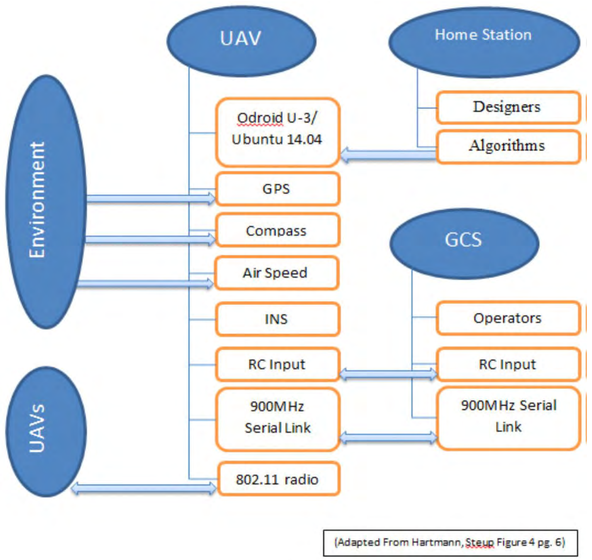
Study of Security Primitives for the Robot Operating System (ROS) of UAV Swarms

Naval Postgraduate School



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

- 1) Begin with a comprehensive survey on ROS and its internal dynamics
- 2) Test and experiment with the ROS implementation and management on the Odroid of the UAV
- 3) Implement security primitives in the ROS environment
  - Study the implementation of Message Authentication Codes (MAC) for ROS message authentication
  - Study the implementation of the Advanced Encryption Standard (AES) for dealing with plain text ROS messages
  - Study the impact of security primitives on various threat models, specifically man-in-the-middle (MITM)

- Highlight ROS vulnerabilities and study its use and management in the UAV swarm, including how messages are sent, received, and processed
- Study the implementation of security primitives (authentication, authorization, and encryption) for the ROS used in UAVs
- Quantify the performance change (if any) that these security primitives incur on ROS and the UAV system as a whole
- This is a continuation of work stated in FY16 in which security for the UAV communication link was studied
- We take the baseline security algorithms studied in FY16 and apply them to the other major vulnerability of a UAV-the ROS

- To develop additional security enhancements to the UAV swarm
- To continue to develop a comprehensive security architecture for the UAV swarm
- 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.

CRUSER Consortium for Robotics and Unmanned Systems Education and Research

FY17 Call for Proposals

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