Security Vulnerabilities of Drones and Countermeasures : An Experimental Study

Drone Applications

Book-Delivery

Health-care

Agricultural

Surveillance

Experimentally Validated Drone Vulnerabilities

DJI Phantom-4 pro Drone

- Cracking DJI SDK
- Reverse Engineering Firmware
- GPS Spoofing

Parrot-2 Bebop Drone

- Open Wi-Fi
- Open Telnet with root access to file system
- De-authentication attack
- Open FTP port
- Replaying captured telemetry packets
- DoS attack

Attack Surfaces and Techniques

DRONE SECURITY
A hijacker can exploit security weakness in radip transmission used to pilot a drone. Sending false signals or jamming legitimate ones can divert the drone's flight path and send it crashing into the ground. Security researchers have demostrated potential scenarios for foul play, shown here in the diagram.

GPS Signal

A handheld electronic controller can forge signals from GPS satellites that identify an aircraft. Spoofing can overpower these transmissions and cause a frone to veer off course or come dangerously close to other aircraft.

Noise transmission can block GPS navigation and other critical signals for piloting a drone. The craft can be programmed to return to a home base if a control signal is jammed, but no satisfactory solution exisis if both GPS and a control signal are obstructed.

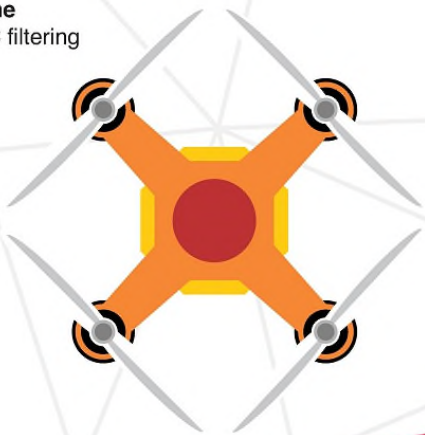
Control Signals

Countermeasures

DJI Phantom-4 pro Drone
- Using encryption/packer to protect library files
- Using obfuscator to prevent de-compilation

GPS anti-spoofing
- Checking GPS sub-frame data
- Checking latency(motion speed)

Parrot-2 Bebop Drone
- Hidden SSID, MAC filtering



Vikramkumar Pudi and Anupam Chattopadhyay
School of Computer Science and Engineering
pudi@ntu.edu.sg, anupam@ntu.edu.sg