Specification of Radiocom 2000

0 Introduction

This document is an unofficial description of the Radiocom 2000 mobile standard. It is the result of reverse engineering. It is incomplete and several elements might be wrong. Please look at osmocom-analog source for implementation example.

The base station is called “Relais”, the mobile station is called “Station Mobile” or “SM”.

1 Radio

256 Channels are used in UHF band. Down-link frequency 424.800 MHz is used for channel 0 and 427.9875 MHz is used for channel 255. (channel spacing 12.5 KHz) Up-link frequencies range from 414.800 MHz to 417.9875 MHz respectively. For complete list of frequencies, refer to osmocom-analog source code (src/r2000/r2000.c).

Pre-emphasis and de-emphasis is used on speech and 1200 Baud FFSK.

A syllabic 2:1 compandor is used in direction Relais to SM, according to ITU-T G.162. The unaffected level is 1500 Hz (???) deviation at 1000 Hz.

2 FSK Modulation

For call setup and release, FFSK with 1200 bits per second is used. Each bit starts with a sine wave at zero crossing . The frequencies are:

$$F_0 = 1800 \text{ Hz}$$

$$F_1 = 1200 \text{ Hz}$$

The frequency deviation varies, due to pre-emphasis. At 1500 Hz the deviation shall be ±1425 Hz.

During call, FSK with 50 bits per second is used. The frequencies are:

$$F_0 = 136 \text{ Hz}$$

$$F_1 = 164 \text{ Hz}$$

No emphasis is applied. The deviation shall be ±300 Hz.

3 Coding

Each frame consists of 21 bits of dotting: 101010101010101010101 and a sync word: 11100010010 followed by 176 bits (base station) or 144 bits (mobile station).

To protect the bits, a (6,19) Hagelbarger code is used. The initial bits of the coder’s shift register are set to 0. The initial bits of the decoder’s data shift register are set to 0 and check shift register are set to 1. For complete algorithm, refer to osmocom-analog source code (src/common/hagelbarger.c).

The message frames itself are 66 or 82 bits long. The last two bits are 0 and shall be ignored on reception. All other bits are sent MSB first.

4 Frames

4.1 Messages from base station to mobile

0: INSCRIPTION ACK

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmm-----ccc----DDDIII++---PT---
```

1: IDLE

```
V-CCCCCCCCRRRRRRRRRMMMMM-------------------------------------DDDIII++---PT---
```

2: PLEASE WAIT

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmm------------DDDIII++---PT---
```

3: ASSIGN INCOMING

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmmaaaaaaaa----DDDIII++---PT---
```

4: ASSIGN INCOMING (GROUP)

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrfffffffffmmmmmmmaaaaaaaa----DDDIII++---PT---
```

5: ASSIGN OUTGOING

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmmaaaaaaaa----DDDIII++---PT---
```

9: RELEASE ON CC

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmm------------DDDIII++---PT---
```

16: IDENTITY REQ

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmm------------DDDIII++---PT---
```

17: INVITATION

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmm-----nnniiiiDDDIII++---PT---
```

24: RELEASE ON TC

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmm------------DDDIII++---PT---
```

26: SUSPEND REQ

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmm------------DDDIII++---PT---
```

4.2 Messages from mobile to base station

0: INSCRIPTION REQ

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmmsssssssssssss
```

1: CALL REQ (PRIVATE)

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmmsssssssssssss
```

2: CALL REQ (GROUP)

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrfffffffffmmmmmmmddddddddsssss
```

3: CALL REQ (PUBLIC)

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmmsssssssssssss
```

6: RELEASE ON CC

```
V-CCCCCCCCRRRRRRRRRMMMMMttttrrrrrrrrrmmmmmmmmmmmmmmmmm-------------
```

16: IDENTITY ACK

```
V-CCCCCCCCRRRRRRRRRMMMMMtttrrrrrrrrrmmmmmmmmmmmmmmmmm------------
```

17: ANSWER

```
V-CCCCCCCCRRRRRRRRRMMMMMtttrrrrrrrrrmmmmmmmmmmmmmmmmm-----------
```

19: DIAL 1..10

```
V-CCCCCCCCRRRRRRRRRMMMMM1111000033332222555544447777666699998888
```

20: DIAL 11..20

```
V-CCCCCCCCRRRRRRRRRMMMMM1111000033332222555544447777666699998888
```

24: RELEASE ON TC

```
V-CCCCCCCCRRRRRRRRRMMMMMtttrrrrrrrrrmmmmmmmmmmmmmmmmm-----------
```

26: SUSPEND ACK

```
V-CCCCCCCCRRRRRRRRRMMMMMtttrrrrrrrrrmmmmmmmmmmmmmmmmm-----------
```

4.3 Information elements

A dash (-) states that this bit shall be transmitted as zero and ignored on reception. A plus (+) states that this bit shall be transmitted as one and ignored on reception.

V: Channel Type

Relais to SM: Set to 1 for messages on control channel and 0 for messages on traffic channel.

SM to Relais: Set to 0 for messages on control channel and 1 for messages on traffic channel.

C: Channel number

Defines the channel number 0..255. The corresponding frequency is 424.800 MHz (Relais) and 414.800 (SM) for channel 0. The frequency step per channel number is +12,5 KHz.

R: Base station ID

Defines the Base station ID of the base station. Ranges from 1..511.

M: Message type

The code as shown above with the message definitions.

D: Deport (TBD)

I: AGI

Inscription parameter:

0 = Prohibited control channel (no mobile allowed)

1 = New registration prohibited (registered mobiles allowed)

2 = Registration is reserved to test mobiles

3 = Registration for nominal mobiles (home network)

4 = Registration is reserved to special mobiles

5 = Reserved (treat as 7)

6 = Reserved (treat as 7)

7 = Registration permissible for all mobile station

P: Power
0 = low Power

1 = high Power

T: Taxe (TBD)

t: Type of SM
1 = Public

(TBD)

r: Home base station ID
Home base station ID of the subscriber. This is used for roaming. 1..511.

f: Mobile Flotte
Identifies the mobile group within its home network.

m: Mobile ID
Identifies the station mobile within its home network.

d: Called Flotte
Called mobile group.

c: CRINS
Response to inscription of the mobile:

0 = Finished or just registering

1 = Localization impossible (queue full)

2 = Mobile station temporarily disabled

3 = Mobile station definitely disabled (WILL BRICK THE PHONE!)

4 = Blocked localization (BS out of order)

5 = Reserved

6 = Reserved

7 = Calling subscriber unknown

Note: Using 3 will destroy the phone. The manufacturer or service can only unlock the phone. Never use this response! I told you – NEVER, unless you know what you doing!

a: Assigned Channel
Channel number, which is assigned to the station mobile.

s: Sequence Number (TBD)

n: NCONV
3 Bit binary information that is transmitted during speech via 50 Baud Modem.

i: Invitation
3 = Invitation to answer (invitation à décrocher)

10 = Invitation to dial (invitation à numéroter)

0-9:
Digits of the dialled phone number.

5. Protocol

5.1 Inscription (Registration)

Inscription tells the base station where the mobile station is located. Whenever the mobile station selects a base station with a different ID (R), the mobile will register to this base station using INSCRIPTION REQ message on control channel.

When the base station receives INSCRIPTION REQ message, it acknowledges with INSCRIPTION ACK message. The CRINS information element contains the result of inscription.

When the mobile station receive INSCRIPTION ACK message, it will act upon CRINS information element.

If the INSCRIPTION ACK message is not received within 4 (???) seconds, it will repeat the INSCRIPITON REQ message two more times. Then it will do the cell search again.

5.2 Channel assignment

There are three situations where a channel is assigned:

- Base station calls mobile station (incoming call)
- Mobile station calls base station (outgoing call)
- Base station calls back the mobile station (recall)

When the mobile station initiates a call to the base station, it will request a channel. This causes a channel assignment toward the mobile station. After dialling the phone number, the connection is released until the called person answers. After answer, the mobile station is recalled.

The base station sends ASSIGN INCOMING (incoming call) or ASSIGNMENT OUTGOING (outgoing call or recall) on control channel and switches to the assigned traffic channel. There it sends IDENT REQ messages on traffic channel 4 times (??? continuously) and waits for IDENT ACK message on traffic channel. All communication is then done on traffic channel.

When the mobile station receives ASSIGN INCOMING or ASSIGN OUTGOING message, it switches to the assigned channel and waits for the IDENT REQ message. If it receives this message, it sends 3 IDENT ACK messages and waits for INVITATION message.

If the base station does not receive IDENT ACK message within 4 (???) seconds, it repeats the assignment procedure 2 (???) times.

If the mobile station does not receive IDEN REQ or INVITAITON message within 4 (???) seconds, it proceeds with the release process.

5.3 Incoming call

After assigning channel and invitation to answer, the base station waits for ANSWER message and sends a ring-back tone to the caller.

As soon as the mobile station receives INVITATION message, it sends a ringing tone to the subscriber.

When the subscriber answers, the mobile station sends 3 times the ANSWER message, removes the ringing tone and through-connects the auto path.

When the base station receives the ANSWER message, it will stop the ring-back tone and through-connects the audio path.

If the mobile station does not send the answer signal within 60 (???) seconds or the caller hangs up, the base station will proceed with the release process.

When the mobile station still receives the INVITATION message 4 (???) seconds after sending ANSWER message, it will proceed with the release process.

5.4 Outgoing call

The subscriber of the mobile station dials a phone number. The mobile station sends the CALL REQ message and waits 4 (???) for channel assignment procedure. This process is repeated up to three times. If all attempts fail, the cell search process is initiated.

After assigning channel and invitation to dial, the base station waits for DIALING 1..10 message from the mobile station.

As soon as the mobile station receives INVITATION message, it sends 3 times DIALING 1..10 message, followed by optional DIALING 11..20 message, if required.

When the base station receives the DIALING messages, it will continuously send SUSPEND REQ message and waits for SUSPEND ACK message.

If the base station does not receive the DIALING messages within 4 (???) seconds, it returns to idle state.

When the mobile station receives the SUSPEND REQ message, it will send 3 times the SUSPEND ACK message and returns to idle state, but waits for a call back assignment on the control channel.

When the base station receives the SUSPEND ACK message, it setups call to the dialled number and waits for answer.

If the mobile station does not receive the SUSPEND REQ message within 4 (???) seconds, it will proceed with the release process.

If the base station does not receive the SUSPEND ACK message within 4 (???) seconds, it will proceed with the release process.

The call to the dialled number is initiated by the base station. As soon as the called party answers, the recall assignment is initiated. The same channel assignment process is used again, but this time the mobile station is invited to answer the recall.

5.5 Call

During call, the mobile station and the base station sends 50 Baud FSK signal. The following pattern is repeated continuously:

```
010000000001rrrrnnn1
```

The 4 'r' bits represent the 4 lowest bits of the relais ID (R). The relais ID is sent LSB first. The 3 'n' bits represent the NCONV value, which was used in the INVITATION message. The NCONV is sent LSB first.

On the downlink (base station to mobile station), all seven 'r' and 'n' bits are inverted.

The bits must match!

If the mobile station receives the pattern initially, it starts the transmitter, if the bits match. Then it sends the pattern not inverted.

If the matching pattern it is not initially received within 4 seconds or if it is not received for 20 seconds, the release process is initiated.

5.6 Release

The base station initiates the release on control channel by sending RELEASE message 4 (???) times. Then the base station returns to idle state.

The base station initiates the release on traffic channel by sending RELEASE message continuously for ??? seconds or until the mobile station replies with the RELEASE message. Then the base station returns to idle state.

If the mobile station receives a RELEASE message or initiates the release process, it sends 4 (???) times the RELEASE message and returns to idle state.