**ABSTRACT**

Increasing smart phone penetration combined with the wide coverage of cellular infrastructures, renders smart phone based traffic information systems (TISs) an attractive option. The main purpose of such systems is to alleviate traffic congestion that exists in every major city. Nevertheless, to reap the benefits of smart phone based TISs, we need to ensure their security and privacy and their effectiveness (e.g., accuracy).

This is the motivation of this paper: We leverage state-of-the art cryptographic schemes and readily available telecommunication infrastructure. We present a comprehensive solution for smart phone-based traffic estimation that is proven to be secure and privacy preserving.

We provide a full-blown implementation on actual smart phones, along with an extensive assessment of its accuracy and efficiency. Our results confirm that smart phone-based TISs can offer accurate traffic state estimation while being secure and privacy preserving. Traffic congestion deteriorates the quality of life of citizens and contributes significantly to environmental pollution and economic loss.

Traffic information systems (TISs)aim at solving this problem by collecting traffic data, producing traffic estimates, and providing drivers with location-specific information. The increasing smart phone penetration, along with the wide coverage of cellular networks, defines an unprecedented large-scale network of sensors, with extensive spatial and temporal coverage, able to serve as traffic probes for TISs. This is a task that cannot be achieved only by relying on the security of the mobile-to-cellular infrastructure communication.