1. Problem definition

Location privacy violation
- Collected location information can bring about privacy violations such as crime and unwanted advertisement.
- To prevent privacy violation, many research exists on preventing privacy violation (location k-anonymity, pseudonym).
- However, existing research is difficult to apply to real-world LBS (Location-based Service) because it’s data utility-privacy tradeoff.

Our solution
- We propose collaborative caching technique which share query results among users to overcome the privacy-data utility tradeoff.
- Proposed technique is analyzed in terms of privacy, broadcasting cost and update cost.

2. Proposed architecture

3. Collaborative caching technique

Necessary of collaborative caching
- Location k-anonymity is used to reduce the possibility to infer a user’s exact location.
- However, it generates an extra number of query results.
- To reduce an extra number of query results, we propose P2P collaborative caching technique based on counting bloom filter.

PDS grouping algorithm
- Based on P2P, no trusted third party to manage entire query information. Thus, broadcasting costs are huge burdensome in P2P.
- We propose a PDS grouping algorithm for reducing broadcasting cost.

- Single-bit indexing
  - The black squares represent the selected bits in bloom filter, and the gray squares show the bits that were selected at an ancestor. The red triangles represent the sub-trees.

- DHT-based p2p network using chord protocol
  - PDSs establish a DHT-based P2P network using chord protocol and each PDS’s count bloom filter index for POI. In this example, initial PDS is PDS A.
  - After the single-bit tree is built, the PDS assigns its address to the single-bit tree’s corresponding node.

4. PDS grouping analysis

Privacy
- x1, x2, and x3 are the elements inserted into the bloom filter BF (S).
- v1, v2, and v3 are the hiding elements.
- Bloom filter returns the true for x1 element, but it is deniable because v1, v2, and v3 also set the x1’s bit position in the bloom filter.

Deniability: If the bloom filter returns a true, we can deny the existence of the data by the bloom filter’s false-positive property

Broadcasting cost
- The number of PDSs assigned to a leaf node is reduced while the single-bit tree’s depth increases.

Update cost
- When data stored in the PDS is changed, false-positive and false-negative errors may occur

$$\rho = S \times \frac{X_0}{|X_0| + |X_1| \times \left(1 - \frac{1}{m}\right)^{|X_1|}}$$

- False-positive probability
- False-negative probability

5. Experiment

- Simulation results show that the proposed technique achieves sufficient privacy protection while minimizing system performance degradation.