An Uncrewed Aerial Vehicle Attack Scenario and Trustworthy Repair Architecture

Kate Highnam*
Kevin Angstadt*
Kevin Leach*

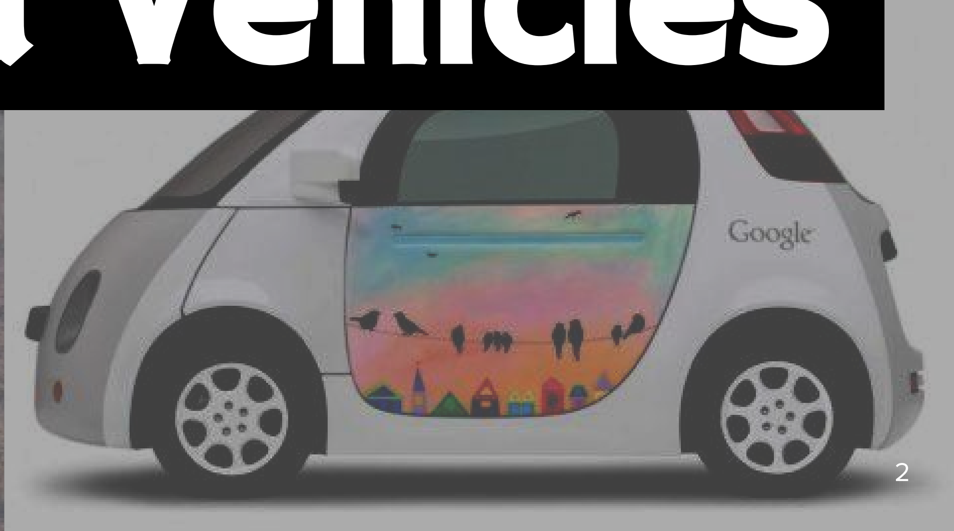
Westley Weimer*
Aaron Paulos[†]
Patrick Hurley[‡]

*Department of
Computer Science
University of Virginia
Charlottesville, VA
22904

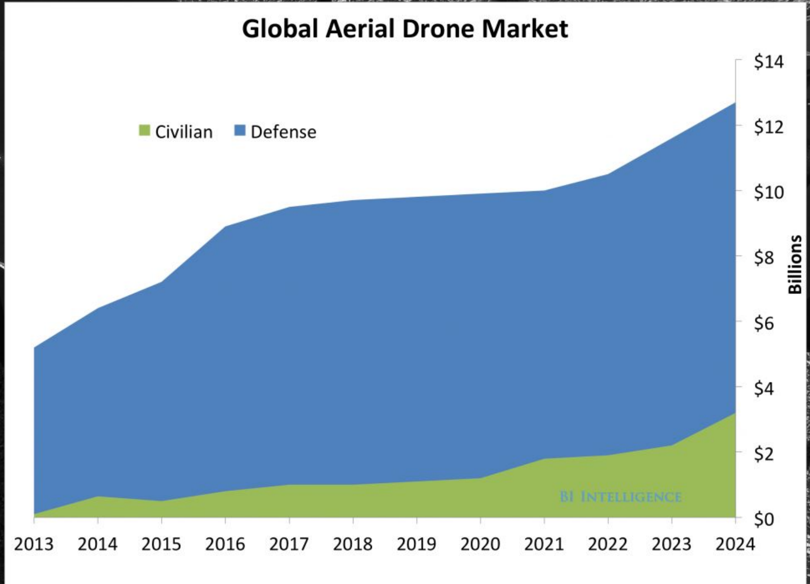
[†]BBN Raytheon
Cambridge, MA 02138

[‡]Air Force Research
Laboratory
Rome, NY 13441

Uncrewed Vehicles



UAV deployment is projected to increase substantially



Sources: Teal Group, BI Intelligence Estimates, Michael Toscano

These cyber-physical systems admit safety concerns in benign and malicious settings.

Warning . . . .

Systems must be resilient to malicious attacks and unforeseen environments

2014 Triathlete injured by drone
“someone hacked or ‘channel-hopped’ the drone, taking over the controls”

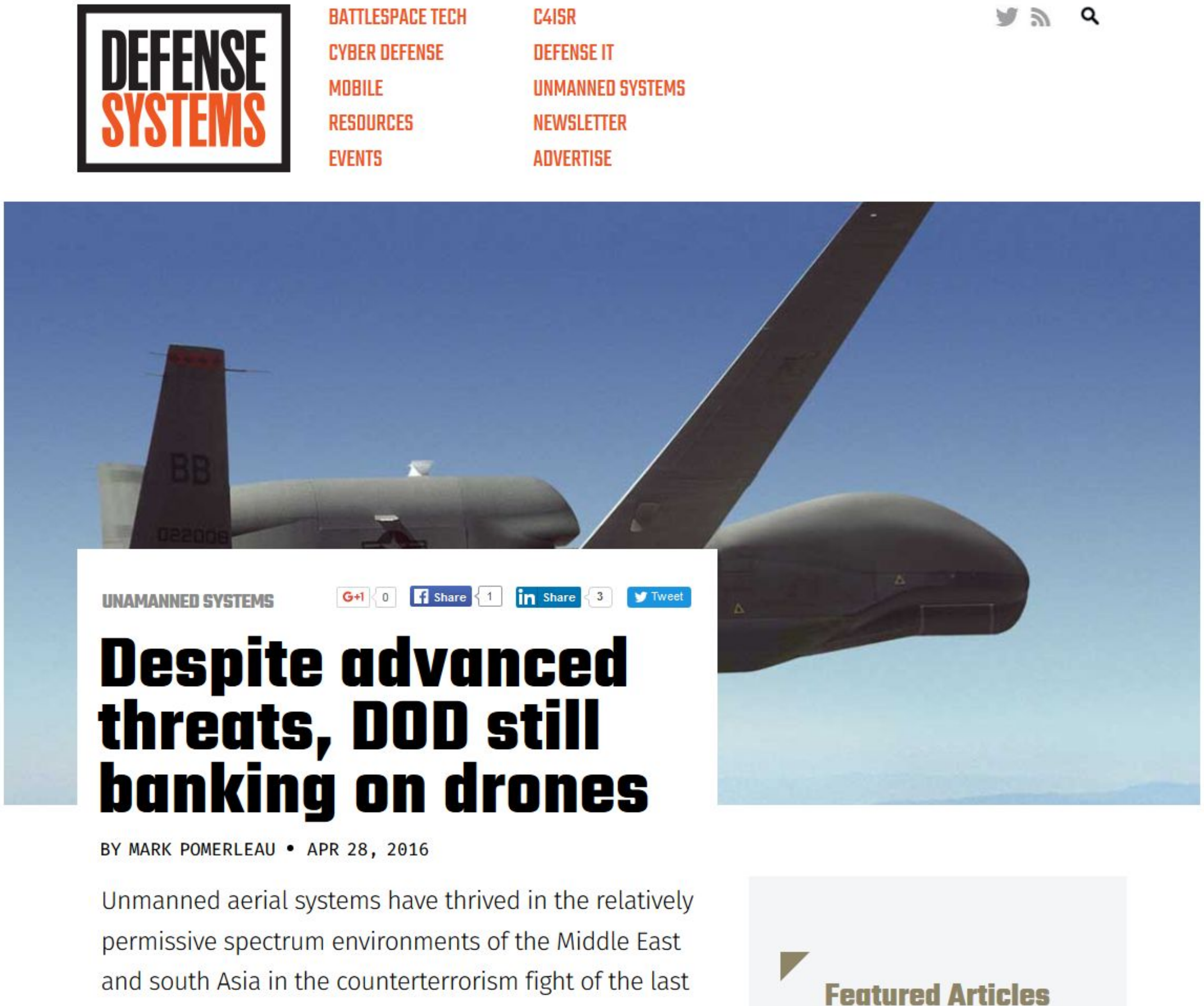
Enrique Iglesias’s fingers sliced by drone during concert (2015)
“Iglesias reached out to the flying device as it photographed the audience”

Injuries in the Lab

Resiliency is not always present...

Google Self-Driving Car pulled off the road for traffic violation

Predator drone crashes near U.S. Air Force base (2009)



Despite advanced threats, DOD still banking on drones

BY MARK POMERLEAU • APR 28, 2016

Unmanned aerial systems have thrived in the relatively permissive spectrum environments of the Middle East and south Asia in the counterterrorism fight of the last

How can we evaluate **trust** and **resiliency** within research of UAVs?

Proposed UAV Attack Scenario Case Study

(for the evaluation of future research)

Indicative mission

Commodity systems

Commodity communication

Stealthy attack

Attack detection

For This Presentation

Dependability

A measure of how consistently the UAV platform successfully completes its assigned mission.

Trustworthy

A UAV is trustworthy if the human operators believe it to be dependable.

Ex: DARPA High-Assurance Cyber Military Systems (HACMS)

Resilient System

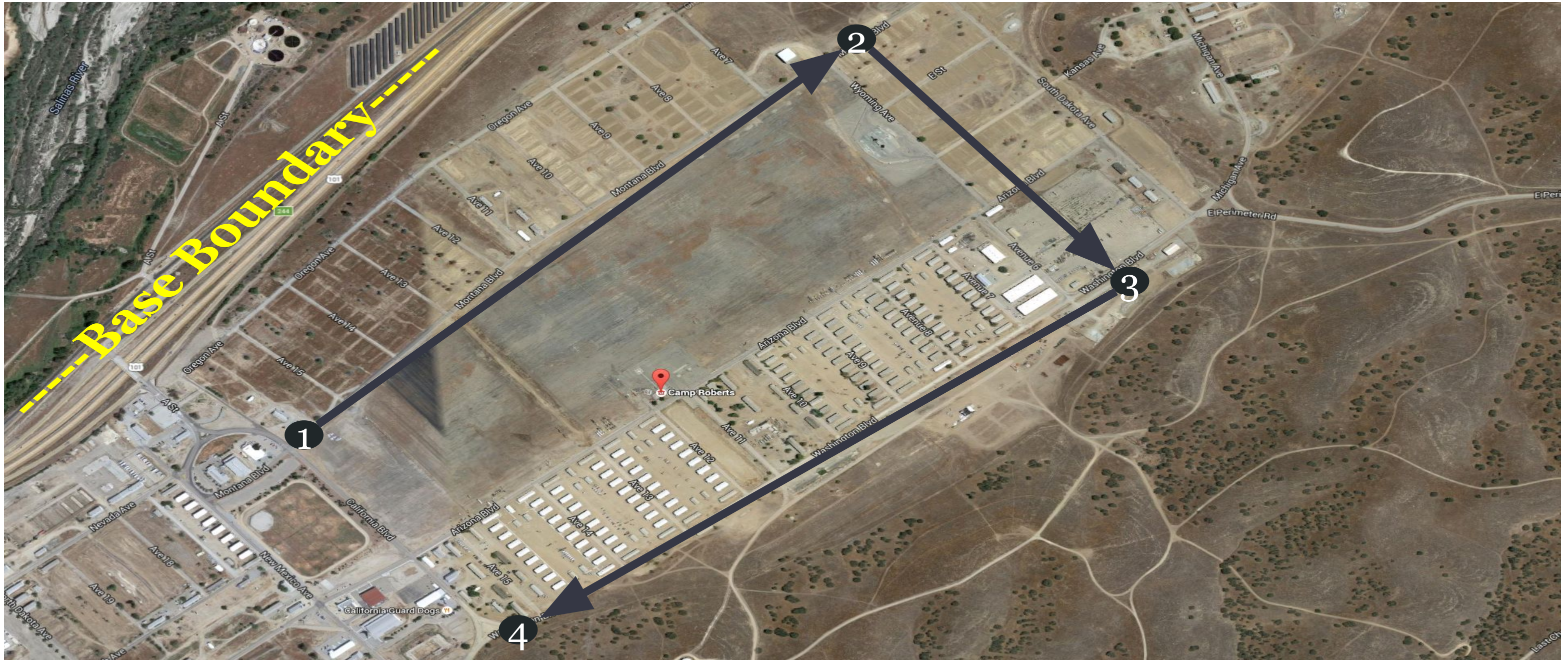
Capable of recovering from or avoiding human, platform or environmental factors that adversely affect the mission.

Ex: Automated Program Repair, Fault Tolerance Techniques

Our Proposed UAV Attack Scenario

Indicative Mission

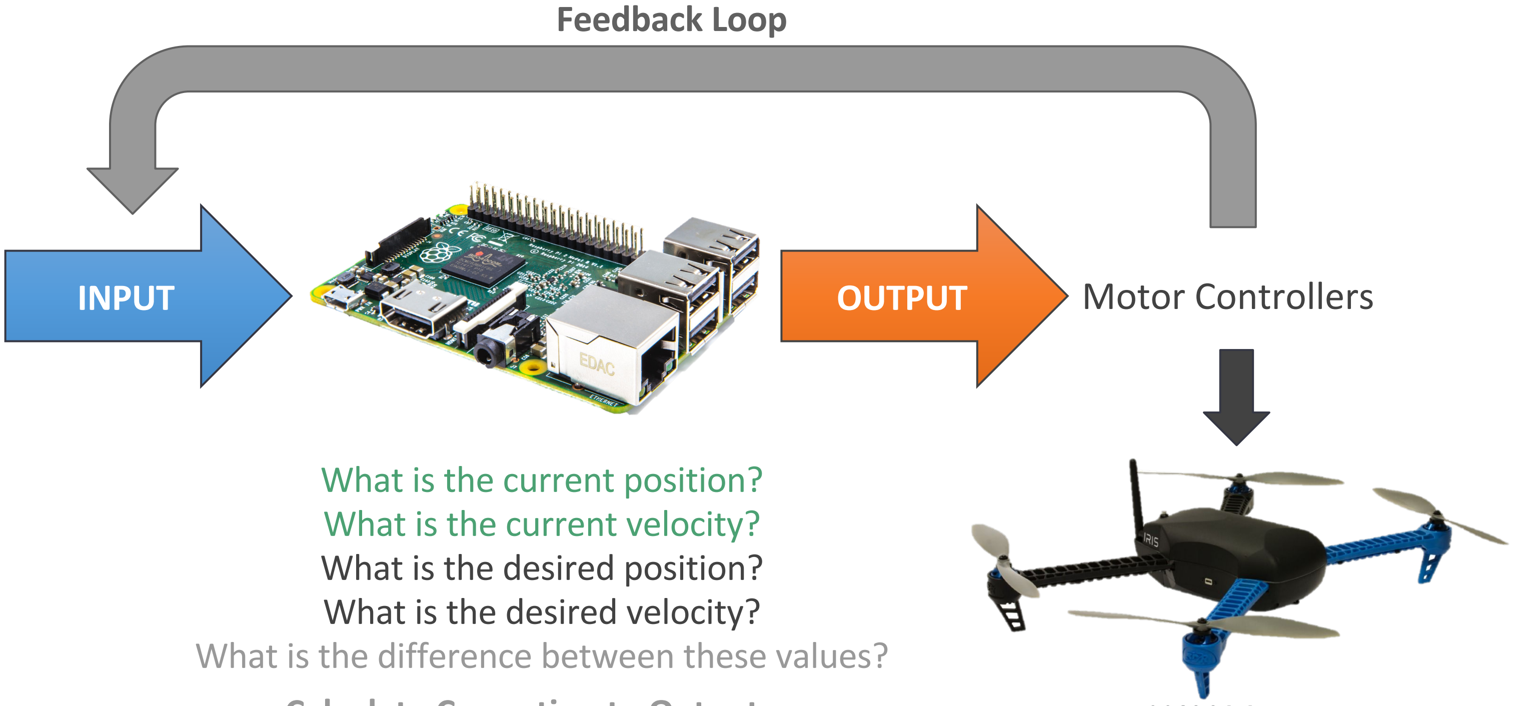
UAV with camera: surveil 4 waypoints in sequence



Commodity Systems

- **Common UAV**
  - Ex: 3DR Iris+ Pixhawk, Erle-Copter, Raspberry Pi kit copters, etc.
- **Runs a Unix-like Real-Time Operating System**
  - Ex: RT-Linux or NuttX
- **Which supports autopilot software**
  - Ex: ArduPilot (C++)

How does a UAV fly?



Feedback Loop

GPS Data
Accelerometer
Compass
Altimeter
RC Input
Motor Speed

INPUT

OUTPUT

Motor Controllers

What is the current position?
What is the current velocity?
What is the desired position?
What is the desired velocity?
What is the difference between these values?

Calculate Correction to Output

UAV Moves

Commodity Communication

Flight Plans

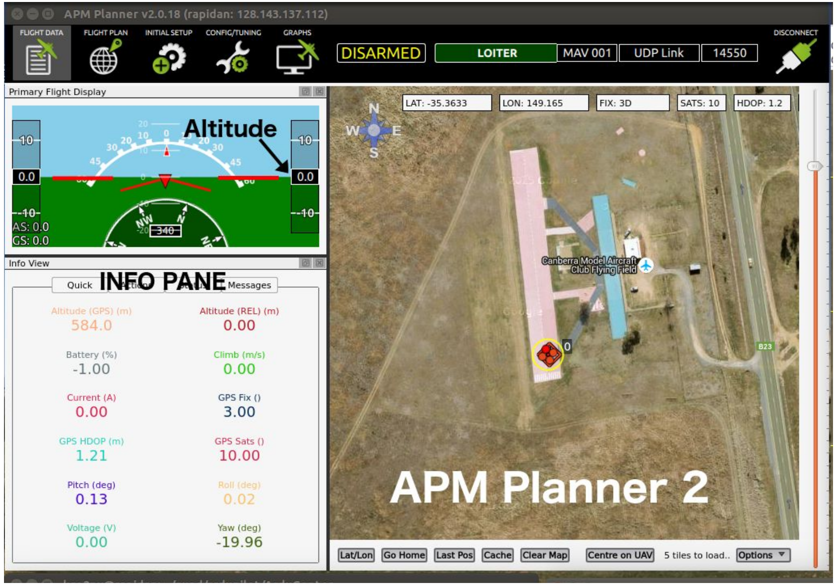
Position (and other) Information

Ground Control Station

(Ex: APMPlanner, QGroundControl)

Computer + Telemetry Radio

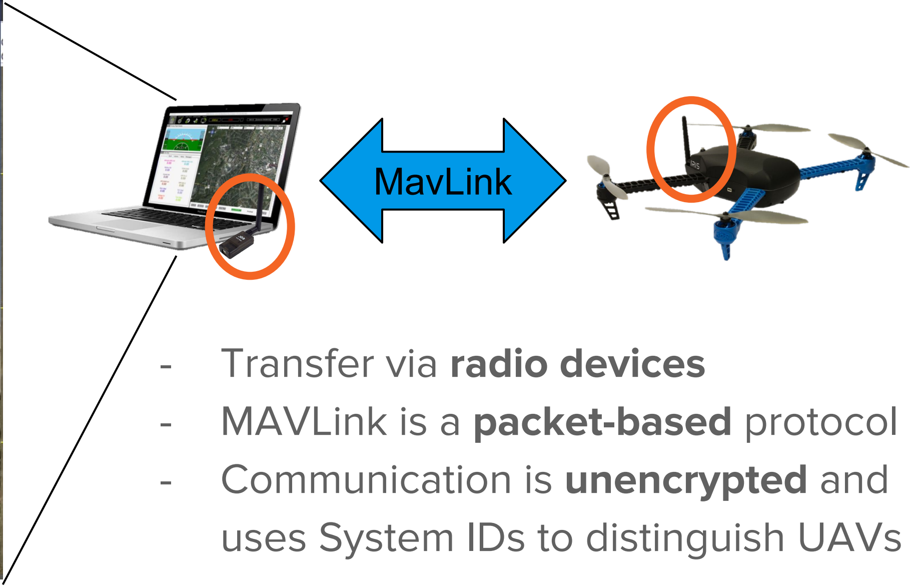
MavLink Package Connection



APM Planner v2.0.18 (rapidan: 128.143.137.112)

LAT: -35.3633 | LON: 149.165 | FIX: 3D | SATS: 10 | HDOP: 1.2

Altitude (GPS) (m) 584.0 | Altitude (REL) (m) 0.00
Battery (%) -1.00 | Climb (m/s) 0.00
Current (A) 0.00 | GPS Fix () 3.00
GPS HDOP (m) 1.21 | GPS Sats () 10.00
Pitch (deg) 0.13 | Roll (deg) 0.02
Voltage (V) 0.00 | Yaw (deg) -19.96



- Transfer via **radio devices**
- MAVLink is a **packet-based** protocol
- Communication is **unencrypted** and uses System IDs to distinguish UAVs

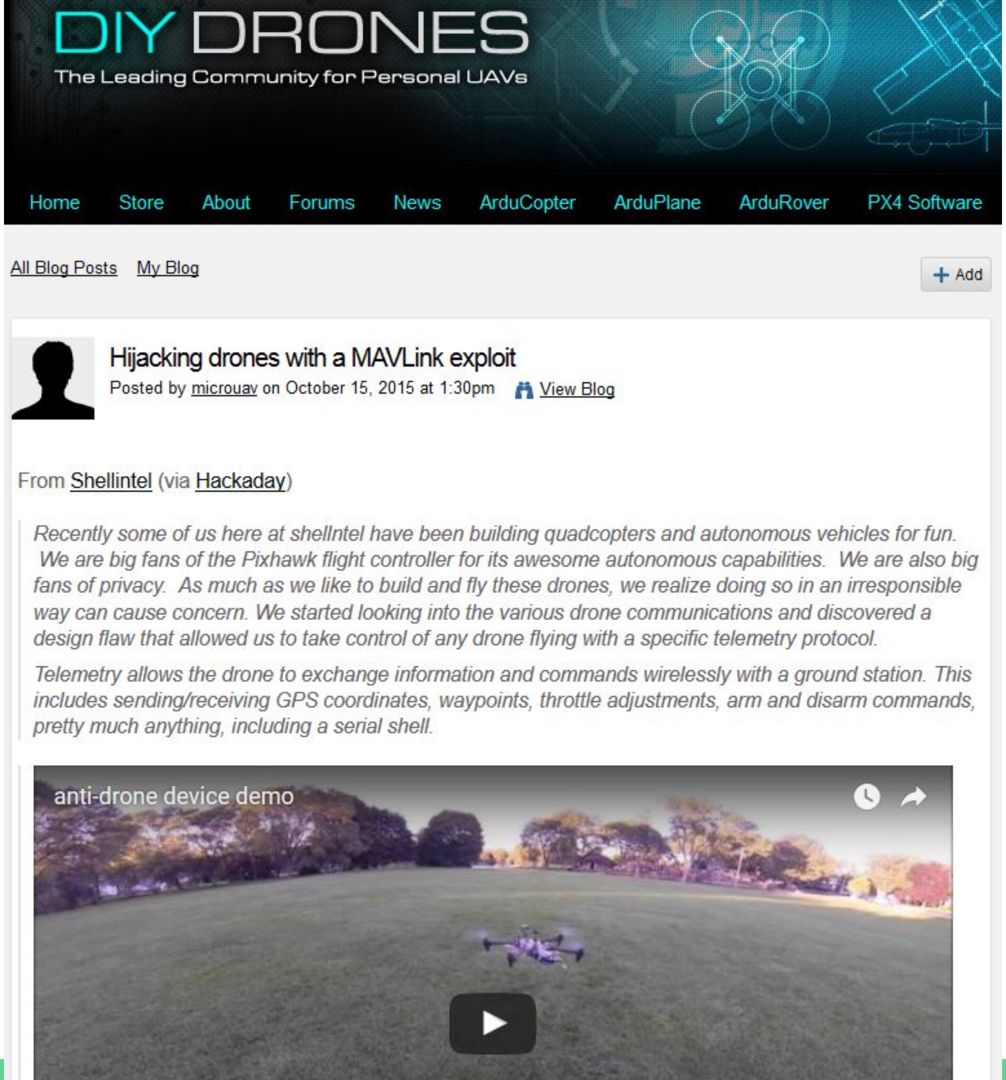
Stealthy Attack

Capture System ID and Spoof MAVLink packets (to Disrupt Surveillance)

Demonstrated by hobbyists with $25 of commodity hardware

<u>Our Scenario:</u>

Attacker does ***not*** wish to be detected (i.e., does not immediately crash UAV)



Hijacking drones with a MAVLink exploit

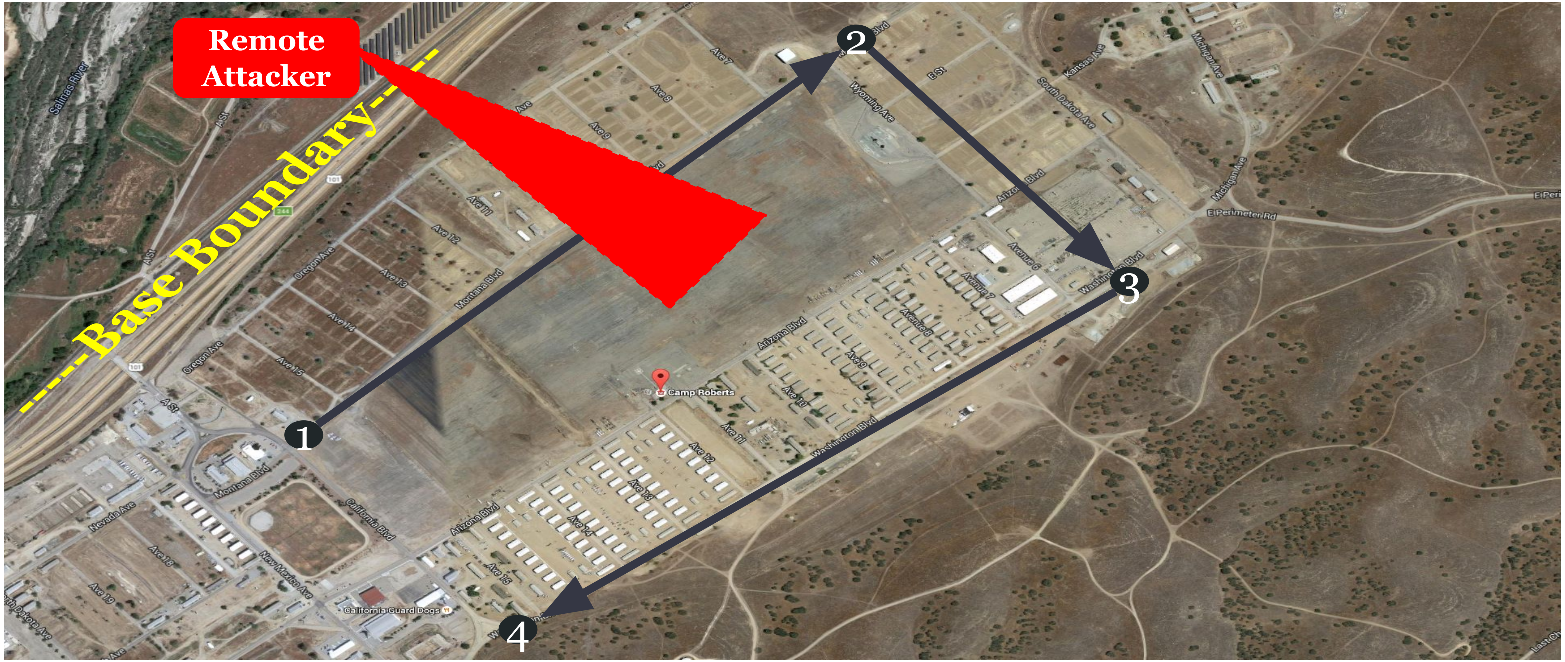
Posted by microuav on October 15, 2015 at 1:30pm

From Shellintel (via Hackaday)

> *Recently some of us here at shellntel have been building quadcopters and autonomous vehicles for fun. We are big fans of the Pixhawk flight controller for its awesome autonomous capabilities. We are also big fans of privacy. As much as we like to build and fly these drones, we realize doing so in an irresponsible way can cause concern. We started looking into the various drone communications and discovered a design flaw that allowed us to take control of any drone flying with a specific telemetry protocol.*
>
> *Telemetry allows the drone to exchange information and commands wirelessly with a ground station. This includes sending/receiving GPS coordinates, waypoints, throttle adjustments, arm and disarm commands, pretty much anything, including a serial shell.*

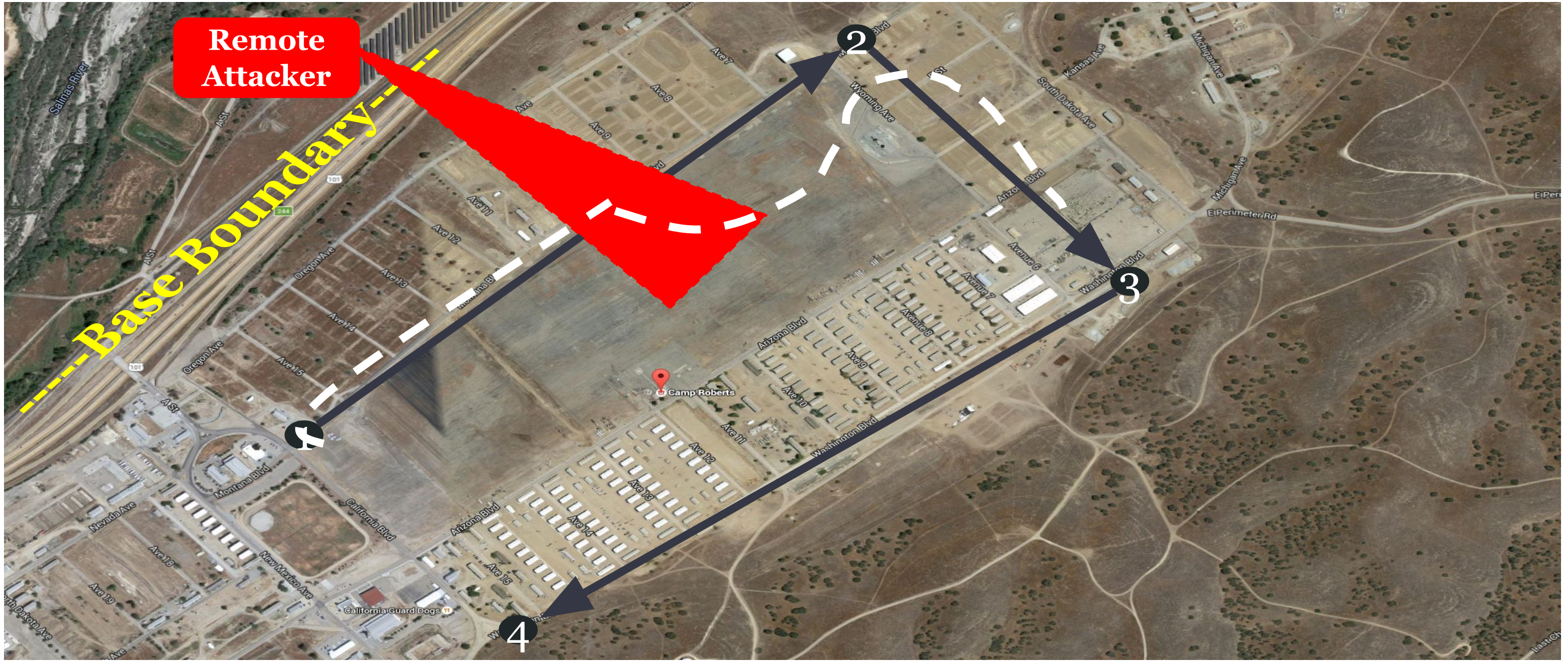
Stealthy Attack

Capture System ID and Spoof MAVLink packets: degrade surveillance of #2 (change camera facing slightly, SET_POSITION_TARGET_GLOBAL_INT, etc.)



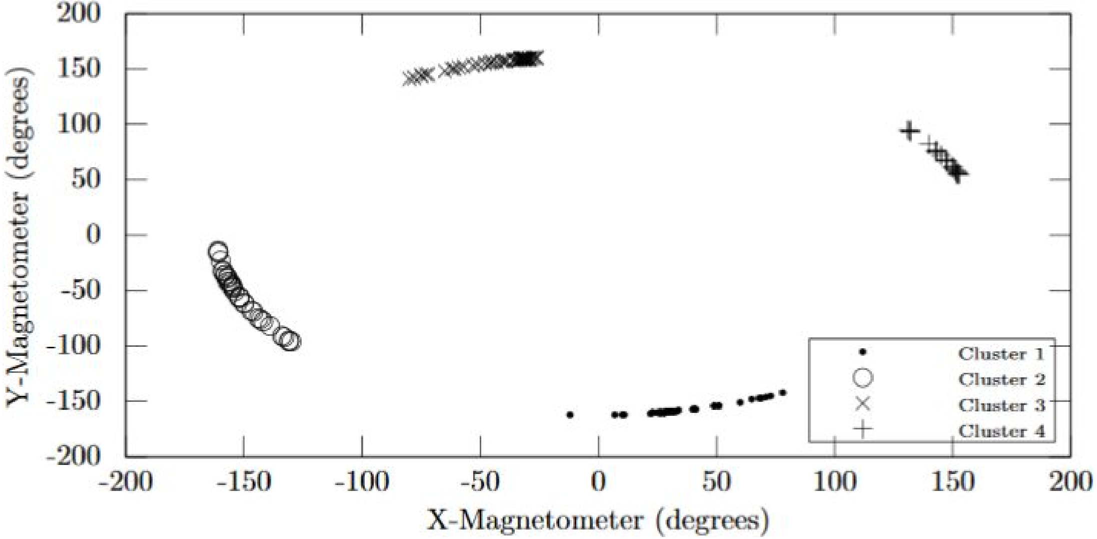
Stealthy Attack

Capture System ID and Spoof MAVLink packets: degrade surveillance of #2 (change camera facing slightly, SET_POSITION_TARGET_GLOBAL_INT, etc.)



Attack Detection

- UAVs broadcast a wide range of telemetry information (MAVLink)
- Such attacks can be detected by **anomaly detection** against training information collected from previous successful missions
- The four clusters shown correspond to the four legs of the mission



Materials Available

Reproduction tutorials &
Real-world measurements

Summary

- UAV deployment continues to **increase**
- Researchers need scenarios to *evaluate* and *motivate* techniques that explore the space of **trustworthy and resilient systems** (no “SPEC” for UAVs … yet)
- Our proposed benchmark attack scenario
  - Indicative Mission
  - Commodity Systems
  - Commodity Communication
  - Stealthy Attack
  - Attack Detection
- We attest that it is indicative of commercial and defense deployments!
- Materials available at http://genprog.cs.virginia.edu/start/

Attack Scenario Outline

- **Indicative Mission**
  - Intelligence, Surveillance and Reconnaissance (ISR)
  - Patrol and surveil four waypoints
- **Commodity Systems**
  - Unix-like Real-Time Operating System (RTOS)
  - Ground Control Station
- **Commodity Communication**
  - Micro Autonomous Vehicle Link (MAVLink)
- **Stealthy Attack**
  - Capture System ID and Spoof MAVLink packets
- **Attack Detection**
  - Telemetry Information

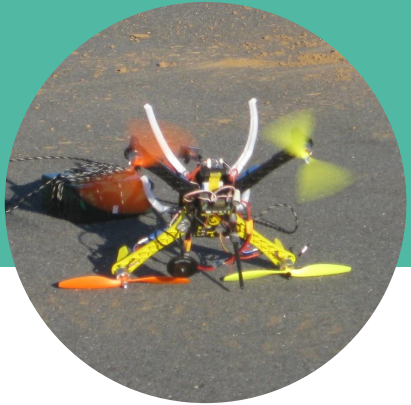
Commodity Systems

- **UAV runs a Unix-like Real-Time Operating System**
  - RT-Linux or NuttX
- **Which supports autopilot software**
  - ArduPilot (C++)
  - Very abstractly, given sensor input (GPS localization, magnetometer, etc.) and a goal location, solve differential equations (physics) to drive actuators (rotors)
- **Captures common commercial systems**
  - 3DR Iris+ Pixhawk, Erle-Copter, Raspberry Pi kit copters, etc.

Commodity Communication

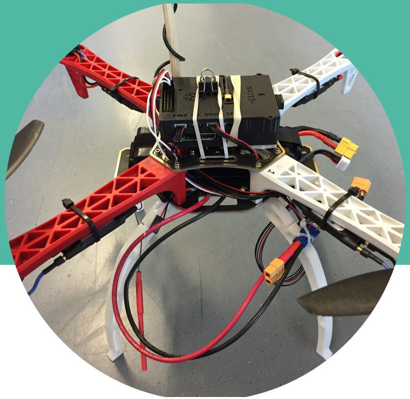
- **Ground Station Software**
  - Supports mission planning, setting waypoints, etc.
  - APMPlanner, QGroundControl, etc.
- **Uses Micro Autonomous Vehicle Link (MAVLink) Protocol**
  - Communicates motion commands, arm/disarm, telemetry information, etc.
  - Physical and link layer via radio devices
  - MAVLink is a packet-based protocol
  - Communication is unencrypted and uses System IDs to distinguish UAVs
- (Why no encryption? Requires additional processing and battery on the UAV, additional cost on the ground controller, is not present in near-future systems, and does not defeat all attacks.)

Common Hardware



Erle Brain Quadcopter

Iris+ PixHawk Quadcopter



Raspberry Pi Quadcopter