Secure Data Collection and Exchange in the Smart City

Joshua Joy (jjoy@cs.ucla.edu), Mario Gerla (gerla@cs.ucla.edu)

Autonomous vehicles will create a new wave of safe and efficient transportation means. These vehicles are essentially huge sensors that collect both external (environmental and other cars) and internal (driver) information. The autonomous vehicles are connected to the infrastructure cloud (e.g., Amazon), the edge cloud, and also the mobile cloud (vehicle to vehicle). Cities rely on big data to enable smart urban applications such as intelligent transport and epidemics detection. However, the gathering of big data, especially from mobile platforms like pedestrians and cars, brings large privacy concerns.

Data generated by the vehicular network is dynamic and real-time. Many of the statistical machine learning algorithms operate in the infrastructure cloud. They enable real-time smart transportation systems that influence driver behavior and reduce traffic and pollution. For example, NSF funded Green City project at UCLA showed that combined monitoring of pollutant concentration and traffic conditions allows to optimize local traffic and thus reduce congestion and pollution. Using on-board emission measurements, vehicles perform local estimates and also upload data to the cloud for further large scale correlations.

However, storing all collected data on centralized servers in the infrastructure cloud is a potential security vulnerability for data breaches. Additionally, a centralized data silo, where data is not shared, limits its impact and utility. For example, only after a traffic jam occurs do users become interested in its causes. They then turn to centralized services (e.g., Google Waze) to help them reroute. However, by the time the traffic jam has occurred, it is often too late to effectively reroute out of it. In contrast, it has been shown that vehicle to vehicle (V2V) communications (in the mobile cloud) enable vehicles to learn about traffic congestion almost instantly. Additionally, safety is increased by V2V communications allowing vehicles to continuously be aware of each other position and state. For example, abrupt braking can be communicated several cars behind thus preventing shockwaves (a major cause of accidents and congestion).

Clearly, infrastructure and mobile cloud must work together. Sharing vehicle data with the infrastructure is required for intelligent transportation systems. This will happen only if privacy is guarantees. In addition, vehicle to vehicle communication are subject to security threats. To address this, we propose the secure mobile cloud. The secure mobile cloud allows for the real-time sharing of private data amongst distinct analysts (e.g., Department of Transportation, Department of Energy, etc). Analysts in the infrastructure cloud issue signed queries to the mobile cloud asking for traffic and pollution conditions. Each vehicle maintains its data locally and answers the queries privately (e.g., randomizes its answer satisfying differential privacy requirements). From the aggregate randomized data, the analyst is still able to extract real time trends (eg, traffic congestion) and then intelligently reroute traffic. Likewise vehicles can communicate securely within the mobile cloud to avoid local traffic jams. The synergy between infrastructure cloud and mobile cloud is essential for vehicles to share date in real-time with the Internet and with their peers, reducing traffic congestion, minimizing air pollution, and helping the smart city energy budget.

Travel

Travel expense reimbursement would be appreciated.

Background

Mario Gerla is the PI for NSF Award 1111971, NeTS: Large: Collaborative Research: Closing the loop between traffic/pollution sensing and vehicle route control using traffic lights and navigators, $3M, 09/15/2011 to 08/31/2015. The project aims at using Internet Cloud Intelligence (in the form of Traffic Navigators and Air Quality Simulators) to improve urban traffic and pollution conditions in a synergistic, joint optimization. In this effort, the Internet Cloud based traffic controller is assisted by distributed, cooperative management (of local traffic, for example) run on vehicles operating as a Mobile Cloud. A multidisciplinary team spanning three Campuses and six Departments has engaged in real life ad hoc networking, traffic and pollution experiments on actual vehicles in various locations. The results have been extrapolated to urban scale using simulation and have been extensively published. The major intellectual merit of the project has been the innovative use of V2V and V2I communications to address safety issues (e.g., shockwave prevention, platooning, intersection collisions avoidance) as well as traffic/pollution problems. The broader impact is on urban drivers, residents and society at large, by improving their quality of life, and; on future autonomous vehicles, developing basic technologies (like platoon communications and shockwave avoidance) that will pave the way to their introduction. The current project directly leads to the proposed project - data passed by vehicle to Internet Servers is made private to protect drivers.

Joshua Joy is a PhD candidate in Computer Science under the guidance of Mario Gerla. His interests include intelligent transportation enabled by the real-time exchange of data utilizing secure and private mechanisms.