Drones Security and Privacy: Attacks to Sensors

CPS and IoT Security

Alessandro Brighente

Master Degree in Cybersecurity

Unmanned Aerial Vehicles

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- Unmanned Aerial Vehicles (UAVs) are flying devices without any crew or pilot on board

- They come in different shapes and size, and can reach different altitudes

Fixed-wing rotor   Quadcopter   Tricopter

Operating Mode

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- UAVs may be operated by pilots located on the ground

- Remotely Piloted Aircraft Systems (RPAS)

- Formally, "a set of configurable elements consisting of a remotely piloted aircraft, its control station, the command and control links and any other system elements required during flight operation"
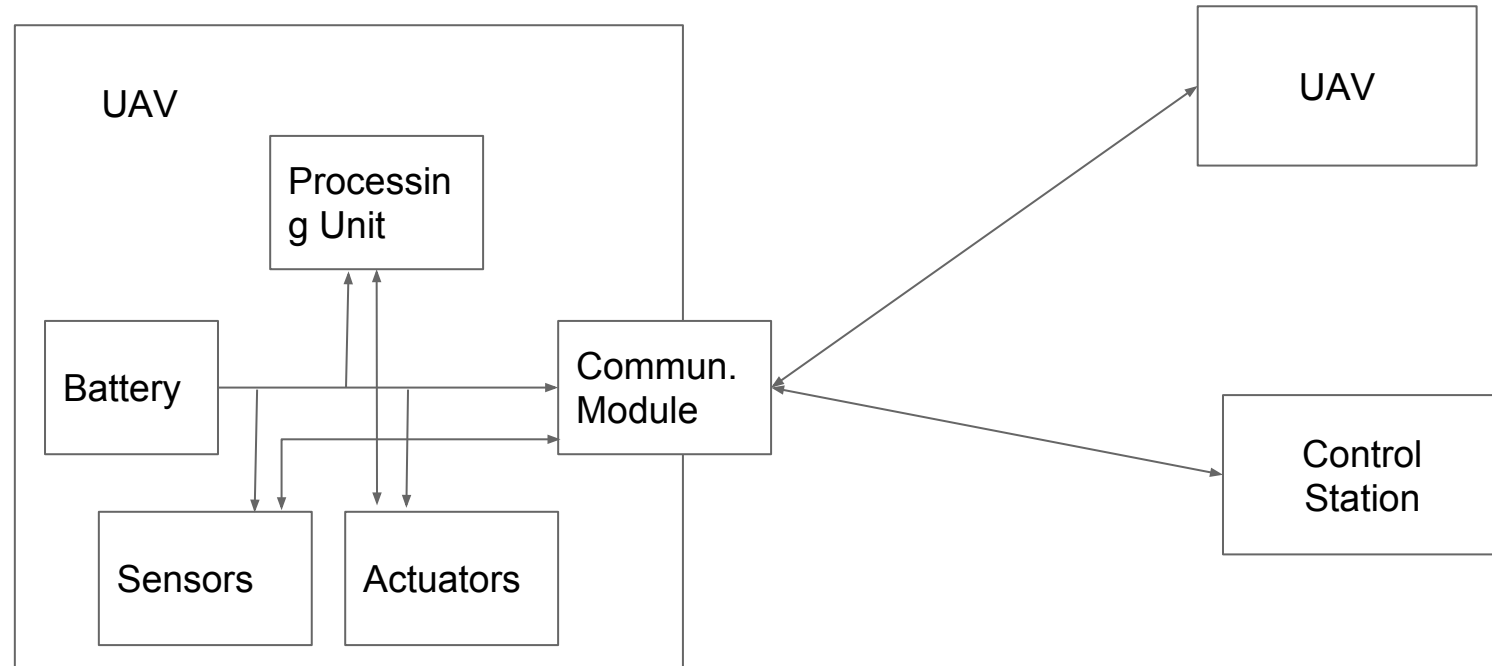
Control

Data reporting
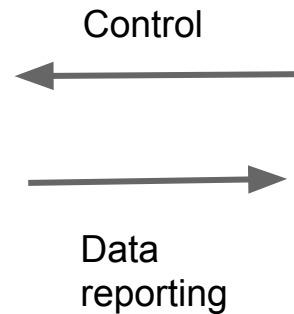
- UAVs may be autonomous and coordinate with other drones to deliver a common objective

- Fleet of UAVs

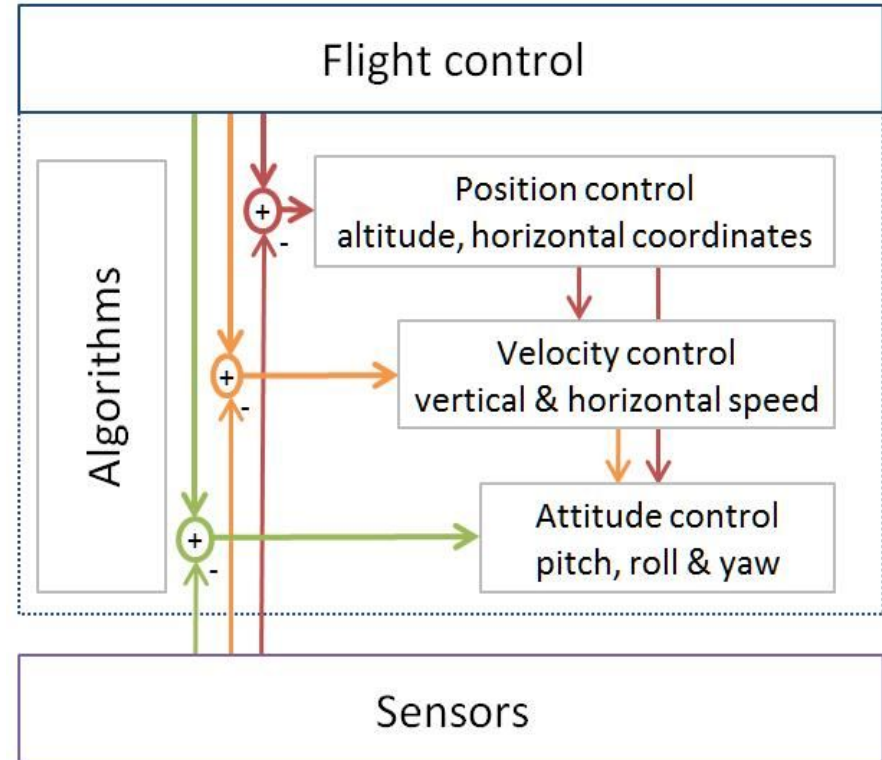- Need to communicate with other fleets to avoid crashes

Structure of a Drone

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- Multiple modules to acquire and process data

- Communication module as enabler

Operating Principle

- UAVs employ control loops

  possibly with sensor feedback

By Maxorazon - Own work, CC BY-SA 4.0,
https://commons.wikimedia.org/w/index.php?curid=46770558

Applications

- UAVs have been firstly proposed for military applications

- Seventeen countries armed UAVs, and more than 100 countries use UAVs in military capacity

- Civil applications are instead more recent

- Thanks to their high adaptability, UAVs find applications in many different fields

  - Infrastructure
  - Transport
  - Media and Entertainment
  - Telecommunication
  - Agriculture
  - Search and Rescue

- A drone ecosystem is composed by six unique targets:

1. Drone hardware: CPU, sensors, firmware

2. Drone chassis and package: all non-electronic devices

3. Ground control station: may be fixed or mobile

4. First-Person View (FPV) channel: control channel via common communication protocols

5. Pilot: person remotely controlling the drone

6. Cloud services: some drone send telemetry of flight information to a cloud server if needed

- Attacker aim: disrupt the legitimate task of flying a drone

- Attackers may be both civilian or military

- Although military may have sophisticated equipments (e.g., cannons or predator birds), a civilian may still be able to impact on the drone

- We consider a civilian that has access to equipments that can be purchased at a moderate cost

  - Software-Defined Radio

  - Computer

  - Commercial lasers

  - Butterfly net

  - Magnets

- An attacker may be of three types:
  - With direct physical access → access the drone or the GCS to modify the firmware or replace hardware parts
  - Physically proximate → send, modify, and replay radio transmissions in order to hijack a drone
  - Distant adversary → resides on the Internet and applies attacks against servers, drones, the GCS

- The impact of the attack can be measured according to the CIA triad
  - Confidentiality: attack that reveals information about drone, pilot, telemetry or collected data
  - Integrity: attack that modifies the information delivered to or collected by the drone, GCS, cloud server or pilot
  - Availability: attack that causes the pilot to lose control of the drone due to forced landing, crash or hijacking

Drone Hardware Attacks

- Find vulnerabilities in the devices or software used by the drone
- Attack to the compass
  - Use a magnetic field to fool the compass and either hijack or prevent take off

- Attack on the stabilizing algorithm via camera sensor
  - Drones use a camera to collect images and stabilize the flight
  - To detect movements, UAVs use optical flow
  - Features can be modified by projecting laser beams on the ground, or projecting images on the ground
  - The drone will follow the projected features

Optical Flow

- Optical flow is the pattern of apparent motion of objects, surfaces, and edges (basically, everything from which we can extract simple features) in a visual scene caused by the relative motion between an observer and the scene

- Optical flow uses a sequence of successive images to allow for the estimation of motion

- It tries to calculate the motion between two image frames which are taken at a predefined rate at every voxel position

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- UAVs use a downward facing optical flow camera

- They collect images and use the estimation to stabilize the flight

- It can detect whether the drone is drifting by comparing successive frames of the ground below

- The sensor system will attempt to infer if the ground plane image has moved by a relative offset $(\Delta x, \Delta y)$

- If so, the system assume that the ground is stationary and the drone has drifted

- Optical flow first requires a feature detection algorithm to identify regions of the ground plane easy to track

- These features are then provided as input to the optical flow algorithm

- It then identifies the location of these features in successive images and uses the difference to compute the displacement

- Classic configuration: use the Shi-Tomasi corner detection algorithm for feature detection and the Lucas-Kanade method to compute the optical flow

- Optical flow first requires a feature detection algorithm to identify regions of the ground plane easy to track

- These features are then provided as input to the optical flow algorithm

- It then identifies the location of these features in successive images and uses the difference to compute the displacement

- Classic configuration: use the Shi-Tomasi corner detection algorithm for feature detection and the Lucas-Kanade method to compute the optical flow

- Basic idea: use the derivative of the image to detect whether the is a sudden change of color in one direction

- If only in direction, then an edge is detected

- If in two direction, then a corner is detected

- It is generally used because efficient, compared to more sophisticated but slower feature detectors (SURF, SIFT)

Lucas-Kanade Optical Flow

- Assumes that the difference between two consecutive frames is small and approximately constant within some neighbourhood

- This assumption is arranged for UAVs considering a combination of sufficiently high frarate and sufficiently low resolution

- For each corner pixel p returned by the feature detector, let us define a local window of n neighbourhood pixels q_i for $i \in \{1, \ldots, n\}$

- For each i let $I_x(q_i)V_x + I_y(q_i)V_y = -I_t(q_i)$, where I denote the image matrix, pedix denotes partial derivative, and V the velocity or motion along a coordinate → estimate V via Least Squares

- A successful attack to sensors needs three requirements

- <u>Environment influence</u>: the adversary can alter the physical phenomenon that the system measures

- <u>Plausible input</u>: create an input to the sensor that will actually be used by the system as valid input

- <u>Meaningful response</u>: the attacker can induce a behavior on the UAV representing the control the attacker has over it

- The adversary must be able to alter or obscure the ground plane to alter the pixel values reported by the optical flow camera

- Onerous example: cover part of the area with feature-rich pattern

- More concrete example: project features on the ground via laser/light beams

- In the first case, the attacker can use a battery operated projector loading images e.g., from a USB stick

- In the second case, use an array of laser elements to create features

Plausible Input to Optical Flow

- The basic idea of optical flow is to instruct the UAV to compensate a drift by moving of the same amount in the opposite direction

- The system assumes the image on the ground to be stationary, so it interprets feature motion along a vector as a movement in the opposite direction

- By moving the ground feature, the attacker can control the movement of the drone

Meaningful Response to Optical Flow

- The attacker's goal is to project a sharp gradient onto the ground so that the feature detection algorithm will pick up the light as a corner

- Since the Lucas-Kanade-based optical flow computes a final displacement based on the average displacement of each feature, the attacker needs to generate a large number of corners

- In practice, the attacker can simply sweep their projected light across the ground plane

- Most UAVs are enabled with the Return to Home (RTH) functionality

- The UAV records its location of departure, and in case of emergency it will automatically fly back to home

- Emergency includes low battery or loss of the control signal for more than 3 seconds

From DJI's RTH guide

- Most UAVs rely on the Global Navigation Satellite System (GNSS) for positioning (e.g., Europe's Galileo)

- However, this system has the main issue of not being authenticated

- We can hence spoof the GNSS signal and control the location of the drone

- However, the drone is controlled by its pilot

Capturing Drones

Position Information

Control signal

Spoofed Position Information
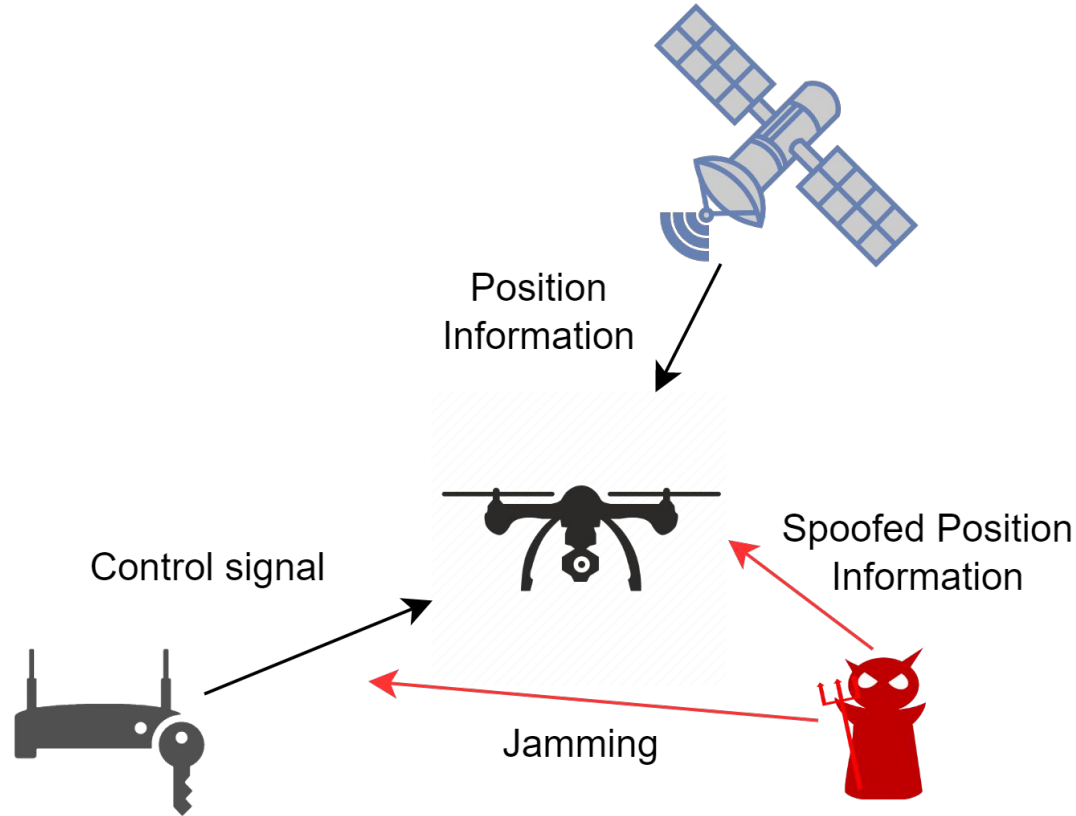
Jamming

- When jamming the signal for enough time, the drone enters the RTH mode and starts to fly back to the home location

- With the help of the GPS module and the on-board compass, it can derive a trajectory based on its current location S and the home location H

- The attacker aims at sending spoofed location information to capture the drone in the minimum time by bringing it to a controlled location D

- To achieve the shortest capturing time, the attacker may want the UAV to fly along the straight line SD

- However, the drone has a pre-recorded H and will try to return there

- If only one could spoof an arbitrary location to the UAV, then the UAV will change its direction immediately to any desired angle

- For instance, given a location S' such that S'H || SD, then the UAV will fly to D along SD

- However, GPS accepts only physics-reasonable coordinates

Greedy Algorithm for UAV Capture

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- Constraint: the maximum location change speed of GPS spoofing is Vs

- Idea: to minimize the capture time, the UAV trajectory shall be spoofed such that it points towards D as soon as possible

GPS Spoofing Algorithms for Capturing UAVs (x, y axis unit: meter)
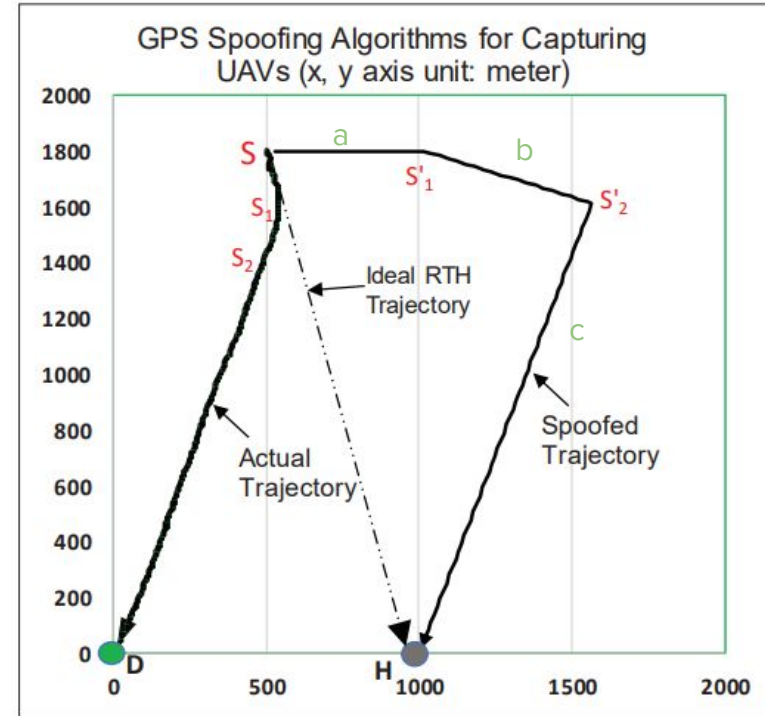
- Loiter mode: the UAV tries to hold its position S by correcting any drift. We exploit this feature to have the drone gradually moving to D

- An ideal spoofing trajectory is the one starting from the horizontal line a, where the arriving point is exactly above H

- Besides spoofing, the UAV will always point towards the direction of H tanks to its compass

- Whenever it believes it is on the left side of S1', it moves closer to H horizontally

- After passing S1, the UAV direction will turn left until it points precisely at D

- Denoting S2' as the turning point in the spoofed trajectory and its corresponding point in the actual trajectory as S2, S2'H || S2D

- The UAV, convinced to be taking the spoofed trajectory S2'H, will fly along the straight line S2D until it reaches D

- How to determine the spoofed trajectory S1'S2' such that its actual trajectory becomes S1S2 and S2'H becomes parallel with S2D at the earliest time?

- Greedy algorithm to compute S2'

- At the spoofed location S1', the next spoofed point Sx' is such that S1Sx' is perpendicular to S1D

- If SxD || Sx'H, done

- Otherwise, repeat

GPS Failsafe

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- GPS systems may occasionally drop the signal or suffer from glitches, i.e., provide significantly inaccurate position information

- The GPS failsafe is mechanism to provide safety to the drone in case of GPS signal oss or glitches

- In this case, the drone may either land or switch to a manual control

- To protect against glitches, the drone has a short memory of GPS position and compares the new measurement with the old one (you can use Kalman filter also in this case)

Classification

- We can classify consumer grade drones based on their behavior after failsafe mode

- First type: switch from the failsafe mode to positioning mode which utilizes GPS

- Second type: resume autopilot just before loss-of-lock

- Third type: maintain GPS failsafe even though GPS is available and wait until a pilot gives a new command

- We want to develop an anti-drone system such that, as soon as we detect the drone, we do not simply interrupt the control channel and have the drone to hover over a sensitive area

- To carry out a mission that evades RC jamming by anti-drone solutions, terrorists will operate drones in autopilot mode based on GPS and will not rely on a remote controller

- Therefore, spoofing GPS might be a solution to safely remove drones from an area they should not be into

Soft GPS Spoofing

- The spoofing signal is aligned with the authentic GPS signal

- The operation is not interrupted and the victim gradually locks to the spoofed GPS signals in three steps
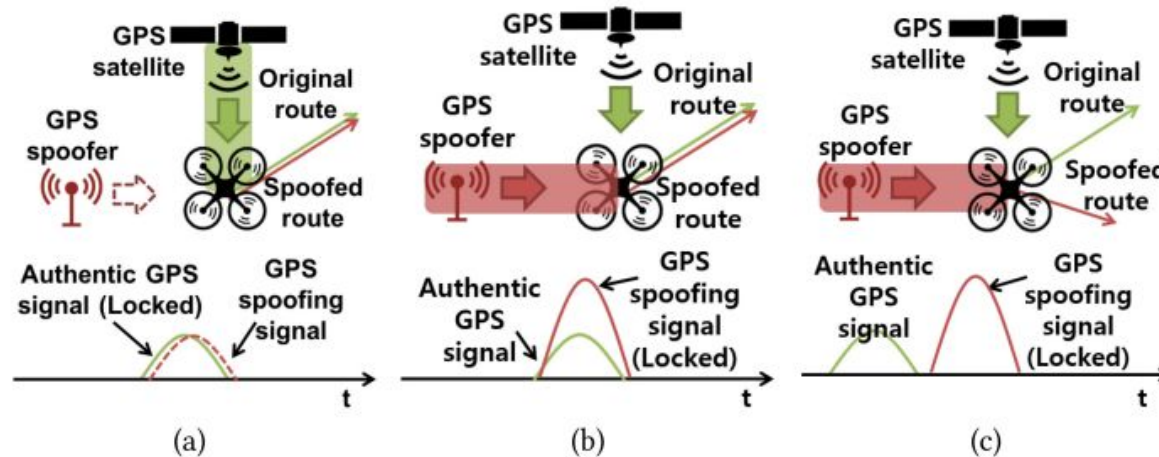
Hard GPS Spoofing

- Soft spoofing has some requirements to satisfy to avoid losing the lock

- When one of the requirements is not satisfied, we call this signal as hard GPS spoofing

- It initially acts like a jamming signal and the victim may lose its lock on the authentic signal

- The spoofing signal is stronger, thus the victim will reconnect to the spoofed signal

Strategy A

- It deals with type 1 drones

- The drone is trying to maintain its original position

- The attacker spoofs the target drone's GPS position as if the drone is moving in a certain direction

- The target drone generates speed in the opposite direction, so the drone moves in that direction in the real world

- It deals with type 2 drones

- Based on the drone's characteristic that control their body according to their path-following algorithm (e.g., in RTH)

- If the GPS position is manipulated as the drone deviates from the path, then it will move in a different direction from the original direction to return to the track

- The hijacker can determine the hijacking direction and calculate the corresponding fake location

- It deals with type 3 drones

- Since they need to wait for a pilot command, manipulation of GPS signal is not effective

- Therefore, we want to hijack them without losing the connection with the GPS (soft GPS spoofing)

- However, it might be complicated to move the drone if it uses a combination of GPS and IMU sensors to determine its location

- 3DR Solo does not have a fallback mechanism when losing connection with the GPS

- It is complicated to hijack, because it uses both GPS and IMU for localization

- It has a complicated path-following algorithm that uses Intermediate Target Position (ITP), necessitating moving the spoofed GPS location accordingly to safely control the behavior of the target drone

- Good case study for strategy C!

- During flight the drone might deviate from the track because of external influences such as wind

- The path following algorithm is what prevent the drone from completely deviating from its mission

- The ArduCopter path following algorithm is based on the ITP position

- ArduCopter periodically advances the ITP along the track in small increments and causes the drone body to move to the ITP

- If the drone mistakenly determines that it has deviated from the track owing to GPS spoofing, then it will move in the direction away from the manipulated location to the ITP

- The path following algorithm uses a *leash length*, i.e., a minimum distance from the current position to the main path

- The attacker can exploit this distance to hijack the drone's location

- The ITP is fixed or only slightly changed when the GPS location deviates from the main track by more than the leash length

- We can hence say that the physical location of the drone immediately before hijacking is an approximation of the updated ITP

- The attacker hance derive the possible coordinates of the initial fake location from the approximated ITP and the intended hijack direction

- The drone will try to move to the ITP if the leash length is higher than 13m (leash length)

- The direction from the initial fake location to the ITP should be the same as the hijacking direction

$$a_{init} = p_{init} + k \cdot (p_{target} - p_{init}), \quad \text{where } k < 0 \text{ and } \|a_{init} - p_{init}\| > (leash \ length)$$

Manipulated
location

ITP

Target
location
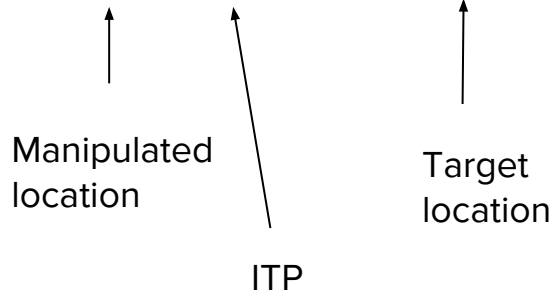
- The stabilization of drones is an automatic task executed by au automatic controller

- It uses Inertial Measurement Unit (IMU) to gather information

- An IMU is an electronic device using a combination of accelerometers, gyroscopes, and sometimes magnetometers to measure a body's specific force

- In a UAV, an IMU measures the orientation, rotation, and acceleration

- Micro-Electro-Mechanical Systems (MEMS) gyroscopes are used to make flight control modules small

MEMS Gyroscope

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- The principle of the MEMS gyroscope is the Coriolis effect, i.e., the deflection of a moving object in a rotating reference frame

- In the observer's view, the path of the moving object observed to be bent by a fictitious force

Continuously vibrating at a given frequency

Acoustic Noise Effect
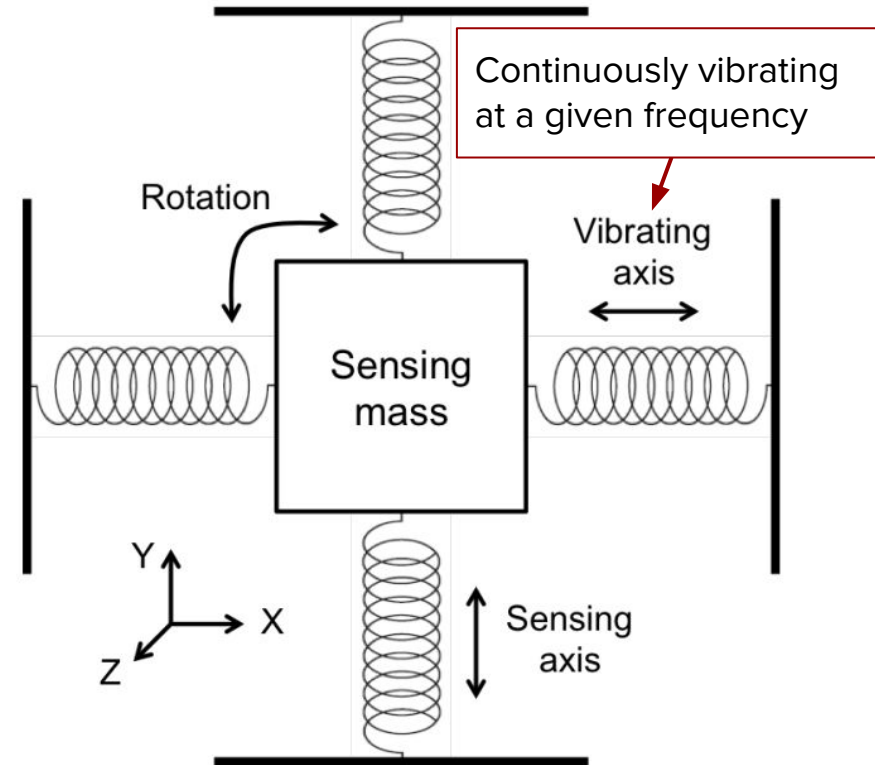
- MEMS gyroscopes are highly vulnerable to harsh acoustic noise

- Such noise cause accuracy degradation, thus providing wrong results

- A MEMS gyroscope has a resonant frequency related to the physical characteristics of its structure

- Due to this resonance, if met, the gyroscope generates unexpected outputs that cause system malfunctioning

- Usually, such frequencies should be ultrasound
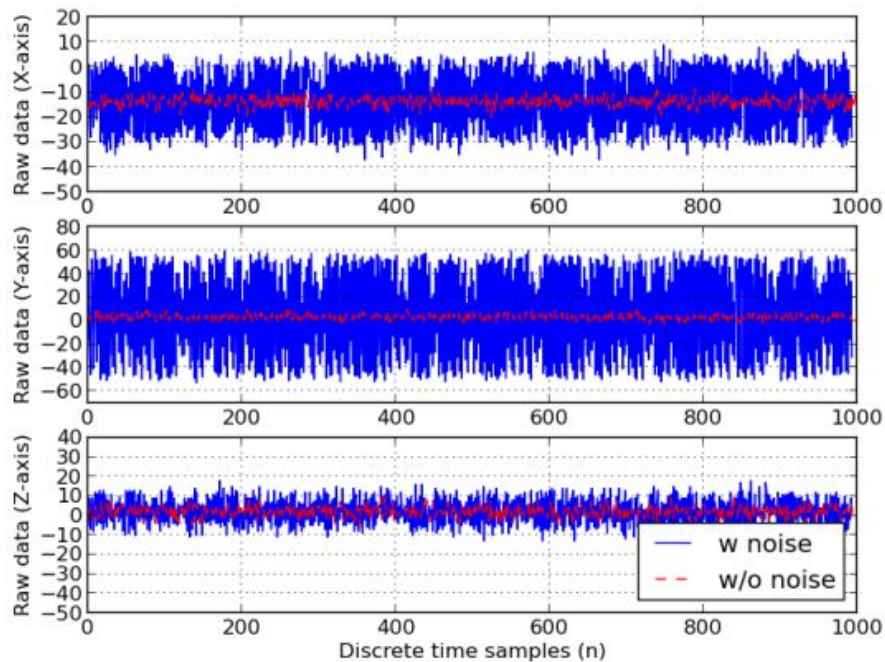
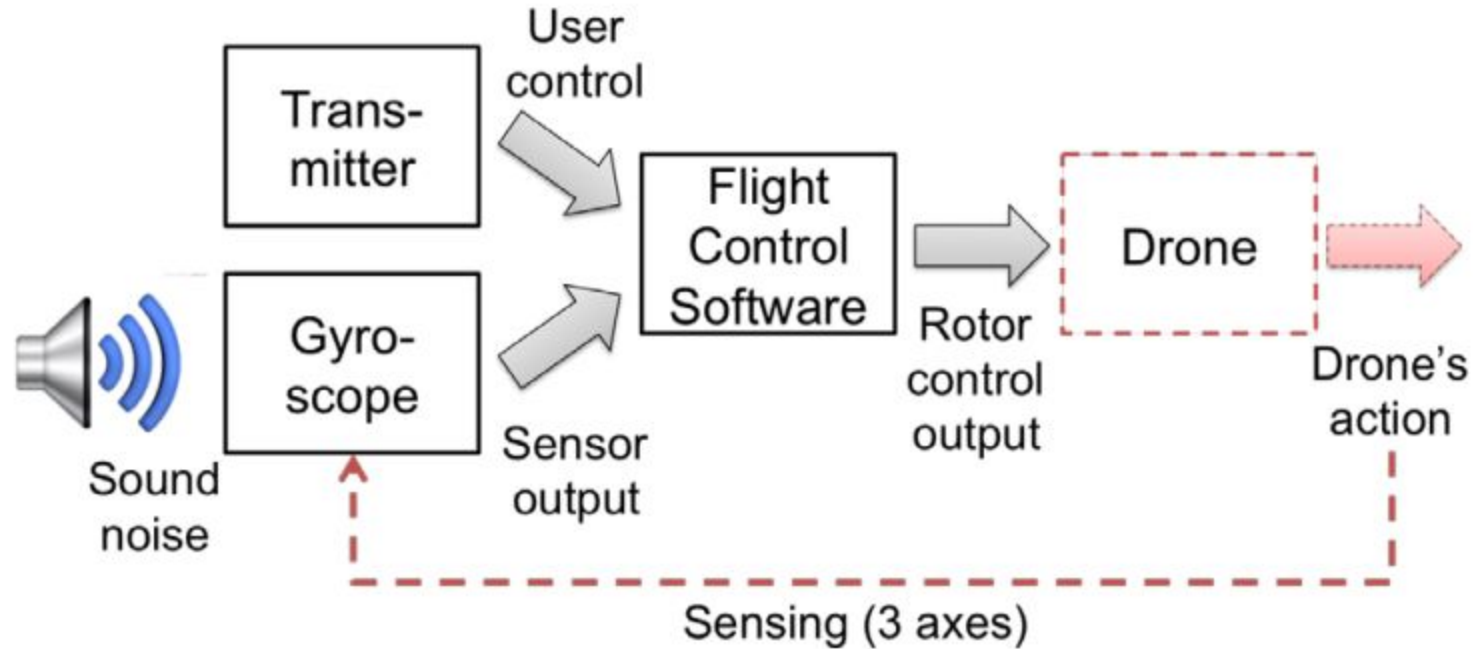- The sensitivity to noise can be exploited by an attacker

Noise Effect on MEMS

Propagation of Signals

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA
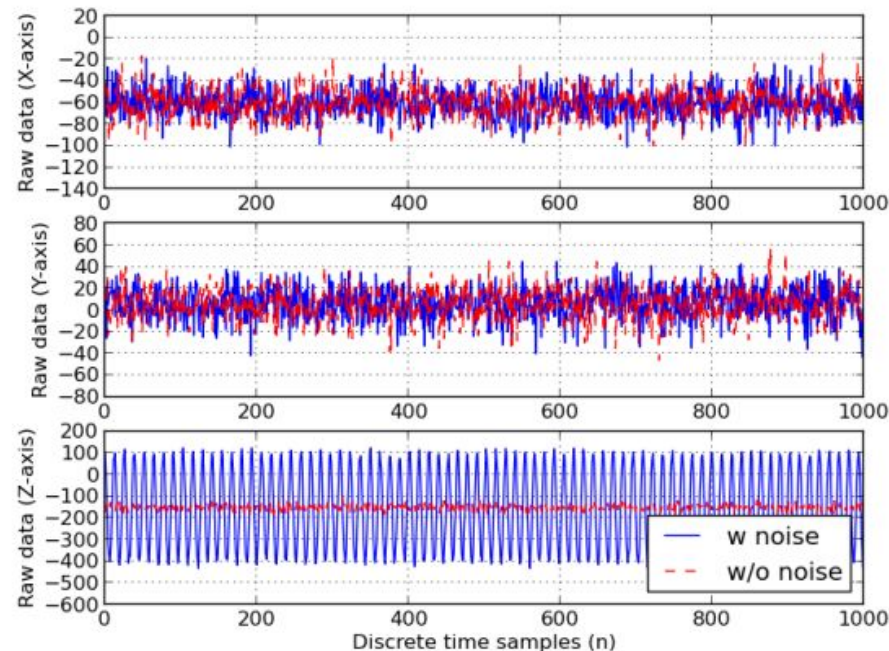
- The attacker, in order to design a good strategy, needs to understand what the drone is doing

- Static analysis of the controller code to understand the reaction of sensor and actuators to noise

- Usually drones can support different gyroscope implementations, however the main software routing is the same for all of them

- The main processor reads the raw data from the gyroscope's registers along with the control data provided by the user

- Such raw data are them main inputs of the controller, which uses a PID logic to instruct rotors as follows

  - P is proportional to the present output of the gyroscope, and if the present output is abnormally large the control from the transmitter can be ignored

- Such raw data are them main inputs of the controller, which uses a PID logic to instruct rotors as follows
  - I is proportional to the accumulated error between the output from the transmitter and the gyroscope, which can be ignored because usually its gain is very small
  - D is proportional to the changes between the present output values and the gyroscope
- Throughout the whole process the gyroscope data is not checked
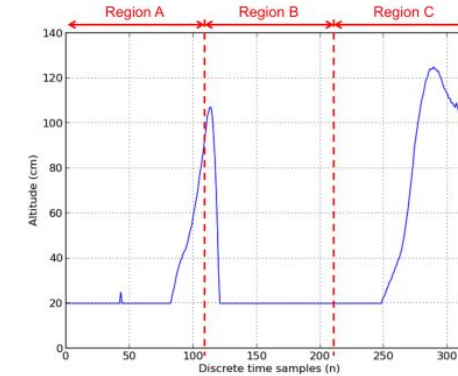
Attack Effects
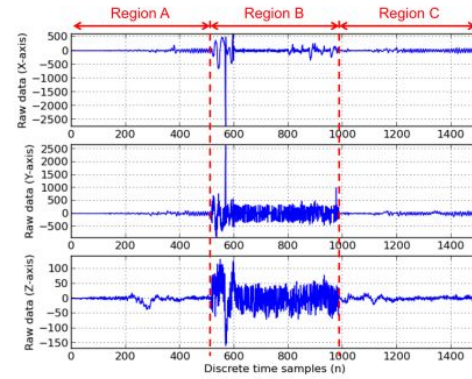
(a) Raw data samples of the gyroscope
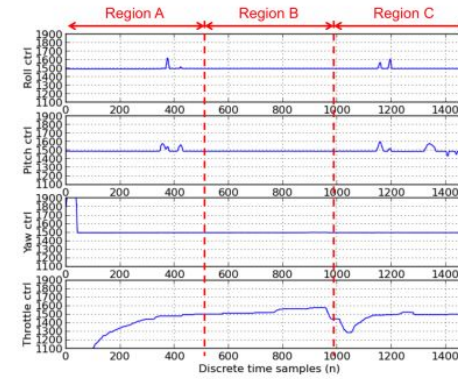
(b) Received data samples from the transmitter
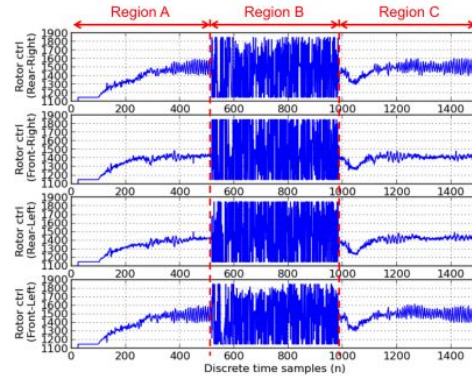
(c) Rotor control data samples (from the flight control software)

(d) Altitude data samples from sonar