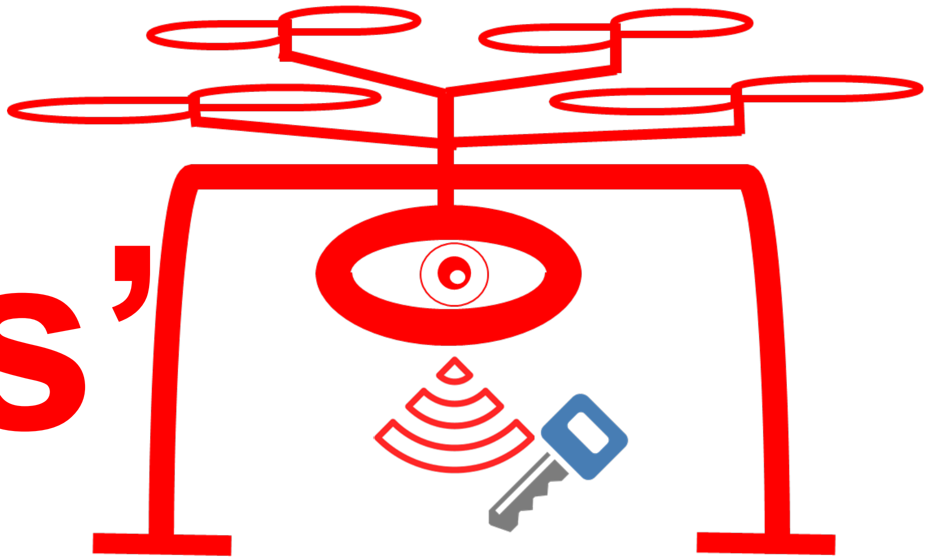
CBG
Cyber@ Ben-Gurion University
Telekom Innovation Labs

Drones' Cryptanalysis



Ben Nassi Raz Ben-Netanel
Prof. Adi Shamir Prof. Yuval Elovici

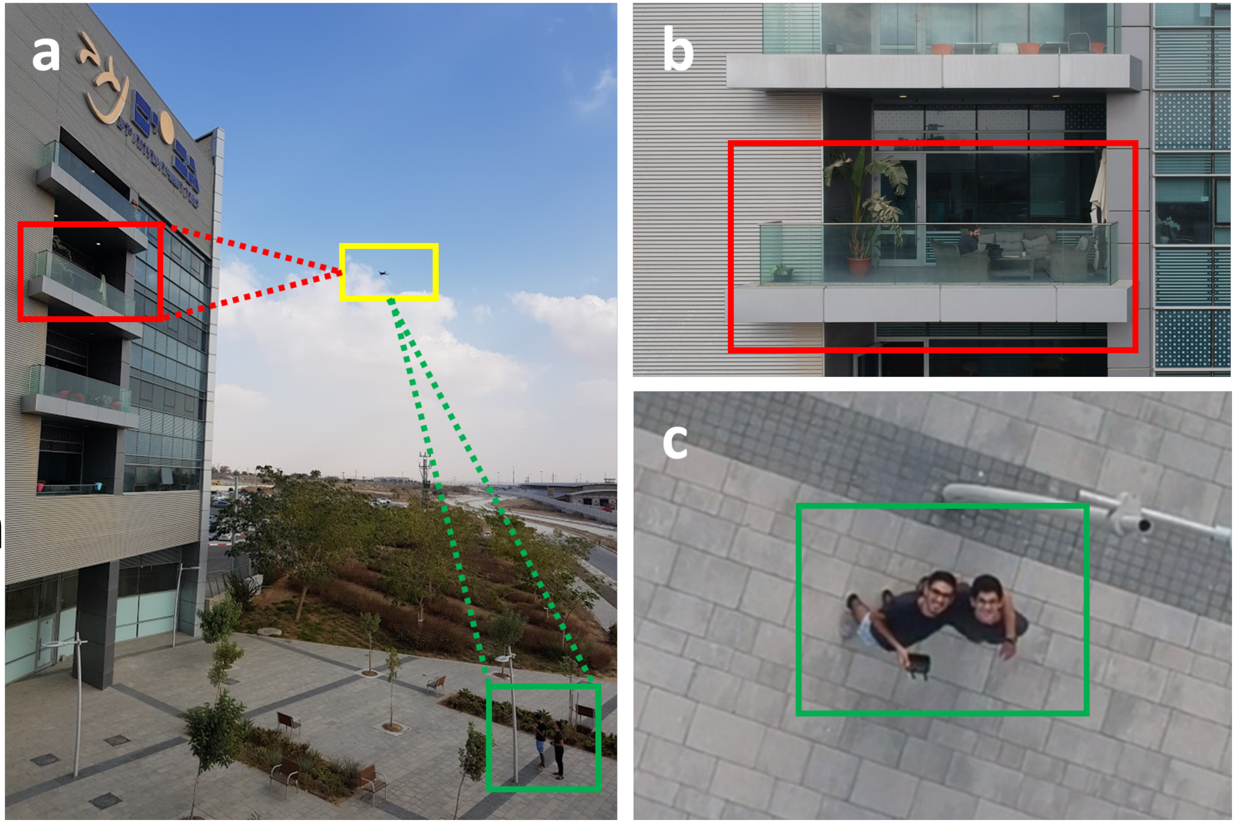
IEEE COMPUTER SOCIETY

Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting Whether an FPV Channel is Being Used to Spy on a Victim
6) Locating a Spying Drone in Space
7) Hiding the Flicker from the Drone's Operator
8) Evaluation in Real Scenarios

Research Question

In an "Open Skies" era in which drones can fly between us, a new challenge arises: how can we determine whether a drone that is passing near a house is being used by its operator for a legitimate purpose (e.g., delivering pizza) or an illegitimate purpose (e.g., spying on an organization)?



Drones Create a New Threat to Privacy

Not in my backyard! Woman throws stones before using a GUN to get rid of nosy neighbour's drone

MailOnline

Kentucky Man Arrested After Shooting Down Neighbor's Drone

NBC NEWS

Spouses are using DRONES to catch their cheating partners

MailOnline

Eyes In The Sky: The Public Has Privacy Concerns About Drones

Forbes

Are Drones Spying on Miley Cyrus and Selena Gomez?

People

Drone complaints soar as concerns grow over snooping

theguardian

The drones among us: Reports of drone-related incidents are going up and up and up

NATIONAL POST

Drone Adoption Rates Increase Around the World

- **<u>Drone Adoption</u>**
  Businesses around the world have started to adopt drones for various purposes (e.g., deliveries).

- **<u>"Open Skies" Policy</u>**
  Regulations are being changed, allowing drones to fly in populated areas (adopting an "Open Skies" Policy in cities).

JACK STEWART TRANSPORTATION 10.26.17 08:00 AM

PRESIDENT TRUMP MOVES TO FILL AMERICA'S SKIES WITH DRONES

FAA proposes relaxing drone laws, potentially allowing drone deliveries to begin

Loz Blain | January 15th, 2019

Geofencing Methods for Drone Detection

Radar

Camera

LiDAR

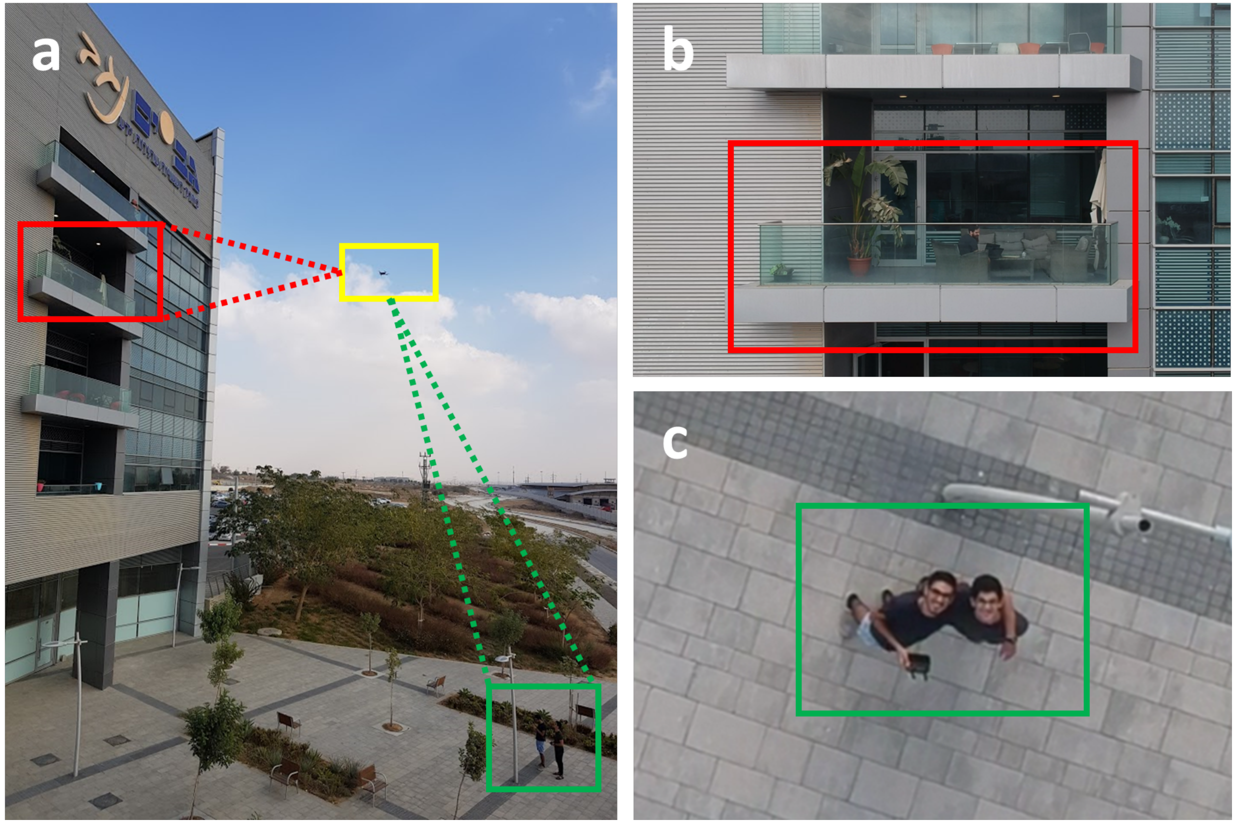
Microphone Array

These methods are able to detect the presence of nearby drones.

Geofencing Methods for Drone Detection

Do Geofencing methods effective at detecting a privacy invasion attack?

1. The presence of drones is **no longer restricted** in populated areas.
2. The difference between legitimate use of a drone and illegitimate use depends on the drone's **camera orientation** rather than on the drone's location.



Geofencing methods are irrelevant for detecting a privacy invasion attack in the "Open Skies" era.

Objective

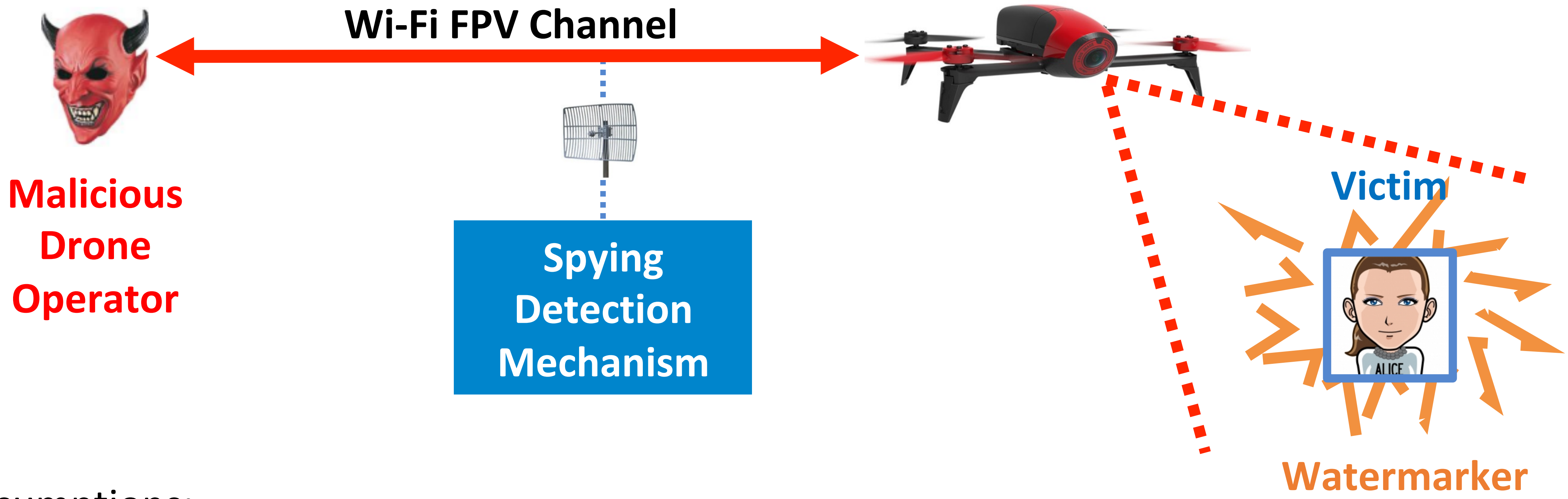
Main Objective: Detecting a privacy invasion attack.

- Classifying a suspicious radio transmission as an FPV channel.
- Detecting an FPV channel’s quality (FPS and resolution).
- Detecting whether an FPV channel is being used to spy on a victim (even if the victim is not static).
- Locating a spying drone in space.
- Detecting a privacy invasion attack without the awareness of the drone’s operator.

Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting Whether an FPV Channel is Being Used to Spy on a Victim
6) Locating a Spying Drone in Space
7) Hiding the Flicker from the Drone’s Operator
8) Evaluation in Real Scenarios

Target Detection Scheme



Assumptions:

1) The attacker is using a Wi-Fi FPV drone (located in a range of up to 5 KM from the victim).
2) The spy detection mechanism is connected to an RF scanner with a proper antenna for intercepting suspicious radio transmissions.

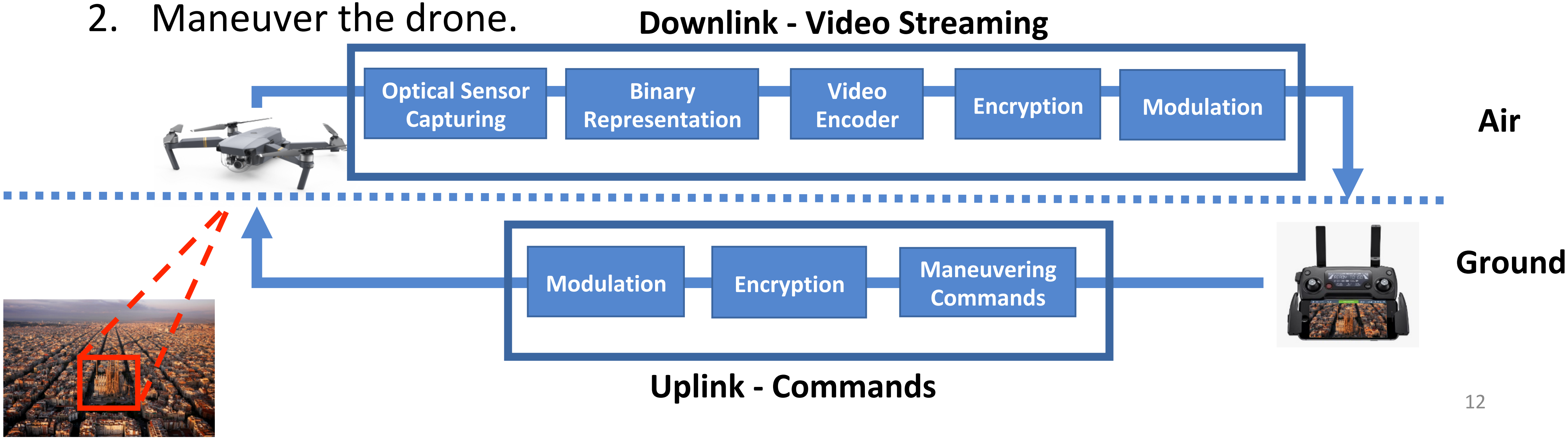
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting Whether an FPV Channel is Being Used to Spy on a Victim
6) Locating a Spying Drone in Space
7) Hiding the Flicker from the Drone’s Operator
8) Evaluation in Real Scenarios

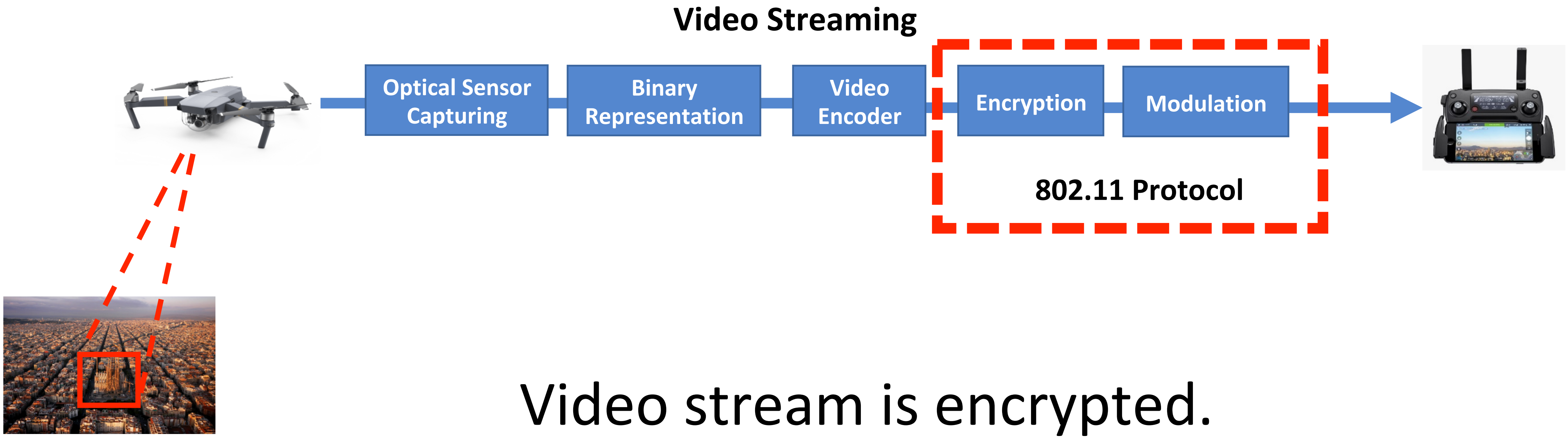
Wi-Fi First-Person View Channel

<u>Wi-Fi First-Person View (FPV) Channel</u> - a communication channel based on Wi-Fi communication designed to:

1. Stream the video captured by the drone’s video camera to the operator’s controller.
2. Maneuver the drone.



Downlink - Video Streaming Channel



Video stream is encrypted.

Does encryption ensures confidentiality?

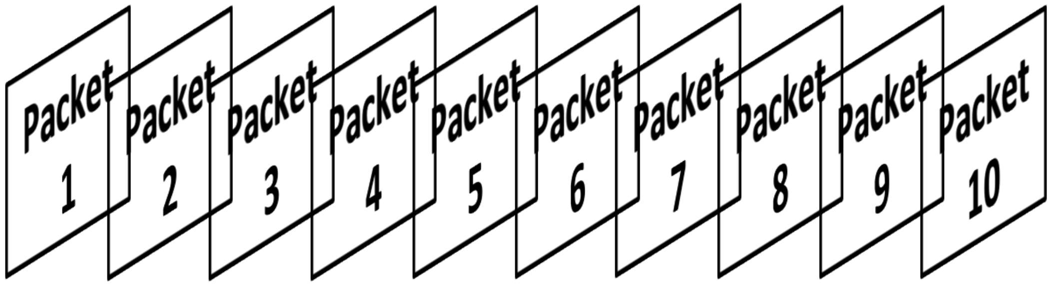
Interception of an FPV Stream

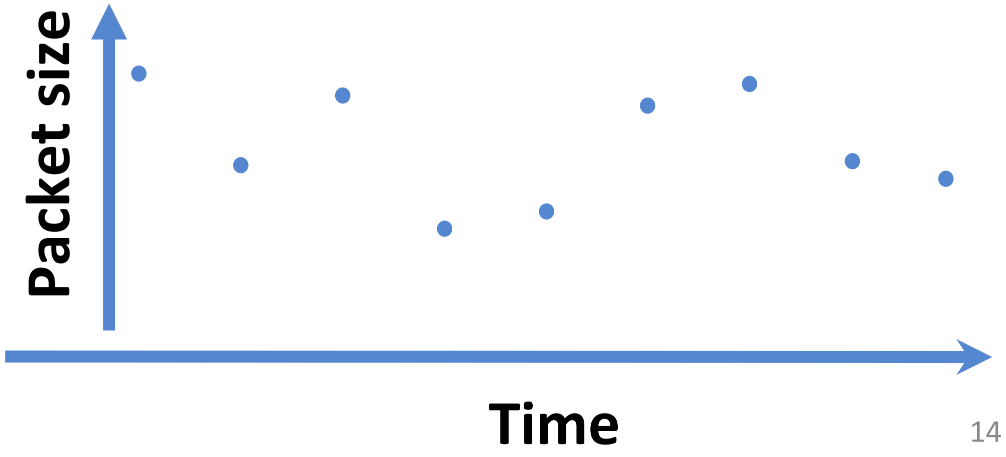
Given a suspicious Wi-Fi transmission, we create an ***intercepted bitrate signal***:

1) Sniffing Wi-Fi Packets
   - Enabling NIC's monitoring mode (attack mode)
   - Sniffing a network using **Airmon**

2) Extracting a time series signal from unencrypted metadata (2nd layer)
   - Packet length (frame.len)
   - Packet arrival time (frame.number)

3) Downsampling (by aggregating time series in a fixed window)





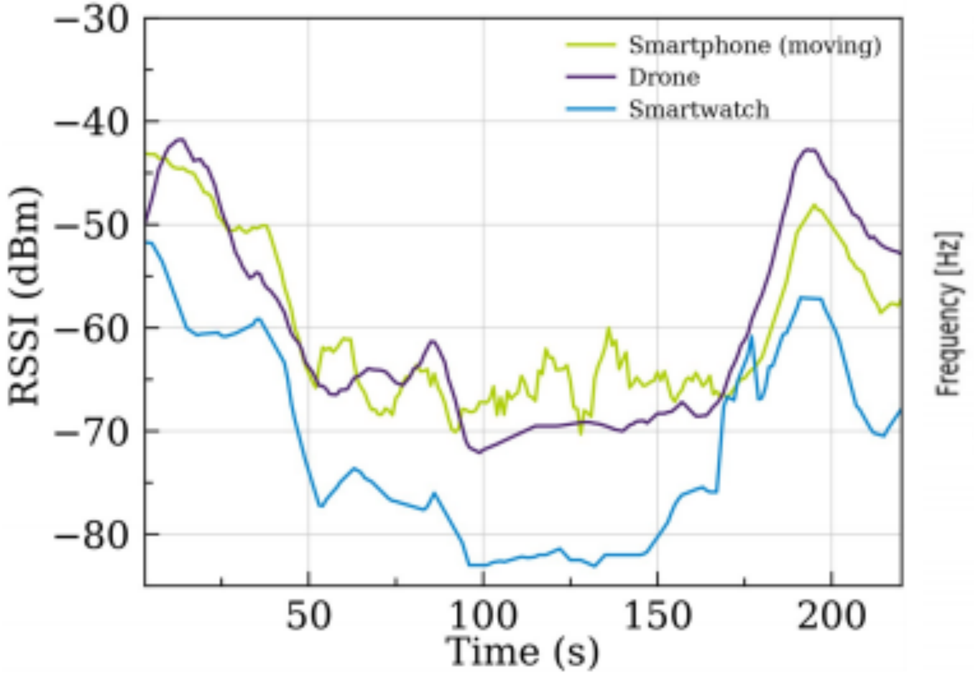
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) <u>FPV Channel Classification</u>
5) Detecting Whether an FPV Channel is Being Used to Spy on a Victim
6) Locating a Spying Drone in Space
7) Hiding the Flicker from the Drone's Operator
8) Evaluation in Real Scenarios

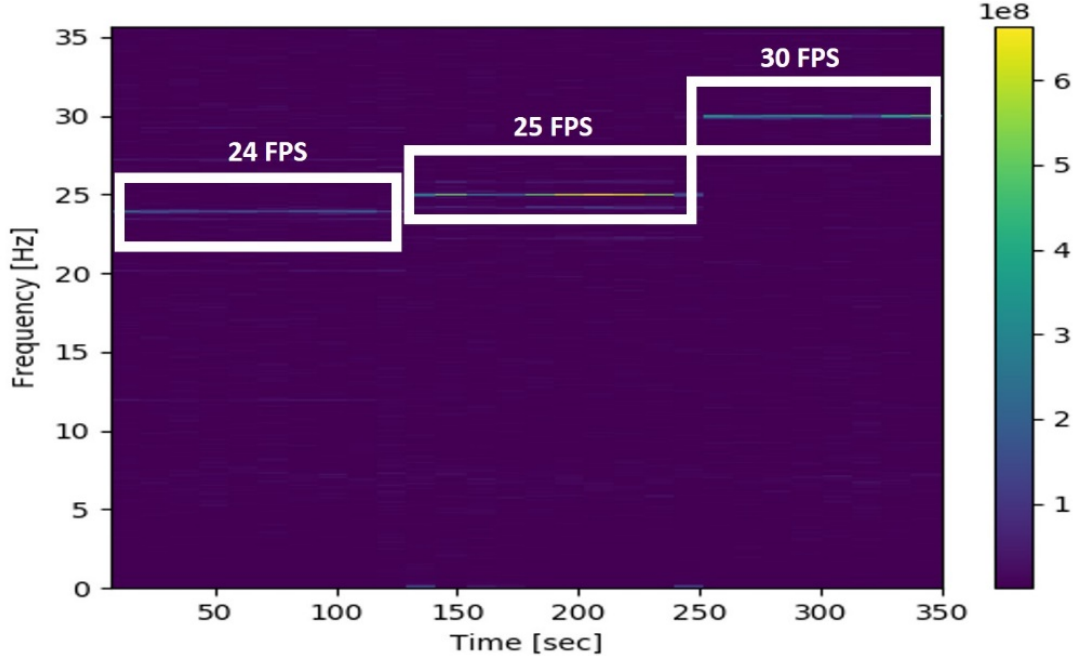
Classifying a Suspicious Transmission as an FPV Channel

Key Observation: A drone is a flying camera.

Moving Device Detection

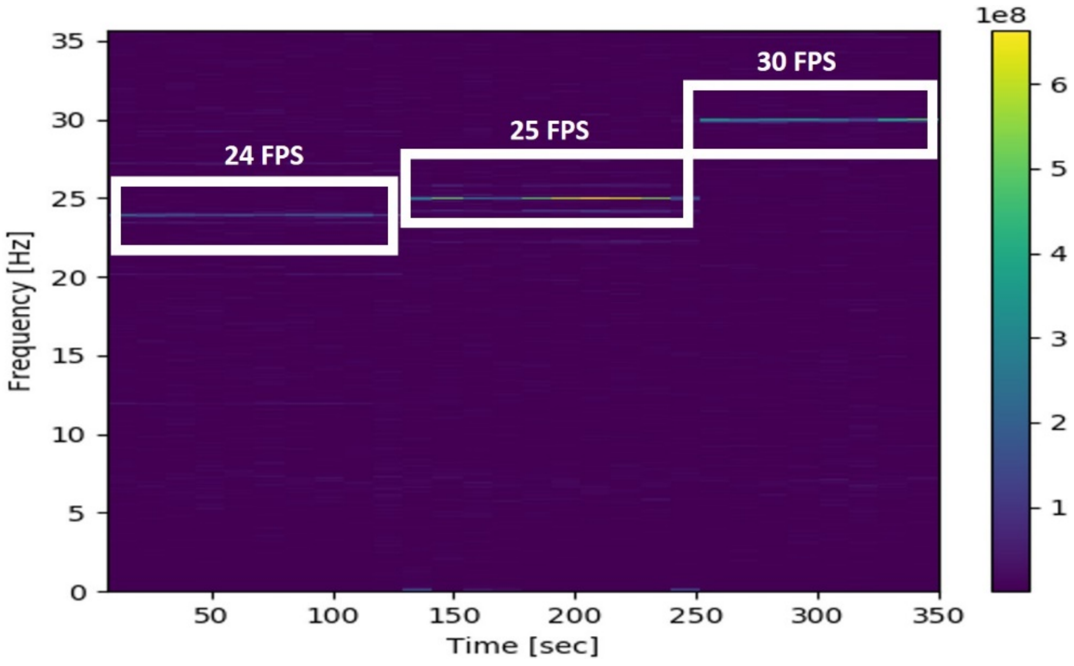


Camera Detection



Classifying a Suspicious Transmission as an FPV Channel

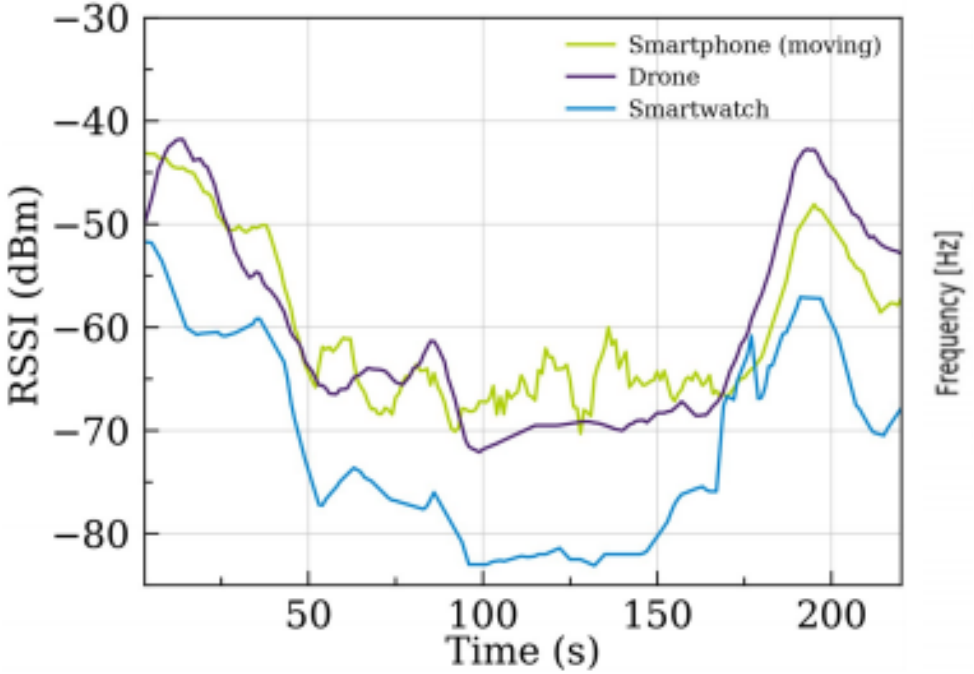
Camera Detection



1) Analyzing the intercepted bitrate signal in the frequency domain.
2) Finding the frequency with the maximum magnitude.
3) Compare the frequency with the maximum magnitude to known frame per second rates of drones {24,25,30,60,96,120}.

Classifying a Suspicious Transmission as an FPV Channel

Moving Object Detection

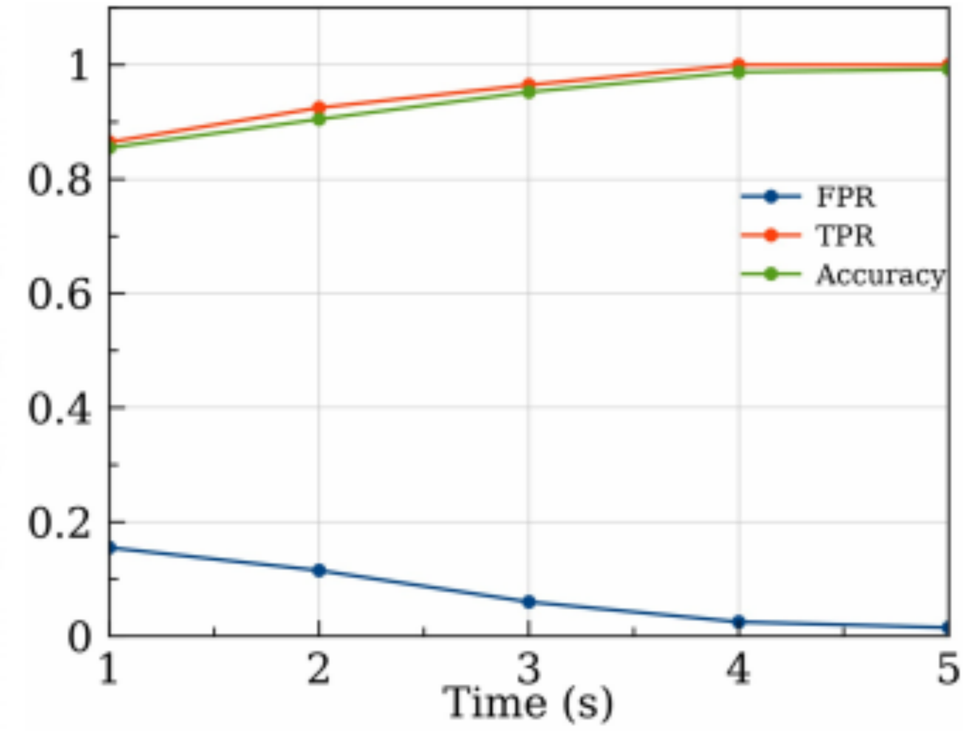


1) Analyzing received signal strength indication measurements for a given device (MAC) over time.
2) Determining that a device is on the move according to measurement changes.

Classifying a Suspicious Transmission as an FPV Channel

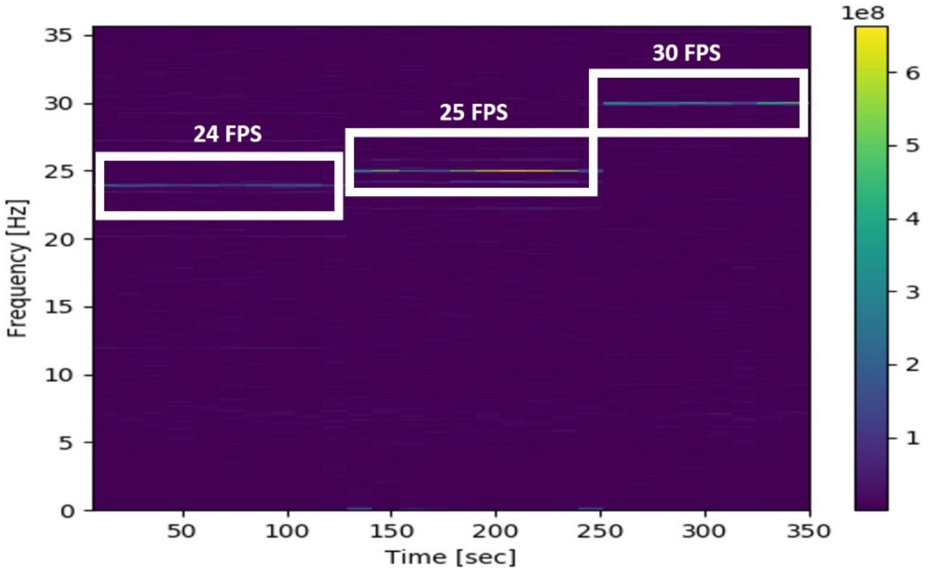
Algorithm 2 Classifying an FPV Channel

```
procedure isFpvChannel?(network,time)
    frequency = 70
    for (macAddress : network) do
        //Detecting Moving Objects
        if (isMovingObject(macAddress)) then
            bitrate[] = extractBitrateSignal(macAddress)
            fft [] = FFT(bitrateArray,frequency)
            index = frequencyWithStrongestMagnitude(fft)
            //Detecting video channel
            if (index==24 || index==25 || index==30)  then
                return true
    return false
```



We can determine whether a suspicious radio transmission is an FPV channel within 4 seconds with accuracy of 99.9%.

Detecting FPS and Resolution



FPV channel (bits per second) =
Drone to controller traffic (BPS) + Controller to drone traffic (BPS) =
Video stream + Metadata about the transmission + Maneuvering commands + Transmission's metadata =
Video stream + O(c) =
FPS x Resolution (Delta resolution) + O(c).

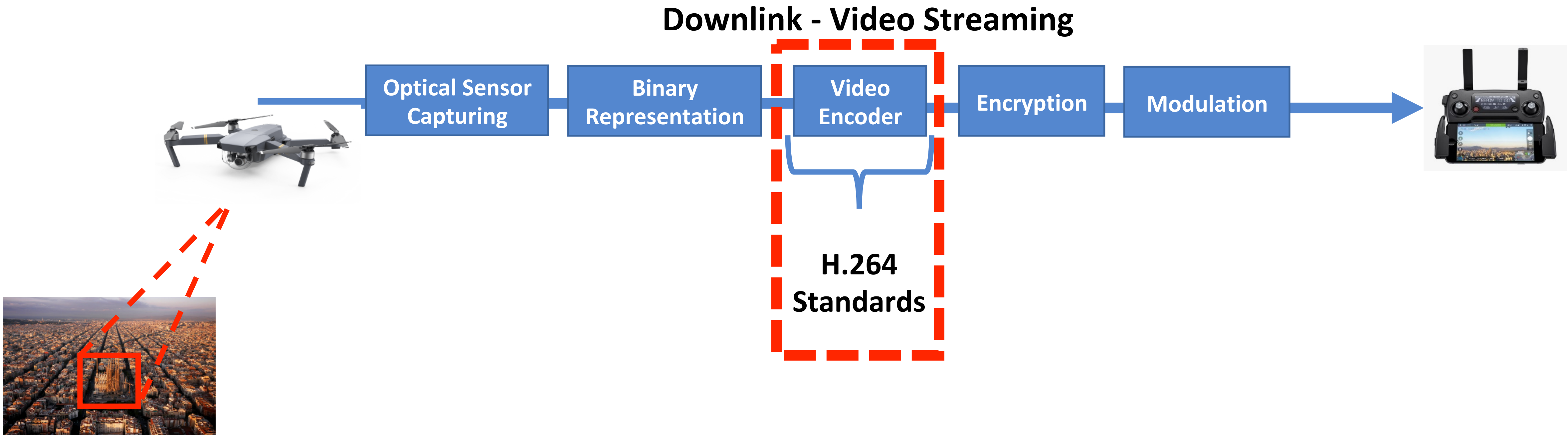
$$\text{Resolution} = \frac{\text{FPV Channel (Bits Per Second)}}{\text{FPS}}$$

By applying FFT to the intercepted bitrate signal of an FPV channel we can detect the FPS and use it to calculate the resolution by analyzing the bitrate per second.

Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting Whether an FPV Channel is Being Used to Spy on a Victim
6) Locating a Spying Drone in Space
7) Hiding the Flicker from the Drone's Operator
8) Evaluation in Real Scenarios

Video Compression Stage

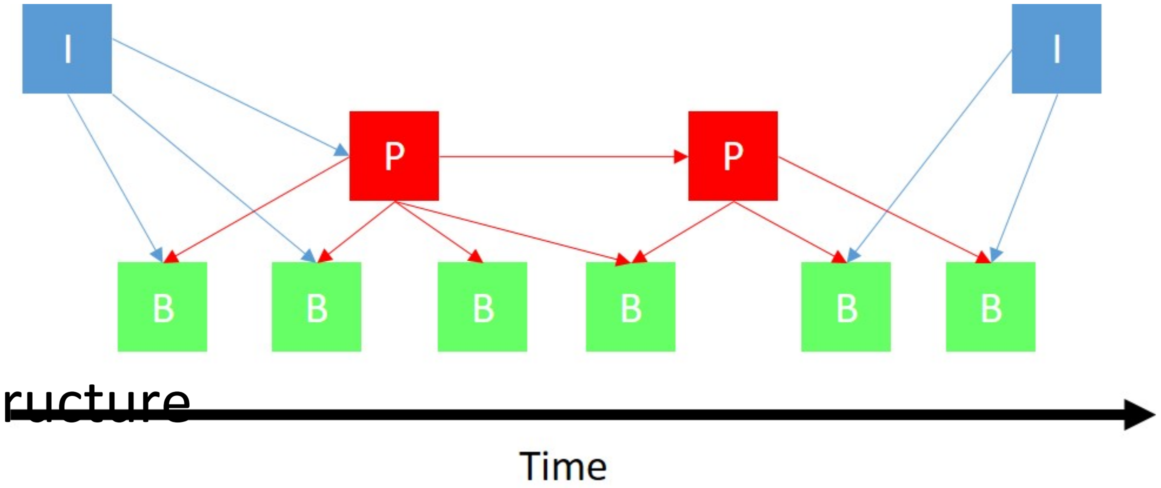


H.264 Compression Standards

Motion Compensation Algorithm

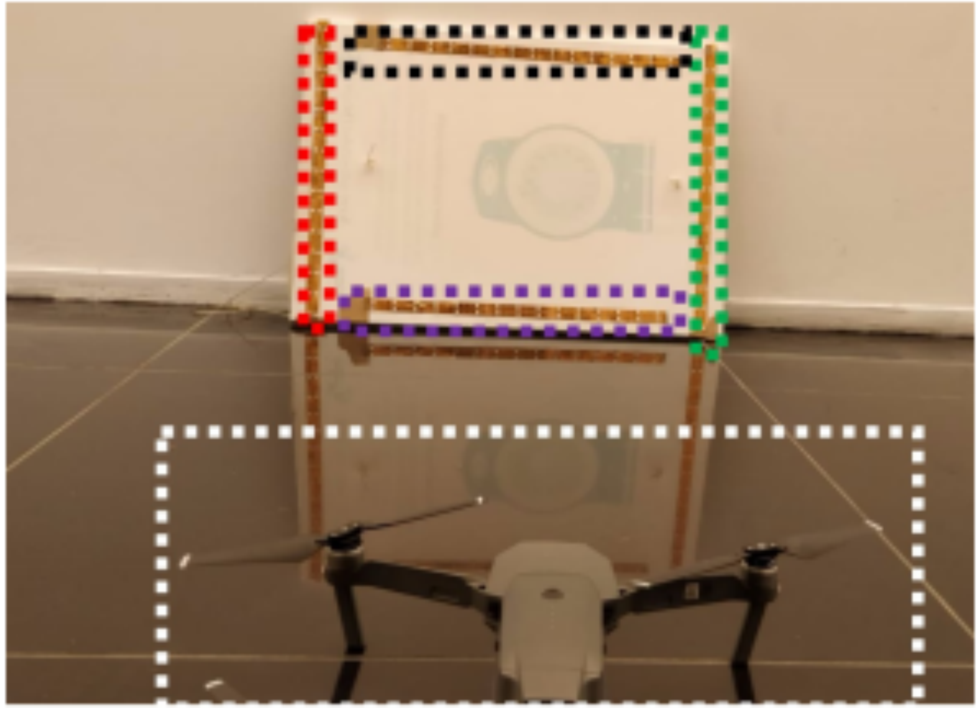
Instead of sending an entire frame, a frame is described as a delta (changes) from another frame, and this information is sent.

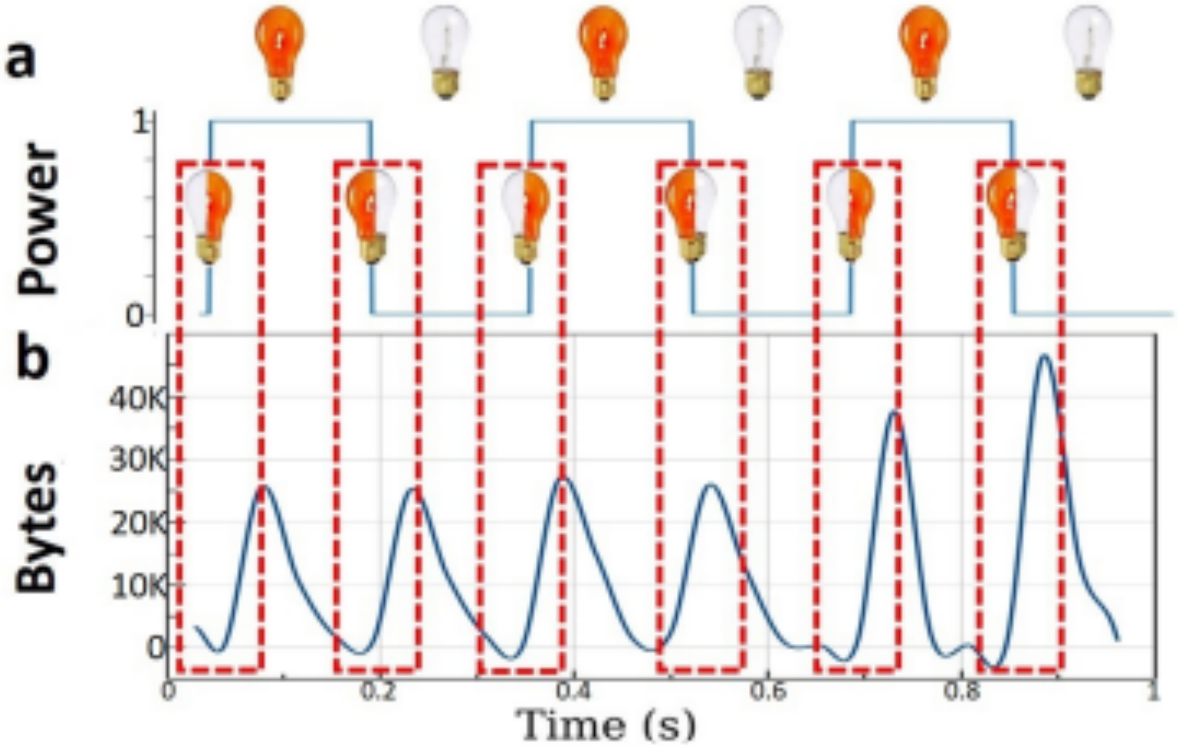
- Self-Contained Frames (I-Frames)
- Delta Frames (B-Frames and P-Frames)
- Data is sent in a GOP (group of picture) structure



The result: If there are a lot of changes between two consecutive frames, a lot of data needs to be encoded, so the delta frames are much larger comparing to delta frames of two similar consecutive frames.

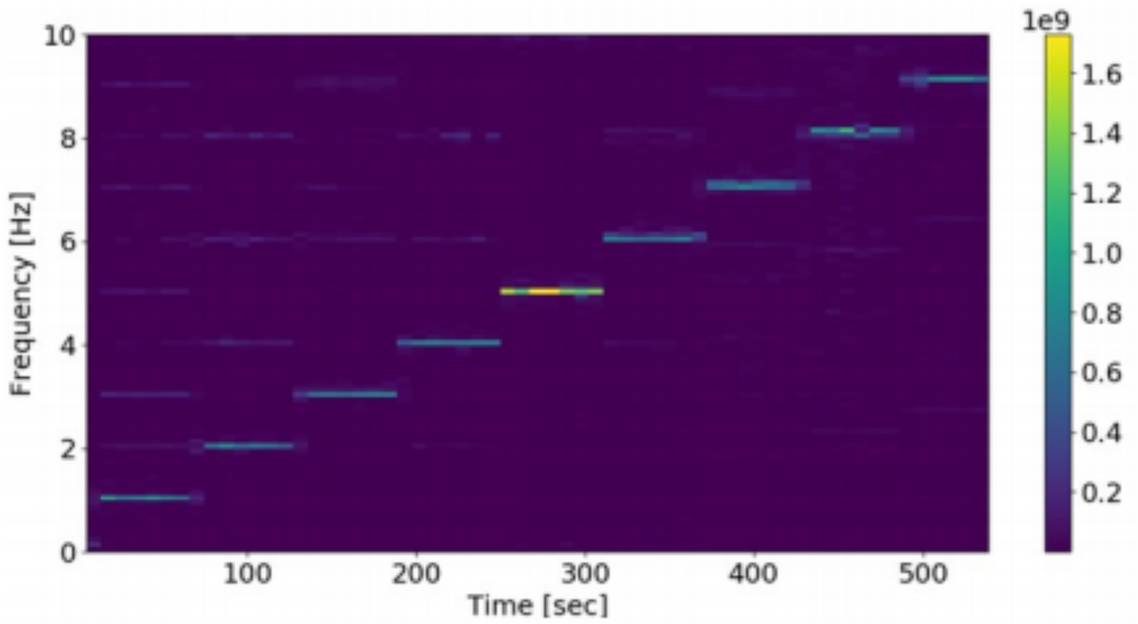
Influence of Periodic Physical Stimulus on the Frequency Domain





<u>Key Observation</u>: a 3 Hz flickering LED created 6 bursts in the intercepted bitrate signal.

Watermarking a Target Frequency



We can watermark each and every frequency of the intercepted bitrate signal using a flickering LED.

1. Detecting whether a specific POI is being streamed by a FPV channel by:
   - Launching a flicker with a frequency *f.*
   - Testing the change of magnitude of frequency *2f* of the intercepted bitrate signal in the frequency domain.

2. Frequency of maximum physical stimulus is limited to 12 Hz (because the minimal FPS rate of a commercial drone is 24 Hz)

Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting Whether an FPV Channel is Being Used to Spy on a Victim
6) Locating a Spying Drone in Space
7) Hiding the Flicker from the Drone's Operator
8) Evaluation in Real Scenarios

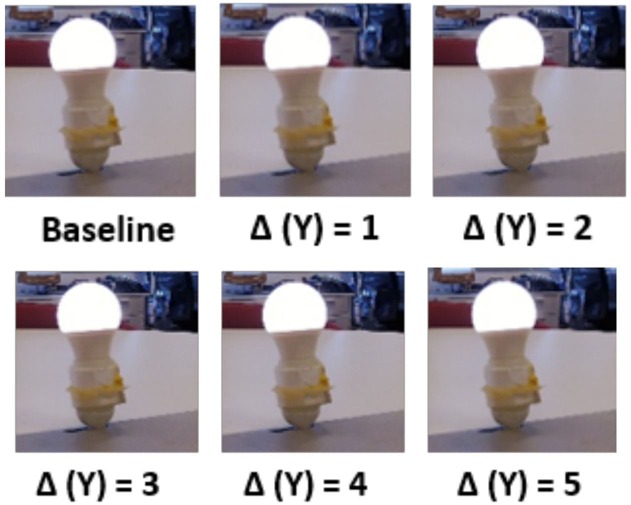
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting Whether an FPV Channel is Being Used to Spy on a Victim
6) Locating a Spying Drone in Space
7) <u>Hiding the Flicker from the Drone's Operator</u>
8) Evaluation in Real Scenarios

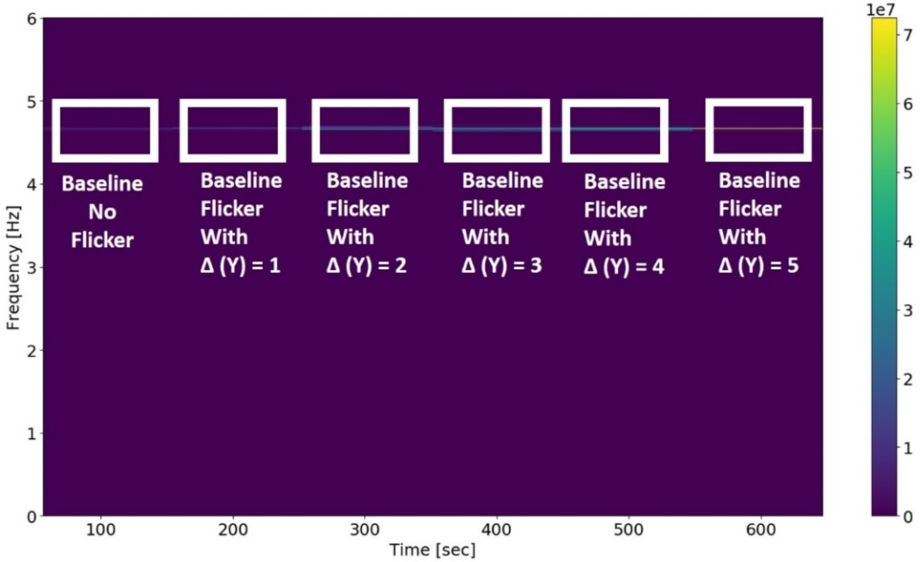
Hiding the Physical Stimulus

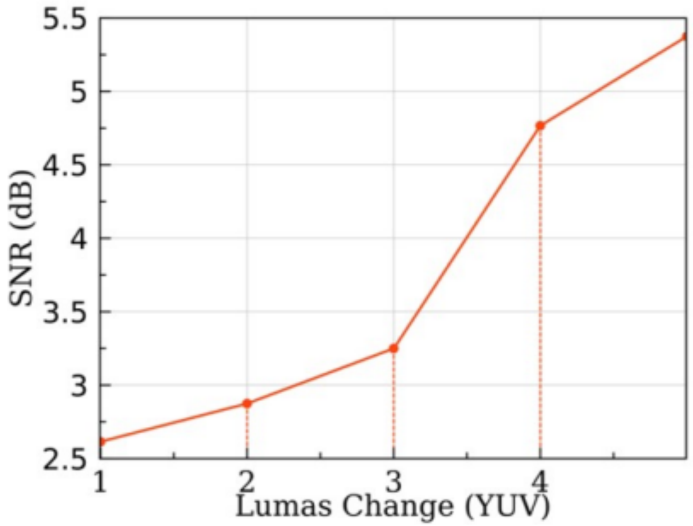
Flickering between two similar hues

a) Undetectable by direct observation ✓
b) Undetectable by indirect observation ✓
c) Watermark ✓



Luma (Δ)	YUV	RGB
Baseline	**231**,26,143	253,255,51
1	**230**,26,143	252,254,50
2	**229**,26,143	251,253,49
3	**228**,26,143	250,252,48
4	**227**,26,143	249,251,47
5	**226**,26,143	248,250,46





Optional Methods For Hiding the Physical Stimulus That Were Failed

Using an infrared projector

a) Undetectable by direct observation ✓
b) Undetectable via the controller ✗
c) Watermark ✓

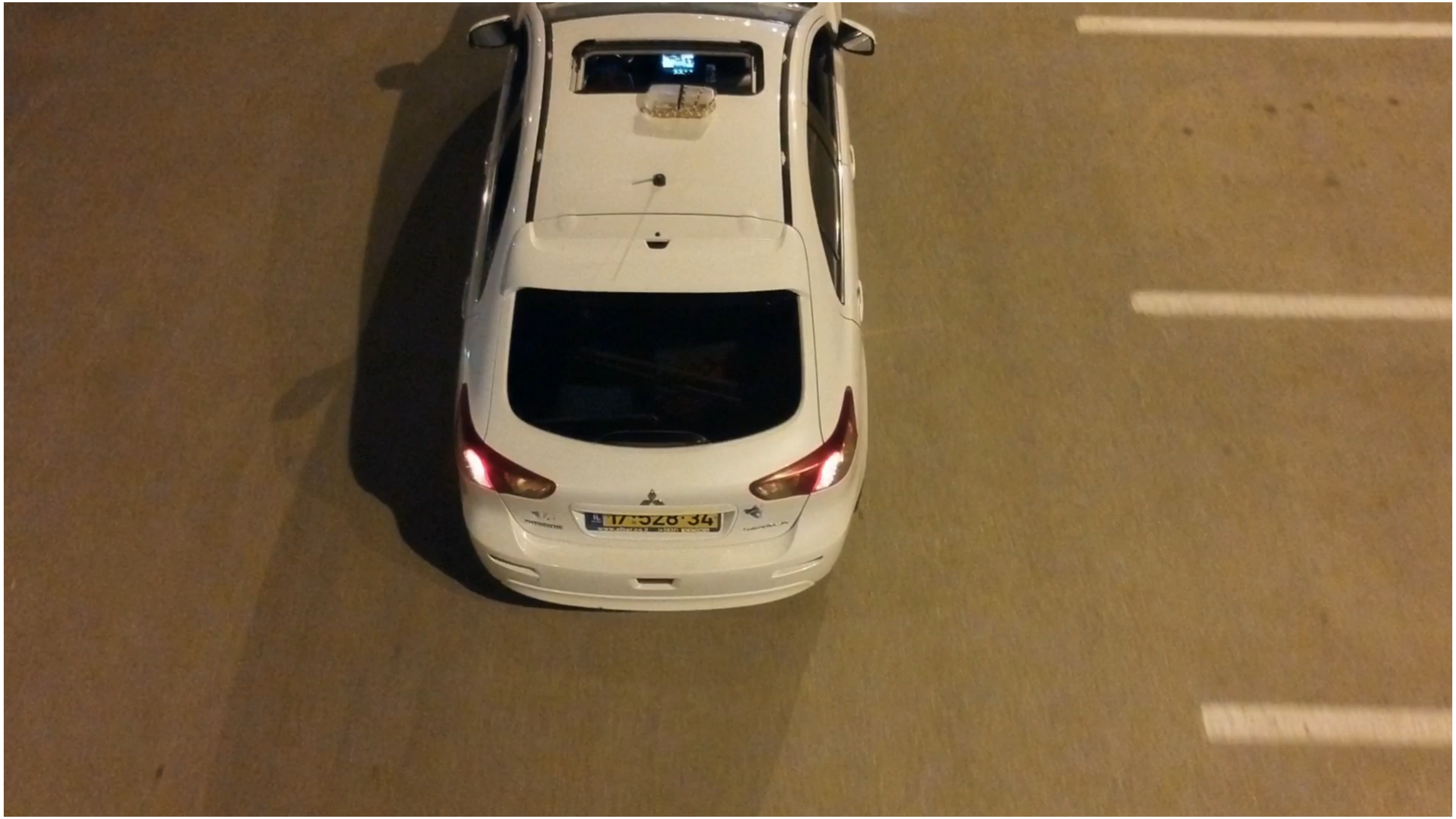
Applying the physical stimulus for a period of time that the human eye is unable to perceive (e.g., 10 milliseconds)

a) Undetectable by direct observation ✓
b) Undetectable via the controller ✗
c) Watermark ✓

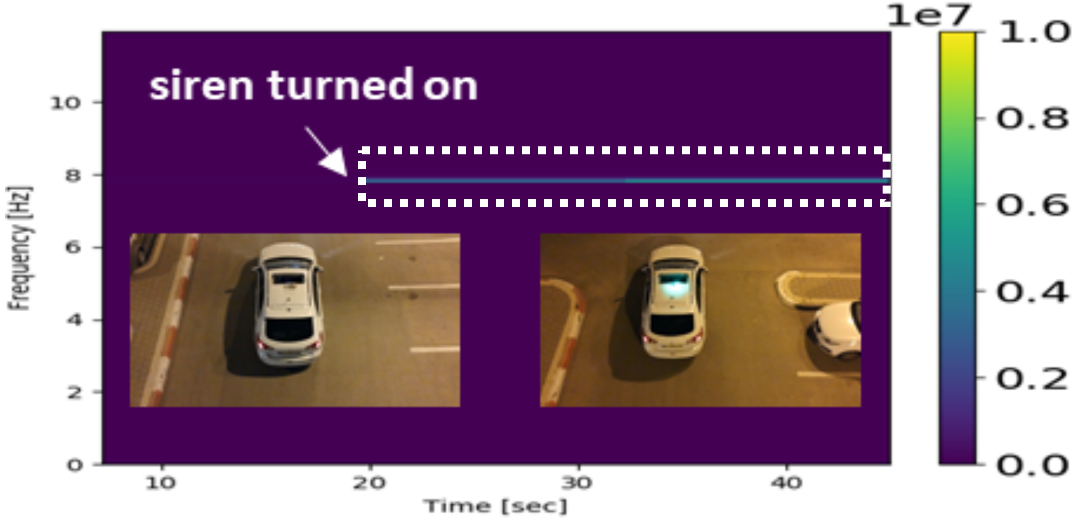
Agenda

1) Motivation
2) Detection Scheme
3) Wi-Fi FPV and Video Compression
4) FPV Channel Classification
5) Detecting Whether an FPV Channel is Being Used to Spy on a Victim
6) Locating a Spying Drone in Space
7) Hiding the Flicker from the Drone's Operator
8) Evaluation in Real Scenarios

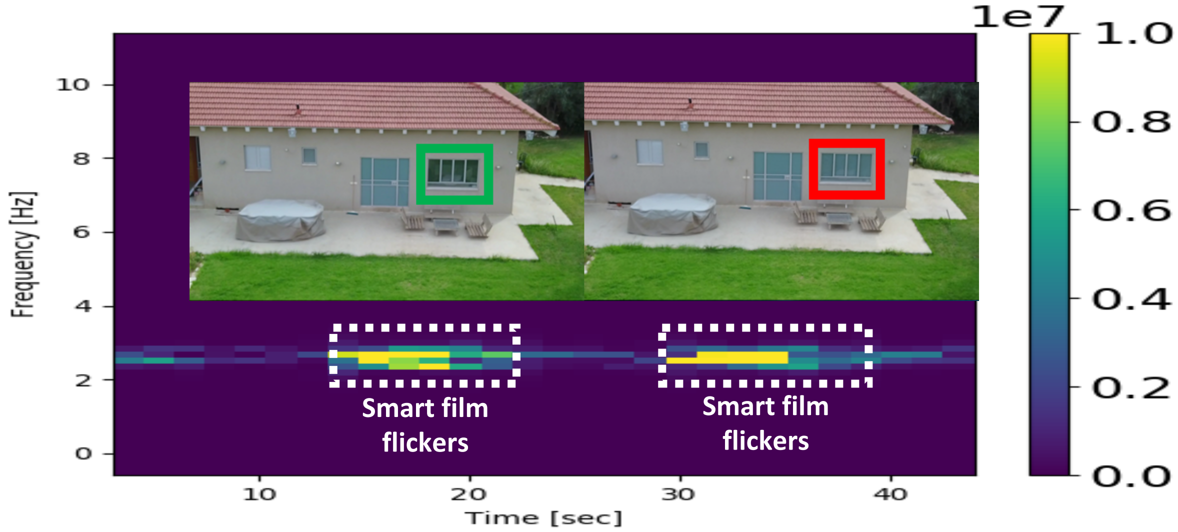
Demos



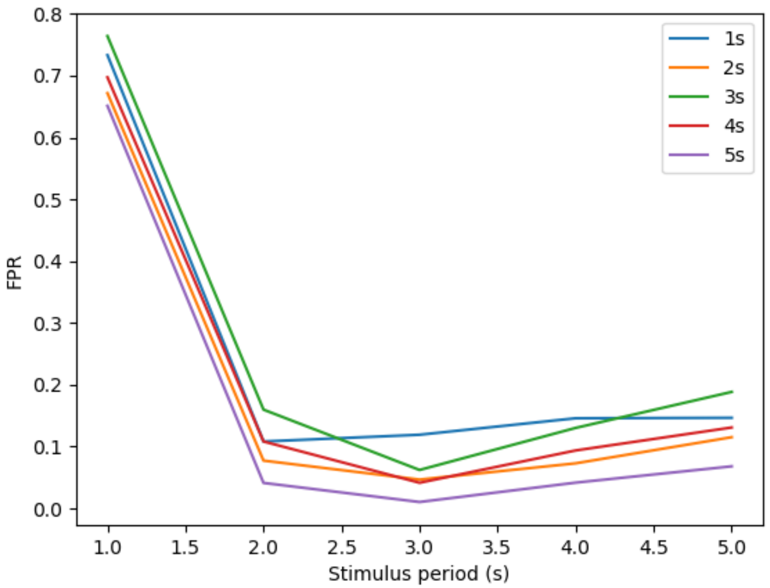
Results



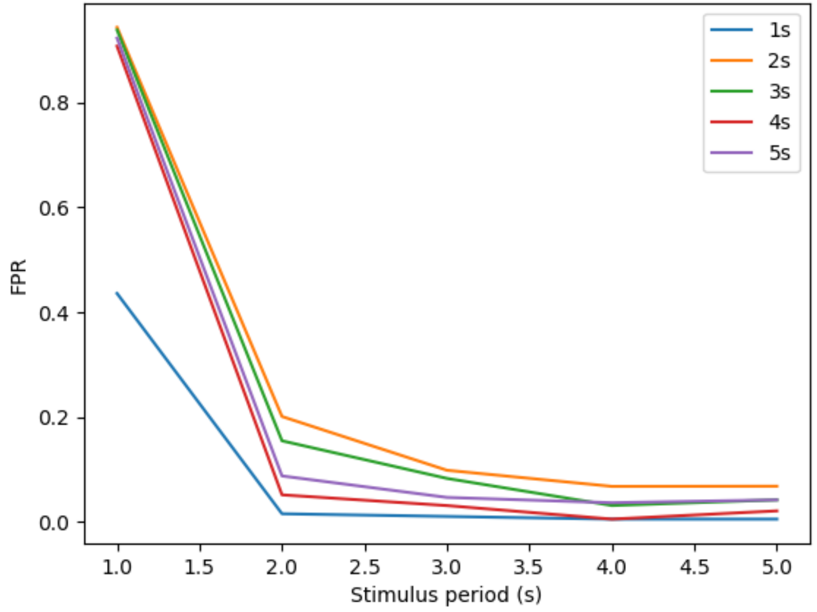
1e7
siren turned on
Frequency [Hz]
Time [sec]



1e7
Smart film flickers
Smart film flickers
Frequency [Hz]
Time [sec]



FPR
Stimulus period (s)
1s
2s
3s
4s
5s



FPR
Stimulus period (s)
1s
2s
3s
4s
5s

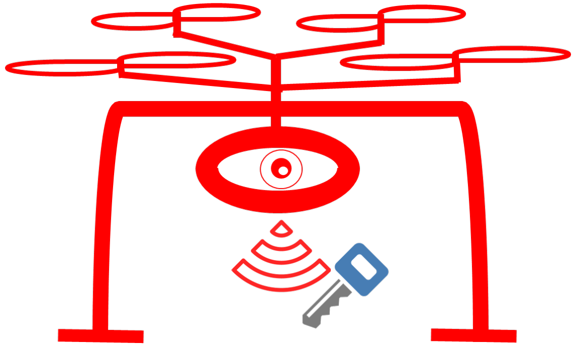
Misc

<u>Additional Information that can be found In the paper</u>:

1) Locating the spying drone in space
2) Countermeasure Methods.
3) Analysis of the Impact of Ambient Factors (Wind and Light).
4) Other Methods that we considered for hiding the flicker.
5) Exact Details of the Experiments.

<u>Others</u>: Preliminary Version of the Paper - Detecting a Privacy Invasion Attack using Time Domain Analysis – "Game of Drones", on Arxiv.

Don’t Forget: The P in IoT stands for Privacy.



@ben_nassi

My Twitter

Paper’s Website

Questions???