Diversity-Multiplexing Tradeoff for MIMO Wire-tap Channels with CSIT

Melda Yuksel
EEE Department
TOBB University of Economics and Technology
Ankara, Turkey
yuksel@etu.edu.tr

Elza Erkip
ECE Department
Polytechnic Institute of NYU
Brooklyn, NY 11201
elza@poly.edu

***Abstract*—In this paper fading multiple-antenna (MIMO) wire-tap channels are investigated under short term power constraints. The *secret* diversity-multiplexing tradeoff (DMT) is calculated analytically, when the destination and the eavesdropper have receiver side channel state information (CSI) and the source has transmitter side CSI (CSIT). It is shown that the eavesdropper *steals* transmitter antennas and the secret DMT depends on the effective number of antennas left. This is in contrast to the no CSIT case, where the eavesdropper effectively steals both transmit and receive antennas. A *zero-forcing* type scheme is shown to achieve the secret DMT when CSIT is available.**

I. Introduction

Eavesdropping is inevitable in wireless communications as any transmission is broadcast and can be overheard. Eavesdroppers can identify confidential messages such as user IDs, passwords, or credit card numbers. In future wireless applications it is anticipated that communication load is going to increase even more, and sensitive information is going to become even more vulnerable to eavesdropping. Therefore, there is a recent surge of interest in unconditional security techniques; techniques that are secure even if eavesdroppers have infinite computing time and power.

The notion of unconditional security is first discussed by Shannon [1]. Wyner introduced the physically degraded wire-tap channel in [2], established the perfect secrecy rate; i.e. the transmission rate, up to which perfect secrecy is possible, and the tradeoff between the secrecy rate and the communication rate. Later in [3], these results were extended to less noisy and more capable broadcast channels. The secrecy capacity for the Gaussian wire-tap channel was found in [4]. Recently fading wire-tap channels are investigated in [5], [6], for which the ergodic secrecy capacity is calculated when both the transmitter and the receivers have channel state information (CSI). In [5] the ergodic secrecy capacity, when the source node does not have the eavesdropper's CSI, is also evaluated.

In wireless channels, multiple antennas increase robustness against fading, and also transmission rates. Multiple antennas are considered in the context of wire-tap channels in [7], [8]-[12]. In [8] the authors find the secrecy capacity of the Gaussian multiple-input multiple-output (MIMO) wire-tap channel, when the source and the destination have two antennas each and the eavesdropper has only a single antenna. Concurrent work in [9] and [10] establish the secrecy capacity for the fading MIMO wire-tap channel under the full CSI assumption for arbitrary antenna numbers. A closed-form expression for the secrecy capacity is found in [13].

For the wire-tap channel, outage approach are considered in [7], [14] and [15]. Outage probability for a target secrecy rate is also investigated in [6], when the source, the destination and the eavesdropper have CSI, and optimal power allocation policies that minimize the outage probability are calculated. On the other hand, the notion of *secure degrees of freedom* are investigated in [16], [17], [18], [19] and [20].

An important performance measure for MIMO fading channels is the diversity-multiplexing tradeoff (DMT), established in [21]. The DMT is a high SNR analysis and describes the fundamental tradeoff between the diversity gain and the multiplexing gain. The diversity gain is the decay rate of the probability of error, and the multiplexing gain is the rate of increase of the transmission rate in the limit of high SNR. The DMT is strongly related to the probability of outage as probability of error is generally dominated by the outage event at high SNR. The *secret* DMT was defined in [22] and it was found that the eavesdropper "steals" both transmitter and receiver antennas if there is no CSIT. The secret DMT for the relay channel with an eavesdropper was found in [23].

In this paper we investigate the MIMO wire-tap channel DMT when there is full CSIT. We find that the eavesdropper "steals" only transmitter antennas and the number of *effective* antennas left determine the secret DMT. For the full CSIT case considered in this paper, we also suggest a *zero-forcing* type scheme, which achieves the secret DMT upper bounds.

Next, we introduce the system model in Section II. Section III covers the secret DMT when there is CSIT. Section IV presents the zero-forcing scheme, and compares it with the artificial noise method. Section V concludes the paper.

II. System Model and Preliminaries

We consider a MIMO wire-tap channel, in which the source, the destination and the eavesdropper have m, n and k antennas respectively. Both the destination and the eavesdropper have receiver side CSI, and there is full CSIT.

[1]This material is based upon work partially supported by NSF Grant No. 0635177, by the Center for Advanced Technology in Telecommunications (CATT) of Polytechnic Institute of NYU.

For each channel use the channel is represented as follows:

$$\mathbf{Y}_D = \mathbf{H}_D\mathbf{X} + \mathbf{Z}_D \quad (1)$$

$$\mathbf{Y}_E = \mathbf{H}_E\mathbf{X} + \mathbf{Z}_E. \quad (2)$$

In the above equations $\mathbf{X}$ is an $m \times 1$ vector, which denotes the transmitted source signal. $\mathbf{Y}_D$ and $\mathbf{Y}_E$ are $n \times 1$ and $k \times 1$ vectors, and represent the received signals at the destination and the eavesdropper respectively. Similarly, $\mathbf{Z}_D$ and $\mathbf{Z}_E$ are $n \times 1$, and $k \times 1$ vectors that indicate the independent additive noise at the destination and the eavesdropper. Both $\mathbf{Z}_D$ and $\mathbf{Z}_E$ have independent and identically distributed (i.i.d.) complex Gaussian entries with zero mean and unit variance. The matrices $\mathbf{H}_D$ and $\mathbf{H}_E$, consisting of i.i.d. complex Gaussian entries with zero mean and unit variance, are of size $n \times m$, and $k \times m$. They respectively denote the channel gains between the source and the destination and the source and the eavesdropper. As the fading is assumed to be slow, $\mathbf{H}_D$ and $\mathbf{H}_E$ are fixed for the whole duration of the communication.

Under secrecy constraints, the equivocation rate R_e

$$R_e = \lim_{N\to\infty} \frac{1}{N} H(W|Y_E^N) \quad (3)$$

describes the eavesdropper's confusion about the source message W given its observation Y_E^N [2]. The rate-equivocation rate region [2] indicates the transmission rates over the main channel and the level of obscurity at the eavesdropper. An operating point in the rate-equivocation rate region is called *perfectly secure*, if the equivocation rate, R_s is arbitrarily close to the information rate R. Moreover, the perfect secrecy rate

$$R_s = [I(\mathbf{X};\mathbf{Y}_D) - I(\mathbf{X};\mathbf{Y}_E)]^+ \quad (4)$$

is achievable [3] for any input distribution $p(\mathbf{X})$, where x^+ denotes $\max\{0, x\}$. The highest perfectly secure rate is called the secrecy capacity [2].

In this work, we assume perfect secrecy, $R = R_s$, and investigate the high SNR behavior of the secrecy probability of error with a target secrecy rate equal to $R_s^{(T)}(\mathrm{SNR})$. We assume the system is delay-limited and requires constant secrecy rate transmission. There is also short-term average power constraint $m\mathrm{SNR}$ that the transmitter has to satisfy for each codeword transmitted. The *secret* multiplexing gain, r_s, and the *secret* diversity gain, d_s, are defined in [22] as

$$\lim_{\mathrm{SNR}\to\infty} \frac{R_s^{(T)}(\mathrm{SNR})}{\log \mathrm{SNR}} \triangleq r_s, \qquad \lim_{\mathrm{SNR}\to\infty} \frac{\log P_e(\mathrm{SNR})}{\log \mathrm{SNR}} \triangleq -d_s,$$

where $P_e(\mathrm{SNR})$ is the probability of error. In this paper, we establish the tradeoff between secret diversity gain d_s and the secret multiplexing gain r_s, $d_s(r_s)$, when there is both transmitter and receiver CSI.

We assume that transmitter has perfect CSI about the channel between itself and the eavesdropper, as well as its channel to the destination. While it may be possible for the source to obtain eavesdropper CSI if both the destination and the eavesdropper are part of the same network, the full CSIT assumption may be harder to justify if the eavesdropper is merely an illegitimate listener. Nevertheless, this assumption will help us understand the limitations and properties of secret DMT. Note that secret DMT is still a meaningful metric as we consider constant secret rate applications that operate under short-term power constraints, which can suffer from outage despite the available CSIT.

In a system with secrecy constraints, the probability of error is due to two events: Either the destination does not receive the secret message reliably, or perfect secrecy is not achieved [24]. When the channel block length-N is long enough and good codes are used, probability of error is dominated by the corresponding outage events. Then we can write

$$\begin{aligned} P_e(\mathrm{SNR}) &= P(\text{perfect secrecy not achieved or} \\ &\quad \text{main channel decoding error}) \\ &\leq P(\text{perfect secrecy not achieved}) \\ &\quad + P(\text{main channel decoding error}) \\ &\doteq P(\text{perfect secrecy not achieved}) \\ &\quad + P(\text{main channel outage}) \end{aligned} \quad (5)$$

where

$$\begin{aligned} &P(\text{perfect secrecy not achieved}) \\ &\quad = P(R_e < R_s^{(T)}(\mathrm{SNR})) \\ &P(\text{main channel outage}) \\ &\quad = P(I(\mathbf{X};\mathbf{Y}_D) < R^{(T)}(\mathrm{SNR})). \end{aligned}$$

Here R_e is the instantaneous secrecy rate achieved defined in (3), $2^{NR^{(T)}(\mathrm{SNR})}$ denotes the total number of codewords transmitted (possibly including dummy bits) and $I(\mathbf{X};\mathbf{Y}_D)$ is evaluated for the chosen transmission scheme. On the other hand, probability of error is lower bounded by

$$\begin{aligned} P_e(\mathrm{SNR}) &\geq P(\text{perfect secrecy not achieved}) \\ &\overset{(a)}{\geq} P([I(\mathbf{X};\mathbf{Y}_D) - I(\mathbf{X};\mathbf{Y}_E)]^+ < R_s^{(T)}(\mathrm{SNR})) \\ &= P(I(\mathbf{X};\mathbf{Y}_D) - I(\mathbf{X};\mathbf{Y}_E) < R_s^{(T)}(\mathrm{SNR})) \\ &\triangleq P(\text{perfect secrecy rate outage}), \end{aligned} \quad (6)$$

where (a) is because for any input distribution $p(\mathbf{X})$ corresponding to an achievable scheme, $R_s = [I(\mathbf{X};\mathbf{Y}_D) - I(\mathbf{X};\mathbf{Y}_E)]^+$ calculated for this particular $p(\mathbf{X})$ is an upper bound on the equivocation rate.

In the following we will calculate both terms in (5) and (6) to establish upper and lower bounds on probability of error and to establish the secret DMT, under full CSI assumptions. Note that the "perfect secrecy not achieved" event does not always imply the "main channel outage" event. However, we will observe that these two events are the same for the achievability scheme in Section III.

In the rest of the paper, we will compute the secret DMT results with full CSIT and compare them to the DMT without secrecy constraints [21] and to the secret DMT without CSIT [22]. Note that when there is no secrecy constraint, the diversity-multiplexing tradeoff $d(r)$ is the piecewise linear function joining the points $d_{m,n}(l) = (m-l)(n-l)$,

$l = 0, 1, ..., \min\{m, n\}$. The secret DMT without CSIT is given as the piecewise linear function joining the points $d_s(l) = (m-k-l)(n-k-l)$ if $k < \min\{m, n\}$, and $l = 0, 1, ..., \min\{m, n\} - k$. If $k \geq \min\{m, n\}$, then the secret DMT without CSIT is the single point $(0, 0)$.

Finally, we assume a single transmission block of N channel uses under short-term power constraint. This is unlike the scenario in [15]. In [15] there are many blocks to communicate and there is long-term power constraint. The first communication block is merely used to generate a secret key, and in the next block this key is used to enhance secrecy, while another key is generated to be used in the following block. In other words, the key generation process [15] is delay-insensitive, and keys generated this way are used to protect the delay-sensitive secret messages. In our system, communication session lasts a single code block, during which secrecy has to be maintained. The transmitter and the receiver have to start secure communication immediately at the beginning of the transmission block and there is not enough time to generate a secret key.

III. Channel State Information at the Source

In this section we establish the secret DMT with CSIT and in the next section we investigate different schemes that achieve the best secret DMT with CSIT.

The secrecy capacity for the non-fading MIMO wire-tap channel with channel knowledge both at the receivers (the destination and the eavesdropper) and the transmitter (the source) is found in [9], [10] as

$$C_s = \max_{\substack{Q \succeq 0, \\ \mathrm{Tr}(Q) \leq m\mathrm{SNR}}} \log \frac{\left|\mathbf{I}_n + \mathbf{H}_D Q \mathbf{H}_D^\dagger\right|}{\left|\mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^\dagger\right|}, \quad (7)$$

where $\mathbf{I}_n$ is an identity matrix of size n, Q is the input covariance matrix at the transmitter, and $\mathrm{Tr}(.)$ denotes the trace operation.

To establish the secret DMT with CSIT, we first need the following lemma.

Lemma 1: If $k < \min\{m, n\}$, then $p = \dim\{\mathrm{Null}(\mathbf{H}_\mathrm{D})^\perp \cap \mathrm{Null}(\mathbf{H}_\mathrm{E})\} > 0$, where $\mathrm{Null}(\mathbf{H}_D)^\perp$ is the orthogonal complement of the null space of $\mathbf{H}_D$ and $\mathrm{Null}(\mathbf{H}_E)$ is the null space of $\mathbf{H}_E$. If $n \leq k < m$ or $k \geq m$, then $p = 0$.

Proof: The subspaces $\mathrm{Null}(\mathbf{H}_E)$ and $\mathrm{Null}(\mathbf{H}_D)^\perp$ are defined in the vector space $\Re^m$. If $k < \min\{m, n\}$, then $\mathrm{Null}(\mathbf{H}_E)$ and $\mathrm{Null}(\mathbf{H}_D)^\perp$ respectively have dimensions $m-k$ and $q = \min\{m, n\}$, and have the basis sets $\mathcal{U} = \{\mathbf{u}_1, \mathbf{u}_2, ..., \mathbf{u}_{m-k}\}$ and $\mathcal{W} = \{\mathbf{w}_1, \mathbf{w}_2, ..., \mathbf{w}_q\}$. In other words, the sets $\mathcal{U}$ and $\mathcal{W}$ are both linearly independent sets. However, as $m-k+q > m$, $\mathcal{U} \cup \mathcal{W}$ is linearly dependent. The intersection of the hyper-planes $\mathcal{U}$ span and $\mathcal{W}$ span, includes at least one non-zero vector. Thus $p > 0$.

If $n \leq k < m$, then the basis sets $\mathcal{U}$ and $\mathcal{W}$ are same as above with $q = n$. However, in this case $\mathcal{U} \cup \mathcal{W}$ is a linearly independent set, as $m - k + q = m - k + n \leq m$. The intersection of the hyper-planes $\mathcal{U}$ span and $\mathcal{W}$ span only include $\{\mathbf{0}\}$ and thus $p = 0$.

If $k \geq m$, then $\mathrm{Null}(\mathbf{H}_E)$ consists of only $\{\mathbf{0}\}$. Then $\mathrm{Null}(\mathbf{H}_D)^\perp \cap \mathrm{Null}(\mathbf{H}_E) = \{\mathbf{0}\}$, and thus $p = 0$. ∎

Theorem 1: For the MIMO wire-tap channel defined in (1) and (2), with full CSI at all the terminals, if $k < m$, the secret diversity-multiplexing tradeoff, $\hat{d}_s(r_s)$ is a piecewise linear function joining the points $(l, \hat{d}_s(l))$, where $l = 0, 1, ..., m-k$ and

$$\hat{d}_s(l) = (m-k-l)(n-l).$$

If $k \geq m$, then the secret diversity-multiplexing tradeoff reduces to the single point $(0, 0)$.

Proof: When the secrecy capacity is expressed as in (7), it is hard to calculate the secret DMT. We make use of the high SNR secrecy capacity approximations provided in [9] to find the secret DMT. We investigate the three cases $k < \min\{m, n\}$, $n \leq k < m$, and $k \geq m$ separately.

For the first case $k < \min\{m, n\}$, $p > 0$ by Lemma 1 and $\mathbf{H}_E$ is not full column rank; i.e. $k < m$, then the secrecy capacity at high SNR is given by [9]

$$\tilde{C}_s(\mathrm{SNR}) = \sum_{j:\sigma_j \geq 1} \log \sigma_j^2 + C_\perp\left(m\mathrm{SNR}/p\right) + o(1), \quad (8)$$

where σ_j, $j = 1, ..., \min\{m, n\} - p$, are the generalized singular values of matrices $\mathbf{H}_D$ and $\mathbf{H}_E$,

$$C_\perp(\mathrm{SNR}) = \log\left|\mathbf{I}_n + \mathrm{SNR}\mathbf{H}_D\mathbf{H}_E^\perp\mathbf{H}_D^\dagger\right|, \quad (9)$$

$\mathbf{H}_E^\perp \in \mathbb{C}^{m\times m}$ is the projection matrix onto $\mathrm{Null}(\mathbf{H}_E)$, and $o(1) \to 0$ when $\mathrm{SNR} \to \infty$. To find the secret DMT we investigate the perfect secrecy rate outage probability

$$\begin{aligned} & P(\text{perfect secrecy rate outage}) && (10)\\ &= P\left(\tilde{C}_s(\mathrm{SNR}) < r_s \log \mathrm{SNR}\right) && (11)\\ &\doteq P\left(C_\perp\left(m\mathrm{SNR}/p\right) < r_s \log \mathrm{SNR}\right) && (12)\\ &= \int ... \int P\left(C_\perp(m\mathrm{SNR}/p) < r_s \log \mathrm{SNR}\right. \\ &\qquad \left. \mid \mathbf{H}_E^{(11)} = H_E^{(11)}, ..., \mathbf{H}_E^{(km)} = H_E^{(km)}\right) \\ &\qquad \cdot \prod_{i=1}^{k}\prod_{j=1}^{m} f_{\mathbf{H}_E^{(ij)}}(H_E^{(ij)}) dH_E^{(ij)} && (13) \end{aligned}$$

For a fixed $\mathbf{H}_E = \mathrm{H}_E$, i.e. when all $\mathbf{H}_E^{(ij)} = H_E^{(ij)}$, $i = 1, ..., k, j = 1, ..., m$, the projection matrix $\mathrm{H}_E^\perp$ can be written as $\mathrm{H}_E^\perp = \mathrm{A}\mathrm{A}^\dagger$. The matrix A is of size $m \times (m-k)$. We can write $\mathrm{A} = [a_1, ..., a_{m-k}]$, where the length-$m$ column vectors a_j form an orthonormal basis for $\mathrm{Null}(\mathbf{H}_E)$. Let $\mathbf{H}_D = [\mathbf{r}_1^\dagger, ..., \mathbf{r}_n^\dagger]^\dagger$ be written in terms of length-m row vectors $\mathbf{r}_i$, $i = 1, ..., n$. Then each entry of $(\mathbf{H}_D\mathrm{A})^{(ij)} = \langle \mathbf{r}_i, a_j \rangle$, $i = 1, ..., n$, $j = 1, ..., (m-k)$. The mean value of each entry is equal to $E\{\langle \mathbf{r}_i, a_j \rangle\} = 0$. We observe that the covariance $E\{\langle a_j^\dagger, \mathbf{r}_i^\dagger \rangle \langle \mathbf{r}_s, a_t \rangle\} = a_j^\dagger E\{\mathbf{r}_i^\dagger \mathbf{r}_s\} a_t$. The value $E\{\mathbf{r}_i^\dagger \mathbf{r}_s\} = 1$, if $i = s$, and it is zero if $i \neq s$. In addition to these, as the vectors are orthonormal, $a_j^\dagger E\{\mathbf{r}_i^\dagger \mathbf{r}_s\} a_t = 0$, if $j \neq t$

for any i and s. Therefore, if $i = s$ and $j = t$, then $E\{\langle a_j^\dagger, \mathbf{r}_i^\dagger\rangle\langle \mathbf{r}_s, a_t\rangle\} = 1$; otherwise, it is equal to zero. Thus, $\mathbf{H}_D\mathrm{A}$ is a matrix, whose entries are i.i.d. Gaussian with zero mean and unit variance. Then we can write the probability in (13) as

$$\begin{aligned} & P\left(C_\perp(m\mathrm{SNR}/p) < r_s \log \mathrm{SNR}\right. \\ & \qquad \left. |\mathbf{H}_E^{(11)} = H_E^{(11)}, ..., \mathbf{H}_E^{(km)} = H_E^{(km)}\right) \\ &= P\left(\log\left|\mathbf{I}_n + \frac{m\mathrm{SNR}}{p}\mathbf{H}_D\mathrm{A}\mathrm{A}^\dagger\mathbf{H}_D^\dagger\right| < r_s \log \mathrm{SNR}\right) \\ &\doteq \mathrm{SNR}^{-d_{(m-k),n}(r_s)}. \end{aligned}$$

In other words, this system is equivalent to an $(m-k)\times n$ MIMO with a well known DMT $d_{(m-k),n}(r_s)$ [21]. Substituting this value in (13), we observe that

$$\begin{aligned} & P(\text{perfect secrecy rate outage}) \\ &\doteq \int \cdots \int \frac{1}{\mathrm{SNR}^{d_{(m-k),n}(r_s)}} \prod_{i=1}^{k}\prod_{j=1}^{m} f_{\mathbf{H}_E^{(ij)}}(H_E^{(ij)}) dH_E^{(ij)} \\ &= \mathrm{SNR}^{-d_{(m-k),n}(r_s)}. \end{aligned}$$

or

$$d_s(r_s) \le d_{(m-k),n}(r_s).$$

To attain perfect secrecy the source uses i.i.d. complex Gaussian codewords with covariance matrix Q and transmits at rate $R^{(T)} = R_s^{(T)} + \log\left|\mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^\dagger\right|$ bits/channel use, where Q is the covariance matrix that attains the maximum in (7). Here the target secret communication rate is $R_s^{(T)}$ bits/channel use. The number of dummy codewords used for each secret message is variable and equal to $2^{N\log\left|\mathbf{I}_k+\mathbf{H}_E Q\mathbf{H}_E^\dagger\right|}$. Then the main channel outage probability is equal to

$$\begin{aligned} & P(\text{main channel outage}) \\ &= P\left(\log\left|\mathbf{I}_n + \mathbf{H}_D Q \mathbf{H}_D^\dagger\right| < R^{(T)}(\mathrm{SNR})\right) \\ &= P\left(\log \frac{\left|\mathbf{I}_n + \mathbf{H}_D Q \mathbf{H}_D^\dagger\right|}{\left|\mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^\dagger\right|} < r_s \log \mathrm{SNR}\right) \\ &= P(\text{perfect secrecy rate outage}) \\ &\doteq \mathrm{SNR}^{-d_{m-k,n}(r_s)}. \end{aligned}$$

On the other hand the probability of perfect secrecy not achieved is

$$\begin{aligned} & P(\text{perfect secrecy not achieved}) \\ &\doteq P(R^{(T)}(\mathrm{SNR}) - R_s^{(T)}(\mathrm{SNR}) < I(\mathbf{X}; \mathbf{Y}_E^N)) \\ &= P(\log\left|\mathbf{I}_k + \mathbf{H}_E Q \mathbf{H}_E^\dagger\right| < I(\mathbf{X}; \mathbf{Y}_E^N)) \\ &\doteq 0. \end{aligned}$$

Combining the upper and lower bounds (5) and (6) we conclude that the secret DMT is equal to $d_{m-k,n}(r_s)$ if $k < m$.

For the second case $n \le k < m$, $p = 0$ by Lemma 1 and the high SNR secrecy capacity expression of [9] cannot be used directly. However, the converse and achievability in [9] can be extended to cover for $p = 0$, by deleting certain rows and columns in the generalized singular value decomposition. Then the same secrecy capacity expression as in (8) holds with p replaced by $p' = \min\{m-k, n\}$. We can follow the same steps in the previous case to calculate P(perfect secrecy outage), and P(main channel outage) and find the secret DMT to be $d_{(m-k),n}(r_s)$ for $n \le k < m$.

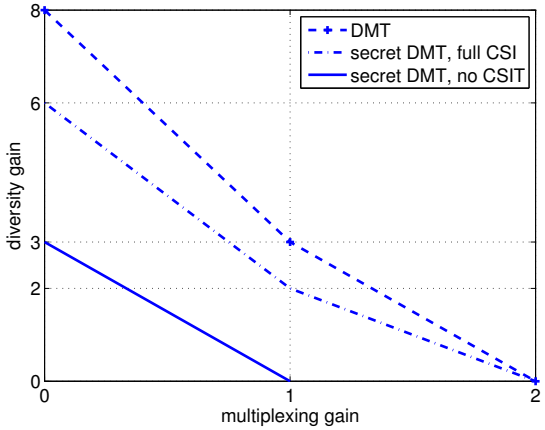

Fig. 1. DMT and secret DMT for $m = 4$, $n = 2$, $k = 1$.

Finally for the last case, $k \ge m$, the secrecy capacity at high SNR is given by [9]

$$\lim_{\mathrm{SNR}\to\infty} \tilde{C}_s(\mathrm{SNR}) = \sum_{j:\sigma_j \ge 1} \log \sigma_j^2. \tag{14}$$

As the capacity expression does not grow with increasing SNR, it is easy to see that the secret DMT is a single point $(0, 0)$. ■

Remark 1: In the proof of Theorem 1, as the number of dummy codewords used for each secret message is variable and equal to $2^{N\log\left|\mathbf{I}_k+\mathbf{H}_E Q\mathbf{H}_E^\dagger\right|}$, no information is leaked to the eavesdropper.

Remark 2: When there is no CSIT, the secret DMT is that of an $(m-k)\times(n-k)$ MIMO if $k < \min\{m, n\}$, and the single point $(0, 0)$ if $k \ge \min\{m, n\}$. In other words, the eavesdropper *steals* both transmitter and receiver antennas. However, when there is CSIT, the eavesdropper *steals* transmitter antennas only. The secret DMT depends on CSIT unlike the DMT without secrecy constraints.

In Fig. 1 secret DMT with CSIT is shown for $m = 4$, $n = 2$ and $k = 1$ in comparison to the secret DMT without CSIT and the DMT without secrecy constraints. The DMT without secrecy constraints, the secret DMT with CSIT and the secret DMT without CSIT are shown to be respectively equal to $d_{4,2}(r)$, $d_{3,2}(r_s)$, and $d_{3,1}(r_s)$. In this example secrecy constraints impose both multiplexing gain and diversity gain losses when there is no CSIT, and only diversity gain losses when there is CSIT.

In Fig. 2 we compare the secret DMT for the wire-tap channel with a 2-antenna source, a 2-antenna destination, and a single antenna eavesdropper for no transmitter CSI and full CSI cases, as well as the DMT without secrecy constraints.

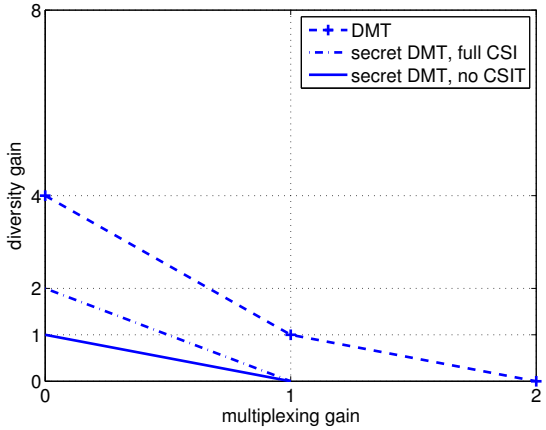

Fig. 2. DMT and secret DMT for $m = 2$, $n = 2$, $k = 1$.

The DMT without secrecy constraints is known to be $d_{2,2}(r)$, and the secret DMT with no transmitter CSI and full CSI are equal to $1 - r_s$ and $2(1 - r_s)$ respectively. For this example maximum secret multiplexing gain is 1 for both with and without CSIT cases.

IV. Alternative Achievability Schemes

In this section we propose a new secret DMT optimal scheme for the full CSIT case as an alternative to the strategy studied in Theorem 1, and compare it to the artificial noise scheme of [25].

A. Zero-forcing

We consider a simple *zero-forcing* method that achieves the full CSIT secret DMT. As $k \geq m$ results in a trivial secret DMT, we assume $k < m$. In the zero-forcing protocol we transmit the secret information in $\mathbf{U}$, which is a length-$(m-k)$ column vector, and send $\mathbf{X} = \mathbf{AU}$ at the transmitter, where $\mathbf{H}_E^{\perp} = \mathbf{AA}^{\dagger}$. Then the received signals at the destination and the eavesdropper respectively become

$$\begin{aligned} \mathbf{Y}_D &= \mathbf{H}_D\mathbf{AU} + \mathbf{Z}_D, \\ \mathbf{Y}_E &= \mathbf{H}_E\mathbf{AU} + \mathbf{Z}_E \;=\; \mathbf{Z}_E. \end{aligned}$$

The destination observes an equivalent channel of $\mathbf{H}_D\mathbf{A}$, whereas the eavesdropper only observes noise because the secret message is transmitted in its null space. As the receiver knows the transmit strategy, it is also informed about $\mathbf{A}$ and thus about the equivalent channel. Then for every realization of $\mathbf{A}$, the equivalent channel gain matrix still has i.i.d. complex Gaussian entries with zero mean and unit variance. Assuming the covariance matrix of $\mathbf{U}$ is $m\mathrm{SNR}\mathbf{I}_{m-k}/(m-k)$, the achievable perfect secrecy rate (7) is

$$I(\mathbf{X};\mathbf{Y}_D) = I(\mathbf{U};\mathbf{Y}_D) = \log\left|\mathbf{I}_n + \mathbf{H}_D\mathbf{H}_E^{\perp}\mathbf{H}_D^{\dagger}\frac{m}{m-k}\mathrm{SNR}\right|$$

as $I(\mathbf{X};\mathbf{Y}_E) = 0$. For this equivalent channel the DMT can easily be shown to be $d_{m-k,n}(r_s)$ as in (10)-(13). This result extends the results in [19] and [20], which prove that the zero-forcing method is optimal in terms of secure degrees of freedom.

Note that for MIMO channels the source node can do beamforming in the direction of the destination, if CSI is available at the transmitter. Whether a secrecy constraint exists or not, beamforming in the direction of the destination only adds coding gain to the achievable mutual information $I(\mathbf{X};\mathbf{Y}_D)$ or $\log\left|\mathbf{I}_n + \mathbf{H}_D Q\mathbf{H}_D^{\dagger}\right|$ term in (7) and does not change the DMT [21] or the secret DMT. However, when there are secrecy constraints, the transmitter CSI can be used to control the *beam direction* of the message. With this information, when the message is transmitted in the null space of the eavesdropper, the secret DMT changes significantly as illustrated in the zero-forcing protocol. In the zero-forcing scheme, as the secret messages are transmitted in the null space of $\mathbf{H}_E$, under any circumstances, there is no information leakage to the eavesdropper.

B. Artificial Noise

In [25] the authors suggest an artificial noise scheme to increase achievable secrecy rates. In the artificial noise scheme the source node sends its messages in the range space of $\mathbf{H}_D$ and sends extra noise in $\mathbf{H}_D$'s null space. Let $\mathbf{T}$ be an $m \times (m-n)$ matrix, whose columns form an orthonormal basis for $\mathrm{Null}(\mathbf{H}_D)$, $\mathbf{V}$ is a length-$(m-n)$ column vector with i.i.d. complex Gaussian entries with zero mean, and $\mathbf{S}$ be a zero mean, length-m column vector that carries source messages. Then source sends

$$\mathbf{X} = \mathbf{S} + \mathbf{TV}.$$

As $\mathbf{V}$ is received in the null space of $\mathbf{H}_D$, the destination is not affected from this extra noise $\mathbf{V}$, but the eavesdropper is. Then the received signals at the destination and the eavesdropper are

$$\begin{aligned} \mathbf{Y}_D &= \mathbf{H}_D\mathbf{S} + \mathbf{Z}_D \\ \mathbf{Y}_E &= \mathbf{H}_E\mathbf{S} + \mathbf{H}_E\mathbf{TV} + \mathbf{Z}_E. \end{aligned}$$

We assume the vectors $\mathbf{S}$ and $\mathbf{V}$ are independent and respectively have the covariance matrices $\mathcal{E}\{\mathbf{SS}^{\dagger}\} = \mathrm{SNR}\mathbf{I}_m/2$ and $\mathcal{E}\{\mathbf{VV}^{\dagger}\} = m\mathrm{SNR}\mathbf{I}_{m-n}/[2(m-n)]$. Note that this choice satisfies the total power constraint as:

$$\begin{aligned} \mathbf{Tr}(\mathcal{E}\{\mathbf{X}^{\dagger}\mathbf{X}\}) &= \mathbf{Tr}(\mathcal{E}\{\mathbf{S}^{\dagger}\mathbf{S}\}) + \mathbf{Tr}(\mathcal{E}\{\mathbf{V}^{\dagger}\mathbf{T}^{\dagger}\mathbf{TV}\}) \\ &= \mathbf{Tr}(\mathcal{E}\{\mathbf{S}^{\dagger}\mathbf{S}\}) + \mathbf{Tr}(\mathcal{E}\{\mathbf{V}^{\dagger}\mathbf{V}\}) \\ &= \mathbf{Tr}(\mathcal{E}\{\mathbf{SS}^{\dagger}\}) + \mathbf{Tr}(\mathcal{E}\{\mathbf{VV}^{\dagger}\}) \\ &= m\mathrm{SNR}/2 + m\mathrm{SNR}/2. \end{aligned}$$

Then the achievable perfect secrecy (4) becomes equal to

$$R_s = \log\left|\mathbf{I}_n + \frac{\mathrm{SNR}}{2}\mathbf{H}_D\mathbf{H}_D^{\dagger}\right| - \log\frac{\left|\mathbf{K} + \frac{\mathrm{SNR}}{2}\mathbf{H}_E\mathbf{H}_E^{\dagger}\right|}{|\mathbf{K}|},$$

where $\mathbf{K} = \mathbf{I}_k + \frac{\mathrm{SNR}}{2(m-n)}\mathbf{H}_E\mathbf{TT}^{\dagger}\mathbf{H}_E^{\dagger}$.

Simulations suggest that the artificial noise scheme also achieves the secret DMT $d_{(m-k),n}(r_s)$. A comparison between zero-forcing and artificial noise protocols is shown in Fig. 3 when the source has 2 antennas and the destination and the eavesdropper respectively have a single antenna each. The

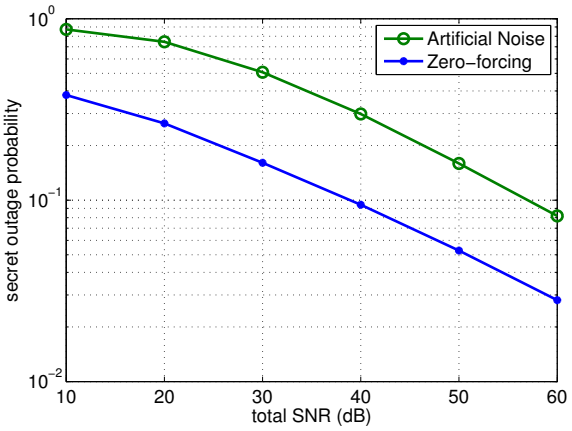

Fig. 3. $m = 2$, $n = 1$, $k = 1$, $r_s = 0.75$.

figure confirms that both schemes achieve a secret diversity 0.25, when the secret multiplexing gain is 0.75.

As a final note, the artificial noise scheme only necessitates the eavesdropper's instantaneous mutual information, $I(\mathbf{X}; \mathbf{Y}_E)$, to determine the codebook structure; i.e. the sizes of the secret message set and the dummy codeword set. However, it does not necessitate the instantaneous channel gain matrix, $\mathbf{H}_E$. To do zero-forcing the instantaneous channel gain matrix is required but its outage probability performance is superior to artificial noise. In zero-forcing the source concentrates its power in the null space of $\mathbf{H}_E$ and it is guaranteed that the eavesdropper does not get any information. Thus, an advantage of zero-forcing is that the source does not have to employ a secret codebook and can continue to use codes designed for reliable communication.

V. Conclusion

In this paper we study the MIMO wire-tap channel when there are stringent delay constraints and short-term power constraint. The secret DMT is equivalent to the DMT of an $(m-k) \times n$ MIMO if $k < m$; otherwise no tradeoff exists between secret multiplexing and secret diversity. This is in contrast to the secret DMT without CSIT, where the secret DMT is equivalent to that of an $(m-k) \times (n-k)$ MIMO if $k < \min\{m, n\}$. We also suggest a zero-forcing scheme, which achieves the secret DMT bound when CSIT is available, and compare it to the artificial noise scheme.

In this paper we assumed the source knows both the main channel CSI and the eavesdropper channel CSI to find the fundamental limits. Investigating the secret DMT when there is only main channel CSI remains to be an interesting open problem. Other possible future directions include finding the secret DMT for imperfect or partial CSI and finding an analytical expression for the artificial noise DMT.

References

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, p. 1355, October 1975.

[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, p. 339, May 1978.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, p. 451, July 1978.

[5] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy of capacity of fading channels," *IEEE Transactions on Information Theory*, vol. 54, no. 10, p. 4687, October 2008.

[6] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," *IEEE Transactions on Information Theory, Special Issue on Information Theoretic Security*, vol. 54, p. 2470, June 2008.

[7] P. Parada and R. Blahut, "Secrecy capacity of SIMO and slow fading channels," in *Proceedings of IEEE International Symposium on Information Theory*, 2005.

[8] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," September 2007, iEEE Transactions on Information Theory, to appear. [Online]. Available: http://arxiv.org/abs/0709.3541

[9] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas: The MIMOME wiretap channel," August 2008, submitted to IEEE Transactions on Information Theory. [Online]. Available: http://allegro.mit.edu/pubs/posted/journal/2008-khisti-wornell-it.pdf

[10] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel." [Online]. Available: http://arxiv.org/abs/0710.1920

[11] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proceedings of 41st Conference of Information Sciences and Systems*, Baltimore, MD, March 2007.

[12] R. Liu and H. V. Poor, "Multiple antenna secure broadcast over wireless networks," in *Proceedings of the First International Workshop on Information Theory for Sensor Networks*, June 18 - 20 2007.

[13] R. Bustin, R. Liu, H. V. Poor, and S. S. (Shitz), "An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel," 2009, to appear in EURASIP Journal on Wireless Communications and Networking.

[14] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proceedings of IEEE International Symposium on Information Theory*, 2006.

[15] K. Khalil, M. Youssef, O. O. Koyluoglu, and H. E. Gamal, "On the delay limited secrecy capacity of fading channels," in *Proceedings of IEEE International Symposium on Information Theory*, 2009.

[16] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wire-tap channels," December 2008, submitted to the EURASIP Journal on Wireless Communications and Networking, Special Issue on Wireless Physical Layer Security.

[17] O. O. Koyluoglu, H. E. Gamal, L. Lai, and H. V. Poor, "Interference alignment for secrecy," October 2008, submitted to IEEE Transactions on Information Theory. [Online]. Available: http://arxiv.org/abs/0810.1187

[18] T. Gou and S. A. Jafar, "On the secure degrees of freedom of wireless x networks," in *Proceedings of 46th Annual Allerton Conference on Communication, Control, and Computing*, 2008.

[19] M. Kobayashi, M. Debbah, and S. S. (Shitz), "Secured communication over frequency-selective fading channels: A practical vandermonde precoding," *EURASIP Journal on Wireless Communications and Networking*, 2009.

[20] M. Kobayashi, Y. Liang, S. S. (Shitz), and M. Debbah, "On the compound MIMO broadcast channels with confidential messages," in *Proceedings of IEEE International Symposium on Information Theory*, 2009.

[21] L. Zheng and D. N. C. Tse, "Diversity and multiplexing: A fundamental tradeoff in multiple-antenna channels," *IEEE Transactions on Information Theory*, vol. 49, p. 1073, May 2003.

[22] M. Yuksel and E. Erkip, "Diversity-multiplexing tradeoff for the multiple-antenna wire-tap channel," in *Proceedings of 42nd Conference of Information Sciences and Systems*, March 2008.

[23] K. T. Gowda, T. Q. S. Quek, and H. Shin, "Secure diversity-multiplexing tradeoffs in MIMO relay channels," in *Proceedings of IEEE International Symposium on Information Theory*, 2009.

[24] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. W. McLaughlin, and J. Merolla, "Applications of LDPC codes to the wiretap channel," *IEEE Transactions on Information Theory*, vol. 53, no. 8, pp. 2933–2945, August 2007.

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