審 査 の 結 果 の 要 旨

氏　　名　　黄　楽平

本論文は「Enhancing Location Privacy for Mobile Communication Systems by Controlling Spatial-Temporal Uncertainty　(モバイル通信システムにおける時空間的不確実性制御を用いた位置情報プライバシー保護)」と題し、モバイル通信システムにおける位置情報プライバシー・特に軌跡のプライバシーを保護する方策とその応用について述べたものであり、全九章から構成されている。

第一章は「Introduction（序論）」であり、本論文が対象とするモバイル通信システムにおける位置情報プライバシーについて論じ、論文全体の概観を行っている。

第二章は「The Basics and Prior Arts（基礎と過去の研究事例）」と題し、位置情報プライバシーに関連して、匿名性を向上する手法、位置同定とトラッキング手法、モバイル通信システム、モビリティモデル、位置情報プライバシーに対する攻撃の種類とその対抗策についての研究動向の要約を行い、本研究の貢献の明確化を行っている。

第三章は「System Assumption and Problem Analysis（対象システムとその問題点）」と題し、本論文の対象となる無線 LAN システムについて概観し、その位置情報プライバシーの問題点として、1CSMA.CD 方式を用いてアドレスを高頻度で広告しなければならないため、オーバーヒアリングによって容易に盗聴が可能であること、またアドレスをヘッダ部の暗号化が困難であること、電解強度情報等を用いればアクセスポイント粒度以上の高精度の位置情報が取得出来るためコリレーションアタックに対して非常に脆弱であることを指摘している。

第四章は「Silent Period for Location Privacy（位置情報プライバシーのためのサイレントピリオド）」と題し、コリレーションアタックに対する対抗策として、意図的に通信を行わない「サイレントピリオド」の概念の提案を行うと共に、その数学的定式化を行っている。また軌跡のプライバシーレベルを定量的に論じるためのメトリックとして GAS(Geographical Anonymity Set)を定義し、これを用いてプライバシーレベルと通信品質との間の関係を理論とシミュレーションの両面から明らかにしている。

第五章は「Silent Cascade for Location Privacy and QoS（サイレントカスケードと QoS）」と題し、短時間の間にアクティブ期間とサイレント期間を繰り返し ID の変更を行うことにより、ストーリミングメディアの通信であっても、品質の劣化を最小限に抑えつつかつ一定のプライバシーレベルを保持することの出来る、サイレントカスケードの手法の提案を行っている。また、サイレントカスケードにより mix-network が構成出来ることを示し、これを手がかりに問題の定式化を行っている。また、アドレスの寿命と最大追跡可能時間の間の関係を理論とシミュレーションの両方によって求め、理論式の妥当性の検証を行うと共に、提案手法の有効性について論じている。

第六章は「Amendment to WLAN Access Network for Location Privacy Protection（無線 LAN における位置情報保護に関する追記）」と題し、実無線 LAN システムにおいて MAC アドレスを頻繁に更新することに起因するオーバヘッド解決策の基本的アイデアを述べている。

第七章は「Application One: Vehicle Ad hoc Network（自動車アドホックネットワークへの応用）」と題し、車車間通信、車とセンタ間の通信における追跡のプライバシーを確保するための手法としてサイレント

ピリオドの考えを応用したAMOEBAの提案を行うと共にその性能評価を行っている。

第八章は「Application Two: Radio Frequency Identification System（RFIDシステムへの応用）」であり、ユーザや商品にRFIDが付与されたシステムにおける位置プライバシー保護の手法として、IDを適宜変更していくことを提案し、サイレントピリオドの考えを流用してそのプライバシーレベルの評価を行っている。

第九章は「Conclusion and Future Work（結論と今後の課題）」であり、論文の成果と今後の展開をまとめている。

以上これを要するに、本論文は、モバイル通信システムにおける位置情報プライバシーを論じる際の手掛かりとなる基本的なモデル化と定式化を行い、具体的なプライバシー保護手法を提案すると共にその有効性を示したものであって、電子情報学に貢献するところが少なくない。　よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。