3GPP TSG-SA WG3 Security — S3#30 **S3-030580**

6 – 10 October 2003

Povoa de Varzim, Portugal

Source: **Nokia**

Title: **MBMS – Overhead of the Re-keying**

Document for: **Discussion**

Agenda Item: **7.20**

1. INTRODUCTION

This discussion paper estimates overhead in data amount in combined [1] and simple point-to-point re-keying methods [2]. The overhead is considered from the point of view of UE, radio resources and BM-SC. The following calculations are rough estimations and they are based on typical RTP traffic and educated guesses.

2. OVERHEAD

The Figure 1 presents the sequence diagrams of the combined method and the Figure 2 presents the sequence diagram of the simple point-to-point method.

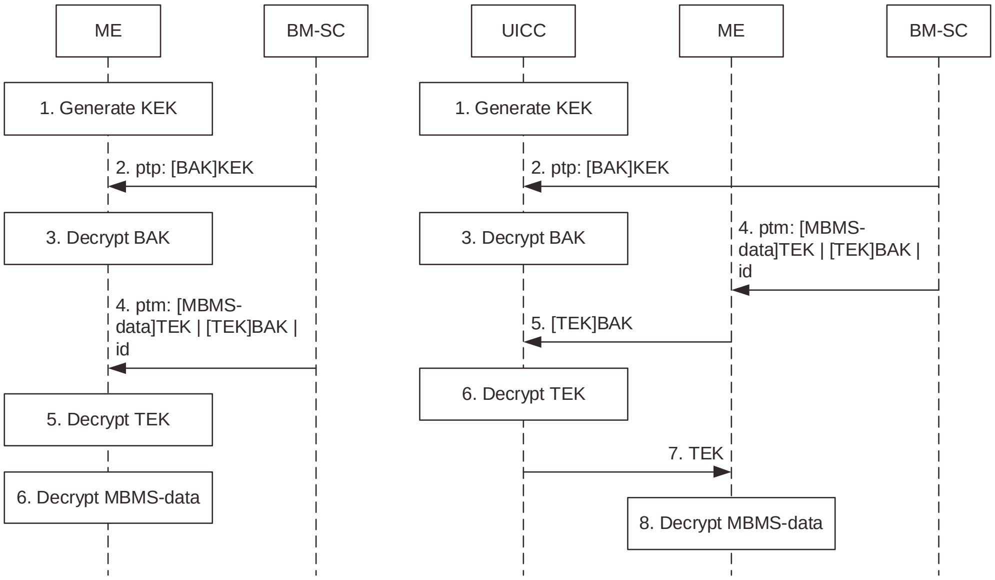

Figure 1. Combined Method Sequence Diagrams

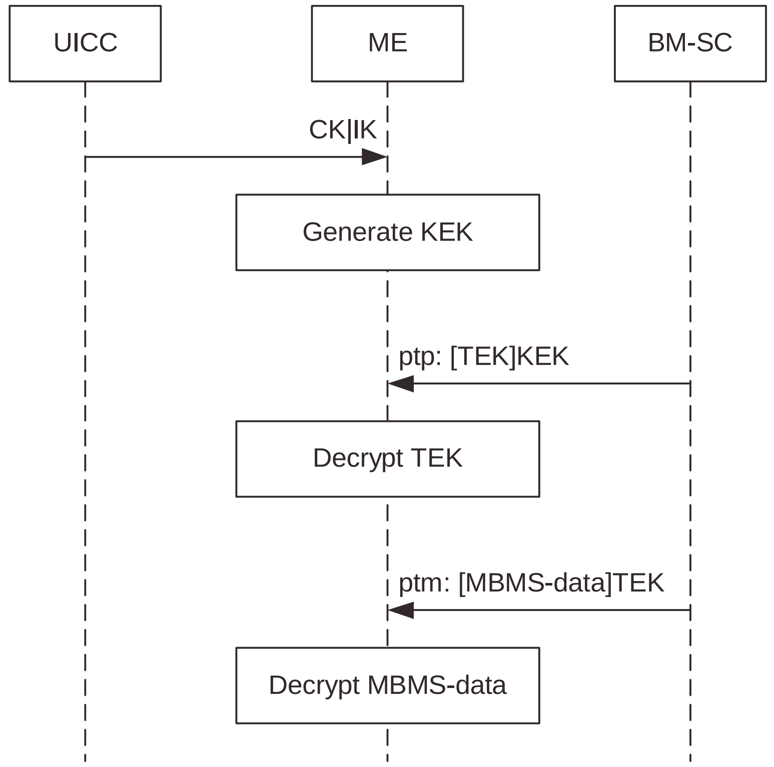

Figure 2. Simple Point-to-Point Method Sequence Diagram

2.1 Assumptions

Calculations are based on the following common assumptions:

- Minimum bitrate of multimedia traffic is 64kbit/s
- Each multimedia traffic payload contains 20msec sample, thus there are 50 multimedia traffic messages in second
- The length of the payload is (64kbit/s) * (byte/8bit) / 50 = 160 bytes
- The length of the MBMS header without a new key is 4 bytes
- The MBMS header always includes a current key identifier. The current key identifier identifies the current traffic encryption key, which is used to encrypt the payload.
- The length of headers is 40 + 16 + 4 = 60 bytes (IPv6 header + UDP header + short MBMS header)
- The total length of the MBMS data packet is 220 bytes
- The length of the MBMS traffic encryption key is 16 bytes (128 bits)
- The number of users of service is 100 000
- Packet loss is 0.2% in multicast. Unicast traffic has typically higher packet loss in high load situations, but multicast traffic has low packet loss, because it uses network more efficiently.
- The traffic encryption key is changed in every 10 minutes
- 10 MBMS users / cell

The combined method specific assumptions are:

- MBMS header includes a current key identifier, a payload key identifier and a key flag. If the flag is set then the key is included into the message.
- The re-keying of BAK is performed in every 24 hours. This is a rare event, thus it has not an effect on overhead calculations.
- An encrypted TEK is repeated into average every 50th MBMS message
- A new traffic encryption key is included more than once into the MBMS headers before the key is actually used.

The simple point-to-point method specific assumptions are:

- MBMS header includes a current key identifier
- The p-t-p re-keying messages uses a common channel
- The length of the p-t-p re-keying request message is 40 + 16 + 4 + 16 = 76 bytes (IPv6 header + UDP header + short re-keying header + key)
- The length of the p-t-p re-keying response message is 40 + 16 + 4 = 60 bytes (IPv6 header + UDP header + short re-keying header)

2.2 Combined Method

In the combined method, a traffic encryption key is encrypted using another key (BAK) and the encrypted TEK is appended to the MBMS data message. The overhead without the key is (220-160)/160 = 37.5%. The encrypted traffic encryption key is sent in average every 50th message, so overhead is ((220 bytes * 49 + 236 bytes) - (160 bytes *50)) / (160 bytes * 50) = 37.7%. Thus the additional overhead is 0.2%.

There are 50 * 60 * 60 * 10 = 1 800 000 MBMS traffic messages in 10 hours. The encrypted traffic encryption key is sent in every 50th message, so re-keying causes traffic 16 bytes * 60 * 60 * 10 = 563 KB / 10 minutes.

A new traffic encryption key should be sent more than once before the key is changed. It is not practical send the key in sequential packets, because lost packets are typically in bursts. If there is 0.2% packet loss and a new traffic encryption key is sent in three unsequential packets before the key is actually changed then probability of second interruption is (0.002)^3 = 0.0000008%. It should be noted that these packets should be sent in certain time frame (in one second in this example), because otherwise joining delay increases.

2.3 Simple Point-to-Point Method

The simple point-to-point method uses a request/response message pair to re-key a single UE. It is assumed that there are 100 000 users, the length of the request is 76 bytes and the length of the response is 60 bytes. Thus the re-keying causes traffic 100 000 * (76+60) bytes = 13 281 KB / 10 minutes. Re-keying request and response messages are sent once in ten minutes, so there is no additional overhead for each UE. The overhead for each UE is 37.5%, because of headers of MBMS traffic messages. The overhead for BM-SC is ((1 800 000 * (220 - 160) bytes) + (100 000 * (76 + 60) bytes))) / (1 800 000 * 160 bytes) = 42.2%. It is assumed that each cell has 10 MBMS users, so the overhead for cell is (((1 800 000 * (220 - 160) bytes) + (10 * (76 + 60) bytes))) / (1 800 000 * 160 bytes) = 37.5%. The packet loss was ignored in above overhead calculations, because it is insignificant in normal load situations.

3. CONCLUSIONS

The following table has a summary of overheads in data amount:

Overhead in:	Combined method:	Point-to-point method:
UE	37.7%	37.5%
Radio resources (cell)	37.7%	37.5%
BM-SC	37.7%	42.2%

Note: The 3GPP2 adopted two-tiered method [3] was not considered as it is assumed to fall in between of these two analysed models.

The combined method is more scalable, because re-keying is performed using point-to-multipoint messages.

4. REFERENCES

[1] TDoc S3z030020, Combined Re-keying Method, Nokia

[2] TDoc S3-030349, MBMS re-keying: PTP with periodic re-keying, Huawei

[3] TDoc S3-030360, Levels of Key Hierarchy for MBMS, Qualcomm