Secrecy Capacity of SIMO and Slow Fading Channels

Patricio Parada and Richard Blahut
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, IL 61801, USA
Email:{paradasa,blahut}@uiuc.edu

***Abstract*— We present a single letter characterization of the secrecy capacity of the single-input multiple-outputs (SIMO) channel under Gaussian (and possibly colored) noise. To do so, we transform the channel into a scalar Gaussian wiretap channel using standard techniques of communications theory. The result is used to study the impact of slow fading on the secrecy capacity of the channel, and how the use of multiple receive antennas could improve the performance of the system.**

I. Introduction

A cryptosystem is considered *unconditionally secure* if it cannot be broken even with infinite computing power [1]. To be more precise, let Alice (legitimate sender), Bob (legitimate receiver) and Eve (eavesdropper) be the main characters of the problem. Alice and Bob wish to convey a secret using a public channel in such a way that Eve gains no information about the secret that is being shared. In [2] Shannon proved that if the one-time cipher is used to encrypt the secret, they would achieve an unconditionally secure transmission, but his proof also concluded that the length of the encryption key should be at least as long as the message itself. In [3] Wyner assumed the presence of noise in the communication channels, in a model that he called the wiretap channel. His main result was that, under certain conditions, a secret message could be transmitted at a positive rate without revealing it to Eve.

This work is an extension of Wyner's ideas to the case of the single-input multiple-outputs (SIMO) channel under (possible colored) additive Gaussian noise. Using some standard calculations from communication theory [4], we show that a SIMO channel has an equivalent scalar channel (from the information theory point of view) and that such a channel is a Gaussian wiretap channel [5]. This fact allows us to get a single letter characterization for the secrecy capacity of the channel. Later, we extend the results to the case of slow fading, this is, the channel gains have random values but fixed for all time.

We have chosen this particular channel by two reasons: it is a nice generalization of Wyner's work on its own right, serving as a model for the distribution of secret keys to several users inside a network, but also, because it put us one step closer to understand how secure a wireless network can be. SIMO channels, and more generally, MIMO channels are successful models for the wireless environment, and it seams natural to ask what kind of limits one faces as an engineer at the moment of evaluating the security of a wireless network.

The structure of the paper is the following. Section 2 summarizes previous results and gives an intuitive idea of what improvements can be expected with the introduction of a multiple-outputs model respect to the traditional Gaussian wiretap channel. Section 3 and 4 presents the core of the calculations. Section 5 concludes with some final remarks and a glimpse of what is under current research.

Finally, a word on notation: scalars will be denoted by *italic* typeface (x), vectors by **boldface** fonts ($\mathbf{y}$) and matrices by roman capital letters (H).

II. Previous results

In [3] Wyner obtained a single letter characterization for the secrecy capacity of the wiretap channel. The wiretap channel (see Figure 1) is a degraded form of a broadcast channel, where the goal is to maximize the transmission rate in the main channel while making negligible the amount of information leaked to the cascade (wiretapper) channel. The secrecy capacity is the maximal rate at which this goal is achieved.

Wyner result states that if the capacity of the main channel is C_M and the capacity of the overall wiretap channel is C_{MW}, then the secrecy capacity of the channel C_S is given by

$$C_S = C_M - C_{MW}.$$

One consequence of this result is that in order to have a positive secrecy capacity C_S the wiretapper channel must be noisier than the one used to transmit the secret.

During the nineties, Maurer [6] presented a strategy that allows a positive rate even when the wiretapper observes a "better" channel than the one used by the legitimate users. The key element of his protocol is a procedure called *privacy amplification* [7], that by using public discussion reduces a initial piece of random nature (to fix ideas, a sequence of bits) into a smaller entity which is known only by the legitimate users. The procedure is of iterative nature; it involves Alice and Bob sharing information by means of a "conversation" in which they get rid of all the bits that are known to Eve.

Now we make an important observation: during the privacy amplification stage, Alice and Bob transmit correlated sequences along successive iterations. In communications systems there exists a similar approach to achieve a completely different objective: if a channel is poor, for example if the

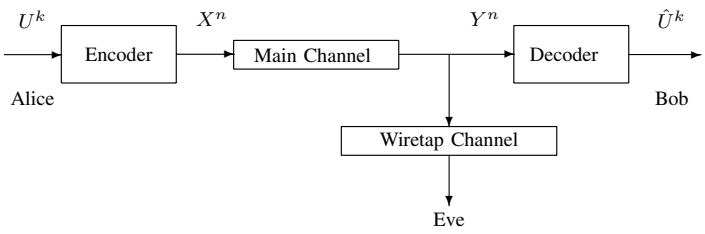

Fig. 1. wiretap channel block diagram.

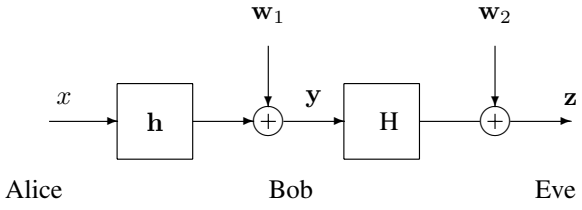

Fig. 2. Degraded broadcast channel block diagram.

environmental conditions change abruptly and the noise power is high, we can retransmit the sequence n times, improving the probability of correct detection in the receiver's end. This is a *repetition code*, and is a very simple example of a more general idea known as *time diversity*. We may ask then: could we use other kinds of diversity (frequency, code, or space) to achieve unconditional security? We will provide a partial answer to this question by the inclusion of multiple receive antennas in our model. But first, we state some known ideas and results about the wiretap channel.

A. The wiretap channel

Consider two discrete memoryless channels (DMC) as the ones depicted in Figure 1.

The encoder takes the input sequence $U^k = (U_1, \ldots, U_k)$ and transforms it into a n symbols sequence $X^n = (X_1, \ldots, X_n)$. The rate of the code is $R = k/n$.

The security engineer must design an encoder/decoder pair that ideally maximizes the transmission rate of the legitimate user, subject to the constraint that the rate at which the wiretapper learns the sequence is as small as possible.

The wiretapper knows the encoding used, and its ignorance about the source depends only on the noise realization present in the channels. The source is assumed to be stationary and ergodic, and takes its values over a finite alphabet. The probability of block decoding error is denoted by

$$P_e = \Pr\{U^k \neq \hat{U}^k\}.$$

The wiretapper uncertainty about the source is measured by the equivocation

$$H(U^k|Z^n),$$

after observing the output of the channel.

Definition 2.1: The fractional equivocation

$$\delta = \frac{H(U^k|Z^n)}{H(U^k)}.$$

The rate of the code

$$R = \frac{H(U^k)}{n}.$$

Definition 2.2: (Achievability) The pair (R^*, d^*) is said to be achievable if for all $\epsilon > 0$ there exists an enconder/decoder pair such that

$$R \geq R^* - \epsilon$$
$$\delta \geq d^* - \epsilon$$
$$P_e \leq \epsilon$$

Theorem 2.1: [3]. The set of achievable pairs (R, d) can be characterized as follows

$$\mathscr{R} = \{(R, d) : 0 \leq R \leq C_M, 0 \leq d \leq 1, Rd \leq C_S\} \quad (1)$$

where C_S is the secrecy capacity and its value is

$$C_S = C_M - C_{MW}.$$

B. Gaussian wiretap channel

Although Wyner's work only considered discrete-time channels, Leung and Hellman [5] proved that the results also hold in a particular case of continuous-time channel. A Gaussian wiretap channel is wiretap channel where the noise is additive white and Gaussian, such that the channel is power limited (P) and the noise processes are independent and have components that are i.i.d. $\mathscr{N}(0, \sigma_1^2)$ and $\mathscr{N}(0, \sigma_2^2)$ respectively.

The achievable region of the Gaussian wiretap channel is the same as defined in eq. 1 with

$$C_M = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2}\right)$$
$$C_{MW} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2 + \sigma_2^2}\right)$$

III. SIMO Gaussian wiretap Channel

Let us consider the degraded Single Input Multiple Output (SIMO) channel depicted in Figure 2. We will determine the secrecy capacity of the SIMO Gaussian wiretap channel under the following conditions:

- Alice sends symbols that have limited average power $P > 0$, i.e.,
$$\frac{1}{K}\sum_{k=0}^{K-1} \mathbb{E}[x^2[k]] \leq P.$$
- Bob uses n_r receive antennas and Eve uses m_r receive antennas to recover Alice message.
- Alice sends no message to Eve, so there are no common messages.
- The channel parameters are represented by $\mathbf{h} \in \mathbb{C}^{\,n_r}$ and $\mathrm{H} \in \mathbb{C}^{\,m_r \times n_r}$.

In the k-th time slot, the following relations are satisfied

$$\left.\begin{array}{rcl} \mathbf{y}[k] & = & \mathbf{h}x[k] + \mathbf{w}_1[k] \\ \mathbf{z}[k] & = & \mathrm{H}\mathbf{y}[k] + \mathbf{w}_2[k], \end{array}\right\} \quad (2)$$

where $\mathbf{w}_1$ and $\mathbf{w}_2$ are independent random vectors, each one of them being complex and jointly Gaussian distributed with mean $\mathbf{0}$ and non-singular covariance matrices Σ_1 and Σ_2 respectively.

Our goal is to show that the channel described by eq. 2 can be represented by an scalar channel and that such representation is in fact a Gaussian wiretap channel [5]. The next lemma is a particular case of the theorem of irrelevance [4], but it is included given that the cryptographic nature of the application under study.

In the following, time dependence will be assumed implicitly and the k index will be dropped from the equations.

Lemma 3.1: Consider the channel

$$\mathbf{y} = \mathbf{h}x + \mathbf{w}, \quad (3)$$

where $\mathbf{w}$ is complex additive Gaussian noise with zero mean and covariance matrix Σ and $\mathbf{h} \in \mathbb{C}^{\,n}$.

A sufficient statistic to correctly determine x from $\mathbf{y}$ is the scalar

$$\tilde{y} = \mathbf{h}^\dagger \Sigma^{-1} \mathbf{y}.$$

Proof: Without lost of generality, let us consider $x \in \{-1, +1\}$. Let

$$\begin{array}{rcl} H_0 & : & \mathbf{y} = +\mathbf{h} + \mathbf{w} \\ H_1 & : & \mathbf{y} = -\mathbf{h} + \mathbf{w}. \end{array}$$

The MAP rule is

$$\begin{array}{c} \Pr\{\mathbf{y}|H_0\} > \Pr\{\mathbf{y}|H_1\} \\ e^{\left(-\frac{1}{2}(\mathbf{y}+\mathbf{h})^\dagger \Sigma^{-1}(\mathbf{y}+\mathbf{h})\right)} > e^{\left(-\frac{1}{2}(\mathbf{y}-\mathbf{h})^\dagger \Sigma^{-1}(\mathbf{y}-\mathbf{h})\right)} \\ \Longrightarrow \ \mathbf{h}^\dagger \Sigma^{-1} \mathbf{y} > 0. \end{array}$$

■

As a direct implication of Lemma 3.1 and the fact that sufficient statistics "preserve mutual information" [8], we have

$$I(x; \mathbf{y}) = I(x; \tilde{y}). \quad (4)$$

Further, the capacity of the channel described by eq. 3 is

$$C = \frac{1}{2} \log\left(1 + (\mathbf{h}^\dagger \Sigma^{-1} \mathbf{h}) P\right). \quad (5)$$

Theorem 3.1: The channel described by eq. 2 is equivalent to the following Gaussian wiretap channel

$$\left.\begin{array}{rcl} \tilde{y}[k] & = & \tilde{h}_1^2 x[k] + \tilde{w}_1[k] \\ \tilde{z}[k] & = & \tilde{h}_2^2 x[k] + \tilde{w}_2[k], \end{array}\right\} \quad (6)$$

where

$$\begin{array}{rl} \tilde{h}_1^2 = & \mathbf{h}^\dagger \Sigma_1^{-1} \mathbf{h}, \\ \tilde{h}_2^2 = & (\mathrm{H}\mathbf{h})^\dagger (\mathrm{H}\Sigma_1 \mathrm{H}^\dagger + \Sigma_2)^{-1} \mathrm{H}\mathbf{h}, \\ \tilde{w}_1[k] = & \mathbf{h}^\dagger \Sigma_1^{-1} \mathbf{w}_1[k] \sim \mathscr{N}(0, \tilde{h}_1^2), \\ \tilde{w}_2[k] = & (\mathrm{H}\mathbf{h})^\dagger (\mathrm{H}\Sigma_1 \mathrm{H}^\dagger + \Sigma_2)^{-1} (\mathrm{H}\mathbf{w}_1[k] + \mathbf{w}_2[k]) \\ & \sim \mathscr{N}(0, \tilde{h}_2^2). \end{array}$$

Proof: Application from the Lemma 3.1 yields the following sufficient statistics for detecting $x[k]$ from $\mathbf{y}[k]$ and $\mathbf{z}[k]$:

$$\tilde{y} = \mathbf{h}^\dagger \Sigma_1^{-1} \mathbf{y} \quad (7)$$

$$\tilde{z} = (\mathrm{H}\mathbf{h})^\dagger (\mathrm{H}\Sigma_1 \mathrm{H}^\dagger + \Sigma_2)^{-1} \mathbf{z} \quad (8)$$

Then, it is direct to obtain the scalar model described by eq. 6.

The resulting degraded broadcast channel is in fact a Gaussian wiretap channel because from the point of view of Bob and Eve, the best strategy they can employ in order to detect correctly $x[k]$ is to compute the projections given by eqs. 7 and 8. In addition, the fact that sufficient statistics conserves the mutual information makes both the scalar and the vectorial channel completely equivalents from the information theory perspective. ■

Corollary 3.1: The secrecy capacity of the SIMO Gaussian wiretap channel is

$$C_S = \frac{1}{2} \log\left(\frac{1 + \mathbf{h}^\dagger \Sigma_1^{-1} \mathbf{h} P}{1 + (\mathrm{H}\mathbf{h})^\dagger (\mathrm{H}\Sigma_1 \mathrm{H}^\dagger + \Sigma_2)^{-1} (\mathrm{H}\mathbf{h}) P}\right) \quad (9)$$

Proof: Since the SIMO Gaussian wiretap channel has a scalar representation that corresponds to the Gaussian wiretap channel, from [5] we known that the secrecy capacity of the channel is

$$C_S = C_M - C_{MW},$$

C_M being the capacity of the main channel and C_{MW} being the capacity of the overall wiretap channel. Their values are

$$\begin{array}{rl} C_M = & \frac{1}{2} \log\left(1 + \mathbf{h}^\dagger \Sigma_1^{-1} \mathbf{h} P\right) \\ C_{MW} = & \frac{1}{2} \log\left(1 + (\mathrm{H}\mathbf{h})^\dagger (\mathrm{H}\Sigma_1 \mathrm{H}^\dagger + \Sigma_2)^{-1} (\mathrm{H}\mathbf{h}) P\right) \end{array}$$

which concludes the proof. ■

A necessary condition to have a positive secrecy capacity C_S is to require that the matrix

$$\Sigma = \Sigma_1^{-1} - \mathrm{H}^\dagger (\mathrm{H}\Sigma_1 \mathrm{H}^\dagger + \Sigma_2)^{-1} \mathrm{H}$$

to be positive definite. If the noise processes $\mathbf{w}_1$ and $\mathbf{w}_2$ are uncorrelated, and

$$\Sigma_1 = \sigma_1 \mathrm{I}_{n_r} \quad \Sigma_2 = \sigma_2 \mathrm{I}_{m_r}, \quad (10)$$

we can find a simpler expression for Σ. The application of the Matrix Inversion Lemma [9] yields

$$\Sigma = (\sigma_1 \mathrm{I}_{n_r} + \sigma_2 \mathrm{H}\mathrm{H}^\dagger)^{-1}. \quad (11)$$

For this case, we know that the matrix Σ is Hermitian, and all its eigenvalues are real numbers. However, this is just necessary to have the positive definiteness condition; we must impose externally the condition that all eigenvalues of Σ must be positive numbers.

IV. The SIMO wiretap Channel under Slow Fading

The results obtained in the previous section can be used to extend the idea of secrecy capacity to the case when the channel parameters are random but fixed for all time (slow fading).

Conditioning on realizations of H and $\mathbf{h}$ the secrecy capacity is given by eq. 9. The effect of fading is included by considering that $\{\mathbf{h}[k] : k \in \mathbb{Z}\}$ and $\{\mathrm{H}[k] : k \in \mathbb{Z}\}$ are random processes, and in consequence, the secrecy capacity is no longer a deterministic value but a random process itself.

The random nature of the problem implies that the usual notions of secure communication are meaningless, in the sense that the probability that the secrecy capacity drops below a given transmission rate R is positive. Because of this, we prefer to study the *outage* event

$$O(R) = \{R > 0 : C_S < R\},$$

and its probability of occurrence P_{out}

$$\Pr\{\frac{1}{2}\log\left(\frac{1+\mathbf{h}^\dagger\Sigma_1^{-1}\mathbf{h}P}{1+(\mathrm{H}\mathbf{h})^\dagger(\mathrm{H}\Sigma_1\mathrm{H}^\dagger+\Sigma_2)^{-1}(\mathrm{H}\mathbf{h})P}\right) < R\}.$$

To get an insight on the behavior of this formula, we study the following case: consider that $\Sigma_1 = {\sigma_1}^2\mathrm{I}_{n_r}$ and $\Sigma_2 = {\sigma_2}^2\mathrm{I}_{m_r}$, and that H is unitary. Then the outage probability is

$$\Pr\{\frac{1}{2}\log\left(\frac{1+\|\mathbf{h}\|^2\mathrm{SNR}}{1+\|\mathbf{h}\|^2\frac{{\sigma_1}^2}{{\sigma_1}^2+{\sigma_2}^2}\mathrm{SNR}}\right) < R\} \qquad (12)$$

where $\mathrm{SNR} = P/{\sigma_1}^2$.

If the main channel is extremely noise, this is, if ${\sigma_1}^2 \gg {\sigma_2}^2$, then $C_S \to 0$ and the system is in outage with probability 1. On the other hand, if ${\sigma_1}^2 \ll {\sigma_2}^2$ then the secrecy capacity C_S tends to

$$\frac{1}{2}\log\left(1+\|\mathbf{h}\|^2\mathrm{SNR}\right).$$

Under Rayleigh fading, $\|\mathbf{h}\|^2$ is a sum of the squares of n_r independent Gaussian random variables and its distribution is a χ^2 density with $2n_r$ degrees of freedom. A standard approximation for this probability (see Chapter 5 [10] for more details) yields

$$P_{out} = \Pr\{\|\mathbf{h}\|^2 < \frac{2^R-1}{\mathrm{SNR}}\} \approx \frac{(2^R-1)^{n_r}}{(n_r!)\mathrm{SNR}^{n_r}}.$$

In any intermediate situation, we have that

$$P_{out} = \Pr\{\|\mathbf{h}\|^2 < \frac{2^R-1}{1-2^R\frac{{\sigma_1}^2}{{\sigma_1}^2+{\sigma_2}^2}}\frac{1}{\mathrm{SNR}}\}.$$

A similar computation to the case of ${\sigma_1}^2 \ll {\sigma_2}^2$ allows us to conclude that the outage probability decays as $1/\mathrm{SNR}^{n_r}$. It is not difficult to see that in the case of $n_r = 1$ (the case of a scalar Gaussian wiretap channel under slow fading), $\|\mathbf{h}\|^2$ has an exponential probability density, and therefore, the outage probability decays as $1/\mathrm{SNR}$. The addition of several receive antennas introduces a diversity gain of n_r.

V. Conclusion

In this work we have presented an extension of Wyner's result to the case of SIMO channels under (possibly colored) additive Gaussian noise.

We have shown that the SIMO channel under Gaussian noise can be represented by a Gaussian wiretap channel, and that all the properties of this class of channels can be carried out to this new scenario. In particular, there exists a single letter characterization for the secrecy capacity of the SIMO channel.

We also observe in a very simple example that under slow fading conditions, the use of multiple receive antennas provides an advantage with respect to a single-antenna channel. Although we cannot conclude from this particular case that antenna diversity improves the security of the system, we believe that it is the general case.

At the time of the submission of this paper, the authors are considering other possible ways to come up with security models for the multiple user channel, including the multiple inputs case and the introduction of fading in the channel. One particular direction corresponds to the case where the broadcast channel is no longer degraded, such as the one considered by Csiszár and Körner [11]. It is conjectured that in this situation unconditional secure communications is still possible, but there is no assurance on a single letter characterization of the secrecy capacity such as the one presented in this paper.

Acknowledgment

The authors wish to thank Jorge Silva by his helpful commentaries and questions during the preparation of this manuscript.

References

[1] D. Stinson, *Cryptography: Theory and Practice*, 2nd ed. Boca Raton, FL: CRC Press, 2002.

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

[3] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.

[4] J. Wozencraft and I. Jacobs, *Principles of Communcation Engineering*. New York: Wiley, 1965.

[5] S. Leung-Yan-Cheong and M. E. Hellman, "The gaussian wire-tap channel," *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[6] U. Maurer, "Secret key agreement by public discussion," *IEEE Transaction on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.

[7] C. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.

[8] T. Cover and J. Thomas, *Elements of Information Theory*. Wiley, 1991.

[9] G. Golub and C. van Loan, *Matrix Computations*. Baltimore, MD: Johns Hopkins University Press, 1996.

[10] P. Viswanath and D. Tse, "Fundamentals of wireless communications," class notes for ECE 459, Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Fall 2003.

[11] I. Csiszár and J. Körner, "Broadcast channels with confinential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.