論文の内容の要旨

論文題目： 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)

氏名： 黄 楽平

This is a thesis about *location privacy* and *identity* in mobile communication systems. Traditionally, user's identity in mobile communication means bit strings (addresses or identifiers) contained in the messages exchanged between user and service provider. Hence, most location privacy technologies focuses on providing confidentiality on user's long-term identifier and unlinkability between user's short-term identifiers. In this thesis, we claim that spatial-temporal information disclosed via a user's wireless communication is also an important side channel of user's identity in the context of mobile communication and high-accuracy geolocation technologies. Continuous disclosure of this information may result in the breach of user's location privacy and long term identity.

In this thesis, we propose two spatial-temporal information disclosure control protocols: *silent period* and *silent cascade*. The basic idea of these two protocols is to control the uncertainty of spatial-temporal information by using a transition period between the use of new and old pseudonyms, when a node is not allowed to transmit. Silent period enhances user's location privacy at the expense of breaks in communication, which may result in the degradation of communication Quality of Service (QoS) in some real time applications. Silent cascade enhances location privacy by trading users' delay in silent cascade for anonymity, and avoids QoS degradation.

Mix-network is a widely used approach in anonymous communication. In this thesis, we formalize the problem of location privacy with respect to spatial-temporal information disclosure into mix-network based models. These models offer two insights: a way of evaluating location privacy protection systems; and serving as a bridge between the new location privacy protection problem and existing defense and attack approaches in the mix-network related research.

Besides, we also propose an improvement to wireless LAN access network to alleviate on the overhead caused by periodical identifier update. Finally, we extend the application area of our spatial-temporal disclosure control protocols into vehicle ad hoc network (VANET) and Radio frequency identifier (RFID) system, and show the unique features on those systems.