A communication protocol for securing connected vehicle platoons using joint hardware-software means

▼ Peijing Li, Computer Science and Engineering, University of Michigan, Ann Arbor, MI

Neda Masoud, PhD, Civil and Environmental Engineering, University of Michigan, Ann Arbor, MI

Corresponding author: Peijing Li, peijli@umich.edu

This poster presents a novel protocol for authenticating and securing communication in platoons of connected vehicles (CV). The protocol utilizes both hardware and software to establish trust between different entities within the platoon. We also propose a validation study for such a protocol using computer simulations. This poster is prepared by Peijing Li, with Dr. Neda Masoud as the faculty advisor of the research project.

The security of vehicular ad-hoc networks (VANETs) and communication topologies within platoons of connected vehicles have been studied with increased interest over the past two decades. However, existing protocols do not specifically account for vehicular platoons, and may make the process of both authentication and securing succeeding communication packets unnecessarily complex. Meanwhile, research over the past decade has focused exclusively on software solutions, and potentials for dedicated hardware such as Trusted Platform Modules (TPMs) have not been fully explored with regards to their impacts on authentication and message integrity checks.

The purpose of this study is to address the issue of improving the efficiency of secured communication within connected vehicle platoons while maintaining the goals of authentication, privacy, and data integrity during the entire process of electing leaders, establishing trust, securing connections, and managing misbehaviors. We propose a new protocol that features the following:

1. A two-level trust system, respectively between an external trust authority and a platoon's leader, and between the leader and remaining members of the platoon.
2. A communication scheme that enables more efficient communication between trusted platoon members via symmetric cryptography.
3. A challenge-response scheme for misbehavior detection that relies upon TPMs of each vehicle to report its operational state to be assessed by a superior in the trust system.
4. A reputation scheme based on the results of said TPM functionalities to determine new leaders of platoons.

This novel protocol should be able to enforce all security goals within a connected vehicle platoon and be resilient against possible attacks and anomalous behaviors, while minimalizing the overhead and number of security-related transactions involved. We will seek to implement and validate this protocol in the near future using traffic and network simulators and compare it against existing protocols in the literature.