

# Wireless Access Control System Using Bluetooth

**Juliano Rodrigues Fernandes de Oliveira**

*Federal University of Campina Grande, Brazil*

**Rodrigo Nóbrega Rocha Xavier**

*Federal University of Campina Grande, Brazil*

**Yuri de Carvalho Gomes**

*Federal University of Campina Grande, Brazil*

**Hygo Almeida**

*Federal University of Campina Grande, Brazil*

**Angelo Perkusich**

*Federal University of Campina Grande, Brazil*

## INTRODUCTION

Security is one of the world's main challenges. Research and industrial applications related to security include several areas such as personal security, organizational security, and computer security, among others. This article is concerned with secure environments, which is related to the control of people entering an environment, building, rooms, laboratories, and so forth. In this context, access control systems are the main security mechanisms to control the access of authorized people to environments.

Nowadays, locks and keys are not enough to keep an environment secure against unwanted or uncontrolled visitors. To have access, mechanical security systems are widely used, however, such systems—purely mechanical—can be easily defrauded. To construct high-security access systems, the embedded electronics have associated to the mechanical security, with the objective of increasing the level of reliability of such systems. Besides, with the increasing use of mobile devices, users are more and more interested in mobile solutions to support several activities, including security-related ones.

This article presents an access control system that uses Bluetooth technology (Ericsson Bluetooth, 2006) to allow control of the entrance to environments. By using the proposed system, a person with a smart phone can use it to get access to environments, such as buildings, labs, rooms, and so forth.

The remainder of this article is organized as follows. First we present the architectural components of the proposed system and detail their functioning. We then discuss future trends and offer concluding remarks.

## BACKGROUND

### Bluetooth

The Bluetooth specification was developed by Ericsson (now Sony Ericsson) and later formalized by the Bluetooth Special Interest Group (SIG). The SIG was formally announced on May 20, 1999, and originally founded by Ericsson, IBM, Intel, Nokia, and Toshiba.

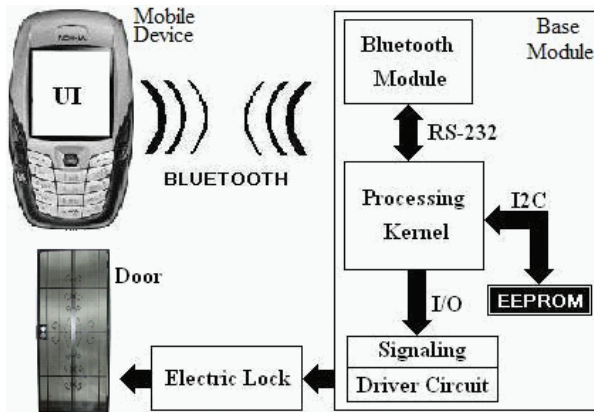
Bluetooth is an industrial standard for wireless personal area networks (PANs), also known as IEEE 802.15.1 (Bluetooth SIG, 2004). It provides a secure, low-cost way to connect and exchange information between devices, such as personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, and digital cameras, in a globally available short-range radio frequency. This technology eliminates cables and wires between devices, facilitates both data and voice communication, and enables ad-hoc networks between multiple Bluetooth devices (Cardei, 2002).

Bluetooth is a radio standard primarily designed for low power consumption, with a short range (power class dependent: 1 meter, 10 meters, 100 meters) and with a low-cost transceiver microchip in each device. It lets these devices communicate with each other when they come in range, even if they are not in the same room, as long as they are within up to 100 meters of each other, depending on the power class of the product (Kardach, 1998).

### Microcontrollers

A microcontroller (or MCU) is a computer-on-a-chip used to control electronic devices. It is a microprocessor empha-

Figure 1. Wireless access control system architecture



sizing self-sufficiency and cost-effectiveness, in contrast to a general-purpose microprocessor used in a PC. It can be defined as a single integrated circuit with a central processing unit, usually small and simple; input/output interfaces, such as serial ports; peripherals, such as timers and watchdog circuits; RAM for data storage; ROM for program storage; and a clock generator, often an oscillator for a quartz timing crystal, resonator, or RC circuit (Stewart, 1993).

In addition to the key features, most microcontrollers today take further advantage of not needing external pins for memory buses. They can afford to use the Harvard architecture: separate memory buses for instructions and data, allowing multiple access to occur concurrently (Cady, 1997).

A typical microcontroller contains all memory and interfaces needed for a simple application, whereas a general purpose microprocessor requires additional chips to provide these functions. Microcontrollers also usually have a variety of input/output interfaces. Serial I/O (UART) is very common, and many include analog-to-digital converters, timers, or specialized serial communications interfaces like I<sup>2</sup>C, serial peripheral interface, and controller area network.

A microcontroller is also a programmable device that can be destined for several purposes. The firmware recorded in its memory is responsible for the characteristic of its application. Microcontrollers are versatile tools and with low cost for embedded systems design.

Originally, microcontrollers were only programmed in assembly language, or later in C code. Recent microcontrollers, integrated with on-chip debug circuitry accessed by in-circuit emulator via JTAG, enable a programmer to debug the software of an embedded system with a debugger (Cady, 1997).

Microcontrollers trade speed and flexibility against ease of equipment design and low cost. This integration drastically reduces the number of chips and the amount of wiring and

space that would be needed to produce equivalent systems using separate chips. Manufacturers and designers have to balance the need to minimize the chip size against additional functionality.

## SYSTEM ARCHITECTURE

The access control system architecture depicted in Figure 1 consists of two modules: mobile and base. A smart phone contains the software responsible for beginning the authentication process, acting as mobile module. The base module is responsible to receive a valid authentication code and to allow the access to the environment by unlocking an electric lock embedded in the environment entrance door.

The base module is composed of a Bluetooth module (Wintec BT Module, 2005); a processing kernel, represented by a microcontroller (Microchip PIC18FXX2, 2002); an external data storage unit, represented by an EEPROM memory (Microchip 24LC256, 2002); and an electric lock interface, represented by a driver circuit to unlock the electric lock.

In general, the user authentication process consists of sending the user authentication key from the application running in a mobile device to the Bluetooth module, through Bluetooth connection. The Bluetooth module sends such information to the processing kernel, which performs the authentication through comparison of the user key sent with that stored in the external data storage unit. Next, the processing kernel sends the search authentication result to the mobile device and to the electric lock interface. If the user key is valid, the electric lock interface unlocks the environment entrance door. Each architectural component is detailed in what follows.

### Mobile Module and Bluetooth Module

Mobile Module is the application embedded in a mobile device that performs the communication with the Bluetooth module. It has been developed in J2ME (2006). Such an application is based on the Bluelet open source software (Bluelet, 2006). The entire connection negotiation process has been implemented using protocols of the Bluetooth protocol stack to perform connections via Serial Port Profile (Wintec Bluetooth, 2004).

The basic process to connection negotiation consists of three steps:

1. Search for the Bluetooth module (discovery function), through the name “Wintec Serial Port” or the Bluetooth module address.
2. Authentication, or pairing, using the code sent by the mobile device to the Bluetooth module (bond function).

3. Connection establishment (connect function) based on serial port profile. A wireless communication is emulated by a connection via serial port with UART protocol (Wintec Bluetooth, 2004).

Regarding the application functioning, first of all it performs a connection to the Bluetooth Module directly, through the Bluetooth module address. Such an address is discovered by localization of Bluetooth devices and stored in the device. If the Bluetooth Module is inaccessible—distant or turned off—or if it is not found in the direct connection attempt, the software automatically performs two more attempts, notifying the user visually. If no attempt works, then the software will be finished.

After the Bluetooth connection establishment, the access control system awaits the sending of the user key. In this case, a string containing the user authentication key is transmitted from the smart phone to the Bluetooth module. This key needs to be registered in the application by the user and then stored in the mobile device. If the operation is successful, the electric lock is unlocked and the user is informed visually that the door has been opened. Afterwards, the connection is closed and the application is finished.

### Processing Kernel

During the connection establishment process between the smart phone and the Bluetooth Module, messages (in ASCII format) are sent from the Bluetooth module to the microcontroller host, which represents the Processing kernel. The firmware contained in the microcontroller host monitors these messages awaiting the final message of connection closing. Meanwhile, it continues awaiting the user authentication key that must be sent by the mobile device. When it receives such a key, it analyzes it, and if the key is registered in the system database, the host will unlock the electric lock. After the data exchange between the mobile device and the Bluetooth module, the microcontroller sends to the Bluetooth module the escape sequence to close the Bluetooth connection.

### External Data Storage Unit

The external memory EEPROM is used as a persistent data storage device in this wireless access control system. It is very important due to the reduced capacity of internal memory available in the microcontroller.

The user information is stored in the external memory as a *login/password* table. A pointer to free memory positions is used to indicate which memory spaces are available to register new users.

The recording operation of user authentication keys begins when the processing kernel receives a *write command*.

The user information, *login* and *password*, contained in this command are then stored in the external memory unit.

The search operation for user authentication keys begins when the processing kernel receives an *access command*. The user information, *login* and *password*, contained in this command are acquired and stored in vectors, for search and comparison with stored data in the memory unit. If user information is valid, the operation will be successful. Otherwise, the operation has failed and the electric lock will not be unlocked.

### Electric Lock Interface

The electric lock Interface is represented by a driver circuit of the electric lock and by a panel composed by LEDs that indicates the current operations during the authentication process. It is responsible for informing of the status of the driver circuit. There are four LEDs. One of them indicates that the circuit is energized and active. Another indicates that a recording operation is currently being performed. Yet another LED indicates that the search operation for user key has been performed successfully and the electric lock was unlocked, allowing access to the environment. The last LED indicates that the search operation has failed (invalid code) and the electric lock has not been unlocked, not allowing the user access to the environment.

### FUTURE TRENDS

In the context of the proposed system, in order to improve the reliability of the data exchange between the remote device and the access control system, revisions in the firmware contained in the processing kernel are necessary. Some suggestions to increase the reliability are: addition of an administrator user, development of new functions for this administrator to control and supervise the system, and better sub-routines to search for registered users.

Regarding future efforts in mobile-related access control technologies, the main trends are concerned with pervasive environments. For example, current access control technology works by keeping the entrance door closed and opening it for authorized persons. But there is another way: the door could be left open and only closes when an unauthorized person tries to enter. In this case, the access control system must be monitoring the environment, and when an unauthorized person comes close, the door is blocked. This example has a pervasive characteristic in which the system is “invisible” for the user. Several access control researches are moving in that direction, to conceive environments that manage and control their security without needing a direct user intervention.

## CONCLUSION

Security is a growing need throughout the world, and lack of security can result in great damage. Many solutions are available for all levels of access control—from highly restricted areas such as laboratories or computer rooms to less restricted areas such as storage rooms.

Access control solutions include electronic keys, magnetic stripe cards, proximity cards, and smart cards or biometric devices, including hand and fingerprint readers. More sophisticated access control capabilities, such as auto-unlock/auto-lock functionalities, allow programming an electronic locking system to lock and unlock any door at any time.

With the increasing personal use of mobile devices and growing industry investments in this area, it is a trend to use mobility capabilities to support user activities, mainly security-related ones. The proposed access control system using Bluetooth is a good example of how to join mobility and reliability to support user activities in a practical and secure way.

## REFERENCES

Bluelet. (2006). *Bluetooth GUI component*. Retrieved from <http://benhui.net/>

Bluetooth SIG. (2004). *Bluetooth Special Interest Group launches Bluetooth Core Specification version 2.0 + Enhanced Data Rate*.

Cady, F. M. (1997). *Microcontrollers and microcomputers*. Oxford: Oxford University Press.

Cardei, M. (2002). Overview over the Bluetooth technology. *Proceedings of the Wireless Networking Seminar*, University of Minnesota.

Ericsson Bluetooth. (2006). *Ericsson Bluetooth*. Retrieved from <http://www.ericsson.com.br/bluetooth/index.asp>

J2ME. (2006). *Java 2 Micro Edition*. Retrieved from <http://java.sun.com/j2me/index.jsp>

Kardach, J. (1998). *Bluetooth architecture overview*. Intel.

Microchip 24LC256. (2002). *Microchip 24LC256 256k I2C CMOS Serial EEPROM datasheet*. Microchip Technology.

Microchip PIC18FXX2. (2002). *Microchip PIC18FXX2 datasheet*. Microchip Technology.

Stewart, J. W. (1993). *The microcontroller*. Englewood Cliffs, NJ: Regents/Prentice-Hall.

Wintec Bluetooth. (2004). *Wintec Bluetooth SPP command interface quick start guide*. Wintec Industries.

Wintec BT Module. (2005). *WBTV42-D-XXX Bluetooth module rev 0.8 guide*. Wintec Industries.

## KEY TERMS

**American Standard Code for Information Interchange (ASCII):** A standard for coding text files. Every character has an associated number, and any text can be represented by a sequence of numbers.

**Electrically Erasable Programmable Read-Only Memory (EEPROM):** A non-volatile storage chip used in computers and other devices (such as USB flash drives, in its flash memory version); also called E2PROM.

**I<sup>2</sup>C (Inter-IC) Bus:** A bi-directional two-wire serial bus that provides a communication link between integrated circuits (ICs).

**J2ME:** Collection of Java APIs for the development of software for resource-constrained devices such as PDAs, cell phones, and other consumer appliances.

**Serial Port Profile (SPP):** Defines how to configure and connect the virtual serial port between two wireless devices supporting Bluetooth technology.

**Smart Phone:** Any electronic handheld device that integrates the functionality of a mobile phone, personal digital assistant (PDA), or other information appliance. This is often achieved by adding telephone functions to an existing PDA or putting “smart” capabilities, such as PDA functions, into a mobile phone. A key feature of a smart phone is that additional applications can be installed on the device. The applications can be developed by the manufacturer of the handheld device, by the operator, or by any other third-party software developer.

**Symbian OS:** An operating system designed for mobile devices, with associated libraries, user interface frameworks, and reference implementations of common tools, produced by Symbian Ltd.

**UART:** Universal Asynchronous Receiver/Transmitter protocol.