The Diversity-Multiplexing Tradeoff of Secret-Key Agreement over Multiple-Antenna Channels

Marwen Zorgui, Student Member, IEEE, Zouheir Rezki, Member, IEEE, Basel Alomair, Member, IEEE and Mohamed-Slim Alouini, Fellow, IEEE

Abstract—We study the problem of secret-key agreement between two legitimate parties, Alice and Bob, in presence of an eavesdropper Eve. There is a public channel with unlimited capacity that is available to the legitimate parties and is also observed by Eve. Our focus is on Rayleigh fading quasi-static channels. The legitimate receiver and the eavesdropper are assumed to have perfect channel knowledge of their channels. We study the system in the high-power regime. First, we define the secret-key diversity gain and the secret-key multiplexing gain. Second, we establish the secret-key diversity multiplexing tradeoff (DMT) under no channel state information (CSI) at the transmitter (CSI-T). The eavesdropper is shown to “steal” only transmit antennas. We show that, likewise the DMT without secrecy constraint, the secret-key DMT is the same either with or without full channel state information at the transmitter. This insensitivity of secret-key DMT toward CSI-T features a fundamental difference between secret-key agreement and the wiretap channel, in which secret DMT depends heavily on CSI-T. Finally, we present several secret-key DMT-achieving schemes in case of full CSI-T. We argue that secret DMT-achieving schemes are also key DMT-achieving. Moreover, we show formally that artificial noise (AN), likewise zero-forcing (ZF), is DMT-achieving. We also show that the public feedback channel improves the outage performance without having any effect on the DMT.

Index Terms—Secret-key agreement, outage probability, high-power, diversity multiplexing tradeoff, artificial noise, conceptual wiretap channel.

I. INTRODUCTION

The increasing need for data transmission by mobile terminals is raising more and more concerns about privacy and security of data communicated over the wireless medium. Addressing these concerns efficiently is paramount in the new communication systems design. Traditionally, protection of the transmitted data relies on public-key cryptography, secret-key distribution and symmetric encryption, which is deemed secure based on the assumption of limited computational abilities of a wiretapper. Henceforth, communication is not provably secure. Such techniques are implemented in the higher layers of the protocol stack with little or absent awareness of the nature of the physical medium. In contrary to this paradigm, information-theoretic security emerged as a solution that guarantees a certain level of security, with no computational restrictions placed on the eavesdropper. Its fundamental idea is to guarantee some secrecy at the physical layer by means of appropriate channel coding techniques. In his seminal paper [1], Shannon introduced the notion of perfect secrecy. His model assumes the existence of a shared key between the legitimate parties that is unknown to the eavesdropper. However, sharing a secret key is not necessary to achieve secrecy. Wyner [2] and Csiszár and Körner [3], later, proved in seminal papers the existence of channel coding guaranteeing not only robustness to transmission errors but also a desired level of data confidentiality, without relying a shared secret-key. In addition to the possibility of transmitting a message securely to a legitimate destination, secret-key agreement arises as one of the promising applications of physical security, in which the objective is to distill a secret-key shared between the legitimate parties. In [4], the achievability of a positive key rate was proved for memoryless binary channels when the destination and the eavesdropper channels are conditionally independent (given the source input symbols), even if the destination channel is not more capable than the eavesdropper channel. The notion of secret sharing is formalized in [5] based on the concept of common randomness between the source and the destination. In the same context, [5] suggests two different system models, called the “source model with wiretapper” (SW) and the “channel model with wiretapper” (CW). The SW model represents a situation in which three parties, two legitimate users and an eavesdropper, observe the realizations of a discrete memoryless source, which is assumed to be outside the control of all parties. The CW model differs in that the source of randomness is controlled by one of the legitimate parties, similar to the basic wiretap channel model [2] with an additional public feedback channel. Extension of both models to the case of secret sharing among multiple users, with the possibility of some terminals acting as helpers has been investigated in [6], [7].

A. Related work

The CW model for secret sharing with conditionally independent destination and eavesdropper channels and continuous channel alphabets is considered in [8], in which the secret-key capacity of such channel is derived. In particular, [8] establishes the secret-key capacity of the ergodic fast-fading multiple-input multiple-output (MIMO) wiretap channel and the corresponding optimal transmit strategy is derived. It is
shown that for such a channel, the source does not require the instantaneous channel state information (CSI) of the legitimate receiver and the eavesdropper. For quasi-static wireless channels, the secret-key capacity is zero in the absence of CSI [9]. In [9], with full CSI knowledge at all the terminals, closed-form expressions for the low-power and high-power regimes are established.

The use of multiple antennas in fading wireless channels not only increases robustness but also transmission rates. One of the important measures that simultaneously investigates both type of gains is the diversity-multiplexing tradeoff (DMT), introduced in [10]. The DMT is a high power performance analysis that characterizes the fundamental tradeoff between the diversity gain and the multiplexing gain. The diversity gain describes the decay rate of the probability of error, and the multiplexing gain represents the rate of increase of the transmission rate in the high-power regime. The DMT analysis and the outage probability are closely related as it is shown that the outage event generally dominates the probability of error in the high-power regime. An outage approach for the wiretap channel is investigated in [11], [12] and [13]. Outage probability for a target secrecy rate is also studied in [14] in the full CSI case where optimal power allocation policies that minimize the outage probability are investigated. The MIMO wiretap channel is investigated in [15] from a DMT point of view. It is shown that in the absence of CSI at the transmitter (CSI-T), the degrees of freedom in the main channel are decreased by the degrees of freedom in the source-eavesdropper channel, and thus the secret DMT depends on the remaining degrees of freedom. Full CSI-T is proven to impact the secret DMT in which case the eavesdropper steals only the transmitter antennas. A zero-forcing scheme is also proposed in [15] and shown to achieve the secret DMT in the case of full CSI-T. In [16], a shorter version of the present paper, we studied secret-key agreement with public discussion over Rayleigh fading quasi-static MIMO channels from a DMT perspective. The notions of secret-key multiplexing gain and secret-key diversity gain were defined. The secret-key DMT was established and it was shown that the eavesdropper is stealing antennas only from the source. This behavior was proved to be insensitive to CSI-T.

B. Contribution of the paper

In this paper, we consider secret-key agreement over quasi-static fading channels as in [16]. We define the secret-key multiplexing gain and the secret-key diversity order. First, we establish the secret-key DMT in case of no CSI-T and provide a detailed proof of the secret-key DMT achievability based on the idea of a conceptual wiretap channel. In this case, we show that the secret-key DMT is equivalent to the DMT of a MIMO peaceful system in which the number of effective transmit antennas is reduced by the number of eavesdropper antennas. In the CSI-T case, we show that, unlike secret DMT, CSI-T does not enhance the secret-key DMT and we present several secret-key DMT-achieving schemes. For instance, we argue that secret DMT-achieving schemes are also secret-key DMT-achieving. In particular, a zero-forcing scheme, shown to be secret DMT-achieving in [15], is secret-key DMT. Moreover, we prove analytically, what has been observed numerically in [15], that artificial noise (AN) is both secret-key and secret DMT-achieving. Finally, we combine a given secret DMT-achieving scheme with the available public channel through a scheme that we refer to as augmented scheme. We show that an augmented scheme improves the outage performance of secret DMT-achieving scheme while still achieving the secret-key DMT. Numerical results supporting the results are presented.

The remainder of this paper is organized as follows. Section II describes the channel model for secret-key agreement. In Section III, we investigate the secret-key DMT in the no CSI-T case and then extend the arguments in the case of available CSI-T in Section IV. We conclude in Section V.

Notations: Throughout this paper, the symbol $\dagger$ indicates the conjugate transpose of a matrix. $I_n$ and $0_{n \times m}$ denote respectively the $n \times n$ identity matrix and the $n \times m$ matrix of zeros. For conciseness, we drop the subscripts whenever the matrix dimensions are clear from the context. Random quantities are denoted with capital letters. We use the symbol $\mathbb{E}\{\cdot\}$ to denote the mutual information between two random variables. We denote the entropy and differential entropy of a random quantity with $\mathbb{H}(\cdot)$ and $h(\cdot)$, respectively. The symbols $|\cdot|$ and $\det(\cdot)$ are used to denote the determinant of a matrix and $\text{Tr}$ denotes the trace operator. We use the notation $A \geq 0$ to denote that $A$ is a positive semi-definite matrix. The expression $f_1(SNR) = f_2(SNR)$ is defined as $\lim_{SNR \to \infty} \log f_1(SNR) = \lim_{SNR \to \infty} \log f_2(SNR)$. Inequalities are defined analogously.

II. System Model and Secret-Key DMT

As illustrated in Fig. 1, we consider the CW model for secret-key agreement between a transmitter and a legitimate receiver in a MIMO wireless network in the presence of an eavesdropper. We assume that the transmitter (Alice), the legitimate receiver (Bob) and the eavesdropper (Eve) are equipped with $m_S$, $m_D$ and $m_E$ antennas, respectively. Transmissions take place over quasi-static fading channels; that is, the MIMO channel matrices $H_D \in \mathbb{C}^{m_D \times m_S}$ and $H_E \in \mathbb{C}^{m_E \times m_S}$ are fixed for the whole duration of the communication. For each channel use, the observation at the legitimate receiver and at the eavesdropper are given by

$$Y_D = H_DX + N_D$$
$$Y_E = H_EX + N_E,$$  \hspace{1cm} (1)

where

- $X$ is the $m_S \times 1$ complex-valued transmitted codeword vector by the source,
- $Y_D$ (resp. $Y_E$) is the $m_D \times 1$ (resp. $m_E \times 1$) complex-valued received codeword vector at the destination (resp. at the eavesdropper),
- $H_D$ (resp. $H_E$) is the $m_D \times m_S$ (resp. $m_E \times m_S$) channel matrix from the source to the destination (resp. the eavesdropper) with independent identically distributed
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2492963, IEEE Transactions on Wireless Communications

Fig. 1. System model of the channel model for secret-key agreement with public discussion.

(i.i.d.) zero-mean unit variance circular-symmetric complex Gaussian entries,
- $N_D$ (resp. $N_E$) is the $m_D \times 1$ (resp. $m_E \times m_S$) noise vector with i.i.d zero-mean unit variance circular-symmetric complex Gaussian entries.

The transmitter is constrained in its total power, that is, equivalent to a trace constraint on the input covariance matrix $K_X = E[XX^H]$, given by

$$\text{Tr}(K_X) \leq m_S \text{SNR}. \quad (2)$$

Note that as the noise variances are normalized to unity, SNR can be seen as the average signal-to-noise ratio per transmit antenna. In addition to the wireless channel, the transmitter and the receiver have access to an interactive, authenticated public channel with unlimited capacity, over which they can exchange unlimited number of public messages. Here, interactive means that the channel is two-way and can be used multiple times, unlimited capacity means that it is noiseless and has infinite capacity and public and authenticated mean that the eavesdropper can perfectly observe all communications over this channel but cannot tamper with the messages transmitted. For a precise description of a key-distillation strategy, we refer the reader to [5]. Concisely, the transmitter sends his codeword (i.e., $n$ input symbols) over the noisy wireless channel. During this process, both legitimate parties can exchange messages over the public channel. At the end, the source generates its secret-key $K$ and the destination generates its secret-key $L$, where $K$ and $L$ take values from the same finite set $\kappa$. We denote the messages sent over the public channel by the random variable $F$. $R_k$ is an achievable secret-key rate through the channel $(X,Y_D,Y_E)$, if for every $\epsilon > 0$, there exists a permissible secret-sharing strategy of the form described above such that

1) $P\{K \neq L\} < \epsilon$,
2) $\frac{1}{n}D(K;Y_E^m,F) < \epsilon$,
3) $\frac{1}{n}H(K) > R_k - \epsilon$, for sufficiently large $n$. The key capacity is the supremum of achievable secret-key rates. Condition (1) means the legitimate parties should agree on a common key with high probability. Condition (2) requires that a negligible rate of information about the key should be leaked to the eavesdropper. Condition (3) implies that the key rate is equal to $R_k$ and condition (4) requires the key distribution to be almost uniform. Note that secret-key agreement schemes can be used in conjunction with wiretap codes to enhance the security of confidential messages. An example is to use the secret-key generated at the end of the process as a one-time pad encryption as [17, Equation 4.4]. This provides weak secrecy guarantees if the secret-key satisfies weak secrecy constraints or strong guarantees if the secret-key generates strong secrecy constraints. We note that while our work studies weak secret-keys, there is a systematic way of creating strong secret-keys from weakly secure keys [18]–[20].

In this work, we investigate the high SNR behavior of the probability of error with a target secret-key rate $R_k^{(T)}(SNR)$ that scales with SNR. We define the secret-key multiplexing gain as

$$\lim_{SNR \to \infty} \frac{R_k^{(T)}(SNR)}{\log SNR} \preceq r_k.$$

The secret-key multiplexing gain indicates how fast the target secret-key rate scales with increasing SNR. We also define the secret-key diversity gain $d_k$ as

$$\lim_{SNR \to \infty} \frac{\log P_e(SNR)}{\log SNR} \preceq -d_k,$$

where $P_e(SNR)$ denotes the probability of error under secret-key constraint.

From the definition of the CW model for secret-key agreement, the probability of error $P_e(SNR)$ of a system targeting a constant (i.e., does not vary with CSI) key rate $R_k^{(T)}(SNR)$ that scales with SNR is, in general, due to three events:

- E1: reliability constraint violation, i.e., condition (1) in the definition of achievable key rate is not satisfied.
- E2: secret-key secrecy constraint violation, i.e., condition (2) is not satisfied.
- E3: uniformity constraint violation, i.e., condition (4) is not satisfied.

Condition (3) will be satisfied as the codebook size complies with the target key rate. Then,

$$P_e(SNR) = P(E1 \cup E2 \cup E3). \quad (3)$$

On the other hand, for given channel realization matrices $H_D$ and $H_E$, the observations of the legitimate receiver and the eavesdropper are conditionally independent given the transmitted signal, i.e., $Y_D \rightarrow X \rightarrow Y_E$ forms a Markov chain. Under the assumption that the channel matrices $H_D$ and $H_E$ are known to all three terminals, [8, Theorem 1] proves that the secret key rate

$$R_k = [I(X;Y_D) - I(Y_D;Y_E)] \quad (4)$$
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2492963, IEEE Transactions on Wireless Communications

\[ K_{Y_k} = \mathbb{E} \left[ Y_E Y_E^\dagger \right], \quad K_{Y_D Y_E} = \mathbb{E} \left[ Y_D Y_E^\dagger \right] \] and \( K_{Y_k Y_D} = K_{Y_D Y_E}^\dagger \). It is easy to check the following expressions: \( K_{Y_D} = H_D K_X H_D^\dagger + I_{m_D}, \quad K_{Y_D Y_E} = H_D K_X H_E^\dagger, \quad K_{Y_K} = H_E K_X H_D^\dagger + I_{m_E} \) and \( K_{Y_k Y_D} = H_E K_X H_D^\dagger \) so that (11) becomes

\[ R_k = \log \det \left( I + H_D K_X H_D^\dagger + I_{m_D} \right)^{-1} H_E K_X H_D^\dagger \] (12)

\[ = \log \det \left( I + H_D K_X \left( I - H_E^\dagger (H_E K_X H_D^\dagger + I_{m_E})^{-1} H_E K_X \right) \right) \] (13)

Optimizing over all covariance matrices that satisfy the power constraint, the secret-key rate outage probability is expressed as

\[ P_{out} \left( R_k^T(SNR) \right) = \inf_{K_X \succeq 0, \text{Tr}(K_X) \leq m_S SNR} P \left( R_k < R_k^T(SNR) \right), \] (14)

where the probability is taken over the random channel matrices \( H_D \) and \( H_E \).

**Lemma 1.** The secret-key rate function \( R_k(K_X) \) in (13) is an increasing function on the set of covariance matrices (positive definite/semi-definite matrices).

**Proof:** Suppose \( K_X \) is non-singular. Using the matrix inversion lemma, for any non-singular covariance matrix \( K_X \), we write

\[ K_X \left( I - H_E^\dagger (H_E K_X H_D^\dagger + I_{m_E})^{-1} H_E K_X \right) = \left( K_X^{-1} + H_E^\dagger H_E \right)^{-1}. \] (15)

Let \( K_1 \) and \( K_2 \) be non-singular covariance matrices such that \( K_1 \preceq K_2 \) (i.e., \( K_2 - K_1 \) is positive semi-definite). Then, it follows that \( K_1^{-1} \succeq K_2^{-1} \) and \( K_1^{-1} + H_E^\dagger H_E \succeq K_2^{-1} + H_E^\dagger H_E \) which also leads to \( (K_1^{-1} + H_E^\dagger H_E)^{-1} \preceq (K_2^{-1} + H_E^\dagger H_E)^{-1} \) and \( H_D(K_1^{-1} + H_E^\dagger H_E)^{-1} H_D^\dagger \preceq H_D(K_2^{-1} + H_E^\dagger H_E)^{-1} H_D^\dagger \). Combining the last expression with (15) and the fact that \( \log \det(\cdot) \) is an increasing function on the cone of positive-definite Hermitian matrices, we obtain \( R_k(K_1) \leq R_k(K_2) \).

The case where \( K_X \) is singular can be handled by substituting \( K_X \) by \( K_X + \epsilon I \). The above derivation still holds, then it suffices to let \( \epsilon \) go to zero in order to prove the result.

If we simply pick \( K_X = \text{SNR} I \), we get an upper bound on the key outage probability. On the other hand, \( K_X \) satisfies the power constraint \( \text{Tr}(K_X) \leq m_S \text{SNR} \), hence \( m_S \text{SNR} I - K_X \succeq 0 \) and \( R_k(K_X) \leq R_k^T(m_S \text{SNR} I) \) by virtue of Lemma 1. Accordingly, the secret-key outage probability satisfies

\[ P \left( R_k(m_S \text{SNR} I) < R_k^T \right) \leq P_{out}(R_k^T) \]

\[ \leq P \left( R_k(\text{SNR} I) < R_k^T \right). \] (16)
At high SNR,
\[
\lim_{SNR \to \infty} \frac{P\left( R_k(SNR I) < R_k^T(SNR) \right)}{\log SNR} = \lim_{SNR \to \infty} \frac{P\left( R_k(m_S SNR I) < R_k^T(SNR) \right)}{\log(m_S SNR)} = \lim_{SNR \to \infty} \frac{P\left( R_k(m_S SNR I) < R_k^T(SNR) \right)}{\log(m_S SNR)}.
\]

Therefore, the bounds are tight on the scale of interest. Hence, we have
\[
P_{out}(R_k^T(SNR)) = P\left( R_k(SNR I) < R_k^T(SNR) \right).
\]

This shows that transmitting independent signals at equal power at each antenna is optimal at high SNR, which complies with the intuition that in absence of CSI, the source has no preference on one direction over the other for its transmission. With this choice of input covariance matrix, the achievable secret-key rate in (13) becomes 1

\[
R_k = \log \det \left( I + SNR H_D \right) \left[ I - SNR H_E \left( I_{m_E} + SNR H_E H_E^H \right)^{-1} H_E \right] H_D^H.
\]

\[
= \log \det \left( I + SNR H_D \left( I + SNR H_E H_E^H \right)^{-1} H_D^H \right)
\]

\[
= \log \frac{\det \left( I + SNR H_E H_E^H + SNR H_E^H H_E \right)}{\det \left( I + SNR H_E H_E^H \right)}.
\]

where (20c) is obtained using the identity $|I + UV^{-1}U^H| = \frac{|V + U^H U|}{|V|}$. To establish the key DMT, we first evaluate the secret-key rate outage probability for a given target key rate $R_k^T(SNR) = r_k \log SNR$.

**Lemma 2.** The secret-key outage probability at high SNR is given by:
\[
P_{out}(r_k \log SNR) = \begin{cases} SNR^{-d_{m_S-m_E,m_D}(r_k)} & \text{if } m_E < m_S \\ 1 & \text{else} \end{cases}
\]

where $d_{m,m}$ is the DMT of a MIMO channel with $n$ transmit and $m$ receive antennas.

**Proof:** For the case $m_E \geq m_S$, it is not hard to check from (20c) that
\[
\lim_{SNR \to \infty} \frac{R_k(SNR)}{\log SNR} = \frac{\det \left( H_D^H H_D + H_E^H H_E \right)}{\det \left( H_E^H H_E \right)}.
\]

Indeed, $\tilde{R}_k(SNR)$ can be written as
\[
\tilde{R}_k(SNR) = \log \frac{\det \left( \frac{1}{SNR} I_{m_S} + H_D^H H_D + H_E^H H_E \right)}{\det \left( \frac{1}{SNR} I_{m_S} + H_E^H H_E \right)}.
\]

As $H_D^H H_E$ is invertible with probability 1 (w.p.1), using the continuity of the function $\Gamma \mapsto \log \det(\Gamma)$ and taking the limit as $SNR \to \infty$, we obtain (22). In this case, the secret-key rate levels off and does not increase with SNR, hence the key outage probability does not decrease with SNR and the key DMT reduces to the single point $(0,0)$.

For the case $m_E < m_S$, $H_E H_E^H$ is invertible w.p.1. From (20a), we can write
\[
\tilde{R}_k(SNR) = \log \det \left( I + SNR H_D \right) \left[ I - H_E \left( \frac{1}{SNR} I_{m_S} + H_E H_E^H \right)^{-1} H_E \right] H_D^H.
\]

Defining
\[
\tilde{R}_\infty(SNR) = \log \det \left( I + SNR H_D \right) \left[ I - H_E \left( H_E H_E^H \right)^{-1} \right] H_D^H,
\]

and expressing the singular value decomposition (SVD) of $H_E$ as $H_E = U_W \left[ S_W 0_{m_S-m_E} \right] \left[ V_W^\dagger V_W \right]$, [8] shows that $\tilde{R}_\infty(SNR)$ can be expressed as
\[
\tilde{R}_\infty(SNR) = \log \det \left( I + SNR H_D \tilde{V}_W \tilde{V}_W^\dagger H_D^H \right).
\]

It is also shown in [8] that
\[
0 \leq \liminf_{SNR \to \infty} \left[ \tilde{R}_k(SNR) - \tilde{R}_\infty(SNR) \right] \leq \limsup_{SNR \to \infty} \left[ \tilde{R}_k(SNR) - \tilde{R}_\infty(SNR) \right] \leq (m_D - j) \log \left( 1 + \text{Tr} \left( \left[ H_E H_E^H \right]^j \right) \right),
\]

where $j$ is the number of positive eigenvalues of $H_D \tilde{V}_W \tilde{V}_W^\dagger H_D^H$. Since $H_D \tilde{V}_W \tilde{V}_W^\dagger H_D^H$ is positive semi-definite, $j$ is equal to its rank. Since the elements of $H_D$ are i.i.d. and are independent of the elements of $H_E$, then $j = \text{rank}(H_D \tilde{V}_W (H_D \tilde{V}_W)^\dagger) = \text{rank}(H_D \tilde{V}_W) = \text{min}(m_D, m_S - m_E)$. Hence, in case $m_D = \text{min}(m_D, m_S - m_E)$, we obtain immediately
\[
\lim_{SNR \to \infty} \tilde{R}_k(SNR) = \lim_{SNR \to \infty} \tilde{R}_\infty(SNR).
\]

Otherwise, since the limit of the difference in (27) is finite, we have
\[
\tilde{R}_k(SNR) \doteq \tilde{R}_\infty(SNR).
\]
Hence, (19) becomes

\[ P_{\text{out}}(R) \]
\[ = P \left[ \mathcal{R}_k(SNR) < r_k \log SNR \right] \]
\[ = P \left[ \mathcal{R}_\infty(SNR) < r_k \log SNR \right] \]  \hspace{1cm} (30)
\[ = P \left[ \log \det(\mathbf{I} + SNR \mathbf{H}_D \mathbf{V}_W \mathbf{V}_W^H \mathbf{H}_D^H) < r_k \log SNR \right]. \]  \hspace{1cm} (31)
\[
= SNR^{-d_{m_S-m_E,m_D}(r_k)}. \]  \hspace{1cm} (32)

Conditioning on the elements of \( H_E, \mathbf{V}_W \) is a deterministic quantity that depends on \( H_E \). Let \( \Psi = H_D \mathbf{V}_W \), since the columns of \( \mathbf{V}_W \) are orthonormal, then, we can check that if \( \Psi \) is an \((m_D, m_S - m_E)\) matrix whose entries are i.i.d. Gaussian entries with zero mean and unit variance as in [15]. The system is equivalent to an \((m_S - m_E) \times m_D\) MIMO system without secrecy constraints whose DMT is well known [10].

\[
P \left[ \log \det \left( \mathbf{I} + SNR \mathbf{H}_D \mathbf{V}_W \mathbf{V}_W^H \mathbf{H}_D^H \right) < r_k \log SNR \mid H_E \right] \]
\[ = P \left[ \log \det \left( \mathbf{I} + SNR \Psi \Psi^H \right) < r_k \log SNR \mid H_E \right] \] \hspace{1cm} (33)
\[ \leq SNR^{-d_{m_S-m_E,m_D}(r_k)}. \]  \hspace{1cm} (34)

Averaging over the realizations of \( H_E \) as in [15], we obtain the result

\[ P_{\text{out}}(r_k \log SNR) \leq SNR^{-d_{m_S-m_E,m_D}(r_k)}. \]  \hspace{1cm} (35)

The key outage probability provides an upper bound on the key DMT. The achievability of this upper bound is proved in the following proposition.

**Proposition 1.** For the multiple-antenna CW channel model, if \( m_E < m_S \), the secret-key diversity-multiplexing tradeoff is given by the piecewise linear function joining the points \((l, d_k(l))\), where \( l = 0, 1, \ldots, \min(m_S - m_E, m_D) \) and \( d_k(l) = (m_S - m_E - l)(m_D - l) \).

If \( m_E \geq m_S \), then the secret-key diversity multiplexing tradeoff reduces to the single point \((0, 0)\).

**Proof:** We already obtained a lower bound on the probability of error. To achieve the lower bound, we use the same scheme proposed in the achievability proof of [8, theorem 1]. The scheme is based on the idea of a conceptual wiretap channel from the destination back to the source which leverages the results of wiretap codes as well as the existence of a public channel with unlimited capacity.

We recall briefly the steps of the scheme. First, the source generates randomness by sending a sequence of i.i.d. codewords \( X^n \) over the wiretap channel such that \( E[|X|^2] \leq m_S SNR \) (so that the power constraint is satisfied). Then, the destination generates, at the target key rate, a sequence \( U^n \) randomly and independent of \((X^n, Y_D^n, Y_E^n)\), observes the realization \( Y_D^n \) and sends \( U^n + Y_D^n \) back to the source through the public channel. This creates a conceptual wiretap channel with input symbol \( U \), for which the source plays now the role of a legitimate receiver and observes \((U + Y_D, X)\) and the eavesdropper observes \((U + Y_D, Y_E)\).

In this scheme, the error events are the same error events in a system with secrecy constraints, which is studied in [15].

\[ P_e(SNR) = P(\text{secrasy not achieved}) \]
\[ \quad \text{or main channel decoding error} \]
\[ \leq P(\text{secrasy not achieved}) \]
\[ + P(\text{main channel decoding error}). \]  \hspace{1cm} (36)

where, as in [15], we have

\[ P(\text{secrasy not achieved}) = P(\mathbb{I}(U; (U + Y_D, Y_E)) > R_d) \]  \hspace{1cm} (38)
\[ \quad P(\text{main channel decoding error}) \]
\[ \leq P(\mathbb{I}(U; (U + Y_D, X)) < R_T), \]  \hspace{1cm} (39)

where \( R_T = R_k + R_d \) denotes the total rate communicated through the conceptual wiretap channel and \( R_d \) is the dummy codewords rate. Since our target key rate scales as \( R_k(SNR) = r_k \log(SNR) + R_d(SNR) \). In order to choose the rates \( R_T \) and \( R_d \), we evaluate the mutual informations involved. Let \( X \) Gaussian with \( K_X = SNR I \).

We first evaluate the mutual information of the main channel.

\[ \mathbb{I}(U; U + Y_D, X) \]
\[ = \mathbb{I}(U; X) + \mathbb{I}(U; U + Y_D | X) \]
\[ = h(U) - h(U + Y_D | X, U) + h(U + Y_D | X) - h(U | X). \]  \hspace{1cm} (40)

Because \( U \) is independent of \((X, Y_D, Y_E)\), we have \( h(U + Y_D | X, U) = h(Y_D | X, U) = h(Y_D | X) \). On the other hand, the term \( h(U + Y_D | X) - h(U | X) \) satisfies

\[ h(U + Y_D | X) - h(U | X) \geq h(U + Y_D | X, Y_D) - h(U | X) \]
\[ = h(U | X, Y_D) - h(U) \]
\[ = h(U) - h(U | X, Y_D) \]
\[ = h(U) - h(U | X) \leq h(U + Y_D) - h(U). \]

Let \( U \) be Gaussian with covariance \( \sigma_U^2 I \). Using [21, Theorem 8.6.5] and the independence between \( U \) and \( Y_D \), the last inequality becomes

\[ h(U + Y_D | X) - h(U | X) \]
\[ \leq \log \det(\pi e K_U + Y_D) - \log \det(\pi e K_D) \]
\[ = \log \frac{\det(K_U + K_Y_D)}{\det K_U}. \]  \hspace{1cm} (41)

\[ \text{Now, since the input symbol } U \text{ has no power constraint, we can choose } \sigma_U^2 \text{ large enough such that for small } \epsilon > 0, \text{ we have} \]

\[ \log \frac{\det(K_U + K_Y_D)}{\det K_U} \leq \epsilon. \]

Indeed, let \( L = \min(m_D, m_E) \) and \( \lambda_i, i = 1, \ldots, L \) be the positive eigenvalues of \( H_D H_D^H \), then

\[ \log \frac{\det(K_U + K_Y_D)}{\det K_U} = \left( 1 + \frac{\sigma_U^2}{\sigma_U^2} \right)^{m_D - L} \prod_{i=1}^{L} \left( 1 + \frac{\sigma_U^2}{\sigma_U^2} + \lambda_i SNR \right). \]
Hence, we have
\[
\log \frac{\det(K_U + K_{Y_D})}{\det K_U} = (m_D - L) \log(1 + \frac{1}{\sigma_U^2}) + \sum_{i=1}^{L} \log(1 + \frac{1}{\sigma_i^2} + \frac{\lambda_i \cdot SNR}{\sigma_U^2}).
\]

(43)
Therefore, if we let \( \sigma_U^2 \) scale as \( \sigma_U^2 = (1 + \lambda_{\text{max}}) SNR^{1+\delta} \) for \( \delta > 0 \) (recall that the destination knows its channel, hence it knows \( \lambda_{\text{max}} \)), then we can write for any \( \epsilon > 0 \) as small as desired and for high SNR
\[
0 \leq h(U + Y_D | X) - h(U | X) \leq \log \frac{\det(K_U + K_{Y_D})}{\det K_U} \leq \epsilon.
\]

Hence, for such choice of \( K_U(\epsilon) \), we obtain
\[
\mathbb{I}(U; U + Y_D, X) \doteq h(U) - h(Y_D | X) + o(\epsilon) \leq h(U) - h(Y_D | X).
\]

(44)
Now (39) becomes
\[
P(\text{main channel decoding error}) \doteq P(h(U) - h(Y_D | X) < R^T(SNR))
\]
\[
= P(\log \det(\pi e K_U) - m_D log(\pi e) < R^T(SNR))
\]
\[
= P(\log \det(K_U) < r_k \log(SNR) + R^d).
\]

(47)
Equation (47) represents the first term of the upper bound in (36) and it will determine later the choice of the dummy-codewords rate. We evaluate the probability of secrecy not achieved. Following the same procedure as above (or simply replacing \( X \) by \( Y_E \), and with the choice of \( K_U \) as explained above, we write similarly
\[
\mathbb{I}(U; U + Y_D, Y_E) = h(U) - h(Y_D | Y_E) + o(\epsilon).
\]

(48)
Applying [22, Lemmas 3 and 4], \( [Y_D^T Y_E^T]^T \) is circular-symmetric complex Gaussian random vector. Hence, using [8, Lemma 1], we obtain
\[
h(Y_D | Y_E) = \log \det(K_{Y_D} - K_{Y_D}Y_EK_{Y_E}^{-1}K_{Y_E} Y_D)
\]
\[
+ m_D \log(\pi e)
\]
\[
= \bar{R}_k(SNR) + m_D \log(\pi e).
\]

(49)
Hence,
\[
P(\text{secrecy not achieved}) \doteq P(h(U) - h(Y_D | Y_E) > R^d)
\]
\[
= P(\log \det(\pi e K_U) - \bar{R}_k(SNR) - m_D \log(\pi e) > R^d)
\]
\[
= P(\log \det(K_U) < \bar{R}_k(SNR) + m_D \log(\pi e)).
\]

(50)
Equations (47) and (51) determine the upper bound on the total probability of error (36). Let \( K_X = SNR I \), and if we let
\[
R^d(SNR) = \log \det(K_U) - \bar{R}_k \log(SNR),
\]

(54)
for \( r_k = 0, \ldots, \min(m_S - m_E, m_D) \). Based on Lemma 2, we obtain
\[
P(\text{secrecy not achieved}) \doteq SNR^{-d_{m_S - m_E, m_D}(r_k)},
\]

(55)
\[
P(\text{main channel decoding error}) \doteq 0.
\]

Overall, the upper bound on the probability of error (36) becomes
\[
P_e(SNR) \leq SNR^{-d_{m_S - m_E, m_D}(r_k)}.
\]

(56)
Therefore, we conclude that the secret-key DMT is equal to \( d_{m_S - m_E, m_D}(r_k) \) if \( m_S > m_E \). If \( m_S \leq m_E \), the key outage probability does not scale with SNR and the key DMT reduces consequently to the single point \((0,0)\).

Proposition 1 states that the eavesdropper steals \( m_E \) antennas from the source only, but does not affect the destination. The key DMT is clearly higher than the secret DMT for which it is shown in [15] that the eavesdropper steals \( m_E \) from both legitimate parties. This advantageous behavior of the key DMT is explained by the availability of the public channel with infinite capacity that compensates for the absence of CSI-T at the source.

When the degrees of freedom in the source-eavesdropper channel, \( \min(m_S, m_E) \) is equal to \( m_S \), then no degrees of freedom are left for the legitimate users and the secret-key DMT, as the key DMT, reduces to the point \((0,0)\).

On the other hand, when \( m_E < m_S \), the CW MIMO system becomes equivalent to an \((m_S - m_E) \times m_D\) MIMO system, from a DMT point of view.

![Fig. 2. The DMT without secrecy constraint, secret DMT with no CSI-T and key DMT. The source, the destination and the eavesdropper have 2, 4 and 1 antennas, respectively.](image-url)
are shown to be respectively equal to $d_{5,3}(r)$, $d_{3,1}(r_s)$ and $d_{3,3}(r_k)$. We clearly see that the secrecy constraint, as in the previous example, imposes not only a diversity gain loss but also a multiplexing gain loss for the secret DMT with no CSI-T in comparison with the DMT without secrecy constraint. On the other hand, the key DMT experiences only a diversity gain loss but still achieves all multiplexing gains. In fact, as highlighted in [15], the secret DMT with no CSI-T always experiences multiplexing gain loss ($m_E$ degrees of freedom) while the key DMT can achieve all multiplexing gains in case $m_S - m_E \geq m_D$ albeit it does experience a secret-key diversity gain loss.

**Remark 1.** If the destination has access to the realization of the eavesdropper channel $H_E$, then no secret-key leakage can be guaranteed in the achievability proof. Indeed, the destination can adapt its dummy codewords rate to its channel to the eavesdropper and set $R^d = \log \det K_U - R_K(SNR)$. Then, (47) and (51) become

\[
P(\text{main channel decoding error}) = P(\log \det K_U < r_k \log(SNR) + R^d) \quad (57)
\]
\[
P(K_k(SNR) < r_k \log(SNR)) = P(\text{secret-key rate outage}) \quad (58)
\]
\[
P(\text{secret-key not achieved}) = 0. \quad (61)
\]

Furthermore, the use of the input covariance matrix $K_X = SNR I$ for the conceptual wiretap channel scheme is not restrictive. In fact, as long as the input covariance matrix $K_X$ achieves the same key rate outage probability, it could be employed as will be discussed further in the following section.

**IV. CHANNEL STATE INFORMATION AT THE TRANSMITTER**

In the previous section, secret-key DMT was investigated with no CSI-T. In this section, we make the assumption that the source has full knowledge about its channel to the destination as well as its channel to the eavesdropper. Though it is arguable that such assumptions are more of a theoretical interest than of a practical regard, investigating the system under this setup will help us understand the fundamental limits of secret-key DMT.

In the next subsections, we establish the secret-key DMT and we revisit some schemes that achieve the key DMT with CSI-T.

**A. secret-key DMT with CSI-T**

We recall the expression of the secret-key capacity (6), known from [9] and given by:

\[
C_K = \max_{K_X \succeq 0, \text{Tr}(K_X) \leq m_S SNR} \mathbb{I}(X; Y_D | Y_E).
\]

Having full CSI-T enables the source to determine the optimal covariance matrix achieving the key capacity, or equivalently minimizing the secret-key rate outage probability. Hence, for $K_X$ attaining the maximum in (6), the secret-key rate outage probability is given by

\[
P_{out}(r_k \log(SNR))
= P(\max_{K_X \succeq 0, \text{Tr}(K_X) \leq m_S SNR} \mathbb{I}(X; Y_D | Y_E) < r_k \log(SNR))
\]
\[
\leq \min_{\text{Tr}(K_X) \leq m_S SNR} P(\mathbb{I}(X; Y_D | Y_E) < r_k \log(SNR)) \quad (62)
\]
\[
\leq SNR^{-d_{m_S - m_E, m_D}(r_k),} \quad (63)
\]

where the last equality follows from (19) and Lemma 2. This states that even though $K_X = SNR I$ would not necessarily be the optimal covariance matrix maximizing the secret-key capacity, from a key DMT perspective, splitting the available power equally among the different source antennas is optimal. Thus, the key outage probability is the same in case of CSI-T. Therefore, the same upper bound on the secret-key diversity still holds in the CSI-T case. Achieving this upper bound is straightforward. The schemes based on the conceptual wiretap channel, as described in the proof of Proposition 1 or in Remark 1, can be used since they do not require CSI-T to achieve the key DMT.

Recall that for the MIMO wiretap channel, a uniform power allocation is not optimal from the secret DMT perspective [15]. This observation highlights again another difference between the key agreement setup and coding for secrecy problem. In fact, splitting the power equally does not achieve the secret outage probability, but rather results in the eavesdropper stealing both transmitter and receiver antennas. To achieve the maximum secret DMT in case of CSI-T, a more sophisticated input covariance matrix must be used as shown in [15]. In Fig. 4, we illustrate the latter idea. We compare the secrecy outage probability and the secret-key outage probability for a 2-antenna source, a 2-antenna destination and a single antenna eavesdropper, using the input covariance matrix $K_X = SNR I$ in both cases. The target multiplexing gain is also the same, and it is assumed to be equal to 0.8; thus the secret diversity gain is equal to 0.2, whereas the key diversity.
Remark 2. Based on the previous analysis, perfect knowledge of CSI-T does not enhance the DMT compared to the case of no CSI-T. The case of estimated CSI-T lies in between these two extremes, which are characterized by the same DMT performance. Thus, we conclude that estimated CSI-T achieves, likewise, the same DMT.

Remark 3. For a single input single output (SISO) system, one can always achieve a positive secret-key rate with perfect CSI-T. However, from a DMT perspective, the achievable multiplexing gain reduces to zero, as the secret-key capacity does not scale with the input power for a SISO system.

B. Other Schemes achieving the key DMT

In the CSI-T case, the secret DMT coincides with the key DMT. This is relevant since a wiretap code over the wiretap channel \((X, Y_D, Y_E)\) is a key-agreement strategy for the CW model. Any scheme achieving the secret DMT could hence be employed to achieve the same key DMT without relying on the existence of the public channel.

A wiretap code over the main channel with the optimum covariance matrix maximizing the secrecy capacity was used to prove the achievability of the secret DMT in [15].

A Zero-forcing scheme is also suggested and proved to achieve the secret DMT. It consists in transmitting information in the nullspace of the eavesdropper, which guarantees not only secrecy but also a good outage performance. Let \(U\) represent the secret information, which is a length \(m_S - m_E\) and \(A\) an \(m_S \times m_S - m_E\) matrix whose columns form an orthonormal basis of the nullspace of \(H_E\). Then, the transmitted signal can be expressed as \(X = AU\). The achievable secrecy rate is shown in [15] to be

\[ R^{ZF} = \log \det \left( I_{m_D} + \frac{m_S}{m_S - m_E} \mathbb{E} \left| H \right|^2 \right). \]  

Instead of using the nullspace of the eavesdropper channel matrix, we can exploit the nullspace of the destination matrix in case \(m_D > m_S\), using an artificial noise scheme. Artificial noise is presented in [23]. It consists in transmitting information in the range space of the destination channel matrix \(H_D\) along with transmitting extra noise in the nullspace of \(H_D\). It is a semi-blind scheme since it requires only the knowledge of \(H_D\) to construct the signaling codebook. Let \(T\) be an \(m_S \times (m_S - m_E)\) matrix, whose columns form an orthonormal basis for the nullspace of \(H_D\), \(V\) an \(m_S - m_D\) column vector with i.i.d. zero mean complex Gaussian entries that represent the extra noise, and \(S\) be \(m_S - m_D\) column vector that carries source messages. Then, the transmitter sends \(X = S + TV\). The achievable secrecy rate is shown in [15] to be

\[ R^AN = \log \left| I_{m_D} + \frac{\mathbb{E} \left| H \right|^2}{2} H_D H_D^\dagger \right| - \log \left| \frac{\mathbb{E} \left| K \right|^2}{2} H_E H_E^\dagger \right|, \]

where \(K = I + \frac{\mathbb{E} \left| H \right|^2}{m_S} H_E T T^\dagger H_E^\dagger\). It is suggested in [15] through simulations, but without a formal proof, that the artificial noise scheme achieves the secret DMT. We formally establish its secret DMT optimality by leveraging our result for the key rate outage expression.

**Proposition 2.** The artificial noise scheme achieves the full secret DMT in case of CSI-T.

**Proof:** See Appendix A.

DMT-optimality of ZF and AN over the wiretap channel with public discussion suggests that the public channel has in fact no value from a DMT point of view. However, as we show below, the public channel may be useful in improving the outage performance. An intuitive way of enhancing the performance of a secret DMT-achieving scheme is to use its corresponding covariance matrix structure to create randomness through the main channel and then communicate the key over the conceptual wiretap channel. We refer to the new scheme obtained that way as the augmented scheme. The outage performance of an augmented scheme is expected to be higher, and this idea is corroborated by the following lemma.

**Lemma 3.** For a given covariance matrix \(K_X\), the achievable secret rate \(R_s(K_X)\) is lower than the achievable key rate \(R_k(K_X)\).

**Proof:** Let \(K_X\) be a non-singular input covariance matrix, we have from (13) and (15),

\[ R_k(K_X) = \log \det \left( I + H_D \left( K_X^{-1} + H_E H_E^\dagger \right)^{-1} H_D^\dagger \right) \]
\[ = \log \frac{\det \left( K_X^{-1} + H_E H_E^\dagger \right)}{\det \left( K_X^{-1} + H_D H_D^\dagger \right)}, \]

where the last equality is obtained using the identity \(|I + U V^\dagger| = \frac{|V + U^\dagger U|}{|V|}\). We also know from [15] that the achievable secrecy rate is

\[ R_s(K_X) = \]
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2492963, IEEE Transactions on Wireless Communications

forcing scheme since $K$.

However, no benefit is obtained by "augmenting" the zero-forcing scheme since $K^{ZF}$, which implies that $H_E K^{ZF}$ is singular can be handled by substituting $K$ by $K + \epsilon I$. The above derivation is hence applicable, then it follows immediately that $R_s(K^{ZF}) = K^{ZF}$.

This reasoning applies to the artificial noise where we have outlined that the secret-key DMT is insensitive to CSI-T. First, we have studied the case of no-eavesdropper's antennas, i.e., $K = K^f H^f E + H^f D H_D$, and the secret-key DMT is equivalent to that of a secret-key DMT is insensitive to CSI-T.

In Fig. 5, the outage performance of the described schemes achieving the key DMT is represented in case of full CSI. The schemes are the conceptual wiretap scheme with equally-split (uniform) power, the zero-forcing and the artificial noise schemes along with their corresponding 'augmented' schemes. The figure confirms that the schemes achieve a secret-key diversity 0.25 for a key multiplexing gain 1.75. Another observation is that transmitting the secret-key in the nullspace of the eavesdropper is the most attractive scheme for two reasons. First, it performs better in terms of outage probability compared to the artificial noise and a uniform power distribution schemes. Second, it does not require the public channel to achieve its performance, hence the cost of using the public channel can be saved.

V. Conclusion

In this paper, we have investigated the secret-key diversity multiplexing tradeoff of Rayleigh fading quasi-static MIMO channels. We have established the secret-key DMT for arbitrary number of antennas at the transmitter, the destination and the eavesdropper. First, we have studied the case of noCSI-T. Our analysis shows that, in the high-power regime, a uniform power allocation achieves the maximum exponent of the probability of error in the considered regime. This means that distributing the power uniformly across the transmit antennas is optimum from a DMT perspective. We have also shown that the transmitter obtains secret-key diversity only if his number of antennas is strictly greater than the eavesdropper’s antennas, i.e., $m_S > m_E$. In this case, the eavesdropper steals $m_E$ antennas from the source and the secret-key DMT is equivalent to that of a $(m_S - m_E) \times m_D$ MIMO system without secrecy constraints. Furthermore, we have outlined that the secret-key DMT is insensitive to CSI-T. This observation implies that coding over the wiretap wiretap channel, without the need of the public channel, is sufficient to achieve the full secret-key DMT, since in this case the secret DMT coincides with the secret-key DMT. In particular, we
have proved analytically that artificial noise, likewise zero-forcing, is secret DMT and key DMT-achieving. In the CSI-T case, it is shown that the public feedback channel improves the outage performance without having any effect on the DMT.

APPENDIX A
PROOF OF PROPOSITION 2

In the artificial noise scheme, with the assumption that the transmitter has full knowledge of both channels matrices, the achievable secrecy rate can be written as [15]

\[ R_{s}^{AN} = \log |I + \frac{SNR}{2} H_{D} H_{D}^{\dagger}| - \log \left| \frac{K + \frac{SNR}{2} H_{E} H_{E}^{\dagger}}{K} \right| , \]

where \( K = I + \frac{SNR}{2(m_{S} - m_{D})} H_{E} T T^{\dagger} H_{E}^{\dagger} \) and \( T \) is an \((m_{S} \times m_{S} - m_{D})\) matrix whose columns form an orthonormal basis for \( \text{Null}(H_{D}) \).

Let \( H_{D} = U \begin{bmatrix} \Delta & 0_{m_{D} \times m_{S} - m_{D}} \end{bmatrix} \begin{bmatrix} T_{2}^{\dagger} \\ T \end{bmatrix} \) be the SVD of \( H_{D} \)

where \( U \) and \( \begin{bmatrix} T_{2} & T \end{bmatrix} \) are unitary matrices.

The secrecy rate outage probability is expressed as

\[ P_{out}^{AN}(SNR) = P \left( \log |I + \frac{SNR}{2} H_{D} H_{D}^{\dagger}| - \log \left| \frac{K + \frac{SNR}{2} H_{E} H_{E}^{\dagger}}{K} \right| \right) \]

\[ < r_{s} \log (SNR) \]

\[ = P \left( \log |I + \frac{SNR}{2} H_{D} H_{D}^{\dagger}| + \log |K| \right) \]

\[ - \log \left| K + \frac{SNR}{2} H_{E} H_{E}^{\dagger} \right| < r_{s} \log (SNR) \]

\[ = P \left( \log \left| I_{m_{D}} + \frac{SNR}{2} H_{D} H_{D}^{\dagger} \right| + \log |K| \right) \]

\[ - \log \left| K + \frac{SNR}{2} H_{E} H_{E}^{\dagger} \right| < r_{s} \log (SNR) \] (77)

We develop now each term separately. Using the fact that \( H_{D} T = 0 \) (since the columns of \( T \) span the nullspace of \( H_{D} \)), we write

\[ A = \left| I_{m_{D}} + \frac{SNR}{2} H_{D} H_{D}^{\dagger} \right| \left| K \right| \]

\[ = \left| I_{m_{S}} + \frac{SNR}{2} H_{D}^{\dagger} H_{D} \right| \left| I_{m_{S}} + \frac{SNR}{2(m_{S} - m_{D})} T T^{\dagger} H_{E}^{\dagger} \right| \]

\[ = \left| I_{m_{S}} + \frac{SNR}{2} H_{D}^{\dagger} H_{D} + \frac{SNR}{2(m_{S} - m_{D})} T T^{\dagger} H_{E}^{\dagger} \right| . \]

Let \( B = \left| K + \frac{SNR}{2} H_{E} H_{E}^{\dagger} \right| \). We carry out the proof on three steps. First, we prove that

\[ A \leq \left| I_{m_{S}} + \frac{SNR}{2} H_{D}^{\dagger} H_{D} + SNR H_{E} H_{E}^{\dagger} \right| . \]

Let \( A_{\infty} = \left| I_{m_{S}} + \frac{SNR}{2} H_{D}^{\dagger} H_{D} + \frac{SNR}{2(m_{S} - m_{D})} H_{E}^{\dagger} H_{E} \right| \). Since \( \begin{bmatrix} T_{2} & T \end{bmatrix} \) is unitary, then \( T_{2}^{\dagger} T_{2} + T T^{\dagger} = I \), which implies

\[ A = \left| I_{m_{S}} + \frac{SNR}{2} H_{D}^{\dagger} H_{D} + \frac{SNR}{2(m_{S} - m_{D})} H_{E}^{\dagger} H_{E} \right| \]

\[ - \frac{SNR}{2(m_{S} - m_{D})} T_{2} T_{2}^{\dagger} H_{E}^{\dagger} H_{E} \] (80)

Then, we write

\[ \log A_{\infty} - \log A \]

\[ = - \log \left| I - \left( \frac{1 + SNR}{2} H_{D} H_{D}^{\dagger} \right)^{-1} \frac{SNR}{2(m_{S} - m_{D})} T_{2} T_{2}^{\dagger} H_{E}^{\dagger} H_{E} \right| \] (82)

\[ = - \log \left| I - \left( \frac{1 + SNR}{2} H_{eq}^{\dagger} H_{eq} \right)^{-1} \frac{SNR}{2(m_{S} - m_{D})} T_{2} T_{2}^{\dagger} H_{E}^{\dagger} H_{E} \right| . \]

where \( H_{eq} = \left[ \frac{H_{D}}{\sqrt{m_{S} - m_{D}}} H_{E} \right] \). From the SVD decomposition of \( H_{D} \), we can easily check that \( T_{2} T_{2}^{\dagger} H_{D} \) \( \left( \frac{SNR}{2} \right)^{-1} H_{D} \).

Indeed,\( H_{eq}^{\dagger} H_{eq} \) which implies \( T_{2} H_{eq}^{\dagger} T_{2} \) and \( T_{2} T_{2}^{\dagger} = H_{eq}^{\dagger} U \Delta^{-2} U^{\dagger} H_{D} = H_{D} \). Then, (83) becomes

\[ \log A_{\infty} - \log A \]

\[ = - \log \left| I - \left( \frac{1}{m_{S} - m_{D}} \right) \left( \frac{1}{SNR/2} \right)^{-1} H_{eq}^{\dagger} H_{eq} \right| \]

\[ = - \log \left| I - \left( \frac{1}{m_{S} - m_{D}} \right) \left( \frac{1}{SNR/2} \right)^{-1} \right| . \]

(84)

\[ \left( \frac{1}{SNR/2} \right)^{-1} H_{eq}^{\dagger} H_{eq} \]

where the last equality is obtained by writing \( H_{eq} = \left[ H_{D} \frac{1}{\sqrt{m_{S} - m_{D}}} H_{E} \right] \left[ I_{m_{D} \times m_{D}} \right] \), and

\[ C = \left[ \frac{1}{m_{D} \times m_{D}} \right] \left( H_{D} H_{D}^{\dagger} \right)^{-1} H_{D} H_{E}^{\dagger} . \]

Using the limit property of a pseudo-inverse [24], we have

\[ \lim_{SNR \to \infty} \left( \frac{1}{SNR/2} \right)^{-1} H_{eq}^{\dagger} H_{eq} \]

\[ \lim_{SNR \to \infty} \log A_{\infty} - \log A \]

\[ = - \log \left| I - \frac{1}{m_{S} - m_{D}} H_{eq}^{\dagger} C \right| . \]

(87)

Therefore,

\[ A \doteq A_{\infty} \doteq \log \left| I_{m_{S}} + \frac{SNR}{2} H_{E} H_{E}^{\dagger} \right| . \]

(88)

Second, we show now that \( B \doteq \left| I_{m_{D}} + \frac{SNR}{2} H_{E} H_{E}^{\dagger} \right| . \)

\[ \log B = \log \left| I_{m_{D}} + \frac{SNR}{2} H_{E} H_{E}^{\dagger} \right| \]

\[ = \log \left| I_{m_{D}} + \frac{SNR}{2} H_{E} H_{E} \right| . \]

(89)

Since \( T \) has orthonormal columns, then \( \text{Tr}(T^{\dagger} T) = \text{rank}(T^{\dagger} T) = m_{S} - m_{D} \), hence
This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TWC.2015.2492963, IEEE Transactions on Wireless Communications

\[ I_{ms} + \frac{1}{2(m_s-m_D)}T^\dagger T \leq \frac{1}{2} I_{ms} \] and

\[ \log B \leq \log \left| I_{ms} + \frac{SNR}{4} H_E H_E^\dagger \right| . \]

Similarly, \( I_{ms} + \frac{1}{2(m_s-m_D)}T^\dagger T \geq I_{ms} \) which implies that

\[ \log B \geq \log \left| I_{ms} + \frac{SNR}{4} H_E H_E^\dagger \right| . \]

In short, we obtain:

\[ \log \left| I_{ms} + \frac{SNR}{2} H_E H_E^\dagger \right| \leq \log B \]

\[ \leq \log \left| I_{ms} + \frac{SNR}{4} H_E H_E^\dagger \right| . \] (91)

which results in

\[ B \geq \left| I_{ms} + SNR H_E H_E^\dagger \right| . \] (92)

Finally, we leverage the results from the secret-key rate outage calculation.

\[ P^{AN}_{out}(SNR) = P \left( A - B < rs \log(SNR) \right) \]

\[ = P \left( \log \left| I_{ms} + SNR H_E^\dagger H_D + SNR H_E^\dagger H_E \right| \right) \]

\[ < rs \log(SNR) \right), \] (93)

From equation (20c), we see that the last expression is exactly the same expression used to calculate the secret-key rate outage probability. Hence, using the result of Lemma 2, we obtain

\[ P^{AN}_{out}(SNR) \geq SNR^{-d_{ms}-m_D}(rs) , \] (95)

which concludes the proof.

REFERENCES


Basel Alomair is an Assistant Professor and Founding Director of the National Center for Cybersecurity Technology (C4C) in King Abdulaziz City for Science and Technology (KACST), an Affiliate Professor and co-director of the Network Security Lab (NSL) at the University of Washington-Seattle, an Affiliate Professor at King Saud University (KSU), and a cryptographic consultant at various companies. He was recognized by the IEEE Technical Committee on Fault-Tolerant Computing (TC-FTC) and the IFIP Working Group on Dependable Computing and Fault Tolerance (WG 10.4) with the 2010 IEEE/IFIP William Carter Award for his significant contributions in the area of dependable computing. His research in information security was recognized with the 2011 Outstanding Research Award from the University of Washington. He was also the recipient of the 2012 Distinguished Dissertation Award from the Center for Information Assurance and Cybersecurity at the University of Washington (UW CIAC). He was awarded the 2015 Early Career Award in Cybersecurity by the NSA/DHS Center of Academic Excellence in Information Assurance Research for his contributions to Modern Cryptographic Systems and Visionary Leadership. He authored/co-authored multiple best paper awards and he is a member of the IEEE.

Mohamed-Slim Alouini (S’94, M’98, SM’03, F09) was born in Tunis, Tunisia. He received the Ph.D. degree in Electrical Engineering from the California Institute of Technology (Caltech), Pasadena, CA, USA, in 1998. He served as a faculty member in the University of Minnesota, Minneapolis, MN, USA, then in the Texas A&M University at Qatar, Education City, Doha, Qatar before joining King Abdullah University of Science and Technology (KAUST), Thuwal, Makkah Province, Saudi Arabia as a Professor of Electrical Engineering in 2009. His current research interests include the modeling, design, and performance analysis of wireless communication systems.