RECORD:
A RECeption-Only Region Determination Attack on LEO Satellite Users

Eric Jederman
RPTU Kaiserslautern-Landau, Germany
jedermann@cs.uni-kl.de

Martin Strohmeier
armasuisse, Switzerland
martin.strohmeier@armasuisse.ch

Vincent Lenders
armasuisse, Switzerland
vincent.lenders@armasuisse.ch

Jens Schmitt
RPTU Kaiserslautern-Landau, Germany
jschmitt@cs.uni-kl.de

Abstract

Low Earth orbit (LEO) satellite communication has recently experienced a dramatic increase of usage in diverse application sectors. Naturally, the aspect of location privacy is becoming crucial, most notably in security or military applications. In this paper, we present a novel passive attack called RECORD, which is solely based on the reception of messages to LEO satellite users on the ground, threatening their location privacy. In particular, we show that by observing only the downlink of 'wandering' communication satellites over wide beams can be exploited at scale from passive attackers situated on Earth to estimate the region in which users are located. We build our own distributed satellite reception platform to implement the RECORD attack. We analyze the accuracy and limiting factors of this new attack using real-world measurements from our own Iridium satellite communication. Our experimental results reveal that by observing only 2.3 hours of traffic, it is possible to narrow down the position of an Iridium user to an area below 11 km of radius (compared to the satellite beam size of 4700 km diameter). We conduct additional extensive simulative evaluations, which suggest that it is feasible to narrow down the unknown location of a user even further, for instance, to below 4 km radius when the observation period is increased to more than 16 hours. We finally discuss the transferability of RECORD to different LEO constellations and highlight possible countermeasures.

1 Introduction

Low Earth orbit satellite constellations such as Starlink, Kuiper and Oneweb are gaining momentum in the market of Internet access providers, promising worldwide, fast, and cheap Internet. This is not a new phenomenon, the Iridium constellation has been providing global telephone and data services to millions of users for 25 years.

In certain application scenarios and for some users of LEO satellite communication, location privacy is of utmost importance for operational security, such as for instance in the military domain. In the current Ukraine conflict, the Starlink constellation plays a crucial role for Internet access, even in critical infrastructure. Obviously, there is a high interest to not reveal even an approximate location of the Starlink receivers on the ground as they may be targeted by hostile physical means when discovered. Similar thoughts apply to activists, dissidents and other actors in areas without reliable ground infrastructure as illustrated in a case in Syria in 2012 [8].

Hence, in this paper, we investigate to what extent location privacy is threatened in LEO satellite communications. At first, one may conjecture that an attacker who wants to find the location of a satellite receiver would have an impossible task if the only thing they know is that the receiver is located in a satellite beam. Despite being only in an orbit between 200 and 2000 km, LEO satellite beams can be quite expansive and easily cover areas of the size of a big country such as Ukraine (an area of $603,700\ \text{km}^2$) sometimes even a whole continent such as Europe (an area of $10,523,000\ \text{km}^2$). In addition, classical wireless localization techniques such as multilateration with distributed ground receivers are not applicable at scale to satellite users as the uplink signals emitted by the terminals are typically oriented towards the sky, and can only be received at most a few kilometers from the users.

However, as we show in this paper this is not the end of the story. We present a new attack called RECORD (RECeption-Only Region Determination), which based on recording the *downlink* communication from a satellite reduces the *region* in which a targeted satellite user is located to an extent that is several orders of magnitude below the beam size of the satellites. In fact, equipped with the knowledge of this region, an attacker can subsequently perform an accurate positioning of a satellite user employing standard localization methods such as multilateration of messages being *sent* by the user. Hence, the RECORD attack can be seen as an enabling threat for a complete loss of location privacy. Crucially, even if the targeted satellite user never sends anything but solely receives (possibly unwanted) traffic, the RECORD attack results in a considerable loss of location privacy as we will demonstrate.

The key idea of the RECORD attack is to estimate the

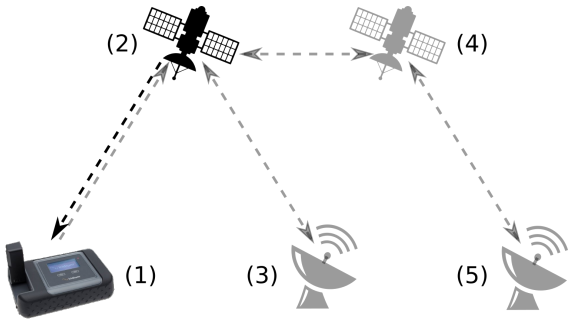


Figure 1: Satellite system schematic: A terrestrial user terminal (1) communicates with a satellite (2). The satellite either has a bent-pipe structure and forwards the signals directly to a ground station (3) or it can process the data and route messages to further satellites (4), which are sending the signals to their terrestrial target, a ground station or user terminal (5).

location of a satellite user based on the reception transition events of the different satellite beams as the satellites move towards and away from the user. We investigate the feasibility of this attack on our own Iridium communication and perform extensive additional simulations. Our experimental results reveal that by observing 2.3 hours of traffic, it is possible to narrow down the position of an Iridium user to a region with a radius below 11 km (compared to the satellite beam size of 4700 km diameter). Our simulations show that the region can be narrowed down further over time, for instance to below 5 km when the observation period is increased to 16 hours.

Note that the attack does not require access to the payload of the communication and thus works even on encrypted communication. This is in contrast to recent work that detected ships' locations in the unencrypted payload of LEO satellites [22]. Our attack is agnostic and works on all users communicating with a typical LEO system — as our experimental and simulative evaluation shows it depends mainly on the observation duration invested by the attacker.

Contributions This paper describes a novel attack to calculate the location region of a stationary terrestrial satellite user. It is based exclusively on observations of downlink receptions and the predictability of the footprints of a communication satellite system. We implement the RECORD attack on a purpose-built distributed satellite reception platform and conduct a measurement campaign using our own real-world data. To fully understand the effect of different parameters of the attack, we further provide a comprehensive simulative evaluation again based on real-world measurements. We observe that the attack is highly effective if sufficient observation time of the downlink satellite communication is invested; and that it can be boosted by an attacker with access to the packet contents in order to gain more knowledge that enables to restrict the area of the targets location even further.

Outline The paper is organised as follows: Section 2 provides the necessary background on the satellite system model and the properties to understand the RECORD attack, which is then described in detail in Section 3. In Section 4, we describe and measure our real-world implementation of the attack including our antenna beam model. With a simulative evaluation in Section 5 we provide further insights. To evaluate the potential location privacy leakage, Section 6 analyses the impact and limitations of the RECORD attack, potential countermeasures and ethical implications, before Section 7 discusses the related work. Finally, Section 8 concludes.

2 Background

2.1 Satellite System Model

In this work, we focus on LEO satellite communication systems with *packet-based communication*. A generic satellite communication system is pictured in Figure 1, where one terrestrial user device (1) is communicating directly with a satellite (2). This satellite is typically of a simple bent-pipe structure and directly forwards the signals from the user device to a ground station (3). But it is also possible for the satellite to process the messages and/or send the messages to other satellites (4) which forward them further (5). Both of these common satellite communication setups are vulnerable to our attack scheme. However, most of the actors and connections in the Figure 1 are greyed out, since they are not directly included in the attack, which will be described in Section 3. Only the target user device (1), the directly connected satellite (2) and the downlink from satellite to target device are required in the remainder of the paper.

One special property of LEO satellites is their high relative angular velocity while orbiting Earth. This causes them to quickly 'wander' across the sky, when seen from a terrestrial observer. As we are working with communication satellites, the receivable area of a satellite is thus also moving, as visualized in Figure 2. First, the satellite is moving over time from left to right. The antenna beams (1) are directed from the satellite towards the Earth and create a footprint (2) on the Earth's surface. Only receivers inside this moving footprint are able to receive signals from this satellite. This reliable and predictable property is crucial for the following work.

It is common that a communication satellite has multiple antennas on board, each of which create a so-called spot beam. This has several advantages: the satellite can focus and increase the signal strength in a certain area and also re-use frequencies across neighbouring beams. This approach is also taken by the satellite systems considered in this work, illustrated in Figure 3. Without loss of generality, the satellites pictured in all figures are shown with one major beam and no separate spot beams. This does not change the concept of the introduced attack but simplifies the explanations and improves the clarity of the graphics.

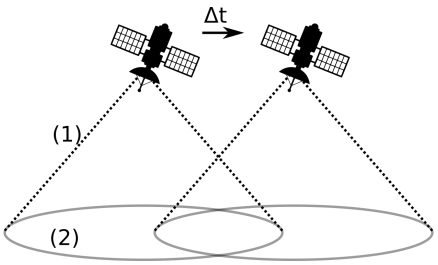


Figure 2: As a LEO satellite moves across the sky, antenna beams (1) and footprints (2) move across the Earth surface.

By design, a terrestrial user terminal is always covered by at least one spot beam during ongoing communication. The messages that are sent on the downlink from the satellite to the terrestrial user terminal are receivable in the whole beam, due to the broadcast nature of such a beam antenna. This is the second fundamental property that we exploit in this work.

2.2 Location Privacy Metric

In order to quantify the impact of our attack on the location privacy of terrestrial satellite users, we require a suitable metric. Wagner and Eckhoff [30] analyzed more than 80 different privacy metrics from the literature for different application fields. They describe different measures to classify adversary capabilities, usable data sources, and output measures.

Based on their work, we choose the size of the *uncertainty region* as a our natural target metric. Defined as the area where the transmitter must be located, it is an intuitive approach to understand the basic location privacy leakage. Throughout the paper we call it the region of interest (*RoI*). To calculate this region, Lamberts equal area map projection is used, as described in the Appendix 9.1. Obviously, the lower the *RoI*, the more accurately the position of the transmitter can be retrieved, and the bigger the privacy leakage of the user.

2.3 Communication Properties

As we are exploiting exclusively the received downlink communication, we define the properties and requirements regarding the reception of such communication.

First, we require one or more hardware receivers to observe the frequency band(s) of the downlink. To not miss any communication, either the whole frequency band must be observed or sufficient knowledge of the underlying communications protocol must be available to ensure a correct and complete recording. For labeling the observations reliably, a synchronized clock and the position of the observer is required. The observer may move during the observation, as long as the location is precisely known at any given time of message reception. In the extreme, this could even be a large distributed sensor network such as SatNOGS [18].

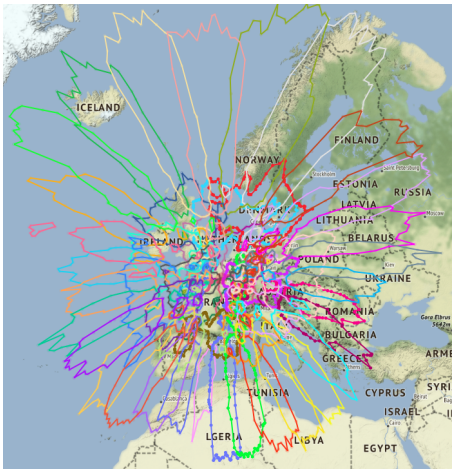


Figure 3: Footprint of a single randomly chosen Iridium satellite, comprising 48 antennas and their respective spot beams.

As we deal with packet-based communication, each packet is assumed to have a property to identify its intended receiver. This can be a device/target address in the packet header, a dedicated frequency channel, or an explicit time slot. It is crucial to note that it is not necessary to understand the payload of the packet, which is often encrypted as in the case of Internet traffic. The question how an adversary selects a specific target or victim is out of the scope of our work and we do not touch other user traffic in our measurements for reasons of ethics and privacy. However, in real-world systems it does not pose a hard problem, as there are typically less than a dozen satellite users in a typical spot beam. Traffic identifiers such as device/IP addresses, statistic traffic analysis or known communication patterns can be obtained through other means as shown in the literature even for encrypted traffic.

2.4 The Iridium Constellation

In this work, we use the Iridium satellite communication system to perform measurements and conduct a real-world implementation of RECORD. The Iridium system consists of 66 LEO satellites covering the globe at an altitude of 780 km. Iridium is the longest-running LEO constellation used by 1.9 million users globally, across military, government and corporate domains as well as by private individuals [10].

The Iridium satellite orbits are in north-south orientation with an orbital period of 100 minutes. In each revolution a satellite performs a uniform rotation, precisely aligned with its orbit period and trajectory. This rotation ensures the consistent alignment of the satellite's downlink antennas with the Earth's surface. A single satellite creates 48 spot beams and covers the size of Europe, as illustrated in Figure 3. A footprint of a single spot beam typically measures 400 km or more in diameter in its smallest dimension. All spot beams combined create a satellite footprint with a diameter of 4700 km.

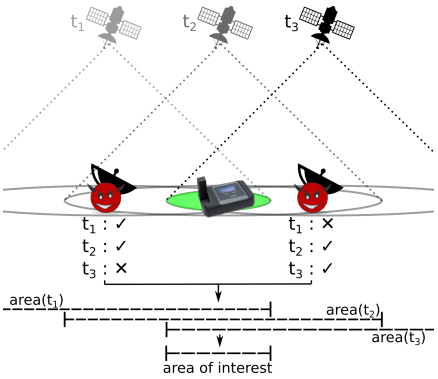


Figure 4: Schematic of the attack. Two observers receive downlink messages over time and combine their observations to estimate the location area of the terminal.

The spot beams alignment is fixed on the satellite. Over the span of a year we observed Iridium satellites and their beam alignments without detecting deviations in the resulting footprint patterns. This makes the Iridium system predictable and susceptible to the proposed attack.

3 Principle of the RECORD Attack

RECORD's goal is to gather information about the position of a terrestrial target device that communicates via a generalized LEO satellite system. Intuitively, the adversary records the freely available downlink communication (inside the spot beam) towards a victim's satellite device and extracts knowledge from the received messages to calculate the *RoI* where the target device is located. Since the attacker is only receiving signals, the attack is entirely passive and does not require any interaction with the target device or the communication satellite. The reason to use the downlink of the satellite communication is that the satellite antenna spreads its signal over the full footprint of the spot beam (see Section 2.1). This enables the attacker to receive messages intended for a specific device, over a large distance of hundreds of kilometers.

Figure 4 visualizes the simplified attack principle. The adversary controls two observers, which are recording the downlink traffic of the target device. At time t_1, the satellite is at the leftmost position and only the left observer can receive. As time progresses and the satellite moves, both observers are able to receive messages at t_2. At t_3 only the right observer can do so. These observed reception events are shown at the bottom for each observer, containing the recording time and location. In the next step, the attacker calculates the area that is covered by the antenna footprint for each observation time. Finally, the intersected area must contain the target.

The attack itself consists of three different phases, a modeling phase, a collection phase and finally the estimation phase.

3.1 Modeling Phase

In the *modeling phase*, the adversary employs one or multiple observers to gather data about the satellite antenna patterns, with the objective of constructing a so-called *satellite model* to enable precise antenna footprint calculations. This is achieved through the creation of a set of empirical antenna models using beam-specific status messages, as demonstrated in Sec. 4.2. By calculating satellite positions relative to the receiver, we derive an antenna model, describing the directional characteristics, i.e. the opening angles, for each satellite antenna. This set of antenna models is combined to the satellite model, modelling the full satellite footprint. Importantly, this phase is a one-time calculation for each satellite constellation.

3.2 Collection Phase

In the *collection phase* the attacker eavesdrops on the downlink communication to the target device. Therefore, it is necessary to identify the packets that belong to the user communication reliably over the whole observation period. The recorded messages are labeled with their time of receiving and the position of the recording. One important aspect is that the modeling phase and the collection phase are independent of each other. They can be conducted in an arbitrary order or even overlapping, using the same measurements.

3.3 Estimation Phase

The goal of the *estimation phase* phase is to combine the antenna model with the recorded messages to get an area of interest in which the target is located. To extract information about the target's position, the recorded messages are transformed into *observation events*, which provide knowledge of the antenna beam used by the target at the observation time and its respective footprint. By intersecting all antenna footprints of the observation period, we then decrease the uncertainty about the target's position.

We have six observation events: The *general reception* (e_{gr}) and *non-reception during communication* event (e_{ndc}) are two fundamental events that appear when the traffic of the target device is received or not. *Reception after handover* (e_{rh}) and *non-reception after handover* events (e_{nh}) occur when the attacker is able to detect beam-handover messages in the observed target traffic. *Sudden reception* (e_{sr}) and *sudden non-reception* events (e_{sn}) are extracted when an observer unexpectedly finds or loses the target traffic, which are likely to be caused by beam switches of the observer or undetected beam switches of the target device.

For each individual event the attacker calculates the *RoI* ($region(e)$) by the rules described in Appendix 9.3. In case of the e_{ndc} event, a negative *RoI* ($not\_region(e)$) is calculated. The resulting region ($region(E)$) is the intersection of all

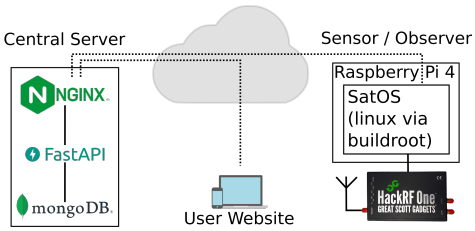


Figure 5: Architecture overview of the observer system.

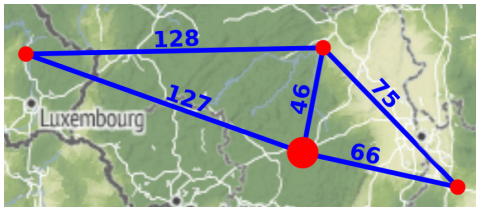


Figure 6: Geographical distribution of the three attackers (small dots) and the Iridium target device.

single regions from all observation events:

$$region(E) = \bigcap_{e \in \{E \setminus e_{ndc}\}} region(e) - \bigcup_{e_{ndc}} not\_region(e_{ndc})$$

For each observed event, the attacker calculates the positions of all satellites using public databases such as CelesTrak [14] or space-track [13]. The satellite positions are combined with the antenna model to calculate the footprint of each satellite antenna. Since the observation events are independent, we can combine multiple separate observation periods.

With the RECORD attack it is possible to gain knowledge from the recorded messages over a large distance and identify an area where the target device has to be located in. This may already provide the desired accuracy for the adversary (see Section 5.2). In case it does not, knowledge of this small area should be sufficient to launch more expensive localized follow-up attacks, such as traditional radio-frequency scanning or multilateration of the uplink communication which have much lower range but better resolution. We illustrate such an end-to-end attack combining RECORD with known methods in the next section.

4 Real-World Attack Implementation

To demonstrate that the RECORD attack is practical and works end-to-end in the real world, we collect traffic using our purpose-built Iridium sniffer and a distributed receiver network. We exclusively target our own Iridium device, which we subsequently attempt to locate. In the following, we explain our experimental setup and discuss the three attack phases.

4.1 Experimental Setup

In Figure 5 an overview of the observer system is given. A central server runs NginX, FastAPI and a monolithic database. The server provides a website to control and manage the system, enabling the creation of new observation tasks.

The heart of each observer is a Raspberry Pi 4 that is connected to a HackRF One with an Iridium antenna and a GPS- & LTE-shield. GPS reception is required to know the precise position of the sensor and to obtain a reliable time-synchronization. The LTE connectivity is an alternative to the WiFi and Ethernet connections of the Raspberry Pi to make the sensor easy to deploy in different environments. The electronics, besides the Iridium antenna and a power connection, are protected by a weather resistant box.

The Raspberry Pi is running a minimal Linux system created with buildroot, which we named 'Satellite data Acquisition Tool Operating System' (SatOS). Inside SatOS, a service automatically sends status reports to the central server and pulls for new tasks. Currently the major task is the collection of Iridium packets via gr-iridium. However, it is planned to enable the connection of different antennas to the sensor, enabling also the recording of other satellite constellations.

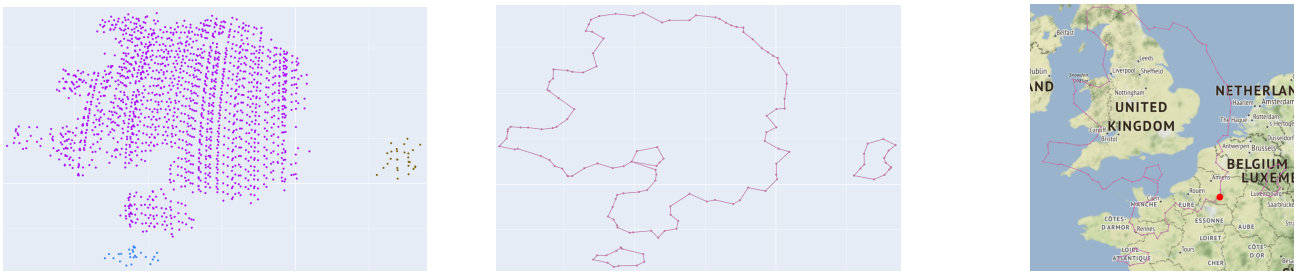
The reason we decided not to use the already available SatNOGS system [18] for our data collection is the different scope and capabilities. SatNOGS mainly targets open radio amateur frequency bands and the tracking/receiving of single satellites. For this work we required a tool to gather data from the complete satellite communication network, that may contain sensitive information.

For our measurements in the following, we used three observers distributed 127 km to the West, 46 km to the North and 66 km to the East of our research institution, represented by the smaller red dots in Figure 6. The large red dot in the center of the map is the location of the Iridium GO! device.

4.2 Phase 1: Modeling the Antenna Beam

For calculating the footprints of the satellite beams a model of each spot beam antenna is required. As previously mentioned, we conduct this modeling phase by collecting Iridium status messages, the so-called Iridium Ring Alerts. They are sent periodically every five seconds. Each message contains the number of the satellite and the beam antenna that was sending the message. By knowing the positions of the satellite and the observer at the receiving time, it is possible to calculate the sending angle of the satellite antenna. Over time a model emerges, revealing the opening angles of all satellite antennas. More details are in Appendix 9.2.

In the first phase of the RECORD attack, we used the observers to collect data of the Iridium system for two weeks and collected 328,000 ring alert messages. For each antenna-specific model, we combined the data from all observed Iridium satellites, since we did not find significant differences between the satellites' antenna patterns.



(a) Clustered measurements. (b) Optimized borders. (c) Projection onto Earth surface.

Figure 7: Example of the modeling phase showing measurements, calculated borders, and surface projection of Iridium beam 32.

Figure 7a shows the combined measurements for beam 32 of the Iridium satellite system. Each data point represents a beam 32 ring alert message, the position of the point represents the sending angle. Thereby the points represent the opening angles of the beam 32 antenna. We kept the full opening angles of every beam, even if they overlapped with neighbouring beams. In this way, the maximum receivable footprint of each antenna beam was extracted. The different point colors represent the different lobes. For many antennas we detected sidelobes, we kept them to obtain the maximum possible antenna footprint. Using the density-based spatial clustering for applications with noise (DB-SCAN) algorithm of the scikit-learn library, the measurements of each antenna were divided into clusters for each lobe of the antenna. We further processed each cluster to keep only the outer data points to represent the footprint. In this way, an efficient and lightweight model for calculating the maximum antenna footprint was created. Figure 7b shows the optimized antenna model of Iridium beam 32.

With a given satellite position, the resulting footprint of the optimized antenna model can be projected onto the Earth surface, covering the complete area where signals of the specific antenna can be received. For our example of beam 32 in Figure 7, we assumed a satellite position in the North of Paris with a North-directed orientation. This results in a complete empirical footprint, covering the whole of England and much of the surrounding area, as shown in Figure 7c. The combination of all 48 antenna models, each for one of the 48 spot beams of an iridium satellite, forms the satellite model. The result is visible in Figure 3, showing all beams superpositioned across the surface of Europe.

4.3 Phase 2: Recording the Victim Traffic

For phase 2, we placed our Iridium GO! device on top of a university building, with free view towards the horizon, as shown in Figure 18. The battery-powered device provides WiFi connectivity and with smartphone apps supplied by the manufacturer, it can be configured to provide an Internet connection via the Iridium satellite network. The device's legacy bandwidth of 2.4 kbps is too slow to comfortably browse modern websites but it still enables the sending and receiving of emails and text messages anywhere on the globe. For the RECORD attack, the bandwidth is irrelevant as we target the fact that there is any communication in the first place, rather than how much communication can be collected. Using this connection, we manually accessed several websites and created the required traffic for our attack. It is important to note that the type of the website and the precise traffic pattern are not relevant as long as any downlink traffic is generated.

Over the course of nine sessions spanning over eight days, we gathered a total of 5 hours of traffic data. Some measurement sessions were done on one day with 1-hour between sessions, while others featured a 5-day pause between measurements. This does not have a significant effect on the combination of the measurements, as detailed in section 5.4. The three observers in the West, North and East recorded the downlink and further processed the recordings locally to compile a list of received Iridium messages. For recording and demodulation, we used gr-iridium [4] and for parsing the packets the iridium-toolkit [5].

To first identify the downlink messages of a target device, one can exploit the connection setup, where a static TMSI is transmitted unencrypted in the downlink. The authentication in Iridium is a restricted version of the GSM authentication process. One of the restrictions is a static TMSI, which allows an attacker to identify devices during connection setup. To get the static TMSI of the target device the attacker can eavesdrop on traffic over a longer time and search for the targets name in unencrypted email or voice transmissions, which are standard in Iridium. Once an interesting transmission is found, one can backtrack the connection to the connection setup, where the TMSI was transmitted. We avoided this for ethical reasons by also recording the uplink and using the uplink channel frequency as a hint, since the downlink channel is always a neighbour of the uplink.

Once the target connection is found, it is easy to follow: A device that enters a spot beam is assigned a dedicated frequency channel. The Iridium network uses clear-text handover messages. Hence, when a device switches from one spot beam to another, the information which frequency channel will be used in the new beam is broadcast. This made it straightfor-

ward to follow a connection and resulted in a list of messages for our (own) target device to give to the estimation algorithm in the third phase of the attack.

There are other practical possibilities for an adversary to identify the traffic of the target device as already discussed in Section 2.3. For Iridium, creating a phone connection offers an additional possibility. Alternatively, it is also realistic to brute-force the locations of all devices in the targeted spot beams, which we also avoided for ethical reasons.

4.4 Phase 3: Estimating the Target Location

(a) Single antenna footprints. (b) Union of the footprints.

Figure 8: The observer (red dot) is able to receive both antennas. For e_{gr} events, the footprints of both are united.

The list of messages of our Iridium target device is transformed into a list of events, as introduced in Section 3.3. We used all our knowledge about the Iridium protocol and the available clear-text status messages to extract as much information from the messages as possible.

With the extracted events, it is possible to calculate the *RoI* for each event. To do so, we identified the satellite antennas with the help of our antenna model, created in phase 1 of the attack. For each antenna we calculated the footprint and depending on the type of event, the footprints are combined. As an example how this process can be visualized, in Figure 8a two antennas are receivable at the observer, the red dot in the middle. The footprints of those two antennas are calculated and in Figure 8b the union of both footprints is created. This represents the *RoI* for one single e_{gr} event.

Via the combination of many events and calculating the region that is shared by all events, the *RoI* is reduced further and further over time. Intuitively, if some seconds later the footprints are shifted several dozen kilometers to the North, the *RoI* is reduced to the overlapping part of both events.

4.5 Results

In total, we conducted 9 independent measurements, at the same locations, with a total uplink time of 5 hours. Table 1 shows the complete data of all 9 measurements. The measurements are ordered by their uplink duration. We also calculated the aggregate of all measurements. The four observations marked with $*$ added valuable information to the combined result, in the form of one edge of the final *RoI*.

measurement	duration	area estimation	event count			
			e_{gr}	e_{ndc}	e_{sr}+e_{sn}	e_{rh}+e_{nh}
1	288 sec	102534 km^2	665	0	0	9
2*	683 sec	81437 km^2	1269	51	5	4
3	1028 sec	81337 km^2	1404	19	1	13
4*	1463 sec	17118 km^2	3371	211	4	23
5	1715 sec	88292 km^2	2463	12	2	13
6*	2085 sec	3240 km^2	5337	93	7	27
7	2318 sec	47704 km^2	4422	14	1	33
8*	4044 sec	8654 km^2	8050	123	21	68
9	4237 sec	43152 km^2	7596	125	17	54
Effective Aggregate	8275 sec	383 km^2				

Table 1: Measurements ordered by the uplink time with their area estimations and their observed events. Event notations are described in Section 9.3.

In the end, these measurements 2, 4, 6 and 8, resulted in a combined length of roughly 2.3 hours, creating a target region of 383 km^2, which is equivalent to a circle with the radius of 11 km. This successfully illustrates the principle of this attack. Starting from an initial guess with more than 100,000 km^2, this is an improvement by a factor of 260 in a relatively short time. Reducing the estimation to an area of this size enables complementary attacks with a more limited range but higher precision, such as triangulation of the uplink signal, depending on the local conditions (see Section 4.6).

The relationship between observation time and size of the estimated area in Table 1 is blurred by the high variance of the estimation. This becomes especially visible when comparing measurements 5, 6, and 7: Measurement 5 with roughly 29 minutes has an area of 88,000 km^2, measurement 6 with 35 minutes only 3,240 km^2 — a fraction of the previous estimation. The following measurement 7 achieves an RoI of 48,000 km^2 with 39 minutes. This illustrates that the recording duration is not the most dominant factor influencing the *RoI*.

Instead, the number of events collected during each measurement is relevant. In particular, the high fluctuation among *ndc* events is striking. Consequently, we calculate the time per e_{ndc} rate by dividing the measurement duration by e_{ndc}, which reveals an interesting property that is illustrated in Table 6.

From this, we note two interesting observations: the measurements that successfully contribute to the combined evaluation are all in the upper half of the table. They contribute by having some of the borders of their individual *RoI* closer to the true position of the target device than all other observations. Thereby, the combination of only these four measurements recreates the result of the combination of all measurements. All four also have a good time-to-area ratio when compared with the other measurements. Therefore, this ratio is a promising property for future applications, in order to provide a solid basis for reliably performing setups. Finally, the positioning of the observers can play an important role in generating useful events. We analyse this in Section 5.3.

Distance (km)	Noise Level (dB)	Signal Level (dBm)
0.226	-109.43	-17.27
2.243	-109.26	-21.01
2.692	-109.89	-24.2
5.184	-109.84	-26.08
31.056	-109.63	-39.92

Table 2: Median signal strength of the Iridium GO! uplink recordings at known distances.

4.6 The Last Mile

4.6.1 Basic Signal Strength Modelling

The RECORD attack can be used to passively determine a small *RoI* in a first step over a large, continent-sized area. In a second step, more expensive and locally-restricted techniques from the literature can be applied within the *RoI* to localize the target more precisely — if it is transmitting uplink data to the satellite system. One possibility to localize a device is to use true-range multilateration techniques based on the received signal strength (RSS) as introduced by Bulusu et al. [2]. To assess the effective range of traditional RSS sensing and range finding techniques in ground-to-LEO communication, we conducted several signal strength measurements targeting our Iridium GO!. The line-of-sight range between the Iridium GO! and our receiver varied between 200 m and 31 km. For recording and processing the signals the *gr-iridium* and *iridium-toolkit* libraries were used. During each measurement we exchanged several emails via the Iridium email portal to generate the necessary traffic. The source identity of the captured traffic could be verified by observing the plaintext login credentials of the used Iridium email account in our recordings. In Table 2, the observed background noise and the signal level during each measurement campaign are given. Each measurement lasted roughly 15 minutes.

The measurements show that Iridium GO! signals can be received at a distance of more than 30 km. The signal levels in Table 2 suggest that in theory also larger distances could be received. However, in reality, larger distances on the ground with line of sight are rare. Therefore, this is a reasonable upper bound, when considering the distance where a Iridium GO! can be precisely located by uplink measurements.

4.6.2 Receiver Localization

To perform uplink measurements to localize an unknown receiver position, we consider the hilly and wooded landscape surrounding our experimental setting. We conduct several measurements at elevated locations with good view of the surrounding area. We start with four measurements well distributed near the boundaries of the *RoI* created previously. Only at measurement point two, we successfully received uplink traffic of our target device, indicating that it is in range. Consequently, we conducted a fifth measurement close to that location. All measurements are listed in Table 3. Using Friis' transmission formula and the measurements from Table 2 as a reference model, we calculate an assumed distance between the target and the measurement locations.

Location	Noise Level (dB)	Signal Level (dBm)	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

Table 3: Median signal strength of the Iridium GO! uplink recordings at unknown distances in last mile attack.

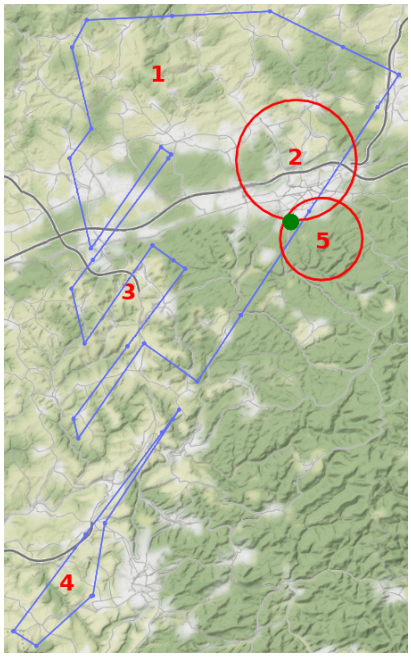


Figure 9: Last mile example: The calculated *RoI* (blue polygon), with the positions of five uplink measurements (red numbers) and the target device (green dot) close to the estimated location.

In Figure 9 the *RoI* is shown in blue, while the five signal strength measurement locations are numbered in red. The locations two and five are surrounded by circles that indicate the modelled distance of the Iridium GO! sender. Only the Western intersection of the two distance circles is inside the *RoI* — and is thereby our final position estimation. The real location of the device is shown as a green dot, which is 457 meters away from the estimation. Further measurements from additional positions can be taken to reduce this estimate even more.

A much simpler but less precise alternative to local uplink measurements is to apply a point estimator to the already calculated *RoI*. Calculating the centroid of the region is a straightforward baseline approach for this. The precision of

this estimator naturally depends on the size of the *RoI*: our simulations indicate that the centroid estimator has an average distance error to the target location of 30% of a circle's radius, assuming a circle with the area equivalent to the *RoI*.

Using the aggregate *RoI* of 383 km^2 from the measurements, this indicates a circle radius of 11 km. In contrast, the centroid has a distance of 8 km to the device location.

5 Simulative Evaluation

Besides the real-world measurement campaign, which illustrated the feasibility of the RECORD attack in principle, we also conducted comprehensive simulations in order to gauge the parameters of the different attack dimensions. This helps evaluating more precisely which characteristics of the system leak the most location privacy information. We focus in particular on the duration of the measurement period, the knowledge of the attackers about the system, and the number of observation devices.

The code of the simulation is published on GitHub: https://github.com/ErJedermann/RECORD.git.

5.1 Simulation Setup

For the simulations we generate artificial observations to evaluate the performance of different attack scenarios. We implemented the simulation in Python with intense usage of numpy vectorization. The simulation is designed to run at least 100 iterations with a fixed parameter set, introduced in this section. In the first part of each iteration, the artificial observations are generated. The second part provides them to the estimation algorithm and evaluates the computed *RoI*. Depending on the selected parameters, the computation time for one iteration matches the simulated observation duration, thus simulating one hour can also take up to one hour.

For generating the artificial observations, we used real satellite position data from the non-profit organisation Celestrak to ensure realistic behaviour and placement of the satellites. The starting time of the simulations was randomly chosen in a 24h interval around the creation time of the satellite data, to ensure their validity. The starting location of each simulation was randomly chosen up to a latitude of 65 degree north/south. To avoid unrealistic behavior, we decided to limit the placement of scenarios, since the simulated Iridium constellation turns off outer spot beams as the satellites approach the poles to reduce overlaps. The attacker's observers were equally distributed on a Fibonacci grid[27], placed around the starting location with a distance d_{obs} between the observers. The target device was placed randomly around the starting location, up to a distance of d_{obs}. More details about the observer placement are available in appendix 9.5. In Section 5.2, we used $d_{obs} = 100$ km, inspired by the closest neighbour distances in the real-world setup, shown in Figure 6. After this, in Section 5.3 the distance was varied.

Attacker	Observers	Beam Model	Event Types
1	1	noisy	weak
2	3	noisy	weak
3	3	strong	weak
4	3	strong	strong

Table 4: Properties of the simulated attackers.

We used four attacker models with different capabilities to evaluate the impact of distinct properties on RECORD. Available capabilities may vary between LEO constellations and based on the attacker's resources. In the following, we discuss three properties, a summary is provided in Table 4.

Observers: Increasing the number of observers enables the attacker to gain information about the signal reception at multiple locations at the same time. In the evaluation in Section 5.2, it will vary between 1 and 3 receivers. In Section 5.3, we also simulated up to 12 observers.

Beam Model: The precision of the beam model used for the evaluation. As a strong beam model we used the same model during the evaluation as for the generation. To weaken the beam model, we added white noise to it that increased the footprint, with a mean of 6.7 km. This is the distance an Iridium footprint moves in one second.

Event Types: The usable event types represent the accessibility of the satellite system to internal information. Weak event types are observations from the outside — a message is received or not. Strong event types allow the usage of internal information (e.g., handover messages).

Knowing the locations of the target, of the observers, and the start time of the simulation, we calculated the positions of all satellites of the Iridium constellation. Every second, the closest satellite and its best aligned antenna towards the target device were determined. To achieve realistic behaviour, we used the satellite antenna beam model from the real-world attack in Section 4.1. The selected antenna was the communication endpoint of the target device. For each observer we checked if it is located in the same footprint as the target device. Depending on the result a message receiving event for the receiver was created. All events discussed in Section 9.3 were generated at this point.

The simulation provides the generated event lists and observer positions to the attack algorithm to determine the final smallest *RoI*. To evaluate the quality of the *RoI* calculation, the resulting area of the returned estimation is used.

5.2 Observation Duration

We first vary the observation duration between 1 minute and 4 hours, shown in Figure 10 for the four different attacker types.

To obtain a better feeling for the areas in Figure 10 we

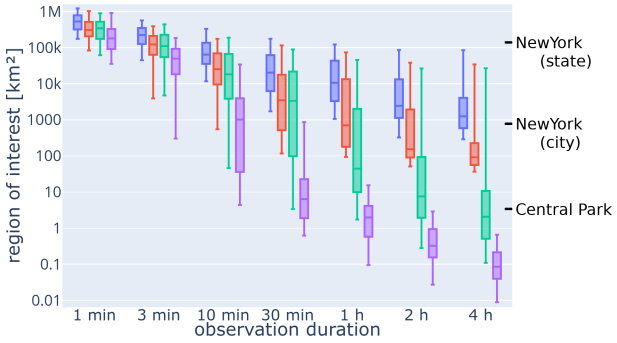


Figure 10: Simulated area estimations of different attackers (attacker 1 - 4: blue, red, green, purple) over different observation periods from 1 minute to 4 hours. Log scale.

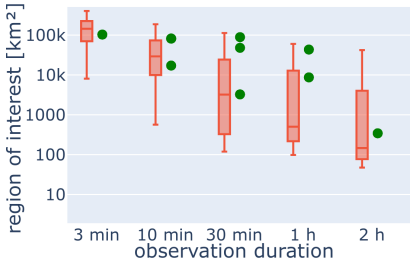


Figure 11: Attacker 2 vs. real world (green dots).

added the areas New York State (141300 km^2), New York City (784 km^2) and the Central Park in New York (3.41 km^2) as reference points.

According to the expectations, a longer observation time results in a better location estimation of the target. All attacker variants start with areas between 100,000 and 1 million km^2 at one minute. It is clearly visible that more advanced attacker types are reducing faster their area estimations than more limited attackers. While attacker 1 reaches 10,000 km^2 after 1 hour of observation, attacker 4 is already at 2 km^2.

At four hours, attacker 4 has reached a median area of 0.086 km^2, which corresponds to a circle with a radius of 166 meters. A more realistic scenario in most cases is attacker 2 with limited information but a few distributed observers. After 1 hour, this limited attacker attains an area of 700 km^2, which reduces to 92 km^2 after four hours.

To compare the simulations with the performed real-world attack, Figure 11 shows the simulations of attacker 2 next to the *RoI* of each measurement from Table 1. The results of attacker 2 are best-fitting to our measured results and also its properties from Table 4 are matching our expectations. Thus, we can expect that improvements on our real-world results are realistic with further measurements.

To analyze the improvements for longer observation periods of up to 16 hours, we simulated a realistic attacker for an increased observation duration (Figure 12). The median size of the *RoI* decreased down to 48 km^2, which corresponds to a

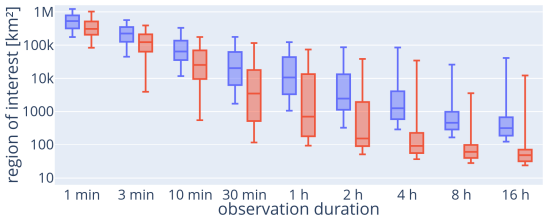


Figure 12: Long-term simulation of attacker 1 and 2.

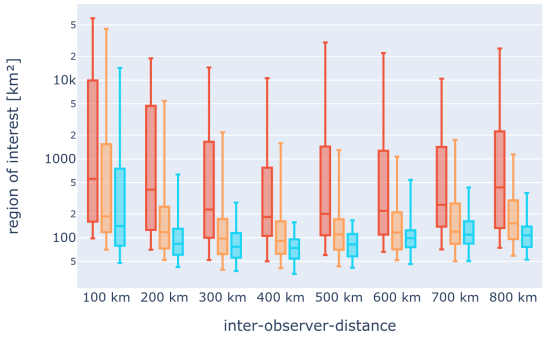


Figure 13: Observer number and spacing. Attacker type 2 with 3, 6 and 12 observers, respectively (red, yellow, blue).

circle with a radius of 3.9 km.

We note that the results of attacker 4 have to be interpreted with care. We expect them to be the upper bound of the RECORD attack. As already mentioned, the antenna beam model used in the evaluation for this attacker was a perfect representation of the ground truth, used for creating the measurement events. To approach this performance in reality is a challenge. This is discussed further in Section 6.2.

5.3 Observer Placement

Placement and number of the utilized observers are the main factors that the attacker can influence. To evaluate the impact of these two parameters, we conducted additional simulations.

First, we examine the observer placement by varying the space between them from 100 to 800 km while fixing the observation duration to 1h. Additionally, we simulated attackers with 3 (red), 6 (yellow) and 12 (light blue) observers, respectively. The evaluation results are available in Figure 13.

All attacker variants, independent of the number of observers, are most effective with a spacing of around 400 km between observers. This is roughly the size of the diameter of a single spot beam in the Iridium constellation (see Section 2.4). This finding supports our assumption that the optimal observer placement depends on the spot beam size of the satellite system.

By increasing the number of receiving observers from 3 over 6 to 12, the median *RoI* reduces from 183 to 91 and 74 km^2, for the optimal 400 km spacing setup. Notably, the variance in size of the resulting *RoI* is much reduced. Besides

the increased performance, it is obvious that the covered area of the attacker scales with the number of observers. For a spacing of 400 km, 3 observers cover 418 and 12 observers cover 836 km^2. However, we can also see that even large inter-observer distances of 800 km remain effective, with 107 km^2 for 12 observers, making RECORD a viable attack across countries and continents.

5.4 Robustness of Fragmented Observations

To support our statement from Section 4.3 that multiple, separate, observations can be combined over time in a robust and stable fashion, we conduct simulations with fragmented observations. We simulate an attacker type 2 with 6 observers and 400 km spacing between them. The attacker recorded traffic for 120 observation intervals of each 30 seconds. Between two intervals, a break of 10 minutes was taken to ensure their independence. The 120 independent intervals were appended to create one combined observation with a total duration of 1 hour, which was used to perform the *RoI* estimation.

The resulting *RoI*s of the fragmented observations had a size of 42, 64, 97, 162 and 557 km^2 (5th, 25th 50th, 75th and 95th percentile). The comparable *RoI* of a continuous 1 hour observation are has a size of 41, 62, 91, 161 and 1579 km^2. Both results are close together and are in the normal variance for this setup. So no significant difference in the resulting *RoI* between those two scenarios was found. This supports the statement that multiple observations can be combined without causing significant drawbacks or advantages.

5.5 Moving Targets

We now extend RECORD to simulations with a moving target. We simulate attackers of type 2 with 6 observers, 400 km observer spacing and 1 hour observation duration. The random way point model by Johnson & Maltz [12] is used for the victim movement. The movement area is placed inside the area covered by the observers, similar to the target location described in Section 5.1. The victim moves in a straight line from a random start to a random destination inside this movement area with a velocity between 3.6 km/h and 50 km/h, somewhere between a walking human and a car driving in a city. At the destination, the victim pauses randomly up to 3 minutes before moving to the next random location.

The diameter of this movement area is our target variable, which is varied between 1 and 8 km. Crucially, we consider an estimation *invalid* if a single of the random way points is outside the final *RoI*.

The results of this simulation are shown in Figure 14. The four histograms reflect the four simulated movement area diameters of 1, 2, 4, and 8 km. Immediately, there is a visible difference in validity: for diameters of 1 and 2 km, there are no invalid estimations found. As the movement diameter of

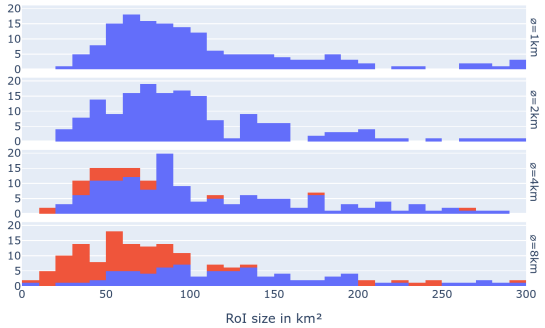


Figure 14: Histograms of valid (blue) and invalid (red) *RoI* estimations at different victim movement diameters.

the victim increases to 4 and 8 km, invalid estimations happen 13% and 49% of the time, respectively, meaning that the victim has left the *RoI* at least partially during observation.

Naturally, as the estimated *RoI* gets smaller, the rate of invalid estimations increases. For 8 km, at a *RoI* size around 50 km^2, 75% of the estimations are invalid, while at 100 km^2 only 30% of the estimations are. This is an expected effect since the probability for way points to move outside the *RoI* increases as the *RoI* gets closer in size to the movement area.

6 Discussion

6.1 Deployment Example

To illustrate the practicality of RECORD over large surveillance areas, we calculate the number of observers needed to cover Europe and compare it to a conventional localization approach against an actively communicating target.

A typical localization hybrid using angle of arrival and RSS [3] can localize a sender within the full reception area of a single observer. Thus, it is more efficient when compared to other approaches such as multilateration, multiangulation or pure RSS, which need additional infrastructure. Using the maximal range measured in Section 4.6, a radius of 31 km, equalling an area of 3019 km^2 per observer can be monitored. Monitoring an area of the size of Europe, 10.523 million km^2, would require 3486 observers, ignoring the fact that achieving line of sight for the whole area is unrealistic.

Using the placement strategy of Section 5.3 and a spacing of 400 km, RECORD requires only 58 observers to cover an area the size of Europe, a reduction by a factor of 60. A more aggressive approach with a spacing of 800 km has a slightly decreased performance but requires only 15 observers, a hardware reduction of factor 230.

6.2 Limitations

A fundamental assumption of RECORD is that the target device does not move too far during the observation period. The

intersection calculation always removes positions from the *RoI* that are not possible at that point in time. If the target device moves too far to an area that was removed previously, its new position will never be added again to the *RoI*. The generated observation events from the new position can reduce the area of interest to zero after some time, indicating that the device has moved, and the localization has failed.

A second challenge that remains open is the reliable identification of other events besides the 'general receiving event' in practice. In the simulation the assumption was made that all observers have a perfect view of the sky and do not drop any packets. In reality, obstacles and noise prevent a perfect reception of satellite signals. Then the challenge is to distinguish between messages that cannot be received due to such obstacles/noise or due to being outside the antenna beam. One possible approach to this challenge is to build an empirical visibility map for each sensor, thus taking into account when satellites are in non-visible areas.

6.3 Countermeasures

The assumption of a static target device shows one of the most effective countermeasures: A moving target device is much harder to detect, as already explained. This is related to the fact that a certain number of observation events is required to estimate the position. So limiting the number of usable observation events is an effective way to preserve some location privacy. This is either possible by limiting the communication time directly or by moving the device to a different location and thereby preventing the combination of observation events before and after the relocation. The frequency of relocations and the distances between the locations affect the preserved location privacy. But all this requires potentially inconvenient actions from the satellite user.

A second type of countermeasures aims at preventing the observer from identifying the traffic of the target device. Without the ability to reliable identify the target traffic, not many communication events can be extracted. This makes the location estimation much harder for an adversary. Techniques as generating artificial traffic, rolling identities or unpredictable channel hopping of multiple devices are just two possibilities to hide the real traffic of the target device. Such countermeasures have to be implemented by the operator of the satellite communication system.

6.4 Applicability to Starlink

The RECORD attack principle is also applicable to other LEO constellations, including Starlink with its millions of users. Starlink, as a highly-publicised and fairly recent operational newcomer, shares the same fundamental network characteristics that make it vulnerable to attacks on users' location privacy. As of May 2023, there were over 4,000 Starlink satellites in orbit and operational, with plans for 12,000 or even 42,000 satellites forthcoming. While not much is publicly known, some technical information about the antenna beams can be derived from official FCC documents [21, 31] and be used to model the antennas. According to the documents, the antenna coverage area should be inside the -3 dB zone which, according to the antenna beam contours is at roughly 2.2^o from the beam center. At an altitude of 550 km this means a spot beam footprint diameter of 42 km at nadir.

Attacker	Observers	Beam Model	Event Types	d_{obs}
3a	1	strong	weak	40 km
3b	3	strong	weak	40 km

Table 5: Properties of the simulated Starlink attackers.

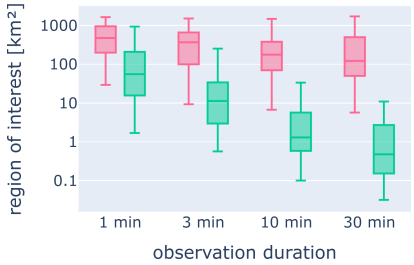


Figure 15: Simulating Starlink attackers 3a (red) and 3b.

Table 5 gives the parameters of simulated Starlink attackers. Both are analogous to attacker 3 in our Iridium setup, with a single observer for attacker 3a and three observers for attacker 3b. Due to the much smaller size of the spot beams, the distance d_{obs} was set to 40 km.

The smaller spot beam also reduces the starting size of the *RoI*: For attacker 3b in the Starlink simulation the median is 56 km^2, compared to 342k km^2 for attacker 3 in the Iridium simulation. Beyond this starting difference, the Starlink attacker 3b converges faster with 2.3% (10 minutes) and 0.85% (30 minutes) of their original starting size, compared to the Iridium attacker 3 with 5.3% (10 minutes) and 1% (30 minutes) of the starting size. This faster convergence is likely caused by the higher frequency of handovers for the Starlink constellation. Overall, the RECORD principle tends to become more accurate with more satellites and handovers but requires more receivers on the ground due to smaller beams.

6.5 Attack Impact

The impact of the RECORD attack on LEO-constellations is manifold: currently Iridium has 1.9 million users around the world and growing. Other LEO constellations such as Starlink (1 million terminals released in Q3 2022), OneWeb and Kuiper will multiply the number of satellite users globally as their ease of access and bandwidth is attractive for many user-bases, in particular in areas without sufficient, reliable or trustworthy ground infrastructure.

We believe this inherent characteristic of many satellite user

groups is what makes the attack impactful. Satellite ground-stations are used by groups of interest such as investigative journalists, activists, government employees and the military, in particular in potentially hostile areas. While it is possible to scan locally for satellite phones' radio emissions, and the satellite service provider naturally also knows the exact position, our attack enables this knowledge for many other groups. Tracking the home base of a target person thus becomes possible for anybody as long as they can place an Iridium sniffer within the reach of a satellite beam, which may easily be in a different country. As time is the main ingredient for accurate localization, privacy-conscious groups should thus strongly consider using their LEO-based communication devices for periods of time at the same position.

This is consistent with advice given by the Committee for Protecting Journalists, which recommended already a decade ago to limit phone use to 10 minutes at a time [8]. However, this advice was aimed mainly at local radio frequency tracking or against the sniffing of weakly encrypted or unencrypted content that might give away the position. With the presented approach even many short transmissions over a long period of time could be dangerous for such vulnerable groups. On the other hand, fairly mobile units for example in the Ukraine war with a Starlink terminal are less likely to be impacted, as their general presence is known and the time/accuracy trade-off is unlikely to be problematic for them.

6.6 Ethical Considerations

As with any potentially network- and privacy-infringing attacks, we took careful considerations to minimize any negative impact on real users. As such, we only passively captured our own communication, which was generated with very low bandwidth as not to impact the service quality of the Iridium system. In order to not make it too trivial to exploit our approach, we also do not release the antenna model, which after (extensive) one-time generation is highly transferable between all Iridium satellites.

Overall, we believe that it is more important for satellite users to know about potential location privacy leakage of their setups, even when they only use it to receive data. This knowledge enables users to protect themselves, and satellite providers to consider this in future system designs.

We publish the code for the simulation and analysis. We do not publish the conducted measurements and the resulting antenna beam models, as they can be used to perform the proposed attack in reality, as we demonstrated.

7 Related Work

Wireless physical-layer security is a longstanding research area, from small sensors to satellites. Canonical overviews are provided for example in [6, 24]. We briefly cover the related work in the areas of wireless localization and privacy in general and in satellite networks in particular.

7.1 Wireless Localization

The localization of wireless transmitters is a popular research discipline and has many applications touching on security (verifying the true location of transmitters) and privacy (leaking transmitter location to eavesdroppers). We discuss the prevalent approaches and how they differ from RECORD.

Opportunistic localization of wireless transmissions These approaches require the target to actively transmit data, which is received opportunistically by the localizer in one or more locations (i.e., the receiver does not transmit itself). Many wireless signal characteristics have been exploited in the literature to estimate or verify positions of such transmitting objects, including time of flight, time difference of arrival, angle of arrival, Doppler shift and RSS [1].

Opportunistic localization and positioning is crucial to many applications. Time difference of arrival for example is applied at scale in the Global Positioning System (GPS) and multilateration of aircraft. Indoor localization has seen use in contact tracing [29], asset tracking and process automation. [17] provides an overview of localization methods.

All of these localization methods fundamentally require the target to be actively transmitting data, and often a line of sight. In case of exploitation by an attacker, victim transmissions must happen while the attacker is present and in range. In contrast, RECORD only needs the target to be receiving data during the attacker's presence in the same satellite beam.

Radar Radar systems transmit electromagnetic waves and exploit the reflection of a target object to detect and localize it. This class of approaches does not require the target to transmit data but is not stealthy as, often very strong, transmission sweeps are conducted by the localizing entity [25].

Here, passive radar [28] is an interesting extension, whereby the localizer opportunistically exploits existing radio signals, such as from television stations, and their reflections in order to stealthily locate the target. However, like all radar detection, it is generally not applicable to ground targets.

Cellular Networks In cellular networks, mobile users are positioned within a static radio environment established by network base stations. Typical localization approaches are proximity, multiangulation, multilateration or fingerprinting based algorithms, that rely on RSSI, TOA or TDOA [7, 16]. There are crucial differences to our approach. The RECORD attack is based on the covered area of the network cell (spot beam) rather than on RSSI, TOA or TDOA. We exploit the continuous and predictable change of the network access nodes (satellites) rather than relying on it static environment.

Also the party, gaining the location information is neither the network operator, nor the user of the network but an outside third party. And the large scale, our attack can be deployed is unmatched compared with other approaches.

7.2 Location Privacy in Mobile Networks

By and large, the focus on mobile location privacy has been on smartphones and their users, including many relevant attacks exploiting privacy leakage on the physical layer.

During the wake of the Covid-19 pandemic, privacy-preserving digital contract tracing using Bluetooth Low Energy (BLE) has gained significant prominence as the DP3T proposal [29] was implemented in billions of smartphones worldwide. DP3T relies on identifying proximity of other users through radio frequency ranging.

Givehchian et al [9] evaluated location tracking attacks on BLE. By fingerprinting beacons on the physical layer, an attacker can effectively bypass cryptographic privacy protections built into applications such as digital contact tracing.

In the work perhaps closest to ours, LTRack [15] allows adversaries to extract both device locations and identifiers by passively sniffing the up- and downlink of LTE phone networks. LTRack illustrates the power of passive localization attacks indoors, reaching an accuracy of several meters.

7.3 Satellite Security

Security and privacy in satellite networks have recently enjoyed a renaissance in the academic community.

In 2020, Pavur et al. outlined the ease of eavesdropping on the downlink contents of unencrypted legacy geo-stationary satellite systems [22]. It illustrated that it is feasible to identify the traffic of a specific user in the same satellite beam.

Oligeri et. al. [20] used Iridium Ring Alert messages to verify their own position and detect spoofed GPS signals.

Recently, Sabbagh et al. [23] show how a receiver can determine its own position using pseudo-ranges from a single known LEO satellite. While achieving location errors below 1 km, this approach requires direct timing measurements at the receiver and is not applicable to a third-party attacker.

In [11, 19, 26], the authors propose several alternative systems in order to authenticate communication satellites based on physical properties. They authenticate the satellite by using a fingerprint of the satellite sender hardware or the time difference of signal arrivals at multiple receivers, respectively.

8 Conclusion

We have described a novel attack on LEO satellite systems that leads to significant leakage of location privacy for their users. The RECORD attack exploits the fact that for such systems the target satellite in LEO frequently changes for the communicating ground user. As they overfly the horizon, satellites and their specific antenna beams leak positional information, which, over time, can give away a user's position.

Using an empirical model for Iridium, we passively exploited the observed downlink communication of a target device in order to estimate its location. The RECORD attack is impervious to encryption and only requires the identification of a device in the downlink. We implemented it in the real world with commercial off-the-shelf hardware to show its feasibility. Through further theoretical and practical evaluation, we showed that with only four hours of observation, the uncertainty region can be reduced to less than a few km^2 after which conventional localization methods may be deployed.

References

[1] Isaac Amundson and Xenofon D Koutsoukos. A survey on localization for mobile wireless sensor networks. In *International workshop on mobile entity localization and tracking in GPS-less environments*. Springer, 2009.

[2] Nirupama Bulusu, John Heidemann, and Deborah Estrin. Gps-less low-cost outdoor localization for very small devices. *IEEE personal communications*, 7(5), 2000.

[3] Y.T. Chan, F. Chan, W. Read, B.R. Jackson, and B.H. Lee. Hybrid localization of an emitter by combining angle-of-arrival and received signal strength measurements. In *2014 IEEE 27th Canadian Conference on Electrical and Computer Engineering (CCECE)*, 2014.

[4] Chaos Computer Club München. Iridium burst detector and demodulator, 2023. https://github.com/muccc/gr-iridium.

[5] Chaos Computer Club München. A set of tools to parse iridium frames, 2023. https://github.com/muccc/iridium-toolkit.

[6] Boris Danev, Davide Zanetti, and Srdjan Capkun. On physical-layer identification of wireless devices. *ACM Computing Surveys (CSUR)*, 45(1):1–29, 2012.

[7] José A del Peral-Rosado, Ronald Raulefs, José A López-Salcedo, and Gonzalo Seco-Granados. Survey of cellular mobile radio localization methods: From 1G to 5G. *IEEE Comm Surveys & Tutorials*, 20(2), 2017.

[8] Frank Smyth. Caveat utilitor: Satellite phones can always be tracked. cpj.org, Feb 2012. https://cpj.org/2012/02/caveat-utilitor-satellite-phones-can-always-be-tra/.

[9] Hadi Givehchian, Nishant Bhaskar, Eliana Rodriguez Herrera, Héctor Rodrigo López Soto, Christian Dameff, Dinesh Bharadia, and Aaron Schulman. Evaluating

physical-layer BLE location tracking attacks on mobile devices. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1690–1704. IEEE, 2022.

[10] Iridium. Iridium announces record second-quarter 2022 results; updates 2022 outlook. iridium.com, Aug 2022. https://investor.iridium.com/2022-07-26-Iridium-Announces-Record-Second-Quarter-2022-Results-Updates-2022-Outlook.

[11] Eric Jedermann, Martin Strohmeier, Matthias Schäfer, Jens Schmitt, and Vincent Lenders. Orbit-based authentication using tdoa signatures in satellite networks. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2021.

[12] David B Johnson and David A Maltz. Dynamic source routing in ad hoc wireless networks. *Mobile computing*, pages 153–181, 1996.

[13] Joint Space Operations Center. Space-track, 2023. https://space-track.org.

[14] Thomas Sean Kelso. CelesTrak - Public Domain Satellite Tracking Data, 2023. https://celestrak.org/.

[15] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Roeschlin, and Srdjan Čapkun. Ltrack: Stealthy tracking of mobile phones in lte. In *31st USENIX Security Symposium (USENIX Security 22)*, 2022.

[16] Christos Laoudias, Adriano Moreira, Sunwoo Kim, Sangwoo Lee, Lauri Wirola, and Carlo Fischione. A survey of enabling technologies for network localization, tracking, and navigation. *IEEE Communications Surveys & Tutorials*, 20(4):3607–3644, 2018.

[17] Dimitrios Lymberopoulos, Jie Liu, Xue Yang, Romit Roy Choudhury, Vlado Handziski, and Souvik Sen. A realistic evaluation and comparison of indoor location technologies: Experiences and lessons learned. In *Proceedings of the 14th international conference on information processing in sensor networks*, 2015.

[18] Julien Nicolas. Satnogs: Towards a modern, crowd sourced and open network of ground stations. In *Proceedings of the GNU Radio Conference*, volume 2, 2021.

[19] Gabriele Oligeri, Simone Raponi, Savio Sciancalepore, and Roberto Di Pietro. Past-ai: Physical-layer authentication of satellite transmitters via deep learning. *arXiv preprint arXiv:2010.05470*, 2020.

[20] Gabriele Oligeri, Savio Sciancalepore, and Roberto Di Pietro. Gnss spoofing detection via opportunistic iridium signals. In *13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2020.

[21] Patricia Paoletta. SAT-LOA-20161115-00118: Application for Fixed Satellite Service by Space Exploration Holdings, LLC, 2016. https://fcc.report/IBFS/SAT-LOA-20161115-00118/1158350.

[22] James Pavur, Daniel Moser, Martin Strohmeier, Vincent Lenders, and Ivan Martinovic. A tale of sea and sky: On the security of maritime VSAT communications. In *2020 IEEE Symposium on Security and Privacy (SP)*, pages 1384–1400. IEEE, 2020.

[23] Ralph Sabbagh and Zaher M. Kassas. Observability analysis of receiver localization via pseudorange measurements from a single leo satellite. *IEEE Control Systems Letters*, pages 1–1, 2022.

[24] Yi-Sheng Shiu, Shih Yu Chang, Hsiao-Chun Wu, Scott C-H Huang, and Hsiao-Hwa Chen. Physical layer security in wireless networks: A tutorial. *IEEE wireless Communications*, 18(2):66–74, 2011.

[25] Merrill I Skolnik. *Radar handbook*. McGraw-Hill Education, 2008.

[26] Joshua Smailes, Sebastian Kohler, Simon Birnbach, Martin Strohmeier, and Ivan Martinovic. Watch this space: Securing satellite communication through resilient transmitter fingerprinting. In *2023 ACM Conference on Computer and Communications Security (CCS 2023)*, 2023.

[27] Richard Swinbank and R James Purser. Fibonacci grids: A novel approach to global modelling. *Quarterly Journal of the Royal Meteorological Society: A journal of the atmospheric sciences, applied meteorology and physical oceanography*, 132(619):1769–1793, 2006.

[28] Danny KP Tan, Hongbo Sun, Yilong Lu, Marc Lesturgie, and Hian Lim Chan. Passive radar using global system for mobile communication signal: theory, implementation and measurements. *IEE Proceedings-Radar, Sonar and Navigation*, 152(3):116–123, 2005.

[29] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, et al. Decentralized privacy-preserving proximity tracing. *arXiv preprint arXiv:2005.12273*, 2020.

[30] Isabel Wagner and David Eckhoff. Technical privacy metrics: A systematic survey. *ACM Comput. Surv.*, 51(3), jun 2018.

[31] William M. Wiltshire. SAT-MOD-20181108-00083: Application for Fixed Satellite Service by Space Exploration Holdings, LLC, 2018. https://fcc.report/IBFS/SAT-MOD-20181108-00083/1569860.

9 Appendix

9.1 Used coordinate systems

During all observations and measurements in the real world we used up-to-date Two Line Elements (TLEs) from Celestrack in combination with the SGP4 library[1] for calculating the positions of the satellites.

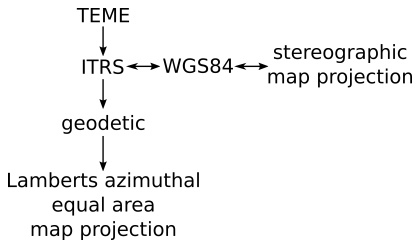


Figure 16: Overview of the used coordinate systems.

The positions of the satellite are given in the 'True Equator Mean Equinox' (TEME) coordinate system, the left upper coordinate system in Figure 16. It is used by the SGP4 library since the movements of the satellites are more precise when described in an inertial coordinate system. We convert the satellite coordinates to the 'International Terrestrial Reference System' (ITRS), which has its z-plane in the equatorial plane of the Earth and is rotating with the Earth. This allows us to combine the antenna model with the satellite position and calculate the antenna footprints at the surface of the Earth. The Earth surface is modelled by the WGS84 model, which follows the ITRS specification. Thereby the antenna footprints are projected on the surface of an Earth ellipsoid, which models the general Earth shape but does not take into account elevations such as mountains.

From the Cartesian 3D ITRS coordinate system the footprints are calculated via the WGS84 model and converted to a stereographic 2D map representation. The map is centered at the observers position and is used to calculate the intersections of the footprints with the shapely library[2]. The resulting *RoI* is converted back to the 3D ITRS. For visualizing the footprints and regions are translated from ITRS to a geodetic coordinate system. We implemented the evaluation of the *RoI* in Lamberts azimuthal equal area map projection, which allows a simple calculation of the covered Earth surface and has a stable transformation from the geodetic coordinate system.

Here it is noteworthy that the majority of the calculations during the algorithm execution are performed in the stereographic map projection. The number of coordinate system and projection translations was kept to a minimum to avoid the accumulation of transformation errors.

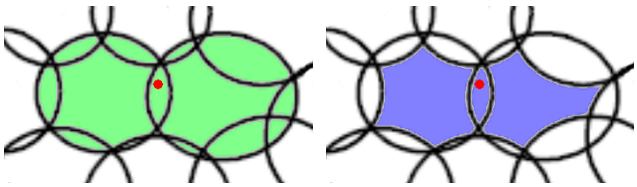
[1] https://pypi.org/project/sgp4

[2] https://shapely.readthedocs.io/en/stable/manual.html

9.2 Model Creation

With RECORD, the attacker has to calculate the footprint of the satellites antennas at all times. To make this possible, the attacker needs to have models of all the antenna footprints of a satellite. This is realized by the procedure, described in sections 3.1 and 4.2. Here we provide additional insights to the generation and usage of the satellite model. The satellite model is a set of antenna models, each modelling one of the satellites downlink antennas. Each of this antenna models holds a list of polygons, representing the lobes of the antenna.

During the model creation, we indirectly use the satellites rotational adjustment, that enables a fixed orientation of the satellite towards the Earth. This ensures that the antennas point to the earth at the same angle during the whole orbit period. At the initial stage of an attack the antenna's exact orientation and the corresponding footprint is not known. The description of the antenna's orientation and the resulting footprint contour, are addressed by the antenna model. During the model creation, the attacker receives status messages, the "Iridium Ring Alerts", containing the satellite ID and the antenna/beam ID. An actual Iridium satellite comprises a constellation of 48 antennas, which are distinguished by the beam ID. Since we know the 3D position and 3D velocity of the satellite and the location of the receiver, we calculate the angle at the satellite, pointing to the receiver, the sending angle. The angle is calculated relative to the velocity vector and nadir of the satellite. This makes the measurement independent of the satellite and observers location and enables the combination of many data points over time. These two-dimensional data points are illustrated in Figure 7a. Through a labeling based on the received antenna/beam identifier, it is possible to combine many data points that belong to a specific antenna. Over time, a profile emerges, revealing many sending angles for each satellite antenna. This aggregation of data points forms the core of the antenna model, revealing the opening angles (the outer hull of the sending angles) of each respective antenna. To reduce the size of the antenna model, we optimize the model by keeping only the outer data points of each antenna. These outer points, which are delineating the footprint, are stored in a polygonal format to streamline computations during upcoming footprint calculations. Such polygons are shown in Figure 7b. This storage format also allows efficient checks if an observer's placement is within the footprint, by verifying the polygonal inclusion of the directional angle pointing to the observer. Since we are working with real systems, the antennas often have side lobes. During the data processing, each antenna lobe is identified (each color in Figure 7a represents a distinct lobe of beam 36) and subsequently encapsulated within a separate polygon. Importantly, the side lobes are preserved within the model, since it is possible that satellite devices also use this side lobes, if no other signal is available. In the end, the satellite model is a set of antenna models. Each antenna model is a set of polygons



(a) Maximum footprint. (b) Minimum footprint.

Figure 17: Max. and min. observer footprints (red dots). The max. consists of the visible antenna beams. The min. subtracts all beams outside the observer's view from the max.

representing an individual antenna lobe.

9.3 Observation Events

We now formalize the relation between the received messages, observation events, and antenna footprints. First, some basics for working with the antenna footprint areas are defined followed by the calculation of the areas of interest, i.e. the location knowledge added by different event types.

Basic Definitions E defines the set of all observation events that are made during an observation.

$e_{l,t}$ is one observation event from the set of events E ($e_{l,t} \in E$), that was detected at location l at time t. In each event, the information about location and time is always included, also in the simplified form e (without the indices) which we use to increase readability.

$region(e)$ describes a function that computes the *RoI* of an event e. Accordingly, $region(E)$ defines the region that is covered by the whole set of observation events.

B_e defines the set of all visible antenna beams during one event e. Since every event includes the location l and time t, it is possible to determine the visible beams. The simplified form is B. In some cases, the visible beams one time step before t are required, they are denoted as B_{t-1}.

b is a single antenna beam in set B ($b \in B$). The full description is $b_{s,n,t}$, which uniquely identifies the beam number n of satellite s at time t.

f_b refers to the footprint of a beam b. All required information for calculating the footprint is given by b.

$max(B)$ is a helper function that describes the maximum footprint of a set of beams B. It is defined as:

$$max(B) = \bigcup_{b \in B} f_b$$

Where $\cup$ is the union of all individual footprints f_b. Figure 17a shows the maximum (highlighted in green) of two antenna footprints for one observer (the red dot in the middle).

$min(B)$ is a second helper function that describes the minimal footprint of a set of beams B. This includes only the area that is covered by the given beams, overlapping areas with other beams are excluded. Following this, it is defined as:

$$min(B) = max(B) - max(B^*)$$

where B^* denotes the negative of B, so the set of all beams that are not visible for an observer at location l and time t. Figure 17b illustrates the minimum footprint of an observer.

Observation Events Definitions During the communication of a target device with the satellite, the attacker observes a sequence of messages. In the following explanation, the translation from observed messages to observation events and the calculation of the resulting *RoI* is provided. The term 'target beam' refers to the satellite antenna beam that is currently used to communicate with the target device. The term 'observer beam' refers to the antenna beam that currently can be received by the observers. Based on LEO satellite geometry and system behavior, we can define six different observation events:

General reception (e_{gr}): An observer that is in the same footprint as a target device is able to receive target messages on the downlink. The target device is in the maximum footprint of all receivable beams (see Fig. 17a):

$$region(e_{gr}) = max(B) = \bigcup_{b \in B} f_b$$

Non-reception during communication (e_{ndc}): Multiple observers cooperate and not everyone is receiving target traffic. The non-receiving observers gain the knowledge that the target is not in their minimal footprint. Hence, a 'negative region' is calculated that is ensured not to hold the target position:

$$not\_region(e_{ndc}) = min(B) = \bigcup_{b \in B} f_b - \bigcup_{b^* \in B^*} f_{b^*}$$

Reception after handover (e_{rh}): When the target device switches from one spot beam at $t-1$ to another, it exchanges messages with the satellite to perform a handover. An observer who receives those messages and is still able to receive downlink messages afterwards at t gains the knowledge that the target device is in an overlapping area of two observable beams:

$$region(e_{rh}) = \bigcup_{b_1, b_2 \in B_{t-1}, b_1 \neq b_2} (f_{b_1} \cap f_{b_2})$$

Non-reception after handover (e_{nh}): An observer who receives handover messages at $t-1$ and is not able to receive downlink messages at t. The observer has to cooperate with other observers to guarantee an ongoing communication. He gains the knowledge that the target device was switching from an observable beam at $t-1$ to a non-observable beam at time t:

$$region(e_{nh}) = max(B_{t-1}) - min(B)$$

$$= \bigcup_{b_{t-1} \in B_{t-1}} f_{b_{t-1}} \cap \bigcup_{b^* \in B^*} f_{b^*}$$

Sudden reception (e_{sr}): This is the case when an observer did not receive target traffic at $t-1$ but suddenly receives messages at time t. This either happens because (a) the target device switched to an attacker beam or (b) the attacker switched to the target beam. In case (a), the target is in the maximum footprint at time t, while not being in the minimal footprint at time $t-1$. For case (b), the target device is in a beam that was observable at time t but not at time $t-1$:

$$region_a(e_{sr}) = max(B) - min(B_{t-1})$$

$$region_b(e_{sr}) = max(B_t \setminus B_{t-1})$$

$$region(e_{sr}) = region_a(e_{sr}) + region_b(e_{sr})$$

$$= \bigcup_{b \in B} f_b \cap \bigcup_{b^*_{t-1} \in B^*_{t-1}} f_{b^*_{t-1}} \cup \bigcup_{b \in \{B_t \setminus B_{t-1}\}} f_b$$

Sudden non-reception (e_{sn}): The observer was able to receive target messages at $t-1$ but not at time t. The causes are either (a) the target device switched from an attacker beam to a new beam or (b) the observer left the target beam:

$$region(e_{sn}) = max(B_{t-1} \setminus B_t) = \bigcup_{b \in \{B_{t-1} \setminus B_t\}} f_b$$

The resulting region is the intersection of all single region from all observation events:

$$region(E) = \bigcap_{e \in \{E \setminus e_{nr}\}} region(e) - \bigcup_{e_{nr}} not\_region(e_{nr})$$

9.4 Real-World Downlink Measurements

Figure 18: Picture of the measurement setup: Raspberry Pi 4, HackRF One, Iridium antenna, Iridium GO!

9.5 Observer Placement Strategy

To distribute the attacker's observers, we use the Fibonacci grid methodology [27] that facilitates a uniform spatial point distribution on the Earth's surface. By manipulating the overall number of points, we influence the inter-point spacing, in a first step. By generating the last 'n' points of this world-spanning grid, we generate the 'n' points in closest proximity to the North Pole. In a second step, we rotate the North Pole-centered points by a random angle, to avoid generating exactly the same pattern. In a third step, the North Pole-centered points are rotated to our designated starting location on the earth surface. Each of these resulting 'n' points becomes one location of the 'n' observers. To assess the quality of the point distribution, we analyzed the distance separating a point from its nearest neighbor. We conduct evaluations across inter-point distances spanning 50 to 1000 km, incremented in intervals of 10 km, coupled with numbers of points ranging from 3 to 100. The mean proximity to the nearest neighbor is 1.15% off from the desired inter-point distance, with a standard deviation of 2.5%. The largest deviation observed attains 9.29%. The distance between an observer location and the target device depends on the number of attackers and the inter-observer distance. For the optimal distance of 400 km, a 12 observer setup covers a circular area with 836 km in radius. The target device is placed randomly around the starting location, up to a distance of the given inter-observer distance. This means the device can be placed on the opposite side of the outer observer, up to 400 km away from the starting location. Thus, the maximum distance of the outer observer to the target device is 1236 km, for this setup.

measurement	duration	area estimation	$\frac{\text{duration}}{e_{ndc}}$
4*	1463 sec	17118 km^2	6.9
2*	683 sec	81437 km^2	13.4
6*	2085 sec	3240 km^2	22.4
8*	4044 sec	8654 km^2	32.9
9	4237 sec	43152 km^2	33.9
3	1028 sec	81337 km^2	54.1
5	1715 sec	88292 km^2	142.9
7	2318 sec	47704 km^2	165.6
1	288 sec	102534 km^2	-

Table 6: Measurements ordered by duration over e_{ndc}.

Table 7 shows the covered area of the observer setups generated in Section 5. It includes covered areas of 24 observer setups to clarify the emerging pattern: when doubling the distance between observers, one can reduce the amount of observers by a factor of 4 and still cover the same area.

inter-observer distance	number of observers			
	3	6	12	24
100 km	34,271	68,542	137,078	247,138
200 km	137,078	274,139	548,203	1,096,112
300 km	308,401	616,708	1,233,043	2,464,594
400 km	548,203	1,096,112	2,191,045	4,377,374
500 km	856,438	1,712,157	3,421,435	6,831,356
600 km	1,233,043	2,464,594	4,923,218	9,822,653
700 km	1,677,942	3,353,119	6,695,180	13,346,129
800 km	2,191,045	4,377,374	8,735,883	17,396,308

Table 7: Covered circular area [km^2] of the observer setups.