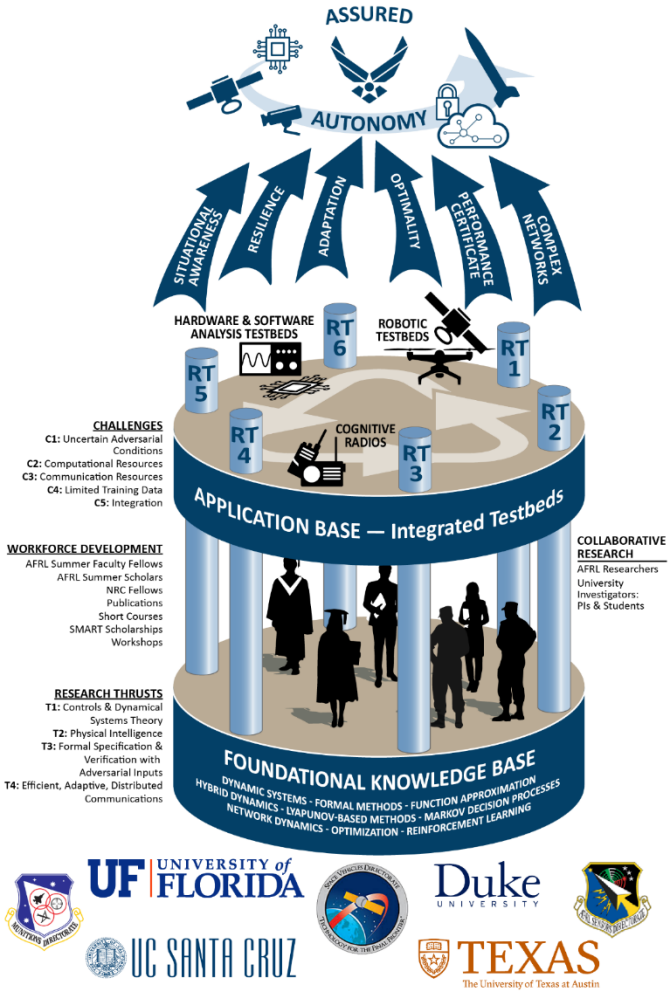
Center Overview

http://ncr.mae.ufl.edu/aacoe.php

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

Center Overview



AFOSR Center of Excellence in Assured Autonomy in Contested Environments

- >$6M over 6 years (3 x 2 year increments)
- 9 PIs @ 4 Universities:
  - K. Butler (UF: cyber resiliency/privacy)
  - W. Dixon (UF: ADP, networks, hybrid)
  - N. Fitz-Coy (UF: optimal, games)
  - M. Hale (UF: networks, privacy)
  - M. Pajic (Duke: cyber resiliency/privacy)
  - R. Sanfelice (UCSC: hybrid, networks)
  - J. Shea (UF: networks, privacy)
  - U. Topcu (UT: formal, hybrid, optimal)
  - M. Zavlanos (Duke: ADP, networks, formal)
- AFOSR provides 50% of funding
- AFRL (RV, RW, RY) provide 50%

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

Center Motivation

- Innovation & technology dominance and strong economy have allowed for exquisite systems that for decades have operated in largely uncontested environments
  - Remote piloted vehicles (RPV) and monolithic satellites provide various strategic and tactical advantages
  - Intelligence, surveillance, and reconnaissance (ISR) in close proximity with RPVs or from protected space assets, while simultaneously striking from distances and with speeds beyond the capability of countermeasures
- These advantages are mitigated as the technology gap closes and as other world economies become near peers and risks to the warfighter and financial costs increase and tactical capabilities become stressed when military operations are in contested or denied environments (i.e., anti-access/area denial (A2AD) environments)
- Increased stand-off distance, persistence, and scaled projection of power have resulted in an urgency for development and fielding of human-in-the loop/semiautonomous systems

Center Motivation

- As these advantages are taken to the limit, coupled with the resultant need for rapid decision-making capabilities, emerging technology will move along a spectrum towards greater automation with less human intervention
- In contested environments, autonomous systems are even further motivated by the potential desire to complete mission execution when communication with a human operator is unavailable
- Autonomous systems must execute high level missions plans with verifiable assurances despite uncertain adversarial environments where the integrity and availability of sensor information and communications are challenged
- Key innovations include analysis, design and synthesis tools that enable autonomous mission execution despite uncertainty within complex dynamics while accounting for the integrity and privacy of information on computationally constrained resources

Center Goals & Vision

- Networks of autonomous systems will require information exchanges of many data types, including high-level mission specifications and sensor feedback for navigation and control
- The goal of assuring autonomy is complicated by the interplay between dynamics of autonomous agents and the stochastic and intermittent dynamics of network traffic
- This challenge is further amplified by delays and asynchrony in information flows
- Information perturbations can also emanate from adversarial actors in unique and complex ways, requiring security-aware design and analysis methods
- For example, we will develop techniques to protect mission-critical information and prevent information disruption/corruption
- These challenges must be addressed considering resource limitations and quantitative tradeoffs.

Research Topics

- Nonsmooth Systems
- Adaptation, Optimality, and Synthesis
- Network Systems
- Asynchronous Information
- Attack-Resilient Design
- Protecting Information

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

Workforce Dev. AFRL Collaborations Publications

UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

Collaborative Interactions

- Project partially supports
  - 4 postdocs/research scientists, ~50PhD
- >30 Alumni
  - 6 postdocs – NVIDIA, Univ. of Sherbrooke, Univ. of Arizona, Apple, Univ. Grenoble Alpes, UC Berkeley
  - 18 PhD – RW (x2), Ford, Qualcomm, Intel, Univ. of the Bio, Opener, Purdue University, Dematic, DJI, Amazon, Satellogic, University of Florida, Zoox
  - 7 MS – Lockheed Martin (Orlando), Walmart Labs, UCSC, Zoox, Intel, AgroAI, Rain
- SMART Fellow for RV: S. Edwards (Dixon)
- >10 Summer 2022 AFRL/Space Scholar/interns
  - RV: G. Behrendt (Hale), A. Allen (Fitz-Coy)
  - RW: W. Warke (Hale), A. Benvenuti (Hale), C. Makumi (Dixon), A. Lee (Dixon), C. Nino (Dixon), K. Sivakumar (Zavlanos), Z. Lamb (Sanfelice)
  - RY/Act3: W. Garcia (Butler), C. Fedele (Butler)
- AFRL Summer Faculty Fellows program
  - Riccardo Bevilacqua (2019 & 2020 RW, 2021 RV)
  - Matthew Hale (2020 RW)
- Additional support could fund new hires (e.g., Yu Wang, outstanding offers in space)

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

Additional Activities

- Publications
  - >250 total, ~30 published or accepted to appear so far in 2022
  - Joint publications - 36 w/ PIs, 29 w/ AFRL

- Testbed Development
  - Netted facility installed
  - Finalizing permitting breaking ground for ground station
  - International collaborations (Brazil)
  - Certification courses and other educational outcomes?
  - Interest by AFRL, AFA, Northrup Grumman, Draper, ….

Additional Activities

- Additional Activities in (late 2021) 2022
  - (All) 7 Keynote, plenary, and invited talks in late 2021, 2022
  - (Fitz-Coy, Dixon) Certificate programs being proposed at UF (Astronautics, Autonomy)
  - (All) Continued bi-monthly seminar series (Spring 2022)
  - (Pajic) Member of the IST-122-ET Research Task Group (RTG) on Designing resilient autonomous vehicles, NATO Science and Technology Organization, 2022-present.
  - (Pajic) Consultant to IST-164 Research Task Group (RTG) on a recently released report on "Securing Unmanned and Autonomous Vehicles for Mission Assurance", part of the NATO Science and Technology Organization
  - (Topcu) Organized a panel on assured autonomy at the annual AAAS meeting: Assured Autonomy: A Socioeconomic-Technical Opportunity and Challenge
  - (Topcu) STTR Phase 2 with Verus Research for is Assured and Autonomous Coordinated Inspection (Sean Phillips)
  - (Pajic) organized a panel on "Resilient Cyber-Physical Systems: State of the Art and Future Challenges" at the 2021 Military Communication Conference (MILCOM), December 2021
  - (Pajic) had an "Interdisciplinary Approach to Resilient Cyber-Physical Systems: State of the Art and Future Challenges", Tutorial at the 2021 MILCOM
  - (Pajic) organized and chaired an NSF-initiated Workshop "Next Big Research Challenges in Cyber-Physical Systems"
  - (Sanfelice) 2nd Workshop on Computation-Aware Algorithmic Design for Cyber-Physical Systems, A co-located workshop of the 2022 CPS-IoT week, May 3-6, 2022.

Click to edit Master title style

- **(Pajic)** updated Gen. Mark Milley, Chairman of the Joint Chiefs of Staff, on the AFOSR CoE efforts in the domain of assured autonomy in contested environments

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

Overview of Today's Talks

UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

Overview

- **Breakthroughs discussed during review**
  - Autonomous rendezvous and docking of spacecraft using hierarchical model-based reinforcement learning
  - Hierarchal reinforcement learning for switched ADP
  - Development of reinforcement learning techniques for optimal synchronization/localization for distributed asset tracking in GPS-denied environments
  - Lyapunov-based deep learning (fully connected and ResNet architectures)
  - Accelerated Gradient Descent Methods for control
  - Deep Q-learning techniques for optimizing spectrum reuse in distributed spectrum sharing
  - New analysis and synthesis methods for developing multiagent systems that are robust to communication loss
  - A new transfer learning method for risk-averse multi-armed bandits (MAB) that uses data from an expert agent who can observe more context to help a learner agent who cannot observe the same context

Overview

- **Breakthroughs discussed during review**
  - A new momentum zeroth-order method for convex games with risk-averse agents. Specifically, a new one-point zeroth-order gradient estimate is proposed that both reuses past samples and previous gradient estimates to reduce the variance
  - General security analysis of perception-based control and autonomous systems, focusing on our recent results showing how to quantify the attack impact on control performance for different threat models
  - Application of formal privacy definitions to behavioral data streams
  - Analyzing multi-task learning in heterogeneous multi-agent systems
  - Feasibility of Higher Order Barrier Functions for uncertain nonlinear systems
  - A new topological regularization method for nonconvex optimization
  - Estimation for hybrid systems (hysteresis-basis switching observers, estimation with partial information)
  - Safety (regularity of invariance-based feedback, monotonicity certificates)
  - Hybrid control (hysteresis-based RL, hybrid opportunistic control, hybrid control on manifolds)