NS2 Network and System Security Laboratory KAIST

RECORD: A *REC*eption-*O*nly *R*egion *D*etermination Attack on LEO Satellite Users

Eric Jedermann[1], Martin Strohmeier[2], Vincent Lenders[2], Jens Schmitt[1]

[1] RPTU Kaiserslautern-Landau, [2] Armasuisse

33rd USENIX Security 2024

Presenter: YoungHyo Kang

Introduction

The Rise of LEO Satellites

NOVASPACE

nvestment concerns

eekWire NEWS JOBS EVENTS LISTS MEMBERS STUDIOS ABOUT Search

Musk's Starlink rockets to 4 million subscribers

Satellite broadband mega-constellation passes mega-milestone

Richard Speed — Fri 27 Sep 2024 // 12:34 UTC

Starlink's subscriber count is accelerating and has passed the 4 million milestone, up from the 2.3 million it claimed in its 2023 progress report.

STARLINK

ZACKS

Eutelsat Boosts OneWeb LEO Constellation With 20 New Satellites

October 21, 2024 — 09:00 am EDT

Written by Zacks Equity Research for Zacks →

EUTELSAT ONEWEB EUTELSAT GROUP

Network Commu

The Power of Satellite, On-Demand

nding: Week in Review: Most popular stories on GeekWire for the week of Nov. 10, 2024

Market study says Amazon is spending up to $20B on Project Kuiper satellite network

BY ALAN BOYLE on September 11, 2024 at 7:29 pm

amazon | project kuiper

...eats in Satellites

Committee to Protect Journalists

News Data Safety Resources Get Involved SEARCH

Features & Analysis

Caveat utilitor: Satellite phones can always be tracked

By Frank Smyth/CPJ Senior Adviser for Journalist Security on February 24, 2012 6:03 PM EST

The Telegraph in London was the first to report that Syrian government forces could have "locked on" to satellite phone signals to launch the rocket attacks that killed journalists Marie Colvin and Rémi Ochlik, as well as many Syrian civilians, besides wounding dozens more including two more international journalists. Working out of a makeshift press center in Homs, foreign correspondents and local citizen journalists alike have been using satellite phones to send images of attacks on civilians around the world.

MORE TANGLED WEB RadioFreeEurope RadioLiberty

February 24, 2012 15:13 GMT

Marie Colvin's Death Raises Concerns About Use Of Satellite Phones

Share

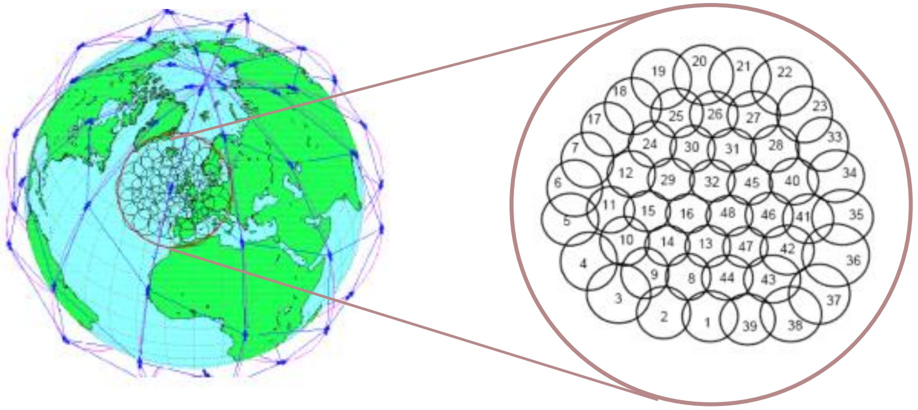
Print

Marie Colvin, an American working for Britain's "Sunday Times," and French photographer Remi Ochlik

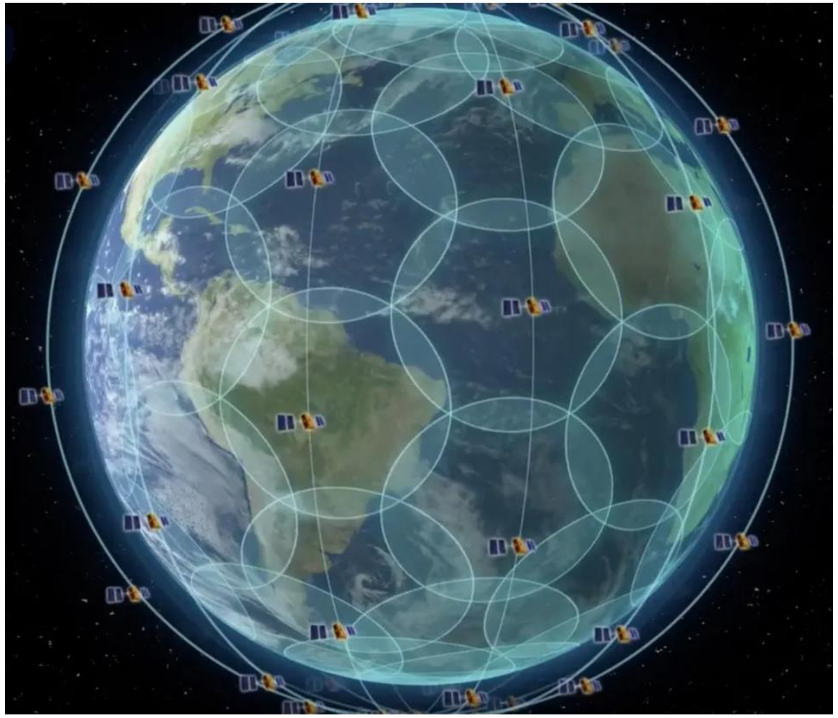
The Electronic Frontier Foundation has highlighted the possible risks for journalists using satellite phones after speculation that their signals might have allowed the Syrian army to target journalists Marie Colvin and Remi Ochlik, who were killed this week in Homs.

Background
Iridium Constellation

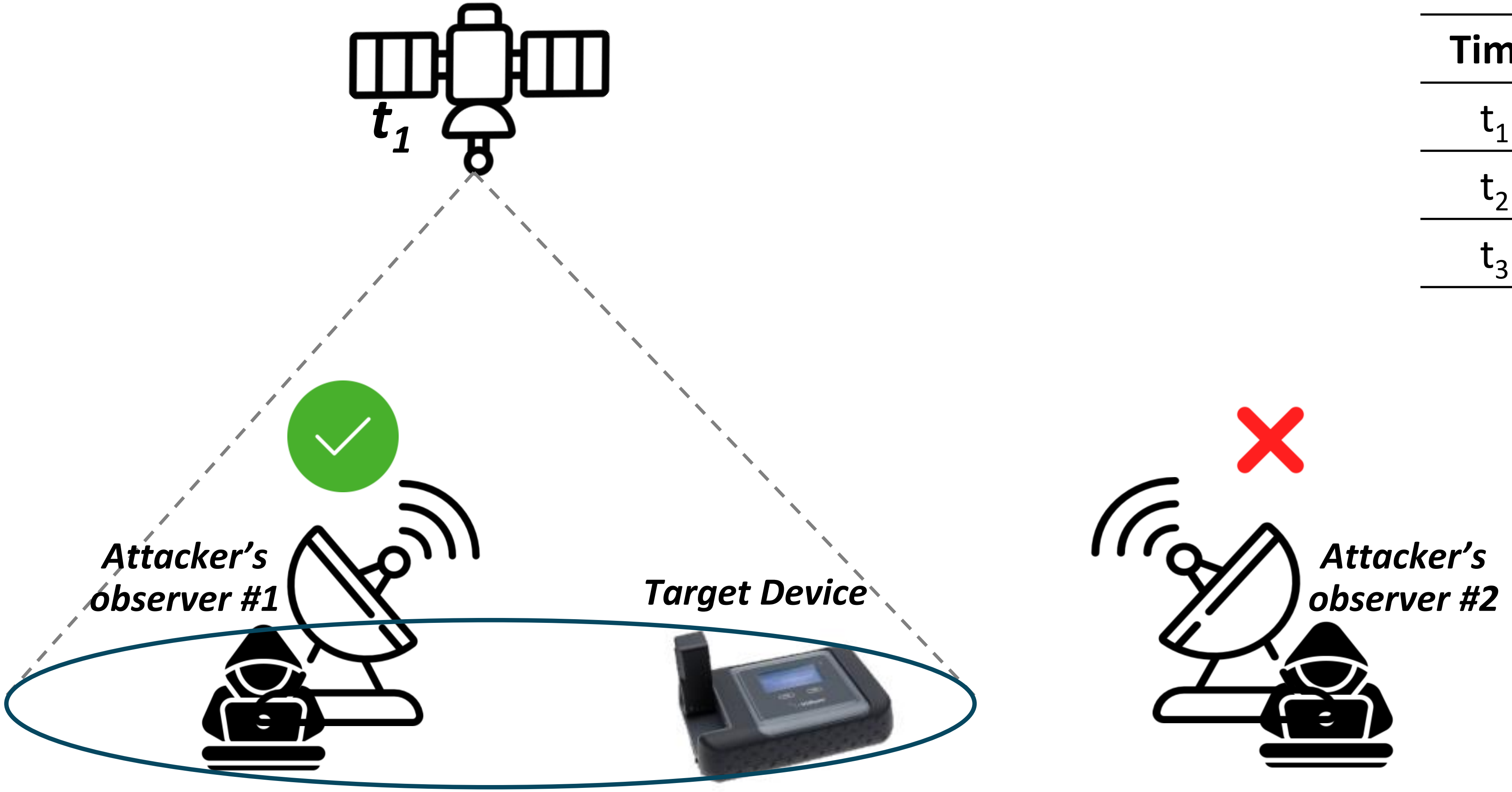
- Iridium constellation consist of **66 LEO satellites**
- Each satellite has **48 spot beams**
  - Diameter of spot beam: **400-1,000km**



Iridium Satellite spot beam

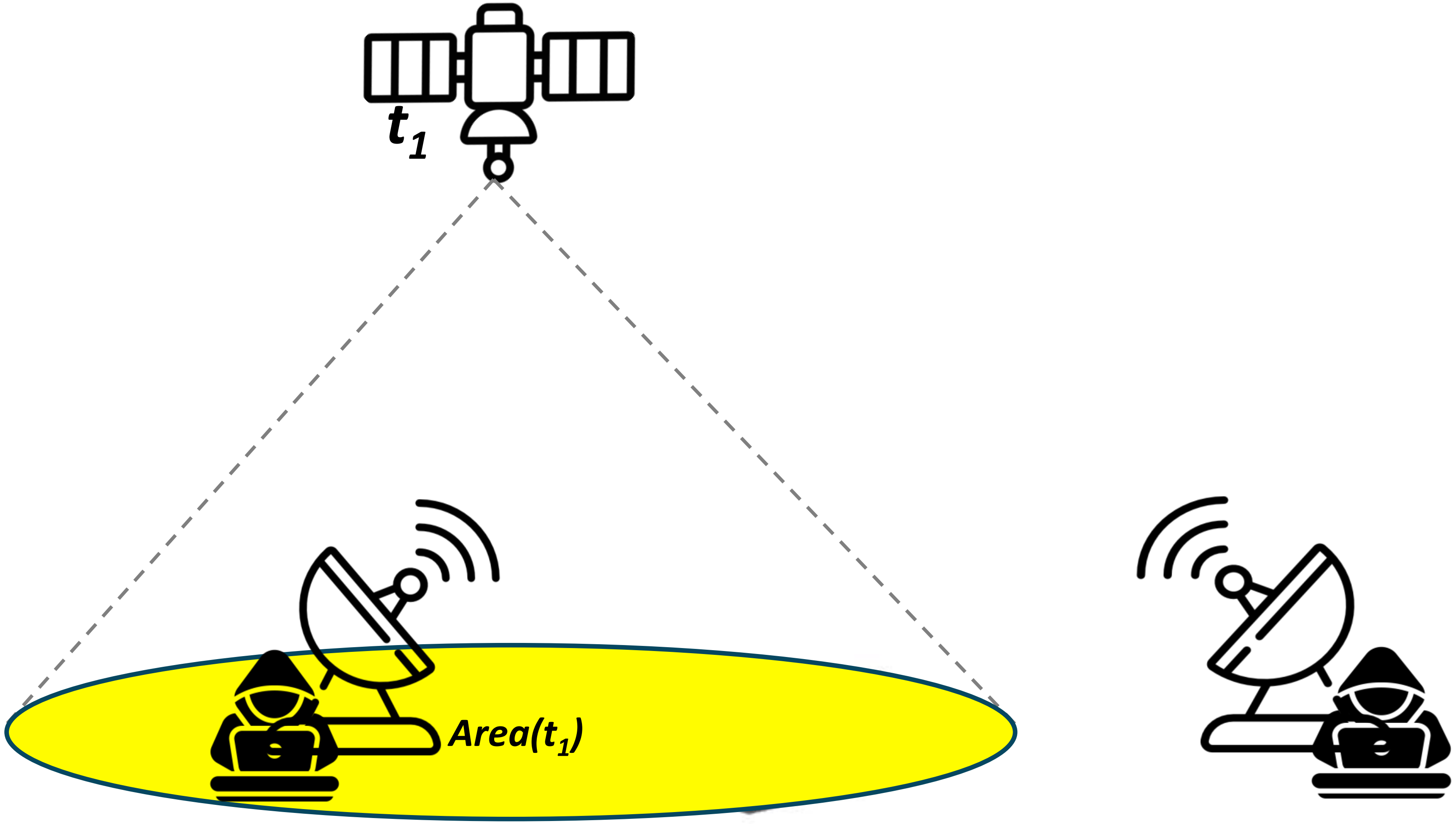


Base Idea of the RECORD Attack



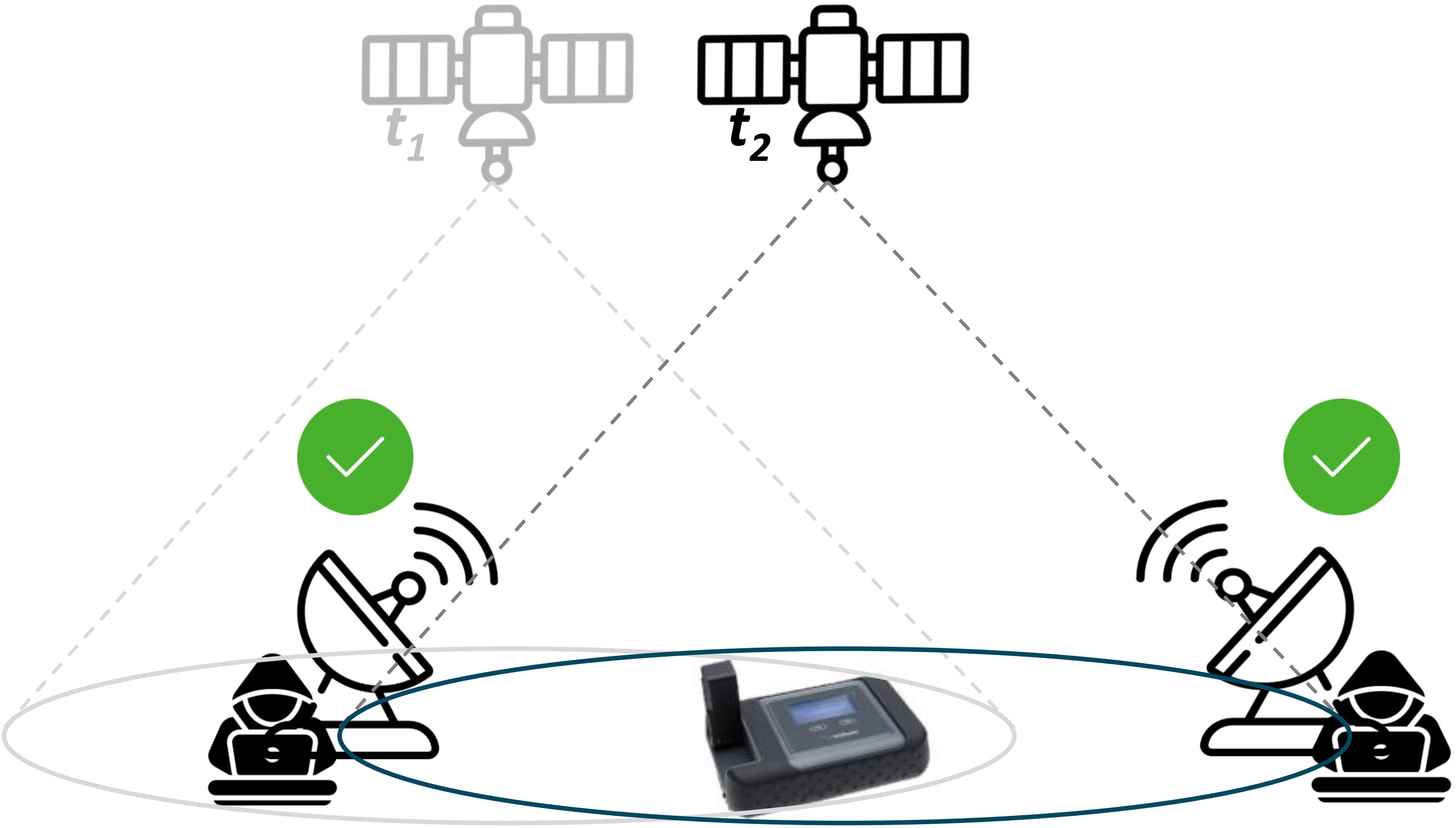
Time	observer_1	observer_2
t_1	Receive	Not receive
t_2		
t_3		

Base Idea of the RECORD Attack



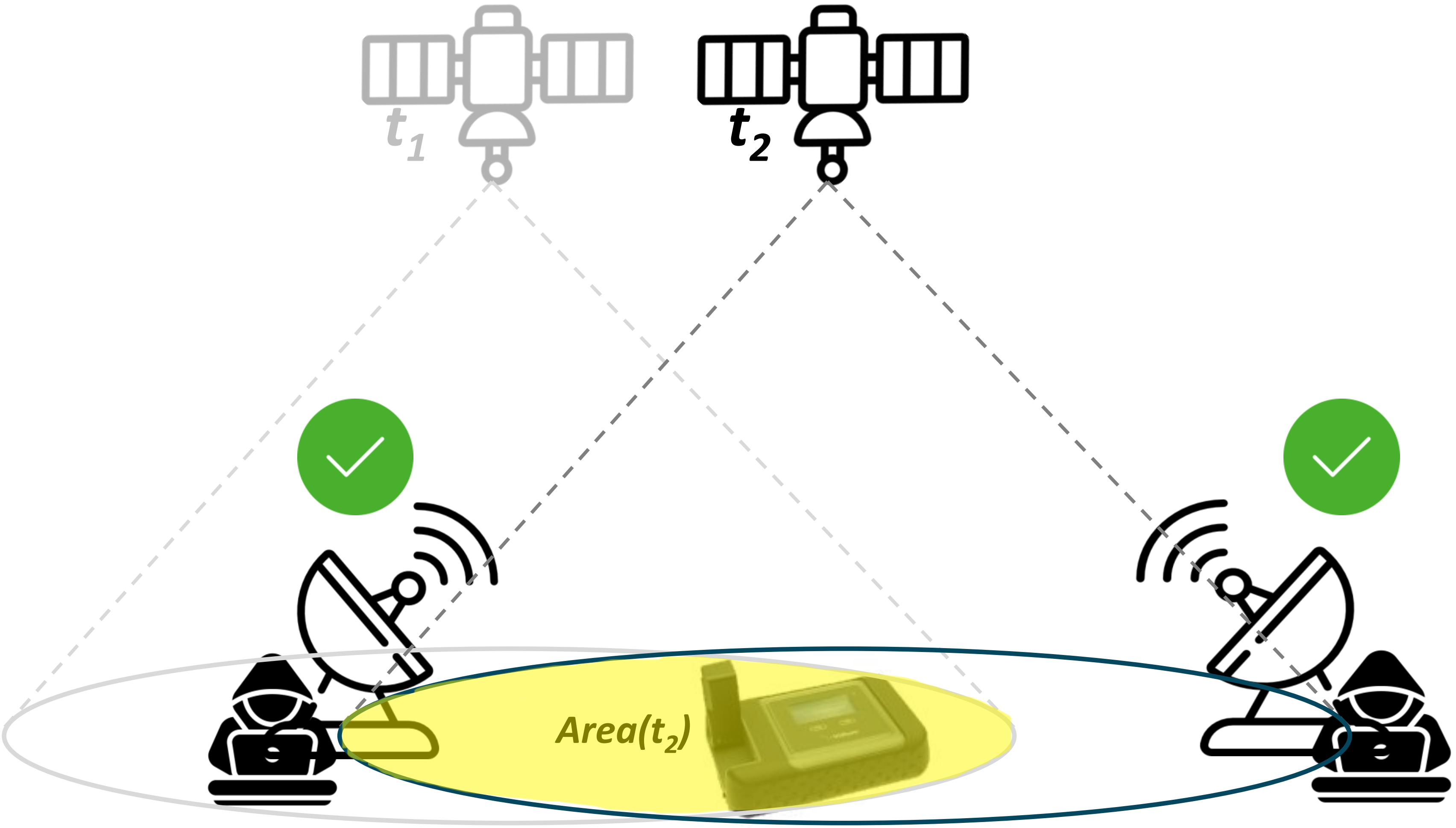
Time	observer_1	observer_2
t_1	Receive	Not receive
t_2		
t_3		

Base Idea of the RECORD Attack



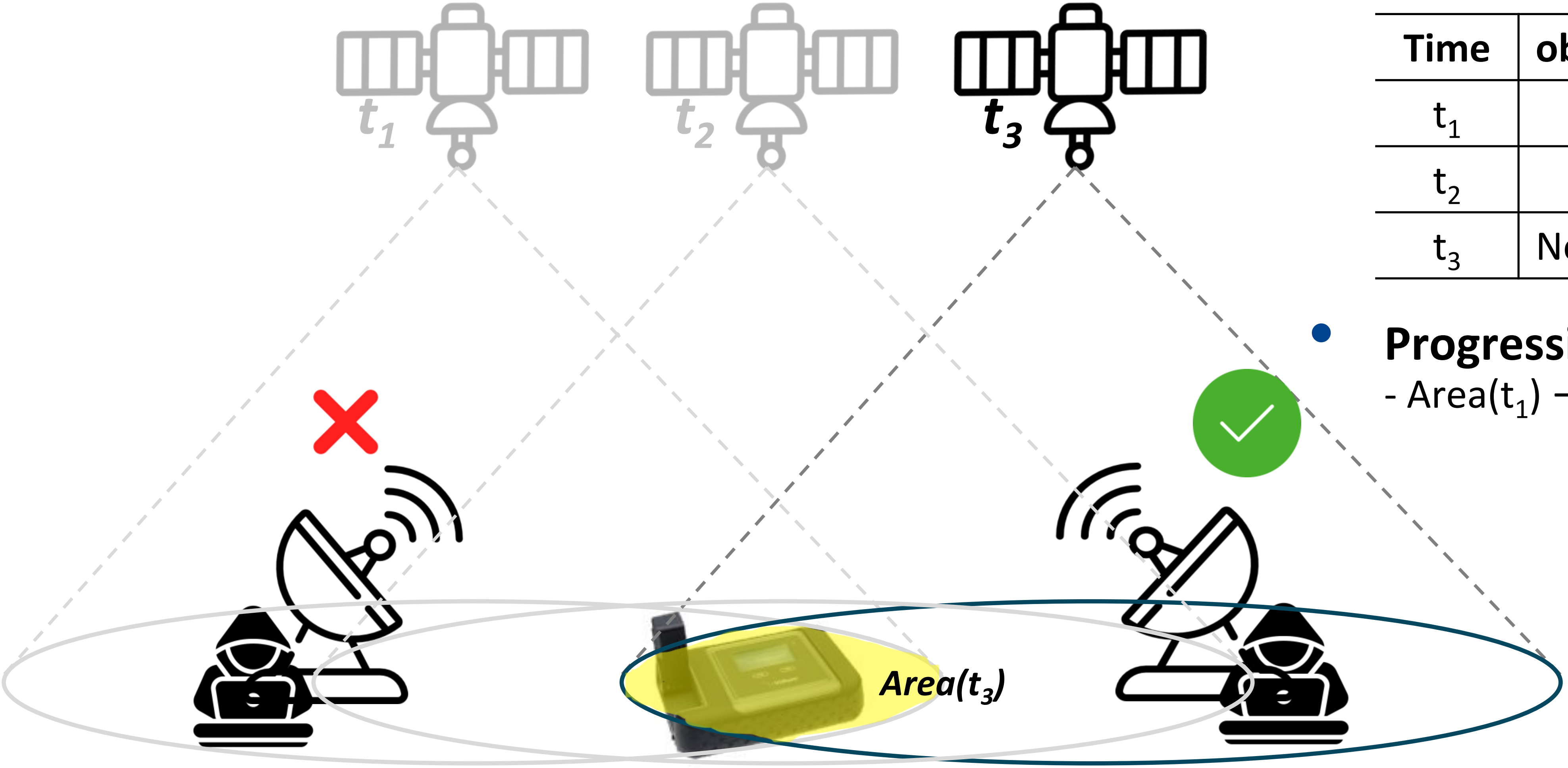
Time	observer_1	observer_2
t_1	Receive	Not receive
t_2	Receive	Receive
t_3		

Base Idea of the RECORD Attack



Time	observer_1	observer_2
t_1	Receive	Not receive
t_2	Receive	Receive
t_3		

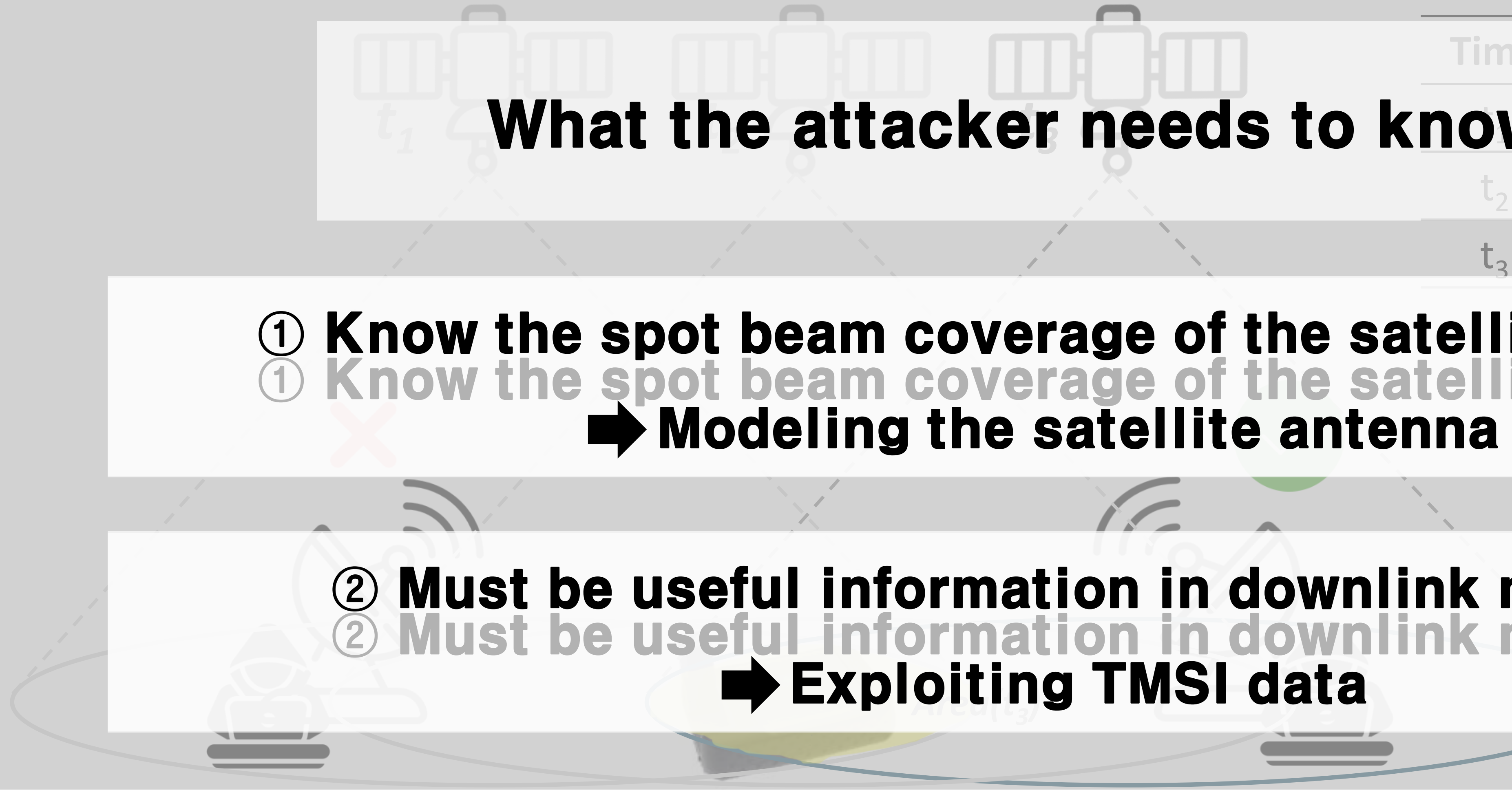
Base Idea of the RECORD Attack



Time	observer_1	observer_2
t_1	Receive	Not receive
t_2	Receive	Receive
t_3	Not receive	Receive

- **Progressively narrows down**
  - Area(t_1) → Area(t_2) → Area(t_3)

Base Idea of the RECORD Attack



Time	observer_1	observer_2
[illegible]	Receive	Not receive
t_2	Receive	Receive
t_3	Not receive	Receive

The attacker progressively narrows down the location of the target device through continuous observation.

- $Area(t_1) \rightarrow Area(t_2) \rightarrow Area(t_3)$

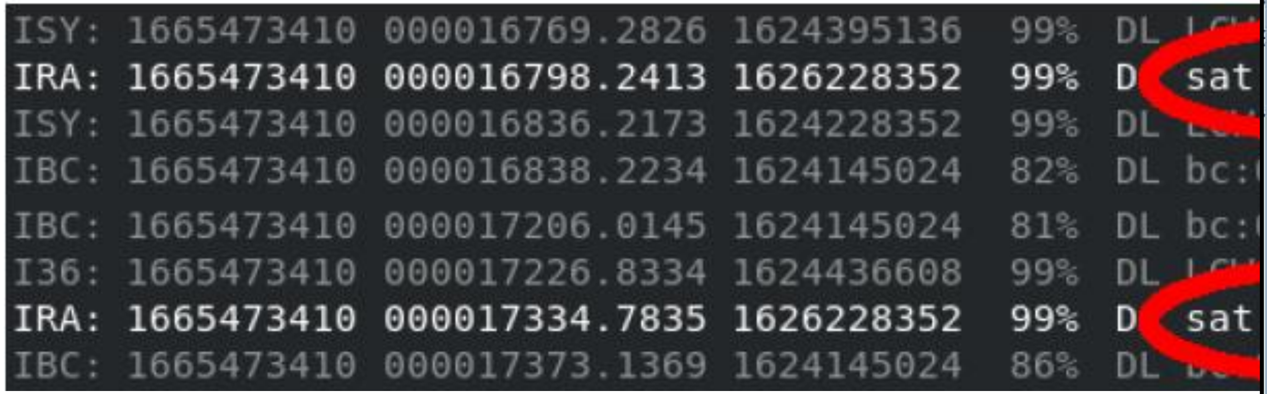
What the attacker needs to know?

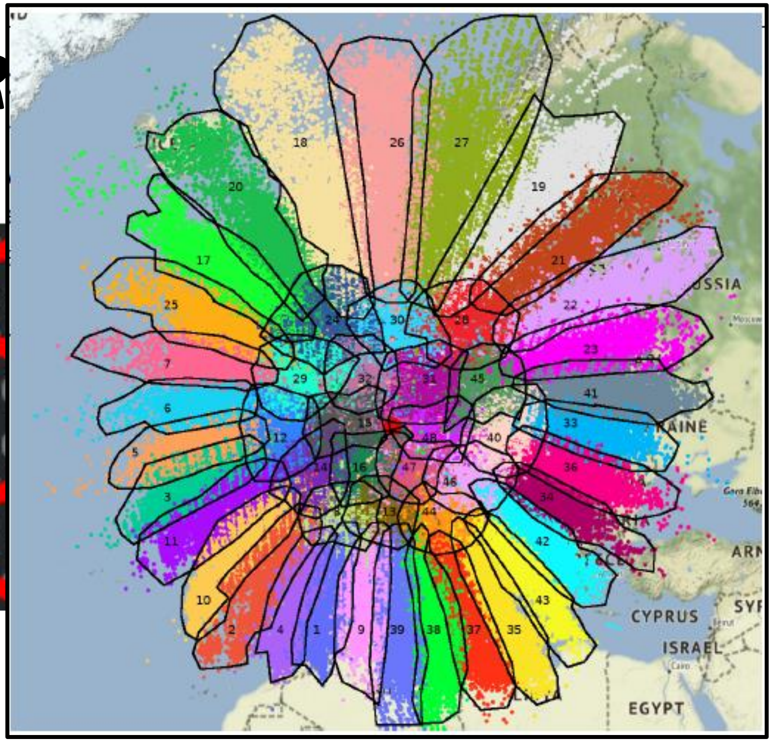
① Know the spot beam coverage of the satellite antenna
① Know the spot beam coverage of the satellite antenna
➡ Modeling the satellite antenna

② Must be useful information in downlink message
② Must be useful information in downlink message
➡ Exploiting TMSI data

Real-world Attack Implementation
Phase 1: Modeling the Antenna Beam

- Goal: Create a model of the satellite antenna footprint.
- Collect Iridium status messages, ***Iridium R***

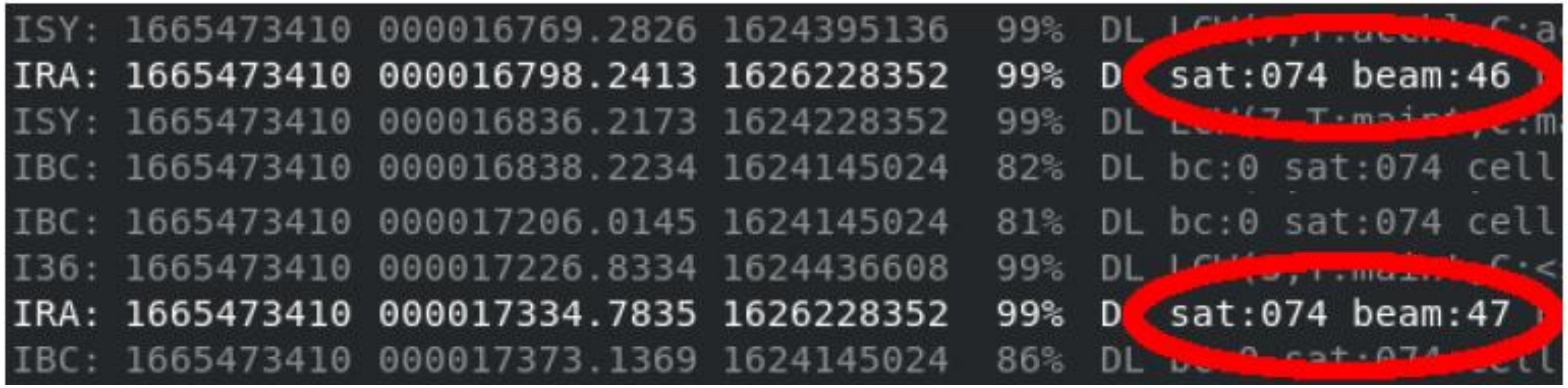


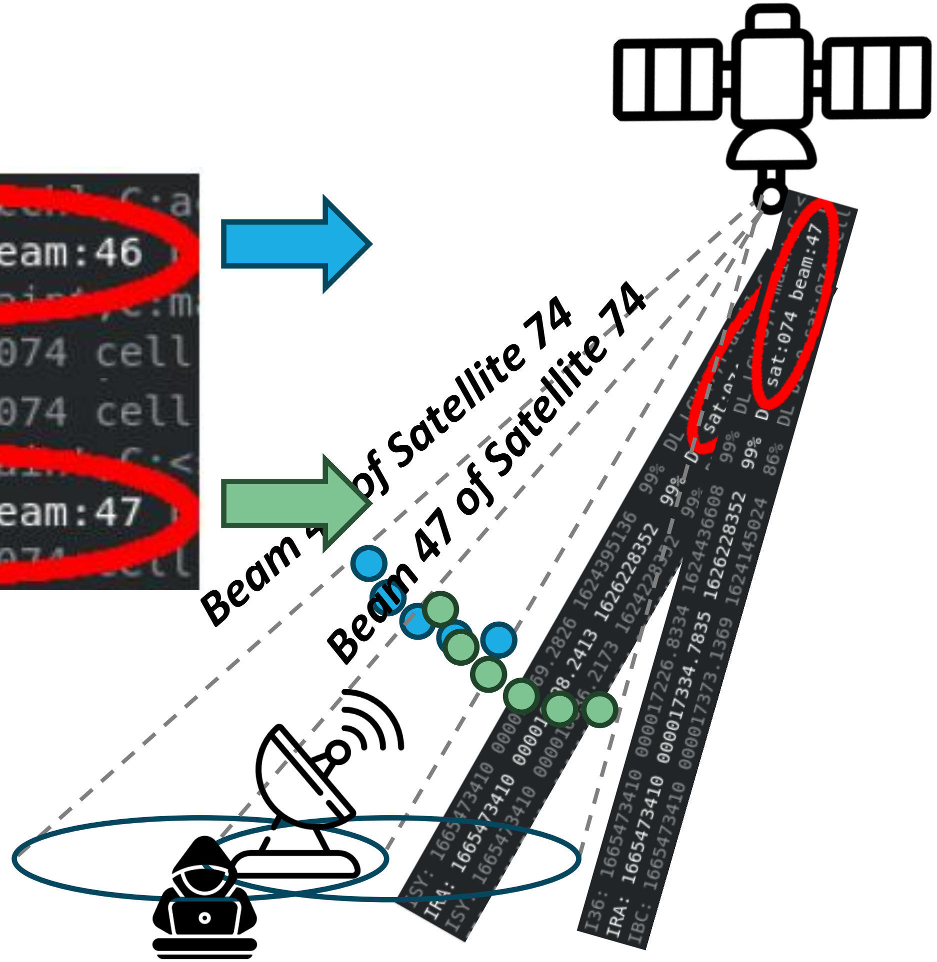


NS2 Network and System Security Laboratory KAIST

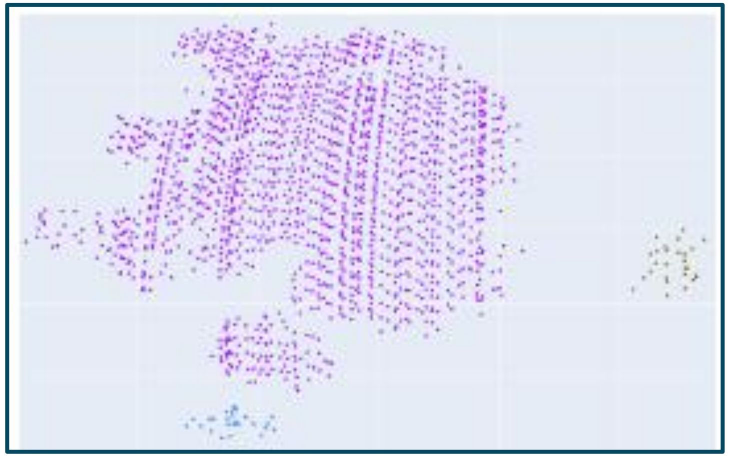
Real-world Attack Implementation

Phase 1: Modeling the Antenna Beam

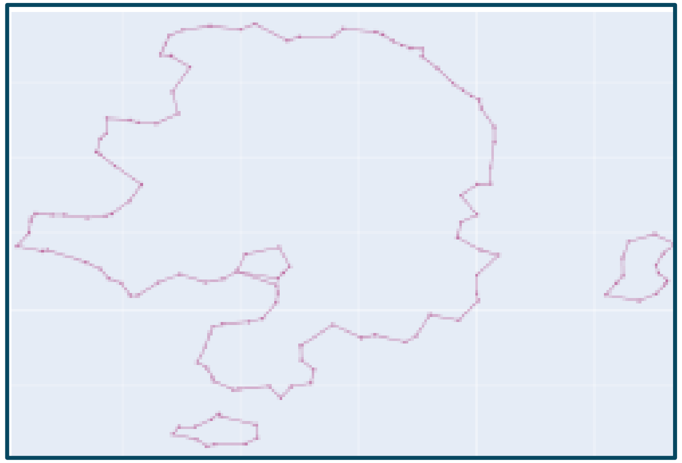

```
ISY: 1665473410 000016769.2826 1624395136  99% DL
IRA: 1665473410 000016798.2413 1626228352  99% D  sat:074 beam:46
ISY: 1665473410 000016836.2173 1624228352  99% DL
IBC: 1665473410 000016838.2234 1624145024  82% DL bc:0 sat:074 cell
IBC: 1665473410 000017206.0145 1624145024  81% DL bc:0 sat:074 cell
I36: 1665473410 000017226.8334 1624436608  99% DL
IRA: 1665473410 000017334.7835 1626228352  99% D  sat:074 beam:47
IBC: 1665473410 000017373.1369 1624145024  86% DL
```



Real-world Attack Implementation
Phase 1: Modeling the Antenna Beam



Clustered measurements



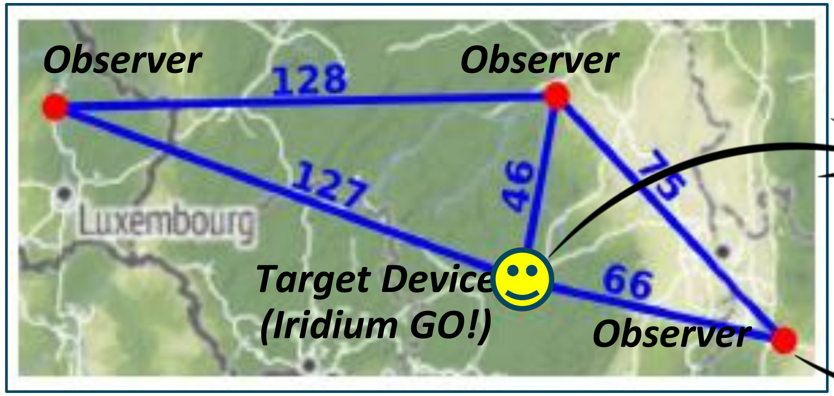
Optimized Borders

Projection onto Earth

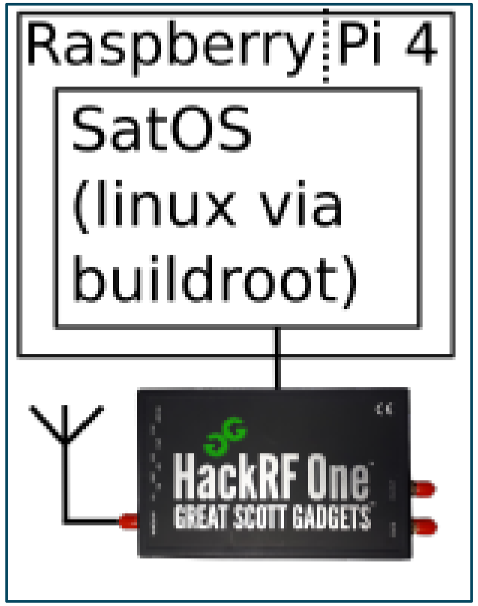
NS2 Network and System Security Laboratory KAIST

Real-world Attack Implementation
Phase 2: Recording the Victim Traffic

- Goal: Collect information about the target device
- Place target device and three observers

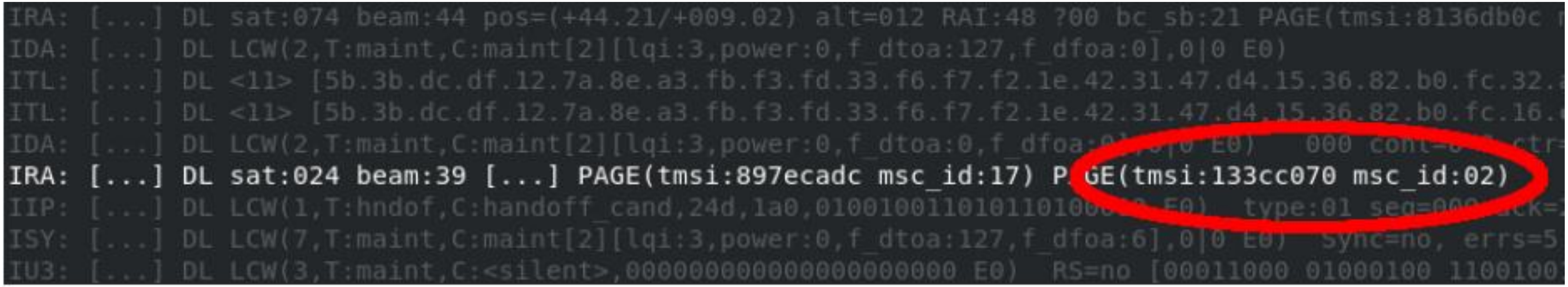


Placement of Observer and Target Device



Real-world Attack Implementation
Phase 2: Recording the Victim Traffic

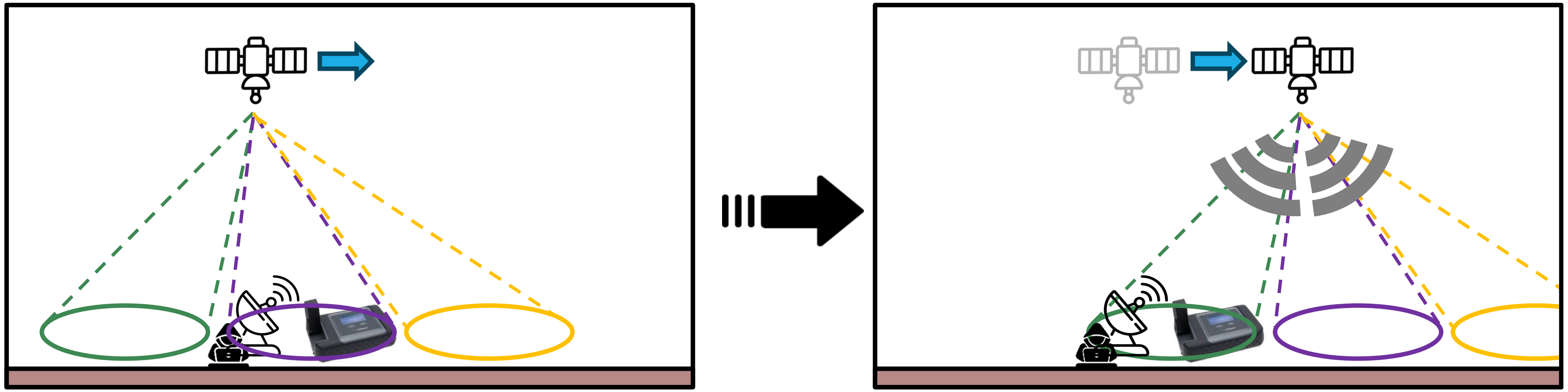
- The receiver collects downlink messages from the satellite
- The ***TMSI*** is transmitted without encryption



Real-world Attack Implementation

Phase 2: Recording the Victim Traffic

- TMSI does not change during connection. `(tmsi:133cc070 msc_id:02)`
  - The ***static TMSI*** allows the attacker to identify devices.
- The Iridium network broadcast **clear-text** handover messages.

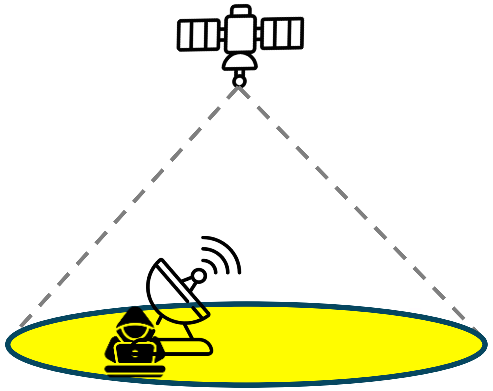


When switch the spot beam (Purple beam → Green beam)

Real-world Attack Implementation
Phase 3: Estimating the Target Location

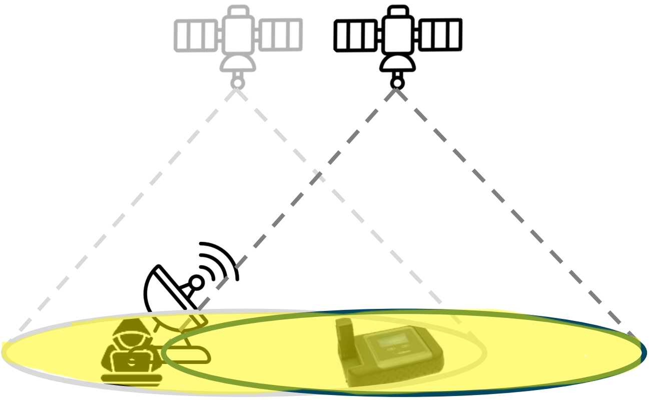
- Goal: Calculate the region of the target device

Real-world Attack Implementation
Phase 3: Estimating the Target Location



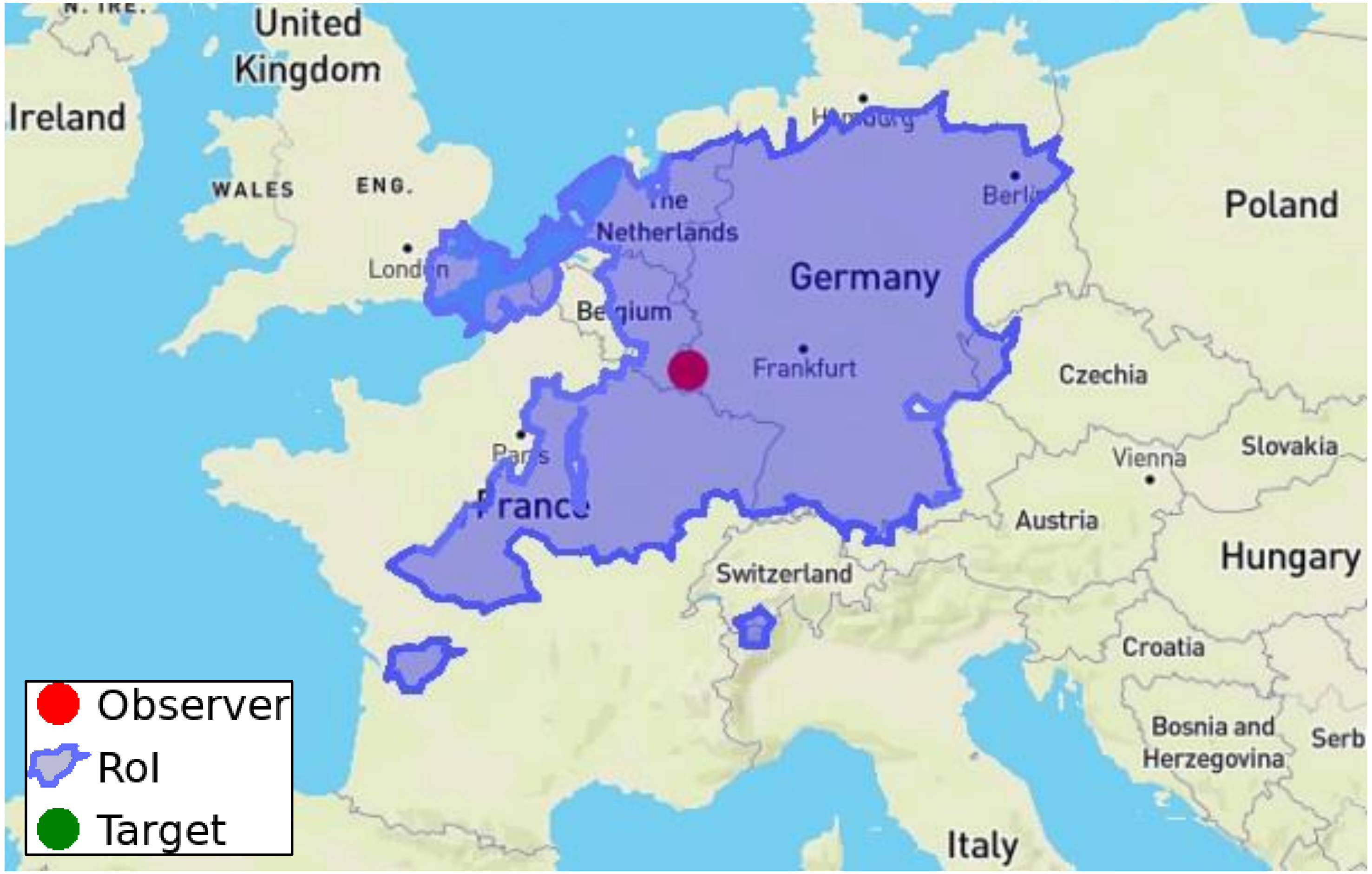
Real-world Attack Implementation

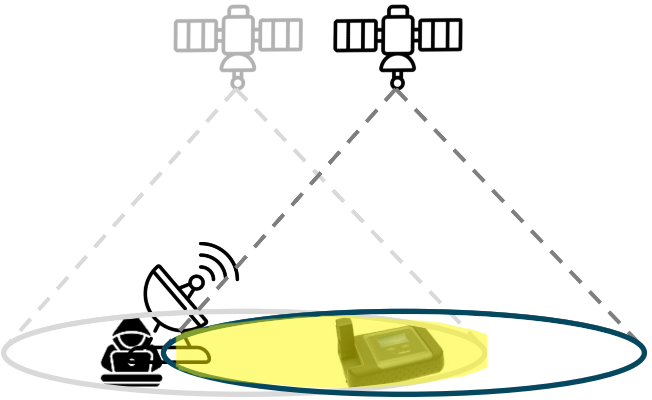
Phase 3: Estimating the Target Location



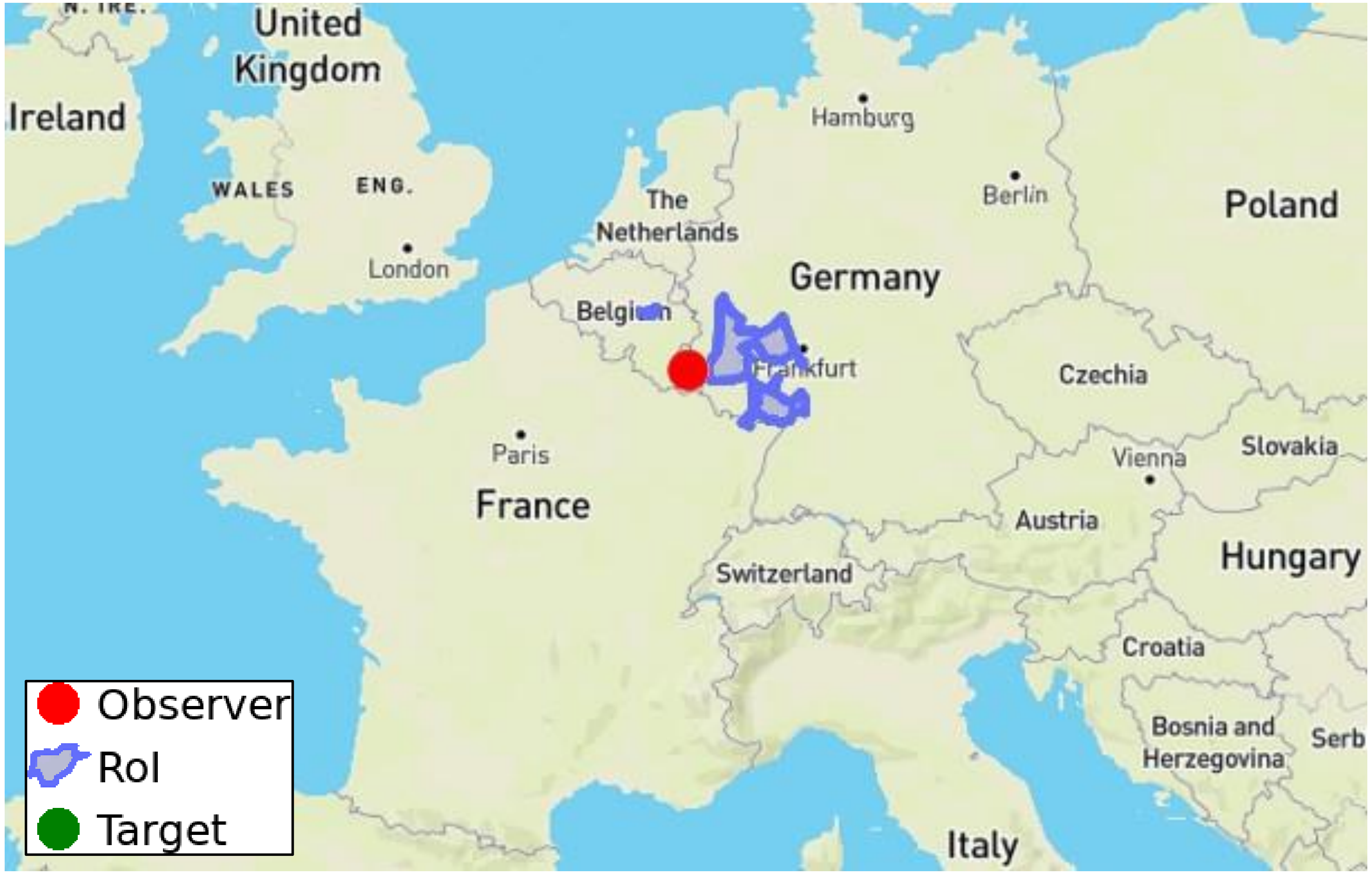
Real-world Attack Implementation

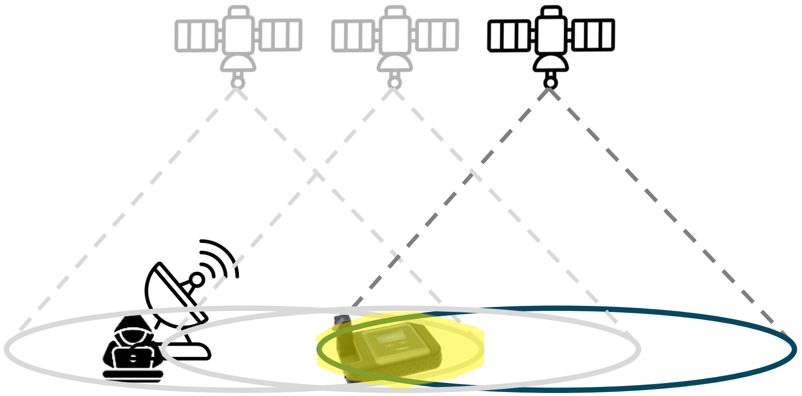
Phase 3: Estimating the Target Location





Real-world Attack Implementation
Phase 3: Estimating the Target Location





Real-world Attack Implementation
Phase 3: Estimating the Target Location

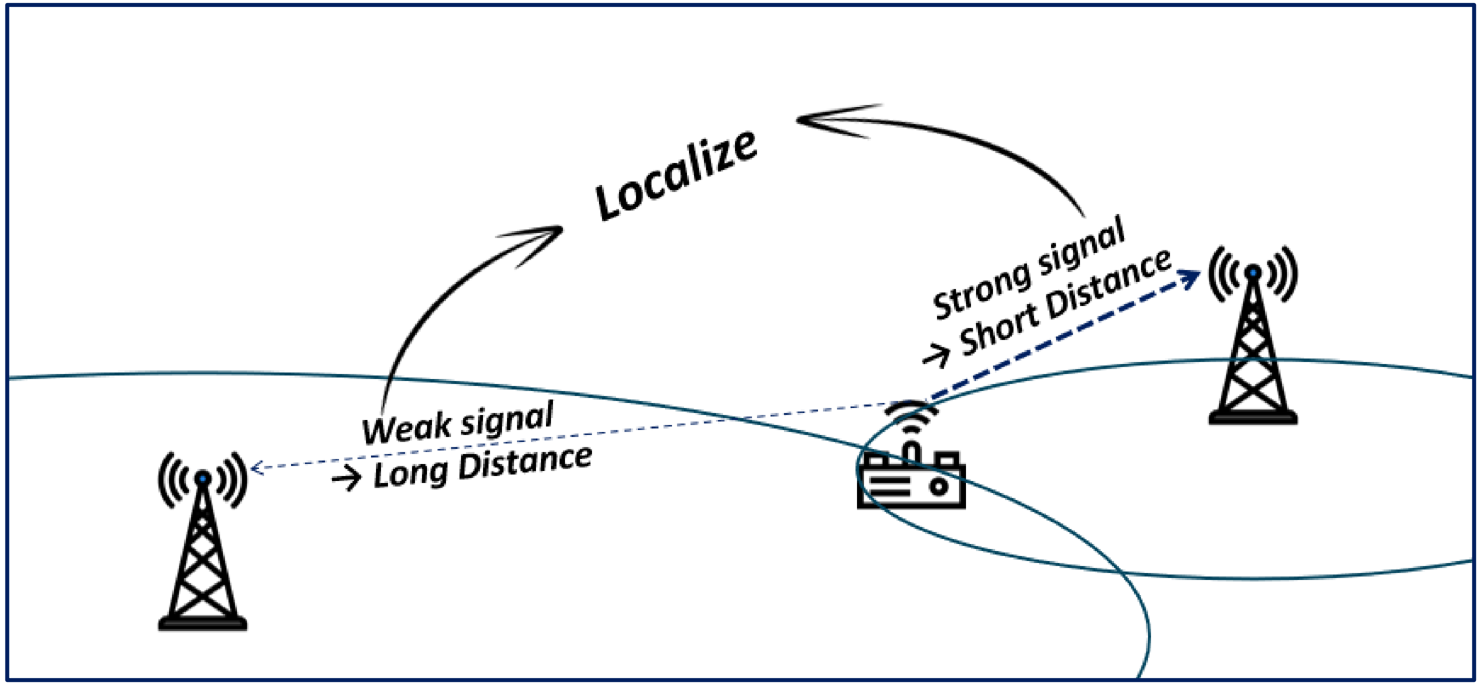
Is the Last RoI good enough?

Last ROI: 383km²

Real-world Attack Implementation

Beyond the RECORD Attack

- Apply **high-cost or locally-restricted techniques** to the ROI
  - Technique based on the ***Received Signal Strength (RSS)***

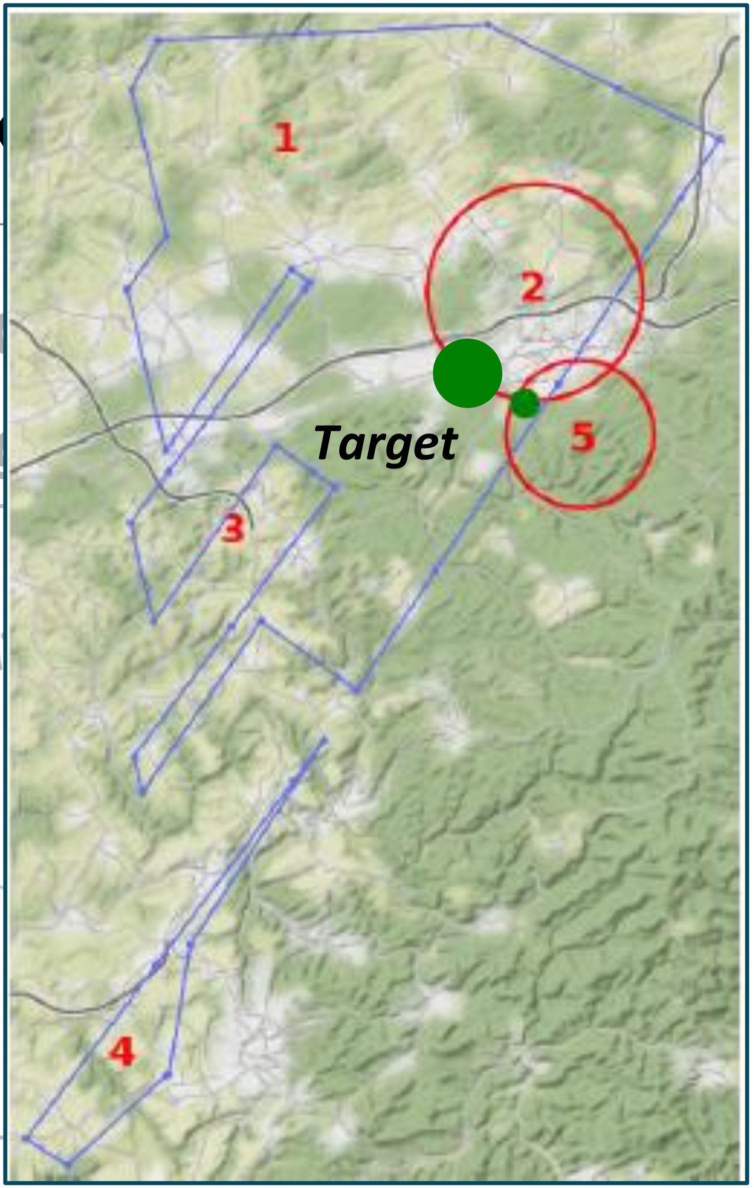


Real-world Attack Implementation

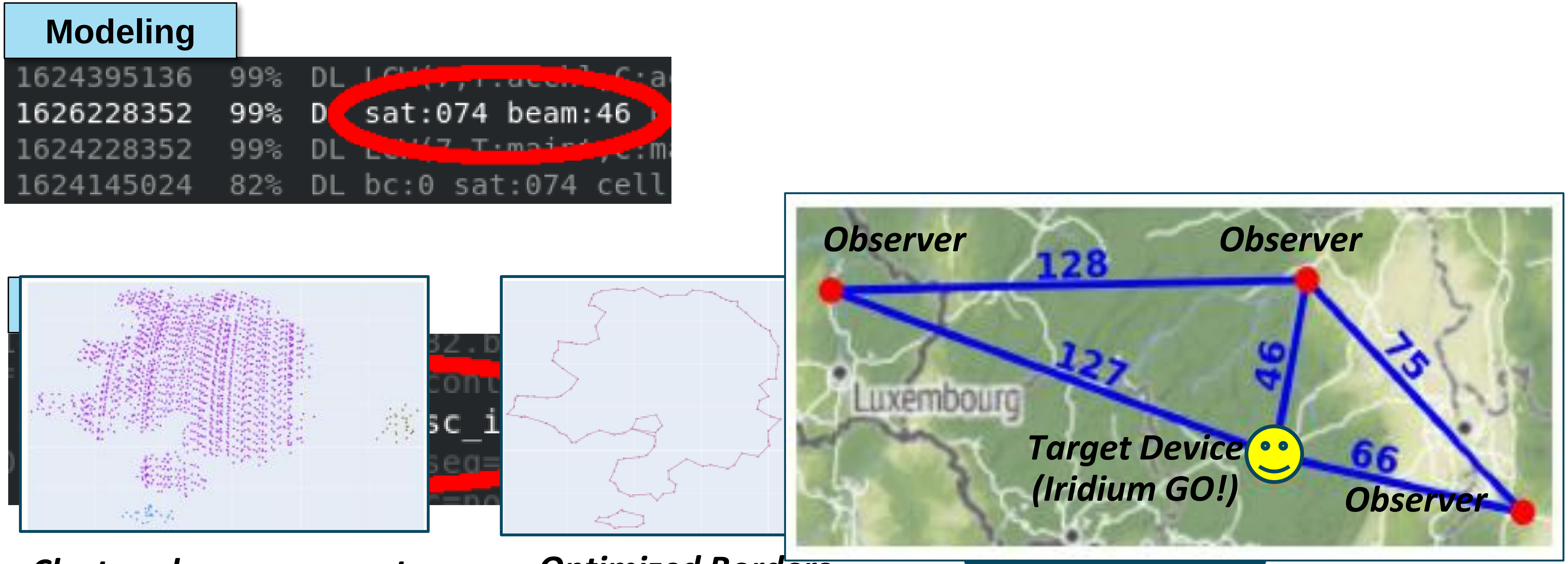
Beyond the RECORD Attack

- Apply **high-cost or locally-restricted techni**
  - Technique based on the ***Received Signal Streng***

Location	Noise Level	Signal Level	Distance(km)
1	-109.17	-	-
2	**-111.07**	**-37.37**	**4.180**
3	-110.91	-	-
4	-109.63	-	-
5	**-110.46**	**-34.08**	**2.862**



One-page overview
RECORD attack on Iridium satellite



Clustered measurements

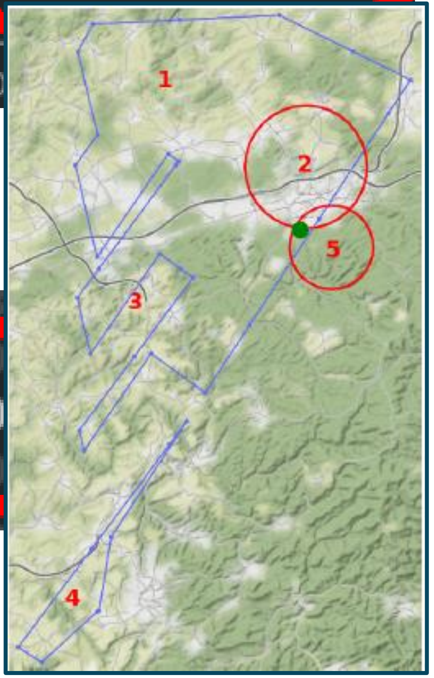
Optimized Borders

Placement of Observer and Target Device

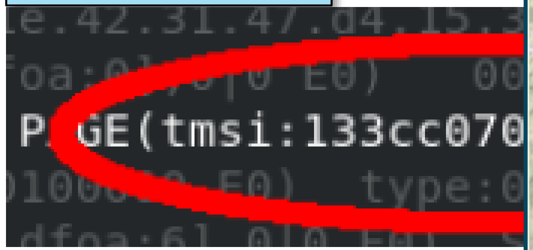
Projection onto Earth

One-page overview
RECORD attack on Iridium satellite

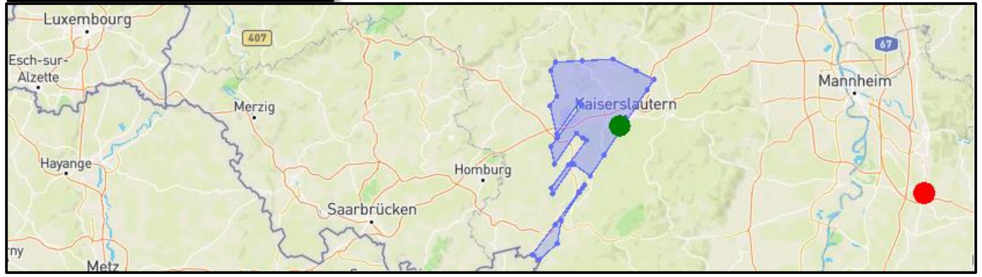
Modeling



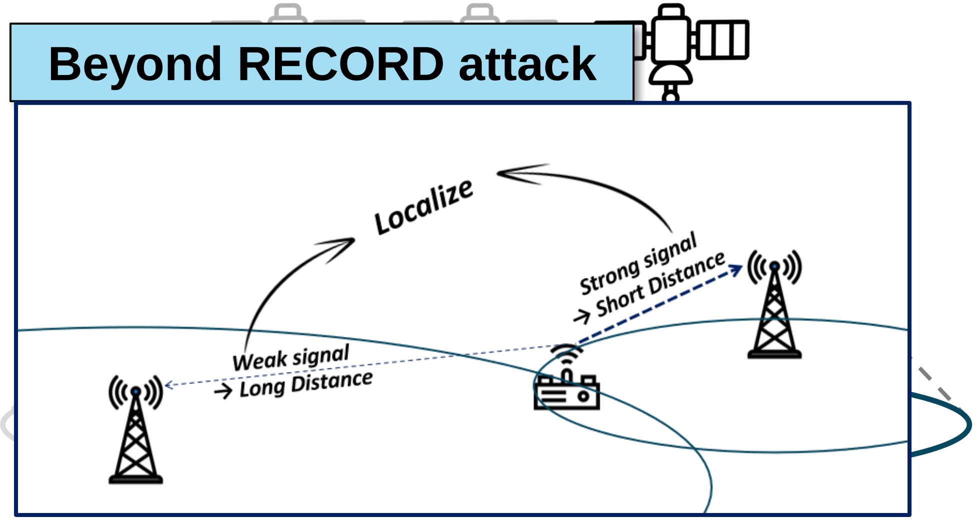
Collection



Estimation

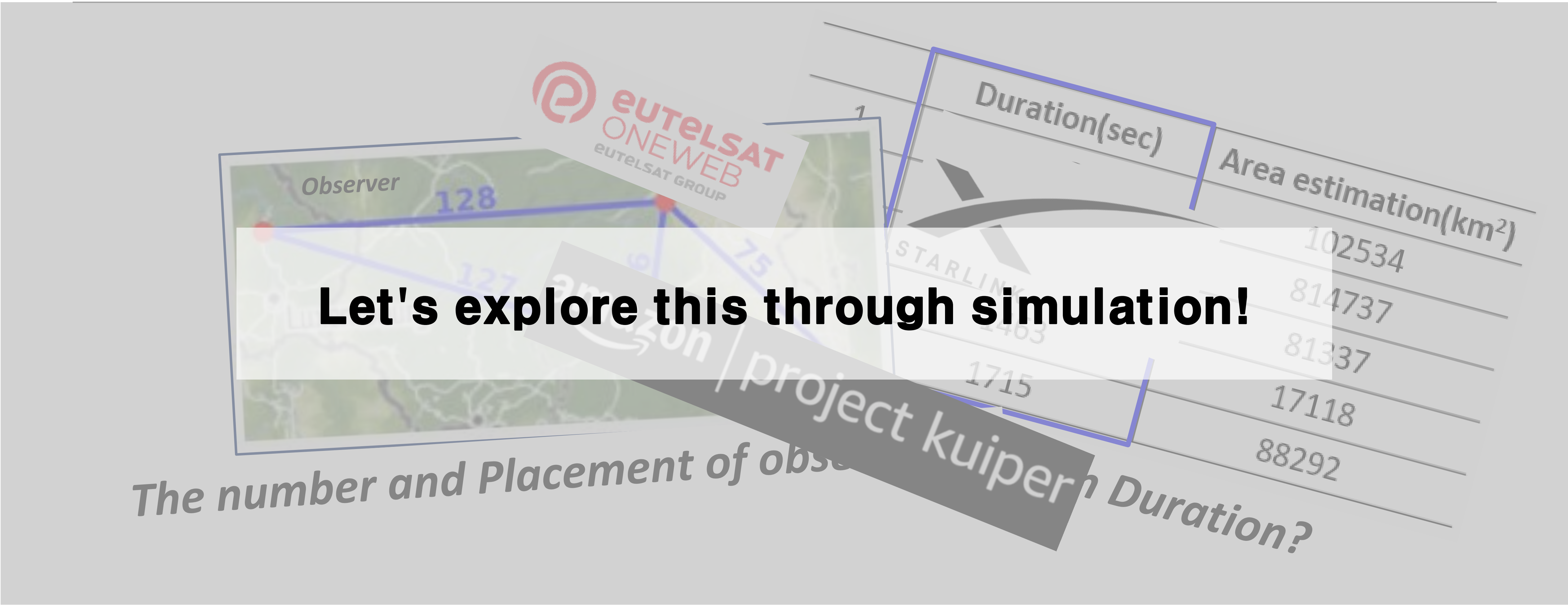


Beyond RECORD attack



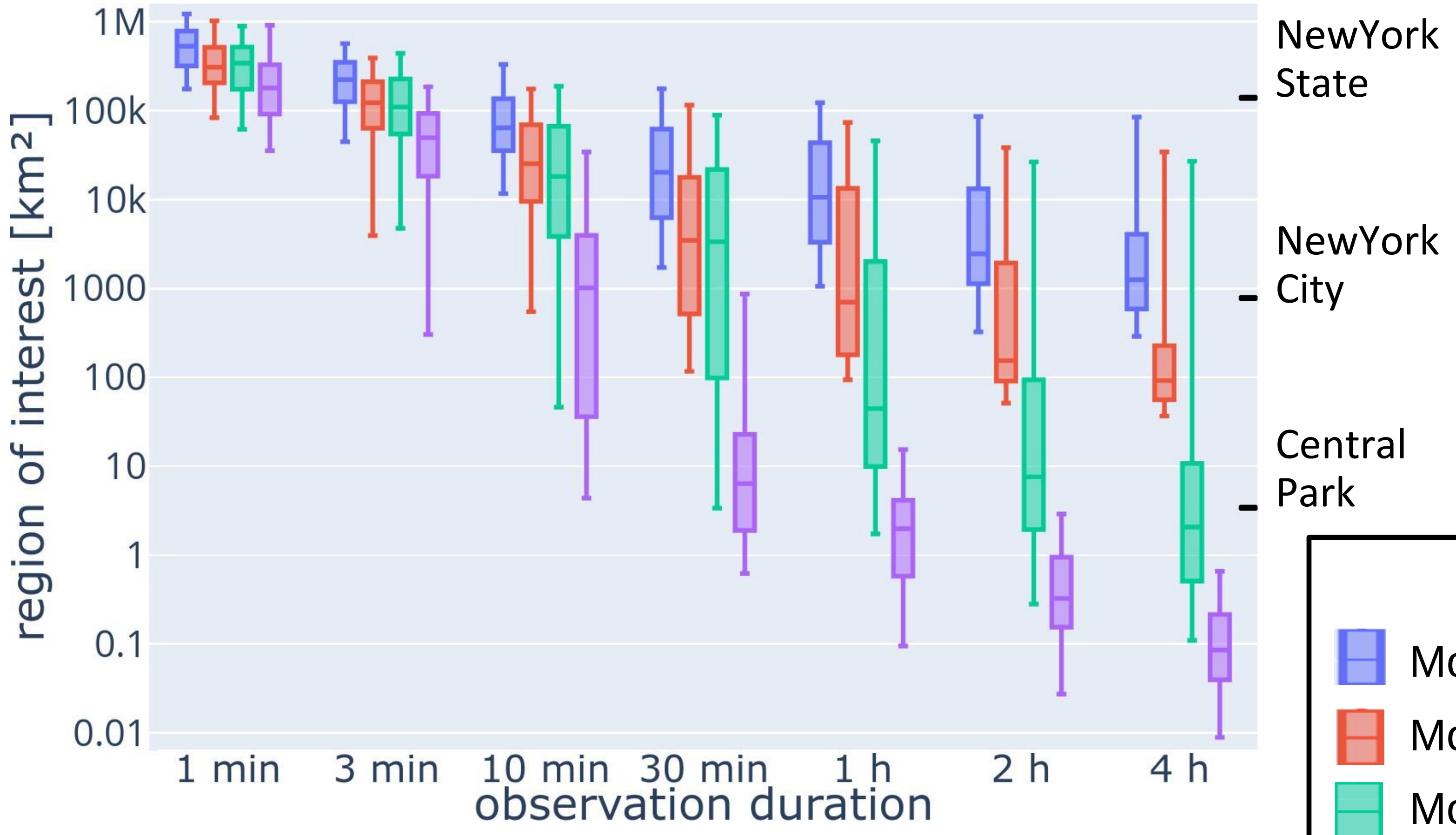
Simulative Evaluation

More Insight about RECORD Attack?



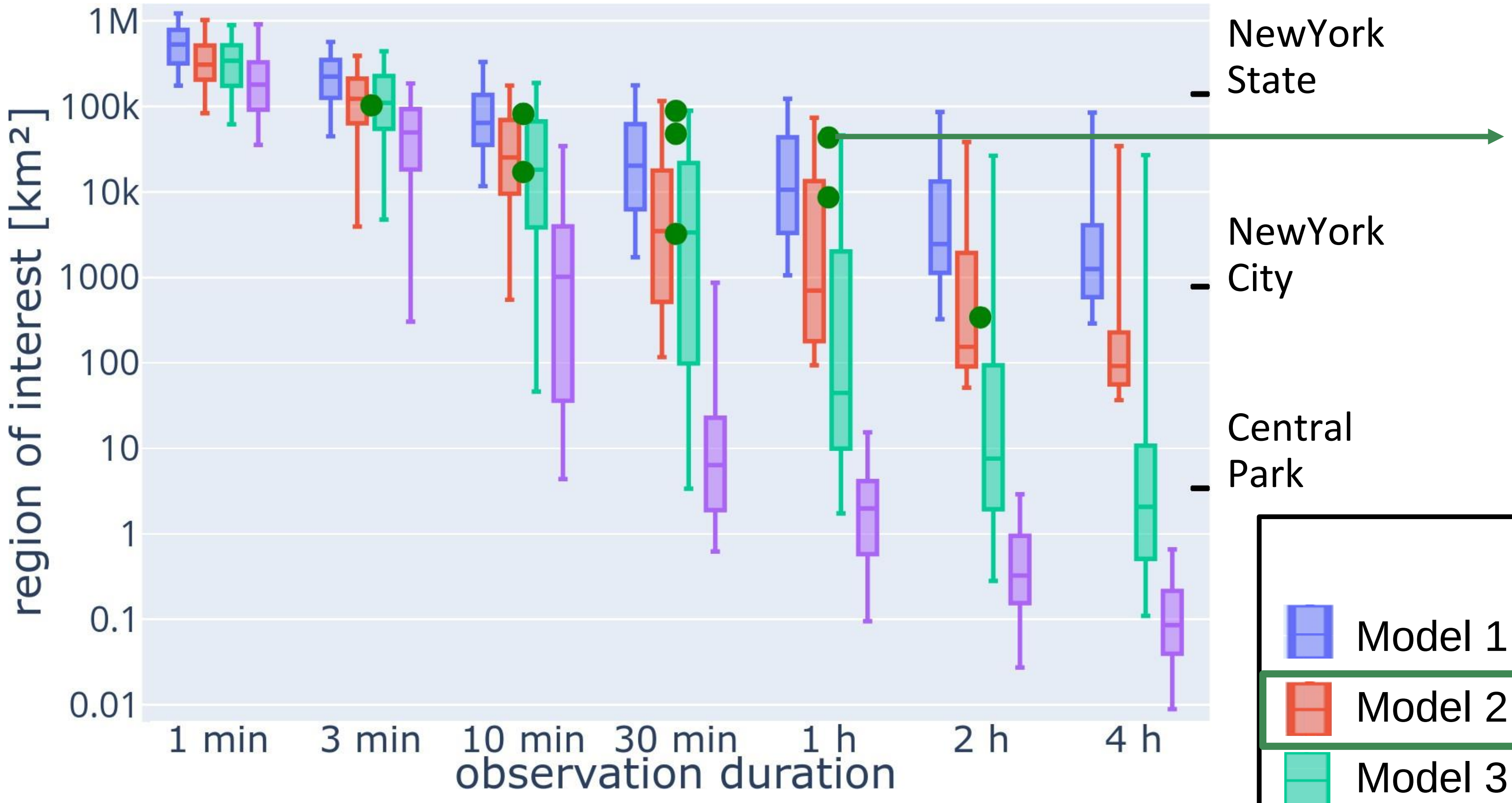
Let's explore this through simulation!

Simulative Evaluation
Finding the Most Realistic Model



	# of Obs	Beam Model	Event Type
Model 1	1	Noisy	Weak
Model 2	3	Noisy	Weak
Model 3	3	Strong	Weak
Model 4	3	Strong	Strong

Simulative Evaluation
Finding the Most Realistic Model

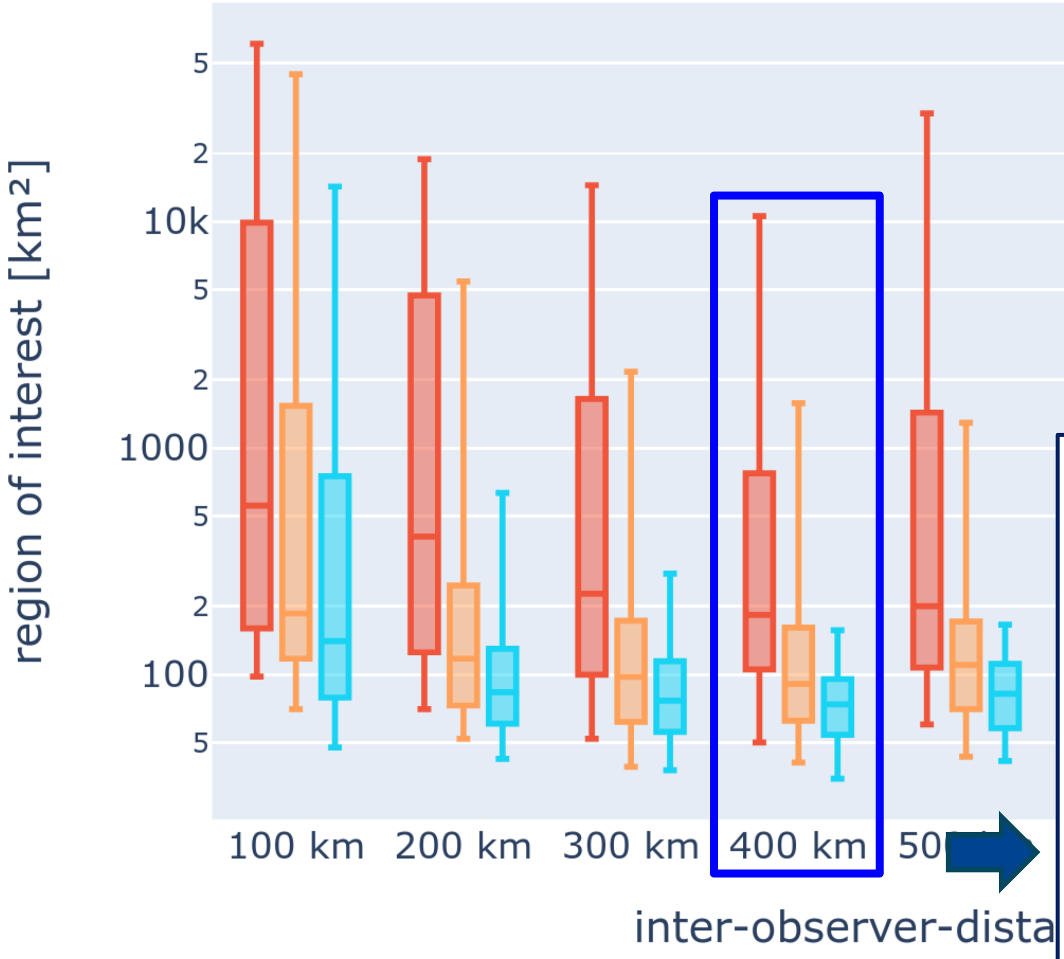


result of Real-World Implementation

	# of Obs	Beam Model	Event Type
Model 1	1	Noisy	Weak
Model 2	3	Noisy	Weak
Model 3	3	Strong	Weak
Model 4	3	Strong	Strong

Simulative Evaluation

Optimal Distance between Observers

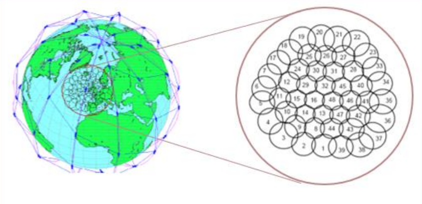


	# of Obs	Beam Model	Event Type
Model 2-a	3	Noisy	Weak
Model 2-b	6		
Model 2-c	12		

Background

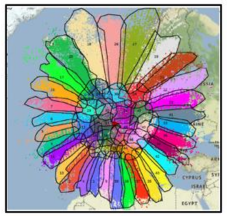
Iridium Constellation

- Consist of 66 LEO satellites
- The number of User: 1.9million
- North-south orientation
- Orbital period: 100minutes
- 48 spot beams for each satellite
  - Coverage of single spot beam (diameter): 400-1,000km
  - Coverage of all spot beams (diameter): 4,700km



Iridium Satellite spot beam

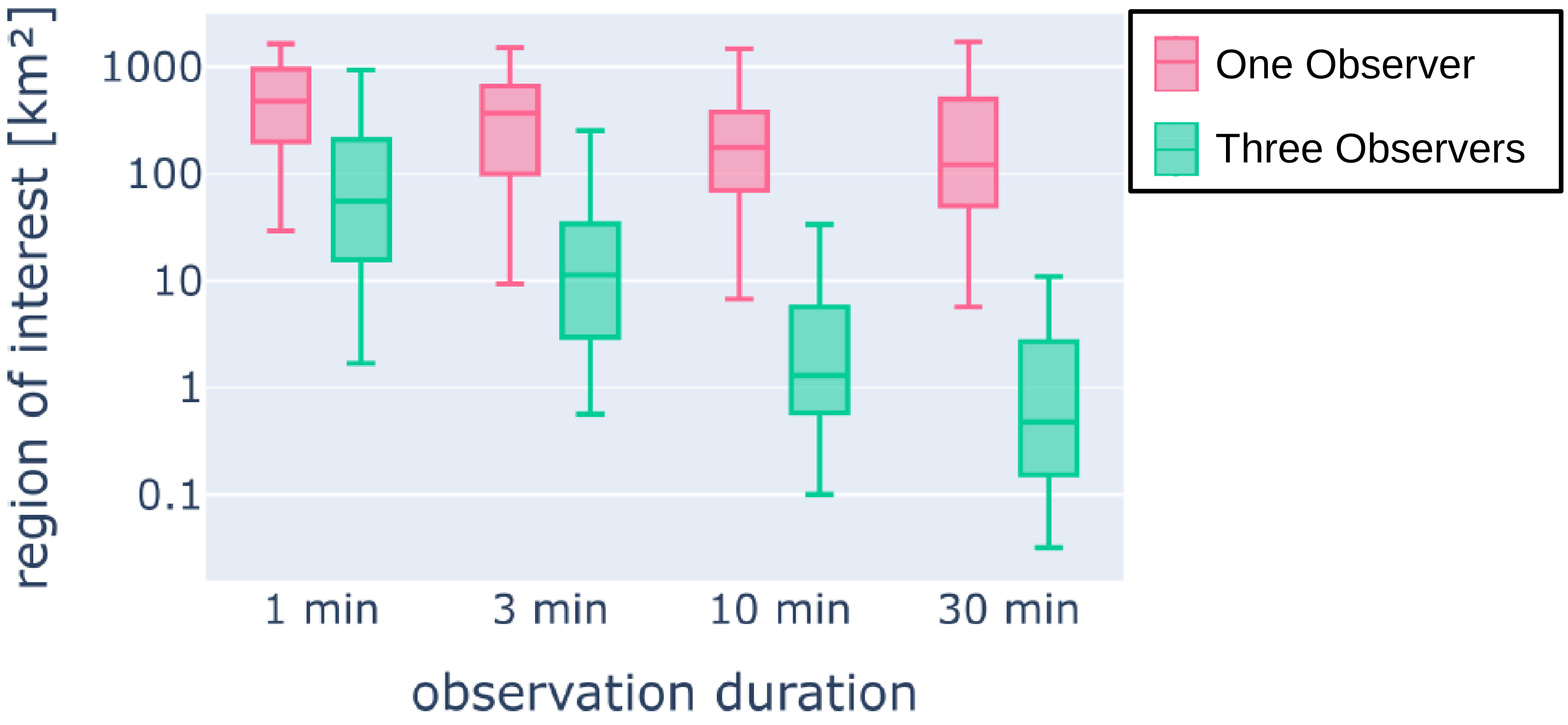
1



Real-world spot beam

Simulative Evaluation

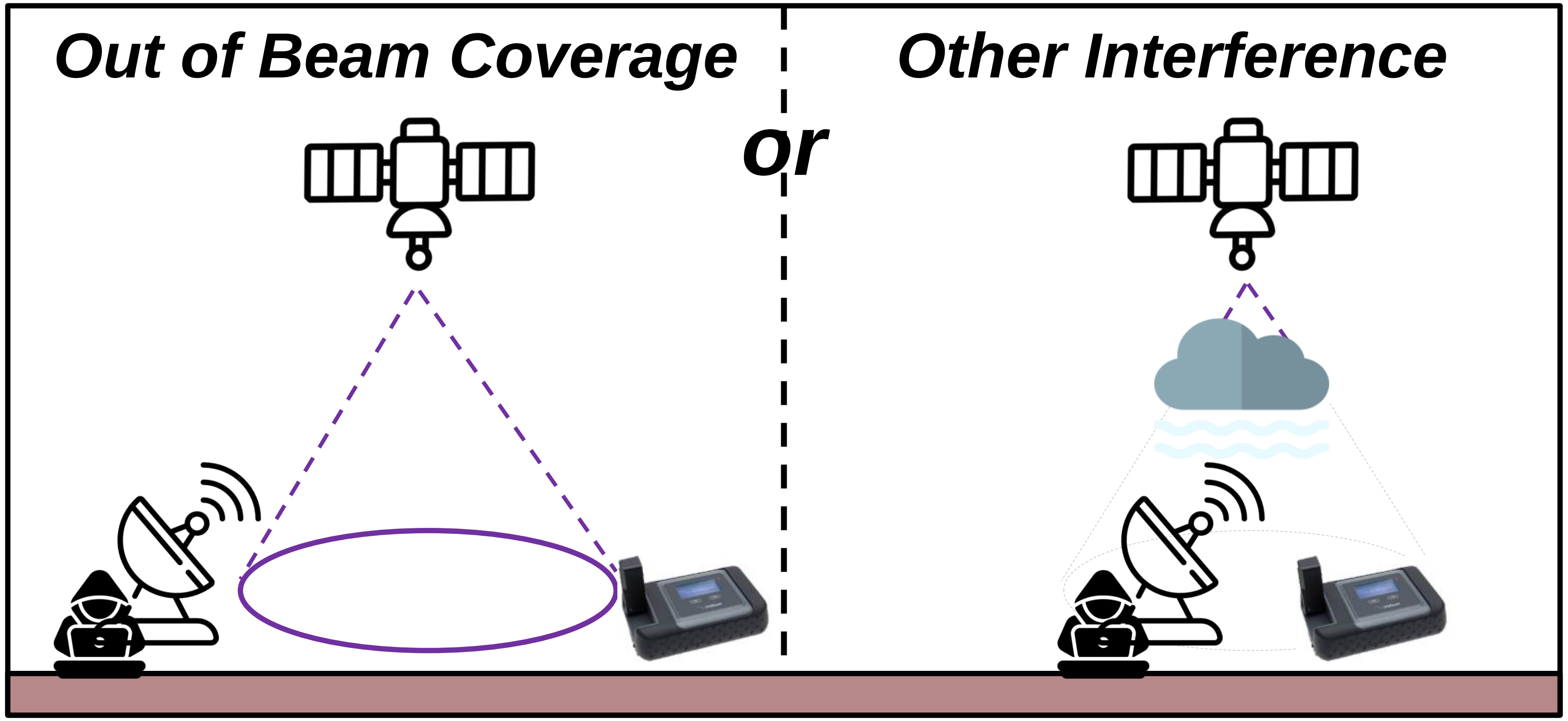
What about Starlink?



Discussion

Limitation of RECORD Attack

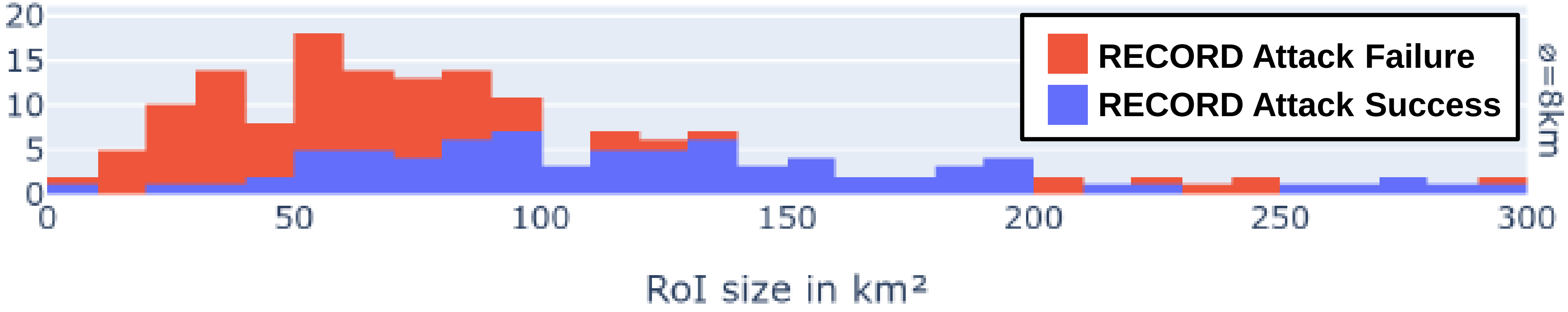
- ***Assumption 1***: All observers do not drop any packets



Limitation of RECORD Attack

- *Assumption 1*: All observers do not drop any packets
- ***Assumption 2***: Target device does not move far

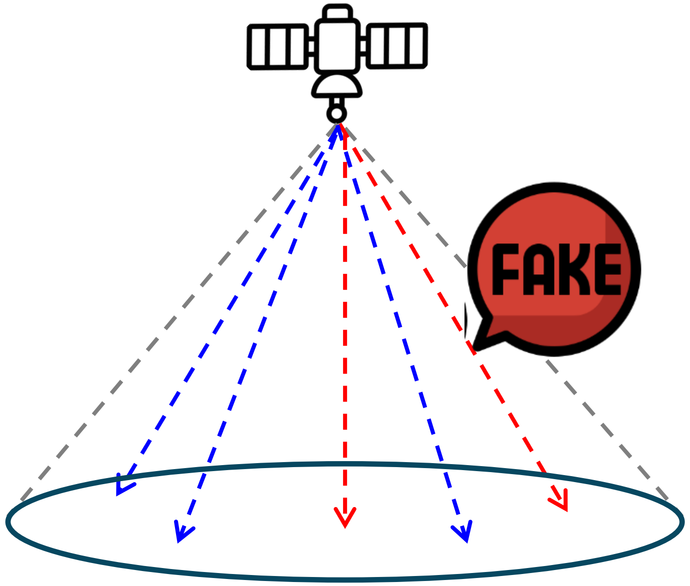
→ If the final **RoI range is outside the target device**, the RECORD attack is invalid



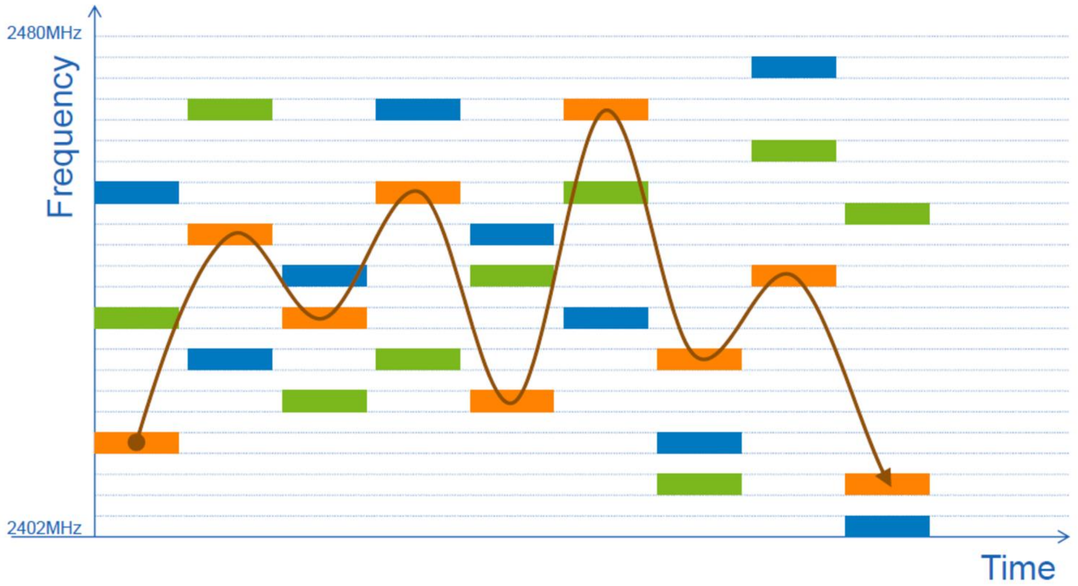
Discussion

Countermeasures of RECORD Attack

- **[User's]** Moving target device or limiting the communication time
- **[Manufacturer's]** Preventing the observers from identifying the traffic



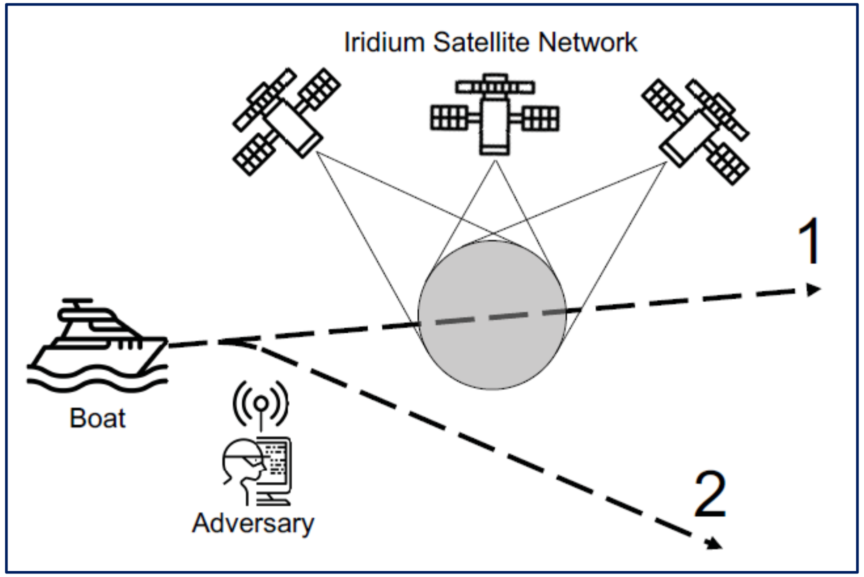
Generate Fake Traffic



Frequency Change or Channel Hopping

Related Work

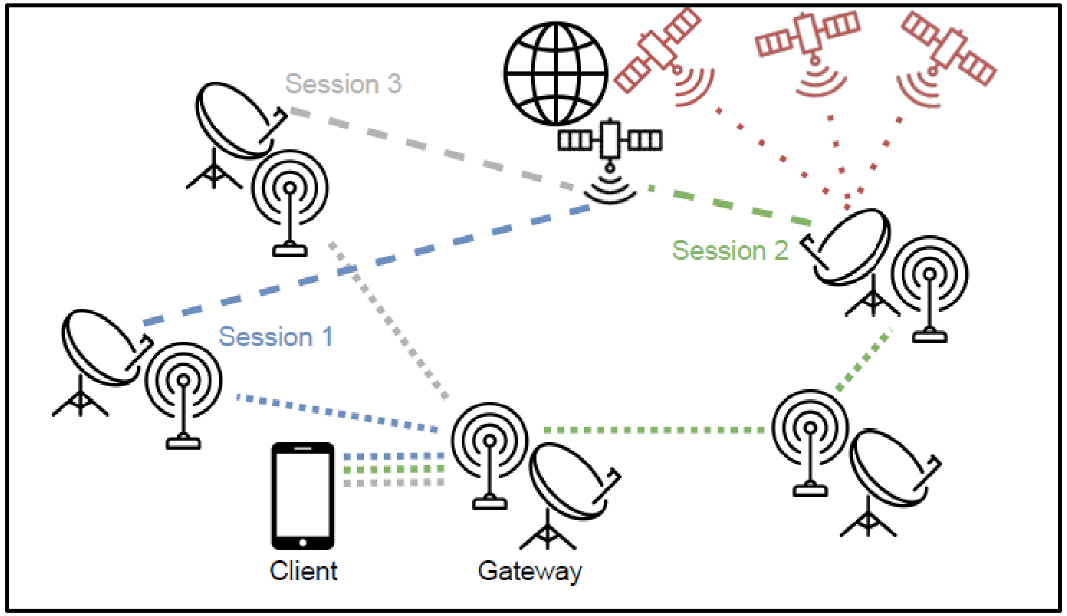
- **Gnss spoofing detection via opportunistic iridium signals**[1]
  - Leverage IRA message data to detect GNSS spoofing attacks



[1] G. Oligeri, et al. Gnss spoofing detection via opportunistic iridium signals. WiSec'20.

Related Work

- **Don’t Shoot the Messenger: Localization Prevention of Satellite Users[2]**



- Propose an infrastructure ***Anonsat***
  - Avoid geo-location attack in conflict zone
  - By distributed installation of multiple gateways

[2] D. Koisser, et al. "Don’t Shoot the Messenger: Localization Prevention of Satellite Internet Users," IEEE S&P'24

Conclusion

- Record attack is highly effective as an initial attack method for huge scale.

> ***Assumption 1***: All observers do not drop any packets

① More experimentation is needed to see how this affects RECORD attack, when the assumptions are not realized.

Conclusion

- Record attack is highly effective as an initial attack method for huge scale.

Assumption 1: All observers do not drop any packets

① More experimentation is needed to see how this affects RECORD attack, when the assumptions are not realized.

② If there are many users on same spot beam, is RECORD attack still efficient? The attacker may know that someone is there, but not who it is.

Good Question!(1/2)

- Could the RECORD methodology be adapted for real-time location tracking, and if so, what technical improvements would be needed?
- It seems beneficial to use the satellite's uplink signals for location estimation attacks in addition to RSS. Are there any limitations to such attacks?
- One limitation of the RECORD attack is the assumption of a static target device. How much movement would be required for the attack to become ineffective?

Good Question!(2/2)

- Could RECORD be adapted to exploit vulnerabilities in other wireless communication systems, such as terrestrial cellular networks?
- What are the practical limitations in scaling this approach across larger geographic regions or denser satellite constellations, such as Starlink's planned 42,000 satellites?
- Can the underlying methodology of RECORD attack be adapted for beneficial applications, such as search and rescue in remote areas or wildlife tracking using satellite-enabled devices?

Best Question!

① Yubin Lee: Satellite communication used to be a very minor field, with only specialized domains using it. With the introduction of Starlink and its rise in popularity, should we be more concerned about LEO satellite attacks?

② Zunnoor Fayyaz Awan: One way to make region determination harder would be to use a randomized mapping from a user to a satellite i.e. a user does not always connect to the nearest satellite covering his region. This would require multiple satellites to be covering a given region simultaneously, which might be a realistic scenario for very large constellations such as SpaceX's Starlink. However, there would come at the cost of performance. Given that localization of users of various services (including cellular communication and ground based internet) is already possible, is such a performance cost for anonymizing user location justifiable?

③ Pierre Noyer: The paper mentions the challenge of reliably identifying events other than the "general receiving event" in real-world scenarios. Could you discuss potential solutions to address this challenge? For example, how feasible is it to build an empirical visibility map for each sensor to account for obstacles and noise?

Thank you!