論 文 内 容 の 要 旨

博士論文題目　A Study on Privacy-Preserving Route Planning for Smart Mobility Applications

（スマートモビリティアプリケーションのためのプライバシー保護経路計画に関する研究）

氏　　名　　Francis Tiausas

（論文内容の要旨）

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 (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. 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 showed that HPRoP reliably produced routes that deviate only by $\leq 20\%$ 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).

氏　名	Francis Tiausas

（論文審査結果の要旨）

経路計画サービス（RPS）は、ダイナミックな都市環境を安全かつ効率的にナビゲートする自律型パーソナル交通システムの中核をなす要素である。しかし、従来の RPS は、ユーザの出発地と目的地を入力として、計算された経路を出力として開示する必要があり、プライバシーに関する大きな懸念がある。過去 10 年間に多くのプライバシー保護型 RPS が開発されてきたが、その多くは通信や処理のオーバヘッドの増大により実用的でないという問題があった。本論文では、実用的なプライバシー保護型 RPS を開発するために、次の 3 つの課題：(1)経路のプライバシーが客観的に定量化されること、(2)経路の正確さ、経路の探索時間、経路のプライバシー保護強度の 3 つの目的が十分に満たされること、(3)生成された経路が有効で最適に近いこと、の解決に取り組んだ：

本研究の学術的貢献は以下のとおりである。

(1) 多目的遺伝的アルゴリズム（MOGA）と組み合わせて、経路探索における異なる目的間の許容可能なトレードオフを実用時間で見つける手法を開発した。

(2) 慣性フロー分割と、経路計画タスクを複数のレベルに分散して経路全体を保護する新しい経路計画ヒューリスティックを組み合わせた、階層的プライバシー保護経路計画（HPRoP）を開発した。

(3) 出発地/目的地のプライバシーと経路自体のプライバシーを定量化するための新しい指標を策定した。

(4) 大阪市の道路網を用いた評価において、25 秒以内に経路を算出可能なこと、ほとんどの経路において最適な最短経路との乖離が 20%以内に抑えることができ、さらに、生成された経路の半数以上が、ほぼ最適な位置プライバシー(～ 1.0)と良好な経路プライバシー(～0.8)を達成した。

全体として、本論文は、エリア分割と分散計算、プライベート情報検索（PIR）、トレードオフ機構を巧みに組み合わせることによって、これまでに無い実用的なプライバシー保護型 RPS を実現しており、本分野において十分な学術的新規性を有していることを確認した。以上より、本論文は、博士（工学）の学位論文として価値あるものと認める。