3GPP TSG SA WG3 Security — S3#29 **S3-030409**
15 - 18 July 2003
San Francisco, USA

Agenda item: MBMS

Source: Samsung Electronics

Title: Some consideration about Ciphering Key usage timing

Document for: Discussion and Decision

1. Introduction

There are two correlated issues about Ciphering in MBMS. The first is the distribution of ciphering key for MBMS and the second is the method for the indication of new CK usage for that MBMS. The good ciphering key distribution can make the illegal UE not to receive MBMS and many contributions related to this issue have been presented during previous meetings. Regarding the second issue, the UE should know when it uses new CK for MBMS in order to decrypt MBMS data correctly. Otherwise, the UE can't decode MBMS data.

In this document, several scenarios related to CK usage timing for MBMS are analyzed. Based on our analysis, we will propose the way forward regarding this issue.

2. Autonomous usage based on absolute timing

As stated in TS 25.402[1], "…In UTRAN although a common timing reference among all the nodes could be useful, it is not required. In fact different nodes' counters, even if frequency-locked to the same network synchronisation reference, may be not phased aligned." As MBMS is intended to serve many users at the same time, these users for one service may likely be dispersedly served by different nodes within the same BMSC serving area. Thus, although UEs located within the same node serving area may be able to achieve a common timing reference, it shall be quite difficult to set a common timing reference for all these UEs for one specific service. This means that UEs' autonomous usage of new ciphering key based on the absolute timing, such as "new ciphering key shall be used at 8:00 am" is not possible to be used.

3. Autonomous usage based on relative timing

Currently, it is agreed within SA3 that only application level ciphering shall be available in MBMS; double ciphering (i.e. both application level and network level) shall not be used in MBMS. In order to prevent the ciphering information from leakage, application level ciphering information can be

transparent to the network level nodes such as RNC. In this case, RNC shall make no difference between the MBMS traffic data encrypted with the old ciphering key and that encrypted with the new ciphering key. As RNC itself shall be able to adjust its transmission considering the number of the users, transmission power, available resource etc, UE shall not be able to know when/where to separate the data encrypted with the new ciphering key from the data encrypted with the old ciphering key. This means that UEs' autonomous usage of new ciphering key based on the relative timing, such as "new ciphering key shall be used instead 15 minutes after the old key is used" is not possible to be used.

4. Autonomous usage based on data volume

Another possible mechanism is based on UE's measurement of data volume. For example, UE and the network (mainly BMSC) shall agree beforehand that new ciphering key shall be used instead after 1M data encrypted with the old ciphering key is received. As MBMS is intended to server many users, either point-to-point or point-to-multipoint transmission modes can be adopted by the RNC itself to use the radio resource efficiently. This mechanism which is based on UE's measurement of data volume seems feasible when point-to-point transmission mode is adopted, where UE shall be able to know the possible data loss and request the RNC for re-transmission to combat this data loss by using dedicated channels. But for point-to-multipoint transmission mode where a lot of users sharing the same service over the common channel may reside within one RNC, it shall be quite difficult for the UE to know when/whether and/or how much data loss occurs. Also, considering system load, it shall be unfeasible for the RNC to combat each UE's data loss by using network layer re-transmission for each of them. This means that UEs' autonomous usage of new ciphering key based on the data volume, such as "new ciphering key shall be used instead after 1M data encrypted with the old ciphering key is received " is not possible to be used as well.

5. Conclusion

Based on these analyses from chap 2 and 4, it seems that the autonomous method for new CK indication is not feasible for MBMS. This means that we need another method for the CK usage and the proposed method should be made in consideration of characteristics of MBMS and UMTS network. So, we proposed SA3 should start studying a method for new CK usage indication.

6. Reference

[1] 3GPP TS25.402, 3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Synchronisation in UTRAN Stage 2