Poster abstract: enhancing user privacy in probe-based traffic monitoring systems using distributed computing

Ahmad Dehwah, Mustafa Mousa, Edward Canepa, Enas Odat, Jiming Jiang and Christian Claudel

Department of Electrical Engineering and Computer Sciences, KAUST, Saudi Arabia

Abstract. This article describes a new type of mixed Eulerian-Lagrangian traffic flow sensor network that offers very strong privacy guarantees compared with existing systems. Traffic sensor data is generated by fixed sensor nodes as well as probe vehicles equipped with a short range communication device. The traffic flow estimation problem is then formulated as a MILP (mixed integer linear program), which is solved by the nodes themselves using distributed computing. The resulting traffic estimates are sent to a centralized server, without requiring the dissemination of privacy sensitive data. The proposed system can easily interface with upcoming car-to-car communication systems.

1 Introduction

Traffic congestion is an increasingly prevalent problem in large urban areas of the world, and is expected to become worse as global traffic demand increases. Traffic sensing can bring solutions to this issue, by enabling advanced traffic flow control or modifying network demand. While fixed traffic sensors are still commonly used, probe based systems using traces generated by probe vehicles are more and more prevalent since they are less expensive than fixed sensor networks. Nevertheless, current systems require users to send their location data to a centralized server, which carries high risks of user privacy intrusion [3]. These privacy risks are preventing the large scale adoption of tracking devices by users, which severely impairs traffic data quality.

2 System description

The proposed system consists of fixed sensor nodes and mobile nodes (vehicles). Some fixed nodes contain traffic sensors (sensing nodes), while the remaining fixed nodes merely act as transceivers (transceiver nodes). All nodes are connected using a customized protocol built on IEEE 802.15.4. In addition to the fixed nodes, vehicles equipped with transceivers act as mobile nodes, and send their velocity or position to the fixed sensor network.
2.1 Sensor nodes

The fixed transceiver nodes consist of a computational platform connected to a solar panel and a battery, with a plastic enclosure mounted on a metallic frame. The fixed sensing nodes share the same platform, and are connected to a traffic sensing device, an example of which is given in Section 3.2. All fixed devices can be mounted on existing urban structures such as buildings, bridges or lamp posts.

2.2 Mobile nodes

The mobile transceivers onboard vehicles monitor the vehicle position and/or velocity, and transmit this information to the surrounding transceiver or sensor nodes. The transceiver or sensor nodes can broadcast messages to adapt the transmission rate of mobile nodes to accommodate for extreme traffic situations: the transmission rate of mobile nodes should be high during low traffic to increase data accuracy, and low during high traffic to reduce packet collisions.

2.3 Distributed traffic sensing paradigm

The principle of operation is illustrated in Figure 1. A given probe vehicle broadcasts its velocity to the surrounding nodes (upper left). The nodes send RSSI data and message contents to a local master node which estimates the position of the vehicle on the road network, using machine learning techniques (upper right). The local master node also collects traffic data from surrounding fixed sensor nodes (lower left), and poses [1] the local traffic estimation problem as a mixed integer linear program (MILP). The resulting MILP is solved using branch and bound methods, distributing the computational load to local nodes (lower right). The solution to the MILP (local traffic flow estimate) is then sent to a central database for dissemination to users. With this system, no information regarding the presence of the original vehicle is exchanged beyond its immediate surroundings, which prevents the dissemination of privacy sensitive data. The only possible method for an attacker to track a vehicle is to listen to all the nodes in the path of the vehicle, a very costly process for large scale networks.

Fig. 1. Distributed Eulerian/Lagrangian traffic sensing approach.
2.4 Sensor fault detection/adversarial Lagrangian traffic data detection

As in all sensor networks, the system may contain faulty sensors that transmit incorrect data. In addition to sensor faults (both hardware and software), it is relatively easy for a user to willingly send bogus data to the system to possibly perturb traffic estimates, the easiest attacking method simply being to tamper with the position or velocity sensors of the mobile nodes. Such bogus data injection can be detected by analyzing the consistency of sensor data with the flow model. The consistency analysis problem results in mixed integer linear constraints [2], which will be checked by the coordinator node before solving the local traffic estimation problem.

3 Current implementation

3.1 Computational platform

In order to minimize power consumption while allowing distributed computing to be performed, we designed a new hardware platform around a 32-bit ARM Cortex M4 underclocked to 32MHz. The platform draws its energy jointly from a solar panel and a rechargeable Li–FePO₄ battery. It contains four UARTs, two SPIs, two I2Cs, and uses an XBee transceiver (Xbee Pro, 802.15.4). It is designed to be OTA (over-the-air programming) capable. The platform layout and its current implementation are illustrated in Figure 2.

![Fig. 2. ARM Cortex-based computational platform.](image)

3.2 Traffic sensor nodes

In our current implementation, the sensor nodes contains one ultrasonic rangefinder and six passive infrared sensors monitoring two lanes of traffic simultaneously, as illustrated in Figure 3. The first lane is monitored using a set of three passive infrared sensors as well as the ultrasonic rangefinder, which are used in conjunction to perform vehicle classification and speed estimation. The remaining three passive infrared sensors monitor the second lane, using the other sensors data as training data to compensate for the lack of an ultrasonic rangefinder.
3.3 Preliminary results

A medium-scale deployment involving 80 transceiver nodes was carried out on KAUST campus (June 2012) with off-the-shelf Libelium Waspmotes to validate the routing protocol designed for this system. The protocol uses a time-varying global cost function to distribute the communication load among all nodes according to energy availability. A screenshot of our network data visualizer is shown in Figure 4.

![Sensor network visualizer](image)

**Fig. 4. Sensor network visualizer.** Left: nodes level and number of packets sent per time unit. Right: nodes global cost and link RSSI.

One traffic sensor node has also been deployed on KAUST campus (November 2012) to test its accuracy. Future steps will involve the implementation of the distributed computing-based traffic estimation scheme in the new platforms, once they are sufficiently developed.

ACKNOWLEDGMENTS

We would like to thank Guodong Li for his help designing and manufacturing the traffic sensor structure, and Sergio Favela for his help writing the embedded code.

References