Location Privacy vs. Service Flexibility

Location Privacy is critical to provide LBS
- user controlled location information access
- a group of entities defined by user to access its location information
- Flexible access to location information is important to support desirable service model and easy deployment
  - hierarchical coding of location information with different granularity
  - providing keys to the group members to decrypt location information

LBGS Network Diagram

MIKEY and LKH

MIKEY as the basis of keying protocol
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

Further Extension – 4 schemes:
- Coding by Information Class
- Coding by Group/ Hierarchy Coding / Flat coding

KeyTree Class Hierarchy

MIKEY and LKH

KeyTree Class Hierarchy

M_AVL Key Tree Algorithm

Realistic Application Practice and Analysis

Flexible Extension for Different Application:
- Small Group Size(10-50)
  - Sample application – Instant Message Service
    - Small number of user update/Small number of user subscription
    - Small number of re-keying: multicast or uni-cast
  - Medium Group Size(100-500)
    - Sample application – IM/Game/Company Group Service
      - Medium number of location update/ Medium number of user subscription
      - Medium number of re-keying: multicast