Opportunity Title: Security of Distributed Safety-Critical Control for Networked Systems Unclassified Key Fellowship
Opportunity Reference Code: ICPD-2024-15

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2024-15

How to Apply

Create and release your Profile on Zintellect – Postdoctoral applicants must create an account and complete a profile in the on-line application system. **Please note: your resume/CV may not exceed 3 pages.**

Complete your application – Enter the rest of the information required for the IC Postdoc Program Research Opportunity. The application itself contains detailed instructions for each one of these components: availability, citizenship, transcripts, dissertation abstract, publication and presentation plan, and information about your Research Advisor co-applicant.

Additional information about the IC Postdoctoral Research Fellowship Program is available on the program website located at: https://orise.orau.gov/icpostdoc/index.html.

If you have questions, send an email to ICPostdoc@orau.org. Please include the reference code for this opportunity in your email.

Application Deadline 2/28/2024 6:00:00 PM Eastern Time Zone

Description

Research Topic Description, including Problem Statement:

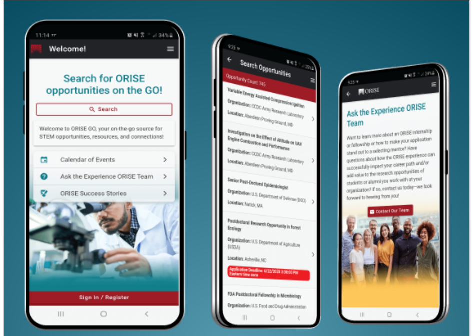
This project explores novel approaches to distributed control over networked systems that address a safety-critical need. Traditionally, control of networked systems does not scale well. Distributed methods are then used to address this scaling issue, often by treating signals from other parts of the system as disturbances and then using a small-gain criteria to guarantee stability. These methods can be overly conservative, however, and new approaches are needed. The overall performance of the system may already be diminished when enforcing the control system to have a distributed structure, so innovations that allow us to capture some of that performance are interesting.

Recapturing performance, however, does not necessarily, in-and-of-itself address security issues. The security of these systems is often seen as an after-thought, and techniques that design and engineer for security from the beginning are needed for tomorrow's applications.

Example Approaches:

Critical infrastructure systems often require high-performance distributed control technologies with safety-critical guarantees and securing them in the cyber-physical-human environment is essential for their practical deployment.

Relevance to the Intelligence Community:


Welcome!
Search for ORISE opportunities on the GO!
Search Opportunities
Ask the Experience ORISE Team

- Securing critical infrastructure systems with safety-critical guarantees, including critical manufacturing, chemical manufacturing, power systems, etc.
- Develop/enhance capabilities to identify and protect critical assets, information systems, technologies, industries, and people.

Key Words: Control System Security, Distributed Control, Networked Systems, Safety-Critical Control

Qualifications

Postdoc Eligibility

- U.S. citizens only
- Ph.D. in a relevant field must be completed before beginning the appointment and within five years of the appointment start date
- Proposal must be associated with an accredited U.S. university, college, or U.S. government laboratory
- Eligible candidates may only receive one award from the IC Postdoctoral Research Fellowship Program

Research Advisor Eligibility

- Must be an employee of an accredited U.S. university, college or U.S. government laboratory
- Are not required to be U.S. citizens

Eligibility Requirements

- **Citizenship:** U.S. Citizen Only
- **Degree:** Doctoral Degree.
- **Discipline(s):**
  - **Chemistry and Materials Sciences** (12 👁)
  - **Communications and Graphics Design** (6 👁)
  - **Computer, Information, and Data Sciences** (17 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (11 👁)
  - **Other Non-Science & Engineering** (2 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (30 👁)