

# Securing Wireless Bluetooth Sensor Systems

<sup>1</sup>Prof. Anand Nayyar

**Abstract**— In this research paper a Low power, Portable and Secure Wireless Bluetooth Sensor System has been designed and its performance has been evaluated. The sensor system is light weight and has interoperability with Personal Area Network (PAN) and the architecture has been implemented by adopting an FPGA and a Bluetooth Module. The analysis of design shows its capability of continuous transmission of analog signals and a high rate of security level. As low sampling rates, the adopted solution offers low power consumption and lower battery capacity can be adopted and sensor weight can be minimized. With higher sampling rates, the Wireless Sensor System is equipped with FGMA which offers best architecture solution and high performance. So Wireless Bluetooth Sensor system can be widely adopted in critical applications like Detecting Vital Signs in Patients having serious pathologies.

**Index Terms**— Bluetooth, Wireless sensor systems, Wireless Technology, Security, IEEE 802.15.1

## I. INTRODUCTION

Bluetooth, A technology which requires no introduction and is being used constantly in Mobile Phones, Computers, Tablet PC'S, TV'S, Gaming Consoles and much more for transferring the data from one device to another. Bluetooth Wireless technology is becoming very popular to replace existing short range wired technology with short-range Wireless technology to enable new types of applications.

With the increase in use of Bluetooth Technology, Various Researches and Manufactures are closely working to use this technology in completely different environments such as in Medical sector to improve the life quality and to reduce the cost incurred by hospitals in treating patients.

A new concept called PAN (Personal Area Network) is evolving along with Bluetooth Technology. A PAN consists of a limited number of units interconnected to form a network and to exchange information among the connected nodes. Bluetooth acts a local connection interface between different personal units like Mobile Phones, PDA's, Keyboard, Mouse, Gaming Consoles and much more. Bluetooth is a true enabling technology for the PAN Vision. The units are typically consumer devices which are used by different manufactures in different ways. So in order to have better interoperability between the personal devices, the security level has to be set up by the user. The Bluetooth technology has been designed in such a intelligent manner which enables even a ordinary user to maintain a good security level to protect the data and communication links in operation.

With the help of PAN Technology, users can access their data wirelessly between different devices, work on them and store

them in an Information System or in Electronic Personal Record.

Wireless Systems implementation has been done by taking into account the following important key points:-

1. Using Wireless devices everywhere and avoiding the location lockdown
2. Interoperability with other technologies for Communications.
3. Enough security to prevent eavesdropping and intrusion avoidance.
4. System high level interface immunity.

But if we implement any technology we have certain expectations. Same is the case with Bluetooth Technology. The following are the desired expectations from the Bluetooth Technology:-

1. Confidentiality Protection.
2. Only authenticated devices should communicate in the Bluetooth Network.
3. Easy to use as well as High Speed Data Connectivity.
4. Proper Security Measures to avoid Malicious Activity and DoS Attacks.

In this Research Paper, A Sensor System Architecture is presented along with its benefits. As well as the Bluetooth technology security is also analysed and solution is proposed.

## II. BLUETOOTH STANDARD

Bluetooth is a proprietary open wireless standard which was created by Telecoms vendor Ericsson in 1994 for exchanging data over short distances using short wavelength radio transmissions from fixed and mobile devices creating Personal Area Networks (PANs) with higher degree of security. Basically Bluetooth standard was designed to replace RS-232 data cables. Bluetooth is regarded as developing network technology which is able to support data and voice communications and is characterized by low complexity, robustness and low power cum cost.

Bluetooth uses a Radio Technology called FHSS (Frequency Hopping Spread Spectrum) which chops up the data being sent and transmits the chunks of data on 79 bands (1 MHz each) in the range of 2402-2480 MHz. This range is in the globally, unlicensed Industrial, Scientific and Medical (ISM) 4.4 GHz short-range radio frequency band.

Bluetooth has the ability to form PANs and is regarded as Packet-Based Protocol with a Master-Slave structure. One master can communicate with up to 7 slaves in a piconet; all the devices share the master's clock. 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 using TDM (Time Division Multiplexing) Technique in which the time is divided into 625  $\mu$ s intervals called slots. The transmission between master and slave starts in even the numbered slots while the slave to master transmission starts in odd numbered slots. Master and slaves are allowed to transmit the packets in 1, 3,5 consecutive slots. Forward Error Correction (FEC), Cyclic

Manuscript received Mar 10, 2011.

Prof. Anand Nayyar, P.G. Department of Computer Science,  
Kamla Lohtia Sanatam Dharam College, Ludhiana,  
(e-mail : anand\_nayyar@yahoo.co.in)

Redundancy Check (CRC), Header Error Check (HEC) and Automatic Repeat Request (ARQ) are the techniques which provide data protection against imperfect channels. The Packet Exchange is based on the basic clock, defined by the master, which ticks at 312.5  $\mu$ s intervals. Two clock ticks make up a slot of 625  $\mu$ s; two slots make up a slot pair of 1250  $\mu$ s. 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 to 2.480 GHz.

The Bluetooth Technology provides high security mechanisms including a globally unique six byte Bluetooth Device Address (BDA), authentication, authorization, encryption and PIN exchange at user level. In general, Bluetooth Security is divided into three modes: (a) Non-Secure; (b) Service level enforced security (c) Link level enforced security. In non-secure, a Bluetooth device doesn't initiate any secure measures. In service-level enforced security mode, "two Bluetooth devices can establish a non secure Asynchronous Connection-Less (ACL) Link. In the link level enforced security, the Bluetooth device initiates security procedures before the channel is established.

### III. BLUETOOTH SENSOR ARCHITECTURE

The Bluetooth Sensor Architecture consists of seven client modules and one master module for System Control. The main component of Bluetooth Architecture is FPGA which is shown in diagram 1. FPGA allows the device to be programmed, debugged and reconfigured after it is soldered onto a printed circuit board which reduces the possibility of lead damage and electrostatic discharge exposures.

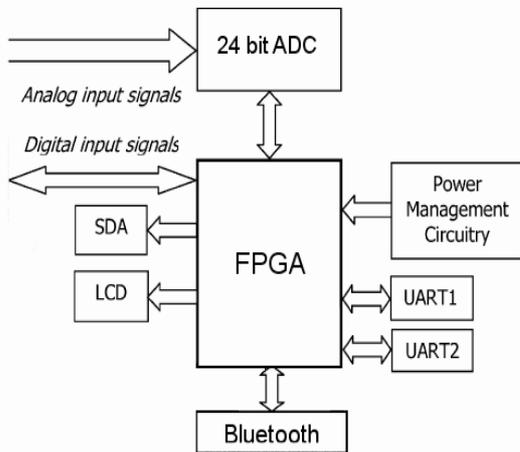


Figure.1 FPGA-The Main Component of Module

In this research paper, signals are generated by biomedical sensors for monitoring critical parameters such as Vital signs in patients. It has been realized in Wireless Sensor Architecture using one Analog/Digital Converter (ADC) and two processors sharing the Bluetooth stack. A 24-bit multiplex sigma-delta converter converts the analogue input signal with 0-5V 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 (PAN 1540). 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 constructs 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 as shown in Diagram 2.

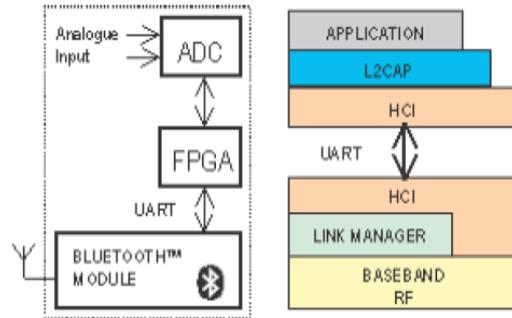


Figure.2 FPGA Control Management

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.

PAN1540 has three general purpose analog interface pins; 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.

### IV. BLUETOOTH SECURITY SENSOR SYSTEM NETWORKING

It is very difficult to find the correct level of security when a new communication technology evolves. It is also very difficult in the case of Bluetooth. In order to offer interoperability and to provide support for a specific application, it has developed a set of profiles. A profile is an unambiguous description of communication interface between two units for one particular service.

As the main purpose behind the development of Bluetooth technology is to replace short range cables. Pure cable

replacement is done through RS232 emulation which is offered by serial port profile. Several other profiles like PAN (Personal Area Network) and LPP (Local Positioning Profile) make use of serial port profile.

This section primarily discusses the security issues and solutions for remote access to SIM (Subscription Identity Module) over Bluetooth connection. A SIM card is regarded as an Integrated Circuit used in GSM Mobile Telephony to store subscriber information. In this research paper a SIM Solution is implemented inside the FPGA ROM memory. Altera QuartusII v5.1 software generates FPGA configuration data file which is stored in FLAH ROM of processor and memory module.

This SIM information is used to connect a remote sensor to a master network in a secured manner (Laptop, Smartphone, PDA Device or Tablet Device) which makes it possible for mobile network operator to identify the subscribers using the network as well as it also allows the operator to enable the connect of mobile network services. The Bluetooth SIM Access Profile defines protocols and procedures for the access to a remote SIM over Bluetooth Serial Port (RFCOMM) Connection. The SIM Access Profile Communication Stack is defined in Diagram 3. The SIM access messages consist of a header and 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

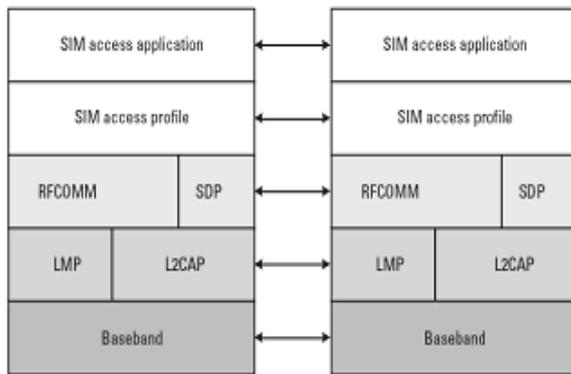


Figure.3 Sim Access Profile Communication Stack

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 defined in Diagram 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.

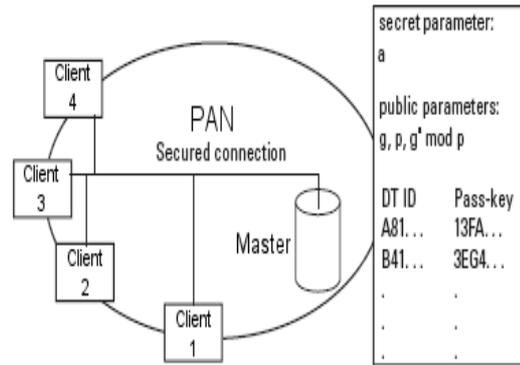


Figure.4 Pan Secured Interconnection System

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. 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. 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 Diagram 5

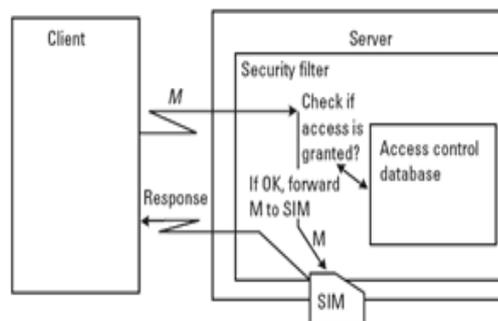


Figure.5 Sim Client- Server Access Control

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

## V. CONCLUSION

In this research paper Bluetooth System has been designed and its performance has been evaluated on security parameters. The solution proposed will reduce the number of components and also the power consumption allowing longer battery lifetime. But of Future development, the ZIGBEE standard will be considered to optimize the power consumption performance of the remote monitoring system. In order to increase the level of network security, A SIM solution is proposed in security mode 3 with 32 digits pass-key. The security required by SIM Access Profile gives the necessary protection for message exchange between client and 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" Internetdocument, [http://www.ee.ucla.edu/kansal/bt\\_primer.pdf](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.Proceedings. 25th Annual IEEE Conference on, Page(s): 143 -154, 2000.
- [7] Bluetooth TM 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. 1 IEEE int. conf on Sensors, Orlando, USA, 2002 pp 304-307
- [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](http://www.panasonic-eutc.com/products/daten/pdf/Web_PAN1540-C.pdf)
- [13] 3rd Generation Partnership Programme, 3GPP TS 11.11, Specification 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.

## BIOGRAPHY



**Prof. Anand Nayyar** (B.Com, M.C.A, M.Phil, M.Tech) currently working as Assistant Professor in P.G. Department of Computer Science in Kamla Lohtia Sanatam Dharam College (KLSD College), Ludhiana. The Author possess many International Credentials like A+,CCNA, MCSE, MCTS, MCITP, RHCE, OCP, CEH, MCS.D.net to name a few. The author has published AROUND 35 research papers in National and 8 research papers in International Conferences and published 6 books on topics like Networking, Database, Data Structures and Information Technology Fundamentals. His areas of interest include Networking, Distributed Systems, Linux & Open Source Technology, Database Management Systems, Software Engineering and Testing, Computer Graphics, Information Systems and Digital Image Processing.

The Author is permanent member of research organizations like IAENG (International Association of Engineers), IACSIT (International Association of Computer Science and Information Technology).