3GPP TSG SA WG3 Security — adhoc **S3z030005**
3 - 4 Sept 2003
Antwerp, Belgium

Agenda item: MBMS 6.3

Source: Huawei Technologies Co., Ltd.

Title: MBMS re-keying : Analyze PTP and LKH

Document for: Discussion and Decision

1 Introduction

Several methods have been proposed for MBMS re-keying. This contribution analyzes several issues that may occur when re-keying with PTP and LKH. The issues covered include “Radio/network resource”, “Time-triggered/event-triggered re-keying with the burden of network”, “Security”, and “Complexity”. Based on this discussion, some of the problems are clearly identified which should make the final decision easier.

2 Discussion

2.1 Radio/network resource

- **Network resource**

  1. With the LKH method, users belong to a subgroup and the subgroup key is shared with all subgroup users. When the server needs to distribute the Traffic Encryption Key (TEK) to users, it can encrypt the TEK with a distinct subgroup key for each subgroup.

  With the Point-to-point method, when the server needs to distribute the TEK to users, it needs to encrypt the TEK with a distinct Key Encryption Key (KEK) for each user.

  From the perspective of the server encrypting the TEK, it is believed that LKH can save more network resources than PTP.

  2. The encrypted TEK is transmitted from the BM-SC to RAN passing through the GGSN and SGSN. This can not be optimized. The encrypted TEK by KEK will be transmitted individually by the RAN. The encrypted TEK by subgroup key may need to be sent to multiple cells. However if each user of the subgroup is located in a different cell, the network resources used would be equal to PTP mode. (It would be very difficult to ensure that all subgroup users were located in the same cell.)

- **Radio resource**

Efficient use of radio resources is MBMS main goal. We should not design a solution where key-exchange messages require extensive use of radio resources.

LKH can distribute TEK with point-to-multipoint in common channel. PTP can distribute TEK with point-to-point in common channel too. Point-to-point can be implemented such that the encryption is point-to-point, but the transmission is to multiple users in a common channel.

As previously discussed, when the users of the same subgroup are in different cells, and when there is only one user in a cell, LKH still uses the whole channel for one user.

2.2 Time-triggered/event-triggered re-keying with the burden of network

- Event-triggered re-keying seems ideal because the server can change the TEK when a user is joining or leaving. The LKH model is good for this in some situations.

When a user leaves a subgroup, the corresponding subgroup needs to change the subgroup key between the server and each user with point to point. The other subgroups don't need this process so the server can change the TEK based on subgroup key. In this case, LKH is efficient. Because PTP needs to distribute the TEK to each user in group, it is less efficient than LKH.

On the other hand, if there are users leaving in each subgroup, each subgroup key should be changed with point to point, and then change the TEK with each subgroup key. In this case, LKH is less efficient than PTP.

If users are frequently joining or leaving, the burden of network to change the TEK is huge whether it is LKH or PTP.

- Time-triggered

With time-triggered re-keying, the TEK changes based on time interval. There may be a current TEK and next TEK, and when time condition is met, the users switch to the next TEK. Before users switch to next TEK, the next TEK should be distributed to all users. LKH and PTP both can be applied.

According the quantity of users and desired level of security, the time interval can be decided. In one time interval, all users must gain the next TEK, and next time interval all users can use this next key. With the PTP method, the problem is avoiding all users requesting and receiving the TEK at the same time. With the LKH the method, the network has to maintain the whole LKH mechanism and the other related mechanisms. E.g. what time the subgroup key should be changed and what time the next TEK should be distributed to users.

2.3 Security

With the PTP method, the TEK is encrypted with a point-to-point key. With the LKH method, the TEK is encrypted with subgroup key. It is obvious that the group key is less safe than the unicast key.

2.4 Complexity

From the view of the implementation complexity, PTP needs to solve the following problems:

1 generate KEK

2 develop a policy to avoid simultaneously distributing TEK to users

LKH needs to solve the following problems:

1 generate the user specific key to protect the subgroup key distribution

2 generate the subgroup key

3 maintain the subgroup

4 have policy to update subgroup key (event-trigger re-keying may not need this)

5 update TEK with some policy (event-trigger re-keying may not need this)

3 Conclusion

We have analyzed several issues related to the PTP and LKH re-keying methods. Although there may be additional criteria to consider, we believe that issues should be clearly identified and analyzed before selecting a re-keying solution. By doing this type of comparison, our ultimate decision should be easier to make.

Proposal : we recommend summarizing the potential problems and corresponding solutions for all re-keying methods before making a final solution.

4 Reference

[1] 3GPP TS33.246, Technical Specification Group Services and System Aspects; Security; Security of Multimedia Broadcast/Multicast Service; (Release 6), version 0.1.1.

[2] TD S3-030349 MBMS re-keying: PTP with periodic re-keying

[3] TD S3-030238 Levels of MBMS key hierarchy

[4] TD S3-030054 Text proposal for MBMS re-keying based on LKH principles