Personnel Security System using Bluetooth Low Energy (BLE) Tag

K.Gautham[*1], G.Raghav[#2], V.Krishnamurthy[*3], N.R.Raajan[#4]
[*1, #2, #4]Department of ECE, SEEE, SAST1RA University
Thanjavur, Tamil Nadu, India
[*3] Director, EI Labs India Pvt Ltd,
Bangalore, Karnataka, India
krishna@eilabs.co.in,
nrraajan@ece.sastra.edu,
gauthamkannan99@gmail.com,
raghavsarath@gmail.com.

***Abstract*— One of the primary aspects of Personal security is through various user authentication techniques like biometrics, password, Smart Card, etc. We propose to design a personal security authentication system using the commonly available Bluetooth technology. The authentication is done on a fixed device, connected to the web and the identity is provided by a mobile device commonly carried by the person. Almost every cell phone has Bluetooth® transceiver for connecting to a wireless headset or to a host PC. Many new cars have Bluetooth to let you talk hands free while driving. Bluetooth has thus emerged as a pervasive technology.**

***The* aim of the paper is to describe a Personnel Security System using Bluetooth Low Energy (BLE) Tag which operates on a coin cell battery that will discover all the available low energy devices in the vicinity and keep track of when it entered and when it left the zone. In addition, this tag can also be used as a positioning device by measuring the Received Signal Strength (RSSI) value. The initial phase is aimed at designing the hardware for the tag. The second phase is initiated towards programming the tag. The final phase is targeted towards testing the designed hardware module and developing a Personnel Security System.**

Keywords **– *BLE, RSSI, ISM, PAN, BD_ADDR, GAP, GATT, ATT, SMP, L2CAP, OSAL, PSAP.***

I. INTRODUCTION

Bluetooth is a Wireless Technology standardised as IEEE 802.15.1 which operates in the ISM (Industrial, Scientific & Medical) band. It operates in the frequency range of 2400-2480 MHz from fixed and mobile devices. It creates a Personal Area Network (PAN) with high levels of security. Bluetooth is mainly used to exchange data over short distances within a certain range. The purpose of Bluetooth is to provide cable replacement between commonly used devices by using wireless radio links. Bluetooth uses Frequency Hopping Spread Spectrum (FHSS) Technique to avoid conflict with other devices. Bluetooth is a packet- based protocol with a master slave structure. One master can communicate with up to a maximum of seven slaves. This constitutes a Piconet and connection of two or more Piconets form a Scatternet. Each Bluetooth module has a unique address known as Bluetooth Device Address (BD_ADDR). The MAC address is 48 bits of length. Classic Bluetooth has various versions such as v1.2, v2.0, v3.0 and v4.0.

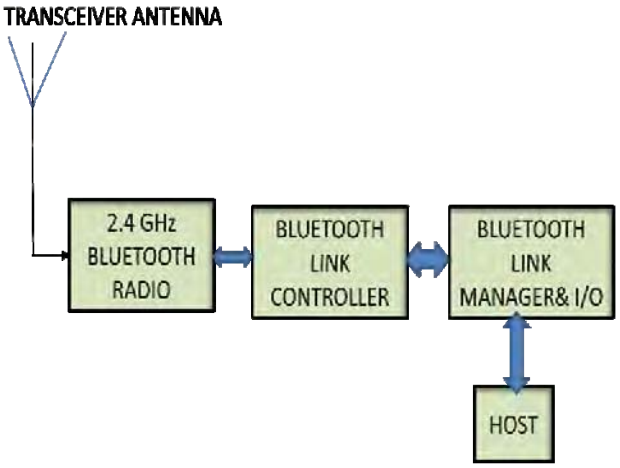

Figure 1 Block diagram of Bluetooth Wireless System

II. BLUETOOTH LOW ENERGY

As the name suggests, Bluetooth Low Energy is designed for ultra low power consumption. It is a wireless protocol standard overseen by the Bluetooth Special Interest Group (BT-SIG). It is a feature of Bluetooth v4.0 wireless radio technology. Bluetooth Low Energy operates at 2.4 GHz in the ISM band. It is aimed at new, principally low-power, low-throughput and low-latency, application for wireless devices within the discoverable range. It uses a coin cell battery (CR 2032) which works on 3volt. It has a life time of more than a year without being recharged. Bluetooth Low Energy takes less time to make a connection when compared to conventional Bluetooth. It consumes approximately 98% less power compared to classic Bluetooth. It is primarily designed for mobile phones and PC ecosystems, but can be used for other applications as well. It is expected to be found in billions of devices over the years to come [1].

BLE uses Gaussian Frequency Shift Keying (GFSK) modulation technique. It has 40 channels with a channel spacing of 2MHz in order to avoid the interference effects. BLE uses 3 fixed advertising channels (37, 38 and 39) for broadcasting and 37 adaptively frequency hopped dynamic data channels. One of the main reasons for low power consumption is that BLE minimizes times on air by employing only "3 advertising channels" to search for other devices or promote its own presence to devices that might be looking to make a connection whereas in a conventional Bluetooth Technology, it uses 32 channels for advertising.

III. HARDWARE DESIGN OF BLE TAG

The initial phase deals with designing the hardware for the BLE Tag. To start with, we have used CC2540 Bluetooth low energy system on chip manufactured by Texas Instruments, which is very small in size (6mm * 6mm) and comes in QFN (Quad Flat No Lead) package. It is a 40 pin IC which is powered by CR 2032 coin cell battery. CC2540 has an inbuilt 8051 microcontroller which provides high performance and consumes low-power. The IC provides 128/256 KB flash block in-circuit programmable non-volatile program memory for the device and 8 KB SRAM for data memory. The chip uses a 32 MHz crystal oscillator with an optional 32.768 KHz crystal oscillator when using power modes. The pins Debug Clock (DC) and Debug Data (DD) are being used to program the chip. Each CC2540 has a unique 48-bit IEEE MAC address.

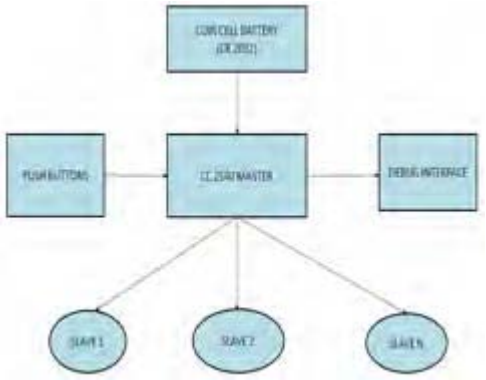

Figure 2 Architecture of BLE Tag

The RF section of the Tag consists of a BALUN (Balanced Unbalanced) Network with a chip antenna being used. The chip has both power on reset and manual reset. The tag which we have designed has a dimension of 25mm (dia) which is equal to that of a 1 rupee coin and can act both as a Master and slave depending on how it is being programmed [2].

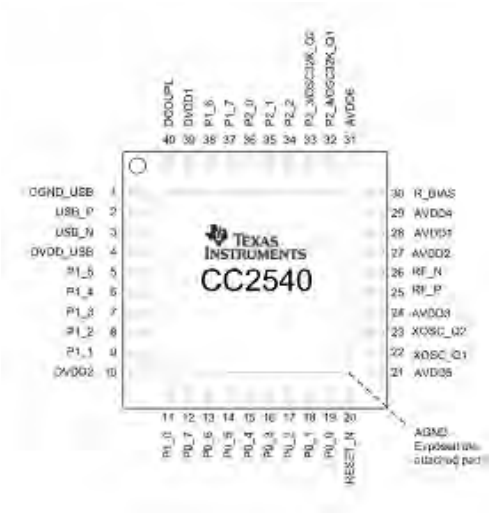

Figure 3 Pin out Information of CC2540

Conventional Bluetooth modules have Dual modes i.e. BR/EDR (Basic Rate or Enhanced data rate) whereas Bluetooth low energy modules are single mode devices which are primarily designed for ultra low power consumption. The pin out information of CC2540 is as shown in Figure 3.

IV. BLE STACK

Bluetooth Protocol Stack is the one through which the software part works. The Bluetooth Protocol Stack is shown in Figure 4.

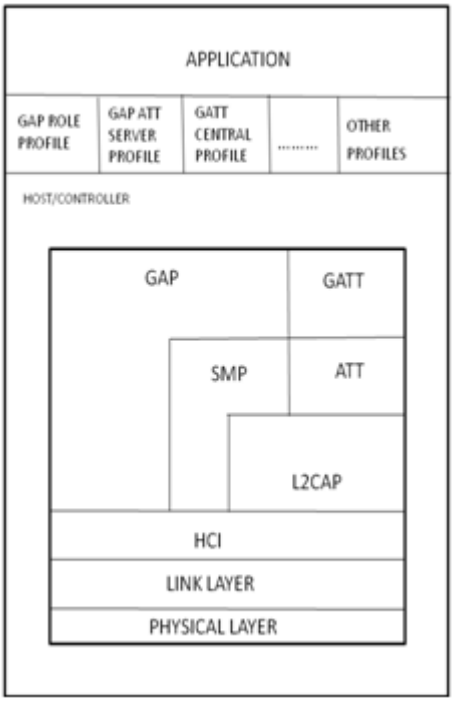

Figure 4 Bluetooth Protocol Stack

Bluetooth Protocol Stack consists of two main sections. They are Controller and Host.
Profiles and Applications sit on top of GAP and GATT layers of Host. Since BLE is a Single Device Solution, the Host, Controller, Profiles and Applications are all implemented together on the same chip.

The Link Layer in a BLE device consists of six possible states. They are Standby, Advertiser, Scanner, Initiator, Master and Slave. BLE is a Star Topology Network. The Master manages the connection and can be connected to multiple slaves, whereas the slave device can be connected to only one master. The flow chart of Link Layer is as shown in Figure 5. A device in the advertising state transmits advertising packets. Those packets contain a data payload and can be directed towards a specific scanner device or undirected.

Advertisements can be either a connectable one or a non-connectable. During one advertising event, an advertisement packet is transmitted on each of the three advertising channels (37, 38, and 39).

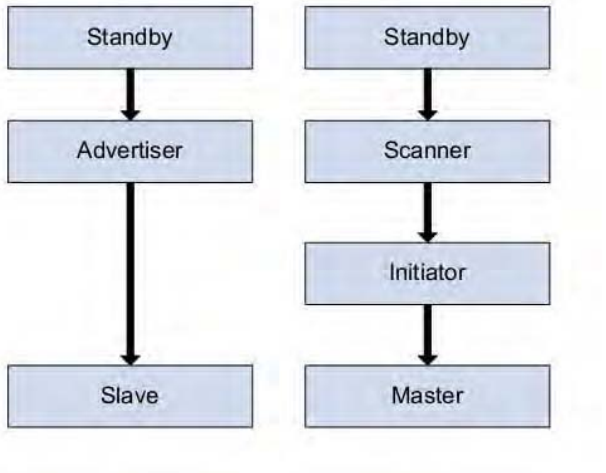

Figure 5 Flow Chart of Link Layer

In the Link Layer, there are four types of Advertisements. They are Connectable undirected, Connectable directed, Non-connectable undirected and Discoverable undirected. The scanning takes place in the Link Layer and there are two types in Scanning. They are Active and Passive Scanning. In active scanning, an advertisement packet is received in response with the "scan request" whereas in passive scanning, the advertisement packet is received without any scan request.

In the Link Layer, there are four types of Advertisements. They are Connectable undirected, Connectable directed, Non-connectable undirected and Discoverable undirected. The scanning takes place in the Link Layer and there are two types in Scanning. They are Active and Passive Scanning. In active scanning, an advertisement packet is received in response with the "scan request" whereas in passive scanning, the advertisement packet is received without any scan request.

In the Host Layer, Logical Link Control and Adaptation Protocol (L2CAP) permits upper level protocols and applications to transmit and receive upper layer data packets. It also provides channel management and connection parameter updates. Security Manager Protocol (SMP) performs authentication and key management. It uses AES128 as the encryption algorithm for security procedures. It works with GAP to manage relationship between the devices such as Pairing, Authentication and Bonding.

Generic Access Profile (GAP) defines generic procedures for connection related services such as Device Discovery, Link Establishment, Link Management, Termination and Security features. It works in one of the four profile roles: Broadcaster, Observer, Central and Peripheral. A Broadcaster is an advertiser that is non-connectable whereas an Observer scans for advertisements that cannot initiate connections.

GAP supports three different Discoverable modes as follows. In Non-Discoverable modes, there are no advertisements. In Limited Discoverable mode, the device advertises for a limited amount of time before returning to standby state. The mode in which the device advertises continuously is General Discovery mode. GAP uses the HCI to communicate with the controller to turn advertising On/Off.

Attribute Protocol (ATT) is a discrete value that has the following three properties.

1. A Handle(address)
2. A Type
3. A set of permissions.

ATT defines the Over-the-Air protocol for reading, writing and discovering. ATT has a Client-Server Architecture as shown in Figure 6

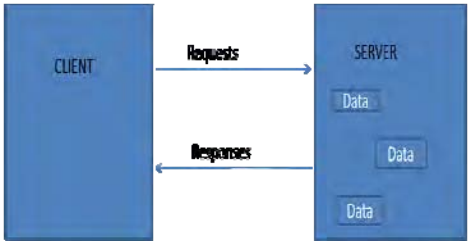

Figure 6 Client-Server Architecture

Generic Attribute Profile (GATT) is designed for use by the application or a profile so that an attribute client can communicate with attribute server. It defines the procedures for configuring the broadcast of attributes and also for using the attribute protocol to discover, read and write. Same Client-Server architecture as ATT except that the data is encapsulated in "Services" and data is exposed in "Characteristics".

A sample advertisement packet and scan response data are shown in Figure 7.a and 7.b.

0X0A LENGTH	0X06 NAME	0X50 'B'	0X72 'L'	0X64 'E'	0X78 'T'	0X79 'A'	0X76 'G'

Figure 7.a Advertisement Packet

0X02 (2)	0X01 FLAGS	0X02 GEN.DIS

Figure 7.b Scan Response data

Bluetooth Low Energy CC2540 Embedded software contains five different sections for the application as follows.

1. Operating System Abstraction Layer (OSAL) - It is not an actual Operating System, rather a control loop that allows software to set up execution of events. Each subsystem of the software runs as an OSAL task and has a unique task identifier (ID). Each task has two functions: Initialization and Event Handler. 2. Hardware Abstraction Layer (HAL) - It provides an application Programming interface to the hardware related functions such as ADC, UART, SPI, etc. 3. BLE Tag Application- This application provides a demonstration of simple wireless Bluetooth low energy. It can be used as a Broadcaster as well as an Observer. 4. BLE Stack- It is based on the approved Bluetooth core specification version 4.0. 5. Profiles- GAP Roles and GATT Services are the profiles [4].

V. **WORKING OF BLE TAG**

This is the final phase which describes about the working of BLE Tag. Initially, the program is compiled and executed with the IAR EMBEDDED WORKBENCH for 8051. The hex code is generated after the successful compilation of the program. This code is flashed to the chip using Smart RF Flash Programmer through the Debugger. Here, the primary address of the CC2540 chip can be rewritten with the secondary MAC address. Now, BTOOL which is the Bluetooth Low Energy PC Application is used to scan for advertisement packets broadcasted by the nearby BLE devices. A Baud Rate of 57600 is being used.

Figure 8 Flow Chart of BLE TAG

Once if the battery is being inserted in the BLE Tag, the tag starts to advertise its MAC address. The host BLE tag scans for any nearby advertisements once when the SCAN button in the BTOOL is being pressed. If any devices in the vicinity are found, then the address of those devices gets displayed in the BTOOL. This is the working of BLE Tag.

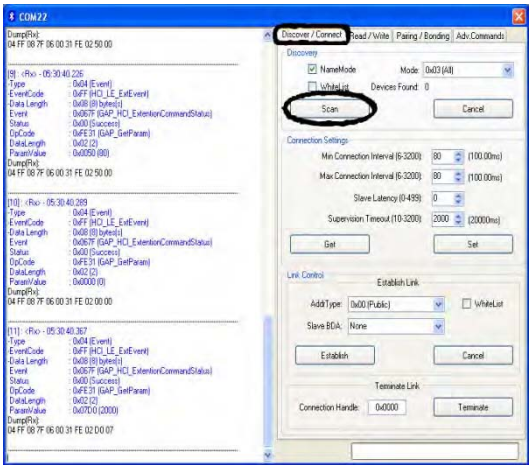

Figure 9.a Device Scan in BTOOL

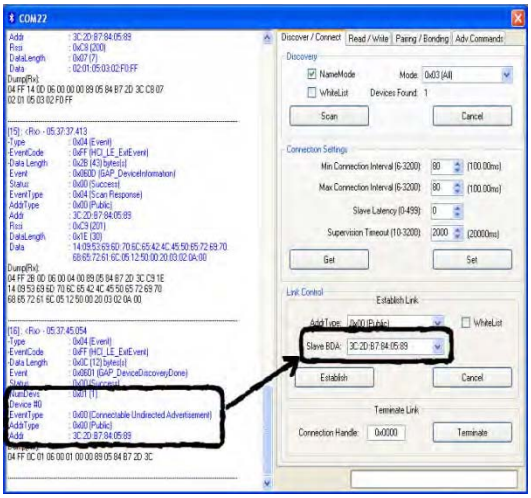

Figure 9.b Address of Discovered Devices

Also, BLE Tag can be used as a Positioning Device by measuring the Received Signal Strength (RSSI) value. This can be done by making use of Smart RF Packet Sniffer which measures the RSSI value through the Least Square Estimation. The RSSI value decreases as the distance between the host and client decreases i.e. RSSI value is directly proportional to the distance. The Received signal strength values are as shown in the Figure 10.

Figure 10 Received signal strength indicator table

The arrow in the table indicates the different RSSI values measured from the tag.

VI. APPLICATION OF BLUETOOTH LOW ENERGY (BLE) TAG FOR PERSONNEL SECURITY SYSTEM

BLE Tag has a number of end applications. Due to its small and compact size, it can be used in defence and security fields. There are various user authentication techniques like biometrics, password, smart card, etc which are used to achieve Personal Security. Personal Security can be achieved with the help of Bluetooth Low Energy Tag. In this application, the BLE Tag is being embedded inside the lock of a door. The authentication is provided in such a way that the door will open only in the presence of the mechanical key plus a Bluetooth identity verification. The Bluetooth low energy electronics being embedded in the lock will scan for all the BT devices in the vicinity, display their corresponding MAC Id and keep track of when it entered and when it left the zone.

The authentication is being provided either by the BLE tag or the BLE supported phone which the user carries. In case of BLE Tag, the MAC Id of the Tag possessed by the user is being scanned by the Bluetooth electronics embedded inside the door. In the case of the mobile phone which the user carries, an app needs to be installed through which an higher level authentication such as the Password entry will provide the security. The app installed in the mobile can be either an ios or an android app.

Nowadays, the security is being provided by means of RFID cards which requires a proprietary card reader whereas in the case of Bluetooth low Energy Tag, the Tag will itself act as a card reader

and there is no external card reader required. However, further developments need to be made for the efficient working of the tag in the years to come.

Besides this the Tag can be used in

- Health & Fitness
- Medical Applications
- Educational tools
- Remote Controls
- Proximity and Indoor locationing
-

Figure 11 Electro Mechanical Lock Systems

VII. BLE VS. NFC (RADIO FREQUENCY IDENTIFICATION)

One of the primary differences between BLE and RFID is that RFID technology needs a proprietary Card Reader for sensing the RFID Tag. Without an external Card reader, RFID Tags cannot be detected whereas in Bluetooth Low Energy, the BLE device itself acts as a card reader and there is no external card reader needed. Bluetooth low Energy has WPAN (Wireless Personal Area Network) whereas NFC follows Point-to-Point communication. Encryption of data is possible in BLE, but not in NFC. NFC can cover a distance of up to 0.2 meters whereas BLE has a range of 50 meters. The frequency being used by BLE is 2.4GHz whereas in the case of NFC, it is 13.56MHz. The amount of time BLE takes to set up a connection is less than 0.003 seconds whereas NFC takes 0.1 seconds. Last but not the least, as the name stands, BLE is mainly designed for Ultra Low Power (ULP) consumption whereas NFC consumes more power when compared to BLE.

VIII. CONCLUSION

From the observations, it remains identified that the Tag can be used as a Personnel Security System which operates on a coin cell battery that has Ultra Low power consumption and can discovery all the Bluetooth devices in the vicinity and keep track of when it entered and when it left the zone. By measuring the Received Signal Strength (RSSI), this tag can be used as a Positioning device as well. Besides this, the Tag can be used for many other applications.

IX. REFERENCES

[1] Diane McMichael Gilster, *"Bluetooth EndtoEnd"*, Wiley Publication.
[2] *CC2540/41 System-on-Chip Solution for 2.4GHz Bluetooth low energy Applications*—User's Guide
[3] *CC2540F128/256 Datasheet*
[4] *Texas Instruments CC2540 BLE Software Developer's Guide*, version 1.0

ACKNOWLEDGMENT

We include our special thanks to all the researchers working in field of Low Power RF and Wireless Systems who in some way helped us to attain our goal. Also, we wish to express our gratefulness to the faculties in our university and the staff members in our company who shared their views and gave suggestions to make our project a great success.