Wireless Campus Project

C.E. Marchioro, A. Ghittino, D. Ferri, R. Borri
CSP innovazione nelle ICT s.c. a r.l., Italy

F. Dovis
Polytechnic of Turin, Italy

Abstract – **This paper addresses Wireless Campus project as a WLAN service deployment and test-field development experience.**
Will be covered aspects about the network, administrative issues and infrastructure and RF coverage. Then will be given details about security problems and solution proposed and mobility issues. Finally will be presented our solution proposal for LBS services to be deployed inside campus.

1. INTRODUCTION

The Wireless Campus project is a research and development initiative jointly performed by the "CSP" Italian Information Communication Technology research centre and the "Environment Park" technology park.
Its primary objective consists in deploying a 802.11b compliant Wireless Local Area Network (WLAN) inside the technology park and other regional sites, both to sustain a real distributed environment scenario of service and create a permanent research laboratory on mobile networks technologies.
The plant is projected as a distributed network including a core hot-spot (in Environment Park) that has aggregating function for other hot-spots in regional territory, all connected through a cabled backbone to the primary one. In this way each society or laboratory located in the technology park can share centralized services with mobile users of a WLAN deployed in other sites. Mobile users from different sites of the same enterprise can therefore access internet/intranet services through a connection to the cabled backbone.

2. WIRELESS CAMPUS NETWORK INFRASTRUCTURE

The network infrastructure is comprised of a core group of access point 802.11b located in proper areas of the park. They cover both internal dedicated areas to provide exclusive internal user services and common areas, e.g. conference centre and the restoration local.
The access points link terminals to a centralized management service centre, which performs DHCP server functions, access points control and management, and user location information storage.
Finally, authentication RADIUS servers support user AAA services, while VPN servers provide tunnelled secure connections for internal users through the APs located in common areas.

3. SECURITY

Security is actually one of the primary issues related to the project. This focus is due to the peculiarities of radio medium, that is difficult to confine and control: key issues about data security are access control and transmission protection.
In particular, the WEP protocol has proven its weaknesses to key-breaking attacks as referred in [1] [2]. Even if many vendors have updated their devices software in order to provide less "interesting" initialisation vectors for WEP ciphered packets, the exclusive use of WEP techniques is not practicable to provide user authentication inside the network.
For this reason, further mechanism have been considered in realizing user AAA subsystem, like 802.1x. IEEE 802.11 standards Task Group on security is working to standardize a long term security architecture for 802.11 and the cornerstone of this solution is the recently approved IEEE 802.1x Standard for Port based Network Access control [3]. The 802.1x standard is intended to provided strong and mutual authentication between users and WLAN network elements, but also access control and key management.

a. AAA SCENARIOS

Wireless Campus primary aim is to create a mixed service environment in which different service models can be reproduced for analysis purposes. The previous service access requirements have been met through the distinction between common areas and internal areas.
Internal areas have the prerogative of providing access for internal people only.

That's to say that every internal user can access these APs through a WEP key and web login to intranet services. In particular, there are two experimental users classes: users provided with 802.1x access and users that login through common web pages with username and password.

The authentication procedures is different for common areas, where both internal and external users can gain access to the network.

In fact, common areas have the double function of permitting any guest user to use common services, like web and some multimedia services for instance. This could require a "light" form of accounting, to adapt configuration requirements almost to every user with PDA or laptop with personal 802.11b cards.

On the other hand, users from Campus organizations have to be recognized by the access system as privileged users and need to reach sensible information on internal network, sharing AP connectivity with external users.

The authentication process uses a primary RADIUS proxy that receives authentication requests and forwards them to the RADIUS server that can handle information for a user group.

Finally, there is also the case of roaming users that are moving from other interconnected hot spots and need to reach their original network service: in this case they can login via web pages or 802.1x according to the APs location. In such a scenario, the authentication request will be forwarded to their home RADIUS server, through the RADIUS proxy in Wireless Campus.

b. ALTERNATIVE AUTHENTICATION METHODS: SIM BASED AUTHENTICATION

SIM authentication is a typical WLAN cellular WISP network feature. It's based on an architecture that extends the GSM network AAA capabilities to WLAN hot-spot users.

If practicable, Wireless Campus network will be connected to the GPRS network of a national cellular operator for testing of SIM based authentication methods and WLAN-GPRS roaming.

In fact, there will be a link from CSP's border gateway to GGSN of the operator to reach Authentication centre forwarding RADIUS requests from WLAN network for user authentication. Every internal user client is provided with a combo GPRS-802.11b card, with a slot for a GMS SIM. The procedure for authentication then follows a proprietary solution that finally leads the AP to know if the user can be registered to the network or not, based on operator's network information.

This kind of authentication can provide interesting information about performance comparison with 802.1x case and paves the way to realize WLAN-GPRS roaming test-bed.

Another interesting theme is the use of SIM slot in WLAN cards as smart-card reader to authenticate users with public certificates, which feasibility has to be investigated as further step.

4. SERVICES

On the application side there are main concerns about multimedia and location based services (LBS) services, as detailed later in the document.

This involves facing some questions, like multicast delivery on mobile networks and Quality of Service issues.

a. MULTIMEDIA SERVICES

The main challenge is the practical testing of multimedia over WLAN service deployment, particularly for real-time Voice over IP services.

In fact, the greater problem of this kind of appliances resides in the transmission delay variability, causing jitter values that can affect communication voice quality.

In the Wireless Campus network one of the main service objective will cover VoIP services to be provided on a SIP network, that will connect to that already deployed in CSP. The chosen of SIP as reference protocol is mainly due to the possibility of integrating standard telephony services over IP with instant messaging and presence services. Such services will help message delivery when user are far from their desk, or while roaming in another hot-spot, moreover making use of user location information.

5. EMBEDDING LOCALISATION CAPABILITIES IN WLAN NETWORKS

Personal communication based on cellular technology is currently facing the issue of providing the network of user localization capabilities for a wide range of applications: location based services, emergency applications, info mobility are only some examples of what is currently considered one of the most promising levy acting onto the market of personal communication services.

The most dramatic failure of the technologies addressed for cellular localisation is the indoor operation, i.e. the functionality in scenarios where the accuracy provided is not suitable for supporting reliable services. Satellite navigation systems are not of help for such a purposes due to the large attenuation experienced buy the signal inside buildings and for the need of at least 4 satellites in view to the user to provide a position solution.

On the other hand Wireless Local Area Network based IEEE802.11b are rapidly being deployed for in-building and short range wireless communication. Many mobile devices such as mobile robots, laptops and PDAs already use such a protocol for accessing the network, in a perspective of interoperability among WLAN, cellular systems (GSM/GPRS or UMTS) and in general the Internet.

Implementation of localisation capabilities within a WLAN is not only a way to complementing a service in an area still not served but opens possibilities for new challenging services. The complex environment (as a indoor building structure as office buildings, hospitals, shopping centres, etc.) makes the possibility of providing localization services a challenge for the technology and the network management.

In the field of mobile computing there are some important uses for localization in wireless Ethernet. System administrators might want to track laptops for security purposes, or the users access to the nearest printer, or getting help for localize a particular office. Relying on high accuracy solutions Location Aware services can be deployed as advertising in shopping centre or information delivery in museums. Localisation can also be the basis for automatic guidance of mobile robots with autonomous capabilities without other external aiding (e.g. vision, laser ranging etc.).

User localisation is also the basis for a smarter use of network resources, helping for example in power saving or in handover management.

Following the framework of what has been proposed for the cellular systems, Localization Techniques can be gathered in two classes

- *user centric methods*: the positioning technology resides in the mobile terminal
- *network centric methods:* the positioning technology resides in the network and the mobile terminal needs not to be modified

The most trivial localization technique suitable to WLAN is the association to each access of a section of the building, and the identification of the user position with the service region of the access point. Even if with poor accuracy such a technique can be easily implemented.

If the user is heard by a set of beacons, *triangulation* techniques can be used. In such a case, the position is obtained through the solution of a set of non linear equations representing circular loci (Absolute Distance -AD- measurements) or hyperbolas (Relative Distance -RD- measurements).

Different methods can be used for defining the geometrical loci:

- Angle-Of-Arrival (AOA)
- Time-Of-Arrival (TOA)
- Time-Difference-Of-Arrival (TDOA)
- Enhanced-Observed Time-Difference (E-OTD)
- Received Signal Strength (RSS)

Each of these has a different degree of complexity an intrusivity on the network and/or the user terminal.

Propagation time estimation is critical in indoor environments due to multipath and signal processing techniques for high sensitivity signal acquisition, multi-path mitigation and data filtering and smoothing (e.g. Kalman filtering) are needed.

On the other hand signal strength varies with time and relative position of TX and RX but is approximately constant over short-distances. Wireless Ethernet devices measure signal strength as part of their normal operation and with proper strategy of combining the measurements localization can be performed.

Within the Wireless Campus project a method based on RSS but not based on triangulation is being tested, as described in the following section.

a. LOCATION FINGERPRINTING RSS TECHNIQUE

The basic location method that has been chosen as a baseline for embedding positioning capabilities within the WLAN belongs to a class usually denoted as *location fingerprinting* positioning or *pattern recognition* methods. This methods rely on the assumption that each building has unique signal propagation characteristics; each spot in a building would have a unique signature in terms of RSS, TOA, and/or AOA, observed from different sensors in the building.

Thank to the limited extension of the coverage region it is possible to obtain from a preliminary acquisition campaign a map of the signatures for the different locations within the building itself.

During the operation phase a pattern recognition system determines the unique pattern features (i.e., the location signature) of the area of interest in a training process, and then this knowledge is used to develop rules for recognition.

In most indoor applications, with quasi-stationary scenarios, pattern recognition outperforms traditional triangulation techniques and Kalman filter-based tracking techniques.

The chosen method is a modified version of the RADAR technique [4] which relies on the definition of a signature map of RSS.
During the preliminary phase the signature database is built; a terminal is carried through the service area transmitting storing the measured RSS. The service area is divided into non-overlapping zones or grids, and the algorithm analyses the received signal patterns and compiles a unique signature for each zone.
It has to be remarked that the signature is a statistical measure of the signal strength and the metric associated to each point of the grid is an histogram of measurements. This metric helps in distinguishing locations that would have similar signatures if, as an example the simple average strength is measured.

Examples of the measurements results are depicted in Figure 1. The two locations have been selected in the same large room as represented in Figure 2: it has to be noticed that in this case the signal undergoes to extremely critical propagation conditions. In fact the access point (AP) is located at the second floor of the building in front of the room chosen for the trials. The signal crosses two windows and a yard before being received. This test has been performed on the border of the coverage area as proved by the very low signal strengths that are monitored. This conditions is in any case not unsuitable for the localisation purposes since large diversity in the fingerprints is experienced for locations few meters apart. This is not the case for locations close to the access point (e.g. in the aisle hosting the AP) where similar fingerprints are obtained due to the very similar propagation conditions even if with larger average strength.

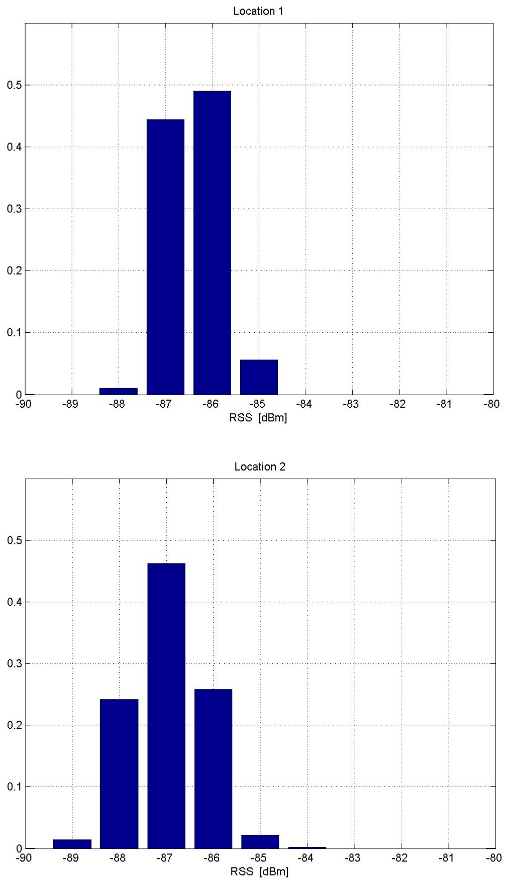

Figure 1: Normalized histogram of the received signal strengths for Location 1 (left) and Location 2

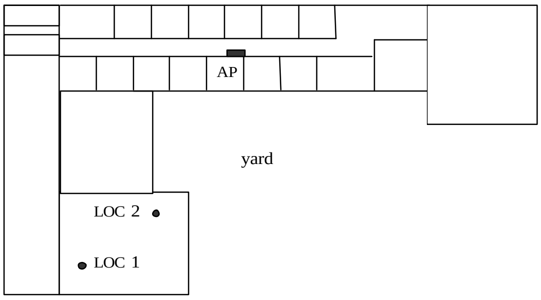

Figure 2: Map of a section of the Electronics building chosen for the preliminary trials of the localisation technique

b. Hybrid solution for outdoor environments

One of the challenges of the Wireless Campus project is the global coverage of an area including indoor and outdoor scenarios.

In outdoor scenarios the signature obtained for close locations is very similar, so hardly limiting the resolution capabilities of the positioning algorithm.
To this aim a hybrid methods based on the data fusion of WLAN and Global Positioning System information is being tested.
Generally speaking, *hybrid solutions* can be found combining different pieces information available for the communication interface, where any measurement (power, propagation delay, "coverage maps",…) jointly contributes to the determination of the user position or for increasing the accuracy.

Within a receiver the hybrid positioning can be performed at different levels: in fact it is possible to consider the two kind of systems separately choosing the most appropriate solution or combining the results, or alternatively to integrate the information coming from the different systems in order to obtain one unique solution. The integration strategies at the receiver level can be classified as:

Solution Selection**: this technique foresees the use if a handset equipped with a satellite navigation receiver (GPS) and a WLAN receiver. Both receivers continuously process the received signals and independently provide a solution. The ultimate solution output to the user is chosen according to a quality criterion (e.g. estimation variance) that can, as an example, depend on the environment in which the handset is operating.**
This technique keeps separate the two technologies and allows for obtaining the best performance of each independent system.

Support systems: also in this case the two receivers (WLAN and GPS) are separately used for the positioning solutions. In addition the WLAN channel is used to provide support information to the GPS receiver in order to aid and speed up the positioning procedure.
GPS acquisition of satellite signals is a critic phase of the positioning procedure and it has to be remarked that in order to provide a solution to the user at least 4 satellites must be in view. [5]. This is not always possible in outdoor environments where high buildings surround the user.
The support data provided through the WLAN links are essentially almanac, ephemerides data and differential correction that are evaluated by a terrestrial reference station connected to the network or alternatively obtained by the Internet (e.g. Sysnet system).

Integration of heterogeneous measurements**: this technique foresees the fusion of heterogeneous measurements within the receiver in order to obtain one unique solution. Such integration can be obtained only acting on the detailed basic architecture, since, in many cases, it involves parameters related to the physical level of the signals.**

The location system currently under study belongs to the support class while research activities are facing the feasibility of a deeper integrated method fusing data at the raw signals level.

6. OPENSOURCE RESOURCES

One of the more currently debated question relates to the introduction of open-source means in real network scenarios. Actually they can't play the role of market products competitors, otherwise they provide a support in research and technology dissemination. Opensource resources can be used to implement in short time the new technology features proposed in the draft, standards and recommendations, to provide a real test environment for analytical tests to verify and support simulation theoretical results.
In this project will be inserted mainly three opensource items:

- Access point HostAP;
- Radius server Freeradius;
- Open 802.1x client.

The latter will be used mainly to study interoperability for authentiction systems provided by our network resources.
The HostAP project [6] instead will be execute on local devices to realize a testing environment on QoS and localization issues. We will perform proper modifications of the software kernel for supporting new functionalities, as for example, the exchanging of location update information with an external server to maintain a pseudo-real time look up for host positioning. Moreover it will be investigated

REFERENCES

[1] Adam Stubblefield, John Ioannidis Aviel, D. Rubin,
"Using the Fluhrer, Mantin, and Shamir Attack to Break WEP"

http://www.isoc.org/isoc/conferences/ndss/02/proceedings/papers/stubbl.pdf

[2] Scott Fluhrer, Itsik Mantin, Adi Shamir, “Weaknesses in the Key Scheduling Algorithm of RC4”
http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

[3] IEEE 802.1x - Port Based Network Access Control
Supplement to ISO/IEC 15802-3:1998 (IEEE Std 802.1D-1998)
http://www.ieee802.org/1/pages/802.1x.html

[4] P. Bahl and V. Padmanabhan, “RADAR: An In-Building RF-Based User Location and Tracking System,” IEEE INFOCOM, Israel, Mar. 2000

[5] E. D. Kaplan, Understanding GPS: Principles and Applications, Artech House, 1996

[6] Host AP project – Qpen Source Implementation of an 802.11 access point
http://hostap.fi/