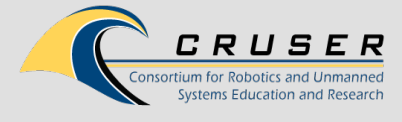# ROS 2: Cyber Security and Network Robustness for Robotics

Key use cases for ROS 2: embedded systems,, DoD products, and multi-robot systems.

How: Collaboration with the Open Robotics

- Provide method of direct collaboration between NPS and OSRF on design, implementation and evaluation of ROS 2.
- Provide software development support for thesis students and researchers at NPS developing secure, robust autonomous systems.
- Provide DoD-specific documentation and training on a certifiable, secure variant of the ROS software ecosystem appropriate for direct DoD implementation.
- Evaluate security implementation of ROS 2 at NPS using proven NPS cyber security models.

- In collaboration with the Open Source Robotics Foundation (OSRF), we propose to design, build and evaluate an update of the Robotics Operating System (ROS) that addresses two DoD/DoN specific issues:
  - Cyber security for robotics
  - Robustness to intermittent communications (e.g., mesh networks and acoustic communications)
- NPS and OSRF will collaborate on the development of ROS 2 through combined design efforts, development of DoD-specific use-cases, guest lectures and seminars by OSRF developers and dedicated technical support from OSRF software engineers to support NPS thesis students.

- Evidence suggests that ROS 1 is the de facto standard in the academic and development communities, including government research labs and warfare centers (http://wiki.ros.org/Metrics).
- A barrier for rapid transition of many of these emerging capabilities is the distinct software needs for DoD programs, including verifiable cyber security and robustness to intermittent communications.
- By participating directly in the development or ROS 2, NPS can help ensure that these capabilities are part of the foundational design to speed future transitions of DoN robotics capabilities.

FY18 Call for Proposals

Brian Bingham, Associate Professor, Mechanical and Aerospace Engineering

Preetha Thulasiraman, Associate Professor, Electrical and Computer Engineering