Quantitative Contract-Based Design Synthesis and Verification for CPS Security

- Alberto Sangiovanni-Vincentelli and Sanjit Seshia
- University of California, Berkeley
- {alberto,sseshia}@eecs.berkeley.edu

- Award 1739816

Description

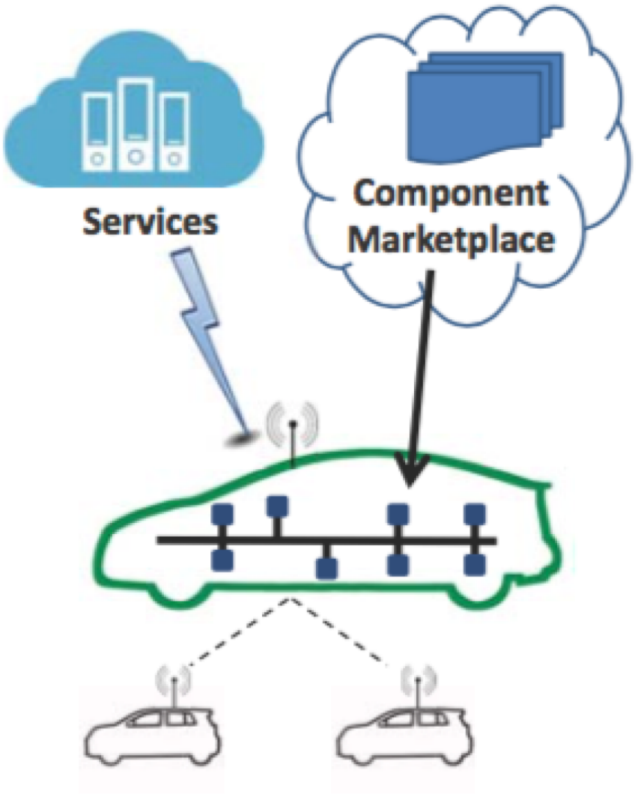
We pursue foundational work on a new methodology for CPS design to enable a "plug-and-play" approach that also ensures the security and safety of the system from the design phase

Goals

- Develop a fundamentally new theory for quantitative contract-based design of CPS that balances security requirements with critical safety and performance concerns

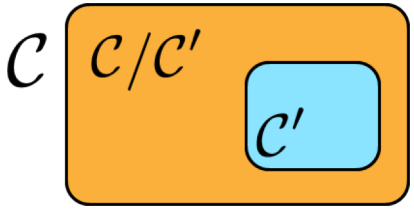
- Provide a precise interface specification for each “plug-in” component in a novel quantitative logical specification

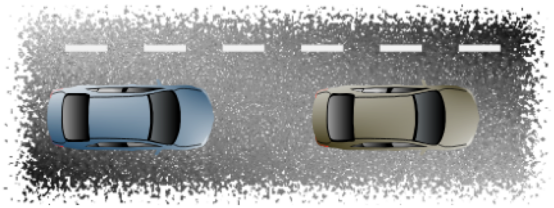
- Develop rapid, run-time verification methods and new approaches to map components onto existing architectures while meeting security and performance constraints



Findings

- Found an explicit form for the quotient of assume-guarantee contracts, an problem open for 10 years
- The quotient is key for decomposing specifications: given a top level spec C and a component C' to be used in the design, how much of the specification is missing?





For example, given a requirement on the minimum distance between vehicles for Cooperative Autonomous Collision Avoidance, we can derive a requirement on network latency

- Currently extending contract-based design to support hyperproperties (security properties) and developing a quantitative language to represent them

Í. Íncer Romeo, A. Sangiovanni-Vincentelli, C.-W. Lin, E. Kang, "Quotient for Assume-Guarantee Contracts", Proc. Int. Conf. on Formal Methods and Models for Co-Design (MEMOCODE), Oct. 2018.