Online Malicious Intent Inference for Safe CPS Operations under Cyber-attacks

PI: Nicola Bezzo

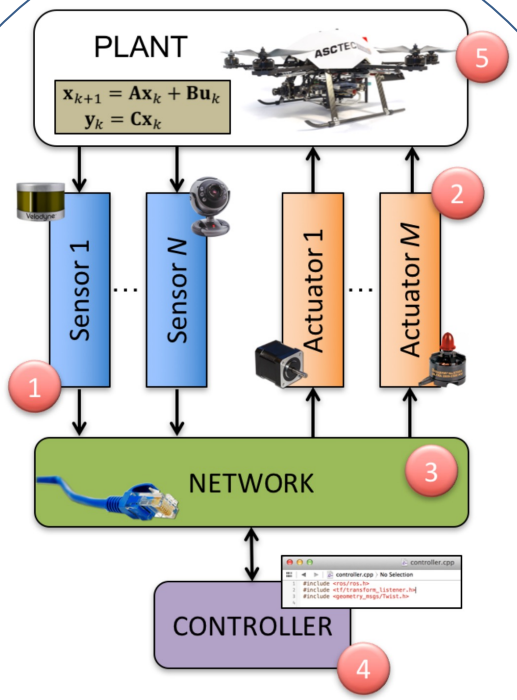
University of Virginia
School of Engineering & Applied Science
Link Lab

Challenge:

- Cyber-attacks on autonomous vehicles can compromise their and surrounding safety.
- Attacks have usually an intent which is challenging to extract.
- Attacks typically hide within known noise and disturbance profiles to avoid detection.

Solution:

- Residual-based method to detect inconsistencies in sensor and communication information.
- Reachability analysis to predict the possible reachable states under cyber-attack constraints.
- Replanning and reconfiguration of the system to continue operating safely



Architecture of a CPS with highlighted the possible attack surfaces.

Scientific Impact:

- Improved detection and isolation of cyber-attacks.
- Proposed techniques scale generally to different types of CPS including single and multi-vehicle systems.
- Proposed residual-approach can be leveraged beyond security to recognize failures.

Broader Impact and Broader Participation:

- Proposed residual and reachability solution can be transferred to different types of CPS and applications.
- Education activities include mini courses on CPS security, lectures, and capstone projects taught by the PI

Award #1816591
PI: Nicola Bezzo
University of Virginia