Demo Abstract: A Practical Secret Communication System by Perturbing Focused Phases Among Distributed Transmitters

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
{ox5bc, zz196, trappe, yyzhang, reh}@winlab.rutgers.edu, zhan2@uh.edu

***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 phase alignment among distributed transmitters, 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}.**

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.

Though traditional designs 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.

Contribution: Going beyond beamforming and jamming based techniques, we propose a new phase combining and dithering based secret communication mechanism. 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 to a transmitter antenna. We refer to this highly efficient yet practical secret communication mechanism as *Secret-Focus*

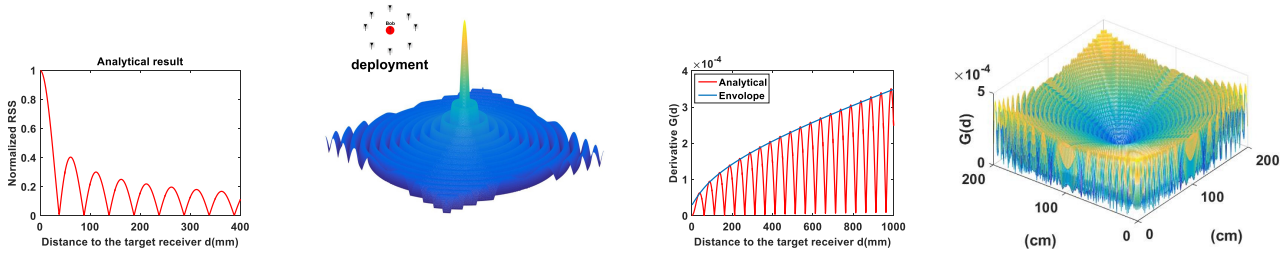
II. PERTURBING ALIGNED PHASES FOR SECRET COMMUNICATION

Information theory centric motivation: 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[1], 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. 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. 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*.

Secret-Focus achieves this objective through two complementary mechanisms introduced in the following subsections.

A. Mechanism 1: Combining Phases Increases μ_y

The first key idea of our design is to place transmitters around the target receiver, to achieve an effect similar to how Fresnel zone plates focus light at a focal point. 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. As we approach an infinite amount of transmitters around the circle,



(a) (b) (c) (d)

Fig. 1. (a) Analytic results for the normalized RSS function $Y(d)$ in (1), where RSS decreases with d. (b) RSS distribution in a $1m$ by $1m$ area around Bob. It is clear that the energy is sharply focused around the target location. (c) The analytical results for $G(d)$ in (2). The envelop of $G(d)$, marked in blue, shows that Eve's RSS variation increases with d. (d) 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.

we can write the normalized RSS at the measurement location as:

$$Y(d) = \frac{R}{2\pi}\left|\int_0^{2\pi} \frac{e^{j2\pi\frac{\sqrt{R^2+d^2-2Rd\cos\varphi}-R}{\lambda}}}{\sqrt{R^2+d^2-2Rd\cos\varphi}} d\varphi\right|. \quad (1)$$

We can see in Fig. 1(a)(b) that the results for the normalized RSS expression $Y(d)$ has a spatial pattern similar to the magnitude of a sinc function ($R = 10m$ and $\lambda = 0.1m$), with the maximum at the target receiver location. The detailed proof and demo are in [2], [3]. This location corresponds to where transmitter signals phase aligned.

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.

We examine the impact that small fluctuations around the phase alignment optimum would have upon recipient's RSS, $G()$. Assume a large number of transmitters on a circle $N \to \infty$, and the target receiver at the center. Similar to Equation 1, 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:

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

In order to understand the implication of $G(d)$ in our design, we show the $G(d)$ distribution in Fig. 1(c)(d). 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. 1(c)). At the same time, such perturbation does not harm Bob's decoding ability ($G(d) = 0$).

III. Effectiveness of the Two Mechanisms

We conducted proof of concept experiments using 18 USRP N210s. Fig. 2 shows: (a) the raw RSS at Eve when transmitters are completely distributed and do not coordinate among themselves, (b) the raw RSS at Eve when transmitters perform phase combining, but keeping the phase at Φ_{align} during

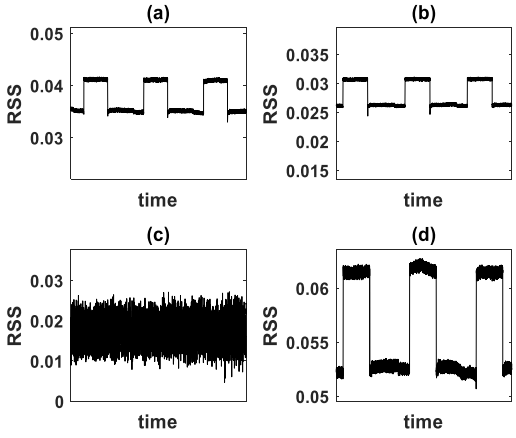


Fig. 2. (a) Raw RSS at Eve for a broadcast channel (neither mechanism employed), (b) raw RSS at Eve for a NO-Perturb system (only mechanism 1 employed), (c) raw RSS at Eve for Secret-Focus (both mechanisms employed), and (d) raw RSS at Bob for Secret-Focus.

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. BER at Eve in this particular experiment is 42.1% while Bob successfully decoded all PAM bits.

References

[1] 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.

[2] W. T. Y. Z. R. H. Xiaoran Fan, Zhijie Zhang and Z. Han, "Secret-focus: A practical physical layer secret communication system by perturbing focused phases in distributed beamforming," in *INFOCOM 2018-IEEE Conference on Computer Communications, IEEE*, 2018.

[3] W. T. Y. Z. R. H. X. Fan, Z. Zhang and Z. Han, "Poster abstract: A practical secret communication system by perturbing focused phases among distributed transmitters," in *INFOCOM 2018-IEEE Conference on Computer Communications, IEEE*, 2018.