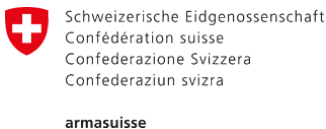
RECORD

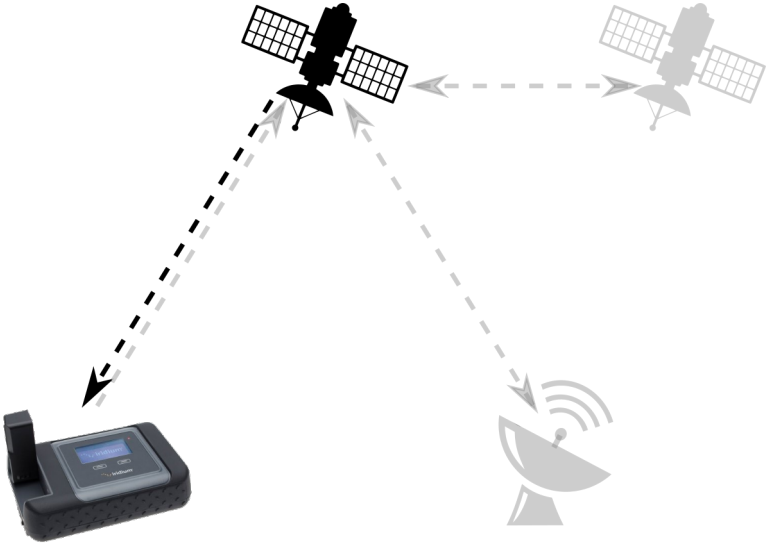
A RECeption-Only Region Determination Attack on LEO Satellite Users

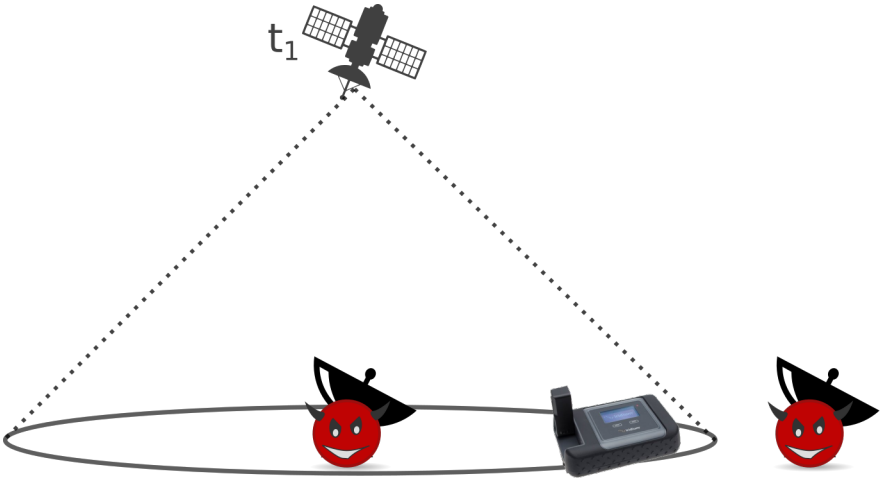
Eric Jedermann, Martin Strohmeier, Vincent Lenders, Jens Schmitt

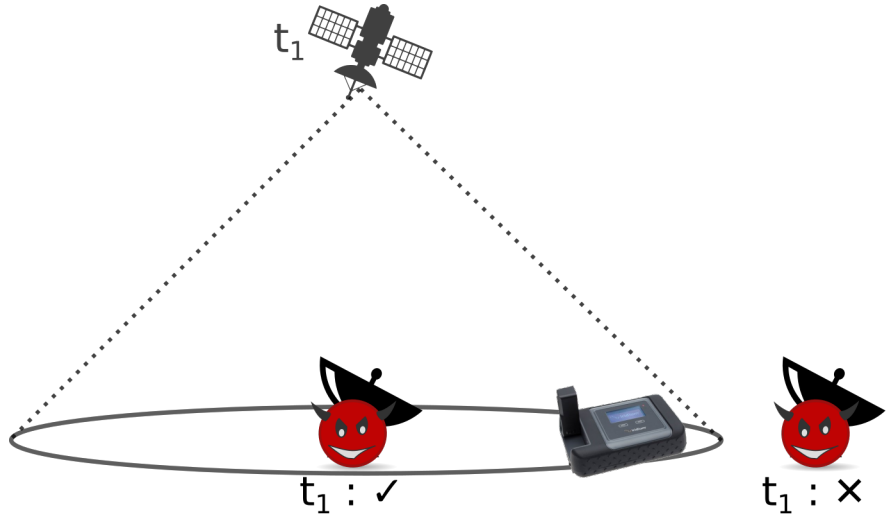
August 16th 2024

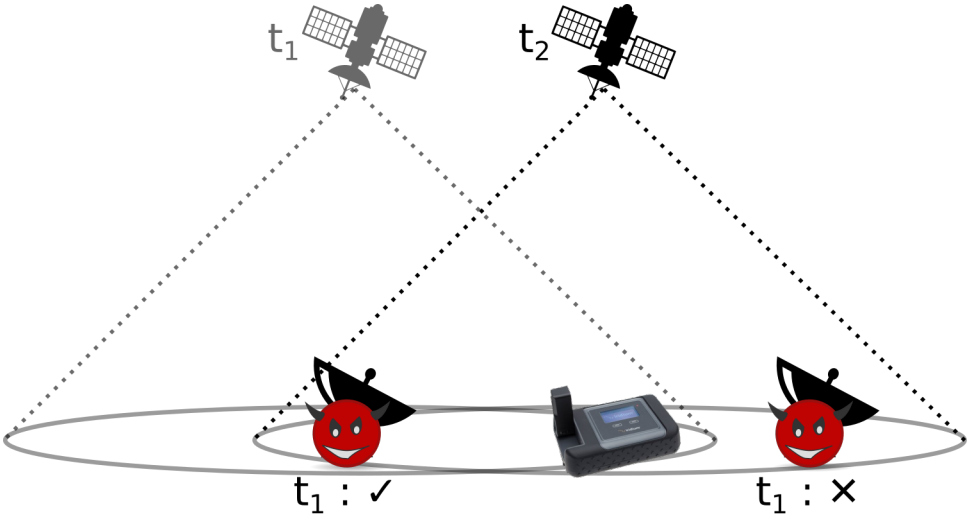


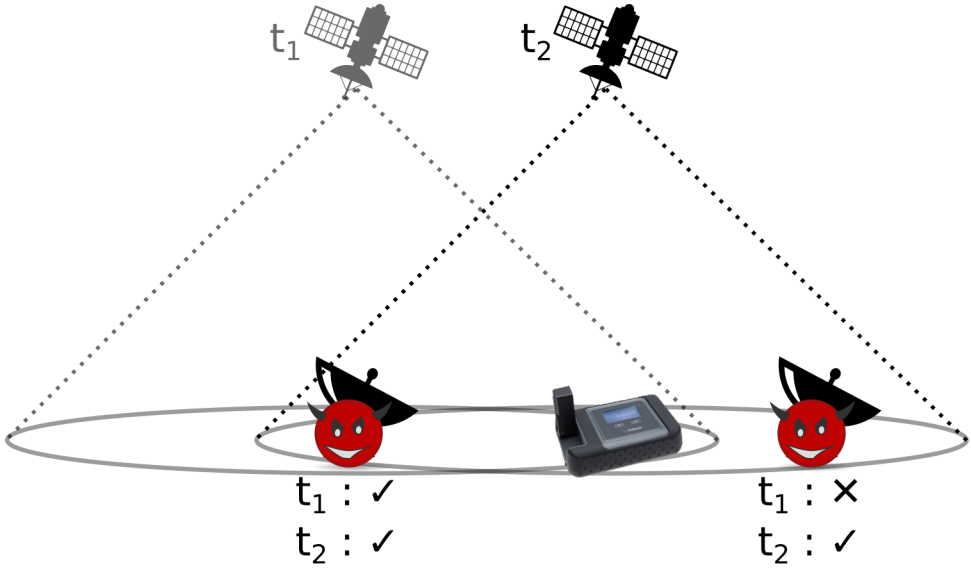
The RECORD Idea

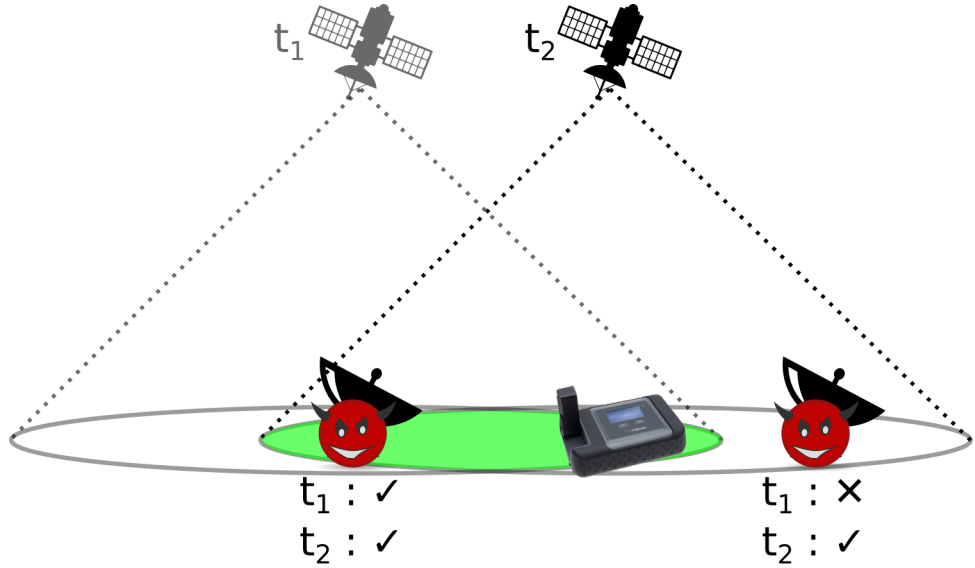


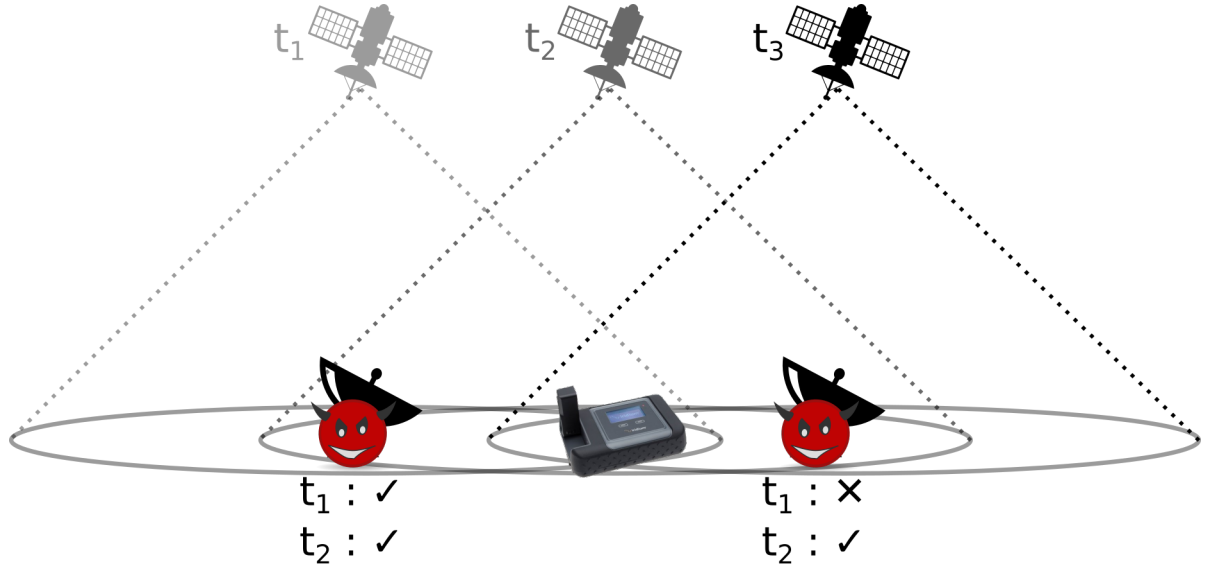

t_1

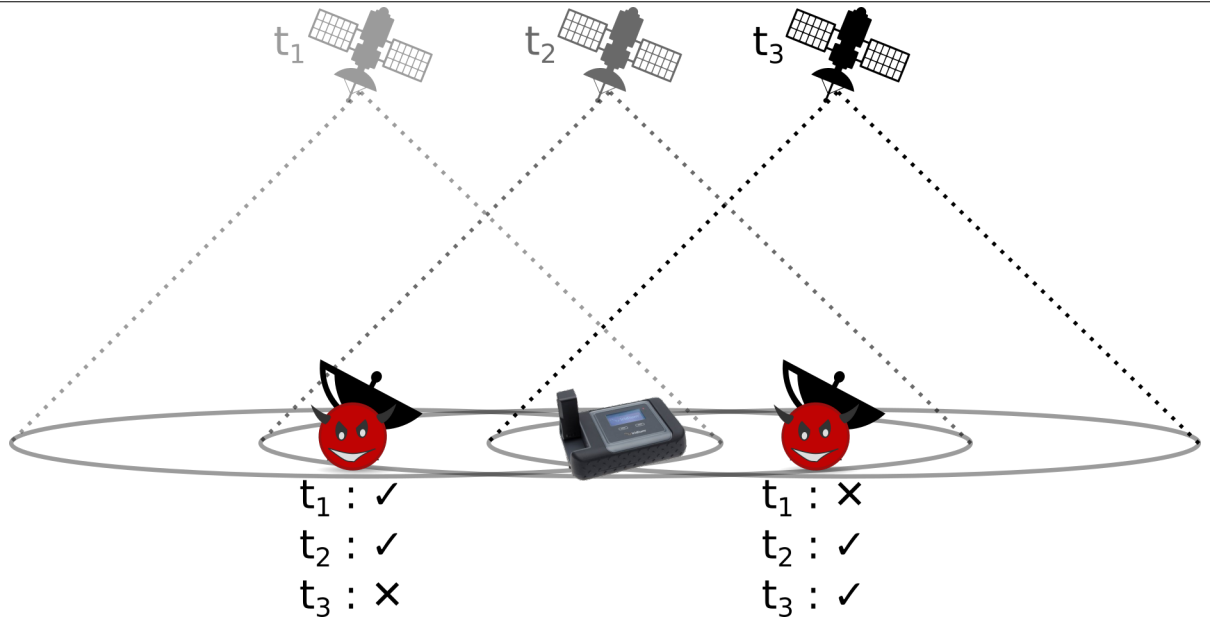

t_1
t_1 : ✓
t_1 : ×

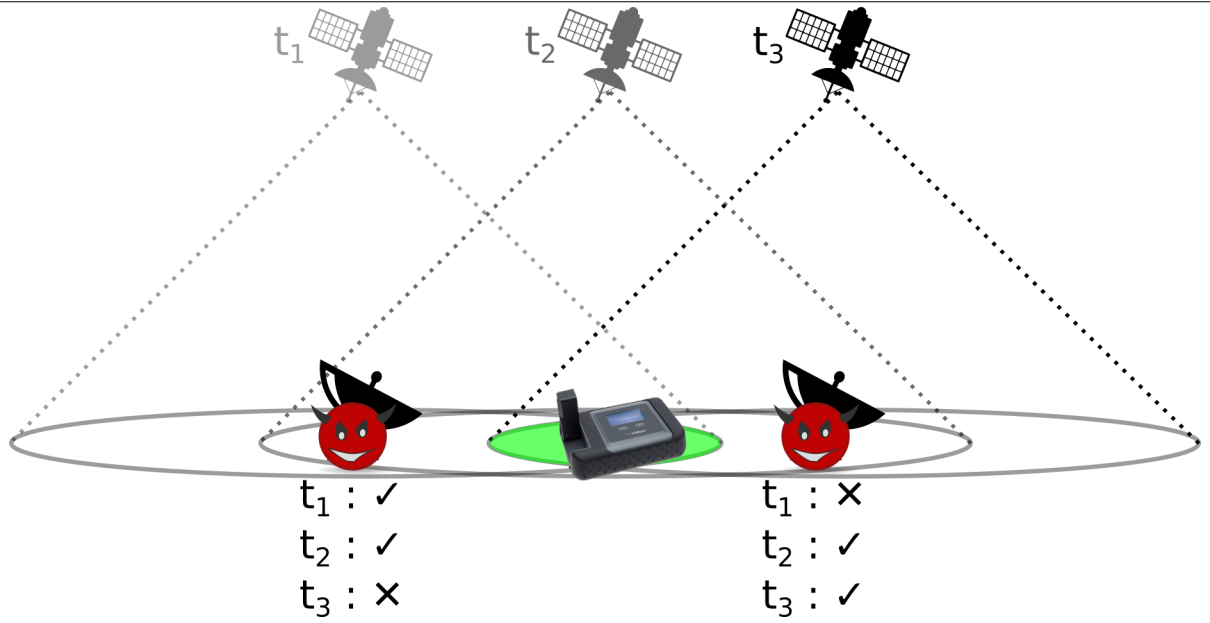

t_1
t_2
t_1 : ✓
t_1 : ✗


t_1
t_2
$t_1 : \checkmark$
$t_2 : \checkmark$
$t_1 : \times$
$t_2 : \checkmark$


t_1
t_2
$t_1 : \checkmark$
$t_2 : \checkmark$
$t_1 : \times$
$t_2 : \checkmark$


t_1
t_2
t_3
t_1 : ✓
t_2 : ✓
t_1 : ×
t_2 : ✓


t1
t2
t3
t1 : ✓
t2 : ✓
t3 : ×
t1 : ×
t2 : ✓
t3 : ✓


t1
t2
t3
t1 : ✓
t2 : ✓
t3 : ✗
t1 : ✗
t2 : ✓
t3 : ✓

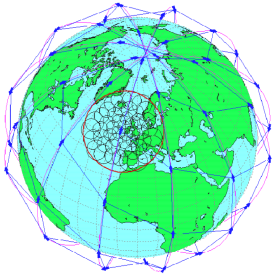
Is it possible in reality to get the region of the target device?

YES !

RECORD in Iridium

Iridium

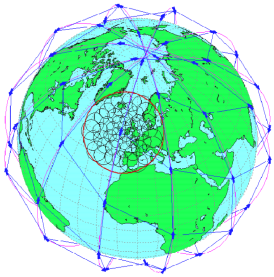
- 66 LEO satellites



src: ICAO Technical Manual For Iridium Aeronautical Mobil Satellite Service, Draft v1.0, 17 May 2006

Iridium

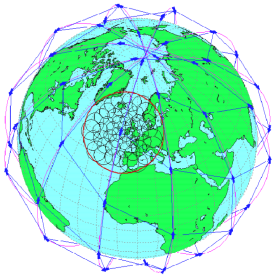
- 66 LEO satellites
- 780 km altitude



src: ICAO Technical Manual For Iridium Aeronautical Mobil Satellite Service, Draft v1.0, 17 May 2006

Iridium

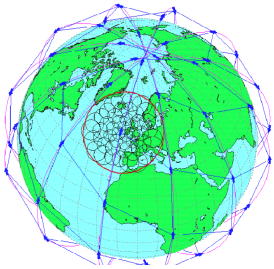
- 66 LEO satellites
- 780 km altitude
- late 1990s

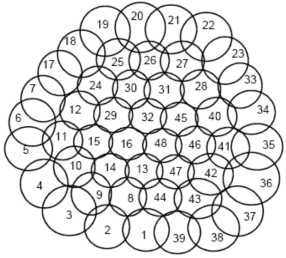


src: ICAO Technical Manual For Iridium Aeronautical Mobil Satellite Service, Draft v1.0, 17 May 2006

Iridium

- 66 LEO satellites
- 780 km altitude
- late 1990s
- 48 antennas per sat

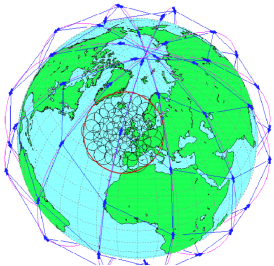


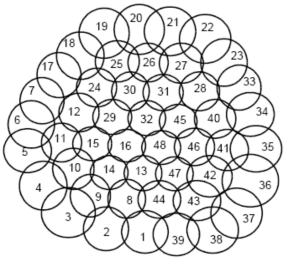


src: ICAO Technical Manual For Iridium Aeronautical Mobil Satellite Service, Draft v1.0, 17 May 2006

Iridium

- 66 LEO satellites
- 780 km altitude
- late 1990s
- 48 antennas per sat
- footprint Ø 400 - 1000 km per antenna





src: ICAO Technical Manual For Iridium Aeronautical Mobil Satellite Service, Draft v1.0, 17 May 2006

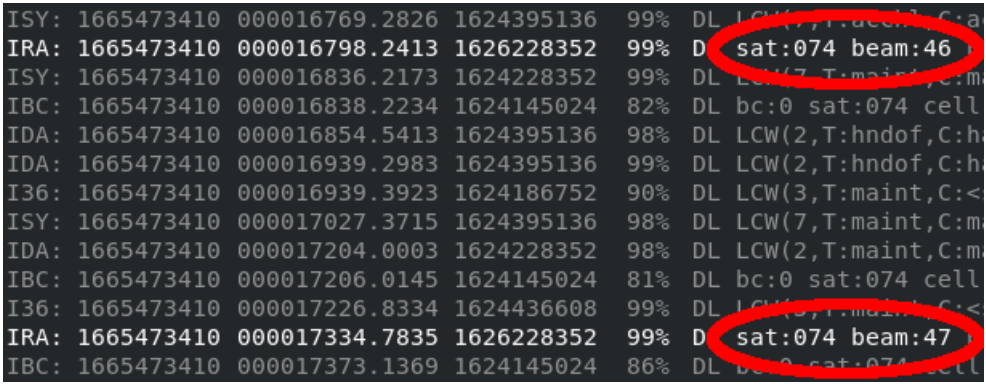
RECORD - Modeling Phase

Goal: Create a model of the satellite antenna footprints!

RECORD - Modeling Phase

Goal: Create a model of the satellite antenna footprints!

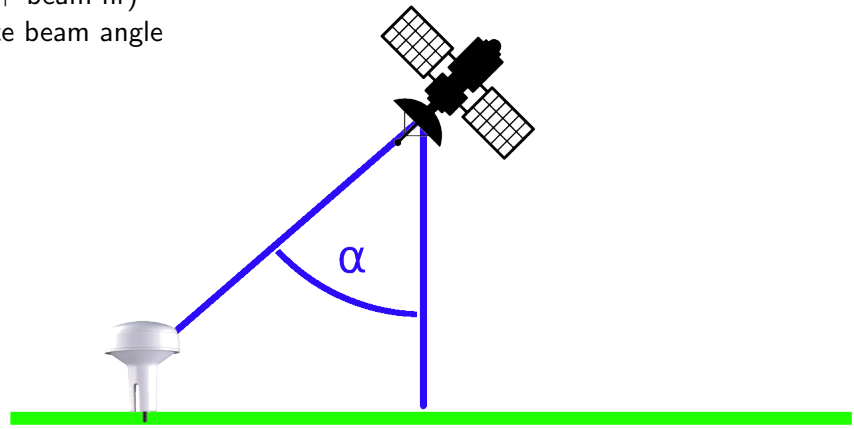
- Receive IRA
  (sat-nr + beam-nr)



RECORD - Modeling Phase

Goal: Create a model of the satellite antenna footprints!

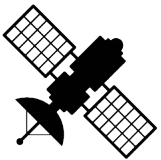
- Receive IRA
  (sat-nr + beam-nr)
- Calculate beam angle



RECORD - Modeling Phase

Goal: Create a model of the satellite antenna footprints!

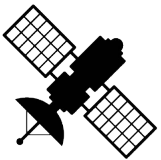
- Receive IRA
  (sat-nr + beam-nr)
- Calculate beam angle



RECORD - Modeling Phase

Goal: Create a model of the satellite antenna footprints!

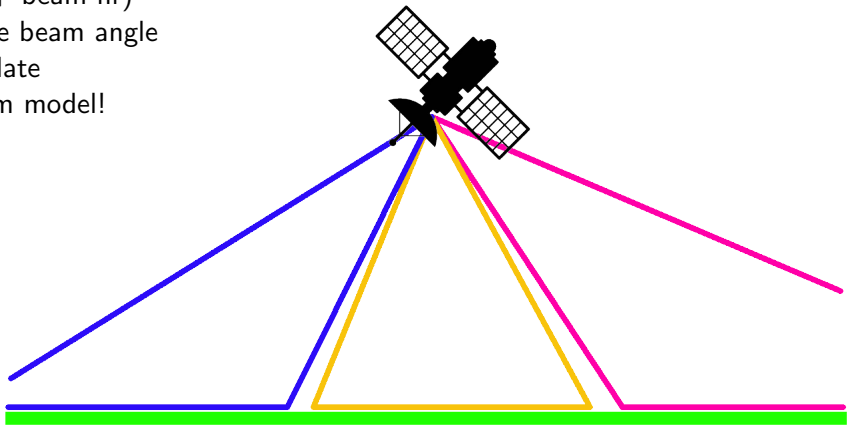
- Receive IRA
  (sat-nr + beam-nr)
- Calculate beam angle
- Accumulate



RECORD - Modeling Phase

Goal: Create a model of the satellite antenna footprints!

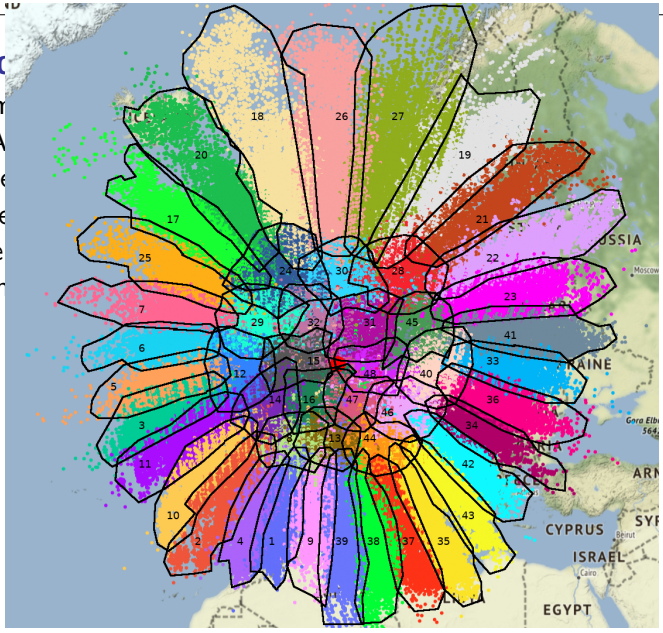
- Receive IRA
  (sat-nr + beam-nr)
- Calculate beam angle
- Accumulate
- Sat beam model!



RECORD - Mo

Goal: Create a m

- Receive IRA
  (sat-nr + be
- Calculate be
- Accumulate
- Sat beam m



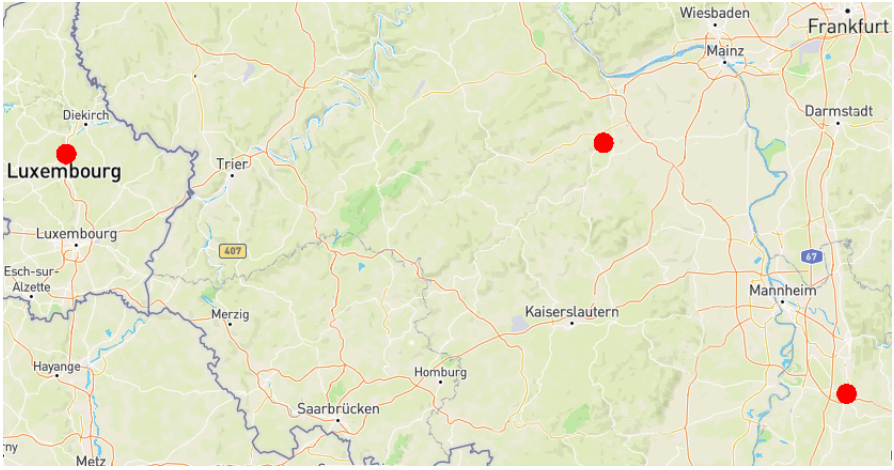
RECORD - Collection Phase

Goal: Collect information about the target!

RECORD - Collection Phase

Goal: Collect information about the target!

- Place observers



RECORD - Collection Phase

Goal: Collect information about the target!

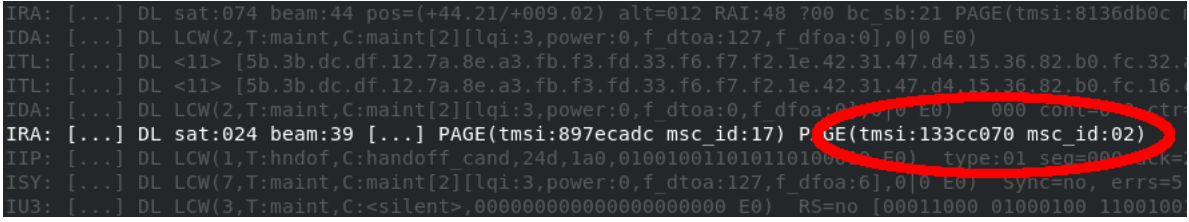
- Place observers
- Eavesdrop on return-downlink

```
eric@erics-ThinkPad:~/Iridium/gr-iridium$ iridium-extractor -D 4 examples/hackrf.conf > output_usenix.bits
gr-osmosdr 0.2.0.0 (0.2.0) gnuradio 3.8.2.0
built-in source types: file rtl_tcp uhd hackrf rfspace redpitaya
[INFO] [UHD] linux; GNU C++ version 8.3.0; Boost_106501; UHD_3.11.0.HEAD-0-ga1b5c4ae
Using HackRF One with firmware 2021.03.1
(RF) Gain: 14.0 (Requested 14)
IF Gain: 40.0 (Requested 40)
BB Gain: 20.0 (Requested 20)
Warning: Setting antenna to TX/RX
1722001950 | i:   0/s | i_avg:   0/s | ok:   0% | ok:   0/s | ok_avg:   0% | ok:        0 | ok_avg:   0/s
Bandwidth: 10000000.0 (Requested 10000000)
1722001951 | i:  17/s | i_avg:   4/s | ok:  72% | ok:  12/s | ok_avg:  72% | ok:       13 | ok_avg:   3/s
WARNING: your SDR seems to be losing samples. ~381k samples lost (3%)
1722001952 | i: 103/s | i_avg:  23/s | ok:  73% | ok:  75/s | ok_avg:  72% | ok:       89 | ok_avg:  17/s
1722001953 | i:  78/s | i_avg:  32/s | ok:  68% | ok:  53/s | ok_avg:  71% | ok:      143 | ok_avg:  23/s
1722001954 | i: 100/s | i_avg:  41/s | ok:  67% | ok:  67/s | ok_avg:  69% | ok:      211 | ok_avg:  29/s
1722001955 | i:  90/s | i_avg:  47/s | ok:  76% | ok:  69/s | ok_avg:  71% | ok:      281 | ok_avg:  34/s
1722001956 | i:  67/s | i_avg:  50/s | ok:  75% | ok:  50/s | ok_avg:  72% | ok:      332 | ok_avg:  36/s
1722001957 | i:  85/s | i_avg:  53/s | ok:  65% | ok:  55/s | ok_avg:  70% | ok:      388 | ok_avg:  37/s
1722001958 | i:  69/s | i_avg:  55/s | ok:  70% | ok:  48/s | ok_avg:  70% | ok:      437 | ok_avg:  38/s
1722001959 | i:  78/s | i_avg:  56/s | ok:  67% | ok:  52/s | ok_avg:  70% | ok:      490 | ok_avg:  40/s
1722001960 | i:  90/s | i_avg:  59/s | ok:  64% | ok:  58/s | ok_avg:  69% | ok:      549 | ok_avg:  41/s
1722001961 | i: 109/s | i_avg:  63/s | ok:  58% | ok:  63/s | ok_avg:  68% | ok:      613 | ok_avg:  43/s
1722001962 | i:  90/s | i_avg:  64/s | ok:  59% | ok:  53/s | ok_avg:  67% | ok:      667 | ok_avg:  43/s
1722001963 | i:  92/s | i_avg:  66/s | ok:  58% | ok:  53/s | ok_avg:  66% | ok:      721 | ok_avg:  44/s
1722001964 | i: 124/s | i_avg:  70/s | ok:  72% | ok:  89/s | ok_avg:  67% | ok:      811 | ok_avg:  47/s
```

RECORD - Collection Phase

Goal: Collect information about the target!

- Place observers
- Eavesdrop on return-downlink
- Identify target traffic



RECORD - Collection Phase

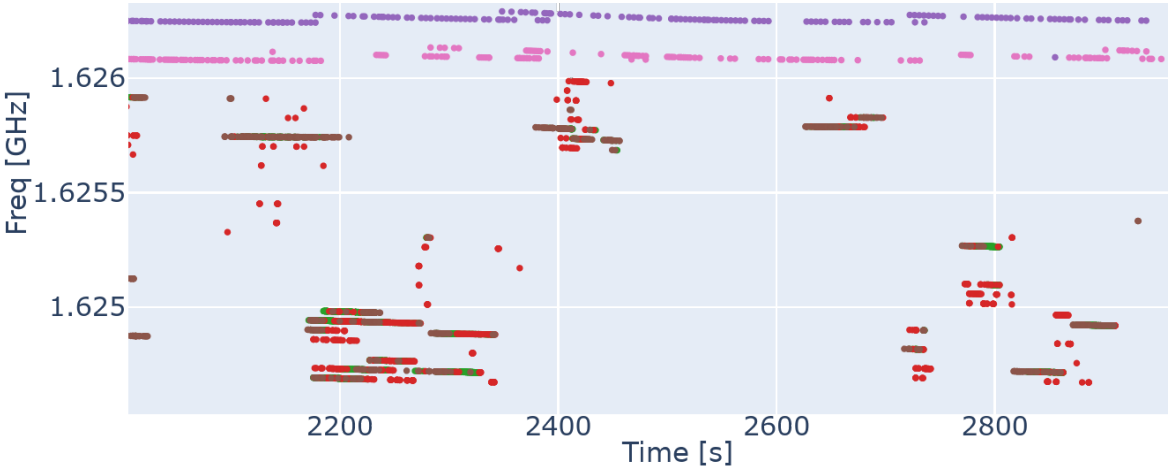
Goal: Collect information about the target!

- Place observers
- Eavesdrop on return-downlink
- Identify target traffic
- Extract events

RECORD - Collection Phase

Goal: Collect information about the target!

- Place observers



RECORD - Estimation Phase

Goal: Calculate the targets region!

RECORD - Estimation Phase

Goal: Calculate the targets region!

- Combine events and sat beam model

RECORD - Estimation Phase

Goal: Calculate the targets region!

- Combine events and sat beam model
- Calculate RoI per event

Observer
RoI
Target

RECORD - Estimation Phase

Goal: Calculate the targets region!

- Combine events and sat beam model
- Calculate RoI per event

Observer
RoI
Target

RECORD - Estimation Phase

Goal: Calculate the targets region!

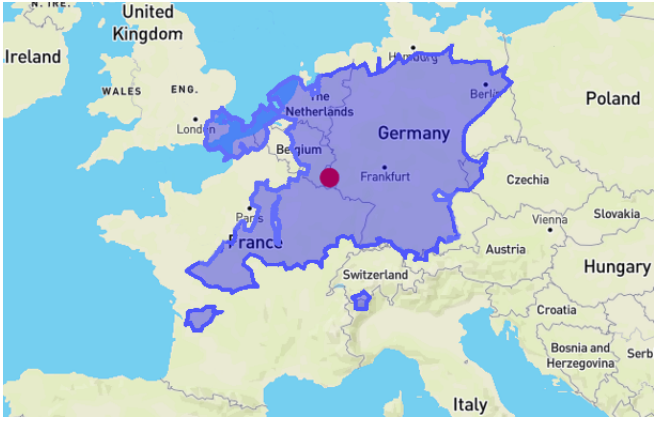
- Combine events and sat beam model
- Calculate RoI per event
- Intersect RoIs

Observer
RoI
Target

RECORD - Estimation Phase

Goal: Calculate the targets region!

- Combine events and sat beam model
- Calculate RoI per event
- Intersect RoIs



Observer
RoI
Target

RECORD - Estimation Phase

Goal: Calculate the targets region!

- Combine events and sat beam model
- Calculate RoI per event
- Intersect RoIs
  - of all events

Observer
RoI
Target

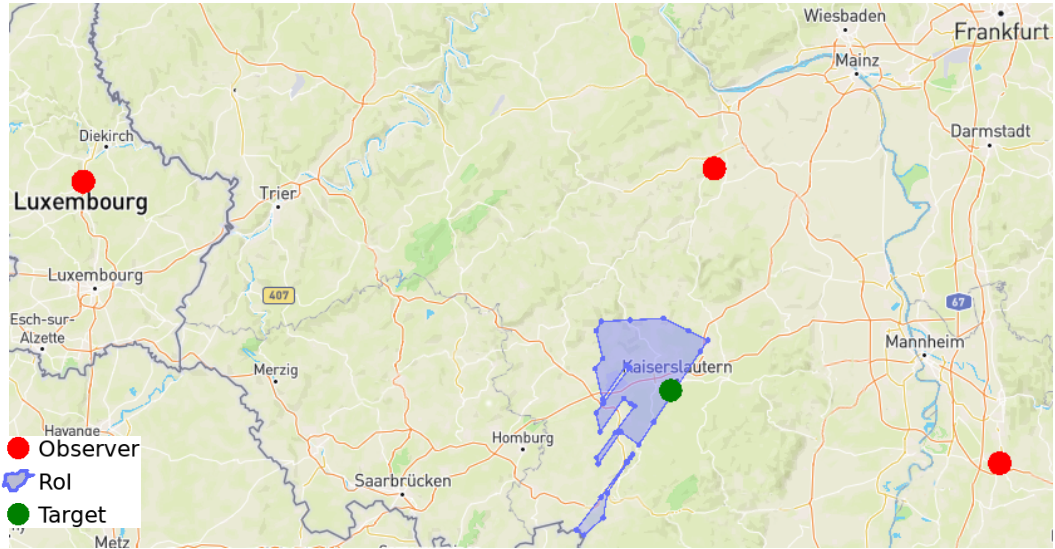
RECORD - Estimation Phase

Goal: Calculate the targets region!

- Combine events and sat beam model
- Calculate RoI per event
- Intersect RoIs
  - of all events
  - of all observers

Observer
RoI
Target

RECORD - Estimation Phase (3 observers + 2 hours recording = 383 km^2)



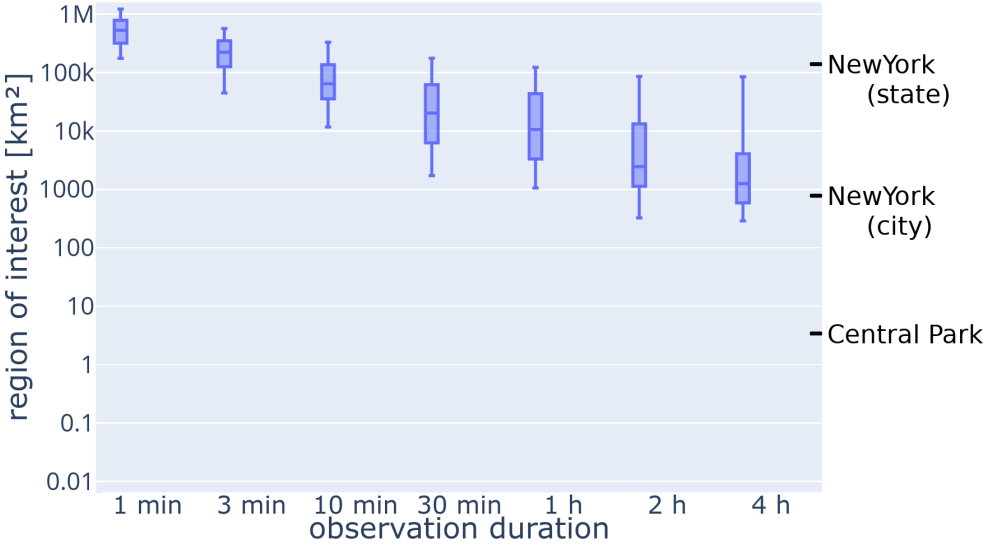
RECORD Simulation

- Code & results available online:
  https://github.com/ErJedermann/RECORD.git

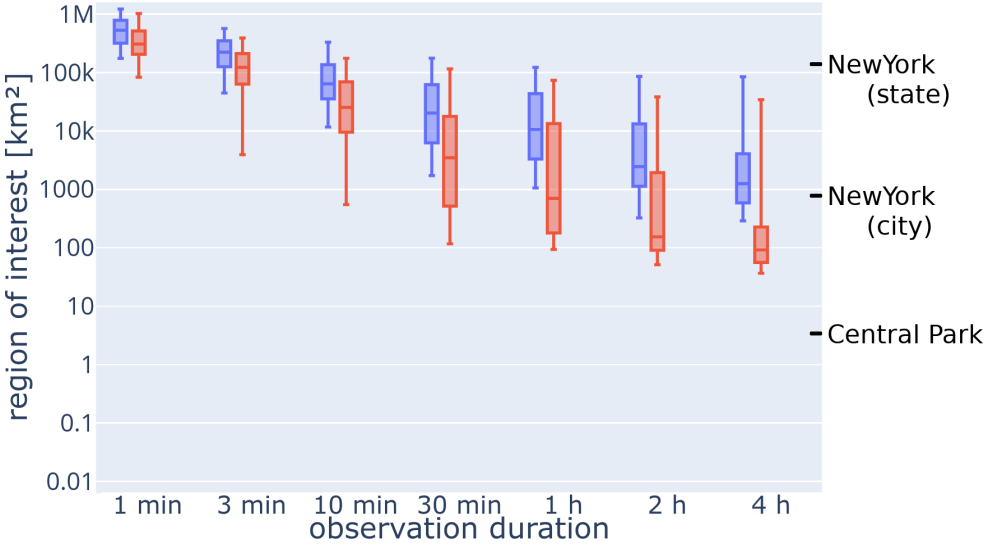
- Code & results available online:
  https://github.com/ErJedermann/RECORD.git

- Why simulations?

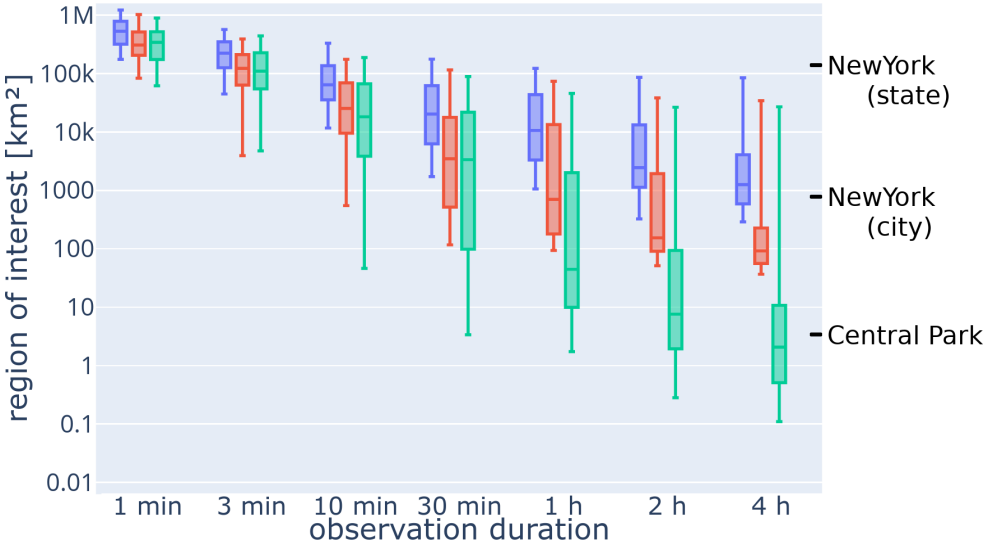
Parameter 1: Time



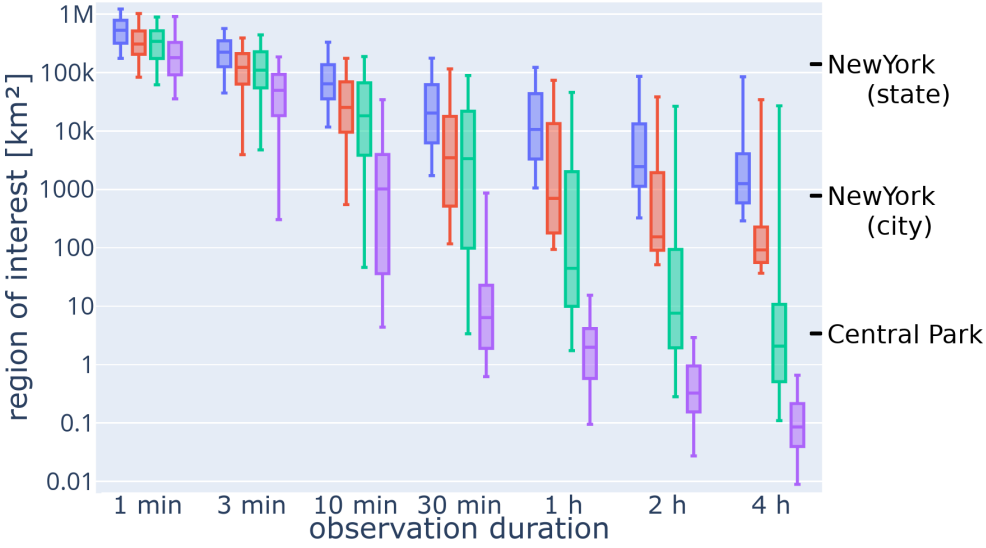
Parameter 2: Resources (3 observers)



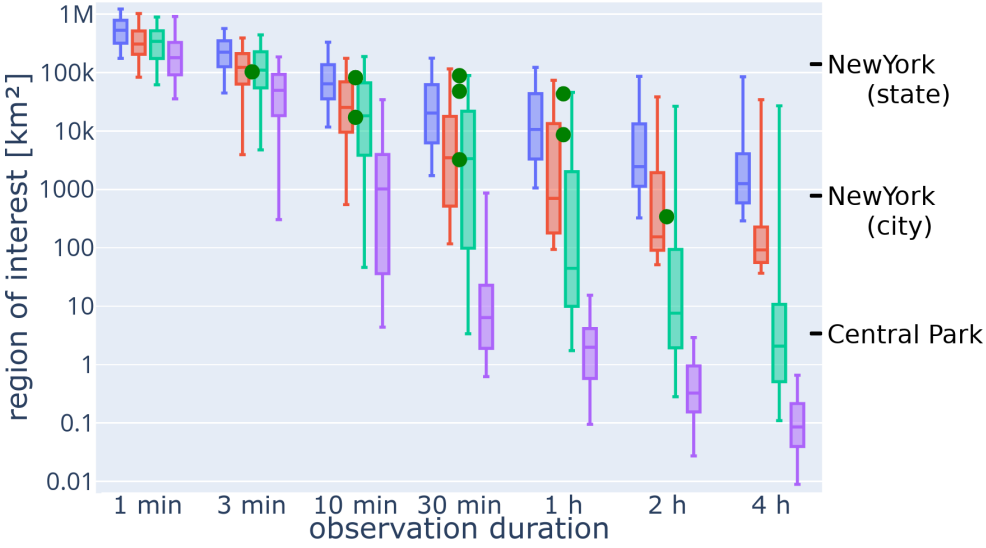
Parameter 3: Beam-Model Precision



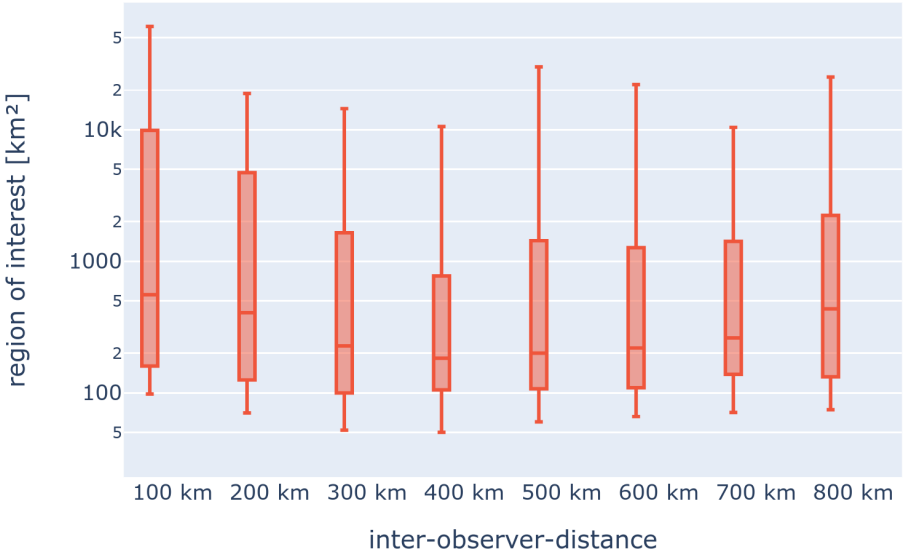
Parameter 4: Attack Intelligence



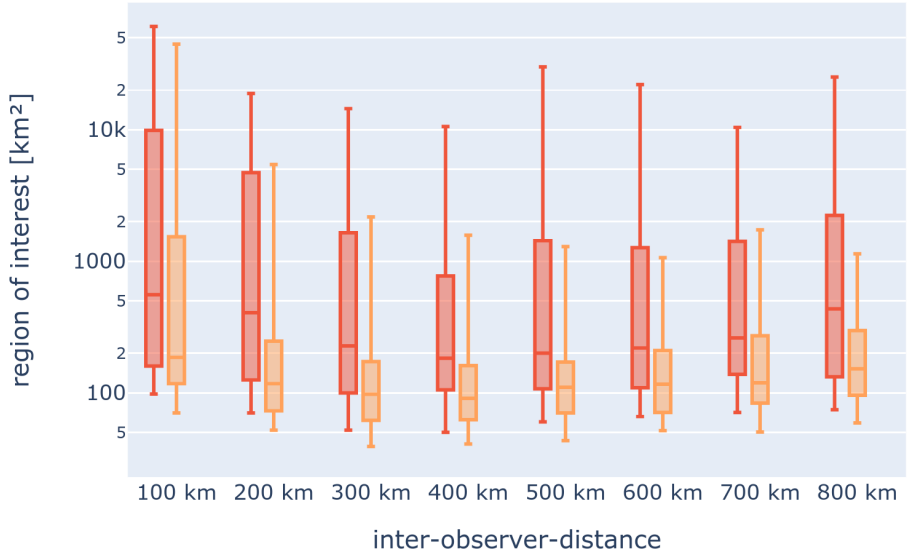
Real World vs Simulation



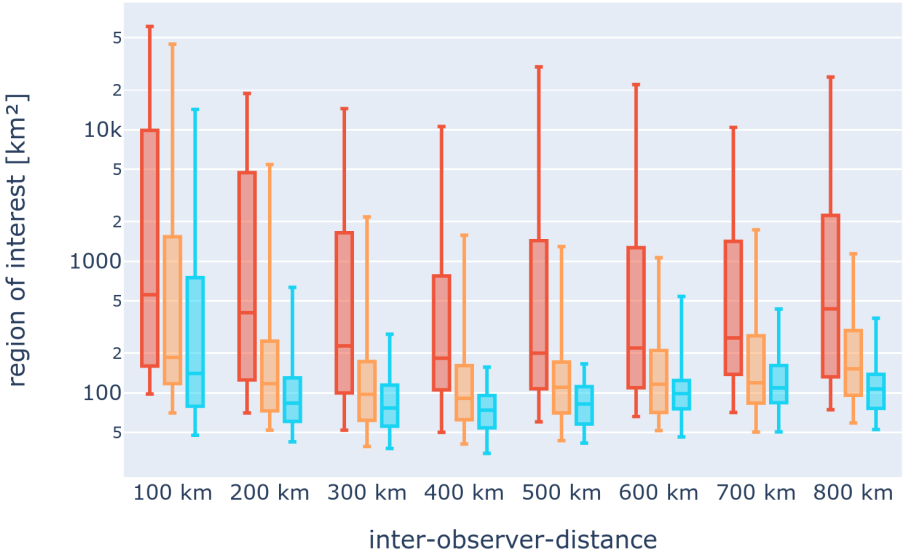
Parameter 5: distances between 3 observers



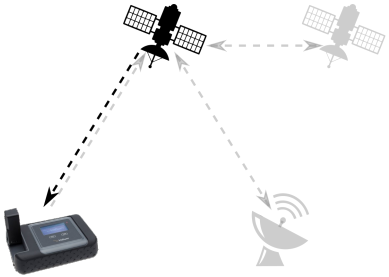
Parameter 5: distances between 6 observers

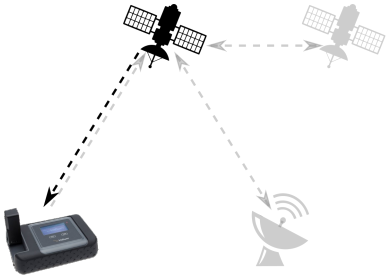


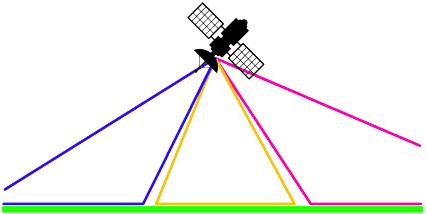
Parameter 5: distances between 12 observers

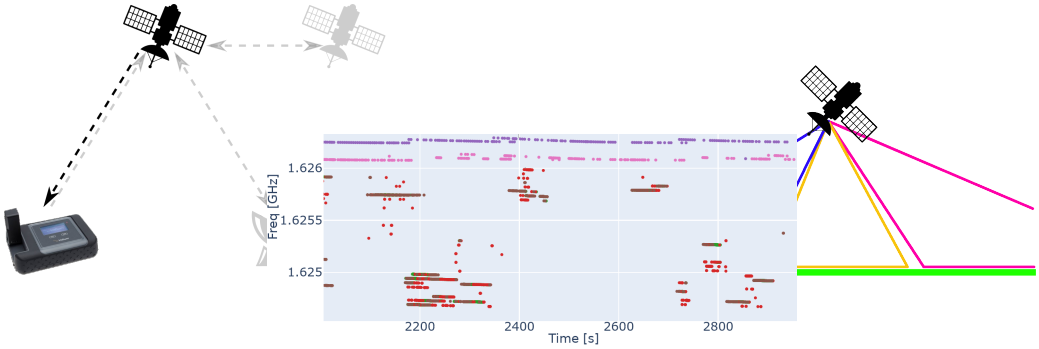


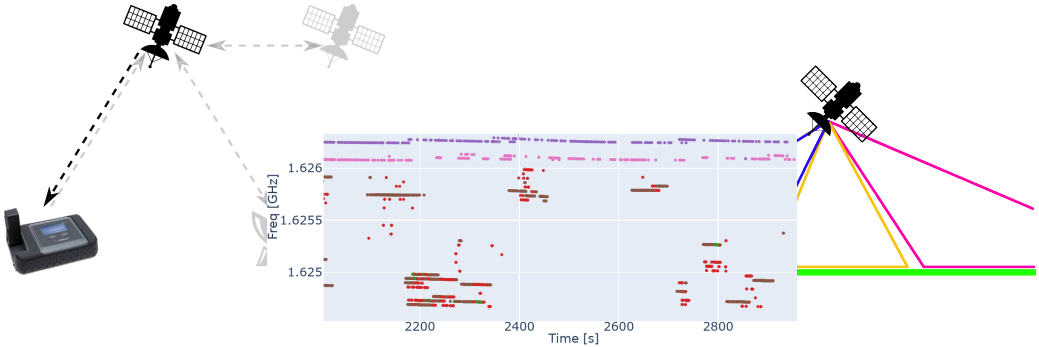
Summary



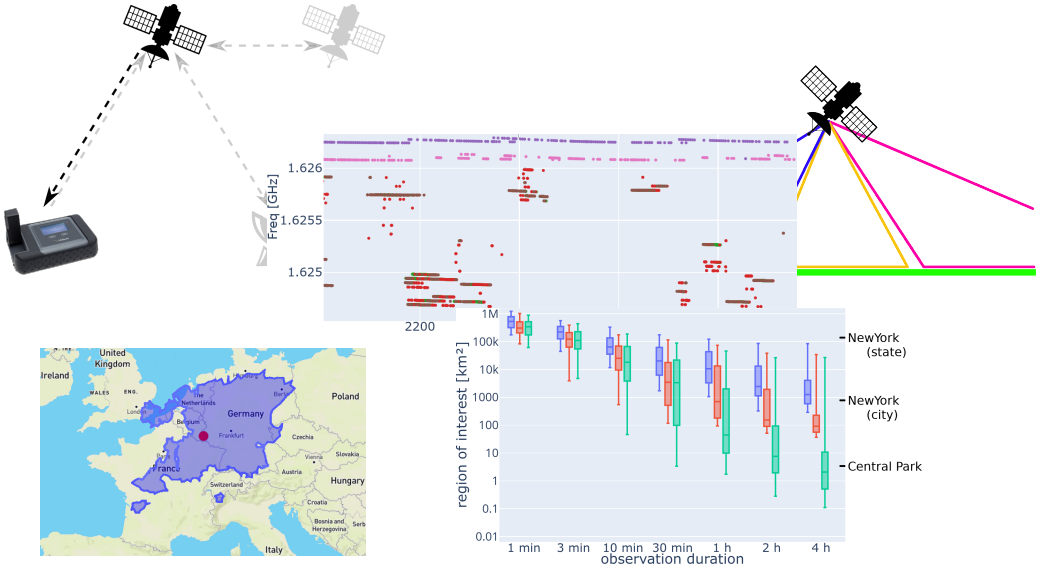





Freq [GHz]
1.626
1.6255
1.625
2200
2400
2600
2800
Time [s]


Freq [GHz]
1.626
1.6255
1.625
2200
2400
2600
2800
Time [s]


United Kingdom
Ireland
WALES
ENG.
The Netherlands
Belgium
Germany
Frankfurt
Poland
Czechia
Slovakia
Vienna
Austria
Hungary
France
Switzerland
Croatia
Bosnia and Herzegovina
Italy


Freq [GHz]
1.626
1.6255
1.625
2200
United Kingdom
Ireland
Poland
Germany
Belgium
Frankfurt
Czechia
Slovakia
Austria
Hungary
Switzerland
Croatia
Italy
region of interest [km²]
1M
100k
10k
1000
100
10
1
0.1
0.01
1 min
3 min
10 min
30 min
1 h
2 h
4 h
observation duration
NewYork (state)
NewYork (city)
Central Park


ANY QUESTIONS?
IF NOT, JUST CLAP
imgflip.com