Research Challenges of Vehicle CPS to Provide Safety Enhancement

Xiuzhen Cheng and David H.C. Du

Introduction

In our vision, a vehicle CPS consists of Dedicated Short Range Communication (DSRC) enabled vehicles and roadside infrastructures (including roadway sensors) that are tightly coordinated to provide *safety enhancement*, *intelligent traffic management*, and *data communications*. In 1999, FCC allocated the 75MHz licensed DSRC spectrum in the 5.9GHz band to support low-latency vehicle-to-vehicle (via On-Board Unit (OBU)) and vehicle-to-infrastructure (via OBU and RoadSide Unit (RSU)) communications for safety and non-safety applications with different priorities. DSRC has become the latest ITS standard that is expected to be ratified in April, 2009. In the following, we briefly introduce the major components that play significant roles in a vehicle CPS.

1. RSU: A RSU could be located in a traffic light or other roadside infrastructure. RSUs process the data collected from passing-by vehicles and roadway sensors.
2. OBU: Generally speaking, an OBU resides in a vehicle GPS. OBU is required to have the ability to transmit and receive standard vehicle status messages conveying information such as position, speed, steering wheel position, heading, yaw-rate, etc. It is also expected to be able to process the data from nearby vehicles and embedded car sensors.
3. Embedded car sensors: There exist thousands of sensors embedded within a modern vehicle to monitor the operations of the engine, air bags, tires, etc. Currently these sensors are mainly used for binary status report.
4. Roadway sensors: In nowadays, advanced sensing technologies such as microwave presence-detecting radar and inductive loop detector have been used for intersection control, freeway incident detection, traffic congestion monitoring, lateral control, traffic data collection, weather and highway condition detection, etc.

In this position paper, we will identify the grand challenges of a vehicle CPS. We will consider the following problems that are the most critical to safety enhancement: *safety message dissemination*, *cooperative safety warning decision making*, *vehicle prognostic health monitoring*, and *driver behavior profiling*.

Grand Challenges for Vehicle CPS:

Vehicle CPS faces a number of grand challenges, with the three most important ones listed below:

1. **The goals of a vehicle CPS are ambitious, which require the joint effort from both academia and industry**. However, car manufactures mainly work themselves independently to enhance the intelligence of individual cars while transportation related research centers at the university level are mainly sponsored by the state Department of Transportation to tackle problems such as traffic modeling and fatality analysis. These two parties seldom share resources and problems, and they publish in totally different venues. How to make these two parties work together to conduct joint research is the most critical grand challenge.
2. **Currently it is almost impossible for the new design on vehicle CPS to be validated under the real vehicle CPS settings.** For example, very few public data on embedded car sensors are available. Therefore it is really hard to tell the effectiveness of the designed algorithms for vehicle structure health monitoring and for driver behavior monitoring. Furthermore, it is very cost-prohibitive to set up a testbed mimicking a saturated wireless vehicle network environment to validate various

algorithms for safety message dissemination and safety warning decision making. Without a convincing validation platform, it is almost impossible to transfer the technologies designed in the laboratory to real world applications.

3. **Providing security and reliability to a vehicle CPS is much more challenging than to Internet-based networking systems, yet it is critical to the wide adoption.** Security is a grand challenge to all systems and it is much more important in a vehicle CPS, which should be available, reliable, and secure 24 hours a day, 7 days a week. Nevertheless, vehicle CPS relies on mobile wireless communications that are intrinsically unreliable and unsecure. The high dynamism and heterogeneity make the problem even harder. For example, the problems such as how to revoke the invalid keys in a vehicle network and how to authenticate the origin and content of a safety message without disclosing any private information are much more challenging compared to the wired Internet. Therefore, transformative research is needed to satisfy the basic requirements on security and reliability in a vehicle CPS.

Technical Challenges associated with interfacing to and interacting with the physical world:

We identify the following three major technical challenges associated with interfacing to and interacting with the physical world in a vehicle CPS to provide safety enhancement:

1. **The pervasive and "chaotic" broadcast environment makes the scheduling of the safety message disseminations to meet the delay requirement very challenging.** In DSRC-enabled vehicle networks, most high-priority safety applications require a short message (200 to 500 bytes) to be broadcasted to all vehicles within a range of 150m to 300m at a frequency of 10Hz via vehicle-to-vehicle and vehicle-to-infrastructure communications at the 10MHz control channel. This requirement implies that CSMA/CA with RTS/CTS handshake to counter the hidden terminal problem is not suitable. Furthermore, the dynamism caused by the Doppler effect and the multipath fading makes reliable broadcast almost impossible since any ACK or retransmission worsens the spectrum saturation and the latency constraint.
2. **Novel fast and effective cooperative warning decision making algorithms are needed to effect realtime warning in a vehicle CPS.** Many of the critical safety applications need the cooperation of the vehicle systems and roadway infrastructures to provide safety warning. For example, in *Traffic Signal Violation Warning*, the OBU will use the information communicated from the RSU located at the traffic light system to determine if the driver should be alerted. Then the question is: *how does the OBU in a vehicle estimate the likelihood of violating the traffic signal phase upon entering the intersection*? Similar questions exist for all other safety applications. A common challenge faced by researchers is that the algorithms designed for cooperative decision making must be fast and reliable.
3. **Novel machine learning based algorithms to investigate the embedded car sensor readings are required for Vehicle Prognostic Health Monitoring (VPHM) and Driver Behavior Monitoring (DBM).** Many of us saw the sudden explosion of the tire in a highway when the motor is heading at a very high speed. This is an extremely dangerous accident to both the driver and other vehicles at nearby lanes. The existent vehicle Predictive Maintenance and Condition Monitoring system can only tell the driver whether a tire is flat or not, but not whether a tire is going to explode or not. By monitoring and mining the readings from embedded car sensors, it is possible to predict possible breakdowns to avoid accidents that are relatively irrelevant to the driving context. This is the problem of vehicle prognostic health monitoring (VPHM). Sample questions that should be answered in VPHM include: How many hours the engine can continue working without fault? When a tire or a battery should be replaced? Is the brake paddle fault-free? Etc. On the other hand, driver behavior plays a critical role for safety enhancement. It can be described by *position control*, *admittance control*, and *force control*, which are governed by the forces applied to the pedals (gas, brake, etc.)

and the steering wheel, and are recorded by embedded sensors. Diver Behavior Monitoring (DBM) asks for precisely profiling the driver behavior such that a warning can be made when the driver is classified as abnormal.

VPHM and DBM are challenging problems to which existing advanced machine learning techniques can not be directly applied since the embedded sensor readings are noisy and diverse under different settings. In addition, very few public data generated by real embedded car sensors are available for the researchers to study. A joint interdisciplinary effort from machine learning, quality management, and signal processing is needed to develop novel technologies for vehicle structure health monitoring and driver behavior monitoring.

Author Information:

Xiuzhen Cheng, Associate Professor
Department of Computer Science, The George Washington University
Tel: 202-994-9751, Email: cheng@gwu.edu

Dr. Xiuzhen (Susan) Cheng is an Associate Professor at the Department of Computer Science, The George Washington University. She received her MS and PhD degrees in Computer Science from the University of Minnesota - Twin Cities in 2000 and 2002, respectively. Her current research interests include Cyber-Physical Systems, Wireless and Mobile Computing, Sensor Networking, Wireless and Mobile Security, and Algorithm Design and Analysis. Dr. Cheng has served in the editorial boards of several technical journals and in the technical program committees of various professional conferences/workshops. She also served as the Program Co-Chair for WASA 2006, and will be the Program Vice Chair for ICPP 2009 and MASS 2009. Dr. Cheng worked as a program director in the National Science Foundation for six months in 2006 and joined NSF as a program director again in April 2008. She received the NSF CAREER Award in 2004.

David H.C. Du, Professor
Department of Computer Science and Engineering, University of Minnesota, Minneapolis
Tel: 612-625-2560, Email: du@cs.umn.edu

Dr. David Du is currently the Qwest Chair Professor of Computer Science and Engineering at University of Minnesota, Minneapolis. He has served as a Program Director (IPA) at National Science Foundation CISE/CNS Division from March 2006 to September 2008. At NSF, he was responsible for NeTS (networking research cluster) NOSS (Networks of Sensor Systems) Program, and worked with Karl Levitt and Ralph Wachter on Cyber Trust Program. Dr. Du received a Ph.D. degree from University of Washington (Seattle) in 1981. He joined University of Minnesota as a faculty since 1981.

Dr. Du has a wide range of research expertise including multimedia computing, mass storage systems, high-speed networking, sensor networks, cyber security, high-performance file systems and I/O, database design, and CAD for VLSI circuits. He has authored and co-authored over 195 technical papers including 95 referred journal publications in these research areas. Dr. Du is an IEEE Fellow (since 1998) and a Fellow of the Minnesota Supercomputer Institute. He is currently serving on the Editorial Boards of several international journals. He has also served as Conference Chair and Program Committee Chair for several major conferences in multimedia, networking, database and security areas. He has had research grants from many federal funding agencies including NSF, DARPA, ONR, and DOE. He has a strong tie with industrial research and has collaborated with a number of companies including IBM, Intel, Cisco, Symantec, Seagate, Sun Micro, etc.