World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:4, No:1, 2010

A degraded Practical MIMOME Channel: Issues in secret data communications

Mohammad Rakibul Islam

Open Science Index, Information and Communication Engineering Vol:4, No:1, 2010 publications.waset.org/11021/pdf

Abstract—In this paper, a Gaussian multiple input multiple output multiple eavesdropper (MIMOME) channel is considered where a transmitter communicates to a receiver in the presence of an eavesdropper. We present a technique for determining the secrecy capacity of the multiple input multiple output (MIMO) channel under Gaussian noise. We transform the degraded MIMOME channel into multiple single input multiple output (SIMO) Gaussian wire-tap channels and then use scalar approach to convert it into two equivalent multiple input single output (MISO) channels. The secrecy capacity model is then developed for the condition where the channel state information (CSI) for main channel only is known to the transmitter. The results show that the secret communication is possible when the eavesdropper channel noise is greater than a cutoff noise level. The outage probability is also analyzed of secrecy capacity is also analyzed. The effect of fading and outage probability is also analyzed.

Keywords—Secrecy capacity, MIMO, wiretap channel, covariance matrix, fading.

I. Introduction

Wireless media is an open medium for communication and is vulnerable to eavesdropping. However, the unique properties of wireless medium might provide ways of combating such security threats. The eavesdropping attack is first studied by Wyner using a single-user wire-tap channel [1]. Wyner introduced the wiretap channel in [1] and established the possibility of creating an almost perfectly secure sourcedestination link without relying on private (secret) keys. In the wiretap channel, both the wiretapper and destination observe the source encoded message through noisy channels, while the wiretapper is assumed to have unlimited computational resources. Wyner showed that when the source-wiretapper channel is a degraded version of the source-destination channel, the source can send perfectly secure messages to the destination at a non-zero rate. The main idea is to hide the information stream in the additional noise impairing the wiretapper by using a stochastic encoder which maps each message to many codewords according to an appropriate probability distribution. By doing this, one induces maximal equivocation at the wiretapper. By ensuring that the equivocation rate is arbitrarily close to the message rate, one achieves perfect secrecy in the sense that the wiretapper is now limited to learn almost nothing about the source-destination messages from its observations. Wyner models the wire-tappers channel from the transmitter to the legitimate receiver as a degraded version of the channel, which is a reasonable assumption in a wired channel. Wyners result is extended to the Gaussian wire-tap channel [2] to show that Gaussian signaling is optimal. And the secrecy capacity is denoted as the difference between the capacities of the main and the eavesdropping channels. Csiszar and Korner [5] study the general wire-tap channel with single-transmitter, single-receiver, single-eavesdropper, discrete memoryless channel with secrecy constraints, and find the expression for the secrecy capacity. The expression is in the form of the maximization of the difference between two mutual information involving an auxiliary random variable which is interpreted as performing pre-processing on the information. The secrecy capacity calculation for a given channel requires the solution of this maximization problem in terms of the joint distribution of the auxiliary random variable and the channel input.

Positive secrecy capacity is not always possible to achieve in practice. In an attempt to transmit messages securely in these unfavorable scenarios, [3] and [4] considered the wiretap channel with noiseless feedback (The authors also considered a more general secret sharing problem.). These works showed that one may leverage the feedback to achieve a positive perfect secrecy rate, even when the feed-forward perfect secrecy capacity is zero. In this model, there exists a separate noiseless public channel, through which the transmitter and receiver can exchange information. The wiretapper is assumed to obtain a perfect copy of the messages transmitted over this public channel. Upper and lower bounds were derived for the perfect secrecy capacity with noiseless feedback in [3] and [4].

The use of multiple transmit and receive antennas has been shown [6] and the results show that the achievable rates increase in the absence of secrecy constraints. An achievable scheme for secrecy in multiple input multiple output (MIMO) communications is proposed [7], where the transmitter uses its multiple transmit antennas to transmit only in the null space of the eavesdroppers channel, thereby preventing any eavesdropping. The Gaussian single-input multiple-output (SIMO) wire-tap channel is studied [8], where an equivalent scalar Gaussian channel is proposed. Secrecy capacity in terms of outage probability is proposed [9], [10] and a complete characterization of the maximum transmission rate at which the eavesdropper is unable to decode any information is provided. It is shown that in the presence of fading, information theoretic security is achievable even when the eavesdropper has a better average signal-to-noise ratio (SNR) than the legitimate receiver. An achievable scheme has been proposed for the Gaussian multiple input single output (MISO) wire-tap channel [11], [12]. The achievable secrecy rate is obtained here by restricting both the channel inputs to be Gaussian and with no pre-processing of information. The secrecy rate found in [11], [12] is shown to be the secrecy capacity of the Gaussian MISO wire-tap channel in [13], [14] where the eavesdropper is allowed to have multiple antennas. In this paper, the secrecy

Mohammad Rakibul Islam is with the Department of Electrical and Electronic Engineering Department, Islamic University of Technology, Boardbazar, Gazipur-1704, Dhaka, Bangladesh. e-mail: rakibultowhid@yahoo.com.

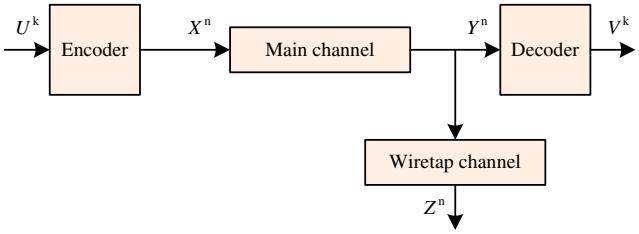


Fig. 1. Wire-tap channel

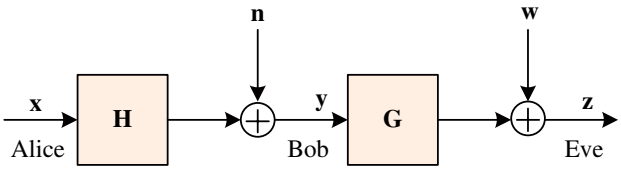


Fig. 2. Degraded broadcast channel

capacity of a MIMO channel using a scalar Gaussian approach is analyzed.

The remainder of this paper is organized as follows: In section II, the system in the light of wire-tap channel and Gaussian wire-tap channel is described. In section III, the representation of MIMO Gaussian wire-tap channel using scalar approach is shown. Secrecy capacity is developed in section IV. In section V, different issues are discussed. Then section VI concludes this paper.

II. System Model

The wire-tap channel shown in Fig.1 is a degraded form of a broadcast channel, where there are two discrete memoryless channels. The main channel is between the source and the targeted receiver and the wiretap channel is between main channel and the eavesdropper. The goal of the wiretap channel is to maximize the transmission rate in the main channel while making the amount of information leaked to the cascade (wiretapper) channel negligible.

Definition 1: Broadcast channel

A broadcast channel consists of one input alphabet $\mathcal{X}$ and two (or more) output alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$. The noise is defined by the conditional probability $P_{Y_1,Y_2|X}(y_1, y_2|x)$.

Examples of broadcast channels are cable television (CATV) network, lecturer in classroom, code division multiple access channels.

Definition: 2 Degraded Broadcast channel

A broadcast channel is said to be degraded if

$$P_{Y_1,Y_2|X}(y_1, y_2|x) = P_{Y1|X}(y1|x)P_{Y_2|Y_1}(y_2|y_1) \qquad (1)$$

It can be verified that when $X \rightarrow Y_1 \rightarrow Y_2$ forms a Markov chain, in which $P_{Y_1,Y_2|X}(y_1, y_2|x) = P_{Y_2|Y_1}(y_2|y_1)$, a degraded broadcast channel is resulted. This indicates that the parallelly broadcast channel degrades to a serially broadcast channel, where the channel output Y_2 can only obtain information from channel input X through the previous channel output Y_1.

The multiple input multiple output multiple eavesdropper (MIMOME) channel shown in Fig. 2 equipped with multiple antenna transmitter, receiver and eavesdropper is considered as the system model for this paper. This MIMOME channel can also be written as MIMO wire-tap channel. A legitimate user named Alice wants to send messages to another user, say Bob. The message block is encoded into a codeword and transmitted over a discrete time channel. A third party named Eve is capable of eavesdropping the signals sent by Alice by observing the channel output. The user and eavesdropper channel attenuations can be represented by $N_r \times N_t$ and $M_r \times N_r$ vectors $\mathbf{H}$ and $\mathbf{G}$, where N_t is the number of transmit antennas whereas N_r and M_r are the number of antennas at the legitimate receiver and eavesdropper. For every N_t transmitting antenna in Fig. 2, Alice sends symbols that have limited average power $P > 0$, i.e.,

$$\frac{1}{K}\sum_{k=0}^{K-1} E\{x^2[k]\} \leq P \qquad (2)$$

Bob uses N_r receive antennas and Eve uses M_r receive antennas to recover Alice's message. Alice sends no message to Eve, so there are no common messages.

The received signals at the receiver and the eavesdropper at k-th time slot are

$$\mathbf{y}[k] = \mathbf{H}\mathbf{x}[k] + \mathbf{n}[k] \qquad (3)$$

and

$$\mathbf{z}[k] = \mathbf{G}\mathbf{y}[k] + \mathbf{w}[k] \qquad (4)$$

where $\mathbf{n}$ and $\mathbf{w}$ are independent random vectors, each one of them being complex and jointly Gaussian distributed with mean 0 and non-singular covariance matrices Σ_1 and Σ_2 respectively. Our objective is to determine the secrecy capacity of the MIMO Gaussian wire-tap channel using the scalar approach.

Secrecy capacity is the issue to be considered here in this paper while the Gaussian wire-tap channel is the application area chosen. A Gaussian wire-tap channel is a wire-tap 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. $\mathcal{N}(0, \sigma_1^2)$ and $\mathcal{N}(0, \sigma_2^2)$ respectively.

The main channel capacity C_M and overall wiretap channel capacity C_W can be shown as

$$\begin{aligned} C_M &= \frac{1}{2}\log(1 + \frac{P}{\sigma_1^2}) \\ C_W &= \frac{1}{2}\log\left(1 + \frac{P}{\sigma_1^2 + \sigma_2^2}\right), \end{aligned} \qquad (5)$$

Open Science Index, Information and Communication Engineering Vol:4, No:1, 2010 publications.waset.org/11021/pdf

Open Science Index, Information and Communication Engineering Vol:4, No:1, 2010 publications.waset.org/11021/pdf

Therefore, the secrecy capacity is given by

$$C_S = C_M - C_W. \tag{6}$$

III. MIMO Gaussian wire-tap channel: a scalar approach

MIMO Gaussian wire-tap channel is described in the previous section where the secrecy capacity analysis is complex in the sense that the transmitter, and two receivers have multiple antennas. As we know that a SIMO Gaussian wire-tap channel can be converted to a scalar Gaussian wire-tap channel [8], we can apply the same in MIMO Gaussian wire-tap channel to make it simple. Therefore in this section, MIMO Gaussian wire-tap channel is transformed into a simple combination of two MISO channels using scalar approach. The scalar approach is a single letter characterization for the secrecy capacity [8]. To do so, the MIMOME channel is converted to several SIMOME channels. The MIMOME channel can be seen as a multiple parallel single input multiple output multiple eavesdropper (SIMOME) channel as shown in Fig. 3. Our goal is to show that the channel described by eq. 3 and eq. 4 can be represented by a summation of several single input multiple output (SIMO) Gaussian wire-tap channels. From eq. 3, it can be shown that a MIMO Gaussian wire-tap channel is the addition of N_t SIMO Gaussian wire-tap channels and can be written as

$$\begin{aligned}\mathbf{y}[k] &= \sum_{i=1}^{N_t} \mathbf{y}_i[k] \\ &= \sum_{i=1}^{N_t} (\mathbf{h}_i \mathbf{x}_i[k] + \mathbf{n}_i[k])\end{aligned} \tag{7}$$

where $\mathbf{y}_i[k] = \mathbf{h}_i \mathbf{x}_i[k] + \mathbf{n}_i[k]$ represents the i-th SIMO channel. Put the value of $\mathbf{y}[k]$ in the eq. 4 to get the eavesdropper channel output as follows

$$\mathbf{z}[k] = \mathbf{G} \sum_{i=1}^{N_t} (\mathbf{h}_i \mathbf{x}_i[k] + \mathbf{n}_i[k]) + \mathbf{w}[k] \tag{8}$$

The main channel and the eavesdropper channel outputs at eq. 7 and eq. 8 for the i-th SIMOME channel of the corresponding MIMOME channel can be written as

$$\mathbf{y}_i[k] = \mathbf{h}_i x_i[k] + \mathbf{n}_i[k] \tag{9}$$

and

$$\begin{aligned}\mathbf{z}_i[k] &= \mathbf{G}(\mathbf{h}_i x_i[k] + \mathbf{n}_i[k]) + \mathbf{w}_i[k] \\ &= \mathbf{G}\mathbf{h}_i x_i[k] + \mathbf{G}\mathbf{n}_i[k] + \mathbf{w}_i[k]\end{aligned} \tag{10}$$

Multiply the eq. 9 by $\mathbf{h}_i^\dagger \Sigma_{1i}^{-1}$ to get the following equation

$$\mathbf{h}_i^\dagger \Sigma_{1i}^{-1} \mathbf{y}_i[k] = \mathbf{h}_i^\dagger \Sigma_{1i}^{-1} \mathbf{h}_i x_i[k] + \mathbf{h}_i^\dagger \Sigma_{1i}^{-1} \mathbf{n}_i[k] \tag{11}$$

Both the sides are now 1×1 in dimension and in fact scalar. Take $\mathbf{h}_i^\dagger \Sigma_{1i}^{-1} \mathbf{y}_i[k] = y_i[k]$, $\mathbf{h}_i^\dagger \Sigma_{1i}^{-1} \mathbf{h}_i = h_i^2$ and $\mathbf{h}_i^\dagger \Sigma_{1i}^{-1} \mathbf{n}_i[k] = n_i[k]$ and the following equation can be written from equation 11.

$$y_i[k] = h_i^2 x_i[k] + n_i[k]. \tag{12}$$

Again multiply eq. 10 by $(\mathbf{G}\mathbf{h}_i)^\dagger (\mathbf{G}\Sigma_{1i}\mathbf{G}^\dagger + \Sigma_2)^{-1}$ to get

$$\begin{aligned}(\mathbf{G}\mathbf{h}_i)^\dagger (\mathbf{G}\Sigma_{1i}\mathbf{G}^\dagger &\\ +\Sigma_2)^{-1}\mathbf{z}_i[k] &= (\mathbf{G}\mathbf{h}_i)^\dagger (\mathbf{G}\Sigma_{1i}\mathbf{G}^\dagger + \Sigma_2)^{-1}\mathbf{G}\mathbf{h}_i x_i[k] \\ &\quad +(\mathbf{G}\mathbf{h}_i)^\dagger (\mathbf{G}\Sigma_{1i}\mathbf{G}^\dagger + \Sigma_2)^{-1}(\mathbf{G}\mathbf{n}_i[k] \\ &\quad +\mathbf{w}_i[k]).\end{aligned}$$

Both sides are now scalar. Take the following relations

$$\begin{aligned}(\mathbf{G}\mathbf{h}_i)^\dagger (\mathbf{G}\Sigma_{1i}\mathbf{G}^\dagger + \Sigma_2)^{-1}\mathbf{z}_i[k] &= z_i[k] \\ (\mathbf{G}\mathbf{h}_i)^\dagger (\mathbf{G}\Sigma_{1i}\mathbf{G}^\dagger + \Sigma_2)^{-1}\mathbf{G}\mathbf{h}_i &= g_i^2 \\ (\mathbf{G}\mathbf{h}_i)^\dagger (\mathbf{G}\Sigma_{1i}\mathbf{G}^\dagger + \Sigma_2)^{-1}(\mathbf{G}\mathbf{n}_i[k] + \mathbf{w}[k]) &= w_i[k]\end{aligned}$$

to get

$$z_i[k] = g_i^2 x_i[k] + w_i[k]. \tag{13}$$

Eq. 12 and eq. 13 show the scalar representation of the i-th SIMOME channel and is shown graphically in Fig. 4 (a). To represent the MIMOME channel, summation of all the SIMOME equivalent scalar channels is needed and is shown in Fig. 4 (b). Therefore the main and eavesdropper channel outputs for MIMOME can be written as

$$\begin{aligned}y[k] &= \sum_{i=1}^{N_t} y_i[k] \\ &= \sum_{i=1}^{N_t} (h_i^2 x_i[k] + n_i[k])\end{aligned}$$

and

$$\begin{aligned}z[k] &= \sum_{i=1}^{N_t} z_i[k] \\ &= \sum_{i=1}^{N_t} (g_i^2 x_i[k] + w_i[k])\end{aligned}$$

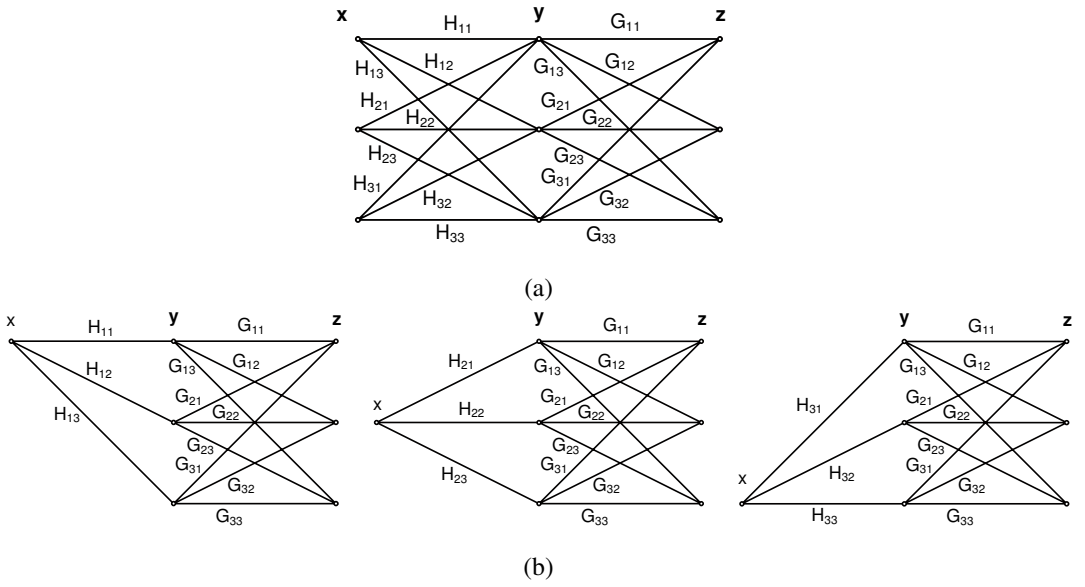


Fig. 3. (a)MIMOME channel (b) Representation of MIMOME into equivalent SIMOME channels

IV. Secrecy capacity

The equivocation rate R_e, is the conditional entropy of the transmitted message, conditioned on the received signal at the eavesdropper. The equivocation rate is a measure of the amount of information that the eavesdropper can attain about the message, and quantifies the level of secrecy in the system. The secrecy capacity, C_S, is the largest rate R achievable with perfect secrecy, i.e., $R_e = R$.

As a SIMOME channel can be converted to a scalar Gaussian wire-tap channel shown in Fig. 4 (a), the main channel and eavesdropper channel capacity of the i-th SIMOME channel can be written as

$$\begin{aligned} C_{M_i} &= \frac{1}{2}\log(1+h_i^2 P) \\ &= \frac{1}{2}\log(1+\mathbf{h}_i^\dagger \Sigma_{1i}^{-1}\mathbf{h}_i P) \end{aligned} \quad (14)$$

and

$$\begin{aligned} C_{W_i} &= \frac{1}{2}\log(1+g_i^2 P) \\ &= \frac{1}{2}\log(1+(\mathbf{G}\mathbf{h}_i)^\dagger(\mathbf{G}\Sigma_{1i}\mathbf{G}^\dagger+\Sigma_2)^{-1}\mathbf{G}\mathbf{h}_i P) \end{aligned} \quad (15)$$

.

The MIMOME channel can be thought of multiple SIMOME channels and according to Fig. 4 (b), a MIMOME channel can be converted to two MISO channels, one is for the main channel and the other is for the eavesdropper channel. Consider the channel gain parameter for main channel is $\mathbf{h}_m = [h_1^2, h_2^2, ..., h_{N_t}^2]$ and eavesdropper channel is $\mathbf{g}_m = [g_1^2, g_2^2, ..., g_{N_t}^2]$. If the original channel gains and the noise covariance matrices are known, the converted channel gain parameters can be calculated.

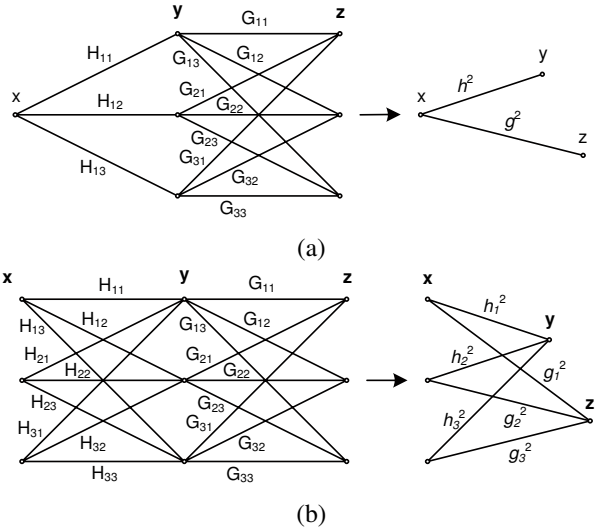


Fig. 4. (a) 2 output representation of SIMOME channel (b) 2 output representation of MIMOME channel

Normally the transmitter is aware of the main channel but is not aware of the eavesdropper channel. In this case, the main channel and eavesdropper channel capacity for MIMOME channel can be written as

$$C_M = \frac{1}{2}\log\left(1+\|\mathbf{h}_m\|^2 P\right) \quad (16)$$

$$C_W = \frac{1}{2}\log\left(1+\frac{\|\mathbf{g}_m\|^2 P}{N_t}\right) \quad (17)$$

Open Science Index, Information and Communication Engineering Vol:4, No:1, 2010 publications.waset.org/11021/pdf

Open Science Index, Information and Communication Engineering Vol:4, No:1, 2010 publications.waset.org/11021/pdf

For identical main channel and eavesdropper channel, the capacity equations become

$$C_M = \frac{1}{2}\log\left(1 + N_t h^2 P\right) \tag{18}$$

$$C_W = \frac{1}{2}\log\left(1 + g^2 P\right) \tag{19}$$

Only the main channel capacity is increased due to its channel knowledge at the transmitter.

Now we focus on the secrecy capacity which is the maximum transmission rate at which the eavesdropper is unable to decode any information. If both the main channel and the wiretap channel are additive white Gaussian noise (AWGN) channels, and the latter has less capacity than the former, the secrecy capacity is equal to the difference between the two channel capacities [2].

Positive secrecy capacity indicates successful secret communication and the secrecy capacity is defined as the difference between main channel and eavesdropper channel capacities. In the MIMO Gaussian wire-tap channel the practical assumption is that the main channel state information is known and the eavesdropper channel information is unknown to the transmitter. In this scenerio, the secrecy capacity can be written from the eqns. 18-19.

$$\begin{aligned} C_S &= C_M - C_W \\ &= \frac{1}{2}\log\left(1 + N_t h^2 P\right) - \frac{1}{2}\log\left(1 + g^2 P\right) \\ &= \frac{1}{2}\log\frac{\left(1 + N_t \mathbf{h}^\dagger \Sigma_1^{-1} \mathbf{h} P\right)}{\left(1 + (\mathbf{Gh})^\dagger (\mathbf{G}\Sigma_1\mathbf{G}^\dagger + \Sigma_2)^{-1}\mathbf{Gh}P\right)} \end{aligned} \tag{20}$$

Considering $\Sigma_1 = \sigma_1^2 \mathbf{I}_{N_r}$ and $\Sigma_2 = \sigma_2^2 \mathbf{I}_{M_r}$, eq. 20 is rewritten as

$$C_S = \frac{1}{2}\log\frac{\left(1 + N_t \mathbf{h}^\dagger (\sigma_1^2 \mathbf{I}_{N_r})^{-1} \mathbf{h} P\right)}{\left(1 + (\mathbf{Gh})^\dagger (\mathbf{G}(\sigma_1^2 \mathbf{I}_{N_r})\mathbf{G}^\dagger + \sigma_2^2 \mathbf{I}_{M_r})^{-1}\mathbf{Gh}P\right)} \tag{21}$$

Considering **G** is unitary [8], the eq. 21 becomes

$$C_S = \frac{1}{2}\log\frac{\left(1 + N_t \frac{\|\mathbf{h}\|^2}{\sigma_1^2} P\right)}{\left(1 + \frac{\|\mathbf{h}\|^2}{\sigma_1^2 + \sigma_2^2} P\right)} \tag{22}$$

Taking $\frac{P}{\sigma_1^2} = \text{SNR}$ we get

$$C_S = \frac{1}{2}\log\frac{\left(1 + N_t \|\mathbf{h}\|^2 \text{SNR}\right)}{\left(1 + \frac{\sigma_1^2 \|\mathbf{h}\|^2}{\sigma_1^2 + \sigma_2^2} \text{SNR}\right)} \tag{23}$$

From the equation 23, it can be shown that the secrecy capacity C_S becomes positive when $\frac{\sigma_1^2}{\sigma_1^2 + \sigma_2^2} < N_t$ or $\sigma_2^2 > \sigma_1^2(\frac{1 - N_t}{N_t})$.

V. Different issues and discussion

Secrecy capacity is the key term by which the confidential communication is properly explained. Therefore it is necessary to know the existence of secrecy capacity prior to confidential data transmission. Fading channel consideration with different fading levels is another issue that should be analyzed. Outage probability analysis using the secrecy capacity should also be discussed. In the following subsections, these issues are explained with findings.

A. Existence of secrecy capacity

From the previous section it is known that the secret communication is possible when the eavesdropper channel is noisy. It is also known that **n** and **w** in eq. 3 and eq. 4 are independent random vectors, each one of which are jointly Gaussian distributed with zero mean and non-singular covariance matrices Σ_1 and Σ_2 respectively. As $\Sigma_1 = \sigma_1^2 \mathbf{I}_{N_r}$ and $\Sigma_2 = \sigma_2^2 \mathbf{I}_{M_r}$, the probability distribution for σ_1^2 and σ_2^2 can be written as $Pr\{\sigma_1^2\} = \frac{1}{\sqrt{2\pi}} e^{-(\sigma_1^2)^2/2}$ and $Pr\{\sigma_2^2\} = \frac{1}{\sqrt{2\pi}} e^{-(\sigma_2^2)^2/2}$ respectively. It is noted that the secrecy capacity C_S becomes positive when $\sigma_2^2 > \sigma_1^2(\frac{1 - N_t}{N_t})$.

The probability of existence of a nonzero secrecy capacity where only the main channel is known is given by

$$\begin{aligned} \Pr\left(C_{S_3} > 0\right) &= \Pr\left[\sigma_2^2 > \sigma_1^2\left(\frac{1 - N_t}{N_t}\right)\right] \\ &= \frac{1}{\sqrt{2\pi}} \int_{\sigma_1^2\left(\frac{1 - N_t}{N_t}\right)}^{\infty} e^{-(\sigma_2^2)^2/2} d\sigma_2^2 \\ &= \frac{1}{2} erfc\left[\sigma_1^2\left(\frac{1 - N_t}{N_t}\right)\right] \end{aligned} \tag{24}$$

In this scenario, the probability for secret communication is more than 50% as $\frac{1 - N_t}{N_t}$ term becomes negative. The probability for secret communication is simulated over main channel noise power and is shown in Fig. 5. The result shows that probability of existence of a nonzero secrecy capacity increases with noise power as well as with diversity order.

B. Outage probability under slow fading

In contrast with the Gaussian wire-tap channel, the fading scenario doesn't require the average SNR of the main channel to be greater than the average SNR of the eavesdroppers channel for a strictly positive (outage) secrecy capacity. In the presence of fading there is always a finite probability that the instantaneous SNR of the main channel is higher than the instantaneous SNR of the eavesdroppers channel [9]. We now extend the idea of secrecy capacity to the case when the channel parameters are random but fixed for all time. In slow fading, **H** and **G** are random processes and the secrecy capacity is no longer deterministic but a random process itself. The random nature of the problem implies that the usual notions of secure communication are meaningless since the probability that the secrecy capacity drops below a given transmission rate R is positive.

Open Science Index, Information and Communication Engineering Vol:4, No:1, 2010 publications.waset.org/11021/pdf

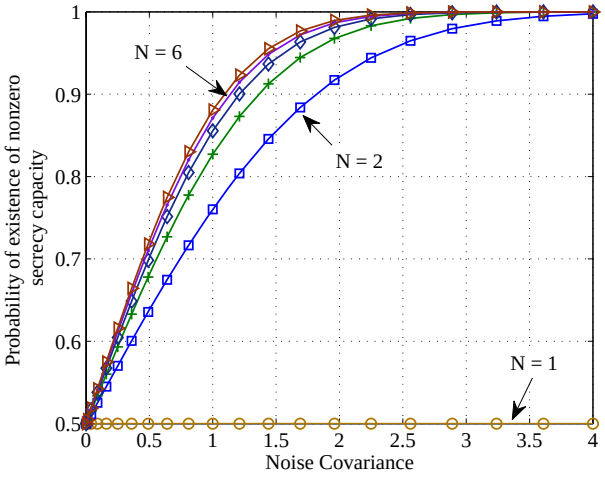


Fig. 5. Probability of existence of a nonzero secrecy capacity over main channel noise power, N = diversity order.

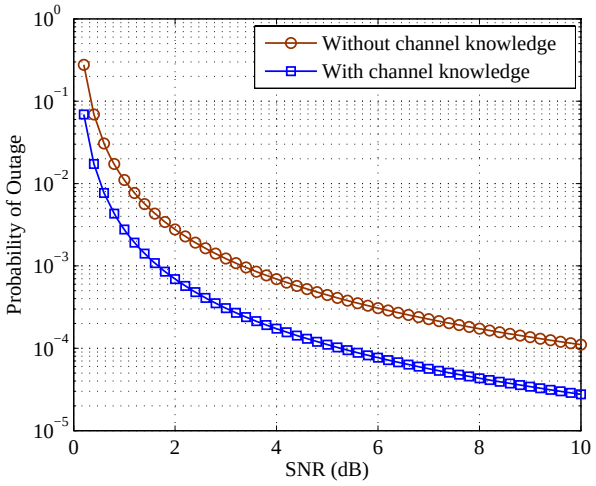


Fig. 6. Comparison between the outage probabilities whether the channel state information for the main channel is available or not

The outage probability in slow fading case is defined as the probability that the instantaneous secrecy capacity is less than a target secrecy rate $R > 0$.

For the channels where the transmitter has the main channel information, the probability of outage can be shown as

$$\begin{aligned} P_{out} &= \Pr\{C_S < R\} \\ &= \Pr\{\frac{1}{2}\log\frac{\left(1+N_t\|\mathbf{h}\|^2\text{SNR}\right)}{\left(1+\frac{\sigma_1^2\|\mathbf{h}\|^2}{\sigma_1^2+\sigma_2^2}\text{SNR}\right)} < R\} \end{aligned} \quad (25)$$

If the main channel is extremely noisy, we can take $\sigma_1^2 >> \sigma_2^2$ and the C_S becomes 0 for $N_t = 1$. In this case, the system is in outage with probability of 1. On the other hand, if the eavesdropper channel is extremely noisy then we can take $\sigma_1^2 << \sigma_2^2$ and the secrecy capacity C_{S_1} tends to $\frac{1}{2}\log\left(1+N_t\|\mathbf{h}\|^2\text{SNR}\right)$. Therefore eq. 25 reduces to

$$\begin{aligned} P_{out} &= \Pr\{\frac{1}{2}\log\left(1+N_t\|\mathbf{h}\|^2\text{SNR}\right) < R\} \\ &= \Pr\{\|\mathbf{h}\|^2 < \frac{2^{2R}-1}{N_t\text{SNR}}\} \end{aligned} \quad (26)$$

Under Rayleigh fading, $\|\mathbf{h}\|^2$ is χ^2- distributed with $2N_r$ degrees of freedom as $\|\mathbf{h}\|^2$ represents the sum of the squares of N_r independent Gaussian random variables. After some approximation [19] the outage probability can be written as follows

$$\begin{aligned} P_{out} &= \Pr\{\|\mathbf{h}\|^2 < \frac{2^{2R}-1}{N_t\text{SNR}}\} \\ &\approx \frac{(2^{2R}-1)^{N_r}}{N_r!\ (N_t\ \text{SNR})^{N_r}} \end{aligned} \quad (27)$$

The probability of outage where the transmitter has or has not the channel state information (CSI) of the main channel are compared and shown in Fig. 6. CSI for the eavesdropper channel has no effect on the outage probability as we consider **G** as unitary.

VI. Conclusion

In this paper, a MIMOME channel is considered where a transmitter communicates to a receiver in the presence of an eavesdropper. The transmitter, receiver and the eavesdropper are equipped with multiple antennas. A technique for determining the secrecy capacity of the MIMOME channel under Gaussian noise is proposed here. To do so, the MIMO Gaussian wire-tap channel is transformed into multiple SIMO Gaussian wire-tap channels and a scalar approach is used with some standard techniques of communications theory. Then the secrecy capacity equations are derived in the condition where only the main channel information is available to the transmitter. Several analysis regarding existence of secrecy capacity and probability of outage are taken. The result shows that the existence of secrecy capacity depends on the eavesdropper channel noise level and the probability of outage decreases with the channel state information. The future work of this paper is to analyze the system under fading environment.

References

[1] A. D. Wyner,"The wire-tap channel," *Bell Syst. Tech. J.*, 54(8):210, October 1975.
[2] S. K. Leung Yan Cheong and M. E. Hellman,"The Gaussian wire-tap channel," *IEEE Trans. on Information Theory,* 24(4):451-456, July 1978.
[3] U. M. Maurer,"Secret key agreement by public discussion from common information," *IEEE Trans. on Information Theory*, vol. 39, pp. 733742, May 1993.
[4] R. Ahlswede and I. Csiszar,"Common randomness in information theory and cryptography, part I: Secret sharing," *IEEE Trans. on Information Theory*, vol. 39, pp. 11211132, July 1993.
[5] I. Csiszar and J. Korner,"Broadcast channels with confidential messages," *IEEE Trans. on Information Theory,* 24(3):339-348, May 1978.
[6] I. E. Telatar,"Capacity of multi-antenna Gaussian channels," *European Trans. Telecommunications,* 10:585-595, November 1999.
[7] R. Negi and S. Goel,"Secret communication using artificial noise,"*IEEE Vehicular Technology Conference,* Toulouse, France, May 2006.

[8] P. Parada and R. Blahut,"Secrecy capacity of SIMO and slow fading channels," *IEEE International Symposium on Information Theory,* Adelaide, Australia, September 2005.
[9] J. Barros and M. Rodrigues,"Secrecy capacity of wireless channels," *IEEE International Symposium on Information Theory*, USA, 2006
[10] M. Bloch, J. Barros, M. Rodrigues and S. Mclaughlin,"Wireless information theoretic security," *IEEE Transactions on Information Theory,* vol. 54, no. 6, pp. 2515-2534, June 2008.
[11] S. Shafiee and S. Ulukus,"Achievable rates in Gaussian MISO channels with secrecy constraints," *In IEEE International Symposium on Information Theory,* Nice, France, June 2007.
[12] Z. Li, W. Trappe, and R. D. Yates,"Secret communication via multi antenna transmission," *41st Conference on Information Sciences and Systems,* Baltimore, MD, March 2007.
[13] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar,"On the Gaussian MIMO wiretap channel," *IEEE International Symposium on Information Theory,* Nice, France, June 2007.
[14] A. Khisti and G. Wornell,"Secure transmission with multiple antennas: The MISOME wiretap channel," *Submitted to IEEE Trans. on Information Theory*
[15] T. Cover and J. Thomas, *Elements of Information Theory* Wiley, 1991.
[16] R. A. Horn and C. R. Johnson, *Matrix Analysis,* Cambridge University Press, 1987.
[17] X. Li and E. P. Ratazzi,"MIMO transmissions with information theoretic secrecy for secret key agreement in wireless networks," *IEEE Military Communications Conference (MILCOM2005),* 2005. Atlantic City, NJ.
[18] X. Li, M. Chen, and E. P. Ratazzi,"Space time transmissions for wireless secret key agreement with information-theoretic secrecy," *IEEE International Workshop on Signal Processing Advances in Wireless Communications (SPAWC05),* 2005. The Italian Academy at Columbia University, New York.
[19] 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.
[20] S. Shafiee, N. Liu and S. Ulukus,"Secrecy Capacity of the 2-2-1 Gaussian MIMO Wire-tap Channel," *ISCCSP*, 2008
[21] A. Paulraj, R. Nabar, and D. Gore (2003) Introduction to Space-Time Wireless Communications, Cambridge, U.K.: Cambridge Univ. Press

Open Science Index, Information and Communication Engineering Vol:4, No:1, 2010 publications.waset.org/11021/pdf