

Analysis of Side Information Impact on the Coverage Region of Wireless Wiretap Channel

saeid pakravan (✉ saeidpak70@yahoo.com)

Ferdowsi University of Mashhad <https://orcid.org/0000-0003-4364-8280>

Ghosheh Abed Hodtani

Ferdowsi University of Mashhad

Research Article

Keywords: Fading wiretap channel, Secrecy capacity, Secrecy coverage region, Side information

Posted Date: June 7th, 2021

DOI: <https://doi.org/10.21203/rs.3.rs-510207/v1>

License:   This work is licensed under a Creative Commons Attribution 4.0 International License.

[Read Full License](#)

Analysis of Side Information Impact on the Coverage Region of Wireless Wiretap Channel

Saeid Pakravan, Ghosheh Abed Hodtani

Department of Electrical Engineering, Ferdowsi University of Mashhad, Mashhad, Iran

Email: Saeid.pakravan@mail.um.ac.ir, hodtani@um.ac.ir

Corresponding author: Ghosheh Abed Hodtani

Abstract—Analyzing wireless communication performances by using information-theoretic results is of practical importance. In this paper, first, an achievable secrecy rate region and an outer bound on the secrecy capacity region for the discrete alphabet and memoryless wiretap channel with side information non-causally known at the transmitter are obtained. Then, by extending the results to the continuous alphabet wireless wiretap channel and by deriving a closed-form expression on the secrecy coverage region (SCR), as a remarkable wireless performance factor, impact of side information on the SCR is analyzed and it is shown that side information increases the SCR as expected intuitively. Numerical evaluation of theoretical results is done finally.

Keywords- Fading wiretap channel, Secrecy capacity, Secrecy coverage region, Side information.

I. INTRODUCTION

Due to the increasing using wireless communication systems, there are many challenges on the security situations of these networks. Security is usually considered as the upper layer in communication systems, and due to the limited computational capabilities, cryptographic algorithms have been used to implement it [1]. Nevertheless, this supposition may not be accurate owing to the expansion in computational procedures resulting in opening encryption algorithms. Therefore, physical layer security as a branch of theoretical information security is

responsible for establishing secure communication against non-permissible accesses. The issue of physical layer security was first reported using Shannon in 1949 [2]. Shannon studied the secure communication and demonstrated that it was possible to achieve this secure communication with a secret key shared between the transmitter and the receiver when the entropy of key is greater than or equal to the entropy of the message to be transmitted. In [3], Wyner studied the degraded wiretap channel (WC) and showed that secure transmission is possible even in the absence of a secret key; the WC is a type of channels in communication systems that a transmitter sends a message to a legitimate receiver while the message is kept secret from an eavesdropper. In this work, secrecy capacity (SC) has been defined as the maximum information rate of the main channel (transmitter-to-legitimate receiver) with the complete uninformed at the eavesdropper and it has been demonstrated by assuming that the eavesdropper channel (transmitter- to-eavesdropper) is a degraded interpretation of the main channel, a affirmative information rate can be obtained. Later, the author's in [4] generalized results of [3] to the general BC (not necessarily degraded) with confidential messages and established the SC. The authors in [5] generalized the results of [3] to the Gaussian version. Some other researchers have been analyzed the importance of secrecy efficiency measures over several fading channels, such as [6-13], etc.

Shannon studied channels with side information (SI) and found the capacity of the single-user channel when causal SI is available at the transmitter [14]. Single user channel, when non-causal SI is available only at the transmitter, was studied in [15]. The results of [14] has been generalized to the case where non-causal SI is available at both transmitter and receiver in [16]. The Gaussian versions of [15] were studied in [17] and [18]. Recently, this concept was demonstrated for the WC. Several works have been done upon this set of channels as [19-22]. In [19] an achievable rate equivocation region for the discrete memoryless WC with respect to

SI is presented and also the achieved results are generalized to the Gaussian case. In [20] a lower bound on the SC of the WC with SI available causally at both the encoder and decoder has been established. In [21] an achievable rate equivocation region for a WC (not necessarily degraded) with two-sided channel SI available at the transmitter and the legitimate receiver was established. In [22] it is illustrated how SI and interference affect secret communications.

Our work. Information-theoretic analysis of the communication systems performances is of practical and theoretical importance. For wireless WC with non-causal SI at the transmitter, first, (i) we derive the SC; then, (ii) the coverage region, as a fundamental wireless communication performance, not analyzed before for our intended channel, is investigated. Specifically, we study the effect of SI on the secrecy coverage region (SCR) of the Rayleigh fading WC by finding expressions in terms of infinite series, and eventually compare the achieved results with the case without SI.

The remaining parts of this paper are formed as follows. The system model is presented in Section II. In Section III, SC for the wireless WC with considering SI available at the transmitter is provided, and then, the SCR of this case is investigated. Numerical results for illustrating the impact of SI on the coverage region is studied in Section VI. Finally, we conclude the paper in Section V.

Notations: It has been used from upper case and lower case letters for the random variables (RVs) and realization of RVs, respectively. Also, the alphabet set is denoted with calligraphic letters. $\text{Max min } \{\cdot\}$ represents maximizing the minimization of a function.

II. CHANNEL MODEL AND DEFINITIONS

The channel model and also some basic necessary definitions that we are going to work upon have been characterized in this section. A wireless channel is studied here, where a transmitter

needs to send a confidential message to a legitimate receiver while the eavesdropper is trying to decode the message from its received signal by knowing the SI known in the transmitter as depicted in Fig. 1.

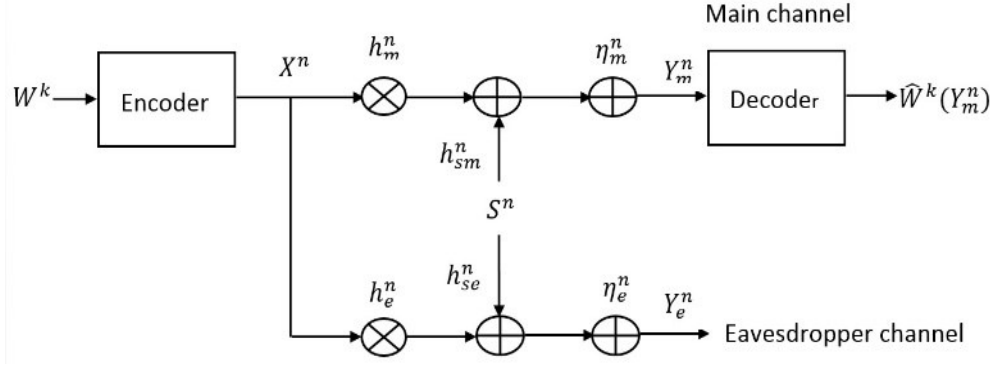


Fig. 1. An uncorrelated Rayleigh fading WC.

Let \mathcal{X} be the input set, \mathcal{Y}_m be the output set of legitimate receiver, \mathcal{Y}_e be the output set of eavesdropper and \mathcal{S} be finite set that denotes SI in the transmitter. The SI is non-causally known at the encoder and S_i , $1 \leq i \leq n$, are independently and identically distributed (i.i.d.) $\sim p(s)$. We want to forward a message $W^k \in \{1, 2, \dots, M\}$ to the legitimate receiver in n uses of the channel. Due to the W^k and S^n , the encoder forwards a codeword X^n to the main channel. Upon obtaining of Y_m^n the decoder at the legitimate receiver creates an estimate $\hat{W}^k(Y_m^n)$ of the message W^k . The corresponding output at the eavesdropper is Y_e^n . So, the received signals in Rayleigh fading WC by considering legitimate receiver as $Y_m(i)$ and eavesdropper as $Y_e(i)$ can be specified as follows:

$$Y_m(i) = h_m(i)X(i) + h_{sm}(i)S(i) + \eta_m(i), \quad (1)$$

$$Y_e(i) = h_e(i)X(i) + h_{se}(i)S(i) + \eta_e(i), i = 1, \dots, n \quad (2)$$

where n is the length of the transmitted signal, $\eta_m(i)$ and $\eta_e(i)$ are i.i.d. additive white Gaussian noise (AWGN) with zero mean and variances N_m and N_e respectively. The channels

between the transmitter to legitimate receiver, and transmitter to eavesdropper have fading coefficients, indicated by h_m and h_e , respectively. The information S is received by legitimate receiver and eavesdropper through h_{sm} and h_{se} coefficients respectively, which are necessarily not equal to h_m or h_e . To consider a Rayleigh fading scenario, all received signals are assumed to be attenuated by a Rayleigh fading channel coefficients which are constant during a transmission block (block fading) and they are known in all transmitter and receivers. So they are fixed in each block (i.e., $h_m(i) = h_m$, $h_{sm}(i) = h_{sm}$, $h_{se}(i) = h_{se}$ and $h_e(i) = h_e$, $\forall i = 1, \dots, n$), and vary randomly from one block to another block. This concept means that the channel power gains (i.e., $g_m(i) = |h_m(i)|^2$, $g_{sm}(i) = |h_{sm}(i)|^2$, $g_{se}(i) = |h_{se}(i)|^2$ and $g_e(i) = |h_e(i)|^2$) are distributed exponentially, where the fading processes are uncorrelated. Moreover, it has been supposed that the codewords forward by transmitter over the channels are constrained to the average power limitation as:

$$\frac{1}{n} \sum_{i=1}^n E\{|X_i|^2\} \leq P, \quad (3)$$

where the average power of the transmission signal is displayed with P . The instantaneous SNR at legitimate receiver and eavesdropper when there is not any SI at the transmitter are respectively specified as $\gamma_m(i) = \frac{P|h_m(i)|^2}{N_m} = \frac{P|h_m|^2}{N_m} = \gamma_m$ and $\gamma_e(i) = \frac{P|h_e(i)|^2}{N_e} = \frac{P|h_e|^2}{N_e} = \gamma_e$; and the average SNR at legitimate receiver and eavesdropper are respectively given as $\overline{\gamma}_m(i) = \frac{PE[|h_m(i)|^2]}{N_m} = \frac{PE[|h_m|^2]}{N_m} = \overline{\gamma}_m$ and $\overline{\gamma}_e(i) = \frac{PE[|h_e(i)|^2]}{N_e} = \frac{PE[|h_e|^2]}{N_e} = \overline{\gamma}_e$. Since in the quasi-static case h_m and h_e are random but remain constant for all time, it is entirely appropriate to see the main channel and the eavesdropper's channel as a complex AWGN channel with SNRs $\gamma_m = \frac{P|h_m|^2}{N_m}$ and $\gamma_e = \frac{P|h_e|^2}{N_e}$ respectively. It is as well as advantageous to bring up the probability density function of γ_m and γ_e . Since the channel fading coefficients h are zero-mean complex

Gaussian RVs and the instantaneous SNR $\gamma \propto |h|^2$, it follows that γ is distributed exponentially, in particular $f(\gamma_m) = \frac{1}{\bar{\gamma}_m} \exp\left(-\frac{\gamma_m}{\bar{\gamma}_m}\right)$, and $f(\gamma_e) = \frac{1}{\bar{\gamma}_e} \exp\left(-\frac{\gamma_e}{\bar{\gamma}_e}\right)$. In considered system model, the transmission rate between transmitter and legitimate receiver is indicated as $R = \frac{H(M)}{n}$. The equivocation rate of eavesdropper that illustrates the secrecy level of confidential messages versus eavesdropper is characterized as $R_e = \frac{1}{n} H(W|Z^n)$. Also, we define average probability of error as follows.

$$P_e^{avg} \triangleq \frac{1}{M} \sum_{i=1}^n \Pr(\hat{W}^k(Y_m^n) \neq i | W^k = i), \quad (4)$$

where $\hat{W}^k(Y_m^n)$ denotes estimated messages by legitimate receiver. The secrecy rate R_s is defined to be achievable, if there exists a code $(2^{nR_s}, n)$ so that for all $\epsilon \geq 0$ and sufficiently large n , $P_e^{avg} \leq \epsilon$ and $R_e \geq R_s - \epsilon$, where, R_e and P_e^{avg} have been defined before this. The SC C_s can be defined as

$$C_s = \sup_{P_e^{avg} \leq \epsilon} R_s. \quad (5)$$

In our paper, we assume that SI exists at the transmitter and define $\gamma_{sm}(i) = \frac{Q|h_{sm}(i)|^2}{N_m} = \frac{Q|h_{sm}|^2}{N_m} = \gamma_{sm}$, $\overline{\gamma_{sm}}(i) = \frac{QE[|h_{sm}(i)|^2]}{N_m} = \frac{QE[|h_{sm}|^2]}{N_m} = \overline{\gamma_{sm}}$, $\gamma_{se}(i) = \frac{Q|h_{se}(i)|^2}{N_e} = \frac{Q|h_{se}|^2}{N_e} = \gamma_{se}$, and $\overline{\gamma_{se}}(i) = \frac{QE[|h_{se}(i)|^2]}{N_e} = \frac{QE[|h_{se}|^2]}{N_e} = \overline{\gamma_{se}}$. We have following marginal distributions for $\gamma_{sm} > 0$ and $\gamma_{se} > 0$, respectively as $f(\gamma_{sm}) = \frac{1}{\bar{\gamma}_{sm}} \exp\left(-\frac{\gamma_{sm}}{\bar{\gamma}_{sm}}\right)$, and $f(\gamma_{se}) = \frac{1}{\bar{\gamma}_{se}} \exp\left(-\frac{\gamma_{se}}{\bar{\gamma}_{se}}\right)$.

Note that the Gaussian WC with SI is an expansion of the dirty paper channel by an eavesdropper. Using an analogous approach of writing on dirty paper, we will have the following communication problem: the transmitter wants to forward a secret message to a receiver and he knows existing of an eavesdropper along the way to the legitimate receiver, the paper obtains the desired distribution dirt; also, it is assumed that eavesdropper has access to

the paper and its distribution. Now the question of our interest is: how much is the SI effect on the coverage region of the wireless WC?

III. MAIN RESULTS

In this section, firstly, for the channel defined in the previous section, related works on SC are presented. Then, (i) an achievable secrecy rate region and an outer bound on the SC region, (ii) extension of the discrete alphabet results to the continuous alphabet wireless WC, iii) the impact of SI at transmitter over SCR are analyzed.

A. Related works

The discrete memoryless lower bound on SC for WC with considering SI at the transmitter has been demonstrated in [19], as:

$$R_s^{low} = \max_{U \rightarrow (X,S) \rightarrow Y_m \rightarrow Y_e} I(U; Y_m) - \max\{I(U; S), I(U; Y_e)\}, \quad (6)$$

and

$$R_s^{up} = \min\{C_m, \max_{U \rightarrow (X,S) \rightarrow Y_m \rightarrow Y_e} [I(U; Y_m) - I(U; Y_e)]\}, \quad (7)$$

where U is auxiliary RV such that $U \rightarrow (X, S) \rightarrow Y_m \rightarrow Y_e$ forms a Markov chain. Also, C_m is the capacity of the main channel with considering SI and it is defined as:

$$C_m = \max_{U \rightarrow (X,S) \rightarrow Y_m \rightarrow Y_e} [I(U; Y_m) - I(U; S)]. \quad (8)$$

Corollary 1. If there exists an auxiliary parameter U_m such that

1. $U_m \rightarrow (X, S) \rightarrow Y_m \rightarrow Y_e$ forms a Markov chain,
2. $I(U_m; Y_m) - I(U_m; S) = C_m$,
3. $I(U_m; S) \geq I(U_m; Y_e)$,

then, for the discrete memoryless WC with SI, the SC C_s is equal to C_m .

Corollary 2. If there exists an auxiliary parameter U_e such that

1. $U_e \rightarrow (X, S) \rightarrow Y_m \rightarrow Y_e$ forms a Markov chain,
2. $I(U_e; Y_m) - I(U_e; Y_e) = R_{e_s}$,
3. $I(U_e; Y_e) \geq I(U_e; S)$,

then, for the discrete memoryless WC with SI, the SC C_s is equal to R_{e_s} .

Lemma 1. The conditions for the above corollaries 1 and 2 are explicitly determined based on the system model parameters as

$$I(U; S) \geq I(U; Y_e) \leftrightarrow \alpha \geq \alpha_0 \text{ or } \alpha \leq \alpha_{-0},$$

$$I(U; Y_e) \geq I(U; S) \leftrightarrow \alpha_{-0} \leq \alpha \leq \alpha_0,$$

where $\alpha_0 = \left(1 - \frac{N_e}{P+N_e}\right) \left(1 + \sqrt{1 + \frac{P+N_e}{Q}}\right)$, and $\alpha_{-0} = \left(1 - \frac{N_e}{P+N_e}\right) \left(1 - \sqrt{1 + \frac{P+N_e}{Q}}\right)$.

Proof. The details of proof are in [19].

Now, suppose that both the main and the WC are complex AWGN channels, i.e. transmit and receive symbols are complex and both zero mean circularly symmetric complex Gaussians. We consider complex fading coefficients for both the main channel and the eavesdropper's channel, as detailed in Section II.

B. Secrecy capacity of the wireless wiretap channel

In this sub-section, we derive SC of the wireless wiretap channel with SI at the transmitter. According to the system model illustrated in section II and results in corollaries 1 and 2 the following theorem provide SC for the wireless WC with SI.

Theorem 1: The SC C_s of the wireless WC with SI at the transmitter, and fading coefficients satisfying the above Corollaries 1 and 2 in section A is given as follows

$$C_s = \begin{cases} \log(1 + \gamma_m) & , \quad \text{Corollary 1} \\ \left[\log\left(\frac{1 + \gamma_m + \gamma_{sm}}{1 + \gamma_e + \gamma_{se}}\right) \right]^+ & , \quad \text{Corollary 2} \end{cases} \quad (9)$$

where $[x]^+ = \max(0, x)$.

Proof. See Appendix A.

C. SCR analyse

The coverage region meaning has been reported for point-to-point channel and has been extended to the relay channel in [24] and [25] respectively. By considering fixed distance between the transmitter and receiver (and also eavesdropper), the path-loss effect is added to the SNRs. Thus, computing the ergodic rates (that depend on the distances) results in computing the coverage region. In our proposed system model, for clarity and without loss of generality, we suppose that transmitter is located at (0,0). In this sub-section, without loss of generality we assumed that $h_{sm} = h_{se} = 1$. So, we define the SCR for uncorrelated fading WC with considering SI at the transmitter as a geographic region at which the secrecy rate of at least $R_s > 0$, is guaranteed, i.e.,

$$\mathcal{G}(d_m, d_e) \stackrel{\text{def}}{=} \{d_m, d_e: C_s(d_m, d_e) > R_s\}, \quad (10)$$

where, from theorem 1, with Corollaries 1 and 2 respectively we have $C_s(d_m, d_e) =$

$$E_{\gamma_m}[\log(1 + \frac{\gamma_m}{d_m^\alpha})] \text{ and } C_s(d_m, d_e) = E_{\gamma_m, \gamma_e, \gamma_{sm}, \gamma_{se}}[\log\left(\frac{1 + \frac{\gamma_m}{d_m^\alpha} + \gamma_{sm}}{1 + \frac{\gamma_e}{d_e^\alpha} + \gamma_{se}}\right)] \text{ that denotes the average}$$

SC when legitimate receiver and eavesdropper are located at d_m and d_e , respectively.

Therefore, the SCR can be derived as the following theorem.

Theorem 2. The SCR for concerned uncorrelated Rayleigh fading WC where SI is available at the transmitter with defined parameters $\overline{\gamma_m}$, $\overline{\gamma_e}$, $\overline{\gamma_{sm}}$, $\overline{\gamma_{se}}$, α ($\alpha > 2$ is the path loss exponent) and R_s , is given by

For Corollary 1:

$$d_m \leq \left(\frac{\pi^2 \overline{\gamma_m}}{\pi^2 - 16} \ln\left(\frac{2R_s}{\sqrt{\pi}}\right) \right)^{\frac{1}{\alpha}}. \quad (11)$$

In this case we don't have any limitation over d_e that means there isn't any minimum distance between transmitter and eavesdropper in order to guarantee secure communication.

For Corollary 2:

$$d_m \leq \left(\frac{\pi^2 \bar{\gamma}_m}{\pi^2 - 16} \ln \left(\frac{2R_s}{\sqrt{\pi}} \right) \right)^{\frac{1}{\alpha}}, \quad (12a)$$

$$\begin{aligned} R_s \leq & \frac{\sqrt{\pi}}{2} \left[\left(\frac{1}{1 - \frac{\bar{\gamma}_m}{\bar{\gamma}_{sm} d_m^\alpha}} - \frac{1}{\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{sm} d_m^\alpha}} \right) e^{\left(\frac{1 - \frac{16}{\pi^2}}{\bar{\gamma}_{sm}} \right)} + \frac{e^{d_m^\alpha \left(\frac{1 - \frac{16}{\pi^2}}{\bar{\gamma}_m} \right)}}{1 - \frac{\bar{\gamma}_{sm}}{\bar{\gamma}_m} d_m^\alpha} + \left(\frac{1}{\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{sm} d_m^\alpha}} - \right. \right. \\ & \left. \frac{1}{\frac{\bar{\gamma}_m}{\bar{\gamma}_e} + 1} \right) e^{d_m^\alpha \left(1 - \frac{16}{\pi^2} \right) \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} \right)} - e^{\left(\frac{1 - \frac{16}{\pi^2}}{\bar{\gamma}_{se}} \right)} + \left(\frac{1}{1 - \frac{\bar{\gamma}_e}{\bar{\gamma}_{se} d_e^\alpha}} - \frac{1}{1 + \frac{\bar{\gamma}_e}{\bar{\gamma}_m}} \right) e^{d_e^\alpha \left(1 - \frac{16}{\pi^2} \right) \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} \right)} - \\ & \left. \left(\frac{1}{1 - \frac{\bar{\gamma}_e}{\bar{\gamma}_{se} d_e^\alpha}} \right) \left(\frac{1}{1 - \frac{\bar{\gamma}_m}{\bar{\gamma}_e} + \frac{\bar{\gamma}_m}{\bar{\gamma}_{se} d_e^\alpha}} \right) e^{d_e^\alpha \left(1 - \frac{16}{\pi^2} \right) \left(\frac{1}{\bar{\gamma}_m} - \frac{1}{\bar{\gamma}_e} + \frac{1}{\bar{\gamma}_{se} d_e^\alpha} \right)} \right]. \quad (12b) \end{aligned}$$

Proof. See Appendix B.

IV. NUMERICAL RESULTS

In this section, the numerical results are presented for the SCR to study how the SI affects the coverage region. The results for the WCs satisfying Corollary 1 are omitted for simplicity and only, we illustrate the results for wireless WCs satisfying Corollary 2 conditions. The SCR for different scenarios is provided in Fig. 2. From analyzing the impact of SI, as it has been depicted in Fig. 2, it is clearly seen that existence of this factor increases the possible distance between legitimate receiver and legitimate transmitter for a given d_e . Furthermore, it is shown that SI has a positive effect over the SCR as seen intuitively.

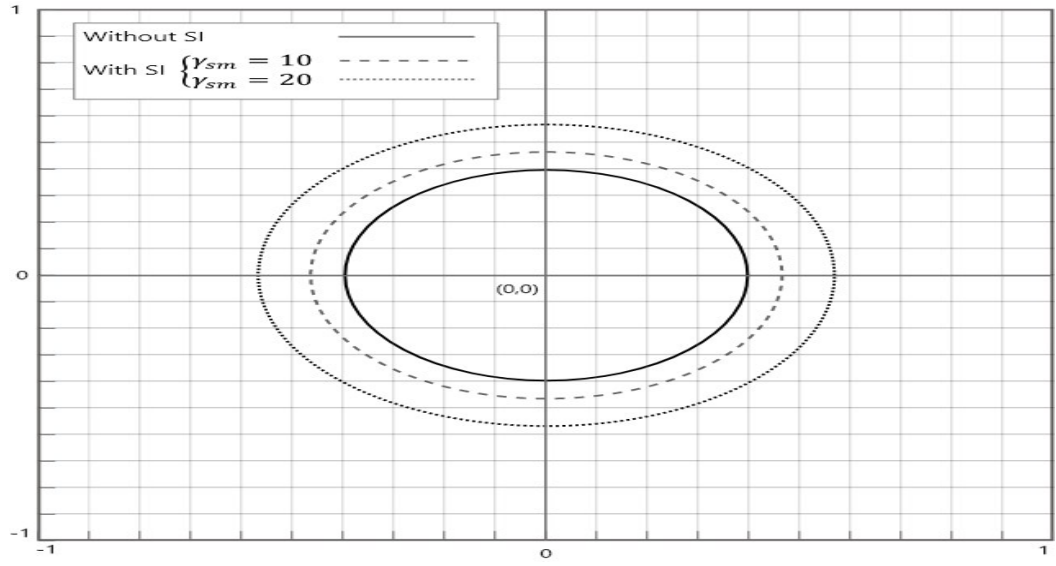


Fig. 2. SCR for different scenarios of SI and different values of $\overline{\gamma_{sm}}$ when, $R_s = 0.1$ bits, $d_e = 0.2$, $\overline{\gamma_m} = 10dB$, $\overline{\gamma_e} = 0dB$, $\overline{\gamma_{se}} = 0dB$ and $\alpha = 3.52$.

Also, the trade-off between d_m and d_e has been indicated in Fig. 3. It is clearly seen that as $\overline{\gamma_{sm}}$ increases, legitimate receiver is getting away from legitimate transmitter for a specified d_e . For example when $\overline{\gamma_m} = 10dB$, $\overline{\gamma_e} = 0dB$, $\overline{\gamma_{sm}} = 10dB$, $\overline{\gamma_{se}} = 0dB$, $\alpha = 3.52$ and $R_s = 0.2$ bits, $d_e = 0.5$, d_m is equal to 0.86, while when we don't have any SI, d_m becomes 0.72.

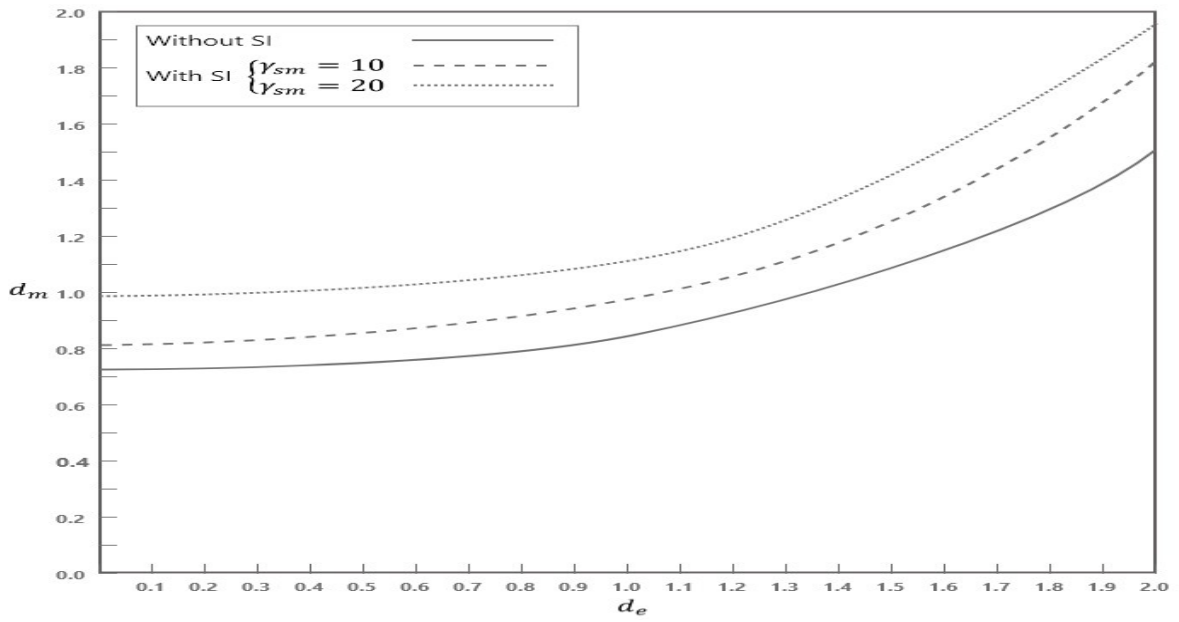


Fig. 3. The trade-off between d_m and d_e for different scenarios of SI and different values of $\overline{\gamma_{sm}}$ when, $R_s = 0.2$ bits, $\overline{\gamma_m} = 10dB$, $\overline{\gamma_e} = 0dB$, $\overline{\gamma_{se}} = 0dB$ and $\alpha = 3.52$.

V. CONCLUSION

In this work, the coverage region in a Rayleigh fading WC with considering SI non-causally available at the transmitter has been analyzed. We demonstrated the impact of SI by deriving closed-form expressions on the SCR as a remarkable wireless performance factor. Also, by mathematical derivations and numerical results, it has been investigated that SI increases the SCR as expected intuitively.

Appendices

Appendix A:

Proof of Theorem 1: An informal proof of this theorem is a straightforward algebra extension of [5], [19], and [20] with some differences caused by known fading coefficients. The coding scheme used to achieve this capacity is similar to the one used in [15], [19], [20]. The coding scheme and error probability analysis is straightforward and is not shown here due to a lack of space. We use definitions in corollary 1 and 2 to compute the capacity of WC with knowing SI at the transmitter and fading coefficients. We have following assumptions:

$$E[X^2] = P, \quad E[S^2] = Q, \quad E[\eta_m^2] = N_m, \quad E[\eta_e^2] = N_e, \quad (13)$$

and U_m and U_e are generated by using generalized dirty paper coding presented in [23]. According to [5], [19], [20], [23] and knowing that $Y_m = h_m X + h_{sm} S + \eta_m$, $Y_e = h_e X + h_{sm} S + \eta_e$ we can write mutual information related to the term C_m in corollary 1 as follows:

$$I(U_m; Y_m) = H(h_m X + h_{sm} S + \eta_m) - H(h_m X + h_{sm} S + \eta_m | X + \alpha_m S)$$

$$\begin{aligned}
&= H(h_m X + h_{sm} S + \eta_m) + H(X + \alpha_m S) - H(h_m X + h_{sm} S + \eta_m, X + \alpha_m S) \\
&= \log((2\pi e)^2 (|h_m|^2 P + |h_{sm}|^2 Q + N_m)(P + \alpha_m^2 Q)) - \\
&\quad \log((2\pi e)^2 \det(\text{cov}(h_m X + h_{sm} S + \eta_m, X + \alpha_m S))) \\
&= \log\left(\frac{(|h_m|^2 P + |h_{sm}|^2 Q + N_m)(P + \alpha_m^2 Q)}{PQ(|h_{sm}| - \alpha_m|h_m|)^2 + N_m(P + \alpha_m^2 Q)}\right), \tag{14}
\end{aligned}$$

and

$$I(U_m; S) = \log\left(\frac{P + \alpha_m^2 Q}{P}\right). \tag{15}$$

Substituting (14) and (15) in C_m with corollary 1, we obtain:

$$C_m(\alpha_m) = \log\left(\frac{P(|h_m|^2 P + |h_{sm}|^2 Q + N_m)}{PQ(|h_{sm}| - \alpha_m|h_m|)^2 + N_m(P + \alpha_m^2 Q)}\right). \tag{16}$$

By maximizing $C_m(\alpha_m)$ over α_m , for corollary 1, we get

$$C_s = \max_{\alpha_m} C_m(\alpha_m) = \log\left(1 + \frac{|h_m|^2 P}{N_m}\right) = \log(1 + \gamma_m). \tag{17}$$

So we have (9) for corollary 1. The proof of this theorem for corollary 2 is similar with negligible change and is omitted for the lack of space. ■

Appendix B:

Proof of Theorem 2: First, we state some integrals that are needed to prove the theorems [26]. Therefore, we have

$$\int e^{-\xi t} \log(1 + \beta t) dt = \frac{1}{\xi} \left[e^{\frac{\xi}{\beta}} Ei\left(-\left(\xi t + \frac{\xi}{\beta}\right)\right) - e^{-\xi t} \log(1 + \beta t) \right], \tag{18}$$

$$\int_0^\infty e^{-\xi t} \log(1 + \beta t) dt = -\frac{e^{\frac{\xi}{\beta}}}{\xi} Ei\left(-\frac{\xi}{\beta}\right), \tag{19}$$

$$\int e^{-vt} Ei(-(\delta + \kappa t)) dt = \frac{1}{v} \left[e^{\frac{v\delta}{\kappa}} Ei \left(-\frac{(\nu + \kappa)(\kappa t + \delta)}{k} \right) - e^{vt} Ei(-(\kappa t + \delta)) \right], \quad (20)$$

$$\int_0^\infty e^{-vt} Ei(-(\delta + \kappa t)) dt = \frac{1}{v} \left[Ei(-\delta) - e^{\frac{v\delta}{\kappa}} Ei \left(-\frac{(\nu + \kappa)\delta}{k} \right) \right], \quad (21)$$

where $Ei(x) = -\int_x^\infty t^{-1} e^{-t} dt$. Also, $Ei(-x)$ was approximated in [27] as follows:

$$Ei(-x) = -4\sqrt{2}a_N a_I \sum_{n=1}^{N+1} \sum_{i=1}^{I+1} \sqrt{b_n} e^{-4b_n b_i x}, \quad (22)$$

where $\theta_0 = 0 < \theta_1 < \dots < \theta_{N+1} = \frac{\pi}{2}$, $a_N = \frac{\theta_N - \theta_{N-1}}{\pi}$, $b_n = \frac{\cos(\theta_{n-1}) - \cos(\theta_n)}{2(\theta_n - \theta_{n-1})}$, and for $N = I = 1$ we have: $a_N = a_I = \frac{1}{4}$, $b_1 = \infty$ and $b_2 = \frac{2}{\pi}$. Thus, $Ei(-x)$ can be approximated as

$$Ei(-x) \sim -\frac{\sqrt{\pi}}{2} e^{-(\frac{16}{\pi^2})x}. \quad (23)$$

For Corollary 1: First, we compute the distance d_m between transmitter and legitimate receiver to ensure reliable transmission. Due to the secrecy outage probability definition, the reliable transmission between transmitter and legitimate receiver happens, when legitimate receiver can decode the confidential messages (i.e., $C_m > R_s$) or

$$R_s \leq E_{\gamma_m} \left[\log \left(1 + \frac{\gamma_m}{d_m^\alpha} \right) \right] = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\gamma_m}}}{\gamma_m} \log \left(1 + \frac{\gamma_m}{d_m^\alpha} \right) d\gamma_m, \quad (24)$$

where by computing the above integral and substituting (23) into (24), the distance d_m between transmitter and legitimate receiver for reliable transmission is obtained as below:

$$d_m \leq \left(\frac{\pi^2 \bar{\gamma}_m}{\pi^2 - 16} \ln \left(\frac{2R_s}{\sqrt{\pi}} \right) \right)^{\frac{1}{\alpha}}. \quad (25)$$

In this case we don't have any limitation over d_e .

For Corollary 2: The distance d_m for reliable transmission is obtained similar to (25). Now, using the derived distance d_m between transmitter and legitimate receiver, we can find the SCR for secure transmission from definition (15) as follows

$$R_s \leq C_s(d_m, d_e) = E_{\gamma_s, \gamma_e, \gamma_m} \left[\frac{\log \left(1 + \frac{\gamma_m}{d_m^\alpha} + \gamma_{sm} \right)}{\log \left(1 + \frac{\gamma_e}{d_e^\alpha} + \gamma_{se} \right)} \right] = D_1 - D_2. \quad (26)$$

We have

$$D_1 = \int_0^\infty \int_0^{\gamma_m} \int_0^\infty \log \left(1 + \frac{\gamma_m}{d_m^\alpha} + \gamma_{sm} \right) \frac{1}{\gamma_{sm}} e^{-\frac{\gamma_{sm}}{\gamma_{sm}}} \frac{1}{\gamma_m} e^{-\frac{\gamma_m}{\gamma_m}} \frac{1}{\gamma_e} e^{-\frac{\gamma_e}{\gamma_e}} d\gamma_{sm} d\gamma_e d\gamma_m, \quad (27)$$

and

$$D_2 = \int_0^\infty \int_0^{\gamma_m} \int_0^\infty \log \left(1 + \frac{\gamma_e}{d_e^\alpha} + \gamma_{se} \right) \frac{1}{\gamma_{se}} e^{-\frac{\gamma_{se}}{\gamma_{se}}} \frac{1}{\gamma_m} e^{-\frac{\gamma_m}{\gamma_m}} \frac{1}{\gamma_e} e^{-\frac{\gamma_e}{\gamma_e}} d\gamma_{se} d\gamma_e d\gamma_m. \quad (28)$$

After some simplifications and by utilizing linear formulas of integration, for D_1 , we receive to

$$D_1 = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\gamma_m}}}{\gamma_{sm} \cdot \gamma_e \cdot \gamma_m} (D_1'') d\gamma_m, \quad (29)$$

where $D_1'' = \int_0^{\gamma_m} e^{-\frac{\gamma_e}{\gamma_e}} D_1' d\gamma_e$ and $D_1' = \int_0^\infty \log \left(1 + \frac{\gamma_m}{d_m^\alpha} + \gamma_{sm} \right) e^{-\frac{\gamma_{sm}}{\gamma_{sm}}} d\gamma_{sm} = \overline{\gamma_{sm}} (\ln \left(1 + \frac{\gamma_m}{d_m^\alpha} \right) + e^{\frac{1+\frac{\gamma_m}{d_m^\alpha}}{\gamma_{sm}}} E_1 \left(\frac{1+\frac{\gamma_m}{d_m^\alpha}}{\gamma_{sm}} \right))$. So, we have

$$D_1'' = j_1' + j_2', \quad (30)$$

where

$$j_1' = \int_0^{\gamma_m} \overline{\gamma_{sm}} e^{-\frac{\gamma_e}{\gamma_e}} \ln \left(1 + \frac{\gamma_m}{d_m^\alpha} \right) d\gamma_e = \overline{\gamma_{sm}} \overline{\gamma_e} \ln \left(1 + \frac{\gamma_m}{d_m^\alpha} \right) (1 - e^{-\frac{\gamma_m}{\gamma_e}}), \quad (31)$$

and

$$j_2' = \int_0^{\gamma_m} \frac{\gamma_m}{\gamma_{sm}} e^{-\frac{\gamma_e}{\gamma_e}} e^{\frac{1+\gamma_m}{\gamma_{sm}} \frac{d_m^\alpha}{d_m^\alpha}} E_1 \left(\frac{1 + \frac{\gamma_m}{d_m^\alpha}}{\gamma_{sm}} \right) d\gamma_e = \overline{\gamma_{sm}} \overline{\gamma_e} \left(1 - e^{-\frac{\gamma_m}{\gamma_e}} \right) e^{\frac{1+\gamma_m}{\gamma_{sm}} \frac{d_m^\alpha}{d_m^\alpha}} E_1 \left(\frac{1 + \frac{\gamma_m}{d_m^\alpha}}{\gamma_{sm}} \right). \quad (32)$$

Thus, by replacing (31) and (32) in (30) and then (29), we have

$$D_1 = k_1' - k_2' + k_3' - k_4', \quad (33)$$

where, by exploiting (19) and (21), we have

$$k_1' = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\gamma_m}}}{\gamma_m} \ln \left(1 + \frac{\gamma_m}{d_m^\alpha} \right) d\gamma_m = -e^{\frac{d_m^\alpha}{\gamma_m}} Ei \left(-\frac{d_m^\alpha}{\gamma_m} \right), \quad (34)$$

$$k_2' = \int_0^\infty \frac{e^{-\gamma_m \left(\frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right)}}{\gamma_m} \ln \left(1 + \frac{\gamma_m}{d_m^\alpha} \right) d\gamma_m = -\frac{\overline{\gamma_e} \cdot e^{d_m^\alpha \left(\frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right)}}{\gamma_m + \overline{\gamma_e}} Ei \left(-d_m^\alpha \left(\frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right) \right), \quad (35)$$

$$k_3' = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\gamma_m}} e^{\frac{1+\gamma_m}{\gamma_{sm}} \frac{d_m^\alpha}{d_m^\alpha}}}{\gamma_m} E_1 \left(\frac{1 + \frac{\gamma_m}{d_m^\alpha}}{\gamma_{sm}} \right) d\gamma_m = \frac{-e^{\frac{1}{\gamma_{sm}}} \left(Ei \left(\frac{-1}{\gamma_{sm}} \right) - e^{\frac{d_m^\alpha}{\gamma_m} - \frac{1}{\gamma_{sm}}} Ei \left(\frac{-d_m^\alpha}{\gamma_m} \right) \right)}{\gamma_m \left(\frac{1}{\gamma_m} - \frac{1}{\gamma_{sm} d_m^\alpha} \right)}, \quad (36)$$

$$k_4' =$$

$$\int_0^\infty \frac{e^{-\gamma_m \left(\frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right)}}{\gamma_m} e^{\frac{1+\gamma_m}{\gamma_{sm}} \frac{d_m^\alpha}{d_m^\alpha}} E_1 \left(\frac{1 + \frac{\gamma_m}{d_m^\alpha}}{\gamma_{sm}} \right) d\gamma_m = \frac{e^{\frac{1}{\gamma_{sm}}} \left[Ei \left(\frac{-1}{\gamma_{sm}} \right) - e^{\frac{d_m^\alpha}{\gamma_m} + \frac{d_m^\alpha}{\gamma_e} - \frac{1}{\gamma_{sm}}} Ei \left(-\left(\frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right) d_m^\alpha \right) \right]}{\frac{1}{\gamma_{sm} d_m^\alpha} - \frac{1}{\gamma_m} - \frac{1}{\gamma_e}} \quad (37)$$

Similarly, for D_2 , we have

$$D_2 = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\gamma_m}}}{\gamma_{se} \cdot \overline{\gamma_e} \cdot \gamma_m} (D_2'') d\gamma_m. \quad (38)$$

where $D_2'' = \int_0^{\gamma_m} e^{-\frac{\gamma_e}{\gamma_e}} (D_2') d\gamma_e$ and $D_2' = \int_0^\infty \log \left(1 + \frac{\gamma_e}{d_e^\alpha} + \gamma_{se} \right) e^{-\frac{\gamma_{se}}{\gamma_{se}}} d\gamma_{se} = \overline{\gamma_{se}} \left(\ln \left(1 + \frac{\gamma_e}{d_e^\alpha} \right) + e^{\frac{1+\gamma_e}{\gamma_{se}} \frac{d_e^\alpha}{d_e^\alpha}} E_1 \left(\frac{1+\gamma_e}{\gamma_{se}} \right) \right)$. So, we have

$$D_2'' = i_1' + i_2', \quad (39)$$

where, by exploiting (18) and (20), we have

$$\begin{aligned}
i_1' &= \int_0^{\gamma_m} \frac{\gamma_e}{\bar{\gamma}_{se}} e^{-\frac{\gamma_e}{\bar{\gamma}_e}} \ln\left(1 + \frac{\gamma_e}{d_e^\alpha}\right) d\gamma_e \\
&= \bar{\gamma}_{se} \bar{\gamma}_e \left[e^{\frac{d_e^\alpha}{\bar{\gamma}_e}} Ei\left(-\frac{d_e^\alpha + \gamma_m}{\bar{\gamma}_e}\right) - e^{-\frac{\gamma_m}{\bar{\gamma}_e}} \ln\left(1 + \frac{\gamma_e}{d_e^\alpha}\right) - e^{\frac{d_e^\alpha}{\bar{\gamma}_e}} Ei\left(\frac{-d_e^\alpha}{\bar{\gamma}_e}\right) \right], \tag{40}
\end{aligned}$$

$$\begin{aligned}
i_2' &= \int_0^{\gamma_m} \frac{\gamma_e}{\bar{\gamma}_{se}} e^{-\frac{\gamma_e}{\bar{\gamma}_e}} e^{\frac{1+\gamma_e}{\bar{\gamma}_{se} d_e^\alpha}} E_1\left(\frac{1+\gamma_e}{\bar{\gamma}_{se} d_e^\alpha}\right) d\gamma_e = -\frac{\bar{\gamma}_{se} e^{\frac{1}{\bar{\gamma}_{se}}}}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \cdot \left[e^{\frac{d_e^\alpha}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se}}} Ei\left(-\frac{\gamma_m + d_e^\alpha}{\bar{\gamma}_e}\right) - \right. \\
&\quad \left. e^{\gamma_m \left(\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}\right)} Ei\left(-\frac{1 + \frac{\gamma_m}{d_e^\alpha}}{\bar{\gamma}_{se}}\right) - e^{\frac{d_e^\alpha}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se}}} Ei\left(-\frac{d_e^\alpha}{\bar{\gamma}_e}\right) + Ei\left(-\frac{1}{\bar{\gamma}_{se}}\right) \right]. \tag{41}
\end{aligned}$$

Thus, by replacing (40) and (41) in (39) and then (38), we have

$$D_2 = d_1' - d_2' - d_3' - d_4' + d_5' + d_6' - d_7'. \tag{42}$$

where, by exploiting (19) and (21), we have

$$d_1' = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m} e^{\frac{d_e^\alpha}{\bar{\gamma}_e}}}}{\bar{\gamma}_m} Ei\left(-\frac{d_e^\alpha + \gamma_m}{\bar{\gamma}_e}\right) d\gamma_m = e^{\frac{d_e^\alpha}{\bar{\gamma}_e}} \left[Ei\left(-\frac{d_e^\alpha}{\bar{\gamma}_e}\right) - e^{\frac{d_e^\alpha}{\bar{\gamma}_m}} Ei\left(-\left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e}\right) d_e^\alpha\right) \right], \tag{43}$$

$$d_2' = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m} e^{-\frac{\gamma_m}{\bar{\gamma}_e}}}}{\bar{\gamma}_m} \ln\left(1 + \frac{\gamma_e}{d_e^\alpha}\right) d\gamma_m = -\frac{\bar{\gamma}_e}{\bar{\gamma}_m + \bar{\gamma}_e} e^{d_e^\alpha \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e}\right)} Ei\left(-d_e^\alpha \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e}\right)\right), \tag{44}$$

$$d_3' = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m} e^{\frac{d_e^\alpha}{\bar{\gamma}_e}}}}{\bar{\gamma}_m} Ei\left(\frac{-d_e^\alpha}{\bar{\gamma}_e}\right) d\gamma_m = e^{\frac{d_e^\alpha}{\bar{\gamma}_e}} Ei\left(\frac{-d_e^\alpha}{\bar{\gamma}_e}\right), \tag{45}$$

$$\begin{aligned}
d_4' &= \int_0^\infty \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m} e^{\frac{d_e^\alpha}{\bar{\gamma}_e}}}}{\bar{\gamma}_e \cdot \bar{\gamma}_m} \left(\frac{1}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \right) Ei\left(-\frac{\gamma_m + d_e^\alpha}{\bar{\gamma}_e}\right) d\gamma_m \\
&= e^{\frac{d_e^\alpha}{\bar{\gamma}_e}} \left(\frac{1}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \right) \left(Ei\left(-\frac{d_e^\alpha}{\bar{\gamma}_e}\right) - e^{\frac{d_e^\alpha}{\bar{\gamma}_e}} Ei\left(-d_e^\alpha \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e}\right)\right) \right), \tag{46}
\end{aligned}$$

$$d_5' = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m} e^{\frac{1}{\bar{\gamma}_{se}}}}}{\bar{\gamma}_e \cdot \bar{\gamma}_m} \left(\frac{1}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \right) e^{\gamma_m \left(\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}\right)} Ei\left(-\frac{1 + \frac{\gamma_m}{d_e^\alpha}}{\bar{\gamma}_{se}}\right) d\gamma_m$$

$$\begin{aligned}
&= \frac{1}{\bar{\gamma}_e \bar{\gamma}_m} \left(\frac{1}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \cdot \frac{1}{\frac{1}{\bar{\gamma}_m} - \frac{1}{\bar{\gamma}_e} + \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \right) e^{\frac{1}{\bar{\gamma}_{se}}} [Ei \left(-\frac{1}{\bar{\gamma}_{se}} \right) - e^{\left(d_e^\alpha \left(\frac{1}{\bar{\gamma}_m} - \frac{1}{\bar{\gamma}_e} + \frac{1}{\bar{\gamma}_{se} d_e^\alpha} \right) \right)} Ei(-d_e^\alpha \\
&\quad \left(\frac{1}{\bar{\gamma}_m} - \frac{1}{\bar{\gamma}_e} + \frac{2}{\bar{\gamma}_{se} d_e^\alpha} \right))] , \tag{47}
\end{aligned}$$

$$d'_6 = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m} e^{\frac{1}{\bar{\gamma}_{se}}}}}{\bar{\gamma}_e \cdot \bar{\gamma}_m} \left(\frac{1}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \right) e^{\frac{d_e^\alpha}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se}}} Ei \left(-\frac{d_e^\alpha}{\bar{\gamma}_e} \right) d\gamma_m = \frac{1}{\bar{\gamma}_e} \left(\frac{1}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \right) e^{\frac{d_e^\alpha}{\bar{\gamma}_e}} Ei \left(-\frac{d_e^\alpha}{\bar{\gamma}_e} \right), \tag{48}$$

$$d'_7 = \int_0^\infty \frac{e^{-\frac{\gamma_m}{\bar{\gamma}_m} e^{\frac{N_e}{\bar{\gamma}_s}}}}{\bar{\gamma}_e \cdot \bar{\gamma}_m} \left(\frac{1}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \right) Ei \left(-\frac{1}{\bar{\gamma}_{se}} \right) d\gamma_m = \frac{1}{\bar{\gamma}_e} \left(\frac{1}{\frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{se} d_e^\alpha}} \right) e^{\frac{1}{\bar{\gamma}_{se}}} Ei \left(-\frac{1}{\bar{\gamma}_{se}} \right). \tag{49}$$

Therefore, from (26), we have

$$\begin{aligned}
R_s &\leq k'_1 - k'_2 + k'_3 - k'_4 - d'_1 - d'_2 - d'_3 - d'_4 + d'_5 + d'_6 - d'_7 \\
&= \frac{\bar{\gamma}_m e^{\frac{d_m^\alpha}{\bar{\gamma}_m}}}{\bar{\gamma}_{sm} d_m^\alpha - \bar{\gamma}_m} Ei \left(-\frac{d_m^\alpha}{\bar{\gamma}_m} \right) - \left(\frac{1}{1 - \frac{\bar{\gamma}_m}{\bar{\gamma}_{sm} d_m^\alpha}} - \frac{1}{\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{sm} d_m^\alpha}} \right) e^{\frac{1}{\bar{\gamma}_{sm}}} Ei \left(\frac{-1}{\bar{\gamma}_{sm}} \right) + \left(\frac{\bar{\gamma}_e}{\bar{\gamma}_m + \bar{\gamma}_e} - \right. \\
&\quad \left. \frac{1}{\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} - \frac{1}{\bar{\gamma}_{sm} d_m^\alpha}} \right) e^{d_m^\alpha \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} \right)} Ei \left(-d_m^\alpha \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} \right) \right) + \left(\frac{1}{1 - \frac{\bar{\gamma}_e}{\bar{\gamma}_{se} d_e^\alpha}} \left(1 - \frac{1}{1 - \frac{\bar{\gamma}_m}{\bar{\gamma}_e} + \frac{\bar{\gamma}_m}{\bar{\gamma}_{sm} d_e^\alpha}} \right) e^{\frac{1}{\bar{\gamma}_{se}}} \right. \\
&\quad \left. \cdot Ei \left(-\frac{1}{\bar{\gamma}_{se}} \right) + \left(\frac{\bar{\gamma}_m}{\bar{\gamma}_m + \bar{\gamma}_e} - \frac{1}{1 - \frac{\bar{\gamma}_e}{\bar{\gamma}_{se} d_e^\alpha}} \right) e^{d_e^\alpha \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} \right)} Ei \left(-d_e^\alpha \left(\frac{1}{\bar{\gamma}_m} + \frac{1}{\bar{\gamma}_e} \right) \right) + \left(\frac{1}{1 - \frac{\bar{\gamma}_e}{\bar{\gamma}_{se} d_e^\alpha}} \right) \right. \\
&\quad \left. \left(\frac{1}{1 - \frac{\bar{\gamma}_m}{\bar{\gamma}_e} + \frac{\bar{\gamma}_m}{\bar{\gamma}_{se} d_e^\alpha}} \right) e^{d_e^\alpha \left(\frac{1}{\bar{\gamma}_m} - \frac{1}{\bar{\gamma}_e} + \frac{2}{\bar{\gamma}_{se} d_e^\alpha} \right)} \cdot Ei \left(-d_e^\alpha \left(\frac{1}{\bar{\gamma}_m} - \frac{1}{\bar{\gamma}_e} + \frac{2}{\bar{\gamma}_{se} d_e^\alpha} \right) \right) \right). \tag{50}
\end{aligned}$$

Now, by considering the obtained approximation in (23), the proof is completed. ■

Funding. This research is supported by the Faculty of Engineering at the Ferdowsi University of Iran.

Compliance with ethical standards

Conflict of interest. The authors declare that they have no conflict of interest.

Ethical approval. This article does not contain any studies with human participants or animals performed by any of the authors.

Availability of data. Not applicable.

Code availability. Not applicable.

References

- [1] Schneier, Bruce. "Cryptographic design vulnerabilities." *Computer* 31, no. 9 (1998): 29-33.
- [2] Shannon, Claude E. "Communication theory of secrecy systems." *The Bell system technical journal* 28, no. 4 (1949): 656-715.
- [3] Wyner, Aaron D. "The wire-tap channel." *Bell system technical journal* 54, no. 8 (1975): 1355-1387.
- [4] Csiszár, Imre, and Janos Korner. "Broadcast channels with confidential messages." *IEEE transactions on information theory* 24, no. 3 (1978): 339-348.
- [5] Leung-Yan-Cheong, S., and M. Hellman. "The Gaussian wire-tap channel." *IEEE transactions on information theory* 24, no. 4 (1978): 451-456.
- [6] Bloch, Matthieu, João Barros, Miguel RD Rodrigues, and Steven W. McLaughlin. "Wireless information-theoretic security." *IEEE Transactions on Information Theory* 54, no. 6 (2008): 2515-2534.
- [7] Ai, Yun, Long Kong, and Michael Cheffena. "Secrecy outage analysis of double shadowed Rician channels." *Electronics Letters* 55, no. 13 (2019): 765-767.
- [8] Li, Jiangyuan, and Athina P. Petropulu. "Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading." *IEEE Transactions on Information Forensics and Security* 6, no. 3 (2011): 861-867.
- [9] Liu, Xian. "Probability of strictly positive secrecy capacity of the Rician-Rician fading channel." *IEEE Wireless Communications Letters* 2, no. 1 (2012): 50-53.
- [10] Omri, Aymen, and Mazen O. Hasna. "Average secrecy outage rate and average secrecy outage duration of wireless communication systems with diversity over Nakagami-m fading channels." *IEEE Transactions on Wireless Communications* 17, no. 6 (2018): 3822-3833.
- [11] Kong, Long, and Georges Kaddoum. "On Physical Layer Security Over the Fisher-Snedecor Wiretap Fading Channels." *IEEE Access* 6 (2018): 39466-39472.

- [12] Badarneh, Osamah S., Paschalis C. Sofotasios, Sami Muhaidat, Simon L. Cotton, Khaled Rabie, and Naofal Al-Dhahir. "On the secrecy capacity of Fisher-Snedecor F fading channels." In *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, pp. 102-107. IEEE, 2018.
- [13] Ghadi, Farshad Rostami, and Ghosheh Abed Hodtani. "Copula-Based Analysis of Physical Layer Security Performances Over Correlated Rayleigh Fading Channels." *IEEE Transactions on Information Forensics and Security* 16 (2020): 431-440.
- [14] Shannon, Claude E. "Channels with side information at the transmitter." *IBM journal of Research and Development* 2, no. 4 (1958): 289-293.
- [15] Gel'fand, S. I., Pinsker, M. S., "Coding for Channels with Random Parameters." *Probl. Contr. Inform. Theory*, 1980, 9, (1), pp. 19-31.
- [16] Cover, Thomas M., and Mung Chiang. "Duality between channel capacity and rate distortion with two-sided state information." *IEEE Transactions on Information Theory* 48, no. 6 (2002): 1629-1638.
- [17] Anzabi-Nezhad, Nima S., Ghosheh Abed Hodtani, and Mohammad Molavi Kakhki. "Information theoretic exemplification of the receiver re-cognition and a more general version for the cost theorem." *IEEE Communications letters* 17, no. 1 (2012): 107-110.
- [18] Anzabi-Nezhad, Nima S., Ghosheh Abed Hodtani, and Mohammad Molavi Kakhki. "A new and more general capacity theorem for the gaussian channel with two-sided input-noise dependent state information." *arXiv preprint arXiv:1507.04924* (2015).
- [19] Chen, Yanling, and AJ Han Vinck. "Wiretap channel with side information." *IEEE Transactions on Information Theory* 54, no. 1 (2008): 395-402.
- [20] Chia, Yeow-Khiang, and Abbas El Gamal. "Wiretap channel with causal state information." *IEEE Transactions on Information Theory* 58, no. 5 (2012): 2838-2849.
- [21] Liu, Wei, and Biao Chen. "Wiretap channel with two-sided channel state information." In *2007 Conference Record of the Forty-First Asilomar Conference on Signals, Systems and Computers*, pp. 893-897. IEEE, 2007.
- [22] Xu, Peng, Zhiguo Ding, Xuchu Dai, and Kin K. Leung. "A general framework of wiretap channel with helping interference and state information." *IEEE transactions on information forensics and security* 9, no. 2 (2013): 182-195.
- [23] Costa, Max. "Writing on dirty paper (corresp.)." *IEEE transactions on information theory* 29, no. 3 (1983): 439-441.
- [24] Aggarwal, Vaneet, Amir Bennatan, and A. Robert Calderbank. "On maximizing coverage in gaussian relay channels." *IEEE Transactions on Information Theory* 55, no. 6 (2009): 2518-2536.
- [25] Alizadeh, Alireza, and Ghosheh Abed Hodtani. "Analysis of capacity and coverage region for Rayleigh fading MIMO relay channel." *International Journal of Communication Systems* 28, no. 8 (2015): 1462-1474.
- [26] Jeffrey, Alan, and Daniel Zwillinger, eds. *Table of integrals, series, and products*. Elsevier, 2007.
- [27] Alkheir, Ala Abu, and Mohamed Ibnkahla. "An accurate approximation of the exponential integral function using a sum of exponentials." *IEEE communications letters* 17, no. 7 (2013): 1364-1367.

Figures

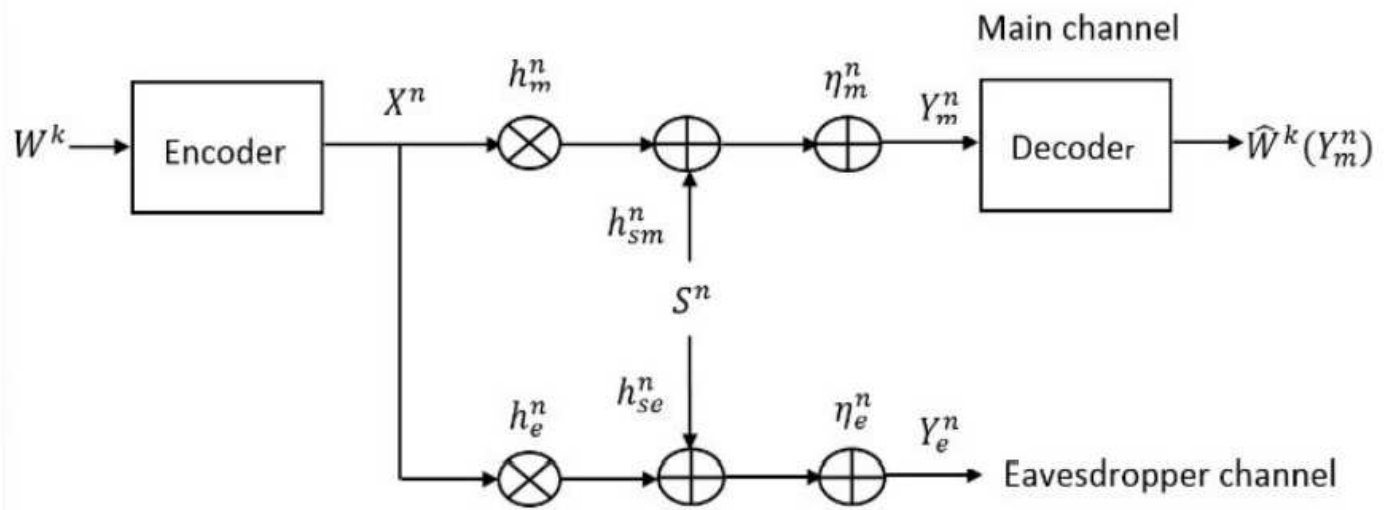


Figure 1

An uncorrelated Rayleigh fading WC.

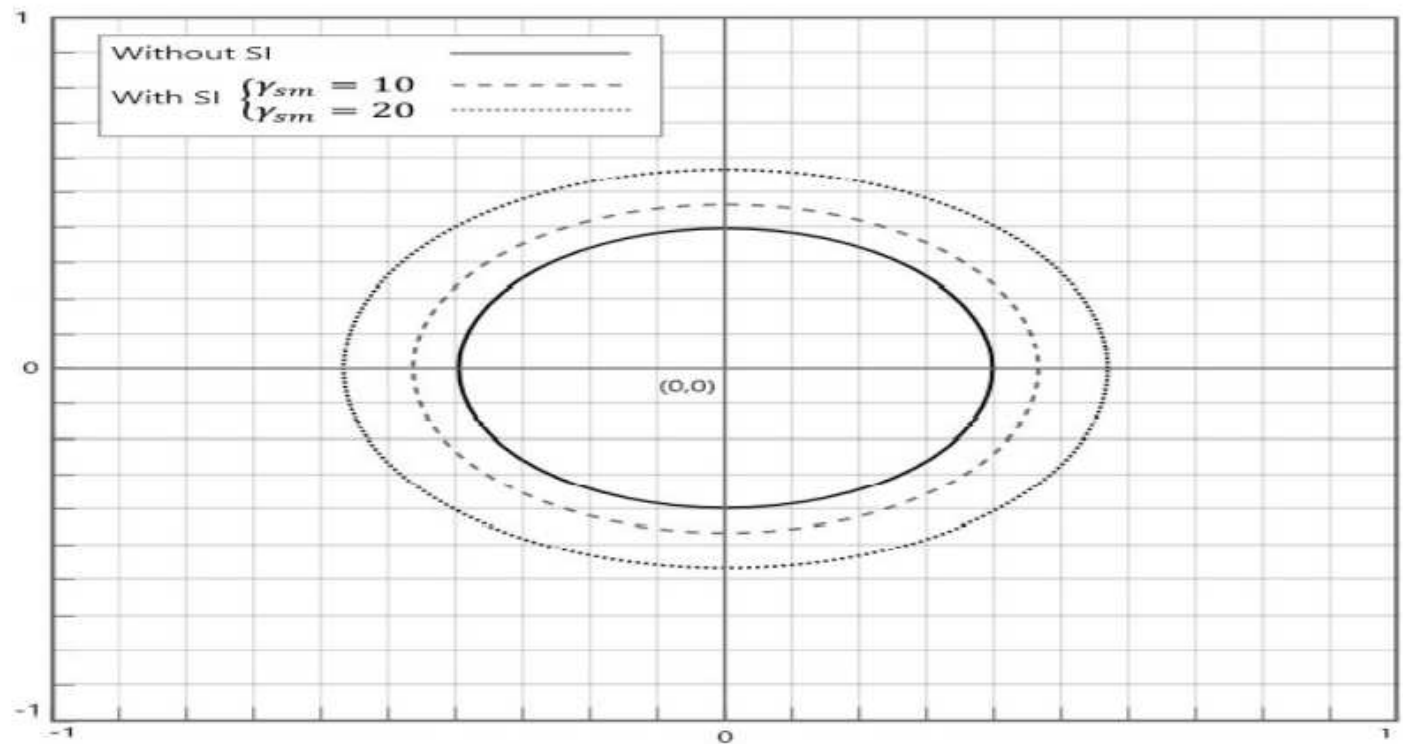


Figure 2

Please see the Manuscript PDF file for the complete figure caption

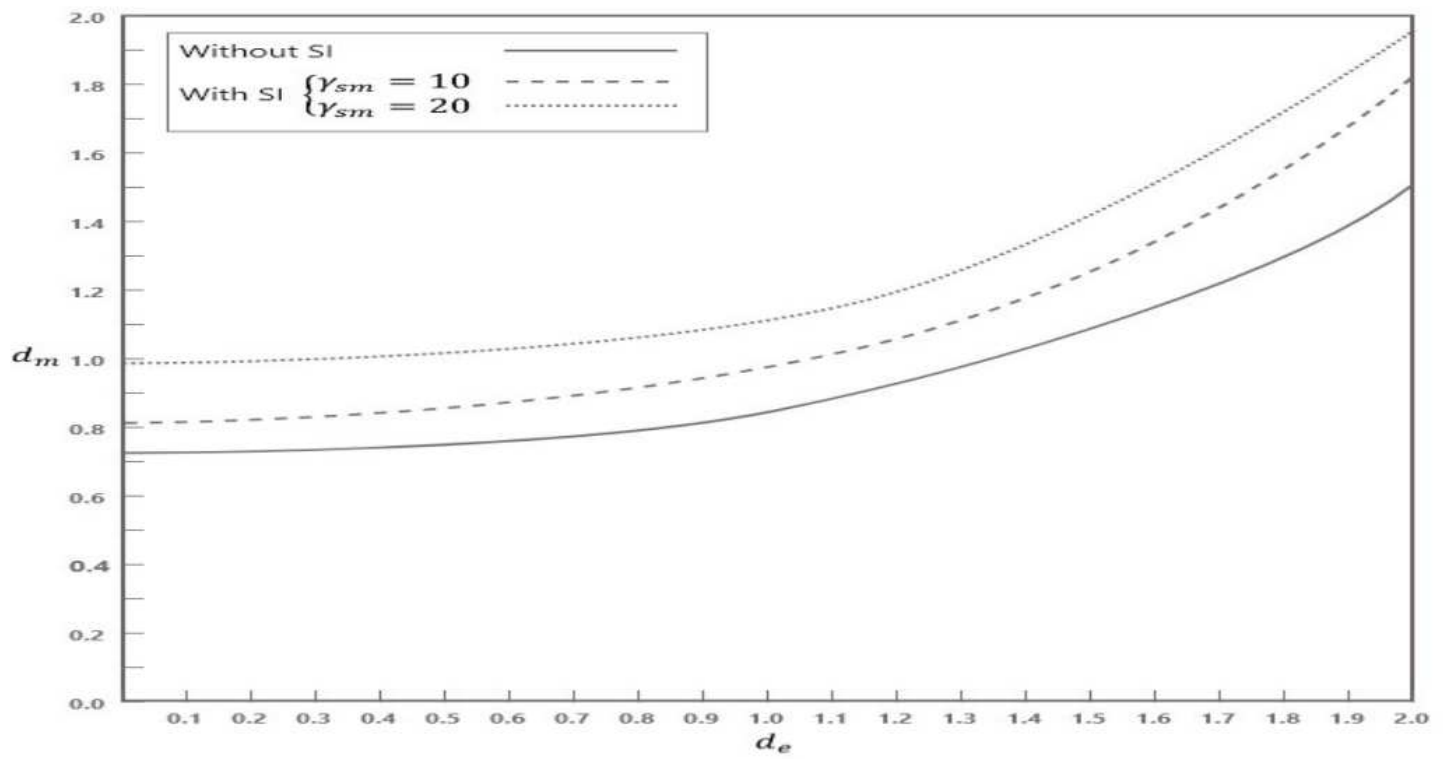


Figure 3

Please see the Manuscript PDF file for the complete figure caption