Trustworthy Processing of Shortest Path Queries over Online Road Network Databases (PI: Dr. Yiu Man Lung; 2010/11)

In this research project, we will study the *trustworthy processing* of shortest path queries at online mapping servers (e.g., Google Maps, MapQuest). Mobile-device (e.g., PDA, iPhone) users typically prefer online servers over offline navigation software simply because online servers capture up-to-date traffic information seamlessly, while navigation software is forced to download map updates regularly. On the other hand, recent studies show that hackers may exploit multi-step intrusion to infiltrate the server and then actively tamper with the server's reported path, compromising the integrity. A tampered path might include detours that are beneficial for some roadside facilities operated by hackers (e.g., gas stations, coffee shops, billboards). This risk becomes more pronounced as the service providers are gradually using the low-cost cloud computing environment, where many security concerns remain unresolved. Several challenges arise from the trustworthy processing of shortest path queries. Conventional solutions like digital signatures only help verifying the integrity of the entire road network dataset stored at the server. However, the integrity of the shortest path, equivalent to showing that there exists no other shorter path other than the result, cannot be achieved by digital signatures directly. The problem is further complicated by the facts that: (i) the road network has a huge data size, so the number of possible paths between the start and target locations is exponential to the path length, and (ii) the traffic information on the road network is updated frequently, so it is not possible to precompute the result in advance.

We envision that our project has a profound impact on many route planning applications that require trustworthy processing of shortest path queries. When emergency services dispatch units (e.g., ambulances, fire trucks) to the incident location, they need the shortest path reported by the server to be trustworthy in order

to minimize life risk involved in the incident. In the tourism context, a taxi driver should present a shortest path integrity proof from the server, so that foreign tourists will clear their doubts of being overcharged. Other applications include urgent parcel delivery, logistic flow planning, etc.

Our main objective is to develop efficient techniques for trustworthy processing of shortest path queries, such that they cope with large road networks and frequent traffic information updates. Our approach is to extract a concise subgraph from the road network as the integrity proof of the shortest path result. Efficient search algorithms and index structures will be developed to facilitate the above process. With respect to the dynamic traffic update issue, incremental techniques will be developed to maintain the shortest path integrity proof, without having to recompute the integrity proof from scratch. We will also study the adaptation of our trustworthy processing techniques for advanced path queries like the maximum flow problem and the traveling salesman problem.