Next Generation Counter-sUAS Swarm Technology

School of Electrical Engineering & Computer Science
UNIVERSITY OF NORTH DAKOTA

Joseph Schwalb, Martin Pozniak, David Johnson, Prakash Ranganathan

Rockwell Collins

DECS

National Airspace Issue

The recent surge in commercial and hobby use of small unmanned aircraft vehicles (sUAS) has created an unprecedented number of aircraft within the National Airspace System (NAS) (**Figure 1**). As a result, the instances of airspace violations and risk to critical infrastructure has increased. This project is focused on development of UAS subsystems supporting autonomous flight missions in a swarm environments. Successful completion will clarify the requirements for off-the-shelf components enabling safe integration into the NAS. Working groups within this project include: Networking, Simulation, Flight Logic, Hardware, Cybersecurity, Power Systems, and Computer Vision.

Flight Logic

The goal of this group is to understand challenges with the technology stack required to control the flight in a congested environment. This includes communication and incremental adjustment of vehicle flight plans. Successful completion will commence with understanding the impact on flight path communication protocols of NAS integration (**Figures 2, 3**).

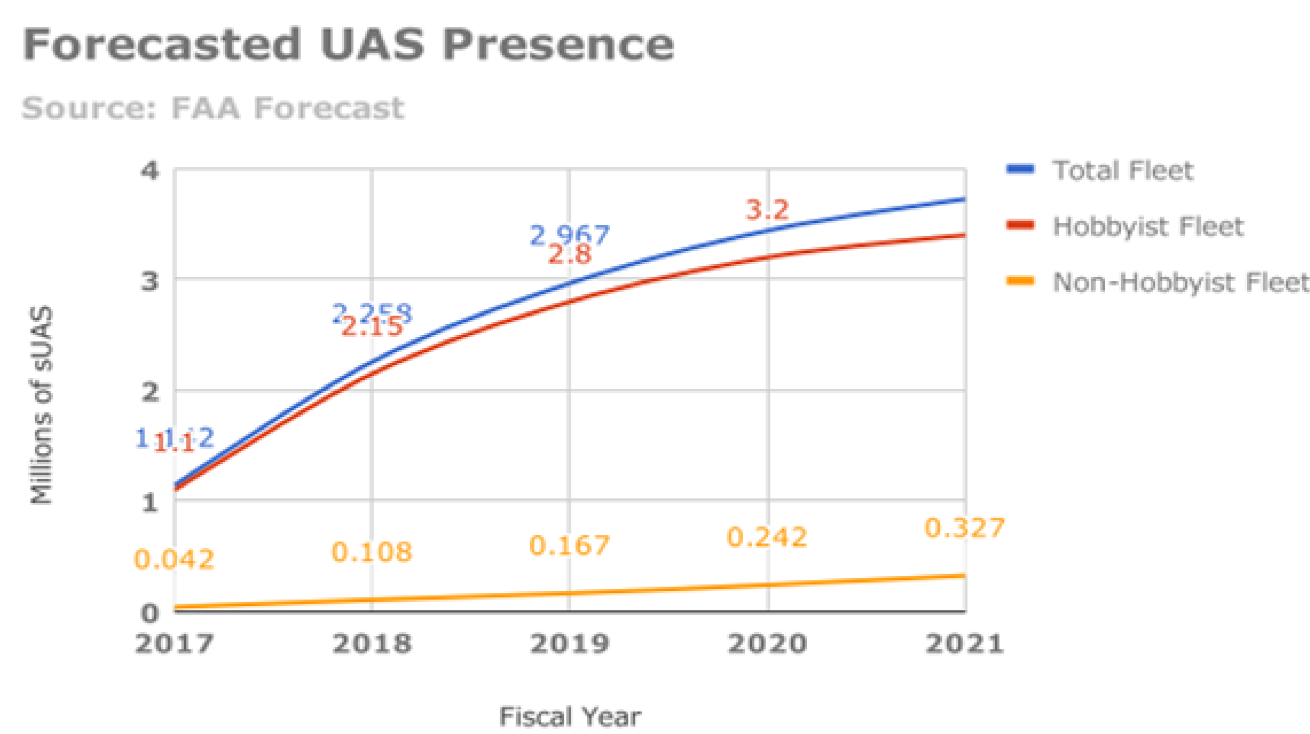

Figure 1 - FAA Forecasted sUAS presence in the National Airspace System (millions of aircraft).

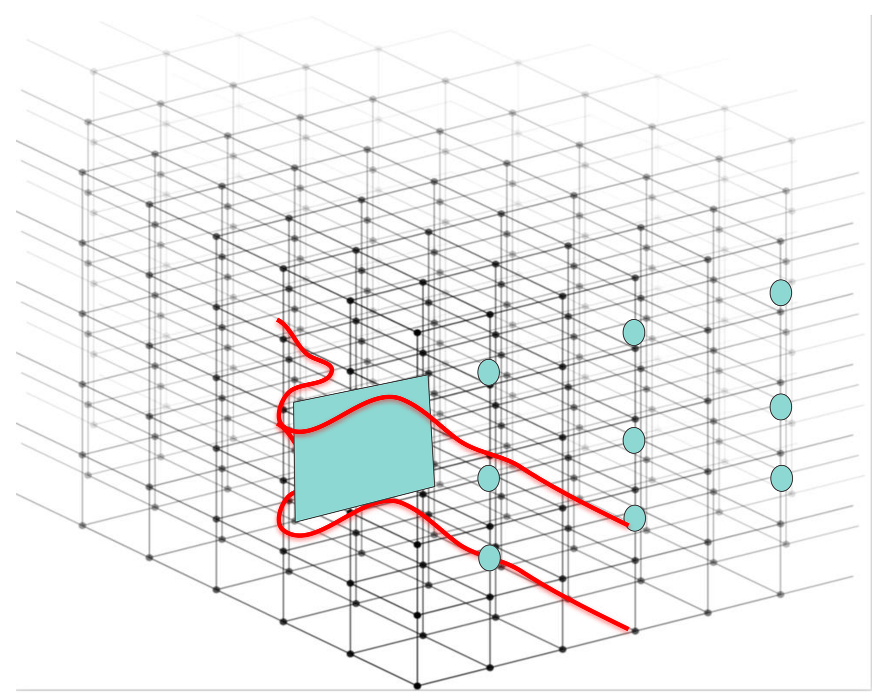

Figure 2 - Visual representation of a flight path around a traffic (Blue) and a desired path (Red).

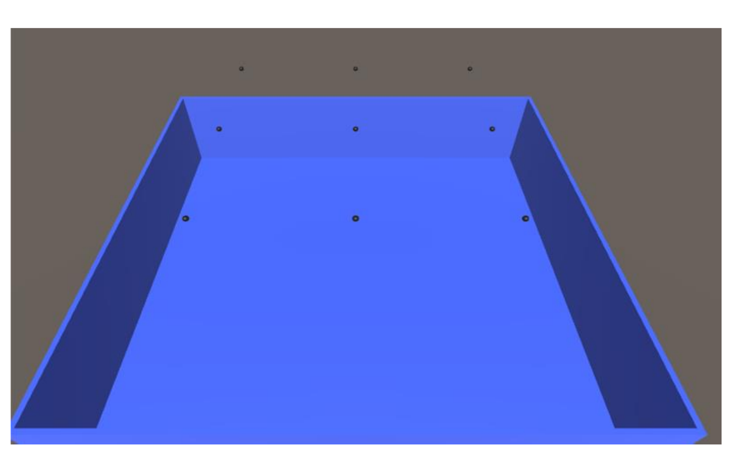

Figure 3 - Top-Down view of simple test environment involving 9 UAVs (Black dots).

Networking

The goal of this group is to understand the peer-to-peer communications protocols required for safe NAS integration. Exploratory efforts focus on networking solutions such as Mobile Ad-hoc Networks (MANETs), and blockchain methods for authentication. Successful completion will commence with understanding of performance characteristics and vulnerabilities tradeoffs (**Figure 4**).

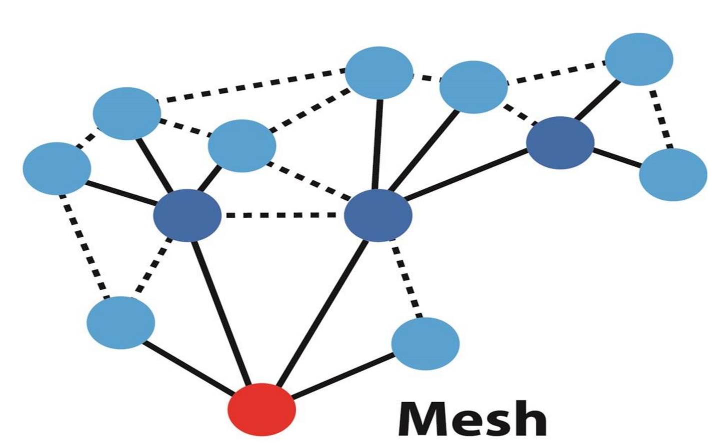

Figure 4 - Partial Mesh Topology.

Power Distribution Board

The goal of this group is to build a Power Distribution Board (PDB) that distributes power to the motors, companion computer, and auxiliary components in extreme temperatures. This task will be considered complete with the flight of our quad-rotor aircraft while powering a companion computer and two auxiliary items simultaneously from a single power source (**Figure 5**).

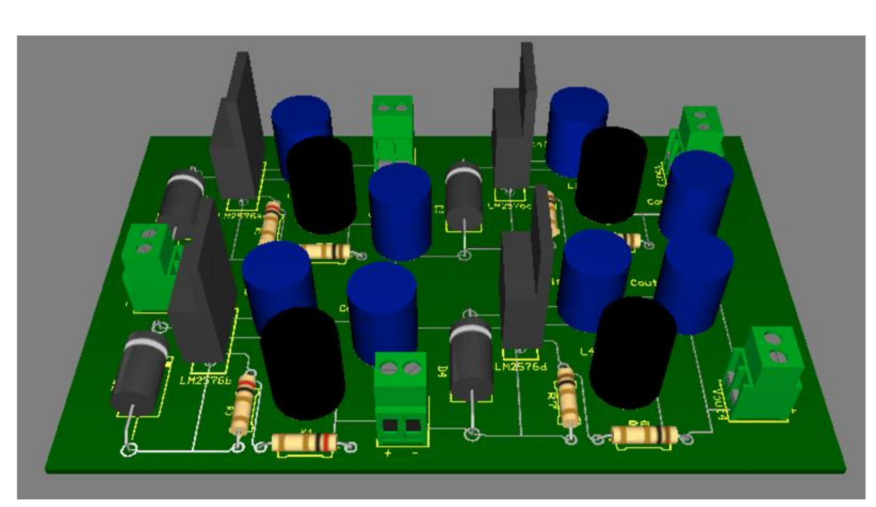

Figure 5 - PDB Prototype

Simulation & Hardware Validation

The goal of the simulation group is to develop a technology stack for validating algorithms and network protocols in a virtual environment. Challenges include integration of Gazebo, ROS, Flask, PX4, and LeafJS to support simulation of dense traffic environments. Successful completion will commence with a working simulation environment (**Figures 5, 6**).

```xml
<!-- UAV(n)-->
<group ns="uav(n)">
    <!-- MAVROS and vehicle configs -->
    <arg name="ID" value="(n)"/>
    <arg name="fcu_url" default="udp://:14540@localhost:14557"/>
    <!-- PX4 SITL and vehicle spawn -->
    <include file="$(find px4)/launch/single_vehicle_spawn.launch">
        <arg name="x" value="((n)+1)"/>
        <arg name="y" value="0"/>
        <arg name="z" value="0"/>
        <arg name="R" value="0"/>
        <arg name="P" value="0"/>
        <arg name="Y" value="0"/>
        <arg name="vehicle" value="$(arg vehicle)"/>
        <arg name="mavlink_udp_port" value="14561 + (n)"/>
        <arg name="ID" value="$(arg ID)"/>
    </include>
    <!-- MAVROS -->
    <include file="$(find mavros)/launch/px4.launch">
        <arg name="fcu_url" value="$(arg fcu_url)"/>
        <arg name="gcs_url" value=""/>
        <arg name="tgt_system" value="$(arg ID)"/>
        <arg name="tgt_component" value="1"/>
    </include>
</group>
```

Figure 5 - XML file describing a MAVROS Node

Figure 6 - Launching of a series of MAVROS Nodes with Gazebo

The goal of the hardware group is to maintain the aircraft and companion computer in an airworthy condition and to follow up successful simulated tests with hardware-in-the-loop tests.

Cyber Security Operations

The purpose of this group is securing the peer-to-peer network the UAVs communicate on. To accomplish this, existing encryption libraries are used and users are notified of abnormal cyber events. Claiming complete security is foolish, therefore completion standards are encryption of communications and the ability to log abnormal system and network events (**Figure 9**).

Computer Vision (HIL)

This working group leverages OpenCV and TensorFlow for implementing state-of-the-art object detection algorithms. The challenge is to identify UAVs with computer vision. Successful is defined as training a model that can differentiate between different UAVs (**Figures 7, 8**).

Figure 7 – UAVs in DECS Lab

Figure 8 - Example of an object detection bounding box

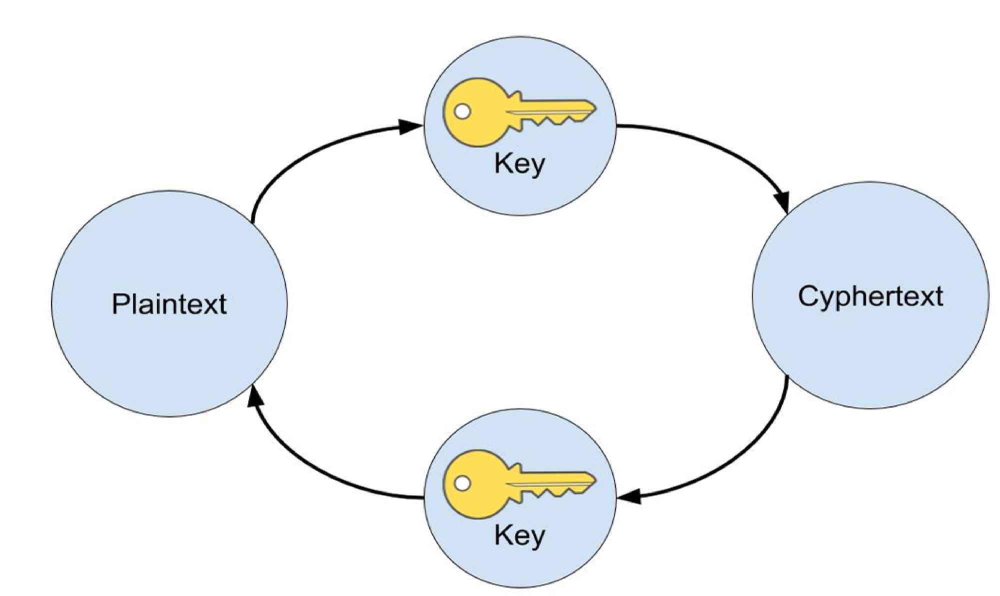

Figure 9 - Symmetric Encryption

ACKNOWLEDGMENT

The authors acknowledge Rockwell Collins Corporation, Cedar Rapids, Iowa for supporting this research work. The following students: Scott Crawford, Mohamed Horor, and Ryan Swartwout are credited for preliminary hardware development.