CLPDI-based Fast Secure Code Estimation and Replay Attacks on GNSS Signals

Simone Soderi[*‡] , Jari Iinatti[†]
[*]IMT School for Advanced Studies Lucca, Lucca, Italy
[‡]Cybersecurity National Laboratory, CINI - Roma, Italy
simone.soderi@imtlucca.it
[†]Centre for Wireless Communications, University of Oulu, Finland
jari.iinatti@oulu.fi

***Abstract*—In an era where satellite communications underpin global interconnectivity, protecting used channels against cyber threats is imperative. This paper introduces a new strategy to expedite spoofing attacks on Global Navigation Satellite Systems (GNSS) by leveraging the novel utilization of Chip Level Post Detection Integration (CLPDI) technique. This research explores the mechanics of CLPDI, discovering a previously underexplored vulnerability that could dramatically shorten the timeline for executing successful GNSS spoofing attacks. Our contribution extends beyond the technical exposition of vulnerabilities; it encompasses the development of robust countermeasures designed to fortify GNSS against the evolving landscape of threats. Through theoretical analysis and practical simulations, we analyzed the mean acquisition time (T_{MA}) and the probability of detection (P_d) as metrics to evaluate the proposed method's robustness. Experiments demonstrate the goodness of using CLPDI to speed up Security Code Estimation and Replay (SCER) attacks on GNSS signals in a multipath fading channel. Using CLPDI, we can improve the T_{MA} to acquire the spreading code by 21.28%, providing a significant advantage to the attacker. This work aims to inspire the security community to explore new defensive strategies and the adoption of our proposed measures to protect the future of satellite communications.**

***Index Terms*—satellite communication, spoofing attacks, Chip Level Post Detection Integration, security, CSK.**

I. Introduction

The advent of satellite communications marks a cornerstone in achieving global connectivity, with applications spanning from precision navigation systems to managing critical infrastructures. Significant technological strides have characterized the evolution of this domain, yet it simultaneously unveils a gamut of security vulnerabilities, particularly within Global Navigation Satellite Systems (GNSS). Spoofing attacks on GNSS signals have emerged as a sophisticated threat vector, undermining the systems' integrity and reliability, crucial for civilian and defence applications. Addressing these vulnerabilities is not just a matter of enhancing existing protocols but requires fundamentally rethinking security strategies in the context of next-generation networks [1].

The transition towards the Sixth Generation (6G) of telecommunications plans the enhanced integration of satellite architectures, including Non-Terrestrial Networks (NTN) and mega-constellations, into the existing communication infrastructure [2]. These advancements promise to redefine connectivity, offering ubiquitous coverage and unprecedented data throughput capabilities. Specifically, mega-constellations, exemplified by pioneering initiatives such as Starlink and OneWeb, stand at the forefront of this transformation, poised to facilitate seamless integration into 6G networks. However, realising these ambitious objectives is contingent upon addressing a series of open issues, particularly about the security and intelligence of the novel NTN architecture. Ensuring the successful deployment and operation of these integrated satellite-terrestrial networks necessitates developing secure, scalable, and reliable innovative solutions [3].

In [4], the authors provide an exhaustive examination of the current advancements in integrated satellite-terrestrial network technologies, highlighting pivotal challenges such as prolonged propagation delays, intricate link conditions, considerable dynamics of network topology, and the paramount importance of security measures. These factors are essential for the effective integration into the forthcoming 6G networks, underscoring the necessity to address security vulnerabilities alongside technical and operational considerations.

Motivation. Given this background, our paper delves into a novel approach to expedite spoofing attacks against GNSS signals, leveraging Chip Level Post Detection Integration (CLPDI) [5]. This investigation aims to illuminate the vulnerabilities inherent in the GNSS framework, prompting a reevaluation of security measures in an era where satellite communications are increasingly integrated with terrestrial 6G networks. By exploring the efficacy of CLPDI in the context of GNSS spoofing, we aspire to catalyze the development of robust countermeasures, thus contributing to the broader discourse on ensuring the resilience of satellite communications against sophisticated cyber threats in a rapidly evolving telecommunications landscape.

Contribution. The main contribution is to propose using the CLPDI technique to speed up Security Code Estimation and Replay (SCER) attacks. The basic intuition is that the attacker successfully reduces the mean code acquisition time used in Code Shift Keying (CSK) modulation by integrating successive samples of the matched filter into receptions. This result then allows the attacker to generate a spoofed signal faster. To the best of our knowledge, this technique for speeding up an attack on GNSS signals is new in the literature. In this article, we refer to code detection as acquisition, not code synchronization. Other contributions of this paper include a security analysis of this attack and a mitigation proposal using physical layer anti-spoofing techniques.

The rest of the paper is organized as follows. Section II describes the main background concepts used in this work, while Section III contains a short overview of revising the literature about satellite security. Section V introduces the attacker model, while Section V-A describes the implementation of CLPDI to CSK modulation. Section VI presents our experiments and their results. Finally, Section VIII concludes the paper.

II. Background

This section provides the basic concepts for understanding how we position our proposed use of CLPDI for physical layer security attacks. It also provides the basic concepts of satellite network architectures, including modulations and protocols, which help evaluate our attack model and its mitigations.

A. GNSS Architecture

The GNSS represents a complex network designed to deliver precise location and timing information to users across the globe. This system operates on signals transmitted in the L-band of the radio frequency spectrum, chosen for its atmospheric penetration capabilities and reduced susceptibility to interference. Various properties characterize these signals, including frequency bands, modulation schemes, and pseudo-random codes. The signal structure is carefully crafted to include a navigation message that carries essential data, such as satellite status, ephemeris, and almanac information, alongside pseudo-random noise (PRN) codes. These codes enable receivers to distinguish signals from individual satellites and accurately measure the time delay for positioning.

GNSS architecture has a structure divided into segments as follows [3]. At the heart of the GNSS architecture lies the *space segment*, a constellation of satellites equipped with highly accurate atomic clocks, orbiting Earth and broadcasting the timing signals crucial for distance calculations. Some GNSS constellations enhance their operational autonomy and reliability by using Inter-Satellite Links (ISLs), facilitating direct communication between satellites. The *user segment* encompasses an array of GNSS receivers, from handheld devices to systems integrated into vehicles, processing the satellite signals to determine the user's position and time. Techniques like Real-Time Kinematic (RTK) positioning are employed within this segment to achieve high-precision location data, utilizing real-time corrections from a fixed base station. Finally, the *ground segment* consists of Earth's monitoring stations and control centres, which are responsible for maintaining and managing the satellite constellation. This segment ensures the integrity of the space segment and delivers correction data through Differential GNSS (DGNSS) and GNSS Augmentation Systems, further refining the accuracy of the signals received by users.

This comprehensive architecture of GNSS highlights the complexity and sophistication of the system, highlighting the integration of advanced technologies and methodologies to provide reliable and precise positioning services to a diverse array of user segments worldwide.

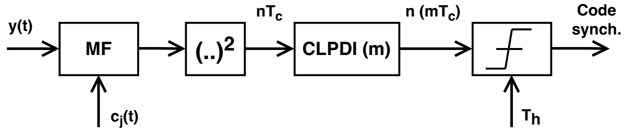

Fig. 1: CLPDI functioning scheme in conjunction with an MF for code synchronization in a non-coherent receiver [6].

B. Chip Level Post Detection Integration (CLPDI)

CLPDI is a crucial technique in enhancing code synchronization within spread spectrum systems under conditions marked by dense multipath propagation. CLPDI operates by integrating multiple chips' energies after matched filtering, amplifying the Signal-to-Noise Ratio (SNR) and ensuring a more reliable synchronization at the beginning of the acquisition phase. This integration is vital in mitigating the adverse effects of multipath dispersion, facilitating the synchronization process [5].

The essence of CLPDI's functionality lies in aggregating signal energies over a set number of consecutive chips. The efficacy of CLPDI is further evidenced by its ability to reduce the mean acquisition time (T_{MA}) significantly, demonstrating its capacity to quicken the detection of multipath signal components and uphold the synchronization mechanism's robustness and reliability [5], [6].

Technically, when a signal is received in a direct-sequence spread spectrum system, this signal passes through a matched filter (MF) that incorporates the time-reversed replication of the spreading code consisting of N chips [7]. The response of this filter is proportional to the code's Auto-Correlation Function (ACF). The MF's output is sampled at the chip rate (notably, T_c is the chip length), and acquisition is successful upon crossing a predefined threshold (T_h). The probability of detection (P_d) correlates with the ACF's peak at zero delays, while false alarms, triggered by threshold crossings at other delays, occur with a probability (P_{fa}). These false alarms are destructive because they cause the incorrect code phase, particularly in multipath channels where multiple peaks emerge due to the MF's response to the encoded signal. As shown in Figure 1, CLPDI addresses these challenges by executing post-detection integration at the chip level, aggregating several successive m samples at the MF's output. This process reduces the uncertainty region and the number of cells to be tested in the uncertainty region to $N_m = \frac{N}{m}$, where N is the length of the spreading code. This positively affects the performance without any extra knowledge of the multipath fading. By sampling in multiples of (mT_c), CLPDI ensures uncorrelated consecutive samples at its output; therefore, the uncertainty zone, or the number of cells to be examined during the acquisition, is lower when compared to the acquisition of pure MF.

Integrating CLPDI into spread spectrum systems highlights the method's adaptability and the possibility of enhancing physical layer security defences against advanced spoofing attacks. Through meticulous application and understanding of CLPDI, this research contributes to the foundational knowledge required to develop robust countermeasures, paving the way for more secure communication systems in the face of evolving cyber threats.

III. Related Works

GNSS are critical in various applications, necessitating secure and reliable signal transmission. However, the inherent characteristics of GNSS signals, including their low strength, make them susceptible to various security threats. This section reviews the literature on security threats against GNSS.

Spoofing and Meaconing Attacks. Spoofing attacks manipulate GNSS signals to deceive receivers about their position or time. Spoljar [8] highlights spoofing as a significant information security issue resulting from malevolent modifications to the navigation message used in the position determination process. Dobryakova [9] further explains that spoofing involves the transmission of interference matched to the GNSS signal structure, aiming to commandeer the victim receiver's tracking loops. This manipulation can severely impact applications requiring secure, assured information, such as asset tracking and fleet management. Meaconing, a replay attack, involves recording GNSS signals to be replayed or retransmitted later. Lenhart [10] and Marnach [11] discuss how meaconing, while offering less adversarial control compared to spoofing, bypasses Navigation Message Authentication (NMA) and remains a potent threat due to its signal-level operation.

Jamming Attacks or RF Jammers. Jamming attacks disrupt GNSS signal reception by intentionally transmitting radio frequency noise. The vulnerability of GNSS to jamming, as discussed by Jeong & Lee [12] and Sheridan [13], derives from the low signal strength of GNSS, making it easy to overpower with strong interference. Elango [14] categorizes jamming into several types, including Continuous Wave Interference (CWI), Multi-CWI (MCWI), and Pulse Interference (PI), each capable of disrupting GNSS signal reception to varying degrees.

Replay Attacks. Replay attacks, particularly SCER attacks [15], represent a sophisticated threat to GNSS security. In SCER attacks, the adversary implements the estimation of secure code bits from GNSS signals to facilitate the replay of manipulated signals. This technique allows attackers to generate signals indistinguishable from authentic GNSS signals to the victim receiver, posing a significant challenge to GNSS reliability and integrity [16]. A notable study in this area has focused on enhancing the strategies for SCER attacks and developing more effective detection schemes for ensuring GNSS signal security. The proposed study by Caparra *et al.* [17] is closer to our work. Their research successfully improved SCER attack strategies, providing deeper insights into the vulnerabilities of GNSS signals and how they can be exploited. The study demonstrated that the actual Likelihood Ratio Test (LRT) detection scheme outperforms its previously proposed modifications, offering a more reliable method for detecting SCER attacks.

Despite the evolving threat landscape, current defence solutions against GNSS security threats are limited by cost, complexity, and processing power requirements [18]. To mitigate these threats, researchers have proposed a variety of countermeasures, including cryptographic security measures [19], signal quality assessment and anomaly detection [20], [21], and use of external assistance for spoofing detection. In conclusion, the security of GNSS remains a critical concern due to the variety of attacks that can be perpetrated against it. The literature emphasises the need for comprehensive security solutions that address the unique vulnerabilities of GNSS signals, including spoofing, jamming, and replay attacks. As GNSS continues to underpin critical infrastructure and services, advancing research and development in GNSS security measures will be essential to protecting this essential technology.

IV. System Model

This paper addresses the physical layer security problem for GNSS systems that employ CSK modulation [22], [23]. The modulation CSK, created for high data rates in band-limited spread spectrum systems, is an M-ary orthogonal modulation. Each symbol (used to transmit $U = \log_2(M)$ bits) is obtained from a different circular cyclic code phase shift of a single fundamental PRN sequence called $c_d(t)$. From this fundamental code, the modulator generates $M = 2^U$ circular code shifts that are expressed as follows

$$c_x(t) = c_d(mod[t - m_x T_c, CT_c]) \quad x = 0 \cdots M - 1, \quad (1)$$

where m_x is the integer number corresponding to the shift of the x-th symbol, T_c is the chip period, and C is the number of chips in the PRN sequence.

The received signal is given by

$$y(t) = A a_{ch}(t) e^{j\varphi_{ch}(t)} c_x(t) + n(t), \quad (2)$$

where A is the amplitude of the transmitted signal, $a_{ch}(t)$ and $\varphi_{ch}(t)$ are the characteristics of the Rayleigh multipath fading channel, $c_x(t)$ is the transmitted CSK waveform, and $n(t)$ is the AWGN.

We then assumed a non-coherent demodulation of the CSK signal. This process consists of recovering the maximum energy of the signal through a matched filter at reception without having information on the transmitted signal's phase [7]. The code MF can be expressed by

$$h(t) = c_j^*(T_c - t) \quad 0 \leq t \leq T_c, \quad (3)$$

where c_j^* is a time-reversed and conjugated version of the j-th CSK code. Finally, proportional to ACF, the MF output is sampled at the chip rate to maximize the SNR. Notably, this assumption is aligned with and propedeutic to the scheme presented in Figure 1 for using the CLPDI algorithm. Thus, the correlation between the received waveform and one of the shifted versions of the fundamental PRN sequence results in each matched filter output.

V. Attacker Model

In this section, we illustrate the model of our attacker. The attacker's main objective is to illegally inject GNSS spoofed signals to the user's receiver to induce the intended spoofed position or, more generally, the intended Position, Velocity, and precise Time (PVT) . As shown in Figure 2, we assume that the adversary can receive the same GNSS signals $y^{S1}, y^{S1}, \dots y^{Sn}$ received by the user. Similarly to [23], the attacker intends to implement a SCER attack, i.e. to estimate the unpredictable information encoded in the CSK modulation in the shortest possible time and to use this estimation to generate a spoofed GNSS signal containing a false PVT. We implicitly assume he can carry out this attack without making assumptions about the attacker's computational capacity.

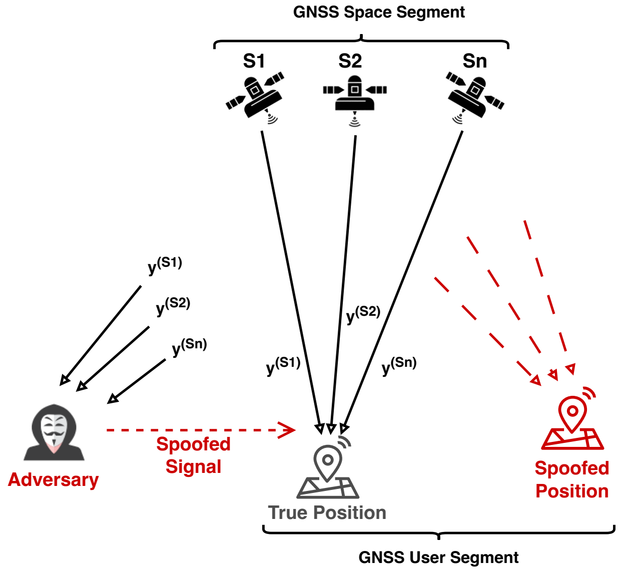

Fig. 2: GNSS spoofing attack model.

Our proposal to use the CLPDI algorithm is intended to focus on the speed of execution of the attack since if the attacker can estimate the CSK modulation spreading code faster, the whole attack will be faster.

A. CLPDI to Accelerate Spoofing Attacks

In this section, we delve into the technical specifics of how CLPDI can be used to improve the speed of SCER attacks, where the goal is to identify the spreading code used in CSK modulation. It is worth noting how this problem is similar to a code-synchronization problem in spread spectrum communications [24].

To understand how to integrate our proposal to use the CLPDI algorithm, we must first recall the architecture of the SCER attack. In SCER, the received signal is processed through an MF that incorporates the time-reversed replication of the spreading code. An estimator is then used to determine the maximum correlation between the spreading code and the received signal. In [16], Maximum Likelihood (ML), Maximum A Posteriori (MAP) estimators, and the Minimum Mean Square Error (MMSE) have been proposed as estimators. Such solutions typically involve the implementation of a parallel architecture. This parallel approach is typically too costly to perform in practice, especially when using somewhat lengthy codes [25]. One more straightforward way would be to test every code using a *serial search strategy* in which the local code phase is changed step by step in equal increments and selecting the highest corresponding detector output; this significantly lowers the implementation complexity. We propose replacing the estimator with the CLPDI algorithm followed by a threshold comparator.

We have assumed using a Rayleigh multipath fading channel. Since we are using a receiving MF, it will provide a peak when the received code matches the MF's impulse response. A multipath channel will produce as many peaks as multiple paths in the channel, as shown in Figure 3. Each of them leads to the code acquisition (ACQ), which results in a significant difference in the acquisition time. When the delay between these peaks is greater than T_c, the easiest way to combine these peaks to implement a modified version of the CLPDI algorithm [5] is to use a moving average filter that sums the consecutive peaks coming out of the MF. As can be seen in Figure 4, by combining $m = 2$ peaks, the number of cells in which we have to search for the code decreases to $N_m = \frac{N}{m}$, i.e., it is halved.

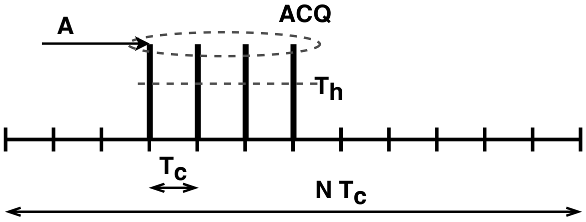

Fig. 3: Code MF output in $L = 4$ paths channel [5].

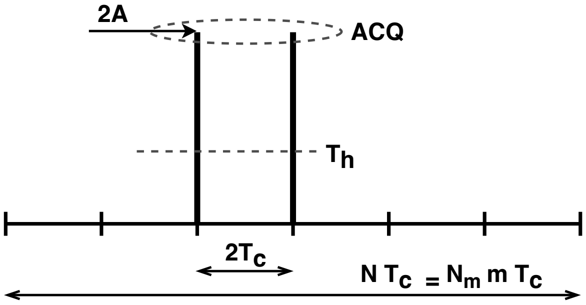

Fig. 4: Modified CLPDI with $m = 2$ in $L = 4$ paths channel [5].

The acquisition of the CSK spreading code can be modelled in the simplest form as a *serial search* in a one-dimensional uncertainty region divided into cells of size T_c. The dominant metric to describe this process is the mean acquisition time (i.e., T_{MA}), which, in the case of a receiver with code MF,

TABLE I: Simulation parameters.

Parameter	Value
CSK cardinality (U)	$1, 3, 5$
Symbols transmitted	2000
E_b/N_0	$[-20 : 20]$ dB
Code length (N)	1024
CLPDI (m)	$2, 4$
Channel paths (L)	$4, 8$
P_{fa} target	0.01
Penalty time (T_{fa})	$100 \cdot T_s$[1]

[1] $T_s = N \cdot T_c$ is the symbol time.

the modified CLPDI with m samples and the presence of a channel with L paths, can be expressed as (when $m \leq L$) [5]

$$
\begin{aligned}
T_{MA} = {} & \frac{P_M^{\frac{L}{m}}\left[LT_c + (N-L)(T_c + T_{fa}P_{fa})\right]}{1 - P_M^{\frac{L}{m}}} \\
& + \frac{\left[NT_c + (N-L)(T_c + T_{fa}P_{fa})\right]\sum_{i=0}^{\frac{L}{m}-1} iP_M^i}{N\sum_{i=0}^{\frac{L}{m}-1}\frac{P_M^i}{m}} + mT_c \\
& + \frac{(N-L)(N-L+m)(T_c + T_{fa}P_{fa})}{2N} + NT_c \qquad (4)
\end{aligned}
$$

where the uncertainty region N is the code's length. Although CSK signals use pilot signals for code synchronisation, in general, a priori, we cannot make any assumptions about the initial phase of the code at the beginning of the acquisition. P_{fa} is the probability of a false alarm at the output of the CLPDI, $P_M = 1 - P_d$ where P_d is the probability of detection in the correct code phase, $T_{fa} = K_p T_c$ is the penalty time caused by a false alarm, and T_c is chip interval.

VI. Evaluation of the Attack

This section presents the methodology and results of evaluating the spoofing attack leveraging CLPDI. Specifically, considering that the proposed method potentially applies to many spread-spectrum systems communicating over an AWGN channel with multipath fading, we simulated the probabilities of detection and false alarms of a CSK modulation in this scenario.

Figure 5 shows the Symbol Error Rate (SER) of the CSK modulation under nominal conditions with the chosen channel and under varying the chosen cardinality (U). The performance of SER as the $E_s/N_0 = NE_b/N_0$ ratio varies, which served as verification that the simulations were consistent with the proposed system model. Notably, E_b is the energy per bit, N is the code length, and N_0 is the noise spectral density.

Table I reports the parameters used for the parametric analysis. In our system, code acquisition is achieved by comparing the code MF with a threshold (i.e., T_h). Therefore, determining an adequate threshold is a process that involves both the P_d and the P_{fa}. We applied the Constant False Alarm Rate (CFAR) criterion to define the threshold level. According to this algorithm, the threshold is adjusted every simulation cycle to maintain a fixed level of P_{fa} (i.e., P_{fa} target), allowing us to compare the T_{MA} values as the other simulation parameters changed.

The function that calculates the threshold implements this process by iteratively adjusting the detection threshold based on the statistical properties of the input correlation scores. Initially, the threshold is set at the midpoint of the range of correlation scores, and adjustments are made iteratively by recalculating the P_{fa} after each modification. This method employs a binary search-like technique where the threshold is increased or decreased depending on whether the computed P_{fa} is lower or higher than the target P_{fa}. Adjustments to the step size facilitate more precise convergence towards the target false alarm rate. This iterative approach ensures that the final threshold optimally balances sensitivity and specificity, as reflected in both simulated and theoretical probabilities of detection and false alarm. This methodology underscores the importance of adaptive thresholding in signal processing to enhance detection accuracy while maintaining control over false alarm rates.

Then, once we identified the threshold that allowed us to obtain the desired P_{fa}, we applied the CLPDI algorithm to evaluate its performance in terms of P_d and T_{MA}.

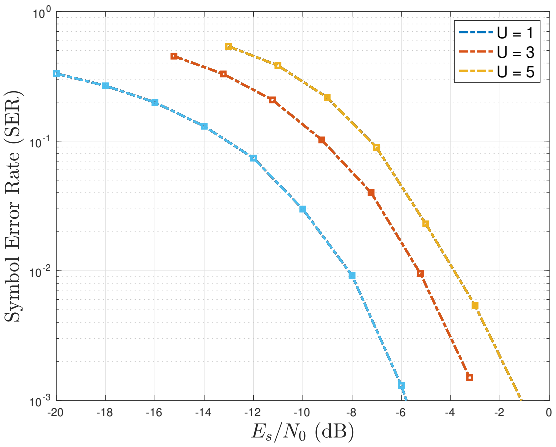

Fig. 5: Symbol Error Rate (SER) for various CSK constellation cardinality under nominal conditions.

Figures from 6 to 10 show, respectively, the P_d and T_{MA} of the receiver in a multipath channel with 4 paths, with CLPDI with $m = 4$ as the E_s/N_0 ratio varies. As can be easily seen, CLPDI provides a *significant performance improvement* by reducing the number of cells to be examined and increasing the probability of detection in the correct cells. Simulation results showed that in a channel with 8 multiple paths, by applying CLDPI with 4 samples, we reduced TMA by 21.28% compared with when the receiver only uses MF code (see Figure 10). It is important to recall that this improvement is achieved *without prior information* about the composition of the multiple channel paths. In particular, performance is better when the SNR ratio of the received signal is not optimal (which can happen to a GNSS receiver in an urban

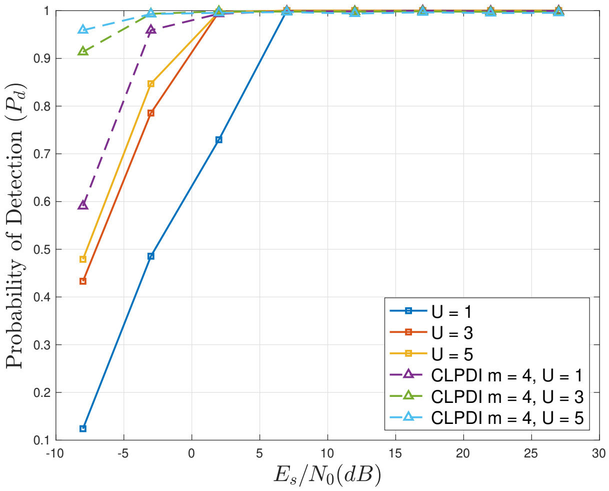

Fig. 6: P_d in multipath channel ($L = 4$) and with CLPDI ($m = 4$) and without it.

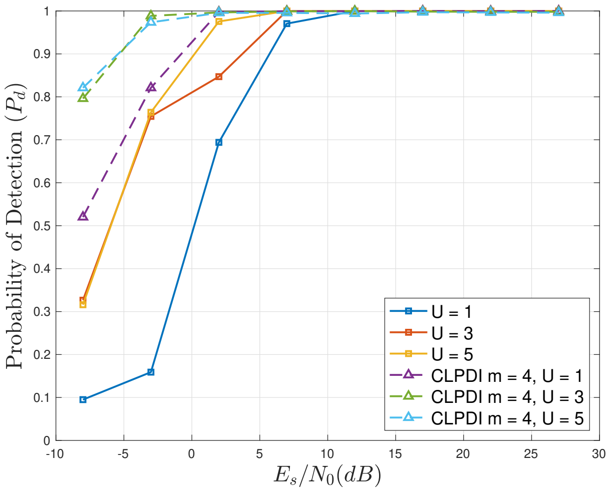

Fig. 7: P_d in multipath channel ($L = 8$) and with CLPDI ($m = 4$) and without it.

environment, for example), making this technique of greater interest in making a SCER attack even more effective.

VII. Discussion

The academic community is still studying spoofing attacks on GNSS signals extensively. The technique we proposed in this paper aims to demonstrate that it is possible to accelerate a known attack by inserting a filter that appropriately sums the output samples of the MF code. Although it is a simple, passive, and low-cost technique (the filter could be implemented via software), the impact on code acquisition time is significant.

Given the difficulty in identifying a passive attack that exploits CLPDI, in this section, we want to offer different food for thought to mitigate man-in-the-middle attacks of this type. GNSS spoofing represents a sophisticated Man-In-The-Middle (MITM) attack, wherein adversaries insert counterfeit signals into the communication channel between GNSS satellites and receivers. This intrusion causes the receivers to process these fake signals as legitimate, generating inaccurate position, navigation, or time information.

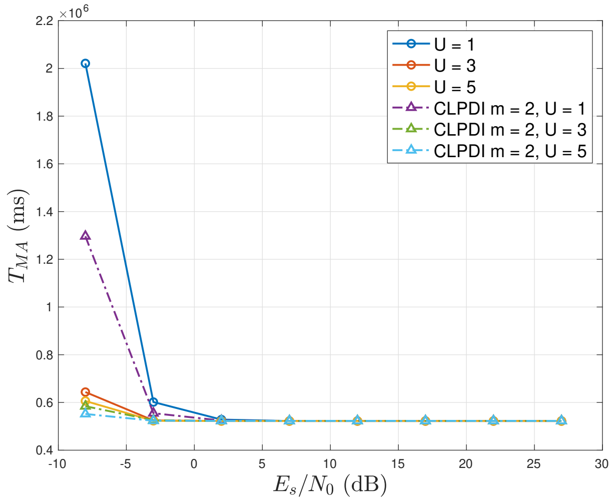

Fig. 8: T_{MA} in multipath channel ($L = 4$) and with CLPDI ($m = 2$) and without it.

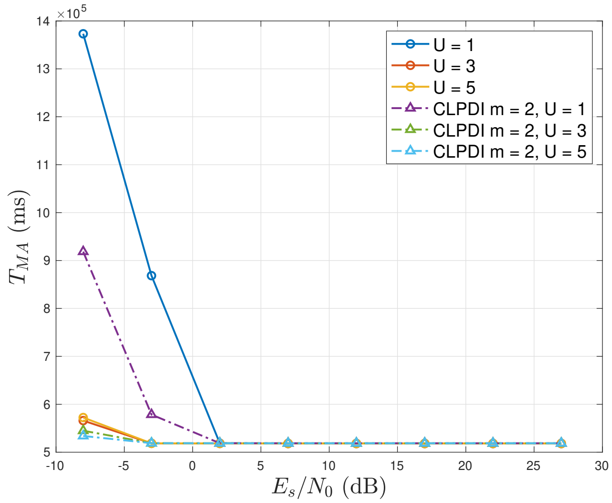

Fig. 9: T_{MA} in multipath channel ($L = 8$) and with CLPDI ($m = 2$) and without it.

The principal security properties compromised by such spoofing attacks are integrity and authenticity. Integrity, a fundamental cybersecurity principle, is breached when attackers manipulate GNSS signals to include false position or time data, leading to the receiver accepting altered information as accurate. This manipulation directly undermines the reliability of systems that depend on precise GNSS data. Similarly, authenticity, which verifies the legitimacy of communicating entities, is violated in spoofing attacks. Receivers are tricked into treating the falsified signals as if they were from genuine GNSS satellites, compromising the authenticity of the communication process.

These breaches have significant implications, particularly in critical applications where the accuracy of positioning and tim-

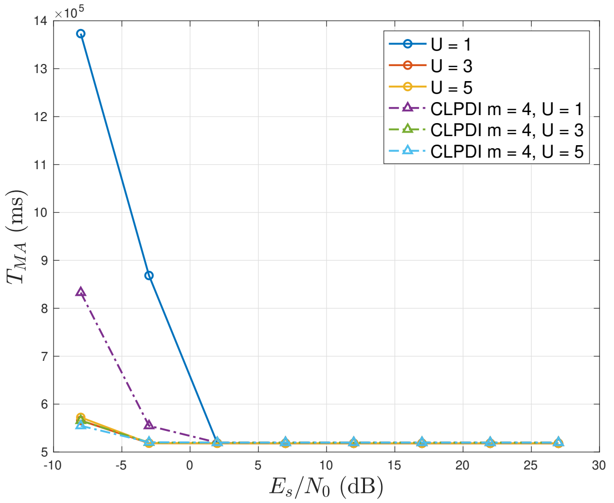

Fig. 10: T_{MA} in multipath channel ($L = 8$) and with CLPDI ($m = 4$) and without it.

ing data is paramount. The challenge posed by GNSS spoofing attacks to the integrity and authenticity of GNSS signals necessitates developing and implementing advanced detection and mitigation strategies. Ensuring the security of GNSS involves not only protecting data integrity and authenticity but also maintaining the trust and reliability of the diverse systems that rely on GNSS for operational functionality.

Detection and mitigation. In GNSS spoofing countermeasures, strategies are broadly delineated into detection and mitigation efforts, each playing a pivotal role in defending the integrity and functionality of GNSS-based systems against spoofing threats. Detection strategies focus on identifying spoofing signals and distinguishing fraudulent signals from legitimate GNSS transmissions. By analyzing signal characteristics such as power levels, signal-to-noise ratios, and the expected behaviour of satellite signals, these techniques enable the system to recognize the presence of spoofing attacks. Although detection does not stop an attack, it is an essential precursor to mitigation by alerting the system or users to potential security breaches.

After detecting a spoofing attack, mitigation efforts are employed to neutralize the threat and assist the affected receiver in regaining accurate positioning and navigational capabilities. Mitigation strategies may include signal processing techniques with sophisticated algorithms. The success of mitigation techniques heavily depends on the timely and accurate detection of spoofing, underscoring the interdependent nature of detection and mitigation in forming a comprehensive defence against spoofing activities.

However, it is crucial to repeat that these considerations apply to any spoofing attack on GNSS signals. Regarding the detecting capability of the proposed method to date, it is not possible to tell whether the attacker is using this technique that allows him to speed up the SCER attack.

Ethical aspects. Our research aims to report a new vulnerability for GNSS receivers widely deployed worldwide. The goal is to stimulate a discussion around SCER attacks to strengthen defences against adverse entities' exploitation of techniques such as the CLDPI algorithm. The proposed technique is entirely passive and can only be identified if the attacker's receiver is inspected. Knowing, however, that there are techniques that can speed up GNSS signal spoofing attacks, we are convinced that it is possible to act at the system level to include mechanisms that can make the use of CLPDI less effective. For example, such mechanisms may include new modulation techniques or cryptographic protocols with session keys that vary sufficiently fast.

VIII. Conclusions

This study marks a significant step in GNSS security research by demonstrating the efficacy of CLPDI in hastening spoofing attacks, unveiling a critical vulnerability that reduces the time for successful exploitation. Through a fusion of theoretical exploration and practical simulation, we meticulously evaluated the mean acquisition time (i.e., T_{MA}) and the probability of detection (i.e., P_d), uncovering the robustness of our method. Our experiments highlighted the power of CLPDI in enhancing the speed of SCER attacks within multipath fading channels, with a notable improvement in T_{MA} by 21.28%, significantly tilting the scales in favour of the attacker. The results described in this article will stimulate the conversation about defending GNSS against sophisticated cyber threats. It sets a precedent for developing advanced defensive mechanisms to ensure the fundamental integrity of satellite communications in our interconnected society.

References

[1] P. Tedeschi, S. Sciancalepore, and R. Di Pietro, "Satellite-based communications security: A survey of threats, solutions, and research challenges," *Computer Networks*, vol. 216, p. 109246, 2022.

[2] M. Giordani and M. Zorzi, "Non-terrestrial networks in the 6g era: Challenges and opportunities," *IEEE Network*, vol. 35, no. 2, pp. 244–251, 2021.

[3] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite communications in the new space era: A survey and future challenges," *IEEE Communications Surveys & Tutorials*, vol. 23, no. 1, pp. 70–109, 2021.

[4] X. Zhu and C. Jiang, "Integrated Satellite-Terrestrial Networks Toward 6G: Architectures, Applications, and Challenges," *IEEE Internet of Things Journal*, vol. 9, no. 1, pp. 437–461, 2022.

[5] J. Iinatti and M. Latva-aho, "A modified CLPDI for code acquisition in multipath channel," in *12th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications. PIMRC 2001. Proceedings (Cat. No.01TH8598)*, vol. 2, 2001, pp. F–F.

[6] S. Soderi, J. Iinatti, M. Hämäläinen *et al.*, "CLPDI algorithm in UWB synchronization," in *in Proc. 2003 Intl. Workshop on UWB Systems*, 2003, pp. 759–763.

[7] J. G. Proakis, *Digital communications*. Boston: McGraw-Hill, 2000.

[8] D. Spoljar, K. Lenac, D. Zigman, and M. Marović, "A Mobile Network-Based GNSS Anti-Spoofing," in *2018 26th Telecommunications Forum (TELFOR)*, 2018, pp. 1–3.

[9] L. Dobryakova, Ł. Lemieszewski, and E. Ochin, "Design and analysis of spoofing detection algorithms for GNSS signals," *Zeszyty Naukowe Akademii Morskiej w Szczecinie*, no. 40 (112, pp. 47–52, 2014.

[10] M. Lenhart, M. Spanghero, and P. Papadimitratos, "Distributed and mobile message level relaying/replaying of GNSS signals," in *Proceedings of the 2022 International Technical Meeting of The Institute of Navigation*, 2022, pp. 56–67.

[11] D. Marnach, S. Mauw, M. Martins, and C. Harpes, "Detecting meaconing attacks by analysing the clock bias of GNSS receivers," *Artificial Satellites*, vol. 48, no. 2, pp. 63–83, 2013.

[12] S. Jeong and J. Lee, "Synthesis algorithm for effective detection of GNSS spoofing attacks," *International Journal of Aeronautical and Space Sciences*, vol. 21, pp. 251–264, 2020.

[13] K. Sheridan, Y. Ying, and T. Whitworth, "Pre-and post-correlation GNSS interference detection within software defined radio," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, 2012, pp. 3542–3548.

[14] A. Elango, S. Ujan, and L. Ruotsalainen, "Disruptive GNSS Signal detection and classification at different Power levels Using Advanced Deep-Learning Approach," in *2022 International Conference on Localization and GNSS (ICL-GNSS)*, 2022, pp. 1–7.

[15] R. Ferre, "Analysis of GNSS replay-attack detectors exploiting unpredictable symbols," Ph.D. dissertation, PhD Thesis, 2018.

[16] T. E. Humphreys, "Detection Strategy for Cryptographic GNSS Anti-Spoofing," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 49, no. 2, pp. 1073–1090, 2013.

[17] G. Caparra, N. Laurenti, R. T. Ioannides, and M. Crisci, "Improving secure code estimate-replay attacks and their detection on GNSS signals," *Proceedings of NAVITEC*, vol. 2014, 2014.

[18] N. Flysher, R. Yozevitch, and B. Ben-Moshe, "GNSS denial of service and the preparation for tomorrow's threats," in *2016 IEEE International Conference on the Science of Electrical Engineering (ICSEE)*, 2016, pp. 1–5.

[19] D. Margaria, B. Motella, M. Anghileri, J.-J. Floch, I. Fernandez-Hernandez, and M. Paonni, "Signal Structure-Based Authentication for Civil GNSSs: Recent Solutions and Perspectives," *IEEE Signal Processing Magazine*, vol. 34, no. 5, pp. 27–37, 2017.

[20] M. Vekselman, "Security of GNSS-Based Synchronization Systems : Monitoring the quality of navigation systems," in *2022 Systems of Signal Synchronization, Generating and Processing in Telecommunications (SYNCHROINFO)*, 2022, pp. 1–4.

[21] J. M. Parro, J. A. Lopez-Salcedo, R. Ioannides, and M. Crisci, "Signal-level integrity monitoring metric for robust GNSS receivers," in *31st AIAA International Communications Satellite Systems Conference*, 2013, p. 5613.

[22] A. J. Garcia Peña, M. Aubault-Roudier, L. Ries, M.-L. Boucheret, C. Poulliat, and O. Julien, "Code Shift Keying: Prospects for Improving GNSS Signal Designs," *Inside GNSS*, vol. 10, no. 6, pp. 52–62, Nov. 2015.

[23] G. Caparra and N. Laurenti, "On the Use of CSK for GNSS Anti-Spoofing," in *2018 9th ESA Workshop on Satellite NavigationTechnologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, 2018, pp. 1–7.

[24] J. Iinatti, "Performance of DS code acquisition in static and fading multipath channels," *IEE Proceedings-Communications*, vol. 147, no. 6, pp. 355–360, 2000.

[25] M. Katz, "Code acquisition in advanced cdma networks," Ph.D. dissertation, University of Oulu, Faculty of Information Technology and Electrical Engineering; Centre for Wireless Communications, 2002.