Proceedings of the 5th WSEAS Int. Conf. on Instrumentation, Measurement, Circuits and Systems, Hangzhou, China, April 16-18, 2006 (pp252-256)

Security of wireless Bluetooth™ sensor systems

MARIA RIZZI, MICHELE MAURANTONIO, BENIAMINO CASTAGNOLO
Dipartimento di Elettrotecnica ed Elettronica,
Politecnico di Bari
v. E. Orabona, 4 - 70125 Bari
ITALY

Abstract: - A low power, portable, and secure Bluetooth™ sensor system has been designed and its performance has been evaluated. Light weight, small size, high interference immunity and interoperability with a personal area network are fundamental characteristics in designing the sensor system so the architecture has been implemented adopting an FPGA and a Bluetooth™ module. The design analysis shows the possibility to transmit continuously analogue signals with a high level of security. At low sampling rates, the adopted solution offers low power consumption and consequently battery with lower capacity can be adopted, minimizing the sensor system weight. With higher sampling rates, the system equipped with a FPGA offers the best architectural solution and performance. Therefore, Bluetooth™ can be satisfactorily adopted in many different applications: in the example reported in the paper, it is used for monitoring critical parameters, such as vital signs in patients having serious pathologies.

Key-Words: Bluetooth™, wireless technology, security, sensor system, telemetry

1 Introduction

Bluetooth™ wireless technology is gradually becoming a popular way to replace existing wireline connections with short-range wireless interconnectivity. It is also an enabling technology for new types of applications.
An increasing number of researchers and manufacturers is working to develop a new generation of wireless technology applications in different environments, such as in medical field to improve the life quality and to reduce the cost of patient care.
The personal area network (PAN) concept is a vision shared by a large number of researchers and wireless technology drivers. A PAN consists of a limited number of units interconnected to form a network and to exchange informations. Bluetooth is used as a local connection interface between different personal units, such as mobile phones, laptops, personal digital assistants (PDA), printers, keyboards, mouses, headsets, and loudspeakers. Hence, Bluetooth™ is a true enabling technology for the PAN vision. The units are typically consumer devices made normally by different manufacturers and having different usage ways. Hence, in order to provide interoperability among the personal devices, the security level has to be chosen by the user. Bluetooth™ security solutions have been designed to make any ordinary user able to configure and manage the necessary security actions, to protect the communication links.

By PANs, users can access to data from their office and store them in an information system or in an electronic personal record [1][2][3].
Connected to a global network or Internet, the above benefits can be used for long distance monitoring or consultation with other users.
The implementation of wireless systems have to take into account the following important key points [4]:

- System high interference immunity;
- Security to prevent eavesdropping or to deny intruders accesses;
- Interoperability with other technologies for communications;
- Possibility to use wireless devices everywhere, avoiding the location track down

There are four fundamental security expectations for Bluetooth:

- Easy-to-use and self-explanatory security configuration;
- Confidentiality protection;
- Authentication of connecting devices;
- Anonymity.

In this paper after a summary of the Bluetooth™ standard, a sensor system architecture is presented and its benefits are indicated. Moreover, the

problem of the Bluetooth security is analyzed and the adopted solution is drawn out.

2 The Bluetooth™ Standard

The Bluetooth™ is now developing as a network technology able to support data and voice communications and characterized by low complexity, robustness, low power and cost [5].
Bluetooth™ supports 723.2 kbit/s [6], which is perfectly adequate for sensor data transfer applications.
To avoid interference from other signals, it uses the Frequency Hopping Spread Spectrum (FHSS) technique and operates at 2.4 GHz in the globally available license-free Industrial, Scientific and Medical (ISM) band. Compared with other systems in the same frequency band, the Bluetooth™ radio hops is very faster and uses shorter packets. There are 79 channels 1 MHz bandwidth, starting from 2.402 GHz up to 2.480 GHz.
Moreover, Bluetooth™ has the ability to form PANs or Piconets composed by one master device with up to seven slave units. When a device is present simultaneously in more than one piconet, a scatternet is established. The master establishes the hop sequence and communicates with active slaves adopting the Time Division Multiplex (TDM) technique in which the time is divided into 625μs intervals called slots [7]. The master to slave transmission starts in even the numbered slots while the slave to master transmission starts in odd numbered slots. Masters and slaves are allowed to send 1, 3, 5 slot packets which are transmitted in consecutive slots. Forward Error Correction (FEC), Cyclic Redundancy Check (CRC), Header Error Check (HEC) and Automatic Repeat reQuest (ARQ) techniques provide data protection against imperfect channels [8].
Bluetooth™ provides for high security mechanisms including a globally unique six byte Bluetooth Device Address (BDA), authentication authorization, encryption and PIN exchange at user level [8].

3 Bluetooth™ Sensor Architectures

The architecture of the system consists of seven client modules and one master module for the system control. The main component for each module is an FPGA, as shown in fig.1, which allows the device to be programmed, debugged, and reconfigured after it is soldered onto a printed circuit board. In this way the possibility of lead damages and electrostatic discharge exposures is minimized.

In this paper signals are generated by biomedical sensors, for monitoring critical parameters, such as vital signs in patients having serious pathologies. The wireless sensor architecture has been already developed [9][10][11]. It has been realized using one Analog/Digital Converter (ADC) and two processors sharing the Bluetooth™ stack (Fig.1). A 24-bit multiplex sigma-delta converter converts the analogue input signal with 0-5Volt range. The sampling rate is 500 Hz on each of two channels. The digital signals are transmitted to a remote acquisition master sensor via Bluetooth™ (PAN1540). The FPGA controls the acquisition from the sigma-delta converter and, as soon as an AD conversion has been made, saves that particular value in the FPGA internal RAM memory.
The FPGA sends the data from the memory to the Bluetooth™ module while controlling and storing the new ADC value. The Bluetooth™ management is implemented in the FPGA and controls the Bluetooth™ module. The FPGA construct and decodes the Host Controller Interface (HCI) packages in order to establish connections and manage data communications. The communications between the FPGA and Bluetooth™ is done by serial UART (Fig.2).

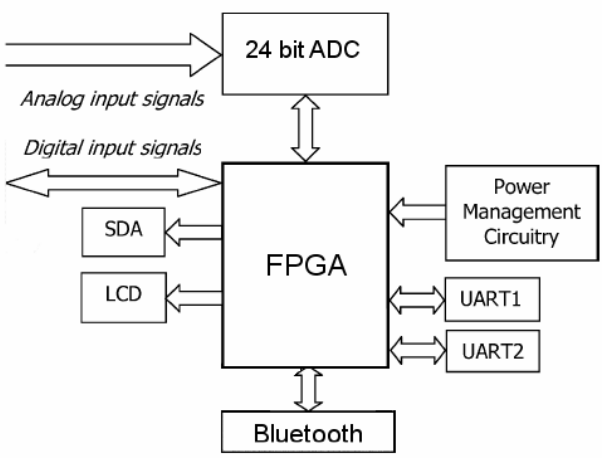

Figure 1: The main component of module

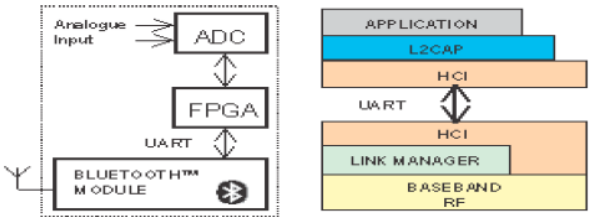

Figure 2: The FPGA control management

The power management circuit, which powers all the modules, consists of linear voltage regulators to

provide positive and negative voltages from a PP3 9-V battery with a rating of 550 mAh. The regulators have a maximum current drain of approximately 500 mA, which although high still allows over an hour of continuous operation. In idle state, the current drain is less than 1.5 mA.

The minimal solution with only 1-chip wireless sensor using the internal uncommitted 8-bit ADC of the PAN1540 is possible. This implementation is an embedded solution where the Bluetooth™ module executes a Virtual Machine (VM) application [12].

Pan1540 has three general purpose analog interface pins [12]; two of them are used as analog inputs for the ADC, which acts as input channel for a sensor signal.

The ADC is controlled by user code, which is interpreted by the VM when the scheduler runs the task.

This solution has been revealed unsatisfactory because the PAN 1540 allows only a limited number of instructions of the VM before changing context. Therefore, there is no guarantee that the ADC will be controlled in real time while another process starts. Moreover, PAN1540 does not support a Real-Time Operating System (RTOS) because the execution latency of embedded code is random.

4 Bluetooth™ Security sensor networking

To find the correct level of security when a new communication technology is defined is a nontrivial task: the versatility of Bluetooth increases the difficulties in finding the correct level. However, in order to offer interoperability and to provide support for a specific application, it as been developed a set of so called profiles. A profile defines an unambiguous description of communication interface between two units for one particular service.

The very original purpose of the Bluetooth standard was short-range cable replacement. Pure cable replacement through RS232 emulation is offered by the serial port profile. Several other profiles, like the personal area network (PAN) and local positioning profile make use of the serial port profile. One level deeper in the profiles hierarchy is the general object exchange profile.

In this section we will discuss security issues and solutions for remote access to a Subscription Identity Module (SIM) over a Bluetooth connection [13]. A SIM card is an integrated circuit card used in the GSM mobile telephony system used to hold subscriber informations. In this paper a SIM solution is implemented inside the FPGA ROM memory. Altera Quartus II v5.1 software generates the FPGA configuration data file, which is downloaded and stored in the Flash ROM of the processor and memory module. Details of the FPGA architecture [14][15] and the software [16][17][18] are beyond the scope of this paper and therefore, are not presented further.

This SIM information are used to connect securely a remote sensor to a master network (PDA, smartphone, laptop). They make it possible to the mobile network operator to identify securely subscribers attempting to the network. Consequently, it also allows the operator to enable the connect of mobile network services. The Bluetooth SIM access profile defines procedures and protocols for the access to a remote SIM over a Bluetooth serial port (RFCOMM) connection. The protocol stack is illustrated in Fig.3. The SIM access messages consists of a header and a payload. The header describes the type and the number of parameters transferred in the message. Messages have been defined for the remote control of the SIM sensor and for transfer SIM messages.

Two different roles are defined in the profile:

1. SIM access client;
2. SIM access server.

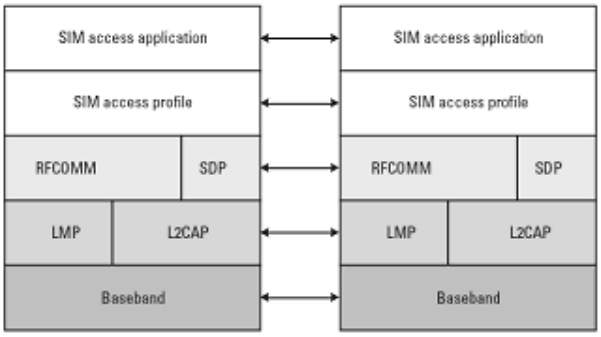

Figure 3: The SIM access profile communication stack

The SIM access client uses the SIM access profile for the connection to another device, the SIM access server, over the Bluetooth. The adopted interconnectivity system is illustrated in Fig.4.

In this scenario, seven SIM access clients are wireless interconnected with one SIM access server (laptop) within PAN wireless network. A SIM access is needed for the subscriber authentication inside the wireless network. The laptop has an integrated Bluetooth module and uses the SIM access profile to access it.

In the implemented sensor architecture, the SIM is used for security critical services in security mode 3 with a 32-digits pass-key.

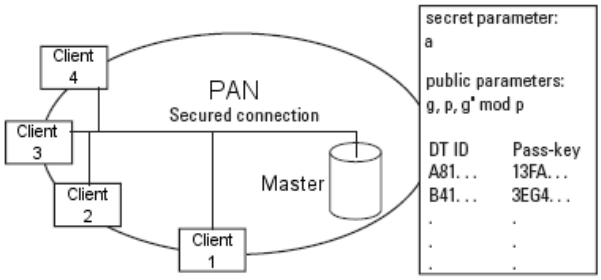

Figure 4: PAN Secured interconnection system

In the FPGA ROM, a 128-bits encryption key has been implemented for a major security level. To avoid the typing of the 32 digits pass-key by the user, in this system the pass-key value is generated by the server and displayed to the user. The security required by the SIM access profile gives the necessary protection for the message exchange between the client and the server. However, to avoid security holes in the master SIM access server implementation, additional security measures has been developed in the implemented architecture.

One problem is that in an implementation that just follows the specification, all the messages from the client to the server have to be accepted and forwarded to the SIM[13]. This is a potential security risk for the sensitive functions in the subscription module, available for the remote device. This device might have been compromised in some way or it might have been infected by a virus or other harmful software. For this reason, the access to the subscription module by the server has to be restricted.

This can be achieved if, at the security pairing, the server selects the set of services in the SIM that the client should be allowed to access[13]. Then the record of allowed services has to be stored in a special and protected access control database. When the client has been authenticated against the server, a filtering process or a security filter has to check all messages from the client to the subscription module, as is illustrated in Fig.5.

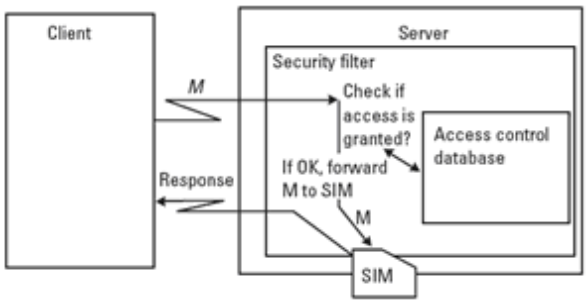

Figure 5: SIM client – server access control

The filter makes sure that only messages allowed according to the access database are forwarded to the subscription module.

5 Conclusion

In this paper a Bluetooth™ system has been designed and its performance has been evaluated in terms of security. The implemented solution works satisfactorily reducing the number of components and thereby power consumption allowing longer battery lifetime or smaller size batteries. In this way, miniaturized applications can be realized. For future developments, the ZigBee™ standard will be considered to optimize the power consumption performance of the remote monitoring system.

To increase the network security level, a SIM solution is implemented in security mode 3 with 32 digits pass-key. The security required by the SIM access profile gives the necessary protection for the message exchange between the client and the server.

References:

[1] Brooks, T, "Wireless technology for industrial sensor and control networks" *Sensor for Industry, 2001, Proceedings of the First ISMEEE Conference*, Page(s):73 -77,2001.

[2] Rauchhaupt, L.; "System and Device Architecture of a Radio Based Fieldbus -*The Rfieldbus System" IEEE International Workshop on Factory Coomunication systems*. Page@): 185-192, Aug 2002.

[3] G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors", *Commun. ACV*, vol43, pp. 51.58, no 5 May 2000.

[4] R. S. H. Istepanian, "Modeling of GSM-based mobile telemedical system," in *Proc. 20th Annu. IEEE/EMBS Conf.*, vol. 20, Hong Kong, 1998, pp. 1166–1169.

[5] Kansal, A.; Desai, U.B.; "Bluetooth primer". Internet document,http://www.ee.ucla.edu/kansal/bt_primer.pdf Page: 4, 2002.

[6] Baatz, S.; Frank, M.; Gopffarth, R.; Kassatkine, D.; Martini, P.; Schetelig, M.; Vilavaara, A.; "Handoff support for mobility with IP over Bluetooth" Local Computer Networks, 2000. LCN 2000. *Proceedings. 25th Annual IEEE Conference on*, Page(s): 143 -154, 2000.

[7] BluetoothTM SIG; "Specification of the BluetoothTM System Core 1.11'' http://www.bluetooth.com, Vol: 1 , Page: 65,2001.

[8] J. S. Park and D. Dicoi, "WLAN security: Current and future," *IEEE Internet Comput.*, vol. 7, no. 5, pp. 60–65, Sep./Oct. 2003.

[9] J. Andreasson, J. G. Castaño, M. Lindén, Y. Bäcklund, "Remote System for Patient Monitoring Using Bluetooth™". *Proc. 2nd International Symposium on Telemedicine*, Gothenburg, Sweden, 2002.

[10] J. Andreasson, M. Ekstrom, A. Fard, J. G. Castano, T. Johnson, "Remote system for patient monitoring using Bluetooth". *Prec. 1st IEEE int. conf. On Sensors, Orlando*, USA, 2002 pp 304-307. e

[11] J. G. Castaño, J. Lönnblad, M. Svensson, A. G. Castaño, M. Ekström and Y. Bäcklund, " Steps Towards a Minimal Mobile Wireless Bluetooth™ Sensor". *Proc. 2004 Sicon, New Orleans*, USA, 2004 pp 79-84.

[12] Internet document www.panasonic-eutc.com/ products/daten/pdf/Web_PAN1540-C.pdf

[13] 3rd Generation Partnership Programme, 3GPP TS 11.11, S*pecification of the Subscriber Identity Module Mobile Equipment (SIM-ME) Interface*, Version 8.10.0, September 2003.

[14] D. A. Bonnett, "Design for in-system programming," in *Proc. Int. Test Conf., Atlantic City, NJ*, 1999, pp. 252–259.

[15] M. Winters, "Using IEEE-1149.1 for in-circuit emulation," in *WESCON/94 Idea /Microelectronics Conf. Rec.*, 1994, pp. 525–528.

[16] J. Andrews, "An embedded JTAG, system test architecture," in *Proc. Electro/94 Int. Conf., Boston, MA*, 1994, pp. 691–695.

[17] M. Bogdan, H. Sanders, M. Shochet, and A. Amadon, "Dual method of configuring Altera 10 K family PLDs," in *Proc. 11th IEEE NPSS Real Time Conf., Santa Fe*, NM, 1999, pp. 312–314.

[18] "Using the Jam Language for ISP & ICR via an Embedded Processor," *Altera Corp., San Jose, CA, Altera Application* Note 88, Version 3.01, Nov. 1998.