Galileo-SDR-SIM: An Open-Source Tool for Generating Galileo Satellite Signals

Harshad Sathaye, *ETH Zürich*
Maryam Motallebighomi, *Northeastern University*
Aanjhan Ranganathan, *Northeastern University*

BIOGRAPHY

Harshad Sathaye is a post-doctoral researcher at ETH Zürich[1] and is currently advised by Prof. Srdjan Capkun. His interests are wireless cyber-physical systems security, specifically sophisticated navigation systems, autonomous vehicle systems, and urban infrastructure.

Maryam Motallebighomi is a Ph.D. candidate at Northeastern University, Boston, MA, USA, conducting research in the security and privacy of wireless and mobile networks. She is advised by Prof. Aanjhan Ranganathan.

Aanjhan Ranganathan is an Assistant Professor at Northeastern University, Boston, MA, USA. His research revolves around the security and privacy of wireless networks with a strong focus on autonomous cyber-physical systems and smart ecosystems. Aanjhan is a recipient of several awards, including the prestigious NSF CAREER award, the outstanding dissertation award from ETH Zurich, the regional winner of European Space Agency's Satellite Navigation competition, and the Cyber Award from armasuisse (Switzerland's Department of Defense).

ABSTRACT

In today's world, satellite navigation systems, like GPS, are crucial for many essential tasks, such as guiding self-driving cars and managing power grids and transportation. These systems depend on signals continuously transmitted by satellites in orbit, providing accurate location and timing information. Galileo is one of these satellite systems that is becoming increasingly important. It has recently added security features to ensure the information it sends is genuine, resulting in a growing demand for Galileo (ESA (2023)). They must be tested thoroughly to ensure Galileo-dependent applications work well and are secure. One challenge is that researchers and developers need a way to create custom Galileo signals for their tests. Commercial signal generators are available but expensive and may not be accessible to many researchers. That's why there's a need for an open-source Galileo Signal Generator that is highly accessible.

This paper introduces "Galileo-SDR-SIM", a tool for generating and transmitting Galileo signals. It connects easily to software-defined radios, making it possible to send these signals in real-time. We've tested it extensively with various GNSS receivers, including software-defined receivers (GNSS-SDR [2]) and hardware receivers from well-known manufacturers like u-Blox [3] [4]. The results show that COTS receivers can obtain a 3D fix with a mean location offset of only 1.055 meters. Finally, we release our implementation as open source for further development[5].

I. INTRODUCTION

Today, satellite navigation is at the heart of various critical infrastructure industries, specifically modern automation systems. Several applications, like power grids, financial institutions, IoT, etc., leverage this highly accurate timing capability. It is rightfully a backbone for several crucial safety- and security-critical applications as stated in (Breeman et al. (2022)). For several years, GPS was the only satellite navigation system capable of providing positioning, navigation, and timing (PNT) information worldwide; expectedly, it has been the area of focus for localization and security research. Even though GPS is the most popular GNSS and is analogous to satellite navigation, newer systems like Galileo are gaining traction. Recent reports suggest Galileo can provide higher precision global positioning and timing services (Cowing (2023)). Moreover, an open-service navigation message authentication (OSNMA) service was recently launched in Galileo, making it the first authentication service accessible to civilians (ESA (2023)). Thus motivating the security evaluation of Galileo.

The primary requirement for performing a security evaluation of any GNSS-dependent application is an open design and flexible

[1] This work was done while at Northeastern University
[2] https://gnss-sdr.org/
[3] `https://www.youtube.com/watch?v=MX8MLP8040U&ab_channel=HarshadSathaye` Proof of concept video
[4] https://www.u-blox.com/en/
[5] `https://github.com/harshadms/galileo-sdr-sim`

https://doi.org/10.33012/2023.19254

satellite signal generator. One that supports constellations other than GPS and can fine-tune the generated signals. Researchers heavily rely on GPS-SDR-SIM, a software-defined GPS signal generator that produces raw IQ samples of GPS L1 C/A signal (Ebinuma (2015)). These samples can be transmitted using a software-defined radio or a file source for offline processing. Over the years, GPS-SDR-SIM has been a beneficial tool in GPS security and performance research and has played a vital role in building and evaluating spoofing and jamming resilient receivers (Wang et al. (2015); Ceccato et al. (2019); Sathaye et al. (2022)). However, it is only limited to GPS signals. Thus, an open-source tool capable of generating and transmitting signals from other systems like Galileo is needed. Currently, there are two main methods for studying Galileo signals: i) capturing real signals from satellites directly and ii) generating the signals using hardware signal generators. While capturing real signals is one approach, it may only sometimes be available or practical for particular research needs. Especially when one needs to examine messages from a specific satellite. For example, in the case of OSNMA, the signal may only be sporadically available. Additionally, hardware signal generators can be expensive and not always accessible to researchers.

To address this gap, in this work, we present Galileo-SDR-SIM,an open-source Galileo signal generator,. This tool allows users to generate Galileo E1B/C signal for any arbitrary location and time, including a dynamic trajectory, which can then be streamed using readily available commercial off-the-shelf RF frontends, e.g., HackRF [6], LimeSDR [7], and USRPs [8]. This makes it both accessible and highly flexible, enabling researchers to generate and analyze a wide range of Galileo signals for further application-specific testing.

The paper is structured as follows: In Section II, we provide an overview of Galileo and describe its diverse services. Following that, in Section III, we present the Galileo E1B/C signal design, encompassing both the physical and logical layers. In Section IV, we describe the architectural design of Galileo-SDR-SIM. Our experimental evaluation of Galileo-SDR-SIM is detailed in Section V. Next, we discuss potential applications and use cases for Galileo-SDR-SIM in Section VI. Finally, Section VII we conclude the paper and describe future improvement plans.

II. BACKGROUND

Conceived in 1999, Galileo is a global navigation satellite system that provides precise positioning, navigation, and timing services. It is a project of the European Union (EU) and the European Space Agency (ESA), with the primary aim of providing civilians with an accurate, independent, and reliable alternative to existing satellite navigation systems like GPS.

Similar to GPS, in the Galileo system, localization is performed based on the principles of multilateration, wherein the receiver calculates its distance from multiple satellites based on the signals' propagation time.

Galileo is unique in its utilization of multiple frequency bands for signal transmission. The L1 and E1 band, operating around 1575.42 MHz, is used for open and free access signals and is suitable for general positioning. The E5a and E5b bands, operating at 1176.45 MHz and 1207.14 MHz, respectively, provide greater accuracy and are resilient to signal distortion caused by the Earth's atmosphere. The E6 band, operating at 1278.75 MHz, is employed for commercial applications requiring precision and robustness. (ESA (2021a))

The navigation messages transmitted by Galileo satellites include satellite ephemeris and clock corrections. These messages enable a receiver to accurately calculate the respective satellite's position and signal propagation time. These values enable the receiver to calculate a "pseudorange". A receiver requires pseudorange measurements for at least four satellites to localize itself with respect to the orbiting satellites accurately.

Galileo is designed to offer different service levels. (Trautenberg et al. (2004)) These services include:

- Open Service (OS): This service is freely accessible to all users and provides positioning, navigation, and timing information with meter-level accuracy.
- Commercial Service (CS): Geared towards commercial users, this service offers better accuracy than the Open Service, making it suitable for applications that demand higher precision.
- Public Regulated Service (PRS): This service is restricted to authorized users, such as government and security agencies, providing encrypted and highly robust navigation signals for sensitive applications.
- Search and Rescue Service (SAR): Galileo satellites are equipped with transponders that can receive distress signals from emergency beacons, aiding search and rescue operations.

With its multi-frequency signals, commitment to interoperability, and emphasis on accuracy, Galileo provides users with reliable and precise positioning information. It has some specific technical features, like the use of multiple frequency bands, advanced

[6] https://greatscottgadgets.com/hackrf/
[7] https://limemicro.com/products/boards/
[8] https://www.ettus.com/products/

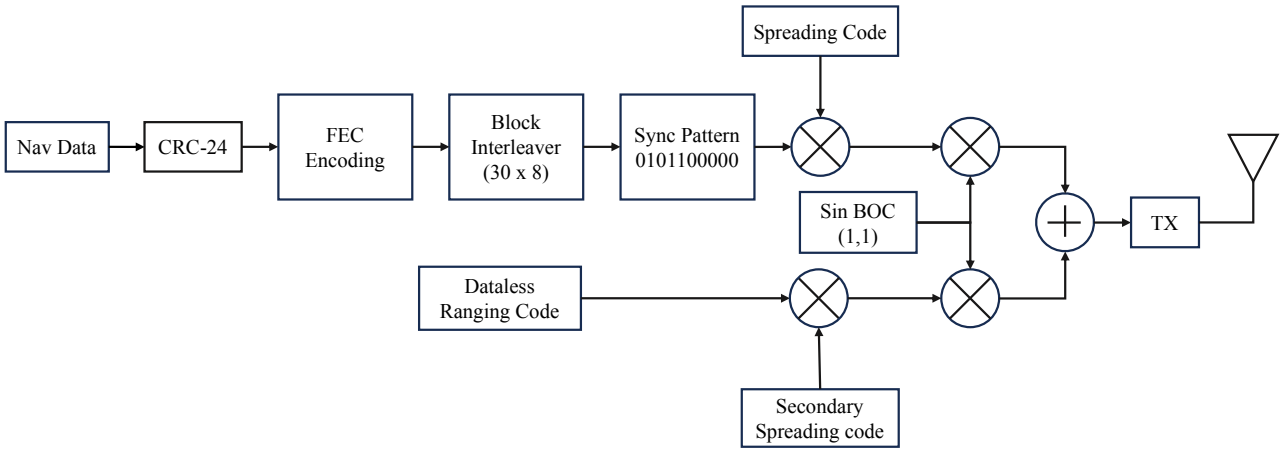


Figure 1: A simplified graphic representation of E1B/C signal generation. The transmitted signal includes a data signal and a dataless pilot signal comprised of a ranging code.

signal modulation, and specialized services.

Having a Galileo signal generator is of paramount importance for further development in the field of satellite navigation. It serves as a fundamental tool for testing and experimenting with Galileo signals, enabling scientists and engineers to analyze and refine navigation algorithms, assess system performance, and innovate new applications, ultimately advancing the capabilities and precision of global navigation technologies.

III. GALILEO E1B/C SIGNAL PLAN

In this section, we will describe the physical layer and the logical layer of Galileo open-service signals. Specifically, we will cover the following: i) Various carrier frequencies, ii) signal modulation schemes, iii) data and pilot signal structure, and iv) Galileo Data structures. Figure 1 depicts a simplified graphical representation of Galileo signal generation and transmission. Please note that a few more components of the Galileo signal are not expected in the schematic.

1. Frequencies

Galileo operates on several frequency bands to provide navigation and timing services. The Galileo system utilizes three main frequency bands: the E1, E5, and E6, each serving specific purposes within the GNSS infrastructure. (**?**ESA (2021b))

- E1 Band (Center Frequency: 1575.42 MHz): The E1 band is used for Galileo's Open Service (OS) signal, which is freely accessible to the public. It includes the E1A and E1B signals, both centered at 1575.42 MHz. E1A is intended for open service navigation, while E1B is reserved for safety-of-life services. The E1 band is compatible with the GPS L1 signal, making it suitable for multi-constellation receiver operation, improving accuracy and robustness.
- E5 Band (Center Frequencies: E5a - 1176.45 MHz, E5b - 1207.14 MHz): The E5 band is designated for the Safety of Life (SoL) service and other specialized services. It includes two signals, E5a and E5b, which operate at slightly different frequencies. E5a is intended explicitly for safety-critical applications like aviation and maritime navigation. E5b is designed to provide better performance in high-multipath environments. The E5 band is also compatible with GPS and Galileo dual-frequency receivers.
- E6 Band (Center Frequency: 1278.75 MHz): The E6 band is primarily used for the Galileo Search and Rescue (SAR) service, which assists in locating distress beacons and saving lives during emergencies. The E6 signal operates in collaboration with the international Cospas-Sarsat SAR system. Additional Frequencies:

In addition to the primary E1, E5, and E6 bands, Galileo also uses frequencies in the L-band, which includes the E2 and E3 bands. These bands are not as commonly used as E1, E5, and E6 but serve specific purposes. Using multiple frequency bands in the Galileo system enhances its performance, accuracy, and reliability. Multi-frequency receivers can use these signals to mitigate issues like signal interference, ionospheric effects, and multipath reflections. This results in more robust and precise positioning and timing capabilities for various applications, from aviation to transportation to agriculture.

2. Signal Modulation

Galileo's advanced signal modulation techniques contribute to its robustness against interference and jamming. It employs Binary Offset Carrier (BOC) modulation for its signals, which improves the system's resistance to multipath interference and enhances its performance in challenging environments. BOC modulation combines two carrier waves with slightly offset frequencies. These frequencies are carefully chosen to be compatible with the receiver's design and anticipated operating conditions.

In a traditional modulation scheme, like BPSK (Binary Phase-Shift Keying), a signal is transmitted by shifting the phase of a carrier wave by the data being sent. However, BPSK modulation is susceptible to multipath interference, where signals reflect off surfaces and arrive at the receiver at different times. BOC modulation, on the other hand, takes a more intricate approach. It combines two carrier waves, each modulated with the same data signal but slightly offset in frequency. This creates a signal with a more complex and distinct pattern. The benefit of BOC modulation lies in its ability to concentrate the energy of the transmitted signal into a narrower bandwidth, effectively reducing its vulnerability to multipath interference.

BOC modulation's ability to concentrate signal energy and its unique frequency offsetting provide several advantages, particularly in scenarios with challenging signal propagation conditions. When the transmitted signal encounters surfaces, such as buildings or natural obstacles, and produces reflected signals, BOC modulation helps the receiver to differentiate between the primary and reflected signals. Due to the distinct pattern of BOC-modulated signals, the receiver can more accurately identify the original signal, even in the presence of reflected signals. This improved identification enables the receiver to filter out the unwanted multipath components, resulting in more accurate and reliable positioning calculations.

3. Data and Pilot Signal Structure

The Galileo E1 signal comprises three distinct channels, namely E1A, E1B, and E1C. E1A is a restricted access signal with encrypted ranging codes and navigation data, primarily used for specific purposes. The data signal, E1B, contains the navigation data modulated by the ranging code, while E1C is the data-free signal, often referred to as the pilot signal. This pilot signal comprises only the ranging code and is not modulated by any navigation data stream.

The E1 signal features a spreading code with a length of 4092 and a chipping rate of 1.023 MHz. This combination results in a repetition rate of 4 ms, which plays a vital role in signal transmission and synchronization. Additionally, the pilot signal incorporates a secondary code of length 25 chips, extending the repetition interval to 100 ms.

One significant advantage of including the pilot signal in the Galileo E1 signal structure is its role in aiding signal acquisition and synchronization. This pilot signal helps receivers lock onto the Galileo signal more quickly and accurately. Moreover, the secondary code, which modulates 25 specific repetitions of the primary code, contributes to signal robustness and reliability. Overall, the well-structured E1 signal, comprising E1B and E1C components, supports various Galileo services and ensures users' accurate navigation and timing information.

Table 1: Galileo E1B/C specifications

	Frequency [MHz]	Signal	Type	Modulation	Chipping rate	Code Length	Length [ms]
E1	1575.42	B	Data	BOC(1,1)	1.023 Mcps	4092	4
		C	Pilot			4092*25	10

4. Galileo Data Organization

The Galileo system relies on the intricate framework of its navigation messages to ensure accurate positioning and precise timing. The system employs four types of navigation messages: the F/NAV, I/NAV, G/NAV (government usage), and C/NAV (commercial use) messages. (Hollreiser et al. (2003)) In this work, we will focus on I/NAV messages. These messages are systematically transmitted at predetermined intervals, ensuring the consistent and timely delivery of essential information vital for navigation. This section will describe the structure and organization of Galileo's messages.

I/NAV Frame Structure: The structural underpinning of Galileo's navigation messages centers on frames, sub-frames, and pages, as shown in Figure 2a. The page is the basic functional unit of Galileo navigation messages. Each page has a type marker that is used for informing the receiver regarding the content of that page. Apart from the type marker on a page, there are no markers to identify frames and sub-frames.

I/NAV message is primarily made up of frames of duration 720 s.(ESA (2011)) Each frame consists of 24 sub-frames, and each sub-frame is 30 s. Within these sub-frames, the navigation message architecture encompasses multiple pages, each designed to

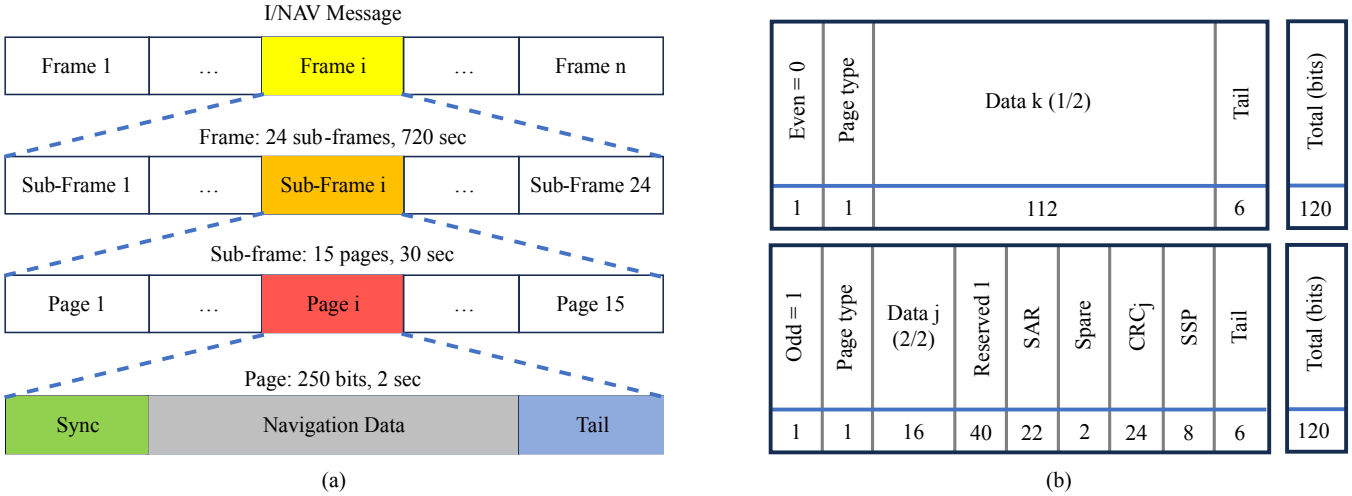


Figure 2: Sub-figure (a) shows the I/NAV message structure consisting of frames, sub-frames, and pages, along with their lengths and periods. **Sub-figure (b)** shows E1B page structure and bit allocation. Note that even and odd parts are transmitted sequentially and form a single I/NAV page.

convey specific categories of crucial information. This organization of page types caters to diverse data categories, including ephemeris parameters, clock corrections, ionospheric models, and satellite health status. The information in Galileo's navigation messages forms the bedrock of the GNSS system's accurate operation. This information encompasses vital components such as time parameters and clock corrections, ephemeris parameters, service parameters and satellite health data, ionospheric parameters model, and almanacs. The broadcasting satellite also includes timestamps at regular intervals to identify the absolute transmission time at the frame boundary. The receiver can then get fractional time by measuring time relative to the leading edge of the first chip of the first code sequence of the first page containing time-of-week information. (Fernández et al. (2016); ESA (2021a)) The obtained timing information and the parameters enable accurate positioning and time-keeping.

Galileo's navigation messages carry richer information due to more frequent broadcasts, allowing for more accurate positioning. This is particularly advantageous in urban canyons and challenging environments. The structure of Galileo's navigation messages, including transmission, frames, sub-frames, pages, and data content, is essential for making the GNSS system accurate and dependable. Moreover, the differences between Galileo and GPS navigation messages underscore the enhanced capabilities of Galileo, rendering it a formidable player in the realm of satellite navigation.

Message encoding The bitstream obtained from the application layer undergoes a specific message encoding sequence before direct-sequence spread spectrum operation and BOC modulation. The Galileo I/NAV (Inverse Navigation) message bitstream is divided into two parts, an even and odd part marked by one bit (even = 0 and odd = 1). Followed by an even/odd marker is the page type bit indicates whether the respective page is a nominal page or an alert page. In E1B I/NAV pages, most navigation data is included in the even part (Data k). The rest is included in the odd part, along with bits reserved for future use, search and rescue data (SAR), a 24-bit cyclic redundancy checksum (CRC), a secondary synchronization pattern (SSP), and a tail. Refer to Figure 2b for E1B I/NAV message bit allocation. Next, the page is forward error correction (FEC) encoded as specified in ESA (2021a) Each encoded page is interleaved using a block interleaver with dimensions (30 x 8) Figure 1 shows the message encoding process. Finally, each page is prefixed with a synchronization pattern, "0101100000" also known as the preamble that marks the beginning of a page.

Pages and word types There are two types of I/NAV pages in the Galileo E1B and E1C signals: Nominal and Alert. Nominal pages have a duration of 2 seconds and are transmitted sequentially in both E5b and E1 frequency bands. Each nominal page consists of two parts, each lasting 1 second, denoted as "even" and "odd." Alert pages, lasting 1 second, are transmitted at the same epoch over both frequency bands and are similarly divided into "even" and "odd" parts. This transmission is repeated at the next epoch, with the two parts switching between the frequency bands. The layout of the I/NAV pages remains consistent for both types.

The navigation messages contain all parameters required to compute a user's position, velocity, and time (PVT) solution. Each navigation message includes parameters like ephemeris, clock correction, health information, and almanac data. Ephemeris parameters provide critical orbital information, while clock correction ensures that satellite clocks are accurately synchronized with the system time, enabling the determination of when the navigation signal was transmitted. The Galileo Almanac, similar

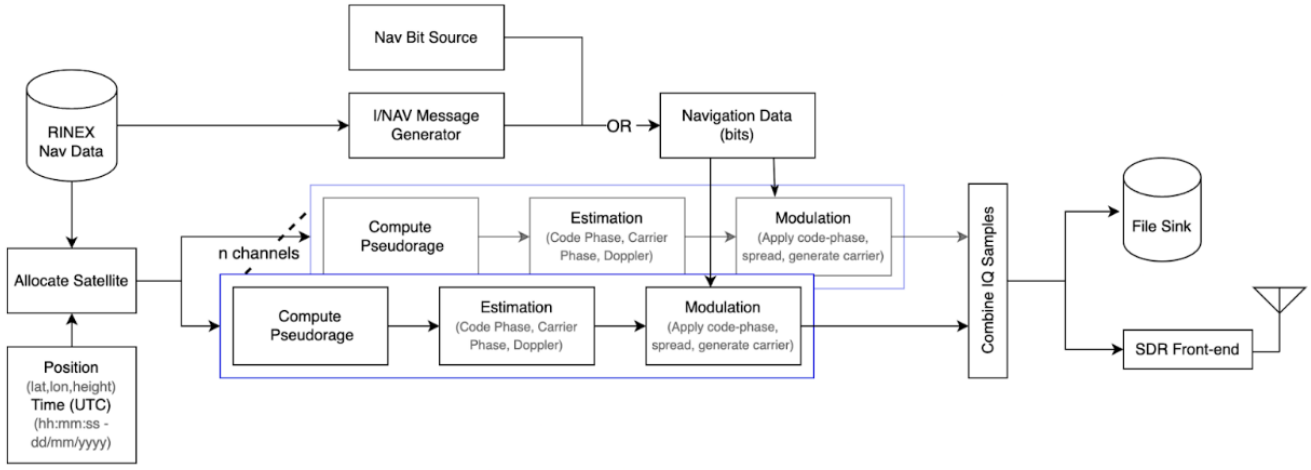


Figure 3: A schematic representation of our Galileo Signal Generator architecture showcasing different signal generation steps, various input blocks and signal storage/transmission capabilities.

to GPS and GLONASS, describes the orbital paths of the satellites, providing essential data for navigation. This structured information is necessary for precise satellite positioning and timing applications. For more details regarding page allotment and word types, please refer to ESA's Interface Control Document. ESA (2021a)

IV. DESIGN

The following factors allow us to pre-compute and synthesize custom Galileo signals:

- Open design and signal plan: Galileo is a public service. All the necessary signal-in-space details regarding data structures and modulation schemes are widely available and published by ESA (ESA (2021b)).
- Predictable orbits: Galileo satellites' ephemeris data is available through precise orbits in receiver-independent Exchange (RINEX) format. This data is vital in generating custom I/NAV messages.
- Known spreading codes: The signal-in-space interface control document provides all the spreading codes, including secondary ranging codes used in the modulation of Galileo signals.
- Common-reception-time: Finally, the essential aspect of satellite navigation is the computation of pseudoranges. Receivers use a common reception time technique that uses relative temporal offsets in satellite signals to compute pseudoranges (Pini et al. (2012)). This enables us to calculate temporal offsets or a specific location. Pseuodoranges and the rate of change of pseudorange also allow us to estimate the Doppler shift.

Our Galileo signal generator program supports four ways of baseband signal generation. These inputs include i) Navigation bits + symbol TOW in ms from an offline file source, ii) navigation bits + symbol TOW in ms from a real-time stream, iii) self-generated I/NAV messages (RINEX) (to be implemented), and iv) self-generated I/NAV messages (RTCM Stream from base stations) (to be implemented). These input options provide flexibility in signal generation, allowing researchers to choose the most appropriate input for their study. Once the navigation messages are obtained, our program modulates the baseband signal according to the Galileo E1b and E1c signal plan, including the pilot signal that aids tracking and synchronization. Figure 3 shows the schematic representation of our signal generator design. Position and time source allows real-time input to generate signals for arbitrary trajectories.

V. EVALUATION

The main evaluation metric for evaluating Galileo-SDR-SIM is the accuracy of the PVT solution calculated by the receiver. Furthermore, we also examined acquisition, tracking parameters, and signal features like Doppler shift, correlator output, and code phase offsets for inconsistencies. Finally, we also examine the correctness of decoded navigation messages by comparing transmitted and received satellite ephemeris elements.

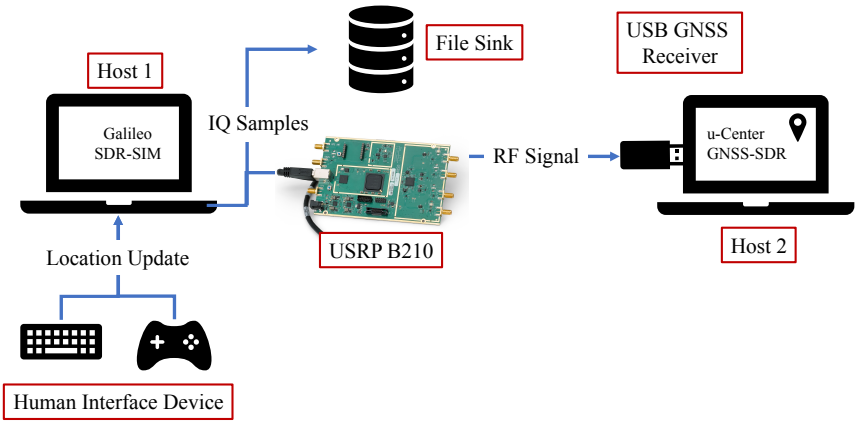
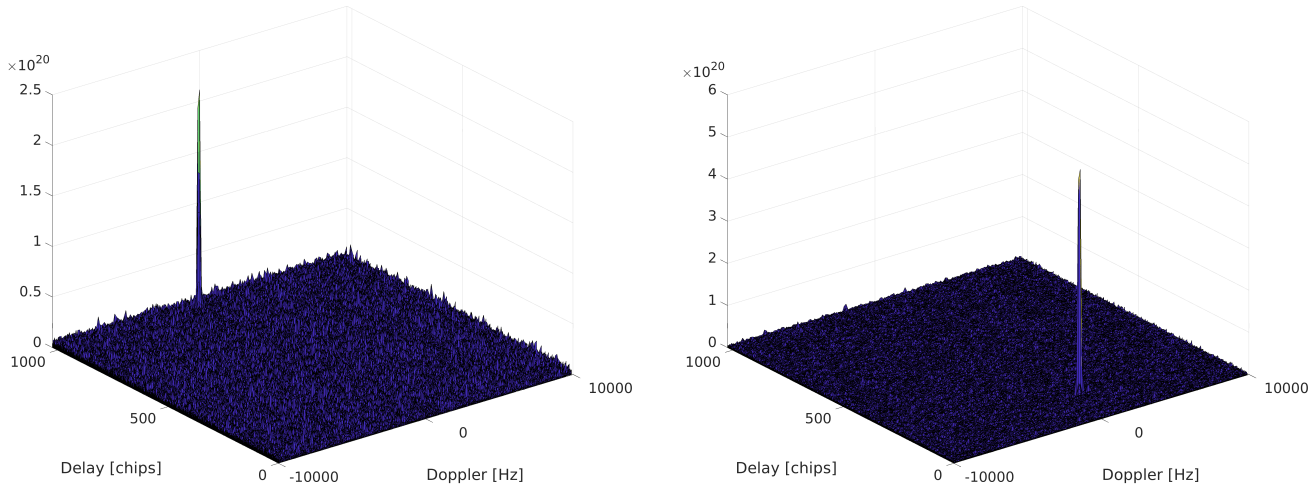


Figure 4: A schematic representation of our experimental evaluation setup. Host 1 is responsible for hosting and executing Galileo-SDR-SIM. It can interface with a USRP B210 over USB and has peripheral human interface devices that can be used to update locations at run time. Host 2 is the designated receiver and has the necessary software to interface with USB GNSS receivers like u-Blox M8N.



(a) Satellite 01

(b) Satellite 31

Figure 5: Acquisition plot for two satellites showing strong correlation peaks, enabling accurate tracking.

To evaluate the performance of our Galileo signal generator program, we used a combination of open-source software-defined receivers, like GNSS-SDR (Fernandez-Prades et al. (2011)), and hardware receivers like u-blox receivers (M8N, M9N, and F9) (uBlox (2022)). Next, to test real-time generation and transmission of signal, support for USRP software-defined radios is integrated into the signal generator. In our tests, we used a USRP B210 for signal generation. We hardwired the transmitter and receiver to comply with local RF transmission regulations to prevent signal leakage. Finally, we used a consumer-grade laptop with an 11th-generation Intel Core-i7 for generating signal samples. Refer to Figure 4 for a schematic of our experimental setup.

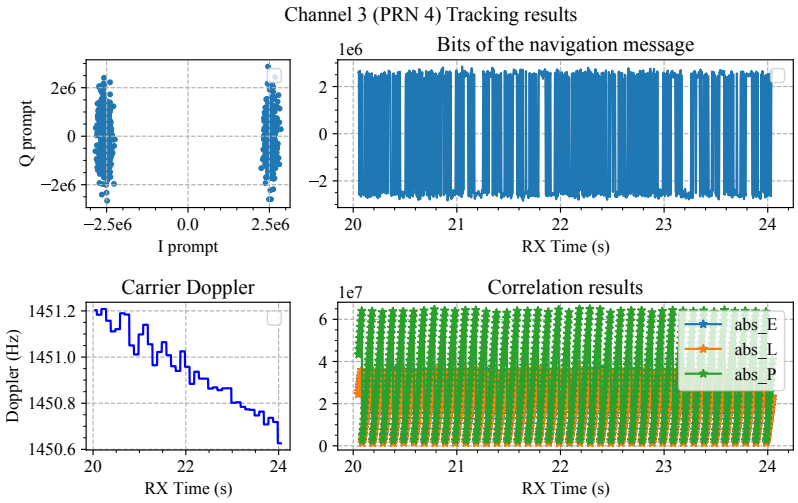


Figure 6: Plots showing a 4 s extract of different tracking variables obtained from GNSS-SDR. The total duration of this static location scenario is 10 m.

We considered the following scenarios to evaluate the performance of our signal generator: i) static location (offline and real-time transmission) and ii) dynamic trajectory (offline and real-time transmission). We generated multiple signal traces for geographically diverse locations to evaluate satellite visibility and correct functionality of the Galileo-SDR-SIM. Once the signals were generated, either offline or in real-time, we used the before-mentioned receivers to examine the accuracy of the calculated PVT solution. It is important to note that these are commercially available consumer-grade receivers widely used in commercial and research environments. Moreover, we use them with right-out-of-the-box factory configuration, i.e., without aftermarket optimizations and enhancements like differential corrections and multi-GNSS mode.

First, we examined the code phase, Doppler shift grid search and signal tracking parameters obtained from GNSS-SDR for inconsistencies. Specifically, we looked at the acquisition plot, carrier phase and frequency error, correlator values obtained from tracking loops, and the decoded navigation bits. Please refer to Figures 5 and 6 for the results.

Once the receiver gains a lock, we record the PVT solution over a span of ten minutes and calculate the position offset between the obtained location and the reference location used by Galileo-SDR-SIM to generate the respective signal. In our tests, the receivers obtained the location with a mean offset of 1.055 m, a standard deviation of 0.35, and a variance value of 0.1247. Next, we examine the dilution of precision (DoP) values and the number of visible satellites at the receiver. Similarly, the receiver successfully tracks real-time location updates introduced via a human interface device. Plots in Figure 7 show PVT solution values in a static and dynamic location scenario. Figures 8a and 8b show a position fix with GNSS-SDR and uBlox, respectively.

VI. DISCUSSION

In principle, all satellite navigation systems implement the same technique of determining pseudoranges using the common-reception-time method. These pseudoranges play a vital role in location calculation. It is generally assumed that one system's vulnerabilities will affect others, and to an extent, it is true. However, certain constellation-specific implementations require closer attention. For example, recently, an open-service navigation message authentication (OSNMA) scheme was introduced in Galileo. Today, it is a fully operational facility that provides NMA in minutes (Götzelmann et al. (2023)). This signal generator will help evaluate galileo-specific implementations, including OSNMA. Our initial analysis shows that our signal generator will play a vital role in enabling a signal relay attack that can defeat delayed key disclosure cryptographic mechanisms like TESLA, as demonstrated in (Motallebighomi et al. (2023)). Moreover, it will also play a significant role in evaluating countermeasures proposed by Seco-Granados et al. (2021); Motella et al. (2021); Shahid et al. (2023).

Several previous techniques (Rügamer et al. (2023); Garzia et al. (2014) have been proposed to fuse PVT solutions and observables from multiple constellations for a robust and more accurate location fix. Such multi-constellation receivers are extremely common and are available for less than $20. Moreover, secure receivers use multi-constellation and multi-band fusion to improve the security of obtained GNSS locations. Works like (Noh et al. (2019)) have shown that simply spoofing GPS alone is insufficient to launch a successful attack. Thus, to better understand the threat landscape, it is essential to evaluate the security of non-GPS navigation systems, especially Galileo, given the introduction of the only operational security feature and

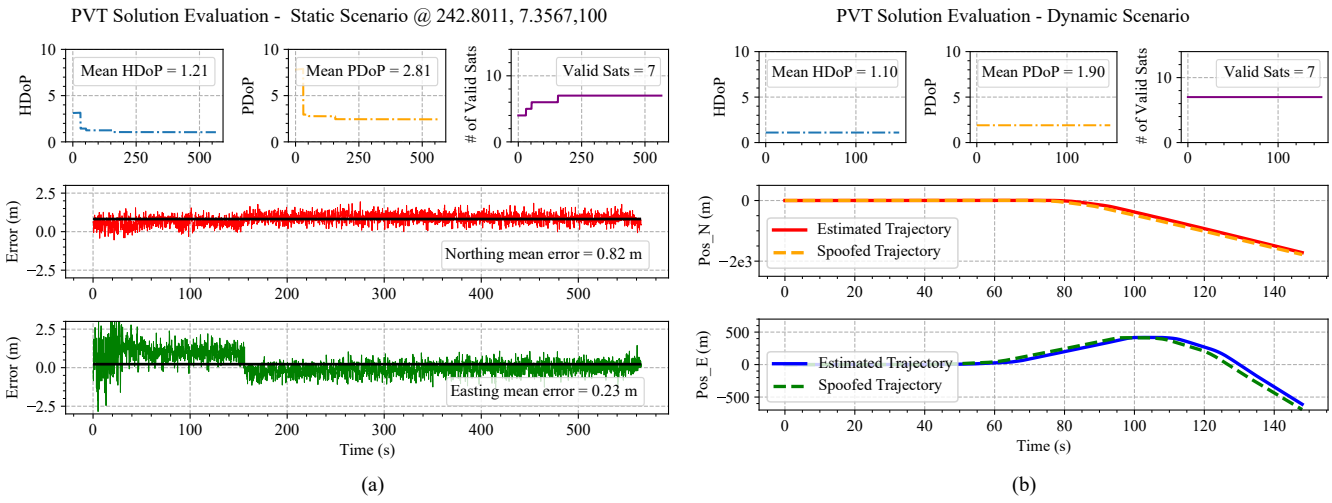


Figure 7: Results from a static scenario (plot a) and a dynamic scenario (plot b). In plot a, the position error is calculated by calculating the difference in UTM position components (Easting and Northing). The dynamic scenario is compared by plotting the difference in UTM position from a common starting point of the trajectory.

its growing popularity.

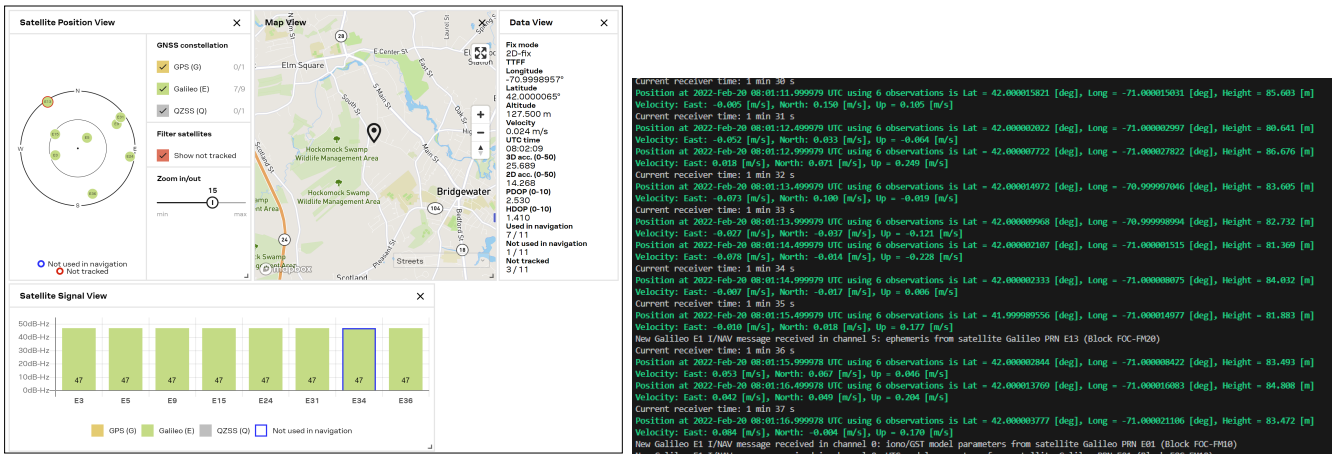


Figure 8: Successful 3D fix obtained by receivers. Figure (a) is a screenshot of the u-Center software connected to a uBlox M8N, and figure (b) is the output of GNSS-SDR. In Both scenarios, Galileo-SDR-SIM is programmed to generate a signal for the location latitude: 42, longitude: 71, and height: 100 m

Future Improvements: The forthcoming enhancements encompass several vital facets of the project. First and foremost, I/NAV message generation development is underway, with an initial proof of concept work already present in the GitHub repository. Next, we want to include real-time and time-synchronized signal generation by leveraging RTCM navigation data streams from continuously operating GNSS reference stations (CORS). These reference stations stream live navigation data and observables from around the world. These streams will help us synchronize with live Galileo signals. Finally, we want to further evaluate our implementation by testing it with receivers that fuse measurements from satellite augmentation systems. The endeavor also entails achieving precise time and frequency synchronization by harnessing live Galileo signals through

the GNSS-SDR monitor. To improve usability and access, we want to facilitate the accommodation of multiple software-defined radios (SDRs), including SDRs like HackRF, LimeSDR, and PlutoSDR, thereby enhancing versatility. Additionally, an ambitious goal is to incorporate GPS L1 C/A (Coarse/Acquisition) functionality into the system, broadening the scope of its capabilities. Moreover, a paramount consideration involves the adoption of fixed-point arithmetic to mitigate the impact of rounding errors, thus bolstering the precision and robustness of the system.

VII. CONCLUSION

In conclusion, our paper introduces Galileo-SDR-SIM, a powerful open-source Galileo signal generator. We have discussed the critical importance of such a tool in enabling flexible Galileo signal generation for various scenarios and applications. This paper includes a detailed breakdown of the Galileo E1B/C signal design and an extensive explanation of the Galileo-SDR-SIM architecture. Through rigorous experimental evaluation, we have demonstrated the tool's performance and versatility. Importantly, we have open-sourced this resource, making it accessible to the research community and furthering the development and study of Galileo and GNSS-dependent applications.

ACKNOWLEDGEMENTS

The work was partially supported by NSF grant 2144914.

REFERENCES

Breeman, M., Grillo, F., and Van de Kaa, G. (2022). Battles in space: De-facto standardization of global navigation satellite systems. *Journal of Engineering and Technology Management*, 65:101693.

Ceccato, S. et al. (2019). Security in global navigation satellite systems: authentication, integrity protection and access control.

Cowing, K. (2023). New Galileo Service Set To Deliver 20 cm Accuracy. https://spaceref.com/newspace-and-tech/new-galileo-service-set-to-deliver-20-cm-accuracy/.

Ebinuma, T. (2015). Software-Defined GPS Signal Simulator. https://github.com/osqzss/gps-sdr-sim.

ESA (2011). Galileo Navigation Message. https://gssc.esa.int/navipedia/index.php/Galileo_Navigation_Message.

ESA (2021a). European gnss (galileo) open service signal-in-space interface control document. *European Commission*. https://www.gsc-europa.eu/sites/default/files/sites/all/files/Galileo_OS_SIS_ICD_v2.0.pdf.

ESA (2021b). galileognss. https://galileognss.eu/.

ESA (2023). Galileo Open Service Navigation Message Authentication (OSNMA). https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma/.

Fernández, I., Rijmen, V., Ashur, T., Walker, P., Seco, G., Simón, J., Sarto, C., Burkey, D., and Pozzobon, O. (2016). Galileo navigation message authentication specification for signal-in-space testing–v1. 0. *European Commission*, 11.

Fernandez-Prades, C., Arribas, J., Closas, P., Aviles, C., and Esteve, L. (2011). Gnss-sdr: An open source tool for researchers and developers. In *Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011)*, pages 780–794.

Garzia, F., Köhler, S., Urquijo, S., Neumaier, P., Driesen, J., Haas, S., Leineweber, T., Zhang, T., Krause, S., Henkel, F., et al. (2014). Napa: A fully integrated multi-constellation two-frequency single-chip gnss receiver. In *2014 IEEE/ION Position, Location and Navigation Symposium-PLANS 2014*, pages 1075–1083. IEEE.

Götzelmann, M., Köller, E., Viciano-Semper, I., Oskam, D., Gkougkas, E., and Simon, J. (2023). Galileo open service navigation message authentication: Preparation phase and drivers for future service provision. *NAVIGATION: Journal of the Institute of Navigation*, 70(3).

Hollreiser, M., Erhard, P., Lorenzi, P., and Dixon, C. S. (2003). Galileo user segment overview. In *Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003)*, pages 1914–1928.

Motallebighomi, M., Sathaye, H., Singh, M., and Ranganathan, A. (2023). Location-independent gnss relay attacks: A lazy attacker's guide to bypassing navigation message authentication. *ACM WiSec 2023*.

Motella, B., Nicola, M., and Damy, S. (2021). Enhanced gnss authentication based on the joint chimera/osnma scheme. *IEEE Access*, 9:121570–121582.

Noh, J., Kwon, Y., Son, Y., Shin, H., Kim, D., Choi, J., and Kim, Y. (2019). Tractor beam: Safe-hijacking of consumer drones with adaptive gps spoofing. *ACM Transactions on Privacy and Security (TOPS)*, 22(2):1–26.

Pini, M., Falco, G., and Presti, L. L. (2012). Estimation of satellite-user ranges through gnss code phase measurements. *Global Navigation Satellite Systems: Signal, Theory and Applications*, pages 107–126.

Rügamer, A., Melgård, T. E., De Wilde, W., Gerstung, H., Wegmann, I., and Schellekens, D. (2023). Validation of a combined gnss correction and nma l-band service against spoofing. In *2023 IEEE/ION Position, Location and Navigation Symposium (PLANS)*, pages 570–579. IEEE.

Sathaye, H., Strohmeier, M., Lenders, V., and Ranganathan, A. (2022). An experimental study of {GPS} spoofing and takeover attacks on {UAVs}. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 3503–3520.

Seco-Granados, G., Gómez-Casco, D., López-Salcedo, J. A., and Fernández-Hernández, I. (2021). Detection of replay attacks to gnss based on partial correlations and authentication data unpredictability. *Gps Solutions*, 25(2):33.

Shahid, H., Canzian, L., Sarto, C., Pozzobon, O., Reyes-Gonzalez, J., Seco-Granados, G., and López-Salcedo, J. A. (2023). Statistical characterization of snapshot osnma spoofing detection. In *2023 International Conference on Localization and GNSS (ICL-GNSS)*, pages 1–6. IEEE.

Trautenberg, H. L., Weber, T., and Schäfer, C. (2004). Galileo system overview. *Acta Astronautica*, 55(3-9):643–647.

uBlox (2022). M8N. `https://content.u-blox.com/sites/default/files/products/documents/u-blox8-M8_ReceiverDescrProtSpec_UBX-13003221.pdf`.

Wang, K., Chen, S., and Pan, A. (2015). Time and position spoofing with open source projects. *black hat Europe*, 148:1–8.