Review: Navigational Path Privacy Protection

Layla Pournajaf
Department of Mathematics and Computer Science
Emory University

My notes  I’d like to talk about this paper too while presenting the other paper ”Shortest path computation with no information leakage”.

Summary  Ken C. K. Lee et al in the paper ”Navigational Path Privacy Protection” proposed an obfuscation method to preserve the path privacy of the users while querying the navigational services for shortest paths. Their method includes a trusted obfuscation server that cloaks the source and destination of the user’s query among a reasonable number of other users’ queries and sends it to the untrustworthy LBS server. Since previous obfuscation methods restricted the amount of privacy due to the computational expense and overhead the authors suggested a set of optimization methods to be used in both query cloaking service and query processor that increased the computational performance and provided stronger privacy.

Positive Points

1. The proposed idea is simple yet useful for providing a minimum amount of privacy when computational overhead is an obstacle.

Negative Points

1. The privacy suggested in this paper is not strong and the authors could not provide any guarantee on the amount of privacy.

2. The evaluation part does not illustrate the trade-off between the computational performance and information leakage.
Discussion Points and Questions

1. The proposed method is focused on the path privacy while the source or target location privacy is not guaranteed (also stated in the paper). It is not discussed that by exposing the source location, the risk of estimation of the path by adversary might increase significantly.

2. I found this paper useful for my research, since I am dealing with a similar problem, just handling a set of nearest neighbor queries for a set of users with a global optimization goal rather than an individual optimization. Reading this paper and the other paper "Shortest path computation with no information leakage" suggested me the idea that more overhead especially in the communications might be the price that I need to pay for better utility. The only concern is whether more communication between the server and the users could lead to information leakage or not. It might be also useful to think of a trusted party in the middle similar to this approach.

3. The clustering methods for finding similar queries has not discussed in details, it might be possible to use other methods such as k-d trees approach suggested in the other paper "Shortest path computation with no information leakage" to create a brief picture of the map in the trusted server for better performance and also storing less information in the trusted server.