SigUnder: a Stealthy 5G Low Power Attack and Defenses

Norbert Ludant
ludant.n@northeastern.edu
College of Computer Sciences, Northeastern University

Guevara Noubir
g.noubir@northeastern.edu
College of Computer Sciences, Northeastern University

ABSTRACT

The 3GPP 5G cellular system is hailed as a major step towards more ubiquitous and pervasive communications infrastructure (including for V2X, Smart Grid, and Healthcare). We disclose and evaluate SigUnder, an attack that enables an adversary to overshadow the Signal Synchronization Block (SSB) with an injected signal at 3.4dB below the legitimate signal (prior work required 3dB above). The attack exploits the polar coding mechanism of 5G and the physical layer OFDM structure. It can be used to make previous DoS and over-shadowing attacks lower-power and stealthy, but also enables new attacks unique to 5G such as setting the cellBarred field in the 5G MIB (and blocking access to a cell). We develop techniques (e.g., phase prediction) to make the attack feasible in a practical setup, and evaluate its performance both in simulations and over the air experiments. We also introduce SICUnder, an extension of Successive Interference Cancellation (SIC) to be able to address the unique challenges that SigUnder poses and demonstrate it effectiveness relatively to standard SIC.

CCS CONCEPTS

• **Networks** → **Mobile and wireless security**; **Denial-of-service attacks**; *Wireless access points, base stations and infrastructure*; **Network security**; Network reliability.

KEYWORDS

wireless communications, 5G, synchronization signals, wireless security, denial of service

ACM Reference Format:
Norbert Ludant and Guevara Noubir. 2021. SigUnder: a Stealthy 5G Low Power Attack and Defenses. In *14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21), June 28-July 2, 2021, Abu Dhabi, United Arab Emirates.* ACM, New York, NY, USA, 11 pages. https://doi.org/10.1145/3448300.3467817

1 INTRODUCTION

Wireless communications revolutionized where, when, and how we communicate and access information and services. The 3GPP 5G cellular system is hailed as a major step towards more ubiquitous and pervasive communications infrastructure. It is indeed flexible and extensible, with slices to support a variety of unique applications requirements, from Massive IoT (MIoT), Ultra-Reliable Low-Latency Communications (URLLC), to enhanced Mobile Broadband (eMBB), and massive Machine Type Communications (mMTC), as well as specific industry requirements such as V2X, Smart Grid, and Remote Healthcare [5, 10]. This capability to address unique needs, along with the redesign around Service Based Architecture, and Network Functions Virtualization is very promising to adequately support a larger number of applications including critical ones such as self-driving cars, robotics, and remote surgeries [12, 20, 37].

Cellular systems, however have a history of security, privacy, and robustness issues since their second generation (GSM) that took security and privacy more seriously. Over the years, researchers were able to demonstrate attacks against every generation of cellular systems from 2G to 4G, by preying on design, implementation, and operation flaws. For instance, that it is possible to clone SIM cards [14], decrypt traffic [33], track users [21–23, 40], DNS spoofing [32], conduct denial of service attacks [25–27, 34], downgrade to insecure versions [34], reinstall old keys [36], and inject malicious messages by over-shadowing legitimate signaling [18, 39].

One of the promises of the 3GPP 5G efforts is to increase security, privacy, and robustness. Towards this goal, 5G introduced the Subscriber Concealed Identity (SUCI), encrypting the Subscriber Private Identity (SUPI) to prevent sending it in the clear, therefore defend against tracking of users. New slice authentication mechanisms were introduced, as well as support for false base-station detection [9]. Robustness to DoS attacks was improved through the use of (capacity achieving) polar codes with very low coding rate (e.g., the 24 bits Master Information Block (MIB) is encoded into a codeword of 864 bits). However, 5G is still designed to streamline discovery and initiate connection with limited computation and communications cost. This has significant implications for robustness, security, and privacy, as the predictability of control-channel is an enabler of wireless attacks [15]. Furthermore, initial access signals are still unprotected, which allows the existence of rogue base stations. As we will discuss and demonstrate in this paper, the introduction of polar code to increase the robustness of the Synchronization Signal Block enables a new form of smart attacks.

In this work, we investigate the possibility of injecting signals at low-power that achieve a stealthy under-shadowing attack (denoted by SigUnder) that successfully replaces the legitimate 5G base station (gNB) SSB with the attacker's one. General signal manipulation were studied demonstrating their potential feasibility under assumptions of controlled amplitude and carrier phase delay of the attacker to closely match the legitimate signal at the receiver [31]. Our exploitation of the OFDM and polar codes structure, as well as phase tracking enable us to develop a specialized and successful attack against 5G SSB in over-the-air communications, with signals that are even weaker than the legitimate ones thanks to selective targeting of sub-carriers and polar codewords. We show that an adversary can achieve this attack while being up to 3.4dB below the legitimate signals. These attacks are 15dB

WiSec '21, June 28-July 2, 2021, Abu Dhabi, United Arab Emirates

ACM ISBN 978-1-4503-8349-3/21/06…$15.00
https://doi.org/10.1145/3448300.3467817

below a Gaussian jammer and several orders of magnitude more efficient than a continuous jammer. The underlying idea is that the adversary can predict SSB OFDM symbols, can search for polar codewords with high-similarity to the legitimate one, and focus its energy on transmitting only on sub-carriers where the malicious SSB differs from the legitimate one. This transmission power on these sub-carriers only needs to be at a power level barely above the legitimate one. Thanks to the energy in the untouched sub-carriers and to the polar code powerful error-correction capability (low-rate), the UE ends-up decoding a Master Information Block (MIB), contained in the SSB as intended by the attacker. The attack exploits the fact that polar code are capacity achieving against Gaussian noise but not against a smart adversary. The `SigUnder` attack enables the adversary to inject crafted broadcast signals similar to the `SigOver` attack [39], but with 6.8dB less powerful emissions and not requiring to transmit a complete subframe (only 3 OFDM symbols), and therefore significantly more stealth. It also enables new attacks against information introduced in the 5G MIB, such as preventing access to a cell (`cellBarred` field), preventing cell re-selection (`intraFreqReselection` field), or forcing UEs to transmit at higher power (`preambleReceivedTargetPower` in SIB1) and therefore enabling their localization. In our analysis and experimental evaluation, we show that while time-synchronization is not a challenge, thanks to the long OFDM symbols and Cyclic Prefix (CP) duration, conducting the attack requires a careful tracking of the phase between the adversary and the gNB. We demonstrate that a phase tracking and prediction algorithm leads to a successful attack in both simulation and over the air experiments, using the Open Air Interface 5G gNB. The essence of the attack is due to a capture effect (the first SSB decoded is used). We introduce and evaluate a mitigation technique based on an extension of Successive Interference Cancellation (SIC). We note that our basic SIC technique mitigates classic over-shadowing attacks, but our subcarrier-selective attack requires a carefully optimized reconstruction of the legitimate signal. Our contributions can be summarized as follows:

- We devise an attack that overshadows the 5G SSB by transmitting a signal at a lower power than the legitimate gNB by exploiting the capacity-achieving error-correcting capabilities of polar codes, and the OFDM structure of 5G.
- We propose techniques to overcome the technical challenges that arise from performing the attack in real scenarios, i.e. phase and time misalignments.
- We demonstrate the complete on over the air channel conditions and overshadow the legitimate SSB by transmitting at 3.4dB power below the legitimate SSB.
- We demonstrate that traditional Successive Interference Cancellation (SIC) techniques are not effective mitigations, then propose and evaluate a new defense, `SICUnder`.

2 5G BACKGROUND

In this section, we describe key aspects of 5G New Radio (NR) Physical Layer, synchronization signals and initial access procedure relevant to the introduced attack and defenses [1–4, 6–8]. We focus on describing the crucial mechanisms and procedures that enable attacks on network availability.

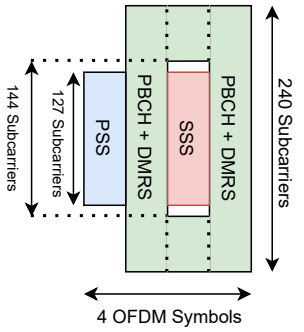


Figure 1: Synchronization Signal Block

2.1 Physical Layer

5G NR Physical Layer is an evolution of the LTE physical layer, sharing multiple common aspects. Most importantly, the same waveform, Cyclic Prefix - Orthogonal Frequency-Division Multiplexing (CP-OFDM), was chosen for 5G NR due to its low complexity and robustness against Doppler and phase noise effects.

5G inherits the frequency domain units and frame structure from LTE, with modifications to account for 5G diverse use cases. For instance, 5G contemplates very low latency requirements, which can be met through adaptations in the physical layer. Furthermore, due to the incorporation of high frequency communications, 5G also supports a wide range of frequency bands, grouped in Frequency Range 1 (FR1) for $f_c < 6GHz$, and Frequency Range 2 (FR2), for $f_c > 6GHz$. We focus our study only on the former, FR1.

In the frequency domain, whereas LTE has a fixed subcarrier spacing (Δf) of 15KHz, in 5G subcarrier spacing is configurable based on a parameter termed numerology, μ. Thus, Δf in 5G ranges from 15 KHz to 480 KHz scaling with numerology such as $\Delta f = \mu \cdot 15$ KHz where $\mu = 0 - 5$. Only 15, 30 and 60 KHz spacings are available for FR1. To facilitate initial access, only a subset of configurations are available for synchronization signals, 15 and 30 KHz subcarriers spacings with normal CP for sub-6GHz communications.

In the time domain, 5G NR frame structure remains similar to LTE; each frame is divided in 10 subframes, divided in slots containing OFDM symbols. Frame and subframe lengths are 10ms and 1ms respectively, and the number of OFDM symbols per slot remains constant, 14 symbols per slot for normal Cyclic-Prefix (CP) and 12 for extended CP, compared to 6 or 7 for LTE. As OFDM symbols are constant per slot, slot length has to scale -inversely- with the numerology. In this way, number of slots per subframe follows the equation $N_{slots} = 2^{\mu}$, and time duration of a slot $T_{slot} = 1/2^{\mu}(ms)$. For instance, for $\mu = 0$, there is 1 slot of 1ms per subframe, 2 slots of 0.5ms per subframe for $\mu = 1$ or 8 slots of 0.125 ms for $\mu = 3$.

Note that a 30KHz subcarriers spacing results in OFDM symbols duration of $33\mu s$, and a CP of $2.34\mu s$, reduces the impact of Inter-Symbol Interference (justifying the popularity of OFDM), but also reduces the challenge of time synchronization for an adversary.

2.2 Synchronization Signal Block (SSB)

5G uses a reduced set of always-on signals for initial access, grouped in what is called Synchronization Signal Block (SSB). This block

consists of Primary Synchronization Signal (PSS), Secondary Synchronization Signal (SSS), Physical Broadcast CHannel (PBCH), and PBCH DeModulation Reference Signal, (PBCH-DMRS). SSB is transmitted in 4 contiguous OFDM symbols across 240 subcarriers as shown in Figure 1. For initial cell selection, the UE assumes a 20 ms SSB periodicity. Multiple SSBs can be transmitted within a frame if beamforming is enabled. Each SSB is transmitted with different beam coefficients and is identified by a SSB Index. A receiver identifies the strongest beam by decoding each SSB. We will focus on a single SSB transmission for SSB description.

2.2.1 Synchronization Signals. As in LTE, PSS and SSS are used for initial time and frequency synchronization, as well as Physical Cell ID (PCI) computation. In 5G NR, PSS is a BPSK modulated m-sequence of length 127, generated from Cell ID sector, $N_{ID}^2 = 0 - 2$, and it occupies the first OFDM symbol in SSB. SSS is one of 336 possible BPSK modulated Gold Sequences, generated using the Cell ID Group $N_{ID}^1 = 0 - 335$. SSS shares the third OFDM symbol with PBCH/PBCH-DMRS. The combination of Cell ID group and sector creates a total of 1008 possible PCI, $N_{ID}^{CELL} = 3N_{ID}^1 + N_{ID}^2$.

2.2.2 Physical Broadcast CHannel-Demodulation Reference Signal (PBCH-DMRS). PBCH-DMRS is a QPSK modulated m-sequence, spanning 144 QPSK symbols. PBCH-DMRS is generated from various initialization values, Physical Cell ID, Half Frame, and SSB Index. PCI also determines the position of PBCH-DMRS subcarriers within the SSB, distributed across symbols 2 to 4. The role of Half Frame and SSB Index will be discussed more in depth in Section 2.3. The purpose of PBCH-DMRS is to identify the time pattern of SSB and serve as pilots for channel estimation for PBCH.

2.2.3 Physical Broadcast CHannel (PBCH). PBCH carries the Master Information Block (MIB), which contains crucial network configuration information, details are described in Section 2.4. One of the main novelties in 5G NR is the introduction of Polar Coding channel coding for control channels. Polar codes are recently discovered codes, designed from information theoretic principles, and have recently become popular due their provable capacity achieving property for various channels, and their efficient encoding/decoding algorithms ($O(n\log(n))$ [11, 13, 16, 35]. The use of very low-rate Polar Coding for PBCH further increases the robustness against noise and interference. However, such codes are not designed to protect smart adversary as we will show in later sections. Other new information incorporated in the MIB include a `cellBarred`, and `intraFreqSelection` fields.

The encoding steps from MIB to PBCH symbols are depicted in Figure 2. In a nutshell, PBCH encapsulates the Broadcast CHannel (BCH), which contains 23 bits from MIB plus one bit indicating the presence of MIB. PBCH appends 8 extra bits of information, 3 bits for System Frame Number 3 LSB, 4 for SSB Index and 1 bit for Half Frame Indicator). PBCH 32 bits are interleaved and scrambled with a scrambling sequence which depends on SFN and PCI. After adding a 24-bit CRC, 56 bits are input to the polar encoder. The 512 output bits are followed by a rate matching block that outputs the final 864 bits for PBCH. The 864 PBCH bits are QPSK modulated resulting in 432 symbols mapped to OFDM symbols 2, 3 and 4 of SSB. This coding rate, mapping 24 bits into 864 bits, is very low and intended to make it hard to selectively tamper with the MIB.

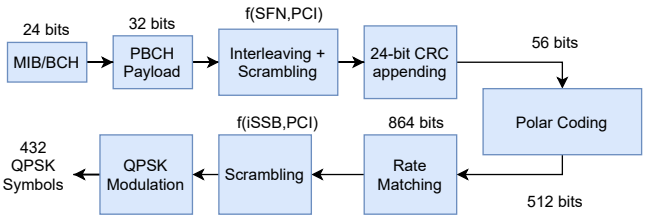


Figure 2: PBCH Encoding Block Diagram

2.3 5G Initial Access Procedure

When a 5G capable device first powers on or tries to connect to a network, it follows a well-defined sequence of procedures to access the network. Note that if any of the initial access steps fail, a device is unable to connect to the network, hence the emphasis on sequences with excellent correlation properties and the addition of robust channel coding for broadcast information.

2.3.1 Cell Search. Cell search consists of time and frequency synchronization and obtaining the cell PCI. The device relies on both PSS and SSS signals for this end. Although specific algorithms for time and frequency offset estimation are not described in the standard, a common approach in the literature is the use of correlation algorithms [30]. In this way, a device searches for the PSS by correlating in the time domain with the three possible PSS sequences. Finding a valid PSS provides coarse frequency and time offset estimation, as well as the Cell ID sector N_{ID}^1. Afterwards, the receiver can retrieve the resource grid after aligning the SSB. In a similar fashion, by computing the cross correlation in frequency domain, the Cell ID group N_{ID}^2 and consequently the PCI can be obtained.

2.3.2 PBCH decoding. After initial synchronization, the receiver extracts the PBCH-DMRS symbols and computes all possible PBCH-DMRS sequences for i_{SSB} based on PCI. Maximum correlation peak would indicate the SSB index and Half Frame bits. Channel and noise estimation for PBCH decoding is performed based on PBCH-DMRS. After channel equalization of PBCH QPSK symbols, UE decodes MIB from PBCH following the inverse procedure of Figure 2.

2.3.3 System Information Block 1 decoding. MIB indicates the frequency and time resources where System Information Block 1 is transmitted. SIB1 is necessary for cell access, as it carries crucial information for the UE, such as random access configuration and thresholds for minimum measured channel quality and received power. If an UE meets the criteria to access the network, it will proceed by performing random access procedure.

2.4 Minimum System Information

Initial access to the network depends on a set of information broadcast by the gNB. The most important blocks of information are MIB and SIB1, referred together as Minimum System Information (MSI).

MIB consists of 23 bits, divided in 8 fields as described in Table 1. `systemFrameNumber` field includes the 6 MSB bits of the System Frame Number, whereas the remaining 4 bits are included during PBCH encoding as part of channel coding. `subCarrierSpacing Common` indicates the subcarrier spacing used for system information messages and paging, 15 or 30 for FR1 and 60 or 120 for

Field name	Size (bits)
systemFrameNumber	6
subCarrierSpacingCommon	1
ssb-SubcarrierOffset	4
dmrs-TypeA-Position	1
pdcch-ConfigSIB1	8
cellBarred	1
intraFreqReselection	1
spare	1

Table 1: Master Information Block (MIB) Contents in 5G

FR2. `ssb-SubcarrierOffset` is used to determine where the data resource grid starts using SSB frequency position as reference. `dmrs-typeA-position` can take values `pos2` or `pos3` and indicates the position of DMRS for physical shared channels. `pdcch-ConfigSIB1` configures which time and frequency resources the UE needs to listen to to retrieve SIB1. `cellBarred` indicates whether UEs are allowed to select this cell. This field was moved from SIB1 in LTE to MIB in 5G. Lastly, `intraFreqReselection` bit indicates if intra-frequency cell selection is allowed when a cell is barred. Tampering with these bits can therefore permit new attacks since the only integrity protection of the MIB is the low-rate polar coding.

System Information Block 1 includes the remaining system information required to establish a connection with the core network. This includes information regarding cell selection parameters, RSRP, RSRQ, cell access information, or random access parameters, e.g. maximum preamble power, response window or random access occasions. Furthermore, SIB1 carries information regarding scheduling of other System Information Blocks (2-9).

3 SigUnder: SUBCARRIER SELECTIVE OVERSHADOWING

In this section, we present our subcarrier-selective overshadowing attack, `SigUnder`. `SigUnder` can be used as a low-power spoofing attack (overshadowing) of network broadcast information. The attack leverages the peculiarities of the Synchronization Signal Block, focusing on making the attack energy efficient and stealthy, as it requires less transmit power than the legitimate gNB transmissions. We present the attack technical details as well as the challenges and techniques developed in order to demonstrate a successful attack.

3.1 Models

3.1.1 Communication model. We assume a wireless cellular model where a 5G base station (gNB) operates at a FR1 center frequency, i.e., $f_c < 6GHz$, such as band 7, 2.6 GHz. The 5G base station transmits SSB signals with standard-defined periodicity for initial access. The gNB serves 5G capable devices (UEs) present within its cell coverage. These 5G capable devices follow the initial access procedure as described in Section 2.3 to connect to the network. The received symbols at the 5G UE experience the channel effect defined by the channel response function $h(t)$. Therefore, the received signal in time is typically described by the equation $y(t) = x(t)h(t) + n$, where n denotes Additive White Gaussian Noise, $x(t)$ is the transmitted signal in time, and $y(t)$ is the received signal. We will assume a fixed position gNB, and in our evaluation we will discuss the implication of UE mobility on the attack performance.

3.1.2 Adversarial model. We assume an attacker positioned within the coverage of the 5G gNB cell. The attacker is able to record and process RF (I&Q) samples from 5G bands. We assume that the attacker can generate and inject 5G wireless signals over the air at desired time instants. As we will demonstrate in our evaluation, this can be achieved using Software Defined Radios (SDR) capable of operating at the minimum 5G bandwidth and sampling rates, e.g., the widely used USRP B210 or USRP X310. We assume that the attacker is also capable of processing 5G SSB signals, and maintaining time and frequency synchronization with the gNB across time. We will demonstrate how an adversary can achieve leveraging the fairly long Cyclic Prefix of OFDM and phase prediction algorithms. The attacker can then forge specific signals and transmit them simultaneously with the gNB at lower power such that a receiver trying to decode the original signal receives in turn a modified version of the desired signal, and denying access to the legitimate signal.

3.2 SigUnder Attack Overview

An attacker sets itself in the proximity of the target gNB and listens to the SSB on the Downlink channel. It performs the initial access steps described in Section 2.3, synchronizing in frequency and time with the gNB and storing the received MIBs. When the attacker decides to spoof the SSB with malicious MIB, it performs the attack as depicted in Figure 4. The attacker chooses a target MIB, different from the legitimate MIB, and performs the PBCH encoding process as described in Figure 2. Then, it compares the forged PBCH symbols with the legitimate PBCH symbols from the gNB, and identifies the subset of symbols that differ with the legitimate signal. These symbols correspond to the sub-carriers that will be spoofed by the adversary. It transmits the given subset of PBCH symbols synchronized with the legitimate gNB transmission at a power level slightly higher than the legitimate gNB. This power level is just sufficient to cancel the legitimate one and barely flip the QPSK symbol at the receiver UE. The receiver receives the additively-combined signals at the same time instant. The addition of both signals over the air results in a PBCH that leads to the UE decoding the attacker's target MIB. This is mostly due to error-correction capability of the polar codes and the high amount of redundancy used (rate $R = \frac{1}{36}$).

Although the decoded MIB is correctly decoded, if the maliciously-spoofed MIB is carefully crafted, it will enable further attacks. This includes new attacks such as the manipulation of new 5G MIB bits (i.e., `cellBarred`, and `infraFreqReselection`), or directing the UEs to a spoofed SIB by modifying `pdcch-ConfigSIB1`. These attacks are possible because no integrity protection mechanisms are used for the SSB (e.g., MAC or digital signatures). The key advantage of `SigUnder` is that it can be achieved with emissions at lower-power than the legitimate gNB, therefore enabling an adversary to remain stealthy and/or operate from farther distances. In effect, `SigUnder` is an overshadowing attack with an undershadow signal, as shown in Figure 3. In the following sections, we will discuss the choice of spoofed MIB, synchronization challenges and techniques, as well as further implications of the attack.

`SigUnder` is motivated by the predictability of SSB, the strong error-correcting properties of polar coding, and the long duration of

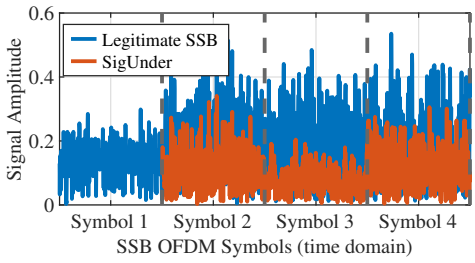


Figure 3: Time domain representation of legitimate SSB and SigUnder overshadowing signal

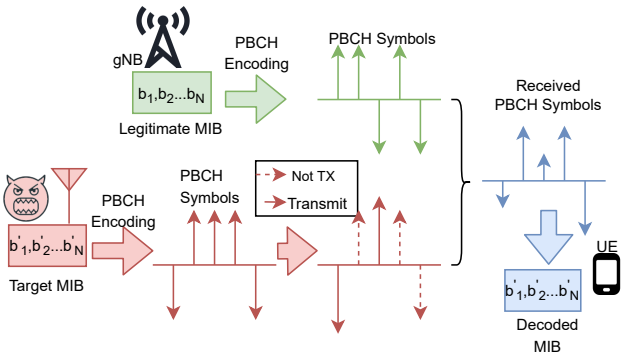


Figure 4: Overview of SigUnder attack

OFDM symbols and cyclic prefix. Polar codes were a breakthrough result in coding theory, are Shannon capacity achieving for various non-adversarial channel models, and have very efficient encoding and decoding algorithms $O(n \log(n))$ [11, 13, 16, 35]. Thus, a traditional white noise jammer would require high power to corrupt the PBCH, but polar codes do not intrinsically protect against malicious adversaries. We develop an attack that transmits a sub-set of the sub-carriers of OFDM modulated QPSK symbols to overshadow the original transmission at the receiver. SigUnder identifies a malicious PBCH that has a small Hamming distance to the legitimate PBCH sequence. Therefore, only samples of a limited number of sub-carriers of the PBCH need to be flipped. Note that on these sub-carriers the adversary only needs to cancel the original and slightly tilt the values towards his malicious PBCH. The polar code takes care of the error correction, decoding the malicious PBCH. The long duration of the 5G OFDM symbol makes time and phase synchronization possible for a wide range of locations, with adequate synchronization techniques as discussion in Section 3.5. The SigUnder attack can be generalized to other signals, as described in Section 3.4. Moreover, blindly transmitting random QPSK sequences to either jam or overshadow the legitimate PBCH is in theory possible, but highly inefficient for an attacker due to polar coding large codeword space (864 bits) and high redundancy.

The choice of QPSK symbols to transmit to overshadow the original transmission depends on the bits from the MIB that the attacker wants to modify. As outlined above, SigUnder saves power by only transmitting on the sub-carriers where legitimate and spoofed PBCH differ. As each MIB combination generates a different 432 symbol PBCH QPSK sequence, the number of overlapping PBCH symbols between two given sequences depends on the choice of MIB bits. In this way, deciding the target MIB used to overshadow is a trade-off between stealthiness (e.g., modifying the System Frame Number can make it easier for a UE to detect the attack), purpose of the attack, and energy efficiency.

SigUnder explores the MIB space to find how many PBCH symbols differ between a target and legitimate MIB. We find that modifying one bit from the MIB can lead to the resulting spoofed PBCH to have a similitude with the original PBCH between 18% and 37% symbols. Exploring the complete MIB space we find that this value can increase up to 54% PBCH symbols being equal, translating in roughly 3dB less power. Furthermore, SigUnder transmits the difference between target and legitimate PBCH symbols in a subcarrier basis. Multiple PBCH symbols might only differ in either real or imaginary parts of the QPSK symbol. Hence, only one of them might be required to be flipped, increasing the energy efficiency.

Legitimate and forged PBCH symbols arrive at the receiver with differing phase from the legitimate PBCH emission, making the attack non-trivial for real systems. For instance, both signals need to be in-phase to constructively create the -attacker- desired symbols at the receiver. This and other technical challenges arising from the wireless channel are described in Section 3.5.

Algorithm 1 describes the procedure an attacker performs to conduct the attack. First, it performs an initial setup following the same procedure as a legitimate UE would. It extracts all required information from SSB, acquiring time and frequency synchronization and retrieving the current MIB being broadcasted by the network, and predicts the future ones as the process is deterministic. With this information, the attacker decides on a target MIB and computes the QPSK sequences that will be used for overshadowing in the future. In parallel, additional steps to track the phase difference with the gNB are performed. An overshadowing opportunity appears every 20 ms, when the gNB transmits the SSB. In this moment, the attacker, synchronized in phase and time with the gNB transmits its own sub-carrier selective QPSK sequence, overshadowing the MIB for some of the users. In Section 4, we evaluate the impact of adversary power on the fraction of impacted users.

3.3 SigUnder for Overshadowing

Overshadowing the MIB transmitted by the legitimate gNB has several implications. Firstly, the MIB is a very compact block of information, containing only essential information. Thus, modifying any MIB bit has an important impact on the receiver, and in most circumstances, it will lead to failures during initial access procedure or any following connection establishment steps. A carefully crafted MIB can also lead to other attacks. Therefore, it is important to analyze the impact of overshadowing specific MIB fields.

For example, an adversary modifying the cellBarred field, and setting it to 1, would block the receiver from connecting to the cell. Furthermore, if intraFreqReselection is also set to 1, the UE would not select another cell in the same frequency. Alternatively, the MIB field pdcch-ConfigSIB1 describes the time and frequency resources where the UE should look for the SIB1 for the cell. An attacker modifying this field can redirect the UE to an empty section of the spectrum and send its own SIB1. An attacker can then forge

its own SIB1, and for instance force the receiving UE's to transmit the Random Access preamble with high power by modifying `preambleReceivedTargetPower` field in SIB1. Such higher power emissions would allow an adversary to identify UE's in the vicinity and/or increasing their power consumption. Modifying SIB1 facilitates modifying any other System Information Blocks (2-9), as scheduling information for remaining SI is described by SIB1. The lack of cryptographic integrity-protection prevents detection of such attacks. Our focus in this paper is to demonstrate and evaluate the feasibility of `SigUnder`.

Algorithm 1: `SigUnder` Attack Algorithm

Result: Overshadowing a legitimate MIB transmission
begin setup
  Compute frequency and time offsets from PSS & SSS;
  Decode MIB;
  Predict future MIB;
  Compute closest rogue PBCH sequence;
  Get first phase estimate $\hat{\Delta\phi}_i$ for SSB
end
while *true* **do**
  foreach *SSB* **do**
    Overshadow adjusting phase from prev SSB:
    Transmit $x(t)e^{-j\hat{\Delta\phi}_i}$;
    Recompute phase and time estimates:
    $\rho = \text{xcorr}(SSB_{i-1}, SSB_i)$;
    $\Delta\phi_i = \angle \max \rho$;
    $\Delta t_i = \max \rho$;
    Add $\Delta\phi_i$ to regression model and Estimate $\hat{\Delta\phi}_{i+1}$;
  end
end

3.4 `SigUnder` for Synchronization Signals

As outlined in Section 2.2, each signal composing SSB is critical to the initial access procedure. An adversary performing a denial of service attack, might target any of the SSB signals to disrupt communication. However, the Hamming Distance of synchronization signals is high, 0.5 for PSS and ranging from 0.44 to 0.5 for SSS. Hence, a Gaussian jammer is required to be lucky in flipping half of the bits of either synchronization signal to confuse the receiver, and would require high jamming power. as shown in Section 4.2.

`SigUnder` can be generalized for other SSB signals, as it relies on the fact that it is smarter and more efficient to move one sequence towards the closest sequence to confuse a receiver, instead of adding randomness as a Gaussian jammer. In addition, targeting PSS, SSS or PBCH-DMRS is energy efficient because they are short sequences, and BPSK is used for PSS and SSS. This means the attacker needs to flip only few subcarriers, requiring reduced power from the attacker. However, spoofing signals such as PSS or SSS can only achieve DoS, and it would not enable any further attacks. We present simulation results of SSB signal spoofing with `SigUnder` in Section 4.2, but we will focus on the performance of `SigUnder` for PBCH overshadowing.

3.5 Technical Challenges to Operating `SigUnder` in Real Systems

As indicated in previous sections, successfully operating `SigUnder` in a real-world scenario raises several challenges.

Time Synchronization. The adversary spoofing signal needs to be synchronized with the legitimate gNB transmission at the target UEs. This is because `SigUnder` relies on the legitimate and forged PBCH symbols adding to a desired symbol. 5G NR choice of waveform includes a Cyclic Prefix (where the OFDM first samples are cyclically repeated during transmission), as a robustness mechanism against multipath and to simplify the equalization in the frequency domain. Interestingly, we find experimentally that if the timing offset between the adversary and legitimate signals is below the CP duration, the two OFDM signals add up and only a phase offset is experienced by receiving UE. Hence, an attacker needs to be synchronized with a timing offset below the CP duration. In 5G, the CP duration depends on numerology μ, in this way, CP length is $4.69\mu s$ for 15 KHz and $2.34\mu s$ for 30KHz , which corresponds to a range of 1407 and 703 meters where the attack can work.

Carrier Frequency and Phase Offset. Due to imperfections in the crystals driving the PLL generating the carrier frequency, an offset typically exists. While estimating and correcting the frequency offset can be done to some extent, a small frequency offset will typically remain (specially if the gNB and/or adversary lack an accurate timing source such as GPS). In order to align the phase correctly at the receiver, the attacker needs to track the phase offset with the gNB. Furthermore, prediction of the phase is required to compensate at the next overshadowing opportunity. We propose to use a Polynomial regression model, building a polynomial with the phase values over time and predicting the phase offset at the upcoming overshadowing opportunity. Note that we do not need a perfect estimation of the offset at a given UE, but only need to maintain a constant offset over time to sustain a successful attack over multiple emissions of the SSB. Details are described in Section 4.3.

Channel estimation with PBCH-DMRS. 5G SSB includes PBCH-DMRS for channel estimation. The estimated coefficients are applied for PBCH symbol equalization. We find that whilst `SigUnder` works for certain scenarios without including channel estimation, its performance decreases without it. We found that adding PBCH-DMRS increases the probability of a successful overshadowing.

4 EVALUATION

In this section, we evaluate the performance of `SigUnder` with both software simulations and over the air measurements. For over the air measurements, we address the technical challenges presented in Section 3.5 and present results for phase estimation. The goal of our evaluation is to analyze the limitations of the attack, its reliability under a real channel and how energy efficient can the attack be.

4.1 Evaluation description

For our simulation evaluation, we test `SigUnder` with MATLAB® software through Monte Carlo simulations. MATLAB® 5G Toolbox™ [28] provides functions to generate standard-compliant 3GPP 5G NR

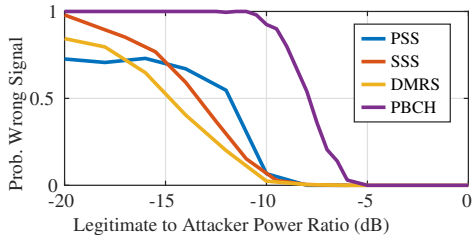
Waveforms as well as receiver capabilities, including polar encoding/decoding. For our simulation scenario we assume a single gNB transmitting initial access signals. SSB is configured with 30KHz subcarrier spacing and the periodicity of the SSB signal is the one for initial access procedure, 20 ms. The receiver follows the initial access procedure as described in the standard, and decodes MIB. The channel used for simulations is an Additive White Gaussian Noise Channel (AWGN). We inject the attacker's overshadowing signal in the channel by adding the signal in time domain.

For OTA experiments, we use high-performance SDRs, specifically, USRP X310, for RF transmission and reception. USRP X310 is able to operate at 5G Frequency Range 1, $f_c < 6GHz$, and over up to 160MHz bandwidth per channel. As our attack focuses on SSB for FR1, the maximum bandwidth required is 240 subcarriers at 30KHz subcarrier spacing, i.e. 7.2 MHz bandwidth. We use 5G Open Air Interface (OAI) [19, 29] 5G NR open-source implementation to generate SSB and transmit it over USRP X310. 5G OAI gNB supports the generation of 5G NR compliant SSB, including a 3GPP compliant polar coder and decoder. We generate 5G OAI SSB signals with physical layer SSB configuration of 30KHz subcarrier spacing with normal CP. SSB is transmitted every 20 ms. We record the transmitted signals from another USRP X310, and perform our attack over the recorded signals.

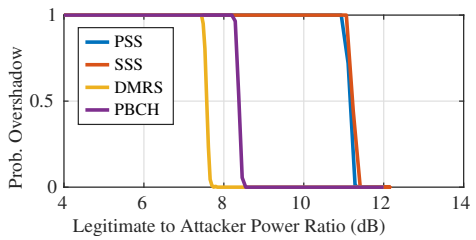
To evaluate the performance of SigUnder and the energy efficiency of the attack, we introduce a metric, termed Legitimate to Attacker Power Ratio (LARP), used across simulations and OTA results. LARP represents the power ratio between the legitimate and overshadowing signals. LARP is computed as the ratio of the root mean square (RMS) power of the Legitimate SSB signal in time and the RMS power of the attacker signal in time, such as: $LARP = \frac{\sqrt{\frac{1}{n}\sum_i^n x_L^2}}{\sqrt{\frac{1}{n}\sum_i^n x_A^2}}$, where n is the number of samples in time domain of the SSB, x_L is the legitimate signal in time, and x_A is the overshadowing signal. We will commonly express LARP in dB scale. Thus, positive values indicate the number of dB the overshadowing signal is below the legitimate signal, whereas negative values indicate the number of dB the overshadowing signal power is above the legitimate one.

4.2 Simulation results

In order to understand the reach of our attack and the energy efficiency of our approach, we present results for a White Gaussian Noise (WGN) jammer as a reference attack. Such an attacker does not require previous knowledge of the legitimate signal to be jammed, apart from the time-frequency resources used for the transmission, which can be achieved simply by finding PSS and SSS. Although SigUnder goes beyond jamming by spoofing a controlled signal, we use the comparison to jamming as a first step of our evaluation. For our evaluation, we simulate a scenario with a gNB transmitting SSBs with 20 ms periodicity. The signals pass through an AWGN channel to the receiver, and we set the SNR at the receiver at 20dB. For the reference jammer, we generate White Gaussian Noise and target the different SSB signals separately to simulate the effect of the attacker. To evaluate the spoofing capabilities of SigUnder, we find the closest sequence for each legitimate SSB signal and conduct the attack separately for each sequence.



(a) White Noise Jammer



(b) SigUnder

Figure 5: Probability of decoding a signal different from the legitimate when each SSB signal is targeted by AWGN jammer and SigUnder overshadowing

Figure 5 shows the probability of a receiver decoding an incorrect SSB signal in the presence of a White Gaussian Noise jammer and SigUnder. The probabilities are presented as a function of the ratio between legitimate and attacker powers (LARP). Results for WGN in Figure 5a show that due to 5G-NR resilient synchronization signals, high power is required to disrupt communication. Jamming PSS or SSS with a probability above 60% with white noise requires the attacker to be at least 15dB above the legitimate signal. The attacker's transmit power needs to be boosted up to 21dB to achieve 100% probability of jamming SSS, whereas the probability of jamming PSS converges to 66% because there is only 3 possible sequences for PSS. Power required increases even further for PBCH-DMRS, which presents 1.5dB gain to SSS, requiring 16.5dB to be jammed 60% of the times, and requires at least 22dB to be jammed with 100% probability. Lastly, PBCH shows good performance but suffers more than the other SSB signals against white noise. PBCH starts to experience errors when jamming power is 6dB above the legitimate signal, 55% at 8dB, and is completely jammed when this value increases up to 11dB.

For SigUnder, results in Figure 5b show that the attacker can be below the power of the legitimate SSB and yet overshadow the legitimate signals (LARP > 0). Performing the attack over PSS or SSS exhibits similar results as the sequence lengths are equal and Hamming Distances similar. An attacker targeting PSS or SSS can be 11dB below the legitimate SSB to spoof the legitimate sequence. The very reduced power required to create a DoS attack with PSS/SSS is justified because less than 127 subcarriers are transmitted out of 830 that constitute the SSB. An attacker using SigUnder with the closest sequence to target PBCH can achieve a successful attack by transmitting 8.2dB below the legitimate signal, and this power is increased to 7.4dB if the target is PBCH-DMRS.

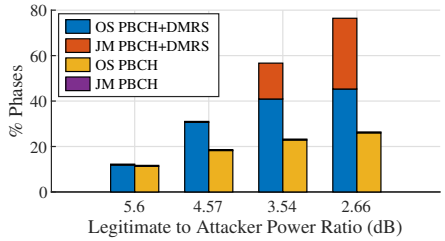


Figure 6: Percentage of phases applied to the attacker signal that Overshadow (OS) or Jam (JM) the legitimate PBCH

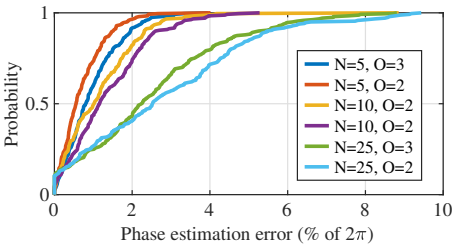


Figure 7: ECDF of the error in the estimation of the phase difference using different polynomial regression parameters

4.3 Over The Air Results

The channel model used for the simulation scenario, AWGN, does not present many challenges for `SigUnder`. However, when the signals are transmitted over the air, the technical challenges in Section 3.5 become tangible. For instance, we found that channel estimation did not impact the performance of the attack for simulations. However, the channels experienced by the two signals coming from the gNB and the attacker generally differ for real world channels. As a results, in this section we include a comparison of the performance of `SigUnder` for two configurations: when `SigUnder` only transmits the PBCH overshadowing signal, and when the attacker's overshadowing signal is accompanied also by PBCH-DMRS, used for channel estimation, as described in Section 2.2.

Analysis of phase adjustement for successful overshadowing. Signals arriving at a receiver might experience different phases at the receiver due to channel effects. One of the first issues encountered by an attacker is to determine which phase rotations of the attacker's signal result in legitimate and attacker signals adding up to obtain the desired signal at the receiver. In order to explore this aspect of the attack, we apply different phase rotations at the attacker signal, and we compute the probability of success in overshadowing or jamming the legitimate signal over 250 consecutive SSB transmissions with different attack powers. Figure 6 depicts the percentage of phase rotations of the attacker signal that result in either overshadowing or jamming at the receiver, as a function of the power ratio between legitimate and overshadowing signal. Results show a notable discrepancy in the results when the attacker transmits only the overshadowing PBCH sequence as compared to also transmitting PBCH-DMRS, specially as the attack power increases. The percentage of phases that are able to overshadow the legitimate MIB at the receiver for both cases are slim when the signal is 5.6dB below the legitimate signal, 11%. This value increases up to 45% at 2.66dB when PBCH-DMRS is also transmitted, whereas the percentage of phases overshadowing when only PBCH is transmitted increases only to 26%. For the standalone transmission of PBCH, jamming is negligible, and either one or the other signal is received, whereas the percentage of phases achieving jamming for PBCH + PBCH-DMRS configuration is substantial, 15% and 31% for 3.54dB and 2.66dB respectively. The results suggest that an attacker requires fine tuning of the phase to achieve energy-efficient attacks, and that the number of users impacted decreases with the attack power. Furthermore, an attacker targeting an UE under a mobility scenario needs to relax the gain of the attack, e.g. below 2.5dB, to ensure that he can offset the effects of highly variable phase differences and succeed with the attack.

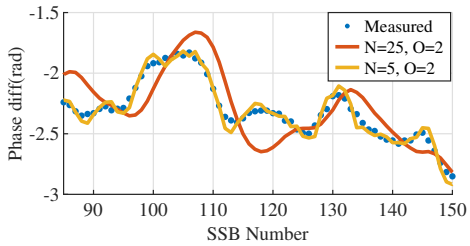


Figure 8: Estimation of phase difference with the gNB over time/SSB using best and worst estimators

Estimation of gNB-attacker phase difference over time. In addition, due to CFO, the phase between the gNB and the attacker changes over time, and needs to be adjusted, specially when the percentage of phases able to overshadow is reduced. To adjust the phase at the time of transmission, the attacker needs to know what the phase difference will be beforehand. To do so, we employ polynomial regression models to predict the phase difference between gNB and the attacker for the next SSB transmission instant. To evaluate our prediction, we compute the measured phase difference between 250 consecutive SSBs transmitted over the air by computing the cross correlation between the PSS for two consecutive signals, and then we use different regression models to forecast the phase difference for the next SSB. We find that the measured values of phase difference do not vary drastically for consecutive SSBs most of the time, as the period between two given blocks is relatively small, 20ms. Figure 7 shows the empirical cumulative probability of the phase estimation error for different polynomial orders, O and windowing values, N when estimating the next SSB value. Results show that all combinations of polynomial parameters explored are below a 10% of 2π error. Furthermore, the estimation benefits from shorter windowing, as $N = 5$ outperforms other windowing values, and from using lower polynomial orders, an order 2 polynomial adapts better to the phase change over time. We find that a polynomial estimator of order 2 with a windowing of the last 5 phase differences can achieve an error below 2% 96% of the time and the error does not exceed 4%. Figure 8 presents a comparison of the phase difference estimation for the best and worst estimators to the measured data.

Over the air overshadowing performance. To evaluate the overshadowing capabilities of `SigUnder` under the effects of a real channel, we inject the overshadowing signal adjusted by the estimated

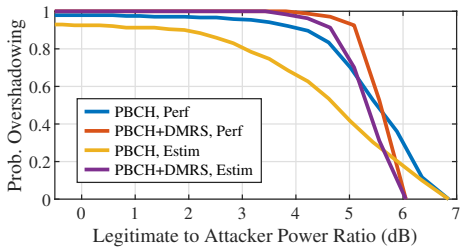


Figure 9: Probability of SigUnder to overshadow the legitimate over the air signal using different attacker configurations with and without perfect phase estimation

phase difference and compute the probability of the receiver to decode the target MIB. Figure 9 shows the probability of overshadowing the original MIB for OTA measurements as function of the legitimate to attacker power ratio when performing the attack over a 5 second measurement. We present results with perfect phase estimation and with a phase estimated based on the best estimator presented in Figure 7. Looking at the results for perfect phase estimation, we observe that the inclusion of PBCH-DMRS is beneficial for the attack. Even though transmitting PBCH-DMRS increases the total power used for the attack, the attack becomes more reliable. In this way, when transmitting PBCH and PBCH-DMRS the attack achieves a 100% probability of overshadowing at 3.8dB LARP when the phase is perfectly estimated, whereas only transmitting the PBCH overshadowing signal is able to overshadow the orginal signal 94% and 97% of the time for 3dB and 0.84dB respectively. Transmitting only PBCH yields higher gains, i.e. the attack is able to work even at 6.5dB below, but with low probability, only 10% of the SSB are overshadowed. Furthermore, coherently with the results presented in Figure 6, as the percentage of phases able to overshadow is reduced when only transmitting PBCH, the attack is more sensitive to phase estimation errors. The probability of overshadowing when using the estimate phase value drops substantially, requiring almost 2dB more power to achieve the same probability as perfect phase case. Similarly, transmitting PBCH + PBCH-DMRS with a sub-optimal phase reduces the attack performance. However, the performance loss is not as impacted, 0.7dB at most, and the attack achieves a 100% probability of success at 3.4dB.

5 SICUnder: MITIGATIONS AND EVALUATION

In this section, we propose and evaluate the performance of mitigation mechanisms at the physical and higher layers. The mitigation works against our attack `SigUnder` and the previous `SigOver` attack. We first discuss and analyze the root causes of several vulnerabilities in currently standardized wireless cellular networks. First and foremost, there are no security mechanisms present in any of the pre-authentication messages. This spans from SSB and MIB, to SIB1, and even the initial Radio Resource Control and Non-Access Stratum messages. Secondly, synchronization signals are easily recognized to facilitate cell access to legitimate users, however, they can be used as a stepping stone by attackers trying to exploit the inherently open wireless medium. Lastly, there is no physical layer mechanisms in the standard to aid in recovering a legitimate critical signal that has been overshadowed. Alternative solutions to overshadowing attacks could aim to reduce the predictability of signals through cryptographic interleaving and modulation [38], however, significant changes to the standard might be required.

Thus, an adequate mitigation should address these two relevant aspects: (1) it should enable the receiver to recover the legitimate signal from the physical layer; and (2) the receiver should be able to verify the integrity and authenticity of these messages. Ideally, this should be feasible in a standard-compliant manner.

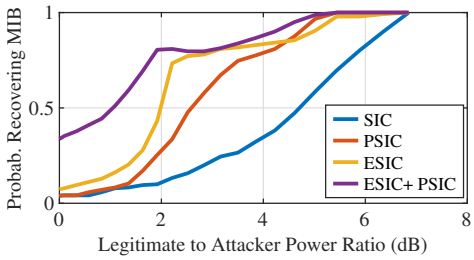
5.1 Successive Interference Cancellation for Retrieving Legitimate Signaling

The problem of discerning multiple concurrent communications has been thoroughly discussed in wireless communications. Successive Interference Cancellation (SIC) was first presented in [17]. The main idea consists of successively decoding-subtracting signals. When a signal is decoded by the receiver, it is subtracted from the received signal and the decoding procedure is performed over the resulting signal again. At first sight, this scheme seems well suited to address the overshadowing of signals, as they are superimposed. For the `SigOver` attack, since the overshadowing and legitimate signal are two distinct and self-contained signals, each one with different amplitudes and well separated frequency information, subtracting the strongest decoded signal does not alter the legitimate signal.

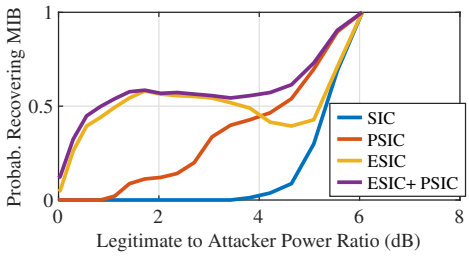
However, for our attack, since the signal transmitted by `SigUnder` is not a self-contained PBCH sequence, but rather a subset of a modified PBCH sequence, it depends on the original transmission being transmitted to result in the final target MIB. Applying a classic SIC scheme in this situation might in turn jeopardize the chances of retrieving the original MIB. For instance, had the receiver in Figure 4 applied SIC, in the first iteration, it would decode and subtract a PBCH sequence from a sequence that is only an addition of two sequences in a reduced set of subcarriers. Hence, subcarrier values that were not overshadowed would be zeroed after the first iteration, preventing any further decoding of the remaining signal. Due to the particularity of this problem, this solution is not optimal and adjustments to the traditional SIC scheme need to be conducted.

5.1.1 Partial Successive Interference Cancellation. Initially, we explore the recovery capabilities of a Partial SIC (PSIC). In this scheme, the first decoded signal is not subtracted in its entirety, but only an amplitude scaled-down version of it is subtracted. This approach relies on the fact that the attacker's intent is to shift the legitimate PBCH to a closer different codeword using low power, as close as possible to the decision threshold for maximum energy efficiency. By only subtracting a fraction of the decoded signal, the subcarriers that are not targeted by the attacker are not cancelled out, and the overshadowed signal can be recovered. The weight applied to the partial SIC depends on various factors such as channel and relative transmit power difference between attacker and gNB. Due to this, we propose a simple iterative heuristic, which increases the decoding overhead linearly with the number of iterations.

5.1.2 Equalized Successive Interference Cancellation. To further improve the probability of recovering the original signal, we developed a scheme that considers an active attacker focusing on a set of subcarriers, Equalized SIC (ESIC). ESIC explores the frequency



(a) Probability of recovering original MIB for different SIC techniques when DMRS is not included



(b) Probability of recovering original MIB for different SIC techniques when DMRS is included

Figure 10: Probability of SIC techniques to recover the legitimate MIB in the presence of SigUnder

domain PBCH symbols to identify the subcarriers that have experienced an abnormal modification, and equalizes the resulting PBCH symbols by only applying SIC to the identified subcarriers. To select the correct set of subcarriers, a receiver can use different metrics. For instance, Error Vector Magnitude (EVM) or computing the distance of each subcarrier to the closest constellation point. Furthermore, the subcarrier selection can be improved by relying on the channel estimation coefficients; if only PBCH is targeted and PBCH-DMRS is not transmitted by the attacker, the receiver would notice channel estimation coefficients and resulting QPSK symbols in PBCH are incongruous. Lastly, Equalized SIC is performed over the equalized PBCH symbols to reduce the disparity across subcarriers caused by the wireless channel.

Note that the described SIC extensions assume that the attacker does not have information regarding the received constellation amplitude at the receiver. Had an attacker access to such information, e.g. mapping the channel at all positions previously, it could adjust its power such that the difference between legitimate and attacker received symbols is minimized.

Figure 10 presents a comparison of the probability of recovering the original transmission for traditional SIC, PSIC, ESIC and PSIC + ESIC, against `SigUnder`. We compare the performance of SIC when `SigUnder` only transmits PBCH or PBCH along with PBCH-DMRS in Figures 10a and Figures 10b respectively, and we apply SIC in the scenario described in Section 4.3. The attacker adjusts the phase at each SSB based on the polynomial estimation with $N = 5$, $O = 2$ from Figure 7. Results show that traditional SIC does not improve the probability of recovering the original transmission, thus, we use the SIC performance curve as a reference, as its probability is the probability of the attack not succeeding. All other techniques are able to reduce the low energy capabilities of the attacker to some extent, recovering the original transmission when the attacker power is low, but the performance is substantially reduced when the attacker power compares to the legitimate signal power. Figure 10a shows that PSIC and ESIC are able to retrieve the original MIB with 100% probability with 1.4 dB gain with respect to SIC when only the PBCH is transmitted by the attacker, but the gain is reduced close to 0 when LARP decreases to 1dB. ESIC combined with PSIC outperforms the individual techniques, mostly at low LARP values, being able to achieve a 34% probability of recovering the original transmission even when LARP becomes 0dB. Figure 10b shows that SIC techniques are not as effective when the attacker increases the robustness of the attack by also transmitting the channel estimation pilots. As in previous graph, a combination of ESIC and PSIC outperform the individual techniques, achieving the best performance. ESIC + PSIC is able to retrieve the original MIB 57% of the time for 1.7 dB LARP, which represents a 3.6dB gain respect to not using SIC. ESIC shows a comparable performance to ESIC + PSIC except for the high LARP region, >3dB. PSIC does not offer substantial improvements in performance. It only proves beneficial when the attack power is very reduced, LARP > 4.6dB, but fails to recover any legitimate MIB already at 0.8dB LARP.

5.2 Integrity Protection

Retrieving the original MIB in the presence of an overshadowing signal is the first of a two-step process of a successful mitigation scheme. Even if the legitimate signal is recovered, the receiver is still unable to distinguish a legitimate from forged MIB since integrity protection for broadcast network information is not included in cellular standards. A feasible proposed solution shall be standard-compliant, or require minimal modifications of the standard. The 5G standard included for the first time the use of a public key cryptography, to encrypt the SUbscriber Permanent Identifier (SUPI) into the SUbscriber Concealed Identifier (SUCI), as a solution for IMSI catchers in 5G [9]. This feature can be used as the base to build a PKI scheme that authenticates network broadcast information such as MIB, SIBs or paging. Integrity protecting broadcast information presents multiple challenges, such as how to update certificates securely, or efficient ways of fitting signatures in the existing standard [24]. For instance, MIB has very limited size, only 1 bit is unused, which makes adding a signature to MIB practically impossible without significant modifications to the structure of the SSB. Therefore, if possible the SIB1 should include a signature of both SIB1 and MIB, such that an UE is able to verify the authenticity of both broadcast information blocks. Incorporating signatures in SIB1 while complying with the standard can be achieved by using the `nonCriticalExtension` fields in SIB1. `nonCriticalExtension` is used to add new fields to already pre-existing messages, and present in most 5G messages. In this way, a gNB can decide to enable authenticated network broadcast information while maintaining compatibility with already deployed systems, as it would be up to the UE to check for signatures.

ACKNOWLEDGMENT

This work was partially supported by grants NAVY/N00014-20-1-2124, NCAE-Cyber Research Program, and NSF/DGE-1661532.

REFERENCES

[1] 2020. 5G; NR; Base Station (BS) radio transmission and reception (3GPP TS 38.104 version 15.7.0 Release 15).

[2] 2020. 5G; NR; Physical layer; General description (3GPP TS 38.201 version 16.0.0 Release 16).

[3] 2020. 5G; NR; Physical layer procedures for control (3GPP TS 38.213 version 16.3.0 Release 16).

[4] 2020. 5G; NR; Services provided by the physical layer (3GPP TS 38.202 version 15.6.0 Release 15).

[5] 2020. Technical Specification Group Services and System Aspects; Release 16 Description; Summary of Rel-16 Work Items (TR 21.916 Release 16).

[6] 2021. 5G; NR; Multiplexing and channel coding (3GPP TS 38.212 version 16.4.0 Release 16).

[7] 2021. 5G; NR; Physical layer measurements (3GPP TS 38.215 version 16.4.0 Release 16).

[8] 2021. 5G; NR; Physical layer procedures for data (3GPP TS 38.214 version 16.4.0 Release 16).

[9] 2021. 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 16.5.0 Release 16).

[10] 2021. 5G; Vehicle-to-Everything (V2X) services in 5G System (5GS); Stage 3 (3GPP TS 24.587 version 16.3.0 Release 16).

[11] Erdal Arikan. 2009. Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels. *IEEE Transactions on Information Theory* (2009).

[12] Alcardo Alex Barakabitze, Arslan Ahmad, Rashid Mijumbi, and Andrew Hines. 2020. 5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges. *Computer Networks* (2020).

[13] Valerio Bioglio, Carlo Condo, and Ingmar Land. 2021. Design of Polar Codes in 5G New Radio. *IEEE Communications Surveys Tutorials* (2021).

[14] Marc Briceno, Ian Goldberg, and David Wagner. 1998. GSM Cloning. http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html

[15] Agnes Chan, Xin Liu, Guevara Noubir, and Bishal Thapa. 2007. Broadcast Control Channel Jamming: Resilience and Identification of Traitors. In *2007 IEEE International Symposium on Information Theory*.

[16] Kai Chen, Kai Niu, and Jiaru Lin. 2013. Improved Successive Cancellation Decoding of Polar Codes. *IEEE Transactions on Communications* (2013).

[17] T. Cover. 1972. Broadcast channels. *IEEE Transactions on Information Theory* (1972).

[18] Simon Alexander Erni. 2020. *Protocol-Aware Reactive LTE Signal Overshadowing and its Applications in DoS Attacks.* Master's thesis. Department of Computer Science, ETH Zürich.

[19] EURECOM. 2020. Openairinterface 5G Wireless Implementation. https://gitlab.eurecom.fr/oai/openairinterface5g.

[20] Caroline Frost. 2019. 5G is being used to perform remote surgery from thousands of miles away, and it could transform the healthcare industry. *Business Insider* (2019). https://www.businessinsider.com/5g-surgery-could-transform-healthcare-industry-2019-8

[21] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. 2018. GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier. In *Proceedings 2018 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA.

[22] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In *Proceedings 2018 Network and Distributed System Security Symposium*. Internet Society, San Diego, CA.

[23] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. 2019. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. *Network and Distributed Systems Security (NDSS) Symposium* (2019).

[24] Syed Rafiul Hussain, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino. 2019. Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19)*. Association for Computing Machinery.

[25] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. 2019. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In *2019 IEEE Symposium on Security and Privacy, SP 2019, San Francisco, CA, USA, May 19-23, 2019*. IEEE.

[26] Mina Labib, Vuk Marojevic, and Jeffrey H. Reed. 2015. Analyzing and enhancing the resilience of LTE/LTE-A systems to RF spoofing. In *IEEE Conference on Standards for Communications and Networking, CSCN 2015, Tokyo, Japan, October 28-30, 2015*. IEEE.

[27] Marc Lichtman, Roger Piqueras Jover, Mina Labib, Raghunandan Rao, Vuk Marojevic, and Jeffrey H. Reed. 2016. LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation. *IEEE Communications Magazine* (2016).

[28] MathWorks. 2020. 5G Toolbox Release 2020b.

[29] Navid Nikaein, Mahesh K. Marina, Saravana Manickam, Alex Dawson, Raymond Knopp, and Christian Bonnet. 2014. OpenAirInterface: A Flexible Platform for 5G Research. *SIGCOMM Comput. Commun. Rev.* (2014).

[30] A. Omri, M. Shaqfeh, A. Ali, and H. Alnuweiri. 2019. Synchronization Procedure in 5G NR Systems. *IEEE Access* (2019).

[31] Christina Pöpper, Nils Ole Tippenhauer, Boris Danev, and Srdjan Capkun. 2011. Investigation of Signal and Message Manipulations on the Wireless Channel. In *Computer Security – ESORICS 2011*, Vijay Atluri and Claudia Diaz (Eds.). Springer Berlin Heidelberg.

[32] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2019. Breaking LTE on Layer Two. In *IEEE Symposium on Security & Privacy (SP)*.

[33] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2020. Call Me Maybe: Eavesdropping Encrypted LTE Calls With ReVoLTE. In *USENIX Security Symposium (SSYM)*.

[34] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2016. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems.

[35] Ido Tal and Alexander Vardy. 2015. List Decoding of Polar Codes. *IEEE Transactions on Information Theory* (2015).

[36] Muhammad Taqi Raza and Songwu Lu. 2018. On Key Reinstallation Attacks over 4G/5G LTE Networks: Feasibility and Negative Impact.

[37] Robotics Online Marketing Team. 2019. 5G-Powered Medical Robot Performs Remote Brain Surgery. *Robotics Online* (2019). https://www.robotics.org/blog-article.cfm/5G-Powered-Medical-Robot-Performs-Remote-Brain-Surgery/213

[38] Triet D. Vo-Huu and Guevara Noubir. 2015. Mitigating Rate Attacks through Crypto-Coded Modulation *(MobiHoc '15)*. Association for Computing Machinery.

[39] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. 2019. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE. In *28th USENIX Security Symposium (USENIX Security 19)*. USENIX Association, Santa Clara, CA.

[40] Chuan Yu, Shuhui Chen, Zhiping Cai, and Jesús Díaz-Verdejo. 2019. LTE Phone Number Catcher: A Practical Attack against Mobile Privacy. *Sec. and Commun. Netw.* 2019 (2019).