TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***TSGR2#3(99) 375***
Berlin, 25-28th May 1999

Agenda Item:	6.3
Source:	Alcatel
Title:	Proposal for RLC+MAC ciphering model
Document for:	Decision

1 Introduction

This document provides a detailed description of the MAC+RLC ciphering model initially proposed in Tdoc RAN WG2 124/99, and refined following discussions at WG2#3 meeting. It has already been discussed through e-mail and comments have been taken into account in this version.

Alcatel proposes to adopt this ciphering model in RAN specifications.

2 Ciphering model

2.1 Location of ciphering function in the UTRAN protocol architecture

The ciphering function is performed either in the RLC sub-layer or in the MAC sub-layer, according to the following rules :

- If a logical channel is expected to be supported on common transport channel and has to be ciphered, it can not use the transparent mode of RLC (it should use the UM RLC mode instead).
- If a logical channel is using a non-transparent RLC mode (AM or UM), ciphering is performed in the RLC sub-layer.
- If a logical channel is using the transparent RLC mode, ciphering is performed in the MAC-d sub-layer.

According to this model, ciphering is always performed in the SRNC, and the context needed for ciphering (Kc, HFN, etc.) is only known in SRNC. This concept is illustrated on the figure below :

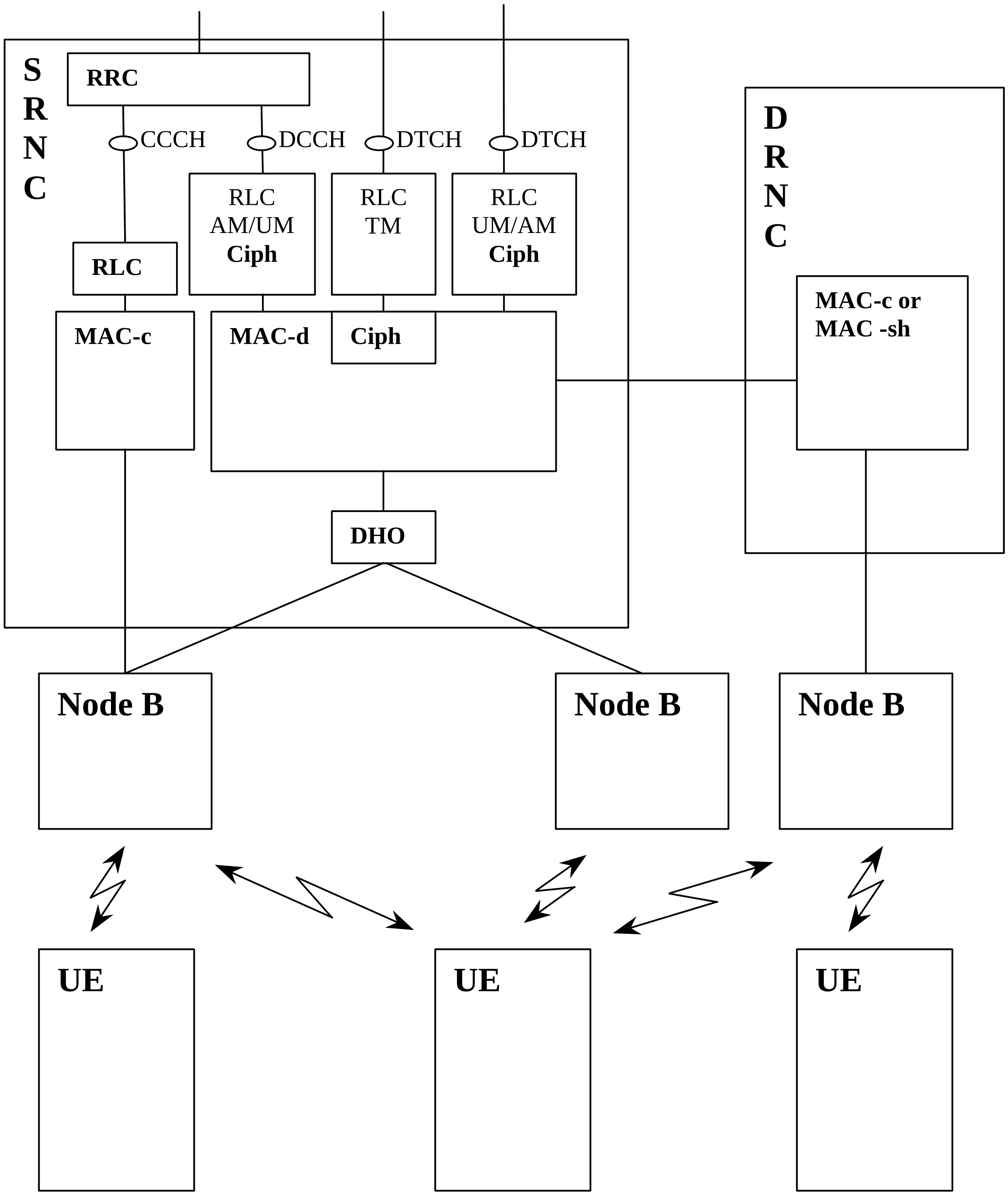

Figure 1 : MAC + RLC ciphering concept (UTRAN side)

2.2 Ciphering algorithm

2.2.1 Overview

When ciphering is performed in the RLC sub-layer, it performs the encryption/decryption of the data part of an RLC PDU, based on XOR combining with a mask obtained as an output of the ciphering algorithm.

When ciphering is performed in the MAC sub-layer, it performs the encryption/decryption of a MAC SDU (RLC PDU), based on XOR combining with a mask obtained as an output of the ciphering algorithm.

The generic algorithm and its parameters are described in the following figure

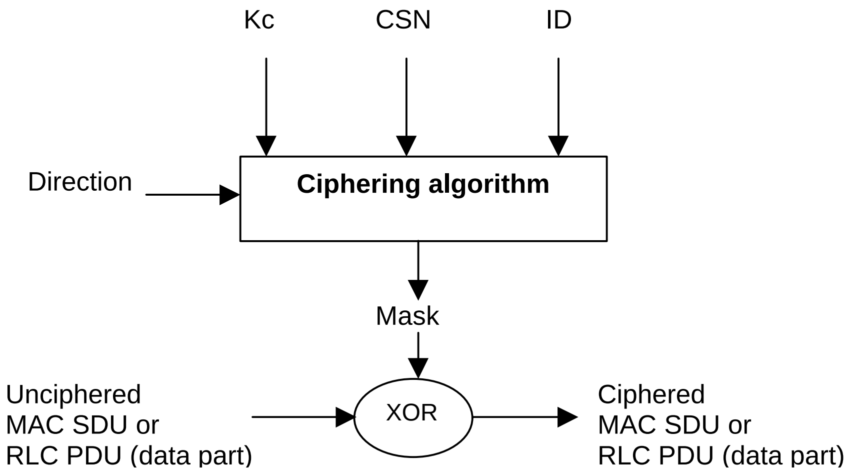
Kc
CSN
ID
Direction
Ciphering algorithm
Mask
Unciphered MAC SDU or RLC PDU (data part)
XOR
Ciphered MAC SDU or RLC PDU (data part)

Figure 2 : Ciphering algorithm and parameters

2.2.2 Ciphering algorithms parameters

2.2.2.1 Ciphering sequence number

The ciphering sequence number (CSN) shall be at least 32 bits long. It is composed of a ‘long’ sequence number called Hyper Frame Number HFN, and a ‘short’ sequence number, which depends on the ciphering mode, as described below. There is one ciphering sequence per logical channel using AM or UM mode plus one for all logical channels using the transparent mode (and mapped onto DCH).

The Hyper Frame Number (HFN) is initialised by the UE and signalled to the SRNC during the authentication procedure. It is used as initial value for each ciphering sequence, and it is then incremented independently in each ciphering sequence, at each cycle of the ‘short’ sequence number. The highest HFN value used during a RRC connection (by any ciphering sequence) is stored in the UE SIM (as agreed in S2.01), and the UE initialises the new HFN for the next session with a higher number than the stored one.

The ‘short’ sequence number is :

- For RLC TM on DCH, the CFN of the UEFN is used and is independently maintained in UE MAC and SRNC MAC-d, as explained in S3.01. The ciphering sequence number is identical to the UEFN.
- For RLC UM and AM modes, the RLC sequence number is used, and is directly available in each RLC PDU at the receiver side (it is not ciphered). The HFN is incremented at each RLC SN cycle.

The figure below presents some examples of the different ciphering sequence numbers, assuming various sizes for the ‘short’ sequence numbers. This proposal permits to exchange a unique HFN and also to use a unique CSN size, which should permit to reduce the implementation complexity of the ciphering function. In this example, the HFN is 25 bits long, and only the 20 MSB are used for the CSN of the RLC AM mode.

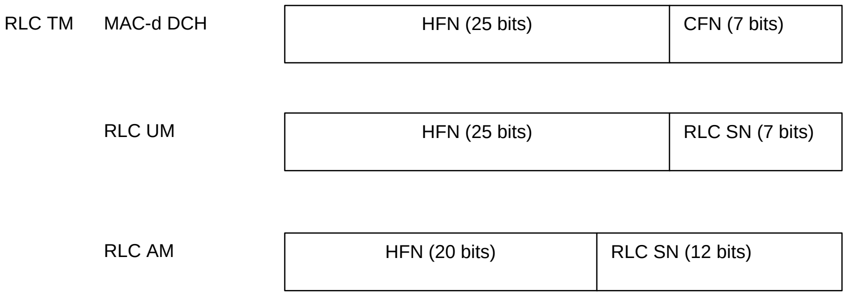

Figure 3 : Example of ciphering sequence number for all possible configurations

2.2.2.2 Ciphering key K_c

K_c is exchanged between the UE and SRNC during the authentication phase. The selection of K_c when a UE is connected with multiple CN is FFS and is not discussed in this document.

2.2.2.3 ID

This parameter indicates the RAB identity / logical channel identity, which shall be unique within a RRC connection. It is used as input parameter of the ciphering algorithm to ensure that the same ciphering mask is not applied to two or more parallel bearers having the same Kc and same CSN. Each RAB ID will be ciphered independently.

2.2.2.4 Direction

This parameter indicates the transmission direction (uplink/downlink).

3 Ciphering and hybrid ARQ

Some questions have been raised regarding the possibility to implement hybrid ARQ with ciphering. With the proposed model, a RLC PDU will be ciphered identically when being retransmitted (using the same RLC sequence number), thus permitting to perform soft combining on ciphered frames in the receiver. The implementation of hybrid ARQ will not require any additional overhead on the air interface because of ciphering.