Diversity-Multiplexing Tradeoff for the Multiple-Antenna Wire-tap Channel

Melda Yuksel
EEE Department
TOBB-ETU
Ankara, Turkey
yuksel@etu.edu.tr

Elza Erkip
ECE Department
Polytechnic University
Brooklyn, NY 11201
elza@poly.edu

***Abstract*— In this paper the fading multiple antenna (MIMO) wire-tap channel is investigated. The *secret* diversity gain and the *secret* multiplexing gain are defined. Using these definitions, the *secret* diversity-multiplexing tradeoff (DMT) is calculated analytically when the source node does not have transmitter side channel state information (CSI). It is shown that the wire-tapper *steals* degrees of freedom from the source-destination channel, and the secret DMT depends on the remaining degrees of freedom. When CSI is available at the source, unlike the case when there are no security constraints, transmitter CSI changes the secret DMT significantly.**

I. Introduction

The broadcast nature of the wireless communication channel makes it highly vulnerable to security threats. All wireless transmissions can be overheard by passive listeners, the wire-tappers or eavesdroppers, who possibly can recover the information. The emergence of wireless networking has thus recently revived the interest in the fundamental limits of secure communication or information-theoretic security.

One of the building blocks of information-theoretic security is the wire-tap channel. The physically degraded wire-tap channel was introduced in [1] and the fundamental coding structure to obtain perfect secrecy was established. Later in [2], these results were extended to less noisy and more capable broadcast channels. The secrecy capacity for the Gaussian wire-tap channel was found in [3]. Recently fading wire-tap channels are investigated in [4], [5], for which the ergodic secrecy capacity is calculated when both the transmitter and the receivers have channel state information (CSI). In [4] the ergodic secrecy capacity, when the source node does not have the wire-tapper'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 [6],[7]-[11]. In [7] 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 wire-tapper has only a single antenna. Concurrent work in [8] and [9] establish the secrecy capacity for the fading MIMO wire-tap channel under the full CSI assumption for arbitrary antenna numbers.

Although the ergodic behavior of fading channels is very important, when there are stringent delay constraints, ergodic capacity is not realizable. In this case, the outage formulation proves to be useful. For the wire-tap channel, outage approach was first considered in [6] and [12]. Outage probability for a target secrecy rate is also investigated in [5], when the source, the destination and the wire-tapper have CSI, and optimal power allocation policies that minimize the outage probability are calculated.

An important performance measure for MIMO fading channels that simultaneously considers probability of error and data rates is the diversity-multiplexing tradeoff (DMT), established in [13]. 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.

In this paper we investigate the multiple-antenna wire-tap channel from the DMT perspective. We define the *secret* multiplexing gain, the *secret* diversity gain and the *secret* DMT. We argue that the wire-tapper can be thought of as "stealing" degrees of freedom from the

source-destination channel, and the *secret* DMT depends on the remaining degrees of freedom. This behavior is also observed in [14] for compound channels only for the maximum multiplexing gain point. Our work can be thought of as a generalization of [14], capturing the behavior for all diversity gains. We also argue that the secret DMT depends on the available transmitter CSI. This is unlike the regular point-to-point DMT without security constraints, which is not affected from the transmitter CSI for constant-rate transmission.

Next, we introduce the system model in Section II and then state our main theorem in Section III. We investigate the case when the source has CSI in Section IV. Then we conclude in Section V.

II. System Model

We consider a multiple-antenna wire-tap channel, in which the source, the destination and the wire-tapper have m, n and k antennas respectively. Both the destination and the wire-tapper have CSI about their incoming channels, but the source node does not have any transmit CSI. We will consider the case when the source has transmitter CSI in Section IV. For both cases, we assume the system is delay-limited and constant-rate transmission is required.

The channel is represented as follows:

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

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

In the above equations $\mathbf{X}$ is an $m \times 1$ vector, which denotes the transmitted source signal. $\mathbf{Y}_D$ and $\mathbf{Y}_T$ are $n \times 1$ and $k \times 1$ vectors, and represent the received signals at the destination and the wire-tapper respectively. Similarly, $\mathbf{Z}_D$ and $\mathbf{Z}_T$ are $n \times 1$, and $k \times 1$ vectors that indicate the independent additive noise at the destination and the wire-tapper. Both $\mathbf{Z}_D$ and $\mathbf{Z}_T$ have independent and identically distributed (i.i.d.) complex Gaussian entries with zero mean and variance 1. The matrices $\mathbf{H}_{SD}$ and $\mathbf{H}_{ST}$, with 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 wire-tapper. In addition to these, the source node has an average power constraint $m\mathrm{SNR}$.

The system performance measure for the wire-tap channel is the rate-equivocation rate region [1], which indicates the tradeoff between transmission rates over the main channel and the level of obscurity at the wire-tapper. An operating point in the rate-equivocation rate region is called *perfectly secure*, if the equivocation rate is arbitrarily close to the information rate. The highest perfectly secure rate is called the secrecy capacity [1].

In this work, we investigate the high SNR behavior of a delay-limited system with a target secrecy rate equal to $R_s^{(T)}(\mathrm{SNR})$. We define the *secret* multiplexing gain as

$$\lim_{\mathrm{SNR}\to\infty} \frac{R_s^{(T)}(\mathrm{SNR})}{\log \mathrm{SNR}} = r_s.$$

The secret multiplexing gain r_s shows how fast the target secrecy rate scales with increasing SNR. The *secret* diversity gain, d_s, is equal to

$$\lim_{\mathrm{SNR}\to\infty} \frac{\log P_e(\mathrm{SNR})}{\log \mathrm{SNR}} = -d_s,$$

where $P_e(\mathrm{SNR})$ denotes the probability of error. 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 [15]. When the channel block length is long enough, the former event is dominated by the main channel outage event. Moreover, it is easy to show that among the two events secrecy rate outage; i.e. the event that perfect secrecy is not achieved, dominates the probability of error. Thus, in the rest of the paper, we will focus on this secrecy outage event only. Finally, the *secret* DMT, $d_s(r_s)$, shows the relation between the secret multiplexing and diversity gains.

In [8], [9], the authors prove that for the fading MIMO wire-tap channel, when all nodes in the system have CSI, Gaussian codebooks are optimum. Therefore, we also assume Gaussian codebooks. However, when CSI is not available at the source, to the best of our knowledge the best input covariance matrix Q is not known. We conjecture that sending independent signals at equal power at each antenna is optimal at high SNR, as all the entries of $\mathbf{H}_{SD}$ and $\mathbf{H}_{ST}$ respectively are identically distributed and the source node does not have CSI. Under these assumptions; i.e. $Q = \mathrm{SNR}\mathbf{I}_m$, we can write the achievable perfect secrecy rate as

$$R_s = \left[\log \frac{\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR})}{\prod_{i=1}^{k}(1+\mu_i \mathrm{SNR})}\right]^+, \quad (3)$$

where $L = \min\{m,n\}$, $0 \le \lambda_1 \le ... \le \lambda_L$ are the ordered eigenvalues of the matrix $\mathbf{H}_{SD}\mathbf{H}_{SD}^{\dagger}$, and $0 \le \mu_1 \le ... \le \mu_k$ are the ordered eigenvalues of the matrix $\mathbf{H}_{ST}\mathbf{H}_{ST}^{\dagger}$. Here, $\dagger$ denotes the conjugate transpose, and $x^+ = \max\{0, x\}$.

III. SECRET DMT

In this section, we state our main theorem.

Theorem 1: For the multiple-antenna wire-tap channel defined in (1) and (2), with full CSI at the destination and the wire-tapper and no CSI at the source, if $k < \min\{m,n\}$, the secret diversity-multiplexing tradeoff is a piecewise linear function joining the points $(l, d_s(l))$, where $l = 0, 1, ..., \min\{m,n\} - k$ and

$$d_s(l) = (m-k-l)(n-k-l).$$

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

Proof: We first prove the secret DMT for $k < \min\{m,n\}$. We will discuss the case $k \geq \min\{m,n\}$ at the end of the proof. To find the secret DMT we find a lower bound and an upper bound on the probability of the secrecy rate outage; $P(\text{outage}) = P(R_s < R_s^{(T)})$, where $R_s^{(T)} = r_s \log \text{SNR}$. Then we show that both of these bounds have the same DMT.

Outage Lower Bound: Define $\mathcal{E}_l = \{\mu_i > a, i = 1, ..., k\}$, where a is a positive real constant and $\mathcal{E}_l^c$ denotes the complement of $\mathcal{E}_l$. Without loss of generality $a > 1$. Then we can write probability of secrecy rate outage as

$$\begin{aligned} &P(\text{outage}) \\ &\quad = P(\text{outage}|\mathcal{E}_l)P(\mathcal{E}_l) + P(\text{outage}|\mathcal{E}_l^c)P(\mathcal{E}_l^c) \quad (4) \\ &\quad \geq P(\text{outage}|\mathcal{E}_l)P(\mathcal{E}_l). \quad (5) \end{aligned}$$

As a is a constant, we find $P(\mathcal{E}_l)$ is also equal to a constant. At high SNR

$$\begin{aligned} &P(\text{outage}|\mathcal{E}_l) \\ &\quad = P\left(\frac{\prod_{i=1}^{L}(1+\lambda_i \text{SNR})}{\prod_{i=1}^{k}(1+\mu_i \text{SNR})} < \text{SNR}^{r_s}|\mathcal{E}_l\right) \quad (6) \\ &\quad \overset{(a)}{\geq} P\left(\frac{\prod_{i=1}^{L}(1+\lambda_i \text{SNR})}{(1+a\text{SNR})^k} < \text{SNR}^{r_s}\right) \\ &\quad \overset{(b)}{\geq} P\left(\prod_{i=1}^{L}(1+\lambda_i \text{SNR}) < \text{SNR}^{r_s+k}\right) \\ &\quad \overset{(c)}{\doteq} \text{SNR}^{-d_{m,n}(r_s+k)} \\ &\quad \overset{(d)}{\doteq} \text{SNR}^{-d_{m-k,n-k}(r_s)}, \end{aligned}$$

where using the definition of $\mathcal{E}_l$ we substituted the minimum value for all μ_i in (6) to obtain (a). (b) follows because $(1+a\text{SNR})^k \geq \text{SNR}^k$. Using the DMT results without secrecy constraints [13], (c) and (d) follow, where $d_{m,n}(r)$ is the piecewise-linear function joining the points $(t, (m-t)(n-t))$, $t = 0, 1, ..., \min\{m,n\}$. As $P(\text{outage}) \doteq \text{SNR}^{-d_s(r_s)}$, we conclude that $d_s(r_s)$ is upper bounded with the DMT of an $(m-k) \times (n-k)$ MIMO system.

Outage Upper Bound: To make the upper bound tight, we need a piecewise analysis, which depends on the secret multiplexing gain. We define c_i as

$$c_i = -(m+n-2k-2i-1)r_s + (m-k)(n-k) - i(i+1),$$

for $i = 0, 1, ..., \min\{m,n\} - k - 1$. We also define the event $\mathcal{E}_{u,i} = \{\mu_k > c_i \log \text{SNR}\}$, and $\mathcal{E}_{u,i}^c$ as the complement of $\mathcal{E}_{u,i}$.

For any i, we can write

$$\begin{aligned} &P(\text{outage}) \\ &\quad = P(\text{outage}|\mathcal{E}_{u,i})P(\mathcal{E}_{u,i}) + P(\text{outage}|\mathcal{E}_{u,i}^c)P(\mathcal{E}_{u,i}^c) \\ &\quad \leq P(\mathcal{E}_{u,i}) + P(\text{outage}|\mathcal{E}_{u,i}^c), \quad (7) \end{aligned}$$

where we have upper bounded both $P(\text{outage}|\mathcal{E}_{u,i})$ and $P(\mathcal{E}_{u,i}^c)$ with 1.

To calculate an upper bound on the first term in (7), we use an upper bound on the probability density function (pdf) of μ_k. We obtain this bound using the joint pdf of the ordered eigenvalues $0 \leq \mu_1 \leq \mu_2 \leq ... \leq \mu_k$ of the matrix $\mathbf{H}_{ST}\mathbf{H}_{ST}^{\dagger}$ [13, Lemma 3], which is

$$p(\mu_1, ...\mu_k) = K_{m,k}^{-1} \prod_{i=1}^{k} \mu_i^{m-k} \prod_{i<j} (\mu_i - \mu_j)^2 e^{-\sum_{i=1}^{k} \mu_i},$$

where $K_{m,n}$ is a normalizing constant. Then,

$$\begin{aligned} &p(\mu_k) \\ &\quad = \int_0^{\mu_k} ... \int_0^{\mu_2} p(\mu_1, ...\mu_k) d\mu_1 ... d\mu_{k-1} \\ &\quad = K_{m,k}^{-1} \mu_k^{m-k} e^{-\mu_k} \\ &\qquad \cdot \int_0^{\mu_k} ... \int_0^{\mu_2} \prod_{i=1}^{k-1} \mu_i^{m-k} \prod_{i<j} (\mu_i - \mu_j)^2 e^{-\sum_{i=1}^{k-1} \mu_i} \\ &\qquad\qquad d\mu_1 ... d\mu_{k-1} \\ &\quad \overset{(e)}{\leq} K_{m,k}^{-1} \mu_k^{m-k} \mu_k^{k(k-1)} e^{-\mu_k} \\ &\qquad \cdot \int_0^{\mu_k} ... \int_0^{\mu_2} \prod_{i=1}^{k-1} \mu_i^{m-k} e^{-\sum_{i=1}^{k-1} \mu_i} d\mu_1 ... d\mu_{k-1} \\ &\qquad\qquad (8) \\ &\quad \overset{(f)}{\leq} K_{m,k}^{-1} \mu_k^{m-k} \mu_k^{k(k-1)} e^{-\mu_k} [(m-k)!]^{k-1} \quad (9) \end{aligned}$$

where (e) is because each $(\mu_i - \mu_j)^2 \leq \mu_k^2$, and there are $k(k-1)/2$ many $(\mu_i - \mu_j)^2$ terms involved. Before

we write (f) we first bound the innermost integral in (8) as

$$\begin{aligned}
&\int_0^{\mu_2} \mu_1^{m-k} e^{-\mu_1} d\mu_1 \\
&\quad = \quad \gamma(m-k+1, \mu_2) \\
&\quad \overset{(g)}{=} \quad (m-k)! \left[1 - e^{-\mu_2} \left(\sum_{l=0}^{m-k} \frac{\mu_2^l}{l!}\right)\right] \\
&\quad \leq \quad (m-k)!,
\end{aligned}$$

where $\gamma(.,.)$ is the lower incomplete gamma function. Note that for (g) we used the series expansion of this function [16]. Applying this result repeatedly to all the integrals in (8) leads to (f). Using this upper bound on the pdf of the largest eigenvalue μ_k, we can now find an upper bound on $P(\mathcal{E}_{u,i})$. Let $C_i = c_i \log \mathrm{SNR}$ for short hand notation. Then,

$$\begin{aligned}
&P(\mathcal{E}_{u,i}) \\
&\quad = \quad P(\mu_k > C_i) \\
&\quad = \quad \int_{C_i}^{\infty} p(\mu_k) d\mu_k \\
&\quad \overset{(h)}{\leq} \quad K_{m,k}^{-1} [(m-k)!]^{k-1} \int_{C_i}^{\infty} \mu_k^{m-2k+k^2} e^{-\mu_k} d\mu_k \\
&\quad = \quad K_{m,k}^{-1} [(m-k)!]^{k-1} \Gamma(m-2k+k^2+1, C_i) \qquad (10) \\
&\quad \overset{(i)}{=} \quad K_{m,k}^{-1} [(m-k)!]^{k-1} e^{-C_i} \sum_{l=0}^{m-2k+k^2} \frac{C_i^l}{l!}, \qquad (11)
\end{aligned}$$

where we used (9) to obtain (h). In (10) $\Gamma(.,.)$ denotes the upper incomplete Gamma function, and we used the series expansion of this function to obtain (i) [16]. Then, it is easy to show that

$$P(\mathcal{E}_{u,i}) \quad \dot{\leq} \quad \mathrm{SNR}^{-c_i}, \qquad (12)$$

as the e^{-C_i} term in (11) determines the high SNR behavior of (11).

For the second term in (7) we show that

$$\begin{aligned}
&P(\text{outage}|\mathcal{E}_{u,i}^c) \\
&\quad = \quad P\left(\frac{\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR})}{\prod_{i=1}^{k}(1+\mu_i \mathrm{SNR})} < \mathrm{SNR}^{r_s} | \mathcal{E}_{u,i}^c\right) \\
&\quad \overset{(j)}{\leq} \quad P\left(\frac{\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR})}{(1+(c_i \log \mathrm{SNR})\mathrm{SNR})^k} < \mathrm{SNR}^{r_s}\right) \\
&\quad \overset{(k)}{\leq} \quad P\Bigg(\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR}) \\
&\qquad\qquad < \quad (2\max\{1, c_i\})^k (\log \mathrm{SNR})^k \mathrm{SNR}^{r_s+k}\Bigg) \\
&\quad \overset{(l)}{\leq} \quad P\left(\prod_{i=1}^{L}(1+\lambda_i \mathrm{SNR}) < A^k (\log \mathrm{SNR})^k \mathrm{SNR}^{r_s+k}\right) \\
&\quad \overset{(m)}{\dot{=}} \quad \mathrm{SNR}^{-d_{m,n}(r_s+k)} \\
&\quad \dot{=} \quad \mathrm{SNR}^{-d_{(m-k),(n-k)}(r_s)}. \qquad (13)
\end{aligned}$$

In the above inequalities, (j) is because the largest eigenvalue μ_k and hence all μ_i's are upper bounded by $c_i \log \mathrm{SNR}$ given $\mathcal{E}_{u,i}^c$. (k) is due to the fact that

$$1 + (c_i \log \mathrm{SNR})\mathrm{SNR} \leq 2\max\{1, c_i\}(\log \mathrm{SNR})\mathrm{SNR},$$

and (l) follows because $c_i \leq (m-k)(n-k)$, for all $i = 1, ..., \min\{m,n\} - k - 1$, and we define $A = 2\max\{1, (m-k)(n-k)\}$. Finally, (m) is because $A^k (\log \mathrm{SNR})^k \mathrm{SNR}^{r_s+k}$ has the same multiplexing gain as SNR^{r_s+k}, and thus the results in [13] apply.

Overall, substituting (12) and (13) into (7), using the definition of c_i, and combining the results for all i we have

$$P(\text{outage}) \quad \dot{\leq} \quad \mathrm{SNR}^{-d_{(m-k),(n-k)}(r_s)}.$$

We can observe that this upper bound on probability of secrecy rate outage is the same as the lower bound we calculated above. Thus, we conclude that $d_s(r_s) = d_{(m-k),(n-k)}(r_s)$, and the secret multiplexing gain satisfies $r_s \leq \min\{m,n\} - k$ for $k < \min\{m,n\}$.

If $k \geq \min\{m,n\}$, then $P(\text{outage}|\mathcal{E}_l)$ in (5) takes a constant value and does not decay with SNR. As $P(\mathcal{E}_l)$ is also equal to a constant, $P(\text{outage})$ is lower bounded by a fixed value in $(0,1]$. Thus, we conclude that when $k \geq \min\{m,n\}$, the secret DMT reduces to the single point $(0,0)$. ■

Theorem 1 states that the wire-tapper costs the system $\min\{m,k\}$ degrees of freedom, which affects the whole secret DMT curve. When the degrees of freedom in the source-wire-tapper channel, $\min\{m,k\}$, is equal to k, then the secret system becomes equivalent to an $(m-k) \times (n-k)$ system. However, if $\min\{m,k\} = m$, then no degrees of freedom are left for the main channel, as $m \geq \min\{m,n\}$, and the secret DMT reduces to the single point $(0,0)$.

Fig.1 shows an example secret DMT for the wire-tap channel, when the source, the destination and the wire-tapper have 3, 4, and 2 antennas respectively. We observe that for the *secret* channel only one degree of freedom is left, and the maximum *secret* diversity can be 2. The figure also compares the secret DMT to the 3×4 channel DMT without secrecy constraints. We can observe the effect of secrecy constraints not only on the degrees of freedom, but also on diversity, for all possible secret multiplexing gain values.

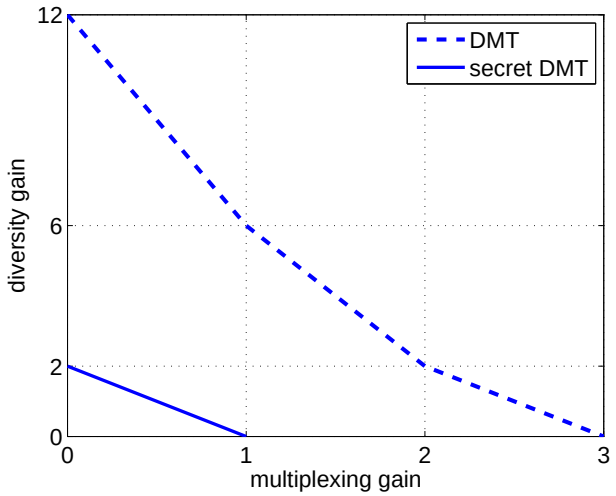

Fig. 1. The source, the destination and the wire-tapper respectively have 3, 4 and 2 antennas. Dashed curve shows the DMT with no secrecy constraints, whereas the solid curve is the secret DMT.

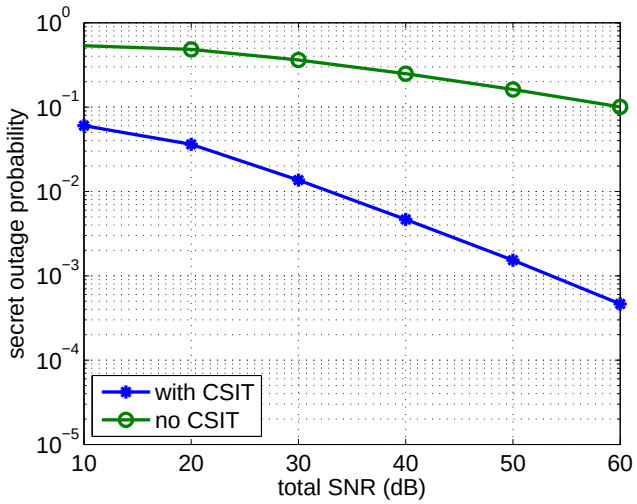

Fig. 2. The source, the destination and the wire-tapper respectively have 2, 2 and 1 antennas, $r_s = 0.75$.

IV. Channel State Information at the Source

In the previous section secret DMT is established for MIMO wire-tap channels without transmitter CSI. In this section we assume that transmitter has perfect CSI about the channel between itself and the wire-tapper, as well as its channel to the destination. 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-rate applications, which can suffer from outage despite the available transmitter CSI.

The secrecy capacity for the MIMO wire-tap channel with CSI both at the receivers (the destination and the wire-tapper) and the transmitter (the source) is found in [8], [9] as

$$C_s = \max_{\substack{K_X \succeq 0, \\ \mathrm{Tr}(K_X) \leq m\mathrm{SNR}}} \log \frac{\det\left(\mathbf{I} + \mathbf{H}_{SD} K_X \mathbf{H}_{SD}^{\dagger}\right)}{\det\left(\mathbf{I} + \mathbf{H}_{ST} K_X \mathbf{H}_{ST}^{\dagger}\right)}.$$

This secrecy capacity is achieved for the optimal input covariance matrix K_X, which sends signals orthogonal to the wire-tapper and as aligned with the destination as possible [7]. When the source and the destination each have 2 antennas, and the wire-tapper has a single antenna, the above secrecy capacity expression can be written as [7]

$$C_s^{(221)} = \log \frac{\mathbf{q}^{\dagger}\mathbf{A}\mathbf{q}}{\mathbf{q}^{\dagger}\mathbf{B}\mathbf{q}},$$

where

$$\begin{aligned} \mathbf{A} &= \mathbf{I} + m\mathrm{SNR}\mathbf{H}_{SD}^{\dagger}\mathbf{H}_{SD} \\ \mathbf{B} &= \mathbf{I} + m\mathrm{SNR}\mathbf{H}_{ST}\mathbf{H}_{ST}^{\dagger} \\ \mathbf{q} &= \frac{\mathbf{B}^{-1/2}\mathbf{w}}{\|\mathbf{B}^{-1/2}\mathbf{w}\|}, \end{aligned}$$

and $\mathbf{w}$ is the largest eigenvalue of $\mathbf{B}^{-1/2}\mathbf{A}\mathbf{B}^{-1/2}$.

In Fig. 2 we compare secrecy outage probability for the wire-tap channel with a 2-antenna source, a 2-antenna destination, and a single antenna wire-tapper for no transmitter CSI and full CSI cases. The secret multiplexing gain is equal to 0.75. The figure suggests that the secret diversity is approximately equal to 0.45 with full CSI. This value is almost double the secret diversity we achieve (approximately 0.23 from the figure, and 0.25 according to Theorem 1) when there is no CSI at the transmitter. Note that for MIMO channels without secrecy constraints if CSI is available at the transmitter, the source node does beamforming in the direction of the destination . However, without secrecy constraints beamforming only brings in coding gains and does not change the DMT. The secret diversity gains we observe from Fig. 2 show a different trend and suggest that the transmitter CSI changes the secret DMT.

V. Conclusion

In this paper we study the MIMO wire-tap channel when there are stringent delay constraints and the source node does not have CSI available. We define and find the *secret* DMT for arbitrary number of antennas at the source, the destination and the wire-tapper. Our

results show that the wire-tapper decreases the degrees of freedom in the direct link by the degrees of freedom in the source-wire-tapper channel. The secret DMT depends on the remaining degrees of freedom. We also study the effect of transmitter CSI on secret DMT. We observe that unlike the DMT without secrecy constraints, the transmitter CSI changes the secret DMT.

REFERENCES

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

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

[3] 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.

[4] P. K. Gopala, L. Lai, and H. E. Gamal, "On the secrecy of capacity of fading channels," October 2006, submitted to IEEE Transactions on Information Theory.

[5] Y. Liang, H. V. Poor, and S. Shamai, "Secure communication over fading channels," November 2006, submitted to IEEE Transactions on Information Theory. [Online]. Available: http://arxiv.org/abs/cs/0701024

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

[7] 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, submitted to IEEE Transactions on Information Theory. [Online]. Available: http://arxiv.org/abs/0709.3541

[8] A. Khisti and G. W. Wornell, "The MIMOME channel," in *Proceedings of 45th Allerton Conference on Communication, Control and Computing*, October 2007. [Online]. Available: http://arxiv.org/abs/0710.1325

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

[10] 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.

[11] 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.

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

[13] 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.

[14] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai, "Compound wire-tap channels," in *Proceedings of 45th Allerton Conference on Communication, Control and Computing*, September 2007.

[15] 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.

[16] I. S. Gradshteyn and I. M. Ryzhik, *Table of integrals, series, and products*, 7th ed. Academic press, 2007.