GNSS Spoofing Detection via Opportunistic IRIDIUM Signals

Gabriele Oligeri, Savio Sciancalepore, Roberto Di Pietro
Division of Information and Computing Technology
College of Science and Engineering, Hamad Bin Khalifa University
Doha, Qatar

ABSTRACT

In this paper, we study the privately-own IRIDIUM satellite constellation, to provide a location service that is independent of the GNSS. In particular, we apply our findings to propose a new GNSS spoofing detection solution, exploiting unencrypted IRIDIUM Ring Alert (IRA) messages that are broadcast by IRIDIUM satellites.

To achieve the above-introduced objective, we firstly reverse-engineer many parameters of the IRIDIUM satellite constellation, such as the satellites speed, packet interarrival times, maximum satellite coverage, satellite pass duration, and the satellite beam constellation, to name a few. Later, we adopt the aforementioned statistics to create a detailed model of the satellite network. Subsequently, we propose a solution to detect unintended deviations of a target user from his path, due to GNSS spoofing attacks. We show that our solution can be used efficiently and effectively to verify the position estimated from standard GNSS satellite constellation, and we provide constraints and parameters to fit several application scenarios. All the results reported in this paper, while showing the quality and viability of our proposal, are supported by real data. In particular, we have collected and analyzed hundreds of thousands of IRA messages, thanks to a measurement campaign lasting several days. All the collected data (1000+ hours) have been made available to the research community.

Our solution is particularly suitable for unattended scenarios such as deserts, rural areas, or open seas, where standard spoofing detection techniques resorting to crowd-sourcing cannot be used due to deployment limitations. Moreover, contrary to competing solutions, our approach does not resort to physical-layer information, dedicated hardware, or multiple receiving stations, while exploiting only a single receiving antenna and publicly-available IRIDIUM transmissions. Finally, novel research directions are also highlighted.

CCS CONCEPTS

• **Security and privacy** → **Mobile and wireless security**; **Software reverse engineering**.

KEYWORDS

GPS Spoofing Detection; Satellite Communications Security; Reverse Engineering; Wireless Security; Cyber-Physical Systems Security.

1 INTRODUCTION

Global Navigation Satellite Systems (GNSS) technologies today are used massively in several application scenarios, spanning from turn-by-turn terrestrial navigation, airborne and maritime navigation, timing purposes in smart grid, to name a few [28]. Despite Global Positioning System (GPS) by the US is the most famous, in the last years several region-specific solutions with the same aim have appeared, such as the European GALILEO, the Russian GLONASS, and the Chinese BEIDOU, to name a few. The vast majority of the functionalities provided by GNSS systems are open and available to the public, e.g., GPS provides an unencrypted (and un-authenticated) signal. While the lack of encryption fueled their adoption worldwide, in many use-case scenarios, unfortunately, the lack of authentication makes these systems prone to cybersecurity attacks. Indeed, the adversary can easily generate fake GNSS signals, and broadcast them to a set of targets, biasing the computation of their actual positions. We refer to the previous behavior as *spoofing* [22].

While requiring minimum background knowledge, cheap hardware, and free-to-use software, location spoofing is easy to play, but hard to detect and mitigate. Indeed, since GNSS satellites are orbiting in a Medium Earth Orbit (MEO), far away from the ground (about 20,000 Km), GNSS signals reach the ground with a very weak signal-to-noise ratio. Therefore, an adversary can easily overcome the aforementioned received signal strength, being always much closer to the target device than the satellite constellation. Eventually, the (spoofed) signals transmitted by the adversary reach the target device and—having a higher SNR—are considered as the actual ones, and adopted for the final computation of the device's location [27]. The low strength of the GNSS received signal makes GNSS technologies also vulnerable to jamming, being it intentional (attack) or unintentional. While there is an active research community on localization of malicious jamming sources and mitigation of their effect, the unintentional jamming, due to radar, radios, and electromagnetic interference (e.g. from pumps and engines), is more difficult to mitigate, and can cause significant issues to the correct reception of GNSS satellite signals, by breaking the link for even long period of time [15].

During the years, several techniques have been adopted to detect and mitigate GNSS spoofing attacks [22]. Some of them analyze the physical layer, trying to distinguish if the signals are coming from one only source (that could be a potential spoofer) or a set of sources, such as a genuine satellite constellation [12]. Other solutions resort to crowd-sourcing, i.e., combining context information from neighbors, ad-hoc infrastructure, and cellular network information. However, the current state of the art does not take into account the specific scenario where signal sources are, by design, solo sources, or when just a few additional sources can be leveraged, but for a limited, intermittent, not predictable, period of time. In such scenarios, the deployment of additional infrastructures might be impractical, and the usage of physical layer information might not be possible due to either the lack of the underlying physical phenomenon, or because of the high price of ad-hoc hardware needed to exploit it.

A striking example is represented by open seas navigation, where ships resort only to GNSS positioning for computing their current location and heading up to the destination. Indeed, open seas navigation is witnessing an emergent trend, and similarly to the automotive industry, ships are becoming more and more autonomous. According to recent forecasts, a landscape of fully autonomous vessels is predicted by the year 2035, where GNSS technology will be massively adopted to provide location awareness [24]. In such a scenario, GNSS jamming and spoofing will become dreadful threats, since autonomous vessels—even more than the human-controlled ones—require a trusted and precise localization procedure [2].

Contribution. In this paper, we provide two main contributions. First, we reverse-engineer several infrastructure configuration parameters of the IRIDIUM constellation. Second, leveraging the previously mentioned result, we exploit opportunistic IRIDIUM Ring Alert (IRA) messages to provide yet another independent localization solution. As for the former contribution, one should notice that, though IRIDIUM Ring Alert are accessible, all other information about IRIDIUM are treated as proprietary by the infrastructure owner: Iridium Communications Inc.. To overcome this lack of information, we ran an extensive measurement campaign using commercially available Software Defined Radios (SDRs), acquiring IRIDIUM Ring Alert messages for more than 1000 hours. Using this large dataset, we reverse-engineered several network configuration parameters of the IRIDIUM constellation, including the satellites speed, packet interarrival times, maximum satellite coverage, satellite pass duration, and the satellite beam constellation—all these data have been released as open-source [16]. We used the above parameters to model the IRIDIUM constellation. Later, we moved to exploit opportunistic IRA messages, combining them with the information acquired during the reverse-engineering process, to estimate the current position of the receiving device.

Our research contributes not only to validate the GNSS information, but also to provide yet another independent localization solution—although being slightly inaccurate compared to the GNSS, given the harsh system conditions—in the presence of GNSS jamming. Being the IRIDIUM constellation characterized by worldwide availability, our solution can be used even in unattended scenarios (deserts and oceans), where no other ad-hoc in-land network infrastructure can be used for crowd-sourcing, and where the available GNSS hardware cannot be replaced or updated with multiple-antenna setups. Finally, we also highlight some novel, challenging research directions.

Paper organization. The paper is organized as follows. Section 2 reviews recent related work on GNSS spoofing detection and mitigation, Section 3 introduces the main system features of the IRIDIUM satellite platform, Section 4 depicts the adversarial model assumed throughout the work, Section 5 illustrates our measurement setup, Section 6 includes the features of the IRIDIUM constellation platform inferred through our measurement campaign, Section 7 provides the details of our spoofing detection technique based on opportunistic IRA messages, while Section 8 provides a systemic comparison between our proposal and the most important related work. Finally, Section 9 draws conclusions and highlights our future research directions.

2 RELATED WORK

GNSS spoofing identification, detection, and mitigation are all research areas that attracted the attention of a lot of researchers during the years. Major contributions are coming from the idea of resorting to other over-the-air information to cross-check the actual position of the targeted spoofed device.

A very recent contribution [17] involves crowd-sourced information from cellular network access points to verify the actual position of the device. Authors showed that beacons broadcast from cellular networks access points can be exploited to retrieve their position, and therefore, checking the consistency of the current position of the device received from the GPS constellation.

Authors in [9] showed that multiple (colluding) GPS receivers can be used to detect a spoofer. Authors showed that by leveraging spatial noise correlations, the false acceptance rate of the countermeasure can be improved while preserving the sensitivity to attacks. A collaborative detection scheme is proposed in [14]. The authors assume a set of vehicles exchange measured GPS code pseudoranges using a dedicated short-range communication. Each vehicle elaborates on the exchanged GPS data and derives independent statistics. These statistics are then exploited to detect high correlations in the time of arrival of spoofed GPS signals, and therefore, highlighting the presence of a GPS spoofer.

A physical layer solution is proposed by [29], involving two antennas with different radiation patterns. Genuine GPS signals are supposed to come from several sources (satellites), and therefore, exploiting a two-antenna deployment involves a different signal-to-noise ratio measured by the two antennas. If the two antennas experience the same signal-to-noise, it means the signal is coming from the same source, and therefore, a GPS spoofer is likely to be in the neighborhood.

Authors in [23] proposed a solution exploiting meteor burst communications to verify the location of the spoofed device. The solution exploits the radio reflection properties of ephemeral meteor trails, combined with multiple anchors that can be deployed even hundreds of Km from the receiver. Although being robust to jamming and eavesdropping, their solution requires dedicated infrastructure. Another crowd-sourcing solution has been proposed by [8]. The authors proposed the deployment of multiple nodes

at the ground to monitor the air traffic from GPS-derived position advertisements that aircraft periodically broadcast for air traffic control purposes. Spoofing attacks are detected and localized by the independent infrastructure on the ground which continuously analyzes the contents and the times of arrival of these advertisements.

A vision-based GPS spoofing detection method for unmanned aerial vehicles (drones) is proposed by [20]. The on-board camera and the inertial measurement unit are used to get the velocity and position of the aircraft, thus detecting unexpected changes in the flight path. Another cooperative solution has been proposed by [6]. The GPS signal is verified by resorting to a network of cooperative GPS receivers. Each receiver in the network correlates its version of the signal with those received by other receivers to detect spoofing attacks. The authors in [12] exploited phase delay measurements from an antenna array to infer between single and multiple GPS sources, and therefore, detect the presence of a spoofer.

In Section 8 we will provide a comparison between our solution and the ones introduced in this section, based on some distinctive system requirements. We remark that the Iridium satellite network has been previously exploited for localization purposes by [10]. The authors exploited physical layer information and a reference anchor in a well-known position to locate the receiver by resorting to both time difference of arrival (TDOA) and frequency difference of arrival (FDOA) techniques. Another similar contribution is provided by [25] and [26]. The authors exploited the instantaneous Doppler effect of IRA messages to infer the position of the receiver. However, using the Doppler shift for GNSS spoofing detection would require the deployment of multiple receivers, organized in ad-hoc network infrastructure, typically not available in deserts and oceans [4], [21].

Finally, we recall that localization and spoofing detection are two different research problems, characterized by different system requirements. Localization techniques are used to either replace or support the traditional GNSS signals, while spoofing detection schemes are usually designed to work in conjunction with the GNSS, taking an active part (raising alarms and indicating corrections) only when they detect inconsistencies between the position reported by the GNSS and the one obtained via local computations.

3 BACKGROUND ON IRIDIUM

The IRIDIUM satellite platform has been described for the first time in the seminal paper [11]. The platform has been set up in 1993, and it is mainly constituted by a set of Low-Earth Orbit (LEO) satellites, able to guarantee the full earth coverage for data and voice communications. IRIDIUM RF operations take place in the L-band, i.e., in the range $[1,616 − 1,626.5]$ MHz, by resorting to dedicated satellite-phones, while the communications between the satellites happen in the 23GHz band. The name of the satellite platform is due to the initial intended number of satellites, being 77 the atomic number of the chemical element Iridium. However, the final deployment of the satellite constellation counts only 66 satellites, which are the ones necessary to guarantee coverage for the whole Earth's surface. On the ground, to initiate and receive IRIDIUM calls, a user can leverage dedicated satellite phones and pagers provided by companies such as Motorola and Kyocera. IRIDIUM services are also used on a subscription basis by aircraft and vessels, thanks to dedicated transceivers units. Moreover, short IRIDIUM-compliant transceivers are also available and currently used within Internet of Things (IoT) products to provide backhaul connections [7].

Each IRIDIUM satellite is characterized by a three-antenna array, forming a honeycomb pattern of 48 beams on the ground. Therefore, a generic IRIDIUM user might experience two types of hand-off, i.e., either from one beam to another beam (intra-satellite) or from one satellite to another one (inter-satellite). In general, when the user is served by a beam at the edge of the honeycomb, the system manages the hand-off to a neighbor satellite.

The channels provided by the system can be divided into two categories, i.e., *system overhead channels* and *bearer service channels* [18]. In this paper, we are interested in one specific *system overhead* channel, i.e., the IRIDIUM Ring Alert (IRA) broadcast channel. This channel operates at $1,626.27$ MHz, and it is an unencrypted downlink-only channel used to send *IRA* messages to individual subscriber units—to be used for handover operations. IRA messages contain the following plain-text information: satellite ID, beam ID, location at ground (in terms of longitude and latitude, as computed by the satellite based on a proprietary algorithm), altitude information (typically around 800 km), and other information useful for handover purposes, such as the Temporary Mobile Subscriber Identity (TMSI) of the end-user equipment performing the handover. Note that, being an unencrypted channel, the IRA broadcast channel can be received by using a general-purpose Software Defined Radio (SDR) and a generic antenna.

The position information computed by the IRIDIUM satellites and emitted through the broadcast IRA channel is used in this paper to compute a location estimation at the receiver side. This information is used to cross-check the position estimated from the GNSS constellation.

4 ADVERSARY AND SYSTEM MODEL

Our adversary model consists of a malicious entity, able to generate fake GNSS signals by resorting to the combination of an SDR, an antenna, and a GNSS spoofing software tool, such as [5].

We assume an isolated playground, not relying on any Internet connection and any other means (e.g., WiFi and Cellular Networks) to derive location information. A typical scenario that fits the previous assumptions might be constituted by wide inhabited open areas, such as deserts, or open seas (oceans), where the target devices cannot receive any additional information to verify their actual GNSS location. Figure 1 shows the system model considered throughout this paper. As a reference scenario, we consider a boat relying on GNSS information for its navigation. The adversary is willing to de-tour the boat by performing a GNSS spoofing attack; in particular, the adversary wants to re-route the boat from path 1 to path 2 in Fig. 1. Our solution exploits the IRIDIUM satellite network to independently verify the actual position of the boat, and therefore, raising an alarm when a de-tour is detected.

It is worth noting that we do not assume any active IRIDIUM subscription. Thus, the IRIDIUM position-providing service Secure Time and Location (STL) cannot be used. Indeed, purchasing unlimited subscription plans to IRIDIUM services can be particularly expensive for shipowners, and it could also require the hiring of
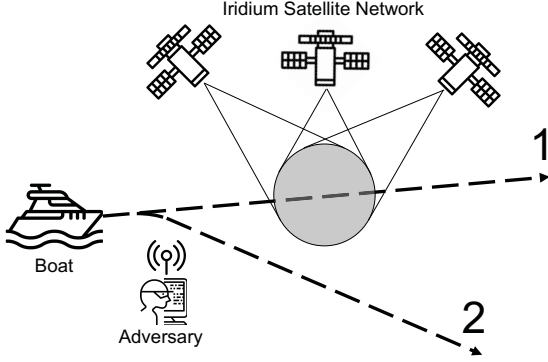
Figure 1: Scenario and Adversary model: The target (boat) is re-routed by the adversary from path 1 to path 2, but our solution enables independent location verification by exploiting the IRIDIUM satellite network. Therefore, eventually the target will be able to detect the GNSS spoofing attack.

dedicated teams to perform the deployment and maintenance in all the vessels. On the contrary, our solution exploits opportunistic IRIDIUM messages; in particular, the IRA messages delivered in clear-text on the *Ring Alert Broadcast Channel* (at the frequency 1,626.27 MHz). Indeed, being unencrypted these messages can be received with a generic low-cost SDR.

In our system model, as depicted by the gray circle in Fig. 1, the boat continuously performs a loose localization process, and therefore, it checks if the current, locally computed, GNSS position is far away from the position provided by our solution exploiting the IRIDIUM constellation. In the remainder of this paper, we will estimate the configuration parameters and evaluate the thresholds to provide timely, independent, and effective verification of the GNSS localization.

5 MEASUREMENT SETUP

Figure 2 shows the setup we adopted to receive the messages from the Iridium constellation. The hardware is mainly constituted by a Software Defined Radio USRP X310, a telescopic *stilo* antenna, and a Laptop Dell XPS15 9560, equipped with 32GB of RAM and 8 Intel Core i7700HQ processors running at 2.80 GHz. As for the software, we adopted the GNURadio development toolkit and the related Iridium module [1]. The output is subsequently parsed to generate meaningful data analytics, available for downloading at [16].

Our measurement campaign has been carried out in very harsh conditions: from a balcony outside our office. This sub-optimal setup significantly affects the number of received packets, being the antenna very close to the wall of the building. Moreover, the stylo antenna is recommended for operation from 75MHz to 1GHz, being therefore not optimal for the reception of the IRIDIUM signals at 1626.270833 MHz. While our setup still guarantees the collection of a reasonable amount of messages in a long term measurement, due to a high packet loss, it does not provide the best performance for a live-test of GPS spoofing detection. In later sections, we provide more details on statistics related to packet loss and how the later
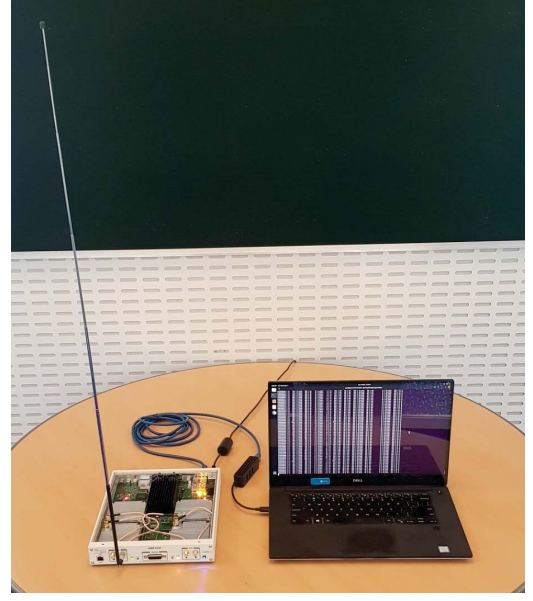

Figure 2: Our receiver setup to collect the IRA messages: a Dell XPS15 9560 laptop and a USRP X310.

one affects our solution. The good results achieved in such harsh conditions undoubtedly show the viability of our approach.

We collected a total of about 1019 hours of measurements consisting of 569,431 samples. An excerpt from the dataset is reported in Table 1. For each data sample, we have the time (seconds and milliseconds), the satellite ID, the beam ID, and both latitude and longitude of the satellite/beam at the ground. Specifically, when the Beam ID is equal to zero, the position (latitude/longitude) refers to the position of the satellite at the ground, e.g., satellite 115 in the example of Table 1. When the Beam ID is different than zero, latitude and longitude refer to the position of the beam at the ground, e.g., the second sample is related to beam 44 belonging to satellite 115 having a position at the ground of ⟨+23.06, +49.81⟩. In all our measurements we counted a total of 66 satellite IDs, i.e., {2, 3, 4, 5, 6, 7, 8, 9, 13, 16, 17, 18, 22, 23, 24, 25, 26, 28, 29, 30, 33, 36, 38, 39, 40, 42, 43, 44, 46, 48, 49, 50, 51, 57, 65, 67, 68, 69, 71, 72, 73, 74, 77, 78, 79, 81, 82, 85, 87, 88, 89, 90, 92, 93, 94, 96, 99, 103, 104, 107, 109, 110, 111, 112, 114, 115}, coinciding with the number of active IRIDIUM satellites reported by the service provider, and the full-beam constellation equal to 48 beam IDs, i.e., {1, ..., 48}.

Table 1: Excerpt of the collected dataset.

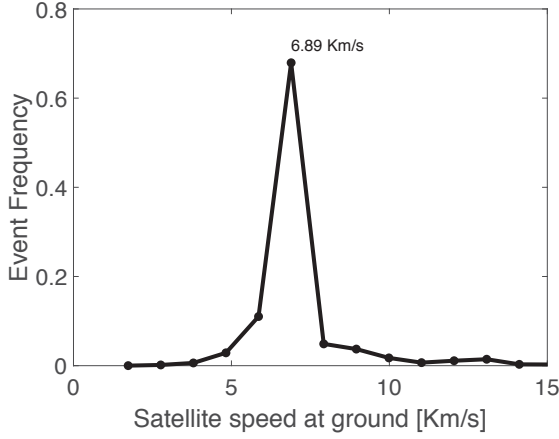| Time (s)	Time (ms)	Satellite ID	Beam ID	Latitude	Longitude
1580712040	000000739	115	0	+29.81	+046.10
1580712040	000004519	115	44	+23.06	+049.81
1580712040	000005059	115	46	+25.95	+051.69
1580712040	000005599	115	47	+26.94	+047.71
1580712040	000008839	115	0	+30.29	+046.13
1580712040	000013159	115	44	+23.56	+049.80
1580712040	000013699	115	46	+26.46	+051.72

Figure 3: Satellite speed at ground: probability distribution function associated with satellite speeds at ground and most likely speed (6.89Km/s).
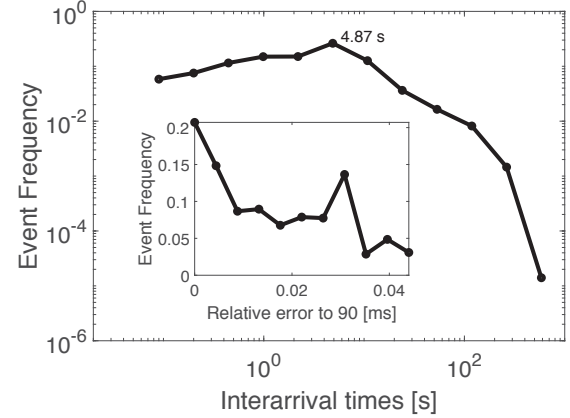

Figure 4: IRA interarrival times: probability distribution function associated to IRA interarrival times and their maximum likelihood at 4.87 seconds. The inset figure represents the relative error respect to 90ms representing the actual rate at the transmitting side (for different beams).

6 IRIDIUM DATA ANALYTICS

In this section, we provide a thorough analysis of the network information that can be extracted from IRA messages.

Satellites speed. Figure 3 shows the probability distribution function associated with the satellites speed at the ground. We took into account all the satellites IDs collected during our measurement campaign, by considering their positions and the absolute time associated with the reception of the packets. The satellite speed v has been computed as the ratio of the difference between two consecutive positions, i.e., δ, and the elapsed time, i.e., ϵ, yielding $v = \frac{\delta}{\epsilon}$. We observe that the most likely speed is about 6.89 Km/s, consistent with the approximate speed of a generic LEO satellite [3].

We also notice the presence of many (unlikely) high-speed samples ($v > 10$ Km/s). These inconsistent speeds are experienced when the time difference between two consecutive messages is particularly high, likely due to the packet loss. In particular, packet loss, especially when experienced in bursts, accumulates a lot of errors as for time and space, leading to inconsistent high speeds. Since we are not aware of the actual accuracy of beam and satellite coordinates at the ground, we guess that large periods between packets (due to packet loss) accumulate the aforementioned errors. However, we notice that this phenomenon does not affect the quality of our solution.

IRA message rate. All our analysis is based on the reception of IRA messages. Figure 4 shows the probability distribution function associated with the interarrival times of the IRA messages. The inset figure shows the relative error to the expected interarrival time of 90 milliseconds, as reported by related work on IRIDIUM [10][25]. Indeed, each beam transmits an IRA message every 4.32 seconds. Being the number of beams 48, a receiver will receive a generic IRA message every 90ms (4320/48). We observe also that the link is characterized by an extremely high packet error rate. Indeed, the likelihood for the interarrival time is about 4.87 seconds, i.e., one message is received every 66 lost ones. Conversely, the jitter is

small; indeed, the computational overhead for message decoding is negligible and the vast majority of the messages experience an interarrival time that is multiple of 90 ms.

Coverage. To understand the maximum coverage range of an Iridium-compliant device, we consider the furthest satellite positions at the ground, independently of the time they have been collected. Figure 5 shows the furthest satellite positions (at ground) from our location represented by the red cross. Many factors can affect the reception of IRA messages: mountains in the north-east and south-west significantly affect the signal propagation, especially when the satellite is far-away from the receiver, at the minimal altitude over the horizon, or simply the presence of buildings. The overall area covered through our setup sums up to about $10^6 \cdot 8.3 km^2$, further demonstrating the capability of a very simple setup to cover even large areas.

Figure 6 shows the probability density function associated with the distance between the receiver and the satellite positions at the ground. As previously discussed, the transmission distance is significantly affected by the geography characterizing the neighborhood of the receiver. The likelihood of the maximum distance is 1, 625 Km. Note that a similar result can be extracted also by fitting the red dots in Fig. 6, using the Pratt method [19], obtaining a distance of about 2, 346 Km.

Satellite pass. Let us consider a specific satellite, i.e., the Iridium satellite 78. Figure 7 shows all the passes extracted from all the measurements we collected about the aforementioned satellite. We adopted the red and green colors for the upward and downward directions, respectively. The overall coverage is consistent with the data we previously discussed for Fig. 5, while we observe a total of 59 passes upward and 59 downward in a period of time of about 1000 hours.
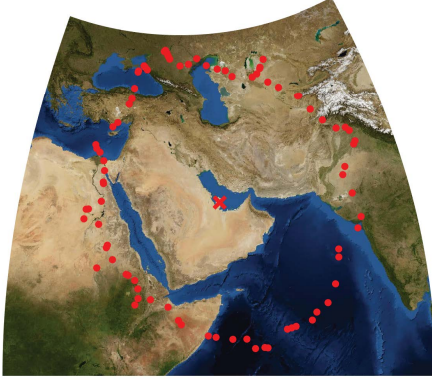
Figure 5: Maximum satellite distances (at ground) from the receiving source.
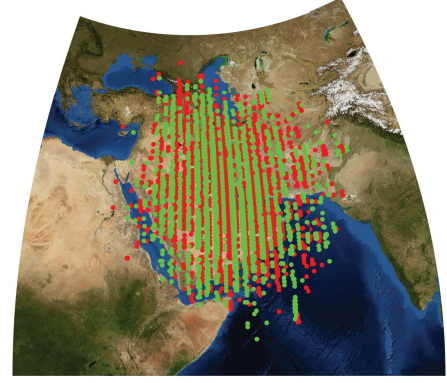

Figure 7: Satellite 78 passes: data collected from Iridium satellite 78, where red and green dots represent upward and downward passes, respectively.
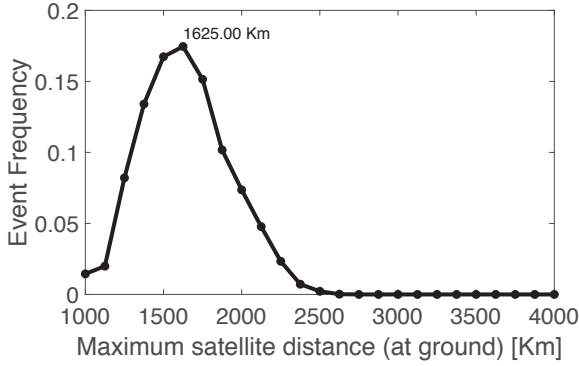

Figure 6: Probability distribution function associated with the maximum satellite distances (at ground) from the receiving source. The maximum likelihood is 1, 625 **Km.**

Figure 8: Pass duration: probability distribution function associated with the duration of a satellite pass.

The pass duration can be computed by considering the time between the instant when the satellite appears at the receiver and the last sample before disappearing. Figure 8 shows the probability distribution function associated with the pass duration, considering all the satellites data collected from all our measurements. The maximum likelihood for the pass is about 7.59 minutes. The distribution presents a heavy tail on the left side, i.e., pass duration less than 4 minutes: this is due to satellites crossing the coverage region far away from the receiver, and therefore, being characterized by short periods of intersection with the coverage area of the receiver. We searched for the best fit distribution and we found that to be the Extreme Value Distribution $evd(t)$, as depicted by Eq. 1.
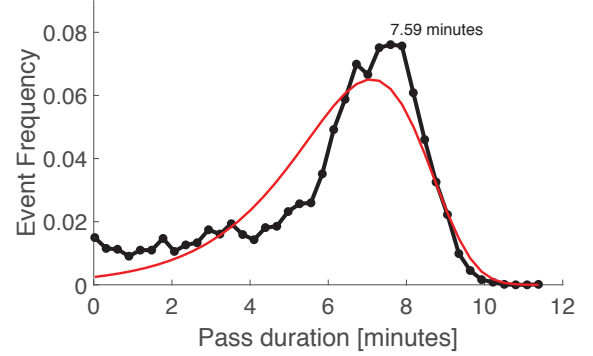
$$evd(t) = \frac{1}{\sigma} \exp\left(\frac{t-\mu}{\sigma}\right) \exp\left(-\exp\left(\frac{t-\mu}{\sigma}\right)\right), \qquad (1)$$

where $\mu = 7.28$ and $\sigma = 1.67$ are the best-fit location parameter and the scale parameter of the distribution, respectively.

Satellite and beams. Figure 9 shows an example pass (red circles) of satellite 78 and the beams (red dots) with the related beam IDs. We recall that both the beam positions at the ground and the beam IDs have been collected from the IRA messages. Due to the previously mentioned packet loss rate, many beams are missing and only a subset of them are available at the receiver. In the aforementioned case study, we were able to retrieve 89 beam positions belonging to 15 different beams (for one satellite pass).
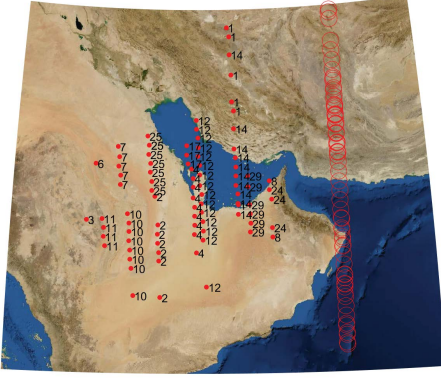
Figure 9: Single satellite pass and beams: red circles represent the position of satellite 78 (at ground) while red dots show the beams' position at the ground. Beams IDs are reported accordingly to the information collected from the IRA message.

Beam constellation. We consider all the satellite beams collected from all our measurements and we computed their displacement to the satellite position. Black dots in Fig. 10 show the beam constellation, while red crosses represent the centroid for each cloud of beams. The labels are consistent with the beam IDs retrieved from the IRA messages. The beam constellation is constituted by 48 beams organized in three concentric circles with radii of about 3.36, 7.98, and 14.35 Km, respectively.

Finally, we observe that, to represent the beams in a well-organized constellation, we had to detect, distinguish, and subsequently compensate, satellites moving north (upward) from the ones moving south (downward). Indeed, as previously discussed, data collected from beams might seem inconsistent, but actually, it is not, when making the following considerations:

- *Same beams belonging to the same satellite moving on different directions.* The same satellite can be observed going north, and subsequently south, after approximately 650 minutes. Indeed, due to its inclined orbit, the satellite will be back to the original position with the opposite transit direction.
- *Same beams belonging to different satellites moving on different directions.* Each location experiences different satellites going to different directions, either north or south.

For both the above configurations, the beam IDs should be mirrored to the x-axis. In particular, the beam constellation reported in Fig. 10 is consistent with satellites going upward, i.e., from the south pole to the north pole.

7 GPS SPOOFING DETECTION

In this section, we provide the details of our GNSS spoofing detection technique, aimed at detecting GNSS spoofing attacks using the IRIDIUM satellite constellation. Section 7.1 introduces the error in the position estimation via the IRA messages, Section 7.2 presents
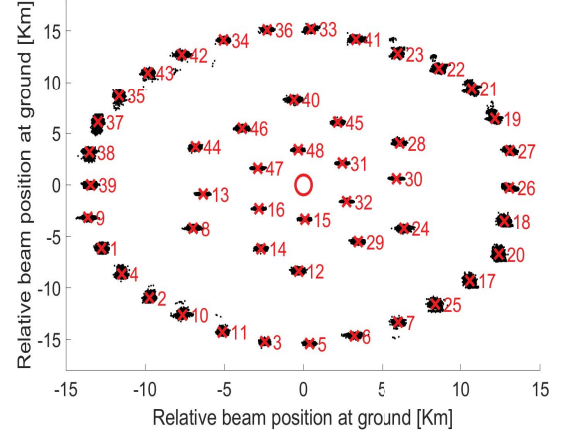

Figure 10: Relative beam positions (at ground) respect to the satellite position (at ground). Each black dot represents a different measurement while crosses represent the centroid of each cloud associated to a different beam. Labels are consistent with the beam identifiers retrieved from the IRA messages.

the details of our spoofing detection solution, Section 7.3 shows the performance of the described technique, while Section 7.4 discusses the feasibility of a combined spoofing attack involving both the GNSS system and the IRIDIUM constellation.

7.1 Position error estimation

In this subsection, we estimate the error between the actual receiver position (taken from the GPS) and the one computed from the information extracted from the IRA messages. The intuition behind our solution consists of computing the mean of all the latitude and longitude coordinates (centroid) collected from the beams. In general, the precision of the position estimation will be affected by the number of collected IRA messages, and therefore, the time required to receive such a number of messages (waiting time).

Figure 11 shows the error between the receiver position and the estimated location, as a function of the number of collected IRA messages. We observe that an error of about 10Km can be reached by collecting about 6,100 IRA messages.

Interestingly, the relationship between the localization error L_{err} and the number of IRA messages n is characterized by a power-law, as depicted by the red line in Fig. 11, that in turn, is represented by Eq. 2:

$$L_{err} = n^m \cdot 10^q, \qquad (2)$$

where $m = -0.5974$ and $q = 3.2826$.

Figure 12 shows the relation between the number of IRA messages and the time to collect them, given different packet error rates, i.e., $\{0.01, 0.1, 0.5, 0.99\}$. In our scenario, given the adopted
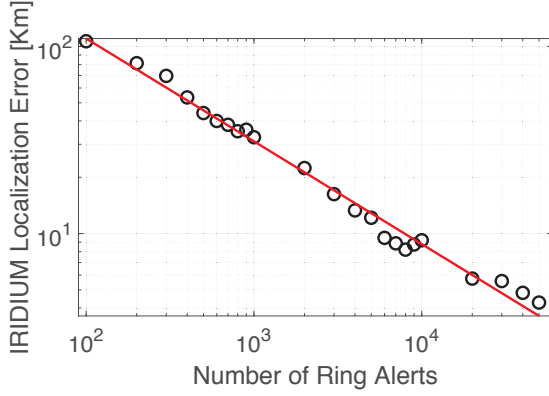
Figure 11: Localization error as a function of the number of received IRA messages.
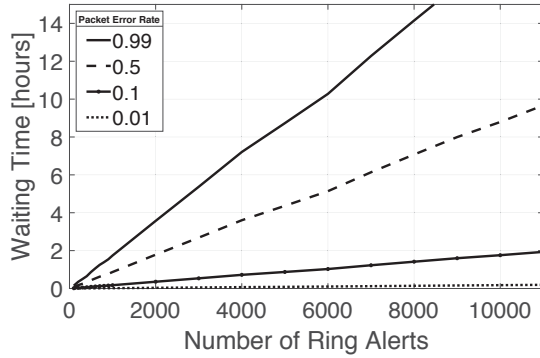

Figure 12: Waiting Time (delay) to collect the IRA messages as a function of the packet error rate.

equipment and setup, we experienced a very high packet error rate (CFR. Fig. 4), summing up to about 1 message received every 66, i.e., a packet error just slightly less than 0.99. In better conditions, lower packet error rates can be easily achieved, leading to a significantly higher amount of collected packets per unit of time. As depicted in Fig. 12, in the worst-case scenario—our deployment, 6100 packets, guaranteeing a localization error of about 10Km, require about 10 hours. Assuming lower packet error rates and good receiving conditions (such as in a desert or ocean), the same amount of packets can be collected in 1 hour or even in 6 minutes, assuming a packet error rate of either 10% or 1%, respectively.

7.2 Exploiting IRA messages to estimate receiver location

Our solution involves a multi-stage algorithm described in the following.

(1) **Collect data.** The user continuously collects IRA messages from the IRIDIUM constellation network, as described in the previous sections.

(2) **Compensate movement.** Given the movement of the receiver during the message collection, the acquired data should be compensated as a function of the movement. Therefore, assuming the acquisition process starts at t_0, and the user is moving with speed v, the collected information from the IRA messages should be compensated as reported by Eq. 3.

$$
\begin{aligned}
\Delta x &= x(t_0) + \cos(v \cdot \Delta t), \\
\Delta y &= y(t_0) + \sin(v \cdot \Delta t),
\end{aligned}
\tag{3}
$$

where Δt is the time between two consecutive IRIDIUM packets, while x and y are latitude and longitude, respectively.

(3) **Compute location I_{pos}.** The position of the receiver is estimated as the centroid computed over the beams' positions at ground, yielding Eq. 4.

$$
I_{pos} = \left(\frac{1}{N} \sum_{i=1}^{N} x_i, \quad \frac{1}{N} \sum_{i=1}^{N} y_i \right),
\tag{4}
$$

where (x_i, y_i) are the latitude and longitude of the position at ground for beam i, while N is the number of beams taken into account for the computation (cfr. Fig. 11).

(4) **Compare I_{pos} with G_{pos}.** The estimated position I_{pos} from the IRIDIUM satellite network is compared with that one received from the GNSS system G_{pos}. Depending on different parameters, that will be discussed later on, an alarm is raised if the difference is greater than a predetermined threshold thr, i.e., $| I_{pos} - G_{pos} |> thr$.

7.3 Performance

Our solution is particularly suitable for scenarios where crowd-sourcing is not possible, i.e., there are no other independent sources in the neighborhood to verify the current GNSS localization. A few examples of such scenarios are deserts, forests, remote rural areas, and open seas. We choose the latter one as our reference scenario, and without loss of generality, we consider a ship moving through a pre-defined path according to different speeds. According to the specific cruise speed, we provide different indicators to measure the performance of our solution.

In the following, we consider different classes of ships [13], as depicted in Table 2. Class S1, i.e., *bulk carriers*, carry unpacked bulk cargo, class S2, i.e., *Container Ships*, carry containers, S3, i.e., *Oil and chemical tankers*, are designed specifically to carry oil and chemicals, S4, i.e., *RORO vessels*, roll on roll off ships are special types of vessels used for the transportation of automobile vehicles, and finally, S5, i.e., *Cruise Ships*, are luxury vessels used to take passengers on pleasure journey.

As previously discussed, the accuracy of the estimated location I_{pos} depends on the number of collected messages. Indeed, recalling Fig. 12, the number of collected messages is correlated to the time dedicated to collect them. Considering a location estimation error of

Table 2: Ship type and speeds.

	Ship Type	Speed [knots]	Speed [km/h]
S1	Bulk Carriers	13-15	24-28
S2	Container Ships	16-24	30-44
S3	Oil and chemical tankers	13-17	24-31
S4	RORO vessels	16-22	30-41
S5	Cruise Ships	20-25	37-46
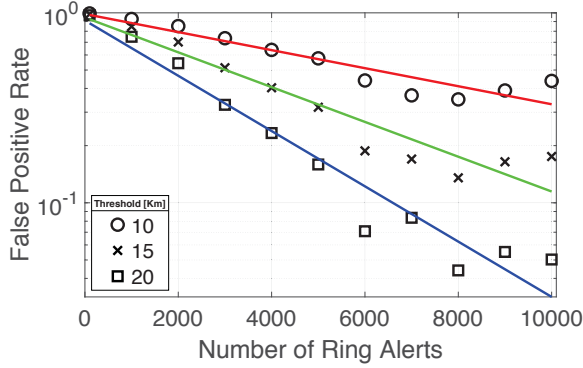
Figure 13: False positive events as a function of the number of collected IRA messages.

about 10 Km, meaning 6, 100 IRA messages to be collected in about 6 minutes (packet loss equal to 1%), the fastest ship, i.e., S5, would have moved off about 4.1Km (worst case). In the best-case scenario, the slowest ship, i.e., either S1 or S3, would have traveled less than 3.1 Km in the same amount of time (6 minutes). This means that, for all the considered cases, the movement performed by the ship is in the same order of the localization error, and therefore, our solution can be effectively adopted to detect GPS spoofing attacks.

Definition 7.1. Given a threshold *thr*, we define a *False Positive* event when no GNSS spoofing attack is present, and a position I_{pos} computed exploiting the IRA messages verifies $|I_{pos} - G_{pos}| > thr$ —where G_{pos} is the position computed from the GNSS constellation.

Figure 13 shows the false positive rate as a function of the collected IRA messages, considering three different thresholds, i.e., $thr \in \{10, 15, 20\}$ Km, for a number of IRA messages varying from 10 to 10,000. We want to stress that we are considering *single* false-positive events, while a more in-depth analysis considering the temporal distribution of false-positive events (bursts of consecutive events) might significantly improve the robustness of our solution to false alarms—this task is left for future work.

Finally, it is interesting to observe that there is a relationship between the false positive rate and the number of IRA messages considered in the location estimation technique. Indeed, we fit the samples belonging to the three different thresholds by using a

linear regression model, yielding the solid lines in Fig. 13, i.e., the red solid line for $thr = 10$ Km, the green solid line for $thr = 15$ Km, and finally, the blue solid line for $thr = 20$km. The best-fit model associated with the aforementioned samples is represented by Eq. 5:

$$y = 10^{m \cdot n} \cdot 10^q, \tag{5}$$

where *n* is the number of IRA messages, $q \approx 0$, and $m = -4.6 \cdot 10^{-5}$, $m = -8.9 \cdot 10^{-5}$, $m = -1.4 \cdot 10^{-4}$ for $thr = 10$, $thr = 15$, and $thr = 20$, respectively.

Overall, Eq. 2 and Eq. 5 allow an end-user deploying our solution to have an immediate idea of the expected system performance. In particular, knowing the number of messages received in a given unit of time, the cited equations can be used to provide an estimation of the expected location accuracy and false-positives rate of the system—this latter one with the caveat that just a single value exceeding the threshold would trigger the alarm.

7.4 Spoofing the IRIDIUM satellite constellation

With our solution in place, the only chance for the adversary to fool the receiver would be to perform a combined attack on both the GNSS and IRIDIUM platforms. In the following, we discuss the feasibility of spoofing IRIDIUM signals. As detailed in the following, it runs out that, given the nature of our solution, spoofing IRIDIUM signals to subvert our localization system is more challenging compared to all the GNSS ones.

Time. Our solution requires a not-negligible amount of time (depending on the packet loss) to locate the vessel with a small precision error (less than 10Km). While GNSS requires seconds to be spoofed, to affect our IRIDIUM-based localization system, the adversary has to deploy a transmitter that should keep transmitting for either minutes or hours, thus becoming easier to detect, identify, and locate.

Signal strength. The IRIDIUM satellite infrastructure is significantly different from the typical GNSS constellations. GNSS satellites are far away from the ground (in a MEO orbit, at about 20, 000 Km), while the Iridium constellation is composed of LEO satellites, orbiting at about 800 Km. Therefore, the received signal strength on the ground is higher than the GNSS ones [26], and hence the adversary requires higher transmission power to overcome the legitimate signal.

Complexity. The adversary should mimic a consistent array of beams moving coherently all together, at a consistent speed, with consistent interarrival times, and eventually, with compatible passes duration. We consider this event very unlikely, especially considering the time factor previously described.

8 SYSTEM-LEVEL COMPARISON WITH OTHER SOLUTIONS

To provide further insights, Table 3 wraps up an overview of the system requirements for both the works previously discussed in Section 2 and our proposal. We notice that most of the already proposed solutions rely on auxiliary network infrastructures. These auxiliary infrastructures can be set up ad-hoc for the spoofing detection task (such as in [23], [8] and [6]), or they can be already in place for other purposes (e.g., the mobile cellular network used in [17]

Table 3: Overview of related work on GNSS spoofing detection and related system requirements.

Ref.	No need for Auxiliary Ad-Hoc Infrastructure	No need for Auxiliary In-land Infrastructure	No need for PHY-layer Information	No need for Dedicated Hardware	No need for Multiple Antennas
[17]	✓	✗	✓	✓	✓
[9]	✓	✓	✗	✗	✗
[14]	✓	✓	✗	✓	✗
[29]	✓	✓	✗	✗	✗
[23]	✗	✗	✗	✓	✗
[8]	✗	✗	✗	✓	✗
[20]	✓	✓	✓	✗	✓
[6]	✗	✗	✗	✓	✗
[12]	✓	✓	✗	✗	✓
Our Proposal	✓	✓	✓	✓	✓

and the avionics network in [8]). However, these infrastructures are generally not available in remote or offshore areas, such as deserts and open seas. Other proposals, such as [9], [14], [29], and [6], rely on multi-antenna detection schemes, requiring a dedicated setup and the hard swap of existing GNSS receivers. Moreover, schemes such as [12] require access to physical layer information of the GNSS signal, and therefore, requiring dedicated equipment to be deployed, they come with consequently high costs.

Overall, the comparison shows that our proposal leveraging opportunistic IRIDIUM signals is the only one that does not require any auxiliary ad-hoc infrastructure, it does not leverage any physical layer information and, finally, it does not require the deployment of either multiple antennas or dedicated hardware. Therefore, our solution is ideal when a specific target receiver is meant to be operated in remote areas (desert or open seas), and whose hardware cannot be modified after deployment.

9 CONCLUSION AND FUTURE WORK

In this paper, we have provided two major contributions: we have reverse-engineered several system features of the IRIDIUM satellite constellation, and we have proposed a new solution to detect GNSS spoofing attacks— combining the cited features with the publicly available IRIDIUM Ring Alert messages. We have provided an efficient and effective location verification algorithm, independent from GNSS technology, that can be used to verify the actual position computed from standard GNSS technologies. Overall, our solution is worldwide-available, cheap, non-invasive, and it does not require either information from the radio physical-layer or multiple antennas. Therefore, it is particularly suitable for unattended scenarios, where there are no other entities that can help to verify the actual position of the receiver. These scenarios include deserts, poles, and open seas, to name a few. The data have been obtained thanks to an extensive measurement campaign lasting over 1000 hours, and they have been also made public to foster research in this challenging field.

Our future work will focus on the characterization of the power-law obeying phenomena highlighted by our experimental campaign, to improve the accuracy of the location verification scheme, as

well as to analyze the time-correlation among false-positive events to declare a GNSS spoofing attack. We will also collect further measurements data, using newly acquired dedicated equipment, such as powerful IRIDIUM-compliant L-band antennas.

ACKNOWLEDGEMENTS

REFERENCES

[1] Iridium burst detector and demodulator. 2019. GNURadio Iridium Out Of Tree Module. https://github.com/muccc/gr-iridium. accessed: 2020-05-15.

[2] Maurantonio Caprolu, Roberto Di Pietro, Simone Raponi, Savio Sciancalepore, and Pietro Tedeschi. 2020. Vessels Cybersecurity: Issues, Challenges, and the Road Ahead. *IEEE Communications Magazine* (2020).

[3] A. Ganz, Yebin Gong, and Bo Li. 1994. Performance study of low Earth-orbit satellite systems. *IEEE Transactions on Communications* 42, 234 (Feb. 1994), 1866–1871.

[4] N. Ghose and L. Lazos. 2015. Verifying ADS-B navigation information through Doppler shift measurements. In *IEEE/AIAA 34th Digital Avionics Systems Conference (DASC)*. 4A2–1–4A2–11.

[5] gps-sdr sim. 2020. Software-Defined GPS Signal Simulator. https://github.com/osqzss/gps-sdr-sim. accessed: 2020-05-15.

[6] L. Heng, D. B. Work, and G. X. Gao. 2015. GPS Signal Authentication From Cooperative Peers. *IEEE Transactions on Intelligent Transportation Systems* 16, 4 (Aug 2015), 1794–1805.

[7] IRIDIUM Corp. 2020. Iridium's Internet of Things - Connect to a World of IoT Possibilities. https://www.iridium.com/solutions/iot/. Accessed: 2020-05-15.

[8] K. Jansen, M. Schäfer, D. Moser, V. Lenders, C. Pöpper, and J. Schmitt. 2018. Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks. In *2018 IEEE Symposium on Security and Privacy (SP)*, Vol. 00. 189–202.

[9] Kai Jansen, Nils Ole Tippenhauer, and Christina Pöpper. 2016. Multi-Receiver GPS Spoofing Detection: Error Models and Realization. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (Los Angeles, California, USA) *(ACSAC '16)*. Association for Computing Machinery, New York, NY, USA, 237–250.

[10] M. Leng, L. Lei, S. G. Razul, and C. M. S. See. 2015. Joint synchronization and localization using iridium ring alert signal. In *10th International Conference on Information, Communications and Signal Processing (ICICS)*. 1–5.

[11] R. J. Leopold and A. Miller. 1993. The IRIDIUM communications system. In *1993 IEEE MTT-S International Microwave Symposium Digest*. 575–578 vol.2.

[12] J. Magiera and R. Katulski. 2015. Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. *Journal of Applied Research and Technology* 13, 1 (2015), 45 – 57.

[13] MarineInsight. 2019. What is The Speed of a Ship at Sea? https://www.marineinsight.com/guidelines/speed-of-a-ship-at-sea. accessed: 2020-05-15.

[14] F. A. Milaat and H. Liu. 2018. Decentralized Detection of GPS Spoofing in Vehicular Ad Hoc Networks. *IEEE Communications Letters* 22, 6 (June 2018), 1256–1259.

[15] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou. 2009. A survey on jamming attacks and countermeasures in WSNs. *IEEE Communications Surveys Tutorials* 11, 4 (2009), 42–56.

[16] G. Oligeri, S. Sciancalepore, and R. Di Pietro. 2020. Collected data from IRIDIUM satellite constellation in Doha, Qatar. https://github.com/cri-lab-hbku/iridium. accessed: 2020-05-15.

[17] Gabriele Oligeri, Savio Sciancalepore, Omar Adel Ibrahim, and Roberto Di Pietro. 2019. Drive Me Not: GPS Spoofing Detection via Cellular Network: (Architectures, Models, and Experiments). In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 12–22. https://doi.org/10.1145/3317549.3319719

[18] International Civil Aviation Organization. 2007. Manual for ICAO aereonautical mobile satellite (route) service. https://www.icao.int/safety/acp/Inactive%20working%20groups%20library/ACP-WG-M-Iridium-8/IRD-SWG08-IP05%20-%20AMS(R)S%20Manual%20Part%20II%20v4.0.pdf. accessed: 2020-05-15.

[19] Vaughan Pratt. 1987. Direct Least-Squares Fitting of Algebraic Surfaces.

[20] Y. Qiao, Y. Zhang, and X. Du. 2017. A Vision-Based GPS-Spoofing Detection Method for Small UAVs. In *13th International Conference on Computational Intelligence and Security (CIS)*. 312–316.

[21] Matthias Schäfer, Patrick Leu, Vincent Lenders, and Jens Schmitt. 2016. Secure Motion Verification Using the Doppler Effect. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '16)*. 135–145.

[22] Desmond Schmidt, Kenneth Radke, Seyit Camtepe, Ernest Foo, and Michał Ren. 2016. A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Computing Surveys (CSUR)* 48, 4 (2016), 1–31.

[23] S. Sciancalepore, G. Oligeri, and R. Di Pietro. 2018. Shooting to the Stars: Secure Location Verification via Meteor Burst Communications. In *IEEE Conference on Communications and Network Security (CNS)*. 1–9.

[24] Septentrio. 2020. Top 3 Positioning Challenges in Autonomous Marine Navigation. https://www.septentrio.com/en/insights/top-3-positioning-challenges-autonomous-marine-navigation. accessed: 2020-05-15.

[25] Z. Tan, H. Qin, L. Cong, and C. Zhao. 2019. New Method for Positioning Using IRIDIUM Satellite Signals of Opportunity. *IEEE Access* 7 (2019), 83412–83423.

[26] Zizhong Tan, Honglei Qin, Li Cong, and Chao Zhao. 2019. Positioning Using IRIDIUM Satellite Signals of Opportunity in Weak Signal Environment. *Electronics* 9, 1 (2019).

[27] N.O. Tippenhauer, C. Pöpper, K.B. Rasmussen, and S. Capkun. 2011. On the Requirements for Successful GPS Spoofing Attacks. In *Proceedings of the 18th ACM Conference on Computer and Communications Security* (Chicago, Illinois, USA) *(CCS '11)*. 75–86.

[28] Yuri DV Yasuda, Luiz Eduardo G Martins, and Fabio AM Cappabianco. 2020. Autonomous Visual Navigation for Mobile Robots: A Systematic Literature Review. *ACM Computing Surveys (CSUR)* 53, 1 (2020), 1–34.

[29] Z. Zhang, M. Trinkle, L. Qian, and H. Li. 2012. Quickest detection of GPS spoofing attack. In *IEEE Military Communications Conference*. 1–6.