Abstract—This paper describes the implementation and deployment of a novel architecture for a metropolitan open wireless access network, shared among different service providers. A layered model that differentiates four different actors (user, Wireless Island, Neutral Operator and Service Provider) is introduced, and the mechanism to allow Service Provider selection by the user is detailed. Other key technical issues like AAA, security, redundancy and scalability are also analyzed. This testbed has been used to provide Internet access to different user communities related to our University and as a experimentation platform for service deployment and testing in a real-life scenario.

I. INTRODUCTION

Wireless access has already become an ubiquitous way to connect to the Internet. With the development of low cost hardware for wireless networking based on IEEE 802.11b/g technology, many access points are deployed in cities around the world. However, this access points belong to private companies and individuals, and cannot be used by the general public.

At present, second and third generation mobile networks offer connectivity with well-defined authentication and authorization procedures for a large customer base, but at lower speed and higher costs than WiFi Networks.

A combination of the two would be desirable, that is, a wide-coverage high-speed low-cost public access network.

A solution to this situation consists in the use of an Open Access Wireless Network, shared by multiple service providers [1] [2]. The idea of the Open Access Network (OAN) consists in decoupling the access and the service provisioning layer. Access to the networks is provided by Wireless Islands that are sets of access points that are deployed and maintained by small network operators. Service Providers (typically Internet Access Providers) offer their services to those users found in the coverage areas.

The rest of the paper is structured as follows: Section II presents the OAN conceptual model, describing the participating actors and their relationships. An economical sustainability model is also suggested. Section III deals with technical issues such as the provider selection mechanism, AAA requirements, Scalability, Redundancy, Security and Location-Aware services. Section IV describes the actual deployment of the concept and offers measurements of real use of the network. Section V offers a vision of the growth of the network and further deployments, analyzing the encountered problems and proposing a solution. Section VI overviews other similar initiatives and finally VII concludes the paper.

II. THE OPEN ACCESS NETWORK MODEL

The Open Access Network model separates physical access to the networks from service provisioning. The same OAN will be used by a number of different providers that share the investments and maintenance cost. This scenario is opposed to the traditional mobile telecommunication model in which each operator owns a different access network and offers services based on that network.

A user that connects to the OAN will be offered a range of services provided by different Service Providers and will have the opportunity to register to one or more of them. Optionally, the Service Provider may charge the users for the services offered. Anyone that has an interesting service can offer it through the OAN without deploying a new network.

A. Actors involved and relationships between them

The OAN architecture is horizontally layered as shown in Fig. 1. Each layer accomplishes a task and is associated to a different actor. The definition of this layers and the interfaces between them gives a starting point to understand the architecture.

The model proposed here differentiates four different actors: 1) Users: The users are the customers of the telecommunication services. The users must have a terminal with a wireless network interface card, that allows them to reach the service providers through the OAN.

2) Wireless Islands: They offer communication services between the users and the Neutral Operator Backbone. Wireless Islands deploy and manage a set of wireless access points that are connected to the backbone. When IEEE 802.16 is available it might be used to provide connectivity with the final user or as a backhaul technology between the Wireless Island and the closest point-of-presence of the backbone.

3) Neutral Operator: It is the central part of the model. Deploys and maintains the Backbone Network connecting the Wireless Islands and Service Providers. It presents the user a list of the different available Service Providers and then manages the connection between the user and the chosen provider.
4) Service Providers: The service providers are those companies or organizations that offer value added services or long distance communication to the users. A few examples would be Internet access, localization services, and e-government services.

B. Sustainability Model

An important aspect when analyzing the OAN model is its sustainability in a commercial environment. Otherwise, it would be relegated to a nice laboratory experiment. To assess and validate its viability, an extensive economic and organizational model has been presented in [3]. Specifically, a payment scheme among all the players involved is presented and evaluated, to ensure the economic viability of the whole system. Its main characteristics are summarized here.

The final users pay for the whole service (including access) to the Service Providers applying a flat rate, a per use time/traffic price scheme or any other payment model deemed appropriate by every Service Provider.

The Service Providers pay regularly to the Neutral Operator for the usage and availability of the network. This payment is composed of a fixed rate and a variable rate based on the real usage (traffic or bandwidth) of the network by that Service Provider’s users.

Part of the income obtained from the Service Providers is dedicated to cover the management expenses of the OAN infrastructure, as well as provide a sufficient profit to its stakeholders. The rest of the income will be shared by the Wireless Islands, proportionally to the traffic generated by their access networks.

In order to guarantee its neutrality, the Neutral Operator could be a non-profit organization in which all the actors are represented. In that case, only the management expenses would have to be covered.

III. OAN ARCHITECTURE

A. Provider Selection

The final users of the Open Access Network should be able to choose one Service Provider among many. When a user connects to the Open Access Network for the first time is assigned to a virtual default provider. This provider does not offer any service, but allows the user to choose a real provider from a list.

The implementation follows the idea originally stated in [4] in which every Service Provider has its own level-3 network on top of a unique level-2 access network. The lower section of Fig. 2 shows that the Access Network contains multiple IP-Subnetworks, three in this example. Subnet 10.0.0.0/24 belongs to the default provider, subnet 10.0.1.0/24 to Provider 1 and subnet 10.0.2.0/24 to Provider 2.

The Provider Selection Server is owned by the Neutral Operator and maintains a database with two tables. The first one contains information about the different Service Providers operating in the network, while the second associates every terminal (identified by its MAC address) with one of the Service Providers. It is understood that if a terminal is not listed in the database, it belongs to the default Service Provider. For each Service Provider there is a DHCP Server configured to assign IP configuration for the clients of that provider (See upper part of Fig. 2).

When a terminal joins the network, it sends a DHCPREQUEST packet. This request is collected by a slightly modified BOOTP Relay Agent [5] that runs on the Provider Selection Server. This agent looks for the terminal’s MAC address in the second table of the database to know to which Service Provider is the user registered, and finally forwards the DHCPREQUEST to the corresponding DHCP Server.

User A in Fig. 2 is not registered with any provider, therefore its MAC address is not listed in the database. User A broadcasts a DHCPREQUEST, the Provider Selection Server receives it, looks at the database, and since the MAC address of terminal A is not there, it forwards the request to the Default DHCP Server which offers the IP 10.0.0.26/24 and default gateway 10.0.0.1 which is the Provider Selection Server.

On the other side, User B is already registered with Provider 1. When User B joins the network, it broadcasts a DHCPREQUEST, the Provider Selection Server receives it, and looking at the database realizes that User B is already registered with Provider 1. For this reason it forwards the request to DHCP Server 1. This server offers configuration from another IP subnet (10.0.1.30/24) and default gateway 10.0.1.2. In order to perform the relaying transaction, the Provider Selection Server needs an IP of the range assigned to Provider 1. For this reason, it uses a virtual interface on the Access Network side with IP 10.0.1.1/24.

User A, not yet registered to any provider, opens a browser and tries to surf. First a DNS query is resolved transparently for the user, since the Provider Selection Server allows DNS traffic. Then, the browser performs a HTTP request which is intercepted by the Provider Selection Server. As an answer, the user receives a form where any of the different Service Providers operating in the Open Access Network can be chosen. The user selects one of the Service Providers and the selection is stored in the database. The next time that user A renews its IP parameters, it will receive a configuration ac-
To facilitate the regular operation every time a user wants to use the network, the user selection is stored in the database and the system uses this information for future network sessions. However, the users should be allowed to change the provider they are registered to at any time. Therefore, every Service Provider that operates in the OAN is required to present a form to the users whenever they begin a new session. This form must contain the terms of use and a link to the provider selection form. A user that changes from one provider to another is requested to renew the IP configuration for the new selection to become effective.

The Access Network is a completely open environment. Unauthenticated users can access to self-register to any of the Service Providers. Because of the use of standardized protocols for registration ([6],[7]), the users do not need to install any specialized client in their computers. User’s Authentication, Authorization and Accounting are left to the Service Providers.

**B. Users Authentication, Authorization and Accounting**

The Access Network is an open environment, consequently the access control has to be performed at the interface between the Access Network and the Service Provider’s network. Every Service Provider is free to apply its own Access Control Policy. However, we suggest an AAA architecture with three different entities: Access Server, Authentication and Authorization Server, and an Accounting Server (See Fig. 4).

The Access Server is an element placed by the Service Provider between the Open Access Network and the protected network, where the services can be found. The Access Server behaves as a dynamic firewall, and allows only traffic from (or for) authenticated and authorized users.

When the Access Server receives HTTP traffic from an unauthenticated user, it redirects it to the Authentication and Authorization Server (from now on, Auth Server). The user has to provide some kind of credentials, typically username and password, to prove his identity. In case of successful authentication, the Auth Server informs the Access Server about which services the user (identified by IP and MAC addresses) is subscribed to. This option has been incorporated to our testbed.

A variant of this procedure consists in the Auth Server offering the user a signed token with authorization information after successful authentication. Then the user hands out this token to the Access Server to obtain access to the desired services.

In any case, the Access Server provides the Accounting Server with accounting information. This reports detail which services have been used, the period of time they have been accessed and the amount of traffic they have generated. This information can be used for billing or auditing purposes. The accounting possibility has not been implemented in our testbed and remains for further study.

A Service Provider could also use SIM card and GSM authentication, authorization and billing schemes as described in [8].
Fig. 4. Service, accounting, authentication and authorization reside in the protected part of the network, separated from the open (unprotected) part by the Access Server.

C. Scalability, Redundancy, Security

The access network consists of a level 2 broadcast domain. This implies certain scalability and security issues. Since it is a switched network, every station receives its own traffic and also broadcast traffic. As long as broadcast traffic is kept low, no efficiency problems will arise. The only broadcast traffic that Linux client terminals generate is ARP and DHCPREQUEST, when they join the network or when their IP lease time expires and they can not reach the DHCP server with unicast packets. Windows client terminals, in addition to DHCP and ARP traffic, generate NetBIOS traffic.

NetBIOS traffic is not necessary to provision the basic services of connectivity offered by the access network, and allowing such a traffic implies a risk of virus propagation. Therefore, NetBIOS traffic should be intercepted and dropped by the switches of the access network.

The Provider Selection Server is a single-point-of-failure of the presented architecture. For the access network to be reliable, a secondary Provider Selection Server should be ready to substitute the primary one in case of malfunction.

Access Servers use the packet’s IP and MAC address to identify to which user it belongs. Apparently, a malicious user can spoof both IP and MAC address of an authenticated user to hijack a connection [9]. However, two stations can not coexist with the same IP and MAC addresses in the same subnet. TCP connections would be reseted and connection aborted. As a consequence, the authenticated user would not be able to renew the session and the access for the hijacked IP and MAC would be forbidden shortly.

[10] identifies the problem of lack of mutual authentication between the user and the Auth Server. A fake Auth Server could be used to obtain the user’s credentials. To avoid this security threat, Auth Servers should be forced to hold a valid certificate signed by a trusted third party that can be recognized by the user.

Being the access network an open wireless environment, any information sent or received by the users can be eavesdropped. Therefore, the use of upper-layer security protocols (such as IPSEC [11] or SSL [12]) is encouraged when transmitting sensitive information.

The proposed model is not resilient to DoS attacks. However, since 802.11 itself is vulnerable to this kind of attacks [13], we consider this problem out of the scope of the article.

D. Location Services

To foster the adoption of the OAN model, value-added services should be offered. For this reason a location service provider has been developed [14], so that the OAN users may access third party location-aware contents. A network-based approach has been adopted to obtain the location information, to avoid the installation of any software in the client terminal.

Different alternatives were considered to obtain the location information:

- If 802.1x is used, the logs of the associated RADIUS server provide information about the association of the terminals to the access points.
- Since the access points are usually configured like a transparent bridge, the clients associated to a given access point can be inferred by looking at the access point’s bridging table. The forwarding table belongs to a standard MIB that usually is supported by all manufacturers.
- Another solution consists in polling the access point to obtain the association table, present in a manufacturer-dependent MIB.
- Finally, SNMP traps can be triggered whenever a terminal associates to an access point, providing the association information while avoiding the polling.

The RADIUS solution was not appropriate because the open access network does not use 802.1x protocol. The refresh time of forwarding tables lead to an unacceptable response time. Finally the unreliability of the SNMP-Traps made that solution undesirable. Thus, the adopted solution consists on having a Location Server keeping track of the users by polling every access point to get the list of associated users.

Table I summarizes the advantages and problems associated to each of the proposed solutions.

<table>
<thead>
<tr>
<th>Solution</th>
<th>Advantages</th>
<th>Problems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Polling</td>
<td>High accuracy, no need for software installation</td>
<td>Long response time, unreliable</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>Low response time, no need for software installation</td>
<td>Limited accuracy, high overhead</td>
</tr>
<tr>
<td>RADIUS</td>
<td>High accuracy, no need for software installation</td>
<td>Long response time, limited accuracy, high overhead</td>
</tr>
<tr>
<td>Location Service</td>
<td>High accuracy, no need for software installation</td>
<td>Long response time, limited accuracy, high overhead</td>
</tr>
</tbody>
</table>

The location information can be distributed to any trusted location-aware application (LAAP) in the Internet, given the user’s explicit authorization. In a typical scenario clients use a LAAP application that is composed of a series of web pages. At a certain point this application needs to know the location of a user to provide him with some contents that are tailored to his location. To obtain this information, the LAAP application has to go through the following steps:

1) It has to redirect the user to a web page that is on the Locator System machine. During this redirection the LAAP application has to pass also three parameters: `name`, `token` and `url`. The `name` is a string that identifies uniquely the LAAP application. The `token` is a string that identifies uniquely this particular user between all the others that are using the LAAP application. The `url` is a string that indicates the place where the user should be redirected, after the authorization page.

2) The Locator System presents the user with a web page in which he has to agree to provide his location information to the LAAP called `name`.
3) If the user has agreed to the previous web page the Locater System redirects the user to the url.

4) When the LAAP receives a request from the client at the resource identified by the parameter url, it can finally ask his location to Locater System using the name and token variable that uniquely identify the user. The LAAP will be allowed to access this information for a certain amount of time, after that it has to redirect the user again to the Locater System web page to get authorization from the user.

The location information is private and sensitive. The described procedure guarantees that this information will be delivered only to well-known LAAPs after the user authorization.

IV. NETWORK AND SERVICE DEPLOYMENT

Universitat Pompeu Fabra adopted the implementation proposed in [2] to create a campus-wide open access network. The campus is composed of five different areas distributed across the city, interconnected by a university MAN. All the access points are connected to the same VLAN.

A seminal implementation of an OAN has been developed at the KTH University in Stockholm [9]. This implementation consists of an 802.2 link level compatible network to which both clients and servers connect. The access network provides two main services: user self-registration to a Service Provider via a web-interface and client IP and default gateway configuration via a DHCPREQUEST relayed to the chosen Service Provider.

In this implementation, Authentication, Authorization and Accounting are left to the Service Provider, since the goal is to provide a common access system with a minimum number of shared services. Therefore, the access network has to be completely open to anyone who wants to connect to it, since unregistered users need to connect to choose their Service Provider.

The idea that lays behind this system is a modified use of the DHCP relay agent [5]. Once the user has chosen a Service Provider, the selection is stored in a database. When the DHCP relay agent receives a DHCPREQUEST from that user, it forwards the request to a DHCP server of the chosen Service Provider. Then the user obtains an IP address and a default gateway of that Service Provider.

This is the approach adopted at our University. The Provider Selection Server includes a DHCRelay agent, a database and a few PHP pages. The terminal to be configured has to be DHCP enabled and needs an HTTP browser as well. In addition to the Provider Selection Server, a DHCP server for each Service Provider is needed.

<table>
<thead>
<tr>
<th>PROS</th>
<th>CONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS</td>
<td>Low response time, low network usage</td>
</tr>
<tr>
<td>SNMP forwarding table</td>
<td>Standard MIB</td>
</tr>
<tr>
<td>SNMP association table</td>
<td>Low response time</td>
</tr>
<tr>
<td>SNMP trap</td>
<td>Low response time, low network usage</td>
</tr>
</tbody>
</table>

A route from the DHCP server to the Provider Selection Server’s private address is needed. Creating such a route through the Internet might be complicated. Our proposal is that the DHCP server resides in the same computer as the Access Server, so that the answer to the Provider Selection Server can travel through the access network.

The database used to implement the Provider Selection Server is PostgreSQL database that contains two tables. The first one stores information related to each Service Provider, namely the associated DHCP server, the Service Provider IP subnet and the authentication URL. The second table associates client MAC addresses to a Service Provider.

Tables II and III show examples of the contents of the database.

<table>
<thead>
<tr>
<th>mac_addr</th>
<th>provider_id</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:0B:CD:SC:51:85</td>
<td>2</td>
</tr>
<tr>
<td>00:10:A4:EC:D7:4C</td>
<td>2</td>
</tr>
</tbody>
</table>

The DHCRelay is modified in such a way as to be able to relay DHCP requests to the DHCP servers of the different providers depending on the requesting client MAC address. If the MAC address appears in the database means that the user requesting configuration is already associated (registered) to a Service Provider. Then the DHCRelay will forward that DHCPREQUEST to the Service Provider’s DHCP server.

If the MAC address cannot be found, it belongs to an unregistered user and the request is forwarded to a default DHCP server that will assign a temporary configuration. This configuration will allow the user to browse the register web pages to choose a provider. The default DHCP lease time will be short (about 30 seconds), since it is only a temporary configuration that has to be changed once the user has registered.

The register web pages are written in PHP, and access the database to get a list of the Service Provider available. Once the user has chosen a Service Provider (has registered) its MAC address is stored into the database together with the selected Service Provider. The next time the user’s terminal sends a DHCPREQUEST, it will be forwarded to the selected Service Provider DHCP server, and the user will get the right configuration for that Service Provider.

The Provider Selection Server needs two network interfaces. One connected to the access network while the other one should be able to reach the different Service Provider’s
TABLE II

Example of the T PROVIDER table, that stores relevant information of each SERVICE PROVIDER

<table>
<thead>
<tr>
<th>provider_id</th>
<th>provider_name</th>
<th>provider_dhcp</th>
<th>provider_auth_url</th>
<th>provider_net</th>
<th>provider_netmask</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>default</td>
<td>193.145.43.230</td>
<td><a href="http://10.0.0.1">http://10.0.0.1</a></td>
<td>10.0.0.0</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>2</td>
<td>upf</td>
<td>193.145.44.71</td>
<td><a href="http://10.0.1.2">http://10.0.1.2</a></td>
<td>10.0.1.0</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

DHCP servers. Of course, there cannot be any other DHCP or DHCRelay servers listening on the access network. The Provider Selection Server does not route any traffic, with the exception of DNS resolution. Additionally redirects all HTTP/HTTPS traffic to the local web server. As a result, when the unregistered user request any URL, the register form is presented (See Fig. 5).

A. Wireless Islands and Service Providers

Two different organizations participate in the deployment of the University OAN, the Universitat Pompeu Fabra (UPF) and the Institut d’Educació Continua (IDEC). Both can be considered Wireless Islands and Service Providers at the same time. Access Points are deployed in the different facilities that these institutions own throughout the city, providing the coverage map shown in Fig. 7.

There is a total of five relevant Service Providers operating in the University OAN. The UPF Service Provider offers connectivity to the academic network and to the Internet for the university community. Similarly, the IDEC has its own Service Provider. These providers can be seen in the OAN’s provider selection form in Fig. 5.

There is still another provider for researchers called MobiiCAT that connect the OAN with the regional experimental advanced network i2CAT. Attendants to conferences held in the University facilities use their own Service Provider with limited access to the Internet, called Congress. Finally, there is a development service provider that is not intended for the public use, but for the validation of new services.

B. Measurements and Validation

Between the months of November 2004 and June 2005, data related to the growing and usage of Barcelona’s Open Access Network has been acquired and analyzed. The database in the Provider Selection Server has been automatically accessed every day to record the number of terminals registered to the different service providers. Additionally, a tool has been developed to parse the logs of the access servers and store the relevant information into a database. This information consists in a user identifier and the time at which the user starts and closes a session.

1) Number of registered terminals: When a user registers with a provider, the MAC of the terminal together with an identifier of the provider is stored in a database in the Provider Selection Server server. Fig. 8 shows the evolution of the
number of registered terminals from March to May 2005.

More than 1500 MAC were registered in three months, most of them (about 80%) with the UPF provider. The IDEC provider is the second in terms of registered users (about 10%). The rest of the providers add up another 10%. One of the advantages of the open access model is that it enables the provision of specific services to small groups.

2) Number of active users: the number of registered users might not reflect the actual network usage. For this reason we have chosen to count the number of clients that use the network everyday. Figure 9 shows the number of daily users for the provider UPF and Figure 10 shows the number of daily users for the provider IDEC.

3) Number of sessions: Every user may establish a number of different sessions during the day. For example, in a meeting room on the morning and in a lab at the afternoon. The number of daily sessions for the providers UPF and IDEC is represented in Figures 11 and 12.

The plots for the number of sessions follow the same tendencies than the ones showing the number of users. In both providers we can detect that the usage clearly decreases during holidays periods.
V. WORK IN PROGRESS

After the validation of the model in the Universitat Pompeu Fabra, the expansion of the existing OAN and the deployment of a new one is in progress. We briefly explain here the main developments currently under way.

A. COSF: Software kit for implementing the neutral operator

An open and free software kit has been developed and distributed to the other universities of Catalonia to create a regional University OAN. Once the integration is concluded, the students and personnel of each university will be able to access the network of their own university from the facilities of anyone of the others. Each university will act as a Wireless Island for all the users and as a Service Provider for its own community.

B. Barcelona’s ICT district 22@bcn

The City Council of Barcelona in collaboration with our research group has set up the initiative 22@WiFi, whose primary target is to deploy a Wireless Neutral Operator to support different telecommunication services in the business district 22@bcn. The main objectives are:

- To enrich the telecommunication services supply in the 22@bcn district.
- To facilitate the market entrance to service operators, reducing the barriers to entry.
- To make a pilot network infrastructure deployment, which will be shared among different Service Providers.
- To make wireless access in public locations managed by the city council, available to all citizens and service operators in a transparent and non-discriminatory way.

In order to carry out the project, the City Council is promoting the implantation of a Wireless OAN that will use part of the municipal network infrastructure based on optical fiber as a backbone.

C. The testbed as a platform for advanced service development and testing

As a testbed, the system presented here serves two purposes: On the one hand, to improve and further develop the OAN model, e.g. with the introduction of location-based services (see [14] for details). On the other hand, to serve as a real-life platform for the development and testing of advanced services. As way of example, at Universitat Pompeu Fabra, the OAN platform is currently being used to support the development of a VoIP over Wireless network service for the University students and staff, providing the necessary infrastructure and management system for itinerant access. Additionally, it is also being used as a platform with real users for testing other research-related advanced services in a real-life setting with a large number of users.

D. Lessons learned and proposed solution

The original project contemplated the possibility of extending the OAN to the other universities in the region. However, a number of weaknesses were identified that slowed down the planned growth. These weaknesses related to the fact that the access network was actually a huge level 2 network. The use of such a big broadcast domain implies security threats and its scalability was put in question.

In addition, the OAN concept is going to grow beyond the university campus to a metropolitan-wide OAN. The Service Providers on that OAN will be private enterprises charging the users for the offered services and paying to the OAN for the use of its network resources. But the universities are reluctant to let the private companies benefit from their network infrastructure.

For this two reasons, a modified architecture is proposed (Fig. 13) to allow the segmentation of the access network while maintaining the main principles of the original implementation.

The access network is divided into a number of VLANs, each of them with its own Provider Selection Server. Some Service Providers might offer their services in different VLANs. It is the case of Service Provider 2 in Fig. 13. For example the Municipality can offer the cultural agenda or free cartographic information about the city, and that information has to be accessible both from the campus and from the street. In the case that a service provider wants (and it is allowed) to offer services in different VLANs, the corresponding access server has to be connected to multi-VLAN port. This solution is currently being incorporated to our testbed.

VI. OTHER RELATED INITIATIVES

The neutral operator idea, in the form presented in this paper, was pioneered by Stockholm Open, an initiative launched by KTH University at the turn of the Millennium. It was based on the deployment and operation of a mixed fiber-wireless access network in the greater Stockholm area, to provide Internet access to Swedish citizens and companies.

The WILMA project [15] [16], operating in the city of Trento, takes a different approach to the concept of OAN. In
The mechanisms that allow a user to choose among a list of different providers and the required AAA policies are detailed. Security, redundancy and scalability issues are discussed. A location information service for open access networks is envisioned and implemented. The actual deployment of the system in the University enables us to check the system's functionalities against real-world usage.

Further deployments and other related initiatives are summarized in the last part of the article.

ACKNOWLEDGMENT

The authors would like to thank to the Security and Communications Services of Universitat Pompeu Fabra for the deployment and administration of the University Open Access Network. To the undergraduate students A.M. Moreno and F. Callejas for providing the data shown in the plots throughout this article. The results presented in this article have been obtained from the Open Wireless Catalonia (COSF) project funded by the Generalitat local government and I2CAT foundation. Barcelona’s Metropolitan Open Access Network is funded by the city Hall and SIMA project (TIC2003-07279-c02-01). Finally, the authors wish to thank the anonymous reviewers for their constructive comments.

REFERENCES