Center Overview

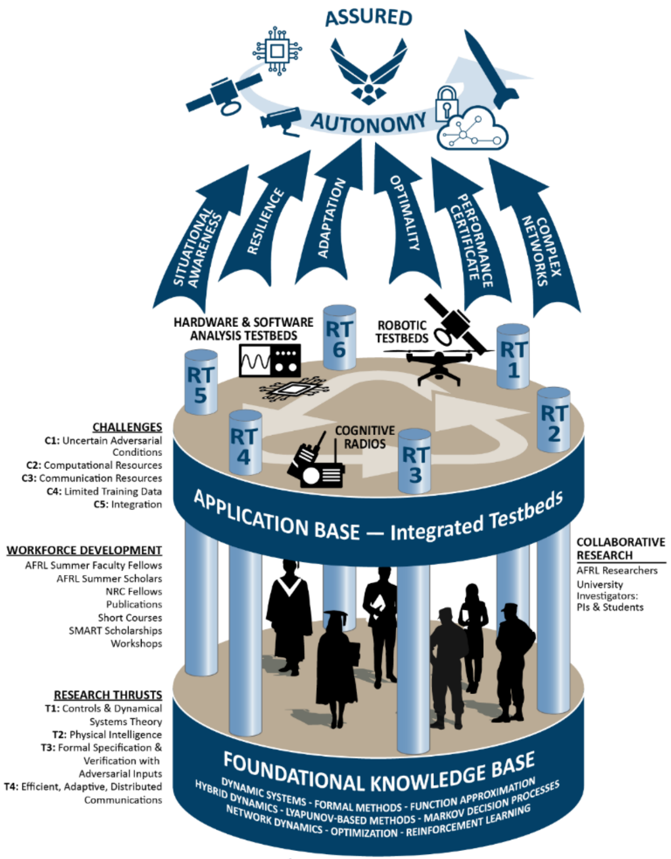
UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

Center Overview


ASSURED
AUTONOMY
SITUATIONAL AWARENESS
RESILIENCE
ADAPTATION
OPTIMALITY
PERFORMANCE CERTIFICATE
COMPLEX NETWORKS
HARDWARE & SOFTWARE ANALYSIS TESTBEDS
ROBOTIC TESTBEDS
COGNITIVE RADIOS
RT 1
RT 2
RT 3
RT 4
RT 5
RT 6
APPLICATION BASE — Integrated Testbeds
CHALLENGES
C1: Uncertain Adversarial Conditions
C2: Computational Resources
C3: Communication Resources
C4: Limited Training Data
C5: Integration
WORKFORCE DEVELOPMENT
AFRL Summer Faculty Fellows
AFRL Summer Scholars
NRC Fellows
Publications
Short Courses
SMART Scholarships
Workshops
COLLABORATIVE RESEARCH
AFRL Researchers
University Investigators: PIs & Students
RESEARCH THRUSTS
T1: Controls & Dynamical Systems Theory
T2: Physical Intelligence
T3: Formal Specification & Verification with Adversarial Inputs
T4: Efficient, Adaptive, Distributed Communications
FOUNDATIONAL KNOWLEDGE BASE
DYNAMIC SYSTEMS - FORMAL METHODS - FUNCTION APPROXIMATION
HYBRID DYNAMICS - LYAPUNOV-BASED METHODS - MARKOV DECISION PROCESSES
NETWORK DYNAMICS - OPTIMIZATION - REINFORCEMENT LEARNING

AFOSR Center of Excellence in Assured Autonomy in Contested Environments

- $6M over 6 years (3 x 2 year increments)
- 10 PIs @ 4 Universities:
  - R. Bevilacqua (UF: optimal, switching)
  - 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%

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.

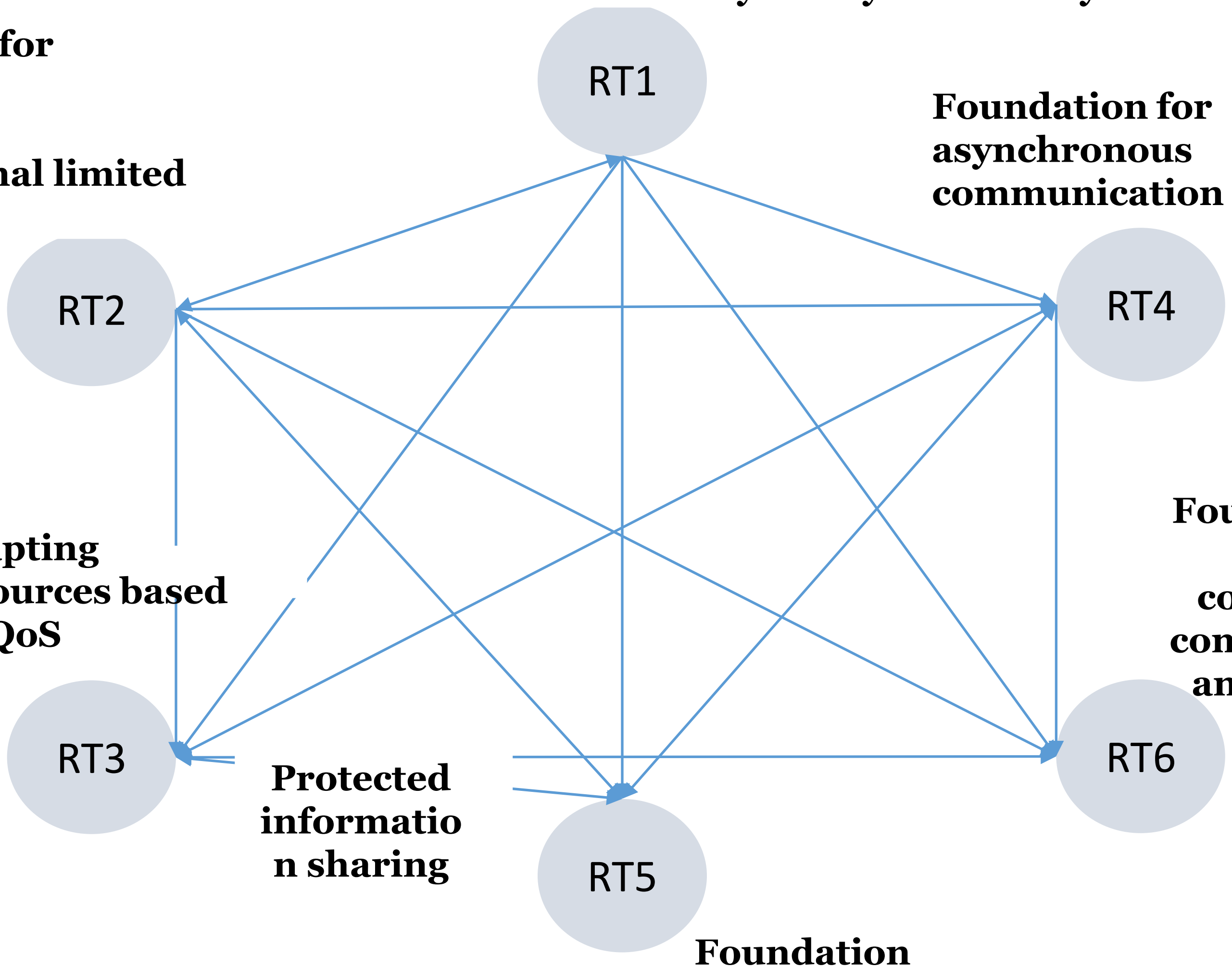
Center Goals & Vision

- 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

Tightly Coupled RTs



Foundation for hybrid systems analysis

Foundation for adaptation, optimality, computational limited resources

Foundation for asynchronous communication

Foundations for protected computation, communication, and execution

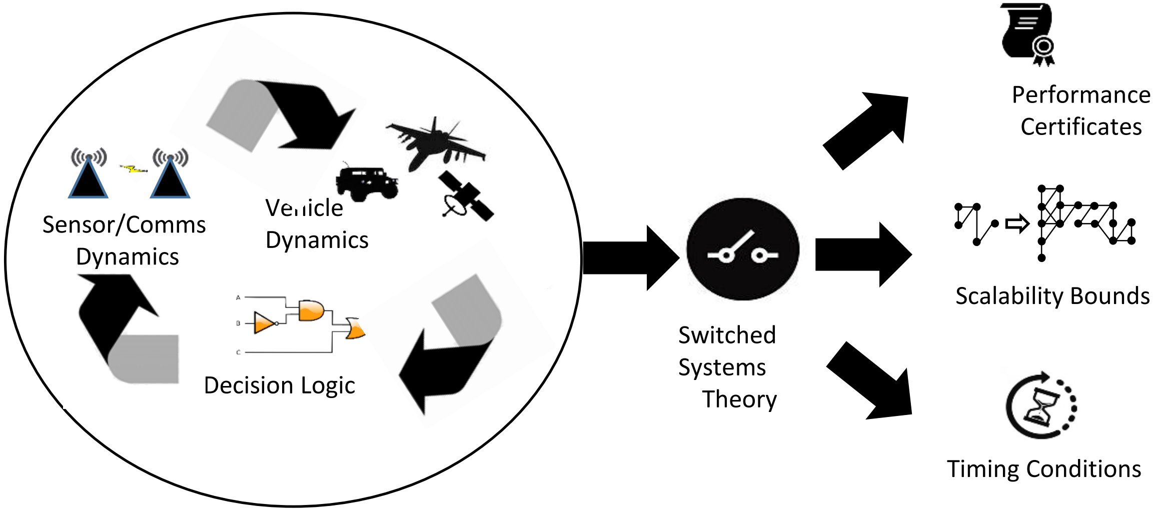
Adapting resources based on QoS

Protected informatio
n sharing

Foundation for resiliency

Nonsmooth Systems

- Most of the results in the center involve complex systems that have multiple modes of operation, interaction with multiple agents, sequent of events that trigger different actions, decision logic that must be reasoned about, etc. – the fusion of information and dynamics
- This RT permeates most of the other RTs, but open questions remain regarding the development new nonsmooth analysis and design frameworks for safety, intermittency, asynchrony, uncertainty.



Nonsmooth Systems

- Some Major Contributions
  - Generalizations of Lyapunov-based methods for arbitrary switched systems, with reduced solutions sets for differential inclusions (e.g., impact today in RT2 topic)
  - Control and coordination under intermittent information, advances in refined understanding of dwell-time conditions (strong connection to RT3)
  - Development of Hybrid MPC methods with sufficient conditions for asymptotic stability of closed sets
  - Integration with temporal logic specifications for verification and barrier certificates for forward invariance (safety) of hybrid dynamic systems (strong connection to RT2 & 5)

Adaptive, Optimal, Synthesis Methods

- Complex environments often exhibit uncertainty, yet, there is a desire for autonomous systems to make the best possible (optimal) decision despite the uncertainty, and in a timely manner e.g., to meet high-level specifications.
- Further complexities emerge when the system is changing among different subsystems, or the uncertainty is time-varying.

- Some Major Contributions
  - Data-based integral concurrent learning (ICL) methods for finite and verifiable system identification and tracking, facilitates the development of dwell-time conditions (strong connection with RT1)
  - Approximate dynamic programming to learning an optimal policy on-line despite uncertainty, stochasity, or switching dynamics and cost while yielding exploration versus exploitation through Bellman Error extrapolation, and considering computational demands through sparse learning, and in a safe and distributed manner, including off-policy learning and learning with constraints

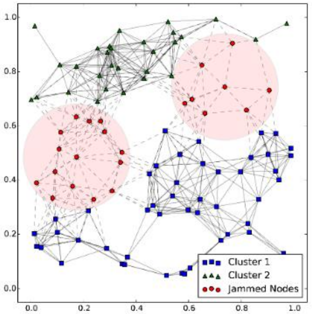
Adaptive, Optimal, Synthesis Methods

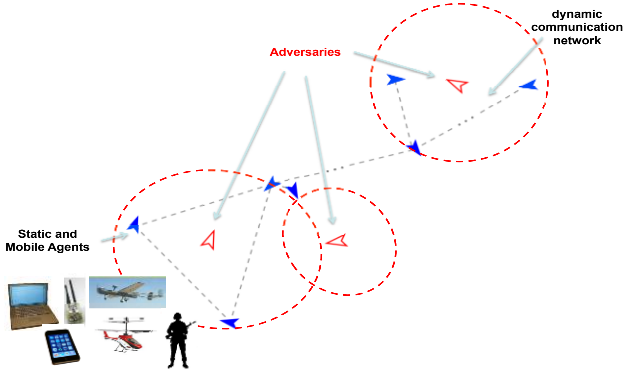
- Some Major Contributions (cont.)
  - Transfer learning to gain experience by leveraging experience gained in related tasks
  - Optimal path-planning in the presence of uncertain and time-varying obstacles, including socially aware path planning around people, or using abstraction-free synthesis methods to satisfy temporal logic specifications (strong connection to RT5), including scalable temporal logic and transfer planning for temporal logic
  - Formal methods and learning advancements such as deep Q learning for Markov Decision Processes (MDP)

RT3 &4

Network Systems & Asynchronous Information

- Ensuring the availability and integrity of information in complex contested environments presents a number of challenges for autonomous agents.
- These challenges are exacerbated for large networks of agents operating in adversarial conditions (e.g., issues of scalability, computational resources, verifiability, collaboration strategies, and additional unique complexities).
- Since such networks are the union between the physical agent dynamics and the information dynamics, this research topic focuses on analysis, design and synthesis methods for agents *within a network and over a network*.
- Moreover, sharing information across the network can lead to variable and unknown time-delays and asynchrony among agents in the network.





Network Systems & Asynchronous Information

- Some Major Contributions
  - Disrupting adversarial networks through optimal and suboptimal jamming of nodes
  - Improving internal networks by identifying bottlenecks in networks of networks
  - Coordination over networks through multi-agent synthesis and control such as formal methods for correct-by construction synthesis, significant efforts in resilience to environmental challenges, remote observation, and intermittent dynamics (strong connection to RT1)
  - Compensating for uncertainty while optimally coordinating agent dynamics (strong connection to RT2) via multi-agent learning and optimization

Attack Resilient Design

- The goal of this research topic is to address security challenges related to attacks against a multi-agent mission where the attacker can (1) take over a sensor and supply wrong or untimely sensor readings, (2) disrupt actuation, (3) affect communication between agents, or (4) even compromise some of the agents involved in the mission.
- These attacks manifest themselves as malicious interference signals, and the defenses against them have to be introduced in the control/autonomy design.
- Our key research results have focused on security-aware control design for systems with varying levels of autonomy, while guaranteeing the desired levels of system performance (i.e., Quality-of-Control) even when the system is under attack. Our goal has been to add resiliency at every level of the autonomy-stack (low-level control, switched controllers, planners).

Attack Resilient Design

- Some Major Contributions
  - Security for network systems (close connection with RT 3&4) via a novel moving target defense strategy that randomly changes the availability of sensor data
  - Integrating security on resource constrained environments through residual intrusion detectors
  - Attack resilience supervisory control of discrete event systems (strong connection to RT1)
  - Secure aware planning through delay actions games and learning policies to maximize the probability of satisfying temporal logic constraints (strong connection to RT2)
  - Modeling, design and analysis for security- and privacy-aware systems by verifying probabilistic hyperproperties
  - 5 software tools have been developed for download

Protecting Safety- and Mission-Critical Information

- Agents' actions can be observed by adversaries and decisions to change modes, e.g., from surveying an area to pursuing a target, can reveal modes of operation and switching strategies to adversaries (strong connection to RT1)
- Agents' communications can also be intercepted, including communications within and between teams of agents, and these communications can contain sensitive information, such as the agents' intents and tactics (strong connection to RT3)
- While adversarial environments can impose a variety of disturbances from external sources, efforts in this research topic will also explore the strategic disruption of information as a means to safeguard agents' actions and communications

Protecting Safety- and Mission-Critical Information

- Some Major Contributions
  - We developed a method for entropy maximization in MDPs under temporal logic specifications (strong connection to RT2) and partial observable MDPs (POMDP)
  - Developed methods to minimize information leakage regarding high-level task specifications
  - We studied the problem of distributed hypothesis testing, where a team of mobile agents aims to agree on the true hypothesis that best explains a sequence of their local and possibly noisy observations (strong connection to RT3)
  - Numerous advances on differential privacy for distributed hypothesis testing, quantifying amount of information to share based on privacy needs, developed bounds for differentially private Kalman Filter, and for synthesizing multi-agent policies that satisfy temporal logic specifications, secure localization
  - Secure machine learning
  - Protocol model learning for embedded systems

Workforce Development & Overview

UF UNIVERSITY of FLORIDA

Duke UNIVERSITY

TEXAS The University of Texas at Austin

UC SANTA CRUZ

Collaborative Interactions

Current AFRL Engagement

- Project partially supports 5 postdocs/research scientists, 35 PhD students, ~5 MS thesis students
- Joint publications
- SMART Fellowship student at RW (Zach Bell) – new student applied and was accepted but not picked up by AFRL
- AFRL/Space Scholar/intern ~10 students summer 2020
- AFRL Summer Faculty Fellows program
  - Riccardo Bevilacqua (2019 & 2020 AFRL/RW)
  - Matthew Hale (2020 AFRL/RW)
- Hiring shift to more domestic students by some PIs

Highly productive year

- 99 publications accepted or to appear