The recent proliferation of smart mobile devices and the advances of smart sensors that can be attached to various moving objects have enabled a wide range of applications benefiting human beings. Among them, mobile crowdsourcing is a promising computing paradigm that solves real-life problems by exploiting the power of massive crowds. However, the key barrier that can hold mobile crowdsourcing from being widely adopted is the concern of compromising the participating users' location privacy. Indeed, many mobile crowdsourcing services require users to submit the locations of the events reported, as well as the user identities (for fraud detection). Therefore, users' location privacy can be easily compromised by attackers or misbehaved service administrators.

In this research, we target designing effective, lightweight, and privacy-preserving solutions for various emerging and promising mobile crowdsourcing services. For example, the ubiquitous computing technologies, such as sensing and wireless communication, have enabled Intelligent Transportation Systems (ITS), with which people can achieve safer and more efficient everyday transportation. In ITS, a popular category of applications is to crowdsource the condition of the transportation system by exploiting the ubiquity of smartphones and smart sensors. In these applications, users report information about transportation system elements (e.g., drivers and road conditions) to the ITS system for services like real time traffic control and roads maintenance. However, before accepting data about a location reported by a vehicle, ITS operators need to verify if the vehicle visited the location at the time indicated in the reported data. Failing to do so will allow malicious users to launch an attack to the ITS system by reporting fake information about places where he did not actually visit. The damages of the attack are particularly serious, since the attacker can report fake information about numerous places by just clicking mouse at home. We have been working on designing a lightweight location proof scheme that enables users to prove that their location claims match its historical locations without revealing their identities and without relying the PKI infrastructure (with which the users location history could still be exposed to service administrators). We have implemented a prototype system and evaluated it with extensive real-world experiments. The results has been appeared in the IEEE Transactions of Vehicular Technologies (`http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6810011&tag=1`).

Beside the location proof scheme, we are also working on other topics of protecting users' location privacy for various services in mobile computing. We envision that this research would effectively promote the adoption of mobile crowdsourcing by alleviating and eventually eliminating the location privacy concern.