This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE Globecom 2010 proceedings.

Providing Secrecy Irrespective of Eavesdropper's Channel State

Xiang He Aylin Yener

Wireless Communications and Networking Laboratory
Electrical Engineering Department
The Pennsylvania State University, University Park, PA 16802
xxh119@psu.edu yener@ee.psu.edu

***Abstract*—A usual concern against physical layer security is that the legitimate parties would need to have (partial) channel state information (CSI) of the eavesdropper in order to design transmission schemes that provide secrecy. In this work, to overcome this concern, we consider the model where the eavesdropper's CSI is completely unknown at the legitimate transmitter(s) and the receiver. A static channel setting, and multiple antennas are considered for all parties, and it is assumed that the eavesdropper has perfect self-CSI. In this setting, assuming that the legitimate parties can employ a larger number of antennas than the eavesdropper, we provide a positive secure communication rate in the sense of strong secrecy. The achievable (guaranteed) secrecy rate we derive for the MIMO wiretap channel matches its converse in terms of secure degrees of freedom. As a side result of our approach, we also derive the secure degrees of freedom region for the MIMO MAC-wiretap channel where the transmitters and the intended receiver have the same number of antennas.**

***Index Terms*—Information theoretic secrecy, MIMO Wiretap channel, MIMO-MAC Wiretap channel, strong secrecy, arbitrary eavesdropper CSI**

I. Introduction

Information theoretic secrecy, introduced by Shannon in [1], uses mutual information as a secrecy measure. Wyner, in [2], used this measure to study the wiretap channel, and established that when the observation of what is transmitted at the eavesdropper is degraded (noisier) compared to that at the legitimate receiver, a positive rate can be supported for communicating confidential messages from the transmitter to the legitimate receiver without requiring keys.

This model [2] [3] has inspired significant effort to date toward identifying the information theoretic limits of a variety of wiretap channel models, see for example, [4] [5] [6], [7]. All of these assume that the transmitter has perfect knowledge of the eavesdropper channel states, which is difficult to obtain in a practical system since the eavesdropper is by nature a passive entity. To overcome this problem, recent references attempt to relax this condition by assuming the transmitter only has partial knowledge about the channel states of the eavesdropper. Notably, this effort includes investigations on the compound channel, where the eavesdropper channel can only be taken from a *finite* selection [8]–[10]; and the fading channel, where the transmitter only knows the distribution of the eavesdropper channel [11]. Each of these calls for a coding scheme tailored to what is available to the system as partial knowledge on the eavesdropper's channel.

In this work, we take a different route altogether and remove all assumptions on the eavesdropper's CSI at the legitimate transmitters. That is to say that the eavesdropper channel is static but can take *any* value unknown to the legitimate parties. We also assume that the eavesdropper has perfect self-CSI. Therefore, the legitimate parties are at a disadvantage with respect to CSI. We investigate the MIMO wiretap channel in this practical setting.

The main contribution of this work is to prove, for the MIMO wiretap channel, the existence of a *universal* coding scheme that secures the confidential message against any eavesdropper channel state. The guaranteed (achievable) secrecy rate derived from this approach is *tight* in terms of secure degrees of freedom (s.d.o.f.). Specifically,, we prove that the s.d.o.f. of the secrecy capacity of this MIMO wiretap channel model is $\max\{\min\{N_T, N_R\} - N_E, 0\}$.

The secrecy rate we prove is a *strong* secrecy rate [12]. It is worthwhile to note that the setting considered is tantamount to assuming an *infinite* number of eavesdroppers are present with *any* channel state values. As a consequence of this fact, strong secrecy results do not follow from weak secrecy through privacy amplification [12].

In related work, reference [13] considered that for the MISO wiretap channel, with a certain probability, a positive secrecy rate can be achieved by introducing artificial noise at the transmitter. The secrecy rate follows using reference [3] which in turn calls for the average performance over a codebook ensemble, from which we deduce that there must exist a codebook in the ensemble that yields good performance. This argument can be repeated for each eavesdropper channel to show the existence of a good codebook in each case. However, a universal coding scheme does not follow from this approach.

Recently, reference [14] noted the need for a universal coding scheme, and proved the existence of such a scheme for an arbitrarily varying *discrete* memoryless wiretap channel in the *weak* secrecy sense. Our work differs from [14] in that we prove *strong* secrecy and consider a continuous model, whose analysis does not follow from its discrete counterpart.

We also extend our result to the MIMO Multiple Access (MAC) wiretap channel, where the transmitters and the legiti-

978-1-4244-5637-6/10/$26.00 ©2010 IEEE

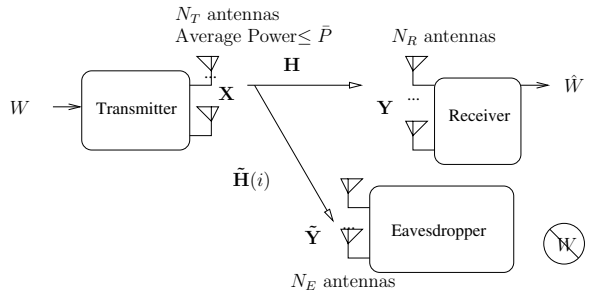

Fig. 1. The MIMO Wiretap Channel.

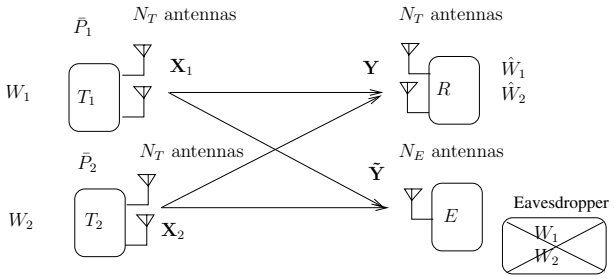

Fig. 2. An Example MIMO MAC Wiretap Channel where each legitimate node has $N_T = 2$ antennas, and the eavesdropper has $N_E = 1$ antenna.

mate receiver have the same number of antennas, and establish its secure degrees of freedom region. Interestingly, the same problem in the setting where the eavesdropper's channel is known by the legitimate parties is still open.

II. System Model

A. The MIMO (N_T, N_R, N_E) Wiretap Channel

We consider the MIMO wiretap channel shown by Figure 1 in which the transmitter has N_T antennas. The intended receiver has N_R antennas. The eavesdropper has N_E antennas.

The input and output of the main channel are related as

$$\mathbf{Y}_{N_R\times 1} = \mathbf{H}_{N_R\times N_T}\mathbf{X}_{N_T\times 1} + \mathbf{Z}_{N_R\times 1} \tag{1}$$

where the subscript denotes the dimension of each term. $\mathbf{H}, \mathbf{X}, \mathbf{Y}$ are the channel matrix, transmitted and received signals respectively. $\mathbf{Z}$ is the additive channel noise composed of independent rotational invariant complex Gaussian random variable each with zero mean and unit variance. We assume $\mathbf{H}$ is known to all parties.

We assume the eavesdropper channel is also a static channel. Hence it can be expressed as

$$\tilde{\mathbf{Y}}_{N_E\times 1} = \tilde{\mathbf{H}}_{N_E\times N_T}\mathbf{X}_{N_T\times 1} \tag{2}$$

where $\tilde{\mathbf{Y}}$ denotes the signals received by the eavesdropper. $\tilde{\mathbf{H}}$ is the channel state matrix for the eavesdropper channel. $\tilde{\mathbf{H}}$ is *not* known at the legitimate parties. Observe that the eavesdropper channel is noiseless, consistent with our goal to consider the worst case scenario for the legitimate parties.

Let W denote the confidential message transmitted to the intended receiver over n channel uses via $\mathbf{X}^n$. We represent $\mathbf{X}^n$ as a $N_T \times n$ matrix. The average power constraint is expressed as

$$\lim_{n\to\infty} \frac{1}{n}\mathrm{trace}(\mathbf{X}^n(\mathbf{X}^n)^H) \leq \bar{P}. \tag{3}$$

Let $\hat{W}$ denote the decoder output of the receiver computed from $\mathbf{Y}^n$. For reliable communication, we require $\lim_{n\to\infty}\Pr(W \neq \hat{W}) = 0$.

We use the parameter γ to denote that the eavesdropper's channel matrix is $\tilde{\mathbf{H}}_\gamma$ and use $\tilde{\mathbf{Y}}^n_\gamma$ to represent the corresponding channel outputs for the eavesdropper. Therefore, the *strong* secrecy constraint is

$$\lim_{n\to\infty} I(W; \tilde{\mathbf{Y}}^n_\gamma) = 0, \quad \forall\gamma. \tag{4}$$

Observe that the convergence should be uniform over all possible eavesdropper channels.

Define the secrecy rate R_e as $R_e = \lim_{n\to\infty}\frac{1}{n}H(W)$. R_e is achievable if W can be decoded reliably, and equations (4) and (3) hold. The supremum of R_e is the secrecy capacity.

The secure degrees of freedom, which provides a high SNR characterization of the secrecy rate is defined as follows

$$\text{s.d.o.f.} = \limsup_{\bar{P}\to\infty} \frac{R_e}{\log_2(\bar{P})}. \tag{5}$$

B. The MIMO (N_T, N_T, N_T, N_E) MAC Wiretap Channel

We consider the following configuration of a MIMO-MAC wiretap channel with the same assumptions we use for the MIMO wiretap channel: Both the main channel and the eavesdropper channel are Gaussian MIMO multiple access (MAC) channels. We assume each transmitter has N_T antennas. The receiver also has N_T antennas. The eavesdropper has N_E antennas. The channel is defined as:

$$\mathbf{Y} = \sum_{k=1}^{2}\mathbf{H}_k\mathbf{X}_k + \mathbf{Z}, \qquad \tilde{\mathbf{Y}} = \sum_{k=1}^{2}\tilde{\mathbf{H}}_k\mathbf{X}_k \tag{6}$$

where $\mathbf{H}_k, k = 1, 2$ and $\tilde{\mathbf{H}}_k, k = 1, 2$ are channel matrices. $\mathbf{Z}$ is the additive Gaussian noise observe by the intended receiver, which has the same distribution as the $\mathbf{Z}$ in the MIMO wiretap channel. An example of the channel where $N_R = N_T = 2, N_E = 1$ is shown in Figure 2.

Each user k wants to transmit a confidential message W_k to the receiver over n channel uses, while both messages must be kept confidential from the eavesdropper. We use γ to index a specific value of $\{\tilde{\mathbf{H}}_k, k = 1, 2\}$ and use $\tilde{\mathbf{Y}}^n_\gamma$ to represent the corresponding channel outputs for the eavesdropper. The secrecy constraint is:

$$\lim_{n\to\infty} I\left(W_1, W_2; \tilde{\mathbf{Y}}^n_\gamma\right) = 0, \quad \forall\gamma. \tag{7}$$

Again the convergence should be uniform over all possible eavesdropper channels.

The average power constraints for the two users are given by $\lim_{n\to\infty}\frac{1}{n}\mathrm{trace}(\mathbf{X}^n_k(\mathbf{X}^n_k)^H) \leq \bar{P}_k, k = 1, 2$. The secrecy rate $R_{e,k}$ of the kth user is once again defined as $R_{e,k} = \lim_{n\to\infty}\frac{1}{n}H(W_k), k = 1, 2$, such that W_k can be reliably decoded by the receiver, the average power constraints and the secrecy constraint (7) hold.

We define the secure degrees of freedom region as follows. Assume $\bar{P}_k = \bar{P}, k = 1, 2$. The secure degrees of freedom region is given by

$$\{(d_1, d_2) : d_k = \limsup_{\bar{P}\to\infty} \frac{R_{e,k}}{\log_2 \bar{P}}, k = 1, 2\}. \quad (8)$$

III. The MIMO Wiretap Channel

A. Main Result

For the MIMO wiretap channel in Figure 1, we have the following theorem.

Theorem 1: Let $N_{T,R} = \min\{N_T, N_R\}$. Let s_i be the $N_{T,R}$ singular values of $\mathbf{H}$. Define P as $\max\{\bar{P} - N_{T,R}, 0\}$. Define $C(x)$ as $\log_2(1+x)$. Then any secrecy rate R_s smaller than

$$\max\left\{\left(\sum_{i=1}^{N_{T,R}} C\left(\frac{s_i^2 P}{(s_i^2+1)N_{T,R}}\right)\right) - N_E C\left(P\right), 0\right\} \quad (9)$$

is achievable. When $\mathbf{H}$ has full rank, the s.d.o.f. of the secrecy *capacity* for the channel model in is $\max\{N_{T,R} - N_E, 0\}$. Due to space limitations, we shall focus on the achievability of (9) in the sequel. For the converse for the s.d.o.f., see [15].

B. Coding Scheme

For simplicity, we assume $N_T = N_R$, $\mathbf{H}$ is diagonal, and $\tilde{\mathbf{H}}$ has the following form singular value decomposition:

$$\tilde{\mathbf{H}} = [\mathbf{I}_{N_E \times N_E}, \mathbf{0}_{N_E \times (N_T - N_E)}]\mathbf{U} \quad (10)$$

where $\mathbf{U}$ is a $N_T \times N_T$ unitary matrix. $\mathbf{I}$ is an identity matrix. It is shown in [15] that all eavesdropper channels can be expressed in the form of (10) and assuming a diagonal $\mathbf{H}$ does not lead to loss of generality.

Fist, we introduce artificial noise at the transmitter. We define $\tilde{\mathbf{X}}$ as $\mathbf{X} = \tilde{\mathbf{X}} + \mathbf{N}$, where $\mathbf{N}$ is a $N_T \times 1$ random vector formed by independent rotational invariant Gaussian random variable with distribution $\mathcal{CN}(0, 1)$. The coding is performed over $\tilde{\mathbf{X}}$.

Define $\bar{\mathbf{N}}$ and $\tilde{\mathbf{N}}$ as $\bar{\mathbf{N}} = \mathbf{H}\mathbf{N}$, $\tilde{\mathbf{N}} = \tilde{\mathbf{H}}\mathbf{N}$. If we view $\tilde{\mathbf{X}}$ as the input to the channel, then the channel model can be expressed as:

$$\mathbf{Y} = \mathbf{H}\tilde{\mathbf{X}} + \bar{\mathbf{N}} + \mathbf{Z} \quad (11)$$

$$\tilde{\mathbf{Y}} = \tilde{\mathbf{H}}\tilde{\mathbf{X}} + \tilde{\mathbf{N}} \quad (12)$$

From the distribution we choose for $\mathbf{N}$ and equation (10), we observe $\tilde{\mathbf{N}}$ has zero mean and has a Gaussian distribution. $E[\tilde{\mathbf{N}}\tilde{\mathbf{N}}^H] = \mathbf{I}_{N_E \times N_E}$.

At this point, it is instructive to highlight the difference from reference [13] in the way we use artificial noise. In [13], the artificial noise is carefully precoded in order not to interfere the intended receiver. This implies that the benefit of artificial noise will diminish when the eavesdropper moves toward the intended receiver, leading to a secrecy outage, an inevitable consequence of the fact that the number of antennas of the intended receiver equals that of the eavesdroppers. In contrast, here, we transmit artificial noise is transmitted over all directions, in the same spirit as [4], which creates interference for both the intended receiver and the eavesdropper. Secrecy is achieved when the intended receiver has more antennas than the eavesdropper.

With the introduction of the artificial noise, secrecy can be guaranteed by using a stochastic encoder at the transmitter. The encoder uses the usual wire-tap channel binning: Each codeword is labeled with a pair of indices (i, j). i is the bin index. j is the index of the codeword inside the bin. Each bin contains the same number of codewords. For the confidential message $W = i$, the transmitted codeword, a $N_T \times n$ complex matrix, is chosen from all the codewords inside bin i according to a uniform distribution. Correspondingly, the intended receiver uses a maximum likelihood decoder to compute the transmitted codeword, and deduces the value of the message from the first index associated with this codeword.

A moment's thought reveals that a given codebook could secure the message for one eavesdropper channel, but completely reveal the message for a different eavesdropper channel. Consider the case when $N_T = N_R = 2$ and $N_E = 1$. If identical signals are transmitted over two antennas, then the signals received by the eavesdropper will be completely nullified when $\tilde{\mathbf{H}} = [1, -1]$, and completely revealed when $\tilde{\mathbf{H}} = [1, 1]$. The challenge therefore is to show the existence of *a codebook* that guarantees secrecy for any value that the eavesdropper channel can take. The main result given in Section III-A claims this with the associated guaranteed secrecy rate. In the next section, we provide a brief outline for its proof.

C. Proof Outline

We use $p_W(w)$ to denote the value of the probability mass function (p.m.f.) of a random variable W at w. $f_{\gamma,A}(a)$ denotes the probability density function (p.d.f.) of a random variable A at value a with parameter γ. $f_{\gamma,A|B}(a|b)$ denotes the conditional p.d.f. of a random variable A conditioned on a random variable B when $A = a, B = b$.

For a given codebook $\mathcal{C}$, let $\tilde{\mathbf{Y}}_{\mathcal{C}}^n$ denote $\tilde{\mathbf{Y}}^n$ when $\tilde{\mathbf{X}}^n$ is uniformly distributed over the codebook $\mathcal{C}$. Define d_γ as the variational distance between two distribution $p_W f_{\gamma,\tilde{\mathbf{Y}}_{\mathcal{C}}^n}$ and $p_W f_{\gamma,\tilde{\mathbf{Y}}_{\mathcal{C}}^n|W}$:

$$\sum_w p_W(w) \int |f_{\gamma,\tilde{\mathbf{Y}}_{\mathcal{C}}^n}(z^n) - f_{\gamma,\tilde{\mathbf{Y}}_{\mathcal{C}}^n|W}(z^n|w)|dz^n \quad (13)$$

The focus of the proof is to show that there exists a codebook $\mathcal{C}$, such that d_γ decreases exponentially with respect to n, which, due to the following lemma, implies strong secrecy:

Lemma 1: [16, Lemma 1]: $I\left(W; \tilde{\mathbf{Y}}_\gamma^n\right) \leq \mathrm{d}_\gamma \log_2 \frac{|W|}{\mathrm{d}_\gamma}$.

The steps in proving that there exists a $\mathcal{C}$ with this property for its d_γ can be outlined as follows:

1) As in [6], [16], we first prove for any eavesdropper channel state value indexed by γ, d_γ averaged over an ensemble of wiretap codebooks decreases uniformly and exponentially fast with respect to the code length n.
2) We then quantize the channel states [17] and construct a finite subset of values of the eavesdropper channel

state. We show that for this subset, there must exist a good codebook that retains the property of the codebook ensemble that d_γ is small.

3) We show that when the eavesdropper channel state is not in the finite subset, the resulting variational distance can be approximated by the variational distance when eavesdropper channel state sequence is in the finite set and hence is also small. This is the approximation argument from [17].

The *codebook ensemble* is constructed as follows:

We begin by choosing the input distribution for $\tilde{\mathbf{X}}$, $Q_{\tilde{\mathbf{X}}}(x)$, as zero mean rotationally invariant complex Gaussian distribution. $E[\tilde{\mathbf{X}}\tilde{\mathbf{X}}^H] = (\frac{P(1-\varepsilon_P)}{N_T})\mathbf{I}_{N_T\times N_T}$. The codebook ensemble is composed of codebooks constructed as in [18, Section 7.3]. In the context of this work, this means defining an n-letter distribution $Q_{\tilde{\mathbf{X}}^n}(x^n)$ as follows: Let x_i denote the ith component of x^n. Let $\|x^n\|$ denote the L_2-norm of x^n. Then $Q_{\tilde{\mathbf{X}}^n}(x^n)$ is given by:

$$Q_{\tilde{\mathbf{X}}^n}(x^n) = \mu_{n,\varepsilon_P}^{-1}\varphi(x^n)\prod_{i=1}^{n} Q_{\tilde{\mathbf{X}}}(x_i) \tag{14}$$

where $\varphi(x^n) = \begin{cases} 1, & \text{if } \frac{1}{n}\|x^n\|^2 \le P \\ 0, & \text{otherwise} \end{cases}$, and $\mu_{n,\varepsilon_P} = \int \varphi(x^n)\prod_{i=1}^{n} Q_{\tilde{\mathbf{X}}}(x_i)dx^n$. $0 < \mu_{n,\varepsilon_P} < 1$.

Any codebook in the ensemble is constructed by sampling 2^{nR} sequences in an i.i.d. fashion from the n-letter distribution $Q_{\tilde{\mathbf{X}}^n}$. R is chosen as $R = I(\tilde{\mathbf{X}};\mathbf{Y}) - \delta'$. δ' is a positive constant that can be made arbitrarily small.

The labels for the codewords are generated as follows. Each time a codeword is sampled, it is labeled with (i,j). The label i takes values from $1,...,N_i$. j takes values from $1,...,N_j$. N_i and N_j are given by:

$$N_i = 2^{n(R-I(\tilde{\mathbf{X}};\tilde{\mathbf{Y}})-\delta_n)} \tag{15}$$

$$N_j = 2^{n(I(\tilde{\mathbf{X}};\tilde{\mathbf{Y}})+\delta_n)} \tag{16}$$

where $\{\delta_n\}$ is a positive sequence whose details will be specified later. Initially, we set $i = j = 1$. After we label a codeword, if $j < N_j$, then we increase j by one. Otherwise, we increase i by one and reset j to 1.

Note that the mutual information in (16) is evaluated when $\tilde{\mathbf{X}}$ has distribution $Q_{\tilde{\mathbf{X}}}$. We drop the subscript γ in this expression since the value of the mutual information does not depend on γ when $\tilde{\mathbf{X}}$ has the distribution $Q_{\tilde{\mathbf{X}}}$.

Let $\tilde{\mathbf{X}}_T^n$ denote $\tilde{\mathbf{X}}^n$ when it is sampled in an i.i.d. fashion from the input distribution $Q_{\tilde{\mathbf{X}}^n}$ instead of the codebook. Let $\tilde{\mathbf{Y}}_T^n$ denote $\tilde{\mathbf{Y}}^n$ when $\tilde{\mathbf{X}}^n$ is $\tilde{\mathbf{X}}_T^n$. For this ensemble of codebooks, the first step in the proof outline is guaranteed by the following two lemmas.

Lemma 2: [6, Appendix II] d_γ is upper bounded by

$$2\sum_w p_W(w)\int |f_{\gamma,\tilde{\mathbf{Y}}_T^n}(z^n) - f_{\gamma,\tilde{\mathbf{Y}}_{\mathcal{C}}^n|W}(z^n|w)|dz^n \tag{17}$$

Lemma 3: If $\forall n, \delta_n \ge \max\{2\varepsilon, \varepsilon + \alpha(\varepsilon_P)\log_2 e/2\}$ for $\varepsilon > 0$, then there exists a constant $c' > 0$, such that the following term is bounded by $e^{-c'n}$. c' only depends on $\varepsilon, \varepsilon_P$.

$$\mathrm{E}_{\mathcal{C}}[2\sum_w p_W(w)\int |f_{\gamma,\tilde{\mathbf{Y}}_T^n}(z^n) - f_{\gamma,\tilde{\mathbf{Y}}_{\mathcal{C}}^n|W}(z^n|w)|dz^n]$$

The proof of Lemma 3 is provided in [15]. From Lemmas 2 and 3, we observe:

$$\mathrm{E}_{\mathcal{C}}[\mathrm{d}_\gamma] \le \exp(-c'n) \tag{18}$$

We next construct the finite subsets of values of the eavesdropper channel, S_M, as follows: If the real and imaginary parts of each element in $M\tilde{\mathbf{H}}$ are integers, $\tilde{\mathbf{H}}$ is in S_M. From $\tilde{\mathbf{H}}\tilde{\mathbf{H}}^H = \mathbf{I}$, it can be shown that S_M is a finite set with at most $(2M+1)^{2N_TN_E}$ elements. Hence, from (18),

$$\sum_{\tilde{\mathbf{H}}_\gamma\in S_M} \mathrm{E}_{\mathcal{C}}[\mathrm{d}_\gamma] \le (2M+1)^{2N_TN_E}\exp(-c'n) \tag{19}$$

Thus, as in [6, Appendix II, Section E], from Markov inequality, we know there must exist one codebook such that

1) the probability of decoding error at the intended receiver vanishes as $n \to \infty$. The average power of each codeword is smaller or equal to P;
2) for each $\tilde{\mathbf{H}}_\gamma \in S_M$, we have

$$\mathrm{d}_\gamma \le 3\times 2(2M+1)^{2N_TN_E}\exp(-c'n). \tag{20}$$

This concludes the second step in the proof outline.

For this fixed codebook, we next consider the case where $\tilde{\mathbf{H}}_\gamma \notin S_M$. d_γ in this case can be bounded by the following lemma, whose proof is provided in [15].

Lemma 4: Define $(r')^2 = \frac{2N_TN_EP}{M^2}$, $r = r' + \sqrt{N_E(1+\varepsilon)}$, and $g(r,r') = r'(2r+r')$. If $ng(r,r') < 1$, then we have:

$$\mathrm{d}_\gamma \le 12(2M+1)^{2N_TN_E}e^{-c'n} + 12e^{-n\alpha(\varepsilon)} + 4ng(r,r'). \tag{21}$$

We then choose M such that (21) decreases exponentially fast with respect to n. Note that $g(r,r')$ decreases at the rate of $1/M$. Hence there must exists a positive constant $c_2 > 0$ that when $M = \exp(nc_2)$, both $(2M+1)^{2N_TN_E}\exp(-c'n)$ and $ng(r,r')$ decrease exponentially fast to 0 with respect to n. This means (21) decreases exponentially fast with respect to n. This concludes the last step in the proof outline.

We have now shown *the existence of a codebook* that can provide secrecy for any eavesdropper CSI. We next provide the secrecy rate when this codebook is used.

The rate of the message W can be determined by choosing δ_n that satisfies the condition in Lemma 3. Let $c_4 = \delta_n + \delta' = \max\{2\varepsilon, \varepsilon + \alpha(\varepsilon_P)\log_2 e/2\} + \delta'$. The codebook rate is then given below, which can be made arbitrarily close to (9).

$$\lim_{n\to\infty}\frac{1}{n}H(W) \ge I\left(\tilde{\mathbf{X}};\mathbf{Y}\right) - N_EC(P(1-\varepsilon_P)) - c_4 \tag{22}$$

Since W is uniformly distributed, $\log_2|W|$ is $H(W)$. As shown by (22), $H(W)$ increases linearly with n. Since the variational distance d_γ decreases to 0 exponentially fast with

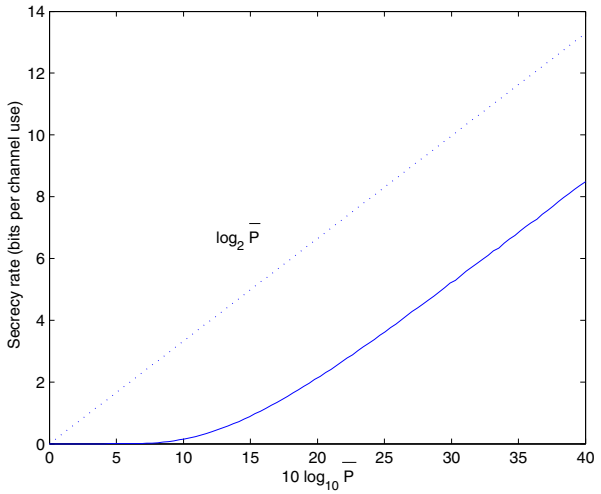

Fig. 3. Secrecy rate averaged over realizations of main channel states, $N_T = N_R = 2, N_E = 1$.

respect to n, from Lemma 1, $I\left(W; \tilde{\mathbf{Y}}_{\gamma}^{n}\right)$ decreases to 0 exponentially fast with respect to n. Hence the rate of the codebook given by (22) is, in fact, a strong secrecy rate.

The achieved secrecy rate and s.d.o.f. can then be found from (22) to be (9) and $\max\{\min\{N_T, N_R\} - N_E, 0\}$ respectively.

For demonstration of our result, in Figure 3, we plot the achievable secrecy rate given by (9). The secrecy rate is averaged over those that correspond to randomly generated 2×10^4 main channel matrices. In particular, $\mathbf{H}$ matrices are generated in an i.i.d. fashion such that all of its elements are independent and sampled from a rotationally invariant complex Gaussian distribution with zero mean and unit variance. (9) is evaluated when $N_T = N_R = 2$ and $N_E = 1$. We also plot $\log_2 \bar{P}$ in dashed lines in Figure 3 and observe that when $\bar{P}$ increases, the curve of the secrecy rate tends to share the same slop with $\log_2 \bar{P}$, hence confirming the s.d.o.f. result in Theorem 1.

IV. (N_T, N_T, N_T, N_E) MIMO-MAC Wiretap Channel

The achievable secrecy rate in Theorem 1 can be readily extended to the MIMO-MAC wiretap channel, for which we have the following theorem.

Theorem 2: For the MIMO MAC wiretap channel (N_T, N_T, N_T, N_E), If $\mathbf{H}_k, k = 1, 2$ has full rank, the s.d.o.f. region of the MAC wiretap channel (N_T, N_T, N_T, N_E) is given by: $d_1 + d_2 \leq \max\{N_T - N_E, 0\}$, $d_i \geq 0, i = 1, 2$.

The achievability follows from Theorem 1 with time sharing. For the converse, we simply combine the two transmitters. The channel then becomes a single-user MIMO wiretap channel, where the transmitter has $2N_T$ antennas, the receiver has N_T antennas, and the eavesdropper has N_E antenna. $d_1 + d_2 \leq \max\{N_T - N_E, 0\}$ then follows from the converse of Theorem 1. For the complete proof, see [15].

V. Conclusion

In this work, we have considered the setting where the eavesdropper's CSI is known only to the eavesdropper and not to the legitimate nodes. With this assumption, we have derived an achievable secrecy rate and the high SNR characterization of the secrecy capacity for the MIMO wiretap channel (and the MIMO-MAC wiretap channel) in the strong secrecy sense. The guaranteed secrecy rate is positive irrespective of the eavesdropper's channel, as long as it has fewer antennas than the legitimate nodes. The approach for the static eavesdropper channel in this work can be extended to an arbitrarily varying eavesdropper channel, see [15].

References

[1] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4):656–715, September 1949.

[2] A. D. Wyner. The Wire-tap Channel. *Bell System Technical Journal*, 54(8):1355–1387, 1975.

[3] I. Csiszár and J. Körner. Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, 24(3):339–348, May 1978.

[4] E. Tekin and A. Yener. The General Gaussian Multiple Access and Two-Way Wire-Tap Channels: Achievable Rates and Cooperative Jamming. *IEEE Transactions on Information Theory*, 54(6):2735–2751, June 2008.

[5] E. Ekrem and S. Ulukus. The Secrecy Capacity Region of the Gaussian MIMO Multi-receiver Wiretap Channel. Submitted to IEEE Transactions on Information Theory, March 2009, available online at http://arxiv.org/abs/0903.3096.

[6] M. Bloch and J. N. Laneman. On the secrecy capacity of arbitrary wiretap channels. In *46th Allerton Conference on Communication, Control, and Computing*, September 2008.

[7] A. Khisti and G. Wornell. Secure Transmission with Multiple Antennas-I: The MISOME Wiretap Channel. to appear in IEEE Transactions on Information Theory, submitted in August, 2007. available online at http://arxiv.org/abs/0708.4219.

[8] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai. Compound Wiretap Channels. *Eurasip Journal on Wireless Communication and Networking, Special issue in Wireless Physical Layer Security*, vol. 2009, Article ID 142374, 12 pages, 2009. doi:10.1155/2009/142374.

[9] E. Ekrem and S. Ulukus. Secrecy Capacity Region of the Degraded Compound Multi-Receiver Wiretap Channel. In *47th Allerton Conference on Communication, Control, and Computing*, September 2009.

[10] M. Kobayashi, Y. Liang, S. Shamai, and M. Debbah. On the Compound MIMO Broadcast Channels with Confidential Messages. In *IEEE International Symposium on Information Theory*, June 2009.

[11] P. K. Gopala, L. Lai, and H. El-Gamal. On the Secrecy Capacity of Fading Channels. *IEEE Transactions on Information Theory*, 54(9):4687–4698, October 2008.

[12] U. Maurer and S. Wolf. Information-theoretic Key Agreement: From Weak to Strong Secrecy for Free. *Lecture Notes in Computer Science*, pages 351–368, 2000.

[13] S. Goel and R. Negi. Guaranteeing Secrecy using Artificial Noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, June 2008.

[14] E. MolavianJazi. Secure Communication Over Arbitrarily Varying Wiretap Channels. *Master Thesis*, December 2009. available online at http://etd.nd.edu/ETD-db/theses/available/etd-12112009-112419/unrestricted/MolavianJaziE122009.pdf.

[15] X. He and A. Yener. MIMO Wiretap Channels with Arbitrarily Varying Eavesdropper Channel States. Submitted to the IEEE Transactions on Information Theory, July, 2010, available online at http://arxiv.org/abs/1007.4801.

[16] I. Csiszár. Almost Independence and Secrecy Capacity. *Problems of Information Transmission*, 32(1):48–57, 1996.

[17] D. Blackwell, L. Breiman, and A. J. Thomasian. The capacity of a class of channels. *The Annals of Mathematical Statistics*, 30(4):1229–1241, 1959.

[18] R. G. Gallager. *Information theory and reliable communication*. John Wiley & Sons, Inc. New York, NY, USA, 1968.