OsmoBSC - Feature #2462

clarify lchan->encr.alg_id

08/24/2017 01:27 PM - neels

Status:	New	**Start date:**	08/24/2017
Priority:	Low	**Due date:**	
Assignee:		**% Done:**	0%
Category:			
Target version:			
Spec Reference:			

Description

In gsm48_send_rr_ciph_mode() I ran into a magic formula:

```
        if (lchan->encr.alg_id <= RSL_ENC_ALG_A5(0))
                ciph_mod_set = 0;
        else
                ciph_mod_set = (lchan->encr.alg_id-2)<<1 | 1;
```

To clarify:

ciph_mode_set should match 3GPP TS 44.018 10.5.2.9:

```
bits
4 3 2
0 0 0   A5/1
0 0 1   A5/2
0 1 0   A5/3
0 1 1   A5/4
1 0 0   A5/5
1 0 1   A5/6
1 1 0   A5/7
1 1 1   reserved
```

which as in a5/x means ciph_mod_set = x - 1

In bssmap_handle_cipher_mode(), we call gsm0808_cipher_mode(cipher) with cipher either 0 or 1. We want cipher x as in a5/x (e.g. a5/3 means cipher 3).

We then set

```
conn->lchan->encr.alg_id = RSL_ENC_ALG_A5(cipher) == cipher + 1;
```

This is the encoding used in the RSL Channel Activation message.

Finally we convert back to x-1, and shift one bit to the left:

```
 ciph_mod_set = (lchan->encr.alg_id-2)<<1 | 1;
```

So it **is** correct, but it would be much easier to read if we stored the a5_n value and converted in the appropriate places, instead of storing one encoding and converting back to the other by a magic formula.

Otherwise at least place comments to clarify.

Related issues:

Related to OsmoBSC - Feature #2461: Improve "encryption" VTY parameter	**Resolved**	**08/24/2017**

History

#1 - 08/24/2017 01:28 PM - neels

- Related to Feature #2461: Improve "encryption" VTY parameter added