Abstract

Increased dependency on networked, software-based control has escalated the vulnerabilities of cyber-physical systems (CPSs). Real-time hard deadlines for safety-critical functions and limited computing resources pose significant challenges in securing communications through cryptography in CPS. In response, a promising alternative is the design of a lightweight secure framework for resource-constrained CPSs. With a similar philosophy, this doctoral thesis endeavors to propose an end-to-end CPS security framework that is safe, performance-aware, yet resource-friendly and makes the CPS attack resilient. The thesis's main contributions are outlined here.

- The thesis develops a rigorous methodology for estimating the vulnerability of automotive CPSs. A computer-aided design (CAD) framework is presented which considers the model-based representation of safety-critical automotive controllers and monitoring systems working in a closed loop with vehicle dynamics and verifies their safety and robustness with respect to false data injection (FDI) attacks.
- The thesis proposes a real-time, data falsification attack on automotive control loops. The proposed attack is a targeted one that is destined to destabilize a given safety-critical control loop while maintaining its stealth against the safety monitors. Also, the attack model considers platform and network-level uncertainties and determines stealthy and optimal control data falsification dynamically in real time.
- This thesis proposes lightweight FDI detection mechanisms for CPSs that adapt their parameters in a state-sensitive manner. Following the detection of an attack attempt, a formal method-based fast attack mitigation module is presented facilitating the quickest alleviation of system state degradation.
- In case of any latency incurred for attack detection, a CPS may face state degradation. To this end, this thesis proposes a novel attack-resilient control framework that judiciously skips/drops certain instances of control task executions for system robustification.

Keywords:*Cyber-physical systems, Security, Vulnerability analysis, Adaptive detector, Attack resilience*