Secure Operation of Autonomous System

Command and Control Unit
- Cyber-Attack on Mission Plane
- Cyber-Attack on Control and Nav. Systems
- No-fly Zones
- RS-2A: Exposure to cyber-physical attacks by characterizing the attack surfaces, i.e., entry points and likelihoods across mission surfaces in technology & mission-invariant manner.
- RS-2B: Provide quantitative safety and feedback to the mission surface when the limits of secure controllability are compromised
- RS-2C: Provide secure communications across the different layers in the informatics plane from detection of signals to networking.

RS-2A: Securing the Mission Surface

Mission Control for Secure Trustworthy Autonomous Systems requires flexible but reliable real-time optimal decision making and monitoring to handle a wide range of attacks.

Methods and Focus:
- Real-Time Non-Convex Trajectory Optimization for Path Planning under constraints from control & communication
- Adaptive and Fault-Tolerant Learning-based Design for Mission Control to improve reliability of safety-critical systems
- Reliable Self-Assessment under Learning-based Scenarios

Adversarial attacks

Critical impacts
- Perception layer: Manipulate the sensory input of an AS, causing the system to perceive incorrect or misleading information.
- Planning layer: Adversarial attacks can also manipulate the AS’s decision-making process.
- Control layer: Affect the control layer of an AS, leading to incorrect or harmful actions.

Requirements for robust to adversarial attacks systems in the context of AS:
- Able to detect attacks
- Able to react to detected attacks
- Evolve with new unknown types of attacks and situations

RS-2B: Securing the Control and Navigation Surface

Autonomous Systems rely on the ability to conduct real-time adaptations of control decisions over attacks or “perceived” attacks:
- Adversaries
- Environment uncertainties
- Degraded performance

Key Solutions for Operational Safety in Learning-Enabled Context
- AI-based Flight Control System Design and Validation of Dynamics
- AI-aided Visual Inertial Navigation for GPS-denied Environments and GPS Spoofing Detection

RS-2C: Securing the Communication Surface

Physical & Control Layer Security

To secure the communication surfaces of AS, current cryptography and physical layer security (CLS) both have some severe security threats, which motivates the design of control layer security (CLS) that is specific for AS.

Cryptography
- Uses common key pool for cipher key generation, but has following issues:
  - Complex key generation & management & distribution
  - No secrecy guaranteed against post-quantum computing
  - High computational complexity & latency

PLS generates cipher keys via the reciprocal channel information, but has an in-the-middle attack threat.

Designed Control Layer Cipher Keys

Legitimate Alice and Bob (two UAVs) create correlated but unobservable states (e.g., yaw angles), via cooperative control, and use these correlated states as cipher key generation.

RS-2: Secure Operations of Trustworthy Autonomous Systems

Researchers: Dr. Yi Li, Dr. Zhuangkun Wei, Dr. Burak Yuksek, Dr. Oscar Villarreal, Dr. Cynthia Yu, Pierre Ciholas, Alvaro Lopez.

Investigators: Prof. Weisi Guo, Prof. Gokhan Inalhan, Prof. Plamen Angelov, Prof. Antoniois Tsiourdos, Prof. Dan Prince.

This work is supported by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1]