Joint *SA3 -GERAN ad hoc on Rel4 and beyond* meeting
Madrid, Spain
27th April 2001

Tdoc S3-010064
Agenda item 5.3
Alcatel

Introduction

Operation in GERAN Iu mode calls for utilising similar security procedures as those used in UMTS. Therefore in GERAN Iu mode of operation, integrity protection and ciphering will be used. The detailed definition of the input parameters has been started in ref. [1]. A number of issues have been raised in the past few months regarding the use and applicability of such procedures in GERAN. This paper intends to summarise some of those issues.

Ciphering issues

Ciphering of layer 2 signalling

It is FFS in ref. [1] whether layer 2 signalling shall be ciphered. In GERAN, this is performed via RLC/MAC control blocks, which are not ciphered today. Two issues can be raised wrt ciphering such blocks:

1. Some RLC/MAC control messages are transported on (packet) common control channels, like resource allocation messages (Packet Uplink Assignment and Packet Downlink Assignment) when there is no TBF already (recently) established for the Mobile Station. Other messages, even though they are sent on Packet Data Traffic Channels, must be read by several users, e.g. in phase of contention resolution at the beginning of a TBF set-up. Those kinds of messages cannot be ciphered since it is not possible to use one key or another, given that the identity of the target MS is not known by the GERAN. Other messages, truly dedicated to one user, contain however a so-called “distribution part” as well as a MAC header which must be read by all users; ciphering such messages would need to ensure that those parts are not ciphered.

2. When a user has moved under coverage of a drift BSS, that drift BSS will be responsible for establishing layer 2 connections at RLC/MAC level with the MS. Therefore, the drift BSS will be responsible for allocating resources for TBFs, maintaining those and releasing them. Indeed the RLC and MAC layers controlling an MS are always those sitting in the drift BSS (when the user has moved out of its serving BSS) since there is no user plane on the Iur-g, i.e. there is no RLC/MAC-d vs MAC-c split like in UTRAN. Then, because the UMTS Security Context, including CK and IK, is only present in the Source BSS, it is not possible for the drift BSS to perform ciphering at RLC/MAC level. The only way to do ciphering in that case would be to make known to all BSSs neighbouring the Serving BSS of an MS its Security context. Indeed it must be known in advance of detecting that the MS has moved out to a Drift BSS coverage since e.g. a TBF may be required to be set-up for sending the CELL UPDATE.

   NOTE: The terminology UMTS Security Context is proposed to be re-used for GERAN since the same algorithms will be re-used and therefore the same elements of that context should exist in GERAN and in UTRAN. This needs to be validated by S3.

Given the above considerations, it appears that ciphering of layer 2 control blocks in GERAN cannot be done in all cases; even some given messages may or may not be ciphered. **It is therefore proposed that RLC/MAC control blocks in GERAN are not ciphered.**

Input parameters

Current ciphering input parameters in GERAN include the RBid; it is shown as ffs in ref. [1] whether this is transported in the RLC/MAC header. As long as there is a unique mapping between RBid and TFI (identifier of the RLC/MAC connection), then the inclusion of the TFI in each RLC/MAC block is sufficient for the receiving entity to derive the corresponding RB and use the appropriate input for deciphering the contents. Section 6.1.4 of ref. [1] clearly states now that one RLC instance carries data from one RB and uses services from one TBF. **Therefore it is proposed that the RBid is not transported in each RLC/MAC header and that the ffs be removed.**

Ref [1] also shows that it is FFS whether the GSM TDMA Frame Number or the HFN is used to generate the ciphering mask in GERAN when in Transparent RLC mode. In Non transparent RLC mode, the HFN is proposed to be used. The size of the HFN is also still FFS. However if the HFN corresponds to the HyperFrame Number in the TDMA frame numbering scheme, then, according to ref. [2], one HFN = 2048*51*26 TDMA Frames = 2715648 Frames, which requires 22 bits. Note also that when using a SPSCH to send data, the radio unit is called a radio block and spans over 4 frames; when using a DPSCH 4 or 8 frames are used for each data unit. What should actually be used for HFN should be clarified.

Ciphering of RRC messages to be sent over Iur-g

Another issue is how to perform ciphering of RRC messages addressed/coming to/from an MS that is under coverage of a drift BSS given there is no user plane on Iur-g. Indeed such messages are transported over a DCCH logical channel over the Iur user plane when ciphering needs to be done in UMTS so that the RLC layer in the serving RNC performs the ciphering. Since only the control plane on Iur-g is available then it does not appear possible to transfer messages that require ciphering to an MS that is under coverage of a drift BSS. If the only RRC/NAS messages, which need to be ciphered, are those containing new U-RNTI then in that case, it could be specified that a Serving BSS Relocation is performed in GERAN when such messages are required to be sent. Another possibility would be to make the CK and IK keys available in the drift BSS but this would require a ciphered link between the two BSSs before being able to exchange such security information.

Integrity protection issues

Assumptions in GERAN

The latest status in GERAN is the following:

- RRC messages shall be integrity protected with a 32-bit MAC-I field except the following ones:
  - Paging Request Type 1-3
  - RRC Connection Request
  - RRC Connection Setup
  - RRC Connection Setup Complete
  - RRC Connection Reject
  - System Information Type 1-20
- It is FFS whether other RRC messages will be integrity protected with a shorter MAC-I field.
- It is FFS whether RLC/MAC control messages are integrity protected.

Length of the MAC-I field

The main issue with appending a MAC-I field of 32 bits to RRC or RLC/MAC control messages is that it will obviously make those messages longer and therefore call sometimes for additional segmentation due to the limited layer 2 payload size. This will increase the time to send those messages and also increase the probability of radio loss. One possible solution would be to have a variable MAC-I size for a given message (those which are less sensitive or sent less frequently, ideally all), i.e. the size of the MAC-I would depend on the number of bits left in the last layer 2 block carrying that message, with a minimum number of bits required (e.g. 8) and a maximum number desired (e.g. 32 as agreed in GERAN. Does that make any sense from a security standpoint ?

Another possibility would be to have fixed MAC-I sizes per RRC message type and agree on shorter MAC-I fields for messages that are sent most frequently and that are the most sensitive to radio loss and longer transfer time.

Integrity protection of RLC/MAC control messages

When the MS is under control of a drift BSS and RLC/MAC control messages are used to perform resource allocation, another issue is how it is possible to perform integrity protection of such messages. Indeed the Security Context and especially IK is not available in the drift BSS. Therefore it does not appear possible to integrity protect such messages, even when they are not sent on Common Control Channels.

Another issue is again related to the appending of the MAC-I field, even though RLC/MAC control messages performing resource allocation function should not be that frequent in the scope of the delayed TBF release feature. This will indeed cause additional segmentation. Studies so far have shown that the current limitation in terms of segmentation of those RLC/MAC control messages would not be infringed with the appending of 32 bits. However, in the scope of the support of multiple TBFs per MS per direction, this appending would limit the number of TBFs that can be established/modified/released within a single RLC/MAC control message.

Another issue is related to when an uplink TBF is allocated in fixed MAC mode. Indeed Packet Uplink Ack/Nack messages can contain resource allocation information. Therefore this would need to be integrity protected. However, such messages are sent very frequently during a TBF and therefore this would leave much less space for encoding acknowledgement bitmaps and add a significant overhead to the TBF if it cannot fit in one block (likely case).

Therefore, integrity protection on RLC/MAC control messages appears questionnable.

Vocabulary

Iur-g	Iur like interface between GERAN nodes
TBF	Temporary Block Flow, i.e. a “packet” connection between the MS and one GERAN only.
TFI	TBF Identifier

References

[1] 3GPP TS **43.051** v5.1.0 “Technical Specification Group GSM/EDGE Radio Access Network; Overall description - Stage 2; (Release 5)”

[2] 3GPP TS **45.002** v4.0.0 “Multiplexing and multiple access on the radio path; (Release 4)”