the authentication request is received by the home Local RII, it checks the local database and authenticates the user according to its security credentials.

In the second method (Figure 3b) global RII creates the temporary user IDs and distributes them among the network operators. Network operators, based on the SLA with their users, distribute the user IDs to their subscribers. Once the Access networks receive these temporary user IDs, they distribute them to users and map with them their permanent

Figure 3a: Authentication Flow Using Global RII.

Figure 3b: Authentication Flow Using Temporary IDs and Global RII.
New Trends in Network Management

user IDs (this maintains high privacy of the subscribers by not relaying their user details but instead using temporary IDs and using a trusted source to translate the credentials). Once the visiting network identifies the authentication request from a user with NAI of global RII it forwards the authentication request to the global RII AAA server. Once the AAA server of global RII receives an authentication request from a temporary user ID, it checks the database for the access network to which it had previously assigned this temporary ID. Once identifying the access network the AAA server proxies the request to the home network of the user. With the temporary user ID, an authentication request to the AAA server authenticates the user and provides services.

4 Ontologies for Intermediary Architectures

According to Gruber [15], ontology is a specification of a conceptualization. Ontologies are widely used in network management mainly because of their powerful semantics and inherent integration capabilities. Also, a strong community support is provided by active user forums (HP Jena, Stanford Protégé, etc.). Arguably, using an ontology language for unifying the syntax and the semantic of the architecture artifacts, promises to greatly simplify the task of integrating heterogeneous operators’ service delivery platforms. Based on our previous work [16], we have developed, using a bottom-up approach, a minimalist ontology for our scenario. Figure 4 outlines the extensible ontology framework used in this paper. We started by designing an ontology that captures the network characteristics and the operators service level agreements in the heterogeneous networks. The SLAs and Operators’ information are abstracted and entered into the system using a tool, and using this information integration is maintained at different layers of management between the operators.

Having designed the ontology we have used Protégé for creating instances compliant to our specifications as shown in Figure 5. Then, in order to accelerate the deployment of network configurations, we have developed a tool to load the instance ontology, manage it and generate different configuration files for the platform. The transformations of ontology instances into configurations files implement a transformation pattern that corresponds to our platform. If the platform or the operators’ network artifacts change, the ontology-based tool can easily be adapted.

Figure 4: Bottom Up Approach for Metadata Specification.

Figure 5: RII Ontology Framework.

Figure 6 gives a brief overview of the ontology instance schema. In this example we have deployed different operators and their users and access technologies. These operator networks contains core RIIs and Local RIIs which are inter connected with the global RII of the network. In this example operator 1 contains several users whose details are stored in a database, can be accessed by Core RII of the network, and using a Protégé based tool this information can be retrieved at any given instance.

5 Testbed Implementation and Deployment

5.1 RII Platform Implementation

In this Section we provide information of RII architecture implementation for mobility management, security management components and network management using ontology.

In our testbed, the global RII assigns the temporary identities for its connected access networks. The access network will communicate such an identity to its subscribers for roaming purpose. The Extensible Authentication Protocol (EAP) [11] is used for authentication signalling.
within the network entities. When the users roam to a visiting network, they will include the assigned temporary identity as its home network identity and the Network Access Identity (NAI) of the global RII within an EAP-Identity/Response message. Based on this information, the visiting networks check if the NAI in the EAP-Identity/Response belongs to their administrative domain. Accordingly, the user authentication request will be handled locally or will be forwarded to the global RII. The global RII holds a database that makes it possible to retrieve the user home network. The authentication requests are then routed to the home networks to complete the authentication procedure. One of our future goals is to implement the security context transfer from the home network to the visiting network before users roam to a visiting network.

Figure 6: Overview of the Resulting Ontology.

5.2 Testbed Description

We detail our roaming & interworking testbed of WiMAX with cellular operator and Wi-Fi WISP using the RII architecture described previously. The implemented architecture is shown in Figure 7. Testbed setup is shown in Figure 8. Our multi-interface user terminal used is a DELL Latitude-410 equipped with Option GLOBETROTTER 7.2 ready MAX data card for EDGE access and integrated Wi-Fi interface for WLAN access. For the WiMAX access network, the terminal connects to the WiMAX CPE.

WiMAX network domain:
The WiMAX network domain in the test-bed is composed of the Infinit’s pre-WiMAX equipment, operating at the frequency of 5.4 GHz. The user terminal connects to the router of the CPE through Ethernet and the CPE connects to the WiMAX BS via the air interface. The WiMAX network contains a BS and a local WiMAX RII. The security and routing functionalities of an ASN gateway are implemented inside the local WiMAX RII. The local RII acts as an AAA server for WiMAX subscribers. The dynamics MIP mechanism and the Remote Access Permission Server (RAPS) [21] are implemented in the local WiMAX RII to perform the mobility management and security management components, respectively.

WLAN network domain:
The WLAN network consists of Wi-Fi APs (Linksys WRT54 and Cisco Aironet AP350) connected directly to a WLAN Access Gateway (WAG) which is co-located inside the local WLAN RII. We also use the Host AP (device drivers for Linux) [14] which allows a WLAN card to perform all the functions of an AP where the IEEE 802.1X with the EAP-TLS and NAI extensions have been implemented. The security component of the local RII is implemented by the Free RADIUS [15] which acts as the WISP AAA server. Like in the local WiMAX RII, the Foreign Agent is implemented in the local RII to manage the foreign users. The WLAN access network belongs to a WISP which is independent of the WiMAX operator. When a user attempts to access the network, it will authenticate with the AAA server, and then initiate the MIP registration with the HA within the WISP network.
New Trends in Network Management

Figure 8: User Terminal with a GUI to Maintain Different Interfaces with the WiMAX CPE and EDGE Datacard with SIM.

EDG network domain:

The cellular network used in our testbed is the EDGE network operated by the French network operator Bouygues Telecom courtesy of MVNO Transatel. When the user accesses to the operational EDGE network, the authentication signalling will be forwarded to the core RII located in our premises. The core RII acts as an AAA and HLR server for EDGE users. The access to the circuit switched network is authenticated by SIM whereas the access to packet-switched network is granted using Password Authentication Protocol (PAP) based mechanisms. For the packet-switched network access, the modem dials using AT commands on the data card interface with the NAI provided by the home network and the Access Point Name (APN) of the access networks. The cellular network APN which was used is netgprs.com. The AAA server in the netgprs.com gateway routes or authenticates users according to the NAI, the user name and the password. In our testbed, when the user dials with the NAI of the home network, the gateway AAA routes the authentication requests to the core RII. If the user is assumed not to belong to the core RII subscriber database, it will forward the authentication requests to the global RII. The global RII communicates with the destination local RII of the user home network for authentication and roaming. Once the authentication is successfully achieved, the user will be assigned an IP address and then initiate the IPIP tunnel with the FA and the HA of the home network for maintaining the session.

6 Experimental Results

As described previously, the UE in our testbed roams between WiMAX, WLAN and EDGE networks. We do not consider the UE movement and the network selection within our testbed. So, the handover initiation is done manually. The three access networks considered belong to three different operators. Hence the handover and roaming is achieved with the help of the global RII. We have repeated many inter-system inter-operator handovers where the UE is running a VoIP or video on demand application. This handover latency includes the security, mobility and roaming delay to carry out all necessary signalling exchanges. The overall handover latency for the roaming between WiMAX and EDGE is around 3 seconds whereas the latency for roaming between WiMAX to WLAN is around 1 second. When the UE roams from the home WLAN network to the visiting WLAN network using the global RII, the latency is observed around 4 seconds. The handover latency differs for different roaming scenarios. The signalling messages for authentication and mobility management required in different access networks are different. The high latency of WLAN-WLAN roaming is due to the fact that the WLAN horizontal handover using only one radio interface necessitates a Wi-Fi scanning and association phase.

It should be noted that the handover latency given here is not the handover interruption time. The inter-system handover using two interfaces can be managed in such a way that the communication on the serving RAN is only released when the communication on the target RAN is already started. Furthermore, the handover latency is expected to be significantly reduced once the security context transfer is implemented. Currently the capability of maintaining the communication session while the user roams to a foreign network having no roaming agreement with its home network is a disruptive result in the roaming management. As mentioned earlier we have managed to develop an ontology tool using Protégé and Java based JNI to load the instances created using Protégé. The screen shots of the implemented network management in the RII architectures are shown in Figures 9 and 10.

7 Conclusions

In this paper, we have presented a novel RII entity which offers a flexible means for interworking/roaming among different access systems. The proposed solution allows users to freely and securely move across different access systems without the need of a pre-existing subscription. The advantage of the RII architecture for roaming between
WiMAX, cellular and Wi-Fi networks has been demonstrated via a testbed implementation. The solution is feasible and economical since it does not require much change in the existing network infrastructure. Indeed, the WiMAX/cellular operator that wants to benefit from such interworking and roaming facilities only needs to add the local/core RII functionalities in its access gateway by upgrading its software. Virtual operators are interested in implementing the global RII to provide third party roaming services. With the adoption of the proposed RII architecture, the network availability will be widely extended. Firstly, the users will have great interest since it can connect to any
access networks. Secondly, the network infrastructure utilization will increase, which will give opportunities to operators to improve their profitability. In our future work, we will extend our RII ontology to align the test-bed artifacts with industry standards (IETF, DMTF, TMF, etc.). We are also exploring the possibilities of deploying the location aware context transfer in the architecture to reduce the latency and unified signalling mechanisms to transport context and management information between different components of the RII architecture. Naturally, network context and management information will be expressed using the W3C Web Ontology Language.

Acknowledgments

This work is undertaken in the frame of the Eureka CELTIC SEIMONET (SEcure Interworking of MObile & wireless NETworks) project. The authors would like to thank Transatel, Alcatel-Lucent and Starhome partners for providing the environment necessary for this research, and particularly the testbed implementation.

References


