PHYS.ORG

New methods keep bugs out of software for self-driving cars

June 21 2011

Driver assistance technologies, such as adaptive cruise control and automatic braking, promise to someday ease traffic on crowded routes and prevent accidents. Proving that these automated systems will work as intended is a daunting task, but computer scientists at Carnegie Mellon University have now demonstrated it is possible to verify the safety of these highly complex systems.

To do so, the researchers first developed a model of a distributed car control system in which computers and sensors in each car combine to control acceleration, braking and lane changes, as well as entering and exiting the highway. They then used mathematical methods to formally verify that the system design would keep cars from crashing into each other.

"The system we created is in many ways one of the most complicated cyber-physical systems that has ever been fully verified formally," said Andre Platzer, an assistant professor of computer science. He and his collaborators, Ph.D. students Sarah M. Loos and Ligia Nistor, will present their findings at the International Symposium on Formal Methods, June 22 at the University of Limerick, Ireland.

"Auto accidents cost society billions of dollars and too many lives, so automated systems that could increase both the safety and efficiency of our roads only make sense," Platzer said. "It would be foolish to move to such a system, however, unless we can be certain that it won't create problems of its own. The dynamics of these systems have been beyond the scope of previous formal verification techniques, but we've had success with a modular approach to detecting design errors in them."

Formal verification methods are routinely used to find bugs in computer circuitry and software; Platzer is a leader in developing new techniques to verify complex computer-controlled devices such as aircraft collision avoidance systems and robotic surgery devices, known collectively as cyber-physical systems, or hybrid systems. He also is a member of the Computational Modeling and Analysis of Complex Systems (CMACS) center, a CMU-based initiative sponsored by the National Science Foundation to apply verification techniques to a variety of complex biological or physical systems.

Using these formal methods to either find errors in automated vehicle control or prove they are safe is particularly challenging, Platzer said. Like other cyber-physical systems, they must take into account both physical laws and the capabilities of the system's hardware and software. But vehicle control systems add another layer of complexity because they are distributed systems — that is, no single computer is ultimately in control, but rather each vehicle makes decisions in concert with other vehicles sharing the same road.

Platzer, Loos and Nistor showed that they could verify the safety of their adaptive cruise control system by breaking the problem into modular pieces and organizing the pieces in a hierarchy. The smallest piece consists of just two cars in a single lane. Building on that, they were able to prove that the system is safe for a single lane with an arbitrary number of cars, and ultimately for a highway with an arbitrary number of lanes. Likewise, they were able to show that cars could safely merge in and out of a single lane and then extended it to prove that cars could safely merge across a multi-lane highway.

Platzer cautioned that this proof has a major limitation — it only applies to straight highway. Addressing the problem of curved lanes, sensory inaccuracy and time synchronization are among the issues that will be a focus of future work. The methods the Carnegie Mellon researchers developed can, however, be generalized to other system designs or to variations in car dynamics.

"Any implementation of a distributed car control system would be more complicated than the model we developed," Platzer said. "But now at least we know that these future systems aren't so complex that we can't verify their safety."

Provided by Carnegie Mellon University

Citation: New methods keep bugs out of software for self-driving cars (2011, June 21) retrieved 20 April 2024 from https://phys.org/news/2011-06-methods-bugs-software-self-driving-cars.html