# Secrecy in Wireless Communication through Closed-Loop Receiver De-Synchronization

Antonios Argyriou
Department of Electrical and Computer Engineering
University of Thessaly, Greece
anargyr@uth.gr

***Abstract*—A subset of the synchronization algorithms in a wireless receiver are responsible for tracking the phase and frequency of a digitally modulated signal. If variations of the phase in the signal are substantial, then the receiver might be unable to track them leading to inability to demodulate the data. In this paper we propose a method for improving the secrecy of wireless communication by ensuring that an arbitrary unauthorized receiver (URx) cannot track these phase and frequency changes but a legitimate (LRx) one can. This is accomplished by introducing artificial variations in the phase of a wireless transmitted signal that exceed the capabilities of a certain class of receivers. We explore receivers that employ closed-loop synchronization, namely a phase-lock loop (PLL) and we devise an artificial frequency variation pattern that can de-synchronize it. Our results indicate that with our method the bit error rate (BER) of an URx can be maintained at a pretty high level even for very favorable channel conditions.**

## I. Introduction

Cryptography is the main tool for securing wireless communication [1]. Solutions based on cryptography are typically implemented above the physical layer (PHY) where keys are generated, and digital messages are encrypted and decrypted. Newer ideas regarding security at the PHY exploit the randomness of the wireless channel, receiver, transmitter, and other components of the communication system so as to achieve robust cryptographic key generation [2]. Nevertheless, cryptography does not secure at all the fundamental operation of the PHY which is signal demodulation, that is the conversion of a waveform into bits. We consider the problem of preventing signal demodulation, i.e. improve the secrecy, in the fundamental wiretap communication topology: A transmitter (Tx) communicates with the legitimate receiver (LRx), while an unauthorized receiver (URx) is the adversary that eavesdrops the communication from the Tx to the LRx. This is an old and well-studied problem in wireless communication systems.

One way to prevent the URx from eavesdropping the wireless communication between the Tx and Rx is through frequency-hopping spread spectrum (FHSS). By changing the carrier frequency among a number of several distinct frequencies occupying a large spectral band, a URx is unable to demodulate the desired data since it does not know both the carrier and the narrow band used for data at a specific time instant. The fundamental advantage of FHSS is that the data signal is not received at all at the URx. But the disadvantage of FHSS is that bandwidth utilization is low since the bandwidth of the FH system is approximately equal to $NB$, where $N$ is the number of carrier frequencies available for hopping and $B$ is the bandwidth of the data signal.

Recent works focus on preventing data demodulation by hiding the used modulation type from an eavesdropper of the wireless signal [3]–[6]. Unlike FHSS, this is an indirect way to render unable a receiver to demodulate since the signal is received in the first place. Hiding the modulation, also called (*modulation spoofing*), has been at the forefront of these works. In [4], [5] the authors presented methods to obfuscate quadrature amplitude modulated (QAM) symbols at the transmitter. The authors of these works may flip the symbol location in the constellation diagram [3], embed symbols from a lower order modulation to a higher order constellation [5], or reorder the symbols in time [4]. Then they detect the symbols of the modified constellation which means that the symbol detection probability is dictated by the distance between the constellation points in the new mapping. CryptoJam in [5] embeds symbols from a lower order modulation to a higher order QAM constellation. The receiver detects the symbols of the higher order modulation which means that the detection probability will be dictated by the distance between the constellation points in the higher order mapping. Other works like iJam [7] randomize the value of a received modulated signal by allowing intentional RF jamming from the receiver. This leaves an eavesdropper unable to know which of the repeatedly transmitted symbols is the correct one, while the receiver has this information. In [8] a carefully positioned fourth node, emits a signal that obfuscates the amplitude, delay, or frequency of the signal. The obfuscating node, that acts as an amplify-and-forward relay, operates continuously (despite the need of it or not) and requires coordination and synchronization between itself, the Tx and the Rx. Generating a different PHY signal compared to the one the eavesdropper expects, can also be an option for spoofing the transmission between the Tx and the legitimate Rx but has not been used as such. An interesting approach is Phycloak [8] where a carefully positioned fourth node, emits a signal that obfuscates the amplitude, delay, or frequency of the signal.

In this work we depart from the FHSS and modulation spoofing concepts for ensuring communication secrecy. The transmitter employs residual-carrier wireless communication, that is a carrier signal is transmitted along with the data [9]. At the Tx both the data and the carrier signals are subjected to an *artificial (spoofed) time-varying frequency variation* so as to prevent successful tracking of the carrier at the URx.

The LRx knows the frequency spoofing strategy (Similar to a FH receiver knowing the hopping pattern) which allows it to reverse its effect. *Hence, the novelty of our method is that we improve secrecy, not by introducing a new communication method, but by focusing on disabling a critical functionality of eavesdropping wireless receivers since successful tracking of the carrier is essential for demodulation in wireless communication systems [9].* The advantage of our method with respect to related work [3]–[6] is that it prevents symbol detection by being applicable in any wireless digital communication system since it is independent of the used modulation. The second advantage is that it does not require any helping nodes [8]. Third, and unlike FHSS bandwidth utilization is very high since the bandwidth of the data signal is only spead by a factor equal to the maximum variation of the spoofing frequency (artificial Doppler spread). Overall our contributions are twofold: 1) We propose a new methodology for improving the secrecy of wireless communication links by making data demodulation more challenging at a URx through the insertion of artificial de-synchronization signals. 2) We develop analytical expressions that allow the Tx to select the optimal de-synchronization signal with a low-complexity algorithm given the performance requirements for the URx.

## II. Background & System Model

**Transmitter/Receiver Architecture:** A typical single-carrier wireless communication system that is implemented at the nodes of our topology can be seen in Fig. 1. In this figure $x(t)$ represents the complex baseband symbol that is transmitted every $T$ seconds (symbol period) and can take a value from a dictionary of complex symbols $\mathcal{M}$ that is defined according to the used modulation [10]. The complex symbols go through the transmit filter with impulse response $g(t)$ and so the transmitted random signal $s(t)$, which is the convolution of the two $s(t) = x(t) * g(t)$, is characterized by the power spectral density (PSD) $S_{ss}(f)$. The bandwidth of this signal is $W$ Hz. After the digital-to-analog converter (DAC) the signal is upconverted to the carrier frequency $f_c$ and after the power amplifier (PA) the signal is transmitted over a time-varying channel with single-tap impulse response $h$ (flat fading). The fist stage of the receiver is responsible for filtering the desired signal with bandwidth $W$ Hz using a bandpass filter (BPF), and then downconverts the signal to baseband by mixing with frequency $f_c$ (or to an intermediate frequency if a heterodyne Rx is used). For non-bursty communication tracking of the carrier in both the LRx and the URx is accomplished with closed loop techniques and more specifically with phase-lock loops (PLLs) [11]. The PLL tracks the carrier (its phase and frequency offset are estimated), and after the signal is corrected with the phase and frequency estimate, the residual phase error is propagated to the matched filter (Rx filter). While the basic architecture holds for both the LRx and URx, Fig. 1 also illustrates how the proposed scheme could operate in conjunction with classic cryptography-based secure communication system at the LRx (dashed line in this figure). The Tx can piggyback in a transmitted frame the artificial frequency variation ($f_{\text{SP}}$) that will be used in the following

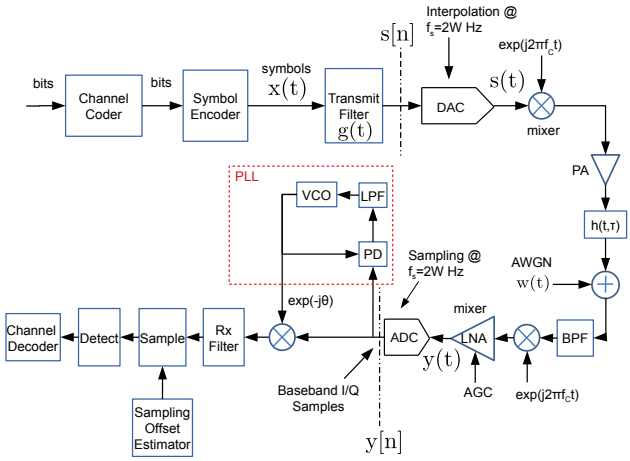



Fig. 1: A single-carrier wireless communication system with a direct conversion Rx and a PLL for phase/frequency tracking.

frame, and when the LRx decrypts its value it can compensate for it.

**PLL Performance Tradeoff:** PLLs are feedback systems that typically use a phase detector, a lowpass loop filter (LPF) and a voltage-controlled oscillator (VCO). When the channel with a transfer function $H(f)$ is relatively static, the coherence bandwidth of the channel is narrow which means that tracking the carrier can be accomplished with a PLL that uses a loop filter with a very narrow bandwidth (Fig 2(a)). The sideffect is that data can be demodulated easier and potentially be decoded both by LRx and also by a URx. By artificially increasing frequency variation $f_{\text{SP}}$ relative to the frequency $f_c$ of the carrier signal (the maximum frequency variation is the Doppler spread), the coherence bandwidth of the signal is increased and so the URx is forced to use a higher bandwidth loop filter. But this leads inadvertently to more noise accumulation due to the noise floor of the receiver (Fig 2(b)).

**Signal Model for Residual Carrier Communication with Spoofed Frequency Variation:** Now we gradually develop the signal model for URx. The total power budget $P_T$ is split into carrier power $P_c$, and data power $P_d$. The modulation index $\beta$ determines how this power is split. In the most popular form of the modulation index, we take a trigonometric function of it to indicate the power dedicated to the carrier as $P_c{=}P_T\cos^2(\beta)$ while the data power is $P_d{=}P_T\sin^2(\beta)$. Now in a BPSK system the transmitted passband signal for the data symbols $x(t)$ encoded as non-return to zero (NRZ) ($\pm1$) is:

$$s(t) = \sqrt{P_T}\sin(2\pi f_c t + \beta x(t)) \tag{1}$$

If we analyze this expression to separate it further to the carrier and the data it becomes equal to:

$$s(t) = \sqrt{P_T}\cos(x(t)\beta)\sin(2\pi f_c t) + \sqrt{P_T}\sin(\beta x(t))\cos(2\pi f_c t)$$

For NRZ BPSK $\cos(x(t)\beta) = \cos(\beta)$ and $\sin(x(t)\beta) = x(t)\sin(\beta)$. So the received signal with only the addition of

the passband noise would be:

$$y_{\text{PB}}(t) = \sqrt{P_T}\cos(\beta)\sin(2\pi f_c t) + \sqrt{P_T}\sin(\beta)x(t)\cos(2\pi f_c t) + n_I(t)\cos(2\pi f_c t) - n_Q(t)\sin(2\pi f_c t)$$

The first term in this equation is the carrier and the second corresponds to the carrier modulated with the symbols $x(t)$. Towards our complete model we must include the flat fading complex gain $a(t)$ (that is $a_I(t) + ja_Q(t)$), plus the spoofed frequency of the transmitted signal which is the sum of $f_c + f_{\text{SP}}$. We assume that the URx knows $f_c$ but not $f_{\text{SP}}$ which is impossible since it is a time-varying function selected by the Tx. So the consequence is that the difference between the frequency of the oscillators at the Tx and URx will be $f_{\text{SP}}$ Hz. This means that the received baseband signal becomes[1]

$$y(t) = a(t)e^{2\pi f_{\text{SP}} t}(\sqrt{P_d}x(t) - \sqrt{P_c}j) + n(t), \qquad (2)$$

where $n(t) = n_I(t) + jn_Q(t) \sim \mathcal{CN}(0, \frac{N_0}{2})$ is the complex AWGN sample. That is, with BPSK modulation information bits are transmitted in the I channel while the Q channel contains the carrier signal. This signal is the input to the PLL as our receiver in Fig. 1 indicates.

**Signal Model with PLL:** From (2) we observe that the phase of the input carrier signal that has to be tracked by the PLL suffers from AWGN, fading, and the spoofed frequency that all aggregate to $\phi(t)$ rad/sec:

$$\phi(t) = \tan^{-1}\frac{a_Q(t)}{a_I(t)} + \tan^{-1}\frac{\sin(2\pi f_{\text{SP}} t)}{\cos(2\pi f_{\text{SP}} t)} + \tan^{-1}\frac{n_Q(t) - \sqrt{P_C}}{n_I(t)} \qquad (3)$$

If $\theta$ is the phase estimate that the PLL produces, the phase estimation error is $\theta_e = \theta - \phi$. So with this phase offset due to imperfect carrier tracking from the PLL, the previous analysis leads to the passband signal being after the phase correction:

$$\begin{aligned} z_{\text{PB}}(t) &= |a(t)|(\sqrt{P_d}x(t)\cos(2\pi f_c t + \theta_e) + \sqrt{P_c}\sin(2\pi f_c t + \theta_e)) + n(t) \\ &= |a(t)|(\sqrt{P_d}x(t)\cos(2\pi f_c t)\cos(\theta_e) - \sqrt{P_d}x(t)\sin(2\pi f_c t)\sin(\theta_e) \\ &+ \sqrt{P_c}\sin(2\pi f_c t)\cos(\theta_e) + \sqrt{P_c}\cos(2\pi f_c t)\sin(\theta_e)) \\ &+ n_I(t)\cos(2\pi f_c t) - n_Q(t)\sin(2\pi f_c t) \qquad (4) \end{aligned}$$

The final baseband equivalent model is then:

$$\begin{aligned} z(t) &= \sqrt{P_d}|a(t)|x(t)\cos(\theta_e) + j\sqrt{P_d}|a(t)|x(t)\sin(\theta_e) \\ &+ \sqrt{P_c}|a(t)|\sin(\theta_e) - j\sqrt{P_c}|a(t)|\cos(\theta_e) + n(t) \\ &= \sqrt{P_d}|a(t)|x(t)\exp(j\theta_e) - \sqrt{P_c}|a(t)|j\exp(j\theta_e) + n(t) \qquad (5) \end{aligned}$$

One detail of our final model in (5) is that for higher order modulations like QAM the main difference of the PLL is at the phase detector [12]. Even though a new analysis would be needed, the fundamental operation of the PLL and its impact is the same on the data signal, which is that a residual phase estimation error $\theta_e$ remains. Also, note that the signal model in (5) could be enhanced with additional Tx/Rx impairments like carrier phase offset (CFO), sampling clock offset, I/Q imbalance, etc, but these parameters are independent to our analysis. Finally, we must note that even with perfect tracking of the time-varying phase in the last equations the amplitude of the fading that is equal to $|a(t)|$ still affects the received signal.

[1]Recall that from a passband signal the baseband model is derived using $y_{\text{PB}}(t) = \Re[y(t)\exp(j2\pi f_c t)]$.

## III. Controlling the Phase Estimation Error at the URx

The signal model in (5) allows us to see clearly that we can prevent demodulation of $x(t)$ if we can control $\theta_e$ which is a random process. To make the idea practical we propose a strategy for controlling the phase noise to ensure that it reaches a level that disallows the unauthorized receiver to lock onto the carrier. We desire to know what is the phase noise variance as a function of our spoofing strategy so that we can select the optimal $f_{\text{SP}}$ for maximizing $\sigma^2_{\theta_e}$ at the eavesdropper. But the phase noise is a random process that is affected by an additional noise source besides $f_{\text{SP}}$. This element considers the impact of AWGN and we discuss it first.

### A. Phase Noise Model with AWGN

The model we developed in (5) is independent of the used PLL or more general the phase/frequency tracking method. In this paper we study a particular class of popular PLLs namely a second order PLL while different tracking methods can be investigated using a similar methodology. The closed-loop transfer function of a second order PLL is [11]:

$$H(s) = \frac{2\xi\omega_n s + \omega_n^2}{s^2 + 2\xi\omega_n s + \omega_n^2} \qquad (6)$$

In the above $\xi$ is the damping factor and $\omega_n$ is the natural frequency of the loop.[2] Instead of using the previous two parameters, the typical operating parameter of a PLL is the single-side *noise bandwidth of the loop* denoted as $B_L$ and calculated as follows for the 2nd order PLL [11]:

$$B_L = \frac{1}{2}\int_{-\infty}^{\infty}|H(j2\pi f)|^2 df = \frac{\omega_n}{2}(\frac{1}{4\xi} + \xi) \qquad (7)$$

For this PLL our goal is to calculate the variance of the phase estimation error $\theta_e = \theta - \phi$, that is the quantity:

$$\sigma^2_{\theta_e} = \text{Var}(\theta_e) = \mathbb{E}[|\theta - \phi|^2] \qquad (8)$$

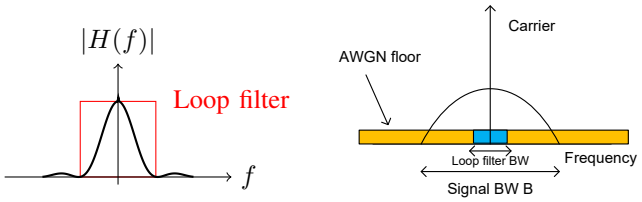
For calculating the variance of the phase error we need both the transfer function and PSD $S_w(f)$ of the noise random process at the input of the PLL (eqn. 3.15 in [11]), since it is:

$$\sigma^2_{\theta_e} = \int_{-\infty}^{\infty} S_w(f)|H(j2\pi f)|^2 df \qquad (9)$$

The difficulty of the previous calculation depends primarily on $S_w(f)$. At the receiver the typical strategy is that the bandwidth of the BPF is equal to the bandwidth of the signal $W$ Hz. With AWGN and no other impairments at the receiver if $N_0$ Watt/Hz is the noise PSD before the BPF, then after filtering from the BPF, and sampling with the ADC at a rate of $2W$ the noise is still white and has a PSD of $N_0$ Watt/Hz. With a carrier of power $P_c$ the PSD of the noise process at the input of the PLL is (eqn. 3.13a in [11]):

$$S_w(f) = N_0/P_c \text{ Watt/Hz} \qquad (10)$$

[2]$\xi$ is 1 for critically-damped PLLs.




(a) (b)

Fig. 2: a) The loop filter bandwidth depends on the coherence bandwidth of the channel b) Phase noise tradeoff in a PLL with direct carrier modulation.

After replacing (10) in (9), integrating over the magnitude of the transfer function of the PLL (within $[-W, W]$), and finally by replacing (7), the derivation leads to

$$\sigma^2_{\theta_e} = \int_{-\infty}^{\infty} S_w(f)|H(j2\pi f)|^2 df = \frac{N_0}{P_c}\int_{-\infty}^{\infty} |H(j2\pi f)|^2 df$$
$$= \frac{N_0 2B_L}{P_c} = \frac{N_0\omega_n}{P_c}(\frac{1}{4\xi} + \xi). \quad (11)$$

This is the variance of the phase noise for a PLL that tracks a modulated carrier with power $P_c$ in an AWGN channel. With direct carrier modulation (data is modulated directly into the carrier) besides the AWGN floor that will impair the PLL, it will also suffer from a fraction of the data signal that is filtered through the PLL LPF leading to the addition of a term (again this is illustrated in Fig. 2(b)) in the denominator of the carrier-to-noise ratio (CNR) as follows:

$$SNR_L = \frac{P_c}{B_L N_0 + P_d \frac{2B_L}{W}} \quad (12)$$

### B. Phase Noise with a Frequency Ramp

Now the question is how to control $f_{\text{SP}}$ at the Tx so its variations will be robust against a URx which configures a PLL that tries to track the carrier. Clearly the design of the PLL dictates its tracking ability. A more potent phase/frequency tracker will require a different behavior for $f_{\text{SP}}$. Another aspect is that regardless of the PLL, when the URx is closer to the Tx it can achieve higher CNR in (12) with lower $B_L$. So in this case the additional phase noise that is introduced due to $f_{\text{SP}}$ must be able to disallow the PLL from locking to the carrier even with this improved CNR (worst case scenario for the Tx/Rx pair). Here we make use of the fact that second order PLLs will have a constant *phase estimation error* when a frequency ramp used [11]. Consequently, this is what we propose to use as the spoofing signal.

With a frequency ramp we set $f_{\text{SP}}{=}f_1 t/2$, and so the overall frequency of the signal changes linear with time as $f_c + f_1 t/2$. Hence, the transmitted signal in (1) becomes $s(t) = \sin(2\pi(f_c t + \frac{f_1}{2}t^2) + \beta x(t) + \phi]$ and the frequency of the local oscillator (LO) at the URx is $\sin[2\pi f_c t]$. At the output of the phase detector we have that[3]

$$\frac{1}{2}\cos[2\pi f_c t + 2\pi(f_c + f_{\text{SP}})t] + \frac{1}{2}\cos[2\pi f_{\text{SP}} t],$$

and after the loop filter the output is $\frac{1}{2}\cos[2\pi f_{\text{SP}} t]$. Consequently, by choosing $f_{\text{SP}} = f_1 t/2$, the phase change at the PLL input is given by $\theta_i(t) = \frac{1}{2}2\pi f_1 t^2 u(t)$ and $\theta_i(s) = \frac{2\pi f_1}{s^3}$. For any PLL the Laplace transform of the phase error is:

$$\theta_e(s) = \frac{s\theta_i(s)}{s + K_o K_d F(s)} \quad (13)$$

$K_o$ is the VCO gain factor, $K_d$ is the phase-detector gain factor, and $F(s)$ is the loop filter transfer function. The steady state error for a PLL under the frequency ramp becomes:

$$\lim_{t\to\infty}\theta_e(t) = \lim_{s\to 0} s\theta_e(s) = \lim_{s\to 0}\frac{2\pi f_1}{s[s + K_o K_d F(s)]} \quad (14)$$

For the 2nd order PLL the transfer function of a proportional-plus-integrator loop filter with an infinite DC gain is $F(s) = k_1 + \frac{k_2}{s}$ leading to:[4]

$$\lim_{t\to\infty}\theta_e(t) = \lim_{s\to 0}\frac{2\pi f_1}{s^2 + 2\xi\omega_n s + \omega_n^2} = \frac{2\pi f_1}{\omega_n^2} \quad (15)$$

This means that the received signal after the PLL in (5) experiences a phase noise with a mean equal to (15) (that prevents successful tracking) and a variance equal to (11).

### C. Bit Error Rate (BER)

When the data rate is higher than the bandwidth of the loop filter the phase noise $\theta_e(t)$ is a random process that varies slowly with respect to the symbol period $T$. Hence, the phase can be approximated to be constant within $T$. The same is also true for the channel fading parameter $a(t)$ which is also considered to be static (or slowly varying in practice). To obtain the BER at the URx we have to average over all the fading states of $a(t)$ and the phase noise $\theta_e(t)$ since they affect the power of the data signal in (5). For BPSK modulation the data signal is $\sqrt{P_d}|a(t)|x(t)\cos(\theta_e)$ which means that the instantaneous power is random and equal to $P_d|a(t)|^2\cos^2(\theta_e)$. Based on the previous discussion the BER is expressed:

$$PE = \mathbb{E}_{a,\theta_e}[Q(\sqrt{\frac{2P_d|a(t)|^2\cos^2(\theta_e)}{N_0}})] \quad (16)$$

In this work we focus on producing simulation results for the BER that can be used for driving the decisions of the algorithm we describe in the next section. In the above the PDF of $|a(t)|^2$ depends on the channel model, i.e. it is exponential in our case. The phase noise follows a Tikhonov distribution(p.p. 205 [13]) with PDF

$$f(\theta_e) = \frac{\exp(SNR_L\cos(\theta_e))}{2\pi I_0(SNR_L)} \text{ for } \theta_e \le \pi, \text{ and 0 otherwise,} \quad (17)$$

where the function $I_0$ is the modified Bessel function of 0th order. But with the addition of the specific frequency ramp we only affect the mean [11]. This allows for a straightforward simulation model of $\theta_e, a(t)$.

[3]The Costas loop removes the impact of the data $x(t)$ on the phase [12]

[4]$\xi = \frac{k_1}{2}\sqrt{K_0 K_d/k_2}, \omega_n = \sqrt{K_0 K_d k_2}$

## IV. Tx Configuration Algorithm & Receiver

Our algorithm is presented in Algorithm 1. It uses simulation data obtained for different phase noise variance versus BER. The algorithm searches the minimum $f_{\text{SP}}$ and modulation index $\beta$ that induces a certain phase noise variance $\sigma^2_{\theta_e}(\beta, f_{\text{SP}})$ and this in turn a certain BER denoted as $PE_{\text{URx}}$ for the URx. This search is executed as follows: Our algorithm increases $f_{\text{SP}}$ monotonically since from the phase noise in (15) we know that the BER will increase monotonically. The same monotonic behavior is not necessarily true for $\beta$. Nevertheless $\beta$ has a more limited variability across different values since it controls the allocation of power between the carrier and the data. In our algorithm it starts iterating from a value of $\frac{1}{20}\frac{\pi}{2}$ rad (nearly all power allocated to the data) and goes all the way up to $\frac{19}{20}\frac{\pi}{2}$ rad (nearly all power allocated to the carrier).

Note that $\beta, f_{\text{SP}}$ are parameters that will be set at the Tx. But we also include another element in the algorithm that accounts for the behavior of the URx. As we explained in (II) the URx can sweep different values for $B_L$ (that control the CNR $SNR_L$) so that it can improve the operation of the PLL. This is what we also do in the inner for loop of our algorithm where estimate the BER for different values of the CNR in the PLL. Here we note that this sweeping of $SNR_L$ (and indirectly $B_L$) affects of course only $\sigma^2_{\theta_e}(\beta, f_{SP}, B_L)$ and not $P_c, P_d$ which are selected by the Tx.

The previous approach ensures convergence of the algorithm to the desired BER by selecting the minimum $f_{\text{SP}}$ and optimal $\beta$ that satisfy it. Since we seek to maximize the BER at the URx, we set the lowest allowed BER for the URx to $10^{-2}$ (which is something that can be changed by the user): If we do not have a URx BER higher than $10^{-2}$ then algorithm continues until it finds a solution. Since $f_{\text{SP}}$ is selected based on simulation data, in real life the performance of URx will be even worse, which means that our algorithm effectively calculates the performance lower bound for the BER. Given the capabilities of a specific LRx and URx (noise power), the algorithm needs to be executed once and the exhaustive search that it entails (complexity is $O$(number of $\beta$ steps $\times$ number of $f_{\text{SP}}$ steps)) is of no practical concern.

**Algorithm 1:** Frequency Spoofing Algorithm

```
Input: Noise floor of URx and LRx → σ_e^2, → σ_b^2
Input: Minimum desired BER → 10^-2
Output: Optimal β, f_SP
while f_SP < f_c do
    while β < 1 do
        P_c(β), P_d(β) ← Calculate power for given β;
        for SNR_L = 0, SNR_L <= 20 dB do
            B_L ← Calculate from (12) for given
              P_c, P_d, SNR_L;
            if PE_URx < 10^-2 then
                σ^2_θe(β, f_SP, B_L) ← (11), (15) ;
                PE_URx(curr) ← (17) ;
            else
                stop;
            end
            SNR_L = SNR_L + 3dB.
        end
        increase β by desired step;
    end
    increase Δf_SP by desired step;
end
```

### A. Receiver Discussion

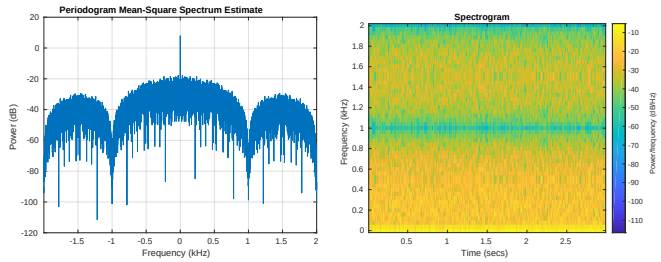
Clearly there are several subtleties to the design of the communication system. The most promising avenue for implementing the proposed idea is as highlighted in Fig. 1 where the artificial Doppler is communicated to the LRx through an encrypted message. When this is the case, a more advanced version of the system could transmit a more sophisticated artificial Doppler pattern that changes over time. This may be implemented so that the instantaneous Doppler frequency $f_{\text{SP}}$ does not monotonically increase. We have explained earlier that communication of these more sophisticated patterns is similar to a FHSS communicating the frequency hopping pattern which means that our system does not have any requirements beyond the widely popular FHSS.

In the case where the spoofing signal cannot be encrypted, a slope estimator can be used at the legitimate Rx to calculate $f_{\text{SP}}$ and remove it from the signal before feeding it to the PLL. This means that the PLL has to track only channel imperfections and not the frequency ramp. Of course the risk in this case is that an URx could also use a slope estimator to calculate the artificial Doppler spread. Hence, this is the less favorable option for implementation.

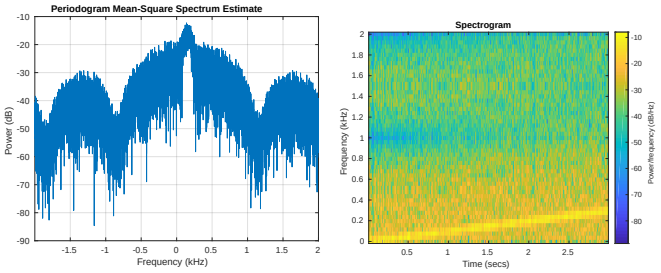
## V. Performance Evaluation

For our simulation we considered a static Rician flat fading channel while the path loss exponent was set equal to 2. The distance between the Tx and LRx is 10 meters, while the distances we tested between the Tx and the URx were 10, and 1 meters. $f_c$ is set to 2.4GHz, while the bandwidth of the signal $W$ is 100KHz. Based on these data we can calculate the available signal power at the URx. For the given signal power and modulation index, the URx can decide to operate the PLL at different CNRs denoted with $SNR_L$. If it decides to track the carrier more accurately because of the artificial Doppler $f_{\text{SP}}$ it must increase the bandwidth of the loop $B_L$. But this means lower operating CNR which of course increases the AWGN power that comes through the LPF. On the other hand if it reduces $B_L$ too much to increase the CNR, then it will not be able to track the carrier effectively leading again to increased phase noise. So the receiver's poor phase tracking ability is caused either by AWGN or by the high Doppler from $f_{\text{SP}}$. This is a well known tradeoff in PLLs that necessitates the optimal selection of $B_L$. We explore different partitions of the transmitted signal power $P_T$ through the selection of the modulation index $\beta$, and for each one of these partitions we perform the optimization we discussed in the last paragraph: For a given $\beta$, $P_d$ is fixed and so is the $E_b/N_0$. For this $E_b/N_0$, we calculate the remaining power dedicated to the carrier $P_c$ and then we sweep different loop filter bandwidth values $B_L$ to derive the CNR that leads to the lower BER. This is how

a data point is produced in the BER plots and the notation $SNR_L^*$ indicates that this optimization was carried out.




(a) w/o Doppler (b) w/o Doppler




(c) Doppler $f_{SP} = \frac{100}{2}t$ Hz (d) Doppler $f_{SP} = \frac{100}{2}t$ Hz

Fig. 3: PSD and Spectrogram of BPSK NRZ signal at 1Kbps with no Doppler and an artificial Doppler.

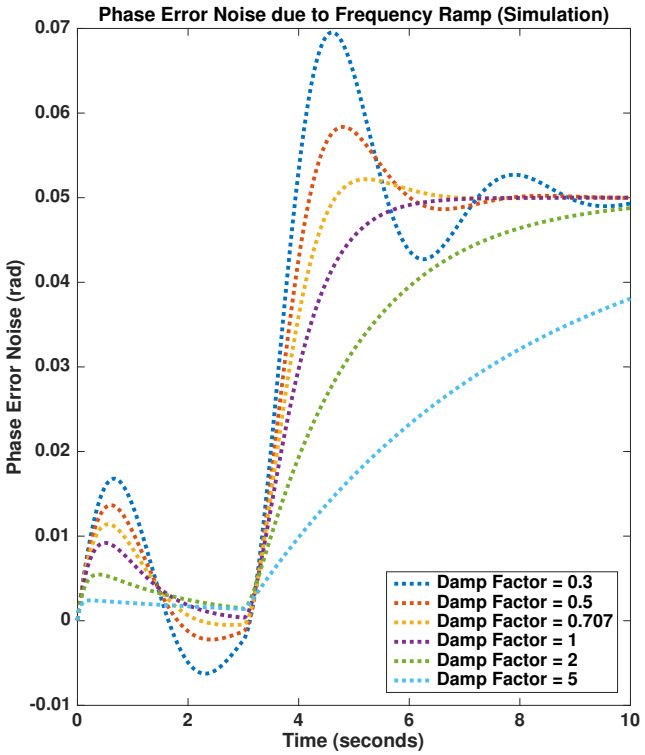



Fig. 4: Phase/frequency estimate at the PLL for the used frequency ramp. No AWGN is used at the URx.

First, to understand the behavior of the spoofing transmitter in Fig. 5 we present the PSD and the spectrogram of the modulated signal when it is subjected to the artificial frequency spoofing. It easy to see that the high power DC component of the baseband signal (that is the carrier signal) is widened. The same of course holds for the data signal but in this case it is difficult to visualize which frequency bins are shifted in the frequency domain. Regarding the behavior of the artificial Doppler spread over time the spectrogram illustrates that the desired behavior is obtained, that is the instantaneous frequency of the signal is increased linearly over time.

Before we discuss BER we first present the inability of URx to track the carrier with the artificially high Doppler in Fig. 4. We observe the constant phase error for different values of $\xi$ that correspond to different $B_L$, while $\omega_n$=1 rad/sec. For higher $\xi$, and so $B_L$, we observe the extremely slow convergence of the phase error but again to a constant $\theta_e$.

BER is presented in Fig. 5. The reason for this non-monotonic behavior of the BER at the URx is that as $E_b/N_0$ is increased, $P_c$ is decreased and so to maintain the CNR the loop filter $B_L$ is increased. This leads to higher phase noise due to AWGN (as seen in (11)), poor tracking performance, and so high BER. This is true for both BER lines that are illustrated in Fig. 5 and correspond to different distances between the Tx and URx. With shorter distance a higher signal power on average is available at the URx. This means that the URx can achieve the same CNR with a narrower $B_L$ since the carrier signal power is higher (captured in (12)). The best performance that URx can achieve is approximately $10^{-2}$ for Tx-URx distance of 1m (with an optimal $SNR_L^*$=20dB leading to high value for $B_L$), and even after careful sweeping of different values of the CNR $SNR_L$. For slightly higher distance the performance is even worse and the optimal CNR is higher at $SNR_L^*$=30dB which means a narrower $B_L$ and poor tracking performance of the artificial Doppler spread. On the contrary, LRx can successfully track the carrier for higher $E_b/N_0$ since it can narrow the loop filter bandwidth $B_L$, leading to lower $SNR_L$ of 10 and 20 dB, regardless of the distance and without any loop filter optimization.

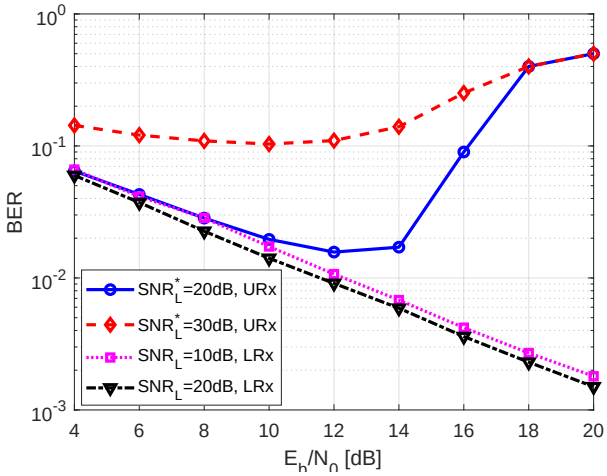



Fig. 5: BER at URx and LRx for different CNR versus $E_b/N_0$.

## VI. Discussion and Conclusions

In this paper we presented a new approach for improving the secrecy of wireless communication by preventing carrier

signal acquisition for the necessary receiver synchronization and eventual signal demodulation. The basic idea suggests the insertion of an artificial (spoofed) frequency variation at the transmitted signal that is designed with specific receivers in mind. We explored this idea for receivers that employ 2nd order PLLs and we provided an algorithm for selecting the spoofing signal which is supported by an analytical tool.

The concept is applicable to any type of modulated signal waveform and different receiver architectures. The proposed scheme can be used for improving communication secrecy as an alternative to FHSS or the more complex modulation spoofing methods.

## REFERENCES


[1] M. A. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes," *Journal of Network and Computer Applications*, vol. 101, 2017.

[2] X. Wang, P. Hao, and L. Hanzo, "Physical-layer authentication for wireless security enhancement: current challenges and future developments," *IEEE Communications Magazine*, vol. 54, no. 6, June 2016.

[3] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," in *ESORICS*, 2011, pp. 40–59.

[4] M. I. Husain, S. Mahant, and R. Sridhar, "CD-PHY: Physical layer security in wireless networks through constellation diversity," in *MILCOM*, Oct 2012.

[5] H. Rahbari and M. Krunz, "Friendly CryptoJam: A Mechanism for Securing Physical-layer Attributes," in *ACM WiSec*, 2014, pp. 129–140.

[6] T. Xiong, W. Lou, J. Zhang, and H. Tan, "Mio: Enhancing wireless communications security through physical layer multiple inter-symbol obfuscation," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 8, pp. 1678–1691, Aug 2015.

[7] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *2011 Proceedings IEEE INFOCOM*, April 2011, pp. 1125–1133.

[8] Y. Qiao, O. Zhang, W. Zhou, K. Srinivasan, and A. Arora, "PhyCloak: Obfuscating Sensing from Communication Signals," in *NSDI*, 2016.

[9] A. Stocker, A. Argyriou, A. Giorgetti, E. Paolini, D. Siddle, A. Zeqai, P. Tortora, J. D. Vicente, R. Abello, and M. Mercolino, "Simulating the reliability of radio links during superior solar conjunctions," in *EuCAP*, 2018.

[10] A. Goldsmith, *Wireless Communications*. Cambridge Univ. Press, 2005.

[11] F. Gardner, *Phaselock Techniques*. John-Wiley and Sons, Inc., New York, 1979.

[12] J. G. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2000.

[13] J. H. Yuen, *Deep Space Telecommunications Systems Engineering*, 1st ed. Springer Publishing Company, Incorporated, 2013.