FadePrint: Satellite Spoofing Detection via Fading Fingerprinting

Gabriele Oligeri*, Savio Sciancalepore†, Alireza Sadighian*
*Division of Information and Computing Technology (ICT)
College of Science and Engineering (CSE), Hamad Bin Khalifa University (HBKU), Doha, Qatar
{salhazbi, goligeri}@hbku.edu.qa
†Eindhoven University of Technology, Eindhoven, Netherlands, s.sciancalepore@tue.nl

***Abstract*—Detecting spoofing attacks to a satellite infrastructure is a challenging task, due to the wide coverage, the low received power from the satellite beams, and finally, the opportunistic nature of radio broadcasting. Although message authentication can be implemented at several communication layers, only a few solutions have been provided at the physical layer—this one exposing features that are invaluable for authentication purposes. Currently available solutions provide physical-layer authentication of the transmitter by combining deep learning and physical-layer features, thus requiring a long and computationally-intensive training process for any new transmitter joining the network. In this work, we propose FadePrint, a solution capable of detecting satellite spoofing attacks by fingerprinting the noise-fading process associated with the satellite communication channel. Indeed, the fading of a satellite link is different from the one of a terrestrial link—used very often to launch spoofing attacks—thus allowing to discriminate between the two. FadePrint does not require re-training when new transducers join the network, and it does not rely on the hardware impairments of both the transmitter and the receiver. We test FadePrint with real satellite and spoofed terrestrial radio measurements, under several different scenario configurations. We prove that FadePrint can effectively discriminate between a satellite transmitter and a fake terrestrial one, with an accuracy higher than 0.99 for all the considered configurations.**

***Index Terms*—Physical-Layer Security, Applications of AI for Security, Wireless Security.**

I. Introduction

Wireless signal *spoofing* is a malicious activity typically associated with the use of wireless communication technologies, aiming to generate radio messages with a forged source identifier [1]. Given the broadcast nature of the radio spectrum, spoofing is particularly effective, making verification of the source of the message more challenging. Spoofing attacks have been proved to be effective against several wireless technologies, e.g., LTE [2], 6LoWPAN [3], AIS [4], and GPS [5], [6]. Special attention has been paid to spoofing attacks to satellites [1]. In fact, many satellite systems emit wireless signals that are neither encrypted nor authenticated, thus easily becoming a privileged target for spoofing attacks: an adversary (the *spoofer*) can generate fake signals, e.g., by resorting to a Software Defined Radio (SDR) and publicly available software [7], [8]. Moreover, the satellite scenario is particularly prone to spoofing, due to the predictable trajectories of the satellites (transmitters location), low level of received power at the ground, possible lack of message authentication, and possible tampering/leakage of the secrets leveraged for enforcing the authentication process. Several techniques have recently been proposed for spoofing detection, mainly spanning from the application layer to the Physical-layer (PHY), so involving the usage of secrets shared among the communicating devices. In this context, PHY device fingerprinting is particularly promising. Indeed, each device features analog electronic components characterized by small differences, not affecting the device functions but that can be exploited to uniquely identify the device itself—assuming the existence of a technique able to detect, identify, and measure such differences. A recent trend involves the use of Artificial Intelligence (AI)-driven techniques to fingerprint the radio transducer at the PHY, thus preventing spoofing attacks by design [9], [10], [11]. Although PHY device fingerprinting was shown to be effective for authentication, it requires the receiver to build a *model* of each transmitter. Thus, such a technique might not scale up with the number of possible transmitters, especially in satellite scenarios.

At the same time, we observe that an effective strategy for spoofing detection in a satellite scenario could consist of the identification of the *type of link* experienced by the received signal. Indeed, if we rule out state-level adversaries equipped with their own satellite infrastructures, an adversary willing to spoof a satellite signal should deploy its transmitter on the ground and reach the receiver through a terrestrial link. However, the noise pattern (namely, the *fading*) associated with the satellite link is very different from that of a terrestrial link, due to the long distances between the communicating entities and the reduced amount of obstacles [12]. Therefore, the presence of a spoofer might be detected by only evaluating if the signal has been received from a terrestrial wireless link rather than from the (expected) satellite link.

Contribution. In this paper, we present *FadePrint*, a new satellite spoofing detection solution based on the PHY fingerprinting of the fading affecting the communication link. In summary, *FadePrint* builds a model of the expected pattern of the legitimate satellite signal received at PHY and uses this model at run-time to identify the fading process the received signal was subject to, thus identifying the presence of a terrestrial spoofing attack. We tested *FadePrint* using real satellite data from the IRIDIUM satellite constellation and a set of real spoofing attacks, carried out in several different

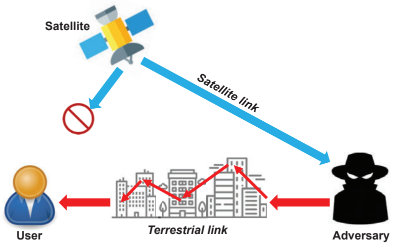


Fig. 1: Scenario and Adversary model. A user receives fake signals, either forged or replayed by the adversary. The user's challenge is to detect the spoofing attack.

scenarios (indoor, outdoor LoS/NLoS, in static and dynamic settings), achieving outstanding spoofing detection accuracy, i.e., over 0.99 in all the scenarios analyzed. Compared to current solutions, *FadePrint* does not require the generation and management of multiple transmitter models, making it lightweight and scalable by design. Finally, we also released the data generated for our performance assessment as open source to facilitate further research [13].

Roadmap. The paper is organized as follows. Section II presents the scenario and adversary model, Section III introduces the preliminaries and the dataset, Section IV provides the details of *FadePrint*, Section V provides the performance assessment, Section VI discusses additional considerations, Section VII summarizes related work, and finally, Section VIII tightens the conclusions and outlines future work.

II. Scenario and Adversary Model

Our reference scenario includes three entities: (i) a *satellite transmitter*, emitting Radio Frequency (RF) signals; (ii) a *User*, featuring a satellite receiver; and finally, (iii) an *Adversary*, able to perform either a *replay* (namely, *meaconing*) or a *spoofing* attack, as depicted in Fig. 1. The user can receive the satellite messages either from the (legitimate) actual satellite network or from a (malicious) terrestrial ground station. To discriminate between the two scenarios, we resort to the analysis of the fading process that affects the received signal. Indeed, the satellite link is characterized by a Line-of-Sight (LoS) link, with a very low Signal-to-Noise Ratio (SNR) (due to the large distance between the transmitter and the receiver), while the terrestrial link is affected by a more complex fading process, due to the presence of obstructions (shadowing) and reflections (multipath).

We considered four terrestrial scenarios.

- *Indoor.* We consider a typical office environment, without a direct LoS between the transmitter and the receiver and people moving close to the measurement setup.
- *Outdoor / Static / LoS.* We consider a crowded parking lot and we deploy both the transmitter and receiver so that LoS between them was always guaranteed.
- *Outdoor / Static / nLoS.* We consider the same parking lot as before, but we deploy the transmitter and the receiver so that there is Non-Line-of-Sight (NLoS) between them.
- *Mobile.* We set up the transmitter inside a car and we drive the car around the receiver in the same parking lot as before. In this scenario, the LoS might be present or not depending on the relative position of the transmitter and the receiver and the presence of moving entities in the parking lot.

We stress that all the bit sequences considered in this work have been taken from real satellite communications [11]. Such a choice allows us to emulate *Replay Attacks* carried out by adversarial transmitters, as per our adversary model.

Adversary Model. We consider the adversary, i.e., the terrestrial spoofing ground station, as a transmitter that can act both indoor and outdoor. The main purpose of the adversary is to deliver radio messages to the user by spoofing a satellite transmitter and have its messages accepted as legitimate. As previously mentioned, we consider all the authentication mechanisms—if any—compromised, thus making the terrestrial messages indistinguishable from the satellite ones when compared at layers higher than PHY. We remark that this is a reasonable consideration in many real-life satellite-based use cases, such as GPS, IRIDIUM, and NOAA satellites, to name a few, where no authentication protocols are in place.

III. Background and Measurements

In this section, Sec. III-A introduces the IRIDIUM satellite infrastructure and the dataset and Sec. III-B provides preliminary measurements statistics.

A. Satellite infrastructure

As a reference use-case, in this paper, we focus specifically on the IRIDIUM satellite constellation [14]. IRIDIUM was first operated in 1993 by Motorola, and the project has been recently taken over by Thales, with a new brand (Iridium NEXT) and the renewal of the satellites and the communication technology [15]. IRIDIUM is based on a total number of 66 operational satellites, orbiting on the Low-Earth Orbit (LEO), approx. 800 km over the Earth's surface, moving with a speed of approx. 7 km/s [7]. IRIDIUM satellites transmit signals in the band $[1,616 - 1,626.5]$ MHz, and users can receive and decode such signals using dedicated equipment, such as the one made available by Kyocera and Motorola. Nowadays, due to its global coverage, IRIDIUM is mostly used in the avionics and maritime domain, to allow global connectivity. However, it is also increasingly adopted in the Internet of Things (IoT) domain, especially for low-energy deployments in remote areas [16]. IRIDIUM channels can be divided into *system overhead channels*, used for the delivery of system-related information, and *bearer service channels*, used for data exchange. Within the *system overhead channels*, the IRIDIUM Ring Alert (IRA) channel is the one used by receivers on the ground to discover the presence of the IRIDIUM service and receive information on the channel where to carry out authentication and exchange data. The IRA channel uses the center frequency $1,626.27$ MHz, and it is a broadcast channel, where the satellites deliver Differentially-encoded Quadrature-Phase Shift Keying (DQPSK) messages.

Such messages can be up to 103 bytes long and contain the satellite's unique identifier, the identifier of the beam emitting the message (the beam ID 0 is reserved for the satellite radio), the satellite location (latitude, longitude, and altitude), and additional handover information (through the Temporary Mobile Subscriber Identity (TMSI) of target wireless stations). In this paper, for satellite measurements, we used the dataset released by the authors in [11], containing 589 hours (24 days) of recording of continuous acquisition of IRA messages, for a total number of $102,318,546$ physical-layer data in the form of I-Q samples ($1,550,281$ per satellite, on average). For each received IRA packet, we have the log of the reception timestamp on the receiver, the satellite ID, the beam ID, the latitude, longitude, and altitude of the emitting satellite, and the raw I-Q samples of the IRA packet. For ease of analysis, in our work, we focus the analysis on *satellite* IRA packets, i.e., the ones having beam ID 0. We refer the readers to [17] and [11] for a detailed explanation of the rationale of I-Q samples and physical-layer fingerprinting processes.

B. Measurement characterization

In this section, we perform a preliminary statistical analysis of the measurements, evaluating their SNR, signal amplitude and phase.

Signal to Noise Ratio (SNR). The SNR can be computed according to [18], i.e., by considering the periodogram of the signal $s(t) = \sqrt{i^2(t) + q^2(t)}$ and evaluating the ratio between the main signal component (first harmonic) and the other ones. Figure 2 shows the probability mass function associated with the SNR computed on the traces of our five measurement scenarios, i.e., Satellite (black solid line), Indoor (red solid line), Outdoor with LoS (blue solid line), Outdoor without LoS (green solid line), and finally, Outdoor with moving transmitter (magenta solid line). First, we observe that the SNR associated with the satellite trace is significantly higher than the other ones: this is mainly due to the antenna and the pre-amplifier adopted during the collection of the measurements in [11]. Moreover, note that there are several samples characterized by the same SNR of the terrestrial measurements, making challenging to distinguish the legitimate satellite transmitter from a ground station by simply using the SNR—there are many samples from the terrestrial scenarios with SNR greater than 0. At the same time, the value of the transmission power can be easily modified at the transmitter side, making the SNR an unreliable parameter for spoofing detection.

Amplitude analysis. An important metric is the magnitude associated with each I-Q sample, i.e., the amplitude of the phasor identified by the sample. Without loss of generality, in our analysis, we consider only the first quadrant of the I-Q plane, while similar considerations apply to the remaining quadrants. Recall that the IRIDIUM receiver station contains an Adaptive Gain Control (AGC) block in the chain. Therefore, we worked on normalized I-Q samples, i.e., assuming the expected sample to be at coordinates $[1, 1]$,—magnitude equal to 1 and phase equal to $\pi/4$. Figure 3 shows the probability distribution function of the normalized amplitude, considering all the scenarios. The maximum density is around the amplitude value of 1, while the indoor scenario has the highest variance in the terrestrial measurements—this is due to the office environment, where people move around the transmitter and receiver, producing significant fading. Finally, we observe that the satellite link is characterized by remarkable variability.

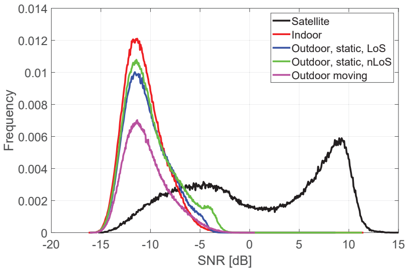


Fig. 2: SNR computed on the I-Q samples for each of the considered datasets.

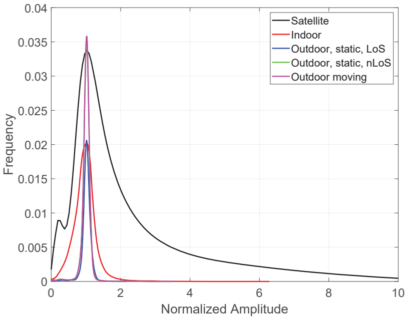


Fig. 3: Normalized amplitude of the I-Q samples belonging to the first quadrant of the I-Q plane, considering the five different scenarios taken into account in this work.

Phase analysis. We now consider the phase of each phasor identified by the associated I-Q samples in the first quadrant. As previously discussed, similar considerations apply to the samples in the other quadrants. The ideal phase should be $\pi/4$, i.e., the phase associated with the phasor with coordinates $[1, 1]$. Figure 4 shows the probability distribution function associated with the phasors' phase. All the distributions are overlapping, confirming the peak at the value $\pi/4$.

The statistical analysis of the collected traces proves the challenge of inferring the source (either satellite or ground station) when considering parameters such as the SNR, the amplitude, and the phase. Our solution grounds on the intuition of representing I-Q samples in a spatial domain (images constituted by consecutive samples) and applying a state-of-the-art anomaly detection algorithm to detect which image belongs to samples coming from a terrestrial transducer. We provide more details in the next section.

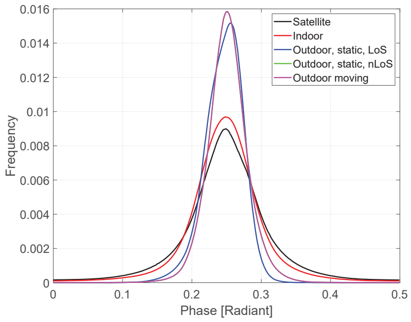


Fig. 4: Phase associated with the phasor of the I-Q samples belonging to the first quadrant of the I-Q plane, considering the five different scenarios taken into account in this work.

IV. Methodology

Figure 5 outlines the different phases of *FadePrint*. The first step involves the conversion of batches of I-Q samples into images, to then apply anomaly detection using the Fully Convolutional Data Description (FCDD) network. As shown by [19], the FCDD can be effectively used to detect the presence of anomalies in an image, overcoming other state-of-the-art techniques. I-Q samples are collected from an SDR as complex numbers, where the real part represents the in-phase component (**I**) and the imaginary part represents the quadrature component (**Q**). The subsequent step involves the computation of a bi-variate histogram on batches of I-Q samples, e.g., $N = 10,000$, by grouping them into bi-dimensional bins. The tiling should fit the input requirements of the tool used for classification, which in our case is a CNN, requiring images of size 225×225. We will evaluate the effect of choosing a different value of N in Sec. VI. The result is a matrix (bi-variate histogram), where the value of each element counts how many I-Q samples belong to the tile. Each element is considered as the value of a pixel ($[0, 255]$) of the image, provided as input to the CNN. The output of the bi-variate histogram can be greater than the maximum pixel value (255), thus requiring a proper calibration of the I-Q batch size. *FadePrint* involves a three-stage process:

- **Training.** The training process trains the FCDD network with images associated with the satellite I-Q samples. For all the scenarios, we trained the network by randomly selecting all the I-Q samples from all the satellites except two, used later on for calibration and testing.
- **Decision threshold estimation.** Here, we perform the calibration process. We test the trained model against two datasets: one constituted by I-Q samples from a terrestrial measurement and another one including I-Q samples of a satellite one. We highlight that the later satellite dataset has not been used during the training process. The calibration process returns an *anomaly index* for each processed image, thus allowing the classification of each image as either *normal* (constituted by I-Q samples coming from a satellite link) or *anomaly* (constituted by I-Q samples coming from a terrestrial link). Finally, we considered all the anomaly indexes and define a threshold minimizing both the FNs and FPs.
- **Testing.** During the testing phase, we consider two new image datasets (from both the satellite and terrestrial links) and we compute the anomaly indexes associated with each image. Note that both the satellite and terrestrial datasets considered during this phase have not been used before, either for training or for calibration. Finally, we use the previously-defined threshold to categorize the images as constituted by I-Q samples coming from either the satellite or the ground station (in different scenarios).

Our data corpus is constituted by the following datasets:

- *Satellite data.* The satellite dataset includes 66 streams of I-Q samples, i.e., one per satellite.
- *Terrestrial data.* For each scenario, we collected five streams of I-Q samples of 10 minutes each, i.e., one stream for each TX-RX pair (we used five (5) different transmitting radios for each scenario). The terrestrial data stream uses the same modulation (QPSK) and bits of the satellite one, imitating real replay and spoofing attacks.

In line with the literature, we considered three (3) datasets, i.e., $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$, for the training, calibration, and testing, respectively, of the CNN. The training set is constituted by a random permutation of images generated from I-Q samples coming from 64 out of 66 available satellite streams. The calibration dataset $\mathcal{Y} = \{Y_S, Y_T\}$ is constituted by two sets of images, i.e., Y_S being generated from one of the satellite streams not considered in $\mathcal{X}$, and Y_T being the set of images generated from one of the terrestrial measures. Finally, the testing set is represented by $\mathcal{Z} = \{Z_S, Z_T\}$, where Z_S is a set of images from a satellite stream (considered neither in $\mathcal{X}$ nor in $\mathcal{Y}$), while Z_T is a set of images from the terrestrial scenario— different from the ones in $\mathcal{Y}$.

V. Performance evaluation

In this section, we report the performance results of *FadePrint* in four different scenarios, i.e, (i) indoor (Sec. V-A), (ii) outdoor with LoS (Sec. V-B), (iii) outdoor with NLoS (Sec. V-C), and finally, (iv) outdoor with a moving transmitter (Sec. V-D). For all the analyzed scenarios, we computed the threshold (output of the calibration process in Fig. 5) by computing the anomaly indexes on the images coming from both the satellite and the terrestrial measurements, and then we applied the following Eq. 1.

$$thr = E[max(I_S), min(I_T)], \tag{1}$$

where I_S and I_T are the anomaly indexes associated with the images of the satellite and terrestrial datasets, respectively. Note that such a strategy allows for setting the threshold as the average between the highest anomaly score associated with the satellite images and the lowest anomaly score from the terrestrial images. This choice represents the best trade-off between FP and FN, minimizing their combined value.

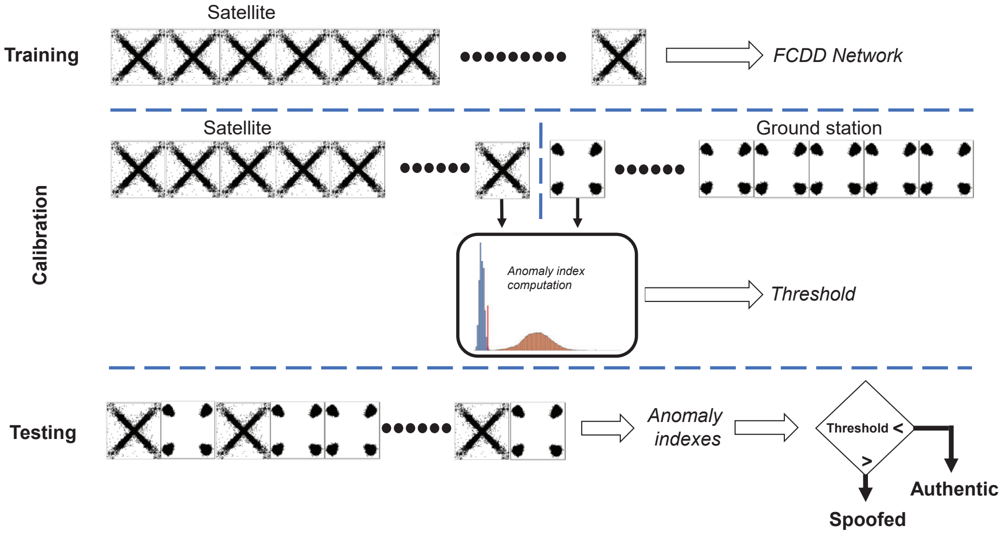
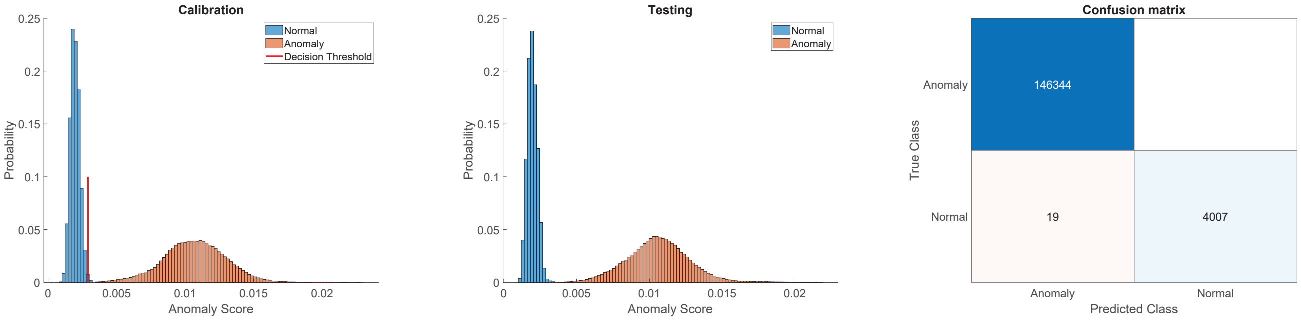


Fig. 5: *FadePrint* in brief: we considered three steps, i.e., (i) training with images generated from satellite I-Q samples, (ii) computation of the threshold from the anomaly indexes, so as to minimize False Positives (FP) and False Negatives (FN), and, (iii) testing sequences of images of both the satellite and ground station, by comparing their anomaly indexes to the threshold.



(a)

(b)

(c)

Fig. 6: Indoor scenario: (a) decision threshold calibration, (b) testing, and (c) resulting confusion matrix.

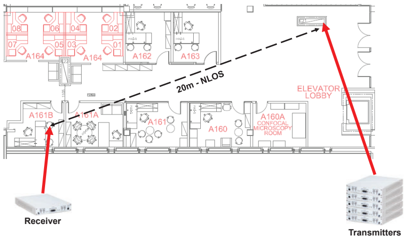


Fig. 7: Indoor scenario: the receiver is deployed 30 meters from the transmitters in an office scenario, with NLoS.

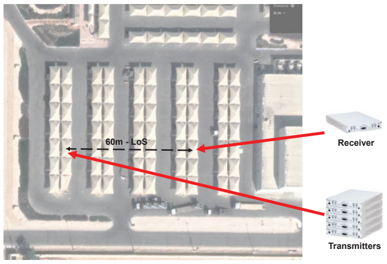


Fig. 8: Outdoor scenario with LoS: we considered a parking lot with LoS between the transmitters and the receiver.

A. Indoor Scenario

We consider as indoor scenario a typical crowded office environment, where the five transmitters are located 30 meters away from the receiver, without a line of sight (NLoS). We deployed the receiver inside the office, while we positioned the transmitters in a corridor, with people moving around. We performed several 10-minutes long measurements, one for each TX-RX pair, for a total of five measurements $(146M+$

I-Q samples for each measurement). Figure 7 shows the floor plan of the considered indoor scenario and the associated layout of the equipment. Figure 6 shows the results of (a) the calibration process, (b) the testing, and finally, (c) the confusion matrix associated with the testing process for the indoor scenario. After the training, we performed the calibration by computing the anomaly score on two datasets of images (generated from satellite I-Q samples and from terrestrial ones). Then, we computed the histograms over the normal (satellite) and anomaly (terrestrial) indexes, represented with blue and orange bars, respectively, and we computed the detection threshold (solid red line) as in Eq. 1. Note that the threshold value for this specific scenario is $thr = 2.9 \cdot 10^{-3}$. We subsequently computed the anomaly indexes over two new datasets from a satellite and a terrestrial measurement. We ran the aforementioned procedure by randomly permuting the satellite and terrestrial streams 100 times, to de-correlate our results from specific satellites and terrestrial transmitters, obtaining Fig. 6(b)—testing phase. Finally, we computed the confusion matrix (Fig. 6(c)) by applying the previously computed decision threshold thr to the anomaly indexes generated during the testing. We obtain an accuracy greater than 0.99 and only 19 FPs out of $150,370$ samples.

B. Outdoor Scenario: Static Receiver with Line of Sight (LoS)

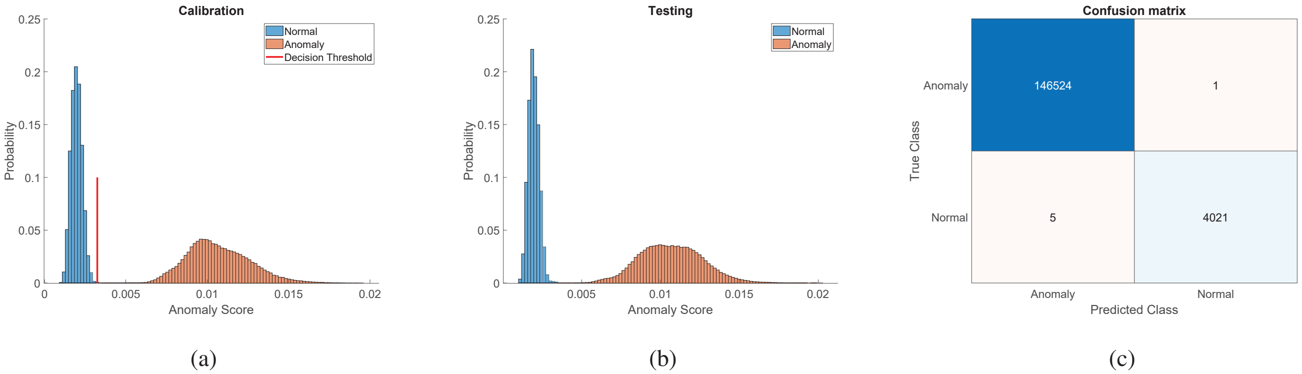
In this section, we consider an outdoor parking lot, where we placed the five transmitters 60 meters away from the receiver while guaranteeing the LoS. As for the previous scenario, we collected five measurements, i.e., one for each transmitter-receiver pair, lasting 10 minutes each, summing up to $146M+$ samples per measurement. Figure 8 shows the considered scenario and the relative positions of the transmitters and the receiver. Figure 9 shows the results from the considered *FadePrint* phases: (a) calibration of the decision threshold, (b) testing, and finally, (c) confusion matrix associated with the testing process. As previously discussed, we considered 100 random permutations of satellite and terrestrial measures (streams), to de-correlate our results from specific emitters. Moreover, at each round, we performed a new training process, we generated the anomaly indexes for the threshold calibration, and we computed the threshold value according to Eq. 1, considering the anomaly indexes obtained from the testing process. Fig. 9(c) shows the resulting confusion matrix. Note that the specific value of the decision threshold computed for this scenario is $3.2 \cdot 10^{-3}$. The confusion matrix proves that *FadePrint* can detect the presence of a terrestrial spoofer also in an outdoor scenario with LoS between the transmitter and the receiver. In particular, we experienced only 1 FNs and 5 FPs out of $150,551$ considered samples, resulting in an overall accuracy greater than 0.99.

C. Outdoor Scenario: Static Receiver with NLoS

The second outdoor scenario we consider takes into account the same parking lot, but without the line of sight (NLoS). In particular, we placed the five transmitters and the receiver 30 meters away, while the LoS was obstructed by the presence of multiple moving cars and people. Note that the described measurement condition is specifically intended to match an actual live spoofing attack, where several unpredictable factors might affect the scenario. Figure 10 depicts the scenario and the layout of the equipment deployment considered for this measurement. Figure 11 shows the results of the data processing: (a) calibration, (b) testing, and (c) the resulting confusion matrix. The calibration phase involved the computation of the detection threshold thr according to Eq. 1, being equal to $4.3 \cdot 10^{-3}$. Figure 11 (b) reports the histogram computed over the anomaly indexes from the images belonging to the testing dataset, while Fig. 11 (c) shows the confusion matrix computed with $thr = 4.3 \cdot 10^{-3}$. We remark that the presented confusion matrix wraps up on 100 random permutations of satellite and terrestrial measurements, to de-correlate our results from specific transducers. Note that our solution can perfectly detect the presence of a terrestrial spoofer here, reporting zero FPs and FNs out of $150,456$ images.

D. Outdoor scenario: Moving transmitter

In the final scenario, we consider a static receiver and five moving transmitters deployed in the same parking lot described above. While the receiver was static on top of a table, the transmitters (one per time) have been set up inside a car moving around the receiver's position inside the parking lot, as depicted in Fig. 12, where the blue dots represent the GPS coordinates of the trajectory performed by the transmitter radio. The distances between the transmitters and the receiver varied between a few meters and 60 meters, with and without the LoS depending on the presence of random obstructions due to cars and people moving around. As for the previous scenarios, we show the decision threshold calibration, the testing, and finally, the resulting confusion matrix in Fig. 13(a), (b), and (c), respectively. Similarly, to de-correlate our results from specific satellite transducers and terrestrial transmitters (device fingerprinting), we run 100 random permutations of satellite and terrestrial measurements, performing the training and the computation of the anomaly indexes on disjoint datasets. Then, we considered the histograms associated with the anomaly indexes and we computed the decision threshold according to Eq. 1, reporting the value $3.1 \cdot 10^{-4}$. We then considered a testing dataset and applied the previously-computed decision threshold to obtain the confusion matrix, as per Fig.13(c). Although the discrimination accuracy is still remarkable, i.e., greater than 0.99, we acknowledge that our solution reports also 10 FPs and 75 FNs cases out of $150,421$ considered images. Indeed, the mobile scenario is affected by a fading process that is much more random than the scenario previously considered. The I-Q samples are grouped into clouds that are frequently changing in shape and position, and for a few of them ($75 + 10 = 85$), it is not possible to detect them as anomalies compared to the ground truth (satellite images). However, such cases amount to less than 1%.



(a)

(b)

(c)

Fig. 9: Outdoor scenario, static receiver with LoS: (a) decision threshold estimation, (b) testing, and (c) confusion matrix.

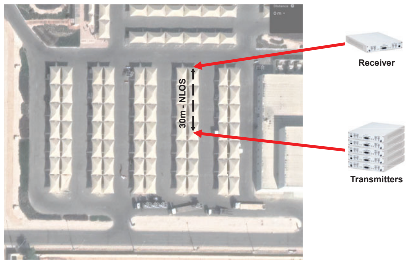


Fig. 10: Outdoor scenario with NLoS: we placed the receiver 30 m away from five transmitters in a crowded parking lot.

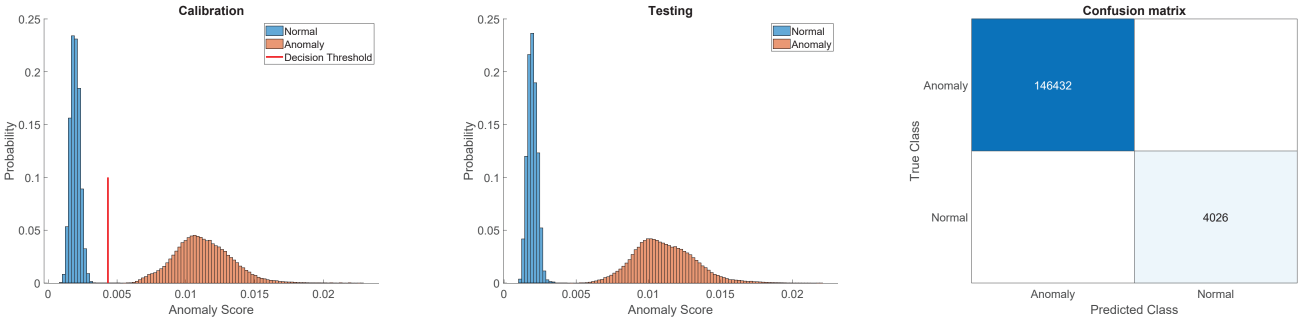
VI. Discussion

The results presented in the previous sections highlight the suitability of our solution for terrestrial spoofing detection. Also, such results demonstrate the implicit scalability of our solution with respect to the number of transmitters. Indeed, as described in Sec. IV, the testing set $\mathcal{Z}$ contains samples of satellites not considered neither for training nor for testing. Thus, *FadePrint* can identify legitimate satellites, without the need for training on that specific satellites. This is a critical distinguishing feature of *FadePrint* compared to RF fingerprinting approaches such as [11], making our solution more scalable. We also note that the overhead of *FadePrint* is very limited. We considered a server with 512GB of RAM and 2 TESLA M100, where training and calibration took approx. 6 hours, worst-case. However, such training time is required only once, before system deployment. *FadePrint* uses such models for a classification task, requiring a time in the order of a few milliseconds on a standard off-the-shelf laptop.

An important parameter of *FadePrint* is the number of I-Q samples per image, i.e., the number of I-Q samples taken into account when generating each image. This number affects the detection performance, since a low number of I-Q samples might produce many images without the features required for the training, calibration and testing. Conversely, a high number of I-Q samples per image might reduce the image dataset size (the total number of I-Q samples is fixed) and hide the features in the noise caused by other I-Q samples. Moreover, the more I-Q samples per testing image, the more the time to acquire them, and the higher the acquisition time and energy consumption of *FadePrint*. Figure 14 shows the accuracy of *FadePrint* as a function of the number of I-Q samples N per image, considering the reference case of the static outdoor scenario without the Line of Sight (LoS). Without loss of generality and due to space constraints, we consider only one scenario (outdoor / static / nLoS) while we verified similar results for the other ones. The accuracy of *FadePrint* is close to zero when $N < 5,000$ samples, while it approaches 1 when $N > 10,000$—this one being the number of samples per image adopted in this work. Moreover, considering that the satellite sample rate is 2Msa/s [11], we highlight that the time to acquire all the samples belonging to one image is about 5 ms, making our solution very fast. We summarize our findings in Table I. Note that the "outdoor moving" scenario is characterized by temporal variations in the environment: the distance between the transmitter and the receiver was varying between a few meters and 60 meters, while the LoS was affected by (random) obstructions during the whole measurement. The accuracy is very high (> 0.99) for all the considered scenarios, practically demonstrating the effectiveness of the proposed solution. Although the thresholds are quite different, their selection is based on factors well-known in advance at the receiver side, i.e., environment (indoor or outdoor), and receiver state (static or moving). Thus, the receiver can easily set such a threshold according to current operational conditions, maximizing the performance. Finally, note that the maximum distance of 60 meters set in our experiments is due to limitations associated with the maximum transmission power of the adopted radios.

VII. Related Work

Spoofing and replay (meaconing) of satellites' messages is increasingly becoming an actual threat [20], [21]. Several recent contributions investigated PHY fingerprinting in many different forms and objectives, also with reference to GPS satellites [22]. A few works already noticed the correlation between the raw received messages and the experienced channel. To name a few, Shawabkha et al. [10] analyzed the



(a)

(b)

(c)

Fig. 11: Outdoor scenario, static receiver with nLoS: (a) decision threshold estimation, (b) testing, and (c) confusion matrix.

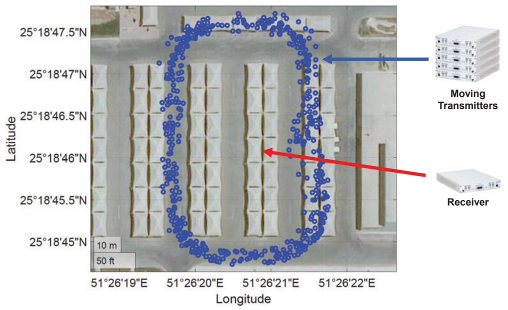


Fig. 12: Outdoor Moving Scenario. We considered five different moving transmitters and a static receiver in a crowded parking lot, with the trajectory represented by the blue dots.

TABLE I: Scenarios, decision thresholds, and performance.

Scenario	**Distance [m]**	**LoS**	**Decision threshold** $[\times 10^{-3}]$	**Accuracy**
Indoor	30	✗	2.9	> 0.99
Outdoor Static LoS	60	✓	3.2	> 0.99
Outdoor Static NLoS	30	✗	4.3	1
Outdoor Moving	[5-60]	✓/ ✗	3.1	> 0.99

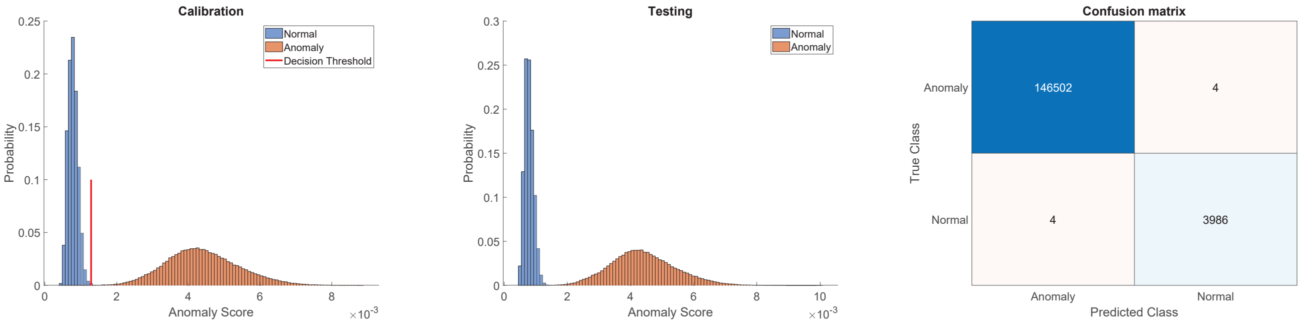
impact of the wireless channel in the PHY authentication process, identifying the undesirable effects of the fading on device identification. However, they did not deepen further their analysis [23], [24]. Similarly, works such as [25] used the Signal Quality Monitoring (SQM) as an indicator to detect satellite spoofing. As shown in Sec. III-B, legitimate and spoofing signals might appear to have the similar SQM, being instead different when comparing the respective I-Q samples. A few works use plaintext or side-information to infer traffic exchanged in a communication link. For instance, Trinh et al. [26] classified mobile traffic using radio-link data, despite encryption. However, this fingerprinting applies to traffic features. Conversely, our work leverages PHY features. A few works used the Channel State Information (CSI) to fingerprint a static communication channel, e.g., [27] and [28]. However, such solutions cannot work in a mobile scenario, like ours. Location-based fingerprinting has been used also in the avionics domain, to authenticate aircraft, e.g., by using the Channel Impulse Response (CIR) [29], and carrier phase [30]. However, as reported in [31], these approaches require transmitter collaboration. Conversely, our approach is completely opportunistic. Finally, other related works such as [32], [33] leveraged PHY-layer metrics for GNSS technologies. However, the proposed metrics are specific to the application scenarios and they cannot be applied in other contexts, e.g., any (LEO) satellite constellation. In summary, to the best of our knowledge, no previous works proposed to detect satellite spoofing through the fingerprinting of the fading phenomena using raw I-Q samples. Also, there are no real data available about actual spoofing attacks on LEO satellites.

VIII. Conclusion and Future Work

We proposed *FadePrint*, a spoofing detection technique for satellite links, based on the fingerprinting of the fading of the communication channel to infer the presence of a spoofer (terrestrial transmitter) despite a legitimate satellite transmitter. Differently from the literature, *FadePrint* does not require training a new model every time a new transducer joins the network, since it exploits the unique features of the fading process of a satellite link—being completely different from the ones of a terrestrial link. We tested *FadePrint* using real satellite (ground-truth) and real terrestrial measurements in different configurations, taking into account indoor and outdoor scenarios with different mobility features. *FadePrint* proved to be very effective in detecting the presence of a spoofer (link with a fading process typical of a terrestrial communication link), with accuracy greater than 0.99 for all the considered scenarios. Future work involve the analysis of *FadePrint* with different satellite technologies, anomaly detection algorithms, and a wider range of configuration parameters.

References

[1] Schmidt, D. et al., “A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures,” *ACM Comput. Surveys*, vol. 48, no. 4, pp. 1–31, 2016.



(a) (b) (c)

Fig. 13: Outdoor moving scenario: (a) decision threshold estimation, (b) testing, and (c) confusion matrix.

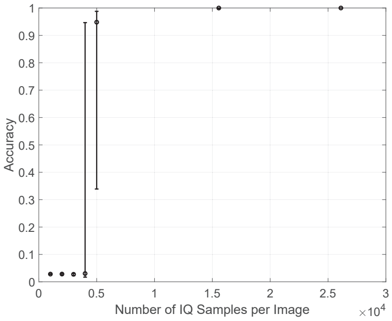


Fig. 14: Accuracy as a function of the number of I-Q samples per image, for the static outdoor scenario with nLoS.

[2] Lichtman, M. et al., "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," *IEEE Commun. Mag.*, vol. 54, no. 4, pp. 54–61, 2016.

[3] M. Mavani and K. Asawa, "Modeling and analyses of IP spoofing attack in 6LoWPAN network," *Comput. & Secur.*, vol. 70, pp. 95–110, 2017.

[4] Ray, C. et al., "DeAIS project: Detection of AIS spoofing and resulting risks," in *OCEANS*, 2015, pp. 1–6.

[5] Jafarnia-Jahromi, A. et al., "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *Int. Jour. of Navigation and Observation*, vol. 2012, 2012.

[6] Tippenhauer, N. et al., "On the requirements for successful GPS spoofing attacks," in *ACM Conf. on Comput. and Commun. Security*, 2011, pp. 75–86.

[7] Oligeri, G. et al., "GNSS Spoofing Detection via Opportunistic IRIDIUM Signals," in *ACM Conf. on Security and Privacy in Wirel. and Mob. Netws.*, 2020, p. 42–52.

[8] Raponi, S. et al., "Road Traffic Poisoning of Navigation Apps: Threats and Countermeasures," *IEEE Security Privacy*, pp. 2–11, 2021.

[9] Sankhe, K. et al., "No radio left behind: Radio fingerprinting through deep learning of physical-layer hardware impairments," *IEEE Trans. on Cognit. Commun. and Netw.*, vol. 6, no. 1, pp. 165–178, 2019.

[10] Al-Shawabka, A. et al., "Exposing the fingerprint: Dissecting the impact of the wireless channel on radio fingerprinting," in *INFOCOM 2020*. IEEE, 2020, pp. 646–655.

[11] Oligeri, G. et al., "PAST-AI: Physical-layer Authentication of Satellite Transmitters via Deep Learning," *IEEE Trans. on Informat. Forensics and Security*, vol. 18, pp. 274–289, 2022.

[12] Vinogradov, E. et al., "Tutorial on UAV: A blue sky view on wireless communication," *arXiv preprint arXiv:1901.02306*, 2019.

[13] Anonymized Authors, "Data Collection for Satellite Spoofing Detection via Fading Fingerprinting," https://www.dropbox.com/sh/ei098dpb0vsxb9n/AADRt67w3pQaJnzlMHvklVkKa?dl=0, Jun. 2022, (Accessed: 2023-Jun-26).

[14] Pratt, S. et al., "An operational and performance overview of the IRIDIUM low earth orbit satellite system," *IEEE Commun. Surveys*, vol. 2, no. 2, pp. 2–10, 1999.

[15] IRIDIUM Corp., "Happy Birthday IRIDIUM Next," https://www.thalesgroup.com/en/worldwide/space/news/happy-birthday-iridium-next-0, January 2022, (Accessed: 2023-Jun-26).

[16] ——, "Iridium's Internet of Things - Connect to a World of IoT Possibilities," https://www.iridium.com/solutions/iot/, February 2020, (Accessed: 2023-Jun-26).

[17] T. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. USA: Prentice Hall PTR, 2001.

[18] Mathworks, "snr - Signal to Noise ratio," https://nl.mathworks.com/help/signal/ref/snr.html, (Accessed: 2023-Jun-26).

[19] Liznerski, P. et al., "Explainable Deep One-Class Classification," in *Int. Conf. on Learn. Representat.*, 2021.

[20] Simple Flying, "Finnair Noticing GPS Abnormalities Near The Russian Border," https://simpleflying.com/finnair-gps-abnormalities-russian-border/, March 2022, (Accessed: 2023-Jun-26).

[21] Lenhart, M. et al., "Distributed and Mobile Message Level Relaying/Replaying of GNSS Signals," in *Int. Technical Meet. of The Institute of Navigation*, 2022, pp. 56–67.

[22] Foruhandeh, M. et al., "Spotr: GPS Spoofing Detection via Device Fingerprinting," in *ACM Conf. on Security and Privacy in Wirel. and Mob. Netwks.*, 2020, pp. 242–253.

[23] Restuccia, F. et al., "DeepRadioID: Real-Time Channel-Resilient Optimization of Deep Learning-Based Radio Fingerprinting Algorithms," in *ACM Mob. Ad Hoc Network. and Comput.*, 2019, p. 51–60.

[24] Soltani, N. et ak,, "More Is Better: Data Augmentation for Channel-Resilient RF Fingerprinting," *IEEE Commun. Mag.*, vol. 58, no. 10, pp. 66–72, 2020.

[25] Pini, M. et al., "Signal Quality Monitoring applied to Spoofing Detection," in *ION GNSS)*, 2011, pp. 1888–1896.

[26] Trinh, D. et al., "Mobile Traffic Classification Through Physical Control Channel Fingerprinting: A Deep Learning Approach," *IEEE Trans. on Netw. and Serv. Managem.*, vol. 18, no. 2, pp. 1946–1961, 2021.

[27] Tong, X. et al., "CSI Fingerprinting Localization With Low Human Efforts," *IEEE Trans. on Network.*, vol. 29, no. 1, pp. 372–385, 2020.

[28] Wang, X. et al., "CSI-Based Fingerprinting for Indoor Localization: A Deep Learning Approach," *IEEE Trans. on Veh. Technol.*, vol. 66, no. 1, pp. 763–776, 2016.

[29] Zhang, J. et al., "Mobility assisted secret key generation using wireless link signatures," in *IEEE INFOCOM*, 2010, pp. 1–5.

[30] Wang, Q. et al., "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *IEEE INFOCOM*, 2011, pp. 1422–1430.

[31] Strohmeier, M. et al., "Security of ADS-B: State of the Art and Beyond," *arXiv preprint arXiv:1307.3664*, 2013.

[32] Calvo-Palomino, R. et al., "Short: LSTM-based GNSS Spoofing Detection Using Low-cost Spectrum Sensors," in *Int. Symp. on "A World of Wirel., Mob. and Multimedia Netwks."*, 2020, pp. 273–276.

[33] Sun, C. et al., "Robust Spoofing Detection for GNSS Instrumentation Using Q-Channel Signal Quality Monitoring Metric," *IEEE Trans. on Instrumentat. and Measurem.*, vol. 70, pp. 1–15, 2021.