Identification of devices in Bluetooth networks

ZDENEK MIKESKA, STANISLAV HANUS, JOSEF VOCHYAN
Department of Radio Electronics
Brno University of Technology
Purkyňova 118, 602 00 Brno, Czech Republic

Abstract: - This paper presents the discovering of devices within range in Bluetooth networks described by the Bluetooth specification 1.1. This searching of other devices is performed using the inquiry communication procedure. In this procedure, the special hopping sequence derived from LAP of inquiry access code is used. The computation of this sequence was implemented in MATLAB for the purposes of procedure monitoring. The implementation accuracy was verified making the measurements in the real Bluetooth networks.

Key-Words: - Bluetooth, inquiry communication procedure, device discovering, modeling, MATLAB

1 Introduction

The inquiry procedure is used by the discovering device for searching the other Bluetooth device within range. In this case, the address and the clock of destination device are unknown. During this procedure, the source device transmits two ID packets in every transmitting time slot and listens to the FHS (Frequency Hopping Synchronization) packets in receiving time slots. Every founded device is stored into the source's device database. The inquiry hopping sequence is determined by the LAP (Lower Address Part) address from the Inquiry Access Code (IAC). The General Inquiry Access Code (GIAC) or the Discover Inquiry Access Code (DIAC) can be used. The GIAC is applied for searching all Bluetooth devices within range, the DIAC for searching the active devices within range. The LAP address of GIAC is 0x9E8B33 in hexadecimal notation. The LAP address of DIAC is chosen as 0x9E8B00 to 0x9E8B3F (63 hopping sequences). The inquiry sequence is divided into A-train and B-train, every with 16 hop frequencies. The A-train (B-train) is chosen when the parameter K_{OFFSET} is set up to 24 (8). The single train has to be repeated at least $N_{\mathrm{i}} = 256$, then the other train is chosen. The change of train is made by adding 16 to the current value of K_{OFFSET}. Within the inquiry procedure length, 3 changes have to be done. It corresponds to 10.24 s. Nevertheless, the procedure can last shorter or longer time.

The inquiry scan state is entered by the device that want be discovered. This device listens to the GIAC or DIAC at single hop frequency during the scan window last. This scan window $\mathrm{T}_{\mathrm{WINQUIRYSCAN}}$ has to cover 16 hop frequencies. Then the single hop frequency is changed. The period of change is 1.28 s. It corresponds to $\mathrm{CLKN}_{16\text{-}12}$. The inquiry scan sequence is determined by the LAP address from the GIAC.

The inquiry response state is only related to the destination device. The source device doesn't send a response. If the scanning device receives the ID packet, it transmits the FHS packet at the corresponding hop frequency after the RAND time slots are expired. The RAND represents the random number 0-1023 generated after the ID packet has been received. This number is used for the purposes to prevent the collisions.

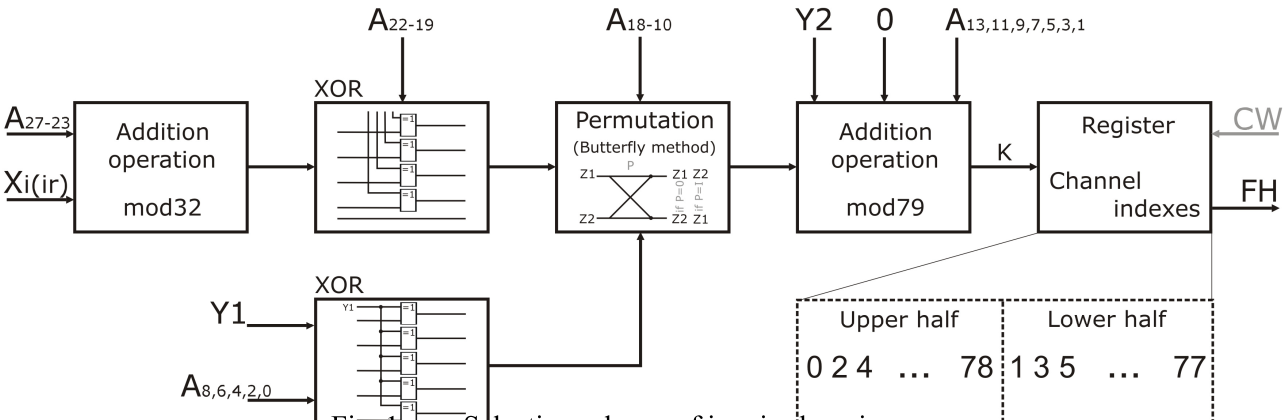

Fig. 1: Selection scheme of inquiry hopping sequence

2 Inquiry Procedure

The inquiry sequence is calculated pursuant to the selection scheme. The scheme is illustrated in Fig. 1. The address A is constructed from the LAP address of IAC and from the Default Check Initialization (DCI) 0x00. The length of address is 28 bits ($A_{27\text{-}0}$). The input X is determined by the following expressions (1), (2):

$$Xi_{4-0} = \left(CLKN_{16-12} + K_{OFFSET} + CLKN^{*}\right)\text{mod}\,32 \qquad (1)$$

$$CLKN^{*} = \left(CLKN_{4-2,0} - CLKN_{16-12}\right)\text{mod}\,16 \qquad (2)$$

$$Xir_{4-0} = \left(CLKN_{16-12} + N\right)\text{mod}\,32 \qquad (3)$$

The parameter Xi corresponds to the inquiry sequence, Xir corresponds to the inquiry scan and inquiry response sequence. The CLKN represents the native clock of the inquirer. The K_{OFFSET} determines the choice of the A-train (B-train). The parameter N presents the counter and could be accomplished according to the inquiry response FHS packet transmitting. The initial value of N is arbitrary. It's generally set up to 0.

The address $A_{27\text{-}0}$ specifies the segment of hop frequencies. These frequencies aren't stored but are progressively calculated and visited pursuant to the actual value of Xi (Xir) input. In Table 1, there are stated the values of Xi, Y1 and Y2 inputs in the inquiry, inquiry scan and inquiry response states. Dev1 presents the inquirer, Dev2 presents the discovered device.

	Dev1	Dev2	
Mode	Inquiry	Inquiry Scan	Inquiry Response
Xi(ir)	$Xi_{4\text{-}0}$	$Xir_{4\text{-}0}$	$Xir_{4\text{-}0}$
Y1	$CLKN_1$	0	1
Y2	32x $CLKN_1$	0	31x1

Table 1: The values of Xi, Y1 and Y2 inputs in a discover procedure

The inquirer device (Dev1) transmits ID packets with IAC at frequencies which are generated pursuant to the address $A_{27\text{-}0}$ (LAP, DCI) and the Xi value (1). The frequency is changed every 312.5 μs ($CLKN_0$). The $CLKN_1$ distinguishes the transmitting ($CLKN_1$ = 0) or receiving ($CLKN_1$ = 1). The segment of 16 transmitting frequencies and 16 receiving frequencies is available during 10 ms (16 time slots). When the $CLKN_1$ = 1, the inquirer listens to FHS packet at two different frequencies corresponding to the inquiry response hopping sequence.

The device under discover mode (Dev2) scans to its IAC at frequencies which are generated pursuant to the address $A_{27\text{-}0}$ and the Xir value (3). The frequency change corresponds to the $CLKN_{12}$. The device stays at single hop frequency for 10 ms to cover 16 transmitting frequencies. If the device receives its IAC, it doesn't freeze the clock. It generates the random number from 0 to 1023 and waits until these random number time slots are expired. During these time slots, the device can perform other activities. Then it returns to inquiry response state and sends the FHS packet at the frequency calculated from the $A_{27\text{-}0}$ and Xir (3). The response has to be sent 625 μs after the ID packet was received.

In Fig. 2, there is illustrated the spectrum of inquiry hopping sequence used by Dev1. The axis y contents the help scale. Next time, it will present the transmit power in dBm. The spectrum will be created using FFT. In Fig. 3 and 4, there are stated the sequences using by Dev2.

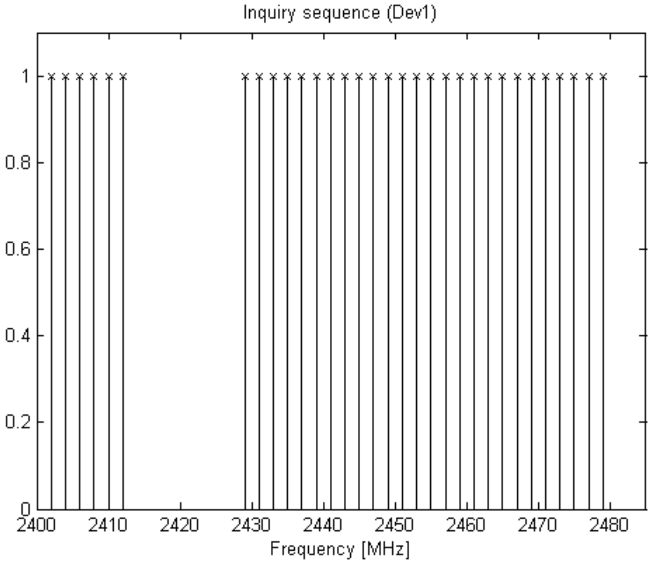

Fig. 2: Inquiry hopping sequence

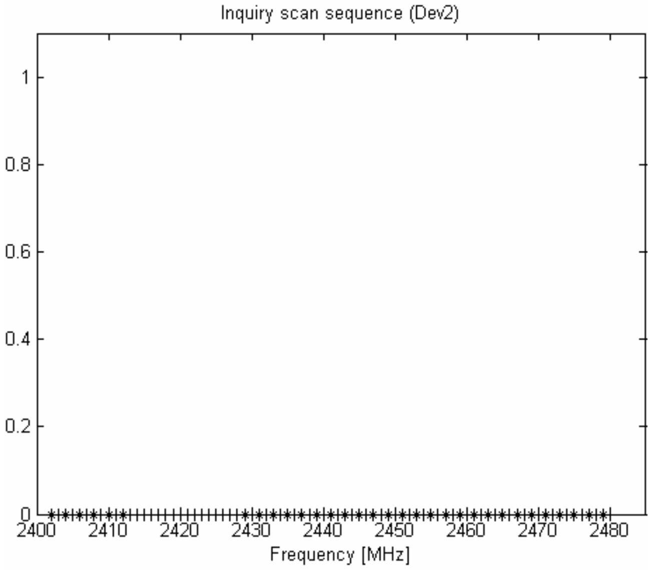

Fig. 3: Inquiry scan hopping sequence

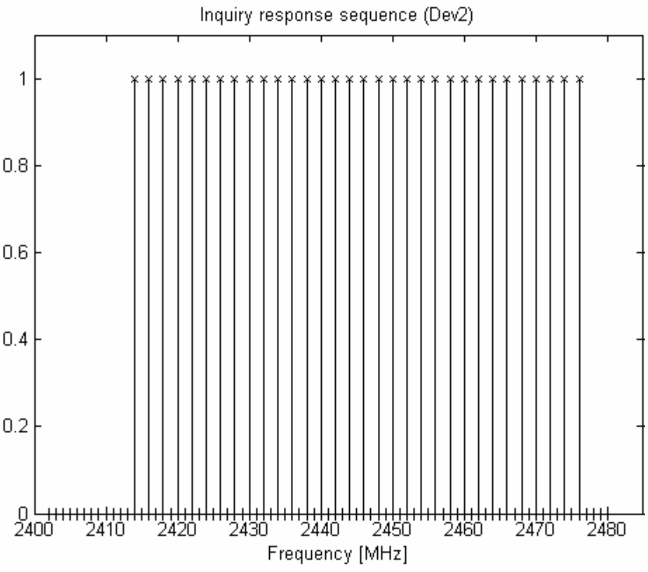

Fig. 4: Inquiry response hopping sequence

3 Procedure implementation, MATLAB

In this chapter, there are stated the main parts of program for the inquiry hopping sequence calculation.

. . .

```
%The selection scheme
%X parameter (The phase in sequence)
Sub=binsub(([CLKN(1) CLKN(3:5) 0]),(CLKN(13:17))
);Sub=Sub(1:4); %Mod16
Xi=bi2de(CLKN(13:17)) + (bi2de(Sub)) + Offset;
Xi=de2bi(Xi,6); Xi=Xi(1:5); %Mod32

%First addition operation (ADD1)
ADD1=bi2de(Xi) + bi2de(A(24:28));
ADD1=de2bi(ADD1,6);
ADD1=ADD1(1:5);

%First XOR operation (XOR1)
XOR1=[(xor(ADD1(1:4),A(20:23))) ADD1(5)];
z=XOR1;

%Second XOR operation (XOR2)
Y1=CLKN(2);
XOR2=[xor(Y1,A(1)) xor(Y1,A(3)) xor(Y1,A(5))
        xor(Y1,A(7)) xor(Y1,A(9))];

%Permutation operation (PERM5)
P=[A(11:19) XOR2]; %P(1:14)
 %Butterfly elements (7 stages)
 %1.stage (P14 {z2,z3}, P13 {z1,z4})
        if P(14)==1
                z_pom=z(2);
                z(2)=z(3);
                z(3)=z_pom;
        end
        if P(13)==1
                z_pom=z(1);
                z(1)=z(4);
                z(4)=z_pom;
        end
                              .
                              .
                              .
 %7. stage
        if P(2)==1
                z_pom=z(3);
                z(3)=z(4);
                z(4)=z_pom;
        end
        if P(1)==1
                z_pom=z(1);
                z(1)=z(2);
                z(2)=z_pom;
        end
PERM5=z; %Output of the permutation


%Second addition operation (ADD2)
Y2=CLKN(2)*32;
E=[A(2) A(4) A(6) A(8) A(10) A(12) A(14)];
ADD2=(bi2de(PERM5)) + Y2 + (bi2de(E)) + 0;
ADD2=de2bi(ADD2,8); ADD2=ADD2(1:7);

%K (Adressing of the Register of channel indexes)
K=bi2de(ADD2)+1;

%Hop Frequency sequence
if Y1==0 %TX
%DEV1 transmits
        if K>79
                K=K-79;%Mod79
        end
        Map=register;%Register of channel indexes
        Chnnl_idx1=Map(K);
else
%Dev1 receives
```

. . .

4 Measured Inquiry Sequence

The results obtained from MATLAB were necessary to check in practice. There was a need to prove the right of simulations. The measurement was made using the MS-6967 USB Bluetooth modules and the spectrum analyzer Advantest R3132. However, only the general inquiry hopping sequence was possible to measure with this spectrum analyzer, see Fig. 5. The inquiry scan hopping sequence and inquiry response hopping sequence wasn't possible to determine from technical reasons but it could suppose that the results of inquiry scan sequence and inquiry response sequence are correct.

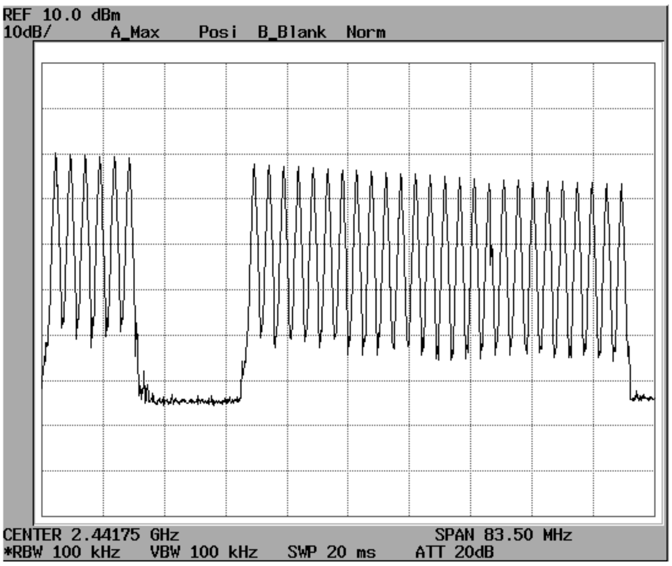

Fig. 5: Measured spectrum of general inquiry hopping sequence

5 Conclusion

The last of the inquiry procedure expressively influences the creation of connection if the neighborhood is unknown. So there is a tendency to short the last of the inquiry procedure. Using of IrDA in the discover mode is one of many possibilities. But this solution isn't very effective because of the line of sight between devices. This could be always used only between two devices. It is much better solution to short the period of change of single hop frequency (< 1.28s) or to extend the inquiry scan window to cover more inquiry frequencies than 16.

Acknowledgements:

This paper was supported by the grant of "Models of mobile networks and their optimalization" No. GA 102/04/2080 and "Bluetooth and WLAN wireless systems coexistence research" No. 2235/2005.

References:

[1] Morrow, R.: *Bluetooth Operation and Use*. The McGraw-Hill Companies, USA, 2002, ISBN 007138779X

[2] Bakker, D., Gilster, D.: *Bluetooth End to End*. USA, 2002, ISBN 0764548875

[3] Special Interested Group: *Bluetooth v1.1 Core Specification*. Websites of SIG, http://www.bluetooth.org, 2001

[4] Special Interested Group: *Test Specification for the Bluetooth System*. Websites of SIG, http://www.bluetooth.org, 2003