TSG-RAN Working Group 2 (Radio layer 2 and Radio layer 3) ***TSGR2#3(99)237***
Yokohama, Japan 13th to 16th April 1999

Agenda Item: 6

Source: Rapporteur of Ciphering ad-hoc group

Title: Status report from Email discussion on **Radio Interface ciphering**
~~3rd DRAFT VERSION~~

Document for: Discussion

---

1. INTRODUCTION

This paper summarizes the email-discussion on ciphering between 3GPP RAN WG2 meetings #2 and #3.
Discussion on radio interface ciphering was started in 3GPP RAN WG2 meeting #2 based on the following contributions:

[1] TDoc TSGR2#2 111 Radio Interface Ciphering, Nokia
[2] TDoc TSGR2#2 124 Ciphering Function in UTRAN, Alcatel
[3] TDoc TSGR2#2 146 Ciphering Models, Ericsson

The following contributions should also be noted:
[4] TDoc TSGR3#2 177 Ciphering and ARQ dependencies in UTRAN, Siemens
[5] TDoc TSGR2#2 85 ARQ error control techniques, Siemens
[6] TDoc 3GPP S3-99081 Security functionality in the RAN (LS from SA WG3 to RAN WG2)

2. PROPOSED CIPHERING METHODS

The following ciphering methods have been proposed:

1. MAC solution [1]

2. MAC+RLC solution [2] and [3]

3. Ciphering sub-layer [3]

4. Integrity control for CCH [3]

Each of these methods is shortly introduced and analyzed in the following sub-chapters.

2.1 MAC solution

The MAC solution introduced by Nokia [1] uses the same mechanisms for DCH, CCH and DSCH (USCH FFS.). The sequence number (SN) (input for ciphering algorithm) is UEFN which is based on the CFN, which (CFN) is incremented every 10ms. Ciphering is performed as the upmost function of MAC-d entity.

2.1.1 Open questions

- how does the concept work with type II hybrid ARQ ?
- how to initialize the HFN (Most Significant Bits of the UEFN) ?

- how does the concept work on common channels or DSCH, if scheduling is performed on different physical node (e.g. CRNC or NodeB) than ciphering ?

[Alcatel+Nokia] If ciphering is performed in MAC-d, using the CFN, then probably a header has to be added and filled by MAC-c or MAC-sh to indicate the time difference between CFN used for ciphering and CFN used for transmission.

[Nortel] Ciphering in the CRNC. As far as I understand, this fulfills the security requirements, and makes it possible to do something. This means that the MAC-c header would not be ciphered, but all the rest would (from MAC-d upwards). Also, Iub is ciphered entirely. Of course, the common channels on Iur would not be ciphered, but should be sufficient as a protcetion with Iub. Of course, if another solution at MAC level can also cipher Iur, then it would be a likely better candidate (provided it is not too complex). The common channels would work entirely at the MAC-c level with the following:
* In the uplink, the UE would cipher on the basis of a cell specific frame number, and Node B would append the radio frame number so that deciphering can be performed in the CRNC
* In the downlink, the CRNC would cipher based on a frame number which it controls (or learns from the Node B) and which is broadcast under the cell. The UE would then decipher according to it.

[Alcatel] Regarding the proposal from Nortel to perform ciphering in CRNC for common channels, I would like to know whether this implies that cell frame number has to be a 32 bits (currently it is assumed that FN is comprised between 0 and 71). If this is the case I wonder what are the implications on the UTRAN synchronisation scheme (if any). If not, I would assume that you exchanged an initial 32 bits counter and that the FN is appended to this initial counter (as for the RLC scheme). However, there is also a need for the OC counter (as for the RLC scheme), and this might be more complex to manage since the FN sequence is changed at each handover. Since the FN sequence is chnaged at each handover, there is a potential higher risk for loss of synchronisation, in case the new FN reference is not properly decoded by the UE. I do not see this scheme as really much simpler than the MAC+RLC scheme, since you are still using two types of counters, and on top of it, you need to change the counter for common channels at handover...

[Nortel] To reply on your (Alcatel) question, yes, the implication is that for common channels, there needs to be a counter that can be derived from the downlink FN that has at least 32 bits. Still, I do not see any impact on synchronisation because it is not used for other purposes than ciphering, and therefore I would not call it FN. This counter can be derived from the downlink FN, and can be based on some data sent on the BCCH, therefore for handover with common channels. I do not see any problem since it is necessary to read the BCCH to select a cell on common channels (even if some day we would come to not reading the BCCH, there are solutions to this, but it needs to be seen on a real case).

- what happens to CFN after DCH->CCH transition (should also clarify details how CFN is (re)initialized in CCH->DCH transition) ?

[Nokia] When changing from DCH to CCH the CFN is re-initialized to the cell frame number (that is broadcasted on BCCH). To avoid the possibility for reusing same UEFN due to this channel type switch, the HFN is incremented by one at the same time moment.

- are the input parameters "Bearer ID" and "Direction" needed (This should be decided by the group defining the ciphering algorithm - TSG SA WG3) ?

  [Nokia] ~~NEW COMMENT~~ According to [6], bullet point 7 "Avoid multiple use of the same cipher stream", this kind of input parameters seems to be necessary.

- how to cipher CCCH messages (if required) ?

2.1.2 Major benefits

- One mechanism for all channel types and bearer types.
- [Nokia] Only one HFN needs to be initialized and maintained even if several parallel services exist.
- Allows distributed implementation.
- Avoids using same SN twice, even if parallel bearers are multiplexed into same radio frame.

2.1.3 Major drawbacks

- [Nokia] Major drawbacks at a moment are the (non)working with type II/III hybrid ARQ and the ciphering of common channels. (*If these cannot be solved, this alternative can be used only for transparent RLC's*).
- [Alcatel] If ciphering is performed in MAC-d, using the CFN, then probably a header has to be added and filled by MAC-c or MAC-sh to indicate the time difference between CFN used for ciphering and CFN used for transmission. The length of this header will put some constraints on the relative time difference between MAC-c and MAC-d, that might be difficult to prejudge at this stage. The header migh risk to be overdimensioned or underdimensioned. Furthermore, this would look very much as a duplication of counter for UM and AM modes. I see this as a major issue for a pure MAC solution.
  - [Nokia] This is the solution we have also been thinking of, however, we don't see the problem of "prejudging" as severe as Alcatel.

2.2 MAC+RLC solution

This hybrid solution was introduced by Alcatel [2] and by Ericsson [3]. This solution utilizes the radio frame based SN for transparent RLCs and the RLC frame sequence number for non-transparent RLCs. Ciphering is performed on RLC layer for non-transparent RLCs and on MAC layer for transparent RLCs.

2.2.1 Open questions

- is "detection of erroneous de-ciphering", as introduced in [3], really a) possible b) required ?

  [Siemens] Concerning the detection of erroneous deciphering we were not able to really understand the sense of this function. In the most envisaged cases we conclude to a non detected transmission error which should be handled at the connection level,but not by ciphering. Is someone able to explain us this function ?

  [Ericsson] Regarding the detection of erroneous de-ciphering, I think the function should be called detection of a fraud user PDU instead. Take the example that a fraud user is stealing your c-RNTI and sends an RLC PDU. Then the deciphering will leave a PDU with randomly(?) selected bits. This PDU will be send to the RLC entity that tries to interpret the PDU. There is a probability that the PDU will not cause a protocol error to occur. However, if a protocol error occur, we cannot be sure of why it happened. The safest way would probably be to change c-RNTI and restart the protocol. On the other hand, if we know that the PDU was from a fraud user, we can change c-RNTI and continue without restarting the protocol. Well, I have not thought so much about the consequences of a fraud user stealing a c-RNTI, but I think that it would be an advantage if we can detect fraud users as early as possible. It remains to be studied if it is worth the price to do it at RLC level.

[Nokia] I don't really understand how you can detect fraud user by adding extra CRC in RLC layer. If someone can modify your data then he can also "correct" the CRC accordingly. Adding the Message Authentication Code is the way to ensure that the sender was not a fraud user (or more accurately, ensure that the message is from correct originator and that it has not been modified)

- how to use the ciphering on transparent RLCs using common channels (same problem as in 2.1.1) ?

[Alcatel] For ciphering on transparent RLC using common channels, first of all we think such configuration is likely to be very rare since transparent mode is mainly intended for speech, and speech will always be transmitted on dedicated channel. Nevertheless, in order to keep complete flexibility in UTRAN specs, we propose that in case a service using a transparent mode is likely to use a common channel (this should be known by the RRC), the RLC sub-layer attachs a RLC header contaning the SN as for RLC UM mode, and that ciphering is performed as for the transparent mode. This can be considered as transforming the transparent mode in unacknowledged mode, but we do not see any other solution.

[Siemens] We support the position of Alcatel about the ciphering in RLC transparent mode. We did not find the big applications using this transparent mode on the common channels, so that in our opinion the drawback is rather theoretical than real. But we are open for good advices.

[Ericsson] It is a reasonable assumption that it is not possible to use ciphering. If ciphering should be used for message/services using common channels, they need to use non-transparent RLC (either acknowledged or un-acknowledge). I think this is the intent with Patric's comment.

- can same ciphering algorithm be used for both transparent and non-transparent RLCs(this is a question to TSG SA WG3) ?

[Vodafone] I assume that this comes down to using the same algo for both speech and data. Yes, is the answer, if you design the algorithm for both uses. The current GSM and GPRS algorithms are probably not suitable for dual use, or there would have been no need to design the GEA (the GEA can certainly not be used for speech). At our meeting SA3 identified the need to only specify one standard ciphering algo. I presume this algo will therefore be suitable for both speech and data use – comments from SA3?

- how long is the RLC sequence number and what is the exact SN used for ciphering non-transparent RLC-s (RLC sequence number only is not enough) ?

[Alcatel] As proposed in our contribution, a 32 bits counter INITCOUNT is exchanged between UTRAN and UE during connection set up, and the RLC SN only represents the LSB of a ciphering counter being INITCOUNT + RLC SN. This should not put any additional constraint on SN length, that should be first determined according to RLC protocol needs. For GPRS, a binary overflow counter OC has been added and is incremented each time SN exhausts its modulo (see 04.64 Annex A for details). The same approach could be used in our case, and should be acceptable by SA WG3 (since SMG10 agreed with the GPRS ciphering scheme !). In GPRS the LLC SN is 9 bits long, and I guess the UMTS RLC SN might be even greater.

Regarding hybrid ARQ, as mentioned by Siemens in WG3 177/99, I think the RLC SN would be the same for both transmissions of PDU, and thus combining of both PDUs could be performed, but I leave up to hybrid ARQ experts to check whether I am right or not.

[Siemens] The solution proposed by Alcatel is also our, I can confirm that from our point of view it works very well with hybrid ARQ. The length of the SN may depend on the adopted protocol but does not change the principle. Due to the high bit rate handled in UMTS the counter could be extended up to 12 bits.

[Nokia] The difference to GPRS comes from the possibility to have several parallel radio access bearers active simultaneously. For security reasons, the "INITCOUNT+ RLC SN" (='UEFN' in Nokia's proposal) should be different for each RLC. Thus, we must define a mechanism how to initialize "INITCOUNT" (='HFN' in Nokia's proposal) also in cases there is more than one RLC. Also separate 'OC' (='HFN' in Nokia's proposal) must be maintained for each RAB.

- How to avoid using same SN within too short period if retransmissions happen ?

[Ericsson] Regarding the question about how to avoid using the same SN within too short period if retransmisson occurs, I don't understand the problem. Maybe somebody can explain that to me.

[Nokia] If I have understood anything, the requirement for 32bit long input parameter (SN) for the ciphering algorithm is for security reasons. The length of the SN tells directly how often same number is repeated (= how often same ciphering mask is produced, if Kc is not changed). Now, if the SN is based on RLC PDU number then due to retransmissions same SN may be used in less than the _required_ 2^32 * 10ms (~497 days) period. I want to add here that I don't : a) think this is a major problem to solve at least partly b) know whether this is really a problem at all, but I don't see any other reason for the requirement of at least 32 bit long SN, than to avoid repeating same SN within too short time period

[Vodafone] The 32 bit SN is for cryptographic reasons, so the same ciphering mask is not used for different blocks of data. A large number is used so the SN does not cycle through all its values during the use of one cipher key.

[Nokia] As an addition to our comment, as long as the retransmitted data is identical to the original data, there is not this problem at all. The problem is only if the same ciphering key is used to cipher different data, because from the predictable parts of the message the fraud listener may find something about the data. Assuming that retransmission does not mean re-ciphering or the reciphering is done with exactly same parameters as for the first transmission, there is no problem.

2.2.2 Major benefits

- This kind of solution is used also in GSM-GPRS, may be easiest to adopt existing algorithms [Nokia] According to [6] the GSM/GPRS ciphering algorithms will not be reused for UMTS, but a new UEA (UMTS Encryption Algorithm) will be defined, thus this is not a valid benefit anymore.

- Allows distributed implementation

- [Alcatel] As another benefit, the proposed scheme permits to perform ciphering always in the SRNC, and thus permits to cipher transmission on Iur. It also does not put any constraint on the location of MAC entity within UTRAN architecture.

2.2.3 Major drawbacks

- The model includes 2 methods for ciphering. This might increase implementation complexity.

- Rather big sequence number needed for unacknowledged mode RLC

  [Alcatel] I think the approach used in GPRS (and described above) does not put any constraint on SN length in UM or AM mode.

- [Nokia] For each parallel RLC, a separate ciphering counter is needed (using GPRS terminology – "OC", using terminology proposed by Nokia – "HFN")

2.3 Ciphering sub-layer

The separate ciphering sublayer was introduced by Ericsson [3]. The ciphering sublayer would be located on top of RLC and it would add a SN and a CRC for ciphering purposes for each RLC-SDU. This would mean considerable overhead.

This solution was decided to be kept as a "worst case scenario" if no other solutions are proved to work.

2.4 Integrity control

The motivation and mechanism for integrity control was presented by Ericsson [3]. It is an alternative for ciphering on common channel transmission. A Message Authentication Code is attached to each message sent on RACH or FACH.

2.4.1 Open questions

- How is the Message Authentication Code calculated (input parameters, algorithm(s)) ?

- ~~What is the real motivation for integrity control (the arguments presented in [3] should be checked, perhaps a question to SA WG3) ?~~

- Is the integrity control always "an alternative" for common channels or should it be used together with ciphering (a question to SA WG3) ?

- Which signalling messages need to be protected by ~~Should~~ integrity control (this question may need to be solved together with SA WG3)~~be used also for signalling messages on dedicated channels (a question to SA WG3) ?~~

2.4.2 Major benefits

- This feature may be important in addition to ciphering to 'authenticate' messages sent (at least) on common channels.

- From security viewpoint this is safer method than ciphering short (easily predictable) signalling messages on common channels (e.g. cell update, ura update procedures)

2.4.3 Major drawbacks

- Intergrity control requires its own algorithm(s) and key(s) (*needs to be checked*) which adds implementation complexity

3. OPEN QUESTIONS CONCERNING ALL PRESENTED METHODS

- should Kc for signalling link be changed if UE - having connection to two CNs - drops connection with one CN (whose Kc was used for the signalling link) but connection to another CN remains active ?

  [Vodafone] The SA3 requirement in [6] is that the most recently generated cipher key is always used for the signalling plane. Therefore, if one connection drops, then the signalling should not revert to the cipher key established on the other plane, but stay using the most recently generated cipher key, even if that came from the connection which has just dropped.

4. CONCLUSIONS

Three different ciphering mechanisms and one alternative solution for common channels has been introduced.

Methods 1 and 2 (chapters 2.1 and 2.2) are the strongest candidates at a moment.

Method 1 has a clear advantage of using same mechanism and one ciphering counter for all channel types and for all services. However, two major open questions must be solved before the method can be proved to work: 1) the interworking with type II/III hybrid ARQ and 2) ciphering of common channels. For 1) there is no solutions presented at a moment. For 2) two possible solutions have been identified, which should be further studied. If these questions are not solved, this method is applicable only for transparent RLC's.

Method 2 has less open questions and is 'closer' to existing solutions (GMS+GPRS). However, since it seems that for UMTS, a new ciphering algorithm will be defined [6], the possible similarities with GSM-GPRS ciphering do not necessarily mean any big benefits. A major drawback is the additional implementation complexity (in practice, ciphering may need to be implemented into two different protocol layers and for each paraller service a separate ciphering counter has to be maintained). However, if all the open questions of method 1 cannot be solved in time, this may be the only real alternative for '99 spec release. Parts of method 1 can be incorporated into method 2 (= ciphering in transparent mode).

Method 3 is only a "worst case scenario" and if (when) a working assumption based on methods 1 and 2 is established, this alternative should be dropped out from the documents and discussions.

Method 4 (the integrity control mechanism) is not an alternative but rather an additional security mechanism. It seems that ~~The real motivation and the situations when~~ integrity control is a requirement from SA WG3, but many details are not presented yet.~~needed - in addition to technical details - must be solved. At least here SA WG3 should be included in the discussion.~~

5. PROPOSAL

After solutions for the open questions of method 1 has been presented (preferably in RAN WG2 meeting #3), and assuming that support for both methods (1 and 2) still exists, an evaluation sheet should be drawn where pros and cons of each method are listed. Based on this evaluation, a decision can (hopefully) be made.~~The open questions of methods 1 and 2 should be clarified (by email discussion) so that a selection for the basic ciphering method can be done in TSGR2 meeting #3.~~

The selected "working assumption on radio interface ciphering" (with possible open questions) should then be submitted to SA WG3 (or to the proposed joint meeting).~~for evaluation.~~

6. ITEMS FOR LIAISON STATEMENTS TO OTHER 3GPP GROUPS

t.b.d.