Undercover Disruption: Stealth Jamming Attacks on 5G Synchronization Stages

Rosolino Alaimo[1,†], Roberto Corallo[1,†], Silvia Schilleci[1,†], Alessandra Dino[1,†], Stefano Mangione[1,3,†], Ilenia Tinnirello[1,3,†] and Domenico Garlisi[2,3,*,†]

[1]University of Palermo, Engineering Department, Palermo, Italy
[2]University of Palermo, Mathematic and Computer Science Department, Palermo, Italy
[3]CNIT, Parma, Italy

Abstract

This paper presents a comprehensive study on selective jamming, focusing on its impact on the synchronization phases of the 5G New Radio (NR). We introduce STORM, a novel framework tool designed to assess jamming attacks on the cell search phases of 5G User Equipment (UE). The research incorporates both simulation and experimental evaluations, providing a detailed account of the methodology employed. A unique aspect of the proposed approach is the implementation of a jamming technique that remains undetectable to external entities due to its synchronization with the gNB's Synchronization Signal Block (SSB). Furthermore, the implemented jamming operates at a duty cycle of 3.55% of continuous jamming, leading to significant optimization in terms of energy consumption and computational resources. STORM underscores that the success rate of jamming attacks and the necessary Signal to Interference Ratio (SIR) for effective disruption are significantly influenced by the specific configurations of the jamming signal. The paper discovers that the Primary Synchronization Signal (PSS) exhibits a higher degree of resilience compared to the Secondary Synchronization Signal (SSS), requiring a greater jammer transmission power to interfere with the cell search procedure.

Keywords

Selective Jamming, 5G, Jamming Attacks, User Equipment, 5G security, PSS, SSS

1. Introduction

5th Generation (5G) cellular systems are essential technologies supporting society with numerous services and applications, providing ultra-low latency, high-speed connections across a rapidly growing number of devices [1][2]. Due to their widespread use, commercial mobile communication networks are also susceptible to malicious attacks to access or to interfere with network operations. One of the most significant threats in this context is jamming, which consists in the transmission of a Radio Frequency (RF) signal to alter, or disrupt, a target signal, by reducing its Signal-to-noise Ratio (SNR) [3].

Recently, more sofisticate jamming techniques are represented from smart jamming attacks, they operate with low power, target selected devices and frequency bands [4]. In this work, we focus on smart jamming techniques that attack 5G physical network channels, specifically the Physical Broadcast Channel (PBCH) or the Physical Random Access Channel (PRACH), causing severe disruptions by blocking the access of User Equipment (UE) to the network, or preventing the periodical UE synchronization. In this context, the PBCH represents a target of the jamming attacks, as well as the 5G networks synchronization process. There are several kinds of jamming, such as delusive, random, responsive, go-next, or control channel jammers, according to the duty cycle of the injected signal, or if the jammer is synchronized with the 5G network, and whether it targets shared or dedicated channels [5].

In this article, we present STORM (Stealthy Timing Obstruction and Radio Assessment) framework. This framework is designed to explore the impact of covert jamming on the synchronization phases

Joint National Conference on Cybersecurity (ITASEC & SERICS 2025), February 03-8, 2025, Bologna, IT
*Corresponding author.
†These authors contributed equally.
rosolino.alaimo01@unipa.it (R. Alaimo); roberto.corallo@community.unipa.it (R. Corallo); silvia.schilleci@you.unipa.it (S. Schilleci); alessandra.dino01@unipa.it (A. Dino); stefano.mangione.tlc@unipa.it (S. Mangione); ilenia.tinnirello@unipa.it (I. Tinnirello); domenico.garlisi@unipa.it (D. Garlisi)

of 5G networks, with a particular focus on studying the effects of selective jamming in specific time and frequency domains. Our approach specifically targets Synchronization Signal Block (SSB), to jam the Primary Synchronization Signal (PSS) and Secondary Synchronization Signal (SSS) components, thus preventing UEs from completing the synchronization process. This precise and selective strategy maximizes the impact of the attack, minimizing power consumption and avoiding unnecessary interference. Furthermore, the attack remains hidden, as it does not introduce detectable changes in spectrum utilization, making it difficult to identify. The standard provides for an SSB boost; therefore, even if jamming is performed at higher power levels in a selective manner, it remains difficult to determine whether such selective jamming is actually present.

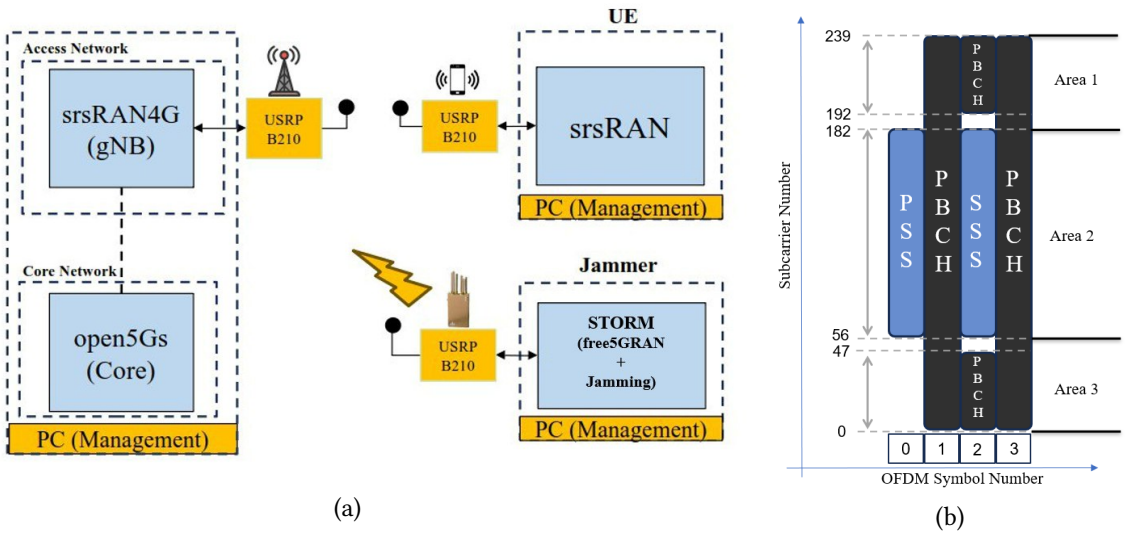


Figure 1: The architecture of the proposed system for study synchronized and hidden jamming in 5G NR (a). SSB symbols and subcarriers representation (b).

The system architecture, presented in Fig. 1a, shows the target scenario, it exploits open-source platforms to replicate a complete 5G scenario. Open5GS is used for the 5G core, srsRAN for the gNB and UE, finally, we extend the capabilities of free5GRAN[1] to implement the STORM framework. The gNB, UE, and jamming stations are individually associated with distinct Software Defined Radio (SDR) units. For the purpose of this experimental study, we have employed National Instruments' USRP (Universal Software Radio Peripheral) devices, opting specifically for the USRP-B210 model. Notably, free5GRAN is not inherently designed for jamming purposes, but just for the cell search phase. As part of this work, we developed and integrated STORM within free5GRAN, enabling it to perform and study hidden attacks selectively in time and frequency. This framework automatically extracts target cell parameters from broadcast channels and performs jamming attacks based on these parameters. We study the effect of the attack by analyzing the association phase of the UE under varying interference power and area. Moreover, our experimental evaluation is supported by simulated evaluation enforced with the MATLAB 5G toolbox[2].

More specifically, we consider a scenario where an adversary targets a 5G base station with a time-selective jamming attack aimed specifically at disrupting the SSB, while avoiding interference with other parts of the transmission. The attacker begins by listening to the broadcasted system information from the target 5G cell, extracting critical parameters like the periodicity and timing of SSB. Using this information, the attacker synchronizes with the base station frame structure to precisely time the jamming signal targeting only the SSB bursts. This selective targeting effectively blocks users from detecting and associating with the cell, disrupting network access. The technique presents key challenges such as ensuring precise timing synchronization, which is achieved by the implementation of a strictly time synchronization between the host and the radio. Detection is minimized because the

[1] https://github.com/free5G/free5GRAN
[2] https://it.mathworks.com/products/5g.html

attack affects only the SSB, while other parts of the transmission remain untouched, making it harder for network security to detect interference. Consequently, new device associations are prevented, denying service to users within the coverage area without affecting ongoing communications. The reduced transmission power also contributes to the difficulty for operators to detect and address the attack.

Background The 5G NR cell search procedure for a user, which involves signal detection and synchronization, laying the groundwork for understanding the subsequent communication procedures and jamming techniques. A device must perform a cell search to connect to a 5G cell. The first step of this process is to select the nearest cell that, typically, transmits stronger signals for that device. UE discards weaker signals and selects the strongest ones to ensure better Quality of Service (QoS). The cell search begins by detecting the SSB block, which is composed of three elements: PSS, SSS, and PBCH. As visible in Fig. 1b, they are mapped to 4 OFDM symbols in the time domain and 240 contiguous subcarriers (20 Resources Blocks) in the frequency domain [6].

During the cell search, PSS and SSS are used, respectively, for time and frequency synchronization. There are 3 different combinations for PSS and 336 for the SSS. With the first one we can obtain $N_{id}^{(2)}$, and $N_{id}^{(1)}$ with the second one. The UE extrapolates the Physical Cell ID (PCI) as:

$$PCI = 3N_{id}^{(2)} + N_{id}^{(1)}. \tag{1}$$

The PBCH, the third element of the SSB, contains the Master Information Block (MIB), which contains the common search space parameters needed to detect the System Information Block 1 (SIB 1), which itself carries the information needed to initiate a Random Access procedure. This process also supports mobility functions, such as handovers and cell reselection. Ultimately, the gNB assigns a Radio Network Identifier (RNTI) to the UE and supplies it with the essential parameters needed to decode Downlink Control Information (DCI). With this process complete, the UE is now registered and ready to exchange data with the network. For the initial synchronization process, the UE scans the possible frequencies where the SSB could be transmitted by the gNB, within the cell, called Global Synchronization Channel Numbers (GSCN). This process involves both PSS and SSS signals and is known as Synchronization Signal (SS) detection. Coarse time and frequency synchronization is performed by time-domain correlation between the received signal [7]-[8] and the 3 possible PSS sequences. The value of $N_{id}^{(2)}$ parameter is selected from the sequence that obtained the maximum correlation peak value. Subsequently, fine synchronization (and subsequent tracking of time and frequency errors) is performed by frequency domain correlation with the SSS sequences; again, $N_{id}^{(1)}$ is selected from the SSS sequence yielding the maximum correlation. Now, the UE can decode the PBCH, that contains the MIB. It provides information about the cell, such as the System Frame Number (SFN), Subcarrier Spacing (SCS), and the Common Search Space parameters required to search for the CORESET 0 (the first control channel message) and its associated shared channel message, the SIB 1, carrying the whole cell configuration parameters.

Main contribution In this work, we propose a methodology and an experimental evaluation to study how jamming attacks on cell search procedures can disrupt UE association process. The primary contribution of this paper is to offer a comprehensive investigation of these issues, evaluating the risks associated with jamming attacks on 5G NR cell search and synchronization phases, especially formulated from hidden jamming techniques. We demonstrate an integration of cell search and jamming functionality within the same framework. Our main contributions can be summarized as follows:

1. We demonstrate the integration of cell search and jamming functionalities within a unified framework. This allows the jammer to leverage extracted cell parameters, including the configurations of the PSS and SSS, to enable highly effective jamming strategies;
2. We demonstrate how high-performance covert jamming techniques, selective in time and frequency, can disrupt 5G synchronization phases. Furthermore, we investigate their impact across different areas of the SSB.

To validate our analysis, we conduct both simulations and real-world experiments. The structure is organized as follows: Section 2 revisits briefly the state-of-the-art time and frequency synchronization techniques of jamming attacks and their applications on Orthogonal Frequency Division Multiplexing (OFDM) systems and 5G networks; Section 3 defines our system framework; Section 4 summarizes the results of this work; Section 5 draws the conclusions.

2. Related Work

There are several types of jamming attacks targeting a 5G NR cell, depending on the specific physical channel being targeted: PBCH, Physical Downlink Control Channel (PDCCH), Physical Uplink Control Channel (PUCCH), or Physical Downlink Shared Channel/Physical Uplink Shared Channel (PDSCH/PUSCH). These attacks are designed to interfere with the broadcast, control, or data channels (both downlink and uplink) [9]. One of the most critical characteristics of an effective jammer is its high energy efficiency, which enables the creation of a low-cost device while maintaining a sufficient coverage range. To achieve this, a jammer can be specifically designed to target particular subcarriers of physical channels by fine-tuning key parameters such as central frequency, time synchronization, and bandwidth. In the remainder of this paper, we use the term 'time selective jammer' to refer to a jamming technique where the jamming duration is time-limited and overlaps with specific portions of the reference signal. Conversely, we use 'frequency selective jamming' to refer to the obstruction of only a subset of the subcarriers utilized by the modulation. Moreover, we will discuss about SSB jamming attack; our jammer is designed to attack PSS, SSS, and PBCH, before communication between gNB and UE can even begin. Due to the low Signal to Interference Ratio (SIR) of the received signal, UEs will be unable to decode PBCH and synchronize to the cell [10]. Also, jamming the SSs will cause already synchronized UEs to lose synchronization and disconnect.

Many studies have delved into strategies for executing synchronized attacks on wireless networks, each concentrating on various facets of time and frequency synchronization. Most of these studies are related to jamming in OFDM systems. [11] analyses attacks designed to compromise time synchronization during the signal acquisition phase. The authors focus on techniques such as the false preamble timing attack, which exploits knowledge of the preamble to introduce false peaks in the correlation phase.

A more comprehensive analysis of time and frequency synchronization is presented by the authors in [12], they focus on pilot tone attacks in MIMO-OFDM systems. This study shows that jamming synchronization in both domains (time and frequency) maximizes the effectiveness of the attack, while time or frequency mismatches significantly reduce the impact. For example, a temporal offset of 25% results in a loss of effectiveness of about 0.5 dB, while a normalized frequency offset of 0.5 can reduce jamming performance by up to 3 dB. This work emphasizes the importance of combined synchronization to ensure effective attacks. Instead, in [13] authors expand the focus on practical approaches to selective jamming in modern environments such as private 5G and NB-IoT networks. Here, the focus shifts to frequency synchronization to jam specific OFDM domain resources, such as pilot tones, while minimizing power consumption. The authors show how the use of targeted jamming signals can drastically reduce the accuracy of channel estimates, with a significant impact on the quality of service. Although time synchronization is less emphasized, the proposed selective approach represents an effective and discrete solution, suitable for advanced operational scenarios. These studies highlight complementary approaches to synchronization for jamming. The presence of only temporal synchronization is useful for attacks that aim to confuse temporal metrics, such as attacks on preambles. However, the integration of frequency synchronization allows for more sophisticated attacks, such as those on pilot tones or in selective jamming contexts, better suited to modern technologies. In contrast to the aforementioned works, our approach proposes the design of a jammer that synchronizes in both the time and frequency domains, allowing it to directly target the SSB.

Our method uniquely focuses on the PSS, SSS and PBCH within the SSB and produce selective jamming in time and frequency. This precise and selective strategy not only amplifies the effectiveness of the attack

while minimizing unnecessary interference but also makes the jamming virtually undetectable. The disruption remains concealed until the decoding process fails, ensuring the jamming blends seamlessly with standard signal activity, maintaining a covert and indistinguishable profile.

3. System architecture and characterization

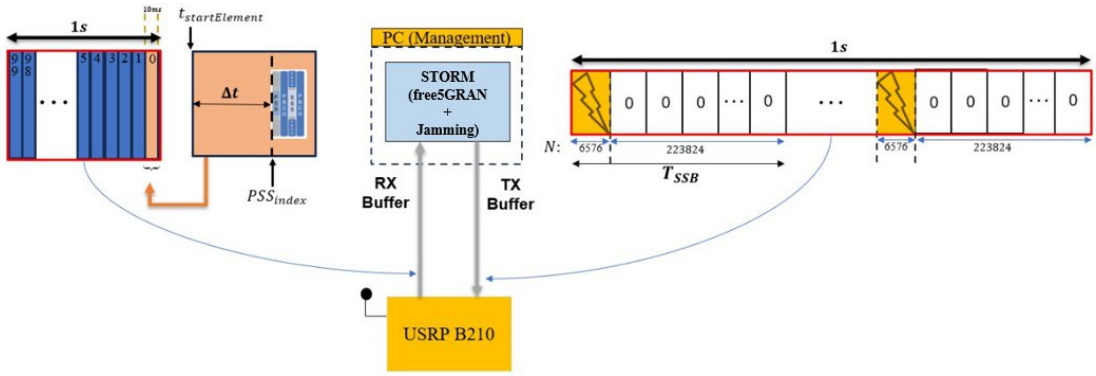


Figure 2: STORM's schematic representation of the RX and TX buffer implemented to receive and transmit signal on air.

Initially, we developed a continuous jammer tuned to the central frequency of the SSB with adjustable bandwidth, allowing us to assess the extent of synchronization disruption between the UE and gNB by targeting different portions of the SSB. Transitioning to free5GRAN, we successfully integrated both the cell search and jamming processes into a unified system, called STORM. This enabled us to extract critical parameters to ensure precise overlap between the extracted SSB signal and the transmitted jamming signal, both in time and frequency. During the cell search phase, the raw signals received over the air are stored in a Rx buffer composed of 100 elements. Each of the elements in the RX buffer contains $10ms$ of data received from the USRP-B210 (sampling rate set to $23.04MSs$), as shown in Fig. 2.

Buffer elements are processed in pairs, each corresponding to a $20ms$ trace, to ascertain the presence or absence of the SSB. This process is repeated iteratively until a gNB is successfully detected. Upon successful PBCH decoding and MIB extraction, critical parameters essential for ensuring an acceptable time synchronization between the jammer and the SSB can be obtained. By identifying the element in the RX buffer that contains the SSB, along with the first sample of the PSS, we can pinpoint the start of the entire SSB block. Each first sample of the received elements is associated with a timestamp derived from the USRP-B210 clock. This mechanism ensures an accurate estimation of the acquisition time for the first sample of each element in the RX buffer.

Based on this measurement, the time $PSS_{startTime}$ can be derived, representing the time interval between the reference time of the USRP-B210 and the start of the first element in the SSB block.

$$\Delta t = \frac{PSS_{index}}{SampleRate} \qquad PSS_{startTime} = t_{startElement} + \Delta t \tag{2}$$

By knowing the SSB period T_{SSB} ($10ms$ in our experimental setup), the first sample of the next SSB block can be determined by incrementing $PSS_{startTime}$ by multiples of T_{SSB}. The next step involves continuously monitoring the USRP-B210 timer and identifying the first available time instant to transmit the jamming signal, $NEXT\_PSS_{startTime}$ calculated as $PSS_{startTime}$ plus T_{SSB} or its multiples (Fig. 3a).

A circular temporal buffer, shown in Fig. 2, is created for the TX phase. This buffer will be used to transmit the jamming signal once the USRP timer reaches the value $NEXT\_PSS_{startTime}$. The TX buffer contains white noise samples to be transmitted at the appropriate moment during the subsequent jamming phase. The parameters required to construct the jammer signal were determined following the 3GPP standard[3].

The transmission buffer consists of $N = 23.04 \cdot 10^6$ samples. Therefore, with a sampling frequency of $f_s = 23.04$ MHz, the TX buffer is transmitted throughout one second and subsequently retransmitted cyclically. The samples in the buffer consist of white noise and are arranged to transmit four symbols during each T_{SSB} period as illustrated in Fig. 2.

According to the 3GPP standards, the number of samples per symbol is calculated as follows:

$$N_{symbol} = \frac{1}{SCS} \cdot (1 + \frac{9}{128}) \cdot f_s = 1644 \tag{3}$$

Finally, the number of samples required to transmit the four symbols of the SSB is $4 \cdot N_{symbol} = 6576$ or time duration of $274us$. During a T_{SSB} period, $N_{10ms} = \frac{f_s}{100}$ samples are transmitted. To achieve this, $4N_{symbol}$ samples of white noise are transmitted first, followed by $N_{10ms} - 4N_{symbol}$ samples set to zero. This process is repeated until the buffer is fully populated, as illustrated in Fig. 2.

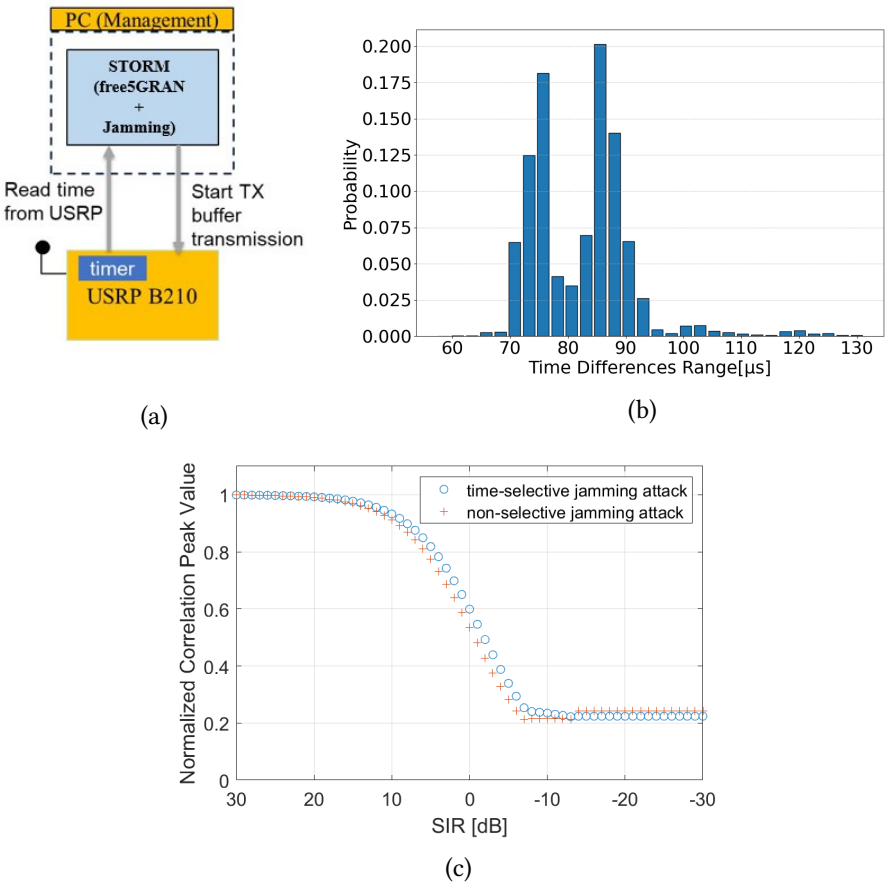


Figure 3: System representation of the USRP timer monitoring (a). Probability distribution of USRP response times for time reference requests (b). Result of jamming attack by using MATLAB 5G Toolbox simulation with and without time selectivity (c).

Characterization of the synchronization proposed scheme To ensure the precise alignment between the jamming signal transmitted by STORM and the SSB broadcast by the gNB, we considered

[3]https://www.etsi.org/deliver/etsi_ts/138200_138299/138211/16.02.00_60/ts_138211v160200p.pdf

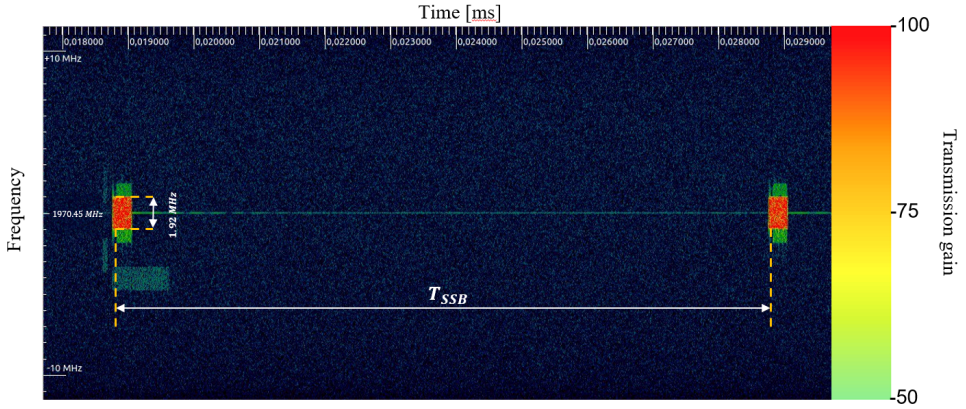


Figure 4: Spectral analysis with STORM active: the entire Area within the SSB block is completely jammed.

it essential to examine the system latency during the monitoring of the USRP timer. Consequently, we conducted an experimental evaluation to characterize the delay introduced by monitoring the USRP-B210 timer, and thus the delay in the process interaction between the host and the USRP device. We executed $100,000$ requests and derived the probability distribution of the response times. The histogram of this probability distribution is presented in Fig. 3b. The host system used is noted in the footnote[4]. The average response time is $81us$, for this reason we extend the duration of the noise signal to $355us(274 + 81)$ which represents the statistical uncertainty of the implemented system.

Finally, Fig. 4 shows the waterfall that demonstrates the effect of STORM in jamming the SSB signal.

Improvement due to the time-selective jamming We present now a discussion about the differences between a non-selective and a time-selective jamming attack. In particular, Fig.3c compares the impact of the two strategies on the correlation peak value for the SSS sequence during the synchronization process. The two methods are simulated through MATLAB 5G Toolbox. The SSB is produced, and a noise signal is subsequently introduced at the receiver side. Specifically, the first attack is simulated by adding to SSB a normalized white noise signal which covers all symbols and consequently includes also the PBCH subcarriers present at symbols 1 and 3 (see Fig.1b); in the second case, instead, the noise signal covers only symbol 0 and 2 and consequently the attack is performed only on PSS and SSS. As Fig.3c shows, the SSS correlation peaks go under 0.6 value when the SIR is lower than $1dB$ in the first case, and when the SIR is $0dB$ in the second case. So, we obtain the same effect on synchronization signals impairment but significantly reduced energy and computational efforts because we move from a 100% to 3.55% ($355us/10ms$) of duty cycle.

4. Experimental Evaluation

In this section, we showcase the outcomes of the time-selective jamming attack on a 5G network, we design an experimental setup involving three hosts, each equipped with an SDR device. These hosts represent the key components of the network: i) the gNB, this host implements the 5G base station, responsible for transmitting synchronization and control signals required for user association; ii) the UE, this host serves as the victim device attempting to connect to the gNB; iii) the attacker, this host acts as the adversary, generating a jamming signal to disrupt the synchronization process of the UE. The goal is to thoroughly investigate the influence imposed by an attack across distinct power levels and to examine the impact on various targeted SSB areas. The complete experimental setup is illustrated in Fig. 1a. The assessment employs a methodical approach through iterative experiments, systematically adjusting the jammer power and the SSB targeted region. We implement the following cycle:

[4]Operating System Linux Mint 21.3 Cinnamon v.6.0.4 - Kernel Linux 6.8.0-48-generic - Processor 13th Gen Intel© Core™ i9-13900x24 - RAM 32 GB

- Iterate Over Jamming Power Levels: The jammer transmission power is adjusted in one step, increasing the SDR gain from 60 dB to 80 dB. This allows us to measure the degradation in synchronization performance as the jamming power increases.
- Iterate Over Targeted SSB Areas: The attack is repeated for three different areas of the SSB, denoted as Area 1, Area 2, and Area 3, all visible in Fig. 1b. This helps determine if certain portions of the SSB are more resilient to jamming than others. Areas 1 and Area 3 correspond to the transmission bands of the PBCH, while Area 2 represents the transmission band of the PSS, SSS, and a portion of the PBCH. The 5G NR setup is configured to operate on the n2 band [14], with a frequency of 1970.45 MHz (we use zero numerology and so an SCS of 15 kHz, as specified by the 3GPP standards).

The experiment steps are as follows:

1. Activate the gNB to begin normal network operation.
2. Activate the jammer with the defined power level and area of attack.
3. Activate the UE, allowing it to attempt network discovery and association.
4. Monitor the UE state, evaluating whether the cell search and association process is successful.

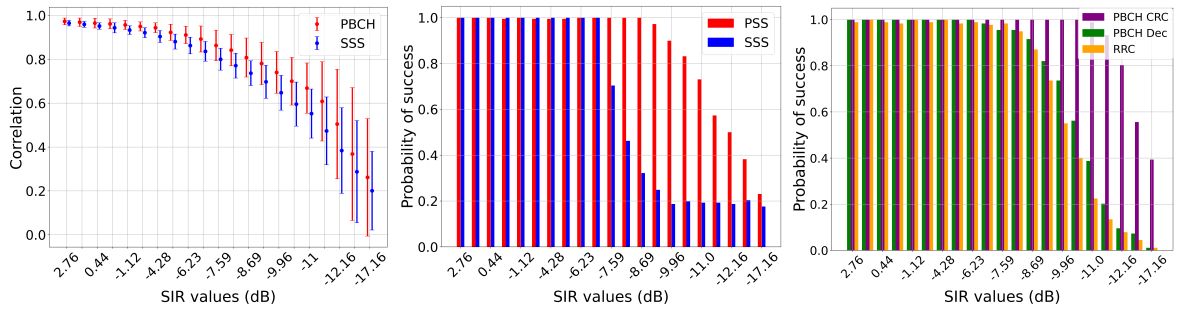
For each experiment, we monitor the success rate of the cell search and the network association process by monitoring the following parameters:

- PSS correlation: Measures how well the UE detects the PSS.
- SSS correlation: Evaluates the detection accuracy of the SSS.
- PSS decoding: Determines whether the UE successfully decodes the PSS.
- SSS decoding: Evaluate whether the SSS is correctly decoded.
- PBCH Decoding: Measures the success of PBCH decoding.
- PBCH CRC: Indicates whether the CRC for the PBCH is successfully extracted.
- RRC Association: Determines whether the RRC association is established, indicating a successful connection to the network.

The data collected for each iteration is reported in terms of the SIR, which is calculated as the ratio between the UE signal power and the jammer signal power. To derive the SIR, we considered STORM configurations with transmission gain values spanning between a transmission gain of 60 db and 80 db. After the cell search phase, STORM can be configured to the same central frequency for transmitting white noise samples, maintaining a bandwidth of 1.92 MHz. To target specific areas, an offset is applied to the jamming signal relative to the central frequency. Consequently, an offset of 1.92 MHz is set for Area 1, 0 MHz for Area 2, and -1.92 MHz for Area 3.

Each experiment targeting the three different areas was repeated 100 times. We report the average correlation values for the SSS, along with the probability of success based on the combined PSS and SSS correlations, and the probability of correctly decoding the PBCH. Furthermore, we outline three distinct results for accurate decoding of the PBCH. The first result is the full decoding, labeled as PBCH Decoded probability; The second involves the verification of the CRC, labeled as the PBCH CRC probability; and the final result is the comprehensive process where the Radio Resource Control (RRC) is successfully extracted. The experiments were conducted in a semi-anechoic chamber under controlled conditions to eliminate interference from other active UEs on the network. In this setup, the UE is positioned 150 cm from the gNB, while STORM is placed between the gNB and the UE, with a distance of 50 cm from the UE and 100 cm from the gNB. Data collected from the experiments, obtained during the attempet of the synchronization phases, allowed us to analyze how STORM's configuration impacts the correlation parameters of the PSS, SSS, and PBCH. Specifically, we present the probability of success as a function of the SIR values of the UE.

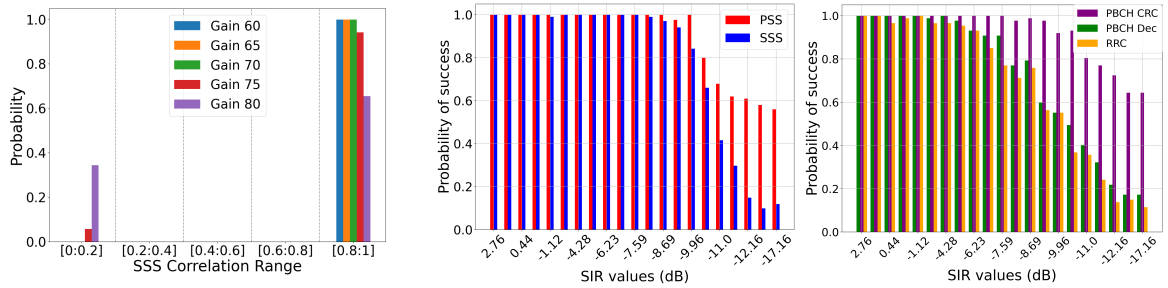
Fig. 5 illustrates the attack executed by STORM on Area 2. This attack targets solely the 128 subcarriers that constitute Area 2. As a result, in this configuration, the PSS and SSS are completely disrupted, while the PBCH is partially corrupted. Fig. 5a represents the outcomes of the correlation process. It



(a) (b) (c)

Figure 5: Experimental scenario involves interference of our UE in AREA 2: Correlation graph of SSS and PBCH (a); Probability of successful correlation for PSS and SSS (b); Probability of successful PBCH decoding, PBCH CRC and RRC connection (c).

can be observed that the correlation results for both PBCH and SSS decrease as the STORM's power is increased and the SIR decreases. To obtain all the normalized correlation values, we had to modify the srsRAN application, as it did not normalize the obtained values. In particular, Fig. 5b shows the success probability with which the PSS and SSS are obtained. Considering that the PSS can have only three distinct values, which allow the extraction of N_{ID}^2, while the SSS provides 336 values of N_{ID}^1, it is more likely to obtain the PSS than the SSS. Furthermore, it can be observed that the PSS has greater robustness compared to the SSS, requiring higher transmission power to disrupt the UE's cell search procedure. As a result, it is necessary to increase STORM's transmission gain to interfere more effectively with the PSS. Fig. 5c illustrates that as the transmission gain of STORM increases, the probability of successfully decoding the PBCH decreases, thereby reducing the likelihood of establishing the RRC connection, crucial for determining whether the UE has successfully synchronized with the gNB.

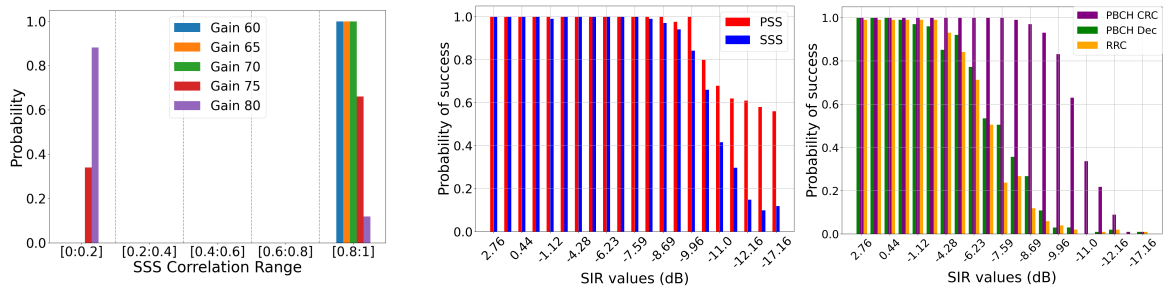


(a) (b) (c)

Figure 6: Experimental scenario involves interference of our UE in AREA 1: SSS correlation analysis with varying transmission gains (a); Probability of successful correlation for PSS and SSS (b); Probability of successful PBCH decoding, PBCH CRC and RRC connection (c).

Fig. 6 illustrates the attack executed by STORM on Area 1. This attack targets only the PBCH region. Fig. 6a illustrates four distinct regions, each corresponding to specific correlation values calculated for the SSS. Each correlation value is associated with a probability that represents its relative frequency of occurrence within the respective regions. Furthermore, the graph features five bars of different colors, each representing the probability that the SSS correlation assumes a given value in 100 experiments conducted with five different transmission gains: blue for a transmission gain of 60, orange for 65, green for 70, red for 75, and purple for 80. Fig. 6b shows that as the SIR decreases, the probability of correctly detecting the PSS and SSS declines. This can be attributed to the focus of the analysis on Area 1, where only the PBCH is present. However, as illustrated in Fig. 6c, the probability of a successful RRC drops significantly, despite the inherent robustness of the PSS and SSS. This occurs because, under the application of our STORM framework in Area 1, the PBCH is degraded to the point where it becomes undecodable by the UE, resulting in a loss of critical parameters required for the

configuration and synchronization of the UE with the gNB.



(a) (b) (c)

Figure 7: Experimental scenario involves interference of our UE in AREA 3: SSS correlation analysis with varying transmission gains (a); Probability of successful correlation for PSS and SSS (b); Probability of successful PBCH decoding, PBCH CRC and RRC connection (c).

Fig. 7 illustrates the attack executed by STORM on Area 3. How presented for the Area 1, Fig. 7a illustrates four distinct regions, each correlation value is associated with a probability that represents its relative frequency of occurrence within the respective regions. Despite the attack on Area 3, Fig. 7b reveals that the probability of detecting PSS and SSS progressively decreases as the SIR decreases. Furthermore, Fig. 7c illustrates that the probability of establishing an RRC connection remains notably low at higher SIR values compared to those observed during the attacks on Area 1 and Area 2. Fig. 6 and Fig. 7 offer compelling visualizations of the jamming attack on AREA 1 and AREA 3, respectively. These areas represent the segments where the PBCH resides, with no interference on the PSS and SSS. In both illustrations, it is noticeable that the RRC becomes non-functional with SIR under -9 dB and -7 dB for the AREA 1 and AREA 3 respectively, despite the PSS and SSS maintaining high correlation levels. This is due to the PBCH being so heavily corrupted that the UE can't retrieve the correct MIB after decoding the PBCH, preventing it from synchronizing with the gNB. This suggests that jamming the PBCH requires significantly less jammer transmission power compared to the power needed to disrupt the SSS or, in particular, the PSS.

5. Conclusion

In conclusion, this study explored selective jamming (in terms of time and frequency) and offered an in-depth analysis of how various jamming configurations affect different components of the 5G NR synchronization phases. We developed STORM, a framework tool designed to evaluate jamming attacks on 5G UE cell search phases. A key aspect of our implementation is that the jamming is concealed from detection by external entities due to its synchronization with the gNB's SSB. We conducted both simulations and experimental evaluations, each accompanied by a comprehensive explanation of the methodology used. The findings emphasized that the success rate of jamming attacks and the necessary SIR for effective disruption are contingent on the specific configurations of the jamming signal. The study showed that the PSS demonstrated more resilience than the SSS, which required higher jammer transmission power to disrupt the cell search process. Furthermore, the research highlighted that interference in an area where only PBCH was present resulted in complete disruption of the PBCH decoding and RRC extraction, with a SIR of -9 dB and -7 dB for the AREA 1 and AREA 3 respectively. Finally, the paper shows that selective jamming improves energy efficiency and computational efficiency because it reduces the jamming duty cycle to 3.55%.

Acknowledgments

This work was partially supported by the European Union - Next Generation EU under the Italian National Recovery and Resilience Plan (NRRP), Mission 4, Component 2, Investment 1.3, CUP

E83C22004640001, CUP E63C22002070006, CUP F83C22001690001, and CUP B53C22004050001, partnership on “Telecommunications of the Future”, PE00000001 - program “RESTART”, and Investement 7 PE00000014 - CUP D33C22001300002, program SERICS.

Declaration on Generative AI

During the preparation of this work, the author(s) used ChatGPT, Grammarly in order to: Grammar and spelling check, Paraphrase and reword. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication’s content.

References

[1] K. G. Eze, M. N. Sadiku, S. M. Musa, 5g wireless technology: A primer, International Journal of Scientific Engineering and Technology 7 (2018) 62–64.

[2] I. Parvez, A. Rahmati, I. Guvenc, A. I. Sarwat, H. Dai, A survey on low latency towards 5g: Ran, core network and caching solutions, IEEE Communications Surveys & Tutorials 20 (2018) 3098–3130.

[3] H. Pirayesh, H. Zeng, Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey, IEEE Communications Surveys & Tutorials 24 (2022) 767–809. doi:10.1109/COMST.2022.3159185.

[4] F. Girke, F. Kurtz, N. Dorsch, C. Wietfeld, Towards resilient 5g: Lessons learned from experimental evaluations of lte uplink jamming, in: 2019 IEEE International Conference on Communications Workshops (ICC Workshops), IEEE, 2019, pp. 1–6.

[5] Y. Arjoune, S. Faruque, Smart jamming attacks in 5g new radio: A review, in: Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 2020, pp. 1010–1015. doi:10.1109/CCWC47524.2020.9031175.

[6] X. Lin, et al., 5g new radio: Unveiling the essentials of the next generation wireless access technology, IEEE Communications Standards Magazine 3 (2019) 30–37. doi:10.1109/MCOMSTD.001.1800036.

[7] D. Inoue, K. Ota, M. Sawahashi, S. Nagata, Physical cell id detection using joint estimation of frequency offset and sss sequence for nr initial access, in: Proceedings of the 2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring), Helsinki, Finland, 2021, pp. 1–6. doi:10.1109/VTC2021-Spring51267.2021.9448662.

[8] A. Ali, M. Elsaadany, G. Gagnon, Performance of time and frequency approaches for synchronization tracking in 5g nr systems, in: Proceedings of the 2021 International Symposium on Networks, Computers and Communications (ISNCC), Dubai, United Arab Emirates, 2021, pp. 1–6. doi:10.1109/ISNCC52172.2021.9615890.

[9] M. E. Flores, D. D. Poisson, C. J. Stevens, A. V. Nieves, A. M. Wyglinski, Implementation and evaluation of a smart uplink jamming attack in a public 5g network, IEEE Access (2023).

[10] S.-D. Wang, H.-M. Wang, W. Wang, V. C. M. Leung, Detecting intelligent jamming on physical broadcast channel in 5g nr, IEEE Communications Letters 27 (2023) 1292–1296. doi:10.1109/LCOMM.2023.3260194.

[11] M. J. L. Pan, T. C. Clancy, R. W. McGwier, Jamming attacks against ofdm timing synchronization and signal acquisition, in: MILCOM 2012 - 2012 IEEE Military Communications Conference, 2012, pp. 1–7. doi:10.1109/MILCOM.2012.6415749.

[12] C. Shahriar, S. Sodagari, T. C. Clancy, Performance of pilot jamming on mimo channels with imperfect synchronization, in: 2012 IEEE International Conference on Communications (ICC), 2012, pp. 898–902. doi:10.1109/ICC.2012.6364202.

[13] P. Skokowski, K. Malon, M. Kryk, K. Maślanka, J. M. Kelner, P. Rajchowski, J. Magiera, Practical trial for low-energy effective jamming on private networks with 5g-nr and nb-iot radio interfaces, IEEE Access 12 (2024) 51523–51535. doi:10.1109/ACCESS.2024.3385630.

[14] ShareTechnote, 5g frequency range and bandwidth, https://www.sharetechnote.com/html/5G/5G_FR_Bandwidth.html, 2024.