An Architecture and Key Management Approach for Maintaining Privacy in Location Based Group Services

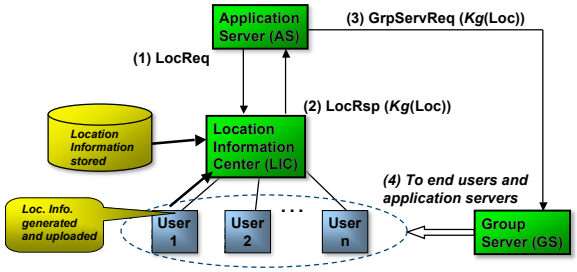
Y. Sun, P. Liu, P. Kermani, T. F. La Porta

Location based services are becoming increasingly important to the success and attractiveness of next generation wireless systems. It is a challenge to maintain location privacy while still providing the flexible access to location information required to enable a rich set of location based services.

Design Philosophy

- user controlled location information access
- a group of entities defined by user to access its location information
- hierarchical coding of location information with different granularity
- providing keys to the group members to decrypt location information

LBGS architecture



Service Example

Location Based Instant Message Service:

For example: alert is sent to subscribers when a buddy is within a certain proximity.
Two models:

- end users and LIC are members of the location information group
- IM server is also a member of the location information group

Service Characterization

WHERE location information is generated
- by the end device or the network.

WHERE location information is stored
- in the end device, network, or not at all.

HOW information is accessed
- pushed at various intervals or pulled on-demand.

with WHOM the location information is shared
- information may be shared with other end users, network servers, or both.

MIKEY and LKH

MIKEY as the basis of our protocol:

- lightweight protocol.
- adopted by the 3GPP MBMS group for 3G multimedia services

Two limitations of MIKEY:

- no hierarchy of group key servers support
- no re-keying support

Basic Solution:

- apply LKH to MIKEY to improve scalability with re-keying.

MIKEY-LKH Applied to Hierarchical Coding

Coding by Information Class

A user subscribes multiple groups to receive multiple granularity of location information. The cost of re-keying :

$$C_{class}(N) = \sum_{i=1}^{C_{max}} r_i (2K(\sum_{j=1}^{i} \log((\sum_{m=j}^{i} r_m) \cdot N)) + iP)$$

Coding by Group

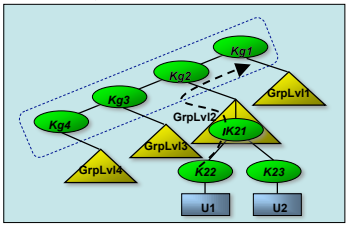
Each group re-keys independently of other groups. The cost of re-keying :

$$C_{group}(N) = \sum_{i=1}^{C_{max}} r_i (2K \log(r_i \cdot N) + P)$$

Nested Hierarchy Coding

This relies on information hierarchy
The cost of re-keying :

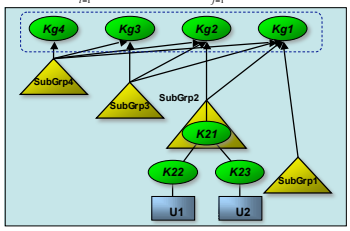
$$C_{nested}(N) = \sum_{i=1}^{C_{max}} r_i (2K(\log(r_i \cdot N) + i) + P)$$



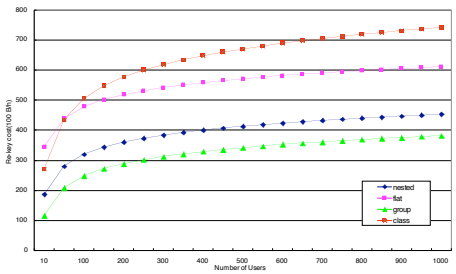
Flat Coding

A flat relationship among sub-groups.
The cost of re-keying :

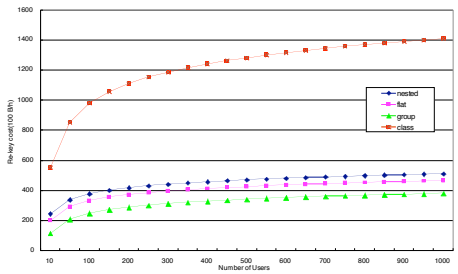
$$C_{flat}(N) = \sum_{i=1}^{C_{max}} r_i (K(2\log(r_i \cdot N) + \sum_{j=1}^{i} (c - j + 1)) + P)$$



Performance Evaluation



Hierarchical LKH re-keying overhead (r1:r2:r3:r4=30:10:8:5)



Hierarchical LKH re-keying overhead (r1:r2:r3:r4 = 5:8:10:30)

Summary of Evaluation

Method	Class	Group	Nested	Flat
User Storage	-	+	-	-
Multi-cast groups	-	-	+	-
Re-key	-	+	0	0
Message delivery	-	+	+	-
Computing at end device	-	+	-	-
Flexibility	+	0	0	+

Note: + corresponds to an attractive characteristic, - corresponds to a drawback, and 0 is neutral.