CENTER FOR TRANSPORTATION RESEARCH

PROJECT SUMMARY

Texas Department of Transportation

0-6845: Connected Vehicle Problems, Challenges and Major Technologies

Background

Connected vehicles (CVs) are the future of transportation. CV technology utilizes wireless communication to realize real-time information exchange among vehicles, transportation infrastructure, and personal communication devices. The CV technology underpins many potential applications in safety, mobility, and infotainment. Looking to effectively and securely deploy these applications, industry and academia have paid considerable attention to making connections between vehicles as secure as possible while maintaining efficient wireless network use and protecting the privacy of users of CV technology. The goal of this project was to provide an up-to-date understanding of information flow quality and security issues in CV environments, as well as a preliminary guideline for optimizing information flow in Texas.

In terms of information flow quality, the objective was to compare and evaluate existing and emerging VANET (vehicular ad-hoc network) technologies in CV environments, including, but not limited to, the architecture, routing protocols, and hardware of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. This project focused on two major communication standards: dedicated short-range communications (DSRC) and Long-Term Evolution (LTE). In the area of information flow security, the team identified the open problems through a critical review of current security measures and potential issues. Extensive studies have shown that the security measures in existing standards are deficient and must be augmented for safe operation of CVs.

The team reviewed these security issues and proposed potential solutions to address the security gaps. Based on analysis of the information flow quality and security issues, the team developed preliminary guidelines and analyzed two examples of CV-enabled applications for traffic management.

What the Researchers Did

The team conducted the following research activities:

- Provided a critical review of key candidate technologies (including DSRC and LTE) enabling CV applications, along with a baseline analysis on the tradeoffs and challenges presented by various current and future approaches to CVs.
- Conducted an extensive simulation study to evaluate VANETs with DSRC protocol (which uses the IEEE 802.11p standard), under a variety of performance metrics, including packet delivery ratio, throughput, and end-to-end delay. The performance of DSRC was compared with LTE.
- Analyzed DSRC and LTE costs and developed a customizable Excel spreadsheet tool to perform calculations.

Research Performed by:
Center for Transportation Research

Research Supervisor:
Chandra Bhat

Researchers:
Jeffrey Andrews
Robert Heath
Chang-sik Choi
Todd Humphreys
Lakshay Narula
Jia Li

Project Completed:
12-31-2016

- Provided a critical review of security issues in CV environments and identified the open problems and major threats.
- Recommended and demonstrated a Real-Time Kinematic GNSS positioning system towards addressing GNSS spoofing. Secure own-vehicle positioning is a necessary pre-requisite for secure CVs. This secure centimeter-accurate positioning system is a must-have for all CVs.

What They Found

Major findings include the following:

- DSRC's typical transmission range is estimated to be on the order of 450 feet, with a best-case range under the most favorable conditions of less than 2000 feet.
- Comparing DSRC and LTE, we found that LTE generally performs better, except for extremely short-range one-hop communication between slowly moving vehicles.
- We established the position and velocity accuracy requirements for safe operation of CVs. Our findings indicate that a vehicle's own position must be estimated with decimeter-level accuracy for lane-keeping, and must be able to verify a neighbor's position to within a meter to disambiguate the lane that the neighboring vehicle occupies.
- We showed that even if the malicious neighbor cannot present itself as a credible node of the CV network, it can perform man-in-the-middle attacks to make the CV technology ineffectual.

What This Means

- **DSRC vs. LTE:** From technological perspective, LTE generally outperforms DSRC. This was confirmed by the team's simulation study that examined a variety of performance metrics and compared DSRC and LTE security features. Nonetheless, we should recognize that DSRC is likely to be favored over LTE in short to mid-term deployment due to its maturity, stability, the independence of cellular network coverage, and the lack of subscription fees. To achieve a wide, reliable CV network, leveraging the cellular technology and network infrastructure could be a promising direction to explore.
- **CV Security:** Infrastructural control is critical to establishing secure vehicular communication, and LTE-based cellular networks provide such infrastructure. We suggest that DSRC, or any alternative communication technology for CVs, be combined with other modern vehicle sensors such as radar or optical cameras to enhance the security of neighbor position verification protocols. Finally, this project's analysis suggests that standards for credential revocation in CVs be revamped to defend attacks against CV networks.

For More Information

Research and Technology General Information:
Darrin Jensen, RTI (512) 416-4728

Research Supervisor:
Chandra Bhat, CTR (512) 471-4535

Technical reports when published are available at **http://library.ctr.utexas.edu.**

Research and Technology Implementation Office
Texas Department of Transportation
125 E. 11th Street
Austin, TX 78701-2483

www.txdot.gov
Keyword: Research