A new control access solution for a multi-provider wireless environment

Artur Hecker[1], Houda Labiod[2], Guy Pujolle[3], Hossam Afifi[4], Ahmed Serhrouchni[5] and Pascal Urien[6]

[1,2,5] {hecker,labiod,serhrouchni@enst.fr} INFRES Department, Ecole Nationale Supérieure des Télécommunications 46 rue Barrault – 75634 Paris Cedex 13 – France
[3] {Guy.Pujolle@lip6.fr} LIP6 -8, rue du Capitaine Scott 75015 Paris
[4] {Hossam.Affifi@int-evry.fr} INT-Evry, 9 Rue Charles Fourier, Dépt. Réseaux & Systèmes de télécommunications – 91011 Evry Cedex
[6] {Pascal.Urien@louveciennes.tt.slb.com} SchlumbergerSema, 36-38 rue de la Princesse, BP 45, 78431 Louveciennes Cedex, France

Abstract

The fundamental goal in future 4G mobile multi-service networks is to provide an efficient mobile computing environment which enables a user with its portable computer equipped with multiple wireless access interfaces to seamlessly move between different providers' networks. Besides seamless roaming, a key consideration is also devoted to quality-of-service provision. In this article, we propose a model and architectural framework for supporting end-to-end QoS in the context of interconnected multi-provider wireless systems. The proposed integrated COPS-based management and RADIUS-based control access architecture will allow providers to offer multimedia services while optimizing the use of underlying network resources. We suggest new concepts and protocols to provide solutions to the challenges and describe an ongoing research project named MMQoS to build such future networks.

Keywords: *4G networks, multi-provider context, SIM-IP card, COPS, RADIUS*

I. Introduction

The advent of ubiquitous computing and the proliferation of portable computing devices have raised the importance of mobile and wireless networking. Recently, there has been a tremendous interest in broadband wireless access systems, including wireless local area networks [1], broadband wireless access and wireless personal area networks (WLAN/WPAN/ WWAN). Obviously, a convergence of all these technologies with 2.5G/3G mobile networks [2][3] will probably lead to various integrated solutions and combinations of standards that will globally improve the seamless connectivity. Each standard will be optimized for a different environment. Standardization activities are fully undertaken throughout many committees like ITU-R, ETSI BRAN and IEEE 802 with its Working Groups 802.15 for WPAN, 802.11 for WLAN and 802.16 for WWAN.

The boom of the Internet has launched a chain reaction in the end of the 20th century resulting in the Internet technology spreading fast in almost every communications branch. Applications like email, instant messaging and web services build the new business and private communication standards. Such applications are ready to use on the modern notebooks, PDAs and other portable devices. Hence, the access to these applications is an important feature. Today, almost every network technology is prepared or even explicitly designed to transport IP-packets. Thus, the 4G architecture should incorporate all those heterogeneous networks and the native core-router IP-backbone. Moreover, as the Internet evolves toward the global multiservice network of the future, a key consideration is to support services with guaranteed quality of service.

Within this heterogeneous and future-oriented context, users will probably have mobile terminals with several different physical interfaces at their disposal. Users will choose the access networks dependent on the wished services. However, a fixed contract with each used provider is an expensive solution which is also difficult to manage. Users would rather like to pay per used service independent on the provider itself but depending on the real quality of the used service (QoS) i.e. the really experienced bandwidth, delay and jitter values.

The proposed Differentiated Services approach [4] seems to be an appropriate solution for providing end to end QoS in this architecture. But still, the involved networks need to be capable of supporting elementary QoS functions. Besides, user identification and network access are critical issues in the QoS context.

The WLANs are an especially interesting opportunity due to their extreme low cost characteristic and comparably high performance. The WLANs currently experience amazing development and rapid growth uing standards IEEE 802.11a/b. In spite of known security problems and frequency usage restrictions in some countries, more and more WLAN installations spread out. Indeed, the deployment of the WLANs is believed to become a down-top process and not a

top-down proliferation like in the case of the mobile networks. Huge WLANs with national level coverage are theoretically feasible but not very probable in the next future. Nowadays, the WLANs are rather organized in form of so-called hotspots i.e. relatively small networks covering a particular location with a high traffic load and providing broadband and easy-to-use Internet access to their customers. Classical examples are airports, hotels, city centers (e.g. Seattle [5], Stockholm [6]), etc. Currently, there are around 4000 hotspots in the United- States and about 1000 hotspots in Europe. On the other hand, some national telcos announced launches of WLAN-focused enterprises (e.g. Deutsche Telekom AG [7]). Such operators consider the WLANs being an attractive access technology providing a limited mobility but with a high bandwidth. Therefore, they are interested in developing seamless mobility mechanisms between such wireless infrastructures and their own mobile networks. Additionally, national providers could collaborate with governmental organizations and participate in the development and the deployment of the WLANs in metropolitan areas.

As regards to the given context with making an accent on WLANs, in this paper, we focus on designing a global architecture that provides a solution for secure network and service access with roaming and potential QoS support in the recent heterogeneous wireless environments.

The rest of the paper is organized as follows. In Section II, we describe the multi-provider context of the 4G architecture and point out the main technological challenges. Then, in Section III, we briefly discuss the MMQoS research project goals currently being carried out by a group of French national universities and industry partners. A detailed description of our global system architecture is given in Section IV highlighting the main ideas we propose to resolve the critical issues cited in Section II. In Section V, we emphasize on our control access approach. Finally, Section VI provides concluding remarks.

II. Multi-provider network context

The participating networks in such a heterogeneous 4G Internet will be managed by some authorities. Though there certainly will be national providers offering access to almost all network technologies, in the most general global case we have to consider a multi-provider context. In such a context, mobility and in particular roaming are critical issues if changing networks and allowing remote access is of any interest for both users and providers.

Seamless mobility between different 2.5G/3G mobile networks is applied. However, national roaming, although technically possible, is usually prohibited by the national telecommunications regulation institutions in order to encourage developing of gapless national coverage.

In the case of WLAN, the most hotspots will be probably served exclusively by one provider for performance reasons. Hence, the choice for the user will rather be to change the geographical location than to choose another provider at the same location, with some natural exceptions. In this manner, even completely local providers will be nevertheless in a competition situation. Some reasonable amount of cooperation and fusion will probably lead to providers extending their activities to at least regional levels. Such specialized enterprises will use their experience in order to entertain numerous hotspots. Since the on-site competition will be kept minimal or not exist at all, the main advantages of a provider will be the effective throughput, the quality of service and the number of sites where the user can use the service. Hence, an interesting form of cooperation between the WLAN providers will be the possibility to provide access for the users of the partner enterprises, thus extending their own advertised coverage area.

Besides provisions for physical interconnections of concerned networks and a common naming scheme for users, the involved service providers have to make different agreements (service level, technology, prices, …) in order to enable roaming access from and to their partners' networks. Details related to such "roaming contracts" are out of the scope of this paper and will be generally negotiated between providers. In the following, we summarize the technological problems. Mainly we can find three different issues:

- Mobile access control: we have to enable Provider A to offer secure access for potentially unknown users of Provider B.
  - What will be the exact used naming scheme for user identities?
  - Where will this identity be stored and how can it be protected from fraud?
  - Which credentials can the mobile user present to the visited network and how could A verify such credentials of B's users?
  - Once authenticated, how can a user obtain access to the network services? How can we provide access to the services located in the home network of the user?

- Quality of service: due to the limited bandwidth, the wireless environments are particularly sensitive to service deterioration in case of high network load.
  - How can we control user traffic in particular sensitive wireless environments?
  - How can an offered service be guaranteed to visitors with respect to the requested quality?
  - How can Provider A prove to the user X and his Provider B respectively that this user really used A's resources?
- Billing: the exact billing information is subject of the respective roaming contract but we have to allow for billing information record, storage and exchange.
  - How can we collect billing information for roaming users?
  - How can we prove it?

Being maintained by national level telecommunications companies, 2.5G and 3G networks provide different quality of service levels and well-defined billing mechanisms. The authentication is based on a so called subscriber's identity module (SIM in GSM [8], USIM in UMTS [9]) which stores the credentials and the authentication algorithms. So, this type of networks is relatively well prepared to serve as an authoritative domain in a multi-provider context. Provisions have to be made for IP stack installations on the terminals. As mentioned, national roaming is to avoid due to the current regulation.
In contrary, none of the three points is covered by the existing WLAN standards although there are currently different working groups (WG) at the IEEE implied in the solution of related problems. The concerned WGs are:

- 802.1X WG which defines secure access control mechanisms for 802 networks with provisions for roaming
- 802.11e WG which currently works on different QoS aspects
- 802.11i WG which proposes a global standard for enhanced security in wireless networks

Obviously, the results of these working groups will be used to solve some of the problems in the described context. But still, the collaborating providers have to install sub-systems in their networks enabling support for agreed upon features. The exact architecture of such systems has to be defined. The challenge is to design a system architecture that is feasible and sufficient in terms of security and QoS.

III. MMQoS project objectives

III.1. A brief description

With respect to the introduced problems, a French national project named MMQoS [10] started in 2001. The main project objective is to provide user mobility with support for end to end quality of service in a multi-provider context of up-to-date heterogeneous wireless networks with different management authorities (see Figure 1). The SIM-IP card [11], which is described in detail in Section IV.3, is a key element in the proposed architecture. Basically, it is used to provide identity storage, controlled network access and other procedures. In particular, policy-based QoS management is applied since it is well adapted to our project context. In the preliminary project phase, we restrict our investigations by considering only 802.11b WLAN hotspots.

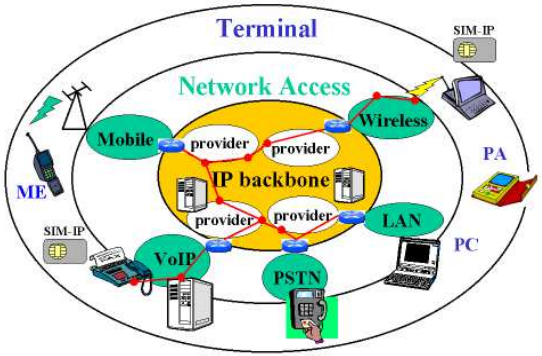

Figure 1 MMQoS global architecture

In the following, we briefly describe the project objectives.

III.2. Mobility

In the MMQoS context, mobility is the main feature. We define mobility as a potential possibility of relatively rare network changes without identity change. The rare network changes represent the real life situation in a multi-provider network consisting of geographically separated hotspots. The identity fidelity is, on one hand, indispensable to provide correct and global per user billing. On the other hand, we are talking about established long term user-provider relationships and not about short spontaneously purchased login tokens which would not require any roaming. Consequently, procedures such as seamless handovers and fast handoffs are not the main objectives of the MMQoS project. Hence, no state information about user's connections needs to be exchanged between the current and the destination networks.

III.3. QoS

The QoS issue consists of two main objectives. The first objective is to ensure to the user that the service has fulfilled required QoS criteria. The second objective is to provide a solution which enforces user's resource usage according to user's service profile requirements. In order to achieve a flexible solution for QoS management, we propose to use COPS [12]. Introducing a central network control entity, it allows dynamic QoS profile adaptation depending on the current network load and enables profile exchange between the concerned providers.

III.4. Security

Security is the implicitly defined objective. Indeed, in order to ensure secure network access to guarantee QoS based on user's service level and to provide reliable billing, strong authentication mechanisms are indispensable. Furthermore, those mechanisms need to allow for roaming. In the context of wireless communications, reliable encryption is necessary. Additionally, we have to include user identity information in the packets in order to ensure secure service access in both foreign and home networks.

IV. The proposed solution

Aiming to explore the fundamentals of next-generation mobile network architectures and protocols, we propose to consider the 4G system architecture described in Figure 2 looking beyond the issues addressed by today's WLAN solutions. It allows evolution of mobile network services to include basic mobility features (such as authentication and roaming) as well as newer requirements (for example QoS). This section contains a brief presentation of the global architecture's entities and protocols. It includes a general description of the functional global architecture. Then, it provides a detailed description of a service provider network architecture.

IV.1. 4G system architecture

In particular, the concerned 4G system architecture is viewed as an open-architecture that permits evolution of service features via collaboration of various wireless and wired network entities. Basically, it is composed of panoply of service provider networks (SPNs) connected with an IP-based-core network for global routing. WLANs hotspots are managed by each provider.

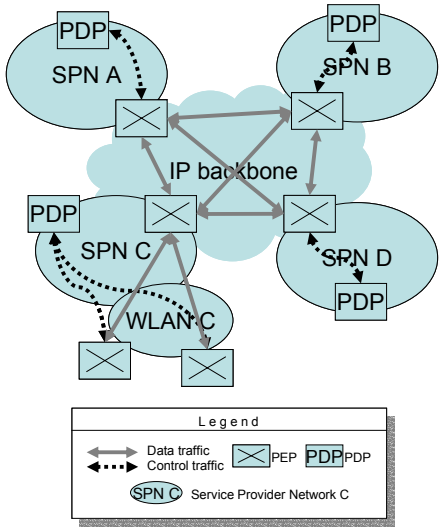

Figure 2 Global system architecture

Management tasks are fulfilled based on using management policies that reflect provider and customer requirements. For this purpose, main entities of COPS are included such as PDPs (Policy Decision Point) and PEPs (Policy

Enforcement Point). PEPs which are also edge routers are connected via high speed communication links.

IV.2. Service Provider Network Architecture

The proposed service provider network architecture consists of several entities acting in different planes (see Figure 3) and communicating by protocols depending on the plane and the nature of the entities. Actually, the functional architecture is composed of three planes: a business plane, a management plane and a network plane.

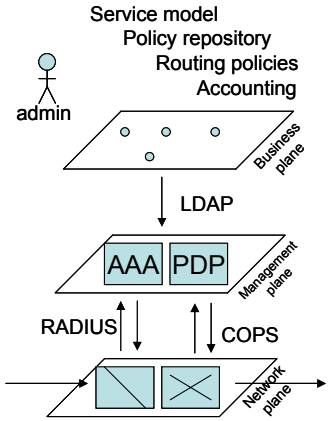

Figure 3 MMQoS planes

As illustrated in Figure 4, firstly, the operating system (OS) represents the user himself by executing all user commands. The OS uses the SIM-IP card to access the actual terminal equipment (TER), i.e. generally the network adapter. Secondly, the network itself is characterized by an edge device i.e. an access point (AP), the servers responsible for the core management functions and some optional user servers which depend on the provider as shown in Figure 4. The core services are described below as part of the actual architecture. Moreover, we want to propose the SIM-IP card to implement some of these core services. Such services include:

- Network access using 802.1X and RADIUS
- QoS based on COPS
- Service access based on IP-identification information within sent packets

Every provider claiming to support our solution has to integrate at least the necessary network access and QoS management services as presented here. As we will show later, the SIM-IP card actually is a part of the visited network. Indeed, since it can integrate network internal services and user control mechanisms, it is a necessary requirement. Hence, first the SIM-IP card connects to the visited (home or foreign) network. Obviously, due to the diversity of the potential physical networks, the SIM-IP card has to support the network access methods specified within each used technology. The card has to be able to answer the challenges of the edge devices of the visited networks, e.g. access points or base station transceivers since it is the only equipment which carries the needed identifiers and algorithms. Therefore, the first link, i.e. the wireless link between TER and AP is protected by ISO/OSI layer 2 (L2) encryption based on card-stored user credentials. In some later phase, the SIM-IP card verifies the user identity.

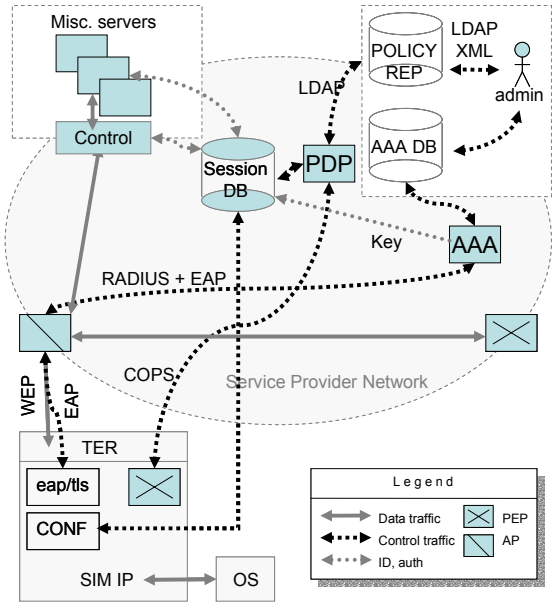

Figure 4 Service provider network architecture

However, the WLAN context is more complicated. The network access methods are not well-defined compared to telephone networks. For this purpose, we propose to apply the best method currently available. However, this mechanism does not solve the problem of user identification for service access since IP-services do not have the necessary L2-information at their disposal in order to verify user's identity.
We assume that the cores of the visited networks are internally secure or can be secured by the maintaining authority by the means of physical subnet separation, encryption or some other appropriate well-known measures. Hence, this work reasonably focuses on the security of the network access and of the network-to-user link protecting it from unauthorized usage.
Some databases are needed to carry user management information, we mainly distinguish:

- A policy repository maintaining all needed policies
- An AAA database (AAA DB) as a part of Radius authentication infrastructure
- A session data base (SessionDB) to collect all information on the connected users to the provider network

As clearly illustrated in Figure 4, both SIM-IP card and COPS protocol appear as the most important elements in our solution.

IV.3. SIM-IP card

IV.3.1. Description

The SIM-IP card is an IP-capable Java-based intelligent subscriber's identity module (SIM) with integrated services as it is shown in Figure 5. Similarly to the GSM/3G SIM cards, it provides a mechanism for user authentication and accounting. Additionally, it includes the IP functionality and can thus complete the terminals which do not support IP natively. The card carries a set of user credentials, the authentication procedures, algorithms and stores data in XML files. It can execute Java applets in a protected environment. In particular, it integrates a highly trusted web server and supports various protocols like HTTP, LDAP, COPS, EAP, etc.

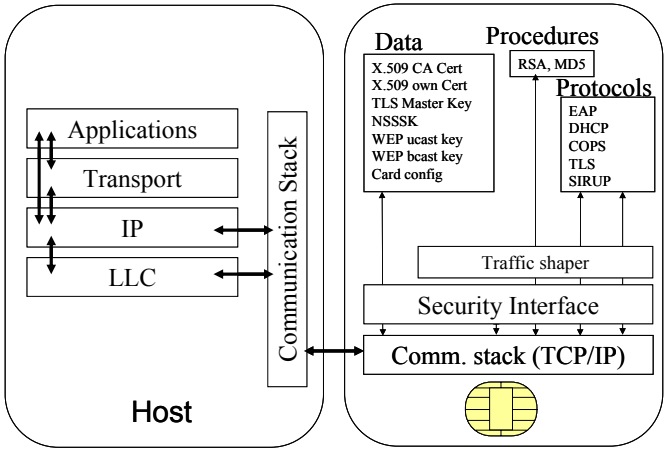

Figure 5 SIM-IP card

Basically, it can be seen as a network node with embedded services which offers three main advantages:

- Common, reliable and extensible authentication service
- TCP/IP stack independent from the associated terminal and thus acting as an Internet host
- An opportunity to include service end points on the card enables further interesting solutions

We want to use the SIM-IP in order to provide secure network access, QoS and network services on card. Since we plan to install network internal components on the card, each SIM-IP remains property of a provider. It is pre-configured by the issuing provider and seen as a trusted node of his network after successful connection. It can then provide network access to the user and apply classification and control of user traffic. Thus, we have two network access phases. In one phase, the card connects to the provider network using installed credentials and algorithms as already mentioned above. In the other phase, the card verifies the user (OS) credentials. Herein, the user (OS) verification is very simple since it can be processed internally by some proprietary algorithm (PIN, password, token, etc.). However, we still have to define a secure method for SIM-IP card access to the network, especially in the context of current WLANs.

IV.3.2. SoC concept

The integrated logic of the card and its mentioned IP capabilities enable service prolongation from the network till on the card. This gives new opportunities. A provider issuing a card could install some of its own classically internal control components such as e.g. classifiers, filters, packet counters, on the card allowing control or even enforcement of contract-consistent user behavior. On the other hand, a provider could integrate service access points in the SIM-IP card, thus offering to the user what we call Services on Card (SoC), i.e. services available directly from the card, independent of the actual location of the related service end point. After the connection phase, the service access points located on the card dynamically choose the service provider (home vs. foreign network) depending on the availability of the service in the currently visited network or on some other criteria such as service properties, etc.

Basically, the network access service already represents a network-internal service prolonged till onto the SIM-IP card. The card acts as an edge device which typically belongs to the network infrastructure. The control and enforcement points for QoS, mobility, encryption and packet signing belong to the same category. The other category contains the usual services like e.g. HTTP, SMTP or SIP. Such services can be implemented as proxies configured by default to contact the home network. The card issuer could assure the service availability in its network, thus designing its card according to its offer. In the case of the service presence in the visited network, the SoC-proxy can be dynamically reconfigured by the card logic and use the local service provider.

The advantage of this approach is the ability to provide access to home network services, higher service availability and complete service transparency for the user.

But is this approach always reasonable? Let P1,…,Pn be providers with associated SS1,…,SSn provided service sets, i.e. for each Pi there is SSi := {Service1, …, ServiceN}. Indeed, in the case where all service sets are equal (SS1 = … = SSn) user can always be sure to find the service in the visited network in a common way. In this case, the services on card would be useless.

In the case where the service sets are strictly disjoint, visited network services are unknown to the card and the home services are not available in the visited network. It results in the constant connection to the home network. Under some circumstances not even network access to the visited network could be provided. Thus, in this context, we speak about common minimal service subsets (MSS) defined as the result of the conjunction of all SSi. To provide the advantage of the SoC-idea, the MSS should at least consist of all services necessary for the defined management functions (access, QoS, etc.). Ideally, the MSS would be a real superset of the management services set but a real subset of the result of the disjunction of all SSi.

Moreover, for QoS provision, a module named Traffic Shaper is integrated in the SIM-IP card. It classifies the passing IP packets according to the used protocol/application. Different traffic classes are defined describing diverse criteria (delay, bandwidth, throughput, …). Each class is given a priority level.

IV.3.3. Implications

The SIM-IP card requires changes in the system configuration. First of all, the user applications on the host OS have to be configured in an appropriate way if they use SoCs. E.g. if a user uses an SMTP server, he configures an on-card SMTP server in his mail user agent. The on-card server could then act as a so-called smarthost relaying the messages to the actually used SMTP server. Secondly, we have to provide a discovery and dynamic configuration mechanism for the card itself, since after or during the authentication phase the card will have to know which services are actually available in the visited network. Then, at least for every potential SoC it is reasonable to reconfigure the on-card proxy respectively (e.g. configure the on-card SMTP-smarthost to point to the SMTP server available in the currently visited network).

Finally, we must not forget the implications on the security when putting potentially network-internal elements on the card. Usually, such "network-internal" protocols are not sufficiently secured by the protocol design itself. In order to prevent attacks, such protocols rely on other protection measures like e.g. underlying encryption layers (IPSec, secure tunneling, etc.) or appropriate network design (physical separation of user and provider-own traffic). In the case of the installation of network internal components on the wireless equipment, such protocol connections would be run in parallel to the user-traffic over an air-interface. Obviously, we have to secure such (management) traffic against every possible fraud.

IV.4. Common Open Policy Service protocol (COPS)

COPS [12] is a proposed standard protocol for exchanging network policy information between specific entities. In our architecture COPS plays one of the central roles. The standard describes a centralized architecture that consists of a central policy decision point (PDP) and a set of policy enforcement points (PEP) usually installed in the network edge devices. This enables centralized

QoS policy installation and management on the PDP and dynamic load-dependent policy adjustments and traffic control on the PEPs, i.e. network edges.
However, in the context of wireless access links this has one main disadvantage: the users can still behave incorrectly on the link between the terminal equipment and the edge device, i.e. exactly on the link with typically limited shared resources.
We propose to install the PEP on the SIM-IP card (see Figure 4). This gives new opportunities like e.g. enforcing QoS policies depending on the link load and controlling user traffic at its source preventing the OS (user) from sending incorrect packets. Then, we can optimize the load of the wireless links.
There is a security issue related to this proposition: as a network-internal protocol COPS is barely unprotected and still we propose to put its entities on different ends of wireless links. However, since COPS protocol information is exchanged after successful SIM-IP card connection to the visited network, the related packets will traverse the distance from the card to the secure core network over per-user L2-encrypted link. In this manner, assuming reliable encryption, no other user can read the data emitted by the AP or by the card even if this user is connected to the same AP. This is in particular also true for the WLANs due to the usage of dynamic WEP keys with rapid re-keying or even WEPv2 as explained in Section V.1.

V. Network access architecture

Typically, security features are considered as a focal point of each provider network. In this Section, we give the guidelines of how to secure our 4G architectural context taking into account user global roaming.

V.1. Card to network connection by 802.1X

As mentioned, we have to resolve the problem of secure SIM-IP card connection to the visited provider's network in the context of WLANs.
We propose to use IEEE 802.1X [13] with EAP/TLS [14] for the network port access control in the WLANs. This will help to resolve the currently existing flaws [15] in the provided WEP-based shared key authentication (SKA) of the 802.11 WLANs [16]. The needed architecture for this type of network access control consists of at least one central EAP/TLS-capable RADIUS-server and several RADIUS [17] and 802.1X capable APs. Additionally, in our proposition, every user-host is to be equipped with the SIM-IP card which stores the needed private key of the user (in the form of certificate), the certificates of the used certification authorities (CA) and the algorithms needed for the EAP/TLS method (see Figure 5). The SIM-IP and the network core RADIUS-server authenticate mutually by using TLS [18] transported in the EAPOL frames [13] and negotiate a TLS master secret [18]. Both sides then derive the communication keys called Negotiated Shared Session Secret Keys (NSSSK) independently. The RADIUS server sends this key to the AP together with the confirmation of the successful authentication, as described in [19]. The AP opens the associated communication port, creates the dynamic WEP keys and sends them to the SIM-IP card signed and encrypted by the communication key (NSSSK) in the EAPOL-Key frame [13]. The EAP/TLS method i.e. the SIM-IP card installs the received WEP-keys in the network adapter and activates WEP encryption on the link.
In this manner, the data transmission over the wireless link is first possible after the card's identity has been confirmed. Moreover, it is encrypted using dynamic WEP. The AP can and should change the used keys frequently. Till the release of WEPv2, this is the best method we can do to natively protect the SIM-IP card connection to the provider network in the WLAN context.

V.2. Roaming

The SIM-IP card is responsible for the verification of user credentials, traffic control and user service access. Since the user always connects to and through his SIM-IP card, no provisions for user roaming are necessary in our architecture. After card's reconnection the user can simply use the services in the same manner independent on the visited network.
Conversely, we have to provide mechanisms for SIM-IP card roaming. More precisely, there are three issues related to that problem:

- Roaming network access
- Roaming SIM-IP card configuration
- Roaming service access

Those will be described in the three following sections.

V.2.1. Roaming network access

IEEE 802.1X standard proposed here for card network access recommends RADIUS usage as backend authentication server. The access procedure itself is

described in Section V.1. Using RADIUS, it can be applied with minor changes to provide roaming.
The used 802.1X EAP-method (EAP/TLS) requires certification authorities and certificate deployment. However, a common Public Key Infrastructure (PKI) is not necessary i.e. every provider can simply install and maintain his own independent CA. Besides, the certificate deployment is particularly easy, since the certificates are to be installed in the card and the latter is issued by the provider. Using RADIUS feature called proxying [17], we can enable card roaming with local 802.1X. The EAP/TLS conversation takes place between the SIM-IP card and its home RADIUS-server over the AP and the foreign RADIUS-server. The home RADIUS-server delivers the session key (NSSSK) to the foreign RADIUS server which hands it to the concerned AP.
The necessary provision for RADIUS proxying is the RADIUS-server interconnection of the concerned providers. For security reasons, we propose to interconnect the concerned RADIUS servers by using IPSec protocol.
Detailed exchanges, security considerations and thinkable more optimized solutions are presented in [20].

V.2.2. Roaming SIM-IP card configuration

The whole connection procedure can be subdivided into four main phases:
1. The card physically connects to the visited network; negotiates WEP keys and establishes an encrypted L2-link. This is described in the previous section.
2. The card executes a DHCP query and obtains its own IP address and the IP address of the SessionDB server. The card connects to the SessionDB server using the proprietary SIM-IP Roaming Update Protocol (SIRUP). The SessionDB connects to the card's home network if necessary using RADIUS and exchanges user accounting information. During SIRUP conversation, the card obtains the configuration information, the necessary available service and QoS class descriptors, etc.
3. The card presents a login possibility to the user proposing him information about the visited network, i.e. particular available services and e.g. prices. The user logs in using his user/password combination.
4. Depending on user's choice or launched applications; the card negotiates and reserves the QoS.
The SIM-IP Roaming Update Protocol (SIRUP) is the most important part of the process. This protocol is to be developed but since the card is already equipped with a TLS protocol stack, the involved methods (RSA, MD5, etc.) and HTTP, we plan to base it on HTTPS. This is particularly easy since there are provisions for applet handling and Java integration in HTTP. In fact, since the RADIUS server and the EAP/TLS method have already negotiated a TLS master secret, we can directly proceed with the next TLS phase which will encapsulate the whole HTTP transfers. For that reason, the RADIUS-server writes the key information in the SessionDB after successful user connection.
During the SIRUP TLS conversation, the SessionDB installs the bidirectional IP-to-user mapping which it extracts out of arriving TLS-protected IP packets. It gives access to this information to all registered network services.
Additionally to the information on the available QoS classes and user services, the card could download and install new applets. Those could be proxies or, in the home network, core service updates. The card uses obtained network information in order to properly configure its service access points.

V.2.3. Roaming Service access

The user based L2 encryption ends are the SIM-IP and the AP. Hence, after the packets finally arrive in the IP-based part of the provider network, no user identity information remains included in those. So, how could we possibly identify the user in order to provide him personalized service access? The only information which is still included in the IP header is the source IP address itself. Due to the simplicity of the so-called IP-spoofing attack, this mechanism usually can not guarantee reliable user identification. We believe that with some changes this simple but powerful identification method can be used in a relatively secure way.
The IP-configuration information provided to the card by DHCP is transported over the per-user encrypted L2-link so it can not be sniffed by attackers. The host OS reacts with a DHCP request on the link establishment event. This message will be intercepted and replied to by the SIM-IP card, thus providing the OS (user) with the necessary IP information. From now on, every packet issued by the OS will be verified by the SIM-IP for its source-IP correctness. With the assumed security of the provider network itself, the personal L2 encryption till to the edge device and the impossible IP-spoofing by the connected users (due to the card-based control), no packets with wrong source-IP address can enter the network.
Servers are to be located in the IP-based part of the provider network, which is physically or logically (subnetting, firewall or packet filter) protected from whichever access originating in the public networks like e.g. the Internet.
The SessionDB uses the SIRUP conversation with the card to map the user identity to an IP-address. The obtained mapping can be easily used by all

network servers. The SessionDB installs the appropriate routing rules for card's source IP e.g. allowing or disallowing the Internet traffic. Each service being requested access by some source IP can identify the user by interrogating the SessionDB.
For roaming purposes, the two concerned providers maintain an IPSec tunnel. The traffic from card's source IP to its home network should be routed over this IPSec-tunnel. Then, the IP-to-user mapping obtained from the visited SessionDB can also be used by the home network servers in order to allow or bill service access.

VI. Conclusion & future work

In this paper, we underlined some critical issues that appear in the context of future 4G heteregeneous mobile networks such as network control access, roaming and QoS. Mainly, the flexibility and distribution are the principal features to be addressed to build a suitable architecture that fulfill these requirements. Thus, we give the main guidelines for designing a new and open-architecture composed of a collection of network providers. We restrict ouselves to a case which consists of an interconnection of remote WLANs hotspots. Then, we focus particularly on the network access control since it is a main point of the study undertaken in this work. For further work, we intend to demonstrate the feasibility of applying the proposed concepts and to evaluate the cited approaches through a testbed in terms of protocol functionality and software performance.

VII. References

[1] L.M.S.C of the IEEE Computer Society, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: Higher Speed Physical Layer Extension in the 2.4GHz Band", IEEE standard 802.11b, 1999 Editions, 1999.

[2] V. Bharghavan, "Challenges and Solutions to Adaptive Computing and Seamless Mobility over Heterogeneous Wireless Networks", International Journal on Wireless Personal Communications, 1996.

[3] C. Lindemann, M. Lohmann, A. Thummler, "Adaptive Performance Management for Universal Mobile Telecommunication System Networks", IEEE Computer Networks, 2002.

[4] P. Trimintzias and al., "A Management and Control Architecture for Providing IP Differentiated Services in MPLS-Based Networks", IEEE Communication Magazine, 2002.

[5] http://www.80211hotspots.com/, http://www.seattlewireless.net

[6] http://www.homerun.telia.com/

[7] VoiceStream website "VoiceStream - Global Wireless by T-Mobile", http://www.voicestream.com

[8] GSM 11.11, "Digital Cellular Telecommunication System (Phase 2+), Specification of the Subscriber Identity Module – Mobile Equipment (SIM-ME) Interface".

[9] 3GTS 33.102 Release 99, "3GPP: Technical Specification Group (TSG), 3G Security: Security Architecture".

[10] The website of the MMQoS project, http://www.mmqos.org

[11] P. Urien, A. Tizraoui, M. Loutrel, K. Lu, "Integration EAP in SIM-IP smartcards", Workshop ASWN, 2002.

[12] D. Durham, Ed., J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry, "The COPS (Common Open Policy Service) Protocol", RFC2748, Internet Society , January 2000

[13] L.M.S.C of the IEEE Computer Society, "Port-Based Network Access Control", IEEE Standard 802.1X, June 2001

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

[15] N. Borisov, I. Goldberg and D. Wagner, "Intercepting Mobile Communications: the Insecurity of 802.11", Proc. Of the 7th ACM International Conference on Mobile Computing and Networking, July 2001.

[16] L.M.S.C of the IEEE Computer Society, "Wireless LAN medium access control (MAC) and physical layer (PHY) specifications", IEEE standard 802.11, 1999 Editions, 1999

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

[18] T. Dierks, C. Allen, "The TLS protocol version 1.0", RFC 2246, IETF June 1999.

[19] G. Pall, G. Zorn, "Microsoft Point-To-Point Encryption (MPPE) Protocol", RFC 3078, March 2001.

[20] A. Hecker., H. Labiod, A. Serhrouchni, "Authentis: Through Incremental Authentication Models to Secure Interconnected Wi-Fi WLANs", IEEE ASWN 2002, Paris