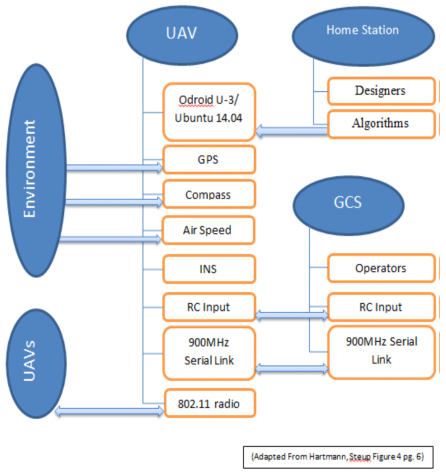
Study of Cybersecurity Requirements for the Military Robot Operating System (ROS-M) using ROS 2.0 on Unmanned Aerial Networks

CRUSER
Consortium for Robotics and Unmanned Systems Education and Research



Representation of the UAV architecture and the various vulnerable entry points into the system

How

- 1) Begin with studying ROS-M cybersecurity requirements; Understand ROS-M technical scope, particularly ROS 2.0
- 2) ROS-M Cybersecurity Framework
  - Build PKI on the ROS-M environment using techniques specified by SROS and ROS 2.0
  - Study management of public and private keys for PKI and how to securely disseminate keys among different ROS-M nodes
  - Evaluate the ROS-M PKI via simulations of small UAV networks using the Gazebo simulation platform
  - Evaluate how ROS-M cybersecurity mitigates different threat models

What/Deliverables

- Manage cybersecurity risk such that near term capabilities for systems autonomy can be achieved
- Assessment of the military security standards associated for open source software and determine if such security practices can be implemented for ROS-M using Secure ROS (SROS)/ROS 2.0 as proposed by OSRF
- Study cybersecurity primitives in the ROS-M environment (public key infrastructure (PKI), key management for PKI and securing wireless channel through secure handshake) based on SROS and ROS 2.0
- Analysis of exploitation avenues for ROS-M on small aerial networks
- This is a continuation of work executed in FY17 in which security for the standard ROS 1.0 platform was investigated

Why/Objective

- DoD is seeking to build a military centric ROS
- Implementation of ROS-M and ROS 2.0 is currently in its development phase
- Adoption of one operating framework (ROS-M) would lead to cost savings in program development cycles as well as an increase in reliability and operability
- Ability to securely control ROS-M enabled platforms free from adversarial interference is of the upmost importance.
- The proposed research is operationally relevant and will contribute to relevant thesis study for NPS students
- Cybersecurity is an important research and curricular component at NPS and thus furthers the mission of the school, Navy and DoD.

FY18 Call for Proposals

Dr. Preetha Thulasiraman, Associate Professor
Department of Electrical and Computer Engineering
pthulas1@nps.edu, Office Ph: 831-656-3456