Out-Phased Array Linearized Signaling (OPALS): A Practical Approach to Physical Layer Encryption

Eric Tollefson, Bruce R. Jordan Jr., and Joseph D. Gaeddert
MIT Lincoln Laboratory
Email: eric.tollefson@ll.mit.edu, bruce.jordan@ll.mit.edu, joseph.gaeddert@ll.mit.edu

***Abstract*—Traditional methods of securing communications rely on methods such as encryption which require coordination between the transmitter and the receiver. Physical layer encryption techniques propose exploiting transmit arrays to cover the transmitted signal with beamformed noise or to generate directional modulation to provide security without requiring coordination *a priori* between the transmitter and receiver. These techniques suffer from implementation difficulties such as high computational requirements and higher amplifier linearity requirements. In this paper we propose out-phased array linearized signaling (OPALS) which provides a practical approach to physical-layer encryption through spatial masking. Our approach modifies just the transmitter to employ the outphasing amplifier design to generate a unique masking signal to each element of an antenna array. This approach improves the peak-to-average power ratio (PAPR) of the transmitter, provides a high degree of confidentiality, and requires no coordination with or modification to the intended receiver.**

***Index Terms*—PHY security, array, beamforming, LINC, outphasing, directional modulation, physical layer encryption**

I. Introduction

Historically, cryptography has been the most commonly-used tool to guarantee the secrecy of communications. Modern cryptographic techniques are very effective, but have two major drawbacks. First, they require coordination between the sender and the receiver about the cryptographic method used and a key for encryption and decryption. Key distribution is a major logistical challenge and is resource-intensive as keys are typically changed at regular intervals. Second, most cryptographic techniques are vulnerable to compromise. Shannon proved that only cryptographic systems which use keys equal in length to the message are provably secure [1], such as one-time pad systems. Most widely-used systems rely on making attacks computationally-intensive, but this is not guaranteed against well-resourced adversaries or advances in computing technology. Even the most secure system may be compromised by users accidentally or deliberately revealing keys or algorithms.

In 1975 Wyner [2] coined the term *wiretap channel* and showed how the secrecy of communications is related to the relative channel capacity between the eavesdropper and intended receiver—this is frequently known as the Alice-Bob-Eve problem. Specifically, he proved that perfect secrecy is possible at some non-zero rate if the channel to the intended receiver has a greater capacity than the channel to the eavesdropper. The difference between the receiver's capacity and the eavesdropper's is known as the *secrecy capacity*. This was the genesis of the area known as *physical layer encryption (PLE)*, which seeks to exploit that fact in a practical system.

Physical layer encryption is a promising new technology and encompasses a variety of techniques to provide security without the sharing of keys [3]. The secrecy provided by PLE is quantifiable and provable. Based on this, secrecy cannot be compromised by the loss of keys or algorithms nor by the application of massive computing resources. A variety of approaches have been proposed. One group of techniques uses information from the shared channel between transmitter and receiver as a key for traditional cryptography. The other group of techniques, which we will focus on, changes the design of the transmitter to intentionally degrade the eavesdropper's channel capacity. Most of these techniques accomplish this by transmitting an additional signal on top of the communication signal, which we will refer to as the *masking signal*. PLE can be applied alone, but may be better used in conjuction with traditional cryptography so that the technologies complement each other and provide defense in depth.

The masking signal can take a number of forms including random noise and signals derived from the communication signal. In some cases, the receiver is designed to cancel the masking signal, but in most systems the transmitter uses an array to shape the pattern of the masking signal to null it at the intended receiver without any action by the receiver. This is advantageous because it makes the receiver simpler and also removes the need for coordination between the transmitter and receiver. The "key" required for communication in such a scheme is the location of the intended receiver in the null of the masking signal. In effect, this type of physical layer encryption system transforms communication security into a physical security problem where the transmitter and receiver must ensure that any potential eavesdropper is kept out of this region. For this paper, we will use *plaintext (PT) region* to denote this region, where the communication signal is dominant, and *ciphertext (CT) region* to denote the region where the masking signal is dominant. Figure 1 clearly shows the way that a masking signal and communication signal

Distribtuion A: Public Release. This work is sponsored by the Office of the Assistant Secretary of Defense for Research and Engineering under Air Force Contract FA8721-05-C-0002. Opinions, interpretations, conclusions and recommendations are those of the author and are not necessarily endorsed by the United States Government.

interact to create the CT region (in red) and the PT region (in blue.)

To date, two main approaches have been proposed for the design of the masking signal. The original type, first proposed by Goel and Negi [4], uses random noise. The noise applied to each antenna element is weighted such that it lies in the null space of the intended receiver's channel, so no receiver modification is needed and no coordination is required. The main drawback of methods based on noise addition is one of practicality. Noise requires a large dynamic range and thus a high-power, highly-linear, and expensive power amplifier.

The second type is known as directional modulation (DM), such as the methods proposed by Daly [5] and Pellegrini [6]. This type seeks to choose a set of beamforming weights such that the desired symbol is generated at the intended receiver, while a distorted symbol is generated at other angles. The weights are generally chosen so that the transmitted signals are constant-envelope, although filtering and pulse-shaping are not generally considered in the literature to-date which will introduce amplitude variation to the final signal. In some systems, such as [5], a single set of weights are chosen for each symbol and used for all instances of that symbol. This is known as static DM and leads to a distorted constellation for an eavesdropper, but not necessarily an unintelligible one as the constellation points may be distinct and separable for some angular offsets. It has been shown [7] that better security is provided by choosing a new set of weights for each symbol in random fashion. This is called dynamic DM. However, calculation of the required weighting vector is computationally-intensive as it involves repeated inversion of the channel.

With Out-Phased Array Linearized Signaling (OPALS), we propose a new masking technique that has some advantages of each of the previous methods. We use a masking signal which is based on the principles of Linear Amplification with Nonlinear Components [8], or LINC. This method is computationally simple and we will show that it provides secrecy comparable to noise-based masking and produces a signal with limited dynamic range. Simulation results will be presented using realistic communication signals.

II. Method Description

A. Masking Transmitter

A generic masking transmitter architecture is shown in Figure 1 for an array of N evenly-spaced antenna elements. The modulator produces a single series of complex-valued data symbols which are summed with a masking symbol before applying the beamforming weights and filtered using a continuous-time band-limiting pulse. The continuous-time transmitted signal on the n^{th} of N antenna elements is

$$s_n(t) = \sum_{k=-\infty}^{\infty} w_n\Big(a[k] + M_n[k]\Big)g(t - kT) \qquad (1)$$

where

- w_n is the beamforming weight of the n^{th} element,
- $a[k]$ is the complex data symbol at time index k,
- $M_n[k]$ is the masking symbol for the n^{th} element at time k,
- T is the signaling interval, and
- $g(t)$ is a square-root Nyquist filter with bandwidth $1/T$.

For our analysis we assume that the antenna elements are symmetrically spaced along the y-axis. Setting $w_n = 1$ puts the boresight of the array along the x-axis where we assume the intended receiver is located. If the elements are spaced at a distance d wavelengths apart, the received signal at an angle θ off the x-axis is therefore

$$r(t;\theta) = \gamma \sum_{n=0}^{N-1} s_n(t) e^{j2\pi d \cos\theta} + \varphi(t) \qquad (2)$$

where γ is a constant path-loss component due to propagation and $\varphi(t)$ is additive white Gaussian noise with a power spectral density $N_0/2$. From (1) and (2) it is clear that the choice of the masking signal $M_n[k]$ greatly affects the signal fidelity of a receiver as a function of θ.

In general we impose the restriction that $\sum_{n=0}^{N-1} M_n[k] = 0$ such that the mask imparts no interference on the intended receiver. The simplest choice for the mask is to set $M_n[k] = 0$ for all n and k which reduces the system to just a traditional beamforming array. This method suffers from side-lobes off the main beam which are vulnerable to an eavesdropper employing a high-gain antenna. Noise masking physical-layer encryption techniques improve upon the traditional beamforming approach by selecting $M_n[k]$ to be additive white Gaussian noise such that the power level makes decoding off the beam impossible. The constraint $\sum_{n=0}^{N-1} M_n[k] = 0$ must still be met to satisfy the cancellation requirement at the intended receiver and the standard deviation of the noise, σ_M can be chosen to satisfy the security requirements. While this approach provides security, the transmitter efficiency is greatly diminished as the signal's peak-to-average power ratio (PAPR) increases significantly, as will be shown later in Section III-B.

B. OPALS Mask

Linear amplification using non-linear Components (LINC) was developed by Cox in 1974 [8] and is built upon the outphasing amplifier first described by Chireix in [9]. The heart of a LINC system is the signal component separator which produces constant-envelope branch signals by combining the communication signal with a linearizing signal further described in [10]. The OPALS masking signal is based upon a linearizing signal similar to that used in LINC. Given a complex sample $a[k]$, the linearizing signal is computed as

$$e[k] = \begin{cases} j\sqrt{\frac{R_{max}^2}{\|a[k]\|^2} - 1}, & 0 < \|a[k]\| \le R_{max} \\ 0, & \text{otherwise} \end{cases} \qquad (3)$$

which can be used to create two sub-components of the original sample,

$$a^+[k] = a[k]\Big(1 + e[k]\Big) \qquad (4)$$

$$a^-[k] = a[k]\Big(1 - e[k]\Big) \qquad (5)$$

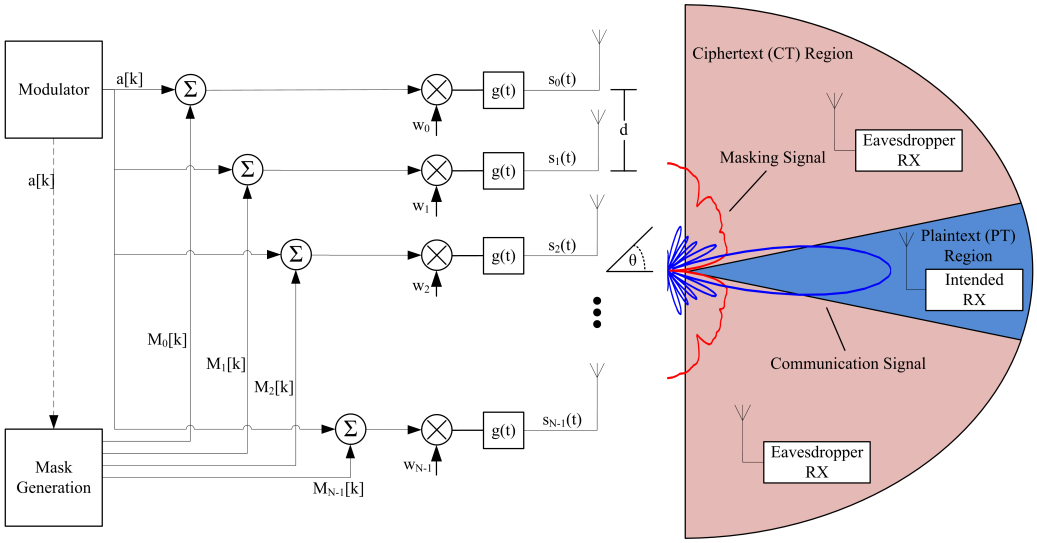


Fig. 1. System Context

These sub-components have two very important properties:

1) summing them together produces a scaled version of the original sample, viz $a^+[k] + a^-[k] = 2a[k]$
2) $\|a^+[k]\| = \|a^-[k]\| = R_{max}$ provided that $\|a[k]\| \leq R_{max}$

The discussion for the OPALS masking method follows: the first property provides the masking condition to prevent distortion for the intended receiver, and the second provides a constant-modulus signal for large enough values of R_{max}, which reduces stress on the amplifier. This is a key difference from the conventional LINC definition, which always assumes $\|a[k]\| < R_{max}$, providing for a gradual transition from the original signal to a constant-modulus one as R_{max} increases.

The masking signal to the n^{th} element, $M_n[k]$, is defined as:

$$M_n[k] = a[k]e[k]r_n[k] \tag{6}$$

where $r_n[k]$ is the n^{th} element of the *scrambling vector* $\boldsymbol{r}[k]$ such that:

$$\{r_n[k] = \pm 1, \quad \sum_{n=0}^{N-1} r_n[k] = 0 \quad \forall k\} \tag{7}$$

The scrambling vector is randomly generated on a per-symbol basis to randomly assign $a^+[k]$ and $a^-[k]$ to each element with the condition that there must always be an equal number of each.

In standard LINC, $N = 2$ and $\boldsymbol{r}^T = [-1, 1]$ for two branches with $\boldsymbol{r}$ fixed. It can be trivially shown that for this definition that $M_0[k] = -M_1[k]$ and $M_0[k] + M_1[k] = 0$. In the OPALS masking signal we extend this to an arbitrary number of elements $N \in [2, 4, 6, \dots]$, while maintaining the condition that $\sum_{n=0}^{N-1} M_n[k] = 0, \forall k$. This guarantees that the masking signal always cancels at the intended receiver.

Randomly generating the scrambling vector $\boldsymbol{r}[k]$ for each symbol has the same effect of generating a different distortion for each symbol as in dynamic DM. There are a finite number of permutations of $\boldsymbol{r}$, which is determined by N and given by:

$$C = \frac{N!}{\left[\left(\frac{N}{2}\right)!\right]^2} \tag{8}$$

The number of permutations, C, grows very rapidly with the size of the array.

C. Security Model

The system context of the security model for this work can be seen in Figure 1. For this work it is shown that the OPALS transmitter creates two distinct areas of reception: the *ciphertext (CT) region* and the *plaintext (PT) region*. These two regions differ in the fact that within the PT region the communication signal dominates, while in the CT region the masking signal dominates. For this sytem, the PT region is treated as though it is an area denied to the adversary; that is, the adversary is limited to only placing eavesdroppers in the CT region. It is important to note that that while the terms ciphertext and plaintext are usually used to denote cryptographic solutions, in this case they are used simply to denote whether or not the signal is obfuscated by the masking signal.

For the security model, the eavesdropper is modeled as a highly capable adversary. The most strenuous case of the adversary is that they have perfect knowledge of the transmitter and waveform. That is, the adversary knows the modulation scheme, the encoding, the frame structure and any other transmitter-specific parameters required. Furthermore, the adversary can estimate the correct time and phase offsets to recover the symbols.

The eavesdropper described is also modeled as having better gain than the intended receiver. This is in line with the worst case scenario where the adversary is aware of the fact that there is a communication signal. For our purposes we assume that the gain of the eavesdropper's system is sufficiently high

to be able to receive the worst-case sidelobe in the traditional beamforming (i.e. non-OPALS) transmitter.

III. Simulation

We have constructed a MATLAB model to characterize the performance of our OPALS technique and compare it against noise masking. Our model is a simplified version of a real-world communications system but deliberately includes many of the same features to measure performance under realistic conditions. This model includes a transmitter as shown in Figure 1, a simple non-fading AWGN channel model as in (2), and a receiver. The model implements a frame-based waveform using a preamble sequence and interspersed pilot symbols for synchronization. All results shown here were generated using 10^4 bits per frame with 120 preamble symbols and pilot symbols every 16 data symbols. This provides very robust frame detection and synchronization. A convolutional encoder/decoder are implemented with rate $1/2$ and constraint length 7. Results are shown here for QPSK and 16-QAM modulation using a root-raised cosine filter with upsampling ratio 8, filter length 4 symbols, and excess bandwidth 0.3. The transmit array is assumed to be 8 elements at $d = \lambda/2$ spacing with no amplitude weighting.

The eavesdropper receiver is identical to the intended receiver and gives identical results when no masking is added. Assuming a high gain, the receive SNR is set sufficiently high to allow reception in all sidelobes with no masking added.

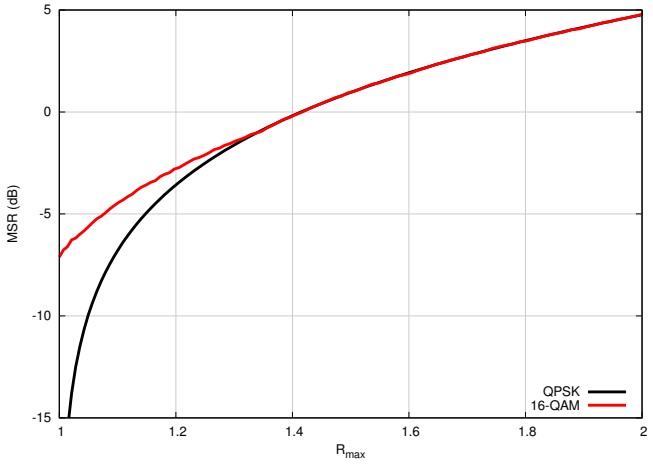
Besides the OPALS transmitter, two other transmitter designs are simulated for comparison. A transmitter with no masking is used as the conventional beamforming baseline. A noise-masking transmitter is also implemented to compare OPALS against the current state-of-the-art for physical layer encryption. The transmitted signals at each antenna element are normalized to have the same root-mean-square (RMS) amplitude for all masking types and parameters. All transmitters use the same root-raised cosine filter and have similar spectral content.

A. OPALS Secrecy Performance

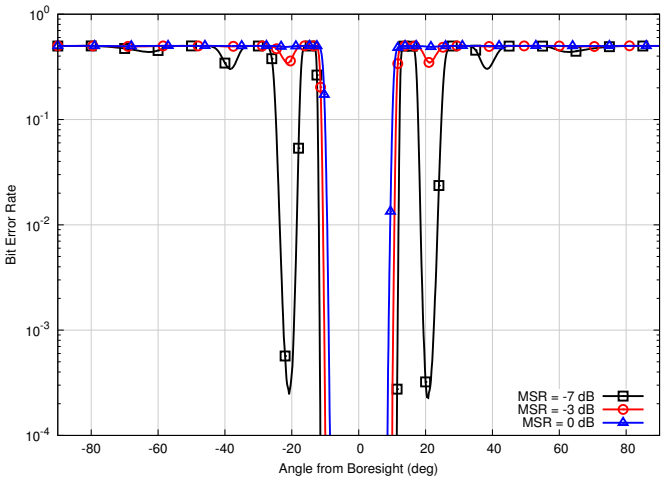
The OPALS transmitter design has a parameter R_{max}, as previously defined in (3), which can be chosen to adjust the trade space between secrecy and communication performance. R_{max} affects the amount of mask which is added to the signal. To provide a meaningful comparison between OPALS and other techniques, we introduce the *mask-to-signal ratio (MSR)*, defined as follows:

$$MSR[dB] = 20\log_{10}\frac{M_{rms}}{a_{rms}} \tag{9}$$

The MSR shows how much mask power is being transmitted relative to the signal power. For communication purposes, we wish to minimize the MSR in order to maximize the transmit power of the signal. Figure 2(a) shows the MSR for various values of R_{max}. MSR is zero (-inf dB) at $R_{max} = 1$ where no masking is present for QPSK. There is a lower limit of roughly -7 dB for 16-QAM modulation because some masking power is still added to the inner symbols even when $R_{max} = 1$, although it will eventually reach zero (-inf dB) for sufficiently small R_{max}. MSR reaches 0 dB (i.e. mask and signal amplitude are equal) at $R_{max} = \sqrt{2}$ for both modulation types. The MSR as defined in (9) can be applied to any masking technique, and will be used to compare the performance of OPALS against noise masking below. We will also attempt to determine an optimum MSR, which will be the minimum level at which an acceptable degree of secrecy is achieved.



(a)



(b)

Fig. 2. OPALS Secrecy Performance: (a) OPALS mask-to-signal ratio (MSR) vs. R_{max} and (b) OPALS bit error rate (BER) vs. angle for different values of mask-to-signal ratio (MSR) using QPSK

Figure 2(b) shows bit-error rate versus angle for OPALS transmitters with different levels of masking using QPSK modulation. With MSR at -7 dB, the first sidelobe is potentially vulnerable to an eavesdropper with the BER $< 10^{-3}$. Fairly good security is achieved for MSR at -3 dB, where the first sidelobe BER is now only slightly less than 0.5. A very high degree of security is achieved for MSR at 0 dB with BER equal to 0.5 everywhere outside the PT region. The width of

the PT region changes slightly moving from -7 dB to 0 dB MSR, narrowing from ± 12 degrees to ± 10 degrees.

B. Comparison to Noise-Masking

Now we will compare the secrecy performance of OPALS and noise-masking for similar values of MSR and both modulation types, using metrics for secrecy and transmitter dynamic range. As a secrecy metric, we will use first sidelobe BER. The BER in the first sidelobe tends to be the area of weakest secrecy outside the PT region as the magnitude of the signal is relatively high, as seen in Figure 2(b), so it serves as a useful metric for the relative performance of different techniques and mask levels.

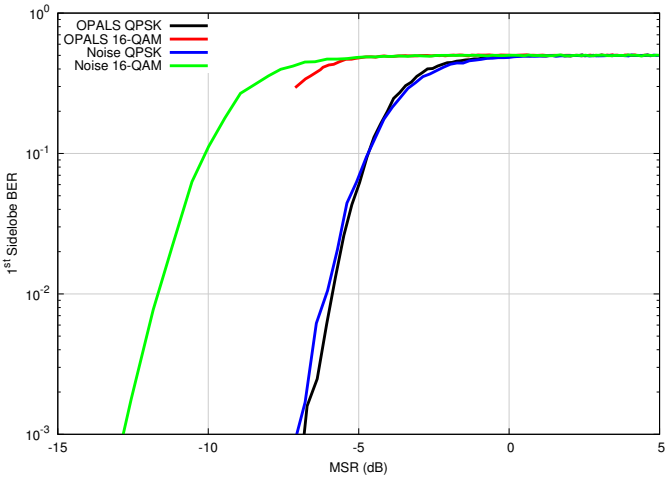
To measure the transmitter dynamic range we use the standard *peak-to-average power ratio*, or *PAPR*, which is defined as follows:

$$PAPR[dB] = 20 \log_{10} \frac{max\|s(t)\|}{s_{rms}} \tag{10}$$

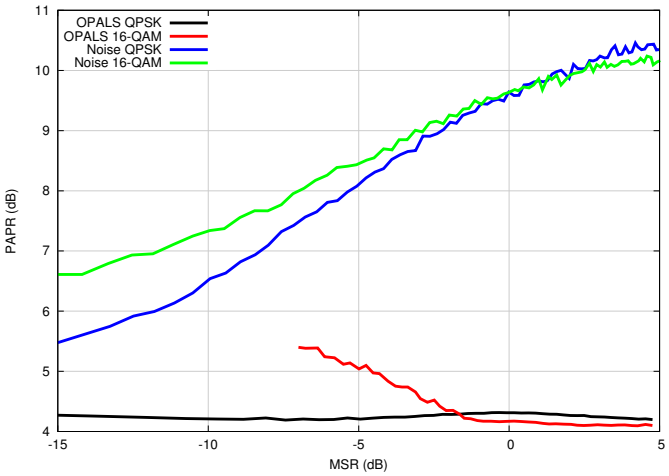
where s_{rms} is the RMS value of the signal $s(t)$.

Figure 3(a) shows the BER in the first sidelobe of the array pattern (here, $\theta = 21$) for OPALS and noise masking. We see here that OPALS and noise masking provide similar secrecy performance given the same mask-to-signal ratio. Noise masking provides slightly more secrecy at very low MSR for 16-QAM, but both offer a high degree of secrecy here and performance is identical at higher MSR so there is no significant advantage. Both techniques perform very similarly for QPSK over the entire range. For all modulation types, masking levels -3 to 0 dB below the signal power provide excellent secrecy.

Figure 3(b) shows how PAPR varies for different values of MSR for OPALS and noise masking using QPSK and 16-QAM modulation. First, note that the PAPR for noise masking is always relatively high, ranging from near 7 dB for low MSR and steadily increasing to over 10 dB as the masking power increases. Pure white noise has a very high PAPR, so as the MSR increases the PAPR of the combined signal also increases and noise begins to dominate. At the same time, the OPALS PAPR remains constant or decreases as the masking power increases. OPALS with QPSK modulation has a relatively constant PAPR of between 4.1 and 4.4 dB. Using 16-QAM modulation, the PAPR starts around 5.5 dB, steadily decreases, and is then constant at 4.1 dB as MSR increases. The structure of the OPALS masking signal guarantees that the pre-filter symbols have a constant magnitude, producing very good PAPR performance which is mostly constant with mask power. The shown PAPR results are for a system using a very aggressive pulse-shaping filter with sharply limited bandwidth, which introduces amplitude variation into the transmitted signals. The PAPR of an OPALS signal will decrease for less-aggressive filtering and will eventually become nearly. constant-envelope with sufficient bandwidth (expected to be roughly 2-3x the signal bandwidth). For a practical application, it is desirable for the transmitted signal to have the smallest PAPR possible for easy amplification to high power.



(a)



(b)

Fig. 3. OPALS and noise masking performance comparison for QPSK and 16-QAM modulations: (a) BER at the first sidelobe vs. MSR, and (b) PAPR vs. MSR

C. Optimum Masking

Previously we showed that both types of masking signals are able to achieve a high degree of secrecy given sufficient masking power is present. Now we will attempt to determine an optimum operating point for the masking signal which provides adequate security with maximum communication performance. To provide very good security with margin and deny as much information as possible to the adversary, a BER close to 0.5 is desirable, which indicates that the eavesdropper gains no more information from the message than from random guessing. Both OPALS and noise masking achieve this degree of secrecy at -5 dB MSR for 16-QAM modulation and at 0 dB for QPSK modulation.

We show the BER for conventional beamforming, noise masking, and OPALS across all angles in Figure 4(a) for QPSK and Figure 4(c) for 16-QAM. The eavesdropper is able to receive the conventional beamforming signal across almost all angles, except where nulls are present in the array

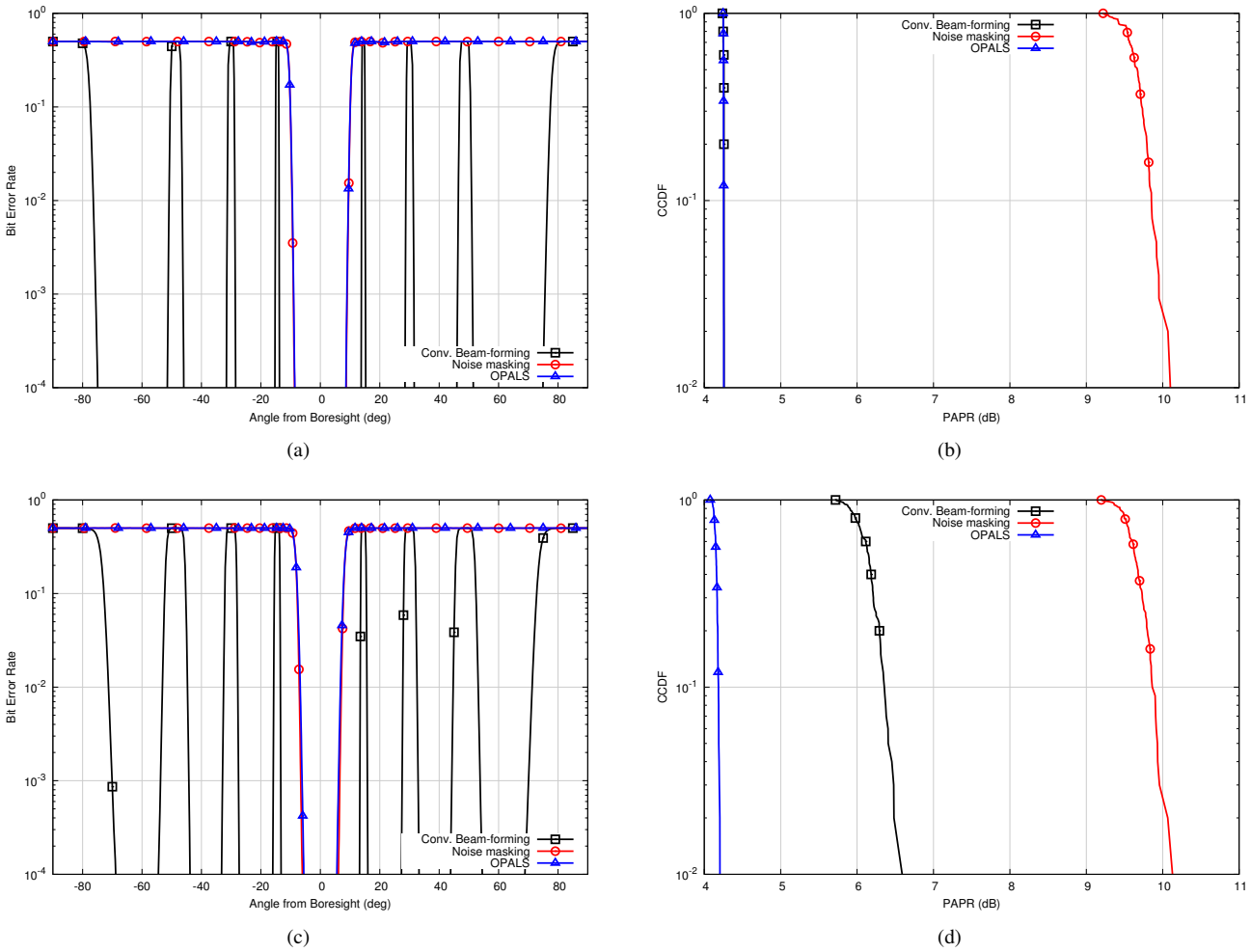


Fig. 4. Conventional beamforming, noise-masking, and OPALS at 0 dB MSR: (a) BER vs. angle, and (b) CCDF of PAPR for QPSK; (c) BER vs. angle, and (d) CCDF of PAPR for 16-QAM

pattern. Both noise masking and OPALS provide a high degree of secrecy with 0 dB MSR. As expected based on the performance shown in Figure 3(a), 16-QAM performs identically to QPSK under these conditions.

To illustrate the transmitter dynamics, the complementary cumulative distribution function (CCDF) is provided in Figure 4(b) and 4(d) for QPSK and 16-QAM respectively, showing the distribution of per-frame PAPR for each transmitter type and both modulations. The PAPR for OPALS is almost identical to the conventional transmitter and significantly less than noise masking for QPSK modulation. Using 16-QAM, the PAPR of OPALS is lower than both conventional transmitter and noise masking. The linearizing characteristics of OPALS remove the normal PAPR penalty a transmitter suffers when using a non-constant envelope modulation such as 16-QAM.

IV. Conclusions

In this paper we have described a new physical layer security technique which uses a masking signal based on LINC. We have shown that OPALS provides secrecy comparable to that of noise masking but with a significant improvement in amplifier efficiency as seen through a reduction in the peak-to-average power ratio to the transmitted signal for each antenna element. The OPALS transmitter architecture is designed so that it is transparent to existing receivers, allowing for it to be utilized in existing systems, and requires no key-sharing.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal, The*, vol. 28, no. 4, pp. 656–715, Oct 1949.

[2] A. Wyner, "The wire-tap channel," *Bell System Technical Journal, The*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[3] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *Communications Surveys Tutorials, IEEE*, vol. 16, no. 3, pp. 1550–1573, Third 2014.

[4] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[5] M. Daly and J. Bernhard, "Directional modulation and coding in arrays," in *Antennas and Propagation (APSURSI), 2011 IEEE International Symposium on*, July 2011, pp. 1984–1987.

[6] V. Pellegrini, F. Principe, G. de Mauro, R. Guidi, V. Martorelli, and R. Cioni, "Cryptographically secure radios based on directional modulation," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, May 2014, pp. 8163–8167.

[7] Y. Ding and V. Fusco, "Establishing metrics for assessing the performance of directional modulation systems," *Antennas and Propagation, IEEE Transactions on*, vol. 62, no. 5, pp. 2745–2755, May 2014.

[8] D. Cox, "Linear amplification with nonlinear components," *Communications, IEEE Transactions on*, vol. 22, no. 12, pp. 1942–1945, Dec 1974.

[9] H. Chireix, "High power outphasing modulation," *Proceedings of the Institute of Radio Engineers, The*, vol. 23, no. 11, pp. 1370–1392, Nov 1935.

[10] A. Birafane, M. El-Asmar, A. Kouki, M. Helaoui, and F. Ghannouchi, "Analyzing linc systems," *Microwave Magazine, IEEE*, vol. 11, no. 5, pp. 59–71, Aug 2010.