# Sensitivity of the Secrecy Capacity of a Wiretap Channel to the Channel Gains with Imperfect Channel Information

Mahboobeh Sedighizad, Hamid G. Bafghi, Babak Seyfe

***Abstract*—In this paper, the impact of a small variations in the channel gains on the secrecy rate of the wiretap channel is studied, in which it is assumed that the imperfect channel knowledge is available at the transmitter. First, we consider general additive noise model for both legitimate and eavesdropper channels in the wiretap channel, and compute the variation of the secrecy rate resulting from the small variations in the channel gains. Then, we focus on the Gaussian wiretap channel, as a special case and calculate the sensitivity of the secrecy capacity to the channel gains with imperfect channel knowledge. Interestingly, it is shown that in some situations the effect of the channel variation on the secrecy capacity can be canceled out.**

***Index Terms*—Imperfect channel information, mutual information variation, secrecy capacity, wiretap channel.**

## I. Introduction

Secure communications over the wireless medium has attracted considerable attentions in recent years [1]–[5]. Wiretap channel model, consisting of three terminals: a transmitter which generates the channel input $X$, an intended receiver which observes the channel output $Y$, and an eavesdropper which observes the channel output $Z$, is a fundamental model for studying the security problem over the channels [6]–[13]. A basic principle coding, namely *Random Coding* is introduced by Wyner [6] which achieves the secure capacity for the wiretap channel. This coding is based on the fact that the eavesdropper is not able to decode any information more than its channel capacity.

The Multiple Input-Multiple Output (MIMO) wiretap channel with additive Gaussian noise are studied in [7]–[10]. The case of broadcast channel with a confidential message is studied by [12], and the secrecy in the cognitive model based on the wiretap channel is studied by [5], [13], [14]. In all these works, it is implicitly assumed that the transmitter who wishes to keep its message secure at the unintended receiver, has access to the information of the channel at the legitimate and unintended receivers, perfectly. Then, using the random coding, the information leakage to the eavesdropper is canceled out. But, this assumption, seems a little ideal in the applications. Recently, some attempts are taken place on the capacity of the wiretap channel with imperfect knowledge of the channel information [15]–[17]. Reference [17] studies the impact of the imperfect channel estimation on the secrecy performance of a Single-Input Multiple-Output Multiple antenna Eavesdropper (SIMOME) wiretap channel, and then a closed form solution of secrecy outage probability is derived.

In this paper, we study the case of the wiretap channel when the imperfect channel information is available at the transmitter, which causes some variations in the secrecy rate of the wiretap channel. This model is motivated by the wiretap channel in which the transmitter estimates the gains of the main and the wiretap channels with some errors.

First, we consider a general wiretap channel with additive noise, in which the distribution of the noises of the legitimate and eavesdropper channels are not restricted to be Gaussian. For this model, a general expression for the variation of the secrecy rate caused by small variations in the channel gains is derived. To find such a general expression, we use a recently introduced notion of the mutual information variation in [11], which enables us to compute the variation of the mutual information, resulting from a small variation in its arguments. Then, we specialized our result to the Gaussian wiretap channel and calculate the sensitivity of the secrecy capacity to the channel gains with imperfect channel information. It is shown that for some values of the system parameters, the variation of the secrecy capacity induced by the variation of the channel gains will be canceled out.

The rest of the paper is organized as follows. In Section II, we introduce the problem formulation and the notion of the mutual information variation. In Section III, we derive the secrecy rate variation due to the variation in the channel gains in an arbitrary but fixed distributed additive noise wiretap channel. In Section IV, we specialized our result to the Gaussian wiretap channel and fading wiretap channels, where we find the sensitivity of the secrecy capacity to the legitimate and eavesdropper channel gains. The paper is concluded in Section V.

## II. Channel Model and Preliminaries

### A. Channel Model

Consider a wiretap channel shown in Fig. 1. The input-outputs relations of this channel at time instant $t$ are given by

$$Y(t) = h_r(t)X(t) + W_r(t), \quad (1)$$

$$Z(t) = h_e(t)X(t) + W_e(t), \quad (2)$$

Mahboobeh Sedighizad and Babak Seyfe are with the Information Theoretic Learning System Lab. (ITLSL), Department of Electrical Engineering, Shahed University, Tehran, Iran. All the authors are with the Information Systems and Security Lab. (ISSL), Deptartment of Electrical Engineering, Sharif University of Technology, Tehran, Iran. Emails: {m.sedighizad, Seyfe}@shahed.ac.ir, h.bafghi@staff.sharif.edu.

978-1-5090-4784-0/17/$31.00 ©2017 IEEE

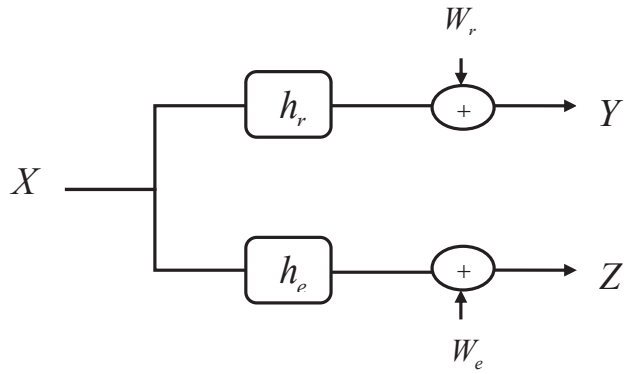


Fig. 1. Channel model: Wiretap channel.

where $h_r(t)$ and $h_e(t)$ are the channel gains associated with the legitimate and eavesdropper channels respectively, which are assumed to be fixed during each transmission. The channel input $X(t)$ is power constrained as $\mathrm{E}\left\{X^2(t)\right\} \leq P$, and the additive noise $W_r(t)$ and $W_e(t)$ are arbitrarily distributed random variables and are independent across the time index $t$. $Y(t)$ and $Z(t)$ are the legitimate and eavesdropper channels outputs, respectively.

### B. Mutual Information Variation

Now, we use the notion of the mutual information variation resulting from a small variation in its argument, given in [11], for the system model

$$Y = hX + W, \tag{3}$$

to calculate the mutual information variation caused by small changes in the channel gain. In this model, $X$, $h$ and $Y$ are the channel input, channel gain and channel output, respectively, and $W$ is an arbitrary but fixed distributed additive noise. All random variables are assumed to be continuous.

*Lemma 1:* In a point-to-point channel with arbitrary but fixed distributed additive noise as (3), if a small variation occurs in the channel gain as $\hat{h} = h + \varepsilon$ then, the deviation in the channel rate $I(X;Y)$ can be derived as follows,

$$\begin{aligned} \Delta I &= I\left(X;\hat{Y}\right) - I\left(X;Y\right) \\ &= -\mathrm{E}_{X,Y}\left\{\varepsilon X \varphi_Y\left(Y\right)\right\} + o\left(\varepsilon\right), \end{aligned} \tag{4}$$

in which, $\varphi_Y(y)$ is the *Score Function* (SF) of the random variable $Y$ which is defined as log-derivative of its density [18], i.e.,

$$\varphi_Y\left(y\right) = \frac{\partial}{\partial y} \ln p_Y\left(y\right), \tag{5}$$

and for deterministic variable $\varepsilon$ we say that $r\left(\varepsilon\right) \triangleq o\left(\varepsilon\right)$, if $\lim\limits_{\varepsilon \to 0} \frac{r(\varepsilon)}{\varepsilon} = 0$.

*Proof:* The proof readily follows from [11, Theorem 2]. ■

## III. Secrecy Rate Variation in a General Additive Noise Wiretap Channel

Now, we want to investigate the impact of the variations in both legitimate and eavesdropper channel gains on the secrecy rate of the system model introduced by (1), (2). Toward this end, suppose that the channel gains vary from $h_r(t)$ and $h_e(t)$ to $\hat{h}_r(t) = h_r(t) + \varepsilon_r(t)$ and $\hat{h}_e(t) = h_e(t) + \varepsilon_e(t)$ respectively, where $\varepsilon_r(t)$ and $\varepsilon_e(t)$ are assumed to be small values which are fixed during each transmission. Hence, the transmitter expects that the channel input $X$ experiences the following system model,

$$\hat{Y} = \hat{h}_r X + W_r, \tag{6}$$

$$\hat{Z} = \hat{h}_e X + W_e, \tag{7}$$

in which, the time index $t$ is ignored for convenience. Substituting $\hat{h}_r$ and $\hat{h}_e$ in (6) and (7) we have,

$$\hat{Y} = Y + \varepsilon_r X, \tag{8}$$

$$\hat{Z} = Z + \varepsilon_e X. \tag{9}$$

On the other hand, the secrecy rate of a degraded wiretap channel can be written as [6]:

$$R_s = I(X;Y) - I(X;Z) \tag{10}$$

that for the new channel gains will be as,

$$\hat{R}_s = I(X;\hat{Y}) - I(X;\hat{Z}). \tag{11}$$

Now, the variation of the secrecy rate of a wiretap channel induced by small a variation in the channel gains with imperfect channel information can be found as,

$$\begin{aligned} \Delta R_s &= \hat{R}_s - R_s \\ &= \left(I(X;\hat{Y}) - I(X;Y)\right) - \left(I(X;\hat{Z}) - I(X;Z)\right) \\ &= \Delta I_r - \Delta I_e \\ &= -\mathrm{E}_{X,Y}\left\{\varepsilon_r X \varphi_Y\left(Y\right)\right\} + \mathrm{E}_{X,Z}\left\{\varepsilon_e X \varphi_Z\left(Z\right)\right\} \\ &\quad + o\left(\varepsilon_r\right) + o\left(\varepsilon_e\right) \end{aligned} \tag{12}$$

where, the last equality follows from Lemma 1, and $\varphi_Y(y)$ and $\varphi_Z(z)$ are the SFs of the random variables $Y$ and $Z$, respectively.

From (12) the sensitivity of the secrecy rate to the channel gains can be found as,

$$\frac{\partial R_s}{\partial h_r} = -\mathrm{E}_{X,Y}\left\{X \varphi_Y\left(Y\right)\right\} \tag{13}$$

and

$$\frac{\partial R_s}{\partial h_e} = \mathrm{E}_{X,Z}\left\{X \varphi_Z\left(Z\right)\right\} \tag{14}$$

which are obtained by $\varepsilon_e = 0$, $\varepsilon_r \to 0$ and $\varepsilon_r = 0$, $\varepsilon_e \to 0$, respectively.

Note that, equations (12), (13) and (14) hold for any additive noise wiretap channel. In the next section, we specialize this result for Gaussian wiretap channel and calculate the sensitivity of the secrecy capacity to the channel gains.

## IV. Secrecy Capacity Variation in Gaussian Wiretap Channel

Although the capacity of the degraded wiretap channel is derived by Wyner in his essential work [6], but the capacity of a general case of this channel is introduced in [12] as

$$C_s = \max_{p_{(u)}} (I(U;Y) - I(U;Z)). \tag{15}$$

where, $U$ is an auxiliary random variable with probability distribution $p_{(u)}$. Replacing $U = X$, the capacity of the degraded wiretap channel will be derived [19].

This result is derived by using the random coding which uses this fact that the eavesdropper cannot decode any information more than its channel capacity with low error probability. Moreover, it is implicitly assumed that the transmitter has access to both the channel gains, to use the random coding. In other words, the transmitter who wishes to keep its message to be confidential from the eavesdropper, must observe both channels to constructs its codes in random coding scheme. But, if the transmitter has access to imperfect versions of the channel knowledge, it cannot meet the capacity of the channel as (15). It means that the code construction at the transmitter suffers some deviation from the expected secrecy rate of the channel because of the imperfect channel estimations.

In this section, we first calculate the variation of the secrecy capacity of a Gaussian wiretap channel induced by the variation of the channel gains, where we assume that during each transmission the channel gains and their estimation errors are fixed. The obtained result is used to find the sensitivity of the secrecy capacity to the channel gains. Then, we consider the case in which the channel gains and their estimation errors are random variables and the average variation of the secrecy rate is studied.

### A. Gaussian Wiretap Channel with Imperfect Channel Knowledge

The capacity of a Gaussian wiretap channel can be obtained from

$$C_s = \max_{p_{(x)}} (I(X;Y) - I(X;Z)). \tag{16}$$

Let $X^* \sim p_X^*(x)$ be the capacity achieving input of this channel. Now, suppose that the channel gains vary from $h_r$ and $h_e$ to $\hat{h}_r$ and $\hat{h}_e$, respectively. Hence, in this situation the capacity can be written as,

$$\hat{C}_s = \max_{p_{(\hat{x})}} (I(\hat{X};\hat{Y}) - I(\hat{X};\hat{Z})). \tag{17}$$

On the other hand, since the channel is Gaussian the capacity achieving input distribution does not change. Hence, the variation of the secrecy capacity can be written as,

$$\begin{aligned} \Delta C_s &= I(X^*;\hat{Y}) - I(X^*;\hat{Z}) - (I(X^*;Y) - I(X^*;Z)) \\ &= \Delta I_r^* - \Delta I_e^* \end{aligned} \tag{18}$$

This equation has an explicit expression for the variation of the secrecy capacity in terms of the signal and noise statistics and channel gain variations which is given in the following Theorem.

*Theorem 1:* In a Gaussian wiretap channel with input-output relations described by (1) and (2), where, $W_r$ and $W_e$ are Gaussian zero mean random variables with variances $\sigma_r^2$ and $\sigma_e^2$, respectively and Gaussian input $X^* \sim \mathcal{N}(0,P)$ is the capacity achieving input, in which the transmitter has access to the imperfect channel knowledge, the variation in the secrecy capacity caused by the channel gains variations will be as follows,

$$\Delta C_s = \frac{h_r P}{h_r^2 P + \sigma_r^2}\varepsilon_r - \frac{h_e P}{h_e^2 P + \sigma_e^2}\varepsilon_e + o(\varepsilon_r) + o(\varepsilon_e). \tag{19}$$

*Proof:* Since, in the Gaussian case the input $X^* \sim \mathcal{N}(0,P)$ is the capacity achieving one, $\Delta I_r^*$ can be calculated as,

$$\begin{aligned} \Delta I_r^* &= -\varepsilon_r \mathrm{E}_{X^*,Y}\{X^* \varphi_Y(Y)\} + o(\varepsilon_r) \\ &= -\varepsilon_r \int\int p_{X^*,Y}(x^*,y) \left(\frac{\partial}{\partial y} \ln p_Y(y)\right) x^* dx^* dy \\ &\quad + o(\varepsilon_r) \\ &= -\varepsilon_r \int x^* p_X^*(x^*) \left(\int p_{Y|X^*}(y|x^*) \frac{\frac{\partial}{\partial y} p_Y(y)}{p_Y(y)} dy\right) dx^* \\ &\quad + o(\varepsilon_r) \\ &= -\varepsilon_r \int \frac{x^*}{\sqrt{2\pi P}} e^{-x^{*2}/2P} \\ &\quad \left(\int \frac{1}{\sqrt{2\pi\sigma_r^2}} e^{-(y-h_r x^*)^2/2\sigma_r^2} \frac{\frac{\partial}{\partial y} p_Y(y)}{p_Y(y)} dy\right) dx \\ &\quad + o(\varepsilon_r) \end{aligned} \tag{20}$$

Then, noting that

$$p_Y(y) = \frac{1}{\sqrt{2\pi\left(h_r^2 P + \sigma_r^2\right)}} e^{-y^2/2\left(h_r^2 P + \sigma_r^2\right)}, \tag{21}$$

and taking the derivative, we have

$$\frac{\partial}{\partial y} p_Y(y) = -p_Y(y)\left(\frac{y}{h_r^2 P + \sigma_r^2}\right). \tag{22}$$

Thus, we can write

$$\begin{aligned} \Delta I_r^* &= \varepsilon_r \int \frac{x^*}{\sqrt{2\pi P}} e^{-x^{*2}/2P} \\ &\quad \left(\int \frac{1}{\sqrt{2\pi\sigma_r^2}} e^{-(y-h_r x^*)^2/2\sigma_r^2} \frac{y}{h_r^2 P + \sigma_r^2} dy\right) dx^* \\ &\quad + o(\varepsilon_r) \\ &= \frac{\varepsilon_r h_r}{h_r^2 P + \sigma_r^2} \int \frac{x^{*2}}{\sqrt{2\pi P}} e^{-x^{*2}/2P} dx^* + o(\varepsilon_r) \\ &= \frac{h_r P}{h_r^2 P + \sigma_r^2}\varepsilon_r + o(\varepsilon_r) \end{aligned} \tag{23}$$

Similarly, for $\Delta I_e^*$ we have,

$$\Delta I_e^* = \frac{h_e P}{h_e^2 P + \sigma_e^2}\varepsilon_e + o(\varepsilon_e) \tag{24}$$

Substituting (23) and (24) in (18), we can finally obtain the result. ■

In what follows, we show that the secrecy capacity variation in (19) can be verified by direct calculation of the variation

in the secrecy capacity of a Gaussian wiretap channel caused by the small variations in the channel gains. The capacity of a Gaussian wiretap channel with channel gains $h_r$ and $h_e$ is [20],

$$C_s = \frac{1}{2}\log\left(1+\frac{h_r^2 P}{\sigma_r^2}\right) - \frac{1}{2}\log\left(1+\frac{h_e^2 P}{\sigma_e^2}\right) \tag{25}$$

If the channel gains vary to $\hat{h}_r$ and $\hat{h}_e$, then,

$$\hat{C}_s = \frac{1}{2}\log\left(1+\frac{\hat{h}_r^2 P}{\sigma_r^2}\right) - \frac{1}{2}\log\left(1+\frac{\hat{h}_e^2 P}{\sigma_e^2}\right) \tag{26}$$

Therefore, $\Delta C_s$ will be,

$$\begin{aligned}\Delta C_s &= \frac{1}{2}\log\left(\frac{1+\hat{h}_r^2 P/\sigma_r^2}{1+h_r^2 P/\sigma_r^2}\right) - \frac{1}{2}\log\left(\frac{1+\hat{h}_e^2 P/\sigma_e^2}{1+h_e^2 P/\sigma_e^2}\right)\\ &\overset{(a)}{=} \frac{1}{2}\left(\frac{1+\hat{h}_r^2 P/\sigma_r^2}{1+h_r^2 P/\sigma_r^2}-1\right) - \frac{1}{2}\left(\frac{1+\hat{h}_e^2 P/\sigma_e^2}{1+h_e^2 P/\sigma_e^2}-1\right)\\ &\quad + o(\varepsilon_r) + o(\varepsilon_e)\\ &= \frac{h_r P}{h_r^2 P+\sigma_r^2}\varepsilon_r - \frac{h_e P}{h_e^2 P+\sigma_e^2}\varepsilon_e + o(\varepsilon_r) + o(\varepsilon_e)\end{aligned} \tag{27}$$

where, in equality $(a)$ we have used $\log x = (x-1) - (1/2)(x-1)^2 + \cdots$ in the neighborhood of 1, and the last equality follows by substituting $\hat{h}_r = h_r + \varepsilon_r$ and $\hat{h}_e = h_e + \varepsilon_e$.

We can use equation (19) to obtain the sensitivity of the secrecy capacity of a Gaussian wiretap channel to the channel gains as,

$$\frac{\partial C_s}{\partial h_r} = \frac{h_r P}{h_r^2 P+\sigma_r^2} \tag{28}$$

and

$$\frac{\partial C_s}{\partial h_e} = -\frac{h_e P}{h_e^2 P+\sigma_e^2} \tag{29}$$

which are obtained by $\varepsilon_e = 0$, $\varepsilon_r \to 0$ and $\varepsilon_r = 0$, $\varepsilon_e \to 0$, respectively. Again, these results can be verified by taking the derivative of the secrecy capacity with respect to the channel gains, directly.

*Remark 1:* As it is known if the value of legitimate channel gain increases the secrecy capacity variation will be positive, where (28) quantifies this variation. On the other hand, by increasing the eavesdropper channel gain secrecy capacity variation will be negative which is quantified in (29).

Fig. 2 shows a schematic view of equation (19), where $\Delta C_s$ is plotted versus the ratio of $SNR$ at the legitimate receiver $\Omega_r = \frac{h_r^2 P}{\sigma_r^2}$ to the $SNR$ at eavesdropper receiver $\Omega_e = \frac{h_e^2 P}{\sigma_e^2}$, as $\Omega_r/\Omega_e$, and we assume that two last terms of the (19) are negligible. The channel gains variations are assumed to be arbitrary but fixed as indicated in the figure. As it can be seen from this figure, in $\Omega_r/\Omega_e = 0dB$ with $\varepsilon_r = \varepsilon_e$, $\Delta C_s$ will be zero. This means that, although the channel gains vary from those are available at the transmitter, the situation of both legitimate and eavesdropper channels are the same. Hence, based on equation (19) the effect of imperfect channel knowledge will be mitigated. For the case of $\varepsilon_r = 1$ and $\varepsilon_e = 0.1$, $\Delta C_s > 0$ and the channel capacity is underestimated. Whereas, for $\varepsilon_r = 0.5$ and $\varepsilon_e = 1.1$, the channel capacity is overestimated.

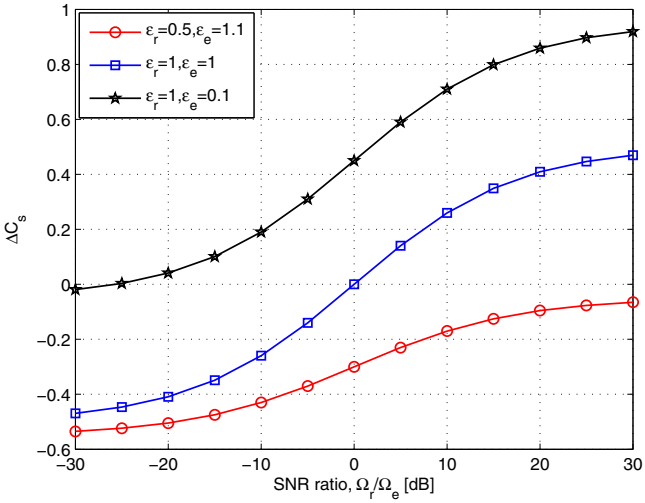


Fig. 2. $\Delta C_s$,versus the ratio of $SNR$ at the legitimate receiver to the $SNR$ at eavesdropper receiver, for the $h_r = h_e = 1$.

### *B. The Effect of Imperfect Knowledge of the Channel Fading Coefficients on the Secure Communication*

In this section, we study the impact of channel fading coefficients estimation error, on the average secrecy capacity of a fading channel. We assume that both the main channel (i.e., channel between the transmitter and legitimate receiver) and eavesdroppers channel experience fading channels. Let $h_r(t)$ and $h_e(t)$ denote the fading coefficients for the main and the eavesdroppers channel, respectively. Then, at any time instant $t$, the received signal at the legitimate receiver and eavesdropper can be written as

$$Y(t) = h_r(t)X(t) + W_r(t) \tag{30}$$

and

$$Z(t) = h_e(t)X(t) + W_e(t) \tag{31}$$

where, $W_r(t)$ and $W_e(t)$ are zero-mean Gaussian distributed noise of the legitimate and eavesdropper channels with variances $\sigma_r^2$ and $\sigma_e^2$, respectively.

In order to quantify the effect of the channel estimation error, we assume that both the legitimate and eavesdropper channel coefficients at any time instant $t$ are estimated with error according to the following models,

$$\hat{h}_r(t) = h_r(t) + \varepsilon_r(t) \tag{32}$$

and

$$\hat{h}_e(t) = h_e(t) + \varepsilon_e(t) \tag{33}$$

where, we assume that $h_r(t)$ and $h_e(t)$, are zero-mean Gaussian random variables with $\sigma_{h_r}^2$ and $\sigma_{h_e}^2$ as their variances, representing the legitimate and eavesdropper true fading channel coefficients at time instant $t$. Moreover, $\varepsilon_r(t)$ and $\varepsilon_e(t)$ are zero-mean Gaussian random variables with $\sigma_{\varepsilon_r}^2$ and $\sigma_{\varepsilon_e}^2$ as their variances which stand for the estimation errors of the legitimate and eavesdropper channels, respectively. We consider the correlation coefficient between the true channel

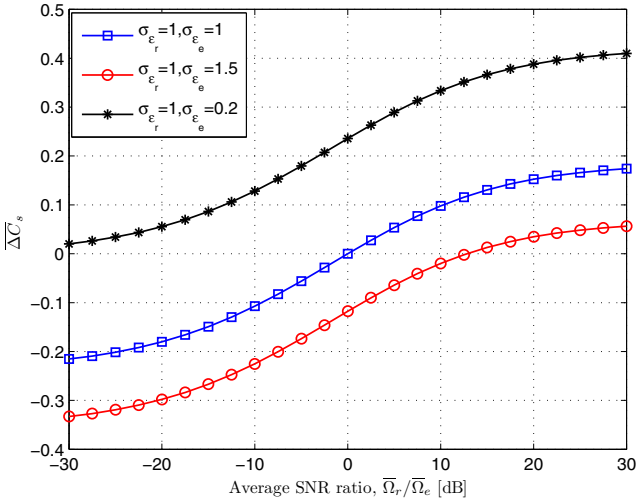


Fig. 3. $\overline{\Delta C}_s$,versus the ratio of average $SNR$ at the legitimate receiver to the average $SNR$ at eavesdropper receiver, for the $\rho_r = \rho_e = 0.7$.

coefficients and their estimates as $\rho_r$ and $\rho_e$. These coefficients belong to $[0, 1]$ and approach to 1 as the channel estimator becomes more accurate. As it can be seen from equation (30) and (31), at any time instant $t$, we have a Gaussian wiretap channel. Therefore, the secrecy capacity for one realization of the fading wiretap channel will be the same as a Gaussian wiretap channel. Hence, for any realization of the channel coefficients and channel estimation errors, similar to the equation (19) we will have,

$$\Delta C_s(t) = \frac{h_r(t)P}{h_r^2(t)P + \sigma_r^2}\varepsilon_r(t) - \frac{h_e(t)P}{h_e^2(t)P + \sigma_e^2}\varepsilon_e(t) + o(\varepsilon_r(t)) + o(\varepsilon_e(t)). \quad (34)$$

Taking the expectation over channel coefficients and estimation errors, we get

$$\overline{\Delta C}_s = \mathrm{E}_{h_r,h_e}\{\mathrm{E}_{\varepsilon_r,\varepsilon_e}\{\Delta C_s | h_r, h_e\}\} \quad (35)$$

Fig. 3 shows the average $\Delta C_s$, versus the ratio of average $SNR$ at legitimate receiver, $\overline{\Omega}_r = \frac{\mathrm{E}\{h_r^2\}P}{\sigma_r^2}$, to the average $SNR$ at eavesdropper receiver, $\overline{\Omega}_e = \frac{\mathrm{E}\{h_e^2\}P}{\sigma_e^2}$, where we assume that the two last terms of the equation (34) are negligible. It can be seen that, similar to the case of Gaussian channel, in $\overline{\Omega}_r/\overline{\Omega}_e = 0dB$ with $\sigma_{\varepsilon_r} = \sigma_{\varepsilon_e}$, $\overline{\Delta C}_s$ will be zero.

## V. Conclusion

In this paper, the impact of the channel gains variations on the secrecy rate of a general additive noise wiretap channel, with imperfect channel information at the transmitter, was studied. Then, the result was specialized for the Gaussian and fading wiretap channel, where the secrecy capacity variation expressed in terms of the system parameters. Consequently the sensitivity of the secrecy capacity to the channel gains was derived. The results were verified by direct analysis of the capacity of a Gaussian wiretap channel. It was shown that, for some values of the system parameters the variation of the secrecy capacity will be mitigated totally.

## References


[1] F. Renna, N. Laurenti, and H. V. Poor, "Physical-layer secrecy for OFDM transmissions over fading channels," *IEEE Trans. on Inf. Forens. and Security*, vol. 7, no. 4, pp. 1354–1367, 2012.

[2] E. C. Song, P. Cuff, and H. V. Poor, "A rate-distortion based secrecy system with side information at the decoders," in *52th Annual Allerton Conf. on Comm., Control, and Comp.*, Oct. 2014.

[3] E. C. Song and P. Cuff, "Secrecy is cheap if the adversary must reconstruct," in *IEEE International Symposium on Information Theory (ISIT)*, Jul. 2012, pp. 66–70.

[4] Y. Liang, H. Vincent Poor, and S. Shamai, *Information Theoretic Security*, Now Pub. Inc., 2009.

[5] H. G. Bafghi, M. Mirmohseni, B. Seyfe, and M. R. Aref, "On the secrecy of the cognitive interference channel with partial channel states," *Trans. on Emerging Telecom. Tech.*, vol. 27, no. 11, pp. 1472–1485, 2016.

[6] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[7] S. Shafiee and S. Ulukus, "Towards the secrecy capacity of the gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. on Inf. Theory*, vol. 55, no. 9, pp. 4033–4039, Sep. 2009.

[8] T. Liu and S. Shamai, "A note on the secrecy capacity of the multiple antenna wiretap channel," *IEEE Trans. on Inf. Theory*, vol. 55, no. 6, pp. 2547–2553, May. 2009.

[9] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," *IEEE Trans. on Inf. Theory*, vol. 57, no. 8, pp. 4961–4972, Aug. 2011.

[10] A. Khisti and G. W. Wornell, "Secure transmission with multiple antennas - part ii: The MIMO wiretap channel," *IEEE Trans. on Inf. Theory*, vol. 56, no. 11, pp. 5515–5532, Nov. 2010.

[11] M. Sedighizad and B. Seyfe, "A generalized expression for the gradient of the fundamental information measures," *Available at arXiv: 1607.05875v2[cs.IT]*, Feb. 2017.

[12] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[13] Y. Liang, A. Somekh-Baruch, H. Vincent Poor, S. Shamai, and S. Verdú, "Capacity of cognitive interference channels with and without secrecy," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–618, Feb. 2009.

[14] H. G. Bafghi, S. Salimi, B. Seyfe, and M. R. Aref, "Cognitive interference channel with two confidential messages," in *Int. Symp. on Inf. Theory and Applic. (ISITA)*, Taichung, Taiwan, 2010, pp. 952–956.

[15] Z. Rezki, B. Alomair, and M.-S. Alouini, "On the secrecy capacity of the miso wiretap channel under imperfect channel estimation," in *IEEE Global Comm. Conf. (GLOBECOM)*, Dec 2014, pp. 1602–1607.

[16] Z. Rezki, A. Khisti, and M.-S. Alouini, "On the secrecy capacity of the wiretap channel with imperfect main channel estimation," *IEEE Trans. on Comm.*, vol. 62, no. 10, pp. 3652–3664, Oct 2014.

[17] K. S. Ahn, S. W. Choi, and J. M. Ahn, "Secrecy performance of maximum ratio diversity with channel estimation error," *IEEE Sig. Proc. Letters*, vol. 22, no. 11, pp. 2167–2171, Nov. 2015.

[18] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, John Wiley and Sons, Inc., 2nd edition, 2006.

[19] A. El Gamal and Y.-H. Kim, *Network Information Theory*, Cambridge University Press, 2011.

[20] S. Leung-Yan-Cheong, "On a special class of wiretap channels," *IEEE Trans. on Inf. Theory*, vol. 23, no. 5, pp. 625–627, Sep. 1977.