3GPP TSG SA WG3 Security **S3-020364**

9th – 12th July, 2002

Helsinki, Finland

Agenda Item:

Source: Lucent Technologies

Title: Encryption for MBMS Multicast

Document for: Discussion & Decision

1. Introduction

MBMS multicast mode allows the unidirectional point-to-multipoint data transmission from a single source to a multicast group in a multicast area. To ensure that only legitimate users can receive the service, a reliable and secure multicast encryption protocol is necessary.

For the point-to-point service, the encryption key distribution is straightforward. The encryption key CK is provided from the CN to the RNC and from the USIM to the UE. The connection between the RNC and UE is protected by the CK. This encryption key is set up during the authentication stage and is generated based on each USIM private key. Because each USIM has its own private encryption key, the encryption key is only used for dedicated logical channels.

If the multicast service is carried on the dedicated channel, the same key CK can be used to encrypt the multicast traffic. This mandates that each UE receive its own data streams encrypted by its own ciphering key. However, since the main objective of introducing MBMS is to save network and radio resource, multicast traffic is very likely to be carried on the channel received simultaneously by several users. Currently, 3GPP has no specifications on ciphering on non-dedicated channels.

2. Application layer encryption and RLC/MAC encryption

There are two layers where data ciphering can take place.

1. Application layer encryption
2. RLC/MAC layer encryption

If application layer encryption is used, all the data traffic has to be encrypted using the same ciphering key. The ciphering key may be distributed to the group members through protected channels. Although this is simpler than having many keys, the key distribution protocol may not scale as the number of subscribers grow. For example, if a multicast group member decides to terminate the service, the ciphering key has to be updated to prevent the terminated member from receiving the service. This requires that all of the existing members be notified of the key update. Because the key-updating message has to be securely distributed to the individual members, it has to be carried on the protected channels. The volume of the key-updating message is proportional to the number of group members and frequency of the membership changes. For large multicast groups, this is not desirable.

If RLC/MAC layer encryption is used, the data multicast to the different cells or carried on the different transport channels can be ciphered with different ciphering keys. If a UE leaves the multicast group, only the UE’s who shared the same ciphering key with the departing UE need to be updated with the new ciphering key. The rest of the UE’s can continue using their keys. Although having different keys may present other challenges, compared with application layer encryption, this solution saves radio resource and signalling overhead involving key updating, especially when the group size is large and membership changes frequently.

Another benefit of introducing RLC/MAC layer encryption is that the carriers are given more control over the application services provided over their wireless infrastructures. Since the set-up of the encryption key involves USIM identity, the cost of the multicast service can be directly associated to the UE. The RLC/MAC layer encryption for multicast service means that the Network should be aware of the multicast service provided and be able to update the ciphering key used in RLC/MAC when group membership changes. The ciphering algorithms used for dedicated channels could be reused for non-dedicated channels, but the session key generation and distribution procedures need to be defined for multicast services and require further study.

3. Conclusion

The existing security features in 3GPP are not adequate for supporting MBMS multicast mode. Ciphering can be done at two layers: application layer and RLC/MAC layer. While application layer encryption with a single key may be simpler, it may not scale well when the multicast group size is large and membership changes frequently. On the other hand, the RLC/MAC layer encryption is scalable and also gives carrier more control over multicast service provided over UTRAN but adds complexity. Further study is required to determine the implications of the different options and associated solutions.