Universal Bluetooth™ Access Control and Security System

Francisco José Bellido-Outeiriño[(1)]
José Luis de la Cruz Fernández [(2)]
[(1)]Dept. of Computers Architecture, Electronics and Electronics Technology;
University of Cordoba
14071 Cordoba, Spain
fjbellido@uco.es; fa1crfej@uco.es;

Antonio Moreno-Muñoz[(1)]
Pedro M. Canales Aranda[(1)],Benito Pérez Jarauta[(3)]
[(2)]Dept. of Applied Physics;
[(3)] Stop Casa Segura S.L.
University of Cordoba
14071 Cordoba, Spain
amoreno@uco.es; p52caarp@gmail.com;
jarauta_seguridad@hotmail.com

Abstract— **In this paper, we describe the use of Bluetooth™ technology for the development of novel applications for home and intelligent buildings scenarios, as well as scenarios in which security and access control is necessary (e.g., garages). The design of the solution has been done following a hierarchical scheme, starting from a simple and functional module and providing new features that will give an added value to the final product. This methodology allows to generate a wide range of products with several features for the final consumer and end users. The developed system is low cost, autonomous, scalable (both from a physical point of view and functionality) and capable of interacting and being controlled by the end user and by other similar modules in range. Establishing communication with the system is quite simple as well as cost effective, since the universal key for these access points can be managed by user's mobile phone or PDAs. The solution has been implemented using Java. In addition, the developed software is offered in order to provide a friendly interface and to allow the system administrator to manage the control unit (e.g., edition of authenticated users, download record files of event, data sharing with other modules in range, etc.), giving an added value to Bluetooth™ system and to the mobile devices integrating this technology.**

Keywords - Bluetooth™, Home Automation & Control, WLANs e-Key, Security.

I. INTRODUCTION

Wireless communication has been a great quantitative and qualitative jump in information management, allowing access and interchange without a physical wire connection [1]. Wireless transmission of voice and data has a continuous evolution into new standards, like Bluetooth™ [2], Wibree™ [2] or Zigbee™ [3].

These newest wireless technologies are focused on communication systems of short-medium range and are optimized so as to be low cost and with low power consumption, to be integrated in mobile devices or embedded systems [4]. Hence, they have been established as the future technology for mesh nets or distributed acquisition and control systems.

The concepts of network embedded systems stem from hierarchically interconnected networks, which are based on tiered architectures that provide cost-effectiveness and scalability, and adapt straightforwardly to various application requirements [5], regarding security and users' aspects in the overall system design [6].

In the field of home automation, security or access control systems with wireless technologies, several interesting applications can be found. In figure [7] it is presented a Zigbee™'s based system for a digital door lock and in [8], [9], [10] the use of Bluetooth™ for home security and/or monitoring purposes is shown.

As to the applications that use Bluetooth™ (via the mobile phone or PDA) to perform control actions to third parties, we can find several software applications that allow the mobile phone to be used as a remote control for the PC (e.g., to manage Windows Media Player or Power Point presentations). Many of them are even freeware or shareware.

These tools, usually Windows-based, communicate with the application layer of Bluetooth™ systems using DLLs drive via USB dongles. Although the proposed solutions consider e-keys for user authentication when the e-key is being managed by mobile phone or PDA devices, the authentication process is carried out in each session by running an autonomous microcontroller unit, in which the management of the lower levels of the Bluetooth™ stack takes place, and not by back-end computers, which are LAN connected to the Bluetooth™ device and use predefined profiles for phone-metric recognition, some of them are similar to USB encrypted keys.

In this paper, we describe an interesting application of Bluetooth™ technology to access control systems, which is suitable for home and building applications and extendable to any security system or controlled access points such as parking garages. The proposed system, based on [1], has been designed following a hierarchical scheme, starting from

a simple but fully functional module and new features have been included in order to build a final product with an added value, as well as to offer a wide range of products with several features to the final customer or end user [5].

The developed system is low cost, autonomous, physically and functionally scalable and with control and interactive capabilities.

The main problem is that the system described in this paper has implemented an autonomous Bluetooth™ module by managing the stack and profiles at lower levels, with no computer or operating system requirements. The system could work, with or without additional software applications, for users and system administrators, in which higher security levels for access and control applications are implemented.

In addition to these or either to traditional RF devices for remote control access, we present a novel application with great potential, a step further due to Bluetooth™ use. These characteristics allow us to offer a very simple, powerful and cost effective means to manage the identification of users and to perform subsequent actions.

The paper is organized as follows: in the next section**,** an analysis of the challenges and requirements of the proposed system is presented and discussed and, in Section III, a full description of its structure and implementation is done. Finally, we discuss the advantages and applications of the developed system in some real scenarios.

II. CHALLENGES AND REQUIREMENTS

The main objective of our work has been to design and to build a universal access control and monitoring system, bearing in mind such requirements as power consumption, range, cost, network capabilities, and a standardized technology [4].

In the field of WPANs technologies, we find several possibilities: Bluetooth™ and Zigbee™. They are considered to be the optimal ones; RFID [11] could also be fit for this purpose. All of these technologies comply with the necessary features for the development of security control and identification systems, but they also show some disadvantages for this kind of applications.

For example, RFID tags work in different frequency bands; some of them are not allowed worldwide. There are also several standards for the Tags, like EPCGen 2 (Electronic Product Code consortium) [12] that are not adopted by all the companies. Therefore, a RFID based system could not guarantee a universal or worldwide functional system.

On the other hand, Zigbee™ and Bluetooth™ operate in the ISM band, and both standards have interoperability features. Then, according to our criteria, Zibgee and Bluetooth™ are the ones selected in this first analysis.

An analysis of both technologies in depth about the requirements of the application shows that Bluetooth™ is the optimal solution, since nowadays most of mobile devices (mobile phones, PDAs, laptops, etc.) support Bluetooth™, most people have at least one mobile phone, and it is a technology commonly used by mobile phone users. This means that the communication scheme between users and the access point, that is to say the user's terminal, is carried out without additional cost and without the need to carry new keys, ID-cards or remote control devices.

Since Bluetooth™ is a standard we could think that any digital device equipped with it can communicate with other devices. However, this is not completely true because Bluetooth™ Specifications [2] define several Profiles for different applications, and not all the Profiles are implemented or supported by all devices, e.g., in mobile phones it is usual to have only File Exchange and Audio capabilities, but it is not possible to manage the Serial Port with a Bluetooth™ adapter like in a desktop that supports the full stack run in a PC.

Therefore, it is necessary to design a *Control and Access Point Terminal* system that could be detected by any other device with Bluetooth™ capabilities. The solution proposed in this paper, as described in the next section, is to enable a minimum set of profiles to cover at least those profiles implemented in any electronic device equipped with Bluetooth™, thus all devices would be able to detect the Terminal by means of one of these profiles.

III. SYSTEM DESCRIPTION

In this section**,** we present the basis of the proposed system, we place special emphasis on some fundamental considerations about the Bluetooth™ profiles, and we propose the structure and architecture of the system and perform the system implementation.

First, we will establish the implementation scope of this system within the framework of access control. An access control could be defined as a system applied to an access that ensures the identification of users and authorizes them or not to enter, on the basis of a set of stored information.

A basic classification of access control systems could be as follows:

- According to connectivity
  - Off-line
  - On-line
- According to power source
  - Battery powered
  - Mains powered
  - Autonomous (power source located in the key)
- According to the kind of reading
  - Insertion (mechanical/classical key)
  - Contact (magnet key, chip, RFID)
  - Remote (remote control, mobile phone)
- According to security level
  - Level I. Something we have (e.g., a key)
  - Level II. Something we have plus something we know (e.g., a key+ PIN)
  - Level III. Something we have plus something we know plus something we only have (key + PIN+ biometric features).

The system proposed is off-line (on-line supported), mains powered, remote keyless (contact is made through RFID antennas) and it supports any security level: I, II or III (L-III interconnected to a biometric reader).

A. How the Bluetooth™ Access Point Terminal works

A way to achieve that any other device with Bluetooth™ capabilities could find the system is by enabling both Hands Free Profile and Serial Port Profile, so that any device could discover the Terminal.

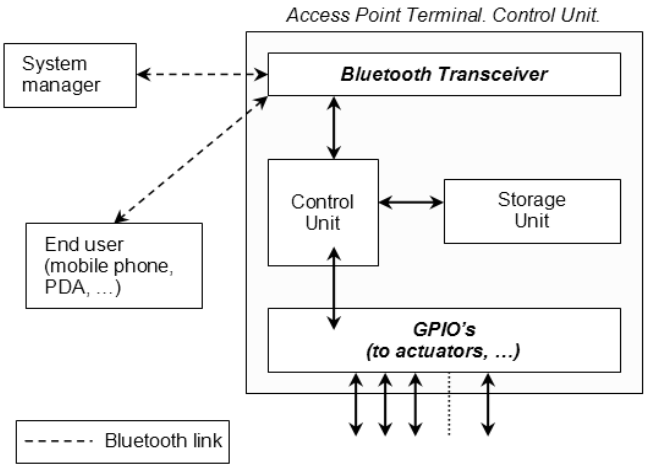

Figure 1. Main components of the system architecture.

The device appears to the end user as a hands free unit, and thus establishing communication with it (e.g., to try to be identified to open a door automatically) is very simple and inexpensive as *universal key* for these access points can be the user's own mobile phone or PDA. Thus, with his own personal device (i.e., the mobile phone) the user can gain entry to several places (parking door lock, clocking-in at work, enabling/disabling home alarm system, etc).

Figure 1 shows the main components of the system architecture.

The system core is the so-called "*Access Point Terminal*". It could be configured in three ways, depending on the application:

1. *Basis application*: it stores the data of authenticated users (preloaded). Unencrypted information and operation mode.
2. *Advanced application*: it stores encrypted data by means of which it recognizes authenticated users even when they have a different and unique encrypted key based on unique parameters of the own user.
3. *Net advanced application*: as the one above, except that it sends the information of events to other *Terminals* in range (Figure 2).

For security reasons, the *Terminal* is normally in a semi sleep mode, reading periodically the input channel for any request. If the Terminal receives information, both in operation modes (1) and (2) (mode 3 is formally like 2), it checks the user status and performs the operation and it carries out other general actions like storing the event information or sending the event information (if operation mode is 3).

For a better robustness, if the same MAC Bluetooth tries to connect several times and it proves to be an unauthorized user, this MAC is put into a filter table that is used in the first steps to avoid service denial due to the presence of sniffers.

The brain of the *Access Point Terminal* is the Control Unit that manages the communication and control through the following components:

- Bluetooth transceiver, in charge of sending/receiving the user's requests.
- Storage unit, which reads/writes data or updates firmware.
- Power subsystem, in charge of checking the auxiliary battery charging process, when needed.
- Inputs, like 'open door' relays or some others similar depending on the controlled item.
- Outputs: actuators, relays, etc.

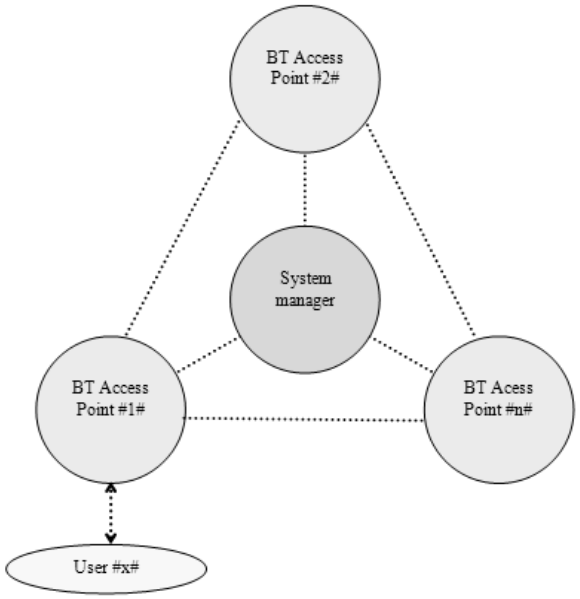

Figure 2. Networking scheme for data interchange.

The end user operation is quite simple. As to the basis application (see left side column, item "1"), it is only necessary to search for a Bluetooth device and once it is discovered, the user tries to connect to it (i.e. Garage#1). It will appear as a Headset or Hands Free device in the users mobile. If the user data is preloaded in the Application Point Terminal (see Figure 1) then the subsequent action will be done.

In respect to the advanced operation mode, which is explained in detail in Section F, the administrator must previously discharge the user from the system (only the first time), using the web server application developed for this purpose.

This "signing up" operation will download a simple MIDLet application which will generate the unique and encrypted key for this mobile phone in particular –taking some data out of it so as to generate the key, and only for a set of predetermined gates or terminals.

Once the key is installed in the mobile phone or PDA then the associated application is run and it transparently sends the users' encrypted key code to the Terminal.

The Net advanced application mode is similar to the Advanced application, except that in this mode the Terminals in range have the capacity for sending and receiving the events between each others. Thus all the Terminals connected could know if user "#x" has entered in the garage, and the "#door#" s/he used. This functionality allows to implement easily anti-passback strategies in multiple gate installations, or to filter users by their trajectory, etc.

As previously pointed out, the Access Point Terminal works normally off-line, and supports on-line connections as well.

Figure 3. Typical scenario of application

In the off-line operation, for downloading the event log or updating the firmware the user is required to connect to the system with administrator privileges; this is called System Manager in Figure 1 and Figure 2.

The System Manager consists of a Bluetooth connection to the Terminal which runs the manager software tool (which will be described in Section D.). For this purpose, only a SmartPhone, PDA or mobile phone with Windows Mobile and GPRS/3G connection is needed. Moreover, off-line updating done by the System Manager is carried out in three steps:

i. Download the file for uploading the Terminal from the Web Application Tool
ii. Connect to the Terminal, download the .log file and upload (if needed) the new configuration file.
iii. Reload, from the Web Application Tool, the log file obtained from the previous step and store it in the appropriate Terminal workspace.

B. Bluetooth™ profiles. Practical considerations

In the Bluetooth™ Specification [2], two types of links to support applications of voice and information are defined: an asynchronous link without connection (ACL, Asynchronous ConnectionLess) and a synchronous link orientated to connection (SCO, Synchronous Connection Oriented).

The ACL links support traffic of information without any guarantee of delivery; the transmitted information might be user information or control information.

The SCO links support voice in real time and multimedia traffic, using a reserved bandwidth. Both the voice and the information are transmitted in packages and the Bluetooth™ Specification allows implementing ACL and SCO links simultaneously. The asynchronous channel supports symmetrical and asymmetric communication. In the asymmetric communication 723.3 Kb/s can be sent from the server and 57.6 Kb/s towards the server, whereas in the symmetrical communication 433 Kb/s are sent in both directions.

In order for the system to include the expected functionality, we have implemented both selected profiles: Serial Port and Headset (ACL and SCO links). Thus, any electronic device with Bluetooth™ is able to discover the Bluetooth™ Access Control system.

The Bluetooth™ standard was created to be used by a great number of manufacturers and to be implemented in unlimited areas. To assure that all the devices that use Bluetooth™ would be compatible among them, standard schemes of communication are necessary. Therefore, different profiles have been defined considering several user communication models.

A profile defines a selection of messages and procedures of the Bluetooth™ Specification and it offers a clear description of the air interface for specific services. A profile can be described as a complete section of the stack of protocols, as shown in Figure 4.

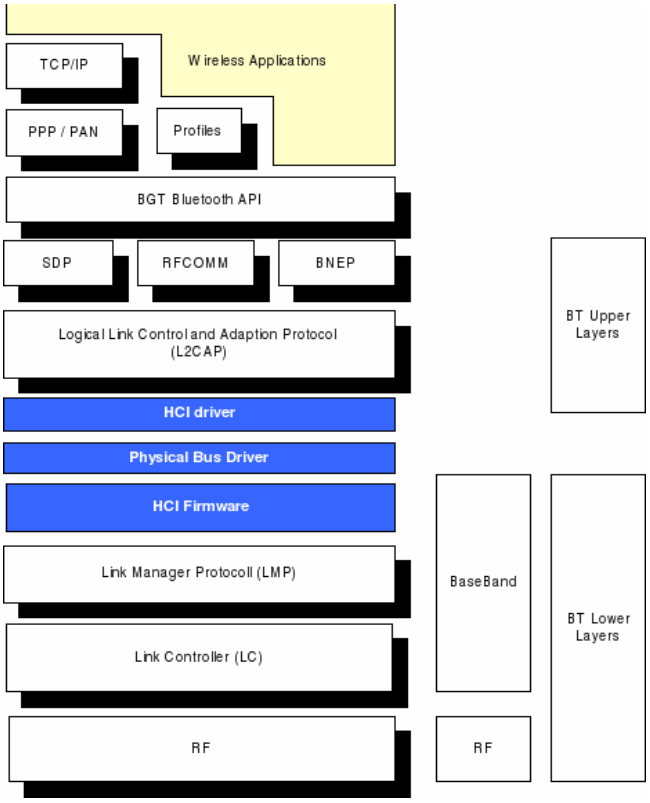

Figure 4. Bluetooth™ protocol stack [12]

There are four general definite profiles, on which some of the most important models of use and its profiles are directly based. These four models are Generic Access Profile (GAP), Serial Port Profile (SPP), Service Discovery and Application Profile (SDAP) and Generic Object Exchange Profile (GOEP), shown in Figure 5.

The Generic Access Profile (GAP) defines the general procedures for connection discovery and establishment between Bluetooth™ devices. The GAP handles the discovery and establishment between units that are not connected and ensures that any couple of Bluetooth units, no matter its manufacturer or application, could interchange information via Bluetooth ™ and discover the type of applications which support each unit. Furthermore, there are defined procedures related to the use of the different security levels.

The Serial Port Profile (SPP) defines the necessary requirements for Bluetooth™ devices to establish a connection of emulated serial cable between two similar devices using the RFCOMM protocol. This profile only requires support for one-slot packages. This means that information rates are the highest rates. RFCOMM is used to transport the user information, modem control signals and other configuration commands.

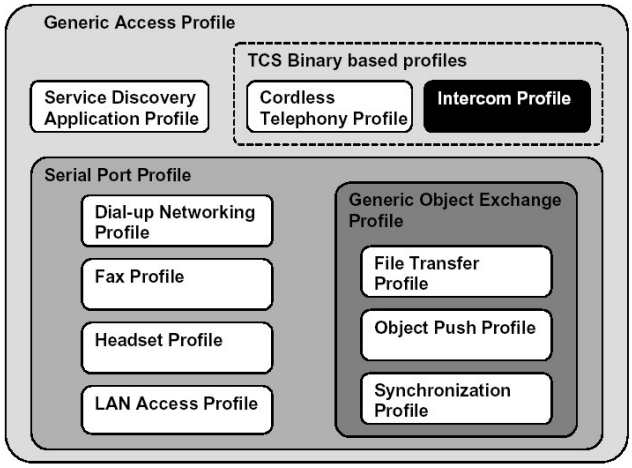

Figure 5. Bluetooth™ profiles –reduced set [2].

The Serial Port Profile is derived from the Generic Access Profile, therefore all the obligatory requirements of the Bluetooth specification applied to that profile are also applicable to the Serial Port Profile, and likewise those requirements defined as optional for the profile Generic Access Profile are also optional for the Serial Port Profile [2].

The Service Discovery Application Profile (SDAP) defines the protocols and procedures of an application in a device Bluetooth in which someone might want to discover and to recover information related to the services located in other devices. The SDAP is dependent on the GAP.

TABLE I. BLUETOOTH™ PROFILES RFCOMM UUIDS [2].

Profile Name	UUID
Serial Port	1101
LAN Access Using PPP	1102
Dialup Networking	1103
IrMC Sync	1104
OBEX Object Push	1105
OBEX File Transfer	1106
IrMCSyncCommand	1107
Headset	1108
Cordless Telephony	1109
Intercom	1110
Fax	1111
Audio Gateway	1112
WAP	1113
WAP_CLIENT	1114

The Bluetooth protocols stack contains the Service Discovery Profile (SDP), which is used to locate available services for devices that are found inside the environment or that are in range of some other devices. As soon as one has located the available services in one o more neighbouring devices, the user can choose one for his/her use. The selection, access and use of a service is the aim of this

profile. Though the SDP protocol is not directly involved in the procedure of access to a service, the information obtained through it facilitates the access to the above-mentioned service.

The Generic Object Exchange Profile (GOEP) defines the protocols and procedures used by applications to offer characteristics of exchange objects. The uses can be, for example, synchronization, transference of files or Object Push model. The most common devices that use this model are Personal Digital Assistants (PDAs) and mobile phones. The GOEP derives from the serial port profile.

We only have made a reduced list of them since our purpose was only to make an introduction and justification of the selected ones.

Table I shows the RFCOMM UUIDs codes of the Bluetooth™ Specifications considered.

Another issue is to set the device class code**,** which will be sent in subsequent inquiry responses. As observed in Table II, the device class code consists of a 6 digit hexadecimal derived number as defined in section "1.2 The Class of Device/Service Field" of the Bluetooth™ specification "Bluetooth™ Assigned Numbers" [2].

TABLE II. DEVICE CLASS CODE ASSIGNED TO HEADSET PROFILE [2].

Code (Hex)	Name	Major Service	Major Device	Minor Device
200404	Headset	Audio	Audio	Headset

Lower layers set up the SCO channel, and as soon as a SCO link is established, the following response is asynchronously sent to the host. It is very important to configure the three SCO channels correctly so as to support any BT audio device connection.

The user's security authentication and other related aspects need no further consideration since they are supported by all devices and are not a main source of problems. Final application in each case will force us to select the right security level among the possibilities that Bluetooth™ offers.

C. *Other practical considerations for the design*

Among the different alternatives of implementation, the adapters and the integrated modules, according to a two-processor model, are especially more adapted to the development of application systems with Bluetooth™ capabilities.

The main characteristics of this kind of systems will be exposed and the practical considerations will be taken into account before approaching their development. In Figure 6, it is shown a detailed graph of a model of a complete two-processor system based on the Bluetooth ™ technology [15].

In Figure 6, it can be observed that there are two main areas: the upper one or "Bluetooth Host" and the lower one or "Bluetooth Module". The top area or Host would contain the hardware/software support for the application that manages the communication with the Bluetooth ™ module, independently of the supported platform, and it also implements the higher layers of the Bluetooth protocol (upper central area with a white background). The lower area is the acquired Bluetooth™ module, that is, the one that physically will perform the wireless transmission tasks.

Therefore, we have to work on the development of the top layer, which includes the application, protocols of the top levels of the Bluetooth ™ Specification and the HCI driver (Host Controller Interface), by means of which Bluetooth™ manages the communication with the transceiver module (where the lower layers of the protocol are located).

In this area mentioned above, we also find the protocols (Figure 6, central area). The protocols are only a series of functions, procedures and commands with a given functionality established by the Bluetooth™ Specification. The manufacturers generally provide the protocols previously mentioned when the Bluetooth ™ module is acquired.

Thus it is necessary to develop an application that, by means of the use of the specification protocols [8], allows us to use the Bluetooth ™ technology like any other wireless communication as well as to implement the physical integration of the system previously mentioned with the Bluetooth™ transceiver module.

D. *Programming languages*

As to the application, it is necessary to develop the protocol profiles adapted to the functionality of the complete equipment. A profile defines a selection of messages and procedures of the Bluetooth ™ Specification and offers a clear description of specific services of the air interface.

A profile can simply be described as a complete section of the protocols stack.

When choosing the programming language, by means of which the application will be developed, it is very important to know the requirements of the environment on which it will be executed, and the main features are exposed in the following epigraph.

In relation to the real possibilities of implementation of both the protocols and the profiles, there is no restriction or limitation. Any programming language, of high and low level, is capable of supporting the collection of routines, functions and procedures that are established by the Bluetooth ™ Specification. This task will be more or less simple, obviously, depending on the chosen language.

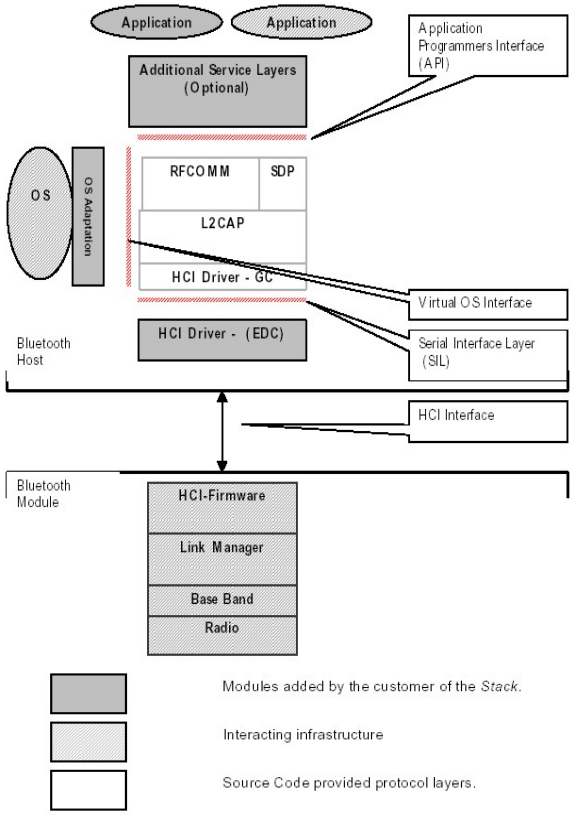

Figure 6. Diagram of a model of a complete two processor system [2]

At this point, it is important to remember that the Bluetooth™ Specification includes hardware, software and interoperability requirements. Therefore, the development of the process of protocols and profiles cannot be limited to a partial development of a running application, because they must comply with all the characteristics imposed by the norm, so in order to be qualified as Bluetooth™, the software must overcome the corresponding procedure of certification (Bluetooth Qualification Program).

Nevertheless, there are two languages that are especially better placed than the latter for this purpose: Java and C. With regard to its capabilities, power, existence of development and debugging tools, etc; for applications under multiple operating environments (in multiple operating systems) it is important to highlight two fundamental aspects that make these languages better than others for its use in applications with Bluetooth™ technology.

With regard to Java, we find great versatility for applications in embedded systems like PDAs, mobile telephones, etc., to the extent that a specific standard has been developed to support the Bluetooth ™ technology: JABWT (Java APIs for Bluetooth Wireless Technology) [14].

In the case of C language, we find also a similar versatility to Java since the code can be easily reusable and be integrated in an application developed by using high-level language or object oriented language, likewise it can be reusable for the programming of the systems based on such architectures as microprocessors or microcontrollers.

TABLE III. OPERATING SYSTEM REQUIREMENTS

Task	Comment
Process abstraction	Process can not be created, iniciated or stopped dinamically. Each process can only have one example.
Stack	Each task must have its own stack.
Message queue	Each task can only read from one message queue.
Dinamic memory management	The stack reads, assigns and frees memory dinamically.
Timers	Each task manage its own timer/counter.

E. The Virtual Operative system (VOS)

There is an element of great importance that might go unnoticed; it is the Virtual Operating System or VOS (Tables III and IV). The VOS is an abstraction of the services that an Operating System has to provide to the stack of protocols in order to be executed over a specific environment.

These services are a subset of the services that an O.S. would provide for multitasking and that are summarized in Table III; Table IV shows a classification of the most common operating systems, from a technical point of view.

TABLE IV. OPERATING SYSTEMS CLASIFICATION

OS	Description
Class A Windows 95/98/CE, Unix, Mac OS	Multithread (or multitask) with priority. Standar and advanced O.S. Provides a wide variety of services for multitasking. Adecuated for standard protocols and applications development.
Class B EPOC, OSE, PSOS+, VRTX,VxWork, MTOS	Multithread (or multitask) with priority. Multitask O.S. for embedded systems. Designed to be executed on proprietary hardware platforms. Limited set of services in relation to class A operating systems
Class C Windows 3.x	Multithread. Basic O.S. Lack of critical services. Main difference with class A and B operating systems.
Class D Palm OS, no operating system	Monothread or monotask. Doesn't provide multitask services in real time execution.

The aim of the design and development of the concept of the virtual operative system (*VOS*) is that the Bluetooth protocol stack could be directly exported towards environments of an A or B class. This fact does not imply that it could not be exported to more basic environments, it simply means that the management of the multiple processes, that internally provide an A or B class OS, must be re-implemented by the developer, using the methods of variable management and shared processes, such as semaphores or other multithread strategies.

F. System structure

The developed system has been designed following a hierarchical scheme, starting from a simple but fully functional module and adding new features in order to

improve the functionality and open connectivity with mobile devices. As Figure 1 shows, the user establishes a connection with the Terminal. Then, the Control Unit processes the information and generates a subsequent action. These actions could be of the kind of a simple activation of an output (to actuators), recording the timestamp and event, requesting or sending data to/from other similar units or managing the system using, for instance, air interfaces (see Figure 1 and Figure 2).

There are two models of the proposed system that correspond with two levels of security. As to the simple –and cheapest one, the basis is to carry out previously the recording of the MAC addresses of the authorized users in the control unit. Only by performing a connection to the system, that appears like a hands free unit, the Control & Access Point Terminal (Figure 1) knows MAC users, it checks if the user is authorized and performs some predefined actions (e.g., activates an output for door opening, activates/deactivates an alarm, etc.). This way, the end user does not need any additional software or human-machine interfaces.

Additional features are based on the processing of different actions depending on the value of the PIN requested or in other data, like recording the events in a file or sending a message to another control unit.

In addition, Java MIDP 2.0 and JSR82-based software [14] is thought to enable an end user friendly interface, present in most of the mobile phones in market, as an optional feature. This MIDlet is necessary for the so-called "Advanced App." mode of operation (see Section III – A), which performs higher security levels.

The core of this mode of operation (which includes mode .iii Network Advanced) is a Web Server Application that manages the unit control, as shown in Figure 7.

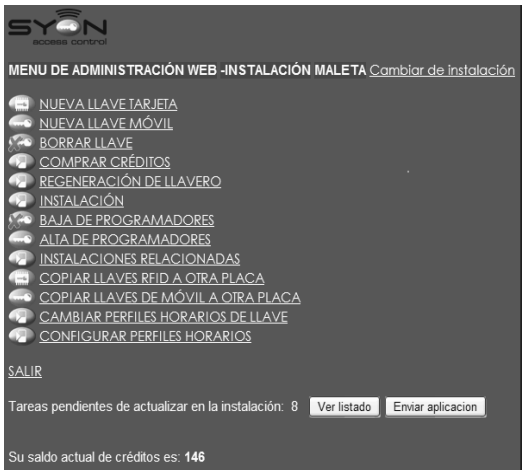

Figure 7. Web application for administrators.

When a user is registered (its phone number), s/he will receive a SMS with a link to this web application. This only takes place once. If the user runs the link, a MIDlet application will be installed in his mobile phone, generating the encrypted id-code for the user and for an Access Point Terminal in particular. Also, a little application stays in the mobile in order to manage the sending and receiving process while requesting to "open" a door or any other action associated to a module or terminal. Nowadays, the MIDlet is present in most of the mobiles in market, having only some limitations in functionality with the iPhone, which are supposed to be resolved in brief through AppleStore.

The main features of this web application are:

- Multilingual web application
- An Activate/deactivate key is fully functional worldwide.
- Management of event record file: downloading and sensing by email or even via SMS.
- Schedule users (e-keys) in real time.
- Valid for most mobile operators worldwide (SMS and GPRS connection must be supported).
- Management of several installations in the same application.

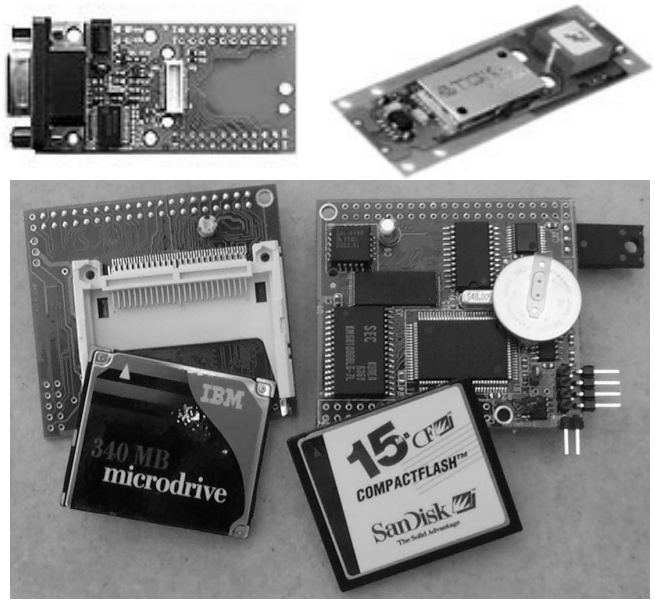

Figure 8. Bluetooth™ Class I modules (upper) and MCU (bottom) used.

Thus, by using this web-based application, the system administrator could easily manage any installation equipped with this kind of modules, e.g.:

- The edition of authenticated users in real time.
- Downloading event record files.
- Ordering the access profile for a key/user –by time and date.
- Association of multiple users and/or multiple installations (terminals).
- Administration of users' privileges.
- Generation of emergency keys, valid only temporarily.
- Other management utilities.

This web application allows to authorize new users in real time without the need to update online the main access module. It is important to point out that the modules work both off-line and on-line, in both cases they preserve the same features and functionality.

When registering new users, we find several gaps with additional information about the end user, like full name, surname, address, country, phone number (country code generates automatically, etc.). When we generate the authenticated user an SMS will be sent containing a link to this web application.

Then, the user connects to the link, if the user mobile phone is validated, then a simple MIDLet application will be downloaded and launched, taking out further information of some parameters of the mobile phone, and generating automatically an unique encrypted code for the selected key which will remain installed in the mobile phone. The security features make this code only valid for the user selected and for the gates predetermined in the signing up process carried out by the administrator.

It is only is necessary to connect to the Internet through the mobile phone the first time we install the MIDlet (encrypted e-key) in the mobile. The rest of the operation and use will be done using Bluetooth™, that is, free of any charge for the end user and independent from the degree of GPRS network coverage.

G. *Proposed implementation*

The developed system is based in a Class I Bluetooth™ module plus a microcontroller-based board acting out as Control Unit (Figure 8).

The Control Unit has as main features the followings: 20 GPIO, 16-bits ADC inputs, 12-bit output DAC, Real Time Clock, SPI ports, Timers and it supports Compact Flash Cards. The Bluetooth™ module is attached to one of the serial ports of the board.

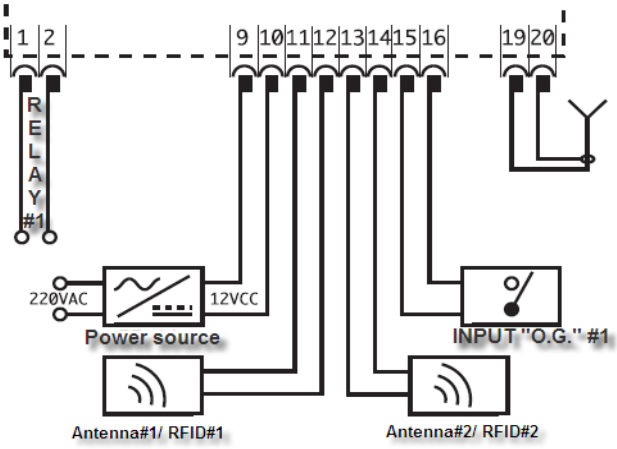

Figure 9. Wiring diagram of terminals for module developed.

This system is low cost and with low power consumption, so it complies perfectly with the system requirements for the controller role assigned (see Section III), which have been proposed and exposed in the present work. The complete wiring diagram is shown in Figure 9.

Additionally, two RFID antennas have been installed to enhance the behavior and market deployment and to provide an added value for the end user. So, the system supports simultaneously access control via Bluetooth and RFID, allowing it to be installed e.g., in a garage of a building and allowing the users to choose the kind of key they prefer. The antennas used in the modules are present in 125kHz tags, preferably Unique® brand.

Also, the Access Point Terminal has up two "open gates" inputs. Each input (12Vdc) must be returned to the system through a free potential conductor. These inputs are used as a feedback in the control unit.

Hardware relays up to four outputs. These outputs are connected to non-potential relays, with maximum power ratings of 1 A - 110Vac or 30 Vdc.

Finally, in Figure 10, a demo board set up in a suitcase is shown. On top of it there are several lights emulating the opening of a door, the activation/deactivation of an alarm, the opening of a garage and the lights switching on/off. Also, both RFID readers and the central switch represent journey endings or "Gate- opening" sensor as module inputs.

At the bottom, we can observe the module itself (bottom right corner) and some RFID tags, some mobile phones and the main DC power sources.

Figure 10. Prototype set up in demo suitcase

IV. CONCLUSION AND FUTURE WORKS

Wireless connectivity has become recognized as a flexible and reliable medium for data communication in a broad range of applications. This is due to wireless networks potential to operate in demanding environments providing clear advantages as far as the cost, size, power, flexibility, and distributed intelligence levels are concerned.

This paper presents a novel application of Bluetooth™ technology to access control systems suitable for home and building applications. The proposed system is low cost, autonomous, physically and functionally scalable and with control and interaction capacities. Moreover, using Bluetooth™ allows designing flexible networks for these kinds of applications. In the paper, some considerations about configuration, security, data management and other features have been presented and discussed.

The final system is divided in three modules: the web server based administrator tool, the end user application and the module itself, which is installed in the access point. Several software posibilities have been developed for an isolated usage or for more complex information exchange among multiple access points.

Further improvements can be done by using this Bluetooth™ based system for pervasive enviroments scenarios. Whilst the system by itself give us the neccesary network infrastructure for communicate, new applications can run to manage the gathered user information for other comfort issues. Of course, security and privacy of data must be assured.

ACKNOWLEDGEMENTS

R&D Project "Bluesensory". Local Government Funding for Research Projects. (Andalucia, Spain) & Stop Casa Segura S.L.

Spanish Patent Pending No.: 200501374/2264387. European Patent Pending No.: 06380014.8

REFERENCES

[1] Bellido Outeiriño F.J.; Canales Aranda, P.M.; de la Cruz Fernández, J.L., Pérez Jarauta, and B. "Universal Bluetooth™ Access Control and Security System for e-Keys Enviroment". Proc. of the 4th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE 2010). Published by CPS. ©IEEE. 2010, pp. 247-250, DOI 10.1109/SECURWARE.2010.47. ISBN 978-0-7695-4095-5. Best Paper Award.

[2] Bluetooth™ SIG. Bluetooth™ Specifications. Core and Profile. http://www.bluetooth.org, December 2011.

[3] Zigbee™ Alliance. http://www.zigbee.org, December 2011.

[4] Bellido Outeiriño, F.J., Flores Arias, J.M., Real Calvo, R., and Torres Roldán, M., "LR-WPAN Technologies. An approach to industrial applications". Proceedings of International Conference IT Revolutions 2008. pp. 1-4, Venice (Italy). IEEEXplore D.O.I 10.4108/icst.itrevolutions2008.5112

[5] Miroslav Sveda and Radimir Vrba, "Meta-Design with Safe and Secure Embedded System Networking" International Journal On Advances in Security, issn 1942-2636 , Vol. 2, no. 1, year 2009, pp. 8-15.

[6] Seppo Heikkinen, Kari Heikkien, and Sari Kinnari, "Security and User Aspects in the Design of the Future Trusted Ambient Networked Systems"International Journal On Advances in Security, issn 1942-2636, Vol. 2, no. 2&3 year 2009, pp. 156-170.

[7] Il-Kyu, H. and Jin-Wook. B., "Wireless Access Monitoring and Control System based on Digital Door Lock". IEEE Trans. On Consumer Electronics, Vol. 53, No 4, Nov. 2007, pp. 1724-1730.

[8] Soo-Hwan, C. Byung-Kug, K., Jinwoo, P., Chul-Hee, K., and Doo-Seop, E., "An Implementation of Wireless Sensor Network for Security System using Bluetooth™". IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, Feb. 2004, pp. 236-244.

[9] Tajika, Y., Saito, T., Teramoto, K., Osaka, N., and Isshiki, M., "Networked home appliance system using Bluetooth™ technology integrating appliance control/monitoring with Internet service", IEEE Transactions on Consumer Electronics, Vol. 49, No. 4, Nov. 2003, pp. 1043-1048.

[10] Bellido Outeiriño, F.J., de la Cruz Fernández J.L., Torres Roldán M., and Moreno Muñoz, A., "Wireless technology applied to stimulation systems for auditory deficit children". Proc. of the 12th IEEE International Symposium On Consumer Electronics (ISCE 2008). Vilamoura-Portugal, pp. 1-3, D.O.I. 10.1109/ISCE.2008.4559501

[11] RFID. Association for Automatic Identification an Mobility. http://www.rfid.org, December 2011.

[12] EPC Global http://www.epcglobalinc.org, December 2011.

[13] Bluegiga http://www.bluegiga.com, December 2011.

[14] Kumar, C.B. Bluetooth™ Application Programming with the JAVA APIs, Elsevier Science & Technology Books, 2003.

[15] J. Haartsen, *The universal radio interface for hoc, wireless connectivity*, Ericsson Review Vol. 75 (1998):3, pp. 110-117.