ISSN XXXX XXXX © 2017 IJESC

Research Article Volume 7 Issue No.6

Device Based User Authentication in Wireless Network

Vidyadheesh Pandurangi[1], Dr. Vijay Mishra[2], Dr.Manjula Shenoy .K[3]
M.Tech(Software Engineering)[1], Chief Technology Officer[2], Professor[3]
Department of Information & Communication Technology
Center for NanoScience & Engineering IISc, Karnataka, India[2]
Manipal Institute of Technology, Manipal, Karnataka, India[1, 3]

Abstract:
Wireless networks are very often vulnerable to various threats from different unintended users. Authentication of the user is very challenging task in such a network medium. It is very much essential to authenticate the user. The usage of smart devices has increased in recent times. The Bluetooth technology in smart phones could be used for the authentication purposes. Bluetooth is a technology used for short distance communication and exchange of information. LMX9838 is one such Bluetooth serial port module which is fully integrated with Bluetooth 2.0 baseband controller. This serial port module can be used as Bluetooth node to authenticate the users in order to provide access to the system. The pairing of the Bluetooth device is helpful in the authentication procedure. The LMX 9838 serial port device acts as master node and searches for the slave nodes which request for the pairing. This master node acts as the authenticating the user in the wireless medium. And suitable messages are displayed on successful pairing of the devices. Even thou this master node could pair with 7 other Bluetooth devices simultaneously; it will only pair with those devices with which it is defined to pair. This could be one of the ways to authenticate the users in wireless medium.

Keywords: Authentication, Bluetooth 2.0, LMX9838 serial port device, Master node, Smart devices.

I. INTRODUCTION

The advancement in the field of Internet has led the growth rate of internet users to a very high level. On the other hand the advancement in the field of smart and portable devices has increased the rate of internet users as well. The usage of smart devices has changed the way of life. The various business transactions, confidential data exchanges take place over an insecure channel on the internet. To secure these activities, authentication of the users and network plays an important role. The user authentication mechanism that allows only legitimate users to access the network data becomes critical for maintaining the confidentiality and integrity of the network information. Bluetooth technology is widely used by many organization and individuals for various purposes. The Bluetooth technology is not only used in the personal area devices like smart phones, other intelligent systems but also helpful and a recommended as a standard communication protocol in Internet of things [6]. Authentication of the intended user is the challenging issue in the present days. The communication using network is vulnerable for the outside attackers. As it is a wireless medium, intruders are bound to attack and break the communication or to get access. The Bluetooth can be used for the individual device identification to uniquely identify the users. It can range up to 10 meters which can be a factor for the authentication purpose.

II. BACKGROUND

Access control in the field of either physical security of information security is a selective restriction of access to a place or resource. The percentage of population using smart mobile devices is increasing at a rapid rate [1]. This has opened up opportunity of associating a device identity with an individual and using this device identity as an alternate identity that may be used in secured premises for restricted users' entry or the places valid only for registered/authorized users [2]. As Bluetooth is a wireless technology for exchanging the data over short distances it could be helpful to use it as a parameter for authentication of the user. The uniqueness of the individual Bluetooth device (ie each device will be having its own ID) helps in identifying the particular device. A master node and a slave node needs to decided properly in order to communicate. The master node of Bluetooth will be scanning for the slave Bluetooth devices for identifying and get connected for communication. Once the master node finds a desired slave node it gets connected for the communication after the process authentication. The uninterrupted scanning of the device informs that the Bluetooth is within the range of communication and helps to be an authenticated user. The Bluetooth device could be uniquely identified with the MAC address of the device provided it should be in the range of Bluetooth. The main objective of LMX9838 Bluetooth serial transceiver is that it is capable of operating in command (Master) mode. This means that other devices cannot act or change the behavior of the Bluetooth module. This is done by changing the default pin configuration of the module which means no device pair without the pin. Even though if anyone can pair it with by the means of brute force it is impossible to crack the MAC address of the mobile which is hardcoded in the hardware and cannot be changed at all.

III. METHODOLOGY

LMX9838

The Texas Instruments LMX9838 Bluetooth Serial Port module [3] is a fully integrated Bluetooth 2.0 baseband controller, 2.4 GHz radio, crystal, antenna, LDO and discrets combined to form a complete small form factor (10 mm x17 mm x 2.0 mm) Bluetooth node. All hardware and firmware is included to provide a complete solution from antenna through the complete lower and upper layers of the Bluetooth stack, up

to the application including the Generic Access Profile (GAP), the Service Discovery Application Profile (SDAP), and the Serial Port Profile (SPP). The LMX9838 is prequalified as a Bluetooth subsystem. The module offers an automatic slave mode without any configuration necessary from an external host. Additionally it offers a command set for hardware configuration and full Bluetooth operation over SPP. The LMX9838 is intended to be an add-on module to an existing microcontroller. In this function it either appears as cable like interface for the UART or can also be controlled with a simple application on the external microcontroller to establish links itself. The LMX9838 offers Bluetooth operation up to the Serial Port Profile (SPP), which is the basis for many other profiles like DUN or Headset. In case such profiles shall be

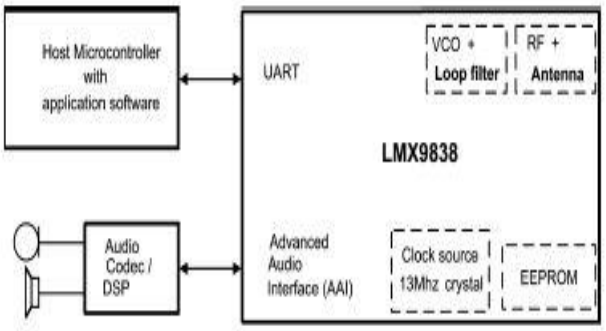

Figure.1. LMX9838 Main Interface Blocks

Supported by the end product, the additional profile needs to be implemented on the host application, which uses the LMX9838 as kind of "SPP gateway".

The LMX9838 includes the complete Bluetooth stack including the following protocol layers:

- Link Controller
- Link Manager
- L2CAP (Logic Link Control and Adaptation)
- RFCOMM
- SDP (Service Discovery Protocol)

An on-chip application together with those protocol layers offers the following profiles:

- GAP (Generic Application Profile)
- SDAP (Service Discovery Application Profile)
- SPP (Serial Port Profile)

The application manages all profile related interactions to the stack but also offers a simplified command interface over the UART. The interface is used for configuring the device, setting up the link and receiving events from the module.

UART Communication

The main communication interface between the LMX9838 and the host is the UART Interface [3]. The UART interface between host and LMX9838 needs to be connected in Null Modem configuration, meaning RTS/CTS and TX/RX are crossed.

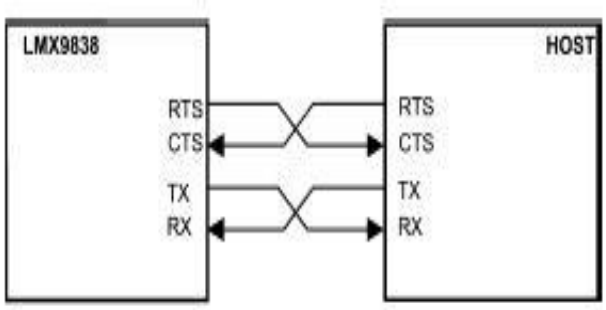

Figure.2.UART Null Modem Connection

The LMX9838 uses the RTS lines to indicate low buffers and reacts on the CTS from the host, immediately stopping sending packages to the host.

The UART interface consists of four signals:

- TX: Transmit output
- RX: Receive input
- RTS: Ready-to-Send output, indicating the host "I am ready to receive data"
- CTS: Clear-to-Send input, allows the host to stop the transmission from the LMX9838 to the host.

The LMX9838 will ALWAYS use the RTS to indicate to the host, that it is ready to receive data and it will ALWAYS sample the CTS input to check, if the host is able to receive data. Therefore, it has to be made sure that the CTS pin is pulled low in case the host is ready. Otherwise the LMX9838 will not start sending out data or events. The handshake functionality is based on the RTS / CTS signaling, which is used in both Command Mode and Transparent Mode. The LMX9838 indicates with its RTS signal (RTS=low), that it is able to receive data and will raise it high in case the TX buffers are full. In case, the LMX9838 is not connected to any other device and gets an incoming link request, it will:

- ask for authentication or pin code exchange
- accept the link
- notify the application by an indicator
- change state to "Single Slave"

Single Slave

The Bluetooth specification defines a Bluetooth slave as the device which is connected by another device and adjusting to the timing of that device (Master). The slave synchronizes to the clock of Master and to its hopping sequence.

The LMX9838 can be assumed to be in Single Slave after one of the following actions appeared:

- The LMX9838 accepted an incoming link and reports it by the "SPP Link Established Indicator" while the Automatic Operation flag is set to 0x00 (Non-automatic).
- The host sends a UART Break to a LMX9838 in "Transparent Slave".

Setting the Link with command Interface

Setting up a Bluetooth link between devices requires that the devices know specific parameters of each other. The first command "Inquiry" is to search for the Bluetooth devices in the range and gets the BD_Addr – Bluetooth Device address.

A) The Inquiry Command - 02 52 00 03 00 55 0A 00 00 03

- The **start delimiter** is always 0x02.
- The **packet type id** for a request is 0x52.
- The **opcode** for Inquiry is 00
- The **payload length** indicates the length of the payload after the checksum. - 0A 00 00
- The **checksum** is calculated as sum of packet type id, opcode and packet length, 0x52 + 0x00 + 0x03 + 0x00 = 0x55

B) The Device Found Indicator:
The first response to the inquiry command from the LMX9838 is the Device_Found_Indicator. In hex: 02 69 01 09 00 73 46 95 28 D9 0A 00 04 02 52 03

The **Payload:** 46 95 28 D9 0A 00 04 02 52

- BD_Addr - 46 95 28 D9 0A 00
- Class of Device - 04 02 52

C) The Inquiry Confirm
Every command on the LMX9838 command interface is confirmed by an appropriate event. The confirmation always has the opcode as the command sent to the device.

The confirmation in hex: 02 43 00 01 00 44 00 03

Package header:

- Start delimiter - 0x02
- Packet type - confirm: 0x43
- Opcode - 0x00 (confirmation, same as command)
- Payload length - 0x0001 (byte swapped in the package)
- Checksum - 0x43 + 0x01 + 0x00 + 0x00 = 0x44

The payload of a confirmation consists at least of the status byte. In this case 0x00.

SDAP

a) Create SDAP connection :
To create a SPP connection to another device, the local RFComm channel [3] has to know which remote FComm Channel to address. Each service is registered to a specific RFComm channel number. To get this number the local device has to do a Service Request on the remote device and get the service entry. The first command necessary for this is the "Create SDAP Connection". This command establishes a SDP based connection to the other device.

TABLE .I. LOG OF CREATE SDAP COMMAND

Direction	What	HEX Code
TX	Request	02,52,32,06,00,8A,46,95,28,D9,0A,00,03
RX	CFM	02,43,32,01,00,76,00,03

Interpretation by Simply Blue Commander

- TX Cmd: SDAP Connect BdAddr :469528D90A00
- RX Event :SDAP Connect status :00

The only parameter of the command is the BD_Addr to connect to: 46 95 28 D9 0A 00 (byte swapped) .
The command is confirmed by the LMX9838 with the appropriate confirmation event. If status is 0x00 the link has been established.

b) SDAP Service Browse for SPP
After the SDAP connection is established, the service request can be sent. To search for a remote SPP entry, UUID 1101 can be used. As any multi-byte parameter the UUID has to be sent byte swapped to the LMX9838 within the command.

TABLE.II. LOG OF SDAP BROWSE FOR SPP

Direction	What	HEX Code
TX	Request	02,52,35,02,00,89,01,11,03
RX	CFM	02,43,35,0D,00,85,00,01,02,10,01,11,04,0543,4F,4D,31,00,03

Interpretation by Simply Blue Commander

- TX Cmd: Service Browse, Browse Group ID: 0111
- Rx: Event: Service Browse, Status: 00, Browse Group ID: 0210, Service ID: 0111, PortNo: 04, Service Name: COM1.

The full event includes the following parameters:

- Status byte (Error code) – 0x00
- Number of services – 0x02 (Number of services found)
- Browse Group ID – 0x1002 (Public Browse Group)
- Service UUID – 0x1101 (The service found)
- RFComm Port Number – 0x04
- Number of bytes in the service name
- Name of the service

C) SDAP Disconnect:

After a successful Service Browse the connection has to be released again. As there can only be made one SDAP link at the time, the SDAP Disconnect command has no parameters. The confirmation of the command just returns the error/status code.

TABLE. III. LOG OF SDAP DISCONNECT

Direction	What	HEX Code
TX	Request	02,52,33,00,00,85,03
RX	CFM	02,43,33,00,77,00,03

Interpretation by Simply Blue Commander

- Tx: Cmd: SDAP Disconnect
- Rx: Event: SDAP Disconnect, Status: 00

Simply Blue Commander

The Simply Blue Commander is a tool to send commands to the LMX98xx Bluetooth® serial port module [3]. The software allows monitoring of the ingoing and outgoing traffic on the UART and interprets the events sent back by the LMX98xx. The simply blue commander is used to visualize the values sent and received from the LMX9838 serial port module. It helps to scan through to find the active devices and get connected with them. The Hex values sent and received can be viewed on fig4.

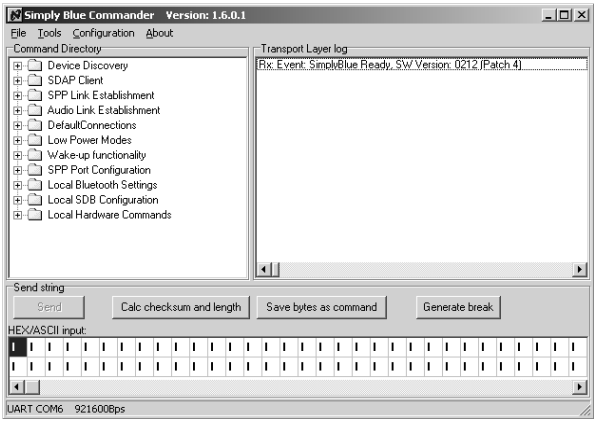

Figure. 3.Simply Blue commander Window.

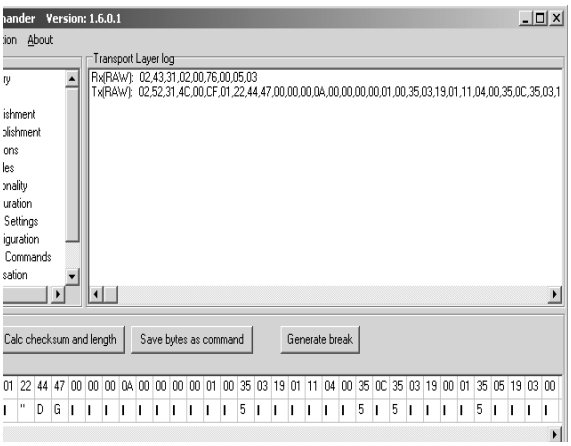

Figure .4. The Display of RX and TX values.

IV. WORKING DETAILS

The LMX 9838 Bluetooth serial port module is connected to the arduino board to have the connection with the device. The UART – Universal Asynchronous Receive Transmitter acts as an interface between theLMX9838 and the arduino and helps in transmitting the messages. The simply blue commander is an application which helps to send and receive data from the LMX9838. This device makes it easy to understand the communication between the devices. Once the LMX9838 gets connected to the arduino, it is taken as a master node which starts scanning for Bluetooth devices nearby in the range. The value of MAC address can be specified in the simply blue commander in order to search for a particular Bluetooth device. This MAC address varies from one device to another which is a factor of authentication. The transmitting values are in the hexadecimal format. The master node checks for the activeness of the Bluetooth device every 3 seconds and outputs different set of hexadecimal values. So it runs in a loop for every 3 seconds to verify the Bluetooth's status.

The following algorithm will help in checking for the activeness of the Bluetooth device after the specified amount of time.

1. include library Software Serial
2. store the SDAP_ Connect hex values in a byte
3. send value to arduino by serial. Write (sdap_ connect,13);
4. check if(starting byte is 0x02) {
5. store the value in one array or variable.
}untill end of the byte is 0x03
6. if (5th array is 0x00 or 0x32)
the Bluetooth is connected
7. else
disconnected

Initially all the hexadecimal values received will be stored in the array and then further processed to verify for the status of the Bluetooth device. The algorithm checks for the 5th array that is where the change of status is noticed. It output window displays the appropriate message according to the conditions specified in the algorithm.

V. RESULTS AND CONCLUSION

The Bluetooth serial port LMX 9838 used in here is giving prominent results. The simply blue commander was used to send and receive the data from the Bluetooth device. It was helpful to analyze and visualize the hex vales received from the master node and the slave node. Few garbage value were noticed while reading the data. But then those were overcome. As we connect the LMX9838 device along with arduino, the light will start to blink just to indicate that it is acting as a master node. After that searches for the active Bluetooth device with a particular MAC address. If it is found it says a message saying it is connected as shown in figure 5.

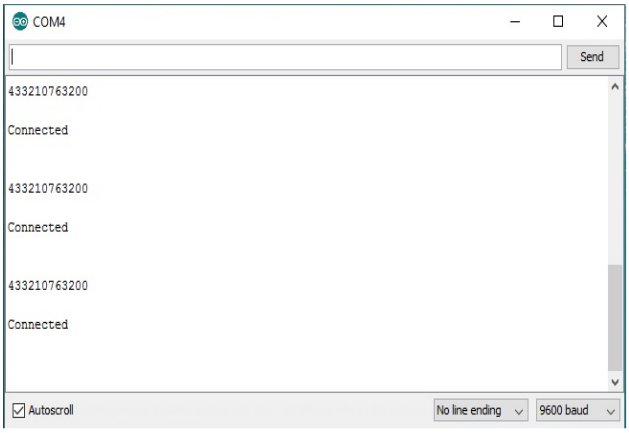

Figure .5. The output message saying "Connected".

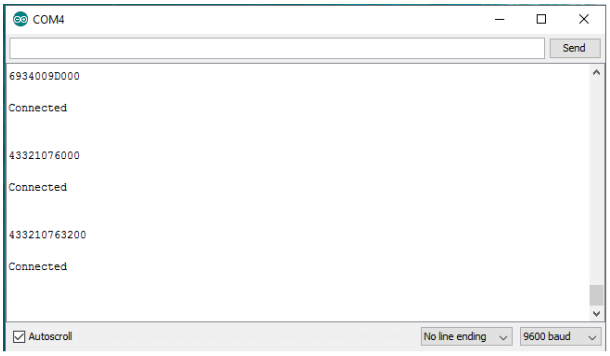

Figure .6. The different codes of connected state

The figure 6 shows some different codes for the connected state. The master nodes keeps scanning for the active device after every 3 seconds. It checks for the activeness even if the

device is connected. Once the Bluetooth of the slave device is turned off the arduino will display the appropriate message for disconnected state. It is shown in figure 7.

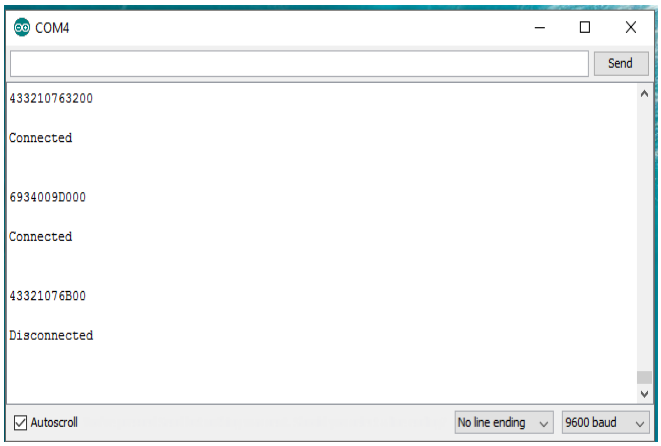

Figure. 10. Disconnection status.

VI. CONCLUSION

With the help LMX 9838 Bluetooth serial port module, we are able to connect to the Bluetooth device with the specified MAC address. Since LMX 9838 acts as master node , it starts scanning for the active Bluetooth devices nearby. We are to receive the message saying whether the Bluetooth device is with connected or disconnected state. And hence the device can be connected without any delay. This has helped in uniquely identifying the user and for any further authentication processes.

VI. REFERENCES

[1]. "The World in 2013: ICT Facts and Figures" Website: http://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFa ctsFigures20 13.pdf;

[2]. Sohum Misra ,Appl. Electron. & Instrum. Eng., Heritage Inst. of Technol., Kolkata, India "A Very Simple User Access Control Technique through Smart Device Authentication using Bluetooth Communication "

[3]. Bluetooth® Serial Port Module LMX9838 website:" www.ti.com", SNOSAZ9C –JULY 2007–REVISED FEBRUARY 2013,Texas Instruments

[4]. Haider Hussein Alwasiti, Ishak Aris and Adznan Jantan. Brain Computer Interface Design and Applications: Challenges and Future, World Applied Sciences Journal 11 (7): 819-825, 2010,ISSN 1818-4952.

[5]. Rebsamen, B., E. Burdet, C. Guan, H. Zhang, C. Teo,Q. Zeng, M. Ang and C. Laugier, 2006. A brain controlled wheelchair based on P300 and path Guidance.

[6]. Alexander Yohan, Nai-Wei Lo, Da-Zhi Sun, Xiao-Hong Li "Pairing and Authentication Security Technologies in Low-Power Bluetooth", pp. 1, 2016, ISBN 9781450341424.