Authentication of \( k \) Nearest Neighbor Queries in the Presence of Obstacles

Sharifa Tahmida Kaniz, Jibon Naher Boishakhi

Department of Computer Science and Engineering (CSE), BUET

Introduction

Location-based services:
- Where am I?
- What is here around me?

With the popularity of LBS, the usage of data outsourcing has grown rapidly over the past few years.

Motivation

- In data outsourcing paradigm, results may be altered:
  - For personal benefit of SP
  - To reduce computational overhead
  - Hacked by a third party

- How can a client become sure that SP has returned the correct result?

Motivation

- Must have some authentication strategies

Location-based services:
- Where am I?
- What is here around me?
- Where is the nearest restaurant?

With the popularity of LBS, the usage of data outsourcing has grown rapidly over the past few years.

Problem Definition

A pedestrian’s path may contain obstacles like buildings, trees or lakes. A \( k \)NN query in the obstructed space returns first \( k \) nearest POIs e.g., restaurants, hospitals or markets that have \( k \) smallest obstructed distances from the query point \( q \).

Verification Object Construction by SP

- Two MR-trees:
  - POIs tree
  - Obstacles tree
- Each VO contains 3 types of entities:
  - Data objects of visited nodes
  - MBR and hash value pairs for pruned nodes
  - Two special symbols to indicate the scope of a node

Verification by Client

Reliability Check:
- No POIs or obstacles are added or removed by SP
- Reconstruct hash roots from the VOs
- Decrypt signed hash roots using DO’s public key
- Compare these hash roots

Correctness Proof:
- Results are the real \( k \) NNs
- Construct a visibility graph using the extracted POIs and obstacles from VOs
- Find first \( k \) nearest neighbors using any shortest path algorithm
- Compare the set with result set to detect discrepancy

Future Challenges

- Implement our approach to evaluate the efficiency and effectiveness
- Develop authentication techniques for range and group nearest neighbor queries

Conclusion

We develop an approach to authenticate \( k \)NN queries in the presence of obstacles. Our algorithm constructs VO simultaneously with the query processing and ensures that VO contains necessary information to verify the reliability and correctness of the result.

References