1. Introduction:

Bluetooth is a new wireless standard for low cost, low power, local radio communications. This technology is designed to be small enough to fit inside any electronic device, hence revolutionizing wireless connectivity by enabling many new and innovative services for its users. Several usage models and applications are already being identified for various Bluetooth wireless mobile devices such as headsets, phones, computers, modems, and so forth.

In this paper, we propose a new architecture called NMMB (New Messenger for Mobile on Bluetooth) which defines a Bluetooth usage model that provides new messenger depending on transfer data without paying any cost[1].

A mobile phone or mobile (also called cell phone and hand phone) is a long-range, electronic device used for mobile telecommunications (mobile telephony, text messaging or data transmission) over a cellular network of specialized base stations known as cell sites. Mobile phones differ from cordless telephones, which only offer telephony service within a limited range, e.g. within a home or an office, through a fixed line and a base station owned by the subscriber and also from satellite phones and radio telephones[5].

2. Bluetooth:

Bluetooth is an open wireless protocol for exchanging data over short distances (using short radio waves) from fixed and mobile devices, creating personal area networks (PANs). It was originally conceived as a wireless alternative to RS232 data cables. It can connect several devices; there are many characteristics of Bluetooth Technology, are:

Function

Bluetooth technology functions as a 10-meter personal bubble that supports the simultaneous transmission of both voice and data information for more than one device. As a matter of fact, up to eight data devices can be connected in a single piconet, with up to 10 piconets existing within the 10-meter bubble. Not only that, but each piconet also supports up to three simultaneous full duplex voice devices [3].

Types

There are many types of Bluetooth technologies out there, all of which help users stay connected without actually having to be connected. Types of Bluetooth devices include dongles, headsets, radios, and PC cards, among other products. Stereo headphones are becoming increasingly popular as a wireless Bluetooth option that can be used with iPods, music phones or other MP3 players. Also, laptop's and other small Internet-enabled devices are offering accessories that utilize Bluetooth technology for wireless functionality, such as in wireless keyboards and mice.

Benefits

There are many benefits to utilizing Bluetooth technology. For example, Bluetooth dongles enable consumers to simply plug their dongle into an Internet-enabled personal computer. This allows them to wirelessly check email, download Windows updates or transfer files, among other tasks. Bluetooth headsets may offer the most benefits because they allow us to use our cell phones hands-free, which is especially useful now that many states have passed laws that make it illegal to talk on your cell and drive at the same time[2].

Features

. Operates in 2.4GHz ISM radio band.
. Utilizes 79 channel FHSS (frequency-hopping spread spectrum) technology
. Communication channel can support both data (asynchronous) and voice (synchronous) communications with a total bandwidth of 1 Mb/sec.
. Provides a 128 encryption mode for security .
. Supports 8 active and 255 inactive (parked) devices.
. Automatic error correction and retransmission
. Well defined attachment profiles contained in SIG controlled specification Architecture

Bluetooth devices can interact with other Bluetooth devices in several different ways. The simplest scheme is when only two devices are involved. This is referred to as point-to-point. One of the devices acts as the master and the other as a slave. This ad-hoc network is referred to as a piconet. As a matter of fact, a piconet is any such Bluetooth network with one master and one or more slaves. There can be up to seven active slaves in a piconet. In the case of multiple slaves, the communication topology is referred to as point-to-multipoint. In this case, the channel (and bandwidth) is shared among all the devices in the piconet[2].

3. Physical Link Characteristics:

1. Radio Specification

Bluetooth operates in the 2.4 GHz.

The operational frequency band is divided into 79.

RF channels, spaced 1 MHz apart. The bit rate is 1Mb/s per channel. Bluetooth uses a modulation scheme called Gaussian Frequency Shift Keying. A binary one is represented as a positive frequency

deviation and a zero by a negative deviation from the RF channel center frequency. Compared to other modulation schemes, GFSK has the following advantages

- Constant envelope, allowing high RF amplifier
efficiency
- Narrow power spectrum: adjacent channel interference
is minimized
- Good bit error rate (BER) performance

GFSK modulation is also used in GSM systems [3].

2. Bluetooth channel

A Bluetooth *channel* is defined as a pseudo-random hopping sequence trough the 79 (or 23) RF channels. The channel is divided into *time slots* of 625□S, i.e. 1600 slots per second. The frequency is changed2 each time a new time slot, or *hop* begins. Thus, a data transmission on a single BT channel could use the RF channels 4,77,43,21,9,8,61... The frequency switch takes place in the beginning of each time slot. The frequency hopping scheme is adopted to make Bluetooth more insensitive to interference from other devices (such as a microwave oven or a baby monitor).

4. Bluetooth Links and Packets:

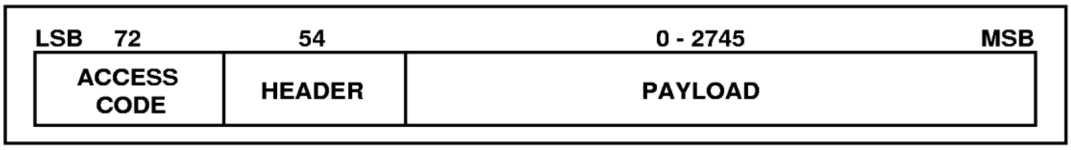
1 Bluetooth Link Types

Between two (or more) Bluetooth devices two types of links can be established:

- Synchronous Connection-Oriented (SCO) link
- Asynchronous Conncetionless Link (ACL)

2 Bluetooth Packet Format

The standard Bluetooth packet consists of three parts: the access code, the header and the payload (see figure 1), [3].



LSB 72	54	0 - 2745 MSB
ACCESS CODE	HEADER	PAYLOAD

Figure (1) Bluetooth packet

3. The Access Code:

The 72-bit3 access code is mainly used to identify packets transmitted over a Bluetooth channel: all data packets sent on the channel share the same access code. In addition, the access code is used for device paging (finding out if a specific device is in range) and inquiries (used to discover new devices). A Bluetooth device monitors the access code of each packet; if the device is not directly or indirectly addressed, the rest of the packet is ignored. The access code is very fault-tolerant (the minimum Hamming distance between code words is 14, so up to 6 bit errors can be corrected. The access code is also used to determine receiver timing.

4. The Packet Header

The 18-bit packet header contains the following information:

- A 3-bit target device address, which addresses an active device on the Bluetooth channel. A broadcast address is also provided.
- A 4-bit type code. Identifies the type of data or control packet.
- Fields for flow control, sequencing and packet acknowledgement.
- An 8-bit header CRC

To protect the header from transmission errors each bit is repeated three times in row (the Bluetooth spec refers to this as 1/3 FEC encoding) yielding a total length of 54 bits.

5. The Packet Payload

The payload part (0 to 2745 bits) of the packet carries the actual data. For ACL links, the payload begins with an 8- or 16-bit header, which indicates the length of the data packet and provides fields for logical channels and flow control. The header also supports fragmentation of data packets[3].

6. Packet Types

Bluetooth supports a wide variety of packet types depending on the type of link, throughput and bit fault tolerance. On SCO links packets for low, medium and high quality voice as well as combined data and voice are supported. For ACL links 1, 3 and 5 slot packets using medium (5 check bits for each 10 bits) and high (no additional check bits) data rates are supported [3] .

5. Security:

There are many security threats to mobile subscribers and operators. It is easy to sneak a virus as a Trojan attachment in an SMS message. There are, of course, other common and not-so-common ways to attack mobile devices, including denial of service (DoS) attacks that blast multiple inbound messages and block outbound calling as well as the usual spam and spyware that is already migrating from PCs to phones.

Before diving into specifics, here are the GSM Association definitions (IR.70 SMS SS7 Fraud Paper, dated February 2005) for the various types of SMS fraud.

□ **Spam:** Spamming is an action where the subscriber receives an unsolicited SMS. An unsolicited SMS is one the subscriber did not request to receive. The act of spamming does not define the content but only the fact that the SMS was received without solicitation. The content of the spam SMS is incidental to the act. The spam SMS may take on various forms of content to include: commercial information, bogus contest and other message generally intended to invite a response from the receiver.

□ **Spoofing:** The spoofing case is related to an illegal use of the HPLMN SMS-C by a third party. In this case, an SMS MO with a manipulated A-MSISDN (real or wrong) is coming into the HPLMN network from a foreign VLR (real or wrong SCCP Address).

□ **Flooding:** The act of flooding is when a large number of messages are sent to one or more destinations. These messages may either be valid or invalid. The value or parameter used to define flooding is the extraordinary number of messages sent.

□ **Faking:** A fake SMS is originated from a foreign SS7 network and is terminated to a mobile network. This is a specific case when SCCP or MAP addresses are manipulated. The SCCP or MAP originator (for example: SMSC Global Title, or A_MSISDN) is wrong or is taken from a valid originator [4].

6. The Proposal NMMB:

The proposal NMMB aim to provide new technique to transfer data through mobiles, buy using new messenger built for mobile depending on Bluetooth techniques without paying any cost to the Contact.

The NMMB depending on a way to play the Messenger, who works on the search for Bluetooth devices nearby, By searching for the names of mobiles, and After finding the name of the mobile, program starts to act first to ensure the safety of communication between the device and another through the protection that exists within this Messenger.And then opening a window for communication between the mobiles through this Messenger for the exchange of information between these devices.

6.1. First View to NMMB:

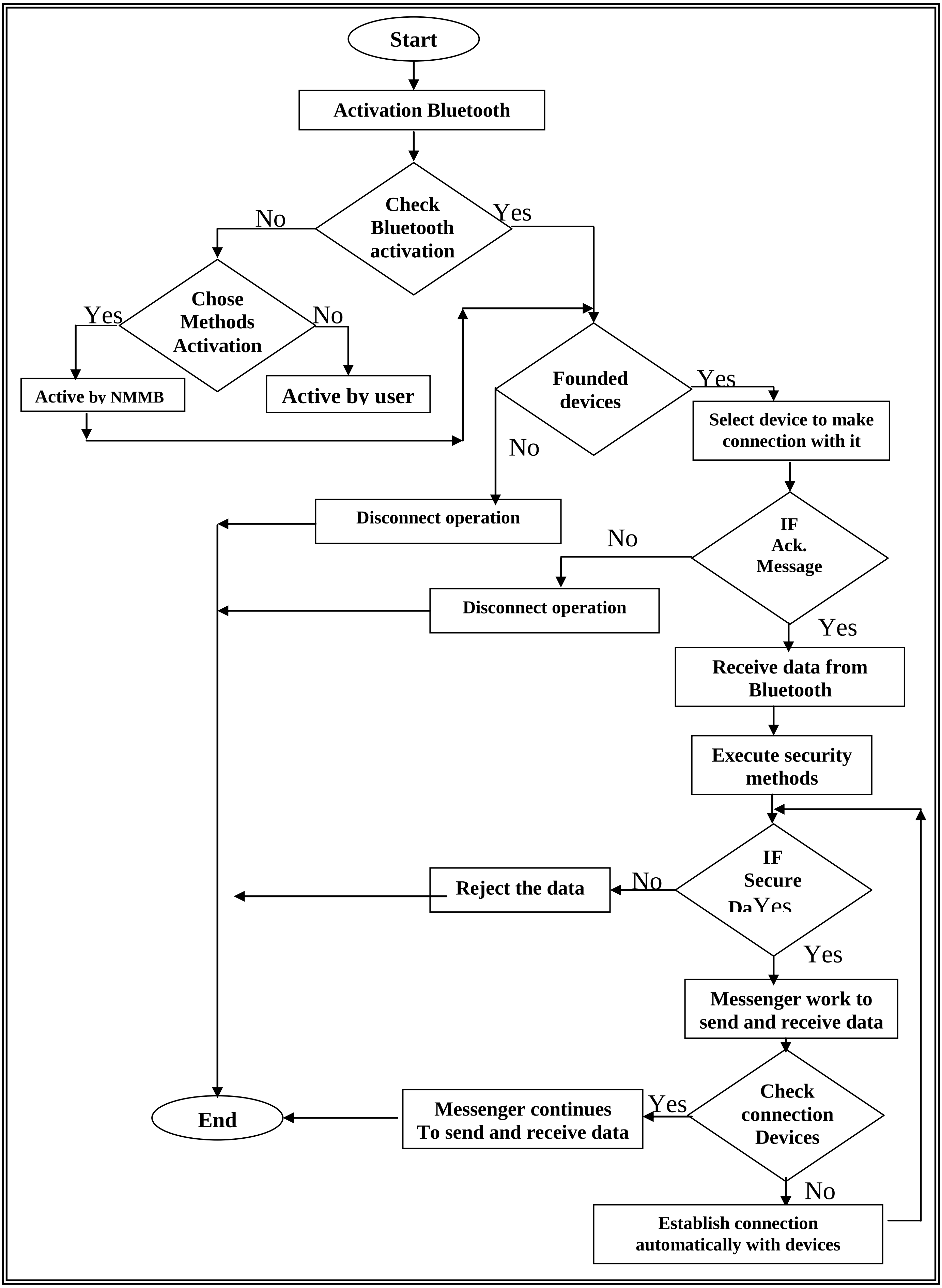
This model is designed to provide new technology to transfer information between the mobile devices a safely and quickly without payment any amounts of money when data is transfer.

It explains the design and conceptual work of the suggested proposal to transfer information through messenger via mobile's Bluetooth, it contains three parts:

First: discovery of new Bluetooth devices close through activation of Bluetooth in mobile, and ensure of the type of connection between these devices by **Bluetooth stage**.

Second: check the safety and security of data transmitted received for Bluetooth by **security stage**.

Third: new messenger work to transfer data between devices in **Messenger stage**.


Start
Activation Bluetooth
Check Bluetooth activation
No
Yes
Chose Methods Activation
Yes
No
Active by NMMB
Active by user
Founded devices
Yes
No
Select device to make connection with it
Disconnect operation
IF Ack. Message
No
Disconnect operation
Yes
Receive data from Bluetooth
Execute security methods
IF Secure DaYes
No
Reject the data
Yes
Messenger work to send and receive data
Check connection Devices
Yes
Messenger continues To send and receive data
End
No
Establish connection automatically with devices

The main algorithm of NMM is shown in Figure (3):

```
Input: Receive unsecured data from Bluetooth.
Output: exchange secure data via messenger.
Process:
Step 1. Activation Bluetooth device .
Step 2. If Bluetooth not activation then
        2.1. System active the device automatically by NMMB.
        Else
            Active Bluetooth by user.
Step 3. If founded closes devices then
          3.1. Select the device.
          3.2. Send Ack. Message to these device.
          3.3. If receive Ack. Then
                3.3.1. Execute security method on coming data.
                3.3.2. Exchange data over messenger.
                Else
                    Go to step 4.
          3.4. Check connection over time.
          Else
                  Go to step 4.
Step 4. End.
```

Figure (3) NMMB Algorithm

6.2 The main NMMB architecture:

This section covers the implementation of proposed NMMB which consists of the following stages:

1. Bluetoothe stage.
2. Security stage.
3. Messenger.

Figure (4) illustrates this architecture of NMMB

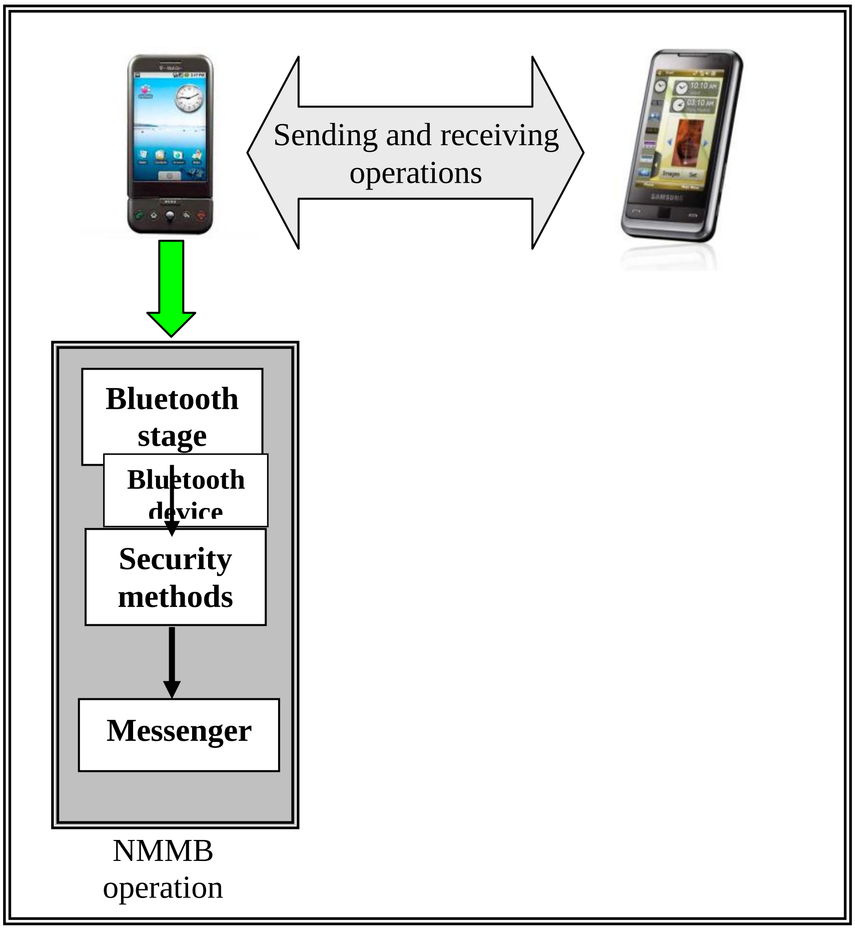


Figure (4) NMMB architecture

6.2.1. Bluetooth STAGE :

This stage relies on open Bluetooth device and configured to communicate with other devices, through the exchange of Bluetooth Packets.

Give each device sending message an IP, this IP generated through program Exist in each mobile. The coming figure (5) show the activation operation to Bluetooth device.

```
private void doDiscoveryDevices
       try}
          local = LocalDevice.getLocalDevice؛
{
       catch (BluetoothStateException bluetoothstateexception}
          bluetoothstateexception.printStackTrace  ؛
{
       agent = local.getDiscoveryAgent  ؛
       try}
          inquiry = agent.startInquiry(0x9e8b33, this
{
       catch (BluetoothStateException bluetoothstateexception1

public void doServiceSearch(RemoteDevice remotedevice)
       UUID auuid[] = new UUID[1];
       auuid[0] = new UUID("86b4d249fb8844d6a756ec265dd1f6a3", false);
       int ai[] = {
          256
       };
       try {
          searchService = agent.searchServices(ai, auuid, remotedevice, this);
       }
       catch (BluetoothStateException bluetoothstateexception) {
          bluetoothstateexception.printStackTrace();
       }
       catch (Exception exception)
    {
```

Figure (5) Bluetooth Activation

Following figure (6) show Bluetooth operations.

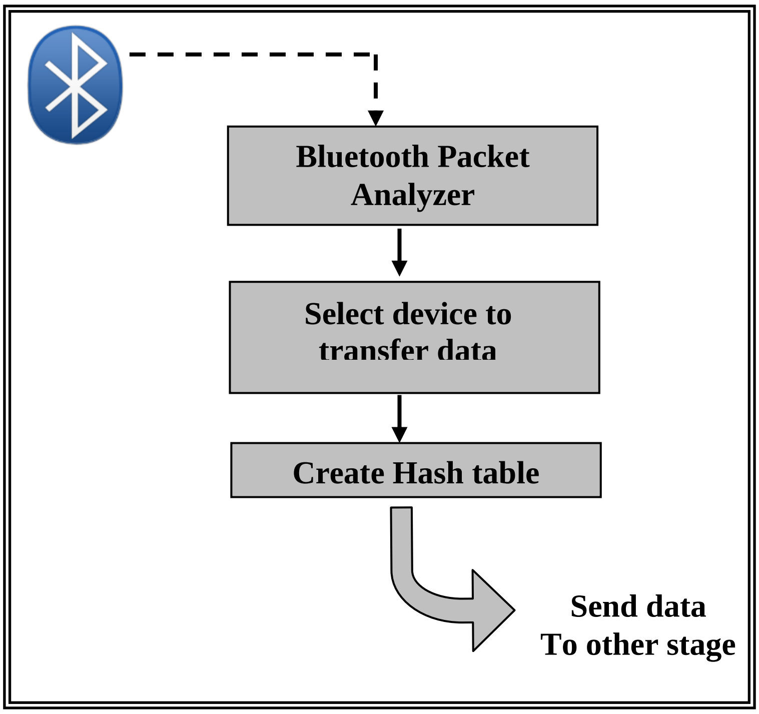


Figure (6) Bluetooth stage

Bluetooth Packet Analyzer:

The function of the packet analyzer depends on receiving data by mobile and analyzing it.
The maximum size of a message sent 2M consists of 120 characters, as shown in figure (1).
After receiving packet thorough Bluetooth, these packet consist of data (message) and header that contain control information to Bluetooth packet.
This stage contains of **IP-Generation** that give an IP to each Bluetooth device connected to others. The aims of **IP-Generation are:**

1. Determine which devices are connected with each other (client-server).
2. When device tack an new IP, We do not need to re-definition of the connected device again, having become authorized to communicate with other devices after contact was lost.

After analyzed packet, the final shape of packet is: **||؛ت¾ ,** The operation of the **IP-Generation** show in figure (87

```
searchService = 0؛
      System.out.println("devices.size() -> " + index + "   " + devices.size
      synchronized (devices} (
         if (devices != null && index < devices.size() - 1}
            if (serviceFound != null && serviceRecFound != null} (
               Main.getChooseDeviceForm().newDevice(serviceFound, serviceRecFound
{
            index؛++
            RemoteDevice remotedevice = (RemoteDevice)devices.elementAt(index؛(
            waiter.go(remotedevice؛(
 {          else}
            if (serviceFound != null && serviceRecFound != null} (
               Main.getChooseDeviceForm().newDevice(serviceFound, serviceRecFound
{
            Main.getChooseDeviceForm().populateAndSetActive؛()
            index = 0؛
            canceled = true؛
{
{
      switch (j} (
      case 1: // '\001'
         System.out.println("everything is completed
         break؛

      case 6: // '\006'
         System.out.println("not reachable
         break؛

      case 4: // '\004'
         System.out.println("no records
         break؛

      case 2: // '\002'
         System.out.println("search canceled
         break؛
{
```

Figure (7) IP-Generation

The Figure (8) show the_Packet Analyzer

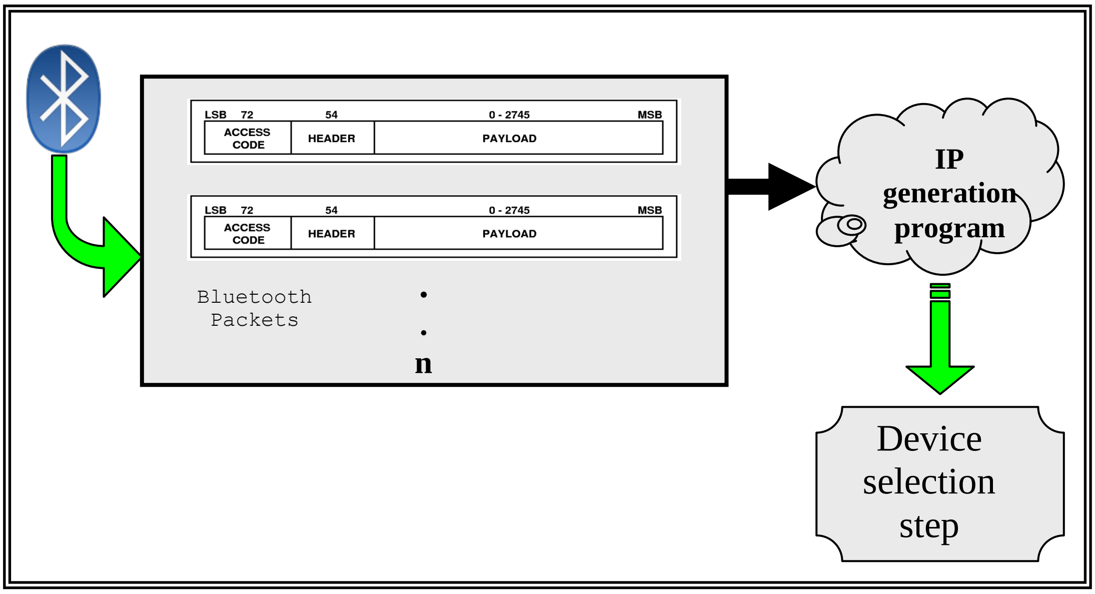


Figure (8) Packet analyzer

<u>Select device to transfer data:</u>

This stage checks the devices linked and the list of Bluetooth devices to make connection with it, Maximum number of devices to be a connected are the four devices. Figure (9) shows the how to chose device to make connection with it.

```
Choose Device ( Friend )

public ChooseDevice() {
        forma = new List("Online: ", 3);
        chatForm = new Hashtable();
        completeNamesNicknames = new Vector();
        oldTicker = "";
        try {
            newMessage = Image.createImage("/newmsg.png");
        }
        catch (IOException ioexception) {
            ioexception.printStackTrace();
        }
        forma.setCommandListener(this);
    } ( Friend )

public ChooseDevice() {
        forma = new List("Online: ", 3);
        chatForm = new Hashtable();
        completeNamesNicknames = new Vector();
        oldTicker = "";
        try {
            newMessage = Image.createImage("/newmsg.png");
        }
        catch (IOException ioexception) {
            ioexception.printStackTrace();
        }
        forma.setCommandListener(this);
    }
```

Figure (9) Choose Device

Create Hash table

After activate then the devices as shown in figure (5) , send to **Hash-table** to gave each devices Unique code , and each device send acknowledged message to corresponding device to check it work or not. After receiving message form each device and active each one to connect to other, these devices adds to list of Bluetooth devices to make chatting with it.

The aim of **Hash-Table** is to send information form device to another. Its consist of three components:

1. Name of Bluetooth device.
2. Bluetooth address.
3. Service types, the services that use chatting program are peer-to-peer connection .

There are three types of services:

1. Send service.
2. Send and receive services.
3. Chek form sends and receives process by send acknowledged message.

Figure (10) show the hash-table operation

```
String s
        boolean flag = false؛
        ConnectionStruct connectionstruct = null؛
        if (Server.access$000().size() != 0 && Server.access$000().containsKey(friend} ((
            connectionstruct = (ConnectionStruct)Server.access$000().get(friend؛(
{
        if (connectionstruct != null && friend != null}
            do}
                if (flag   )  (break؛
{
                String s1؛
                if (connectionstruct != null) (

                   if ((s1 = connectionstruct.read()) != null} (

                        if (OptionsForm.alertSound.equals("true} (("
                            AlertType.INFO.playSound(Main.getDisplay؛(()
{
                        if (OptionsForm.vibrate.equals("true} (("
                            Main.getDisplay().vibrate(800؛(
{
                        Main.getChooseDeviceForm().getChatForm(friend).addMsg(friend.substring(0,   friend.indexOf("_"))   +   ":   "   +
s1.toString(), friend؛(
                        if (Main.getChooseDeviceForm().getChatForm(friend).isFormShown} (()
                            Main.getChooseDeviceForm().getChatForm(friend).scroll؛()
{
 {                     else}
                        flag = true؛
                        Main.getChooseDeviceForm().getChatForm(friend).addMsg("< " + friend.substring(0, friend.indexOf("_")) + " left
>", friend؛(
                        Main.getChooseDeviceForm().getChatForm(friend).removeCommandChat؛()
                        if (Main.getChooseDeviceForm().getChatForm(friend).isFormShown} (()
                            Main.getChooseDeviceForm().getChatForm(friend).scroll؛()
{
                        Main.getChooseDeviceForm().getChatForm(friend).setFriendLeft؛()
{
{
 {           while (true؛(
```

Figure (10) hash-table operation

6.2.2. Security Stage:

This stage depends on confirmation of the authenticity, integrity and security of the data hyphen or sent by Bluetooth devices, the following figure (11) show these operation.

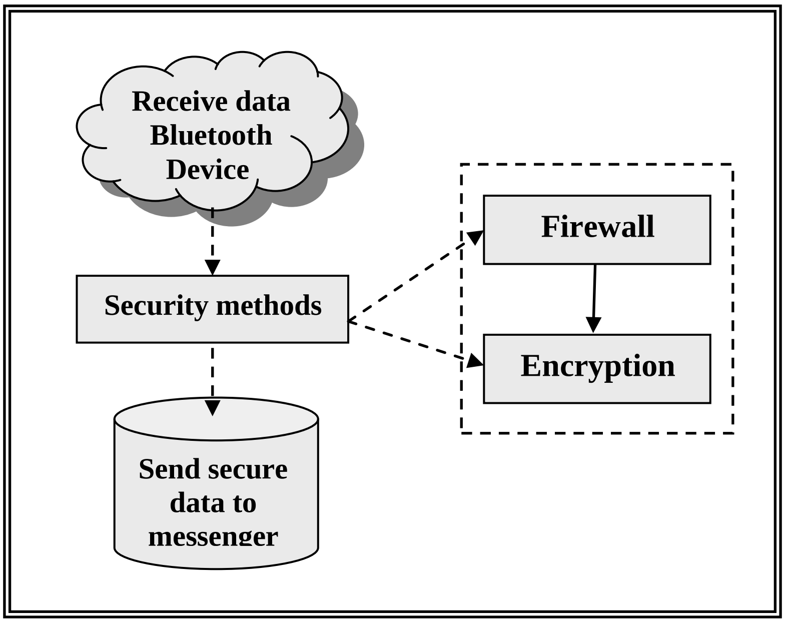


Figure (11) security methods

This stage use firewall to check the coming/outing data if it is authorized or not and usesRSA algorithm to encrypted data to prevent any unauthorized devise make contact and access to transfer data

6.2.3. Messenger:

After to ensure the safety and security of data received from the Bluetooth device and giving the IP for each device and a hyphen, now is work, which depends on the search for the names of the devices near it, for connection with by Bluetooth.

After you find the nearby mobile devices as shown in figure (9), the user chooses the devices that wish to establish contact with them through the selection of the name of this device , figure (12) shows these operation.

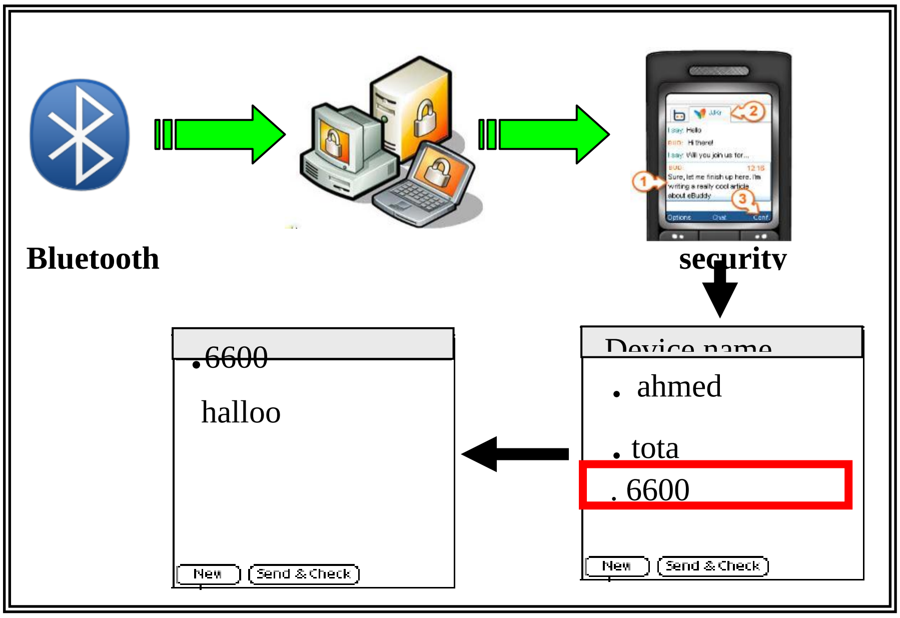
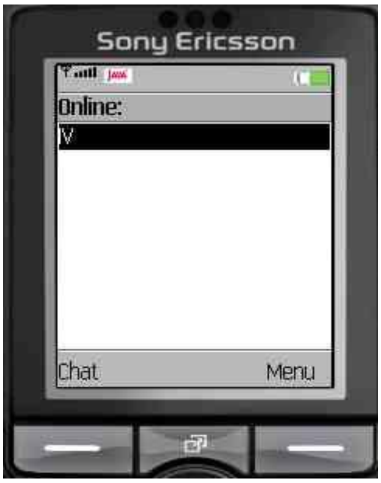


Figure (12) messenger stage

7. NMMB Implementation:

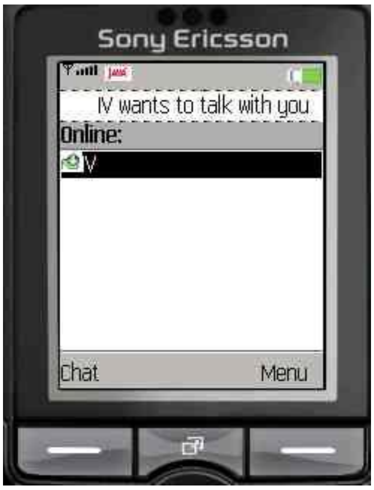
The implementation of the proposed NMMB can show in following figures (13,14,15,16,17,18) .



Online:

V

Figure (13)

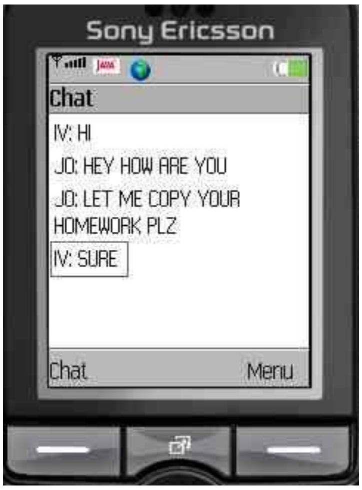


IV wants to talk with you

Online:

V

Figure (14)



Chat

IV: HI

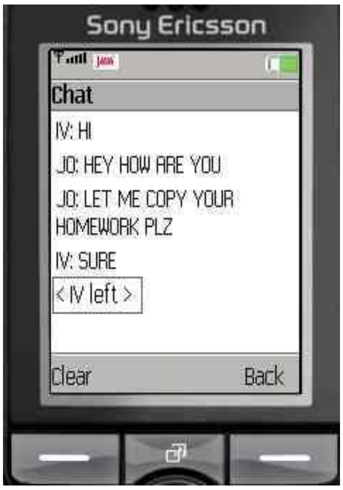
JO: HEY HOW ARE YOU

JO: LET ME COPY YOUR HOMEWORK PLZ

IV: SURE

Figure (15)

Figures (13, 14, 15, 16, 17, 18) Implementation of NMMB



Chat

IV: HI

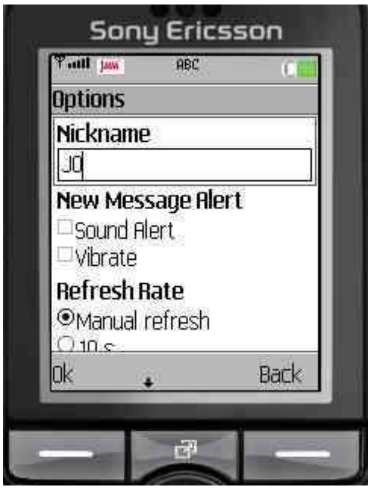
JO: HEY HOW ARE YOU

JO: LET ME COPY YOUR HOMEWORK PLZ

IV: SURE

< IV left >

Figure (16)



Options

Nickname: JO

New Message Alert

□ Sound Alert

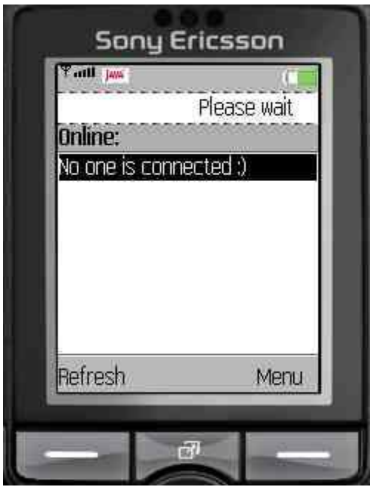
□ Vibrate

Refresh Rate

● Manual refresh

○ 10 s

Figure (17)



Please wait

Online:

No one is connected :)

Figure (18)

Figures (13, 14, 15, 16, 17, 18) Implementation of NMMB

8. Conclusion

The following conclusions can be extracted from the pleat of the research:

1- NMMB is completely free.

2- It Uses Bluetooth technology, no fees to pay whatsoever.

3- The scrolling alert and graphical alert inform the user the receiving of a new message.

4- It provides extra large screen for easy-to-read chat sessions.

5- It supports automatic scrolling of conversations when chat sessions get too long.

6- It supports chatting/switching between different people at the same time.

7- It supports nickname personalization.

8- It supports sound or vibration alert, or both when a new message arrives.

9- It supports automatic or manual refresh of online contact list.

10- Most phone models are supported by NMMB, for example:

a. Sony Ericsson

K550i , K600 K608 , K610 K700 K750 , K790 , K800 , K810 , K850 (bugs) , K850i , S500 , W200 , W300i , W550 , W600 , W610 , W700 W710 W800 , W810 , W850 W880 W900 Z550 Z610

b.Nokia

5200 , 6085 , 6188 , 6230 , 6288 , 6265i , 6300 , 6600 , 6630 , 7710 , N73 N73 ME , N76 , N80

c.Motorola
L6 , SLVR L7 , V360 , V3i

11- NMMB is Fun, fast, and easy to use.

9. Suggestions for Future Work:

1. Production of a new search engine by using Bluetooth.
2. Increase the number of chatting devices in one time to scalable number with different types of devices.
3. Add multimedia effect to the messenger (sound effect, picture, and Webcam).
4. Saving the transferred messages in the mobile.

7. References

[1]. Bluetooth, http://en.wikipedia.org/wiki/Bluetooth

[2] Joe Eitel, type of Bluetooth technology, http://www.ehow.com/about_5509210_type-bluetooth- technology.html

[3]. Setting up a Bluetooth Packet Transport Link
Tancred Lindholm, Department of Computer Science, Helsinki
University of Technologyctl@cs.hut.fi

[4]. **SMS Security, Malicious attacks are just around the corner. Are you protected?**, Technologyctl@cs.hut.fi

[5] Mobile phone, http://en.wikipedia.org/wiki/Mobile_phone