FENU, G. and PIRAS, L. 2008. A portable wireless-based architecture for solving minimum digital divide problems. In *Reznik, L. and Popescu, M. (eds.) Proceedings of 4th International conference on wireless and mobile communications 2008 (ICWMC 2008), 27 July - 1 August 2008, Athens, Greece*. Piscataway: IEEE [online], pages 130-136. Available from: https://doi.org/10.1109/icwmc.2008.21

# A portable wireless-based architecture for solving minimum digital divide problems.

FENU, G. and PIRAS, L.

2008

# A Portable Wireless-Based Architecture for Solving Minimum Digital Divide Problems

Gianni Fenu
*University of Cagliari*
*Department of Computer Science*
*Cagliari I-09124 ITALY*
*fenu@unica.it*

Luca Piras
*University of Cagliari*
*Department of Computer Science*
*Cagliari I-09124 ITALY*
*luca_piras@hotmail.it*

## Abstract

*In today's society digital services have become the key to the success of anyone. Hence, for being competitive it is important that these services are available, employ the latest technology and are low cost. Unfortunately, it often happens that these good intentions do not correspond to reality. In this paper an information system is proposed, targeted at those small realities affected by the digital divide and at those companies that employ out of date, high cost technologies, that provides data and voice services in a unified manner using heterogeneous devices. The system utilizes innovative technologies, in particular wireless technology, to deliver low cost solutions. The distinctive feature is that it does not depend on the network hardware infrastructure and the underlying platform. Furthermore, it deals with the configuration, accounting, security, management, and monitoring aspects while maintaining its flexibility and simplicity of use both for the administrator and end user.*

## 1. Introduction

The technology revolution, which has resulted in the continued development of innovative technologies, has had a major impact on development and communication in present day society. All sectors are faced with dynamically changing situations. Human activities now rely in many cases on new technologies that offer benefits in terms of efficiency, greater functionality, greater flexibility and simplicity of use and often also of costs.

Keeping pace with technological change generally promotes the development of society in a big way.

However, depending on local situations and in scarcely populated areas this is not always possible, not so much because of a lack of knowledge or unwillingness to introduce these new practices, but rather because the area does not have access to technologically advanced services.

Often this situation cannot be simply defined as digital divide (DD), as the areas in question fall within broader areas having access to advanced technology, but Minimum Digital Divide (MDD). However people living or companies operating in these areas fall behind, leading to static competition within the market and within society itself.

This paper is concerned with solving some of the problems associated with the vast issue of digital divide. The attention is focused on voice and data communication services and a software model is proposed that is able to satisfy demand while providing an acceptable quality of service (QoS).

These small areas are often disadvantages by geographical restrictions to creating infrastructures for providing technologically advanced services, or the number of users who would benefit there from is too small to offset infrastructure costs. This paper intends to contribute to solving these problems by means of a wireless network architecture [1, 2].

Data and voice traffic are both transmitted over IP protocols, by means of XDSL and VoIP respectively.

These technologies have made it possible to significantly reduce the cost of these services.

As will be seen later, the network hardware and software architecture is compact, flexible and similar to the architecture of the Wi-Fi hotspot services installed in airports, hotels, universities internet points, shops, cafés, etc. worldwide.

Hotspots generally employ the captive portal technique [3], whereby a client first accessing the web is presented with a login page and after authentication can access the web. Subsequent access requests are fulfilled automatically. These systems generally deal with authentication, authorization and accounting functions, optionally with billing, monitoring and network management. They often present a security

threat [4] but this can be improved for example by means of cryptographic techniques [5, 6, 7, 8].

The purpose of this work was to design and set up an architectural layer, starting with a knowledge of the information systems in the specific sector [3, 9, 10], [11, 12]), that was able to achieve all the above functionalities and to include innovative ones regardless of the user terminal. Thus, a hardware-independent and platform independent application was devised that was able to satisfy the requirements of heterogeneous devices while maintaining administrator and end user ease of use [7].

Note that, as per the design hypothesis, the system, which consists basically of an ad hoc configurable application can operate on different platforms sharing common specifications for accessing any type of wi-fi hotspot network and is thus vendor-independent.

Platform independent means that the device can be installed on any network server operating system, thanks to the fact that the software has been developed in Java, a partially compiled and interpreted language able to run on a Java Virtual Machine (JVM). In this way it is possible to interact with heterogeneous devices such as notebooks, handheld and smartphone devices, IP-phones) using the same application Thus the system has been designed with a view to obtaining a low cost device, quick and easy to install on different types of devices that can be easily configured and managed by the administrator, especially as far as the more complex functionalities are concerned, thereby ensuring flexibility and ease of use, features not commonly found in the majority of systems.

## 2. Application scenario

In this section an application scenario of the service is examined. An overall picture of the situation is given, though implementation codes and specifications are not provided.

The scenario that best lends itself to the information system described herein is a small thinly populated village where the digital divide consists of the lack of broad band internet connection, let alone a VoIP voice service.

In these situations at the most there exists low speed ISDN or ADSL internet access.

In small communities such as these, the Town Hall can be conveniently chosen as a congregation point for providing data and optionally voice services for its own offices and citizens.

The only assumption is that the Town Hall is provided with XDSL and VoIP. To this is connected and configured a vendor independent, compact and flexible hardware architecture having the common and necessary specifications of all types of hotspot Wi-Fi networks.

The ultimate aim is to enable the network administrator to activate data and voice services simply by installing the JVM on a specific server, should it not already exist, and to copy, without the need to actually install it, the information system server side software which takes only a few minutes to configure.

At this point, anyone interested can go to the Town Hall and ask to open an account. The operator using accounting software written in Java installed in his/her computer, can interact with the server to obtain information about the services offered and a series of parameters useful for the client, which are decisive in choosing the service profile which the client is interested in. Once this procedure has been completed an account is created and provided authentication credentials.

To access the data service, the user simply needs to have an IEEE 802.11b/g wireless equipped desktop, notebook, smartphone or cell phone. Should the voice service also be desired then an IP-phone or Unlicensed Mobile Access (UMA) cell phone will also be required.

The above devices come under those envisaged by the project as user terminals.

By connecting to the Town Hall's access point the user will not be able to surf the net straight away, the request for web pages will not be satisfied, except in particular cases which will be dealt with later. The user is presented with a web page requesting him to proceed with authentication using the software to be downloaded from the same page. The package downloaded consists of the JVM, to be installed if not already present, and the client side software that enables to perform a series of useful operations.

The software downloaded does not need to be installed but can be used directly. Once the client application has been accessed the user is requested to provide authentication credentials to log in. This procedure provides access to the data and voice services specified in the profile.

At this point the user can perform a variety of activities, using the device, for example check log-in status, log out, display contract terms and change them, obtain information on special rates and activities, consult their own personal use statistics, etc.

## 3. Network architecture

To show by an image, the network architecture, we depict, in follow Fig.1, the main devices included in our system.

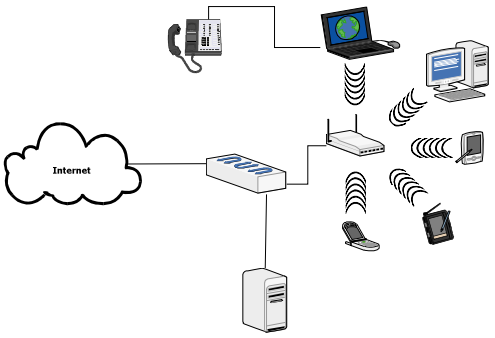


**Figure 1. Network architecture underlying the information system**

It is very simple, cheap and exhibits the basic features shared by all types of hotspot wi-fi networks. On the server side there is an internet connection, a switch, a server, an access point and a computer, on the client side devices such as notebook, computer, smartphone, PDA (Personal Digital Assistant), wi-fi cell phone, IP-Phone and UMA-Phone.

All the devices on the client side are equipped with IEEE 802.11b/g wireless technology and transmit requests for data and voice services. These requests are sent via the internet connection, but the data flow is managed by the hardware contained in the centre of the figure. The access point receives all the requests from the client side and is configured such that all requests are forwarded to the server. The server deals with accounting, authorization, authentication, network management and monitoring, security. The server side computer is used by the Town Hall operator, or administrator, who interacts with the server itself, enabling accounts to be created and managed.

These data flows are made possible by switch supervision. The switch is configured such as to create 3 full duplex channels, one from the access point to the server, one from the server to the internet and one from the operator computer to the server.

Thus the server has a Proxy functionality within the network. In fact, it intercepts client requests and, depending on authentication status and specific authorizations, decides whether or not to satisfy those requests. This functionality is implemented almost entirely by the software architecture which is examined in the next section.

## 4. Software architecture

Let us recall that the system has been designed to be hardware, vendor and platform independent.

As far as the hardware profile described above is concerned, the software does not require any special devices, but the same ones used for hotspot Wi-Fi as well as a very simple configuration.

Regarding the software, the use of Java technology on both the server and client side means that one is not restricted to the use of a particular platform. Furthermore, the applications proposed here do not require special installation or configurations All operations on the server and client side perform complicated procedures internally that to the user's eyes appear as simplified as possible.

All these features allow the system administrator to set up and manage the system rapidly and easily. The same considerations apply to the client, who interacts with a very compact, simple and functional program.

### 4.1. Server side software

The server side software consists of 2 programs, Accounting Software and Server Software described below.

**4.1.1. Accounting software.** The aim of this program is to enable clients to define a service profile, and if necessary to stipulate a contract with the Town Council for voice and data services. This task is entrusted to an operator at the Town Hall. In this phase the different profile conditions are defined depending on connection speed, BMG, accounting traffic, etc.

The options proposed to the client are processed in relation to the different parameters and information, chiefly associated with the local specificities.

All this information is managed by the server software and then processed so that the accounting software can display on the screen the contractual options which the client can then choose from.
Furthermore, new accounts can be created using the accounting software, always interacting with the server software. The client's personal data are requested and the program provides the authentication credentials for the new account created. The user can subsequently change the personal details, authentication credentials or contractual terms of the account.

**4.1.2. Server software.** The server software is the key application of the system. It acts as a proxy and provides functionalities such as accounting, authentication and authorization [5]. The software is

installed in the server and as it is written entirely in Java, it does not require a specific underlying architecture platform.

The first time the administrator activates the hotspot Wi-Fi he/she first makes sure that the operating system contains JVM and if not installs it, then simply copies the software program in question onto the server without installing it.

At this point the administrator can implement the application and proceed with configuration. This involves setting a number of parameters, such as the maximum number of clients that can be served, the maximum and minimum band widths allowed for download and upload per user, filling in the white&black IP list and the white&black Web list, choosing whether to use cryptographed client-to-server communications.

In particular, the IP white&black list makes it possible to distinguish between hosts that are able to access the network and those that cannot.

A list of hosts who do not require authentication for external access could also be compiled. This could prove useful when using shared printers, webcams, video camera or other devices that cannot provide credentials for authentication.

The white&black web list is another interesting functionality, as it indicates those websites which can be accessed without authentication or viceversa those that cannot be accessed even by authenticated users. It may be useful, for example, to indicate sites that can always be visited such as the emergency police, ambulance and fire services, or block access to others. The same can be said for VoIP calls.

Choosing to use cryptographed data ensures greater security in client-server communications and prevents personal credentials falling into the wrong hands. Cryptographing can be done in a number of ways, for example using hardware devices that support WPA or WPA2, or working at a higher level cryptographing communications using https in place of http. The difference between these two methods resides in the fact that the first involves using devices that support these protocols, while the second involves implementing https in the information system. The latter was preferred for this specific project because it allows to devise an information system that is all the more independent of the underlying hardware.

**4.1.3. Accounting, authorization, authentication.** An account consists of an IP address, user name and password. To each account is associated the user's personal information. Here the IP addresses are not dynamically assigned as happens in DHCP, but statically assigned. In this way accounting is improved and security enhanced. Static assignment is possible given the circumscribed number of expected users.

When defining the profile, the user provides his personal details, chooses the conditions that suits him/her best and the user name. The password and IP address are assigned by the system, but the password can be changed using the client side software. Moreover, the user can decide whether to opt for data and (optionally) voice services, and the account authorizations are assigned accordingly.

As far as authentication is concerned, the server software acts as a proxy, intercepting client requests, dealing with them and replying. When a client request is received, the hardware architecture forwards it to the server. The server software, that listens on port 80, intercepts the request and decides whether host identification is necessary. This depends on the type of request. For example, if the client wishes to access web sites or call numbers in the white list, then the request is satisfied directly, otherwise the server proceeds with identification, checking the IP address. Once the client has been identified, then the software checks the authentication status and whether the client is authorized access to the service requested. If the user is already authenticated and authorized then the request is satisfied. Otherwise in the absence of authorization no service is provided, or if the user is not authenticated; an html page appears inviting him/her to login using the client side software. This software and the JVM can be downloaded from the web page that appears on request for authentication. This web page also indicates the white list, i.e. a list of all accessible sites and telephone numbers that can be called even without authentication and authorization. When the user sends his/her login credentials, namely IP, user name and password, if they are correct then authentication is granted and if authorized to access the service, then the request is satisfied. Each time a request is satisfied the server forwards the request on and when he receives the reply, forwards it to the client.

Once the user is authenticated, depending on contractual terms, it may be necessary to initiate processes that deal with billing and logout after a specified time [3, 13, 14, 15].

For managing a 24 hour flat rate contract, these measures are not required, but in the event an hourly rate is applied or credits are purchased then these functionalities should be incorporated.

The software also keeps a permanent record of the user's identity, type of service requested, date, start and end time of service provided in a historical repository.

In many countries these functionalities are required by law for security reasons so that users and the operations performed within the network can be traced.

**4.1.4. Additional functionalities.** Additional software functionalities are for network management [16], credit management, utilization statistics and information channel.

For network management means are provided for checking the network and load status, for managing bandwidth and introducing measures for preventing and solving any problems that may arise. Some problem solving techniques, for instance for easing congestion, envisage disconnecting some clients or a temporary bandwidth reduction until such time as the system has been restored [17, 18, 19]. In any case, congestion prevention is envisaged and this is possible because the system contains information about the terms of contracts stipulated with users and the physical features of the network. When new contracts are requested the system processes the information and indicates suitable bandwidths to ensure optimum and efficient network management, thereby preventing these problems.

Credit management is one means of paying for the services provided. In practice, the user purchases a rechargeable card that can be used for both data and voice services. The system allows users to check their credit, recharge the card and blocks service provision when credit is insufficient.

Another important feature of the software is that it is able to process utilization statistics either for groups of or for individual users [20]. These can be consulted by users to obtain information about utilization, but also in more detail by the administrator for a number of purposes. The system, by activating predetermined automated data mining processes purpose built for the scenario proposed here, provides the administrator with concise information enabling him/her to take certain decisions. For instance to assess new rate plans or special user rates, or to prepare specific proposals for a given user, thus enacting a loyalty policy. This process is automated but the administrator who has access to the data can create new ad hoc procedures for specific problems for the above described purposes.

Once it has been established what rates to offer to the user, these can be promoted and subscribed to by the user via the information channel in the client side software.

## 4.2. Client side software

Once the user has defined his/her profile, he attempts to access the network for the first time. In the first place, the user should manually set the IP address provided and connect to the access point. Having done that, he/she can download the JVM for the specific operating system and the client side Java application, called “client software”, directly from the web page that appears every time a non-authenticated user accesses the network. Client software does not require installation, and as it is platform and hardware independent, it can be run on heterogeneous devices such as notebooks, desktop computers, smartphones, PDA, wi-fi cell phones, UMA-phones etc.

The operations already described above are briefly outlined below but this time in a client specific context.

The application allows the user to perform a series of operations. First and foremost the login, which enables authentication of the user within the network. The program requests authentication credentials, in the specific case username and password, The request is sent to the server which replies: if the outcome is positive then the user can start to use the services for which he/she is authorized.

The user can also check his/her login status. For post-paid or credit contracts information is also provided concerning units accumulated or remaining credit respectively. In the event the credit amount is running out or is exhausted, the card can be recharged directly using the software, simply providing credit card details or by some other means.

Another interesting functionality is the possibility for the user to access his/her own personal data, contractual terms and change them if necessary. For example the user can change his/her password or personal details or increase or reduce upload or download bandwidth, increasing or reducing the rates paid accordingly, or subscribe to the VoIP service.

The user can also consult his/her own utilization statistics so as to have a complete picture of his/her own requirements and compare the special rates offered along with the rate plans in the information channel and subscribe to them with a simple click. The information channel consists of a window displaying two groups containing special rates and rate plans. The first group shows the general offers, the second specific rates tailored to user needs.

VoIP calls can also be made using the software either directly from the same device by means of a small digital numeric keyboard or connecting to a wired IP-Phone. If the user possesses a wireless IP-phone then it is possible, using an IP address that does not require authentication, to make calls connecting directly to the access point.

Moreover, the software notifies the user about certain events for example disconnection, exhausted credit or when a certain amount has been reached.

Because of multiple heterogeneous functionalities which the program envisages, to several levels of complexity, a Java-Based client solution is much more suitable than a Browser-based one. Furthermore this is a proper way to obtain a real platform independence into an environment of heterogeneous devices. In fact Java Technologies in place of Browser-based client solution allow to eliminate the dependence by specific browser features as much as possible.

## 5. Conclusion

This paper is concerned with the design of an architecture model for solving certain problems associated with the minimum digital divide. The model allows to provide low cost data and voice services, in areas not presently covered, with the aid of IEEE 802.11b/g, XDSL and VoIP technology.

The architecture offers both flexibility and portability thanks to the use of Java technology which allows hardware and platform independent use. The model can be readily and rapidly integrated into a large number situations. Furthermore, no installation is required and the architecture is compact, flexible, inexpensive and simplified to the greatest possible extent as far as configuration, administration and management are concerned, and is user-friendly. Lastly, thanks to its great flexibility it can be implemented on wireless or mixed architectures.

Once the design and pre-testing phases will be completed, the system will be implemented according to the specifications described herein. The next phase will consist in testing the system for the purpose of assessing performance for different loads and uses, paying special attention to the developments envisaged for security aspects and new services.

In particular future research will focus on providing services such as digital TV and streaming on demand.

Among the new functionalities user personalized procedures are being examined for example that automatically disconnect or notify the user of the event, when a certain traffic or time threshold has been attained. This may prove useful also for a kind of real-time control on both data and voice services.

A variant of the voice service is currently being examined that enables free calls to numbers within the area covered.

This work makes use of results produced by the ARCAS Project managed by the Department of Computer Science (University of Cagliari) and Impiantica Srl, a project co-funded by the Sardinian Government within the "Programma Operativo Regionale 2000-2006 – Asse 3 – Risorse Umane, Misura 3.13 – Ricerca e sviluppo tecnologico nelle imprese e territorio".

## 6. References

[1] J. Lloret, J. J. López, C. Turró, and S. Flores, "A Fast Design Model for Indoor Radio Coverage in the 2.4 GHz Wireless LAN" *in Proc. 1st International Symposium on Wireless Communication System*, Mauritius, 2004, pp. 408–412.

[2] S. Miyamoto, S. Harada, and N. Morinaga, "Performance of 2.4 GHz-band wireless LAN system using orthogonal frequency division multiplexing scheme under microwave oven noise environment" *in Proc. 16th International Symposium on Electromagnetic Compatibility*, Zurich, 2005, pp. 157–162 Vol. 1.

[3] H. Xia, and J. Brustoloni, "A Virtual prepaid tokens for Wi-Fi hotspot access" *in Proc. 29th Annual IEEE International Conference on Local Computer Networks*, Tampa, 2004, pp. 232–239.

[4] S. Fayssal, S. Hariri, and Y. Al-Nashif, "Anomaly-Based Behavior Analysis of Wireless Network Security" *in Proc. 4th IEEE/IFIP Annual International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services*, Philadelphia, 2007, pp. 1–8.

[5] H. Luo, and P. Henry, "A Secure Public Wireless LAN Access Technique That Supports Walk-Up Users" *in Proc. IEEE Global Telecommunication Conference*, San Francisco, 2003, pp. 1415–1419 Vol. 3.

[6] H. Wang, A. R. Prasad, P. Schoo, K. M. Bayarou, and S. Rohr, "Security mechanisms and security analysis: hotspot WLANs and inter-operator roaming" *in Proc.59th IEEE Vehicular Technology Conference*, Milan, 2004, pp. 2492–2496 Vol.5.

[7] J. Lee, J. Kim, J. Park, and K. Moon, "A Secure Wireless LAN Access Technique for Home Network" *in Proc. 63rd IEEE Vehicular Technology Conference*, Melbourne, 2006, pp. 818–822.

[8] E. S. Barka, E. E. Mohamed, and K. Hayawi, "A End-To-End Security Solutions for WLAN: A Performance Analysis for the Underlying Encryption Algorithms in the Lightweight Devices" *in Proc. international conference on Wireless communications and mobile computing*, Vancouver, 2006, pp. 1295–1300.

[9] J. Jamaluddin, M. Doherty, R. Edwards, and P. Coulton, "A Hybrid Operating Model for Wireless Hotspot Businesses" *in Proc. 1st IEEE Consumer Communication and Networking Conference*, Las Vegas, 2004, pp. 611–615.

[10] A. Hasib, and A. O. Fapojuwo, “A Mobility Model for Heterogeneous Wireless Networks” *in Proc. 8th IEEE Radio and Wireless Symposium*, Orlando, 2008, pp. 815–818.

[11] J. Hortelano, J. C. Cano, C. T. Calafate, and P. Manzoni, “A Wireless Mesh Network-based System for Hotspots Deployment and Management” *in Proc. 3rd International Conference on Networking and Services*, Athens, 2007, pp. 16–21.

[12] K. Takaaki, F. Kenji, and O. Yasuo, “The MIAKO.NET Public Wireless Internet Service in Kyoto” *in Proc. 1st ACM international workshop on Wireless mobile applications and services on WLAN hotspots*, San Diego, 2003, pp. 56–63.

[13] Y. Fang, I. Chlamtac, and Y. Lin, “Billing strategies and performance analysis for PCS networks” *IEEE Trans. on Vehicular Technology*, vol. 48 Issue 2 ED-41, pp. 638–651, March 1999.

[14] B. Bhushan, J. Hall, P. Kurtansky, and B. Stiller, “OSS functions for flexible charging and billing of mobile services in a federated environment” *in Proc. 9th IFIP/IEEE International Symposium on Integrated Network Management*, Nice, 2005, pp. 717–730.

[15] H. A. Ibrahim, B. M. Nossier, and M. G. Darwish, “Billing system for Internet service provider (ISP)” *in Proc. 11th Mediterranean Electrotechnical Conference*, Cairo, 2002, pp. 260–268a.

[16] M. K. Han, B. Overstreet, and L. Qiu, “Greedy Receivers in IEEE 802.11 Hotspots” *in Proc. 37th IEEE/IFIP International Conference on Dependable Systems and Networks*, Edinburgh, 2007, pp. 471–480.

[17] S. Sesay, J. Xiang, J. He, Z. Yang, and W. Cheng, “Hotspot Mitigation With Measured Node Throughput in Mobile Ad Hoc Networks” *in Proc. 6th International Conference on ITS Telecommunications Proceedings*, Chengdu, 2006, pp. 749–752.

[18] Z. Yang, and H. Ma, “A Game-Based Mechanism for Avoiding Routing Hotspot in P2P Streaming Distribution” *in Proc. IEEE International Conference on Multimedia & Expo*, Beijing, 2007, pp. 2166–2169.

[19] S. Tartarelli, and G. Nunzi, “QoS Management and Congestion Control in Wireless Hotspots” *in Proc. 10th IEEE/IFIP Network Operations and Management Symposium*, Vancouver, 2006, pp. 95–105.

[20] G. Divgi, and E. Chlebus, “The Impact of Internet Access Account Categories on Users and Traffic in a Commercial Nationwide Wi-Fi Hotspot Network” *in Proc. 5th IEEE Consumer Communications and Networking Conference*, Las Vegas, 2008, pp. 54–58.