VIP (VHE in Mobile IP Networks) Architecture

Octavio Ramírez Rojas, Jalel Ben Othman, Safouane Sfar
Université de Versailles/Laboratoire PRiSM, Versailles, France
Email: {Octavio.Ramirez, Jalel.Ben-Othman, Sfar}@prism.uvsq.fr

Lynda Mokdad
Université de Paris Dauphine/Laboratoire LAMSADE, Paris, France
Email: mokdad@lamsade.dauphine.fr

***Abstract*—In this study we propose a new architecture named VIP (VHE in mobile IP networks) which guarantees authorized user access and user mobility management. The main goal is to bring the VIP architecture closer to the current GSM networks. To achieve this goal our architecture is based on LDAP and RADIUS services. VIP is able to ensure user's mobility across different IP domains. For the transportation of personalized services across different networks VHE (Virtual Home Environment) is employed. VHE gives a set of recommendations for providing users their home environment in foreign networks. The VHE services are activated to transport the user's profile between the home and the foreign network.**

***Index Terms*—VHE, Roaming, IEEE 802.11, Security**

I. Introduction

Macro-mobility management has as goal to handle mobility between different IP domains. When a user moves from one domain to another, the IP address change and we must integrate functionalities that support user's mobility across different domains. Thus, several mechanisms as user location and user authentication were taken into account in this study. Moreover, we consider that mobile users require personalized management of their internet services. Therefore, in order to have a transparent transition between the home and foreign networks, we propose a new architecture which provides personalized user services even if user moves across different foreign networks. A foreign network behaves in a fashion similar to the users' home network with the result that the same services are provided, no matter where they are located. VHE [1] gives a set of recommendations for providing users their home environment, even if they move to a foreign network. Into VHE, users are consistently presented with the same personalized features. VHE is planned to make users benefit from added values. In addition to the adaptation according to the serving network, the added value will consist in adapting the service to the user profile preferences.

In this study we propose a new architecture named VIP (VHE in Mobile IP networks) which guarantees authorized user access at the home and the foreign network. In addition, VIP allows the updating of user profile even if the user roams to foreign networks. The main goal is service adaptability regardless of the user or the equipment utilized. VIP is an entity to manage user mobility and services. VIP manages user information and it is able to provide current user location. VIP could be integrated in a university, a business organization, or in any place where user profile management is required. It is possible to extend/modify user attributes, besides user ID and password. Thus VIP is adaptable considering organization needs.

This paper is structured as follows. Section II presents current work concerning user mobility management. Work related to securing user authentication in wireless networks is described in section III. In section IV we give an introduction to the GSM architecture which we took as inspiration model. Our solution is presented in section V. In order to demonstrate that the overhead (or extra traffic) created by our model is not significant, a comparison was made between the simulations of our architecture and the traditional model based on Mobile IP. Simulations results are given in section VI. Also, we have created an analytical model to calculate the packet loss rate concerning our solution; numerical results are given in section VII. In last section we summarize the main contribution of our work in the mobility management issue and we present the trend of future work.

II. Current Work on User Mobility

Mobile nodes are prone to change their point of attachment during data communication. Roaming management is a key requirement for wireless networks; therefore, the need to make agreements between service providers is a priority. As a result, a subscription to one service would let users access virtually to any available Wireless Internet Service Provider (WISP). Currently, the mechanisms to manage user roaming in mobile IP networks are not as efficient as those of GSM (Global System for Mobile communications) networks.

Current work on user mobility is organized as follows. First, *standardization work* in future mobile networks is described. Then, we explain some *proposals* which resulted from research work reviewed in this issue. Finally, we present our conclusion concerning that work.

A. Standardization work in mobile networks

Considering the natural characteristics of mobile environments, mobile users want to be able to reach their personalized services in any visited network. Obviously, these services have been subscribed by the user. Moreover, the localization of the user's terminal is a crucial point in order to provide personalized user services. Hence, the supply and the execution of services must necessarily take into account user context. Thus, by managing the user context we will be able to offer and guarantee the Quality of Service wished by the user.

The problems concerning "supply of services in future mobile networks" were raised by several standardization authorities. Some standardization work treated these problems according to several points of view: terminal, operator network and service provider. Terminal-oriented solutions (such as MExE [2], WAP [3] and iMode [4]) are interested in the adaptability of services to several mobile terminals. Network-oriented solutions and architectures (such as CAMEL [5], SPIRITS [6] and PINT [7]) are interested in problems related to the supply and control of services in heterogeneous networks. Service provider-oriented solutions (such as OSA [8] and the Web Services [9]) offer network interfaces that allow service providers to reach functionalities and capacities of the network no matter its nature. Currently, reports on this issue prove the absence of a global vision of these problems. In fact, existing standardization work treats partially the supply of services (considering the comments of networks operators and service providers). Therefore, there is not a complete solution which meets the needs for all actors implied in the process "supply of services".

B. Proposals in future mobile networks

In opposite to standardization work, the majority of proposals have a global vision concerning the problems of supply of services. Those proposals integrate some principal actors as: mobile user, mobile terminal, services providers and possibly networks operators. Problems concerning services supply combine several research fields as: mobility, heterogeneity, personalization, QoS management, adaptability, discovered services, sensitivity to the context, etc. However, we have identified that existing solutions treat only part of the needs related to this issue.

Some solutions like CAMELEON [10], NorARC (Ericsson Norway Applied Research Centre) [11], MONTAGE [12] and SOMA [13] are interested in the implementation of mobile agents for services personalization. Moreover, they included the user's nomadicity in mobile environments.

In fact, the CAMALEON project is based on mobile agents to provide services to the final user. In order to evaluate this concept, a service concerning the management of adaptive profiles was developed. The basic idea consists in customizing the management of the calls made by users, and then routing and filtering them according to specific rules.

The work done on the NorARC is based on the duplication of applications and data. For this purpose, we have two mechanisms:

1) *Pre-duplication*: which consists in copying applications, data and profiles before the user arrives to the visited network.
2) *Dynamic duplication*: to be carried out after the user is detected in the visited network.

Nevertheless, this work is not used anymore since the technology of mobile agents derives on a loss of speed.

Relatively recent solutions, such as EURESCOM P920 project [14], VESPER [15], and CESURE [16], are more focused on the sensitivity of the context and the adaptability of services.

The EURESCOM P920 project made a VHE implementation on an IP platform. Mobility tests management, localization, roaming, as well as protocols and signalization mechanisms are included. The goal is to create an architecture and the services for global mobility based on heterogeneous local access networks.

The VESPER project has been inspired by work done on the P920 project. This project focuses on the adaptation of services according to the user preferences and is based on the VHE concept and the OSA/Parlay Platform. VESPER is focused on the issues involved in VHE from a wider angle. VESPER includes the introduction of a suitable VHE architecture and the implementation of service continuity, service portability, service personalization and session mobility.

C. Conclusion of current work on user mobility

In summary, for all developed works we have no indications concerning neither the time of remote loading nor the size of data or programs. Also, we have no specifications on the type of operation execution to ensure mobility management and VHE concept (light or heavy execution) on the level of visited network. In addition, the assured adaptability is often static and is not carried out according to the dynamic change of the environment. Moreover, the context is often represented either by network resources, or by the capacities of the terminal.

The goal of this paper consists to give solutions concerning services supply into a mobile environment IP under VHE constraints. An important implication in VHE is that the Quality of Service (QoS) provided by networks affects the provision of such VHE services to the user. Users may choose to map VHE services to the QoS requested from the network by creating mapped services to "preferred network QoS" considering the user profile.

In this work, particular attention was given to VHE specificities. Thus, these specificities were managed and implemented in the developed VIP architecture; they are related to the idea of universality of services. Services can be adapted in two ways: considering the parameters of user personalization or considering users terminal and network access. We have focused on the principal limitations concerning user mobility under VHE. Thus we took into account those limitations for the creation and implementation of the VIP architecture. Thereby, we have considered several points:

1) *Personalization of services*: the personalization of services offers users the possibility to define or modify the way in which their services are delivered in order to satisfy their preferences.
2) *Sensitivity to the context*: the possibility of using information on the context is crucial for the development of adaptive mobile applications. Within the framework of supply of services, we are able to provide services to mobile users. Besides, services are adapted according to user needs considering current environment as well as possible.
3) *Service discovery*: on this issue, the number, variability, and diversity of services that will be available to mobile users in the networks, are taken into account. Service Discovery proves that it is essential to design an effective mechanism for personalized discovery services for mobile users.
4) *Adaptability*: we define "adaptation" or "adaptability" of a system as a change in the system. This modification must be taken into account in the environment of the system [17]. In the VIP architecture, adaptability corresponds to the capacity to synchronize services with its environment. The context of execution and the functionalities required by the user are related simultaneously in order to guarantee the required Quality of Service [17].

At this point, we have presented and analyzed current work concerning user mobility. However, future mobile networks require security implementation in user access. Thus, a user authentication is necessary in order to provide a level of security in wireless networks. Therefore, we will be able to offer personalized user services. In the next section, we present current work concerning security and user authentication on mobile IP networks.

III. SECURITY AND USER AUTHENTICATION PROBLEMS

Since wireless LANs operate in an unsecured medium, authentication is an essential step to network security, mainly when a user roams between different networks. Thus, roaming management is a key requirement for wireless networks. Therefore, users may access subscribed services even if they connect with any other internet service provider. Thus, it is necessary to establish agreements between internet services providers based on authorized user access.

Current work concerning user authentication in mobile IP environments is organized as follows. First, we describe some solutions to solve the problem concerning security aspects and user authentication in wireless IP networks. Then, we present our conclusion concerning the work exposed.

A. User authentication solutions in mobile IP networks

EAP/TLS [18] (Extensible Authentication Protocol/ Transmission Layer Security) is an authentication method that works within the structure of 802.1x [19], which is the standard that defines port based security within networking. The 802.1x EAP/TLS works with 3 components: the "supplicant" which is the user or client that wants to be authenticated, the "authentication server" (i.e. RADIUS [20] server), and the "authenticator" such as a wireless access point. The mobile node communicates with the access point which forwards the information to the RADIUS server. Nevertheless, Mishra and Arbaugh [21] explain different types of attacks implemented on the 802.1x.

Another solution, LEAP [22] (Lightweight Extensible Authentication Protocol) is a mutual authentication algorithm that supports dynamic derivation of session keys. With LEAP, mutual authentication relies on a shared secret—the user's logon password—which is known by the client and the network, and is used to respond to challenges between the user and the RADIUS server. The trade-off is that the LEAP is a Cisco-proprietary method of implementing EAP Authentication and all products involved should be Cisco.

In other approach, the WEP [23] algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network; this function is not an explicit goal in the 802.11 standard, but it is frequently considered to be a feature of WEP.

Currently, all the 802.11a, b, and g devices support WEP encryption. Borisov, et.al. [24] discuss advantages and drawbacks of security protocols with respect to security aspects by showing serious weakness in WEP. On the other hand, WPA [25] is a system to secure wireless networks. In 802.11i (standard for network security), the goal is a robust set of security improvements. On the road to 802.11i, WPA (Wi-Fi Protected Access) has been required by the Wi-Fi Alliance to fix all of WEPs problems. WPA is a subset of 802.11i which allows full backwards compatibility for most 802.11a and b devices made before 2003. WPA allows Authenticated Key Management using 802.1X/EAP; moreover it uses an encryption TKIP (Temporal Key Integrity Protocol). The IEEE 802.11i Draft is the future WLAN security standard.

B. Discussion

Security using WEP (Wired equivalent privacy) keys is easy to crack. WEP does not integrate a mechanism of distribution of keys; however WEP is still used. Thus, WEP imposes an organization to distribute and configure manually the key on each customer. Therefore, the use of WEP is not easy for users and this implies an important weakness of this solution. Another limitation of WEP is the use of the same key of session for all mobile stations in a wireless network. Thus, the key is very easily obtained and the secure access to the network is not guaranteed any more.

Concerning the solutions based on the 802.1x structure, several weaknesses were revealed. Following a detailed technical analysis of LEAP, Cisco published a security note [26] concerning its LEAP. It was proved that LEAP was very sensitive to attacks by dictionary (utilization of login and password as a mechanism of authentication). Another drawback is that LEAP is property of Cisco systems. Consequently, all products must be Cisco compatible.

Finally, security implemented by WPA seems powerful because it allows the management of the authentication by using 802.1X/EAP. Besides, it continues using the session key.

One of the goals of this study consists in managing the authorized user access in the home and foreign networks. Thus, we have implemented an authentification method based on the use of a RADIUS server which is associated with an LDAP [27] database. Therefore, we are able to provide a user authentication based on the management user's profile. This method will be explained in detail at the section V.

At this point, we have presented and analyzed the current work concerning user mobility and authorized user access. We have proved that these functionalities are not implemented "together" in mobile IP networks. Nevertheless, technologies as GSM include these functionalities. Thus, we have considered the GSM architecture as a model in order to adapt its potential on mobile IP networks. In the next section, we present a general description of the GSM technology in order to identify the similitude with our solution proposed.

IV. An insipiration model: GSM

Functional GSM networks inspired the VIP architecture. GSM is the technology that underpins most of the world's mobile phone networks. The GSM platform is a hugely successful wireless technology and an unprecedented story of global achievement and cooperation. From the consumer's point of view, the key advantage of GSM has been higher digital voice quality and low cost alternatives to making calls such as text messaging. The advantage for network operators has been the ability to deploy equipment from different vendors because the open standard allows easy ***"inter-operability"***.

GSM allows network operators to offer ***"roaming services"*** which means subscribers can use their phones all over the world. This last point is very important for us because currently we have no roaming implementations in wireless IP networks.

GSM is able to manage ***"personalized user services"*** by using the SIM (Subscriber Identity Module) card and several databases that we will explain in the following subsection. The SIM is a detachable smartcard containing the user's subscription information and phonebook. This allows users to retain their information after switching handsets. Alternatively, a user can also change operators while retaining the handset simply by changing the SIM. The SIM card is very important when performing ***"user authentication"*** and it is a crucial point for roaming management.

For the VIP architecture we have considered several important points managed in the GSM architecture: *equipment inter-operability, roaming management, user authentication and personalized user services.* In fact, "roaming management" is a new and strong functionality implemented in the VIP architecture. Obviously, we have integrated this functionality based on the roaming mechanism used in GSM networks. In the following subsection the basic features of roaming management in GSM network are explained.

A. Roaming management in GSM networks

Roaming is defined as the ability for a cellular customer to automatically make and receive voice calls, send and receive data, or access other services when traveling outside the geographical coverage area of the home network, by means of using a visited network. Roaming is technically supported by mobility management, authentication and billing procedures. Establishing roaming between network operators is based on –and the commercial terms are contained in– Roaming Agreements. GSM roaming is usually done with a SIM, a Subscriber Identity Module, also known as "SmartCard". The SIM is just a packaged computer chip so that it can be safely removed. Roaming with a SIM requires removing it from your phone at home (home network) and then placing it in a rented phone at your destination (visited network). Taking your phone would seem to be more convenient, but it might not be possible if the destination country uses different frequencies.

Concerning mobile IP networks, currently there are no roaming agreements between WISPS (Wireless Internet Service Providers). Thus, GSM is highly efficient compared to Mobile IP using IEEE 802.11 networks considering the roaming issue. Moreover, user's authentication mechanisms are not standardized in the wireless IP networks. Even, the management of the user profile is not considered.

The effectiveness of GSM concerning the mobility management issue is based on the administration of user's profile. GSM uses different databases to manage user information. The two main databases that involve user information are explained.

1) *Home Location Register (HLR)* is a database used for storage and management of subscriptions. The HLR is considered the most important database as it stores permanent data about subscribers, including a subscriber's service profile, location information, and activity status. When an individual buys a subscription from one of the GSM operators, he or she is registered in the HLR of that operator.
2) *Visitor Location Register (VLR)* is a database that contains temporary information about subscribers that is needed by the Mobile Services switching center (MSC) in order to service visiting subscribers. The VLR is always integrated with the MSC. When a mobile station roams into a new MSC area, the VLR connected to that MSC will request data about mobile station from the HLR. Later, if the mobile station makes a call, the VLR will have the information needed for call setup without having to interrogate the HLR each time.

Concerning the VIP architecture we have implemented mechanisms to manage user's profile by using the user's database. VIP was developed to offer personalized services for users that are moving between different IP domains. Roaming management and authorized user access are also guaranteed. The main goal is to bring the VIP architecture closer to the current GSM networks. In the following the solution we developed is exposed.

V. VIP (VHE IN MOBILE IP NETWORKS) ARCHITECTURE DESCRIPTION

This section introduces a new architecture to assure roaming management in mobile IP networks. Thus, user mobility management is improved. This section is organized as follows. We start with an introduction of our solution. Then we describe the management of roaming intra and inter domain implemented in the VIP architecture. After that, we explain the VHE integration in this solution. Finally we explain the structure of a user's profile.

A. Introduction

Currently, IP networks do not really include mobility management such as GSM systems. The goal of Mobile IP [28] is to give an IP address to the device in the visited network and include functionality to support user location management. However, in Mobile IP authorized user access and user profile management are not taken into account.

We propose a solution to manage user mobility. We introduce the VIP architecture, which manages user internet services and mobility. In addition, authorized user access is guaranteed. Our goal consists in offering services to users according to their profile. Even if they roam, their connections and services will be uniform.

B. VIP managing intra-domain mobility

Maner and Kojo [29], define roaming as a set of formal agreements between operators that allows a mobile node to get connectivity from a foreign network. Roaming (a particular aspect of user mobility) includes, for example, the functionality by which users can communicate their identity to the local Access Network (AN), so that inter-AN agreements can be activated and service and applications in the mobile node's home network can be locally available to the user. However, roaming management in wireless IP networks is almost inexistent.

Therefore, we are taking into account two main aspects: *"security"* and *"connectivity"*. In an intra-domain scenario the VIP architecture manages roaming based on user authentication and uses a protocol which guarantees access points interoperability. Fig. 1 depicts this scenario.

In the presence of intra-domain mobility, the idea consists in using a database that contains the user profile as well as the subscribed Internet services. For that purpose we use an LDAP server. The authentication of users is carried out by using a RADIUS server, which searches LDAP databases. The mobile node sends the user ID and password via the access point to which it is associated. Thus, users can then access their home WISP services. The idea is that mobile wireless LAN users could connect to any WISP even in foreign networks.

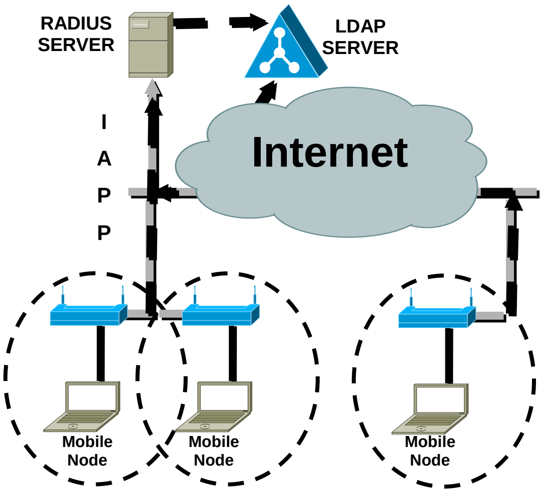

Figure 1. VIP intra domain

When the mobile node is associated to a new Access Point (AP) into an ESS (which is formed by one or several BSS -Basic Service Set-), the roaming management is done by IAPP [30] and RADIUS. IAPP is a protocol which guarantees access points interoperability, even though access points do not belong to the same manufacturer. A roaming station entering the coverage area of the new AP will initiate handover to the AP. This triggers the AP to use IAPP to retrieve the appropriate station information from the RADIUS server, to inform the old AP of the new association and perform a context transfer with the old AP. Based on security level, communication session keys between APs are distributed by a RADIUS server. RADIUS server also provides a mapping service between AP's MAC address and IP address. Thus, in order to manage the roaming intra-domain, the VIP uses IAPP and RADIUS to transfer the user context between the access points into an ESS. Therefore, VIP always knows the last location of the user. Fig. 2 illustrates the signaling messages between IAPP and RADIUS. The IAPP protocol uses TCP or UDP for inter-Access Point communication and UDP for RADIUS request/response exchanges.

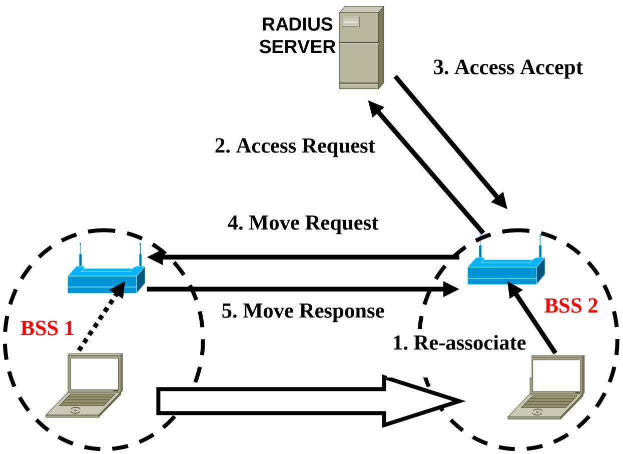

Figure 2. IAPP signaling messages

In summary, IAPP defines the procedures for AP to AP communication. On a WLAN, when a user moves from one BSS to another, his association with the previous AP is interrupted and gets associated with the AP of a new BSS. RADIUS server verifies that the APs belong to the same ESS. The user's identity and BSS, to which he is currently associated, are conveyed to other APs by the IAPP protocol.

At this point we have reviewed three basics features implemented in GSM networks: *user authentication, roaming services (intra-domain) and equipment interoperability* (c.f. section IV).

Nevertheless, we have focused on a second scenario: inter-domain mobility. Currently, there are no standard solutions to manage roaming inter-domain. Hence, the VIP architecture innovates with a performing functionality concerning this issue. In the following section our proposal is explained.

C. VIP managing inter-domain mobility

When a user leaves an ESS, another mechanism of mobility management such as Mobile IP will be necessary. In a mobile IP environment, we focus the user internet service adaptation according to the VHE context. In this case the added value consists in adapting the service to user preferences. In fact, Mobile IP provides a solution to manage transparent handoffs when the user leaves his/her home network; however, the delay and encapsulation overhead increases. Besides, Mobile IP doesn't take into account features as: *roaming management, personalized user services and user authentication in wireless IP networks.* Fig. 3 depicts our adapted solution in an inter-domain scenario.

According to our VIP architecture, LDAP servers contain user location information and user preferences. This information (stored in the LDAP home subscriber profile) is essential for roaming management.

Since LDAP server contains the user profile, we have considered establishing one LDAP server by domain (or organization). When mobility inter-domain occurs, the exchange of user information will be performed between the LDAP servers of each domain.

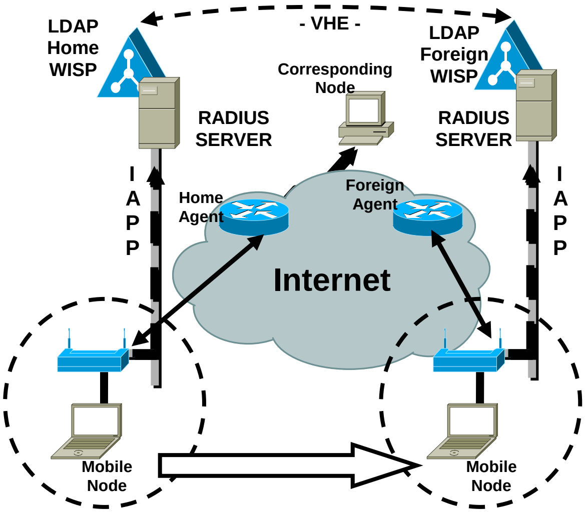

Figure 3. VIP inter domain

Compared to GSM networks, the LDAP server at the home network makes the HLR (Home Location Register) function and the LDAP server at the foreign network makes the VLR (Visitor Location Register) function (c.f. section IV). A user's profile will be transported from a network to another by VHE services. Next we explain the use of VHE according to our solution.

D. VHE services in the VIP architecture

VHE is an integrated network capability that provides operator specific services that are accessible to a user even when the user is roaming outside the home network (ITU-T Recommendation Q.1711 [31]). The VHE function related to the providing specific service profiles is required to ensure that the visited network receives the appropriate information; besides invoking VHE supplementary services.

Into a VHE environment, personal and terminal mobility are ensured in addition to service mobility. Terminal mobility allows a mobile node to change its access point without losing connection. Personal mobility allows users to use any mobile node or fixed terminal available, in any network, to reach their personal services subscribed in their home network.

VHE and mobility management are different concepts. Once we have managed user mobility, we could offer personalized services through VHE. VHE is defined as an environment that enables the user to receive customized services, notwithstanding location, access network or terminal type. VHE is based on standardized service capabilities that are consistently presented, allowing the user to experience the service always the same way. This way the user will not notice a difference in using services while roaming in other networks.

VHE offers network operators the flexibility to develop customized services across different networks (e.g. wireless, cellular or satellite networks), without requiring modifications of underlying network infrastructure. In addition, VHE offers service providers a set of components for flexible service creation, enabling them to develop services whose appearance adapts to network and terminal capabilities.

According to our architecture, LDAP servers contain user location information and user preferences. This information (stored in the LDAP server at the home WISP) is essential for mobility management. Due to the advantages of our model the personalization of user internet services is guaranteed. Nevertheless a complete VHE environment is required to support customized services. Hence, it is necessary to add specific functions to our model to enable this kind of environment (e.g. download the VHE profile from the home network to the foreign network).

Fig. 4 depicts the integration of user authentication at the home and the foreign networks implemented in the VIP architecture. The transport of user profile towards foreign network is also included.

It can be seen from fig. 4 that mobile node is associated with an access point in its home network. User authentication is done by LDAP and RADIUS services.

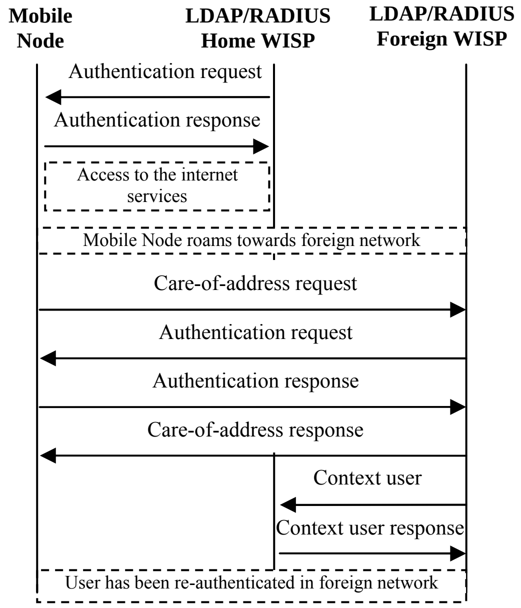

Figure 4. User authentication

Once users are authenticated, they have access to internet services. When a user roams towards the foreign network, the mobile node must change its IP address. An authentication at the foreign network is done before the assignment of the new IP address. Thus, it is necessary to have agreements between the different WISPs to allow the continuity of internet services. Once the authentication at the foreign network is done, the user has internet services as at the home network. The transport of user profile (user context) between home and foreign networks is executed by the VHE services.

The VHE function related to provisioning specific service profiles is required to ensure that the visited network receives the appropriate information, and that the VHE supplementary services are invoked. The VHE service profiles contain the trigger information that has to be exchanged between the home network and the foreign network.

The VHE structure is compatible with LDAP database structure, in such a way that the transport of user profile (or context) is executed efficiently.

Management of user profile is essential in our solution; in the following subsection we explain the basic structure of user's profile.

E. User profile in the VIP architecture

Concerning our solution, all users have a profile into LDAP database that contains the user's ID, the password, the specific fields that determine the AP's address IP (and MAC) which the mobile node is associated to, as well as the services to which the user has subscribed(c.f. fig. 5). We have an LDAP server to retrieve users' profiles.

When a user roams and associates to a new access point, the LDAP database updates the user localization. The same update process is performed when the user leaves the home network (ESS). LDAP servers contain services to modify, add, and delete the contents of a database.

User profile example

- ***User information***

<Username>octavio
<Alias>sandino
<Password>octavio_prism
<Domain>prism.fr

- ***User services***

<Nameservice1>streaming_video

- ***User preferences***

<AddedValue1>subtitled_french

- ***User location***

Home_Address: X.X.X.X
Last_Visitor_Address: X.X.X.X
New_Visitor_Address: X.X.X.X

Figure 5. User profile attributes

When that user is associated to an access point, it is possible to modify the field called "access point address" with the new information gathered in the association process. Thus, we will always have the precise location of the mobile node. When the mobile node leaves its home network and associates to a new AP (in a foreign network) roaming management will be performed by Mobile IP.

We have considered an initial structure of the user's profile that is stored in an LDAP database. Regarding LDAP functionalities, we have been able to add more services to the user. In fig. 5 we can see the basic attributes of a user profile, we explain this example: the user "Octavio" belongs to the domain "prism.fr". Octavio may be referred by his alias "sandino", LDAP services allow this functionality. The password for Octavio is "octavio_prism". Octavio has hired "streaming_video" service and the added value concerning this service is subtitles in French. In relation to user location, we have several fields that store the home and foreign IP addresses of the different networks visited by the user.

The size of a user's profile file is not more that 20Kb. This way, the transport of the user profile does not cause congestion in the network. In order to validate this architecture we made several simulations under NS 2.27 (Network Simulator). Besides, in order to compute the extra traffic generated using VIP, we have modelled our solution to demonstrate that VIP reduces the packet loss. The simulation and the queueing network models are given in the following.

VI. NS SIMULATIONS RESULTS

We performed the simulations of our architecture using NS 2.27 (Network simulator). We have compared a traditional model based on Mobile IP with our proposal. In our simulation model, we have employed 2 wired nodes, 2 access point and 10 mobile hosts (MH), the fig. 6 depicts our model. An FTP connection is established between Mobile Host and corresponding node. Considering a scenario inter-domain, Mobile Hosts (MH) roams between the Home Agent (HA) and the Foreign Agent (FA).

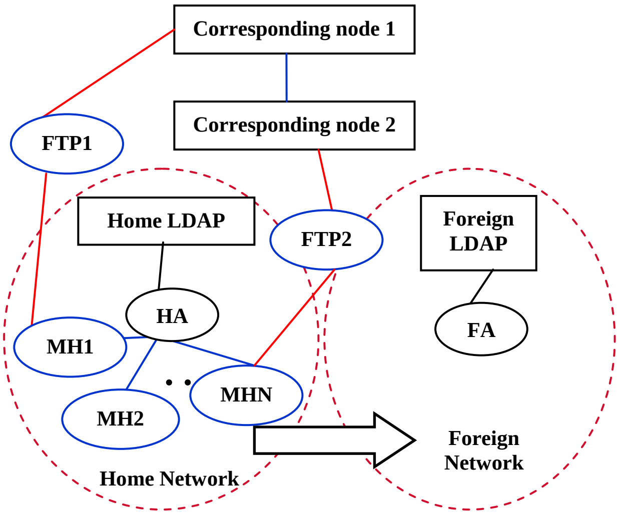

Figure 6. Simulations model

We perform our simulations during 250 seconds and with two scenarios: the first when a mobile nodes move at 20 m/s and for the second the speed is 0.3 m/s.

For the first simulation one mobile host was used. The Mobile Host (MH) roams between the home and the foreign networks. The MH establishes connection with a wired node, via HA. When it roams towards FA, there is an important quantity of packets dropped. MH moves at 20m/s. Fig. 7 illustrates the behavior of MH during the simulation considering the traditional model and the VHE model. At second 100, MH moves towards FA. At the same time, a wired node (the corresponding node) establishes an FTP transaction with the MH. The graph in fig. 7 shows that packets start to drop at around 109 seconds and continue during approximately another 23 seconds.

When the MH moves back from the FA towards the HA the same process occurs again. This operation begins at second 200. We append the exchange of user profile between the LDAP server of home network and the LDAP server of foreign network to the traditional model. In our model, an exchange of user profile is made between LDAPs servers at second 132, and the update of user profile is made at second 232. The LDAP-profile is a text file with a maximal size of 2OKb. This information could be transmitted in a reduced time.

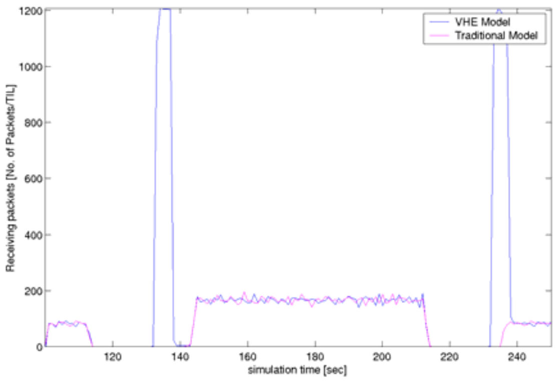

Figure 7. Mobile node move at 20m/s considering both models

We considered 0.5 seconds for this operation, because into the NS program a duplex-link between LDAP's servers with a bandwidth of 5MB was established. A profile exchange is carried out at second 132. The HA receives the packets transporting user information and it forwards then to the LDAP server in the foreign network. Compared to the traditional model, the VHE model generates extra traffic at second 132 (when mobile node leaves its home network) and at second 232 (when mobile node comes back to home network). These operations update the user profile into LDAP's servers. On the other hand, with this model we ensure users the personalization of their internet services, and we find user location information.

For the second simulation, ten mobiles were considered from which six did handover. The process was similar, users moved between the HA and FA at 20 m/s. Fig. 8 depicts the behavior of ten MHs, from which six execute a handover. When the user roams, an FTP connection between a wired node and the mobile node is activated. Throughput of receiving packets at the HA is incremented between second 120 until second 155 approx. At this moment the six user's profiles were transported to the foreign network On the other hand, the FA executes the first updating of user profile at second 180. Throughput of the VHE model is incremented by the exchange of user profile. Nevertheless, after the handover process of all MHs the throughput is under the average of the traditional model. This relation can be seen from second 150 until the end of simulation. Thus, the network is not really congested by the implementation of our model.

For the third simulation, we considered that the MH moves at 0.3m/s. Figure 9 depicts the behavior of both models, considering ten MHs, from which six do handover and consequently they need an updating of user profile. When the speed of MHs is reduced, the throughput of receiving packets at HA and FA is constant for both models. In all simulations, the involved nodes of the packets dropping are always the HA and MHs. The LDAP servers do not have packets dropped. Therefore, the user profile is transported and update correctly.

In order to prove the performance of the VIP Architecture, we have also created an analytical model in order to calculate the packet loss rate when user roams. Next, we present the queuing model and numerical results.

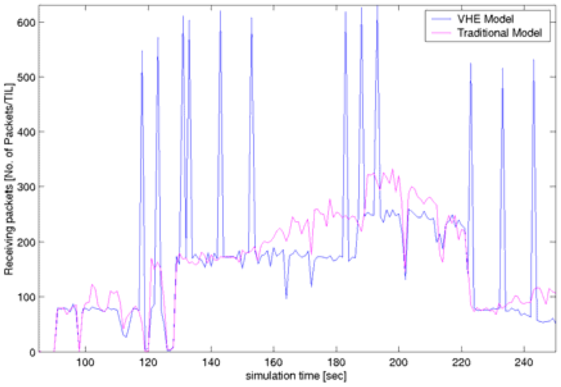

Figure 8. Ten mobile nodes at 20m/s considering both models

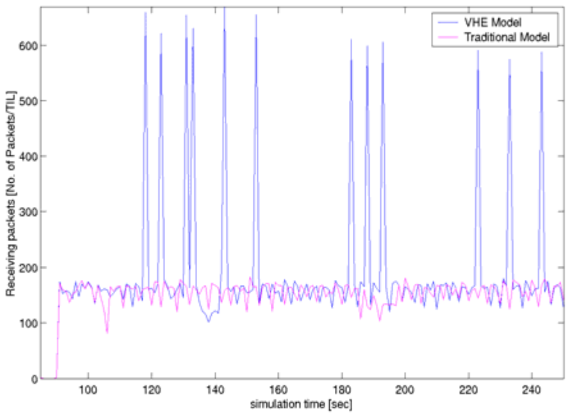

Figure 9. Ten mobile nodes move at 0.3 m/s considering both models.

VII. Performance Evaluation of the VIP Architecture

We consider that we have K access points and in each point, we have N servers. When a packet arrives we check if the user is connected to the corresponding access point. Thus, the routing probabilities are defined as follow:

- p_i, a user i is in the HN and he sends data to the AP,
- q_{ij}, a user i executes a handover to a FN and the data are sent from the LDAP HN to the LDAP FN
- r, we have no information on MN localization, and thus the packet is lost.

We suppose that the arrival of packets follow a Markov Modulated Poisson Process (MMPP) with two phases. This arrival process alternates between high arrival period (state 1) and low arrival period (state2). Fig. 10 depicts this model.

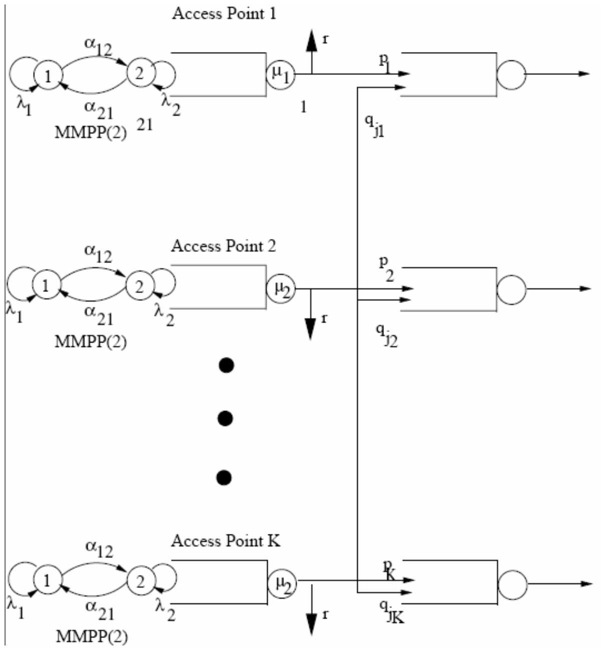

Figure 10. Our model

During the high period, the arrival rate is λ_1 and during the low period rate is λ_2, where $\lambda_1 > \lambda_2$. The mean steady state packet arrival rate λ for this process is given by:

$$\lambda = \frac{\lambda_1\alpha_{21} + \lambda_2\alpha_{12}}{\alpha_{12} + \alpha_{21}} \qquad (1)$$

The service time has an exponential distribution in each queue with rate $\mu_{i.}$

The considered model can be described by a continuous time Markov chain *X(t).*

We define the state x by $(x_1, x_2 .., x_K)$, where: $\forall\, 1 \le i \le K$, x_i is the number of the data packet in the access point i. We denote its stationary probability distribution by $\Pi(x)$.

The resolution of this system is very simple because it is a product-form queuing networks. Thus, efficient and exact solution algorithms exist for this class of queuing networks. Our model is a Jackson network because it fulfills the assumptions concerning arrival and service time distributions and service discipline which is FCFS. Thus, the steady state solution consists of multiplicative factors where each factor is a solution of MMPP(2)/M/N queue.

$$\Pi(x_1, x_2, \ldots, x_K), = \pi_1(x_1) \times \pi_2(x_2) \times \ldots \times \pi_K(x_K) \qquad (2)$$

With this model, we compute the packet loss in access point. Thus, we consider a simple model with $K=2$ and we compute the packet loss rate γ in the access point i using this formula:

$$\gamma = (1 - \pi_i(0))\mu_i\, r \qquad (3)$$

Where π_i is the marginal probabilities for the queue i.

The different values of parameters used in this numerical computation are given in Table I.

In fig. 11 we compare the Packet Loss Rate (PLR) of our architecture with Mobile IP. We give the values of γ by varying the load in the access point 1. The numerical results confirm our assumption that VIP architecture reduces the PLR.

TABLE I.
MODEL PARAMETER VALUES

K	Number of access points	2
N	Server number	1
α_{12}	Transition rate from high to low period	0.01
α_{21}	Transition rate from low to high period	0.2
λ_1	Packet arrival rate for high period	2* λ_2
μ_1	Service time	20
r	Routing probability	0.02

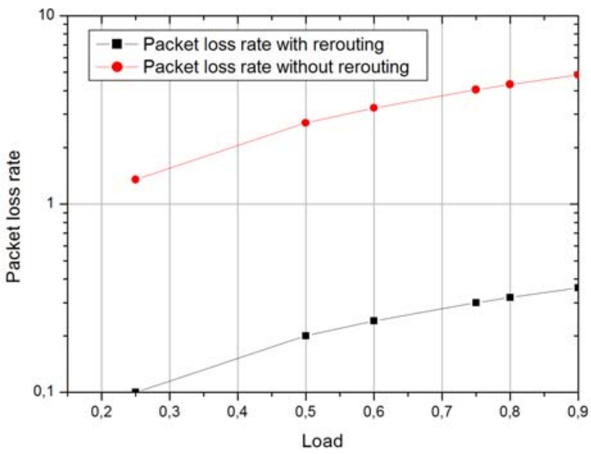

Figure 11. Packet loss rate with and without rerouting of packets at the access point 1

VIII. Conclusions and Future Works

Mobile IP networks are not able to provide mobility services and security as in other telecommunication systems (e.g. GSM, UMTS). Our approach introduces a new architecture which assures roaming management in wireless IP networks.

The VIP architecture solves *intra-domain roaming*, due to the fact that the VIP uses IAPP and RADIUS in order to provide *interoperability and connectivity* to the user in a home network.

We use an LDAP and a RADIUS server to perform *user authentication* to give security in the access networks. The LDAP server contains fields as: user ID, user password, AP's address IP, etc. When a user roams and is associated to a foreign network, the LDAP server is able to update the user location. Our proposal is totally flexible: it is possible to extend LDAP attributes, besides user ID and password, such as time spent on line, etc.

Another problem is solved with our architecture: *inter-domain roaming*. In this case, the VHE services are activated to transport the user profile making a transparent transition between the networks visited by the user. Thus, the VIP architecture will be able to return the specific services to the user. Besides, VHE manages the user profile update. On the other hand, with this model we ensure users the *personalization of their internet services,* besides we find user location information.

According to NS 2 simulations, the LDAP servers do not have dropping packets. So, the user profile is transported and updated correctly. Besides we have demonstrated, by analytical model, that VIP reduces the packet loss rate when a user executes a handover

Based on the VIP architecture, we aim to integrate new solutions considering the new generation of services based on SIP (Session Initiation Protocol) management.

References

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Services Aspects; "Virtual Home Environment (VHE)", Release 1999.

[2] MExE: 3G TS 23.057, "3rd Generation Partnership Project; Technical Specification Group Terminals; Mobile Station Application Execution Environment (MExE); Functional description; Stage 2 (3G TS 23.057 version 3.0.0)".

[3] WAP Forum: Wireless Application Protocol: "Wireless Markup Language Specification, WAP Forum", 1998.

[4] Herman Chung-Hwa Rao and Di-Fa Chang and Yih-Farn Chen and Ming-Feng Chen, "iMobile, a proxy-based platform for mobile services". In *Wireless Mobile Internet*, pages 3–10, 2001.

[5] CAMEL: 3GPP TS 22.078 v5.5.0. "Customised Applications for Mobile network Enhanced Logic (CAMEL)". Service description, Stage 1. December, 2001.

[6] V. Gurbani and A. Brusilovsky and I. Faynberg and H.L. Lu and M. Unmehopa and K. Vemuri and J. Gato, "The SPIRITS Protocol", *IETF Internet-Draf*, April 2003.

[7] S. Petrack and L. Conroy, "The PINT Service Protocol, Extensions to SIP and SDP for IP Access to Telephone Call Services", *RFC 2848*, June 2000.

[8] OSA, Services and System Aspects, Service Aspects, Stage1, "Service Requirement for the Open Service Access (OSA)", Technical Report TS 22.127 v4.1.0, 3rd Generation Partnership Project, Mars 2001.

[9] H. Kreger, "Web Services Conceptual Architecture", Technical Report, IBM, WCSA 1.0, 2001.

[10] ACTS CAMELEON Project; http://www.comnets.rwth-aachen.de/~cameleon/

[11] Do Van Thanh, Sverre Steensen, Jan A. Audestad, "Mobility Management and Roaming with Mobile Agents", Lecture Notes in *Computer Science*; January 2000.

[12] MONTAGE: ACTS MONTAGE project home page. http://montage.ccrle.nec.de.

[13] P. Bellavista and A. Corradi and C. Stefanelli, "The ubiquitous provisioning of internet services to portable devices", in *Pervasive Computing, IEEE*, 1(3): 81–87, July–Sept 2002.

[14] EURESCOM Project P920; UMTS Network Aspects, http://www.eurescom.de/public/projects/P900series/p920/default.asp

[15] Virtual Home Environment for Service Personalization and Roaming Users, http://www.ee.surrey.ac.uk/CCSR/IST/Vesper/

[16] Marie Claude Pellegrini and Olivier Potonniée and Raphaël Marvie and Sébastien Jean and Michel Riveill, "CESURE, une plate-forme d'applications adaptables et sécurisées pour usagers mobiles". In *Calculateurs parallèles, Evolutions des plate-formes orientées objets répartis*, 12(1):113–120, 2000.

[17] Safouane SFAR, "Adaptation Dynamique des Services Télécoms Multimédias Mobiles", *PhD thesis, ENST-Bretagne*, July 2003.

[18] B. Aboba, D. Simon, "PPP EAP TLS Authentication Protocol", *IETF RFC 2716*. October 1999.

[19] LAN/MAN Standards Committee of the IEEE Computer Society. "Port Based Network Access Control. IEEE Std 802.1X-2001", October 2001, http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

[20] C. Rigney, S. Willens, A. Rubens, "Remote Authentication Dial In User Service (RADIUS)". *IETF RFC 2865*, June 2000.

[21] Arunesh Mishra and William A. Arbaugh, "An Initial Security Analysis of the IEEE 802.1X Standard", http://www.cs.umd.edu/~waa/1x.pdf. February 2002.

[22] Product Bulletin No. 1515 *Cisco* Wireless LAN. Security *Bulletin*. November 2000, http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm

[23] LAN/MAN Standards Committee of the IEEE Computer Society. Part 11: "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", *ANSI/IEEE 802.11*, 1999 Edition. Page 59

[24] Nikita Borisov, Ian Goldberg, and David Wagner, "Intercepting mobile communications: the insecurity of 802.11". *Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking*. July 2001.

[25] WPA (Wi-fi Protected Access). *Wi-fi Alliance.* 2004 http://www.wifialliance.com/OpenSection/protected_access.asp

[26] Cisco Systems. Cisco Security Notice : "Dictionary Attack on Cisco LEAP Vulnerability", http://www.cisco.com/warp/public/707/cisco-sn20030802-leap.shtml, August 2003

[27] W. Yeong, T. Howes, S. Kille, "Lightweight Directory Access Protocol", *IETF RFC 1777*. March 1995.

[28] C. Perkins. "IP Mobility Support". *IETF RFC 2002*. October 1996.

[29] J. Maner, Ed., M. Kojo, Ed., "Mobility Related Terminology", *IETF RFC 3753*, June 2004

[30] IEEE, *Working Group 802.11F*. "Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.11", Operation 2003. http://grouper.ieee.org/groups/802/11/index.htm

[31] ITU-T Recommendation Q.1711 (1999): "Network functional model for IMT-2000".

Dr Octavio Ramírez Rojas is an associate professor at the Instituto Tecnoloógico de Jiquilpan, in México. He holds a Ph.D. from the University of Versailles, France in November 2005. Previously, in October 2002 he holds a D.E.A (Master's degree) from the University of Troyes, France. He is currently contributing to research on next generation services mobility based on SIP.

Dr Jalel Ben-Othman is an associate professor at the department of Computer Science at University of Versailles, PRiSM laboratory. He received his PhD in Computer Science from University of Versailles, France in 1998. He received the "D.E.A." degree in Computer Science in 1995 from the University of Versailles, France. His main research interests include radio resource management, security and performance evaluation for wireless and mobile networks.

Dr Safouane Sfar is born in Mahdia, Tunisia, in January 1973. He received his B.S. degree in telecommunications from Ecole Supérieure des Communications de Tunis, Tunisia in 1996, his M.S. degree from Ecole Nationale d'ingénieurs de Tunis in 1998 and his Ph.D. degree in 2003 from ENST-Bretagne, Brest, France. His research interest procedures related to QoS specification and management in UMTS and NGN and multimedia service adaptation.

Dr Lynda Mokdad is an associate professor at the department of Computer Science at University of Paris Dauphine, Lamsade laboratory. She received her PhD in Computer Science from University of Versailles, France in 1997. Her main research interests include performance evaluation for networks and Web services.