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

Hyggo 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.

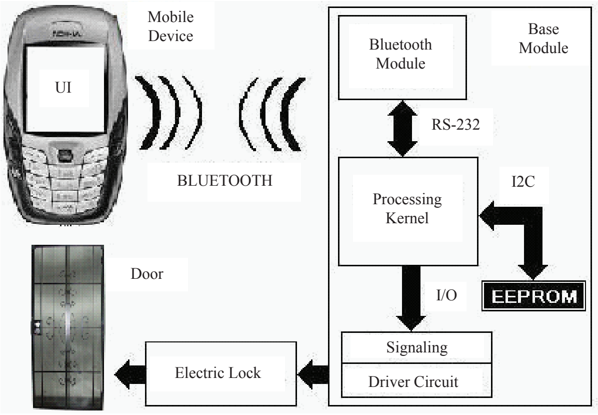
Bluetooth is an industrial standard for wireless personal area networks (PANs), also known as IEEE 802.15.1 (Bluetooth SIG, 2004). It provides a secure, low-cost way to connect and exchange information between devices, such as personal digital assistants (PDAs), mobile phones, laptops, PCs, printers, 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 (MCU) is a computer-on-a-chip used to control electronic devices. It is a microprocessor emphasiz-

Figure 1. Wireless access control system architecture



ing 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^{2}C, serial peripheral interface (SPI), and controller area network (CAN).

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 language (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).