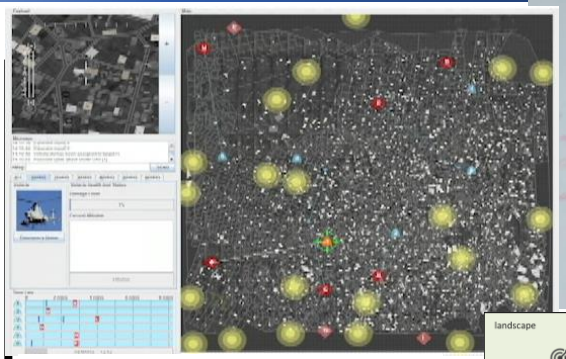
Miroslav Pajic

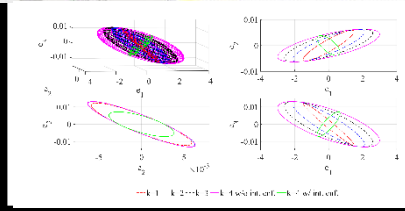
Research Objectives and Key Challenges:

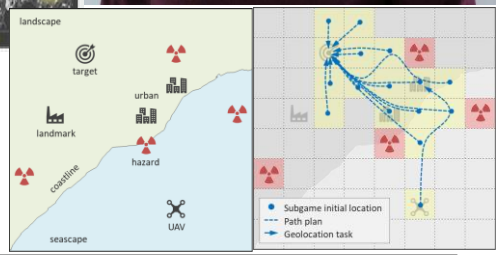
- Provide high-assurance design methods for cyber-physical systems with varying (especially high) levels of autonomy
- Integrate security-awareness in design of control algorithms at each layer of the `control stack' (i.e., hierarchical control)
- How to effectively combine the use of cyber and 'physical' (control-aware security mechanisms in resource-constrained systems

Significance of Work:

- Enable design of autonomous systems with very strong performance (Quality-of-Control – QoC) and mission/safety guarantees even when the systems are under attack
- Enabling control/security co-design to enable quantitative tradeoffs between system guarantees under attack and cost.







High-Level Technical Approach:

- Capturing impact of cyber attacks on (physical) system evolution, as well as performance constraints on the QoC guarantees
- Efficient reachability analysis in the presence of attacks
- Hidden-information games & delayed action games

Potential AFRL Collaboration Areas:

- Attitude control systems
- Navigation estimation with intermittent and corrupted data
- On-line learning of changing dynamics & fault/change detection

Center Research Areas:

- Attack-resilient Design
- Protecting Safety- and Mission-Critical Information

Short-Term Research Vision:

- Mapping the security-aware control algorithms into AF systems

Recent Accomplishments:

- ✓ Developed methods to map available system resources into Quality-of-Control guarantees under attack, as well as to integrate security into resource-constrained legacy systems
- ✓ Developed new strategies for security-aware planning
- ✓ Developed new strategies for attack-resilient design of discrete-event systems while taking into account available resources

Recent Awards:

- 2019 ACM SIGBED Early Career Award, 2019 IEEE TCCPS Early Career Award, ONR YIP, NSF Career, 2018 IBM Faculty Award, 6 Best Paper and Finalist Awards (e.g., EMSOFT'17, ICCPS'14)

Current Funding:

- AFOSR, ONR (including a RHIMES project), NSF (including the Intel-NSF Center on Security and Privacy of Cyber-Physical Systems), and industry partners (e.g., Intel, IBM)

UF UNIVERSITY of FLORIDA · Duke UNIVERSITY · TEXAS The University of Texas at Austin · UC SANTA CRUZ