Physical Layer Encryption for UAV-to-Ground Communications

Ahmed Maksud and Yingbo Hua
Department of Electrical and Computer Engineering
University of California at Riverside
Riverside, California, USA
Emails: amaks002@ucr.edu and yhua@ee.ucr.edu

2022 IEEE International Conference on Communications Workshops (ICC Workshops) | 978-1-6654-2671-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCWORKSHOPS53468.2022.9814512

***Abstract*—Ensuring secure and reliable wireless communication is crucial for Unmanned Aerial Vehicle (UAV) applications. Most of the prior works on secure UAV-to-Ground (U2G) communications focus on trajectory and/or power optimization to ensure that the desired U2G channel is stronger than an eavesdropping channel. In this paper we propose a novel physical layer encryption method that performs symbol and/or constellation hiding for secure U2G communications. Unlike prior works on symbol and/or constellation hiding which aimed at specific detection algorithms by adversaries, our method exploits the secrecy inherent in the reciprocal channel between an UAV and a desired ground station (GS), and is hence in principle robust against any eavesdropping attack algorithms including deep machine learning. Given a pair of estimated reciprocal channel vectors (ERCVs) with a limited dimension at UAV and GS respectively, our method first uses a continuous encryption function (CEF) to transform the two ERCVs at UAV and GS respectively into two sequences of quasi-continuous pseudo-random numbers (QCPRNs) of any desired dimension. Robust to a range of statistical distributions of ERCVs, these QCPRNs follow approximately a known statistical distribution and hence can be further transformed into two sequences of uniformly distributed (UD) QCPRNs. The UD-QCPRNs generated at UAV are superimposed by UAV in a modulo fashion onto its transmitted symbols, and the UD-QCPRNs generated at GS are used for decryption at GS. This paper also studies the impact of the difference between the two ERCVs along with other noises on the performance of the desired U2G channel.**

***Index Terms*—UAV communication, wireless network security, physical layer security, physical layer encryption**

I. Introduction

Unmanned Aerial Vehicles (UAVs) are expected to be widely deployed in near future for applications such as surveillance, transportation, mobile base stations and mobile relays [1]. UAV is often exposed in air, and in this case the information transmitted from UAV is particularly vulnerable to eavesdropping. To protect the information with information-theoretic secrecy against eavesdropper (Eve), there are two fundamental approaches. One is network layer security where a secret key must be pre-established between two legitimate nodes (Alice and Bob) and this secret key can be then used to encrypt and decrypt a large volume of information to gain a computation-based secrecy (in addition to the information-theoretic secrecy from the secret key). The other approach is physical layer security where either a secret key is generated from correlated observations at Alice and Bob or secret information is directly transmitted from Alice to Bob. The direct transmission requires schemes to make the channel from Alice to Bob stronger than that from Alice to Eve, e.g., see [3] and [4] for UAV trajectory and/or resource allocation, [5] for beamforming, and [6] for using full-duplex radios. This requirement is often not possible especially for UAV-to-Ground (U2G) communications where Eves are often hidden and their capabilities are often unknown. And the range of current in-band full-duplex communication may not be sufficiently large. So, without a pre-established secret key between a legitimate pair of UAV (Alice) and GS (Bob), and without the knowledge of Eve's capability, achieving an information-theoretic secrecy for U2G communications should exploit correlated observations that are available to the pair of UAV and GS but are independent of the observations by any Eve. In this paper, we will focus on the use of a pair of estimated reciprocal-channel vectors (ERCVs) obtained by the legitimate pair of UAV and GS respectively for secure U2G communications.

Given two ERCVs at UAV and GS respectively, a central task of the traditional physical layer security approach would be to extract a pair of digital keys at UAV and GS respectively [7], [8], [9]. But in practice, much of the statistics of ERCVs is unknown, and hence reliable key generation directly from the two ERCVs remains a challenge.

However, without an explicit key generation from ERCVs, we can still exploit the secrecy inherent in ERCVs via what is called physical layer encryption as first explored in [10] and [11]. A crucial tool for physical layer encryption is called continuous encryption function (CEF) which is further developed in [12]. This paper shows how to apply a CEF developed in [12] to hide transmitted symbols and/or constellations, which consequently achieves a secure U2G communication.

There have been many works on constellation detection, e.g., see [2] and [21]. More recently, many machine learning based methods have been developed for constellation detection, e.g., see [22] and [23]. Furthermore, various methods

This work was supported in part by the Army Research Office under Grant Number W911NF-17-1-0581 and the Department of Defense under W911NF-20-2-0267. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the Army Research Office or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation herein.

have also been developed to degrade the performances of constellation detection methods [16], [17], [18], [19], [20]. The constellation hiding method shown in this paper exploits an information-theoretic secrecy in ERCVs, which in principle prevents any method from successfully detecting the hidden constellation. Hence, our work also differs from [24] where a hidden constellation can be detected by adversary, and differs from [25] where the hidden information is detectable by adversary.

The remainder of the paper is organized as follows. Section II describes the wireless channel model used in this paper. See Fig. 1. Section III provides a brief introduction of CEF. Section IV-A describes the proposed method for symbol and/or constellation hiding, and highlights the main issues to be discussed in the rest of the paper. In Section IV-B, we discuss how to generate uniformly distributed quasi-continuous pseudo-random numbers (UD-QCPRNs) from the output of a CEF, and evaluate the noise propagation in the encryption/decryption process. In section V, we evaluate the impact of the encryption noise on the performance of the legitimate receiver. A quantized scheme is shown in section VI, which is an efficient form of the proposed method. Section VII concludes the paper.

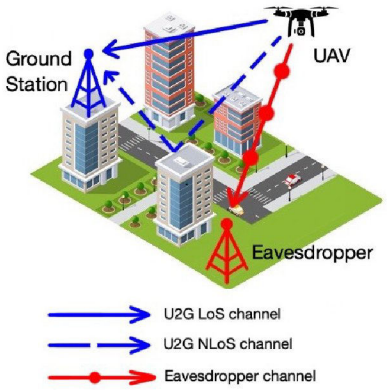


Fig. 1. Illustration of wireless channel model for U2G communication with eavesdropper present.

II. Wireless Channel Model

Following [14], we model the reciprocal complex channel gain at time n (within a time window in the order of milliseconds) between UAV and GS as:

$$g_n = \sqrt{\beta_0 {d_n}^{-\alpha_n}} h_n \tag{1}$$

where β_0 is the large-scale average channel power gain at unit distance, d_n is the U2G distance, α_n is the path loss exponent, and h_n is the small-scale fading coefficient. We assume that Alice and Bob can each get an estimate of g_n by a standard channel estimation technique. Furthermore, we assume that d_n and α_n do not change significantly within the time window of interest and hence Alice and Bob can also each get an estimate of h_n by scaling the estimate of g_n. For U2G communication, h_n in general consists of two components: line-of-sight (LoS) [13] and non-line-of-sight (NLoS), which is often called Rician fading. In this case, h_n can be modelled as:

$$h_n = \sqrt{\frac{K_n}{K_n+1}} e^{j\theta_n} + \sqrt{\frac{1}{K_n+1}} \xi_n \tag{2}$$

where θ_n for all n are i.i.d. and uniformly distributed over $[0, 2\pi]$, denoted by $\mathcal{U}(0, 2\pi)$; and ξ_n for all n are i.i.d. complex Gaussian random variables with zero mean and unit variance, denoted by $\mathcal{CN}(0, 1)$. It follows that $\mathcal{E}\{|h_n|^2\} = 1$ and $\angle h_n \sim \mathcal{U}(0, 2\pi)$. Here K_n is the Rician factor [15]. For all simulations in this paper, we will treat K_n as invariant to n and set $K_n =$ 27dB. Eve is assumed to be located anywhere on the ground and can have LoS with the UAV but less likely have LoS with GS due to terrain and obstacles as illustrated in fig. 1. If Eve knows the exact distance between the antenna of UAV and the antenna of GS at all times, she could try to estimate θ_n for all n. But due to limited precision in estimated distance relative to wavelength, it is reasonable to assume that Eve is completely blind to θ_n. Because of multipath fading, Eve is also completely blind to ξ_n (except for its distribution). The estimates of h_n by Alice and Bob may be denoted by $\hat{h}_{n,A}$ and $\hat{h}_{n,B}$ respectively. Then the amount of secrecy available from $\hat{h}_{n,A}$ and $\hat{h}_{n,B}$ is the mutual information between them.

For notational convenience and with no serious loss of generality, we will from now on let $\hat{h}_{n,A} = h_n$ and $\hat{h}_{n,B} = h'_n = h_n + w_n$ where $w_n \sim \mathcal{CN}(0, \frac{1}{\text{SNR}_h})$. For a time window of $N/2$ samples, we also let $\mathbf{h} = [h_1, h_2, \cdots, h_{\frac{N}{2}}]^T$ and $\mathbf{h}' = [h'_1, h'_2, \cdots, h'_{\frac{N}{2}}]^T$. (Note that the index n in h_n can be also used to represent the index of any spatial or frequency subchannel between UAV and GS.) Furthermore, we define the ERCVs obtained by Alice and Bob as $\mathbf{x} = [\mathcal{R}e\{\mathbf{h}\}^T, \mathcal{I}m\{\mathbf{h}^T\}]^T$ and $\mathbf{x}' = [\mathcal{R}e\{\mathbf{h}'\}^T, \mathcal{I}m\{\mathbf{h}'\}^T]^T$. It follows that $\mathbf{x}' = \mathbf{x} + \mathbf{w}_x$ where $\mathbf{w}_x \sim \mathcal{N}(\mathbf{0}, \frac{1}{\text{SNR}_x}\mathbf{I}_N)$ and $\text{SNR}_x = \text{SNR}_h$

III. Brief Introduction of CEF

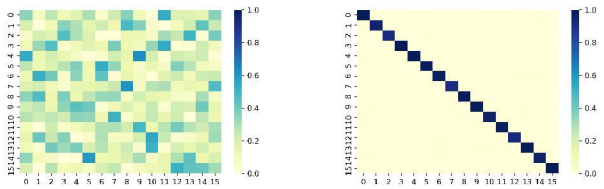
Let $\mathbf{x}$ be an $N \times 1$ real-valued zero-mean random vector, denoted by $\mathbf{x} \in \mathcal{R}^{N\times 1}$. A CEF of $\mathbf{x}$ is an easy-to-compute (i.e., with a polynomial complexity in terms of N) map from $\mathbf{x}$ to a sequence of real-valued numbers $y_1, y_2, \cdots$, which is expressed as $y_k = f_k(\mathbf{x}) \in \mathcal{R}$ for all $k \geq 1$. A good CEF as defined in [12] is such that (1) it is hard (i.e., with an exponential complexity in terms of N) to compute $\mathbf{x}$ from y_k with all $k \geq 1$; (2) there is no such k-invariant function of $\mathbf{x}$, i.e., $g(\mathbf{x})$, that "y_k is an easy-to-compute function of $g(\mathbf{x})$, and $g(\mathbf{x})$ is also easy to compute from y_k with all $k \geq 1$"; (3) the signal-to-noise ratio (SNR) in y_k caused by a noise in $\mathbf{x}$ is not much smaller than the SNR in $\mathbf{x}$; and (4) y_k for all $k \geq 1$ can only have very weak correlations when the entries of a random $\mathbf{x}$ have zero correlations.

The first two properties of a good CEF can be empirically established although a formal proof seems hard if not impossible. The third property of a good CEF can be measured by comparison to a unitary random projection (URP), i.e., $\mathbf{g}_k = \mathbf{R}_k\mathbf{x} \in \mathcal{R}^{N\times 1}$ where $\mathbf{R}_k$ for each index k is a

pseudo random unitary matrix (governed by a seed). The noise sensitivity of URP is considered to be optimal since the norm of the perturbation vector in $\mathbf{g}_k$ for each k is always the same as the norm of the corresponding perturbation vector in $\mathbf{x}$. But URP is not hard to invert (if the seed is known or $\mathbf{R}_k$ for any k is known). The fourth property of a good CEF can be verified via simulations. For URP, there is in general a significant correlation between $\mathbf{g}_k$ and $\mathbf{g}_l$ for $k \neq l$ (subject to fixed $\mathbf{R}_k$ and $\mathbf{R}_l$) even if the correlation matrix of $\mathbf{x}$ is the identity matrix $\mathbf{I}_N$.

A good CEF is proposed in [12], which is based on components of singular value decomposition (SVD) of a pseudo-randomly modulated matrix of $\mathbf{x}$. Specifically, let $\mathbf{Q}_{k,l} \in \mathcal{R}^{N\times N}$ for all pairs of k and l be pseudo-random unitary matrices; $\mathbf{M}_{k,\mathbf{x}} = [\mathbf{Q}_{k,1}\mathbf{x}, \cdots \mathbf{Q}_{k,N}\mathbf{x}]$ where each column of $\mathbf{M}_{k,\mathbf{x}}$ is a pseudo-random rotation of $\mathbf{x}$; and then $\mathbf{u}_{k,x} = \arg\max_{\mathbf{u},\|\mathbf{u}\|=1} \mathbf{u}^T\mathbf{M}_{k,\mathbf{x}}\mathbf{M}_{k,\mathbf{x}}^T\mathbf{u}$, which is the principal left singular vector of $\mathbf{M}_{k,\mathbf{x}}$. Finally, choose y_k to be a particular (e.g. the first) element of $\mathbf{u}_{k,x}$ for each of $k \geq 1$. The prior research [12] supports that the above defined CEF, called SVD-CEF, appears to possess the previously discussed properties. For this reason, we can view SVD-CEF as a scrambler that turns a finite number of real-valued random numbers in $\mathbf{x}$ into an infinite number of QCPRNs y_k for $k \geq 1$. Unlike any of the conventional PRN generators, here y_k is a *continuous* function of $\mathbf{x}$.

To illustrate the correlations among the output values of URP-CEF and SVD-CEF, we now consider the input vector $\mathbf{x}$ described in section II. The normalized correlation matrix of this $\mathbf{x}$ is $\mathbf{C}_\mathbf{x} = 2\mathcal{E}_\mathbf{x}\{\mathbf{x}\mathbf{x}^T\} = \mathbf{I}_N$. For URP-SVD, we know that $\mathbf{C}_{\mathbf{g}_k} = 2\mathcal{E}_\mathbf{x}\{\mathbf{g}_k\mathbf{g}_k^T\} = \mathbf{I}_N$ for each k. But the corresponding cross-correlation matrix $\mathbf{C}_{\mathbf{g}_k,\mathbf{g}_l} = 2\mathcal{E}_\mathbf{x}\{\mathbf{g}_k\mathbf{g}_l^T\}$ for $k \neq l$ is not small in general. The absolute values of all entries in $\mathbf{C}_{\mathbf{g}_k,\mathbf{g}_l}$ for a random realization of $\mathbf{R}_k$ and $\mathbf{R}_l$ are illustrated in the left of Fig. 2 where $N = 16$. For SVD-CEF, we let $\mathbf{y} = [y_1, \cdots, y_N]^T$. Since $\mathbf{u}_{k,x}$ has the norm one, the variance of y_k can be shown to be $\frac{1}{N}$. Then the normalized correlation matrix of $\mathbf{y}$ is $\mathbf{C}_\mathbf{y} = N\mathcal{E}_\mathbf{x}\{\mathbf{y}\mathbf{y}^T\}$. The absolute values of all entries of $\mathbf{C}_\mathbf{y}$ for a random realization of $\{\mathbf{Q}_{k,l}; k = 1, \cdots, N; l = 1, \cdots, N\}$ with $N = 16$ are illustrated in the right of Fig. 2. In both cases, the average is done over 10^5 random realizations of $\mathbf{x}$. Here we see near-zero correlations among entries of $\mathbf{y}$. Since $\mathbf{Q}_{k,l}$ are randomly chosen, the observed phenomenon of near-zero correlations holds for all y_k with $k \geq 1$.



URP-CEF SVD-CEF

Fig. 2. Correlation "heatmaps" of the output of URP-CEF and the output of SVD-CEF.

We will next apply SVD-CEF in a physical layer encryption method where the seed used to construct the pseudo-random unitary matrices, $\mathbf{Q}_{k,l}$ for all $k \geq 1$ and $1 \leq l \leq N$, is assumed to be a public information known to Alice, Bob and Eve.

IV. A Physical Layer Encryption Method

Assume that Alice wants to transmit a sequence of K complex information symbols to Bob. For many commonly used QAM symbol constellations, the real and imaginary parts of the sequence can be each treated as a sequence of M-PAM (real-valued) symbols. Hence we can focus on how to encrypt a sequence of M-PAM symbols, denoted by s_k with $k = 1, 2, \cdots, K$. Also assume that the constellation of s_k for each k is a discrete set of M points equally spaced within $[-1, 1]$. The spacing between two adjacent points is denoted by $\Delta = \frac{2}{M}$, i.e., $\min_{s_k^{(i)} \neq s_k^{(j)}} |(s_k^{(i)} - s_k^{(j)})_{modulo-[-1,1]}| = \Delta$ where $s_k^{(i)}$ and $s_k^{(j)}$ are two distinct realizations of s_k.

A. Basic Approach

Let z_k be a function of y_k such that z_k is uniformly distributed over $[-1, 1]$. Then an encrypted symbol for transmission from Alice is defined as $\hat{s}_k = (s_k + z_k)_{modulo-[-1,1]}$. Clearly, given any s_k, $\hat{s}_k$ has the same uniform distribution as z_k. In this case, no method is able to detect s_k based on $\hat{s}_k$ alone. This is because $I(s_k; \hat{s}_k) = h(\hat{s}_k) - h(\hat{s}_k|s_k) = h(\hat{s}_k) - h(\hat{s}_k) = 0$ where $I(\cdot;\cdot)$ denotes mutual information and $h(\cdot)$ denotes the differential entropy.

At Bob, the received symbol corresponding to $\hat{s}_k$ can be written as $\hat{s}'_k = \hat{s}_k + n_k$ where n_k is the (normalized) channel noise with its power inversely proportional to the transmission power from Alice. Since Bob has $\mathbf{x}' = \mathbf{x} + \mathbf{w}_x$, he can compute y'_k from $\mathbf{x}'$ in the same way as Alice computes y_k from $\mathbf{x}$. Furthermore, Bob can compute z'_k from y'_k in the same way as Alice computes z_k from y_k. Let $z'_k = z_k + w_{z_k}$ with w_{z_k} being the encryption noise.

To decrypt $\hat{s}'_k$ (at the physical layer), Bob computes $s'_k \doteq (\hat{s}'_k - z'_k)_{modulo-[-1,1]} = (s_k + n_k - w_{z_k})_{modulo-[-1,1]}$. As long as the channel-and-encryption combined noise $n_k - w_{z_k}$ is small compared to Δ, Bob can detect the information in s'_k with a small error rate.

In theory, z_k for each k can have a continuous uniform distribution over $[-1, 1]$. But in practice, there is a limited numerical resolution and hence z_k for each k should be discrete over $[-1, 1]$. But the constellation size of z_k must be larger than M in order to hide the constellation size of s_k. If z_k and s_k have the same constellation size M, the symbol s_k is still protected. The power of $\hat{s}_k$ is generally larger than that of s_k. But the difference approaches zero quickly as M increases.

In the next subsection, we will discuss how to generate the UD-QCPRNs z_k from the output y_k of CEF and discuss the impact of the noise in $\mathbf{x}'$ on the noise in z'_k. In section V, the impact of the combined noise $n_k - w_{z_k}$ on the performance at Bob is investigated via simulation.

B. Obtaining UD-QCPRNs from SVD-CEF

It is shown in [12] that if $\mathbf{x}$ consists of i.i.d. Gaussian random variables, then the probability density function (PDF) of each element of the output of SVD-CEF can be approximated by $f_Y(y) = C_N(1-y^2)^{\frac{N-3}{2}}$ where $-1 < y < 1$ and $C_N = \frac{\Gamma(\frac{N}{2})}{\sqrt{\pi}\Gamma(\frac{N-1}{2})}$. We have also found that if $\mathbf{x}$ is the $N \times 1$ random vector constructed as discussed in section II, the output of SVD-CEF can be also approximated by the same PDF. In fact, the PDF of the output of SVD-CEF is rather robust to a range of variations in the statistics of $\mathbf{x}$. This is because of the construction of $\mathbf{M}_{k,\mathbf{x}}$ from $\mathbf{x}$ where each vector $\mathbf{Q}_{k,l}\mathbf{x}$ tends to be Gaussian distributed for a moderate to large N, which follows the well-known large-sample theory of Gaussian random variables.

To obtain z_k with the uniform distribution $\mathcal{U}(-\frac{B}{2}, \frac{B}{2})$, it can be shown that $z_k = T_{SVD}(y_k)$ with

$$T_{SVD}(y) = \int_{-1}^{y} B f_Y(u)du - \frac{B}{2} = BC_N \int_0^{\theta_y} \cos^{N-2}\theta d\theta \tag{3}$$

where $\theta_y = \sin^{-1} y$ and

$$\int_0^{\theta_y} \cos^n \theta d\theta = \frac{\cos^{n-1}\theta_y \sin\theta_y}{n} + \frac{n-1}{n}\int_0^{\theta_y} \cos^{n-2}\theta d\theta. \tag{4}$$

Note that for Alice, we have a process of $\mathbf{x} \to y_k \to z_k$, and for Bob, we have a similar process of $\mathbf{x}' \to y'_k \to z'_k$.

To quantify the relationship between the noise in $\mathbf{x}'$ and the noise in z'_k, we can evaluate $\eta_{x,z} = \eta_{x,y}\eta_{y,z}$ with $\eta_{x,y} = \sqrt{\frac{\text{SNR}_x}{\text{SNR}_y}}$ and $\eta_{y,z} = \sqrt{\frac{\text{SNR}_y}{\text{SNR}_z}}$. Here, SNR_x is the signal to noise ratio in $\mathbf{x}'$, and SNR_y and SNR_z are defined similarly.

1) $\eta_{x,y}$: Assume $\mathbf{x}' = \mathbf{x} + \mathbf{w}_x$ with $\mathbf{w}_x \sim \mathcal{N}(\mathbf{0}, \sigma_w^2 \mathbf{I}_N)$. Then for a given $\mathbf{x}$ and a given set of $\mathbf{Q}_{k,l}$, we can write

$$\eta_{x,y} = \sqrt{\frac{\text{SNR}_x}{\text{SNR}_y}} = \sqrt{\frac{\left(\frac{\mathcal{E}_{\mathbf{w}_x}\{\|\mathbf{x}\|^2\}}{\mathcal{E}_{\mathbf{w}_x}\{\|\mathbf{w}_x\|^2\}}\right)}{\left(\frac{\mathcal{E}_{\mathbf{w}_x}\{\|\mathbf{y}_k\|^2\}}{\mathcal{E}_{\mathbf{w}_x}\{\|\mathbf{w}_y\|^2\}}\right)}}. \tag{5}$$

Since the output of SVD-CEF is invariant to the scaling of $\mathbf{x}$, we can choose $\|\mathbf{x}\|^2 = 1$, $\|\mathbf{x}'\|^2 = 1$, $\|\mathbf{y}_k\|^2 = 1$ and $\|\mathbf{y}'_k\|^2 = 1$. Hence,

$$\eta_{x,y} = \sqrt{\frac{\mathcal{E}_{\mathbf{w}_x}\{\|\mathbf{w}_y\|^2\}}{\mathcal{E}_{\mathbf{w}_x}\{\|\mathbf{w}_x\|^2\}}} \tag{6}$$

which is equivalent to $\eta_{k,x}$ in [12].

A closed form of $\eta_{k,x}$ for small σ_w^2 is available in [12], which is dependent on $\mathbf{x}$ and $\mathbf{Q}_{k,l}$. For a given $\mathbf{x}$, an upper bound of $\eta_{k,x}$ can be set by pruning $\mathbf{Q}_{k,l}$. In Table I, the percentages of pseudo-randomly generated $\mathbf{Q}_{k,l}$ that satisfy the condition $\eta_{x,y} < \eta_T$ for SVD-CEF are shown. To maintain a high percentage, we will choose $\eta_T = 2.5$ in the remainder of the paper. Note that the choices of $\mathbf{Q}_{k,l}$ are publicly known and can be locally generated from a common seed.

TABLE I
EMPIRICALLY OBTAINED % OF $\mathbf{Q}_{k,l}$ THAT SATISFIES $\eta_{x,y} < \eta_T$ FOR DIFFERENT N

$\eta_T \to$	0.8	1	1.5	2	2.5
$N = 16$	4.62	21.98	63.25	80.78	88.26
$N = 32$	0.29	6.75	48.46	73.10	84.03
$N = 64$	0.007	0.84	31.61	63.32	78.35

2) $\eta_{y,z}$: Next we evaluate $\eta_{y,z}$ for small σ_w^2. We first recall (ignoring k for convenience) $z = \int_{-1}^{y} B f_Y(u)du - \frac{B}{2}$ and $z' = \int_{-1}^{y'} B f_Y(u)du - \frac{B}{2}$ where $y' = y + w_y$ and $z' = z + w_z$. It follows that for small σ_w^2,

$$w_z = z' - z = T_{SVD}(y') - T_{SVD}(y) \approx B w_y f_Y(y) \tag{7}$$

and hence

$$\begin{aligned}\mathcal{E}_Y\{w_z^2\} &= \mathcal{E}_Y\left\{B^2 {w_y}^2 f_Y(y)^2\right\} \\ &= B^2 {w_y}^2 \int_{-1}^{1} f_Y(u)^3 du \\ &= B^2 w_y^2 D_N\end{aligned} \tag{8}$$

where $D_N = \frac{\Gamma(\frac{N}{2})^3\Gamma(\frac{3N-7}{2})}{\pi\Gamma(\frac{N-1}{2})^3\Gamma(\frac{3N-6}{2})}$. Hence, $\frac{var(w_z)}{var(w_y)} = B^2 D_N$. Furthermore, since $var(y) = \frac{1}{N}$ and $var(z) = \frac{B^2}{12}$, then $\eta_{y,z} = \sqrt{\frac{\text{SNR}_y}{\text{SNR}_z}} = \sqrt{\frac{var(y)}{var(z)} \times \frac{var(w_z)}{var(w_y)}} = \sqrt{\frac{12 D_N}{N}}$ which is invariant to B but dependent on N.

The above theoretical results of $\eta_{y,z}$ are compared with simulation/empirical results (with $B = 2$) in Fig. 3. In simulation, we used 10^6 realizations of $\mathbf{y}'_k = \sqrt{1-\alpha}\mathbf{y}_k + \sqrt{\alpha}\mathbf{w}_k$ with random $\mathbf{y}_k$ and $\mathbf{w}_k$ satisfying $\|\mathbf{y}_k\| = 1$, $\|\mathbf{w}_k\| = 1$ and $\mathbf{w}_k^T\mathbf{y}_k = 0$. We see that the two results are reasonably close to each other. We also see that for a large N (such as $N \geq 16$), $\eta_{y,z}$ is close to one and hence $\eta_{x,z}$ is dominated by $\eta_{x,y}$. Which implies that for SVD-CEF, $\eta_{x,z} = \eta_{x,y}\eta_{y,z} \approx \eta_{x,y} \leq \eta_T$

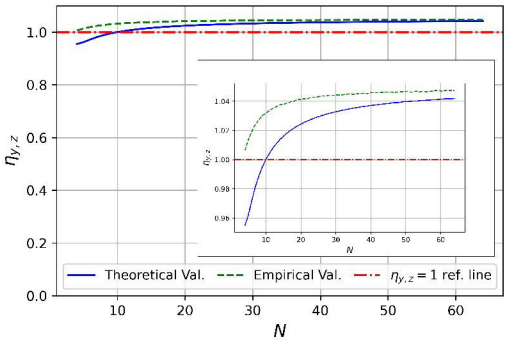


Fig. 3. The plot of $\eta_{y,z}$ vs N (both theoretical and empirical) for $\alpha = 10^{-5}$.

V. SIMULATION

In this section, we show simulation results of the proposed method. These results illustrate the effects of the channel

noise and the encryption noise on the performance at Bob. As explained before, we can focus on M-PAM only.

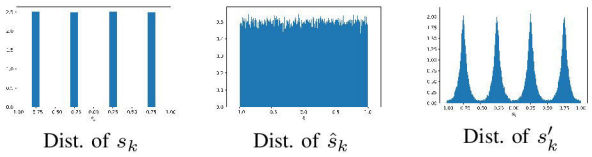


Fig. 4. Distributions of s_k, $\hat{s}_k$ and s'_k where $\text{SNR}_x = 20\text{dB}$ and $1/\sigma_n^2 = 37\text{dB}$

We assume that the channel noise n_k is i.i.d. Gaussian $\mathcal{N}(0, \sigma_n^2)$. The variance of the encryption noise w_{z_k} can be expressed as $\frac{\eta_{x,z}^2}{3\ \text{SNR}_x}$ where $\frac{1}{3}$ is the variance of z_k. In Fig. 4, we illustrate the distributions of the ideal 4-PAM symbol s_k (for which the width of each vertical bar is exaggerated for visual purpose), the encrypted symbol $\hat{s}_k$, and the decrypted symbol s'_k. It is clear that the distribution of $\hat{s}_k$ does not reveal any information about s_k and its constellation.

Once Bob has obtained enough samples of s'_k, he can use any of the existing constellation detection methods [2], [21], [22], [23] to detect M (if unknown to Bob) and then detect the secret symbols using a minimum distance method. The simulation results of the symbol error rates (SER) at Bob under different sets of parameters are illustrated in Figs 5, 6 and 7.

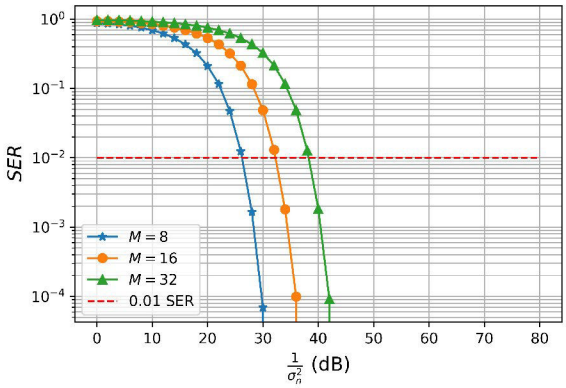


Fig. 5. Plot of SER vs $\frac{1}{\sigma_n^2}$ with no encryption noise for different M

In the simulation it is assumed that Bob has correctly detected the constellation size M from the samples of s'_k. For each chosen set of N, M, σ_n^2 and SNR_x, 10^5 random realizations of z_k, z'_k, s_k, s'_k, $\hat{s}_k$, $\hat{s}'_k$ were generated and the corresponding SER was obtained for each set of parameters. We see that the performance of SVD-CEF degrades slightly as N increases, but empirical study [12] shows that increasing N exponentially increases hardness to attack by the adversaries. This is a trade-off in choosing CEF between the performance at Bob and the hardness to attack by adversaries. It is important to stress here that even if an adversary with unlimited computing power can attack the computation-based secrecy due to SVD-CEF, there is no way for the adversary to attack the information-theoretic secrecy due to the ERCVs $\mathbf{x}$ and $\mathbf{x}'$ used in the physical layer encryption method.

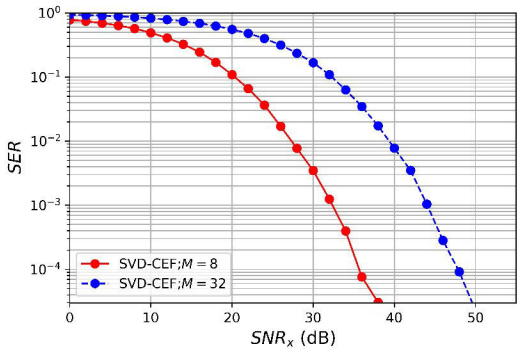


Fig. 6. Plot of SER vs SNR_x with negligible (i.e., $\sigma_n^2 \approx 0$) channel noise for $N = 16$ and different M

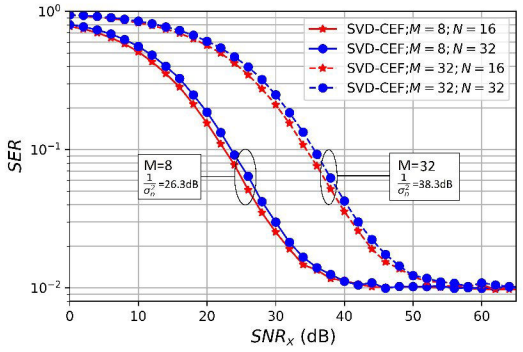


Fig. 7. Plot of SER vs SNR_x. The value of σ_n^2 for each choice of M is such that SER is 1% in Fig. 5

VI. Further Discussions

Computing a continuous (subject to machine precision) uniform random variable z_k from the output y_k of CEF may be costly in practice. To reduce the complexity, we can compute a discrete uniform random number $\bar{z}_k$ from y_k, which is equivalent to a uniform quantization of z_k or a non-uniform equiprobable quantization of y_k. The latter is feasible to implement. The procedures of encryption and decryption at Alice and Bob respectively are given below. The effect on Eve is discussed at the end.

1) Encryption at Alice: Assume $L = 2^l$, $M' = 2^{m'}$ and $M = 2^m$ where $l > m' > m$ are integers.

Alice constructs the true-symbol constellation $\mathcal{S}_M = \left\{\pm\frac{1}{M}(2i+1); i = 0, \cdots, \frac{M}{2} - 1\right\}$, and also in a similar way constructs the encrypted-symbol constellation $\mathcal{S}_{M'}$.

For a known PDF $f_Y(y)$ of y_k, Alice chooses an equiprobable over-quantizer of y_k with the corresponding set of $L+1$ thresholds $\mathcal{T}_L = \{t_i; i = 0, \cdots, L\}$ where $\int_{-1}^{t_i} f_Y(y)dy = \frac{i}{L}$. Note that $\mathcal{T}_L$ also corresponds to a set $\mathcal{I}_L$ of L intervals. Each y_k is quantized into l bits by $\mathcal{T}_L$. The first m' bits of each y_k are used to determine an integer $\bar{z}_k \in \mathcal{S}_{M'}$, and the last $l - m'$ bits of each y_k are transmitted to Bob.

For each true symbol $s_k \in \mathcal{S}_M$, Alice chooses a $\bar{z}_k \in \mathcal{S}_{M'}$ and transmits the encrypted symbol $\hat{s}_k \doteq (s_k +$

$\bar{z}_k)_{modulo-[-1,1]}$ to Bob.

2) Decryption at Bob: Assume that Bob knows l, m' and $\mathcal{T}_L$ as they are in the public domain. For each k, Bob knows $y'_k = y_k + w_{y_k}$ and also $\hat{s}'_k = \hat{s}_k + n_k = s_k + \bar{z}_k + n_k$.

From the last $l - m'$ bits (received from Alice) of each y_k, Bob determines a corresponding set of $2^{m'}$ intervals $\mathcal{I}'_k \subset \mathcal{I}_L$. Then each y'_k is quantized into an integer $\bar{z}'_k$ of m' bits by $\mathcal{I}'_k$ according to minimum distance.

The decrypted symbol by Bob is $s'_k \doteq (\hat{s}'_k - \bar{z}'_k)_{modulo-[-1,1]} = (s_k + n_k + \bar{z}_k - \bar{z}'_k)_{modulo-[-1,1]}$. Provided that $n_k + \bar{z}_k - \bar{z}'_k$ is small, Bob is able to detect the constellation of s_k and also the symbol s_k.

We have observed from simulation that with $l - m' \geq 3$, the quantized scheme shown above has virtually the same performance as the continuous scheme.

3) Effect on Eve: All transmitted $\hat{s}_k$ from Alice are now assumed to be received by Eve without noise. It can be shown that for $\forall M' = 2iM$ where i is any positive integer, $\hat{s}_k \in \mathcal{S}_{M'}$. Without a good estimate of $\mathbf{x}$, Eve is unable to determine a good estimate of $\bar{z}_k$. In this case, Eve is unable to decrypt her received $\hat{s}_k$. Even if Eve's random guess of s_k for $k = 1, \cdots, L$ with any $L \geq 1$ is correct and hence Eve knows $\bar{z}_k$ for $k = 1, \cdots, L$, there is currently no known method with a polynomial complexity in terms of N that Eve can use to compute $\mathbf{x}$ [12] and hence Eve may still be unable to compute $\bar{z}_k$ for $k > L$ in order to decrypt $\bar{s}_k$ for $k > L$.

VII. Conclusion

In this paper, we have developed a novel physical layer encryption method for symbol and/or constellation hiding against any possible detection methods by adversaries. Our method exploits the information-theoretic secrecy in the reciprocal channel between Alice and Bob and at the same time adds a computation-based secrecy to protect any amount of information against adversaries. Our method uses a singular value decomposition based SVD-CEF that transforms a secret real-valued vector of limited dimension into an unlimited-length sequence of QCPRNs. We have found that the statistics of these QCPRNs is rather robust against a range of variations of the statistics of the ERCVs by Alice and Bob. This is an important advantage for many environments where the true statistics of ERCVs is unknown. The proposed method exploits the stable statistics of these QCPRNs to obtain uniformly distributed UD-QCPRNs, which are then superimposed onto transmitted information symbols for encryption, and/or onto received encrypted-symbols for decryption. The effect of various noises on the performance at Bob has also been investigated.

References

[1] Y. Zeng, R. Zhang and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," in IEEE Communications Magazine, vol. 54, no. 5, pp. 36-42, May 2016.

[2] A. Swami and B. M. Sadler, "Hierarchical digital modulation classification using cumulants," in IEEE Transactions on Communications, vol. 48, no. 3, pp. 416-429, March 2000.

[3] K. Xu, M. -M. Zhao, Y. Cai and L. Hanzo, "Low-complexity joint power allocation and trajectory design for UAV-enabled secure communications with power splitting," in IEEE Transactions on Communications, vol. 69, no. 3, pp. 1896-1911, March 2021.

[4] G. Zhang, Q. Wu, M. Cui and R. Zhang, "Securing UAV communications via joint trajectory and power control," in IEEE Transactions on Wireless Communications, vol. 18, no. 2, pp. 1376-1389, Feb. 2019.

[5] X. Sun, D. W. K. Ng, Z. Ding, Y. Xu and Z. Zhong, "Physical layer security in UAV systems: challenges and opportunities," in IEEE Wireless Communications, vol. 26, no. 5, pp. 40-47, October 2019.

[6] Y. Hua, "Advanced properties of full-duplex radio for securing wireless networks," in IEEE Transactions on Signal Processing, vol. 67, no. 1, pp. 120-135, Jan 2019.

[7] U. M. Maurer, "Secret key agreement by public discussion from common information," in IEEE Transactions on Information Theory, vol. 39, no. 3, pp. 733-742, May 1993.

[8] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: measurement and analysis," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 3, pp. 381-392, Sept. 2010.

[9] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," in IEEE Transactions on Information Forensics and Security, vol. 5, no. 2, pp. 240-254, June 2010.

[10] Y. Hua, "Reliable and secure transmission for future networks," IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP) 2020, pp. 5260-5264.

[11] Y. Hua and A. Maksud, "Unconditional secrecy and computational complexity against wireless eavesdropping," IEEE 21st International Workshop on Signal Processing Advances in Wireless Communications (SPAWC), USA, 2020, pp. 1-5.

[12] Y. Hua and A. Maksud, "Continuous encryption functions for security over networks," in arXiv:2111.03163

[13] Study Enhanced LTE Support for Aerial Vehicles, document 3GPP TR 36.777 V1.0.0, Dec. 2017.

[14] C. You and R. Zhang, "3D trajectory optimization in rician fading for UAV-enabled data harvesting," in IEEE Transactions on Wireless Communications, vol. 18, no. 6, pp. 3192-3207, June 2019.

[15] D. W. Matolak and R. Sun, "Air-ground channel characterization for unmanned aircraft systems: The near-urban environment," IEEE Military Communications Conference (MILCOM), 2015, pp. 1656-1660.

[16] M. Z. Hameed, A. György and D. Gündüz, "The best defense is a good offense: adversarial attacks to avoid modulation detection," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 1074-1087, 2021.

[17] M. Sadeghi and E. G. Larsson, "Adversarial attacks on deep-learning based radio signal classification," in IEEE Wireless Communications Letters, vol. 8, no. 1, pp. 213-216, Feb. 2019.

[18] H. Zhao, Y. Lin, S. Gao and S. Yu, "Evaluating and improving adversarial attacks on DNN-based modulation recognition," IEEE Global Communications Conference (GLOBECOM), 2020, pp. 1-5.

[19] B. Flowers, R. M. Buehrer and W. C. Headley, "Communications aware adversarial residual networks for over the air evasion attacks," IEEE Military Communications Conference (MILCOM), 2019, pp. 133-140.

[20] Alex Berian et al. "Adversarial filters for secure modulation classification". in arXiv:2008.06785

[21] F. Hameed, O. A. Dobre and D. C. Popescu, "On the likelihood-based approach to modulation classification," in IEEE Transactions on Wireless Communications, vol. 8, no. 12, pp. 5884-5892, December 2009.

[22] V. -S. Doan, T. Huynh-The, C. -H. Hua, Q. -V. Pham and D. -S. Kim, "Learning constellation map with deep CNN for accurate modulation recognition," IEEE Global Communications Conference (GLOBECOM), 2020, pp. 1-6.

[23] S. Peng et al., "Modulation classification based on signal constellation diagrams and deep learning," in IEEE Transactions on Neural Networks and Learning Systems, vol. 30, no. 3, pp. 718-727, March 2019.

[24] K. Grzesiak, Z. Piotrowski and J.M. Kelner, "A wireless covert channel based on dirty constellation with phase drift," in Electronics, vol. 10, no. 6, p. 647, Mar. 2021.

[25] N. Xie, Z. Li, J. Tan and A. X. Liu, "Detection of information hiding at physical layer in wireless communications," in IEEE Transactions on Dependable and Secure Computing, early access, doi: 10.1109/TDSC.2020.3012461.