Enabling Roaming in Heterogeneous Multi-Operator Wireless Networks

Oscar Salazar Gaitán[1], Philippe Martins[1], Jacques Demerjian[2], and Samir Tohmé[3]

[1]École Nationale Supérieure des Télécommunications, Paris, France
Département INFRES
{salazar, martins}@enst.fr

[2]ALTRAN, France
jacques.demerjian@phdgroup.org

[3]Université de Versailles, Versailles, France
Laboratoire PRiSM
samir.tohme@prism.uvsq.fr

***Abstract*— Next generation wireless networks will take advantage of the popularity and the data rates offered by unlicensed wireless networks to enhance cellular services. Nowadays, it is not surprising to see heterogeneous wireless networks coexisting on a daily basis i.e. UMTS, WiFi, and WiMAX. Unfortunately, technical issues and the lack of roaming agreements between network operators prevent interoperability. One of the goals of next generation wireless networks is to enable service mobility between heterogeneous wireless networks, thus we present in this article a SIP-based roaming architecture to enable service mobility in heterogeneous multi-operator wireless networks. Our objective is to establish mutual trust between cellular network operators and unlicensed wireless networks through a efficient SLA monitoring and enforcement and broker-based access control. All this, with minimal changes in current wireless network architectures.**

***Index Terms*— wireless convergence, service mobility, roaming architecture, heterogeneous wireless networks.**

I. INTRODUCTION

One of the goals of next generation wireless networks refers to the ability of services to be seamlessly transferred between heterogeneous wireless networks. The objective is to exploit the popularity and technical characteristics of unlicensed wireless networks such as WiFi (*Wireless Fidelity*) or WiMAX (*Worldwide Interoperability for Microwave Access*) to enhance cellular services i.e. UMTS (*Universal Mobile Telecommunication System*). Although, there are certain solutions to address service mobility they rely on the assumption that cellular operators also own the unlicensed wireless networks. Thus, as the lack of service agreements between heterogeneous operators could prevent service migration, our research focuses on service mobility under such wireless environments.

Roaming agreements are a mean to establish mutual trust between network operators or service providers, however a challenge rises when cellular operators attempt to establish contractual agreements with independent unlicensed wireless networks. Nevertheless, in spite of the technical and business-related differences between network operators, we consider that building mutual trust between cellular and WiFi/WiMAX networks is feasible. Along this article, we present a broker-based architecture to enable roaming in heterogeneous multi-operator wireless networks. Relying on a broker-based approach contributes in reducing the number of trust relationships between network operators or service providers and unlicensed wireless networks (*principle of transitivity*) [1]. In this context, the HN (*Home Network*), through the RB (*Roaming Broker*), binds roaming agreements with the VNs (*Visiting Networks*) rather than binding roaming agreements with each independent unlicensed wireless network. In our architecture the roaming agreements have as goal the establishment of mutual trust between network operators by ensuring the respect of SLAs (*Service Level Agreement*) and efficient broker-based access control.

The key-elements (*the HN, the VN, and the RB*) of our architecture communicate through an enhanced version of SIP (*Session Initiation Protocol*) [2]. The reasons to choose SIP as signaling protocol were its simplicity and the fact that it already plays an important role in the IMS (*IP Multimedia Subsystem*) in 3G networks [3] [4].

The remaining of this article is organized as follows: section two describes a typical heterogeneous roaming scenario. Section three presents the background and some related work in this domain. Section four provides the underlying assumptions upon our architecture is based. Section five describes our broker-based roaming architecture for heterogeneous multi-operator wireless networks. Section six presents some simulation results and finally section seven concludes this article.

This article is an extended version of “A SIP-based Roaming Architecture For Heterogeneous Wireless Networks,” by O.Salazar, P. Martins, J. Demerjian and S. Tohmé which appeared in the Proceedings of Innovations in Information Technologies 2006, Dubai, United Arab Emirates, November 2006. © 2006 IEEE.

II. Heterogeneous Roaming Scenario

Heterogeneous roaming refers to the ability of moving across networks with different access technologies and in most of the cases different business models. A typical scenario of heterogeneous roaming is the following:

Alice has a dual interface mobile phone i.e. UMTS-WiFi, every time she gets back home her phone is able to switch over her WiFi network to provide voice and data services. This is possible because Alice's cell phone operator also owns the Alice's ISP (Internet Service Provider). However, when Alice's gets back into her office, her cell phone is not able to switch over the company's WiFi network and get UMTS services. The reason is that Alice's company is with an ISP that does not have any roaming agreement with her cellular operator hence she cannot be identified nor authorized to roam into the company's network.

From this perspective, if Alice's company network wants to be an extension of Alice's cellular network it must be part of the trust infrastructure of Alice's HN.

Upon the description of a heterogeneous roaming scenario, we describe in the next section the background and some related work in this area.

III. Background and Related Work

Currently, the literature offers interesting approaches concerning service mobility in heterogeneous wireless networks. In this section we describe the four contributions that we consider that have been of enormous importance for our research.

1. VHE (*Virtual Home Environment*) was conceived as a concept for PSE (*Personal Service Environment*) portability across network boundaries [5]. VHE goal is to offer personalized services and user interface customization irrespective of the network or the terminal. VHE is part of the ITU (*International Telecommunications Union*) initiative IMT-2000 (*International Mobile Telecommunications-2000*) and the UMTS. With VHE the VN is able to emulate the behavior of the user's HN. Thus, the users obtain the same services that they have at the HN. To achieve this, VHE relies on support mechanisms such as CAMEL [6], MExE [7], OSA [8], and USAT [9].

2. AMBIENT Network Project. The concept of Ambient Networks comes from the IST Ambient Network Project [10] which is an integrated project co-sponsored by the European Commission. This project offers a network integration solution to the roaming problem in order to keep in contact with the outside world. Among its goals, this project aims at developing a network *software-driven* infrastructure that runs on top of network architectures to provide a way for devices to connect to each other. In particular, AMBIENT attempts to grant access to any network, including mobile personal networks through the instant establishment of inter-network agreements. Consequently, AMBIENT provides a fundamentally new vision based on the heterogeneity of networks to avoid adding to the growing patchwork of extensions to existing architectures.

3. UMA (*Unlicensed Mobile Access*) is the 3GPP (*3rd Generation Partnership Program*) standard for FMC (*Fixed-Mobile Convergence*) [11]. This technology enables access to mobile services such as voice, data, and IMS services over IP broadband access and unlicensed spectrum technologies. By deploying UMA technology, service providers and network operators can offer seamless roaming or handover between heterogeneous wireless networks using dual-mode mobile handsets. Thus, UMA allows residential, office and public wireless local area networks to be turned into extensions of cellular networks.

4. SIP-based approaches. As our proposal is SIP-based we have studied carefully the approaches that attempt to provide service mobility from the application layer. In [12] and [13], the authors introduce the concept of *Application-Layer Mobility*. They describe how SIP can be used to provide terminal, personal, session and service mobility to applications ranging from Internet telephony to presence and instant messaging. On the other hand, in [14] the authors take advantage of the application-layer protocol abstraction provided by SIP to support seamless mobility in next generation heterogeneous wireless networks. In their article, they propose an architecture that supports soft handover for IP centric wireless networks while alleviating the problem of packet loss.

Although these contributions are valuable for service mobility, they operate under tightly coupled network architectures or under the assumption that the unlicensed wireless networks are managed by the same operator. For this reason, our proposal aims at providing an efficient roaming platform to enable service mobility into VNs that are not owned or managed by the HN.

IV. Underlying Assumptions

The presence of multiple independent network operators or service providers raise new and significant issues. In this context, we consider important to provide the underlying assumptions upon which our proposal is based. As the differences between network operators or service providers are not merely technical we classified our assumptions in network-related and technical.

A. Network-related assumptions

In order to cope with independent network operators, our proposed roaming architecture follows a broker-based model. With this model, the RB aims at establishing

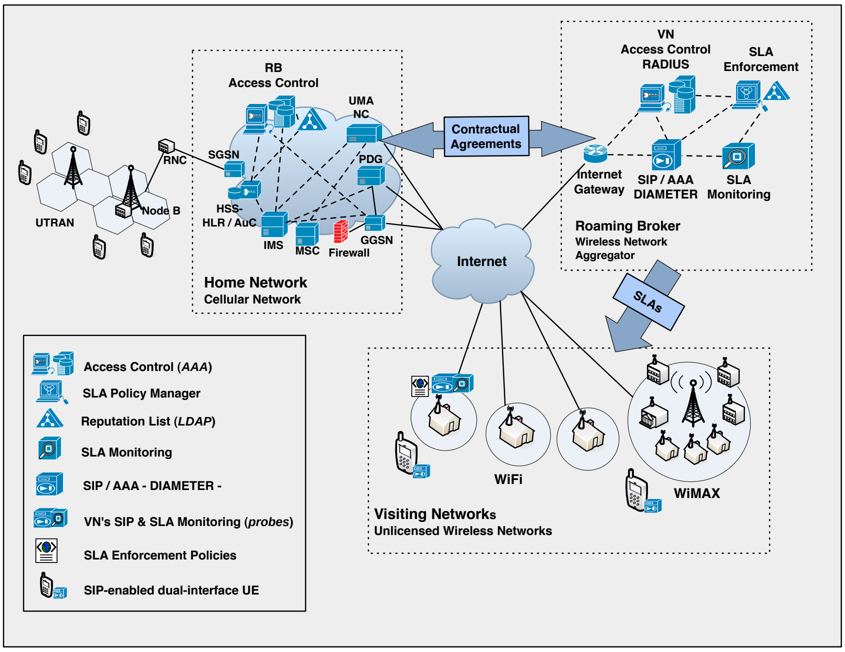

Figure 1. Roaming Architecture For Heterogeneous Multi-operator Wireless Networks

mutual trust between operators not only with the objective of participating in the authentication, authorization and accounting process but also to verify the integrity of the elements of the architecture. Hence, the network-related assumptions in architecture are the following:

- The cellular network is always considered the HN.
- The unlicensed wireless networks such as WiFi or Wi-MAX are always considered the VNs.
- Mutual trust between the RB and the HN is endorsed by contractual agreements. Through these agreements the broker assumes responsibility of the VNs under her domain. Consequently, the RB is also responsible of verifying the functionality and the performance of the VNs.
- Mutual trust between the broker and the VNs is endorsed by SLAs that clearly state on the conditions of service supplying.

B. Technical assumptions

When working with multi-operator wireless networks we are likely to face technical differences, thereby for the further development of our proposal we state the following assumptions:

- The UE should have dual wireless interface and the ability to perform vertical roaming/handover.
- The HN and VN are interconnected through an IP broadband network such as the Internet.
- Our architecture relies on an enhanced version of SIP-AAA [15] as signaling protocol.
- The VNs provide monitoring, logging and statistics to support SLA monitoring and enforcement.

Once stated the underlying assumptions, we present in the next section our broker-based roaming architecture for heterogeneous multi-operator wireless networks.

V. A Broker-based Roaming Architecture

Our broker-based roaming architecture aims at the creation of a suitable environment for the support of seamless service mobility between heterogeneous multi-operator wireless networks, this without major changes in current network architectures. To achieve this, we rely on an element called the roaming broker (*RB*), as illustrated in Fig.1. The goal of the RB is to establish mutual trust between the HN and the unlicensed wireless networks (*VNs*). As trust can be built by different means [1], we consider that mutual trust between the HN and the RB is endorsed by contractual agreements. On the other hand, trust between the RB and the VNs is endorsed by two mechanisms: SLA monitoring and enforcement, and access control. Furthermore, we consider that roaming between heterogeneous wireless networks follows economic rather than technical reasons. Consequently, roaming from cellular to unlicensed wireless networks must be allowed only if the VN respects the accorded SLAs. In this section, we present the RB and its role in our architecture.

A broker-based model simplifies service deployment since the members of the broker's domain do not need to agree among themselves, only with the broker [16]. Additionally, the members of the broker domain could or could not be aware that are participating under a large-scale roaming architecture. In our broker-based architecture the RB is in charge of binding mutual trust between the cellular (*HN*) and the unlicensed wireless networks (*VNs*). In particular, the RB establish mutual trust with

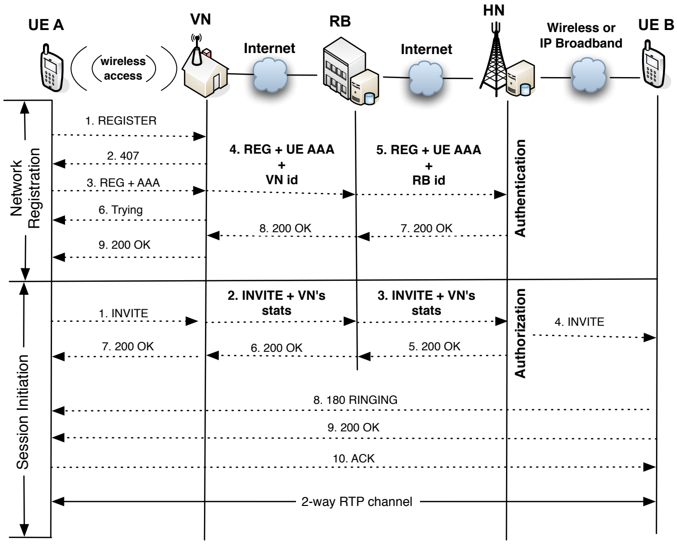

Figure 2. SIP-based Roaming Signaling

the HN by a contractual agreement where the RB assumes responsibility about the VNs. We can imagine the RB entering into contracts with network operators and service providers, and using these contracts to offer roaming services between cellular and independent unlicensed wireless networks. In contrast, we consider that mutual trust between the RB and the VN cannot be established through contractual agreements as it is no efficient to enter into contracts with every unlicensed wireless network. Instead, the RB establishes mutual trust with the VNs through SLAs and a verification mechanism to ensure the functionality of each VN under the broker's domain.

A. SLA Monitoring and Enforcement

We define a SLA as a contract between the RB and the VN of one or more technical features, that rules the supply conditions and that defines constraints of quality levels of such features i.e. *overal capacity/throughput, reporting mechanism, authentication methods, etc*. The SLAs can be composed of a business-legal part and a technical part however this article focuses on the technical part.

Upon the subscription of the VN in the RB's domain and based on its technical capabilities i.e. *Internet bandwidth, wireless bandwidth, etc* the RB creates a SLA for every VN. In order a SLA to become effective, the agreed constraints have to be placed in the real network, thus the SLAs in our architecture are placed in the form of SLA enforcement policies on the wireless access points in the VNs.

Nowadays, there are some techniques to obtain network statistics i.e. *SNMP (Simple Network Management Protocol), Ping, and HTTP requests*. The VN's SLA monitor relies on these techniques to determine and calculate the network statistics. Then, the VN's SLA monitor transmits these network statistics as probes to the RB. Once the RB's SLA monitor receives the statistics, in cooperation with the RB's *SLA enforcer* creates or updates the *reputation list*.

On the other hand, SLA enforcement relies on a SLA policy manager, a SLA Enforcement Policy, a LDAP (*Lightweight Directory Access Protocol*) [17] based reputation list, an SLA monitor in the RB and a VN monitoring mechanism, as illustrated by Fig.1. The SLAs policies are created by the RB from measurable parameters such as network capacity/throuhput, network delay, number of simultaneous VoIP calls, etc. This policies are created, managed and applied in the VN through the SLA policy manager. These policies define a set of rules placed on the access point that make it behave as specified in the SLA. Moreover, the LDAP-based reputation list is created with information provided by the SLA monitor in each VN. In this list we find three types of labels describing the VN's reputation: white, grey and black. These labels are assigned based on the VN's technical capabilities and their respect to SLAs. In this context, white indicates an excellent VN, grey a mediocre VN and black a VN that has continuously broken the SLA.

To address issues such as wireless bandwidth management the VN applies call admission control policies, nevertheless they are out of the scope of this paper. In this context, we propose the utilization of current call admission control policies for unlicensed wireless network, for more details please refer to [18] [19] [20].

B. Access Control

The RB provides access control for VN's under her domain and collaborates with the HN in UE's access control. This is accomplished through two elements located in the RB: the access control database (*RADIUS*) [21] and the SIP/AAA DIAMETER gateway [22]. The former allows the RB to authenticate and authorize VNs to offer roaming services. For authentication, the RB assign the credentials (*VN id and password*) to each VN in the network, this information is stored in the RADIUS server. The authorization is also controlled by the RADIUS server in collaboration with the LDAP reputation list. In this perspective, in addition to VN's identification the RB must verify whether or not the VN has acceptable reputation to offer roaming services.

The other form of access control relates to the UE roaming into the VN. In our architecture, we consider the HN as the roaming decision maker. Neither the VN nor the RB can authenticate or authorize a UE to roam into the VN, this privilege is reserved to the HN. The UE access control is triggered once the UE enters into the VN coverage area. At this point, the access point in the VN acts as an SIP gateway that sends the UE SIP-AAA request to the RB. The RB due to the contractual agreements with the HN is able to forward the SIP-REGISTER message to the HSS-HLR/AuC (*Home Subscriber Server-Home Location Register/Authentication Centre*) in the HN. The SIP/AAA DIAMETER element in the RB translates the SIP-REGISTER/AAA message into DIAMETER to enable communication with the IMS. We add SIP/RADIUS and SIP/DIAMETER elements in the RB because we consider important to offer support to legacy SIP-based technologies. Once the user is authenticated and authorized by the HN, the RB informs the VN to accept the visitor. The signaling from and to the RB is performed through SIP signaling. In this respect, we propose extensions to SIP-REGISTER/AAA [15] and SIP-INVITE to enable broker-based access control and SLA information exchange.

VI. SIP Extensions for Roaming Signaling

In most of the cases, before accessing a resource we are required to perform two mechanisms: authentication and authorization. In our architecture, authentication signaling is related to the network registration and authorization signaling to session initiation process. As stated in [23] the RB acts as an authorized proxy to establish SIP dialogs with the HN on behalf the VNs. The signaling message exchange starts when the UE initiates the network registration process in the VN or when the UE attempts to initiate a multimedia session i.e. *VoIP call.* In this section we describe our proposed SIP extensions for network registration and session initiation to enable broker-based access control and SLA information exchange. It is worth-mentioning that our extensions to SIP follow the guidelines for authors of extensions to the SIP as described in [2]. SIP has been proposed as a solution for numerous problems, including mobility, configuration and management, QoS control, call control, etc. however we do not consider SIP as a solution itself but merely as the roaming signaling protocol of our architecture.

In SIP-AAA [15], the authors propose the addition of the user's credentials within the **REGISTER** message upon the reception of a **407: Proxy Authentication Request** packet as illustrated in Fig. 2. Furthermore, we add the VN broker-based access control and SLA information exchange functionality to the network registration and session initiation.

TABLE I.
Proxy Authentication Request message

```
SIP/2.0 407 Proxy Authentication Required
Via:SIP/2.0/TLS client.mobile.com:5061;
branch=z9hG4bKnashds7
Cal-ID:311316842@mobile.com
From: <sips:bob@mobile.com;user=phone>
To: <sips:bob@mobile.com; user=phone>
CSeq: 1 REGISTER
Proxy-Authenticate: Digest realm=”roamingbroker.com”,
qop=”auth”,
nonce=”ea9c8e88df84f1cec4341ae6cbe5a359”,
opaque=””, stale=FALSE, algorithm=MD5
Content-Length: 0
```

TABLE II.
SIP Registration Message

```
REGISTER sips:ue-id.homenetwork.com SIP/2.0
Via:SIP/2.0/TLS sip-rb.roamingbroker.com:5061;
branch=z9hG4bKnashds7
From: Bob <sips:bob@homenetwork.com;user=phone>
To: Bob <sips:bob@homenetwork.com;user=phone>
Call-ID:88397253@homenetwork.com
Authorization: Digest username=”UE identification”,
realm=”homenetwork.com”,
nonce=”ea9c8e88df84f1cec4341ae6cbe5a359”,
opaque=””, uri=”sip:172.18.193.187”,
response=”dfe56131d1958046689d83306477ecc”
CSeq: 2 REGISTER
Contact:<sips:bob@homenetwork.com;user=phone>
expires=3600
Content-Type: application/vn-info+xml
Content-Length: 154
<?xml version=”1.0” encoding=”UTR-8”?>
<begin>
<vn-id> vn-home-wifi</vn-id>
<vn-password>k2i32ks012</vn-password>
<network statistics>
<vn-ip> 192.168.1.134</vn-sn>
<vn-voip-calls>3</vn-voip-calls>
. . . . . . . . .
. . . . . . . . .
. . . . . . . . .
</network statistics>
</end>
```

A. Network Registration

The network registration process as illustrated in Fig. 2 is the following: the UE requests network access by transmitting a registration message. This message includes a Content-type in the SDP (*Session Description Protocol*) [24] section of the SIP message, specifying the minimum QoS requirements for the application. Once the VN receives the registration message it calculates the available resources. If the VN can fulfill the QoS requirements then the VN replies with a **Proxy Authentication Message: Error 407** asking the UE to provide its credentials (*username and password*), the structure of this message is depicted in Table I. Otherwise the VN transmits an error message indicating that the QoS cannot be guaranteed. Upon the reception of a 407 message,

TABLE III.
401 UNAUTHORIZED MESSAGE

```
SIP/2.0 401 Unauthorized
Via:SIP/2.0/TLS client.mobile.com:5061;
branch=z9hG4bKnashds7
Cal-ID:311316842@mobile.com
From: <sips:bob@mobile.com;user=phone>
To: <sips:bob@mobile.com; user=phone>
CSeq: 1 REGISTER
Proxy-Authenticate: Digest realm=”roamingbroker.com”,
qop=”auth”,
nonce=”ea9c8e88df84f1cec4341ae6cbe5a359”,
opaque=””, stale=FALSE, algorithm=MD5
Content-Length: 0
```

the UE re-transmits the registration message however this time with her credentials. Our contribution to SIP initiates here and comprises the addition of VN credentials and current network statistics (*SLA-related information*) upon the reception of the SIP-REGISTER packet from the UE, see Table II. Now, the VN is ready to forward the SIP-REGISTER message to the RB. To do this, the VN includes her credentials and SLA related information into the SIP-REGISTER packet, as illustrated in Fig. 2. Upon the reception of a registration message from a VN, the RB extracts the VN identifier and the SLA-related information to perform a look up in the reputation list. If the VN has an acceptable SLA reputation and the network statistics fulfill the SLA requirements, then the RB is ready to forward the SIP-REGISTER message to the HN for network registration otherwise it is discarded. Before the transmission of the SIP-REGISTER message to the HN, the RB translates the SIP message into DIAMETER and includes the RB identifier and password assigned by the HN. Finally, once the RB credentials are confirmed and the UE is authenticated and authorized to roam in to the VN, the HN informs through a 200 message that network registration has been successfully accomplished. If there is an error concerning the UE credentials the VN responds with a **401 Unauthorized** message, see Table III. If for any reason the UE receives a 401 message it will not be able to roam into the VN.

B. Session Initiation

Session initiation signaling starts with the **SIP-INVITE** message once a UE attempts to establish a multimedia session i.e. *VoIP call* from a VN. Likewise the network registration process, the application specifies within the SIP-INVITE message in the SDP (*Session Description Protocol*), the minimum QoS requirements in order to establish the session. Our contribution is that upon the reception of the SIP-INVITE message, the VN based on its current capacity and the SLA policies determines whether or not can meet the SLA specified by the RB, as illustrated in Table IV. Once verified the SLA requirements, the VN attaches into the SIP-INVITE message current network statistics and forwards it to the RB. Once the RB receives a SIP-INVITE message from a VN, the RB processes this message and queries the reputation list. If the VN has acceptable SLA reputation it redirects the SIP-INVITE message to the HN which is the entity that will deliver, upon authorization, the message to the other peer. This can be performed through the cellular network or through a broadband IP network. Once the other peer responds to the invitation, both peers are able to start the multimedia session.

TABLE IV.
SIP INVITE MESSAGE

```
INVITE sips:ue-id.homenetwork.com SIP/2.0
Via:SIP/2.0/TLS sip-rb.roamingbroker.com:5061;
branch=z9hG4bKnashds7
From: Bob <sips:bob@homenetwork.com;user=phone>
To: Alice <sips:alice@other-network.com;user=phone>
Call-ID:88397253@homenetwork.com
Authorization: Digest username=”UE identification”,
realm=”homenetwork.com”,
nonce=”ea9c8e88df84f1cec4341ae6cbe5a359”,
opaque=””, uri=”sip:172.18.193.187”,
response=”dfe56131d1958046689d83306477ecc”
CSeq: 1 INVITE
expires=3600
Content-Type: application/vn-info+xml
Content-Length: 154
<?xml version=”1.0” encoding=”UTR-8”?>
<begin>
<vn-id> vn-home-wifi</vn-id>
<vn-password>k2i32ks012</vn-password>
<network statistics>
<vn-ip> 192.168.1.134</vn-sn>
<vn-voip-calls>3</vn-voip-calls>
. . . . . . . . .
. . . . . . . . .
. . . . . . . . .
</network statistics>
</end>
```

VII. SIP SIGNALING DELAY ANALYSIS

Nowadays, wireless local area networks support different types of traffic such as VoIP however in a future it will be common to see several mobile users attempting to roam into unlicensed wireless networks. In this context, we decided to evaluate the impact of VoIP traffic on our SIP-based roaming process, in particular when mobile users attempt network registration and session initiation.

TABLE V.
SIMULATION PARAMETERS

Parameters	Values
Wireless MAC Layer	802.11b
Δ_{HN}	10 ms
Δ_i	150 ms
VN Internet bandwidth	2 Mbps
RB Internet bandwidth	20 Mbps
Max. SIP Pkt. Size	587 bytes
Number of VoIP sources	variable [1,5,10,15]
VoIP codec	GSM - 13.3 kbps
Simulation time	600 seconds

A. Simulation Parameters

Our evaluation was performed on *ns2* network simulator [25] using an enhanced version of Rui Prior's SIP

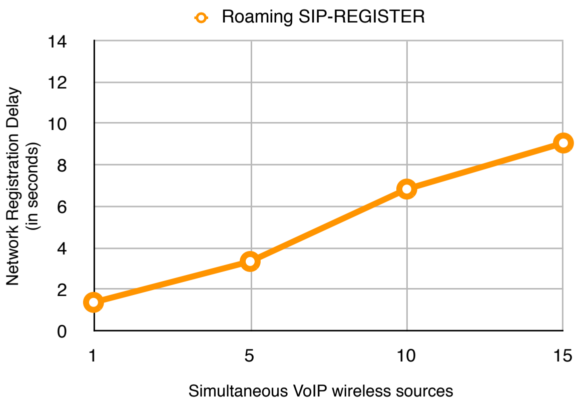

Figure 3. Overall Network Registration Delay

module [26]. Our contributions to this module include: extensions to SIP-REGISTER and SIP-INVITE packets, the processing delay due to authentication and authorization, and the delay introduced by the RB. We also included a traffic model to simulate the VoIP traffic in the VNs.

Our simulation environment comprises four types of nodes: the UE, the VN, the RB and the HN. The HN includes the GGSN (*Gateway GPRS Support Node*), the IMS and the access control server. The simulation parameters as listed in Table V were the following:

- An 802.11b MAC layer with a data rate of 11 Mbps.
- The transmission delay among the GGSN, the IMS and the AAA is 10 ms.
- The Internet delay was 150 ms, based on the findings of [27].
- The VN's Internet bandwidth is 2 Mbps.
- The RB's Internet bandwidth is 20 Mbps.
- The maximum SIP packet size is 587 bytes.

We defined four simulation scenarios to evaluate the impact of different VoIP traffic load conditions on the VN, each scenario with a variable number (*1,5,10, and 15*) of wireless nodes continuously transmitting VoIP traffic. Under each scenario an arriving UE performed the network registration and the session initiation process. We set the maximum number VoIP sources in the VN to 15 because it has been shown [28] [29] that 802.11b hardly support more than 15 simultaneous VoIP calls.

B. Simulation Results

The results presented in this section are the average of twenty independent replications of a 600 second simulation. The independence of replication was accomplished by using different random number seeds for each simulation. Moreover, we present in this section the simulation results of the network registration and the session initiation process. For our analysis we consider the overall delay as the time difference since the UE initiates the network registration, or session initiation process, and the reception of the 200 OK message indicating the success of the process. The access point in the VN is the element with lower computing capacity in our architecture, hence we decided to evaluate the impact of VoIP traffic on the VNs. To do this we decomposed the delay in the VN into average wireless transmission delay and average processing delay.

TABLE VI.
VN NETWORK REGISTRATION

Sources	Avg. Wireless Delay	Avg. Proc. Delay
1	0.0075	0.000151
5	0.8200	0.000856
10	1.3515	0.00155
15	1.5133	0.00162

TABLE VII.
VN SESSION INITIATION DELAY

Sources	Avg. Wireless Delay.	Proc. Delay
1	0.0069	0.000151
5	0.7859	0.000867
10	1.3176	0.00161
15	1.4973	0.00179

The simulation results for network registration, as depicted in Table VI, exhibit under a low traffic load scenario (*1 VoIP source*) an average wireless transmission delay in the VN of 7 ms and an average processing delay of 0.1 ms. For 15 VoIP sources we observed an average wireless transmission delay of 1.51 seconds and a processing delay of 1 ms. On the other hand, the session initiation delay exhibited an average wireless transmission delay of 7 ms in the single source scenario and a 1.49 seconds delay in the 15 VoIP source scenario. The processing delay results for session initiation were similar to those obtained in network registration, 0.1 and 1 ms respectively as depicted in Table VII. Despite that both wireless transmission and processing delay increased when the number of VoIP traffic sources increased it was the wireless transmission delay the most affected by this condition.

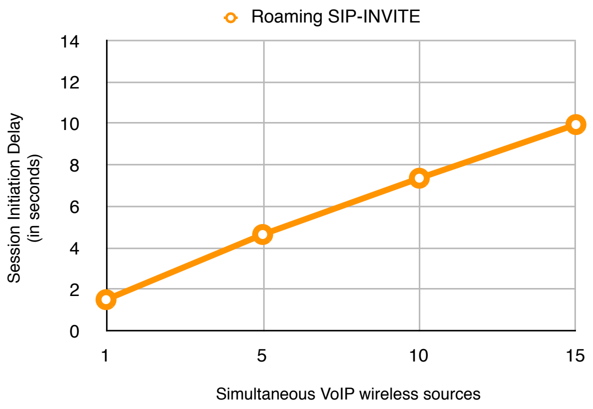

Figure 4. Overall Session Initiation Delay

Furthermore, the overall network registration delay is depicted by Fig. 3. Here, we can see that under low traffic conditions an arriving UE required only 1.13 seconds to successfully register in the VN. Nevertheless, as the number of VoIP traffic sources increased the network registration delay also increased, this mainly caused by the wireless transmission delay as shown in Table VI. The worst case of network registration delay was achieved when the UE attempted to register into a VN where 15 UEs were performing VoIP calls, here the UE needed 9.09 seconds to complete a successful registration in the VN. From this, we can also infer that the overall delay is mostly determined by the average wireless delay in the unlicensed wireless network (*VN*) rather than by the computing capacity of the VN. Thus, with an average wireless delay of 1.5 seconds in the unlicensed wireless network we obtained an overall registration delay of 9.09 seconds.

In terms of session initiation overall delay we obtained the following results, as illustrated in Fig. 4. In the case of low traffic load (*1 VoIP source*) the UE required 1.53 seconds to successfully initiate a VoIP call from the VN. On the contrary, when sharing the wireless network with 15 VoIP sources the UE required 9.98 seconds to initiate the VoIP call. Session initiation exhibited slightly greater delay than network registration because the signaling exchange requires one additional message, as illustrated in Figure 2.

From the computer simulation results we infer that to improve the overall network registration and session initiation delay we must rely on efficient access control mechanisms to reduce the congestion in the unlicensed wireless network.

VIII. Testbed Analysis

To validate the performance and the feasibility of implementing a SIP-based roaming architecture, we decided to analyze the performance of our SIP-based roaming signaling and the SIP servers in our architecture under a more realistic scenario (*testbed*). In this respect, we were mainly interested on evaluating the signaling performance in terms of: SIP network registration delay, and signaling overhead under heavy SIP traffic conditions. The rationale behind these metrics is that network registration delay could impact on roaming mechanisms *i.e. vertical handover* whereas signaling overhead has an impact on bandwidth consumption. In this respect, we consider signaling overhead as an important parameter when developing and implementing a signaling protocol, hence we decided to display the testbed signaling results as follows: bandwidth consumption in both wireless *(802.11g)* and wired domain *(Internet link)* expressed in percentage of the total bandwidth and Bandwidth consumption expressed in Mpbs.

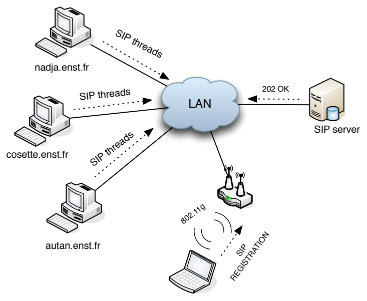

Figure 5. Testbed Implementation

A. Testbed Implementation

Our testbed was developed using the open source SIP server *OpenSER* [30] with the necessary modifications to support our extensions. The SIP server was installed on a computer running Linux Fedora Core 5, this server emulated the IMS in the HH. The SIP clients (*performing the registration*) were installed on five computers running SunOS 5.10, they represented the mobile users attempting to register in the VN. The SIP Outbound proxy emulating the VN was installed on a wireless access point (*Linksys WRT54G*) running dd-wrt [31], a linux-based operating system. It will also followed the required modifications to support our SIP extensions. To simulate hundreds of clients we modified the SIP client *sipsak* [32] to support our extensions and multi-threading. In addition, all the clients were equipped with 802.11g wireless cards. Our testbed implementation is illustrated in Figure 5.

B. Testbed Results

The main difference between our computer simulation analysis and our testbed is that in the latter we did not take into account the Internet delay. The rationale behind this is that we were interested on a performance evaluation of our Roaming-SIP protocol and the SIP servers under heavy SIP traffic conditions. To achieve this, as stated previously, we varied the number of simultaneous SIP sources (*mobile users*) attempting to register into the VN.

For validation purposes, the results presented in this section are the average of thirty independent trials. Thus, this section presents the overall results of our Roaming-SIP compared to plain SIP. This, to find out if our extensions have a negative impact on the performance of SIP. In terms of SIP network registration delay, our protocol presented a slightly increase in the delay as depicted by Figure 6. This, due to the fact that our protocol verifies the available QoS resources in the VN before replying with the *200 OK* message. Nevertheless, the delay introduced is not considerable as it is in the order of 0.01 seconds approximately.

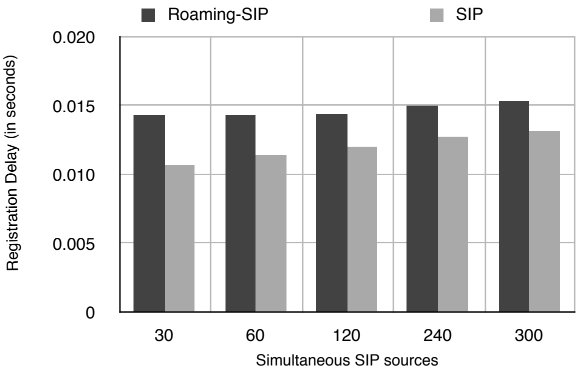

Figure 6. SIP Registration Delay

On the other hand, in terms of signaling overhead in the wireless network, our proposal displayed almost the same performance as SIP, less than 10% of the total bandwidth, as depicted in Figure 7. The reason is that our extensions only add few bytes to the SIP packets ($\approx 100 - 150$ *bytes*) thus under bandwidth such as the provided by 802.11g, the signaling overhead introduced by our protocol (*Roaming SIP*) and SIP remains comparable, as illustrated in Figure 8. As stated previously, the access point operating as VN relies on two network interfaces to provide connectivity: the wireless interface, providing data rates up to 54 Mbps and the wired interface which connects the unlicensed wireless network to the Internet. In this interface, the data rates

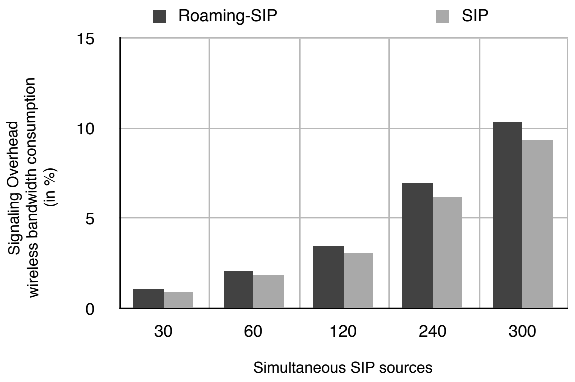

Figure 7. Signaling Overhead in 802.11g (in percentage)

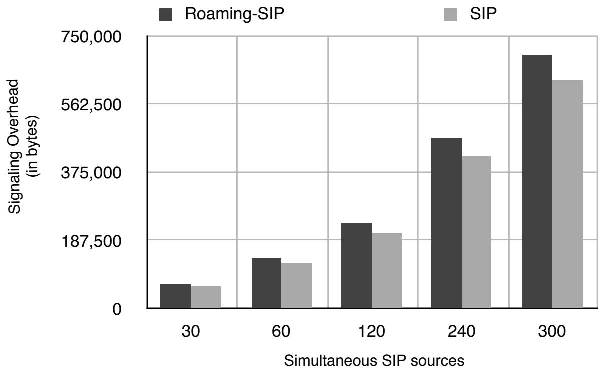

Figure 8. Signaling Overhead in Mbps

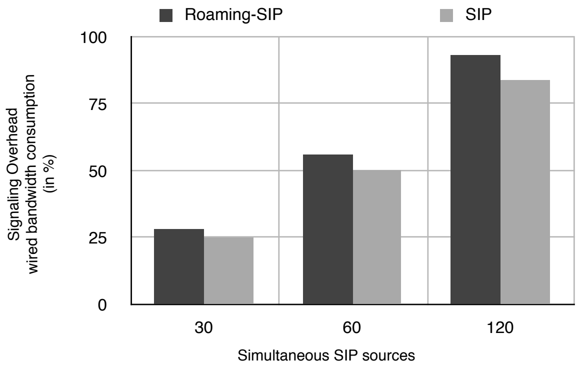

Figure 9. Signaling Overhead in a 2 Mpbs Internet link (in percentage)

are generally smaller than the offered by the wireless domain i.e. ($\approx$ 2 *Mbps in ADSL links*). This characteristic makes the additional overhead introduced by our proposal more noticeable. Nevertheless, as depicted by Figure 9, a significant difference between SIP and our Roaming-SIP starts when more than a hundred simultaneous SIP sources attempt to register. Nevertheless, this scenario is unlikely because wireless local area networks hardly support more than 15 simultaneous VoIP calls [33] [28] [29]. In conclusion, the testbed results indicate that our SIP-extensions do not diminish the efficiency of SIP protocol when enabling roaming in heterogeneous multi-operator wireless networks. We have also demonstrated that due to the simplicity and versatility of SIP, our SIP-based roaming architecture can be deployed under current wireless architecture without requiring major changes.

IX. Conclusion and Future Work

In this article we have introduced a broker-based roaming architecture to enable service mobility between cellular and unlicensed wireless networks. In our roaming architecture, the RB is in charge of establishing mutual trust between the HN the VNs. Another contribution of our work are the SIP extensions to enable broker-based access control and SLA information exchange.

For validation purposes, we decided to evaluate the impact of traffic congestion in the VN on the roaming process by computer simulation means. The results obtained in terms of SIP-based signaling delay showed that our architecture and our SIP-extensions do not have a negative impact on the performance of SIP.

In addition, to verify the feasibility of implementing a SIP-based roaming protocol, we have deployed a testbed. The results obtained through the testbed confirmed that the performance of our proposed Roaming-SIP is comparable to the performance of SIP. The testbed also provided an important insight regarding the wired domain (*Internet link*) of the access point operating as a VN. In this context, we must consider that, in most of the cases, the Internet bandwidth is smaller than the wireless bandwidth. Thus, it is necessary to rely on efficient access control mechanisms in the VN to provide and maintain efficient traffic balance between the wireless and the wired domain. Finally, we could also demonstrate that the implementation of a SIP-based roaming architecture under current wireless architecture is possible and do nor require major changes in current wireless architecture i.e. a simple software upgrade transforms a wireless router into a VN.

Our current work focuses on the implementation and evaluation of new SIP extensions to enable authentication and authorization through PKI (Public Key Infrastructure) [34] and PMI (Privilege Management Infrastructure) [35] mechanisms. Our future work comprises the development of efficient call admission control policies to maintain acceptable QoS levels in the VNs.

References

[1] U. G. Wilhelm and L. Butty, “On the Problem of Trust in Mobile Agent Systems,” in *Symposium on Network and Distributed System Security*, 1998.

[2] J. Rosenberg and H. Schulzrinne, “*Guidelines for Authors of Extensions of the Session Initiation Protocol (SIP),*” IETF RFC 4485, IETF RFC 4485, 2006.

[3] M. Garcia-Martin, “*Input 3rd-Generation Partnership Project (3GPP) Release 5 Requirements on the Session Initiation Protocol (SIP),*” IETF RFC 4083, IETF RFC 4083, May 2005.

[4] J. Soininen, “*Transition Scenarios for 3GPP Networks,*” IETF RFC 3574, IETF RFC 3574, August 2003.

[5] ETSI, “*ETSI TS 22.70. Universal Mobile Telecommunication System (UMTS): Virtual Home Environment,*” *Draft Version*, June 1997.

[6] M. Grech, “Customized Applications for Mobile Network Enhanced Logic (CAMEL),” 3GPP TS 22.078, 3GPP, 2005.

[7] “Mobile Execution Environment (MExE) Service description,” 3GPP TS 23.057, 3GPP, 2005.

[8] “Open Service Access (OSA) Stage 2, Rel. 7,” 3GPP TS 23.198, 3GPP, 2006.

[9] “Universal Subscriber Identity Module (USIM) Application Toolkit (USAT) Rel. 7,” 3GPP TS 31.111, 3GPP, 2006.

[10] B. Ahlgren, L. Eggert, B. Ohlman, and A. Schieder, “Ambient Networks: Bridging Heterogeneous Network Domains,” in *Proc. 16th Annual IEEE International Symposium on Personal Indoor and Proc. 16 th Annual IEEE International Symposium on Personal Indoor and Mobile Radio Communications (PIMRC), Berlin, Germany*, September 2005.

[11] 3GPP, “*3GPP Release 6, Technical Specifications and Technical Reports for a UTRAN-based 3GPP system,*” January 2006.

[12] H. Schulzrinne and E. Wedlund, “Application-Layer Mobility Using SIP,” *SIGMOBILE Mob. Comput. Commun. Rev.*, vol. 4, no. 3, pp. 47–57, 2000.

[13] E. Wedlund and H. Schulzrinne, “Mobility Support using SIP,” in *IEEE/ACM Multimedia Conference WOWMON*, 1999.

[14] N. Banerjee, S. K. Das, and A. Acharya, “SIP-Based Mobility Architecture for Next Generation Wireless Networks,” in *PERCOM ’05: Proceedings of the Third IEEE International Conference on Pervasive Computing and Communications*. IEEE Computer Society, 2005, pp. 181–190.

[15] J. Loughney and G. Camarillo, “*Authentication, Authorization, and Accounting Requirements for the Session Initiation Protocol (SIP),*” IETF RFC 3702, IETF RFC 3702, February 2004.

[16] B. Raman, S. Agarwal, Y. Chen, M. Caesar, W. Cui, P. Johansson, K. Lai, T. Lavian, S. Machiraju, Z. M. Mao, G. Porter, T. Roscoe, M. Seshadri, J. S. Shih, K. Sklower, L. Subramanian, T. Suzuki, S. Zhuang, A. D. Joseph, R. H. Katz, and I. Stoica, “The SAHARA Model for Service Composition across Multiple Providers,” in *Pervasive ’02: Proceedings of the First International Conference on Pervasive Computing*. London, UK: Springer-Verlag, 2002, pp. 1–14.

[17] K. Zeilenga, “*Lighweight Directory Access Protocol (LDAP): Technical Specification Road Map,*” RFC 4510, OpenLDAP Foundation, 2006.

[18] S. Garg and M. Kappes, “Admission control for VoIP traffic in IEEE 802.11 networks,” in *Global Telecommunications Conference, 2003. GLOBECOM ’03. IEEE*, vol. 6, 2003, pp. 3514–3518 vol.6.

[19] D. Gao, J. Cai, and K. N. Ngan, "Admission Control in IEEE 802.11e Wireless LANs," *IEEE Network Magazine*, vol. 19, no. 4, pp. 6–13, 2005.

[20] C. C. Wu and D. P. Bertsekas, "Admission control for wireless networks." [Online]. Available: citeseer.ist.psu.edu/598372.html

[21] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "*Remote Authentication Dial In User Service (RADIUS)*," RFC 2865, 2000.

[22] P. Calhoun, J. Loughney, E. Guttman, G. Zorn, and J. Arkko, "*Diameter Base Protocol*," RFC 3588, September 2003.

[23] O. Salazar, P. Martins, J. Demerjian, and S. Tohme, "A SIP-based Roaming Architecture For Heterogeneous Multi-operator Wireless Networks," in *IEEE Innovations in Information Technology, IIT 2006*, 2006.

[24] M. Handley and V. Jacobson, "*SDP: Session Description Protocol*," IETF RFC 2327, IETF RFC 2327, April 1998.

[25] NS-2, "The Network Simulator - ns-2." [Online]. Available: http://www.isi.edu/nsnam/ns/

[26] R. Prior, "NS 2 SIP module." [Online]. Available: http://www.ncc.up.pt/ rprior/ns/index-en.html

[27] V. Paxson, "End-to-end Internet packet dynamics," in *SIGCOMM '97: Proceedings of the ACM SIGCOMM '97 conference on Applications, technologies, architectures, and protocols for computer communication*. New York, NY, USA: ACM Press, 1997, pp. 139–152.

[28] D. P. Hole and F. A. Tobagi, "Capacity of an IEEE 802.11b Wireless LAN supporting VoIP," in *Proc. IEEE Int. Conference on Communications (ICC)*, 2004.

[29] M. Coupechoux, V. Kumar, and L. Brignol, "Voice over IEEE 802.11b Capacity," in *16th ITC Specialist Seminar on Performance Evaluation of Wireless and Mobile Networks*, 2004.

[30] OpenSER. http://www.openser.org.

[31] Open Source, "dd-wrt Firmware for Wireless Routers." [Online]. Available: http://www.dd-wrt.com

[32] Sipsak. http://sipsak.org.

[33] S. Garg and M. Kappes, "Can I add a VoIP Call?" in *IEEE International Conference on Communications, ICC '03*, vol. 2, 2003, pp. 779–783.

[34] R. Housley, W. Polk, W. Ford, and D. Solo, "*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*," Internet Draft, PKIX Working Group, January 2002.

[35] S. Farrell and R. Housley, "*An Internet Attribute Certificate Profile for Authorization*," Internet Draft, April 2002.

Oscar Salazar Gaitán is currently a Ph.D. candidate at L'École Nationale Supérieure des Télécommunications, in Paris, France. He received his MSc degree in Electrical Engineering from the University of Calgary, Canada in 2003 and the BS degree from the Universidad de Colima, Mexico in 2000. He was TRLabs research fellow in Calgary, Canada, 2001-2002. His research interests include next generation network architectures, wireless security and ubiquitous computing.

Philippe Martins obtained an engineering degree on networking and computer science (ESIGETEL engineering school) and DEA degree on signal processing (Orsay University) in 1996. He obtained his PhD in Electrical Engineering in 2000 from L'École Nationale Supérieure des Télécommunications, in Paris, France where he is currently an associate professor. His research interests are in cellular systems, and more specifically on the air interface and the radio access of cellular and wireless systems.

Jacques Demerjian obtained his PhD degree in Network & Computer Science from L'École Nationale Supérieure des Télécommunications, Paris. He is the founder of PhdGroup.org association and ESRGroups "Engineering & Scientific Research Groups". He is currently a security consultant in ALTRAN, France. His research activities concern wired and wireless network security.

Samir Tohmé was born in Damascus, Syria. He graduated from the École Supérieure d'Électricité, Paris, France and received the PhD degree from the École Nationale Supérieure des Télécommunications, ENST, Paris. He is currently a professor at the University of Versailles, France and director of the PRiSM laboratory. His main research activities concern highh-speed networks, traffic control and next generation networks. Pf. Tohmé is the French Representative to the IFIP Technical Committee TC6 and the Chairman of the IFIP WB 6.2 on Broadband Communication. He is also a member of the IEEE IAC Communications Society.