

Efficacy of Asynchronous GPS Spoofing Against High Volume Consumer GNSS Receivers

M Surendra Kumar
 msurendrakumar2008@gmail.com
 Department of Aerospace
 Engineering, Indian Institute of
 Technology, Bombay
 Mumbai, Maharashtra, India

Gaurav S Kasbekar
 Department of Electrical Engineering,
 Indian Institute of Technology,
 Bombay
 Mumbai, Maharashtra, India
 gskasbekar@ee.iitb.ac.in

Arnab Maity
 Department of Aerospace
 Engineering, Indian Institute of
 Technology, Bombay
 Mumbai, Maharashtra, India
 arnab@aero.iitb.ac.in

Abstract

The vulnerability of the Global Positioning System (GPS) against spoofing is known for quite some time. Also, the positioning and navigation of most semi-autonomous and autonomous drones are dependent on Global Navigation Satellite System (GNSS) signals. In prior work, simplistic or asynchronous GPS spoofing was found to be a simple, efficient, and effective cyber attack against L1 GPS or GNSS dependent commercial drones. In this paper, first we make some important observations on asynchronous GPS spoofing attacks on drones presented in prior research literature. Then, we design an asynchronous GPS spoofing attack plan. Next, we test the effectiveness of this attack against GNSS receivers (high volume consumer devices based on Android mobile phones) of different capabilities and a commercial drone (DJI Mavic 2 Pro) under various conditions. Finally, we present several novel insights based on the results of the tests.

CCS Concepts: • **General and reference** → *Evaluation*; • **Security and privacy** → *Denial-of-service attacks*; *Embedded systems security*; **Usability in security and privacy**.

Keywords: vulnerability, asynchronous, GPS Spoofing, attack plan, GNSS receiver

ACM Reference Format:

M Surendra Kumar, Gaurav S Kasbekar, and Arnab Maity. 2022. Efficacy of Asynchronous GPS Spoofing Against High Volume Consumer GNSS Receivers. In *Proceedings of October 24–28, 2022 (MSWiM '22)*. ACM, Montreal, Canada, 10 pages. <https://doi.org/XXXXXX.XXXXXX>

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.

MSWiM '22, Montreal, Canada,

© 2022 Association for Computing Machinery.
 ACM ISBN 978-x-xxxx-xxxx-x/YY/MM...\$15.00
<https://doi.org/XXXXXX.XXXXXX>

1 Introduction

Unmanned Aerial Vehicles (UAVs) or drones are no more a technology of the future; they are a current story unfolding [19]. Nearly all the businesses, activities, and services carried out by humankind on this planet are on the verge of being disrupted by this technology [5]. Indian national planners too have taken cognizance of this possibility and have liberalized the civilian drone rules along with introducing the Production Linked Incentives (PLI) in our country [23]. The impact of these changes made is seen as a catalyst in expanding the Indian drone industry, which is presently having a turnover of approximately Indian National Rupees (INR) 80.00 crores, to an estimated INR 900.00 crores by 2023 and INR 15,000.00 crores by 2026 [20]. It is also estimated that every year, 10 million plus GNSS enabled drones will be manufactured and shipped this decade [10]. This exponential growth in the number of drones around us makes it imperative for us to assess the vulnerabilities of commercially available UAVs against various threats and be prepared to exploit or counter them.

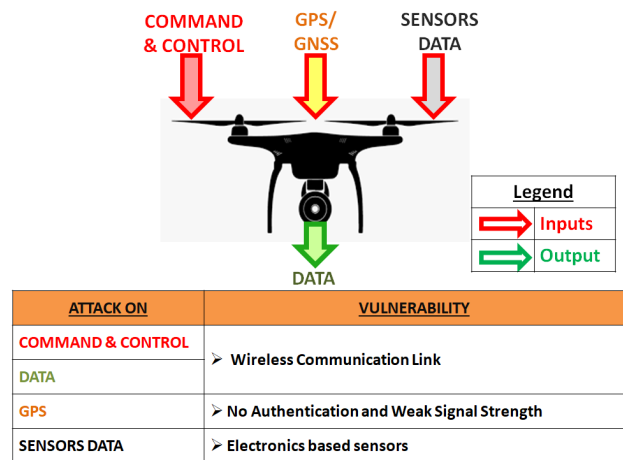


Figure 1. Ingress and egress routes, i.e., inputs into and outputs from a drone along with their vulnerabilities.

Researchers worldwide have studied cyber-security vulnerabilities of UAVs [12, 13, 22, 36, 38]. Cyber threats are often considered equivalent to theft or disruption, and these

are carried out using the ingress or egress routes [14]. Fig. 1 shows the vulnerabilities in ingress and egress routes, i.e., the inputs to and outputs from a UAV. In semi-autonomous and autonomous drones, the GPS or GNSS input is vital since in addition to basic positioning and reporting locations on maps, other functions such as return to home and no-fly zone are based on them. From previous work done in this field, it was found that GPS spoofing is an effective attack and it is applicable against a large number of commercial drones.

Based on the success of GPS spoofing against commercial drones in previous research works, our main aim was to check if GPS spoofing can be used as an effective counter-measure against rogue commercial drones. As more than 90% of high volume consumer devices support only the L1 frequency [9], in this work we set up an asynchronous GPS spoofing attack and test its efficacy against GNSS receivers (single frequency multi-constellation based receivers with different capabilities in high volume consumer devices such as Android mobiles) and a commercial drone. The major contributions of this paper are as follows:

- We first observe the commonality in the conditions under which GPS spoofing attacks reported in prior research literature were conducted.
- Next, we design a detailed GPS spoofing attack plan.
- We generate GPS spoofing signals and transmit them.
- We test our attacks against GNSS receivers and a commercial drone under different conditions.
- We present our observations from the results.

The rest of this paper is organized as follows. Section 2 provides a review of prior research literature. We explain our GPS spoofing attack plan in Section 3. Section 4 describes the experimental setup and scenarios. In Section 5, the results obtained from our experiments are presented and discussed. Section 6 concludes our work.

2 Related Work

Commercial drones can be categorized into three types, based on the role of an operator and its autonomy [1]: 1) Remotely Piloted Vehicle: Driven by drone pilots, always keeping the drone within their visual range, 2) Semi-Autonomous: Has capabilities such as hovering and returning to home without inputs by the operator, 3) Fully-Autonomous: Does not necessarily require a Command-and-Control (C2) link.

The GPS is an all-weather, satellite-based navigation system developed by the Department of Defence (DOD) of the United States. It was developed for military use, but today it continuously provides position, velocity, and time (PVT) services to military as well as civilian users worldwide at or near the surface of the earth [26, 37]. Satellite navigation systems with global coverage are termed GNSS [4]. E.g., United States' GPS, Russia's GLONASS, China's BeiDou navigation satellite system, and the European Union's Galileo are the

four operational GNSS. Japan and India have their regional satellite-based navigation systems [4]. GPS being the earliest in becoming fully functional with global coverage and free of cost, has been widely used commercially. 100% of GNSS receivers manufactured till date have L1 frequency compatibility [25]. Moreover, over 70% of the GNSS receivers can operate only on the L1 frequency [25].

The vulnerability of L1 GPS signals is known for almost two decades now. Civilian GPS signals are vulnerable due to three reasons:

- Transparency of the technology [4, 26, 27, 37]: Owing to this, developers have developed software to generate signals similar to GPS. An open source GPS simulator is [8] (commercially too GPS or GNSS simulators [24, 29] are available).
- The fact that there is no authentication mechanism in civilian L1 GPS signals keeps it vulnerable to spoofing [4, 26, 27, 37].
- The low power of the GPS received signals [4, 26, 27, 37] keeps it vulnerable to being over-powered.

The GPS spoofing threat was assessed and various versions of GPS spoofing were explained by the authors in [18]. Different versions of GPS spoofing include asynchronous spoofing (when an attacker does not synchronize the spoofed signals with the original GPS signals), intermediate spoofing (in this, an attacker synchronizes the spoofed signal based on the knowledge of the receiver's location and time), sophisticated spoofing (in this, an attacker transmits synchronized spoofed signals using multiple antennae to overcome the direction of arrival counter-measure), and meaconing (in this spoofing methodology, an attacker re-transmits the received authentic signals) [18]. The authors of [18] also developed a sophisticated GPS spoofer, but it was too bulky and costly. The authors of [35] explained the nuances of carrying out successful GPS spoofing attacks; however, most of the experiments in this paper were set up in a controlled environment. In [34], the authors demonstrated hacking a commercial civilian UAV using GPS spoofing. The hacking was carried out under the live sky, but used specifically designed GPS spoofing equipment. GPS spoofing using a Software Defined Radio (SDR) was demonstrated in [17]. A software developer developed code for a GPS simulator and made it public by uploading the same on GitHub [8]. This simulator generated L1 civilian GPS baseband signal data streams and required an SDR for generation and transmission (Tx) of Radio Frequency (RF) signals. In [17] and [8], the equipment and process for carrying out an asynchronous GPS spoofing attack were simplified. Numerous research works have been done since then, in the area of GPS spoofing simulations and attacks, showing the vulnerabilities of various commercial drones using open source code or commercial GPS simulators [2, 7, 15, 16, 28, 32, 33, 39]. Nearly all of the GPS spoofing work done till date have been reviewed in [21]. The authors

Table 1. System and conditions of GPS spoofing

Reference	System	Conditions
[16]	SDR (BladeRF X40)+Open Source Simulator (OSS)	<ul style="list-style-type: none"> • Static and dynamic spoofing done against static drone • Experiment carried out indoor
[15]	SDR (USRP B210)+ Replayed received signal	<ul style="list-style-type: none"> • Target's position required • Target drone in loiter or hovering mode
[7]	LABSAT3 GPS simulator	<ul style="list-style-type: none"> • Experiment carried out indoor • Drone in static position
[2]	SDR (BladeRF X40) +OSS	<ul style="list-style-type: none"> • Experiment carried out indoor • Drone landed or hovering
[39]	SDR (HackRF One)+OSS	<ul style="list-style-type: none"> • Attacks carried out against hovering or landed drone
[33]	Aeroflex GPSG -1000 GPS simulator	<ul style="list-style-type: none"> • Experiment carried out under lab conditions • In absence of live-sky signals
[32]	SDR (BladeRF X40)+OSS	<ul style="list-style-type: none"> • Attacks carried out against hovering drone

did not limit their review to GPS spoofing attacks against aerial platforms, but also included non aerial platforms.

Table 1 tabulates some of the recent successful GPS spoofing attacks against commercial civilian drones along with the spoofing system utilised and the specific conditions under which attacks were carried out. It can be observed from Table 1 that most of the spoofing attacks have been carried out against static or hovering drones and indoors (in absence of live sky signals). Moreover, all the attacks were against GPS receivers and not against GNSS receivers. In [40], the authors summarized various countermeasures against GNSS spoofing, along with the sophistication and cost required in implementing them. Table 1 shows that under the conditions listed in the table, GPS spoofing attacks are successful against commercial drones. However, in [31], it has been shown that mass consumer devices like Android mobiles with dual-frequency band GNSS chipset are resilient against synchronous GPS spoofing attacks. In this paper, we seek to evaluate the efficacy of asynchronous GPS spoofing, find out the conditions under which it works and hence can be used as an effective countermeasure against rogue commercial drones, and to suggest countermeasures to protect drones against it.

3 GPS Spoofing Attack Plan

The GPS spoofing attack plan was designed and executed to check the efficacy of asynchronous GPS spoofing against GNSS receivers. The attack plan consists of the following phases: generation, Tx, target, and testing. Fig. 2 shows our attack plan.

3.1 Generation of GPS Spoofed Signal

The generation of a GPS baseband signal has been carried out on a laptop with Windows 10 as its operating system. GPS-SDR-SIM [8] is used as the GPS simulator in our experiments. GPS-SDR-SIM is an open source GPS simulator

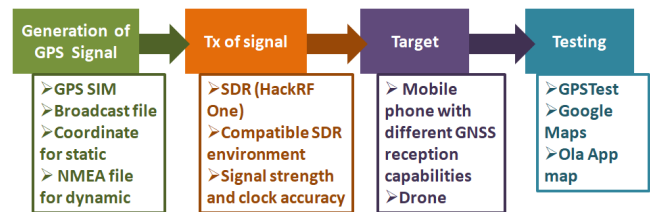


Figure 2. GPS spoofing attack plan designed considering generation, transmission (Tx), targets of attack, and method to test the results.

written in C, which can generate GPS baseband data streams in binary format. A Receiver INdependent EXchange format (RINEX) navigation file for GPS ephemerides is required by GPS-SDR-SIM, which can be downloaded from the cddis.nasa website [6]. The broadcast ephemeris files are named as brdcDDD0.YYn, where DDD is the number of days of the year, i.e., 001 to 365/ 366 and YY are the last two digits of the year. E.g., for 10 Jun 2022, the broadcast ephemeris file is uploaded with the name brdc1610.22n. The broadcast ephemeris file data is uploaded post 4 hours; thus, spoofing was not carried out for real-time scenarios. For static spoofing (i.e., when the generated spoofed signals make a GPS receiver compute its position to be a static location), GPS-SDR-SIM requires the coordinates of the destination in either x,y,z in the Earth Centered Earth Fixed (ECEF) coordinate system or latitude (lat), longitude (long), and altitude (alt) in the World Geodetic System (WGS 84 coordinate system). We used the lat, long, and alt data and sourced these information of the desired spoofed destination locations from Google Maps. For dynamic spoofing (i.e., when the generated spoofed signals make a target GPS receiver compute its position to follow a dynamic path with a certain velocity), GPS-SDR-SIM requires either a user defined Comma Separated Values (CSV) file or

a National Marine Engineering Association (NMEA) GGA stream of data. We utilised Google Earth to define a route at the desired location, exported the Keyhole Markup Language (KML) file onto the SatGen software [24] (Labsat provides a trial version of its SatGen software which can generate a L1 Coarse Acquisition (C/ A) signal) and generated the NMEA GGA data stream. Fig. 3 is a pictorial representation of how the spoofed GPS signal is generated.

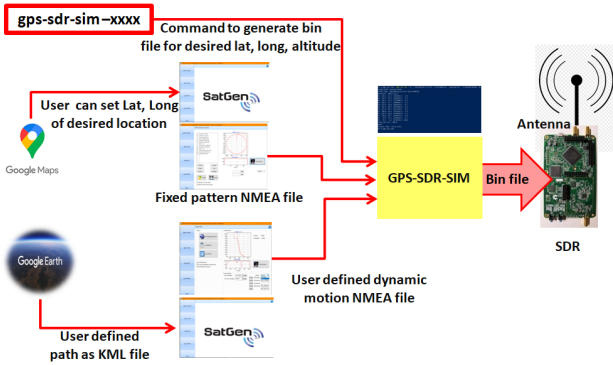


Figure 3. The image shows how generation of various spoofed GPS signals (static or dynamic) has been carried out.

3.2 Tx of Generated Spoofed Signal

The generated GPS baseband data streams are converted to RF using a Software Defined Radio (SDR). We have utilized the HackRF One SDR (the lowest price of HackRF One SDR in comparison to other available SDRs was the reason for choosing it). For Tx of the generated RF signal, a compatible 700-5800 MHz directional patch array antenna was utilised. The intention behind using a directional antenna was to keep the generated spoofed signals in the desired directions only, while carrying out the experiments. The internal crystal clock accuracy of our SDR is 20 parts per million (PPM). To improve the accuracy, we used a Temperature Compensated Crystal Oscillator (TCXO) with accuracy 0.5 PPM. Fig. 6 (top left) shows a TCXO connected to a HackRF One SDR.

3.3 Target and Testing

The efficacy of an asynchronous GPS spoofing attack was tested against GNSS receivers in high volume consumer devices with different chipsets and support for different constellations as shown in Table 2, and against a commercial drone (DJI Mavic 2 Pro). To record the received signals in the Android devices, we utilised the GPSTest Application (App) [3]. Fig. 4 shows various views of the GPSTest App. The left-most screenshot is of the status view. The status view gives a lot of information; the important ones for understanding our results are:

- Lat and Long, both in decimal degrees WGS 84, Alt (meters above the WGS 84 ellipsoid)

- Time To First Fix (TTFF), i.e., the time taken by the GNSS receiver to compute its position in seconds
- Speed in m/ s
- Number of satellites (#Sats) in the format xx/ yy/ zz: where xx shows the number of satellites used in the fix, yy represents the number of satellites in view with valid signal strength, and zz shows the number of satellites known to the device
- C/N0: Carrier to noise density ratio in dBHz.

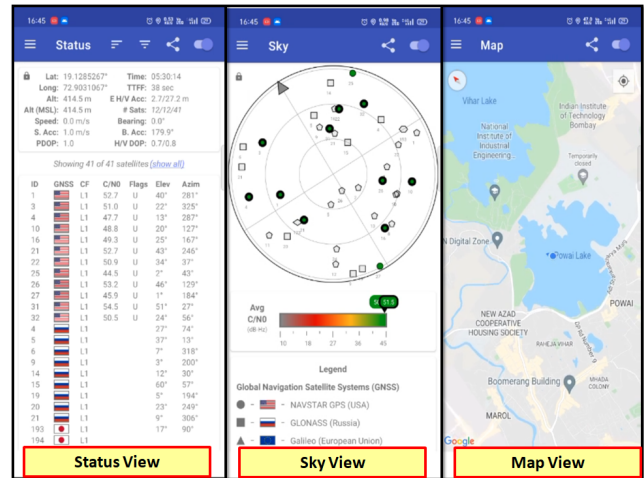


Figure 4. GPSTest App’s various views: status view (left), sky view (centre), and map view (right).

The centre screenshot is of the sky view and the rightmost screenshot is of the map view. In addition to the GPSTest App’s map, we also utilised Google Maps and Ola App’s map for visualising our original and spoofed locations on the Android devices. DJI Go 4 App is the requisite App required by a DJI mobile based controller to fly a DJI drone. We utilised this App to visualize the drone’s location, registered the drone’s home location, and controller location. Our testing was conducted in three phases.

- Phase I: Testing different scenarios onto a single Android mobile device.
- Phase II: Testing different scenarios onto all four Android mobile devices simultaneously.
- Phase III: Testing GPS spoofing attack on drone.

4 Experimental Scenarios and Setup

4.1 Experimental Scenarios

The efficacy of an asynchronous GPS spoofing attack against a GNSS receiver in an Android mobile phone was tested under the following conditions:

1. Receiver placed indoor/ outdoor in the absence/ presence of live sky signals, respectively.
2. Static/ dynamic spoofed signal is transmitted.

Table 2. Models of Android Mobiles, Chipsets and GNSS Capabilities

Sr. No. [@]	Build	Model	Chipset	GNSS Capability
S1	Realme 3	RMX1825	Mediatek Helio P70	G+L+A
S2	Oppo	F7	Mediatek MT6771(Helio P60)	G+L+A
S3	ASUS	Max Pro M1	Qualcomm SDM 636 Snapdragon	G+L+B+A
S4	POCO	M2	Mediatek MT6769V/CU Helio G80	G+L+B+A

G= GPS, L= GLONASS, B= BeiDou, A= Assisted GPS

[@]While assessing the results, we will be referring to different Android devices with their sr. nos., i.e., S1, S2, S3 and S4.

3. Receiver is static/ mobile.

The simulated GPS signals were designed to simulate static and dynamic locations in and around Indian Institute of Technology, Bombay (Mumbai), Maharashtra, India. The experiments were conducted in the outskirts of Madurai, Tamil Nadu, India. The physical crow fly distance between the two locations is nearly 1200 kms. Fig. 5 shows the geographical location of the original own location (left), spoofed own location (center), and the air travel duration between the two locations, which is more than 2 hrs and 30 mins (right).

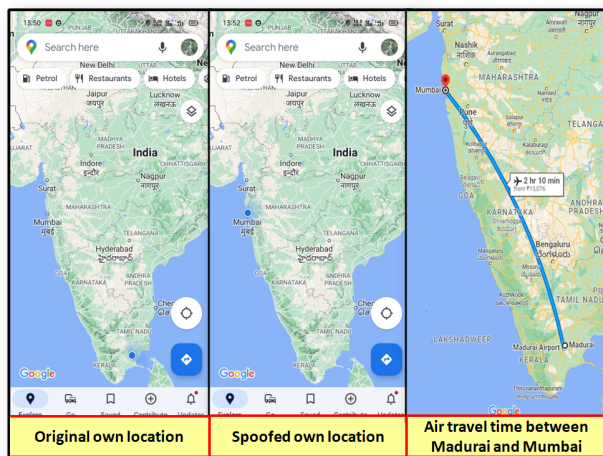


Figure 5. Screenshots of original own location (left), spoofed own location (center), air travel duration between the two (right).

4.2 Experimental Setup

The top (right) and bottom (right) images in Fig. 6 show the experimental setup for conducting the efficacy test against Android mobile phone based GNSS receivers and a commercial drone (DJI Mavic 2 Pro), respectively. As per the user manual, a DJI Mavic 2 Pro's GNSS receiver supports GPS and GLONASS. However, the frequencies and bands utilised by the drone are not shared. DJI drones use a DJI GO App, which can be run on an Android or iOS mobile phone and

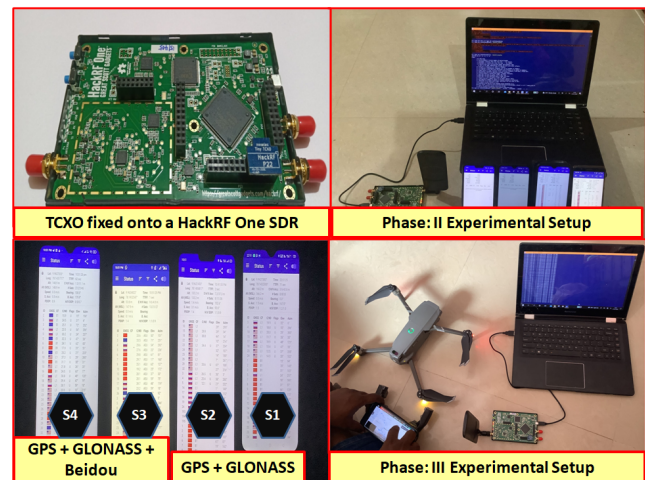


Figure 6. Top left: external TCXO connected on HackRF One SDR; Top right: indoor experimental setup; Bottom left: capabilities of different GNSS receivers; Bottom right: setup for spoofing test against drone.

used as a controller of the drone. We used both Android and iOS mobile phones as the controller and our results in the two cases were the same (see Section 5).

5 Experimental Results and Discussion

Initially, the spoofed signals transmitted by the SDR as planned in Fig. 2 were not received by the Android phone GNSS receiver. However, once an external TCXO with 0.5 PPM accuracy was fixed onto the HackRF One SDR as shown in Fig. 6 (top left), the spoofed signals were received by the GNSS receiver. Figs. 7-18 (explained in the following sections) are screenshots of the GPSTest App, Google Maps, OLA App, camera capture, DJI Go 4 map, and Apple map showing the results of spoofing taken during testing. Table 3 shows the results of various asynchronous GPS spoofing tests conducted over the embedded GNSS receiver of an Android mobile phone S1 (see Table 2).

5.1 Indoor and Outdoor (Static/ Dynamic) Spoofing Against an Android Mobile Phone based GNSS Receiver

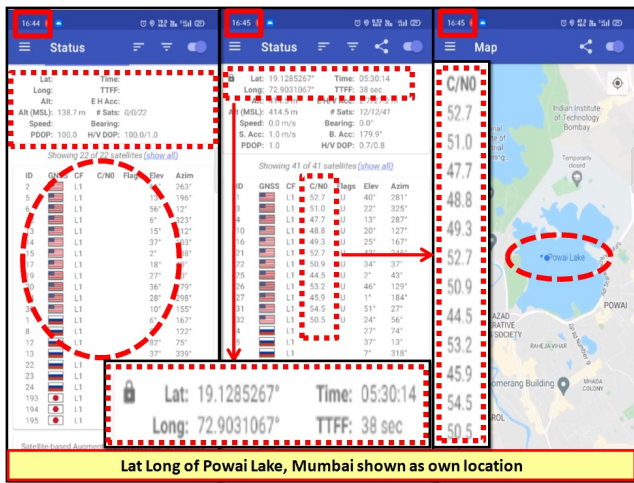


Figure 7. Indoor static spoofing: the leftmost screenshot is of GPSTest App with no original GNSS signal being received, center screenshot shows the reception of the spoofed signal and the GNSS receiver locking onto it, and the rightmost screenshot of Google Maps shows own location as in the middle of Powai lake, Mumbai.

Fig. 7 shows the screenshots (left to right) taken during the static GPS spoofing attack carried out against a GNSS receiver under indoor conditions. The GNSS receiver was not able to receive any signals from GPS or GLONASS constellation satellites, as highlighted in the leftmost screenshot. Once the spoofed signals were transmitted, the GNSS receiver started receiving them instantaneously and was able to compute its position within 30-40 s. The center screenshot highlights that it took the receiver 38 s as TTF. The received C/N0 is found to be ranging from 40 to 55 dBHz. Fig. 8 shows the effect of indoor dynamic spoofing on the GNSS receiver. As was seen in Fig. 7 itself, the receiver was not able to receive any genuine signals indoors. Fig. 8 shows screenshots from the beginning of the dynamic spoofing till the receiver computed its position (left to right). Even though the TTF is shown as 33 s, the own location blip in Google Maps took some time (3-10 s) to follow the dynamic movement. The rightmost screenshot of Fig. 8 highlights the receiver showing its speed as 25.8 m/s.

Fig. 9 shows sequential screenshots (left to right) of the Google Maps App running and showing its location to be shifting around the Gymkhana track of IIT Bombay (as designed in the spoofed signal generation process). The initial results of dynamic spoofing were not consistent, i.e., the movement of own location blip in Google Maps was not corresponding accurately to the designed route. To improve the same, the way-points, while designing the route in

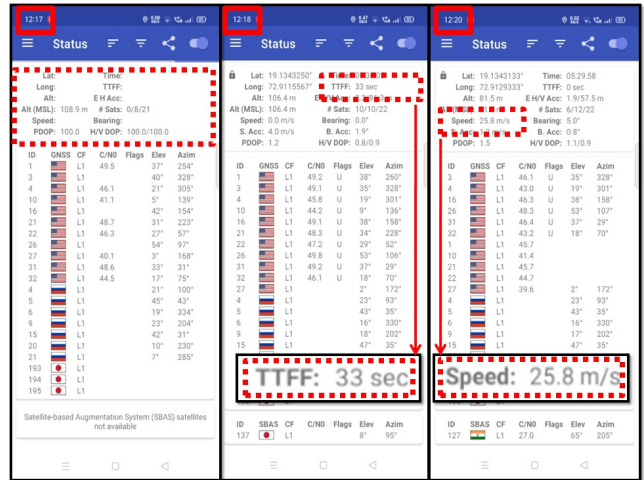


Figure 8. Indoor dynamic spoofing: screenshots of GPSTest App. The leftmost screenshot shows the beginning of spoofing. The middle screenshot shows the TTF and the rightmost screenshot shows speed.

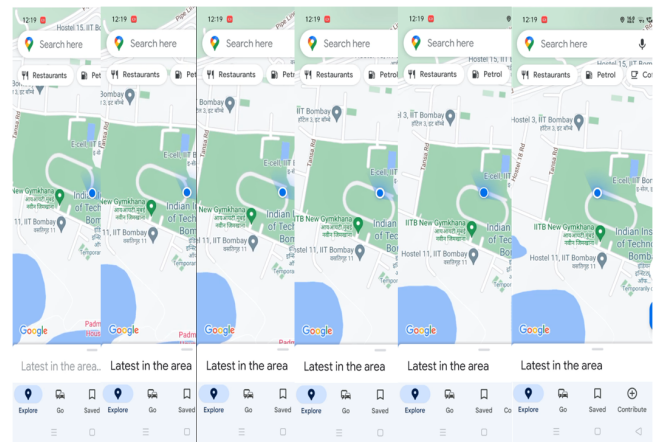


Figure 9. Indoor dynamic spoofing: screenshots of Google Maps App. Left to right are the screenshots showing the spoofed location as if moving around the Gymkhana ground track in IIT Bombay.

Google Earth, were selected at equal distances with several repetitions (see Fig. 10); this improved the spoofing results.

Under outdoor conditions, the receiver was receiving genuine live sky signals. The Tx of spoofed GPS signals led to the non-reception of genuine GNSS signals by the receiver, as the generated signal strength was much higher than the genuine GNSS signal strength. It was found that the time taken by the GNSS receiver to lock onto the received spoofed signals increased under outdoor conditions. Also, the time to lock onto the received spoofed signals further increased when dynamic spoofing was carried out, especially when the GNSS receiver had achieved lock onto genuine signals

Table 3. Results of Phase I Tests

Location of Receiver Receiver	Indoor		Outdoor	
	Static	Mobile*	Static	Mobile*
Static spoofed signal	S(30-40 s)	S(30-40 s)	S(30-50 s)	S(>60 s)
Dynamic spoofed signal	S(30-40 s)	S(>60 s)	S(>90 s)	S (>90 s)

S= spoofing was successful; (xx s) = time taken by the receiver to show spoofed location.

* Movement to the receiver was imparted by manual walking movement with a speed not more than 1 meter (m) per second (s). Also, the maximum distance of the receiver from the spoofer during the experiments was less than 50 m. All the tests were carried out with the cellular 4G network on.

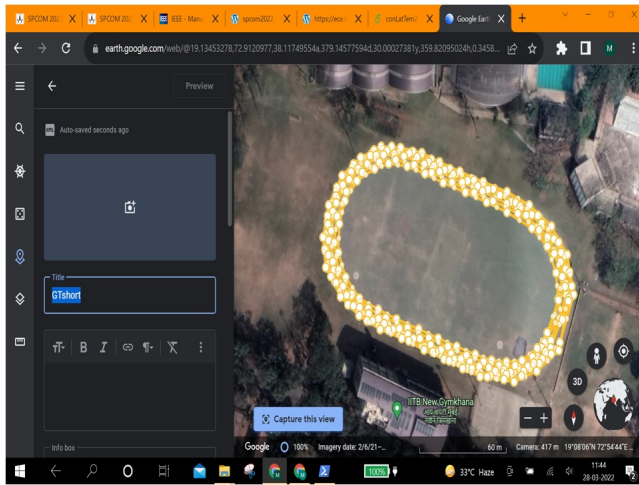


Figure 10. Designing route in Google Earth with numerous waypoints.

before the receipt of spoofed signals. Fig. 11 shows screenshots of Google Maps and OLA App before and after Tx of the spoofed signals under outdoor conditions. Figs. 12 and 13 show the results during dynamic spoofing attacks being tested with the movement of the GNSS receiver, i.e., the Android mobile device. The movement of the Android mobile phone was in a straight line without any change in height, starting from a distance and ending at the spoofing signal generation system. This movement was imparted by walking with the Android mobile phone in hand.

5.2 Results of Static and Dynamic Spoofing under Indoor and Outdoor Conditions on Different GNSS Receivers

Table 4 summarizes all the testing results. Fig. 14 and Fig. 15 show the results. The results show that in presence of live sky signals from three constellations, the receiver did not get spoofed by dynamic signals. Thus, receivers with more constellation support are less prone to get spoofed by dynamic signals (provided the genuine signals are not jammed). In addition, even a three-constellation-supported GNSS receiver can get spoofed if receiver is overwhelmed

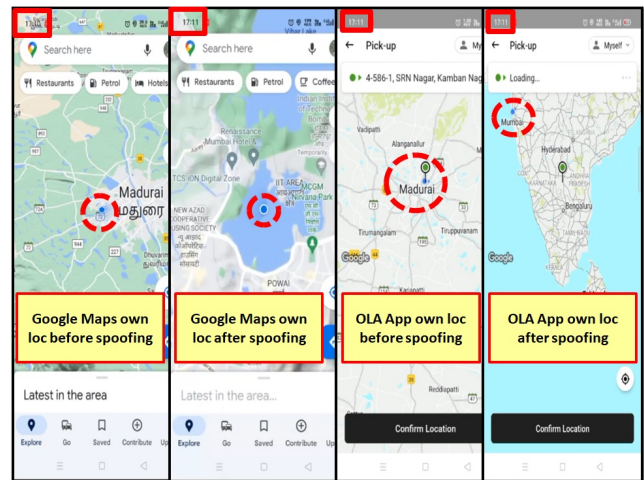


Figure 11. Outdoor static spoofing: the two screenshots on the left are of the Google Maps App before and after spoofing. The two screenshots on the right are of the OLA App map before and after spoofing.

by the spoofing signal, as in the case of static spoofing (S4 getting spoofed during static spoofing). The reason for exemplary resilience shown by S3 of not accepting the spoofed GPS signals, filtering it out and receiving only genuine signals is anti-spoofing measures being employed in it. This was researched and it was found that its chipset supports Observed Time Difference Of Arrival (OTDOA) [30], a Long Term Evolution (LTE) 4G based positioning technique [11]. From our results, it can be seen that S3 utilised its OTDOA positioning and timing to filter out spoofed signals.

5.3 Results of Indoor and Outdoor Spoofing Against a Commercial Drone (DJI Mavic 2 Pro)

When tested indoor (in absence of genuine signals), the drone controller accepted the spoofed signals and showed the spoofed location as its own location. Our results of indoor spoofing against the drone can be seen in Fig. 16. When tested outdoor (once the drone and its controller had locked onto genuine GNSS signals), the drone controller accepted the spoofed signals and showed the spoofed location as its

Table 4. Results of various tests on different GNSS receivers.

Location	Indoor				Outdoor			
	S1*	S2*	S3*	S4*	S1*	S2*	S3*	S4*
Static Spoofing	S	S	@	S	S	S	@	S
Dynamic Spoofing	S	S	@	S	S	S	@	@

* Sr. No. as given in Table 2, S= Successfully Spoofed, @= did not get spoofed

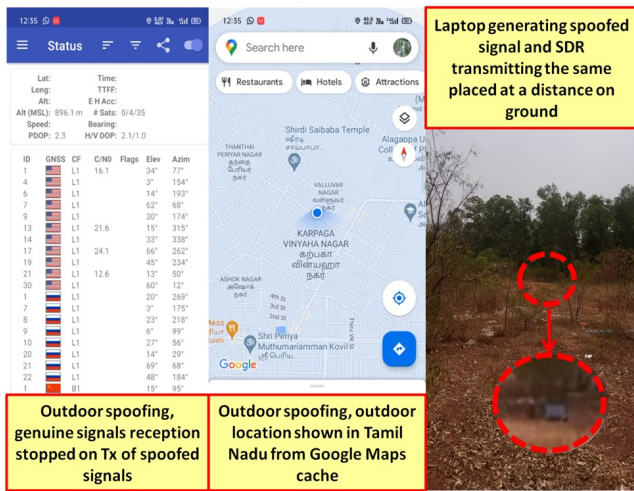


Figure 12. Left to right: screenshots of GPSTest App, Google Maps, and mobile phone camera during outdoor dynamic spoofing.

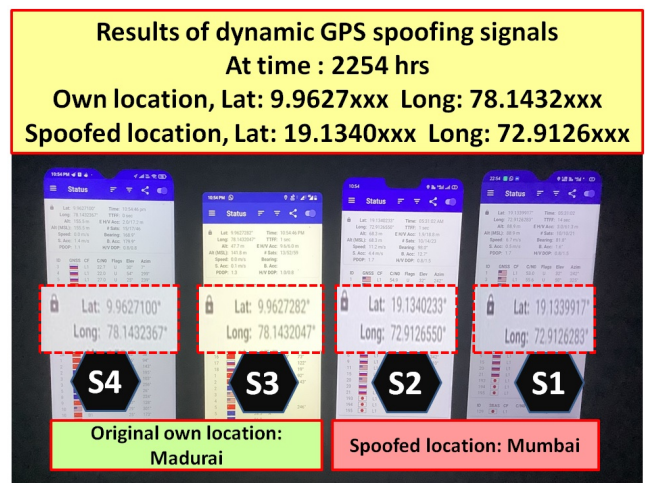


Figure 14. Results of dynamic GPS spoofing on different GNSS receivers.

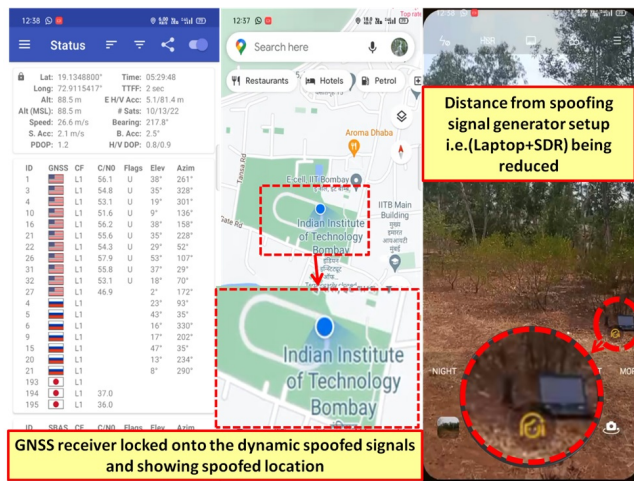


Figure 13. Left to right: screenshots of GPSTest App, Google Maps, and mobile phone camera after receipt of dynamic spoofing signals (outdoor).

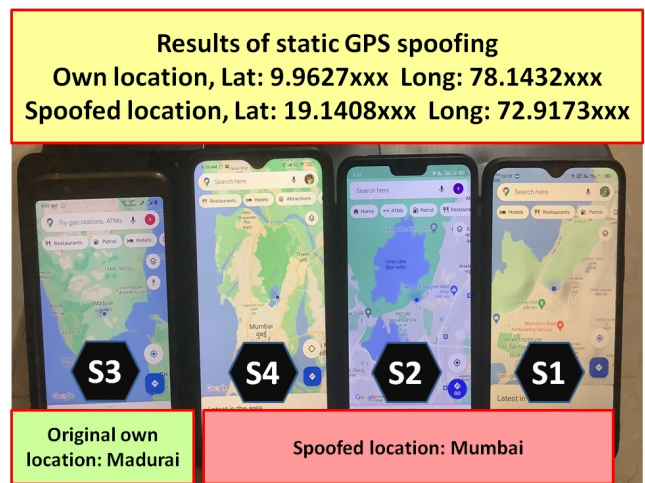


Figure 15. Results of static GPS spoofing on different GNSS receivers.

own location. However, the drone registered its original location as its home location (seen in the bottom half of Fig. 17 as H circled by green color). The drone with its alignment is seen in the screenshots as a red arrow head. Fig. 18

shows similar results received in an iOS based drone controller. From the results received during indoor and outdoor testing against the drone, it was found that the drone did not accept the spoofed signals. It can be assumed that the manufacturers have incorporated countermeasures against GPS spoofing in their latest firmware update. Since we did

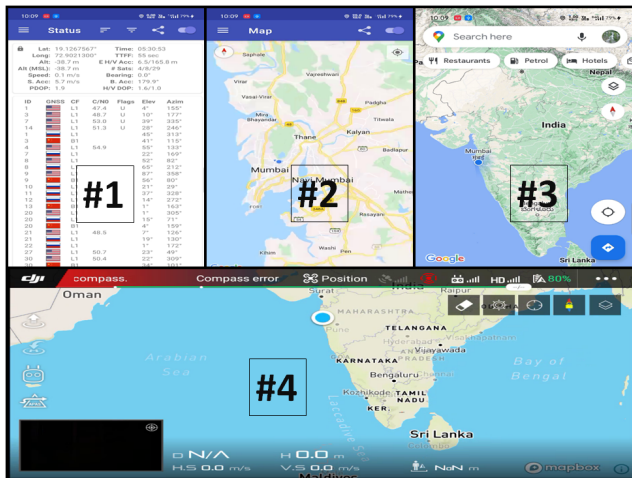


Figure 16. Screenshots taken on drone controller Android device during indoor spoofing: top left #1: GPSTest App showing receipt of spoofed signals, top center #2: GPSTest App map showing controller's location, top right #3: Google Maps App showing controller's location, bottom #4: DJI GO 4 App showing controller's location.

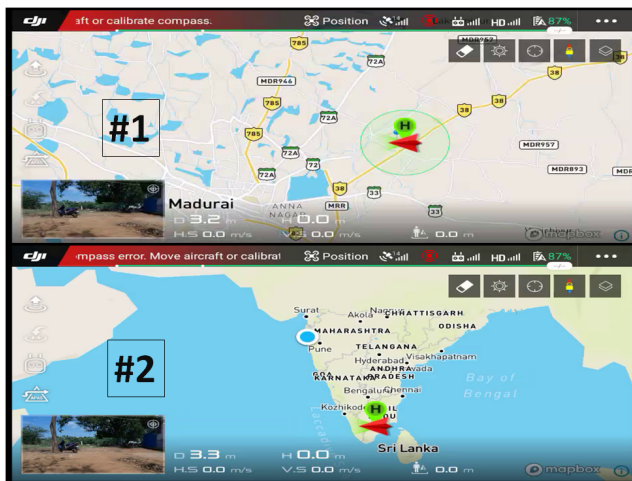


Figure 17. Screenshots taken on drone controller with DJI Go 4 App running. Top: drone own location; Bottom: controller's and drone's locations.

not have proprietary permission, we could not find which particular countermeasure has been implemented in this drone. Our results show that a vulnerability which these drones (DJI made) once had (shown in many research papers till late 2020) has been patched up.

6 Conclusions and Future Work

Our results show that an asynchronous GPS spoofing attack is effective even under live sky signals against GNSS receivers in Android mobile phones with single frequency

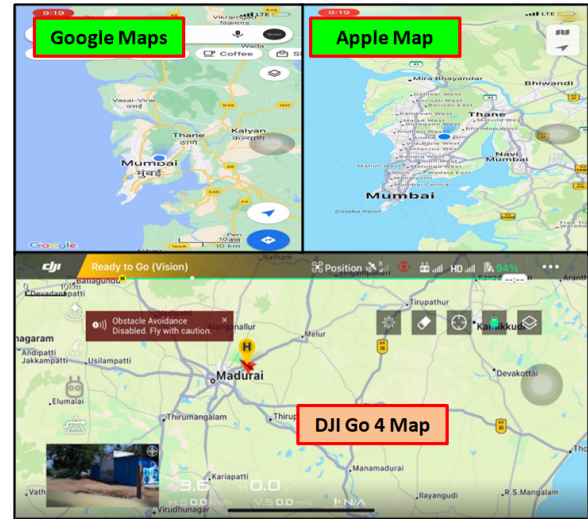


Figure 18. Screenshots taken on ios based drone controller with DJI Go 4 App running. Top left: Google Maps showing spoofed location; Top right: Apple map showing spoofed location; Bottom: DJI Go 4 map showing drone's location and registered home location.

support. A DJI made commercial drone is found to be secure from asynchronous GPS spoofing. The obvious countermeasure against such a GPS spoofing attack is a multi-frequency GPS receiver or GNSS receiver. Since commercial paid GNSS simulators are capable of generating multi-frequency multi-constellation signals, a multi-frequency and a multi-constellation GNSS receiver can also be spoofed. Utilising simple anti-spoofing measures like filtering out high power signals or signals with time errors more than a few milliseconds can be sufficient to protect these high volume consumer device GNSS receivers from asynchronous GPS spoofing. A direction for future research is to explore the efficacy of GNSS simulator based spoofing attacks and countermeasures. It will also be interesting to see how countermeasures such as OTDOA (which utilizes the network for positioning) and those implemented in commercial drones will fare against GNSS simulator based synchronous spoofing attacks.

Acknowledgments

The work was partially supported by SEED grant [RD/0516-IRCCSH0-026 (16IRCCSG009)].

References

- [1] Abdul Aabid, Bisma Parveen, Nagma Parveen, Sher Afghan Khan, and Md Abdul. 2022. Reviews on Design and Development of Unmanned Aerial Vehicle (Drone) for Different Applications. *J. Mech. Eng. Res. Dev* 45, 2 (2022), 53–69.
- [2] Sandra Pérez Arteaga, Luis Alberto Martínez Hernández, Gabriel Sánchez Pérez, Ana Lucila Sandoval Orozco, and Luis

- Javier García Villalba. 2019. Analysis of the GPS spoofing vulnerability in the drone 3DR solo. *IEEE Access* 7 (2019), 51782–51789.
- [3] Sean Barbeau and Mike Lockwood. 2021. *GPSTest android application*. <https://github.com/barbeau/gpstest>
- [4] Juan Blanch, Todd Walter, and Per Enge. 2012. Satellite Navigation for aviation in 2025. *Proc. IEEE* 100, Special Centennial Issue (2012), 1821–1830.
- [5] M.J. Boyle. 2020. *The Drone Age: How Drone Technology Will Change War and Peace*. Oxford University Press, Incorporated, UK. <https://books.google.co.in/books?id=6wbcDwAAQBAJ>
- [6] cddis.nasa.gov. 2022. Broadcast Ephemeris DataFile. [https://cddis.nasa.gov/Data/\\$_sand\\$_Derived\\$_\\$Products/GNSS/broadcast\\$_\\$sephemeris\\$_\\$data.html](https://cddis.nasa.gov/Data/$_sand$_Derived$_$Products/GNSS/broadcast$_$sephemeris$_$data.html)
- [7] Vishal Dey, Vikramkumar Pudi, Anupam Chattopadhyay, and Yuval Elovici. 2018. Security Vulnerabilities of Unmanned Aerial Vehicles and Countermeasures: An Experimental Study. In *2018 31st International Conference on VLSI Design and 2018 17th International Conference on Embedded Systems (VLSID)*. IEEE, Pune, India, 398–403. <https://doi.org/10.1109/VLSID.2018.97>
- [8] Takuji Ebinuma. 2018. *GPS-SDR-SIM*. <https://github.com/osqzss/gps-sdr-sim>
- [9] EUSPA. 2020. GNSS User Technology Report 2020. <https://www.euspa.europa.eu/european-space/euspace-market/gnss-market/gnss-user-technology-report>
- [10] EUSPA. 2022. EUSPA EO and GNSS Market report 2022. <https://www.euspa.europa.eu/2022-market-report>
- [11] Sven Fischer. 2014. Observed time difference of arrival (OTDOA) positioning in 3GPP LTE. *Qualcomm White Pap* 1, 1 (2014), 1–62.
- [12] Joshua Gordon, Victoria Kraj, Ji Hun Hwang, and Ashok Raja. 2019. A security assessment for consumer wifi drones. In *2019 IEEE International Conference on Industrial Internet (ICII)*. IEEE, IEEE, Orlando, FL, USA, 1–5.
- [13] Kim Hartmann and Christoph Steup. 2013. The vulnerability of UAVs to cyber attacks-An approach to the risk assessment. In *2013 5th international conference on cyber conflict (CYCON 2013)*. IEEE, IEEE, Tallinn, Estonia, 1–23.
- [14] ME Hathaway. 2014. MELISSA E. HATHAWAYa and JOHNN. STEWARTb aCouncil of Experts, Global Cyber Security Center (GCSEC). *Best Practices in Computer Network Defense: Incident Detection and Response* 35 (2014), 130.
- [15] Daojing He, Yinrong Qiao, Shiqing Chen, Xiao Du, Wenjie Chen, Sen-cun Zhu, and Mohsen Guizani. 2018. A friendly and low-cost technique for capturing non-cooperative civilian unmanned aerial vehicles. *IEEE Network* 33, 2 (2018), 146–151.
- [16] Eric Horton and Prakash Ranganathan. 2018. Development of a GPS spoofing apparatus to attack a DJI Matrice 100 Quadcopter. *The Journal of Global Positioning Systems* 16, 1 (2018), 1–11.
- [17] Ling Huang and Qing Yang. 2015. Low-cost GPS simulator GPS spoofing by SDR. In *Proc. DEFCON*. DEFCON23, Las Vegas, Nevada.
- [18] Todd E Humphreys, Brent M Ledvina, Mark L Psiaki, Brady W O'Hanlon, Paul M Kintner, et al. 2008. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. In *Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008)*. Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, 2314–2325.
- [19] Divya Joshi. 2019. Drone technology uses and applications for commercial, industrial and military drones in 2020 and the future. *Business Insider* Dec (2019).
- [20] A Karunakaran. 2022. Swarm Drones and Indian Academia. *Journal of Defence Studies* 16, 1 (2022), 73–81.
- [21] Shah Zahid Khan, Mujahid Mohsin, and Waseem Iqbal. 2021. On GPS spoofing of aerial platforms: a review of threats, challenges, methodologies, and future research directions. *PeerJ Computer Science* 7 (2021), e507.
- [22] CG Leela Krishna and Robin R Murphy. 2017. A review on cybersecurity vulnerabilities for unmanned aerial vehicles. In *2017 IEEE International Symposium on Safety, Security and Rescue Robotics (SSRR)*. IEEE, IEEE, Shanghai, China, 194–199.
- [23] Mamidala Jagadesh Kumar. 2021. The sky is not the limit: The new rules give wings to the Drone Technology in India. , 463–464 pages.
- [24] Labsat. 2021. *SatGen GNSS Signal Simulation Software*. <https://www.labsat.co.uk/index.php/en/products/satgen-simulator-software>
- [25] Marco Lisi. 2020. GNSS User Technology Report 2020. *GEOmedia* 24, 5 (2020).
- [26] Jules G McNeff. 2002. The global positioning system. *IEEE Transactions on Microwave theory and techniques* 50, 3 (2002), 645–652.
- [27] P. Misra and P. Enge. 2011. *Global Positioning System: Signals, Measurements, and Performance*. Ganga-Jamuna Press, Lincoln, MA. <https://books.google.co.in/books?id=5WJOyWAACAAJ>
- [28] Juhwan Noh, Yujin Kwon, Yunmok Son, Hocheol Shin, Dohyun Kim, Jaeyeong Choi, and Yongdae Kim. 2019. Tractor beam: Safe-hijacking of consumer drones with adaptive GPS spoofing. *ACM Transactions on Privacy and Security (TOPS)* 22, 2 (2019), 1–26.
- [29] Orolia. 2021. Skydel BroadSim GNSS Simulation Platform. <https://www.oralia.com/document/broad-sim-datasheet/>
- [30] Qualcomm.com. 2022. Snapdragon 636 specifications. <https://www.qualcomm.com/products/application/smartphones/snapdragon-6-series-mobile-platforms/snapdragon-636-mobile-platform-Overview>
- [31] Akmal Rustamov, Neil Gogoi, Alex Minetto, and Fabio Dovis. 2020. Assessment of the vulnerability to spoofing attacks of gnss receivers integrated in consumer devices. In *2020 international conference on localization and gnss (icl-gnss)*. IEEE, IEEE, Tampere, Finland, 1–6.
- [32] Jabang Aru Saputro, Esa Egistian Hartadi, and Mohamad Syahril. 2020. Implementation of GPS Attacks on DJI Phantom 3 Standard Drone as a Security Vulnerability Test. In *2020 1st International Conference on Information Technology, Advanced Mechanical and Electrical Engineering (ICITAMEE)*. IEEE, IEEE, Yogyakarta, Indonesia, 95–100.
- [33] Dinesh Sathyamoorthy, Z Fitry, Esa Selamat, S Hassan, Ahmad Firdaus, and Z Zaimy. 2020. Evaluation of the vulnerabilities of unmanned aerial vehicles (UAVs) to global positioning system (GPS) jamming and spoofing. *Defence S and T Technical Bulletin* 13 (2020), 333–343.
- [34] Daniel P Shepard, Jahshan A Bhatti, and Todd E Humphreys. 2012. Drone hack: Spoofing attack demonstration on a civilian unmanned aerial vehicle.(2012). *Google Scholar* (2012).
- [35] Nils Ole Tippenhauer, Christina Pöpper, Kasper Bonne Rasmussen, and Srđjan Capkun. 2011. On the requirements for successful GPS spoofing attacks. In *Proceedings of the 18th ACM conference on Computer and communications security*. Association for Computing Machinery, New York, NY, United States, 75–86.
- [36] Burak Tufekci and Cihan Tunc. 2021. Vulnerability and Threat Analysis of UAVs. In *2021 IEEE/ACS 18th International Conference on Computer Systems and Applications (AICCSA)*. IEEE, IEEE, Tangier, Morocco, 1–2.
- [37] Wikipedia contributors. 2022. GPS signals – Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=GPS_signals&oldid=1091064831 [Online; accessed 3-June-2022].
- [38] Jean-Paul Yaacoub, Hassan Noura, Ola Salman, and Ali Chehab. 2020. Security analysis of drones systems: Attacks, limitations, and recommendations. *Internet of Things* 11 (2020), 100218.
- [39] Xian-Chun Zheng and Hung-Min Sun. 2020. Hijacking unmanned aerial vehicle by exploiting civil GPS vulnerabilities using software-defined radio. *Sensors and Materials* 32, 8 (2020), 2729–2743.
- [40] Jasmine Zidan, Elijah I Adegoke, Erik Kampert, Stewart A Birrell, Col R Ford, and Matthew D Higgins. 2020. GNSS vulnerabilities and existing solutions: A review of the literature. *IEEE Access* 9 (2020), 153960–153976.