TSG-RAN Working Group 3 meeting #2
Stockholm 15th – 19th March 1999

TSGW3#2(99)167

Agenda Item: 7.1, UTRAN Architecture (S3.01)
Source: Siemens, Italtel
Title: **Ciphering and ARQ dependencies in UTRAN**
Document for:

---

1 INTRODUCTION

In [1] it is stated that the "AN needs to support encryption to prevent from eavesdropping at the radio interface.": this means that a ciphering procedure terminated in UTRAN shall be defined.
A suitable ciphering algorithm needs to be defined in order to fulfil this requirement.
For example, in GSM the ciphering sequence is derived by encoding the ciphering key with a time variable encoding sequence.
This procedure has two main reasons:

1) the short ciphering key can be extended to fit the radio burst length,
2) the ciphering sequence obtained is not fixed, being a result of a coding process with a variable sequence. This increases the security of the process.

In the recalled example the encoding sequence is defined for GSM as the Frame Number (see [3]) and for GPRS as the LLC Frame Number (see [4], Annex A).

In UTRAN error control techniques have been proposed for NRT services, which rely on Automatic Repeat Request (ARQ) mechanisms.
In case when an errored frame is received, a frame retransmission is triggered, whose type is dependent on the retransmission method.([5]).
An incremental usage of the information contained in subsequent retransmissions of the same PDU by means, for example, of maximum likelihood algorithms applied to single bits could improve both reliability and efficiency.

From the description it is clear that ciphering could have undesirable interactions with this error control technique, for example if the Frame Number were used in the ciphering process: two subsequent transmissions of the same PDU could not be combined as described above because the relevant FNs would be different and, consequently, the ciphered bit stream.

It is proposed to define the ciphering algorithm in a way that makes it independent from packet retransmissions, in order to allow the application of ARQ algorithms without constrains.

2 REFERENCES

[1] Universal Mobile Telecommunications System (UMTS) Services provided by the UMTS Radio Access Network URAN UMTS 23.10 version 3.0.0 (1999-02)
[2] RAN Overall Description - 3GPP S3.01 draft V0.0.1 1999-02
[3] GSM 03.20 version 6.0.1 Release 1997 - Digital cellular telecommunications system (Phase 2+); Security related network functions
[4] GSM 04.64 version 6.2.0 Release 1997 - General Packet Radio Service (GPRS); Mobile Station (MS) - Serving GPRS Support Node (SGSN) Logical Link Control (LLC) layer specification
[5] Tdoc. SMG2 UMTS-L23 307/98 ARQ error control techniques; Siemens; Milan, October 6-9, 1998

3 PROPOSAL

It is proposed to add to Chapter 9.1.4 of [2] and in the correspondent chapter of S3.01 the following text:

The ciphering mechanism shall not interfere with ARQ algorithms and shall not prevent the implementation of ARQ decoding incremental methods.