Tractor Beam: Safe-hijacking of Consumer Drones with Adaptive GPS Spoofing

Juhwan Noh, Yujin Kwon, Yunmok Son, Hocheol Shin, Dohyun Kim,
Jaeyeong Choi, Yongdae Kim

SYSSEC

Presenter: Pierre Noyer

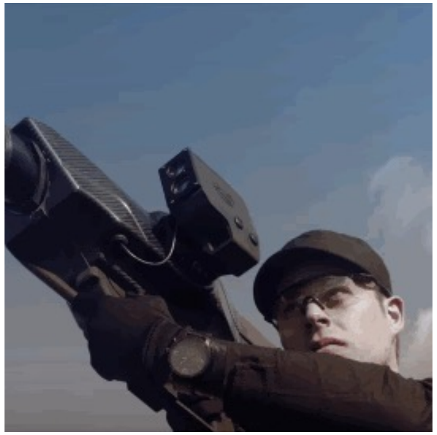
Motivation

- Consumer drone market is booming
- used for terrorists attacks

April 2015

Motivation

- Some anti-drone services exist but are inadequate



Shooting nets

Radio control and GNSS jamming

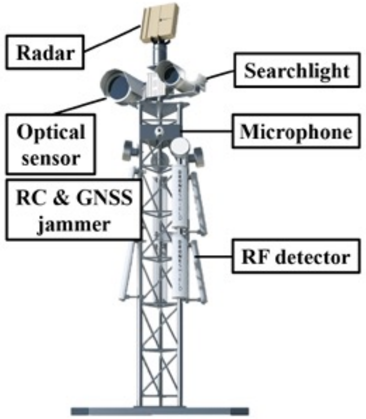
Laser attack

Introduction

- On protected areas, Radio control jamming is always present, making remote control unsuable for attackers drones

- Use of GPS-autopilot

- Existence of fail-safe mode and recovery behavior after recovering GPS signal



Introduction

- Vulnerability: GPS communication is neither encrypted nor authenticated → enabling GPS spoofing

- Goal: use GPS spoofing to move the drone to the desired location according to its different fail-safe mechanism

Background

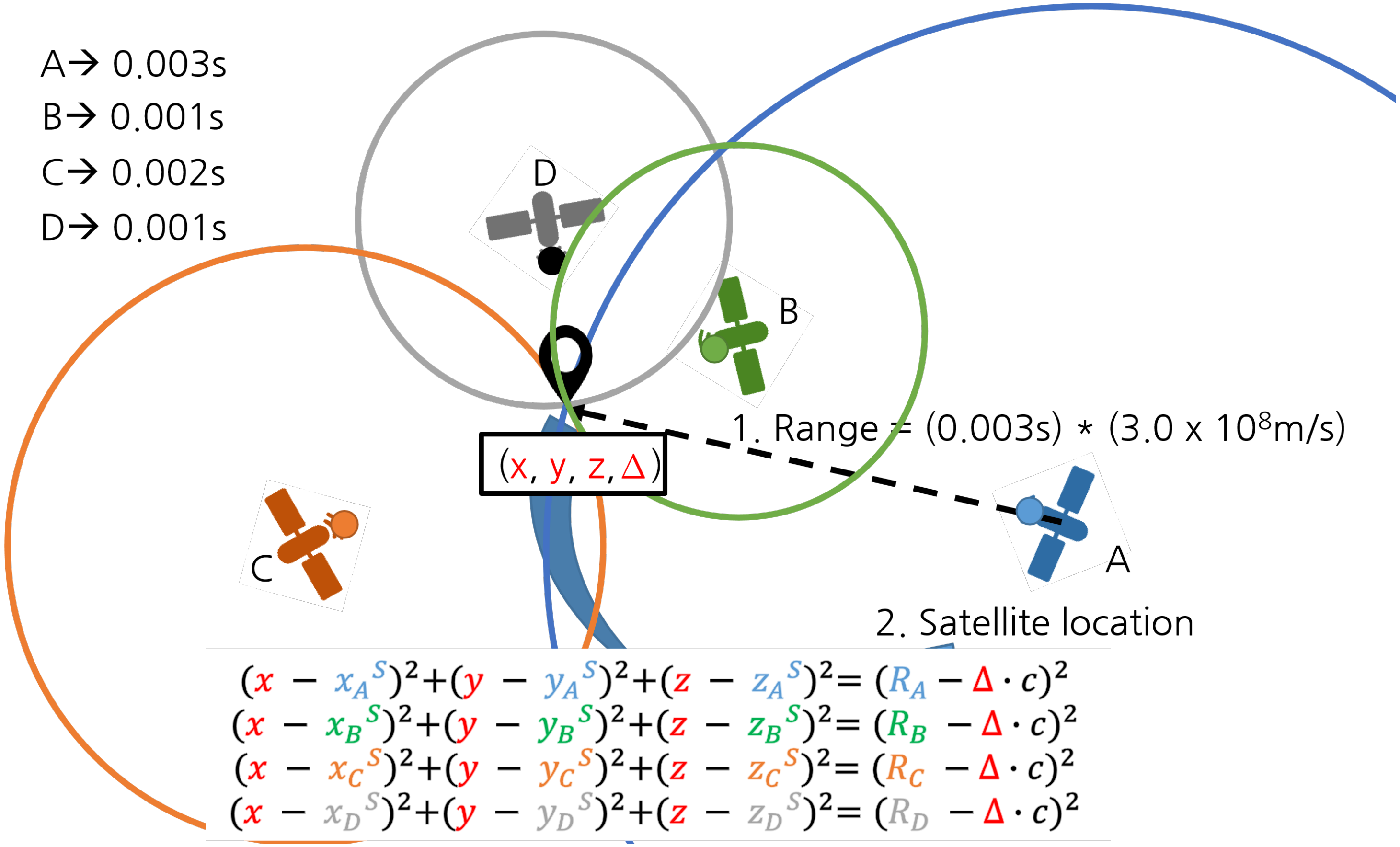
- GPS

A→ 0.003s

B→ 0.001s

C→ 0.002s

D→ 0.001s



(x, y, z, Δ)

1. Range = (0.003s) * (3.0 x 10^8m/s)

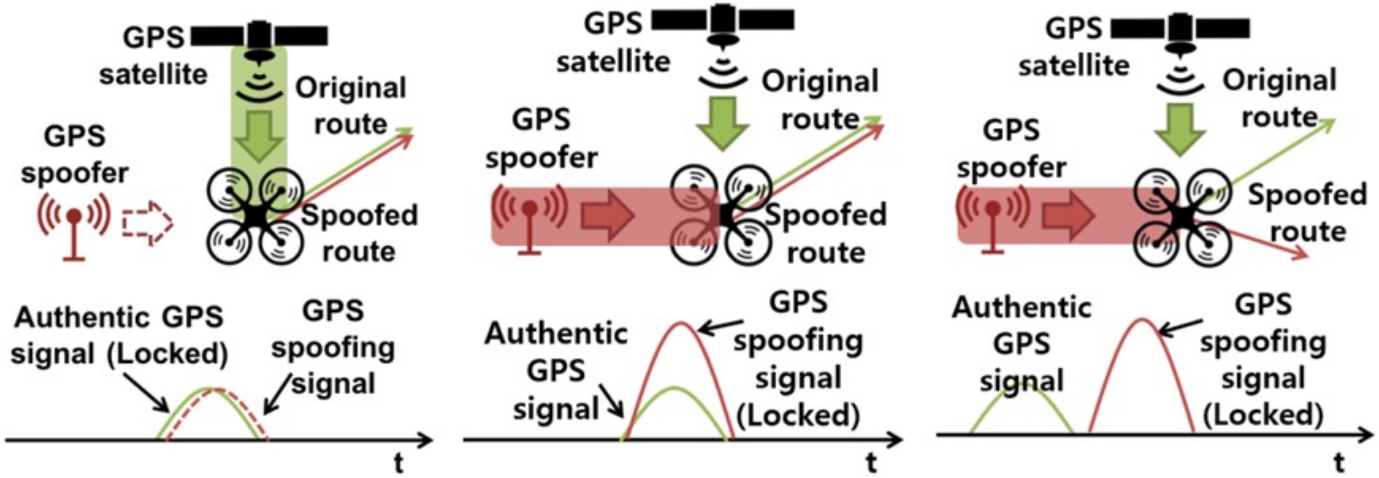
2. Satellite location

$$(x - {x_A}^S)^2+(y - {y_A}^S)^2+(z - {z_A}^S)^2= (R_A - \Delta \cdot c)^2$$
$$(x - {x_B}^S)^2+(y - {y_B}^S)^2+(z - {z_B}^S)^2= (R_B - \Delta \cdot c)^2$$
$$(x - {x_C}^S)^2+(y - {y_C}^S)^2+(z - {z_C}^S)^2= (R_C - \Delta \cdot c)^2$$
$$(x - {x_D}^S)^2+(y - {y_D}^S)^2+(z - {z_D}^S)^2= (R_D - \Delta \cdot c)^2$$

Background

- GPS-spoofing, 2 types:

Soft and Hard GPS Spoofing



Background

- What is fail-safe

[redacted]

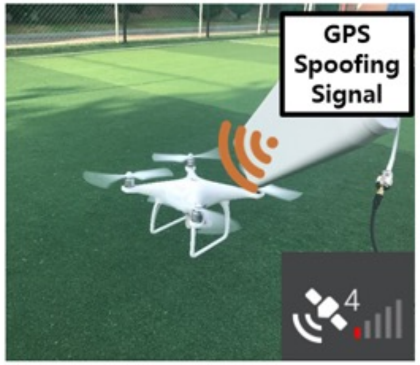
Contribution

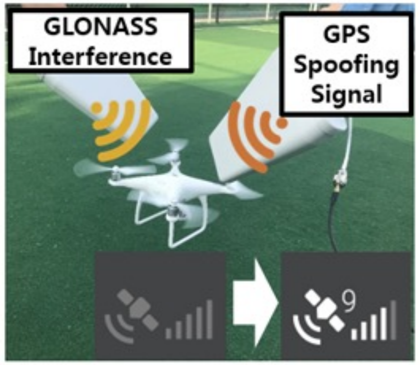
- analyze fail-safe mechanisms used in different drones
- design mechanisms to bypass/misuse those fail-safe mechanisms to hijack consumer drones
- confirm those mechanisms through real-world experiments.

GPS fail-safe mechanisms

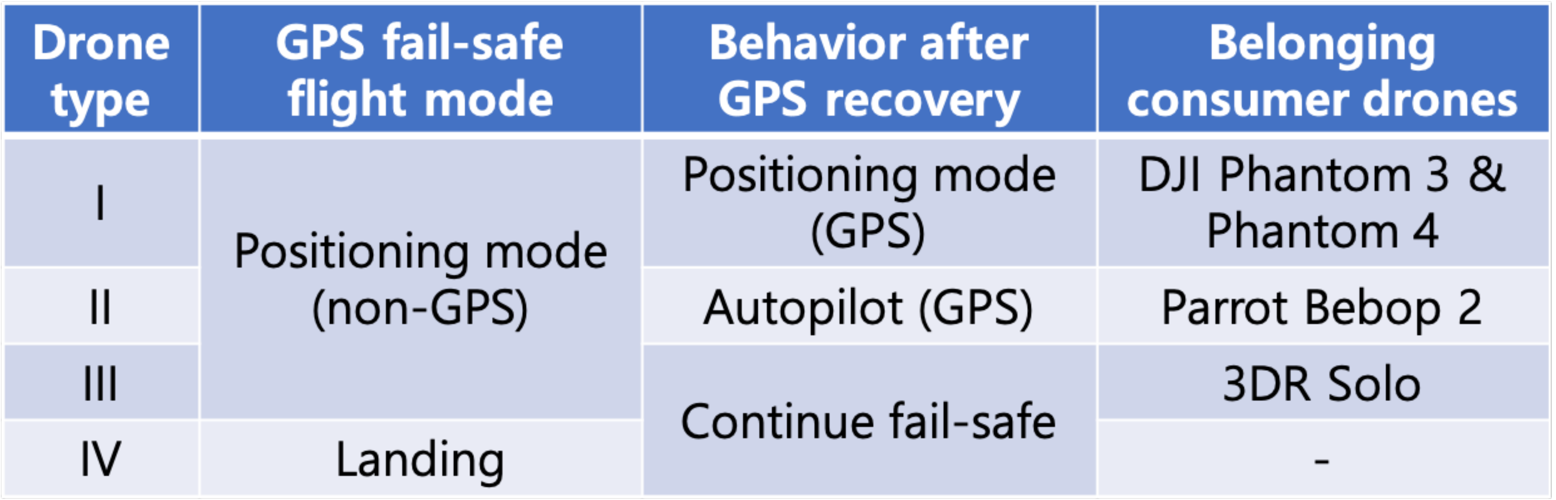
- Dynamic analyses by transmitting hard GPS spoofing signal (black-box setting)

- Analysis of 3DR Solo source code



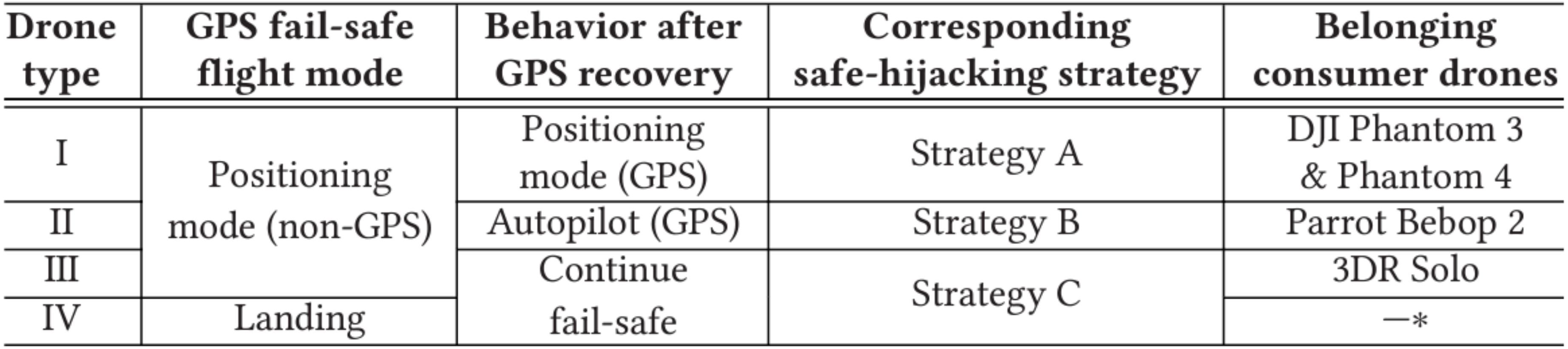


GPS fail-safe mechanisms taxonomy



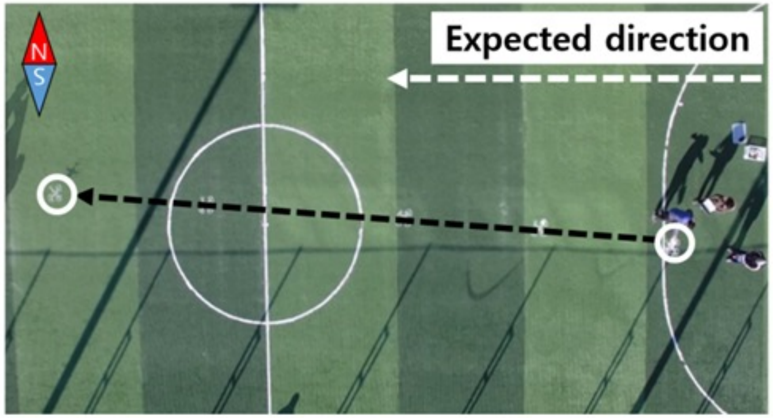
Drone type	GPS fail-safe flight mode	Behavior after GPS recovery	Belonging consumer drones
I	Positioning mode (non-GPS)	Positioning mode (GPS)	DJI Phantom 3 & Phantom 4
II		Autopilot (GPS)	Parrot Bebop 2
III		Continue fail-safe	3DR Solo
IV	Landing		-

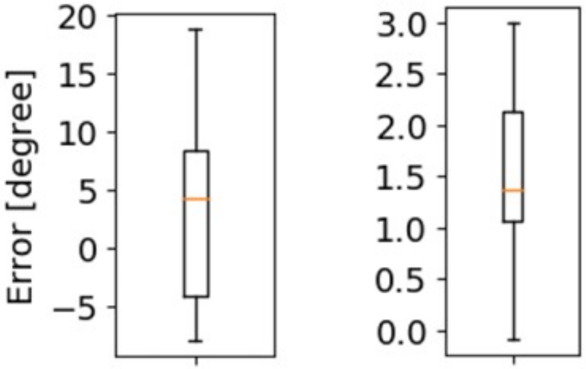
Safe-hijacking strategy



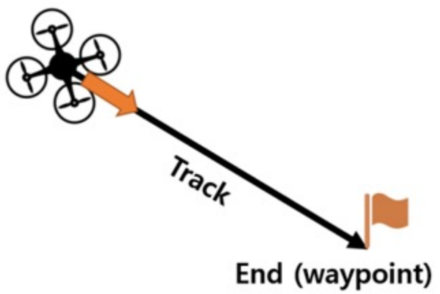
Drone type	GPS fail-safe flight mode	Behavior after GPS recovery	Corresponding safe-hijacking strategy	Belonging consumer drones
I	Positioning mode (non-GPS)	Positioning mode (GPS)	Strategy A	DJI Phantom 3 & Phantom 4
II		Autopilot (GPS)	Strategy B	Parrot Bebop 2
III		Continue fail-safe	Strategy C	3DR Solo
IV	Landing			—*

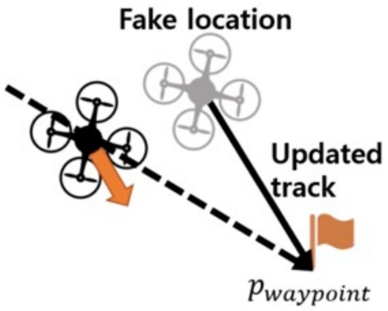
Case study for Strategy A

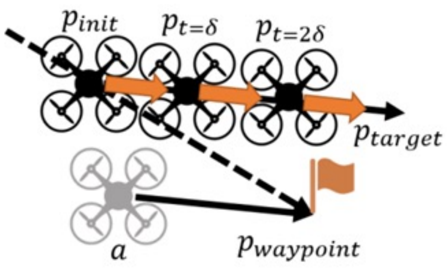


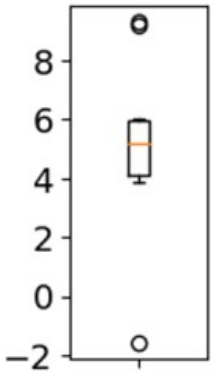


Case study for Strategy B





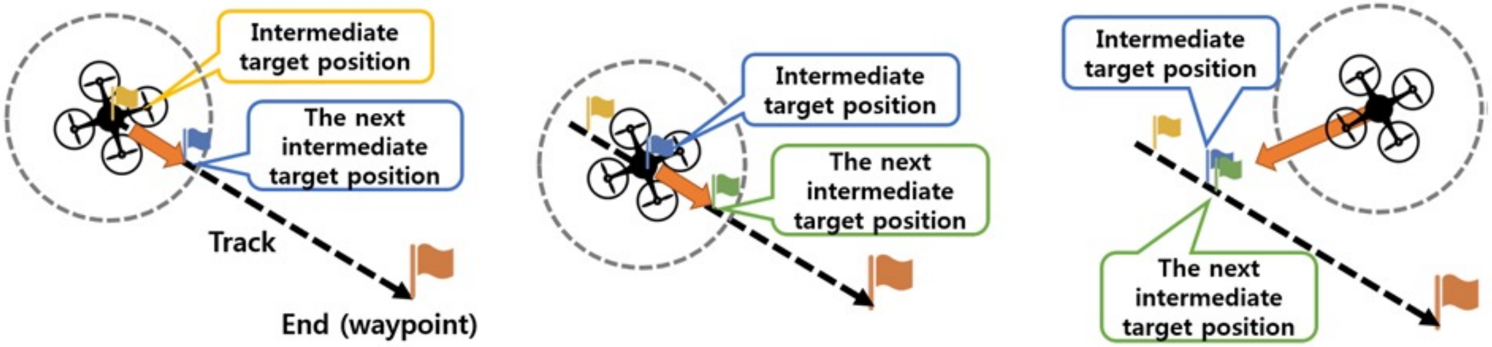




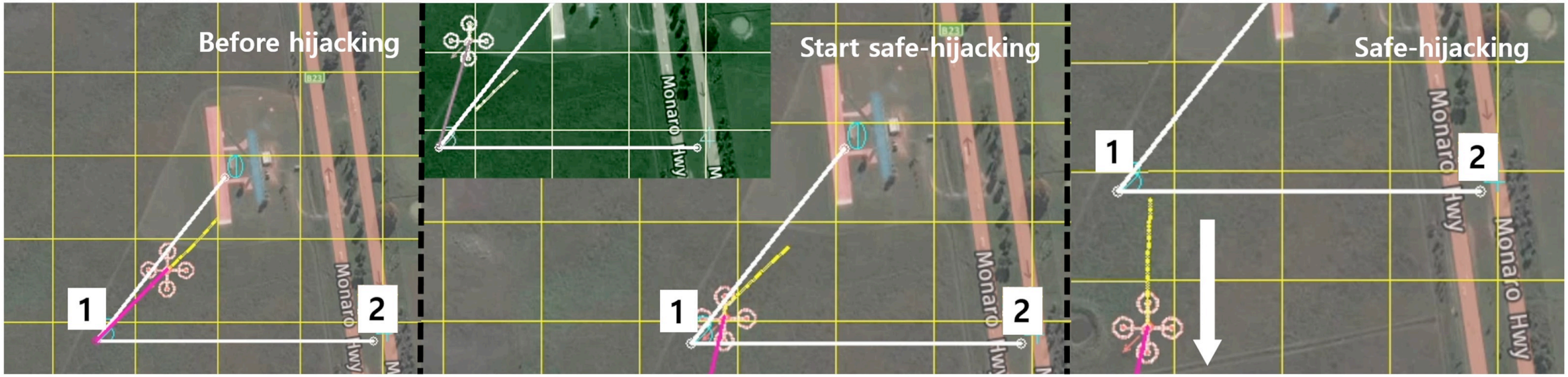
Case study for Strategy B

[redacted]

Case study for Strategy C


Intermediate target position
The next intermediate target position
Track
End (waypoint)
Intermediate target position
The next intermediate target position
Intermediate target position
The next intermediate target position

Case study for Strategy C



Discussion

- Mitigation of GPS spoofing threats to legitimate consumer drones

- Legal and Safety issues of GPS spoofing

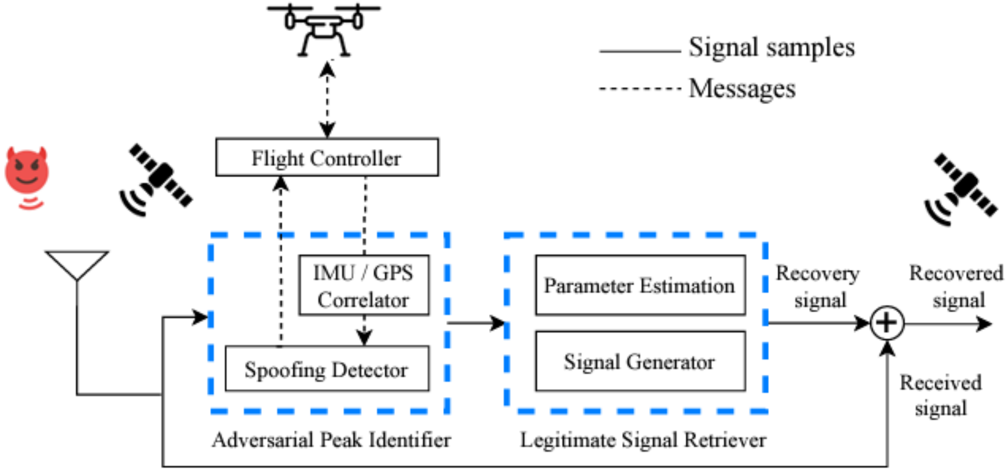
Related Work (before)

- *On the requirements for successful GPS spoofing attacks. CCS '11*

- *Unmanned Aircraft Capture and Control via GPS Spoofing.*
J. Field Robot. 31, 4 (2014)

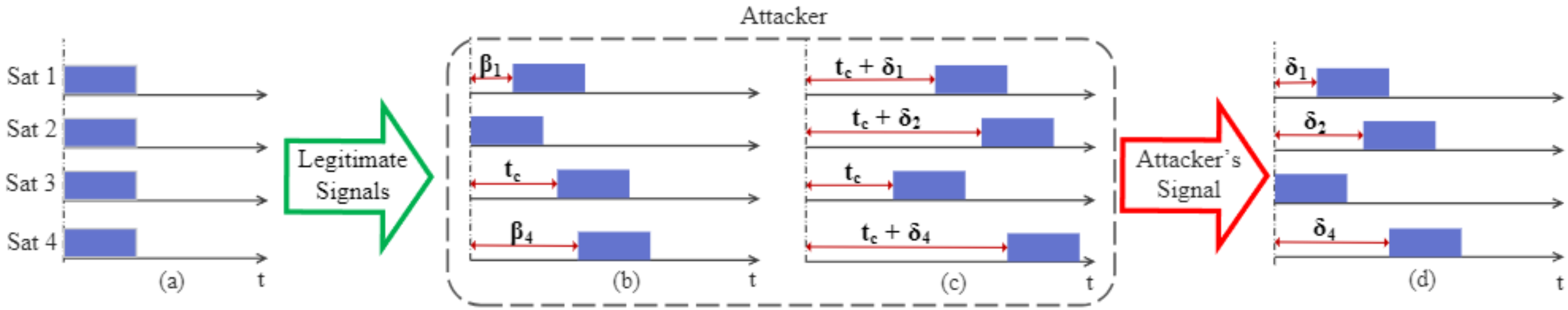
Related Work (after)

- *SemperFi: Anti-spoofing GPS Receiver for UAVs. NDSS (2022)*



Related Work (after)

- *Location-independent GNSS Relay Attacks: A Lazy Attacker's Guide to Bypassing Navigation Message Authentication. ACM WiSec 2023*



Conclusion

- analyze fail-safe mechanisms used 4 popular drones via white and black box analyses to develop a drone taxonomy

- Developed safe-hijacking strategies for fail-safe mechanism

- Demonstrated the efficacy of those mechanisms through real-world experiments.

Good Questions

- This attack can be used to compromise the smartcar's GPS system in auto driving mode and it can cause significant car accidents.
- Is it possible to shoot directional GPS spoofing signal so that it only affects the target drone and causes less collateral damage?
- For defense against hard GPS spoofing, can we utilize techniques like dead reckoning using IMU and refrain from reconnecting to GPS after entering fail-safe mode?
- Would it make sense to incorporate authentication in the C/A code signals to prevent GPS spoofing? If not, what would be the main constraints preventing it?

Best questions

- ***Ilman Mohammad Al Momin*** :Given that 3DR Solo relies on an EKF algorithm for GPS-IMU integration, could predictive modeling of EKF outputs serve as an early detection method to counter adaptive spoofing strategies?

- ***Changgun Kang:*** Is it possible to hijack multiple drones simultaneously?

- ***Hyunmin Ju***: Given the adaptive nature of this GPS spoofing method, how feasible would it be for consumer drones to use real-time cross-verification between multiple sensors as a lightweight yet effective solution? I am curious to hear the presenter’s thoughts on this.