Opportunity Title: Radio Frequency (RF) Spectrum Sensor Network for Detection & Identification of Devices
Opportunity Reference Code: ICPD-2021-52

Organization Office of the Director of National Intelligence (ODNI)

Reference Code ICPD-2021-52

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://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 2/26/2021 6:00:00 PM Eastern Time Zone

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

The rise of the Internet of Things has seen an increased use of wireless technologies to provide connectivity between devices. These platforms are vulnerable to various types of attack, and authentication of devices, spoofing, and detecting unauthorized transmissions are a constant challenge. Some progress has been made to address this through device fingerprinting, which identifies unique elements specific to a device. However, more work is needed to provide greater security to our wireless network, particularly in a dense radio frequency (RF) environment where detection of malicious activity is challenging. This could make it even more challenging to secure environments for legitimate devices.

This topic seeks to understand the dynamic RF landscape and build on previous research to detect and identify a specific radio among similar devices in a dense environment and catalogue these accordingly. The ambition is to achieve an intelligent sensing capability that can detect all devices operating in a dense RF environment and define its fingerprint as legitimate or unauthorized, adding it to a classifier. This will provide better security from malicious activity for the public spaces. This will also help the security community better protect its environment and could be of use to detect unauthorized devices in places such as prisons.

The aim of the research is to:

- Build on existing research in this field and develop a prototype for practical use to detect threats within the dynamic RF landscape.
- Develop a means of identifying unauthorized devices through effective fingerprinting.
- Develop a classifier to identify unique signatures for devices that are robust enough to work in a dynamic environment.
- Develop counter measure approaches for unauthorized devices, such as denial of service or location, to enable recovery and proactive investigations.

Example Approaches:

Some pioneering early investigative work examined the concept of radio fingerprinting, detecting specific devices within a distance of 2 to 50 feet using deep-learning, convolutional neural

Opportunity Title: Radio Frequency (RF) Spectrum Sensor Network for Detection & Identification of Devices
Opportunity Reference Code: ICPD-2021-52

networks. This has also built on previous research examining device fingerprinting in wireless networks.

Relevance to the Intelligence Community:

Detection and location of malicious devices is becoming increasingly challenging. Identifying and effectively classifying devices is important to the security community to protect public spaces and disrupt organized crime. It will also better prevent unauthorized devices from being taken into secure environments, such as prisons. The ambition is to have a classifier of unique device fingerprints, building on previous research.

Key Words: RF, Sensors, Software, Distributed Networks, Pattern Recognition

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** (2)
  - **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** (2)
  - **Physics** (16)
  - **Science & Engineering-related** (1)
  - **Social and Behavioral Sciences** (27)