Next Generation Transportation Systems: Enabling Distributed Decision-Making, Security, and Trust in Networks of Autonomous Automotive Vehicles

Position Statement

December 16, 2013

Alexander M. Wyglinski (PI), Xinming Huang, Taskin Padir, Thomas Eisenbarth,
Lifeng Lai, Krishna Venakatasubramanian
Worcester Polytechnic Institute, Worcester, Massachusetts
{alexw,xhuang,tpadir,teisenbarth,llai,kven}@wpi.edu

Identifying means for distributed, rapidly reconfiguring ad hoc communications robust, decision making and the resulting potential security vulnerabilities associated with networks of autonomous automotive vehicles is vitally important for the future of transportation cyber physical systems (CPS). As well, countermeasures for mitigating these security attacks in order to enhance the protection of this complex CPS framework must be found. These networks of autonomous automotive vehicles employ multiple computing and sensor devices that are used for enabling real-time decision-making by the autonomous platforms in order to perform various operations. However the mechanisms that permit optimizing communications channel management and adaptive distributed decision making in the face of changing information bandwidth, reach and reliability also opens new security sensitivities. Thus these two aspects must be investigated in parallel to obtain the most impactful joint solutions. Consequently, by enhancing the CPS community's understanding on how to "harden" these networks of automotive computing and sensor systems against malicious attacks, we can reduce the likelihood of intentional attacks aimed against networks of semi- and fully-autonomous vehicles in the near future. Although there have been several research activities focused on exploring the potential security vulnerabilities of embedded computing and sensor systems on single vehicular platforms, no one has extensively explored this vast research topic for networks of autonomous automotive vehicles operating in concert, which opens up more potential vulnerabilities relative to any isolated CPS platform; **this effort directly addresses this immediate need for a solution to this problem!** (see more detailed overview of this problems in [1])

Therefore, for *next generation transportation systems* to be realized, we envision that innovative and collaborative work is needed in several key CPS areas:

- **Distributed, Intelligent Decision-Making in Networks of Autonomous Automotive Vehicles**: The concept of optimizing resources across a network has been extensively studied in fields such as management science and wireless networking. However, a network of human-operated, semi-autonomous, and autonomous automotive vehicles attempting to coordinate their activities together can also be viewed as a distributed resource optimization problem of a large CPS framework. Consequently, it is necessary to devise a framework that would enable *distributed optimization of these networks of automotive vehicles*, where each vehicle would possess a state machine-based decision making capability that configures itself based on the prevailing operating conditions at its own location as well as vehicles within its vicinity. Issues such as information latency, robust control, incomplete state information from other vehicles, using different wireless access technologies for facilitating information exchange, and identifying an optimal range for sharing state information with other vehicles would need to be addressed in order to realize a reliable optimization framework for next generation transportation systems.
- **Autonomous Vehicle Security – Intrusion Detection**: When a device depends on information obtained from a remote source or sensor in order to support its operation, it then becomes susceptible to attack by a malicious user. There exist numerous examples in other applications, such as web servers connected to the Internet, and credit card fraud by leveraging WiFi-based financial transactions. In the case of the next generation transportation systems, there exists the danger of a malicious user accessing one or more of the vehicles within the network, and influence it to perform operations that can potentially be detrimental to the overall functionality of part or all of the transportation infrastructure. Consequently, using statistical signal processing techniques such as *distributed change-point detection* can be used to identify the presence of an intruder to the

vehicular network and classify the type of malicious activity being performing, from which actions can be taken by the vehicles within the network to contain the attack and prevent any disruption to the CPS infrastructure.

- **Concept of Trust and Privacy within the Network of Autonomous Vehicles**: Although the detection of malicious activities on the next generation transportation systems is essential to mitigate any intentional disruption to traffic, preventative measures should also be considered. Specifically, devising *trust mechanisms* between vehicles within the next generation transportation system would help minimize intrusions into the network by malicious users by challenging the addition of any new units by requesting specific credentials in order to validate their identify and intent. The objectives of introducing trust within the next generation transportation systems include devising protocols that minimize the probability of missed detection of malicious users, minimize the probability of false alarm when legitimate units request to be added to the infrastructure, and devising trust protocols that are difficult to spoof by an informed malicious user with resource available to generate more sophisticated attacks. Furthermore, in order to prevent data breaches within the next generation transportation infrastructure, which could reveal customer information to malicious entities, *privacy mechanisms* will also be devised to ensure that customer

The following investigators are pursuing research in support of this effort, all of whom possess the following qualifications/expertise:

Dr. Alexander M. Wyglinski, Associate Professor of Electrical and Computer Engineering. Expertise in wireless communications, cognitive radio, software defined radio, distributed optimization/reconfiguration/adaptation.

Dr. Xinming Huang, Associate Professor of Electrical and Computer Engineering. Expertise in embedded systems, computer architecture, field programmable gate arrays.

Dr. Taskin Padir, Assistant Professor of Electrical and Computer Engineering. Expertise in robotics, robust control, cyber physical systems.

Dr. Thomas R. Eisenbarth, Assistant Professor of Electrical and Computer Engineering. Expertise in embedded systems security, side channel attacks and countermeasures, and efficient implementation of cryptographic systems.

Dr. Lifeng Lai, Assistant Professor of Electrical and Computer Engineering. Expertise in wireless communications, information theory, and stochastic signal processing, particularly with respect to their security implications.

Dr. Krishna Venakatasubramanian, Assistant Professor of Computer Science. Expertise in cyber-physical systems and their security, privacy, and trust. Particular foci include system interoperability, credentialing, and maximization of open-source development.

References

[1] Alexander M. Wyglinski, Xinming Huang, Taskin Padir, Thomas R. Eisenbarth, Lifeng Lai, Krishna Venkatasubramanian. “Security of Autonomous Systems Employing Embedded Computing and Sensors.” *IEEE Micro*, January 2013.