



# Wimax protocol Synchronization and Initial Ranging with Real Time Developer Studio



Internship 2014  
ANDRES Elie  
ESIEE Paris

# Table of Contents

Introduction.....	3
Synchronization.....	4
Process Base Station.....	4
Start Base Station.....	4
Creation of the loop.....	5
Creation and sending the messages recursively.....	6
Uplink Channel Descriptor message.....	6
Downlink Channel Descriptor message.....	9
Uplink Map message.....	9
Downlink Map message.....	10
Process Suscriber Station.....	11
Initiate connection.....	11
Synchronizing the Downlink Channel.....	11
Scanning for Downlink channel.....	11
Waiting the DL_MAP.....	12
Changing channel.....	13
Synchronization.....	14
Synchronizing the UL Channel.....	18
Uplink parameters.....	18
Uplink validation.....	19
Ranging.....	21
Initiate Ranging.....	21
From the SS.....	21
From the BS.....	21
From the Suscriber Station.....	22
Sending RNG REQ.....	22
waiting RNG RSP.....	23
Receiving Ranging Response message.....	24
RNG RSP continue.....	25
RNG RSP abort.....	25
RNG RSP success.....	26
From the Base Station.....	27
Receiving Ranging Request message.....	27
Initial ranging.....	28
Conclusion.....	32

# Introduction

The WIMAX is a wireless communication standard, known as the IEEE 802.16 standard.

This project is based under the assumption that the modulation method is under wirelessMAN\_OFDM mode.

The OFDM (Orthogonal frequency-division multiplexing) characterizes the frequential mode adapted to the differents channels.

In this case we modelised a procedure concerning the entry of a subscriber into the network.

To do so, we first created a Suscriber Station and a Basic Station.

- The Susciber Station (SS) is an equipement providing connectivity between the subscriber and Base Station.
- The Base Station (BS) gives the point of access of the network. He manages the differents messages and has a control over the Suscribers Stations.

Here, we are interested in the first approach beetwen these two stations. In the wimax procedure the initialization is set by an exchange of peculiar messages, called "Mac Management Messages", between the BS and the SS.

- The first part concerne the synchronization beetwen the two stations, allowing the specifics channels they would use.
- Then we will show the "ranging" part, concerning the charasteristics the BS want the SS to be submit.

# Synchronization

This part concerns the synchronization for the wimax protocol between a Base Station (BS) and a Subscriber Station (SS).

The synchronization has only one purpose. To determine on which channel the two stations can communicate. Therefore, to check if the characteristics of the channel are supported by the SS.

## Process Base Station

The goal of the Base Station is here to send on different frequencies (called channels) 4 "management messages" that indicate the ways to use these channels.

In order to represent the Base Station trying to establish a contact for all the channels he is responsible for, we create a loop inside which the process sends messages on all the targeted frequencies.

### Start Base Station

When the process Base\_Station is starting, he stops instantaneously in a state called "Begin synchronization".

In order to continue, a message must be sent from the environment (the user). The message "Begin\_BS\_Synchronization" allows the process to send his own messages automatically.

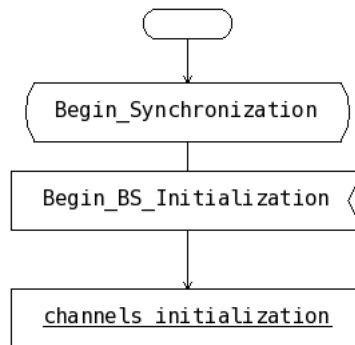
Here, we need to synchronize the Base Station with a Subscriber Station. To do so, the Base Station must be able to communicate on all the wanted channels in a determined lapse of time.

They are defined in the task block "channels initialization".

But the different channels have some specifications the messages must respect. Here we choose a simple model on which, each channel has 3 characteristics resumed in an Array:

- The first one represents if the channel supports TDD or FDD. TDD represents the possibility for a Base Station and a Service Station to exchange their messages on the same channel. At the opposite, FDD shows the impossibility to discuss at this frequency from the Base Station to the Service Station and the other way around.
- The second one shows if the capacity of coexistent frames is possible on the channel. This means that the channel can support several Service Stations. It's a contention based channel.

- The third one is the number of stations connected on this channel. It is limited to 4 for the contention/coexistence-frame based channel, to 1 for the others.



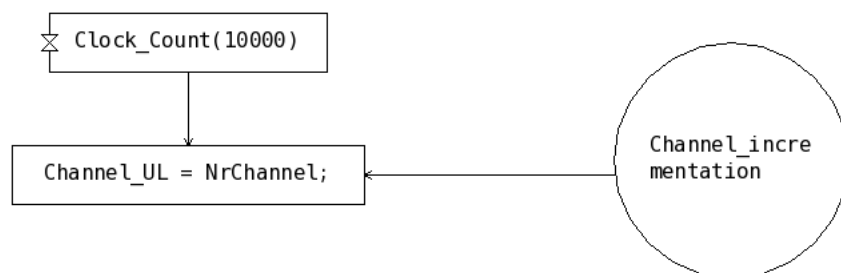
The informations concerning the arrays cannot be changed, each channel has its proper characteristics.

## Creation of the loop

Beginning of the loop:

This loop must respect two constraints:

- Sending the same message on the same channel, must be within 10 sec. That's why we fix a timer indicating when to restart to send messages.
- The number of the channel "NrChannel" is an important information. The number of the channel indicates where is the middle frequency of the transmission.



Here we fix at the beginning of each loop the proposed uplink channel (for the communication from the Subscriber Station to the Base Station) as the same as the Downlink channel. We will see how it can be changed further in the process.

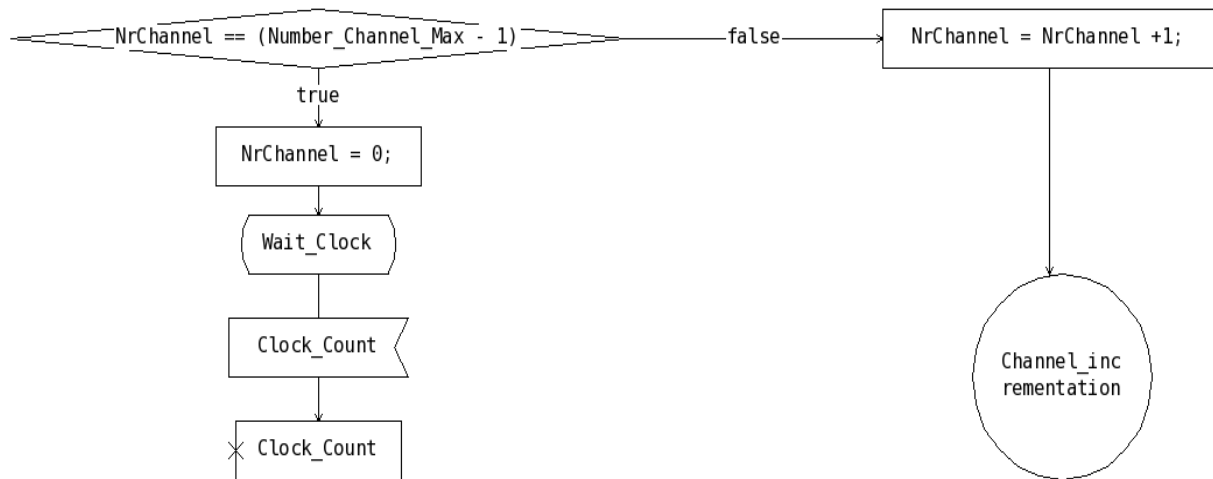
Incrementation in the loop :

Knowing that BS must send some messages on all the channels he is responsible for, we compare after he sent the wanted messages on a channel if this peculiar channel is the last one he has to deal with.

(The NrChannel beginning to 0, the last channel will be the one equal to the Nr\_Channel\_Max -1).

If the NrChannel is not the last in the list, we increment his value in order to send on the next one all the messages BS have to transmit.

If it is the last BS is occupied with, the NrChannel is fixed at the beginning of the list (here = 0) and we wait the 10 sec needed by the BS before he can send again on his frequencies. Then we return at the beginning of the loop, re-starting the timer for the next loop.



The BS will send for each declared channel the wanted messages and will do this operation every 10 seconds.

## Creation and sending the messages recursively

### Uplink Channel Descriptor message

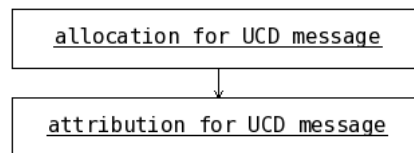
UCD presentation:

The UCD message or "Uplink Channel Descriptor" is the message containing the characteristics of the channel on which the Subscriber Station can send messages to the Base Station.

First of all, we have to allocate the memory needed for the message, then we can give him the values of the different types we have to carry. It will be the same for all the messages.

He includes a number of "burst profiles" containing informations usefull for the future messages to send.

I.e: the different mode of access supported.



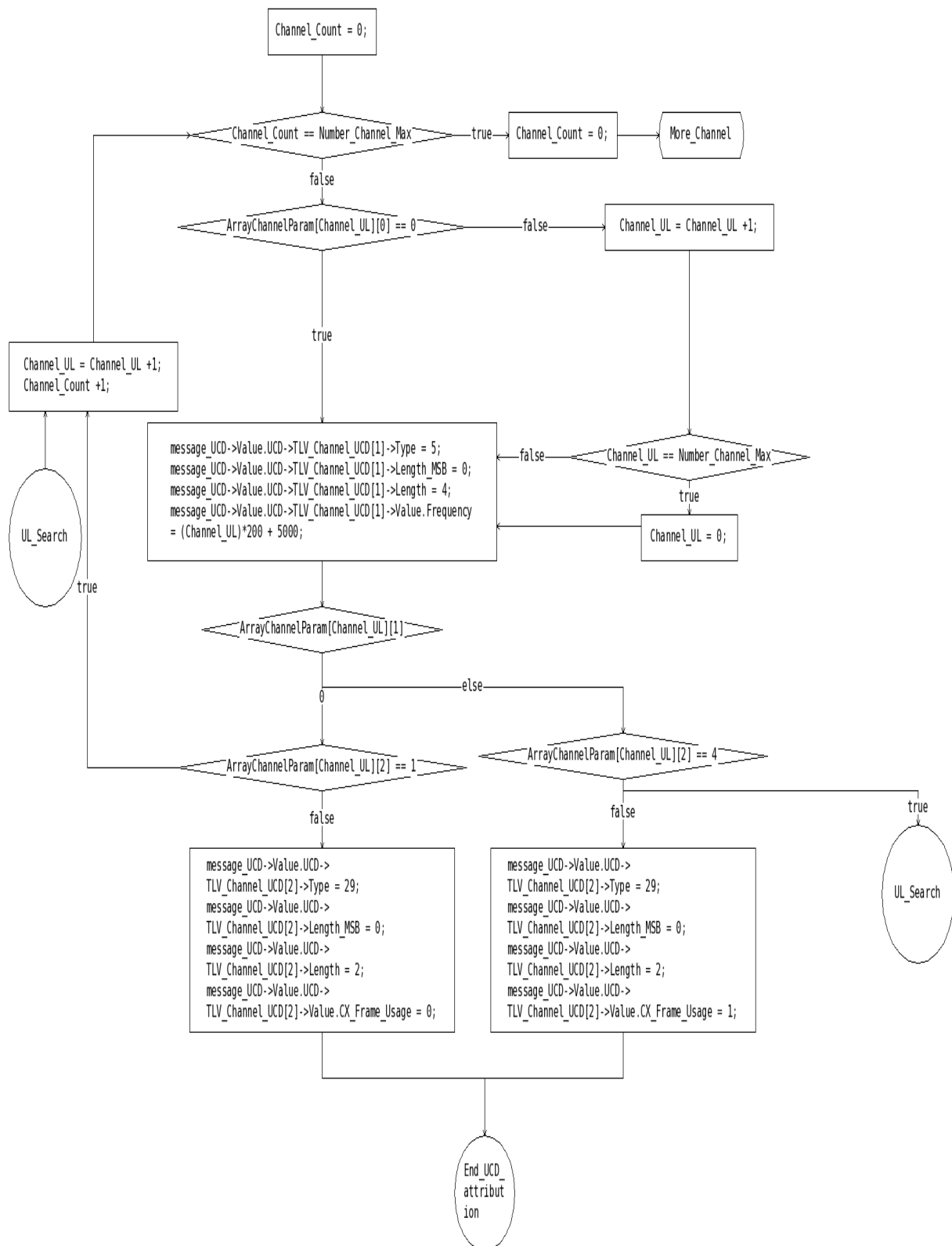
The channel described isn't necessarily the same as the one the UCD message is send on. It depends on the charasteristics given for this frequency.

Charasteristics given to the uplink channel:

This part represents the choices that are made for describing to the Service Station the capacities of the channel on which he can send messages.

Two importants types can change according to the channel they are on. The frequency to transmit, informing if the SS has to go on another channel to transmit. And if this frequency accept multiple SSs.

The informations of the channels are given in the Array that we declared at the beginning of the process.



First we test if both, the BS and the SS can communicate on the same frequency.

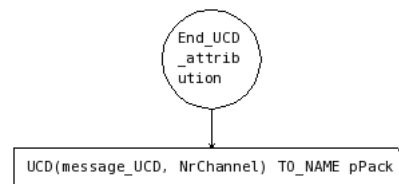
- If yes, we send the frequency corresponding to the number of the channel on which we send the message.
- If not, we check the next possible frequency for the Uplink channel.



Then we check if the the Uplink channel given accept several SS to communicate with the BS.

We allo the type CX\_Frame\_Usage to 1 when it his possible, to 0 when not. Respectively, The cohexistent frame can accept to 4 inoccupants, the non-cohexistant one only 1.

Furthermore, if none of the present channel is convenient, we are placed i the state "More\_Channel" indicating the need of new channel or different characteristics.



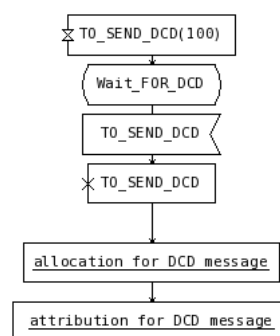
At last, when all the differents parts of the message are given, we can send it on the specific Downlink Channel.

The frequency of the channel, being a physic data, is unregistered in the UCD message, we add it for the synchronization to the message.

### Downlink Channel Descriptor message

DCD message or Downlink Channel Descriptor is the message giving the different characteristics of the channel on which this message is transmitted.

He is send approximatly at the same time at the UCD message. Here, 100 ms after. He indicates at the Suscriber Station what is the exact used frequency, the number of the channel, the available radio ressources...



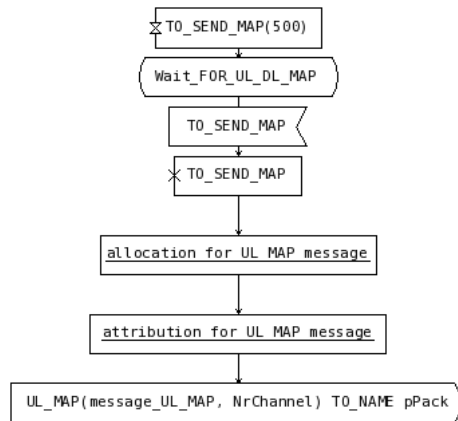
Same as the UCD message he also have "burst profiles" containing informations needed for future uses.

### Uplink Map message

The Maps messages are send a little bit after the Channel Descriptor

messages.

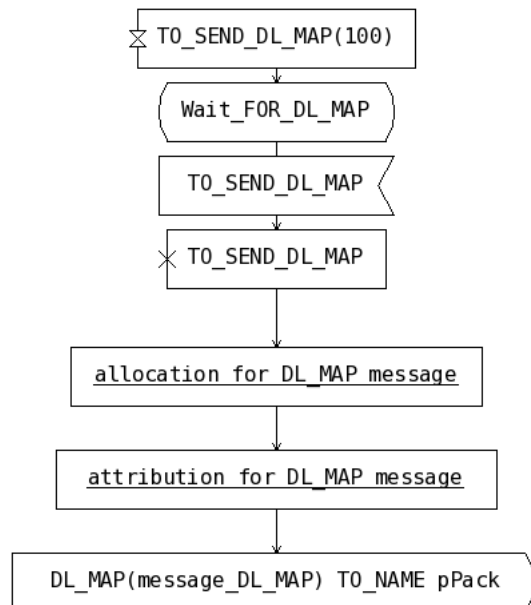
The UL\_MAP message allocates access to the UL channel, he is dependent for the synchronization of the the UCD message, therefore must have the same identifier as him (called UIUC).



This message contains some Informations Elements which are PHY-specifics. They are not relevant in our case.

### Downlink Map message

The DL\_MAP message is mandatory for the synchronization, he is the only message containing the mandatory for the Downlink Channel. He must be recieved at least one by the Suscriber Station in order to proceed.



This message contains some Informations Elements which are PHY-specifics. They are not relevant in our case.

## Process Suscriber Station

At synchronization, the Suscriber Station can only recieve messages on a channel of his choice and see if this channel is convenient for him.

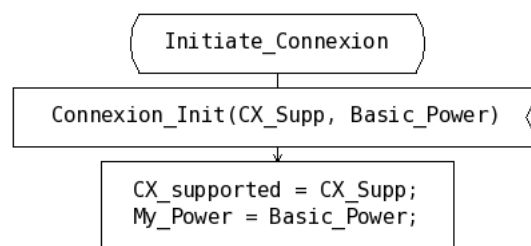
### Initiate connection

At the beginning of the initialization, we have to give this process two characteristics.

The first one, CX\_Supp indicates if the SS want or can support the partition of a channel between him and other(s) SS.

0 = CX non supported, 1 CX supported.

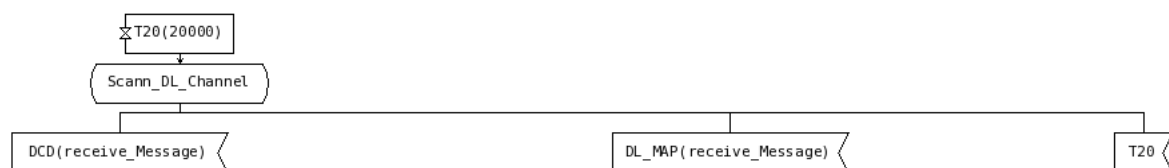
The second one, Basic\_Power indicates the power with which the SS is going to send his first message.



### Synchronizing the Downlink Channel

#### Scanning for Downlink channel

In order to initiate the synchronization with a BS, the SS tries arbitrarily a channel. Here we beginn with the first of the stack: Channel\_Num = 0.

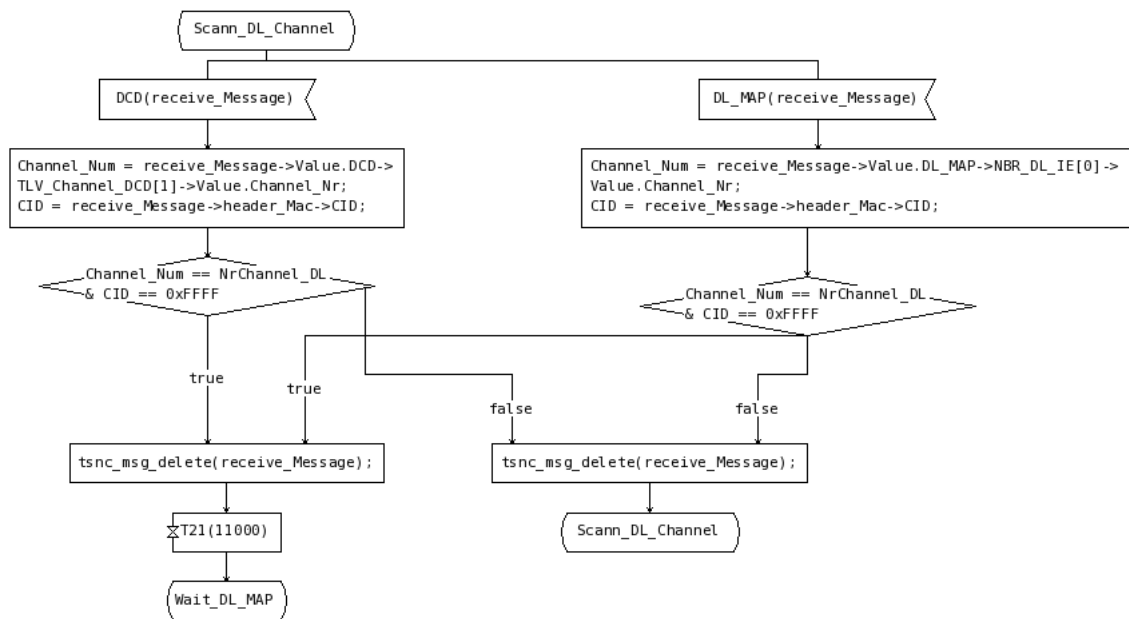


Then, the SS fix a timer. If he doesn't receive within the time fixed a DCD or a DL\_MAP message, he must move and try the connection on the next channel.

When the SS has knowledge of a DCD or a DL\_MAP message at this stage, he must check two things:

- First, if the channel on which the message is send is the same as the one he chooses to inspect. If not, he musn't have receive this message and return to the state "Scann\_DL\_Channel" to look for the good one.

- The second condition concerns the SS if the channel is the one chosen by him. The CID included in the header of the messages must be a broadcast CID, otherwise this message isn't destined to him.



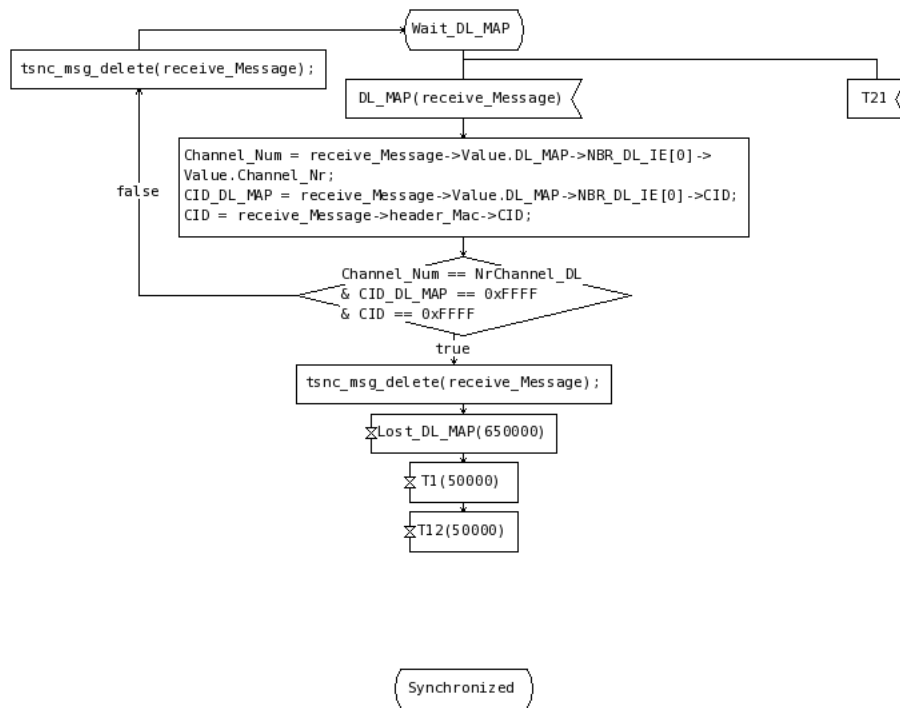
If all conditions are respected, the SS can go on to the next stage, and set a new timer.

### Waiting the DL\_MAP

The principle of the algorithm is basically the same as before.

Here, the SS searches to have only the DL\_MAP corresponding to the channel chosen before. For this, he checks if the number of the channel is the same, and if the CID contained in the header is a broadcast CID (=0xFFFF).

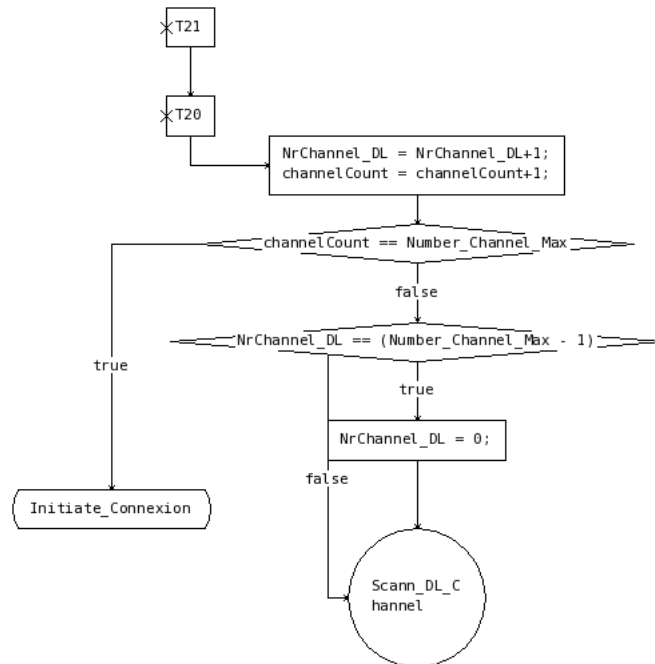
But he has to make sure that the CID of the DL\_MAP is also a broadcast CID. That indicates that the message that the SS receive isn't for another SS already connected.



At the end the SS set 3 timers each one corresponding to the future messages to receive, and pass to the state "Synchronized".

### Changing channel

When a timer expire (T20 or T21), that means that nobody is transmitting on this channel or that the channel isn't suitable.

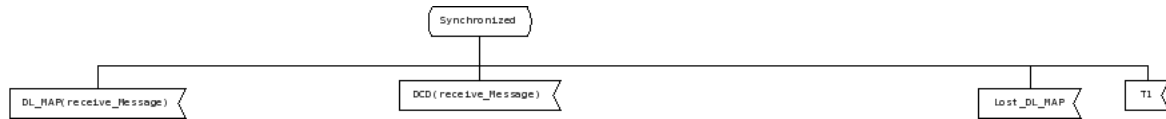


Therefore, we move to another channel by incrementing the channel number, and the SS will wait at state "Scann\_DL\_Channel" after he had set the timer.

If the SS has already check all the existant channels, he restart at the beginning and wait for a message from the environnement.

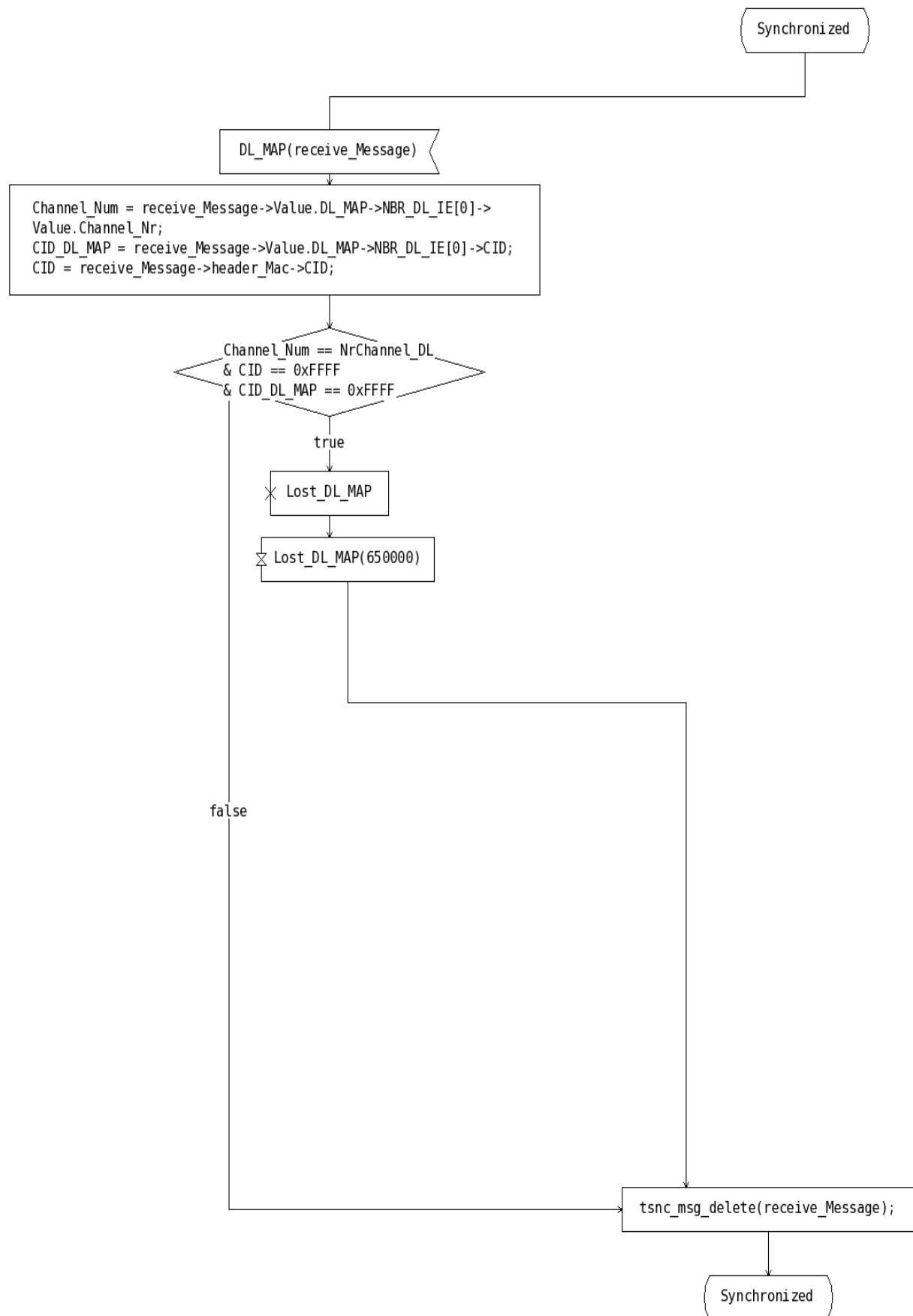
## Synchronization

When in the state "Synchronized" the SS should wait until he recieve a DCD message, a DL\_MAP message or one of the two timers has expired.



If the SS receive a DL\_MAP message corresponding as always to the good channel, with the good identifiers. He must reset the Lost\_DL\_MAP timer.

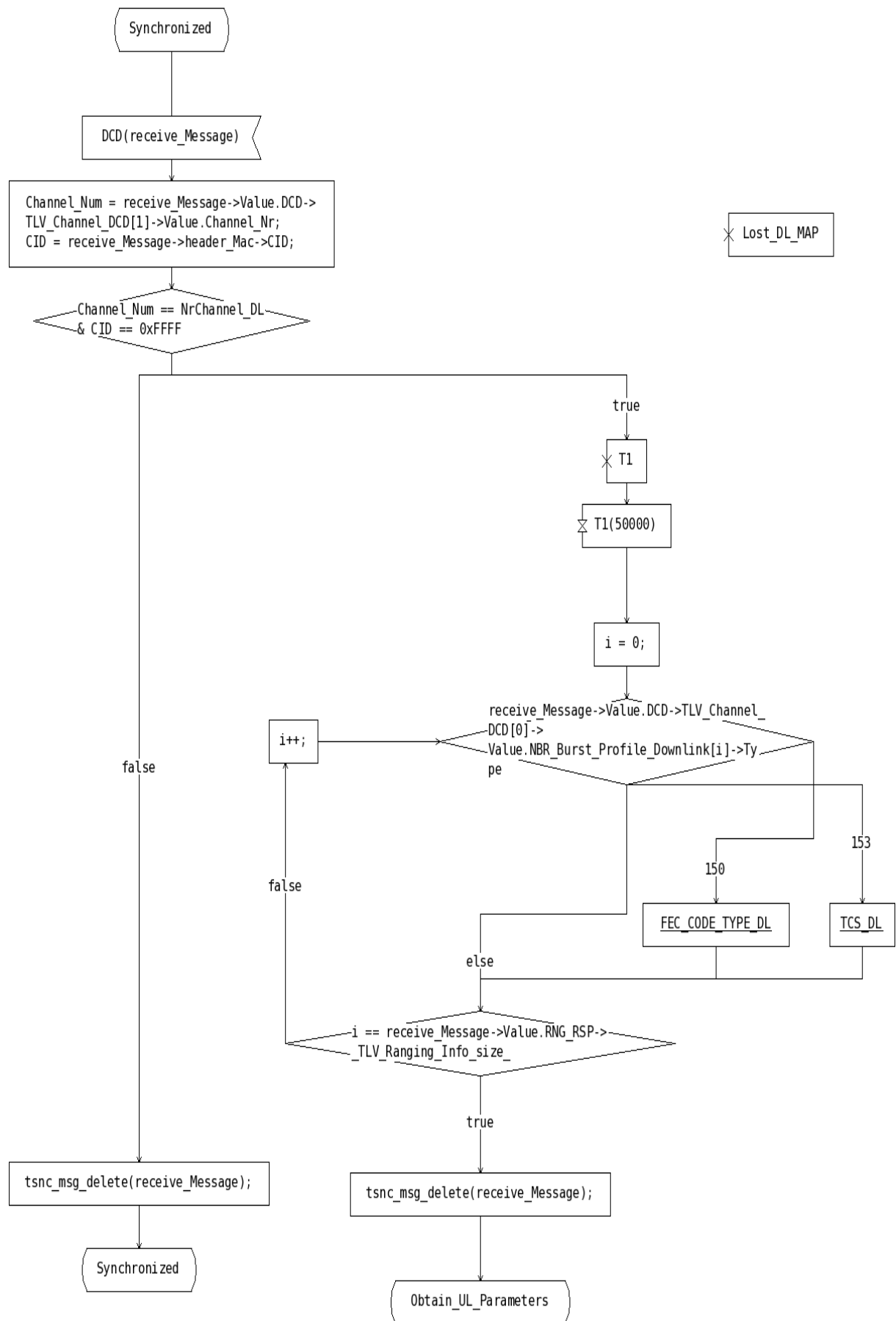
Otherwise, the message isn't taken into account.



Now the SS receive a DCD message. After checking if the message is destined to him, the SS has to register the different information that his contains in his "Burst Profiles".

For this we create a loop and fix the mode of access to this channel (FEC\_Code) and see if the upper layer, Transmition Convergence is enable (TCS\_enable).





After this, the synchronization with the downlink (from BS to SS) is over, we shall pass to the Uplink one.

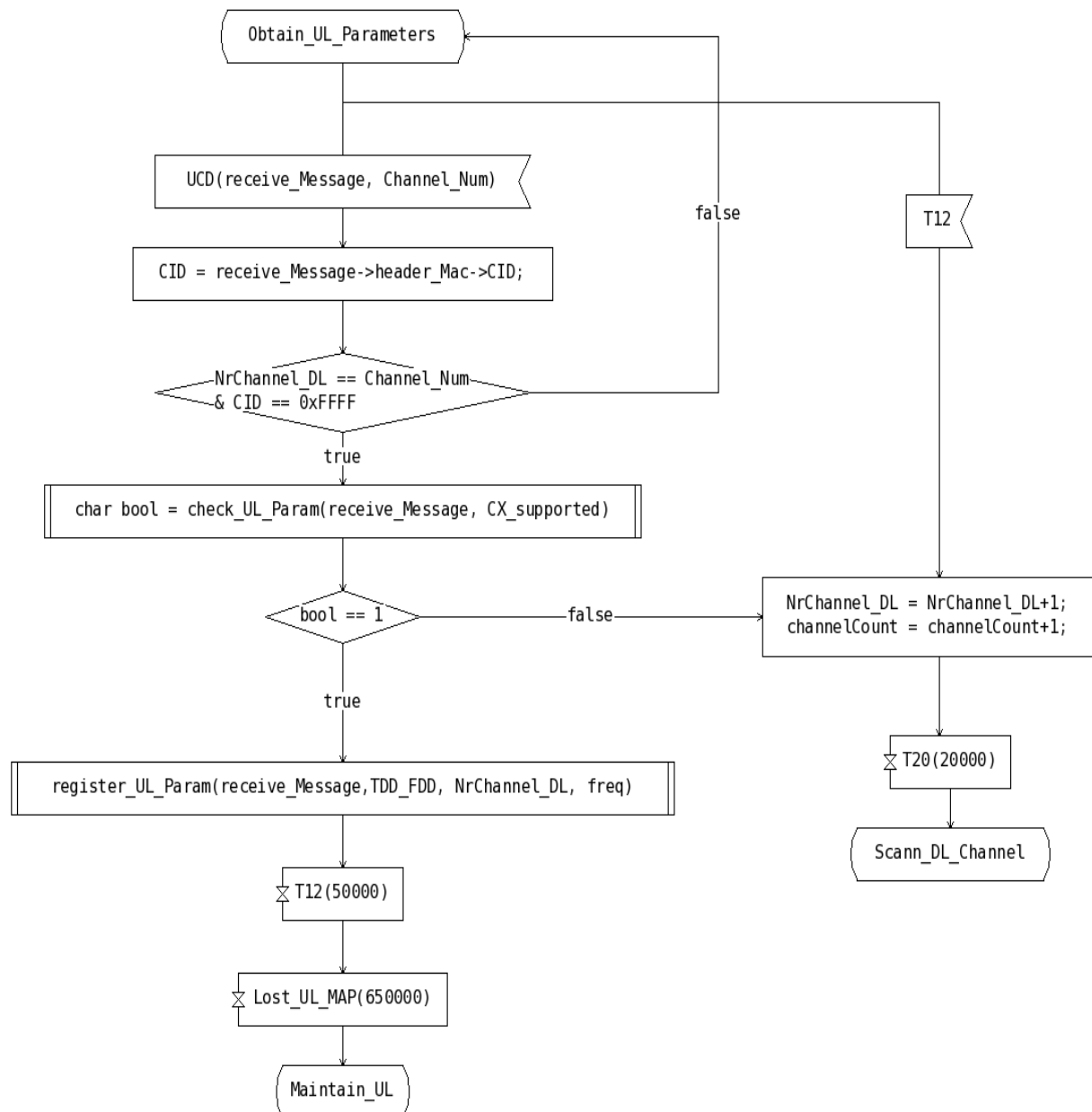
## Synchronizing the UL Channel

### Uplink parameters

The synchronization for the Uplink Channel is basically the same used for the Downlink one.

First of all, the SS must receive a UCD message.

- The SS checks if the parameters are convenient for him.
- He register the new frequency given in the UCD message.



If the parameters of the Uplink channel are not supported, he had to restart checking a new DL Channel.

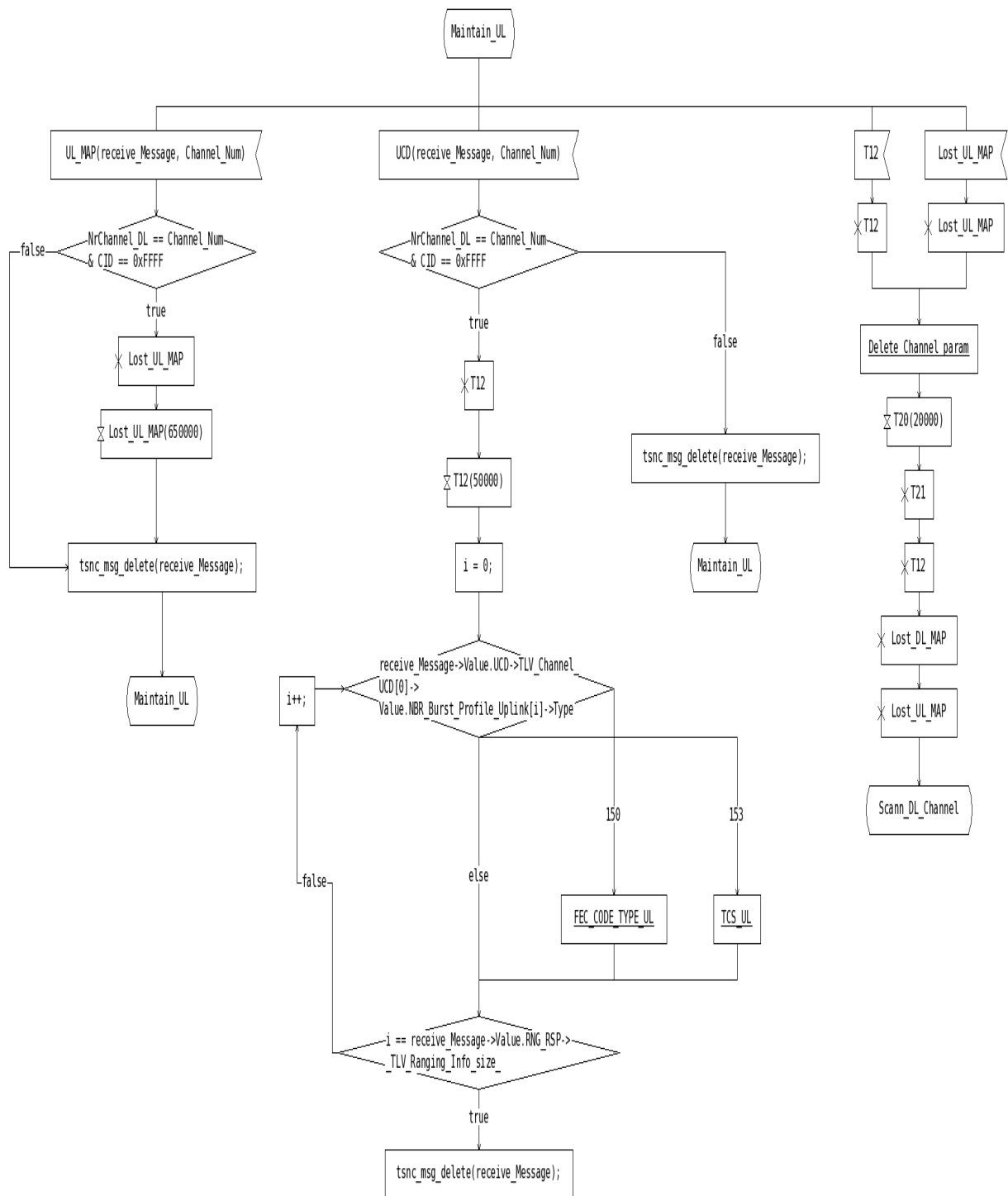
When he register the frequency, the SS deduct if that is the same channel as for the downlink and fill the variable TDD\_FFD (0 = TDD, 1 = FDD).

Finally he set two timers and wait for final informations.

### **Uplink validation**

In this part the SS does exactly the same as for the downlink channel when synchronization occurs.

He maintains the synchronization until he can register the different informations contains in the "burst profiles" of the UCD message.



Now the SS and the BS have finished synchronized, therefore they know on which channel(s) they communicates and how the can do it.

# Ranging

The ranging procedure is made for a better communication on the Uplink Channel chosen before.

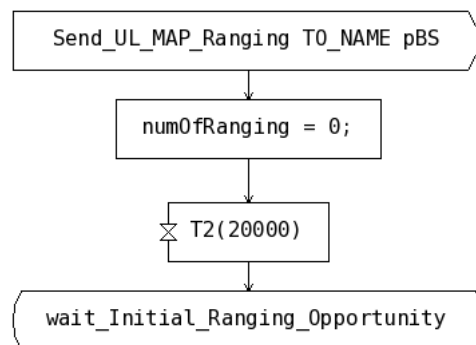
In order to have a better communication, the BS fixes some rules concerning the power needed. Furthermore he assigns identifiers (CIDs) in order to make the conversation easier.

## Initiate Ranging

### From the SS

When the choice of the downlink and uplink channels are over. The SS sends a fictional message to the BS.

This message doesn't exist in the protocol but allows the BS to stop sending useless messages continuously.

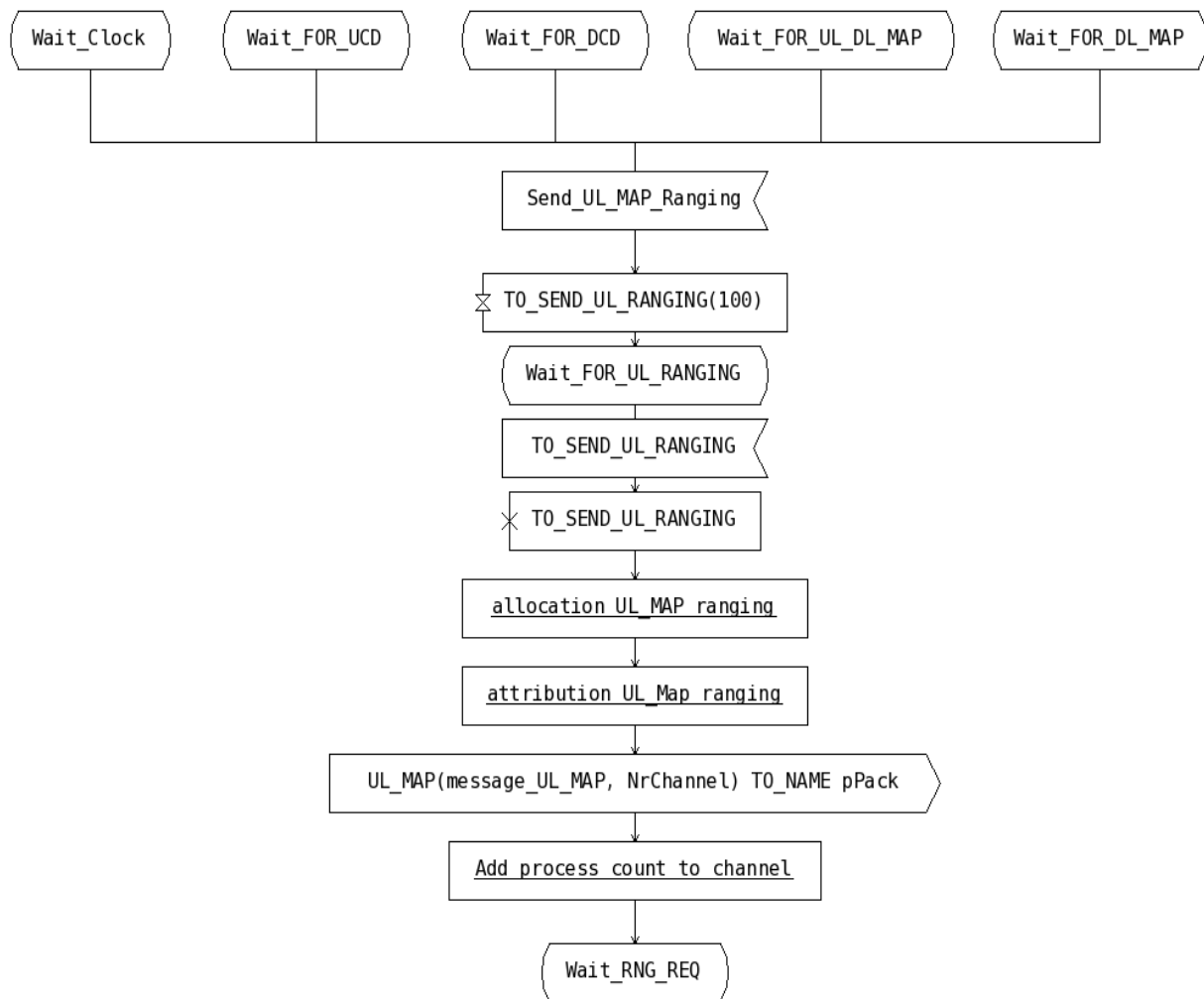


So the SS wait for an opportunity to send his next message.

### From the BS

Here, the BS can receive at any state in the loop the fictional message the SS sent him.

So he checks the last channel he was communicating on, sends the message UL\_MAP with a particular identifier allowing the beginning of the ranging.



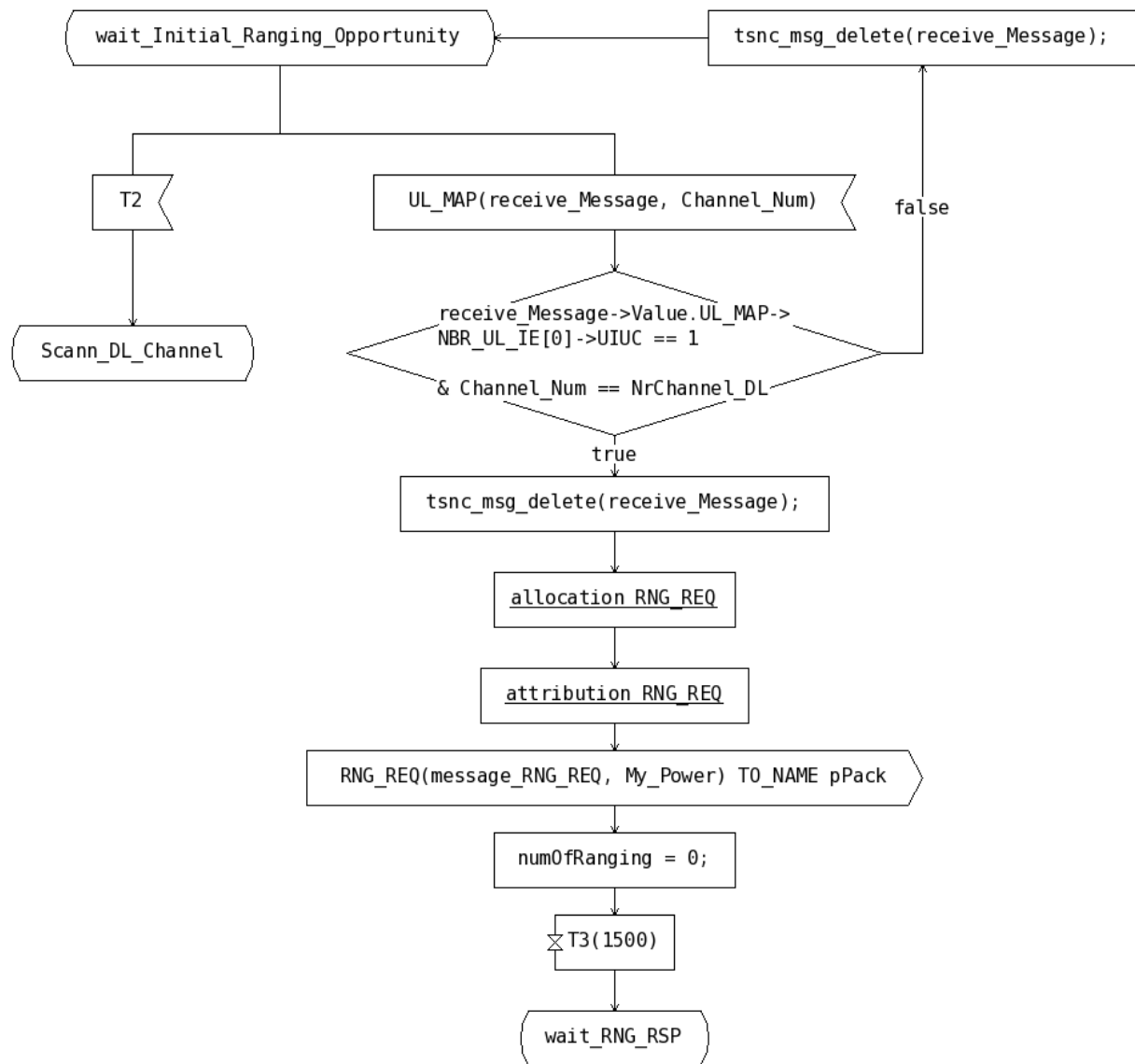
The BS finally update the array of channels by incrementing to the specific uplink channel the number of connected SS.

## From the Subscriber Station

### Sending RNG REQ

The SS has to receive a special UL\_MAP message in order to have the right to continue.

The SS shall determined if the moment is good to send to the BS the next message by checking at the identifier UIUC of the UL\_MAP.



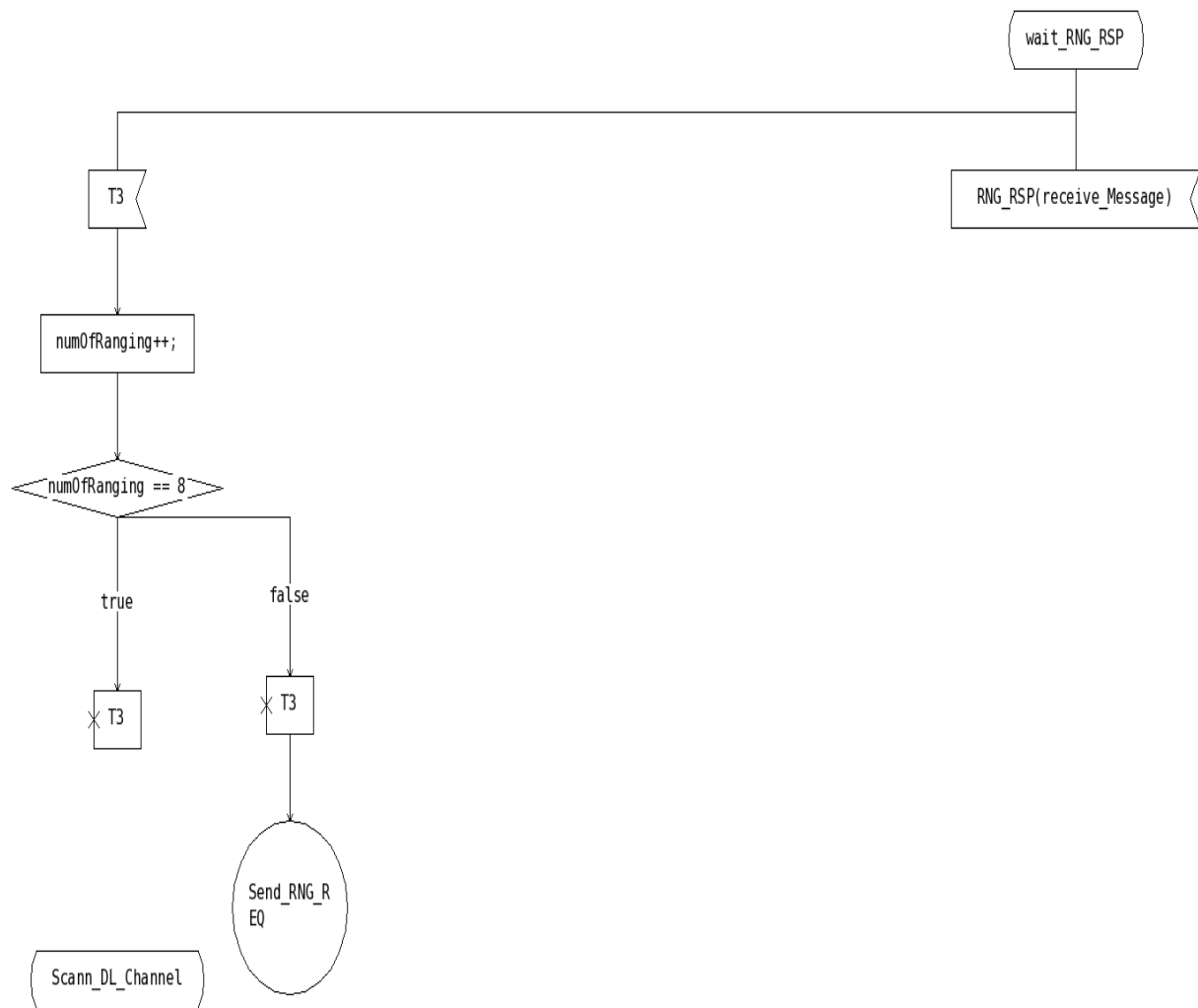
When this is the case, the SS send a Request Ranging message. As for the channel, we had here a physical condition: the Power chosen by the user at the beginning of the procedure.

### waiting RNG RSP

Here the SS shall wait for the response of the BS.

Two cases are possibles:

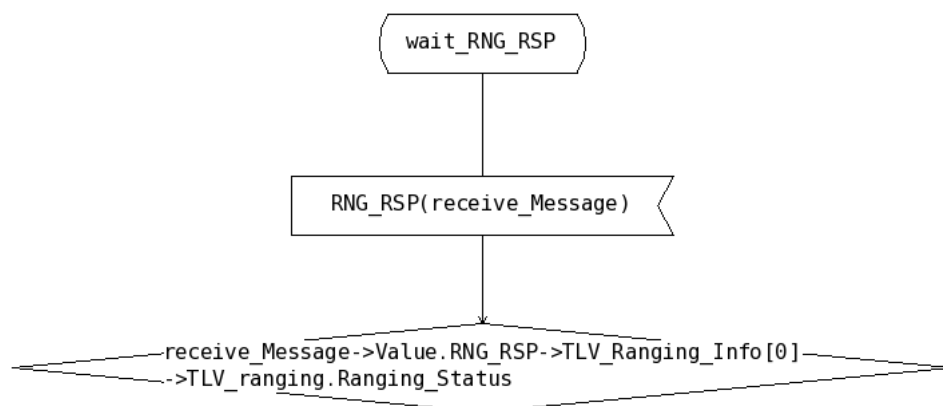
- The BS doesn't respond (the message isn't sent in the appropriates ranges decided before), the SS shall send again a Request message. If after 8 times the BS isn't responding. The SS has to choose another Downlink Channel.
- The BS responds in a confortable amount of time.



## Receiving Ranging Response message

When the SS receive the RNG RSP message he has to check the status that it contains:

- Ranging\_Status = 1: continue (the BS need some modification before going on)
- Ranging\_Status = 2: abort (the BS cannot continue in these conditions)
- Ranging\_Status = 3: success (the operation is a success)



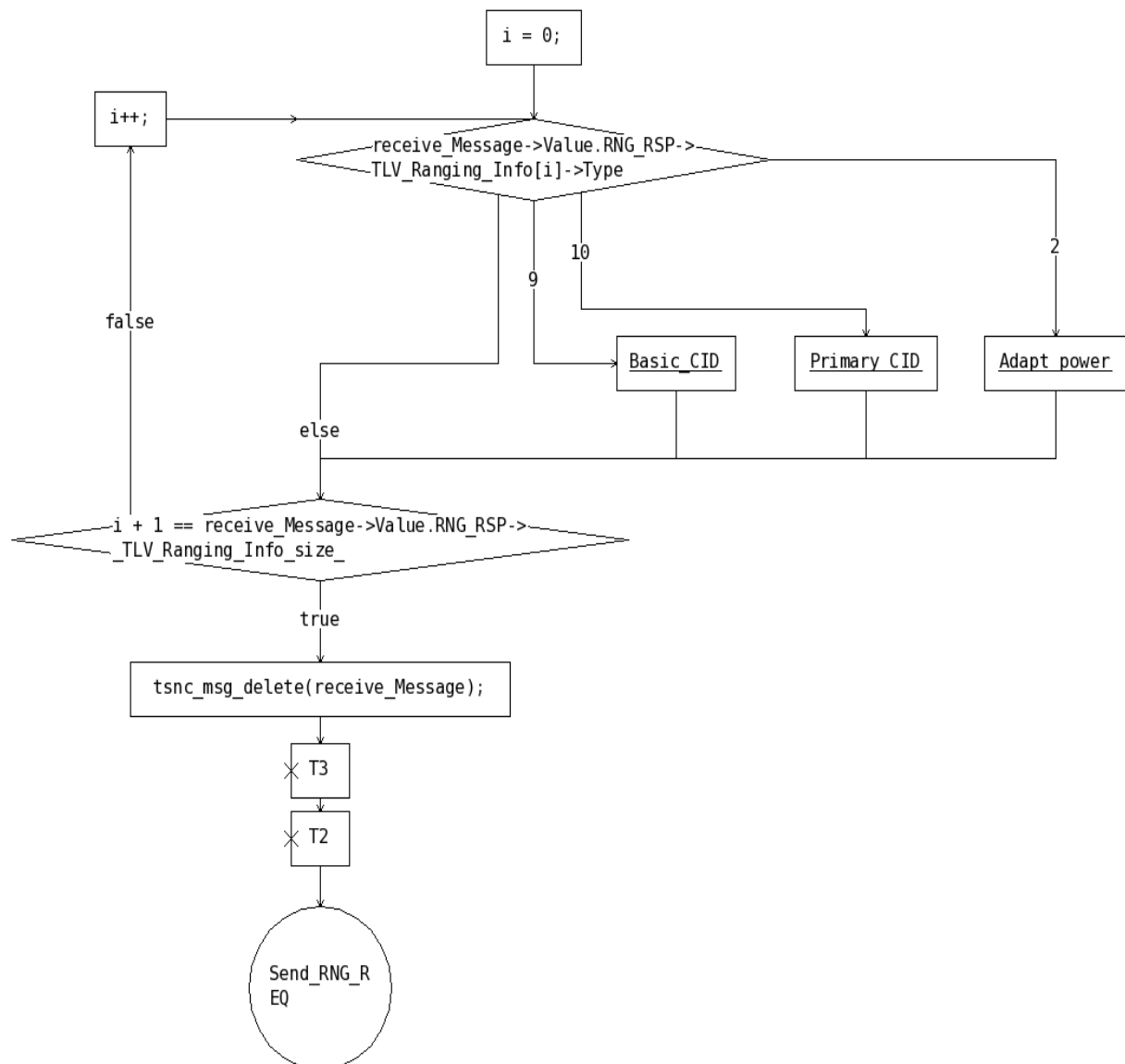


## RNG RSP continue

When receiving RNG RSP with Ranging\_Status = 1, the SS shall search different kinds of informations.

Here, the SS checks if the BS is assigning to him some identifiers, which would make the conversations easier in the future. Therefore the SS registers his basic and primary CID when they are presents.

Furthermore, the SS sees if the BS is giving him indications concerning his power. If so, he has to ajust his power to the level asked.

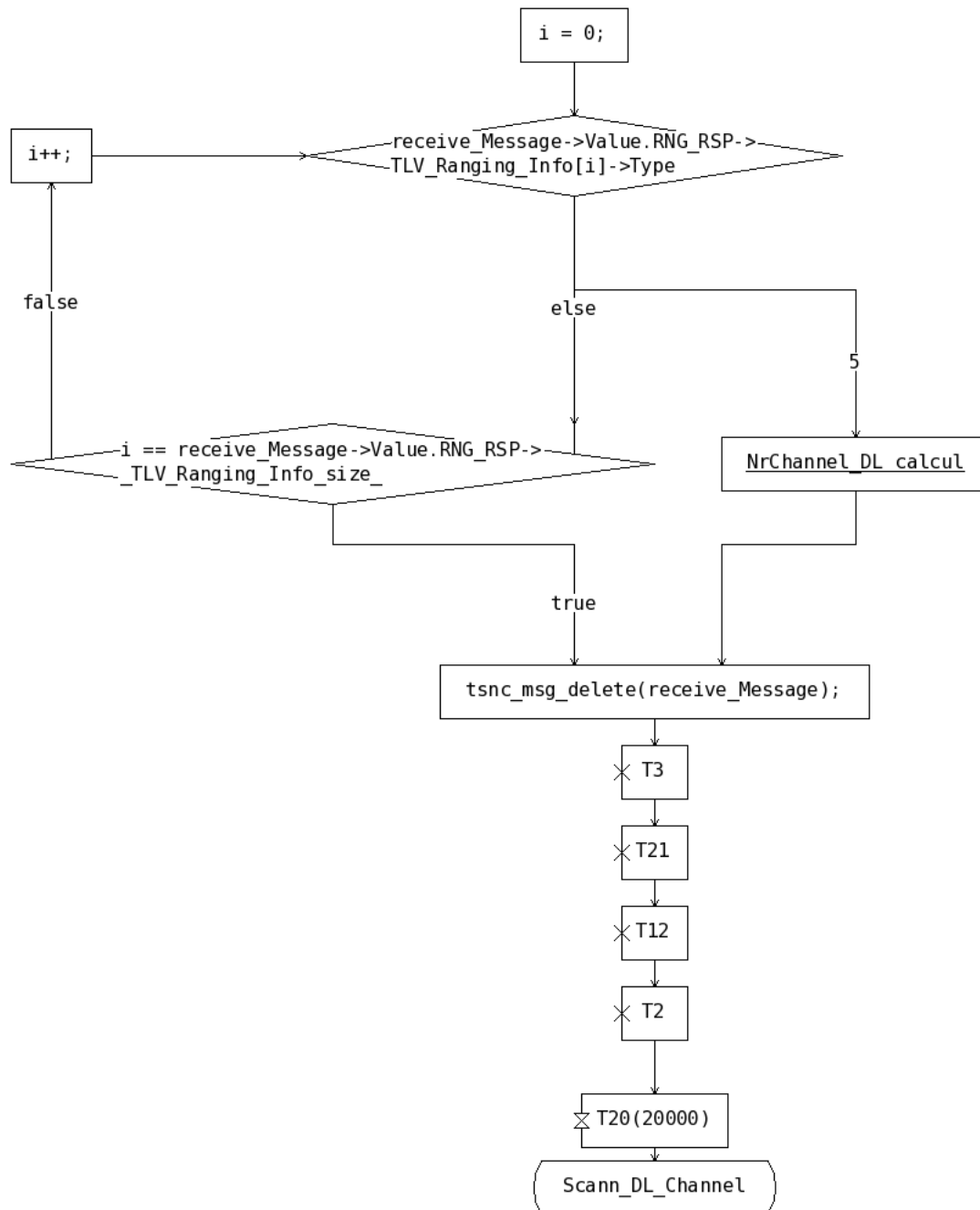


Then the SS shall send again the RNG REQ message, with the ajusted power, until the BS is pleased with the configuration.

## RNG RSP abort

When receiving RNG RSP with Ranging\_Status = 1, the SS shall search if an especial information is present.

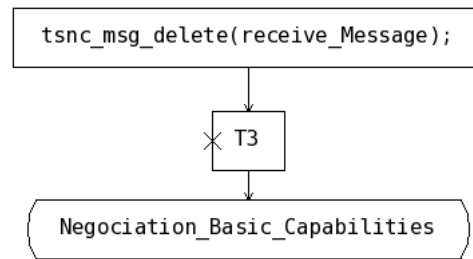
The SS search if the BS has given to him an information concerning a new channel on which the SS will have more chance to succed. If it exist, the SS shall based his new search on this channel.



In any case, the SS has to start from the beginning and shall scann for another downlink channel.

**RNG RSP success**

Here, the SS has nothing to do. The connexion is good enough for the BS.



The SS can now negotiate some basics capabilities with the BS.

## From the Base Station

### Receiving Ranging Request message

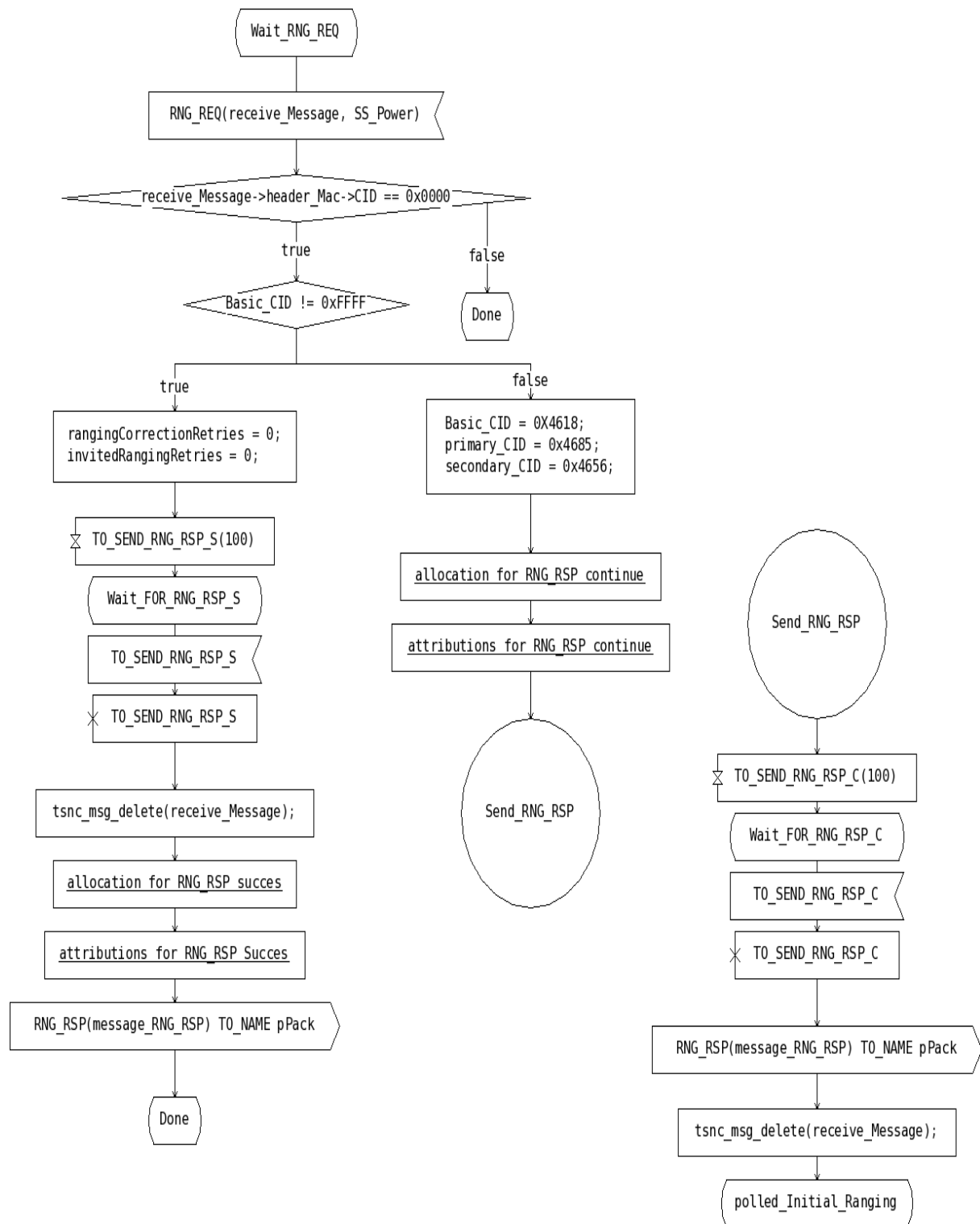
The BS had send an UL\_MAP autorising the SS to send him a request.

When this request arrives, the BS shall test if this message is for ranging or any other purposes.

If the identifier contained in the CID is different from 0, this message is not the one wanted in this part of the protocol.

If it his, the BS shall test if this SS has already be given some identifiers (CIDs) to this SS.

- If it has, that means that the ranging has already been done. The BS send a Ranging Response with succes.
- Otherwise, the BS assigns CIDs to this SS and send it to him with a Ranging Response "continue". Now the BS is ready for the initial ranging procedure



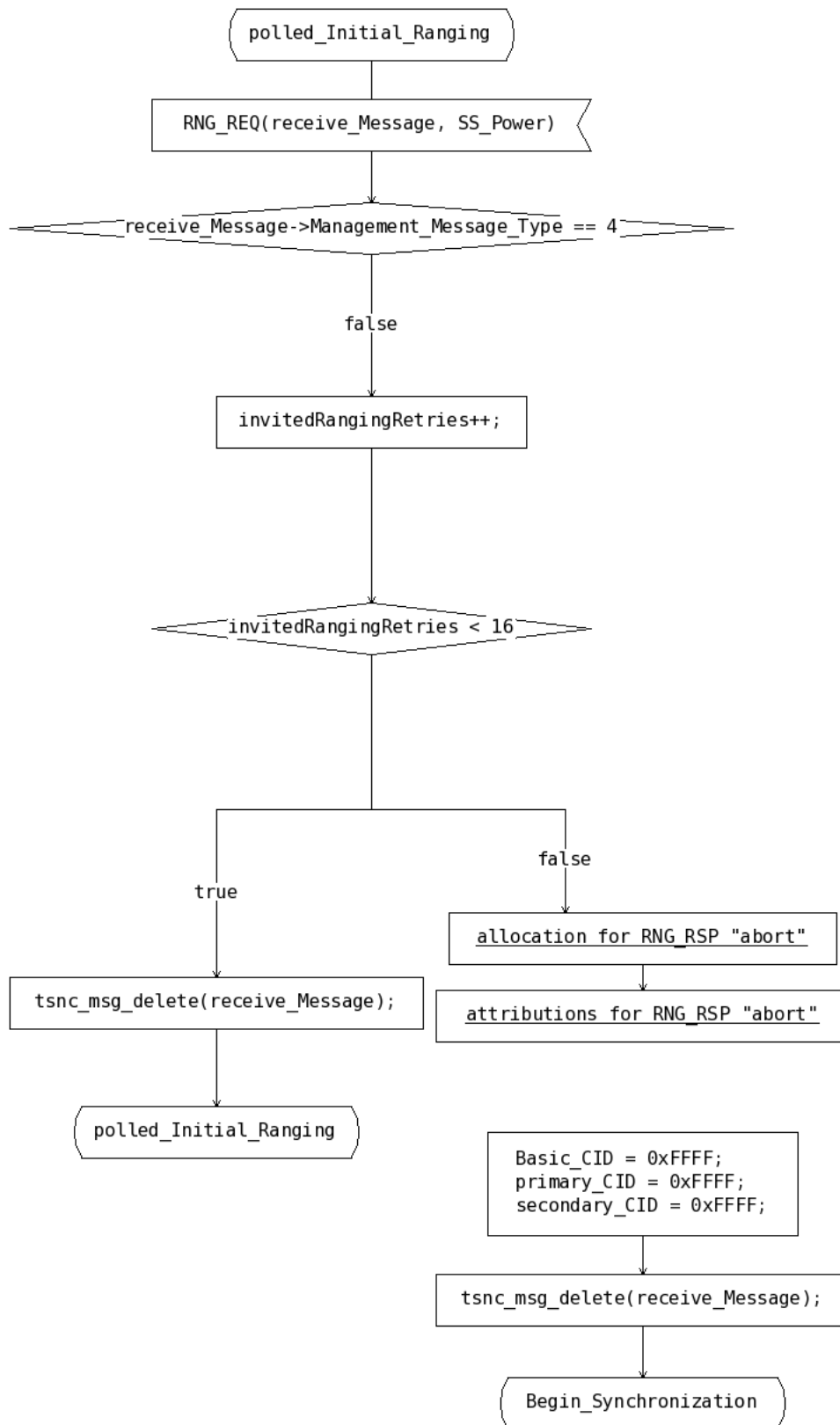
## Initial ranging

At this stage, the BS must receive an initial ranging and checks if it is in not damaged, or in the good slot. Theses are physicall conditions that we can not check.

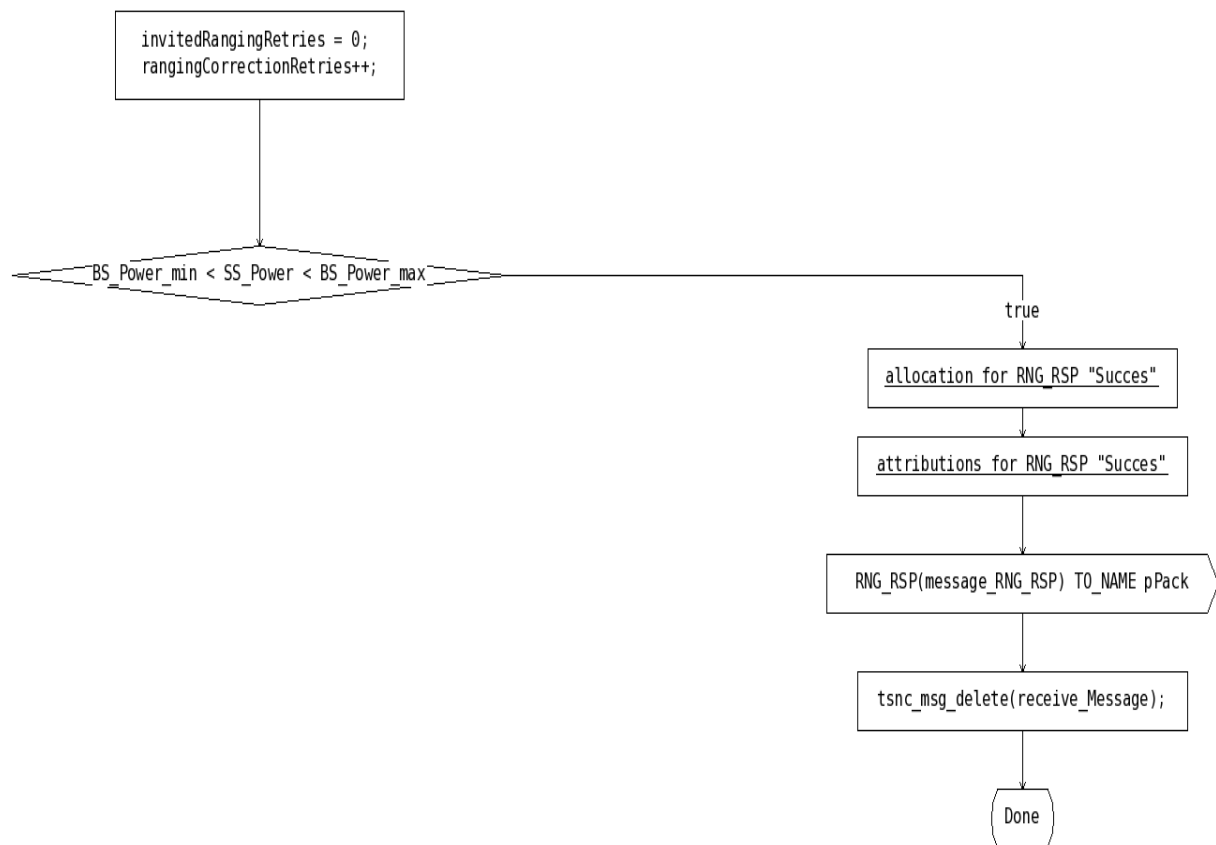
So, we only check if his type is conforme with the RNG\_REQ message.

If the type isn't good, the SS can send 16 times his message before receiving

the indication to abort, and to choose another Downlink channel.



If the received message is correct, the BS tests if the power is in the limits he established.

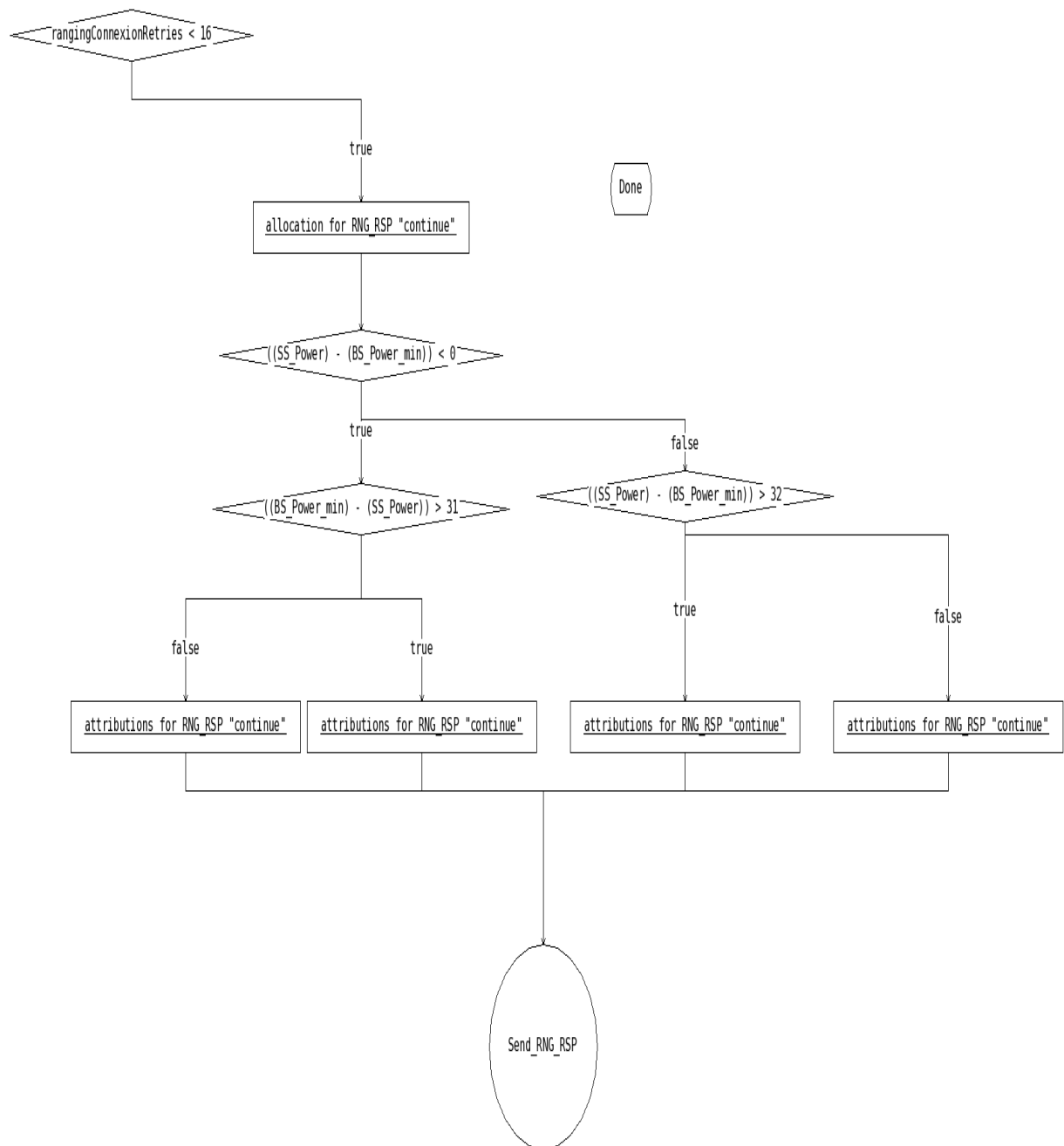


Here, the power is adequate and the response is RNG\_RSP "Success".

If the power isn't in the range determined by the BS, he can send a message RNG\_RSP "continue" with in it, the amount of power the SS add or substract to the current one he is using.

To do so we first determine if the power has to decrease or to increase. Then we check if this operation can be made in one shot or several are needed.

If several ajustements are needed, we give the maximum that the SS can change in one time, then the calcul is done at each RNG REQ message the BS receive.



If after 16 times, the power isn't in the appropriate range, the message sent is RNG\_RSP "abort", indicating that the ranging has failed.

The SS would have to search the connection on another channel.

# Conclusion

This documentation refers to the beginning of the initialization in the Wimax procedure.

First, we have seen an example for the synchronization between a master Station (the BS) and the one trying to establish connection ( the SS).

Messages are continuously send by the BS in order to indicate if the channel is free or not.

The SS checks randomly the differents frequencies for these messages. This part is based on timers, if the laps of time without a good message has expired, the channel isn't suitable.

The second part is the attribution of some choices that the BS wants the SS to do: that's the "initial ranging".

We can see that the BS has all the power of decision. He allows the synchronization and forces the SS to complains to his demands.

The following part of the procedure concerns the Negociation of the basics capabilitIES.

It concerns the needs of the SS. The BS will allows the requests of the suscriber if possible.