

SEL

doc: bd_addr

David Nordfors, Ringvägen 163, 116 31 Stockholm, Sweden

Swedish Pat. 0102758-0

CONNECTING BLUETOOTH DEVICES TO EACH OTHER

FIELD OF THE INVENTION

The present invention relates to a method of connecting Bluetooth compatible or similar devices to each other, to a Bluetooth or similar network and to Bluetooth compatible or similar devices.

5

BACKGROUND

Bluetooth is an open standard for peer-to-peer short distance wireless radio data communication. Bluetooth provides "ad hoc" networking, i.e. Bluetooth compatible units that are within communication distance can spontaneously exchange information with each other. A Bluetooth compatible unit is herein taken to mean a unit working in all respects, as seen from other units, according to the Bluetooth specification. A regular Bluetooth unit or a Bluetooth enabled is herein taken to mean a unit working totally according to the Bluetooth specification. A regular Bluetooth or Bluetooth enabled unit is obviously always a Bluetooth compatible unit.

Bluetooth compatible units can be used for replacing a cord between two objects with wireless communication. Bluetooth compatible units can also spontaneously establish small networks, piconets, including up to eight units. One of the units is assigned the role of "master" of the piconet and the others are "slaves". The slaves communicate with each other via the master. Communication can be established between Bluetooth compatible units that belong to different piconets, either through so called "scatternets", ad hoc peer-to-peer communication between overlapping piconets, or by connecting the piconets to a computer network spanning larger geographic distances and having capacity for more users, e.g. a LAN - purely local or connected to the Internet. Bluetooth is frequently suggested as a solution for the last yards of the mobile Internet, closest to the user terminals.

PRIVACY PROBLEM

According to the Bluetooth specification, including version 1.1 20/2 2001 and previous versions, each Bluetooth enabled unit has a unique Bluetooth device address, BD_ADDR. The BD_ADDR is used for setting up the links and for communicating between the units. It is used from basic levels and upwards in the protocol stack. For example it determines the sequence of frequency hops in the radio

40

communication between units and is used when producing keys for encrypted data communication.

5 This unique address is a threat to privacy, because BD_ADDR is visible for all Bluetooth compatible units within communication distance.

10 For example, once a Bluetooth enabled electronic wallet is used by its owner for a purchase, the retailer will thereafter be able to identify the wallet through its BD_ADDR, also without setting up a communication link. It is enough that the retailer has access to a Bluetooth compatible unit within communication distance of the wallet, for example a Bluetooth LAN access point connected to the Internet.

15

SUMMARY

It is an object of the invention to provide a method of connecting Bluetooth compatible and similar devices to each other preserving the anonymity of the devices.

20

It is another object of the invention to provide a Bluetooth compatible or similar network and devices used in such networks in which the anonymity of the devices of the devices is preserved.

25 Thus generally, a Bluetooth compatible unit is suggested for protecting privacy. It deviates from the Bluetooth specification by not having a unique Bluetooth address BD_ADDR. Instead, it may choose its address from a group of BD_ADDR addresses. The unit switches its BD_ADDR from time to time, thus preserving privacy.

30

Therefore, the suggested Bluetooth compatible unit having address switching facilities does not fully comply with the Bluetooth standard. However, it will still be capable of communicating without any conflict with units following the Bluetooth standard.

35 No Bluetooth compatible unit is capable of distinguishing between a Bluetooth compatible unit using address switching and a regular Bluetooth unit at any given moment.

BRIEF DESCRIPTION OF THE DRAWINGS

40 The invention will now be described by way of non-limiting em-

bodiments with reference to the accompanying drawings, in which:

- Fig. 1 is diagram of a network formed according to the Bluetooth specification,
- Fig. 2 is a picture illustrating the standard format of a packet according to the Bluetooth specification,
- Fig. 3 is a picture illustrating the format of an FHS packet,
- Fig. 4 is diagram of a Bluetooth compatible device having address switching means, and
- Fig. 5 is a block diagram of an address switching unit to be used in a Bluetooth compatible device.

DETAILED DESCRIPTION

A device adapted to communicate according to the Bluetooth specification generally includes a radio unit, a link control unit and a support unit for link management and host terminal interface function. Point-to-point and point-to-multipoint connections can be provided. For a point-to-multipoint connection, the radio band is shared by several units. The units form a small network called a piconet, see Fig. 1. Within such a piconet a unit can be a master or a slave. Within each piconet there may be only one master and up to seven active slaves.

Each unit adapted to communicate according to the Bluetooth specification has a globally unique 48-bit IEEE 802 address. This address, called the Bluetooth unit Address (BD_ADDR), is assigned at the time when the unit is manufactured and it is never changed according to the specification. In addition thereto the master of a piconet dynamically assigns a local Active Member Address (AM_ADDR) to each active slave member of the piconet.

The standard format of a packet used for transmission according to the Bluetooth specification is illustrated in Fig. 2, this format not being used for some types of control packets. A standard packet has a field for an access code having the length of 72 bits and a header field of a length of 54 bits. There is a field for the payload which has a length that can range from zero to a maximum of 2745 bits. The AM_ADDR is located in the packet header followed by some control parameters, e.g. a bit indicating acknowledgement or retransmission request of the previous packet, when applicable, and a header error check (HEC).

The access code used in a packet can be one of three different types: Channel Access Code (CAC), Device Access Code (DAC), and Inquiry Access Code (IAC):

- 5 - The Channel Access Code identifies a channel that is used in a certain piconet, i.e. essentially the CAC identifies the piconet. All packets exchanged within a piconet carry the same the CAC. The CAC is derived from the BD_ADDR of the master unit of the piconet.
- 10 - The Device Access Code is derived from the BD_ADDR of the particular unit. It is used for special signalling procedures, e.g. the PAGE procedure.
- The Inquiry Access Code appears in two variants: the General Inquiry Access Code (GIAC) and the Dedicated Inquiry Access Code (DIAC), both used in the INQUIRY procedure.

15 An important property of any ad hoc network such as a network working according to the Bluetooth specification is the neighbour discovery feature. The neighbour discovery procedure according to Bluetooth consists of the INQUIRY message and the INQUIRY RESPONSE
20 message. An "inquiry" procedure is defined which is used in applications where the device address of the destination is unknown to the source. A Bluetooth compatible unit wanting to discover neighbouring Bluetooth units repeatedly transmits INQUIRY messages and listens for INQUIRY RESPONSE messages. An INQUIRY message
25 consists of an Inquiry Access Code (IAC). It does not contain any information about the source but may indicate the class of devices which should respond. The Inquiry Access Code can be a General Inquiry Access Code (GIAC), which is sent to discover any unit in the neighbourhood, or a Dedicated Inquiry Access Code (DIAC), which
30 is sent to discover only a certain type of units, for which a particular DIAC is dedicated.

A Bluetooth compatible unit receiving an INQUIRY message, including a GIAC or an appropriate DIAC, may respond by sending an INQUIRY
35 RESPONSE message. The INQUIRY RESPONSE message is actually an Frequency Hop Synchronisation (FHS) packet, see Fig. 3. The FHS packet is a special control packet revealing, among other things, the transmitting unit and the clock of the transmitting unit. The payload field in such a packet includes eleven fields. All fields
40 in the packet, except the AM_ADDR field, and of course the

"Undefined" field, indicate properties or parameters of the unit that sends the FHS packet. The three fields Lower Address Part (LAP), Upper Address Part (UAP) and Non-significant Address Part (NAP) fields together contain the BD_ADDR of the transmitting device. By listening for INQUIRY RESPONSE messages the unit that initiated the INQUIRY procedure can collect the BD_ADDR and internal clock values of the neighbouring Bluetooth compatible units.

10 An FHS packet is also used for other purposes according to the Bluetooth specification, in addition to the use as the INQUIRY RESPONSE message, e.g. for a paged master response.

Related to the INQUIRY procedure is the PAGE procedure, which is used to establish an actual connection between two units. Once the BD_ADDR of a neighbouring unit is known to a unit, the paging unit, as a result of an INQUIRY procedure, the neighbouring unit can be paged by sending a PAGE message. Also the knowledge of the internal clock value of the unit to be paged will potentially speed up the PAGE procedure, since it makes it possible for the paging unit to estimate when and on which frequency hop channel the neighbouring unit will listen for PAGE messages.

A PAGE message consists of the Device Access Code (DAC), derived from the BD_ADDR of the paged unit. A unit adapted to communicate according to the Bluetooth specification and receiving a PAGE message including its own DAC responds by sending an identical packet, i.e. including only the DAC of the paged unit. The paging unit then replies by sending an FHS packet, including the BD_ADDR of the paging unit, the current value of the internal clock of the paging unit, the AM_ADDR assigned to the paged unit and some other parameters, see Fig. 4. The paged unit then responds once again by transmitting its DAC and thereby the connection between the two units is established.

35 If the paging unit already was the master of a piconet, the paged unit has now joined this piconet as a new slave unit. Otherwise, the two units have just formed a new piconet having the paging unit as the master unit. Since the INQUIRY message does not include any information on the sender thereof, in particular not its BD_ADDR,

40

the unit that initiated the INQUIRY procedure is the only unit that can initiate a subsequent PAGE procedure. Thus, the unit initiating an INQUIRY procedure will also be the master of any new piconet that is formed as a result of a subsequent PAGE procedure.

5

Thus, in setting up Bluetooth networks, the BD_ADDR is used i.a. to initially define the participating units, this resulting in a privacy problem. The BD_ADDR is also used in other types of communicated information, at various levels.

10

To maintain privacy and still allowing the units to operate according to the Bluetooth specification, being capable of performing all functions specified therein, the units can be provided with an address switching function performed by a block 1, called an address switching unit or AS unit, see Fig. 4, incorporated in or added to the usual Bluetooth circuit 3. The address switching unit 1 provides at all instances, when the unit is operative, a valid BD_ADDR of the device and it is stored in a register 5 and is used by the Bluetooth circuit 3, e.g. in the INQUIRY and PAGE procedures described above. The register 5 is a rewritable, non-volatile memory cell remembering the stored data even when the power is off. The BD_ADDR is accessed from the register 5 in the address switching unit in the same way as for any regular Bluetooth unit.

25

The actual BD_ADDR stored in the cell 5 is randomly switched among a set of valid BD_ADDR addresses, thus making it impossible to say which BD_ADDR address the unit will use at any randomly selected time.

30

Optionally, an additional memory can be used, not shown, called BD_ADDR_CLKN, in which the value of the Bluetooth native clock CLKN is stored at each change of BD_ADDR. The native clock CLKN is described in the Bluetooth specification 1.1, baseband specification section 10.3. This is for handling the case where there are several interacting address switching devices using the same BD_ADDR at the same time, thus creating interference. In that case, the device that first chooses the BD_ADDR will be the one that keeps it, whereas the other will switch BD_ADDR.

40

The functions for controlling and manipulating the BD_ADDR are performed by a group of circuits, the AS circuit 1, in the hardware, as seen in Fig. 5, or by a software block executed in some processor in the host device of the Bluetooth circuit 3. The selecting of a new BD_ADDR is started by a block 11, called TRIG_SELECT_BD_ADDR, activating another block 13, SELECT_BD_ADDR, in which the very selecting is made and the selected BD_ADDR is stored in the register 5. The selecting block includes a unit 15, RAND, for generating random numbers, and a unit 17, BD_ADDR_GROUP, which can include a memory in which all possible permitted choices of addresses are stored. The address unit 17 can instead or additionally include some function generating the possible addresses from some basic data.

Thus, the BD_ADDR of the Bluetooth unit may be changed by the hardware function SELECT_BD_ADDR 13. This function uses the random number, created by the block 15, as an argument to select a BD_ADDR from those specified by the block BD_ADDR_GROUP 17. The selecting function can also include a function, not shown, that writes the value of the Bluetooth native clock CLKN into the memory cell BD_ADDR_CLKN.

The start of the function 13 SELECT_BD_ADDR is triggered by the triggering unit 11, that can be activated by a transition of the unit from the CONNECTION state to the STANDBY state. In the STANDBY state, no connection has been established, see Bluetooth spec. 1.1, sect. 10.7.2, p. 106. Switching the BD_ADDR when the unit is in this state will not effect the operation of any other unit, since no other Bluetooth compatible unit is connected.

Optionally, the unit may be equipped with a manual switch, not shown, operated by the user, disabling the function 13 SELECT_BD_ADDR. BD_ADDR will then remain fixed until the manual switch is set so that SELECT_BD_ADDR is enabled again.

Optionally, the triggering unit TRIG_SELECT_BD_ADDR may also be connected to activate the selecting function 13 when sensing a hard reset of the unit. The Reset command may be induced in various manners described in the Bluetooth specification, or by a manual switch.

Generally, a group of Bluetooth compatible units having address switching units as described above can share a group of BD_ADDR addresses with each other. Then the address switching unit 1 of each of the Bluetooth units of the group will select the temporary BD_ADDR from the same group at all times, thus making it impossible to say which Bluetooth compatible unit is using a certain BD_ADDR at each moment. In such a group the units share addresses only with each other, thus avoiding BD_ADDR conflicts with regular Bluetooth units.

The switching of device address is done in such a way that it does not violate the Bluetooth communication protocol of other units at any given time, thus making it impossible for a regular Bluetooth unit to distinguish between a Bluetooth compatible unit having an address switching unit and a regular Bluetooth unit at any time.

For example a number of BD_ADDR addresses can be reserved, forming one or several address groups. Each Bluetooth compatible address switching unit is instructed to choose every BD_ADDR only from one such group. Conflict can then arise only if two Bluetooth compatible units having address switching facilities selecting addresses from the same group are in direct communication range of each other and use the same BD_ADDR at the same time. Since the BD_ADDR determines the frequency hopping procedure, they may jam the communication. Other identity conflicts will in principle occur simultaneously on higher levels.

But due to the short-range Bluetooth radio communication distances, less than a few hundred meters, the risk of such a conflict can be made very small by setting the number of BD_ADDR addresses in an address group some orders of magnitude larger than the largest number of address switching units using the same address group expected to be within the maximum communication distance of each other.

In all cases, a conflict - however improbable - will be solved when the conflicting address switching devices select new fixed device addresses BD_ADDR or if the communicating devices are programmed to sense the conflict and then trigger a new choice of BD_ADDR.

Communication may be maximally preserved by offering the address switching unit that first chose the BD_ADDR used by the two units to be the last one to switch away from it, for example by setting the default time limit for each unit before switching BD_ADDR proportional to the time that the BD_ADDR has been used by the unit.

CLAIMS

1. A method of communicating between devices including the steps of:
- 5 - a first device transmitting wirelessly a first message inquiring whether there are other devices in the neighbourhood,
 - at least one second device responding to the message by transmitting wirelessly a second message,
 - the first and second devices setting up a communication link between them, and
 - 10 - the first and second devices interchanging information over the communication link,
 - in at least some of the first and second messages and in the setting up and interchanging information first addresses being used to define the first and second devices,
 - 15 **characterized by** the additional step of selecting, before transmitting any message or information containing one of the first addresses of the first and second devices the respective first address from a predetermined group of addresses.
- 20 2. A method according to claim 1, **characterized in** that the selecting is made at random.
3. A method according to claim 1, **characterized in** that the selecting is made when a device becomes unconnected to any of the
25 other devices.
4. A method according to claim 1, **characterized in** that the selecting is made when a device is reset or started.
- 30 5. A method according to claim 1, **characterized in** that in the step of setting up a communication link, second, local addresses are assigned to the first and second devices.
6. An ad hoc wireless network of devices communicating with each
35 other, the devices having means for wirelessly transmitting and receiving information, a first address of each device being used to define the device when connecting to the network and/or transmitting information, **characterized in** that each device includes an address switching unit for selecting the first address
40 from a predetermined group of addresses.

7. An ad hoc wireless network according to claim 6, **characterized in** that the address switching unit includes a generator for generating random numbers, a generated random number used in selecting the first address.

8. An ad hoc wireless network according to claim 7, **characterized in** that the address switching unit includes a triggering unit for starting selecting the first address, the triggering unit being connected to send a signal to start the selecting when the device becomes unconnected to the network.

9. An ad hoc wireless network according to claim 7, **characterized in** that the address switching unit includes a triggering unit for starting selecting the first address, the triggering unit being connected to send a signal to start the selecting when the device is reset or started.

10. A device having means for wirelessly transmitting and receiving information and for connecting to an ad hoc wireless network, a first address of each device being used to define the device when connecting to the network and/or transmitting information, **characterized by** an address switching unit for selecting the first address from a predetermined group of addresses.

25

ABSTRACT

A device having circuits (3) for communication according to the Bluetooth specification deviates from the strict specification by not having a unique Bluetooth device address BD_ADDR. Instead, it
5 has an address switching circuit (1) that chooses the device address from a group of BD_ADDR addresses and stores it in a rewritable register (5). The address switching circuit switches the BD_ADDR stored in the register from time to time, for example triggered by specific events. The device can communicate without
10 any conflict with similar devices and with devices built strictly according to the Bluetooth specification. The switching of device address preserves privacy of the device.

15 (Fig. 4)

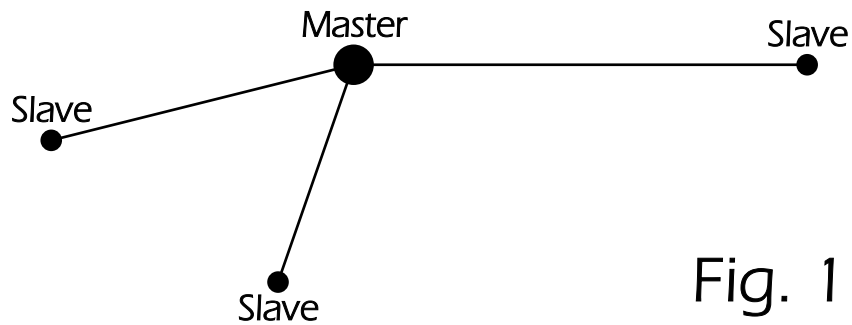


Fig. 2

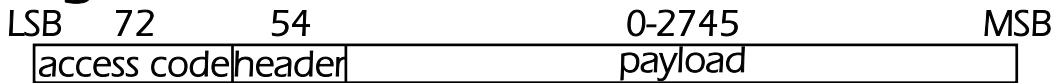


Fig. 3

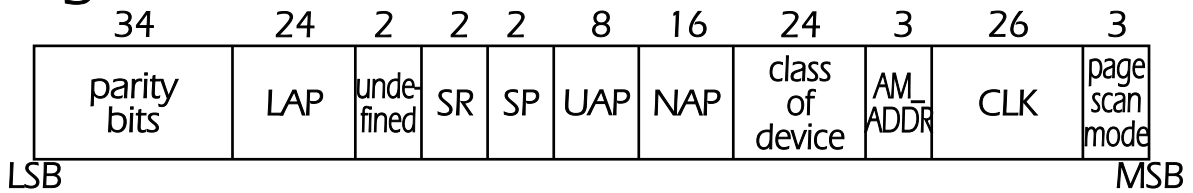


Fig. 4

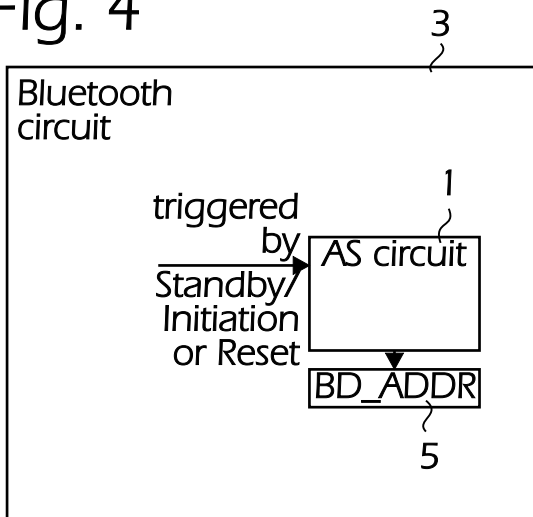


Fig. 5

