Nonlinear Model Predictive Control

Key Part: Uses a Model of the System to Predict and Optimise the Future Performance

Some Applications:
- Path Planning/Obstacle Avoidance
- Optimising Energy Usage/Generate
- Distributed/Denial/Controlled
- Robust/Stochastic Control (Handing Uncertainty)
- Adaptive and Fault Tolerant Control

Advantages:
- Ability to Anticipate Future Events
- Non-reactive control = Smoother Control Actions
- Handling Time Delays, Nonlinear Dynamics and Constraints

Disadvantages/Challenges:
- Requires a relatively accurate model of the system
- Computational burden = Impacts real-time capabilities

Proposed DNS Potential Fields

Two Common Methods:
- Potential Fields (Current)
- Nonlinear Constraints

Advantages of DNS Potential Field:
- Adaptive Obstacle Avoidance parameters according to communication performance metrics.

Disadvantages:
- Sub-optimal w.r.t. NL Constraints

Multi-Rotor Case Study: Simulation Results

Case Study: Large-scale obstacle avoidance/deconfliction of 20 Multi-rotor UAVs within a cylindrical airspace of 15 meters radius with a height of 10 meters and a DNS attack on a designated area.

Simulation Assumptions/Specifications:
- Models: Double-Integrator with acceleration
- Randomly generated waypoints changing approximately every 3 seconds.
- Path Planning Condition: Maintain a minimum distance of 1 meter to other UAVs.
- Communication: Available through the network when not disrupted by the DNS attacks. UAVs transmit state and parameterised trajectories.

Future Work

- Develop efficient auto-generated algorithms for its implementation.
- Increase the model accuracy to couple with inner UAV dynamics and control systems, as well as to model noise in the system.
- Develop an indoor and outdoor experimental validation of the proposed approach.
- Increase the level of uncertainty from the environment including common GPS positioning errors such as drift, scales or bias, as well as other positioning errors obtained from other sensors such as cameras, optical flow or LiDAR.
- Extends approach to handle Distributed Denial of Service (DNS), as well as other cyber-physical attacks such as GPS/Positioning spoofing and jamming, and propose legible(5) MPC solutions for anomaly detection, monitoring and deconfliction between UAVs.

Key Questions

- How to develop efficient, reliable and secure communication between UAVs for obstacle avoidance?
- How to develop legible control systems which would allow analysis and monitoring from an external observer for cyber-security purposes within the context of obstacle avoidance?
- What information should autonomous vehicles share that would allow anomaly detection and monitoring of cyber-physical attacks from an external point of view?
- How to use legibility and correlation between UAVs control signals to achieve efficient encrypted communication?

Laguerre Polynomials as Parametric Curves

Key Part: Rather than using single waypoints, use a "compressed" smooth representation of the planned trajectory.

Advantages:
- Reduced computational burden
- Smooth trajectories with high computational performance if appropriately tuned
- Capture a large plan with few variables
- Less bandwidth requirements
- Less information to encrypt/decrypt

Disadvantages:
- Can be slightly suboptimal
- Less flexible due to limited options

References

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