Journal of Engineering Technology and Applied Physics

Evaluation of The Effect of Spoofing on Dual-Frequency Global Navigation Satellite System (GNSS)

Dinesh Sathyamoorthy*, Ahmad Firdaus Ahmad Kazmar, Amirah Sakinah Mohd Rozlan, Mohammad Ghazdly Adril Ghazali and Noor Hazimah Syamila Mat Najib
Science & Technology Research Institute for Defence (STRIDE), Ministry of Defence, Malaysia.
**Corresponding author:* dinesh.sathyamoorthy@stride.gov.my, *ORCiD:* 0000-0001-5549-0420
https://doi.org/10.33093/jetap.2024.6.1.13
Manuscript Received: 19 November 2023, Accepted: 12 December 2023, Published: 15 March 2024

***Abstract* — This paper aims to assess the impact of Global Navigation Satellite System (GNSS) spoofing on the performance of a Garmin GPSMAP 66sr dual-frequency GNSS receiver. The evaluation is conducted through field assessments under three conditions: 1) single-frequency GPS L1 coarse acquisition (C/A) only, 2) single-frequency GPS L1 C/A and Galileo E1 open service (OS), and 3) dual-frequency GPS L1 C/A and L5, as well as Galileo E1 OS and E5a. The results emphasise the critical role of multifrequency GNSS in mitigating spoofing. In the dual-frequency multi-GNSS mode, spoofing does not occur as the GPS L5 and Galileo E5a signals remain unaffected by spoofing signals in the L1 / E1 band. In the single-frequency multi-GNSS mode, the higher number of observed GNSS satellites contributes to higher minimum spoofing power levels and longer durations between position fix loss and spoofing as compared to the GPS only mode.**

Keywords* - *Dual-frequency Global Navigation Satellite System (GNSS), Spoofing, Field evaluations, Probable error, GNSS satellite geometry

I. INTRODUCTION

Global Navigation Satellite System (GNSS) encompasses constellations of satellites that emit signals from space, delivering positioning and timing information to GNSS receivers. This system comprises the major global constellations, namely the Global Positioning System (GPS), Galileo, BeiDou and GLONASS, alongside regional systems including Quasi-Zenith Satellite System (QZSS) and Navigation Indian Constellation (NAVIC). Leveraging on multiple constellations or multi-GNSS offers enhanced accuracy, redundancy and availability. In situations where the line of sight to satellites is obstructed, the utilisation of multiple constellations ensures continuous service provision. These GNSS systems also utilise various frequency bands, enabling GNSS receivers to track multiple signals from each satellite across different frequencies. This capability facilitates improved positioning accuracy, especially in challenging environments [1-3].

This study aims to assess the impact of spoofing on the performance of a Garmin GPSMAP 66sr dual-frequency GNSS receiver. Spoofing involves the generation and transmission of false navigation messages with the intention of manipulating the navigation solutions provided by GNSS receivers. Spoofing signals are typically generated using commercially available GNSS simulators. In order to successfully execute a spoofing attack, the received power of the counterfeit signal must surpass that of the authentic signal. Subsequently, the receiver processes the manipulated signal as input, calculating the location induced by the spoofer. Spoofing poses a more formidable threat than intentional jamming, as the targeted receiver may be unable to detect a spoofing attack. Consequently, users are not alerted to the untrustworthiness of the navigation solution. While achieving successful spoofing is more intricate than jamming, even unsuccessful attempts can result in significant errors and jamming of GNSS signals over extensive areas [4-7]. Hanlon *et al.* [8], Montgomery *et al.* [9] and van der Merwe *et al.* [10] classified GNSS spoofers into three categories, namely simplistic, intermediate and sophisticated, based on their complexity and level of robustness required for associated counter-spoofing measures. Initially perceived as an emerging risk, recent incidents have elevated GNSS spoofing to a recognised and substantial threat [7, 11-14].

The evaluated receiver has the capability to observe signals from GPS, GLONASS, Galileo and QZSS, with the added feature of performing dual-

Published by MMU PRESS. URL: https://journals.mmupress.com/index.php/jetap/index

frequency observations for GPS, Galileo and QZSS [15]. This study focuses on the functionalities of the evaluated GNSS receiver in relation to the GPS L1 coarse acquisition (C/A) and L5 signals, as well as the Galileo E1 open service (OS) and E5a signals. For the GPS L1 C/A and Galileo E1 OS signals, they have fundamental frequency of 1,575.42 MHz, and their code structures modulate the signals over bandwidths of 2 and 4 MHz respectively. On the other hand, the GPS L5 and Galileo E5a signals share fundamental frequency of 1,176.45 MHz, with code structures that modulate the signals over a broader bandwidth of 20 MHz [2, 16-18].

This study is conducted via field evaluations for three conditions: 1) single frequency GPS L1 C/A only, 2) single frequency GPS L1 C/A and Galileo E1 OS, and 3) dual-frequency GPS L1 C/A and L5 as well as Galileo E1 OS and E5a. In previous studies, field evaluations were employed to study the effects of spoofing on GPS L1 C/A performance [19, 20].

II. METHODOLOGY

The performance of the evaluated GNSS receiver is analysed under simplistic GNSS spoofing attacks using a standalone GNSS simulator, which is currently identified as the most immediate threat. In this form of spoofing attack, the spoofing signal lacks synchronisation concerning power level, phase, Doppler shift and data content with authentic GNSS signals received by the target GNSS receiver. This discrepancy could lead to temporary loss of position fix lock in the GNSS receiver, potentially preceding its takeover by the spoofing signal. Even if the unsynchronised attack manages to avoid causing loss of lock, it could still result in abrupt change in the GNSS receiver's time estimate. Basic counter-spoofing measures, such as amplitude and time-of-arrival discrimination along with loss of lock notification, could be employed to identify these simplistic spoofing attacks. However, it is noteworthy that many present civilian GNSS receivers lack these protective measures, leaving them vulnerable to such straightforward spoofing attacks [5-7].

The tests in this research were carried out at the Science & Technology Research Institute for Defence's (STRIDE) Block B car park, as shown in Fig. 1. The test setup utilised to investigate the effect of spoofing on the performance of the evaluated GNSS receiver is depicted in Fig. 2. The spoofing signal, generated by an Aeroflex GPSG-1000 GNSS simulator [21], is transmitted through a GPS Source A11XLV GPS amplifier [22] and a GPS Source L1P GPS passive antenna [23]. In order to ensure the absence of external interference signals during the tests, an Advantest U3751 spectrum analyser [24] is employed.

The spoofing signal is configured to originate from the position of N 2º 58' E 101º 48', which is approximately 1 km from the test area. The timing of the signal is synchronised with the simulator's GNSS receiver time. Once the evaluated GNSS receiver acquires a position fix, the transmission of the spoofing signal commences at power level of -140 dBm. The power level is then systematically increased in 3 dBm increments at 1 min intervals. Concurrently, the corresponding values of horizontal probable error (HPE), vertical probable error (VPE) and estimated probable error (EPE) are logged using GPS Diagnostics [25]. The test scenarios employed are outlined in Table I.

Fig. 1. Test area located at N 2º 58.056' E 101º 48.586' (*Source:* Screen capture from Google Earth).

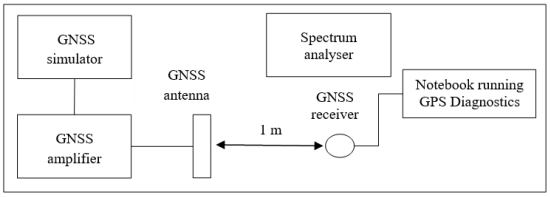

Fig. 2. Test setup employed for evaluation of the effect of spoofing.

Table I: Test scenarios employed for the evaluation of the effect spoofing.

Scenario	Mode	Spoofing Signal
1	Single Frequency GPS only	GPS L1 C/A
2	Single Frequency Multi-GNSS	GPS L1 C/A
3		Galileo E1 OS
4		GPS L1 C/A and Galileo E1 OS*
5	Dual-Frequency Multi-GNSS	GPS L1 C/A
6		Galileo E1 OS
7		GPS L1 C/A and Galileo E1 OS*

*Six satellites for GPS and six satellites for Galileo.

III. RESULTS AND DISCUSSION

The findings of the study are presented in Table II, showing varying minimum spoofing signal power levels, as well as times between position fix loss and spoofing for the recorded readings. The minimum power level of the spoofing signal needed to induce position fix loss and subsequent spoofing is contingent upon GNSS signal coverage during the tests. Notably, during periods of suboptimal coverage when the received GNSS signal power levels are lower, the requisite minimum spoofing signal power levels are correspondingly lower and vice versa.

Table II. The effect of spoofing attacks on the evaluated GNSS receiver.

Scenario	Mode	Spoofing Signal	Reading	Spoofing Signal Power Level (dBm)		Time between position fix loss and spoofing (s)
				First degradation of accuracy	Spoofing	
1	Single Frequency GPS only	GPS L1 C/A	1	-128	-116	48
			2	-128	-116	46
			3	-131	-119	39
			4	-128	-113	45
2	Single Frequency Multi-GNSS	GPS L1 C/A	1	-125	-110	69
			2	-122	-107	53
			3	-125	-110	55
			4	-122	-107	52
3		Galileo E1 OS	1	-122	-107	-
			2	-122	-107	-
			3	-125	-110	-
			4	-122	-107	-
4		GPS L1 C/A and Galileo E1 OS	1	-125	-107	48
			2	-125	-110	50
			3	-125	-107	45
			4	-122	-107	51
5	Dual-Frequency Multi-GNSS	GPS L1 C/A	1	-	-	-
			2	-	-	-
			3	-	-	-
			4	-	-	-
6		Galileo E1 OS	1	-	-	-
			2	-	-	-
			3	-	-	-
			4	-	-	-
7		GPS L1 C/A and Galileo E1 OS	1	-	-	-
			2	-	-	-
			3	-	-	-
			4	-	-	-

Note: - indicates no data as degradation of accuracy / spoofing does not occur.

It is also evident that the minimum spoofing power levels are notably higher in comparison to the received GNSS signal power level (approximately -160 to -130 dBm). This is attributed to the noise-like code structures of GNSS signals, enabling their reception even at low levels of interference. However, it is noteworthy that the required minimum spoofing power levels for inducing position fix loss are lower as compared to the minimum interference signal power levels observed during GNSS jamming tests conducted through both field evaluations [26-28] and GNSS simulation [29-31]. This disparity arises due to the difference in synchronisation between authentic and spoofing GNSS signals, compelling the GNSS receiver to recompute its position fix at relatively lower spoofing signal power levels.

At the minimum spoofing power level, the duration between position fix loss and the initiation of spoofing is contingent on the degree of synchronisation between the genuine and spoofing GNSS signals. When both signals are closely synchronised, spoofing occurs rapidly. Conversely, when the signals are largely unsynchronised, the loss of position fix endures for an extended period as the target GNSS receiver needs to recompute its position fix. The level of synchronisation, or lack thereof, directly influences the efficiency and swiftness of the spoofing impact on the GNSS receiver.

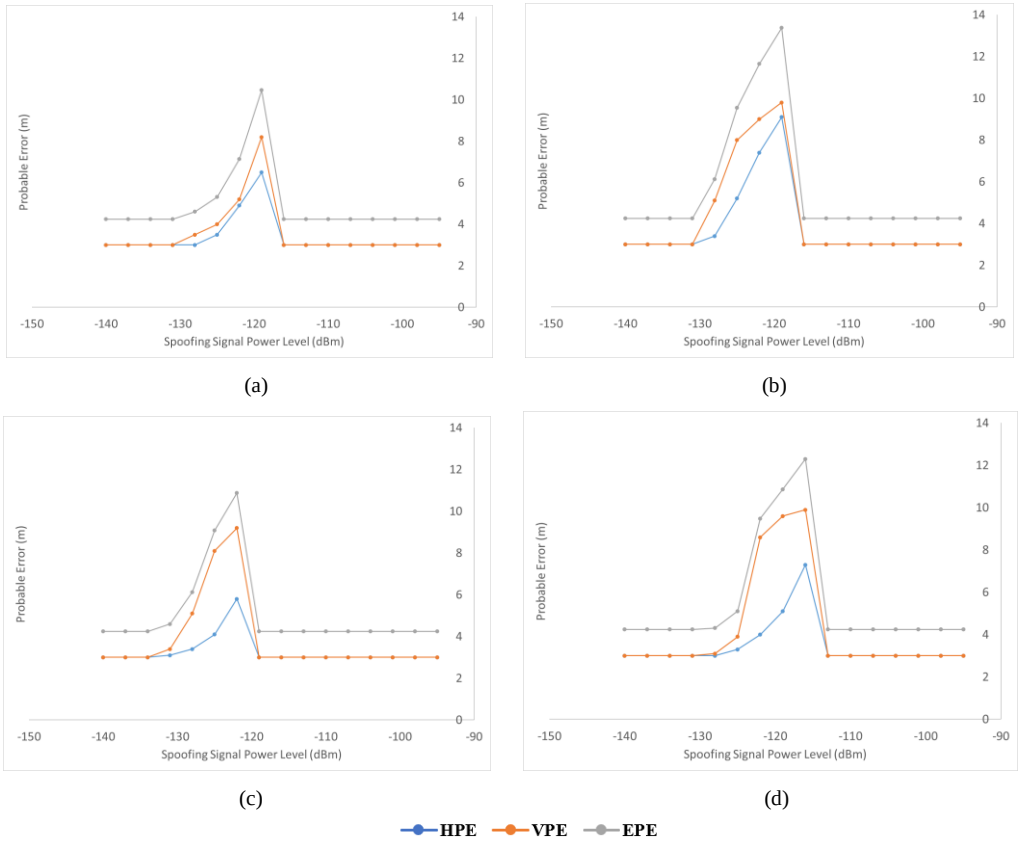

Fig. 3. Recorded probable error values for Scenario 1 (single frequency GPS only with GPS L1 C/A spoofing signal) for: (a) Reading 1, (b) Reading 2, (c) Reading 3 and (d) Reading 4.

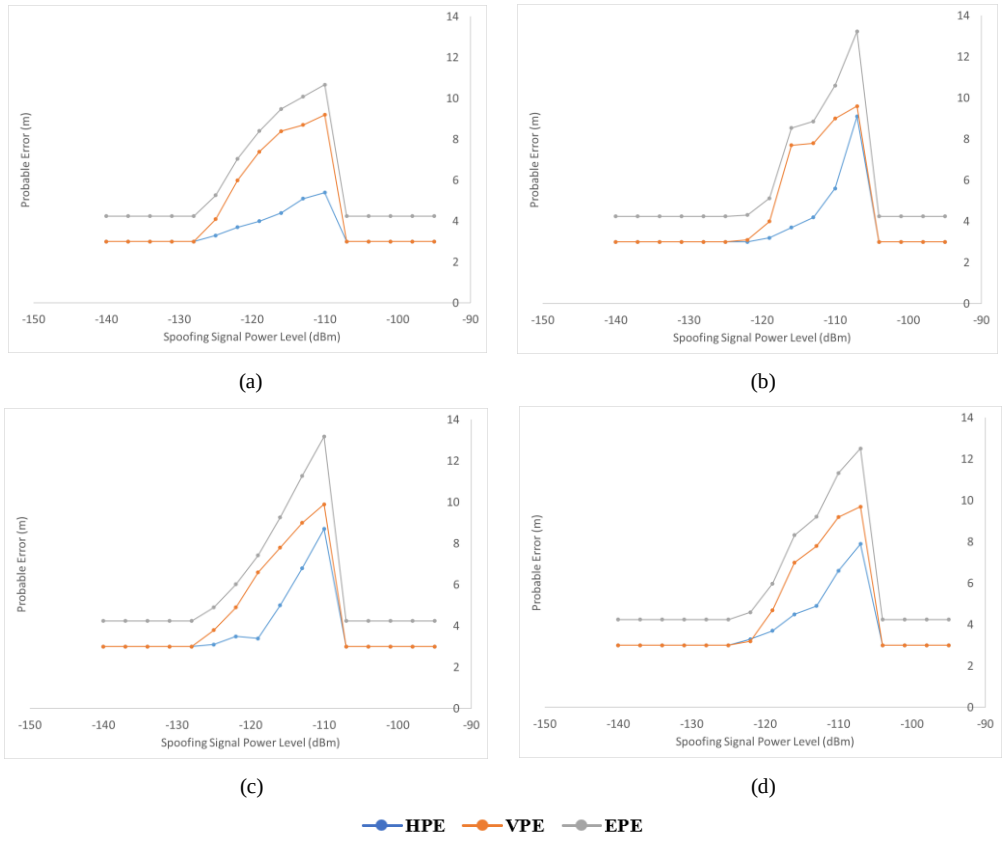

Fig. 4. Recorded probable error values for Scenario 2 (single frequency multi-GNSS with GPS L1 C/A spoofing signal) for: (a) Reading 1, (b) Reading 2, (c) Reading 3 and (d) Reading 4.

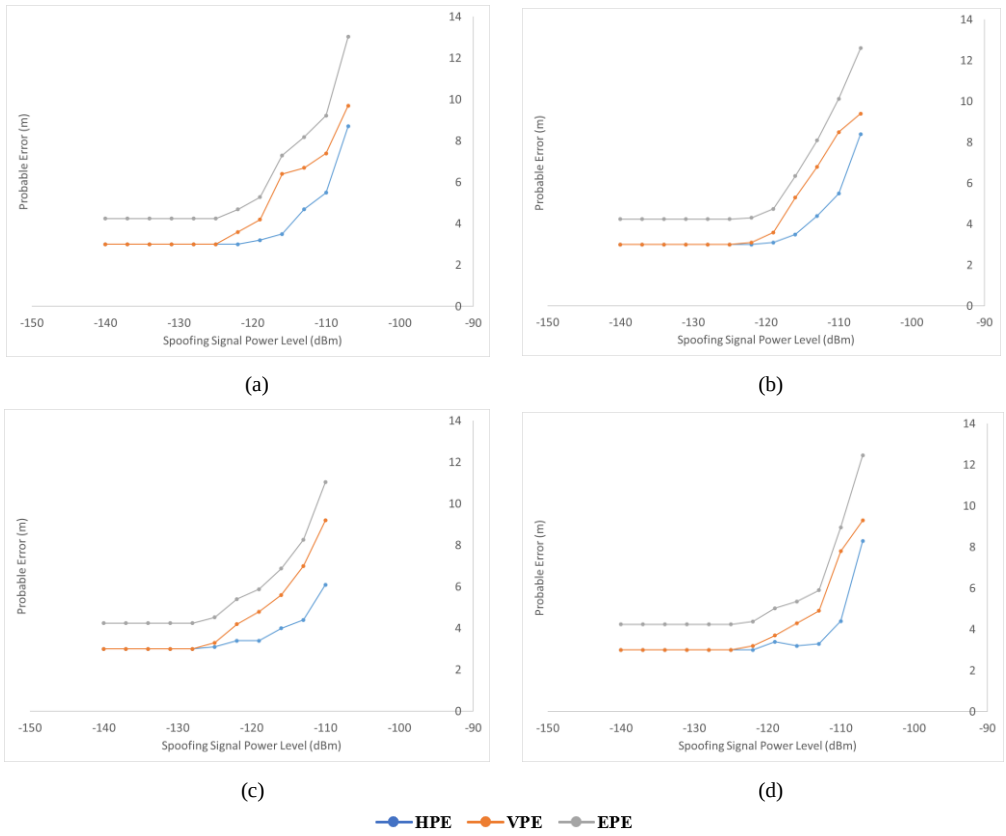

Fig. 5. Recorded probable error values for Scenario 3 (single frequency multi-GNSS with Galileo E1 OS spoofing signal) for: (a) Reading 1, (b) Reading 2, (c) Reading 3 and (d) Reading 4.

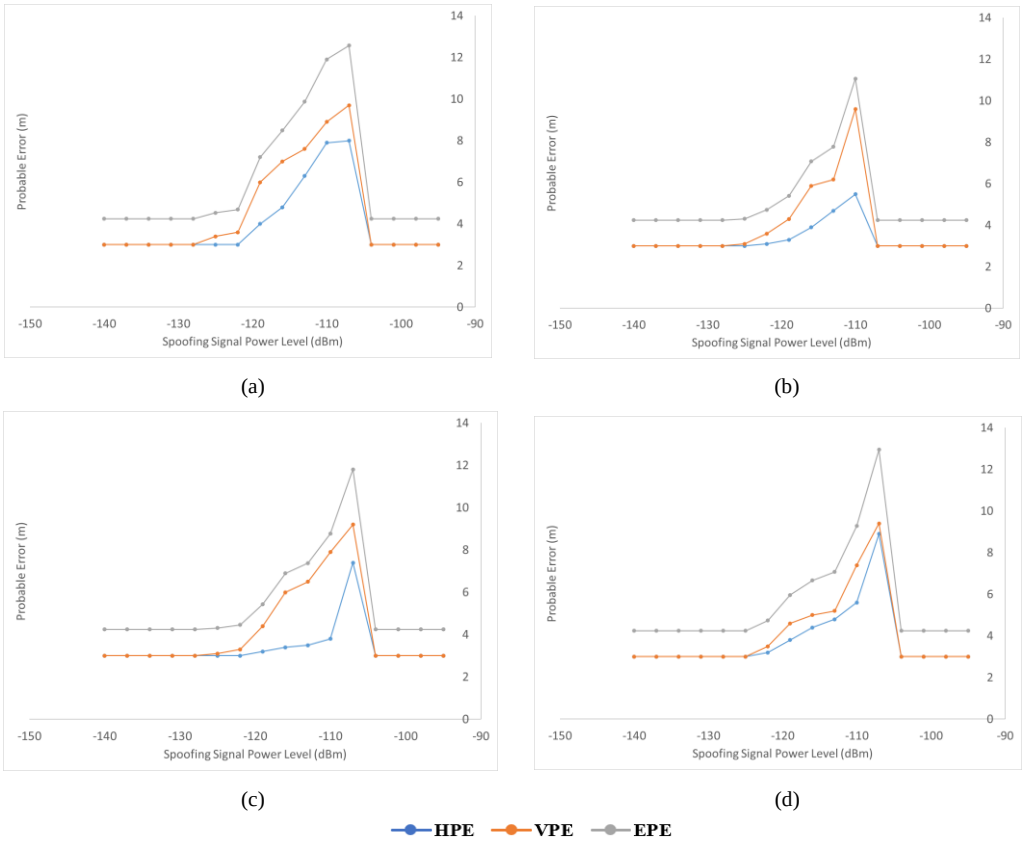

Fig. 6. Recorded probable error values for Scenario 4 (single frequency multi-GNSS with GPS L1 C/A and Galileo E1 OS spoofing signals) for: (a) Reading 1, (b) Reading 2, (c) Reading 3 and (d) Reading 4.

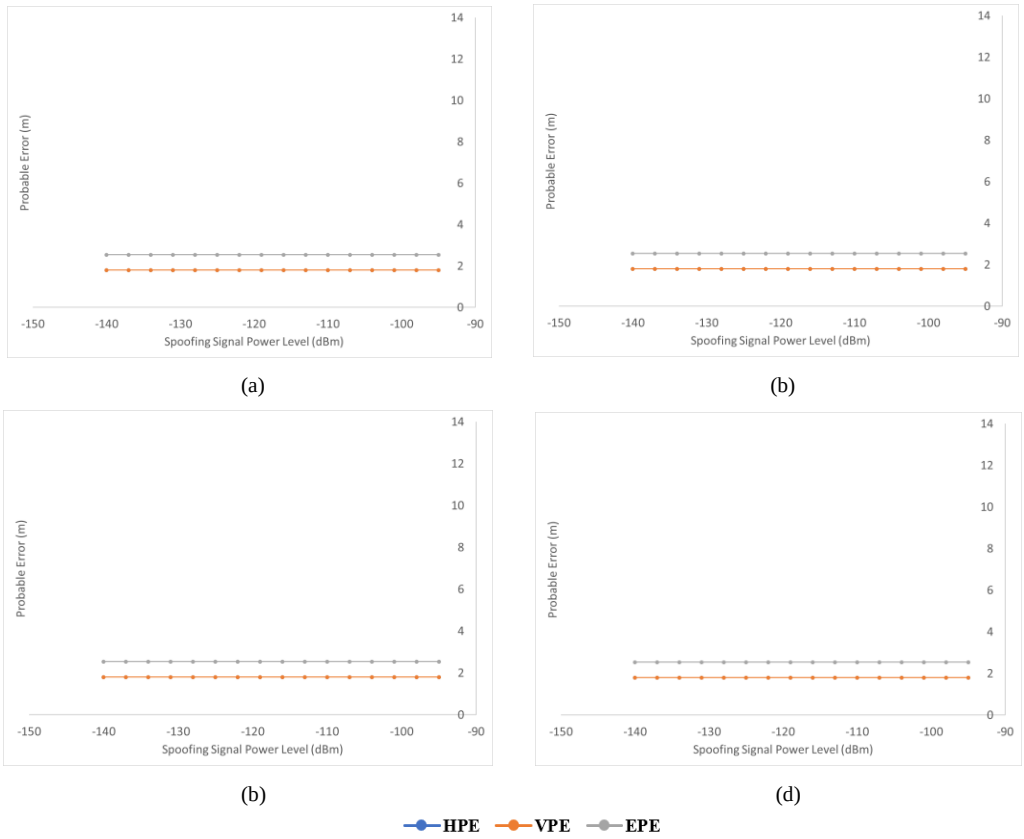

Fig. 7. Recorded probable error values for Scenario 5-7 (dual-frequency multi-GNSS) for: (a) Reading 1, (b) Reading 2, (c) Reading 3 and (d) Reading 4.

The study reveals that the single frequency GPS only mode (Scenario 1) exhibits lower minimum spoofing power levels and shorter durations between position fix loss and spoofing as compared to the single frequency multi-GNSS mode (GPS L1 C/A and Galileo E1 OS) in both Scenarios 2 and 4. This is attributed to the multi-GNSS mode's higher number of observed GNSS satellites, resulting in superior GNSS signal coverage as compared to the GPS only mode. The increased signal diversity also makes it more challenging to execute a successful spoofing attack, with the presence of the Galileo E1 OS signal in the multi-GNSS mode introducing a factor that diminishes the synchronisation between the spoofing and authentic GNSS signals. This effect is particularly pronounced when using only the GPS L1 C/A signal as the spoofing signal. As a result, the complexity introduced by the additional Galileo signal contributes to a higher level of resilience against spoofing in the multi-GNSS mode compared to the GPS only mode.

The probable errors of the GNSS receivers during the spoofing attacks are depicted in Figs. 3 - 7. For Scenarios 1 to 4 (Figs. 3 - 6), it is evident that as the power level of the spoofing signal increases, the probable error values also increase. This phenomenon is attributed to decreasing carrier-to-noise density (C/N_o) levels for GNSS satellites tracked by the receiver. C/N_o represents the ratio of received GNSS signal power level to noise density. Lower C/N_o levels lead to an elevated data bit error rate when extracting navigation data from GNSS signals, resulting in increased carrier and code tracking loop jitter. This, in turn, introduces more noise into range measurements, leading to less precise positioning [2, 17, 32]. The observed increase in probable error values aligns with findings from GNSS jamming tests conducted through both field evaluations and GNSS simulation.

In the readings for Scenarios 1, 2 and 4, it is noteworthy that the highest probable errors occur at the minimum spoofing power levels. However, after the initiation of spoofing, the probable errors decrease to levels similar to those observed prior to the transmission of the spoofing signal. This phenomenon occurs because, at this point, the spoofing signal power levels are relatively large, leading to high C/N_o levels. Consequently, the GNSS receiver achieves high level of accuracy during the spoofing period.

The observation that spoofing does not take place in Scenario 3 (single-frequency multi-GNSS mode) when only the Galileo E1 OS is used as the spoofing signal suggests that the settings of the evaluated receiver's chip restrict readings to instances when the GPS L1 C/A signal is available. While the GNSS receiver does not succumb to the spoofing signal,

Fig. 5 illustrates that the spoofing signal still induces increase in probable error until continuous position fix loss occurs. This behaviour aligns with the premise that the receiver, configured to rely on the GPS L1 C/A signal, remains resilient to spoofing attempts solely involving the Galileo E1 OS signal. However, the increase in probable error suggests that the presence of the spoofing signal, even without taking over the position fix, introduces noise and disruptions, impacting the precision of the positioning measurements.

For the dual-frequency multi-GNSS mode (GPS L1 C/A and L5 as well as Galileo E1 OS and E5a), spoofing does not take place as the GPS L5 and Galileo E5a signals are not affected by spoofing signals in the L1 / E1 band (Scenarios 5 to 7). It is also observed in Fig. 7 that the spoofing signals do not affect the receiver's probable errors. This highlights the importance of multifrequency GNSS in mitigating spoofing. In addition, lower probable errors are observed for the dual-frequency multi-GNSS mode as compared to Scenarios 1 to 4, as the GPS L5 and Galileo E5a signals have larger bandwidth and code length, higher chipping rate as well as stronger transmission power level, which increase its accuracy [2, 16-18].

The observed variations in probable error patterns for each set of readings can be attributed to the dynamic nature of the GNSS satellite constellation. The configuration and geometry of satellites in the constellation change over time, leading to location and time-dependent variations in GNSS accuracy [2, 17, 32]. Additionally, other factors contributing to GNSS error parameters, such as atmospheric conditions and multipath, may introduce further variations in probable error patterns. The complexity and multifaceted nature of these factors contribute to the observed dynamic and variable nature of GNSS accuracy during the course of the study.

In general, values of VPE tend to be higher as compared HPE for GNSS readings. This is as overhead satellites typically have higher C/N_o levels as compared to satellites above the horizon. As a result, the GNSS height solution is inherently less precise than the horizontal solution [2, 17, 32]. However, for the evaluated GNSS receiver, particularly at lower spoofing signal power levels, the values of VPE and HPE appear to be similar. This occurs due to the receiver's high sensitivity, allowing for comparable C/N_o levels for both overhead satellites and satellites above the horizon. Conversely, at higher spoofing signal power levels, the values of VPE become larger than HPE. This is attributed to the significant reduction in C/N_o levels for satellites above the horizon as compared to overhead satellites. The impact of spoofing signals on C/N_o levels contributes to a noticeable divergence in the vertical and horizontal error patterns, with the vertical solution becoming less precise than the horizontal solution under these conditions.

The primary limitation of this study lies in the inherent challenges associated with field evaluations, including various error parameters such as ionospheric and tropospheric delays, GNSS satellite clock and ephemeris errors, GNSS satellite positioning and geometry, external radio frequency interference (RFI), as well as obstructions and multipath effects. These factors introduce uncontrollable variables that may affect the accuracy and reliability of the study results. For future work, a potential avenue is to conduct the study using GNSS simulation, which allows for the tests to be carried out under controlled and repeatable conditions as defined by the users. In a controlled laboratory environment, the tests are not hindered by unintended signal interferences and obstructions [33-36]. Furthermore, expanding the scope of future work could involve evaluating the performance of a wider range of multifrequency multi-GNSS receivers. This would provide a more comprehensive understanding of the effectiveness and robustness of various GNSS receivers in the face of spoofing attacks and other potential threats.

IV. CONCLUSION

The findings from this study underscore the critical role of multifrequency GNSS in mitigating spoofing threats. The dual-frequency multi-GNSS mode demonstrates resilience against spoofing, as the GPS L5 and Galileo E5a signals remain unaffected by spoofing signals in the L1/E1 band. This resilience enhances the security and reliability of the GNSS receiver in the face of potential attacks. In the single frequency multi-GNSS mode, the increased number of observed GNSS satellites contributes to higher minimum spoofing power levels and longer durations between position fix loss and spoofing as compared to the GPS only mode. This emphasises the advantage of incorporating signals from multiple satellite constellations for improved security. For future studies, employing GNSS simulation can provide controlled and repeatable conditions, allowing for a more thorough evaluation of the impact of multi-band spoofing on the performance of the evaluated GNSS receiver. Additionally, expanding the evaluation to a wider range of multifrequency multi-GNSS receivers will contribute to a more comprehensive understanding of their performance in the presence of various spoofing scenarios.

ACKNOWLEDGEMENT

This work was presented during the IEEE Workshop on Geoscience and Remote Sensing 2023 (IWGRS 2023) that was held on 7 November 2023 at Multimedia University Melaka Campus.

REFERENCES

[1] S. Knedlik, *Introduction to Satellite Navigation, Inertial Navigation, and GNSS/INS Integration*. Berlin, Germany, Springer, 2016.

[2] E. D. Kaplan and C. J. Hegarty, *Understanding GPS: Principles and Applications*. Norwood, Massachusetts, U.S, Artech House, 2017.

[3] S. Jin, W. Qisheng and G. Dardanelli, "A Review on Multi-GNSS for Earth Observation and Emerging Applications," *Remote Sens.*, vol. 14, pp. 3930, 2022.
[4] S. Dinesh, "Global Navigation Satellite System (GNSS) Spoofing: A Review of Growing Risks and Mitigation Steps," *Defence S&T Tech. Bull.*, vol. 6, pp. 42-61, 2013.
[5] A. Ruegamer and D. Kowalewski, "Jamming and Spoofing of GNSS Signals – An Underestimated Risk," *FIG Working Week 2019*, 17-21 May 2015, Sofia, Bulgaria.
[6] Y. Liu, L. L. Sihai, Q. Fu and Z. Liu, "Impact Assessment of GNSS Spoofing Attacks on INS/GNSS Integrated Navigation System," *Sensors*, vol. 18, pp. 1433, 2018.
[7] L. Meng, L. Yang, W. Yang and L. Zhang, "A Survey of GNSS Spoofing and Anti-spoofing Technology," *Remote Sens.*, vol. 14, pp. 4826, 2022.
[8] B. O. Hanlon, B. Ledvina, M. L. Psiaki, P. M. Kintner and T. E. Humphreys, *Assessing the Spoofing Threat*. http://www.gpsworld.com/defence/security-surveillance /assessing-spoofing-threat-3171?page_ id=1. [Accessed 4 November 2009]
[9] P. Montgomery, T. E. Humphreys and B. M. Ledvina, "A Multi-antenna Defence Receiver-autonomous GPS Spoofing Detection," *Inside GNSS*, vol. 4, pp. 40-46, 2009.
[10] J. R. van der Merwe, X. Zubizarreta, I. Lukcin, A. Rugamer and W. Felber, "Classification of Spoofing Attack Types," in *Eur Nav Conf 2018*, 14-17 May 2018, Gothenburg, Sweden.
[11] J. A. Bhatti and T. E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," *Nav.*, vol. 64, pp. 51-66, 2017.
[12] *Above Us Only Stars: Exposing GPS Spoofing in Russia and Syria*, C4ADS, Washington D.C., U.S., 2019.
[13] D. Goward, *GPS Circle Spoofing Discovered in Iran*. https://www.gpsworld.com/gps-circle-spoofing-discovered-in-iran. [Accessed 21 April 2020]
[14] T. Harrison, K. Johnson, T. G. Roberts and T. Way, *Space Threat Assessment 2020*, Center for Strategic and International Studies (CSIS), Washington, D.C., U.S., 2020.
[15] *GPSMAP 66 Owner's Manual*, Garmin International Inc., Olathe, Kansas, U.S., 2021.
[16] G. Povero, *GNSS Signals Introduction. Links Foundation*, Torino, Italy, 2019.
[17] *Global Positioning System Standard Positioning Service Performance Standard, Command, Control, Communications, and Intelligence, 5th Ed.*, Department of Defence (DOD), Washington D.C., U.S., 2020.
[18] European GNSS (Galileo) *Open Service Signal-in-Space Interface Control Document*. European Space Agency (ESA), Paris, France, 2021.
[19] S. Dinesh, M. M. Faudzi, B. N. I. Shakhira, A. S. Robiah, S. Shalini, I. Aliah, B. T. Lim, M. A. Z. Fitry, A. K. M. Rizal and H. M. Y M. Hasrol, "Evaluation of Global Positioning System (GPS) Performance During Simplistic GPS Spoofing Attacks," *Defence S&T Tech. Bull.*, vol. 5, pp. 99-113, 2012.
[20] S. Dinesh, M. A. Z. Fitry, S. Esa, E. S. Shahrudin, A. K. A. Firdaus and Z. Zaherudin, "Evaluation of The Vulnerabilities of Unmanned Aerial Vehicles (UAVs) to Global Positioning System (GPS) Jamming and Spoofing," *Defence S&T Tech. Bull.*, vol. 13, pp. 333-343, 2020.
[21] *Avionics GPSG-1000 GPS / Galileo Portable Positional Simulator*, Aeroflex Inc., Plainview, New York, U.S., 2010.
[22] *A11XLV Digital Variable Gain GPS Amplifier*, GPS Source Inc., Pueblo West, Colarado, U.S., 2007.
[23] *L1P GPS Antenna*, GPS Source Inc., Pueblo West, Colarado, U.S., 2006.
[24] *U3741/3751 Spectrum Analyzers*, Advantest Corporation, Chiyoda-ku, Tokyo, Japan, 2009.
[25] CNET, *GPSDiag 1.0*. https://download.cnet.com/GPSDiag /3000-2130_4-10055902.html. [Accessed 9 June 2022]
[26] S. Dinesh, W. H. Wan Mustafa, M. M. Faudzi, M. Kamarulzaman, H. Hasniza, B. N. I. Shakhira, A. S. Robiah, S. Shalini, J. Jamilah, I. Aliah, B. T. Lim, M. A. Z. Fitry, A. K. M. Rizal, B. Azlina and H. M. Y. M. Hasrol, "Evaluation of The Effect of Radio Frequency Interference (RFI) on Global Positioning System (GPS) Accuracy," *Defence S&T Tech. Bull.*, vol. 3, pp. 100-118., 2010.
[27] S. Dinesh, M. Y. Hafizah, A. K. A. Firdaus, M. D. M. Zuryn and K. Maizurina, "Evaluation of The Effect of Radio Frequency Interference (RFI) on Dual-frequency Global Navigation Satellite System (GNSS)," *Defence S&T Tech. Bull.*, vol. 16, pp. 228-237, 2023.
[28] I. A, Norhisyam, S. Dinesh and M. S. Azman, "Effect of Radio Frequency Interference (RFI) on The Performance of Global Positioning System (GPS) Static Observations," in *9th IEEE Colloq. Signal Process Appl.*, 8-10 March 2013, Kuala Lumpur.
[29] S. Dinesh, M. M. Faudzi and M. A. Z. Fitry, "Evaluation of The Effect of Radio Frequency Interference (RFI) on Global Positioning System (GPS) Accuracy via GPS Simulation," *Defence Sci. J.*, vol. 62, pp. 338-347, 2012.
[30] S. Dinesh, M. A. Z. Fitry and A. H. Shahrudin, "Evaluation of Global Positioning System (GPS) Adjacent Band Compatibility via GPS Simulation," *Defence S&T Tech. Bull.*, vol. 10, pp. 229 – 235, 2017.
[31] S. Dinesh, M. Y. Hafizah, A. K. A. Firdaus, M. D. M. Zuryn and K. Maizurina, "Evaluation of Multi-GNSS Performance via GNSS Simulation," *Defence S&T Tech. Bull.*, vol. 16, pp. 13-23, 2023.
[32] *Engineer Manual EM 1110-1-1003: NAVSTAR Global Positioning System Surveying*, US Army Corps of Engineers (USACE), Washington D.C., U.S., 2011.
[33] O. Pozzobon, C. Sarto, A. D. Chiara, A. Pozzobon, G. Gamba, M. Crisci and R. Ioannides, "Developing A GNSS Position and Timing Authentication Testbed: GNSS Vulnerability and Mitigation Techniques," *Inside GNSS*, vol. 8, pp. 45-53, 2013.
[34] G. A. Elango and G. F. Sudha, "Design of Complete Software GPS Signal Simulator with Low Complexity and Precise Multipath Channel Model," *J. Electr. Syst. Inform. Tech.*, vol. 3, pp. 161-180, 2016.
[35] Y. Bi and J. Yuan, "A Portable GPS Signal Simulator Design Based on ZYNQ," in *2nd Int. Symp. Comp. Eng. Intell. Comm.*, 6-8 August 2021, Nanjing, China.
[36] M. Emerick, *EUSPA to Hold GNSS Signal Simulator Manufacturers Forum in December*. https://www.gpsworld.com/euspa-to-hold-gnss-signal-simulator-manufacturers-forum-in-december. [Accessed 23 November 2022]