TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***TSGR2#4~~3~~(99) 389~~236~~***

Berlin, Germany 25 to 28 May 1999

~~Yokohama, Japan 13th to 16th April 1999~~

Agenda Item: 5~~7.5~~

Source: **Rapporteur~~Nokia~~** (Nokia)

Title: Report from the Ciphering email ad-hoc

~~Solution to problem of MAC based ciphering with Type II/III hybrid ARQ~~

Document for: FYI~~Decision~~

---

1. INTRODUCTION

This paper presents the results from email discussion on ciphering/security issues between RAN WG2 meetings #3 and #4.

The ciphering/security subject caused very little discussion and no new conclusions were made during the email ad-hoc.

~~one possible solution how the CFN based ciphering [1] can work with Type II/III Hybrid ARQ. This problem was identified during the ad-hoc email discussions of RAN WG2 [2].~~

2. CIPHERING MECHANISM

No decisions on the ciphering mechanism during the email discussion.

Alcatel provided a more detailed description of the MAC+RLC method, which is a separate ontribution to the R2#4 meeting. Nokia provided more details of the MAC method, especially the noticed problems and possible solutions for them. This is also a separate contribution to the R2#4 meeting.

3. HFN INITIALIZATION

No new ideas presented. The only proposed solution is still the one described in TS 25.301, ver 3.0.1, chapter 8 (saving biggest HFN in USIM after connection release).

4. DATA INTEGRITY

No new input on the integrity control mechanism or on the list of (RRC) messages requiring integrity protection.

5. ADDITIONAL USAGE FOR THE INTEGRITY CHECKSUM

No discussion on this during the email ad-hoc.

6. ONE CIPHERING KEY VS TWO KEY SOLUTION

No discussion on this during the email ad-hoc. Assuming no new input will exist in R2#4 meeting, the "two key solution" will be preferred over the "one key solution".

7. CHANGE OF CIPHERING KEY

No discussion on this subject during the email ad-hoc.

8. QUESTIONS TO SA WG3

No input for this during the email ad-hoc.

~~Since Type II/III hybrid ARQ requires that retransmitted data is exactly identical to the first transmission attempt (to enable combining in the receiver L1), the basic problem with CFN based ciphering is that how does the transmitter know which CFN should be used for ciphering of the retransmissions and how does the receiver know which CFN should be used for deciphering if retransmissions were needed before data was received correctly.~~

~~One solution to this problem is to use the 'outband' signalling (associated with the actual traffic channel) to carry the required information. In addition, the transmitter side MAC entity needs to keep a table for RLC PDU numbers and corresponding CFN information.~~

~~**Note that the exampes concern only downlink and we do not make any proposal here what is the channel or protocol layer used for carrying the outband information.**~~

~~The proposed 'outband' information can be used also for the soft combining in L1, thus RLC PDU number – as described in [3] - is not needed in the outband information anymore. In the example we assume that the RLC PDU itself contains the PDU number ('inband'), thus retransmission requests (by RLC) are done using RLC PDU numbers.~~

~~The proposed mechanism makes it also unnecessary to transmit any outband information with the initial transmission, since the current CFN is obtained 'implicitly' [4].~~

~~The needed outband information is described below:~~

~~CFN Cycles~~	~~CFN~~	~~Position in TBS~~

~~**Figure 1: Outband information signalled with a retransmitted PDU.**~~

~~CFN = the connection frame number used for the first transmission of the PDU~~

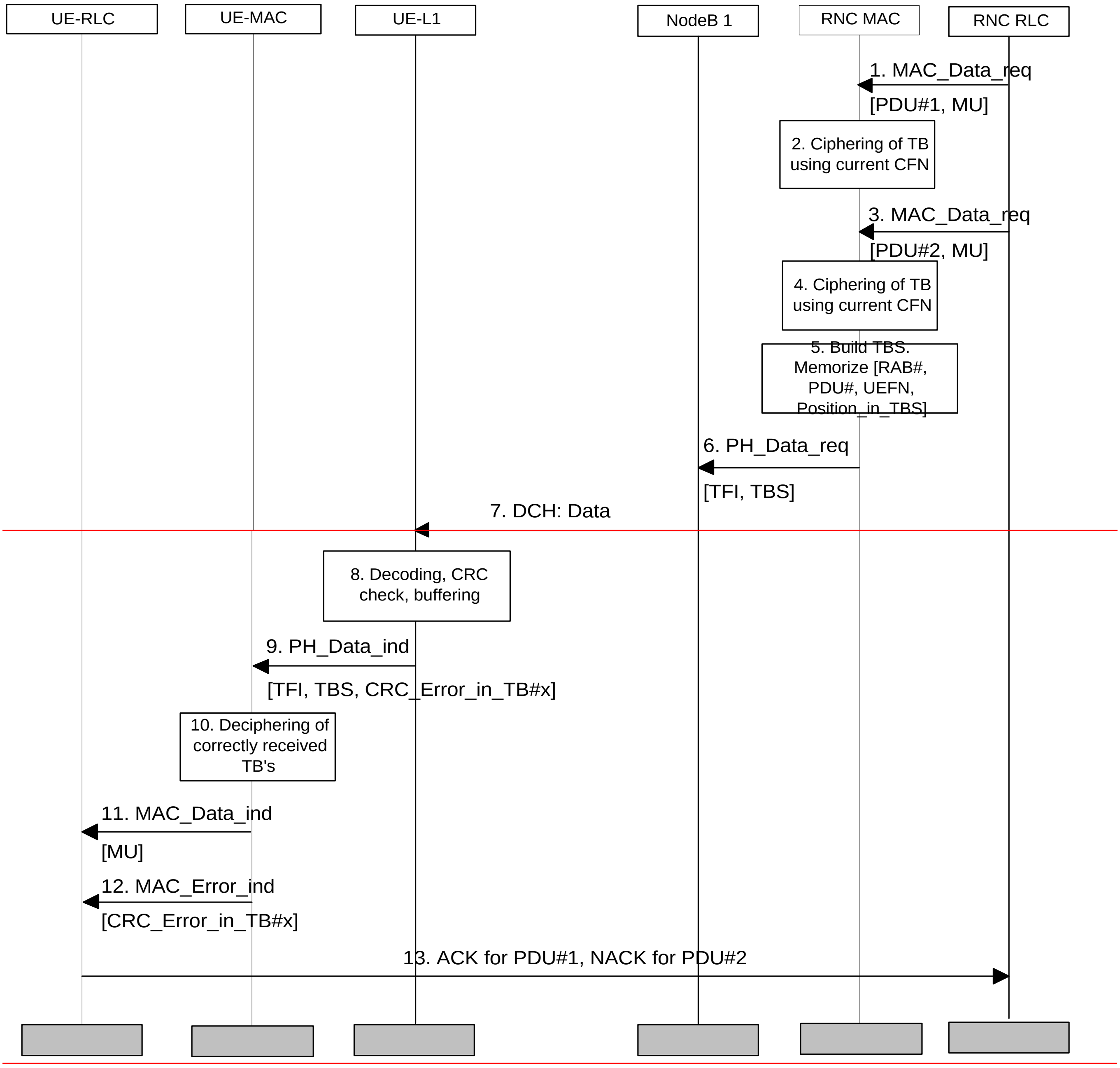
~~CFN Cycles = since the CFN runs in cycles of 720 ms (equivalent to the 'superframe' cycle), some bits may be needed to indicate how many times CFN has elapsed (=how many times HFN has been incremented) after the initial transmission of this PDU. This is dependent on the max allowed retransmission delay (with no extra bits max delay is 720ms, with one bit 1440ms etc.).~~

~~From CFN+CFN_cycles layer 1 can calculate what was the original PDU which should be soft-combined with the received data. MAC can calculate the UEFN used for the original transmission.~~

~~Position in TBS = this parameter indicates which of the transport blocks in the transport block set is in question. This information is needed only for the soft combining in the receiver side.~~

~~In addition, if one "outband channel" is used for several transport channels, a DCH id needs to be included.~~

~~An example signalling flow to clarify the presented method is presented in figures 2 and 3. *(Note that the intention of this example is not to show optimal signalling solution for Hybrid Type II/III ARQ, but only to show how the CFN based ciphering can work together with Type II/III ARQ).*~~


UE-RLC
UE-MAC
UE-L1
NodeB 1
RNC MAC
RNC RLC
1. MAC_Data_req
[PDU#1, MU]
2. Ciphering of TB using current CFN
3. MAC_Data_req
[PDU#2, MU]
4. Ciphering of TB using current CFN
5. Build TBS. Memorize [RAB#, PDU#, UEFN, Position_in_TBS]
6. PH_Data_req
[TFI, TBS]
7. DCH: Data
8. Decoding, CRC check, buffering
9. PH_Data_ind
[TFI, TBS, CRC_Error_in_TB#x]
10. Deciphering of correctly received TB's
11. MAC_Data_ind
[MU]
12. MAC_Error_ind
[CRC_Error_in_TB#x]
13. ACK for PDU#1, NACK for PDU#2

~~**Figure 2. Initial transmission of RLC PDUs #1 and #2**~~

~~**1-4.** In this example, RLC sends two PDU's to MAC within one transmission time interval, thus the TBS will contain both RLC PDUs, #1 and #2~~

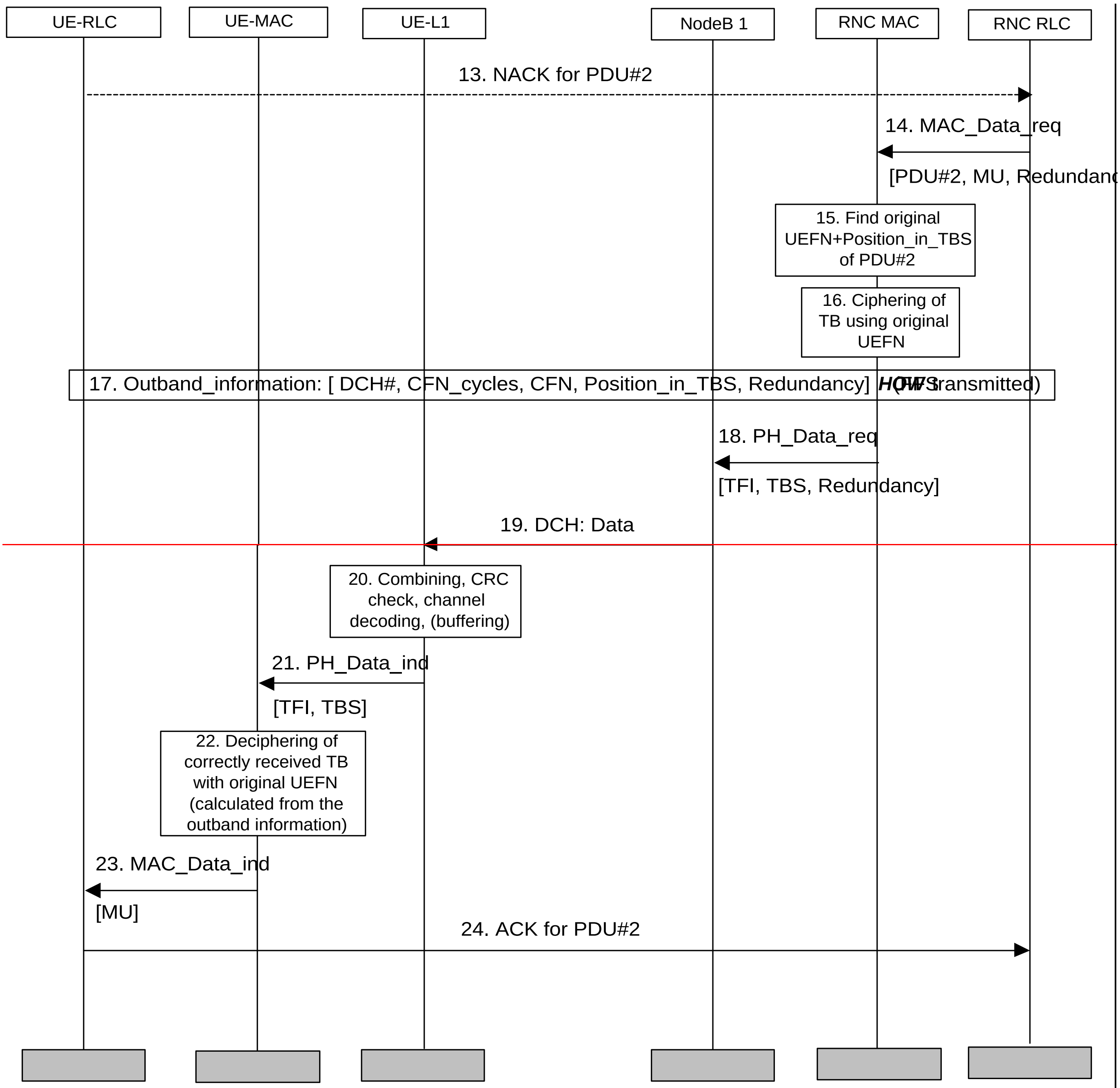
~~**5.** MAC keeps a local table with the following instances:~~
~~[RAB#, PDU#, UEFN, Position_in_TBS]~~

~~**6-8.** Data is transmitted to the receiving side L1. In this example, UE L1 detects CRC error in TB#2 (corresponds to RLC PDU #2 in this exampe). UE L1 buffers PDU data associated with CFN~~

~~**9.** UE L1 indicates to MAC that TB#2 has CRC error~~

~~**10-12.** MAC deciphers correctly received TBs (in this example only TB#1), forwards them to RLC, and indicates to RLC which TBs (RLC PDUs) were erroneous (in this example RLC PDU #2). *Depending on the ARQ mechanism, it is also possible that errors do not need to be indicated to RLC at all but RLC asks retransmissions based on missing PDUs.*~~

~~**13.** UE RLC asks for retransmission of PDU #2.~~


UE-RLC
UE-MAC
UE-L1
NodeB 1
RNC MAC
RNC RLC
13. NACK for PDU#2
14. MAC_Data_req
[PDU#2, MU, Redundanc
15. Find original UEFN+Position_in_TBS of PDU#2
16. Ciphering of TB using original UEFN
17. Outband_information: [DCH#, CFN_cycles, CFN, Position_in_TBS, Redundancy] HOW (Re)transmitted)
18. PH_Data_req
[TFI, TBS, Redundancy]
19. DCH: Data
20. Combining, CRC check, channel decoding, (buffering)
21. PH_Data_ind
[TFI, TBS]
22. Deciphering of correctly received TB with original UEFN (calculated from the outband information)
23. MAC_Data_ind
[MU]
24. ACK for PDU#2

~~**Figure 3. Retransmission of RLC PDU #2**~~

~~**14.** RLC asks MAC to transmit data. From the primitive parameters MAC knows that this is a retransmission and thus ciphering must be done with the stored UEFN information instead of the current UEFN.~~

~~**15-16.** Ciphering~~

~~**17.** 'Outband' information, to be associated wih the retransmitted data, is sent to receiver L1 (details HOW this happends are FFS).~~

~~**18-19.** The data is transmitted to the receiver L1~~

~~**20.** Using the outband information (*CFN_cycles, CFN, Position in TBS*), receiver L1 finds the original/earlier combined data and combines it with the received PDU. In this example we assume, that at this point CRC check is successful, thus no buffering is needed anymore.~~

~~**21-22.** Correctly received PDU is transmitted to MAC that calculates the original UEFN from the received outband information and deciphers the PDU.~~

~~**23-24.** PDU is transmitted to RLC layer that can acknowledge it to the peer entity (*note that this is again just an example of possible signalling, the RLC can also wait for more PDU's before sending acknoeledgement).*~~

~~PROPOSAL~~

~~**IT IS PROPOSED THAT THE PRESENTED SOLUTION FOR THE PROBLEM OF (HYBRID ARQ TYPE II/III) & (CFN BASED CIPHERING) IS CONSIDERED WHEN EVALUATING THE REMAINING RADIO INTERFACE CIPHERING ALTERNATIVES.**~~

~~4.REFERENCES~~

~~[1] TDoc TSGR2#2 111 Radio Interface Ciphering, Nokia~~
~~[2] TDoc TSGR2#3 237 Status report from Email discussion on Radio Interface ciphering~~
~~[3] TDoc TSGR1/Ad Hoc #4, Support of Hybrid ARQ Type II/III in the Physical Layer, Siemens~~
~~[4] TS S3.03, UTRAN Overall Description, ver 0.0.5~~