A Study on Privacy-Preserving Route Planning for Smart Mobility Applications

Name: Francis Jerome G. Tiausas
Laboratory's name: Ubiquitous Computing Systems
Supervisor's name: Prof. Keiichi Yasumoto

Abstract:

Route Planning Services (RPS) are a core component of autonomous personal transport systems which facilitate safe and efficient navigation of dynamic urban environments. However, conventional RPS also require the disclosure of the user's origin and destination as input and the computed route as output which is a major privacy concern. Though a number of privacy-preserving RPS have been developed over the past decade, most are rendered impractical by the increased communication and processing overhead they entail. In this dissertation, the core challenge is to develop an RPS where: (1) route privacy is objectively quantified, (2) Utility, Performance, and Privacy objectives are adequately satisfied, and (3) the produced routes are valid and close-to-optimal. The core idea is to use Private Information Retrieval (PIR) over *partitions* of a road network (distributed across multiple devices) to facilitate privacy-preserving route planning. To satisfy the different system objectives, this was then combined with Multi-Objective Genetic Algorithms (MOGA) to discover acceptable trade-offs between said objectives. However, this optimization step was found to be rather slow, and did not protect the intermediate route at all. Thus, an improved approach called *Hierarchical Privacy-Preserving Route Planning* or HPRoP was developed, combining Inertial Flow partitioning with a novel route planning heuristic which distributes route planning tasks across multiple levels to protect the entire route. New metrics were also formulated to quantify the privacy of the source/destination points (*endpoint location privacy*), and the route itself (*route privacy*). Evaluations on the road network of Osaka City, Japan showed that HPRoP reliably produced routes that deviate only by ≤ 20% in length from optimal shortest paths, while being able to complete routes within ~25 seconds despite using PIR. Moreover, more than half of the produced routes achieved near-optimal endpoint location privacy (~1.0) and good route privacy (≥ 0.8).