TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***TSGR2#2(99)111***
Stockholm 8th to 11th March 1999

Agenda Item: 8.7

Source: Nokia

Title: **Radio Interface ciphering**

Document for: Decision

---

1. INTRODUCTION

This paper discusses the radio interface ciphering concept. The proposal is based on the synchronization principles defined in [1], on the ciphering principles of GPRS [2] and on the requirements for ciphering termination point and frame number length from SGM10 [3].

2. BASIC ASSUMPTIONS

The following basic assumptions have been made:

- a stream ciphering (XOR) mechanism is used (like in GSM and GPRS)
- the basic unit to be ciphered is one RLC PDU
- (radio interface) ciphering is terminated in UE and RNC
- ciphering is based on UEFN as defined in [1] and in this contribution. Thus the frame number used as input for the ciphering algorithm is obtained partly from the radio frame number and NOT included into each RLC PDU header (like in GPRS LLC)
- The input parameters for the ciphering algorithm are: *Kc, UEFN, direction* and *Bearer ID*. The bearer id is added for security reasons (explained in chapter 3.2.3)
- the same ciphering mechanisms can be used also for common channel and DSCH transmission (USCH is ffs.)

3. THE CIPHERING CONCEPT

3.1 Overview

The proposal is that radio interface ciphering in UMTS is a MAC functionality. The ciphering block should be the uppest entity of MAC-d for DCCH and DTCH ciphering. (If ciphering for CCCH is needed then there should be ciphering block as the uppest entity of MAC-c also). It allows the encryption/decryption of MAC SDUs (RLC PDUs) based on XOR combining with a ciphering mask that is obtained as output from a ciphering algorithm. Inputs for the ciphering algorithm are the ciphering key (Kc) the Frame Number (UE FN), the RAB ID and the direction (UL/DL). The ciphering block diagram is shown in Fig. 1.

Definitions of the parameters for the ciphering algorithm follow in the next paragraphs.

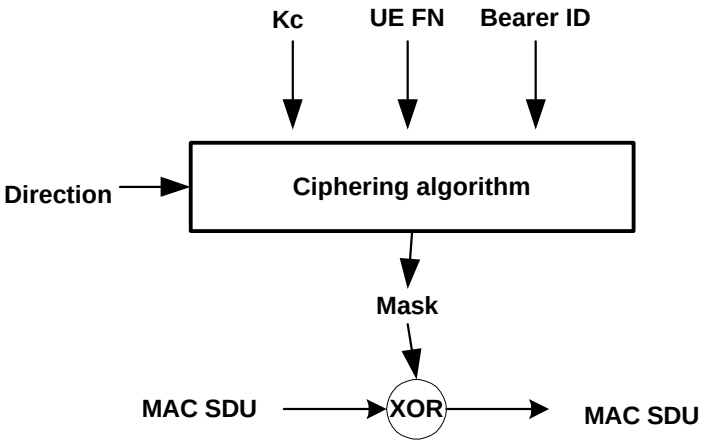


Figure 1: Radio interface ciphering block diagram

3.2 Ciphering algorithm parameters

3.2.1 Frame Number, UE FN

UE FN is defined in [1], see also figure 2 below. UE FN is composed at least of a Connection Frame Number (CFN). To meet the requirements for the length of frame number used for ciphering [3], a Hyper Frame Number (HFN), incremented at every completed cycle of the CFN, is added to the UE FN. With this solution the length of the frame number broadcasted in BCCH need not be as long as the length of frame number used for ciphering (which should be at least 32 bits are stated in [3]).

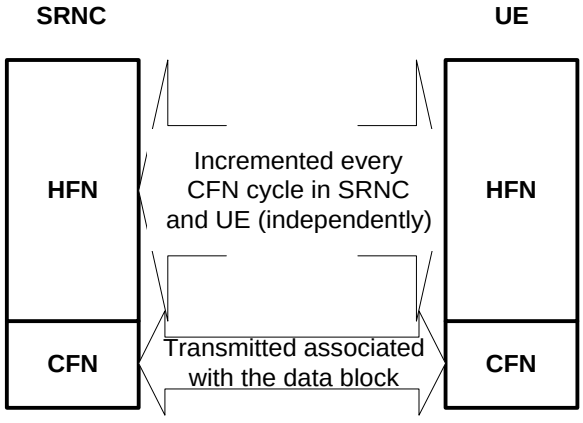


Figure 2: Composition of the UE FN

3.2.1.1 Connection Frame Number - CFN

CFN is tied to the BCCH timing, i.e. it is incremented every 10 ms. CFN is 'transmitted' through the transport channel between UE and SRNC, associated to each data frame (Transport Block Set). In Iub and Iur interfaces it is inserted in the FCL header, and in the Uu interface it is mapped into the Cell FN (=System Frame Number, SFN), broadcast in the BCCH.

Length of the CFN is the same as the length of the cell FN, currently 720 msec (0..71, 7 bits). Longer CFN is FFS.

In case of interleaving periods longer than 10 msec, CFN refers to the first radio frame utilised for the transmission of the interleaving block.

When UE is in CCH state, the CFN is set equal to the Cell FN.

(For further details on CFN and its use, see [1], chapter 9.4)

3.2.1.2 Hyper Frame Number - HFN

The HFN is initialised to a common value in the UE and SRNC, and then it is incremented every CFN cycle. The length of the HFN is at least 25 bits. The HFN should be initialized to a value that is hard to predict by a fraudster.

HFN is initialised before ciphering is started, e.g. during the RRC connection is setup or during the ciphering mode setting procedure.. HFN is maintained (run) for all the time the UE is in RRC connected mode. [FFS:] One possibility is to maintain UE specific HFN reference in SRNC which is related to the SRNC clock via an UE specific offset (= no separate counter for each UE is needed).

The reason why HFN cannot be initialised to a fixed value (e.g. 0) is to prevent the reuse of the same ciphering masks in case the Kc is not changed.

At least during the following procedures the HFN (re)initialization may be needed:
1. RRC Connection Setup (or Cipher mode setting after RRC Conn Setup)
2. GSM to UMTS handover
3. RRC Connection Re-establishment

Also in the following procedures HFN need to be considered carefully:
1. SRNC relocation

The details of HFN initialization are FFS.

3.2.2 Ciphering Key, Kc

Kc:s are calculated in the UE and SRNC during the authentication procedure. 3G MSC and 3G SGSN have two independent MM, and the handling of the ciphering key is independent as well. Thus:

- The RANAP Ciphering Mode Command is used to initiate only the ciphering of the bearer(s) controlled by the CN node that sends the message.

- The Kc obtained from the MSC-authentication will be used for the bearer(s) controlled by the 3G MSC, and the Kc obtained from the SGSN-authentication will be used for the bearer(s) controlled by the 3G SGSN.

The signalling link will use the Kc obtained from the CN node that sends the first Ciphering Mode command message, and keep the same Kc for all the duration of the RRC connection.

3.2.3 Bearer ID

Bearer ID (RAB ID) is a radio access bearer / signalling link specific parameter, unique within one RRC connection. It is used as input parameter for ciphering to ensure that the same ciphering mask is not applied to two bearers that have the same Kc and are transmitted with the same UE FN (in case of L1 or MAC multiplexing).

Thus the ciphering algorithm in Figure 1 must be run for each parallel bearer independently in each interleaving period.

The security problem of ciphering two blocks in one radio frame with same ciphering mask is that an active fraudster listening to the traffic and knowing the structure of transmitted data (e.g. signalling) might get some information by XORing the two ciphered data blocks. In this case:

XOR of ciphered data blocks = XOR of unciphered data blocks

3.2.4 Direction

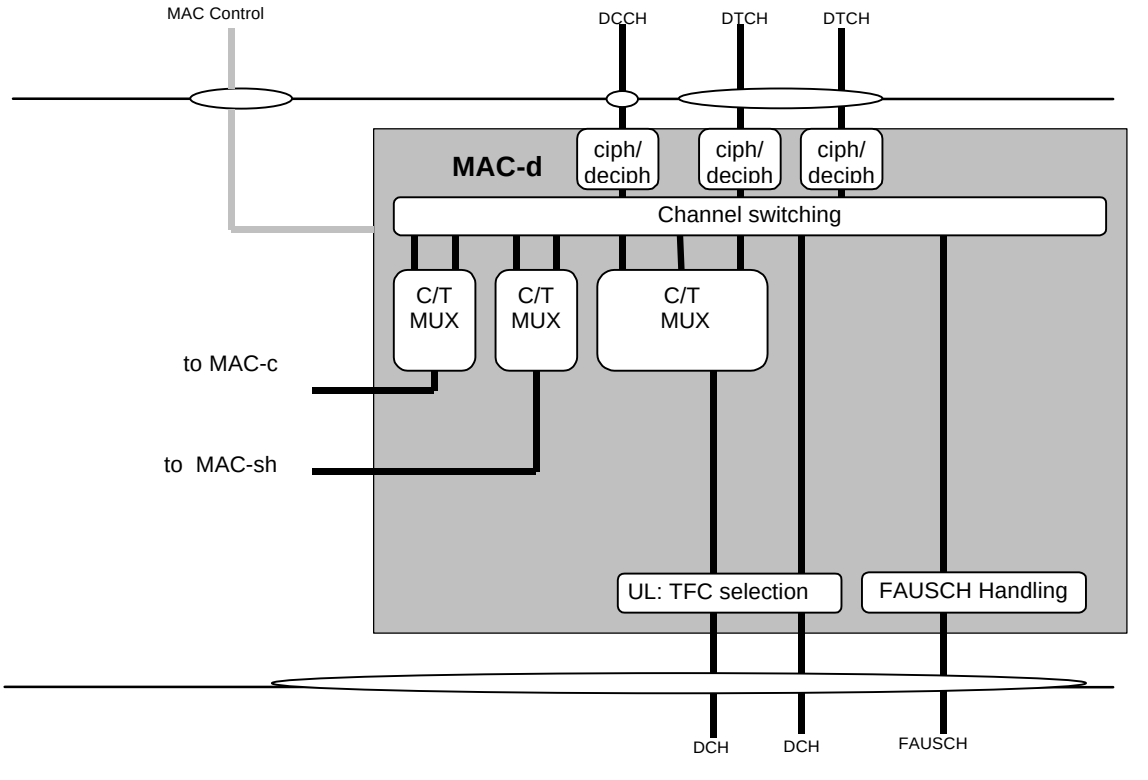
This parameter defines in which direction the data is sent (Uplink / Downlink).

3.3 Ciphering on common channel and DSCH transmission

The same principles can be applied to ciphering of data on CCH and DSCH (USCH is ffs.). The only problem is related to scheduling of data in different place (CRNC or NodeB) where the ciphering is performed (SRNC). In this case, the MAC-d entity executing the ciphering does not know the exact FN used to transmit data. A solution to this problem is ffs.

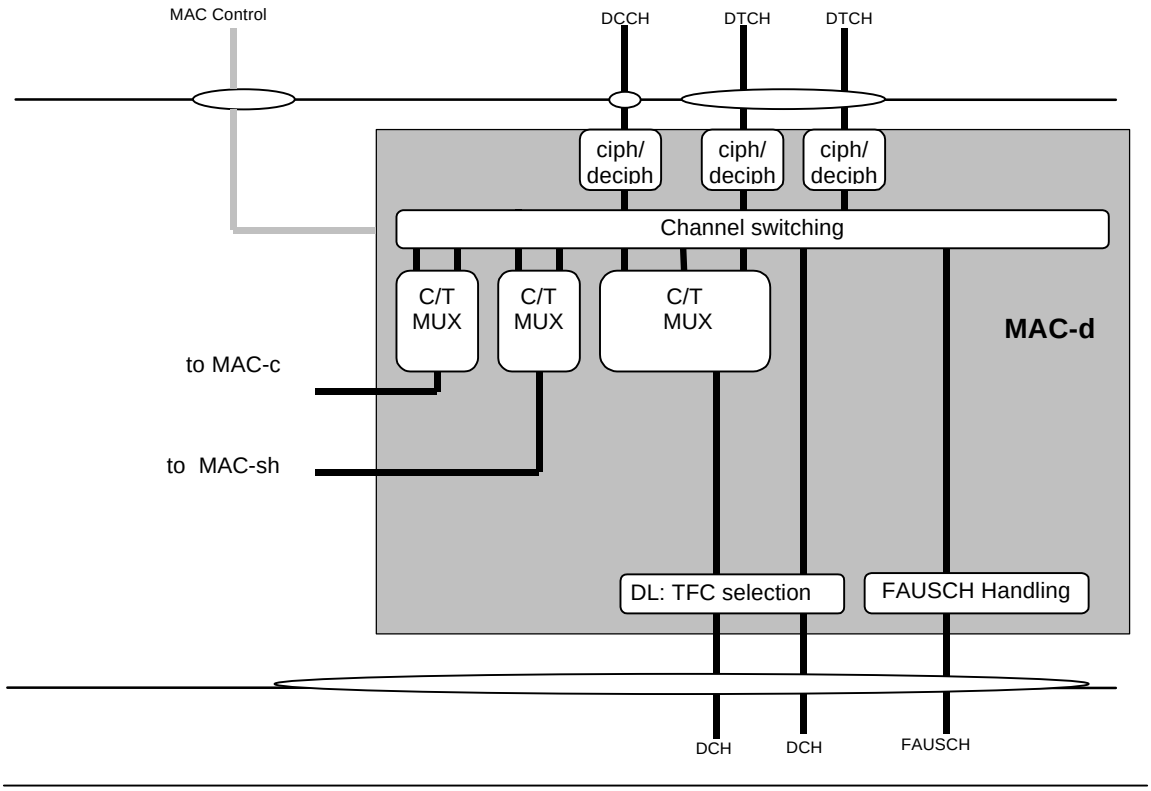
4. MAC-D ARCHITECTURE

The figure numbers refer to figures of [4].



DL	Downlink	RNTI	Radio Network Temporary Identity
TF	Transport Format	UE	User Equipment
TFC	Transport Format Combination	UL	Uplink
Note1 :	For DCH and DSCH different scheduling mechanism apply	Note 2 :	The TFC selection place is under discussion

Figure 4.2.3.3. UE side MAC architecture / MAC-d details



DL	Downlink	RNTI	Radio Network Temporary Identity
TF	Transport Format	UE	User Equipment
TFC	Transport Format Combination	UL	Uplink
Note1 :	For DCH and DSCH different scheduling mechanism apply	Note 2 :	The TFC selection place is under discussion

Figure 4.2.4.3 UTRAN side MAC architecture / MAC-d details

5. PROPOSAL

The following is proposed:

- The concepts desribed in chapters 2 and 3 of this contribution are taken as a working assumption for WG2 and documented into S2.01
- Figures in chapter 4 replace corresponding figures in [4]
- A liaison statement is sent to 3GPP SA WG3 (?) addressing the following questions:
  - Are the assumptions described in chapter 2 valid
  - Is there some additional security requirements that are not fullfilled with the presented ciphering concept ?

6.

REFERENCES

[1] TS S3.01 V0.0.2 (1999-02) "RAN Overall Description"

[2] GSM 01.61 V6.0.1 (1998-07) "GPRS ciphering algorithm requirements"

[3] Tdoc SMG2 UMTS-L23 456/98 LS to SMG2 and SMG12 on encryption termination point

[3] TS S2.21 V0.0.1 (1999-03) " MAC protocol specification"