Believe It or Not: Wireless Walking on Air Drones and Wireless Security

Wade Trappe

September 2018

UAVs

UAVs change the wireless landscape and will have dramatic security implications

- UAVs will come in a variety of sizes and shapes, with a wide range of cyber-capabilities
  - Tasks: environmental monitoring, item delivery, recreation, etc.
  - Use wireless for control
  - Have the potential to cause physical harm
- UAVs change the "wireless game"
  - Require strict guarantees in communication performance
  - Have an elevated perspective that has pros/cons
  - Easy access by hobbyists
  - Advanced "tactical" UAVs have quite different security considerations (talk to me offline!)

- Drones are already commodity technology:
  - DJI Phantom, 3DR, etc… easily accessible and affordable
  - Software kits available for app development (e.g. 3DR's DroneKit API, DJI SDK)

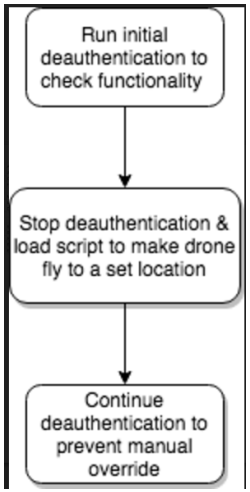
A Case Study illustrates the potential risks associated with UAV: Football Stadium

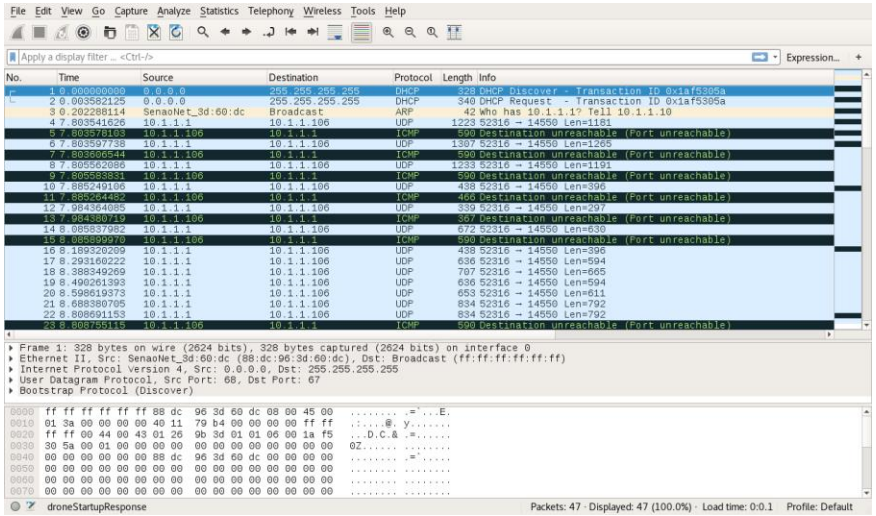
- A recent Rutgers investigation into the use of recreational drones near football arenas:
  - Hobbyists try to fly drones over games to watch the event
    - *Safety: A crash can harm life and infrastructure*
    - *Revenue implications*
  - Sensors deployed around a stadium, with new commercial software used to detect drones
- Lessons learned:
  - Most drone vendors use commodity wireless tech (e.g. Wifi), and most detection uses "wireless" to find the controller.
  - Controller detection was usually successful within 30seconds, location within 150m about 80% of time.
  - Detection performance is dependent upon deployment "geometries"
  - Having an up-to-date drone "RF" signature database (MAC addresses, etc)
- Pre-planned missions or many drones: Not easy to detect→ need for other forms of drone detection

- Legal limitations:
  - The law limits what can be done "to counteract" drones
  - Can't disarm or disable drones, even if they would cause physical harm
  - FAA limitations are ignored by hobbyists
  - Concerns that anti-drone defense systems (jammers) might impact other societal systems (navigation)
  - Need to re-evaluate these limits

It is relatively easy to pwn a drone… sort of.

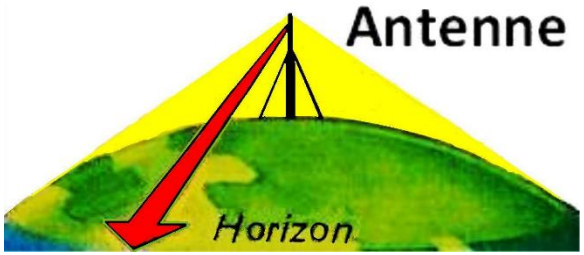
- In a separate study, Rutgers investigated the susceptibility of commercial drones to simple, cyber attacks
- Goals:
  - Analyze drone communications
  - Understand attack vectors to control/disable drone
- Attack scenario:
  - Laptop running Kali Linux
  - Wireshark - packet capturer
  - Aircrack-ng - wireless exploit suite
  - 3DR Solo Drone
  - Sololink - controller/drone wifi network
- We were able to:
  - Capture and replay packets (sent to the drone)
  - Deauthenticate the drone
  - Redirect the drone with the DroneKit API
- Good news: Deauth on the drone did not lead to a crash… drone hovers but does not have a controlled descent.



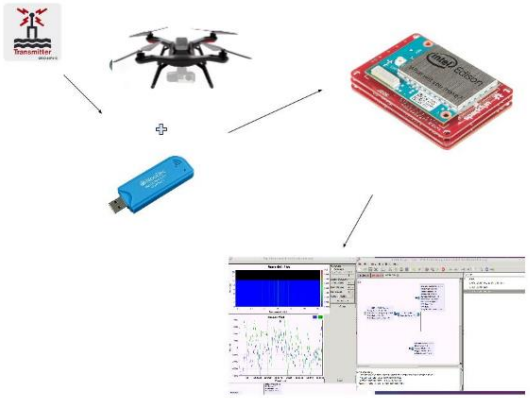


Elevated implications on spectrum: a double-edged sword

- UAVs are an elevated platform
  - Able to receive RF signals from "further away"
  - Able to transmit RF and impact receivers "further away"
- Simple line of sight arguments imply a larger RF footprint/ radio horizon for a drone
  - Larger L1 interference footprint
  - Larger L2 (MAC-layer) impact– think carrier sensing
  - Larger L3 impact (everything is the drone's neighbor)
- The good:
  - UAVs as mobile, emergency cellular basestations
  - UAVs as repeater (bridge between two non-line-of-sight RX)
  - Enhanced spectrum sensing (needs more research on signal separation, spectrum cartography!)
- The bad:
  - But what about a rogue, software-based LTE basestation (e.g. OpenAir LTE)?
  - Jammers…



Picture from Wikipedia



WINLAB spectrum sensing on a drone

- GPS + RF SDR dongle
- Problems with weight, GPS stability

"Any opinions, findings, conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Networking and Information Technology Research and Development Program."

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov