Secret-Focus: A Practical Physical Layer Secret Communication System by Perturbing Focused Phases in Distributed Beamforming

Xiaoran Fan[1], Zhijie Zhang[1], Wade Trappe[1], Yanyong Zhang[1], Rich Howard[1], and Zhu Han[2]

[1]Wireless Information Network Laboratory, Rutgers University, USA
[2]Department of Electrical and Computer Engineering, University of Houston, USA

***Abstract*— Ensuring confidentiality of communication is fundamental to securing the operation of a wireless system, where eavesdropping is easily facilitated by the broadcast nature of the wireless medium. By applying distributed beamforming among a coalition, we show that a new approach for assuring physical layer secrecy, without requiring any knowledge about the eavesdropper or injecting any additional cover noise, is possible if the transmitters frequently perturb their phases around the proper alignment phase while transmitting messages. This approach is readily applied to amplitude-based modulation schemes, such as PAM or QAM. We present our secrecy mechanisms, prove several important secrecy properties, and develop a practical secret communication system design. We further implement and deploy a prototype that consists of 16 distributed transmitters using USRP N210s in a $20 \times 20 \times 3\ m^3$ area. By sending more than $160M$ bits over our system to the receiver, depending on system parameter settings, we measure that the eavesdroppers failed to decode $30\% - 60\%$ of the bits cross multiple locations while the intended receiver has an estimated bit error ratio of 3×10^{-6}.**

***Index Terms*—Secret communication, distributed beamforming, physical layer security**

I. INTRODUCTION

Ensuring confidentiality of communication links is among the most fundamental objectives in developing communication systems. It is crucial for many applications to be able to distribute secure bit strings, such as higher-layer encryption keys, to wireless entities. Providing confidentiality is often a daunting task due to the broadcast nature of wireless links and therefore the ease of eavesdropping.

In addition to cryptographic mechanisms, many mechanisms that exploit a communication system's physical layer properties to protec secrecy have been proposed. These mechanisms usually aim to make the channel to the intended receiver much better than the channel to the eavesdropper. For example, wireless signal's propagation and fading properties have been exploited to increase capacity and enhance security in [1], [2], [3], [4]. Beamforming has been leveraged to increase the signal to noise ratio (SNR) at the intended receiver as well as to minimize the SNR for the eavesdropper using zero-forcing [5]. Artificial noise has been targeted at the eavesdropper to jam their reception [6]. Though these systems have demonstrated capabilities to communicate secretly, they have several drawbacks. Firstly, most of them assume that the eavesdropper's location is known, and there are only a small number (often just one) eavesdropper. Secondly, the practicality and efficient distribution of the secret in these proposed systems is questionable. Thirdly, many systems have shadow areas where the anti-eavesdropping mechanism is less effective. Fourthly, some systems assume the eavesdroppers possess less knowledge than the receiver. Therefore, supporting confidentiality remains a significant challenge in wireless communication systems.

Recently, distributed communication systems that involve a distributed collection of transmitters have received attention in the community. For example, a cellular provider may employ multiple basestations that are connected by dedicated backhaul. At the other end, it could just be a group of transmitters who are willing to coordinate their transmissions to a common receiver [7], [8]. In such systems, referred as distributed beamforming [9], the transmitters can form a coalition and achieve constructive superpositioning of signals at the intended receiver by aligning the received signals' phases, with the receiver sending a small amount of feedback. In this study, we refer to this type of distributed systems as *distributed phase alignment* systems and leverage such a system to facilitate secret communication.

By examining how the transmitter signals coherently combine at the receiver, we show that phase alignment accomplishes highly efficient secret communication against eavesdroppers without knowing their location, nor introducing any additional signal/noise. Also, to engage in secret communication, a distributed phase alignment system only needs to introduce very minor modifications to their normal transmission procedure. Once the transmitters align their phases at the receiver, they may start to communicate secretly to the receiver, by periodically dithering its phase around the proper alignment phase during transmission. In this way, the system naturally achieves secret communication. Firstly, the secret recipient's SNR is largely increased by aligning the phases at the intended recipient. Slight dithering of the phases later on has negligible impact on the alignment, but can create high received signal strength (RSS) variation at other locations, hindering anyone else from decoding the signal. Thirdly, it does not involve using interference for secrecy, which complicates system design, requires complex interference cancellation and

decoding, and regulations suggest is unlikely to be allowed in practical systems. We refer to this highly efficient yet practical secret communication mechanism as *Secret-Focus*.

In this paper, we show the effectiveness of Secret-Focus through both analysis and prototyping (using N210 USRPs). Our experimental results show that the intended recipient has bit error ratio (BER) as low as 3×10^{-6} while eavesdroppers have a much higher BER ranging from 31% to 38%, from measuring different eavesdropper locations for a total of $164.79M$ bits. In addition to the main test area, we have also examined extreme eavesdropper locations to further demonstrate it has little shadow area. We show that when the eavesdropper antenna is side by side(approx. 1cm) with the receiver antenna, the resulting BER is 12.45%; when the eavesdropper antenna is one wavelength (approx. 30cm) away from one of the transmitter antennas, the BER is 27%.

To summarize, we make the following contributions in this work. Going beyond beamforming and jamming based techniques, we propose a new phase combining and dithering based secret communication mechanism, prove its salient properties, and build a prototype system to validate these properties. Without interfering with the underlying communication or hurting the data rate, our mechanism can be easily combined with any amplitude-based modulation schemes such as PAM or QAM. More importantly, our approach works without requiring the system to know the eavesdropper's location or injecting noise before hand, and can disable eavesdroppers even at tricky locations such as in close proximity to the intended receiver or in close proximity (one wavelength) to a transmitter antenna.

II. Background on Secret Communication Systems

As a starting point, we provide a background of physical layer secret communication systems. In a secret communication system, a sender (Alice) wishes to reliably deliver a secret message S to an intended receiver (Bob) in the presence of an eavesdropper (Eve). The secret message S is then subsequently encoded into a signal X that is transmitted by Alice, Bob receives a signal Y while Eve receives a signal Z. The objective in information-theoretic secrecy is to ensure that Eve learns as little information as possible about the original secret message S. The past decade has seen the physical layer community makes significant contributions in providing secrecy for wireless channels.

Physical Layer Secret Communication for Wireless Channel: Several mechanisms have been discussed for achieving secrecy communication over the wireless channel. For example, the properties of wireless signal propagation and fading have been exploited for improving secrecy [10]. Also, the broadcast nature of the wireless channel allows one to introduce interference to hinder eavesdropping [11], [12], [13].

Physical Layer Secret Communication for Beamforming Systems: A number of secret communication mechanisms have been discussed for beamforming systems, such as those in [14], [15], [16]. With beamforming, Alice can leverage the directionality of the beam pattern to gain a better spatial diversity and ensure Bob's SNR is significantly higher than Eve's SNR at most locations. Moreover, by adopting zero-forcing [5], Alice can perform beam-nulling at Eves' location to further decrease their SNR. Further, Eve can also be jammed by the system intentionally sending artificial noise towards its direction [6], as illustrated in Fig. 1(a).

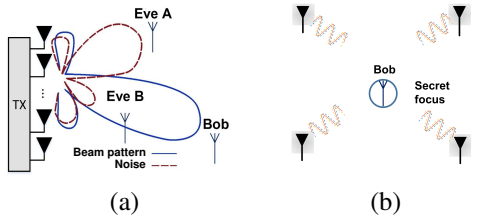


Fig. 1. (a) shows a beamforming based secure communication system, in which artificial noise is used to jam Eve. (b) illustrates Secret-Focus in which distributed transmitters first align their phase at Bob and then perturb their phases around the alignment phase to focus the secret message at Bob.

However, beamforming-based schemes have drawbacks and are quite different in effect than Secret-Focus. Firstly, in order to perform beam-nulling or jamming, a common assumption is that Alice knows Eve's locations. In many scenarios, it is impossible to predict Eve's location. Secondly, some of them may not need to know Eve's location [14], introducing artificial noise can be costly, which may also impair Alice's transmission towards Bob. Thirdly, such a design implies that any eavesdropper in the path of the main side lobe may be empowered to decode the signal. Consequently, linear-array style beamforming is not ideally suited for secrecy communication. Instead, as illustrated in Fig. 1(b), it is desirable to leverage a set of distributed transmitters to collectively communicate to the target receiver. Those are what motivate the design of Secret-Focus. By adopting our methods, we achieve highly secure communication without knowing Eve's location or sending any additional noise.

III. Perturbing Aligned Phases for Secret Communication

Secret-Focus involves a collection of transmitters that are distributed geographically, and who transmit secret bit strings to the intended recipient in a coordinated fashion: first reaching a steady state by aligning their phases at the recipient and then dithering their phases around the steady state phase (which we refer to as Φ_{algn}) while communicating bit strings. Specifically, each transmitter adjusts the phase of their communication signal and, with the help of a small amount of feedback from the recipient (Bob), without assuming any knowledge about Eve, they achieve significantly improved signal quality at the recipient compared to that witnessed by an unintended receiver (Eve).

There are many approaches for transmitters to align their phases, but the specific details for how this alignment occurs has little bearing on how secrecy is achieved. Later, in Section IV-A, we explain the phase alignment procedure we use to prototype Secret-Focus, but here we focus on examining how

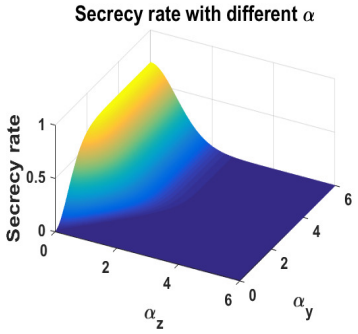


Fig. 2. Theoretical secrecy rate as a function of α_y and α_z. Communication is secret when we have $\alpha_y > \alpha_z$, and while keeping α_z small enough.

phase alignment creates Alice-Bob advantage relative to Alice-Eve, and thereby supports secrecy for Alice-Bob.

To do this, we assume all transmitters know the secret message to transmit. Then, motivated by [10], [17], which showed that discrete signaling can often outperform Gaussian signaling for secrecy, Secret-Focus starts with a basic pulse amplitude modulation scheme in which each transmitter will transmit a suitably phase-aligned *high* signal to transmit a 1 bit, and a phase-aligned *low* signal to convey a 0 bit (see Fig. 3(a)). These will constructively add at Bob to produce a received signal Y, while an eavesdropper Eve will witness a signal Z. With each transmitter slightly dithering phases after alignment, each mode of Y will have a mean corresponding to how well the phase alignment combines constructively at Bob, and a variance from noise. Hence, signal values Y can be modeled by a mixed (complex) Gaussian with two modes, where one mode corresponds to the 1 bit and the other corresponds to 0 bit (see Fig. 3(b)), and similarly for Z.

We may calculate the secrecy rate $I(X;Y) - I(X;Z)$, which captures the achievable rate at which Alice-Bob could secretly communicate in the presence of Eve, with the high/low discrete signaling. Using $I(X;Y) = H(Y) - H(Y|X)$, and the differential entropy $H(Y)$ for a mixed Gaussian[18], we define the intermediate terms, the ratio of the means to variances, as the *secret communication ratio (SCR)* $\alpha = \frac{\mu}{\sigma}$ for each recipient (be it Bob or Eve), where μ and σ are the average signal value and standard deviations, illustrated in Fig. 3(b). Noting that the $H(Y|X)$ collapses to $H(Y|X) = \frac{1}{2}\ln(2\pi e\sigma_y^2)$, $I(X;Y)$ becomes $I(X;Y) = \alpha_y^2 - I_y$, where:

$$I_y = \frac{2}{\sqrt{2\pi}\alpha_y} e^{-\alpha_y^2/2} \int_0^\infty e^{-x^2/2\alpha_y^2} \cosh(x) \ln(\cosh(x)) dx. \tag{1}$$

Thus, the secrecy rate for our choice of X is $(I(X;Y) - I(X;Z))^+ = (\alpha_y^2 - \alpha_z^2 + I_z - I_y)^+$. We illustrate the secrecy rate in Fig. 2.

Then in order to differentiate Alice-Bob from Alice-Eve, a positive and higher secrecy rate is desirable, hence we design Secret-Focus such that $\alpha_y > \alpha_z$, and a higher α_y and lower α_z yields a better secrecy (as illustrated in Fig. 2). Specifically, since $\alpha = \frac{\mu}{\sigma}$, our design goal is to *achieve a higher SNR and lower signal variation at Bob while having a lower SNR and higher signal variation at Eve*.

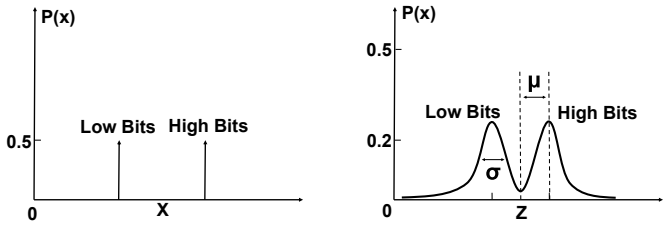


Fig. 3. (a) Alice generates low bits and high bits following amplitude based modulation. (b) shows a typical distribution of bits received by Bob. Received bits follow a mixed (complex) Gaussian distribution.

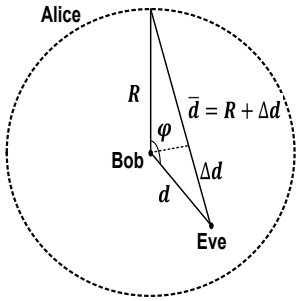


Fig. 4. The geometric relationship between Alice, Bob and Eve, which is used in (3) and (4) when calculating the normalized RSS at Eve's location $Y(d)$.

Secret-Focus achieves this objective through two complementary mechanisms: first, significantly improve μ_y using multiple transmitters focusing their efforts; and, second, relatively increase σ_z at Eve through intentionally introducing additional phase perturbations following phase alignment, which has a minimal effect at Bob. In the rest of this section we discuss these two mechanisms in detail, and also present a discussion in the end.

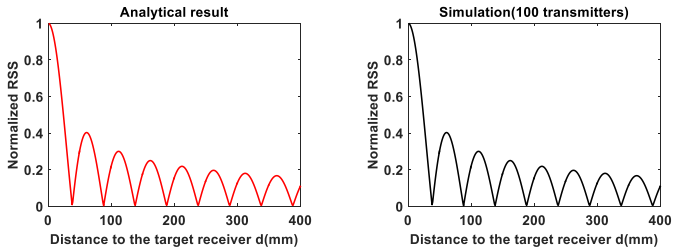
A. Mechanism 1: Combining Phases Increases μ_y

The first key idea of our design is to place transmitters around the target receiver, as illustrated in Fig. 1(b), to achieve an effect similar to how Fresnel zone plates [19] focus light at a focal point. In optical systems, Fresnel zone plates act as a phase shifter for the passing light, similar to how our transmitters alter the phases of emitted radio waves.

To understand the radio focusing effects, suppose we place transmitters on a circle with radius R in free space around the receiver, and they coherently combine their phases at the center. Assuming, without loss of generality, that they align their phases at 0 degrees at the center, then the normalized magnitude of the signal values (RSS) is given by:

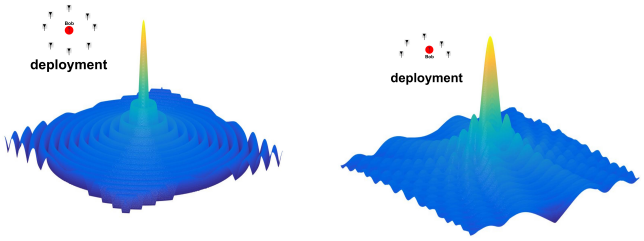
$$Y_{target} = |\frac{R}{N}\sum_{i=1}^{N}\frac{1}{R}e^{j0}| = 1. \tag{2}$$

As shown in Fig 4, suppose we want to measure the normalized RSS at an Eavesdropper's location at a distance d to the target receiver. For an arbitrary transmitter and with the free space model, and with the free space model, the phase



(a) (b)

Fig. 5. (a) Analytic results for the normalized RSS function $Y(d)$ in (4), where RSS decreases with d. (b) Numerical results of RSS versus d, where 100 transmitters were placed in a circle around the target. The numerical results match analytical results exactly.



(a) (b)

Fig. 6. (a) Simulation results of RSS distribution in a $1m$ by $1m$ area around Bob. It is clear that the energy is sharply focused around the target location. In (b), we decrease the number of transmitters to 30, and place them on a half circle. Note the target receiver is also not placed at the center. As can be seen, even though the energy focus is wider, the peak is still very pronounced compared to other locations.

difference between the focus location and the measurement location is:

$$\Delta\phi = 2\pi\frac{\sqrt{R^2+d^2-2Rd\cos\varphi}-R}{\lambda}. \tag{3}$$

As we approach an infinite amount of transmitters around the circle, we can write the normalized RSS at the measurement location as:

$$\begin{aligned} Y(d) &= |\lim_{N\to\infty}\frac{R}{N}\sum_{i=1}^{N}\frac{1}{d}e^{j2\pi\frac{\sqrt{R^2+d^2-2Rd\cos\varphi_i}-R}{\lambda}}|, \varphi_i\in[0,2\pi] \\ &= \frac{R}{2\pi}|\int_0^{2\pi}\frac{e^{j2\pi\frac{\sqrt{R^2+d^2-2Rd\cos\varphi}-R}{\lambda}}}{\sqrt{R^2+d^2-2Rd\cos\varphi}}d\varphi|. \end{aligned} \tag{4}$$

Fig. 5 compares the result from analytic RSS expression $Y(d)$ and the simulation result, for a RF signal being emitted with frequency 3GHz. In the simulation, we placed 100 transmitters on a circle, with the focus location at the center. Note that the results are identical, and therefore verify our analytical derivation. Using our analytical result, for an asymptotically large number of transmitters, one can verify that the 3dB-down distance from the receiver is $d_{3dB} \approx 0.22\lambda$. For a smaller number of transmitters, d_{3dB} would still be proportional to the radio wavelength λ as long as transmitters are placed around the target receiver.

Further, we can see in Fig. 6(a) that the results for the normalized RSS expression $Y(d)$ has a spatial pattern similar to the magnitude of a sinc function, with the maximum at the target receiver location. This location corresponds to where transmitter signals coherently combine (phases aligned) and, intuitively, there is no other location with such high energy.

Mathematically, the normalized RSS function $Y(d)$ gives us what we desire for Secret-Focus: we only have one maximum energy location spatially, and low energy at other locations. Now we take a look at the normalized RSS expression $Y(d)$, due to the symmetry of transmitters placement respect to the focus location, we can ignore the path loss term $\frac{1}{d}$ in our analysis, giving:

$$\begin{aligned} Y(d) &= \frac{1}{2\pi}|\int_0^{2\pi}e^{j2\pi\frac{\sqrt{R^2+d^2-2Rd\cos\varphi}-R}{\lambda}}d\varphi|, \\ &= |\lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N}e^{j2\pi\frac{\sqrt{R^2+d^2-2Rd\cos\varphi_i}-R}{\lambda}}|, \varphi_i\in[0,2\pi]. \end{aligned} \tag{5}$$

While performing above summation, if d is not zero, as φ_i varies in $[0,2\pi]$, $\sqrt{R^2+d^2-2Rd\cos\varphi_i}$ will vary, so that the phase term $2\pi\frac{\sqrt{R^2+d^2-2Rd\cos\varphi_i}-R}{\lambda}$ will not be the same for different i in the summation. We know that the maximum of this summation is achieved when the phase of each term aligns, and as a result we have:

$$\begin{aligned} Y(d) &= |\lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N}e^{j2\pi\frac{\sqrt{R^2+d^2-2Rd\cos\varphi_i}-R}{\lambda}}|, \varphi_i\in[0,2\pi] \\ &\le |\lim_{N\to\infty}\frac{1}{N}\sum_{i=1}^{N}e^{j2\pi\frac{\sqrt{d^2}-d}{\lambda}}| = Y(0). \end{aligned} \tag{6}$$

As d varies from 0 to $+\infty$, according to the above analysis, the only way to align the phase term is to set $d = 0$. Hence, $Y(0)$ is the unique global maximum. In other words, as transmitters aligning their phases at a certain location, the RSS at other locations would be less than the RSS at that location.

In real world implementations, a large number of transmitters are usually prohibitive. However, as long as we have sufficient transmitters placed around the receiver (regardless of whether they are placed in a regular or irregular pattern), we can still achieve a focus on the target receiver. Fig. 6(b) shows another result when only 30 transmitters are placed on a half circle around the target receiver (target receiver is not placed at center). Further, in practice, these results extend straightforward to three-dimensional deployment scenarios.

B. Mechanism 2: Dithering Phase Hurts Eve

The second key idea of our design is to have the transmitters, once phase aligned, repeatedly perturb their phases around the alignment phase. In doing so, the signal values measured by Eve fluctuate significantly, hindering Eve's ability to decode the received signal. At the same time, as we will show, such perturbation does not harm Bob's decoding ability. Below we will prove the effectiveness of this mechanism.

Bob's RSS Remains Stable Even with Perturbation: First, note that the received signal in the free space model at an arbitrary location is:

$$\vec{Y}(\phi_1, \phi_2, ..., \phi_N) = \sum_{i}^{N} A_i e^{j\phi_i}. \quad (7)$$

where A_i and ϕ_i denote the amplitude and phase of the i^{th} signal source received at the location, and N is the number of signal sources (transmitters). Next, the real and imaginary part of the received signal are:

$$\begin{aligned} \vec{Y}_{real} &= A_1 + A_2 \cos\theta_1 + A_3 \cos\theta_2 + ... + A_n \cos\theta_{N-1}, \\ \vec{Y}_{img} &= A_2 \sin\theta_1 + A_3 \sin\theta_2 + ... + A_n \sin\theta_{N-1}. \end{aligned} \quad (8)$$

in which θ_i is the phase difference between signal $i+1$ and the first signal (i.e., with ϕ_1 as the reference phase). Thus, the squared amplitude of the received signal is $Y^2(\theta_1, \theta_2, ..., \theta_{N-1}) = \vec{Y}^2_{real} + \vec{Y}^2_{img}$. The derivative of Y^2 with respect to θ_{i-1} is given by:

$$\begin{aligned} &\frac{\partial Y^2}{\partial \theta_{i-1}} = 2A_{i+1}(-A_1 \sin\theta_{i-1} + A_2 \sin(\theta_1 - \theta_{i-1}) + \\ &A_3 \sin(\theta_2 - \theta_{i-1}) + ... + A_N \sin(\theta_{N-2} - \theta_{i-1})). \end{aligned} \quad (9)$$

in which $i \in [2, N]$. Considering $\theta_1, \theta_2, ..., \theta_{N-1}$ are independent, the impact of small phase perturbations upon $Y^2(\theta_1, \theta_2, ..., \theta_{N-1})$, is the sum of the partial derivatives:

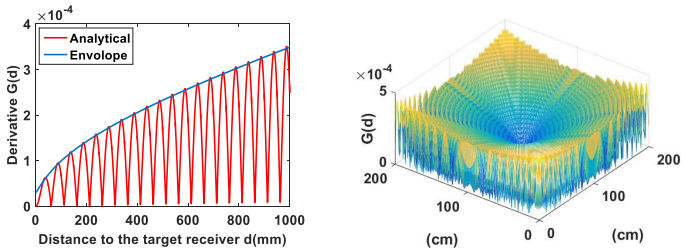
$$\begin{aligned} G(\theta_1, \theta_2, ..., \theta_{N-1}) &= \sum_{i}^{N-1} \frac{\partial Y^2}{\partial \theta_i}, \\ &= -2A_1(A_2 \sin\theta_1 + A_3 \sin\theta_2 + ... + A_N \sin\theta_{N-1}). \end{aligned} \quad (10)$$

Here, $\theta_1 = \theta_2 = ... = \theta_{N-1} \approx 0$ since the signal sources are properly phase aligned, giving $G(\theta_1, \theta_2, ..., \theta_{N-1}) \approx 0$ at the target receiver. In particular, the target location has the lowest variability with respect to phases $\theta_1, \theta_2, ..., \theta_{N-1}$ because the slope $G = 0$. Hence, we have shown that *Bob's RSS values will NOT fluctuate much due to small phase perturbations we choose to introduce*.

Eve's RSS Becomes Unstable and Has Large Variation: Next, we examine the impact that small fluctuations around the phase alignment optimum would have upon Eve. Assume a large number of transmitters on a circle $N \to \infty$, and the target receiver at the center. Similar to Equation 4, we calculate $G()$ at a distance d from Bob's location, which we refer to as $G(d)$. By taking the limit, we get the integral:

$$G(d) = -2 \int_0^{2\pi} \frac{\sin\left(2\pi \frac{\sqrt{R^2 + d^2 - 2Rd\cos\varphi} - R}{\lambda}\right)}{(R-d)\sqrt{R^2 + d^2 - 2Rd\cos\varphi}} d\varphi. \quad (11)$$

In order to understand the implication of $G(d)$ in our design, we show the $G(d)$ distribution in Fig. 7 ($R = 10m$ and $\lambda = 0.1m$). From the results, we observe that if we make a small change in phases around the optimal value for Alice-Bob, then since Eve's $G(d)$ is large, her signal variation will be large, and this variation increases with d (as shown by the envelop curve in Fig. 7(a)). Here, an interesting observation is that, in some cases, Eve's $G(d)$ values actually do reach zero. However, we note that at those points, a tiny change in the distance/phase will lead to substantial changes in $G(d)$. As a result, even if Eve momentarily has $G(d) = 0$, frequent dithering of the phase will lead to a new state with large $G(d)$. Overall, Eve's RSS variation is significantly higher than Bob's, which as we will show later leads to an intolerably high decoding error.



(a) (b)

Fig. 7. (a) The analytical results for $G(d)$ in (11). The envelop of $G(d)$, marked in blue, shows that Eve's RSS variation increases with d. (b) The distribution of $G(d)$ in a $2m \times 2m$ area around Bob shows the same trend. We observe the lowest G value at Bob's location.

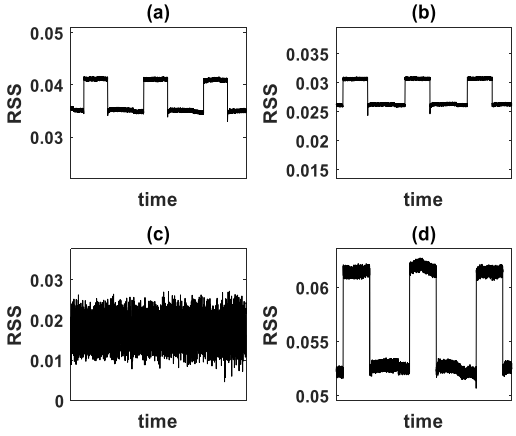


Fig. 8. (a) Raw RSS at Eve for a broadcast channel (neither mechanism employed), (b) raw RSS at Eve for a NO-Perturb system (only mechanism 1 employed), (c) raw RSS at Eve for Secret-Focus (both mechanisms employed), and (d) raw RSS at Bob for Secret-Focus. In this example, only Secret-Focus is able to hinder Eve from decoding received signal and provide secret communication to Bob.

C. Effectiveness of the Two Mechanisms

Fig. 8 shows: (a) the raw RSS at Eve when transmitters are completely distributed and do not coordinate among themselves (thus a normal broadcast channel in which neither mechanism is employed), (b) the raw RSS at Eve when transmitters perform phase combining, but keeping the phase at Φ_{align} during communication without perturbing the phase (which we refer to as *NO-Perturb* in which only mechanism 1 is employed), (c) the Raw RSS at Eve in Secret-Focus that employs both mechanisms, and (d) the raw RSS at Bob in Secret-Focus.

We observe that for the broadcast channel, both Eve and Bob receive the same RSS time series (with slightly different amplitude), and hence no secret between Alice and Bob. We have the similar observation in the NO-Pertub system which also fails to protect secrecy between Alice and Bob. However, applying both mechanism, the signal Eve receives in Secret-Focus fluctuates greatly over time, hiding the secret from Eve.

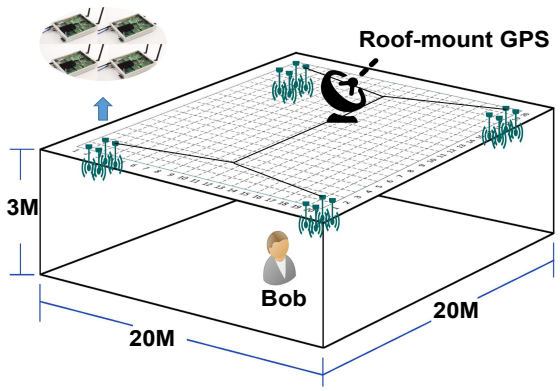


Fig. 9. The Secret-Focus prototype consists of 16 transmitter USRPs. The deployment area of our prototype is $20 \times 20 \times 3\ m^3$.

Having explained how Secret-Focus achieves secrecy, we next build a prototype system in Section IV and evaluate its effectiveness in Section V.

IV. Putting Together a Secret-Focus Communication System

We have proved that having distributed transmitters align their phases and then employ slight dithering (around the proper alignment phase Φ_{algn}) can achieve a positive secrecy rate as it leads to higher and more stable RSS values at the intended receiver, but lower and less stable RSS values at other locations. These properties can be readily harnessed to facilitate secret communication through amplitude-based modulation schemes, such as on off key (OOK) communication, pulse amplitude modulation (PAM), or quadrature amplitude modulation (QAM). In this section, we discuss how we can design a practical Secret-Focus system and present our effort in building a Secret-Focus prototype using USRP $N210$s. Our objective in this paper is to demonstrate that distributed phase alignment among a group of transmitters can achieve secret communication at the target location using the N210s.

Our prototype consists of 16 transmitters mounted on a ceiling, at four corners of a $20\times20\ m^2$ area. We used WBX RF daughter boards on the N210s, and our working frequencies are 915 and 964 MHz in this study. There is no communication back-channel between the transmitters, so they are completely distributed in nature. We synchronized the transmitter clocks through a roof-mount GPS. Fig. 9 shows a typical prototype setup, with 4 $N210$s at each of the four corners (these four USRPs are 1 meter apart from each other). The receiver can be *anywhere* in the deployment area.

Fig. 10 shows how a Secret-Focus system works. It goes through two main stages: the distributed phase alignment stage and the secret communication stage. We next discuss the design and implementation of these two stages.

A. Trial-and-Error Distributed Phase Alignment

We chose to adopt a simple trial-and-error approach proposed in [9]. Assuming all nodes share the same clock, we partition the time into rounds of equal duration. Within each

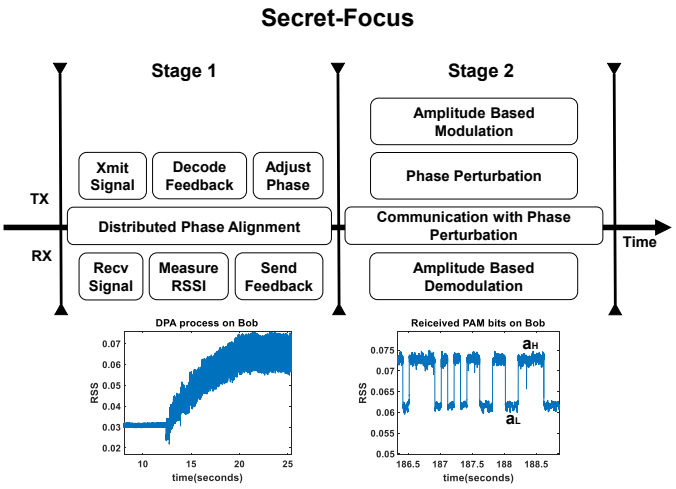


Fig. 10. Secret-Focus consists of two main stages: distributed phase alignment, and secret communication with phase perturbation.

round, every transmitter sends a signal to the receiver at a randomly adjusted phase, with the phase randomly picked within $\pm\Phi^\circ$ of the previous phase value. At the end of each round, the receiver sends a small feedback message to indicate whether the new phase combination gives higher energy than before. If so, each transmitter holds this new phase value; otherwise, it goes back to its previous value. The phase adjustment is defined as:

$$\theta_i(n+1) = \begin{cases} \theta_i(n) + \delta_i(n), & \text{if } Y[n] > \max\limits_{k<n} Y[k], \\ \theta_i(n), & \text{otherwise.} \end{cases} \tag{12}$$

where $\theta_i(n)$ denotes transmitter i's phase in round n, and we have $-\Phi \leq \delta_i(n) \leq \Phi$.

Though simple, we find that this approach effective in focusing transmitting signals and aligning their phases to Φ_{algn}. In implementing this algorithm, we write multiple out-of-tree GNU radio modules (GNU radio version 3.7.6.1.) and adopt a width-based modulation method to encode/decode the receiver feedback beacons. We fix the feedback rate at 25 Hz, which is also the transmitter phase adjustment rate. Received signal at Bob during an example phase alignment is included in Fig. 10.

B. Amplitude Modulation (AM) Based Secret Communication

When the transmitter phases are properly aligned at Φ_{algn}, the receiving USRP (Bob) broadcasts a pre-defined constant signal in 964 MHz to tell the transmitters to start communication. This explicit signaling ensures that all transmitters and receivers enter the communication stage at the same time. In the communication stage, the transmitters (Alice) focus on two tasks: amplitude based modulation and frequent phase perturbation. In our prototype, we chose to use one-bit pulse amplitude modulation (PAM) for its simplicity, in which each symbol's amplitude is modulated as $\bar{A} = [a_L, a_H]$. Here, the amplitude of high bits and low bits, a_H and a_L, are important

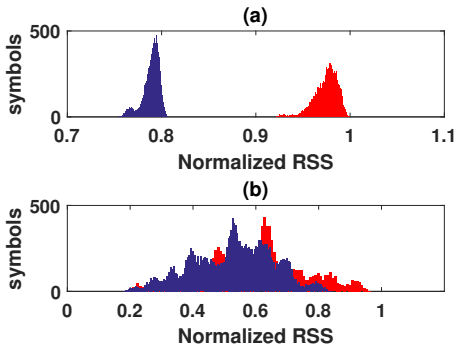


Fig. 11. (a) Histogram of Bob's RSS values, where high bit symbols and low bit symbols are clearly separated. (b) Histogram of Eve's RSS values, where high bit symbols and low bit symbols are largely mixed.

system parameters. We evaluate their impact and present the results in Section V-C1.

Phase perturbation in the communication phase ensures the RSS values at any non-target location have much greater variation than those at the target location, while ensuring all transmitter phases are still aligned at the target location. Specifically, each transmitter perturbs its phase around Φ_{algn} at a certain rate: in each perturbation interval, it randomly picks a value within $\pm\phi$ and adds that value to Φ_{algn}. In the evaluation, we have studied the impact of ϕ and present the results in Section V-C2. In addition, the perturbation rate is also an important parameter. Faster perturbation can handle more capable eavesdroppers. In our prototype, we set the perturbation rate as 100Hz.

At the communication stage, the receiver focuses on measuring the received RSS and decoding each bit accordingly. We assume the receiver (both Bob and Eve) knows the symbol duration t_{sb}. We apply a window based demodulation scheme. Specifically, after receiving the header, for each incoming payload bit, we measure the RSS during its symbol period and compare it against the average RSS within a pre-set window duration. If the current bit RSS is higher than the recent window average, the bit is decoded as 1; otherwise, it is a 0. In this paper, we assume that Eve and Bob both have the knowledge of t_{sb} and header length, but in reality we note that Eve often is not equipped with such knowledge.

C. An Example Scenario

To illustrate the point, let us look at a typical secret communication scenario. In the example setting, we have 16 USRP N210 transmitters (shown in Fig. 9), in which Bob is at the red dot in Fig. 12 and Eve is at the E2 location in Fig. 12. In this example, the transmitters send 1200 bits to Bob, with 80 consecutive low bits as the header, and the rest as the payload (consisting of randomly generated 1s and 0s). We have $a_H = 1$ and $a_L = 0.8$.

For each transmitted bit, we measure the RSS, normalize the value to between 0 and 1, and place it in the corresponding RSS bins. We plot the histogram in Fig. 11. For each normalized RSS bin, we plot the number of bits whose RSS values fall in that bin. We further separate the number of high bits and low bits within each bin. The RSS values for Bob's high bits and low bits are clearly separated by a large margin, while the RSS values for Eve's high bits and low bits are largely overlapped with each other, hard to be separated.

Here, the decoding bit error ratio (BER) is the ratio between the number of incorrect bits and the total bits transmitted. Here Eve's BER is 42.1%, which is close to a completely random system with BER of 50%. At the same time, Bob correctly decodes all the bits. Hence, communication between transmitters and Bob is kept secret. We assume that Bob and Eve both have the knowledge of symbol duration, header length, and communication start time.

V. Prototype Evaluation

In this section, we report the measured results and show that Secret-Focus is indeed able to provide efficient secret communication between the transmitters and the receiver, regardless of eavesdropper's count and locations. Throughout our evaluation, we assume Bob and Eve have the same knowledge and capability.

A. Secret-Focus Makes Eavesdropping Impossible

The objective of the first set of experiments is to show that Eve cannot eavesdrop the communication regardless of the location. For this purpose, we use the $7 \times 7\ m^2$ square in the center of the deployment area as the test area (illustrated in Fig. 12). We place a USRP receiver (Bob) at the center of the test area (see the red dot in Fig. 12) and placed another USRP receiver (Eve) at 100 different locations in the test area (see the blue dots in Fig. 12). We measured more eavesdropper locations closer to the target receiver to investigate whether eavesdroppers near Bob are able to decode the communication. In these experiments, we used all of the transmitters $N = 16$, with $a_H = 0.7$, $a_L = 0.5$, and $\phi = 15°$. At each location, we collected a total of $20,000$ high bit symbols and $20,000$ low bit symbols with symbol duration $t_{sb} = 20ms$.

Fig. 13 shows the measured average α_{Bob} and 100 different α_{Eve} values. We observe that α_{Bob} is clearly much higher than α_{Eve}. Specifically, we have $\alpha_{Bob} = 9.42$, $\alpha_{Eve}^{max} = 1.54$, and $\alpha_{Eve} < 1$ for 81 out of 100 locations.

Next, we compare Secret-Focus with a normal broadcast channel and a NO-Perturb system (in which transmitters do not perturb their phases once aligned). Measuring the same 100 Eve locations, we plot the α_{Eve} distributions for the three systems in Fig. 15. Please recall, as shown in Fig. 2, a system with *better* secret communication has *lower* α_{Eve} values. The results show that Secret-Focus fares much better than the other two systems. In Secret-Focus, α_{Eve} values are within [0.12, 1.53], while [3.03, 5,98] for NO-Perturb, [4.01, 5.99] for Broadcast only.

B. Low Decoding Error for Bob vs High Error Rate for Eves

The objective of the second set of experiments is to show that Bob can decode the secret bit strings with a very high success rate while Eve cannot. In order to estimate Bob's BER that is very low, we send $164.79M$ bits from Alice to Bob

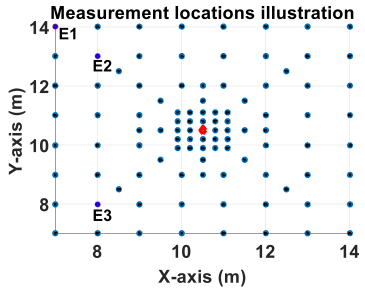


Fig. 12. A 7×7 m^2 test area. We placed Bob (red) in the center, and Eve at 100 possible locations (blue). Eve locations not uniformly distributed, but denser towards the center.

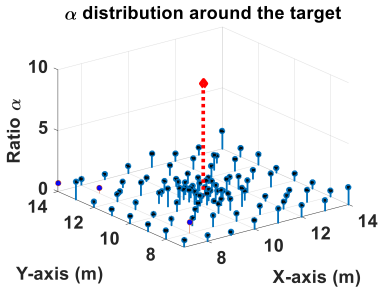


Fig. 13. The measured average α_{Bob} is significantly higher than α_{Eve} at all 100 Eve locations. Thus, Bob can have secret conversation with Alice in the presence of Eve at these 100 locations.

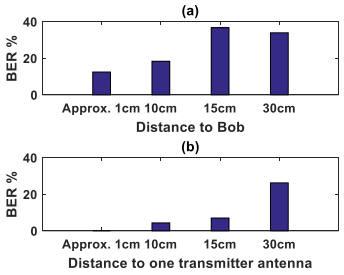


Fig. 14. Extreme Eve locations outside of the test area. BER = 12.45% when she is side-by-side with Bob, and $BER = 7\%$ when she is 15cm (half a wavelength) away from one transmitter antenna.

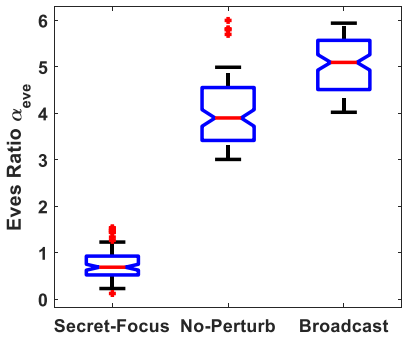


Fig. 15. Secret-Focus has much lower α_{Eve} values than Broadcast and NO-Perturb. It provides better support for secret communication.

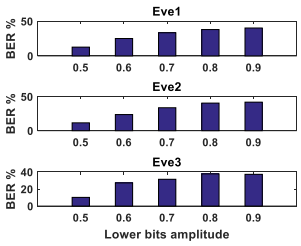


Fig. 16. BER vs. a_L.

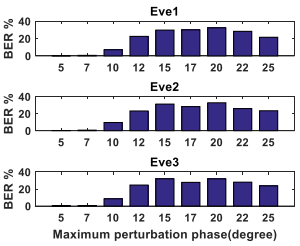


Fig. 17. BER vs. ϕ.

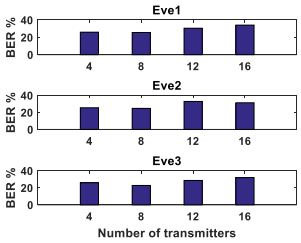


Fig. 18. BER vs. N.

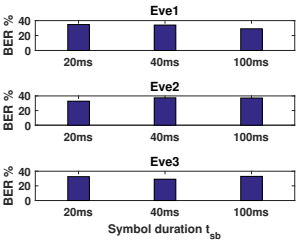


Fig. 19. BER vs. t_{sb}.

in total. Considering the amount of time taken to make the measurements, we only measured the BER values at three Eve locations instead of the entire 100 locations in Fig. 12 (we marked these three locations as E1, E2, and E3 using bright blue color). In the experiments, we have $N = 16$, $a_H = 1$, $a_L = 0.8$, $t_{sb} = 0.05ms$, and $\phi = 15°$.

Table I summarizes the BER values for Bob and three Eve locations. The results show that Bob has very low BER, $BER = 3.1 \times 10^{-6}$, while the BER at each Eve location is much higher, ranging from 31.73% to 38.05%. As a result, we conclude that Secret-Focus is highly effective in providing secret communication.

In addition, we have also tested several extreme Eve locations outside of the test area. First, we placed Eve very close to Bob, and present Eve's BERs in Fig. 14(a). We found that even when Eve is in close proximity with Bob, her BER is 12.45% while Bob was able to decode all the bits sent in this example. Finally, we placed Eve very close to the transmission antenna of a transmitter. As shown in Fig. 14(b), we find that when Eve's antenna is close (approximately 1cm) to the transmitter antenna, it has comparable BER with Bob, but its BER increases to 27% when it is 30 cm away. These results further demonstrate that Secret-Focus is indeed very powerful in protecting secret communication.

TABLE I
AVERAGE DECODING ERRORS STATISTICS FOR BOB AND 3 EVES. BOB HAS EXTREMELY LOW BER WHILE EVES' BER ARE OVER 30%.

	Bob	Eve_1	Eve_2	Eve_3
Total Number of Bits Transmitted (bits)	$164.79M$			
Total Number of Bits Incorrectly Decoded (bits)	$52.31K$	$52.29M$	$62.70M$	$60.36M$
Estimated BER	3.1×10^{-6}	0.3173	0.3805	0.3663

C. Impact of Important System Parameters

The objective of the third set of experiments is to study the impact of several important system parameters.

1) Impact of a_L: Here, we use the same experimental setting as in last set of experiments, Bob in the center of the test area and three Eve locations. we set $N = 16$, $t_{sb} = 20ms$, $a_H = 1$, and $\phi = 15°$, and vary the low bits amplitude in our amplitude modulation: $a_L = 0.5, 0.6, 0.7, 0.8$ and 0.9. We calculate the three sets of BER values and show the results in Fig. 16. From the results, we observe that larger a_L values

lead to a higher BER for Eves. This observation agrees with our previous theoretic analysis in Section III-B. With a larger a_L value, the RSS values at Eve become even less stable, and hence higher BER. Under a more aggressive system parameter setting, $a_L = 0.95$, BER for Eve and Bob are 57.1% and 2.2×10^{-6} respectively.

2) Impact of ϕ: Here, we use the same experimental setting as in the last set of experiments, Bob in the center of the test area and three Eve locations. We set $N = 16$, $t_{sb} = 20ms$, $a_H = 1$, and $a_L = 0.8$, and vary the maximum perturbation angle $\phi = 5°, 7°, 10°, 12°, 15°, 17°, 20°, 22°$ and $25°$. We calculate the three sets of BER values and show the results in Fig. 17. We observe the same trend for all three Eve locations. The results show that there is a sweet spot for ϕ, between $15°$ and $20°$. This can be explained as follows. If ϕ is too large, it may make Bob's RSS values less stable. Meanwhile, if ϕ is too small, then it does not disturb Eve's RSS sufficiently.

3) Impact of N: Here, we use the same experimental setting with Bob in the center of the test area and three Eve locations. We set $\phi = 15°$, $t_{sb} = 20ms$, $a_H = 1$, and $a_L = 0.8$, and vary the number of transmitters $N = 4, 8, 12$ and 16 (by having $1, 2, 3$ and 4 USRP(s) at each corner, respectively). We present the three sets of BER values in Fig. 18. The results show that having more transmitters can yield a higher BER for Eves. We note that having 4 transmitters is sufficient to prevent Eves from eavesdropping, indicating that our system is not only effective, but also very practical.

4) Impact of t_{sb}: Here, we use the same experimental setting with Bob in the center of the test area and three Eve locations. We set $\phi = 15°$, $N = 16$, $a_H = 1$, and $a_L = 0.7$, and vary the symbol duration $t_{sb} = 20, 40$ and 100ms. We present the three sets of BER values in Fig. 19. The results show that choosing different symbol duration values has no significant bearing on Eve's BER values.

VI. CONCLUSION

In this paper, we showed, when distributed transmitters align their phases at a common receiver, that several secrecy-supporting properties result. Further, secrecy is possible without requiring knowledge of the eavesdropper or the use of interference. By leveraging these properties, we present a new approach, referred as Secret-Focus, that builds a highly efficient secret communication channel on top of distributed phase alignment. We implemented a prototype Secret-Focus system that used amplitude-based modulation on top of phase alignment, to achieve secret communication between a coalition and an intended receiver. We presented an implementation using USRPs and experimental results that shows Secret-Focus can be built practically with a distributed set of transmitters employing phase alignment. Our detailed measurements demonstrate that Bob can achieve a very low BER, 3.1×10^{-6} when more than $160M$ bits are transmitted, while Eve's BER is between $30\% - 60\%$ across multiple measurement locations. In addition, we also show that Eve cannot eavesdrop even at extreme locations, such as in the close proximity of Bob, or one wavelength away from one of the transmitters antennas.

VII. ACKNOWLEDGEMENT

We are grateful to the INFOCOM reviewers for their constructive critiques, and Ivan Seskar, for his invaluable comments, all of which have helped us greatly improve this paper. This work was supported in part by the U.S. National Science Foundation(NSF) under grant CNS-1404118, CNS-1443434 and CNS-1423020.

REFERENCES

[1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201–220, 2005.

[2] R. Liu and W. Trappe, *Securing Wireless Communications at the Physical Layer*. Springer, 2010.

[3] S. Mathur, A. Reznik, C. Ye, R. Mukherjee, A. Rahman, Y. Shah, W. Trappe, and N. Mandayam, "Exploiting the Physical Layer for Enhanced Security," *IEEE Wireless Communications Magazine*, vol. 17, pp. 63–70, 2010.

[4] L. Xiao, Y. Li, G. Han, G. Liu, and W. Zhuang, "Phy-layer spoofing detection with reinforcement learning in wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 10 037–10 047, 2016.

[5] N. Anand, S.-J. Lee, and E. W. Knightly, "Strobe: Actively securing wireless communications using zero-forcing beamforming," in *Proceedings of the IEEE Conference on Computer Communications (INFOCOM)*, 2012, pp. 720–728.

[6] W.-C. Liao, T.-H. Chang, W.-K. Ma, and C.-Y. Chi, "Qos-based transmit beamforming in the presence of eavesdroppers: An optimized artificial-noise-aided approach," *IEEE Transactions on Signal Processing*, vol. 59, no. 3, pp. 1202–1216, 2011.

[7] L. Lai and H. El Gamal, "The Relay–Eavesdropper Channel: Cooperation for Secrecy," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4005–4019, 2008.

[8] D. M. Laverty, D. J. Morrow, R. Best, and P. A. Crossley, "Telecommunications for Smart Grid: Backhaul Solutions for the Distribution Network," in *Proceedings of the IEEE Power and Energy Society General Meeting*, 2010, pp. 1–6.

[9] R. Mudumbai, B. Wild, U. Madhow, and K. Ramchandran, "Distributed beamforming using 1 bit feedback: from concept to realization," in *Proceedings of the 44th Allerton Conference on Communication, Control and Computation*, vol. 8, Sep. 2006, pp. 1020–1027.

[10] Z. Li, R. Yates, and W. Trappe, "Achieving Secret Communication for Fast Rayleigh Fading Channels," *IEEE Transactions on Wireless Communications*, vol. 9, no. 9, pp. 2792 –2799, September 2010.

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

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

[13] A. Yener and S. Ulukus, "Wireless physical-layer security: Lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814–1825, Oct 2015.

[14] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor, "Improving wireless physical layer security via cooperating relays," *IEEE Transactions on Signal Processing*, vol. 58, no. 3, pp. 1875–1888, Mar. 2010.

[15] L. Liu, R. Zhang, and K.-C. Chua, "Secrecy wireless information and power transfer with miso beamforming," in *Global Communications Conference (GLOBECOM), 2013 IEEE*. IEEE, 2013, pp. 1831–1836.

[16] H.-M. Wang, Q. Yin, and X.-G. Xia, "Distributed beamforming for physical-layer security of two-way relay networks," *IEEE Transactions on Signal Processing*, vol. 60, no. 7, pp. 3532–3545, Jul 2012.

[17] S. Bashar, Z. Ding, and C. Xiao, "On the secrecy rate of multi-antenna wiretap channel under finite-alphabet input," *IEEE Communications Letters*, vol. 15, no. 5, pp. 527–529, May 2011.

[18] J. V. Michalowicz, J. M. Nichols, and F. Bucholtz, "Calculation of differential entropy for a mixed gaussian distribution," *Entropy*, vol. 10, no. 3, pp. 200–206, Aug 2008.

[19] G. Webb, I. Minin, and O. V. Minin, "Variable reference phase in diffractive antennas: Review, applications, new results," *IEEE Antennas and Propagation Magazine*, vol. 53, no. 2, pp. 77–94, Apr. 2011.