Experiments for Securing Air Traffic Against Cyber-Physical System Attacks

Gano Chatterji
Crown Consulting, Inc.
Moffett Field, California

NASA Interns: Miycoe Call, Phillip Chau, Brent Delano and Jesse Dai

AIAA Aviation Forum, 2-6 August 2021

Outline

- Motivation
- Background — What is Trust
- Trust creation approaches studied
  - Secure communication
  - Data integrity
  - Mission safety
- Summary and conclusions

Motivation

- The future Air Traffic Management (ATM) system needs to ensure availability, integrity, confidentiality and safety of operations

- Safety of vehicles and operations is paramount for successful integration of Urban Air Mobility (UAM), Unmanned Aerial Systems (UAS), supersonic aircraft and launch vehicles with conventional aviation operations in the National Airspace System

- Security is becoming critical because the sensors, networks and computers are far more vulnerable to bad actors than their mechanical or human predecessors

- The goal therefore is to design and develop cyber-resilient systems

What is Trust?

- Trust is the foundation of Cyber-Resilient Autonomy
- Trust is confidence that the system:
  - Blocks access to data or information without proper credentials — **confidentiality**
  - Protects data and itself from getting corrupted — **integrity**
  - Continues to operate and complete its mission even when attacked — **availability**
  - Continues to operate safely and protect crew and equipment in degraded conditions — **safety**

NASA Saw Apollo 13 as a Fiasco. 50 Years Later, Astronaut Jim Lovell Has Made Peace With the 'Successful Failure' by Jeffrey Kluger, April 10, 2020, https://time.com/5816937/apollo-13-50th-anniversary/

"Lovell was the successful commander of a triumphantly successful mission. That historical reckoning comes not despite the fact that his fragile, fickle spacecraft denied him the chance to set foot on the moon, but because of it."

Objective

Investigate methods for creating trust

- Communication is secure to prevent unauthorized access to data
- Data obtained via sensors and by processing are consistent
- Safeguards built-in to prevent mission failure

Approach

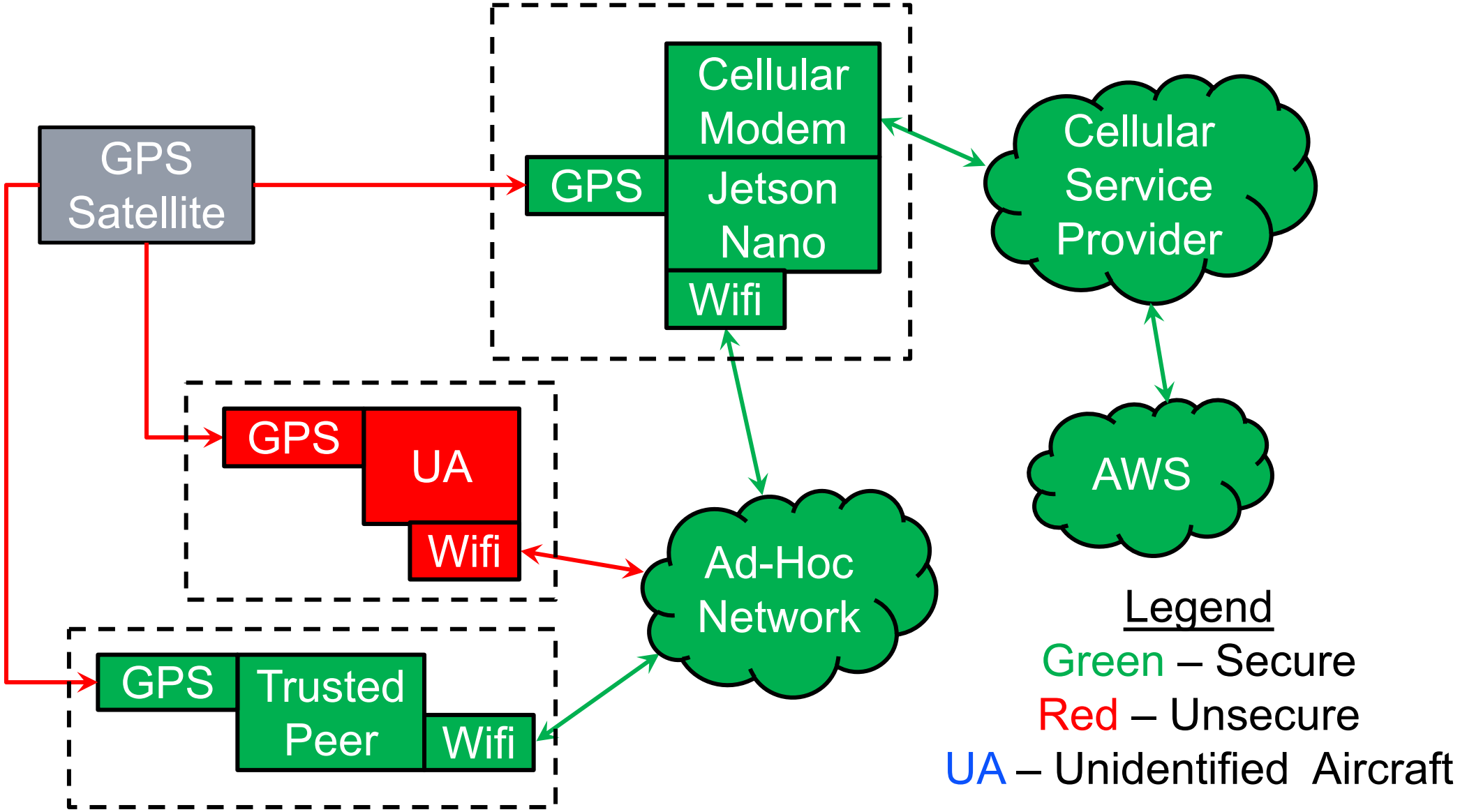
- Secure communication between mobile devices and cloud
  - Nvidia Jetson Nano Single Board Computers and Amazon Web Services (AWS)
- Data integrity
  - Integrated Positioning System
- Mission safety
  - Vision-based obstacle detection for emergency landing
  - Conflict detection and collaborative conflict resolution
  - Battery characterization

Experimental Hardware

Onboard Flight Computer

- Nvidia Jetson Nano
  - 128-core GPU
  - Quad core ARM CPU
  - 4K video 30 frames/second
  - 4GB memory
- GPS
- Inertial Measurement Unit
- Altimeter
- Camera
- 802.11 wireless transceiver
- Cellular transceiver

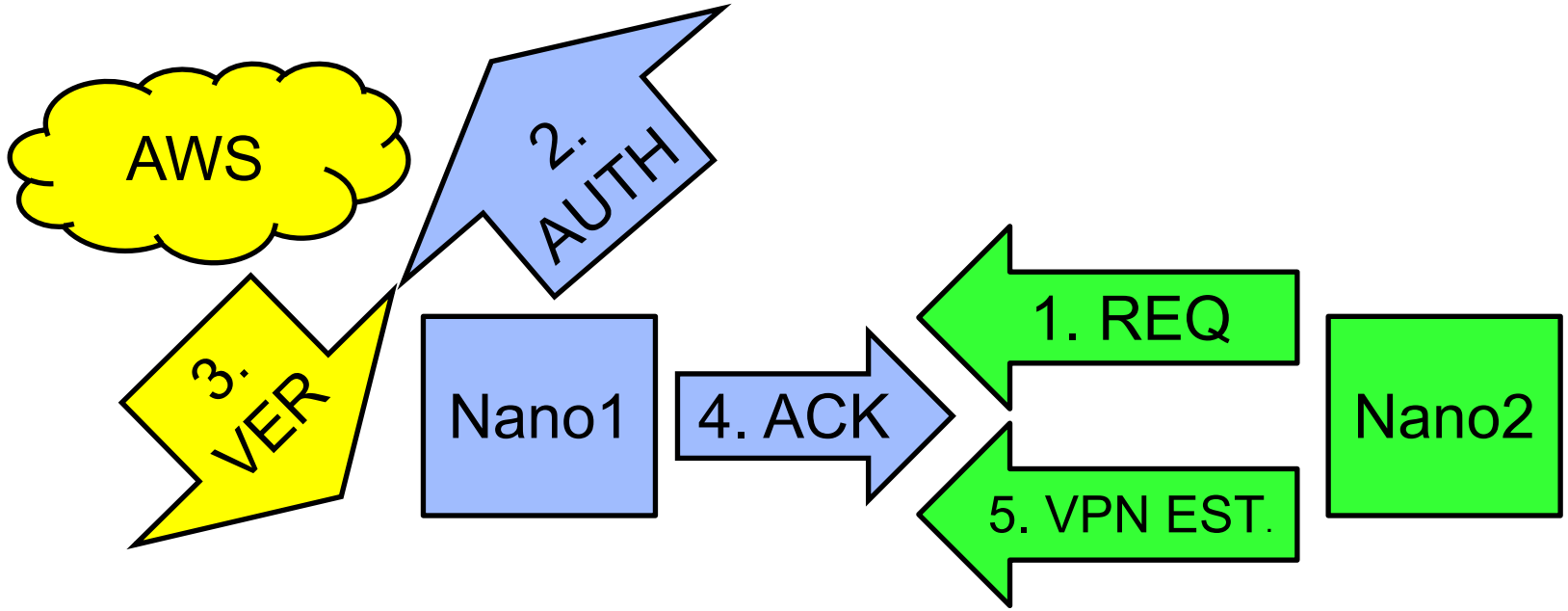
Secure Communication



Secure Communication Setup

Protocol:

1. Nano2 sends credentials and requests secure communication
2. Nano1 sends credentials to AWS to verify
3. Nano1 receives verification from AWS
4. Once verified, Nano1 sends Acknowledgement (ACK), and starts VPN server
5. Nano2 joins VPN as client



Nanos connected to Ad-Hoc network with WPA2-PSK encryption

Positioning Using Image Correlation

- Location reported by sensors should be verifiable with known landmarks
- Compares images acquired with a downward facing camera to Google Maps satellite images using cross-correlation
- Requires a lot of pre-processing and an inertial measurement unit and altimeter

Camera image simulated using portion of Google Maps image on the right

Actual Position

Estimated Position

Camera image is rotated, scaled, gray-scaled, and normalized to match the Google Maps Satellite Image

The Google Maps Satellite Image needs to be gray-scaled and normalized to match the drone image

Integrated Positioning System

GPS

Google Maps Satellite Images & Elevation Data

Camera

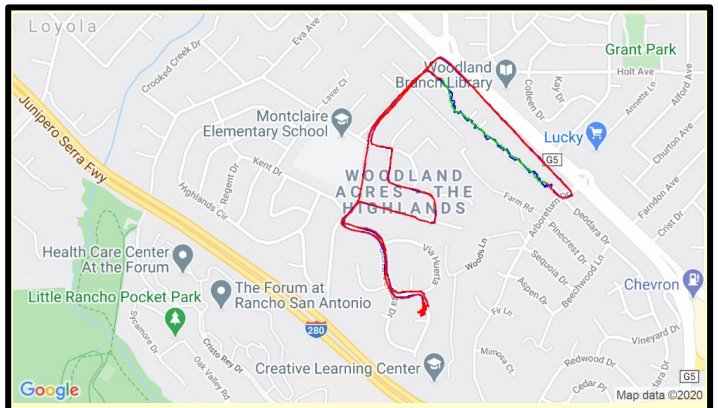
Altimeter

IMU

Image Processing & Cross-Correlation

Kalman Filter

Estimates



Actual GPS data & Simulated Images

Object Detection for Emergency Landing

- MobilenetV2 used for Object Detection
- Implemented pre-trained convolutional neural network on Jetson Nano for object detection, classification and segmentation
- Images recorded during road driving processed offline on Nano

Conflict Detection and Collaborative Resolution

- Conflict Detection & Resolution algorithm implemented on AWS
- Realtime position information sent to AWS from Nano in first car via cellular communication
- Second car simulated on AWS

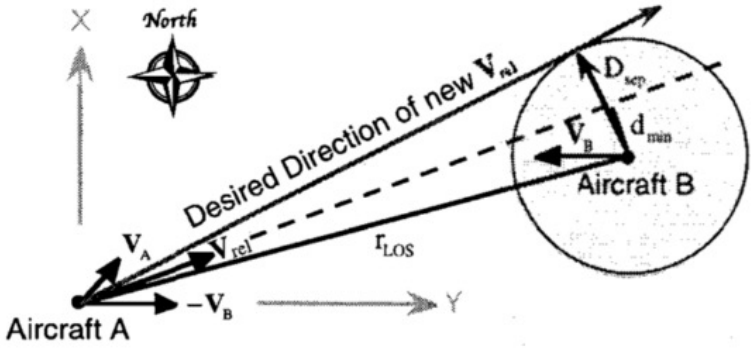
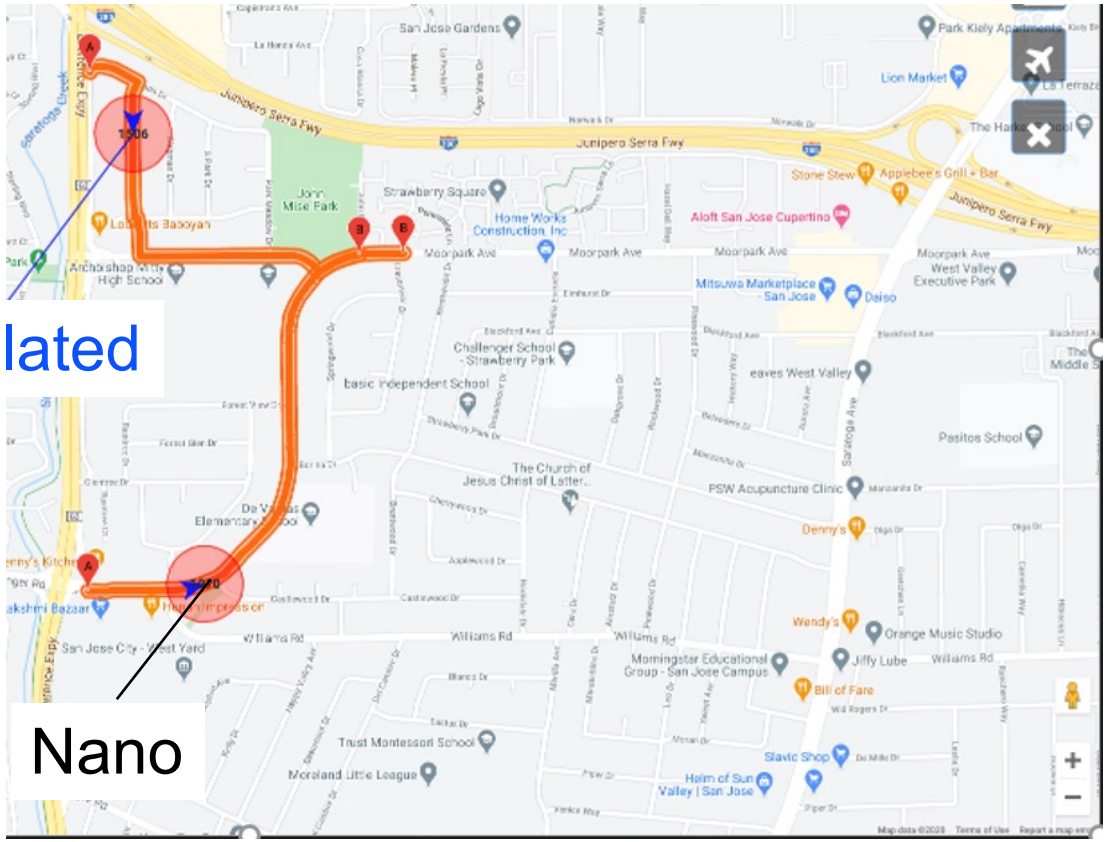


Fig. 2: Aircraft Positions and Velocities

Bilimoria, Karl, "Geometric Optimization Approach to Aircraft Conflict Resolution," AIAA GNC, 2000



Google Map data © 2020 within our App

Battery Characterization

- Energy consumption estimated using Nano reported power consumption is different from battery reading
- Created a model relating estimated to actual energy consumption
- Used model to predict battery remaining

$$t = \left(\frac{1}{P_{avg}}\right)\left\{C_B\left(1 - \frac{x_D}{100}\right) - E_C\right\}$$

$$x_D = \frac{-a_2 + \sqrt{{a_2}^2 - 4a_3[a_1 - x_B]}}{2a_3}$$

E_C – Estimate of Nano energy consumption

P_{avg} – Nano average power consumption

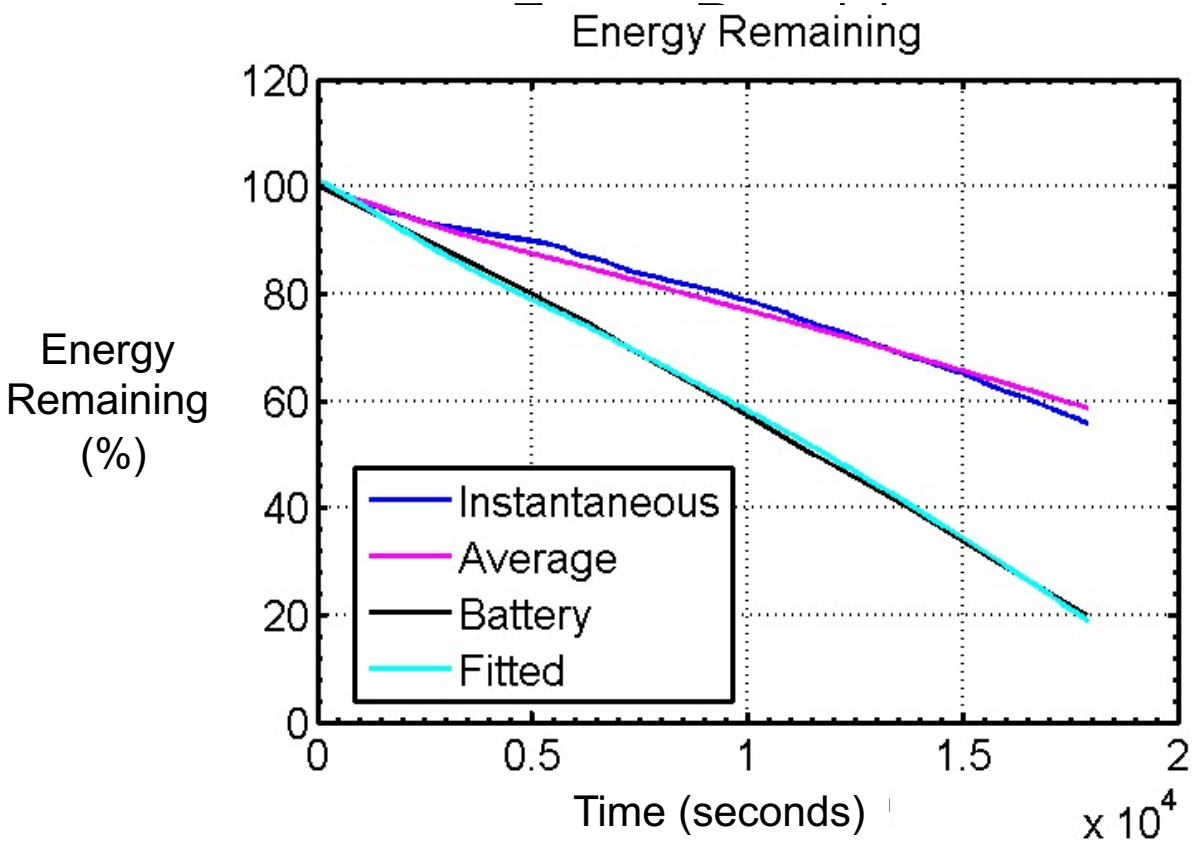
C_B – Battery capacity

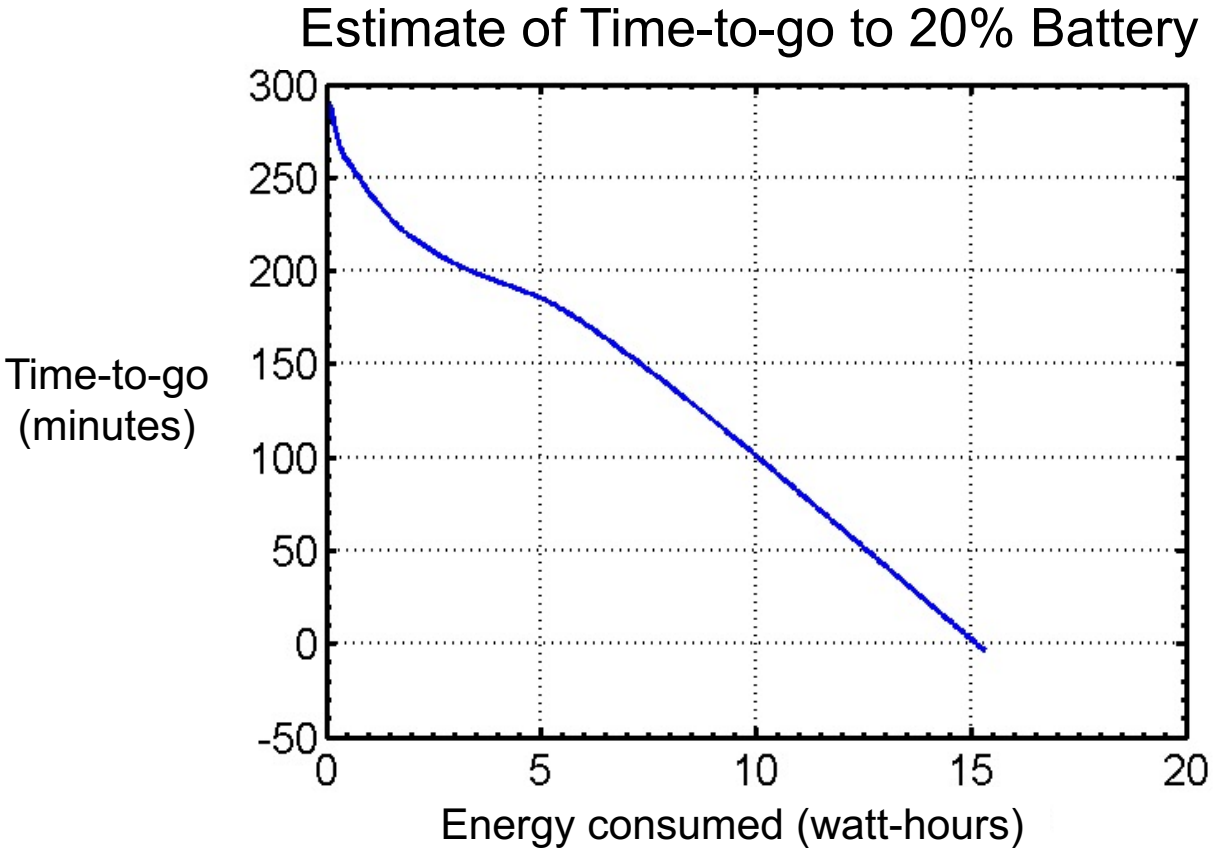
x_D – Nano energy remaining % based on fitted model

x_B – Desired battery % remaining

a_1, a_2, a_3 – Coefficients of the fitted model relating x_B to x_D

Battery Characterization Results





Summary and Conclusions

- We studied approaches for creating a trustworthy—cyber-resilient—UAM system
  - Secure communications between mobile devices and between mobile devices and the cloud
  - Data integrity using sensor fusion
  - Mission safety: obstacle avoidance, separation assurance and battery characteristics
- Learned off-the-shelf hardware can support development of cyber-resilient onboard flight computers
- Trust in system design and implementation can be accomplished by integrating layers in depth (detail) and in breadth (scope)
- Next Steps
  - Secure IEEE 802.11 wireless communication
  - Flight tests for data acquisition for evaluating algorithms
  - Hardening of algorithms