Opportunity Title: Detecting malicious activity on distributed IoT sensor/actuator networks
Opportunity Reference Code: IC-18-36

Organization Office of the Director of National Intelligence (ODNI)

Reference Code IC-18-36

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 2 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://orau.org/icpostdoc/.

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

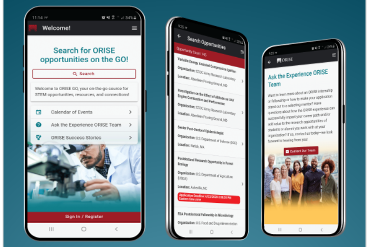
Application Deadline 3/12/2018 11:59:00 PM Eastern Time Zone

Description **Research Topic Description, including Problem Statement:**

- The goal of this research is to identify and confirm approaches to the modelling and detection of malicious entities on networks based on the behavior of the nodes themselves as they operate the network. The principal challenge is being able to model within each node the health and integrity of the entire network without the use of external/global clocks or other global contextual information. Memory, power and processing constraints should be considered in addition to algorithmic challenges.
- Current work on the cyber security of distributed sensor/actuator wireless networks (such as Internet of Things) concentrates on the content being conveyed over the network. However, the network will most likely be attacked at the protocol level in order to deny service, pollute/corrupt routing, fuzz/fake authentication, and so on. There is very little consideration of this in a range of commercial developments with the risk that large scale commercial roll out will preload consumer and critical national infrastructure applications with potential vulnerability.

Example Approaches:

- As related background, it is known that the user bandwidth of linear chains of wireless nodes declines as roughly 1/N (where, N=number of nodes), and that this can be overcome by careful control of the frequency of datagram injection into the chain. This is achieved by time-


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

aligning the states of the node (assuming RX, Proc., and TX states) so that a “green wave” is created. This state oriented view can be extended to include the cyber security of the network by each node modelling the context of its role in the network so that anomalous behavior or effects can be detected: if each node knows what states it can adopt and the relationship of the sequence of those states with its neighbors, it will be possible to both optimize performance through tuning and also the detection anomalies (including potentially in distant nodes).

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 application deadline
- 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** (16 👁)
  - **Earth and Geosciences** (21 👁)
  - **Engineering** (27 👁)
  - **Environmental and Marine Sciences** (14 👁)
  - **Life Health and Medical Sciences** (45 👁)
  - **Mathematics and Statistics** (10 👁)
  - **Other Non-Science & Engineering** (5 👁)
  - **Physics** (16 👁)
  - **Science & Engineering-related** (1 👁)
  - **Social and Behavioral Sciences** (28 👁)