TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***TSGR2#4(99) 390***
Berlin, Germany 25 to 28 May 1999

Agenda Item: 6.3

Source: **Nokia**

Title: Further clarifications of the MAC based ciphering solution

Document for: Decision

---

1. INTRODUCTION

This paper presents some further details of the MAC based ciphering mechanism [1]. A solution is presented for all the problems noticed until now.

2. NOTICED PROBLEMS

2.1. RACH transmission

With the current L1 RACH power ramping solution, UE-MAC does not necessarily know the exact radio frame where the RACH message part will be sent. A straightforward solution to this is to include the LSB bits of the ciphering counter to MAC header. Number of bits needed depends on the time the L1 RACH procedure may take (currently not specified).

2.2. FACH/DSCH transmission

Here the problem is that MAC-d (performing ciphering) and MAC-c/MAC-sh (performing the scheduling) may be physically located in different RNCs (SRNC vs CRNC). Our solution for this is that the time difference between ciphering and transmission is included in MAC-c/MAC-sh header. Max 8 bits should be enough. MAC-c and MAC-sh operation has to be defined so that if the data received from MAC-d is not transmitted within max allowed time difference (~2.5 seconds with 8 bits) the packet is discarded.

2.3. Type II/III Hybrid ARQ

The solution presented in RAN WG meeting #3 [2] works fine as long as there is no MAC level multiplexing. However, with multiplexing on MAC level an additional problem will be that the receiver should know exactly which transport blocks belong to which logical channel, even if MAC header of some TB is corrupted. Otherwise the receiving MAC cannot generate the deciphering masks correctly in all situations. Possible solutions for this could be:

- the extra information is sent out-of-band
- the Dynamic Part of a Transport Format has to be refined so that the receiver can read not only TB size + TBS size but also which TB belongs to which logical channel (this may eat lots of TFCI space)
- restrict MAC layer multiplexing only to such services which have different TBS sizes, so that from the TBS size (read from TFI) the receiver can implicitly know to which logical channel it belongs to. Naturally, an additional requirement is that each transmission time interval (TBS) can contain data from only one logical channel.

This is only problem for non-transparent data. For transparent, the problem can be avoided by not performing MAC multiplexing at all.

Note that this problem has nothing to do with the Hybrid Type II/III ARQ itself, thus the proposed HARQ outband signalling mechanism by Nokia can be used also if ciphering is done on RLC. However, HARQ is not a subject for this contribution.

3. CONCLUSIONS AND PROPOSAL

As described in chapter 2, the solutions for the problems noticed in the MAC based ciphering mechanism [1] are either complex or cause extra overhead on radio interface and/or extra restrictions. For the RLC+MAC ciphering solution the main problems are related to implementation complexity, that the two-layer approach may cause. From purely functional viewpoint, no remarkable problems or restrictions on the RLC+MAC solution have been noticed.

Due to this, we will withdraw our original proposal to adopt MAC based ciphering also for non-transparent data.

Ciphering for non-transparent (UM/AM) RLC should be done on RLC layer (ciphering sequence number based on RLC PDU numbers) and for transparent (Tr) RLC on MAC layer (ciphering sequence number based on the Connection Frame Number).

4. REFERENCES

[1] TDoc TSGR2(99)111 Radio Interface Ciphering (Nokia)
[2] TDoc TSGR2(99)236 Solution to problem of MAC based ciphering with Type II/III hybrid ARQ (Nokia)