Security and Privacy for Connected Vehicles

Marco Gruteser
Rutgers University

Increasingly autonomous and connected vehicles promise a broad spectrum of efficiency and safety improvements. Automotive transportation in the United States is responsible for more than 30,000 traffic fatalities each year and automotive traffic congestion leads to more than $100 billion in economic losses (according to estimates of the Texas A&M Transportation Institute). Automated and connected vehicles may be able to generate driver alerts in dangerous situations or even take over control to avoid accidents. They may further increase throughput and efficiency on our road network by reducing headway between vehicles or by smoothing driving patterns.

Fully achieving these benefits does not only require increasingly autonomous driving but also connectivity between vehicles and connectivity with Internet services. While autonomous vehicles can gather much relevant information through a variety of on-board sensors (e.g., ultrasound, radar, cameras, or lidar), these sensors can only cover the immediate vicinity of a vehicle. When obstructions exist, such as those from other vehicles or from road-side structures, important information may be hidden from such sensors. One example is an intersection collisions avoidance scenario. If an approaching vehicle from a different direction runs a red light and is obscured by a building or truck at the intersection, it may not be possible for an (semi-) autonomous vehicle to take action in time to avoid a collision. It has also been demonstrated that communication leads to much improved performance of platoons of vehicles following each other with adaptive cruise control technology. Since there is a delay for a following vehicle to detect changes in speed of the preceding vehicle with radar sensors, changes in speed lead to control instability and increasingly abrupt behavior of vehicles towards the end of a vehicle platoon. With radio connectivity, however, the actions of the vehicles at the beginning of the platoon become known to all vehicles with only millisecond delays. This allows reducing headway and leads to a much smoother driving experience.

This increased reliance on sensors and on information obtained over communication links, however, also introduces security and privacy challenges. While much research has been conducted in computer security and privacy, the following are challenges that remain open.

Ensuring integrity and availability of sensor information. While sensors are typically designed for accuracy and robustness, they can also be subject to malicious attacks. Examples include intentionally blinding a camera with a laser or spoofing targets on a radar sensor. If a vehicle naively relies on such sensed information, it could lead to control decisions that jeopardize traffic participant safety. Protecting integrity and availability of sensor information requires defining assessment techniques to evaluate denial-of-service and spoofing risks for such sensors. It also requires a methodology for assessing the security of information that is obtained by fusing information from multiple sensors. Furthermore, techniques to detect attacks would be helpful, at least for the most important sensors that autonomous vehicles rely on.

Associating sensed and communicated information. The integrity of some communicated information can also be verified by checking its consistency with data from local sensors. For example, if a nearby vehicle reports acceleration, camera or radar sensors may be used to check whether the change in distance between the vehicles is consistent with the reported acceleration. This requires, however, that the system can associate the communicated information with targets identified from sensors. The currently envisioned Global Positioning System information in DSRC-related standards, for example, is not always precise enough to create such an association based on position alone. This calls for novel techniques for tagging objects so that sensed information can be linked with information from the virtual world. For example, techniques such as visible light communication can help create identifiers that are detectable with cameras. Such techniques allow adding a code to objects detected through vision, which can be used to associate them to information from network messages. This facilitates consistency checks between vision information and communicated information and overall can improve robustness and security of the system.

Privacy – notice and awareness. Privacy concerns arise as vehicles increasingly collect information, retain information, and share information with outside entities. This information could include places visited or driving styles, for example, which may be considered sensitive private information. A central tenet of privacy enshrined in the fair information principles is the notion of awareness. This means, that drivers should understand what data is collected and shared about them. As the storing and sharing behaviors of vehicles become increasingly complex, we require novel methods for explaining these behaviors to drivers to create awareness.

Understanding and overcoming privacy reliability tradeoffs. Existing privacy techniques such as de-identification and differential privacy not only increase system complexity but also reduce data quality. For cyber-physical systems there is often a direct tradeoff between available data-quality and the reliability of control decisions. Can such privacy techniques be integrated while still ensuring reliability in such high-confidence systems? Are there privacy-enhancing techniques that do not pose this tradeoff?

I believe that the aforementioned challenges provide a starting point for fruitful discussions at the workshop and would appreciate an opportunity to participate in this discussion at the workshop.

Short bio:

Marco Gruteser is an Associate Professor of Electrical and Computer Engineering at Rutgers University and a member of the Wireless Information Network Laboratory (WINLAB). He is a pioneer in the area of location privacy and also recognized for his work on connected vehicle applications. Beyond these topics, his 100+ peer-reviewed articles and patents span a wide range of wireless, mobile systems, and pervasive computing issues. He received his MS and PhD degrees from the University of Colorado in 2000 and 2004, respectively, and has held research and visiting positions at the IBM T. J. Watson Research Center and Carnegie Mellon University. His recognitions include an NSF CAREER award, a Rutgers Board of Trustees Research Fellowship for Scholarly Excellence, as well as best paper awards at ACM MobiCom 2012, ACM MobiCom 2011 and ACM MobiSys 2010. His work has been featured in numerous media outlets including the MIT Technology Review, NPR, the New York Times, and CNN TV.