MIMO Wireless Secure Communication Using Data-Carrying Artificial Noise

Andrew D. Harper, *Member, IEEE*, and Xiaoli Ma, *Fellow, IEEE*

***Abstract*— In MIMO wireless channels, channel estimation can provide a source of randomness common to sender and receiver that may be used to generate secret keys. These keys can provide information theoretically secure communication. Alternatively, a known MIMO channel allows transmitting artificial noise in the null space of the main channel to secure communication. In this paper, we show that both methods can be combined to further enhance secrecy. Symbols encrypted at the transmitter simultaneously act as message for the intended receiver and as noise for any potential eavesdroppers. We derive expressions for the minimum-guaranteeable secrecy rate as a function of number of symbols encrypted. Given at least one symbol can be encrypted, our proposed method outperforms the standard artificial noise scheme in terms of both secrecy rate and power expenditure. We first analyze the system assuming keys can be instantaneously extracted from channel measurements. We then derive bounds for rates assuming the overhead time required for key generation produces a Gaussian channel-estimation error.**

***Index Terms*— Artificial noise, physical layer security, wiretap channel, MIMO wireless, secret key generation.**

I. Introduction

THE broadcast nature of wireless communication makes privacy an inherent concern. The use of the wireless channel for *secret key generation* (SKG) has attracted recent interest. Wireless channels are commonly assumed to be reciprocal for a given frequency, i.e., at any instant in time the multipath properties are identical in both directions of the link between transmitter and receiver. For communication systems that exchange training signals in the same frequency band in both directions, temporal variations of the fading coefficients can provide a source of randomness observable on both ends of the link from which a pair of identical keys can be extracted. Key agreement from wireless channel measurements has been attempted from a number of different properties of the received signal. Due to its ease of measurement, signal amplitude is often used (see, e.g. [1]–[3]). SKG methods based on phase differences [4], [5] and time delay (in wideband transmission) [6], [7] have also been studied. Fading channels in rich scattering environments (with no significant line of sight component) are known also to decorrelate quickly in space; distances greater than half a wavelength are commonly assumed to produce significantly uncorrelated channels [8]. Thus, the wireless channel has an important property of being uniquely observable by Alice and Bob, and is therefore invulnerable to discovery by any eavesdropping third party receiving the pilot signals. Secret key agreement from wireless measurements avoids the problem of distributing the keys *a priori* where it might be intercepted by a malicious outsider.

Once a secure key has been agreed upon, it can be used as a one-time pad (OTP) to encrypt communication. OTP encryption is perfectly secure in that is *provably* unbreakable [9]. Unfortunately, OTP encryption is laden with requirements that restrict its practical feasibility for securing wireless communications in most scenarios. For channels to be perfectly reciprocal, both Alice and Bob must measure the channel simultaneously. Most communications systems are half-duplex, and in practice measurements at Alice and Bob are not perfectly reciprocal but rather highly correlated. To generate enough randomness to form new key bits, the channel must vary sufficiently in time; keys produced with static terminals, for example, generally have insufficient entropy [10]. Moreover, a channel that varies rapidly may produce sufficient randomness to generate longer key strings, but also decorrelates in time more rapidly, exacerbating the imperfect reciprocity. The available secret key length is the mutual information between the channel estimates [11], [12]. Unfortunately, the amount of key bits that can be extracted from wireless measurements is generally too low to fully encrypt communication with an OTP [13], and varies with the number of multipath reflections [11], [12]. Maximization of the achievable secret key rate has been studied in, e.g. [14], [15].

Most current cryptographic methods used today, like RSA, rely on the difficulty of certain problems, e.g. prime factorization or discrete logarithms. Though these problems are not currently solvable in polynomial time, they offer no guarantee against clever attacks with new algorithms in the future. Moreover, RSA and other public-key cryptographic methods can be broken by any eavesdropper intercepting transmission given sufficient time and computational power [16]. Since OTP encryption is by itself generally considered unfeasible for most applications, there have been other efforts at finding new *information-theoretically* (i.e. provably) secure methods of communication. In particular, another effort to secure communications information-theoretically at the physical layer is possible given an SNR advantage at the legitimate receiver relative to the SNR of potential eavesdroppers. The pioneering work of Wyner [17] first demonstrated for the wiretap channel that a simple relative advantage in SNR was sufficient to guarantee a nonzero secrecy rate. This notion was extended

Manuscript received February 13, 2016; revised July 6, 2016 and September 4, 2016; accepted September 4, 2016. Date of publication September 20, 2016; date of current version December 8, 2016. This work was supported by NSF under Grant ECCS-1202286. The associate editor coordinating the review of this paper and approving it for publication was M. Elkashlan.

The authors are with the Georgia Institute of Technology, Atlanta, GA 30332 USA. (e-mail: andrewharper@gatech.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TWC.2016.2611581

to the Gaussian wiretap channel by Leung-Yan-Cheong and Hellman [18], and to the general broadcast channel by Csiszár and Korner [19]. Though, in a wireless system, a relative SNR advantage at Bob cannot be guaranteed in general, it can be artificially created in certain circumstances.

Goel and Negi [20], [21] first coined the term *artificial noise* (AN), and showed that a relative SNR advantage could be generated without knowing the exact location of the eavesdropper by transmitting noise in a subspace orthogonal to the main channel.[1] Since inputs steered into the null space of the main channel by definition do not reach the output, the intended receiver is unaffected by the artificial noise while Eve channel is degraded regardless of location or relative proximity to Alice. Like SKG, using AN for secrecy has its own drawbacks. Power efficiency becomes an issue, since power that could be used to transmit information is instead used to transmit AN symbols. Moreover, decomposition of the main channel into orthogonal subspaces requires accurate channel state information at the transmitter (CSIT). Acquiring CSIT is a costly process, both in terms of power and time spent; it is simpler to acquire accurate CSI at Bob (CSIR) only, for example using pilot-symbol aided modulation. Channel estimation error at the transmitter not only leaks artificial noise power into the signal space, it potentially also leaks additional signal power towards eavesdroppers.

Inaccuracies in CSI have been previously modeled in primarily two ways: channel quantization and channel perturbation. In [25], [26], CSI is acquired at Bob and then a quantized version is fed back to Alice on a rate-limited public channel. Our work differs from [25], [26] first in that CSI is kept secret from outside parties and Alice and Bob are assumed to undergo a reconciliation process to resolve discrepancies in their estimations (see, e.g. [27]), and second in that the CSI in our model is not constrained to lie in a predefined finite set of matrices. In this paper, we use a channel perturbation model similar to [28]. However, to derive a robust beamforming technique, [28] assumes that CSIR is error-free. We use the perturbation to model channel evolution in time, therefore we assume that the channel estimates of *both* Alice and Bob are imperfect. Robust beamforming when Bob has only a single antenna is considered in [29] and numerical solutions are found. In this manuscript, the CSI error modeled represents not discrepancies in channel information at Bob and Alice, which must be resolved during the key agreement process, but rather the fact that the key agreement process may consume a non-negligible amount of time during which the measured channel coefficients become slightly outdated.

Secure communication using either SKG or AN requires accurate CSIT. Once the resources have been used to estimate the channel, the information gleaned from the process should ideally be exploited to the greatest extent possible. In this paper we show that achievable secrecy rates can be increased beyond the strictly AN case by exploiting of the redundant channel estimation process required by both AN and SKG. Though both SKG and AN have been well explored in previous literature, we know of no previous study that directly combines the two methods to capitalize upon this redundancy. We call this system *data-carrying artificial noise* (DCAN), since the encrypted symbols exploit the random output properties of an OTP to act as noise to anyone not possessing the secret key while still carrying information to the legitimate receiver.

The proposed method is as follows. Alice and Bob exchange training pulses and estimate the channel. From this channel estimate they form a common secret key consisting of a limited number of bits, with which Alice encrypts none, some, or all of the message symbols using an OTP.[2] Previous studies indicate key rates are generally low compared to achievable communication rates. Therefore, we focus on the case where only a *portion* of the message symbols can be encrypted. The encrypted symbols are spatially multiplexed with the remaining unencrypted message symbols and AN symbols and transmitted. The intended user has the key and can easily decrypt the encrypted symbols. The output of an OTP is uniformly distributed across the message alphabet, and therefore is unconditionally secure without the key. Thus the encrypted symbols act simultaneously as messages to Bob and interference to Eve.

Various studies have been made into the effects of interference in secret communications. Optimal power allocation in a single-antenna 2×2 interference multiple-access channel is examined in [31]. Our work differs from [31] in that we use spatial multiplexing and beamforming in a MIMO system to enhance the effects of interference and generate higher secret communication rates. In this paper, we assume that the transmitted symbols will be *nearly* Gaussian, so that the symbols are drawn from a discrete set, but closely approximates Gaussian signaling. With this assumption, the interference acts as Gaussian noise at Eve. Gaussian noise is known to be most detrimental of all distributions of a given variance [32]. Thus encrypted data symbols can act simultaneously as an information-theoretically secure message at Bob and as Gaussian noise at Eve.

As with the AN-only case, the DCAN method we introduce in this paper offers a minimum guaranteed secrecy regardless of SNR at Eve. The net gain of our proposed scheme can be summarized as follows:

1) Greater information-theoretically secure communication rates, since some secrecy-guaranteeing artificial noise simultaneously transmits information, and
2) Less power (than the AN-only case) required to achieve a desired secrecy rate, since some of the message symbols simultaneously act to confuse anyone intercepting communication that does not possess the secret key.

[1] Although [20] uses the term *secrecy capacity* in reference to the maximum secret rate, it has been shown that in certain cases AN with SVD-based precoding is only *nearly* optimal; see, e.g., [22] for the case of full eavesdropper CSI, and [23], [24] for the case where only statistical information about the eavesdropper channel is available. Throughout this paper, we use the term secrecy *rate*.

[2] The specifics of the SKG process are beyond the scope of this paper; A SKG algorithm for fading channels is given in [27], where Alice and Bob 1) exchange training signals and measure the channel output, 2) perform error correction to reconcile discrepancies between the measurements, and 3) perform privacy amplification [30] through one-way hash functions to ensure Eve remains ignorant of the final key.

The outline of this paper is as follows. Section II presents the MIMOME system model used throughout the paper. Section III studies the achievable secret communication rates in the case of perfectly known channel stat information (CSI). Section IV derives bounds on secret communication rates assuming that CSI is unknown and must be estimated. The theoretical rates for both cases are illustrated by numerical example in Section VI. Finally, conclusions are presented in Section VII.

Notation: The following notation is used throughout the paper. Bold-face lowercase type denotes vector $\mathbf{a}$; bold-face uppercase type denotes matrix $\mathbf{A}$. $|\mathbf{A}|$, $\mathbf{A}^{\mathrm{T}}$, and $\mathbf{A}^{\mathrm{H}}$ are the matrix determinant, transpose, and Hermitian transpose, respectively. The matrix trace $\mathrm{tr}(\mathbf{A})$ denotes the sum of the diagonal elements of $\mathbf{A}$. The identity matrix of size $p \times p$ is denoted $\mathbf{I}_p$. $\mathbb{C}$ is the field of complex numbers. The entropy of vector $\mathbf{x}$ is $h(\mathbf{x})$; conditional entropy given $\mathbf{z}$ is $h(\mathbf{x}|\mathbf{z})$. The mutual information between vectors $\mathbf{x}$ and $\mathbf{y}$ is $I(\mathbf{x};\mathbf{y})$; mutual information conditioned on $\mathbf{z}$ is $I(\mathbf{x};\mathbf{y}|\mathbf{z})$. The hat symbol $\hat{a}$ denotes the estimate of value a. $\mathrm{E}_{\chi}[\cdot]$ denotes expectation with respect to the probability distribution on χ, and $\mathrm{cov}(\mathbf{w})$ denotes the covariance matrix of a vector $\mathbf{w}$. We use $\mathrm{diag}(\mathbf{x})$ to mean a matrix with elements of $\mathbf{x}$ along its diagonal and zeros elsewhere; similarly, $\mathrm{diag}(\mathbf{A}_1\ \mathbf{A}_2\ \ldots\ \mathbf{A}_K)$ is a block-diagonal matrix constructed from $\mathbf{A}_1, \mathbf{A}_2, \ldots, \mathbf{A}_K$.

II. System Model

Define t, r and e as the number of antennas at Alice, Bob, and Eve, respectively. $\mathbf{H} \in \mathbb{C}^{r\times t}$ is the MIMO main (Alice-Bob) channel matrix, and $\mathbf{G} \in \mathbb{C}^{e\times t}$ is the MIMO eavesdropper (Alice-Eve) channel matrix. We assume a rich-scattering environment such that both channels are flat fading. We further assume the block-fading model, where the coherence time of the channel is large enough that coding can be performed within the transmission interval. The entries of $\mathbf{H}$ are independent and identically distributed (i.i.d.) zero-mean circularly-symmetric complex Gaussian (ZMCSCG). The rich-scattering assumption is critical to ensure Eve is not able to glean information during the SKG process and arrive at a good estimate of the secret key, since experimental studies have shown that, in an environment with insufficient reflections, signals received at Eve during the channel estimation phase can be highly correlated with the main channel [33]. In this paper we assume Eve's channel coefficients are independent of the main channel coefficients; effects of spatial correlation are studied in, for example, [34], [35].

For fair comparison of different antenna configurations, we normalize the channel entries $[\mathbf{H}]_{i,j} \sim \mathcal{CN}(0,1)$ such that the average received SNR is independent of number of transmit antennas. Alice communicates using a set of constellation points $\mathcal{S}$ that approximates a Gaussian input scheme. Alice and Bob begin by estimating the channel and agreeing on a secret key $\mathbf{k} \triangleq [k_1\ k_2\ \ldots\ k_{d_a}]^{\mathrm{T}}$, with $k_i \in \mathcal{S}$. Eve is assumed sufficiently distant from both Alice and Bob such that its probability of guessing the key is no better than chance. Define $d_a, d_b,$ and d_c as the respective number of OTP, unencrypted and AN symbols transmitted, and the set $D \triangleq \{d_a, d_b, d_c\}$.

Let $\mathbf{a} \triangleq [a_1\ a_2\ \ldots\ a_{d_a}]^{\mathrm{T}}$, with $a_i \in \mathcal{S}$, be the symbol vector to be encrypted with key $\mathbf{k}$. Define $\mathbf{b} \triangleq [b_1\ b_2\ \ldots\ b_{d_b}]^{\mathrm{T}}$ and $\mathbf{c} \triangleq [c_1\ c_2\ \ldots\ c_{d_c}]^{\mathrm{T}}$ as vectors of unencrypted and AN symbols, respectively. Given t antennas, Alice has t degrees of freedom with which to design her transmit vector. At least e degrees of freedom must be devoted to interfering with Eve, and at most r of which can transmit information to Bob. Formally, the requirements on D are

$$d_a + d_b + d_c \le t \tag{1}$$

$$0 < d_a + d_b \le r \tag{2}$$

$$d_a + d_c \ge e. \tag{3}$$

The inequality in (1) is a result of Alice's limited degrees of freedom. The inequality on the left-hand side of (2) avoids the trivial cases where no information symbols are transmitted, while the right-hand side inequality ensures that Bob is able to decode all symbols sent that contain information. The justification for (3) follows the main results.

Define an encryption function $f_e : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$ and decrypting function $f_d : \mathcal{S} \times \mathcal{S} \to \mathcal{S}$, and let the perfectly encrypted OTP vector be $\breve{\mathbf{a}} = [\breve{a}_1\ \breve{a}_2\ \ldots\ \breve{a}_{d_s}]^{\mathrm{T}}$, where $\breve{a}_i = f_e(a_i, k_i)$. The OTP key $\mathbf{k}$ ensures a one-to-one mapping from symbol to encrypted symbol given the key symbol, i.e. $f_e(a_i, k_i) = \breve{a}_i$ and $f_d(\breve{a}_i, k_i) = a_i$. Moreover, since each key symbol k_i is uniformly distributed over $\mathcal{S}$, no information is leaked to anyone intercepting the encrypted symbol, i.e. $I(\breve{a}_i; a_i) = 0$. Therefore, we have the two following properties:

$$h(\mathbf{a}|\breve{\mathbf{a}}, \mathbf{k}) = 0 \tag{4}$$

$$h(\mathbf{a}|\breve{\mathbf{a}}) = h(\mathbf{a}). \tag{5}$$

Using (1)-(3), Alice forms the message and AN symbol vector as $\underline{\mathbf{s}} \triangleq \underline{\breve{\mathbf{a}}} + \underline{\mathbf{b}} + \underline{\mathbf{c}}$, where

$$\underline{\breve{\mathbf{a}}} = \left[\mathbf{a}^{\mathrm{T}}\ \mathbf{0}_{t-d_a}^{\mathrm{T}}\right]^{\mathrm{T}} + \left[\mathbf{k}^{\mathrm{T}}\ \mathbf{0}_{t-d_a}^{\mathrm{T}}\right]^{\mathrm{T}} \tag{6}$$

$$\underline{\mathbf{b}} = \left[\mathbf{0}_{d_a}^{\mathrm{T}}\ \mathbf{b}^{\mathrm{T}}\ \mathbf{0}_{t-d_a-d_b}^{\mathrm{T}}\right]^{\mathrm{T}} \tag{7}$$

$$\underline{\mathbf{c}} = \left[\mathbf{0}_{d_a+d_b}^{\mathrm{T}}\ \mathbf{c}^{\mathrm{T}}\ \mathbf{0}_{t-d_a-d_a-d_c}^{\mathrm{T}}\right]^{\mathrm{T}}. \tag{8}$$

Using the SVD, Alice precodes with the right singular vectors to form transmitted vector $\mathbf{x} \triangleq \mathbf{V}\underline{\mathbf{s}}$. The received vectors for the main channel and eavesdropper channel, respectively, are then

$$\mathbf{y}_m = \mathbf{H}\mathbf{x} + \mathbf{n}_m \tag{9}$$

$$\mathbf{y}_e = \mathbf{G}\mathbf{x} + \mathbf{n}_e, \tag{10}$$

where the channel matrix entries $[\mathbf{H}]_{i,j}, [\mathbf{G}]_{i,j} \sim \mathcal{CN}(0,1)$ for all $i \in \{1, 2, \ldots r\}$, $j \in \{1, 2, \ldots t\}$, $\mathbf{n}_m \sim \mathcal{CN}(\mathbf{0}, \sigma_{n_m}^2\mathbf{I})$, and $\mathbf{n}_e \sim \mathcal{CN}(\mathbf{0}, \sigma_{n_e}^2\mathbf{I})$. Equations (9) and (10) together define the MIMO wiretap channel. Let the transmit covariance matrices corresponding to (6)-(8) above be $\mathbf{Q}_j \triangleq \mathbf{V}\mathrm{E}[\mathbf{j}\mathbf{j}^{\mathrm{H}}]\mathbf{V}^{\mathrm{H}}$ for $\mathbf{j} \in \{\underline{\mathbf{a}}, \underline{\breve{\mathbf{a}}}, \underline{\mathbf{b}}, \underline{\mathbf{c}}\}$. Let the corresponding powers be $P_a = \mathrm{tr}(\mathbf{Q}_a) = \mathrm{tr}(\mathbf{Q}_{\breve{a}})$, $P_b = \mathrm{tr}(\mathbf{Q}_b)$, and $P_c = \mathrm{tr}(\mathbf{Q}_c)$. Define the set $Q \triangleq \{\mathbf{Q}_a, \mathbf{Q}_b, \mathbf{Q}_c\}$, and let $\mathcal{Q}$ be the set of all Q fulfilling (1)-(3) and $P_a + P_b + P_c \le P$, i.e., $\mathcal{Q}$ is the set of all configurations

TABLE I
SYMBOLS AND DEFINITIONS

$\mathbf{a}$	$d_a \times 1$ vector of message symbols before OTP
$\underline{\mathbf{a}}$	$t \times 1$ zero-padded vector of message symbols before OTP
$\mathbf{b}$	$d_b \times 1$ vector of unencrypted message symbols
$\underline{\mathbf{b}}$	$t \times 1$ zero-padded vector of unencrypted message symbols
$\mathbf{c}$	$d_c \times 1$ vector of artificial noise symbols
$\underline{\mathbf{c}}$	$t \times 1$ zero-padded vector of artificial noise symbols
$\breve{\mathbf{a}}$	$d_a \times 1$ vector of message symbols after OTP
$\underline{\breve{\mathbf{a}}}$	$t \times 1$ zero-padded vector of message symbols after OTP
$\underline{\mathbf{s}}$	$t \times 1$ sum of zero-padded vectors
$\mathbf{x}$	$t \times 1$ full-CSI precoded transmit vector
$\mathbf{y}_m$	$r \times 1$ full-CSI main-channel received vector
$\mathbf{y}_e$	$e \times 1$ full-CSI eavesdropper-channel received vector
$\overline{\mathbf{x}}$	$t \times 1$ precoded transmit vector with CSI error
$\mathbf{w}_m$	$r \times 1$ Bob's noise plus CSI error interference vector
$\mathbf{w}_m$	$e \times 1$ Eve's channel noise plus CSI error interference vector
$\mathbf{z}_m$	$r \times 1$ Bob's received vector with CSI error
$\mathbf{z}_e$	$e \times 1$ Eve's received vector with CSI error

fulfilling both the antenna and power constraints over which we take the maximum to find the maximum achievable secrecy rate. Table I lists the variables defined here in Section III as well as those introduced in Section IV for comparison and easy reference.

III. DCAN WITH ERROR-FREE CSI

In this section, we make the following assumptions about CSI:

A1. Both Alice and Bob have full, instantaneous, and error-free knowledge of the main channel matrix $\mathbf{H}$, and know the statistics of the eavesdropper channel $\mathbf{G}$ but have no knowledge of any specific realization.

A2. Eve has full, instantaneous and error-free knowledge of the eavesdropper channel $\mathbf{G}$ and of the right singular vector matrix $\mathbf{V}$ of the main channel.

Note that in much of the existing AN literature, the worst-case scenario where Eve has full knowledge of $\mathbf{H}$ is commonly assumed. Our more relaxed assumption of known eavesdropper channel statistics is also very common in existing literature (see, e.g., [25], [36]–[38]); this corresponds to the scenario where Eve's environmental surroundings match those of Alice and Bob, and thus yield an eavesdropper channel independent and identically distributed to the main channel. However, since Eve is assumed to be passive (i.e. not transmitting), her exact channel coefficients remain unknown to Alice. Since Eve is able to receive the training signals from Alice, Eve can easily estimate the MIMO channel $\mathbf{G}$ between herself and Alice. For a comprehensive treatment of secrecy outage performance given presence of eavesdroppers with locations randomly distributed according to a Poisson point process (PPP), see [39]; [40] also uses a stochastic geometry approach, and considers probability of achieving secrecy when both the legitimate users (i.e. Alice, Bob) and eavesdroppers randomly distributed according to a PPP.

Rewriting (10) as

$$\mathbf{y}_e = \mathbf{G}\mathbf{V}\underline{\mathbf{s}} + \mathbf{n}_e, \tag{11}$$

it is clear that, to decode the message symbols, Eve must have not only knowledge of her channel but also partial knowledge of the main channel as well. That is, to arrive at an estimate of $\underline{\mathbf{s}}$, Eve must not only undo the mixing effects of $\mathbf{G}$ but also those of $\mathbf{V}$. Eve's best hope of acquiring main-channel state information is to have either Alice or Bob reveal information to her. This might come in the form of feedback during the main-channel estimation process. For example, in the LTE standard, Bob feeds back to Alice the index of a quantized version of the precoding matrix $\mathbf{V}$ [41]. Given sufficient scattering in the environment and spatial separation (i.e. greater than one-half wavelength distance from both Bob and Alice), it is likely to be overly pessimistic that Eve could reliably know $\mathbf{H}$. In the DCAN scenario considered here, main channel knowledge is gained by reciprocal exchange of training sequences, not by feeding back channel information, and thus Eve is unlikely to have knowledge of $\mathbf{V}$ either. One scenario where Eve might have access to knowledge of $\mathbf{V}$ is if Alice and Bob are communicating non-sensitive information without encryption using channel feedback and then switch to the DCAN method to protect transmission of sensitive data. To simplify and facilitate analysis, we assume Eve has perfect knowledge of $\mathbf{V}$ rather than a quantized version. If Eve knows $\mathbf{V}$, then the expressions we derive are exact; if she does not, then our expressions serve as lower bounds on achievable rates.

Given that we assume $\mathbf{V}$ is perfectly revealed to Eve, a natural question is whether or not revealing $\mathbf{V}$ might also inadvertently reveal other information about $\mathbf{H}$. This question is addressed with the following Lemma:

Lemma 1: Given any $n \times m$ matrix $\mathbf{B}$ with entries $[\mathbf{B}]_{i,j} \sim \mathcal{CN}(0,1)$ for all i, j with SVD $\mathbf{B} = \mathbf{U}_B \Sigma_B \mathbf{V}_B^H$, the distribution of the right singular vector matrix $\mathbf{V}_B$ is independent of $\mathbf{U}_B$ and Σ_B.

Proof: Since the entries of $\mathbf{B}$ are zero-mean complex Gaussian, the columns of $\mathbf{B}$ are zero-mean complex Gaussian vectors. Therefore, the product $\mathbf{B}^{\mathrm{H}}\mathbf{B}$ is a central complex Wishart matrix, and has eigenvalue decomposition $\mathbf{V}_B \Lambda_B \mathbf{V}_B^{\mathrm{H}}$, where $\Lambda_B = \Sigma_B \mathbf{U}_B^{\mathrm{H}} \mathbf{U}_B \Sigma_B$. By [42, Definition 2.6], $\mathbf{B}^{\mathrm{H}}\mathbf{B}$ is unitarily invariant, and thus $\mathbf{V}_B$ is a Haar matrix uniformly distributed on the set of $m \times m$ unitary matrices independent of Λ_B. The proof is completed by noting that the product $\mathbf{B}\mathbf{B}^{\mathrm{H}}$ is also a unitarily-invariant central complex Wishart matrix with Haar matrix $\mathbf{U}_B$ independent of $\Lambda_B^{\mathrm{H}} = \Sigma_B \mathbf{V}_B^{\mathrm{H}} \mathbf{V}_B \Sigma_B$. ■

Lemma 1 shows that revealing the right singular vector matrix $\mathbf{V}$ to Eve does not risk revealing additional correlated information about the main channel. We can therefore assume that Eve has full knowledge of $\mathbf{V}$ without compromising the information-theoretic security. Given this model, with requirements (1)-(3) and assumptions A1-2, we present the main results of this paper in the following theorem:

Theorem 1: In a MIMOME wiretap channel, fix the realization of main and eavesdropper channels as $\mathbf{H}$ and $\mathbf{G}$, respectively. Then, for any chosen transmit covariance matrices set Q, the secrecy rate using the DCAN scheme is

$$R_s^Q(\mathbf{H}, \mathbf{G}, Q) = \left[\log_2 \frac{|\sigma_{n_m}^2 \mathbf{I}_r + \mathbf{H}(\mathbf{Q}_a + \mathbf{Q}_b)\mathbf{H}^{\mathrm{H}}|}{|\sigma_{n_m}^2 \mathbf{I}_r|} - \log_2 \frac{|\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_a + \mathbf{Q}_b + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|}{|\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_a + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|}\right]^+, \tag{12}$$

and the maximum is taken over the set $\mathcal{Q}$ as

$$R_s^{\mathrm{DCAN}}(\mathbf{H},\mathbf{G}) = \max_{Q\in\mathcal{Q}} R_s^{Q}(\mathbf{H},\mathbf{G},Q). \tag{13}$$

Proof: The upper bound on achievable secrecy rates in a Gaussian MIMO wiretap channel is defined as the difference in mutual information between the main and eavesdropper channels [43] given channels $\mathbf{H}$ and $\mathbf{G}$. For DCAN, we assume that the main channel mutual information is also conditioned on the given realization of secret key $\mathbf{k}$. Let the SVD of the fixed main channel be $\mathbf{H} = \mathbf{U}\Sigma\mathbf{V}^{\mathrm{H}}$. The secrecy rate achievable with DCAN is upper bounded by

$$R_s^{\mathrm{DCAN}} = \max_{p(\mathbf{x})}[I(\mathbf{a},\mathbf{b};\mathbf{y}_m|\mathbf{H},\mathbf{k}) - I(\mathbf{a},\mathbf{b};\mathbf{y}_e|\mathbf{G},\mathbf{V})]^{+}, \tag{14}$$

where $p(\mathbf{x})$ is the distribution on transmitted vector $\mathbf{x}$. The first and second terms in (14) correspond to the main-channel and eavesdropper-channel rates, respectively. The first term in (14) can be written

$$\begin{aligned} I(\mathbf{a},\mathbf{b};\mathbf{y}_m|\mathbf{H},\mathbf{k}) &= h(\mathbf{y}_m|\mathbf{H},\mathbf{k}) - h(\mathbf{y}_m|\mathbf{a},\mathbf{b},\mathbf{H},\mathbf{k}) && (15)\\ &\overset{(a)}{=} \log_2|\pi e\mathbf{Q}_{\mathbf{y}_m|\mathbf{H},\mathbf{k}}| - \log_2|\pi e\sigma_{n_m}^2\mathbf{I}|, && (16)\end{aligned}$$

where $\mathbf{Q}_{\mathbf{y}_m|\mathbf{H},\mathbf{k}} = \mathrm{E}[\mathbf{y}_m\mathbf{y}_m^{\mathrm{H}}|\mathbf{H},\mathbf{k}]$, and (a) is achieved by choosing $\mathbf{a},\mathbf{b}$ Gaussian. Since the output of the encryption function f_e is uniformly distributed over $\mathcal{S}$, we have that $\mathrm{E}[\check{\mathbf{a}}\check{\mathbf{b}}^{\mathrm{H}}] = \mathbf{0}_{d_a\times d_b}$, and thus

$$\begin{aligned} \mathrm{E}[\mathbf{y}_m\mathbf{y}_m^{\mathrm{H}}|\mathbf{H},\mathbf{k}] &= \mathbf{H}\mathbf{V}\mathrm{E}[\check{\mathbf{a}}\check{\mathbf{a}}^{\mathrm{H}}|\mathbf{k}]\mathbf{V}^{\mathrm{H}}\mathbf{H}^{\mathrm{H}} + \mathbf{H}\mathbf{Q}_b\mathbf{H}^{\mathrm{H}} + \sigma_{n_m}^2\mathbf{I}_r && (17)\\ &= \mathbf{H}\mathbf{Q}_a\mathbf{H}^{\mathrm{H}} + \mathbf{H}\mathbf{Q}_b\mathbf{H}^{\mathrm{H}} + \sigma_{n_m}^2\mathbf{I}_r. && (18)\end{aligned}$$

Combining the log terms, we arrive at the first term in (12). The second term in (14) can be written

$$\begin{aligned} I(\mathbf{a},\mathbf{b};\mathbf{y}_e|\mathbf{G},\mathbf{V}) &= h(\mathbf{y}_e|\mathbf{G},\mathbf{V}) - h(\mathbf{y}_e|\mathbf{a},\mathbf{b},\mathbf{G},\mathbf{V})\\ &\overset{(b)}{=} \log_2|\pi e\mathbf{Q}_{\mathbf{y}_e|\mathbf{G},\mathbf{V}}| - \log_2|\pi e\mathbf{Q}_{\mathbf{y}_e|\mathbf{a},\mathbf{b},\mathbf{G},\mathbf{V}}|\\ &\overset{(c)}{=} \log_2|\sigma_{n_e}^2\mathbf{I}_e + \mathbf{G}(\mathbf{Q}_a+\mathbf{Q}_b+\mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|\\ &\quad - \log_2|\sigma_{n_e}^2\mathbf{I}_e + \mathbf{G}(\mathbf{Q}_a+\mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|, && (19)\end{aligned}$$

where (b) is achieved by designing $\mathbf{a},\mathbf{b}$ and $\mathbf{c}$ Gaussian, $\mathbf{Q}_{\mathbf{y}_e|\mathbf{G},\mathbf{V}} = \mathrm{E}[\mathbf{y}_e\mathbf{y}_e^{\mathrm{H}}|\mathbf{G},\mathbf{V}]$, $\mathbf{Q}_{\mathbf{y}_e|\mathbf{a},\mathbf{b},\mathbf{G},\mathbf{V}} = \mathrm{E}[\mathbf{y}_e\mathbf{y}_e^{\mathrm{H}}|\mathbf{a},\mathbf{b},\mathbf{G},\mathbf{V}]$, and (c) follows from (5). Combining the log terms, the proof is complete. ∎

The choice of Gaussian inputs is motivated by three facts: First, it is well recognized that a Gaussian distributed input maximizes the first entropy term on the right hand side of (15), i.e. the information in the main channel, for a given covariance. Second, it has been shown that Gaussian noise is the worst possible interference for Eve, thereby minimizing the information throughput in the eavesdropper channel for a given $\mathbf{a},\mathbf{b}$. Third, assuming Gaussian inputs greatly facilitates analysis, i.e. the well-known and commonly used log-det equations result from this assumption. Once the input distribution is chosen, the maximum achievable rate is found by optimizing over possible sub-channel and power allocations.

Corollary 1: In a MIMOME wiretap channel with random main channel $\mathbf{H}$*, random eavesdropper channel* $\mathbf{G}$*, and power constraint* P*, the maximum ergodic DCAN secrecy rate is*

$$\bar{R}_s^{\mathrm{DCAN}} = \mathrm{E}_{\mathbf{H},\mathbf{G}}\left[R_s^{\mathrm{DCAN}}(\mathbf{H},\mathbf{G})\right]. \tag{20}$$

Let $\mathcal{Q}^*$ be a subset of $\mathcal{Q}$ with the additional constraints that $P_a = 0$ and $d_a = 0$. We can then define the strictly AN approach as a special case of the DCAN scheme. For comparison with previous works, we introduce the following definition:

Definition 1: [21] *In a MIMOME wiretap channel with random main channel* $\mathbf{H}$*, random eavesdropper channel* $\mathbf{G}$*, and power constraint* P*, the maximum ergodic AN secrecy rate is*

$$\bar{R}_s^{\mathrm{AN}} = \mathrm{E}_{\mathbf{H},\mathbf{G}}\left[\max_{Q\in\mathcal{Q}^*} R_s^{Q}(\mathbf{H},\mathbf{G},Q)\right], \tag{21}$$

and the minimum secrecy rate guaranteed to be achievable with arbitrarily high eavesdropper SNR is

$$\bar{R}_s^{*\mathrm{AN}} = \lim_{\sigma_{n_e}^2\to 0} \bar{R}_s^{\mathrm{AN}} \tag{22}$$

As SNR at Eve grows large, the determinant in the denominator of the second term in (12) is no longer regularized by the noise term. It is noted in [21] that, to ensure a nonzero determinant, the product $\mathbf{G}\mathbf{Q}_c\mathbf{G}^{\mathrm{H}}$ be full rank. Thus in the AN-only case, we have the requirement that $d_c \geq e$. For the DCAN scheme, we have that $\mathbf{G}(\mathbf{Q}_a + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}$ must be full rank, leading to requirement (3). Clearly, with DCAN, thwarting Eve requires fewer degrees of freedom devoted to AN, and more degrees of freedom can then be used to transmit information. It follows that, in comparison to the strictly AN case, the DCAN scheme may allow for higher secure data rates or reduced power expenditure. To show the possible increase in rates over the AN-only case, we introduce the second Theorem using the following Lemma:

Lemma 2: For any positive-semidefinite matrices $\mathbf{A}$ *and* $\mathbf{B}$ *with arbitrary but identical dimension* $n \times n$*,*

$$|\mathbf{A}+\mathbf{B}| \geq |\mathbf{A}|. \tag{23}$$

Proof: See Appendix A. ∎

Threorem 2: In a MIMOME wiretap channel with random main channel $\mathbf{H}$*, random eavesdropper channel* $\mathbf{G}$*, and power constraint* P*, the maximum ergodic DCAN secrecy rate* $\bar{R}_s^{\mathrm{DCAN}}$ *is bounded by*

$$\bar{R}_s^{\mathrm{AN}} \leq \bar{R}_s^{\mathrm{DCAN}} \leq \bar{C}, \tag{24}$$

where the upper bound is achieved when $d_a = r$*, the lower bound is achieved when* $d_a = 0$*, where*

$$\bar{C} = \mathrm{E}_{\mathbf{H}}\left[\max_{Q\in\mathcal{Q}} \log_2\left|\mathbf{I}_r + \frac{1}{\sigma_{n_m}^2}\mathbf{H}(\mathbf{Q}_a+\mathbf{Q}_b)\mathbf{H}^{\mathrm{H}}\right|\right] \tag{25}$$

is the ergodic capacity of the main channel assuming perfect channel state information at the transmitter and receiver.

Proof: We first prove the right hand side of (24). Since all product terms inside determinants in (12) are positive semidefinite, by Lemma 2 we have that

$$\begin{aligned} &|\sigma_{n_e}^2\mathbf{I}_e + \mathbf{G}(\mathbf{Q}_a+\mathbf{Q}_b+\mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|\\ &\quad \geq |\sigma_{n_e}^2\mathbf{I}_e + \mathbf{G}(\mathbf{Q}_a+\mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|, && (26)\end{aligned}$$

and hence that

$$\log_2 \frac{|\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_a + \mathbf{Q}_b + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|}{|\sigma_{n_e}^2 \mathbf{I}_e + \mathbf{G}(\mathbf{Q}_a + \mathbf{Q}_c)\mathbf{G}^{\mathrm{H}}|} \geq 0. \tag{27}$$

Since $\mathbf{Q}_b$ is a covariance matrix, any nonzero $\mathbf{Q}_b$ will result in the left hand side of (27) nonzero, and therefore will yield a rate strictly less than (25). To establish the equality condition, note that $\bar{R}_s^{\mathrm{DCAN}} = \bar{C}$ implies (27) is fulfilled with equality. Then it must be that $\mathbf{Q}_b = \mathbf{0}$, which implies that $d_b = 0$ and $P_b = 0$. Thus achieving the ergodic capacity is possible only by setting $\mathbf{Q}_b$ to $\mathbf{0}$ in (25) and allocating power to $\mathbf{Q}_{\check{a}}$ according to the standard waterfilling solution. Since ergodic capacity is achieved using all receive antennas, we conclude that $d_a = r$.

Next we prove the left hand side of (24). The equality condition is straightforward by removing the possibility of encrypted symbols, i.e. $d_a = 0$ and $P_a = 0$. This is the aforementioned subset $\mathcal{Q}^*$ which leads to (21). To establish the inequality, note that equation (13) is a maximization over $\mathcal{Q}$. Since $\mathcal{Q}^*$ is a subset of $\mathcal{Q}$, any antenna configuration and power allocation yielding a rate less than (21) will be superseded by (21) in the maximization; therefore the rate maximized over a larger set can only yield a greater (or equal) value. ∎

Theorem 2 demonstrates the true utility of the DCAN method, since the achievable secrecy rates are at least as good as the AN-only scheme, and potentially showing rates nearing the ergodic channel capacity. The price paid for the increase in secrecy rates is additional processing in the SKG step; therefore DCAN would be best suited for systems where secrecy is of utmost importance, even at the expense of complexity.

Definition 2: The minimum secrecy rate guaranteed to be achievable with DCAN and with arbitrarily high eavesdropper SNR is

$$\bar{R}_s^{*\mathrm{DCAN}} = \lim_{\sigma_{n_e}^2 \to 0} \bar{R}_s^{\mathrm{DCAN}}. \tag{28}$$

In the proposed DCAN scheme, the ability of any eavesdropper to gain further advantage while remaining passive is self-limiting. Because there is no currently viable method of knowing an arbitrary channel between two distant points in space (in this case, the locations of Bob and Alice), Eve's best hope as a passive attacker is to boost her SNR by moving closer to the Alice. Note that Eve moving closer to Alice does not automatically violate the assumption of independent channel gains, since, for rich-scattering environments, a distance of only 1/2 wavelength will substantially decorrelate the channel. However, the effect of boosting SNR is limited to Eve. In fact, even when $\sigma_{n_e}^2 \to 0$, Eve's channel capacity (i.e. the 2nd term in (12)) does not grow without bound. This results from the fact that it is impossible for Eve to boost her SNR without simultaneously boosting the interference power from Alice.

Definition 3: For a MIMOME system employing DCAN, fix the power P^{DCAN} to meet the desired secrecy criterion. The power savings *of the DCAN approach over an AN-only strategy with total power P^{AN} is defined as*

$$P^{\mathrm{S}} = \min\left[P^{\mathrm{AN}}\right] - P^{\mathrm{DCAN}} \quad \text{subject to:} \quad \bar{R}_s^{\mathrm{AN}} \geq \bar{R}_s^{\mathrm{DCAN}}. \tag{29}$$

In Section VI we use Definition 2 to demonstrate that DCAN offers greater secrecy rates than AN only even in the worst case of zero eavesdropper noise, and Definition 3 to illustrate the power saved by choosing DCAN over an AN-only strategy.

IV. DCAN With Imperfect Channel Estimation

In this section we relax the assumption that error free CSIT and CSIR are instantaneously available. Rather, the channel will be decomposed into a known, estimated part $\hat{\mathbf{H}}$ and a random error $\tilde{\mathbf{H}}$, with $\mathbf{H} = \hat{\mathbf{H}} + \tilde{\mathbf{H}}$. We assume that the legitimate receiver chooses $\hat{\mathbf{H}}$ to be the minimum mean-square error (MMSE) estimate. With Gaussian channel inputs, the MMSE estimate is also the linear minimum mean-square error (LMMSE) estimate. Since the entries of $\mathbf{H}$ are ZMCSCG, and using the fact that for LMMSE estimation the error terms are uncorrelated, the entries of $\tilde{\mathbf{H}}$ are i.i.d. and ZMCSCG with variance $\sigma_{\tilde{\mathbf{H}}}^2$.

If the statistics of the eavesdropper channel match those of the main channel, then the eavesdropper channel will also evolve during the SKG process, and the result is a slight mismatch between the actual and estimated channels at Eve. Similar to the main channel, the actual eavesdropper decomposes additively into estimated and error terms as $\mathbf{G} = \hat{\mathbf{G}} + \tilde{\mathbf{G}}$. The entries of $\tilde{\mathbf{G}}$ are i.i.d. ZMCSCG with variance $\sigma_{\tilde{\mathbf{G}}}^2 = \sigma_{\tilde{\mathbf{H}}}^2$. However, since we are unable to guarantee any estimation fidelity criterion at Eve, we will assume the worst case where $\sigma_{\tilde{\mathbf{G}}}^2 \to 0$. Formally, we have the following modified assumptions:

- A1′. Both Alice and Bob know the estimate $\hat{\mathbf{H}}$, and know only the statistics of the estimation error $\tilde{\mathbf{H}}$ and eavesdropper channel $\mathbf{G}$.
- A2′. Eve has full, instantaneous and error-free knowledge of the eavesdropper channel $\mathbf{G}$ and of the right singular vector matrix $\hat{\mathbf{V}}$ of the estimated main channel.

It is difficult to derive expressions for the achievable rates using DCAN when the channel must be estimated. However, it is possible to derive upper and lower bounds on the mutual information between channel inputs and outputs under different assumptions [32], [44]. We assume Alice diagonalizes the estimated main channel using SVD to minimize AN leakage caused by imperfect CSI.[3] Let the SVD of the estimated channel be $\hat{\mathbf{H}} = \hat{\mathbf{U}}\hat{\Sigma}\hat{\mathbf{V}}^{\mathrm{H}}$. Then the message and AN symbols can be precoded with $\hat{\mathbf{V}}$ to form the transmit vector $\overline{\mathbf{x}} = \hat{\mathbf{V}}\underline{\mathbf{s}}$. Define $\hat{\mathbf{V}}_a, \hat{\mathbf{V}}_b, \hat{\mathbf{V}}_{ab}$ and $\hat{\mathbf{V}}_c$ as the submatrices of $\hat{\mathbf{V}}$ with all rows and selected columns corresponding to $\check{\mathbf{a}}, \mathbf{b}, [\check{\mathbf{a}}^{\mathrm{T}}\ \mathbf{b}^{\mathrm{T}}]^{\mathrm{T}}$ and $\mathbf{c}$, respectively. Define $\mathbf{R}_{ab} = \mathrm{diag}(\mathbf{R}_a\ \mathbf{R}_b)$. The output of

[3] Although not strictly optimal at low SNR [24], the SVD yields optimal precoding as number of antennas grows large and at moderate to high SNR. Even in low SNR conditions, SVD offers a low-complexity precoding approach with near optimal performance.

the main channel is

$$\begin{aligned}\mathbf{z}_m &= \mathbf{H}\overline{\mathbf{x}} + \mathbf{n}_m && (30)\\ &= (\hat{\mathbf{H}} + \tilde{\mathbf{H}})\hat{\mathbf{V}}\underline{\mathbf{s}} + \mathbf{n}_m && (31)\\ &= \hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}[\check{\mathbf{a}}^{\mathrm{T}}\ \mathbf{b}^{\mathrm{T}}]^{\mathrm{T}} + \tilde{\mathbf{H}}\overline{\mathbf{x}} + \mathbf{n}_m && (32)\\ &= \hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}[\check{\mathbf{a}}^{\mathrm{T}}\ \mathbf{b}^{\mathrm{T}}]^{\mathrm{T}} + \mathbf{w}_m, && (33)\end{aligned}$$

where (32) is reached by noting that the AN vector $\mathbf{c}$ reaches the output only through the channel estimation error, and where $\mathbf{w}_m = \tilde{\mathbf{H}}\overline{\mathbf{x}} + \mathbf{n}_m$ is the interference plus noise vector at Bob. The output at Eve becomes

$$\begin{aligned}\mathbf{z}_e &= \mathbf{G}\hat{\mathbf{V}}\overline{\mathbf{x}} + \mathbf{n}_e && (34)\\ &= \mathbf{G}\hat{\mathbf{V}}_b\mathbf{b} + \big(\mathbf{G}(\hat{\mathbf{V}}_a\check{\mathbf{a}} + \hat{\mathbf{V}}_c\mathbf{c}) + \mathbf{n}_e\big) && (35)\\ &= \hat{\mathbf{G}}\hat{\mathbf{V}}_b\mathbf{b} + \tilde{\mathbf{G}}\hat{\mathbf{V}}\mathbf{b} + \mathbf{w}_e, && (36)\end{aligned}$$

where $\mathbf{w}_e = \big(\mathbf{G}(\hat{\mathbf{V}}_a\check{\mathbf{a}} + \hat{\mathbf{V}}_c\mathbf{c}) + \mathbf{n}_e\big)$ is the interference plus noise vector at Eve.

Threorem 3: In a MIMOME wiretap channel with main channel estimate $\hat{\mathbf{H}}$*, eavesdropper channel estimate* $\hat{\mathbf{G}}$*, and power constraint P, the maximum ergodic DCAN secrecy rate* $\bar{R}_{\tilde{s}}^{\mathrm{DCAN}}$ *is bounded by*

$$\bar{R}_{\tilde{s}}^{L} \le \bar{R}_{\tilde{s}}^{\mathrm{DCAN}} \le \bar{R}_{\tilde{s}}^{U}, \tag{37}$$

where

$$\bar{R}_{\tilde{s}}^{U} = \mathrm{E}\left[\log_2 \frac{\left|\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\mathbf{R}_{ab}\hat{\mathbf{V}}_{ab}^{\mathrm{H}}\hat{\mathbf{H}} + (P\sigma_{\tilde{\mathbf{H}}}^2 + \sigma_{\mathbf{n}_m}^2)\mathbf{I}_r\right|}{\left|\big(\sigma_{\tilde{\mathbf{H}}}^2\|\overline{\mathbf{x}}\|^2 + \sigma_{\mathbf{n}_m}^2\big)\big(\mathbf{I}_e + \mathbf{R}_{\mathbf{w}_e}^{-1}\hat{\mathbf{G}}\hat{\mathbf{V}}_b\mathbf{R}_b(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)^{\mathrm{H}}\big)\right|}\right] \tag{38}$$

$$\bar{R}_{\tilde{s}}^{L} = \mathrm{E}\left[\log_2 \frac{\left|\mathbf{I}_{d_a+d_b} + \mathbf{R}_{ab}(\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_m}^{-1}\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\right|}{|\mathbf{I}_e + \mathbf{G}\hat{\mathbf{V}}_b\mathbf{R}_b\hat{\mathbf{V}}_b^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_e}^{-1}|}\right]. \tag{39}$$

Proof: See Appendix B. ∎

Although deriving exact closed-form expressions for the imperfect-CSI case is difficult, instead of exact expressions we may substitute use of the upper and lower bounds, so long as the bounds are tight for values of interest. We show by simulation in Section VI that the derived bounds are tight for a reasonable range of estimation error.

V. Practical Considerations

Our discussion thus far has concerned the secure wireless communication rates achievable using the proposed DCAN scheme. However, there are practical implementation issues which require further exposition. Specifically, we now address the issues of power allocation, sub-channel assignment, secret key bit allocation, and secrecy coding. As evidenced in the following discussion, these issues are intrinsically coupled and may provide a rich source of future research. Here we expose and discuss the primary practical implications for DCAN implementation. Our results in Section VI provide confirmation of our chosen implementation strategy, as well as additional insights into finding optimal strategies.

The upper bound on achievable secrecy rate with DCAN as defined in (21) is found by taking the maximum over both power allocations and subchannel assignments. It is well known that the waterfilling power allocation strategy achieves the MIMO channel capacity when the transmitter has full CSI [8, Ch. 10]. A natural question is, then, whether a waterfilling power strategy could be used to optimize secrecy rates with DCAN as well. The success of the waterfilling strategy for MIMO channels hinges upon allocating more power to subchannels with higher SNR, and less power to subchannels with low SNR for the *total* set of nonzero signaling subchannels. In the DCAN model, the message power is split between encrypted vector $\mathbf{a}$ and unencrypted message vector $\mathbf{b}$, and the standard definition of waterfilling cannot be directly applied. In the traditional waterfilling approach, the subchannels with lowest SNR may be omitted altogether in favor of maximizing the sum rate. Here, varying the power allocated to $\mathbf{a}$ and $\mathbf{b}$ may in fact allocate power to subchannels that would be omitted in the traditional approach. Thus, it is unlikely that waterfilling is optimal for the DCAN case. In fact, since SVD precoding for Bob does not result in parallel SISO channels for Eve, it is not easy to prove analytically that waterfilling is suboptimal either. For the uniform power approach, power is first divided among vectors $\mathbf{a}, \mathbf{b}$ and $\mathbf{c}$ and then allocated to subchannels evenly within each vector. To maintain a valid waterfilling solution within the DCAN context, we implement waterfilling by first dividing power between $\mathbf{c}$ and the pair $(\mathbf{a}, \mathbf{b})$, and subsequently implementing the waterfilling solution over the joint vector.

For the DCAN scheme, the power allocation chosen affects not only the data rate of the main channel, but also the effective noise at the eavesdropper. These effects are certainly coupled since encrypted symbols act both as data for Bob and noise for Eve. Note that the rate gains from allocating more power to stronger subchannels are achieved by using a Gaussian codebook designed for a higher SNR channel, i.e. using the sphere-packing analogy, reducing the radius of the noise spheres allows more spheres to be packed into the space. For the DCAN scheme, adapting the coding based on subchannel strength requires adapting the number of bits per encrypted symbol as well. In other words, by the very virtue of the fact that stronger channels allow more message spheres to be packed into the signal space, the size of a one-to-one OTP encryption function must grow alongside. This is easily seen by considering the fact that the OTP encryption scheme requires that the entropy of the key be greater than or equal to the entropy of the message [9]. Since we assume the total available key bits to be limited, choosing a waterfilling solution immediately precipitates the issue of which subchannels to encrypt. For example, the transmitter may be forced to decide whether to encrypt a smaller number of strong subchannels or a larger number of weaker subchannels. The amount of information conveyed to Bob is independent of which subchannels are encrypted. Since the columns of the SVD-based precoding matrix are uniformly distributed, the average effect of the encrypted symbols at Eve is also insensitive to subchannel selection. Given the fact that the rate-optimizing benefits of waterfilling vanish at high SNR, the added complexity of waterfilling may be avoided altogether by adopting a simpler uniform power allocation for each channel realization. In addition to simplifying codebook design, a uniform power allocation keeps the number of secret key bits required to encrypt a single symbol constant.

It is important to note that simply adding artificial noise (or encrypted symbols) is not sufficient to keep the unencrypted symbols secret from Eve. It is necessary to design a secrecy code which will simultaneously ensure that 1) Bob is able to decode with arbitrarily small probability of error, and 2) Eve is able to decode arbitrarily little information from the intercepted transmission. Designing secrecy codes turns out to be difficult, and is currently an active area of research. However, the channel coding theorem can be used to show the existence of wiretap codes for the block-fading channel [43], [45]. In the block-fading model, the channel coefficients are assumed to remain constant during the transmission, but vary independently between transmissions. Note that the ergodic expressions we derive can be applied directly to the block-fading model by considering vector inputs. As is true in the AN-only case, retraining is necessary for each fading realization. However, with DCAN the information gained in the channel estimation process is more fully exploited.

Though retraining for each channel realization may seem burdensome, it is actually the very fact that the channel varies within the coherence interval of the codeword that enables finding a wiretap code to guarantee secrecy. A more static channel may require less training, but, for any single set of channel realizations, if the full codeword is transmitted within the coherence interval then the probability that Eve has stronger SNR than Bob is always nonzero. In contrast, coding across fading realizations allows the average SNR at Bob to exceed that at Eve, and thus the information leaked to Eve can be made arbitrarily small. What's more, continued channel evolution is essential to generate new independent secret key bits. The DCAN scheme offers, as does the AN-only scheme, a minimum-guaranteeable secret rate independent of Eve's ability to boost her received signal strength. This rate is found by allowing the receiver noise at Eve to vanish, as done in (22). The minimum-guaranteeable rate results from the fact that, unlike real thermal receiver noise, the power of artificially created noise scales alongside the message signal power for any eavesdropper. With this fact, Alice may construct a secrecy code that fulfills the two requirements through a nested code structure [43, Ch. 6], where a set of random inner codes is capacity achieving for Eve's maximum achievable SNR, and the outer (mother) code that selects from the random inner codes according to the message transmitted.

VI. Simulation Results

To verify the perfect-CSI DCAN Theorems 1-2 and imperfect-CSI DCAN Theorem 3 presented in Section II, we use 2×10^3 Monte Carlo simulations using $(8, 4, 4)$ antennas at Alice, Bob and Eve, respectively. We define the main channel and eavesdropper SNR, respectively, in terms of average received power per antenna as $SNR_m = \text{tr}(\mathbf{Q}_a + \mathbf{Q}_b)/\sigma^2_{n_m}$ and $SNR_e = \text{tr}(\mathbf{Q}_b)/\sigma^2_{n_e}$. To measure the effects of a broad range of eavesdropper SNR, we simulate values of $SNR_e = \{0, 10, 35, 100\}$ dB. The $SNR_e = 100$ dB case simulates the worst-case scenario where Eve has attempted to maximize its SNR by moving close to the transmitter. For the case of imperfect CSI, note that our analysis differs fundamentally from [25], [26], where CSI for the main (MISOSE) channel

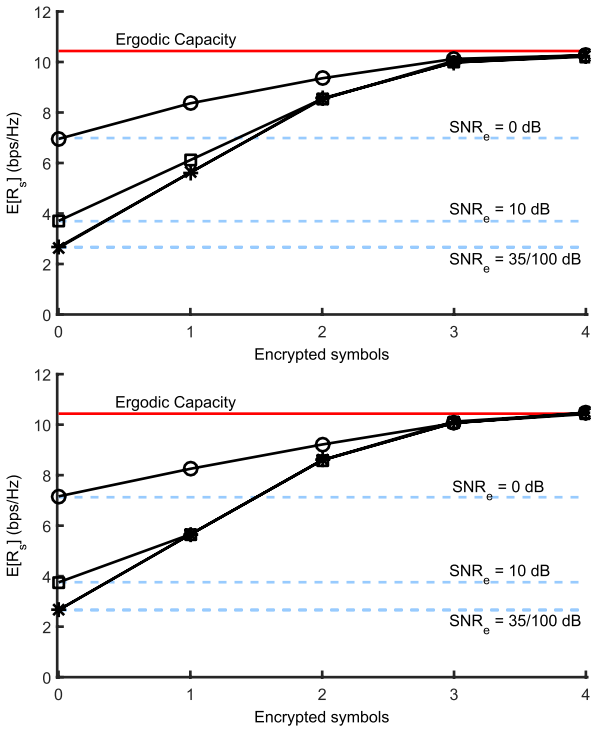


Fig. 1. DCAN achievable rates for a MIMOME system with $t = 8$, $r = 4$, and $e = 4$; uniform power allocation (top) and waterfilling (bottom) for a main-channel SNR of 5 dB. Dotted lines denote the rates achieved by the AN-only case defined in (21); solid lines with $\{\bigcirc, \square, +, \times\}$ markers denote rates achieved with DCAN (20) with respective eavesdropper SNR of $\{0, 10, 35, 100\}$ dB.

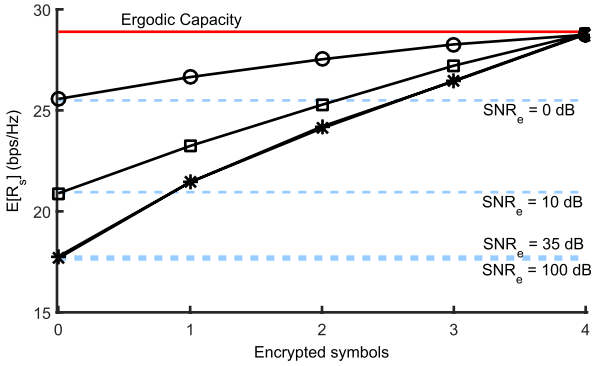


Fig. 2. DCAN achievable rates for a MIMOME system with $t = 8$, $r = 4$, and $e = 4$; (a) and (c) show uniform power allocation at main channel SNR of 5 and 20 dB, respectively, and (b) waterfilling for a main-channel SNR of 5 dB. Dotted lines denote the rates achieved by the AN-only case defined in (21); solid lines with $\{\bigcirc, \square, +, \times\}$ markers denote rates achieved with DCAN (20) with respective eavesdropper SNR of $\{0, 10, 35, 100\}$ dB.

is quantized to a finite number of bits, since we assume both Alice and Bob are able to estimate the main (full MIMOME) channel with sufficient accuracy to form a secret key. Rather, the imperfect CSI in our system is the result of channel evolution during the overhead time associated with the key generation process.

Figures 1-2 show the rates achievable by using DCAN to encrypt varying numbers of transmitted symbols. The ergodic AN-only rate in (21) is selected as the maximum achievable average, allocating signal power $m\alpha P$ and AN power

$(1 - m\alpha)P$, with step size $\alpha = 0.02$ and $m = \{0, 1, \ldots, 50\}$. The results are shown for various eavesdropper SNRs. To benchmark the success of the scheme, these figures also show the ergodic MIMO capacity (horizontal solid line) assuming full CSIT, the same antenna configuration, and the same transmitted power, as well as rates achievable using only AN (horizontal dotted lines) for the various values of SNR_e tested. The top plot in Figure 1 shows uniform power allocation at low (5 dB) main channel SNR. In Figure 2, we compare the DCAN scheme with a main-channel SNR of 20 dB to the corresponding maximum ergodic secrecy rate in the perfect CSI AN-only case (i.e. Definition 1 [20], [21]) for the same values of eavesdropper SNR, antenna configuration and main-channel SNR. Note that the $SNR_e = 100$ line is nearly indistinguishable from $SNR_e = 35$, and thus can be a good approximation for the worst case where $SNR_e \to \infty$.

In each case, the DCAN method is shown to be identical to the AN-only case when no symbols can be encrypted. The bottom plot in Figure 1 shows the curves at low (5 dB) main channel SNR for the waterfilling solution. As expected, when all symbols are encrypted (i.e. $d_a = 4$), waterfilling yields an available secrecy rate matching the ergodic capacity of the channel. The interpretation here is that the achievable secrecy is no longer dependent on the AN symbols, since each information symbol is perfectly encrypted, but rather is limited by the physical properties of the channel and the Gaussian receiver noise at Bob. Similarly, the DCAN curves for uniform power in the top plot in Figure 1 show a maximum rate slightly below capacity even when all symbols are encrypted. Note that, while the rates for waterfilling and uniform power are nearly identical when $SNR_e \to \infty$, uniform power allocation can achieve slightly higher secrecy rates with moderate SNR_e and when a single symbol is encrypted.

Although the AN vector $\mathbf{c}$ is always chosen to lie in the null space of the main channel, the subchannel assignment of $\mathbf{a}$ and $\mathbf{b}$ can be chosen arbitrarily when power is allocated uniformly. This results from the fact that the left singular vectors of $\mathbf{H}$ are uniformly distributed over the unit-radius hypersphere of dimension t [42]. Regardless of assignment, Eve remains ignorant of $\mathbf{U}$ so the interference power is on average spread evenly. If the waterfilling approach is chosen, keeping the number of symbols encrypted constant alongside the number of key bits becomes difficult. Since the limiting factor in encryption is the number of key bits available, the actual number of encryptable symbols may vary with channel realizations. To simplify analysis we again assign the encrypted symbols to the strongest subchannels, and assume that the number of needed key bits in excess of those available is small. As we can see in Figure 1, no significant advantage is gained by waterfilling.

Rates for higher (20 dB) main channel SNR show similar trends as the low SNR cases and increase monotonically with each additional encrypted symbol. When power is allocated uniformly, we see that the greatest secrecy gains come invariably from the first encrypted symbol, and gains decrease monotonically thereafter. This is an encouraging result, since one of the primary drawbacks of generating secret keys from randomness in wireless channels is low key bit rate. Our results

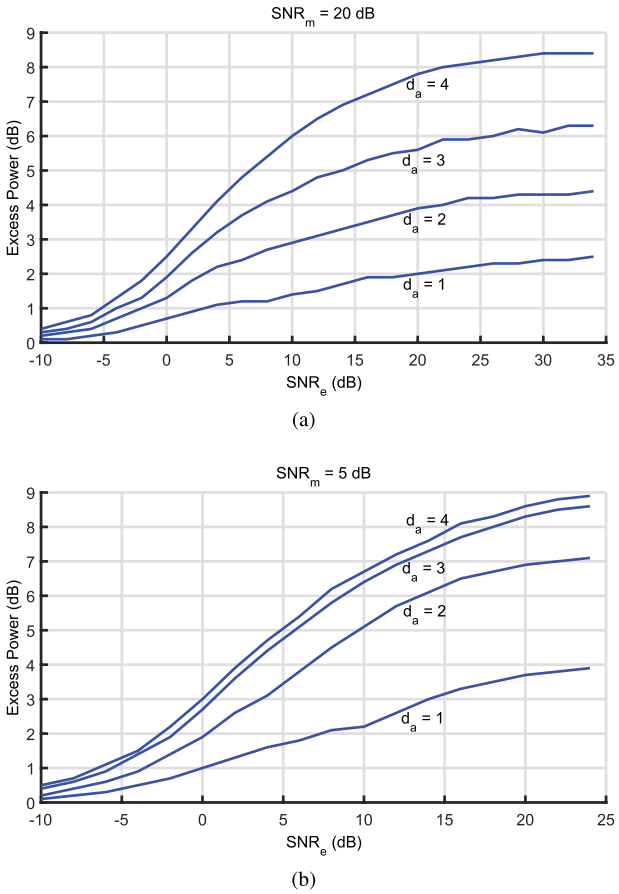


Fig. 3. Excess power required for an AN-only scheme to achieve the same secrecy rate as the DCAN scheme (i.e. power saved by using DCAN), for (a) high, and (b) low, main-channel SNR with $t = 8$, $r = 4$, and $e = 4$.

show that, even when bit rate is low, encrypting just one symbol can have a dramatic impact on achievable secrecy. This fact is supported in Figure 3a, which show the excess power required by an AN-only system to achieve the same amount of secrecy as the DCAN scheme for high main-channel SNR. As SNR_e grows large, a single encrypted symbol saves about 2.5 dB of transmitted power, and each subsequent symbol encrypted saves approximately an additional 2 dB. The low main-channel SNR case is shown in Figure 3b; it is clear that the benefit from encrypting a single symbol is even more pronounced. These results show the benefit of DCAN can be substantial even when the number of symbols the transmitter is able to encrypt is very low. Note that to ensure information is not unintentionally leaked to Eve, the lower bound on secrecy rate must be adopted in designing a proper wiretap code. However, the tightness of the bounds (38)-(39) shows that the penalty paid for using the lower bound is small and, in many cases, nearly negligible.

Simulations for bounds on the DCAN minimum-guaranteed secrecy rate (i.e., $\sigma^2_{\mathbf{n}_e} \to 0$ and $\sigma^2_{\tilde{\mathbf{G}}} \to 0$) defined in Theorem 3 are shown in Figure 4. The three sets of bounds shown are for $\sigma^2_{\tilde{H}} = \{.001,\ .01,\ .1\}$. The solid black, solid red horizontal, and solid blue horizontal lines represent the perfect estimation case, ergodic capacity, and AN-only case for comparison.

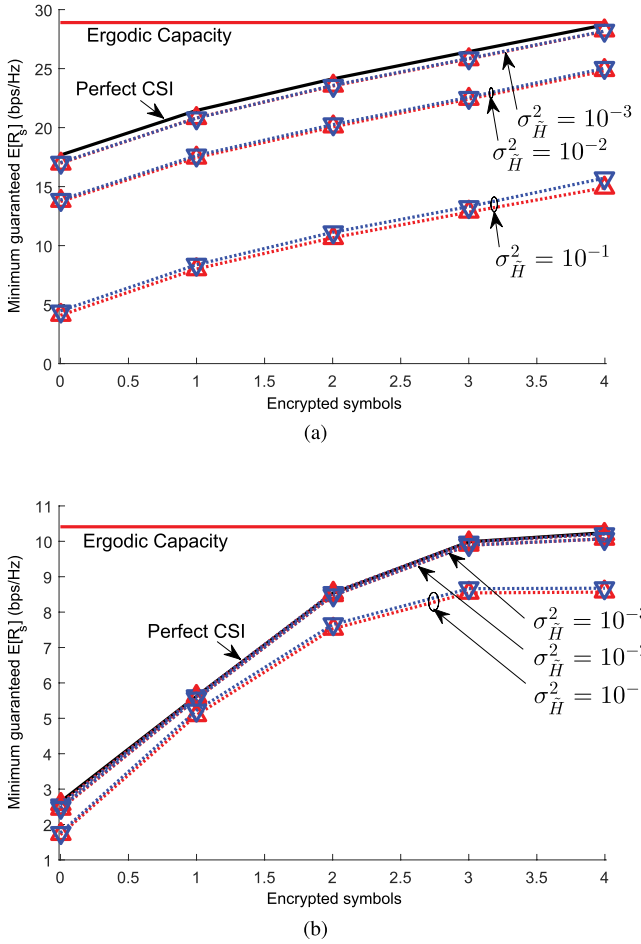


Fig. 4. Bounds on the DCAN minimum achievable secrecy rate with imperfect CSI, for (a) high (20 dB), and (b) low (5 dB) main-channel SNR with $t = 8$, $r = 4$, and $e = 4$. The three sets of bounds shown are for $\sigma^2_{\tilde{H}} = \{.001,\ .01,\ .1\}$. Red "up" markers ($\triangle$) indicate the lower bound, and blue "down" markers ($\triangledown$) indicate the upper bound.

The bounds are tight for estimation errors below 0.1. As expected, the greater error values shift the overall rate down from the error-free case. For high main-channel SNR, the overall trend versus number of encrypted symbols is insensitive to amount of channel estimation error; for low SNR, however, the secrecy rate using lower numbers of encrypted symbols is less affected than the rate at higher numbers.

VII. Conclusions

We have shown how the channel estimation process common to the AN and KG techniques can be leveraged in a MIMOME wiretap channel to enhance achievable secrecy rates and save power over the AN-only scheme. We demonstrate improvements in secret communication rates using a simple uniform power allocation strategy. Our scheme relaxes the common assumption that the eavesdropper has full knowledge of the main channel fading coefficients, and instead assumes only full knowledge of the right singular vector matrix. Our results show that partially one-time padding a message prior to transmission can help protect the remaining unencrypted message, in particular even when only a single message symbol is encrypted per transmission.

Appendix A

By the Minkowsky determinant theorem [46], $|\mathbf{A}+\mathbf{B}|^{1/n} \geq |\mathbf{A}|^{1/n} + |\mathbf{B}|^{1/n}$. Since $\mathbf{A}$ and $\mathbf{B}$ are positive definite, all the eigenvalues for both matrices are strictly positive. Raising to the power n and noting that the determinant of a matrix is the product of it eigenvalues, we may then discard cross terms to arrive at $|\mathbf{A}+\mathbf{B}| \geq |\mathbf{A}| + |\mathbf{B}|$. Noting again the positive-semidefiniteness of $\mathbf{B}$, it follows that $|\mathbf{A}| + |\mathbf{B}| \geq |\mathbf{A}|$, and hence $|\mathbf{A}+\mathbf{B}| \geq |\mathbf{A}|$.

Appendix B

To prove Theorem 3, we first derive upper and lower bounds for the main and eavesdropper channels separately. The average mutual information of the main channel given the MMSE estimate can be written

$$I(\mathbf{a},\mathbf{b};\mathbf{z}_m|\hat{\mathbf{H}}) = h(\mathbf{z}_m|\hat{\mathbf{H}}) - h(\mathbf{z}_m|\mathbf{a},\mathbf{b},\hat{\mathbf{H}}). \tag{40}$$

The first term in (40) can then be written

$$h(\mathbf{z}_m|\hat{\mathbf{H}}) \leq \mathrm{E}\big[\log_2|\pi e\big(\hat{\mathbf{H}}(\hat{\mathbf{V}}_a\mathbf{R}_a\hat{\mathbf{V}}_a^{\mathrm{H}} + \hat{\mathbf{V}}_b\mathbf{R}_b\hat{\mathbf{V}}_b^{\mathrm{H}})\hat{\mathbf{H}}^{\mathrm{H}} + \mathbf{R}_{\mathbf{w}_m}|\big], \tag{41}$$

where $\mathbf{R}_{\mathbf{w}_m} = \mathrm{E}[(\tilde{\mathbf{H}}\overline{\mathbf{x}} + \mathbf{n}_m)(\tilde{\mathbf{H}}\overline{\mathbf{x}} + \mathbf{n}_m)^{\mathrm{H}}]$. Using the facts that $\tilde{\mathbf{H}}\hat{\mathbf{V}}$ is equivalent to $\tilde{\mathbf{H}}$ in distribution and that the entries of $\tilde{\mathbf{H}}$ are uncorrelated ZMCSCG, the error covariance matrix simplifies to $\mathbf{R}_{\mathbf{w}_m} = P\sigma^2_{\tilde{\mathbf{H}}}\mathbf{I}$. Since differential entropy is translation invariant, the second term in (40) can be written

$$h(\mathbf{z}_m|\mathbf{a},\mathbf{b},\hat{\mathbf{H}}) = h(\mathbf{z}_m - \hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}[\mathbf{a}^{\mathrm{T}}\ \mathbf{b}^{\mathrm{T}}]^{\mathrm{T}}|\mathbf{a},\mathbf{b}), \tag{42}$$

and the mutual information in (40) becomes

$$\begin{aligned} &I(\mathbf{a},\mathbf{b};\mathbf{z}_m|\hat{\mathbf{H}}) \\ &\quad\leq \mathrm{E}\big[\log_2\big|\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\mathbf{R}_{ab}\hat{\mathbf{V}}_{ab}^{\mathrm{H}}\hat{\mathbf{H}} + (P\sigma^2_{\tilde{\mathbf{H}}} + \sigma^2_{\mathbf{n}_m})\mathbf{I}\big|\big] \\ &\qquad -\mathrm{E}\big[\log_2\big|(\sigma^2_{\tilde{\mathbf{H}}}\|\overline{\mathbf{x}}\|^2 + \sigma^2_{\mathbf{n}_m})\mathbf{I}\big|\big], \end{aligned} \tag{43}$$

where expectation in (43) is with respect to $\mathbf{H}$ and $\overline{\mathbf{x}}$ for the first and second terms, respectively.

To derive a lower bound, the mutual information in (40) can be equivalently written

$$I(\mathbf{a},\mathbf{b};\mathbf{z}_m|\hat{\mathbf{H}}) = h(\mathbf{a},\mathbf{b}|\hat{\mathbf{H}}) - h(\mathbf{a},\mathbf{b}|\mathbf{z}_m,\hat{\mathbf{H}}). \tag{44}$$

Noting the translation invariance of entropy, the second term in (44) can be written

$$h(\mathbf{a},\mathbf{b}|\mathbf{z}_m,\hat{\mathbf{H}}) \leq h([\mathbf{a}^{\mathrm{T}}\mathbf{b}^{\mathrm{T}}]^{\mathrm{T}} - [\hat{\mathbf{a}}^{\mathrm{T}}\hat{\mathbf{b}}^{\mathrm{T}}]|\mathbf{z}_m,\hat{\mathbf{H}}) \tag{45}$$

for any estimate $[\hat{\mathbf{a}}^{\mathrm{T}}\hat{\mathbf{b}}^{\mathrm{T}}]^{\mathrm{T}}$. It then follows that

$$\begin{aligned} &h(\mathbf{a},\mathbf{b}|\mathbf{z}_m,\hat{\mathbf{H}}) \\ &\overset{(d)}{\leq} h([\mathbf{a}^{\mathrm{T}}\mathbf{b}^{\mathrm{T}}]^{\mathrm{T}} - [\hat{\mathbf{a}}^{\mathrm{T}}\hat{\mathbf{b}}^{\mathrm{T}}]|\hat{\mathbf{H}}) \\ &\overset{(e)}{\leq} \mathrm{E}\big[\log_2\big|\pi e\big(\mathrm{cov}([\mathbf{a}^{\mathrm{T}}\mathbf{b}^{\mathrm{T}}]^{\mathrm{T}} - [\hat{\mathbf{a}}^{\mathrm{T}}\hat{\mathbf{b}}^{\mathrm{T}}]^{\mathrm{T}})\big)\big|\big] \\ &\overset{(f)}{=} \mathrm{E}\big[\log_2\big|\pi e((\mathbf{R}_a + \mathbf{R}_b)^{-1} \\ &\qquad + (\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_m}^{-1}\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{-1}\big|\big], \end{aligned} \tag{46}$$

where (d) follows from the fact that conditioning can only reduce entropy, (e) follows from a Gaussian distribution

maximizing entropy for a given covariance, and (f) follows from using the LMMSE estimate.

Since we choose $\mathbf{a}, \mathbf{b}$ to be Gaussian, the first term in (44) is $h(\mathbf{a}, \mathbf{b}|\hat{\mathbf{H}}) = \mathrm{E}[\log_2|\pi e \mathbf{R}_{ab}|]$, and the main channel mutual information lower bound is

$$I(\mathbf{a}, \mathbf{b}; \mathbf{y}_m|\hat{\mathbf{H}}) \geq \mathrm{E}\big[\log_2\big|\mathbf{I} + \mathbf{R}_{ab}(\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_m}^{-1}\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\big|\big]. \quad (47)$$

Thus, we have that the main channel rate $\bar{R}_m$ is bounded as $\bar{R}_m^L \leq \bar{R}_m \leq \bar{R}_m^U$, where

$$\bar{R}_m^L = \mathrm{E}\big[\log_2\big|\mathbf{I} + \mathbf{R}_{ab}(\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab})^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_m}^{-1}\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\big|\big] \quad (48)$$

$$\bar{R}_m^U = \mathrm{E}\big[\log_2\big|\hat{\mathbf{H}}\hat{\mathbf{V}}_{ab}\mathbf{R}_{ab}\hat{\mathbf{V}}_{ab}^{\mathrm{H}}\hat{\mathbf{H}} + (P\sigma_{\tilde{\mathbf{H}}}^2 + \sigma_{\mathbf{n}_m}^2)\mathbf{I}\big|\big] - \mathrm{E}\big[\log_2\big|\big(\sigma_{\tilde{\mathbf{H}}}^2\|\overline{\mathbf{x}}\|^2 + \sigma_{\mathbf{n}_m}^2\big)\mathbf{I}\big|\big]. \quad (49)$$

The lower bound on the mutual information in the eavesdropper channel can be derived by decomposing the mutual information as

$$I(\mathbf{a}, \mathbf{b}; \mathbf{z}_e) = h(\mathbf{a}, \mathbf{b}) - h(\mathbf{a}, \mathbf{b}|\mathbf{z}_e). \quad (50)$$

The second term in (50) can be written

$$\begin{aligned} h(\mathbf{a}, \mathbf{b}|\mathbf{z}_e) &\overset{(g)}{=} h(\mathbf{a}|\mathbf{z}_e) + h(\mathbf{b}|\mathbf{a}, \mathbf{z}_e) \\ &\overset{(h)}{=} h(\mathbf{a}) + h(\mathbf{b}|\mathbf{a}, \mathbf{z}_e) \\ &\overset{(i)}{=} h(\mathbf{a}) + h(\mathbf{b}|\mathbf{z}_e) \\ &\overset{(j)}{=} h(\mathbf{a}) + h(\mathbf{b} - \hat{\mathbf{b}}|\mathbf{z}_e) \\ &\overset{(k)}{\leq} h(\mathbf{a}) + h(\mathbf{b} - \hat{\mathbf{b}}) \\ &\overset{(l)}{\leq} \log_2|\pi e \mathbf{R}_a| + \log_2|\pi e(\mathrm{cov}(\mathbf{b} - \hat{\mathbf{b}}))|, \end{aligned} \quad (51)$$

where (g) uses the chain rule for differential entropy, (h) follows from the fact that, without the key $\mathbf{k}$, $\mathbf{z}_e$ contains no information about $\mathbf{a}$, (i) follows from the independence of $\mathbf{a}$ and $\mathbf{b}$, (j) follows from the translation invariance of entropy, (k) uses the fact that conditioning can only reduce entropy, and (l) uses the facts that $\mathbf{a}$ is Gaussian and that a Gaussian distribution maximizes the entropy for a given covariance.

Since $\mathbf{a}$ is independent of $\mathbf{b}$, we have that the joint entropy in the first term in (50) can be decomposed as $h(\mathbf{a}, \mathbf{b}) = h(\mathbf{a}) + h(\mathbf{b})$. Choosing $\hat{\mathbf{b}}$ to be the LMMSE estimate yields the lower bound on mutual information

$$I(\mathbf{a}, \mathbf{b}; \mathbf{z}_e) \geq \log_2\big|\mathbf{I}_{d_b} + \mathbf{R}_b(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)^{\mathrm{H}}\mathbf{R}_{\tilde{\mathbf{H}}\underline{\mathbf{b}}+\mathbf{w}_e}^{-1}(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)\big|, \quad (52)$$

where $\mathbf{R}_{\tilde{\mathbf{H}}\underline{\mathbf{b}}+\mathbf{w}_e} = \mathrm{E}[(\tilde{\mathbf{H}}\underline{\mathbf{b}} + \mathbf{w}_e)(\tilde{\mathbf{H}}\underline{\mathbf{b}} + \mathbf{w}_e)^{\mathrm{H}}]$.

To derive the upper bound for the eavesdropper channel, we first show that $I(\mathbf{a}, \mathbf{b}; \mathbf{z}_e) \leq I(\mathbf{a}, \mathbf{b}; \mathbf{z}_e|\mathbf{G})$. Although conditioning can only reduce entropy, no such relationship exists for mutual information in general. In this case, we establish the relationship by subtracting

$$\begin{aligned} I(\mathbf{a}, \mathbf{b}; \mathbf{z}_e|\mathbf{G}) - I(\mathbf{a}, \mathbf{b}; \mathbf{z}) &= h(\mathbf{a}, \mathbf{b}|\mathbf{G}) - h(\mathbf{a}, \mathbf{b}|\mathbf{z}_e, \mathbf{G}) \\ &\quad - h(\mathbf{a}, \mathbf{b}) + h(\mathbf{a}, \mathbf{b}|\mathbf{z}_e) \\ &\overset{(m)}{=} h(\mathbf{a}, \mathbf{b}|\mathbf{z}_e) - h(\mathbf{a}, \mathbf{b}|\mathbf{z}_e, \mathbf{G}) \overset{(n)}{\geq} 0, \end{aligned} \quad (53)$$

where (m) is reached noting that $\mathbf{G}$ is independent of $\mathbf{a}, \mathbf{b}$, and (n) follows from the fact that conditioning can only reduce entropy.

Using (53), we have that

$$I(\mathbf{a}, \mathbf{b}; \mathbf{z}_e) \leq \mathrm{E}\big[h(\mathbf{z}_e|\mathbf{G}) - h(\mathbf{z}_e|\mathbf{a}, \mathbf{b}, \mathbf{G})\big] \quad (54)$$

$$= \mathrm{E}\big[\log_2|\mathbf{I}_e + \mathbf{G}\hat{\mathbf{V}}_b\mathbf{R}_b\hat{\mathbf{V}}_b^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_e}^{-1}|\big]. \quad (55)$$

Thus, we have that the eavesdropper channel rate $\bar{R}_e$ is bounded as $\bar{R}_e^L \leq \bar{R}_e \leq \bar{R}_e^U$, where

$$\bar{R}_e^L = \log_2\big|\mathbf{I}_{d_b} + \mathbf{R}_b(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)^{\mathrm{H}}\mathbf{R}_{\tilde{\mathbf{H}}\underline{\mathbf{b}}+\mathbf{w}_e}^{-1}(\hat{\mathbf{G}}\hat{\mathbf{V}}_b)\big| \quad (56)$$

$$\bar{R}_e^U = \mathrm{E}\big[\log_2|\mathbf{I}_e + \mathbf{G}\hat{\mathbf{V}}_b\mathbf{R}_b\hat{\mathbf{V}}_b^{\mathrm{H}}\mathbf{G}^{\mathrm{H}}\mathbf{R}_{\mathbf{w}_e}^{-1}|\big]. \quad (57)$$

The proof is completed by assigning $\bar{R}_{\tilde{s}}^U = \bar{R}_m^U - \bar{R}_e^L$ and $\bar{R}_{\tilde{s}}^L = \bar{R}_m^L - \bar{R}_e^U$.

ACKNOWLEDGEMENTS

The authors greatly thank Dr. Robert J. Baxley for his guidance in framing the problems addressed in this paper.

REFERENCES

[1] S. N. Premnath *et al.*, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[2] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th Int. Conf. Mobile Comput. Netw. (ACM)*, 2008, pp. 128–139.

[3] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2593–2597.

[4] J. E. Hershey, A. A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

[5] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, Las Vegas, NV, USA, Apr. 2008, pp. 3013–3016.

[6] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," in *Proc. IEEE Int. Conf. Ultra-Wideband (ICUWB)*, Sep. 2007, pp. 270–275.

[7] M. Madiseh, M. McGuire, S. Neville, and A. Shirazi, "Secret key extraction in ultra wideband channels for unsynchronized radios," in *Proc. 6th Annu. Commun. Netw. Serv. Res. Conf. (CNSR)*, May 2008, pp. 88–95.

[8] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge University Press, 2005.

[9] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.

[10] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Int. Conf. Mobile Comput. Netw. (ACM)*, 2009, pp. 321–332.

[11] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting MIMO channel evolution: Algorithms and theoretical limits," in *Proc. 3rd Eur. Conf. Antennas Propag. (EuCAP)*, Mar. 2009, pp. 1499–1503.

[12] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 3, pp. 381–392, Sep. 2010.

[13] J. Croft, N. Patwari, and S. K. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *Proc. 9th ACM/IEEE Int. Conf. Inf. Process. Sensor Netw. (ACM)*, Apr. 2010, pp. 70–81.

[14] B. T. Quist and M. A. Jensen, "Optimal channel estimation in beamformed systems for common-randomness-based secret key establishment," *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 7, pp. 1211–1220, Jul. 2013.

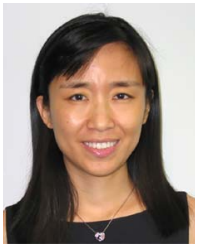
[15] B. T. Quist and M. A. Jensen, "Bound on the key establishment rate for multi-antenna reciprocal electromagnetic channels," *IEEE Trans. Antennas Propag.*, vol. 62, no. 3, pp. 1378–1385, Mar. 2014.

[16] D. Boneh, A. Joux, and P. Q. Nguyen, "Why textbook elgamal and rsa encryption are insecure," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2000, pp. 30–43.

[17] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[18] S. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.
[19] I. Csiszár and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol.IT-24, no. 3, pp. 339–348, May 1978.
[20] S. Goel and R. Negi, "Secret communication in presence of colluding eavesdroppers," in *Proc. IEEE Military Commun. Conf. (MILCOM)*, vol. 3. Oct. 2005, pp. 1501–1506.
[21] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, Jun. 2008.
[22] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas; part II: The MIMOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.
[23] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2007, pp. 2471–2475.
[24] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.
[25] X. Zhang, X. Zhou, M. R. McKay, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission in slow fading channels with limited feedback," in *Proc. IEEE Int. Conf. Acoust., Speech Signal Process. (ICASSP)*, 2014, pp. 3968–3972.
[26] X. Zhang, M. R. McKay, X. Zhou, and R. W. Heath, "Artificial-noise-aided secure multi-antenna transmission with limited feedback," *IEEE Trans. Wireless Commun.*, vol. 14, no. 5, pp. 2742–2754, May 2015.
[27] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[28] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2011.
[29] J. Huang A. L. Swindlehurst, "Robust secure transmission in MISO channels based on worst-case optimization," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1696–1707, Apr. 2012.
[30] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inf. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
[31] J. Zhu, J. Mo, and M. Tao, "Cooperative secret communication with artificial noise in symmetric interference channel," *IEEE Commun. Lett.*, vol. 14, no. 10, pp. 885–887, Oct. 2010.
[32] M. Medard, "The effect upon channel capacity in wireless communications of perfect and imperfect knowledge of the channel," *IEEE Trans. Inf. Theory*, vol. 46, no. 3, pp. 933–946, May 2000.
[33] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction," in *Proc. 4th Eur. Workshop Syst. Secur. (ACM)*, 2011, p. 8.
[34] C. Chen and M. Jensen, "Encryption key establishment using space-time correlated MIMO channels," in *Proc. IEEE Antennas Propag. Soc. Int. Symp. (APSURSI)*, Jul. 2010, pp. 1–4.
[35] C. Chen and M. A. Jensen, "Secret key establishment using temporally and spatially correlated wireless channel coefficients," *IEEE Trans. Mobile Comput.*, vol. 10, no. 2, pp. 205–215, Feb. 2011.
[36] X. Zhou and M. McKay, "Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation," *IEEE Trans. Veh. Technol.*, vol. 59, no. 8, pp. 3831–3842, Oct. 2010.
[37] J. Xiong, K.-K. Wong, D. Ma, and J. Wei, "A closed-form power allocation for minimizing secrecy outage probability for MISO wiretap channels via masked beamforming," *IEEE Commun. Lett.*, vol. 16, no. 9, pp. 1496–1499, Sep. 2012.
[38] N. Yang, J. Yuan, R. Malaney, R. Subramanian, and I. Land, "Artificial noise with optimal power allocation in multi-input single-output wiretap channels," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2014, pp. 2184–2190.
[39] T. X. Zheng, H. M. Wang, J. Yuan, D. Towsley, and M. H. Lee, "Multi-antenna transmission with artificial noise against randomly distributed eavesdroppers," *IEEE Trans. Commun.*, vol. 63, no. 11, pp. 4347–4362, Nov. 2015.
[40] H. M. Wang, T. X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Trans. Commun.*, vol. 64, no. 3, pp. 1204–1219, Mar. 2016.
[41] *Technical Specification LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures (3GPP TS 36.213 version 10.1.0 Release 10)*, document ETSI TS 136 213 V10.1.0, 2011.
[42] A. Tulino and S. Verdu, *Random Matrix Theory and Wireless Communications*. Breda, The Netherlands: Now Publishers Inc., 2004.
[43] M. Bloch and J. Barros, *Physical-Layer Security, From Information Theory to Security Engineering*. Cambridge, U.K.: Cambridge Univ. Press, 2011.
[44] T. Yoo and A. Goldsmith, "Capacity and power allocation for fading MIMO channels with channel estimation error," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2203–2214, May 2006.
[45] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[46] L. Mirsky, *An Introduction to Linear Algebra*. New York, NY, USA: Dover Publications, Nov. 2011.

Andrew D. Harper (M'15) received the B.S. degree in engineering from the Colorado School of Mines in 2008, and the M.S. and Ph.D. degrees in electrical engineering from the Georgia Institute of Technology in 2010 and 2016, respectively. He is currently a Research Engineer with the Georgia Tech Research Institute. His research interests include signal processing for wireless communications, cognitive radio, information and coding theory, and physical-layer security in wireless communications.



Xiaoli Ma (F'15) received the B.S. degree in automatic control from Tsinghua University, Beijing, China, in 1998, the M.S. degree in electrical engineering from the University of Virginia in 2000, and the Ph.D. degree in electrical engineering from the University of Minnesota in 2003. She is currently a Professor with the School of Electrical and Computer Engineering, Georgia Institute of Technology. She has been serving as a Senior Area Editor of the IEEE SIGNAL PROCESSING LETTERS, since 2014 and the journal *Digital Signal Processing* (Elsevier), since 2012. She was an Associate Editor for the IEEE SIGNAL PROCESSING LETTERS from 2007 to 2009 and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS from 2008 to 2013. She received the Lockheed Martin Aeronautics Company Dean's Award for Teaching Excellence by the College of Engineering in 2009, and the Outstanding Junior Faculty Award by the School of Electrical and Computer Engineering in 2010, Georgia Institute of Technology.