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

Saeid Pakravan1 · Ghosheh Abed Hodtani1

Accepted: 29 May 2022 / Published online: 21 June 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

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

1 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, an 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.

1.1 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 Sect. 2. In Sect. 3, 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 Sect. 4. Finally, we conclude the paper in Sect. 5.

1.2 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. Max min \{\cdot\} represents maximizing the minimization of a function.
2 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.

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 $W^k \in \{1, 2, \ldots, M\}$ 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 $Y^n_m$, the decoder at the legitimate receiver creates an estimate $\hat{W}^k(Y^n_m)$ of the message $W^k$. The corresponding output at the eavesdropper is $Y^n_e$. So, the received signals in Rayleigh fading WC by considering legitimate receiver as $Y^n_m(i)$ and eavesdropper as $Y^n_e(i)$ can be specified as follows:

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

$$Y^n_e(i) = h_e(i)X(i) + h_{se}(i)S(i) + \eta_e(i), \quad i = 1, \ldots, n \quad (2)$$

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 $h_e(i) = h_e, \forall i = 1, \ldots, n$), 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:

![Fig. 1 An uncorrelated Rayleigh fading WC](image-url)
\[
\frac{1}{n} \sum_{i=1}^{n} E\left\{ |X_i|^2 \right\} \leq P,
\]

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 \( \gamma_m(i) = \frac{P[h_m(i)]^2}{N_m} = \gamma_m \) and \( \gamma_e(i) = \frac{P[h_e(i)]^2}{N_e} = \gamma_e \); and the average SNR at legitimate receiver and eavesdropper are respectively given as \( \bar{\gamma}_m(i) = \frac{P E[h_m(i)]^2}{N_m} = \bar{\gamma}_m \) and \( \bar{\gamma}_e(i) = \frac{P E[h_e(i)]^2}{N_e} = \bar{\gamma}_e \). 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 \( \gamma_m \) and \( \gamma_e \). Since the channel fading coefficients \( h \) are zero-mean complex Gaussian RVs and the instantaneous SNR \( \gamma \propto |h|^2 \), it follows that \( \gamma \) is distributed exponentially, in particular \( f(\gamma_m) = \frac{1}{\gamma_m} \exp\left(-\frac{\gamma_m}{\gamma_m}\right) \), and \( f(\gamma_e) = \frac{1}{\gamma_e} \exp\left(-\frac{\gamma_e}{\gamma_e}\right) \).

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.

\[
P_{e}^{avg} \triangleq \frac{1}{M} \sum_{i=1}^{n} \Pr \left( \hat{W}^k(Y_m^n) \neq i \mid W^k = i \right),
\]

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 \( R_s \geq R_e - \epsilon \), where \( R_e \) and \( P_{e}^{avg} \) have been defined before this. The SC capacity \( C_s \) can be defined as

\[
C_s = \sup_{P_{e}^{avg} \leq \epsilon} R_s.
\]

In our paper, we assume that SI exists at the transmitter and define

\[
\gamma_{sm}(i) = \frac{Q[h_m(i)]^2}{N_m} = \frac{Q|h_m|^2}{N_m} = \gamma_{sm}, \quad \bar{\gamma}_{sm}(i) = \frac{QE[h_m(i)]^2}{N_m} = \frac{QE|h_m|^2}{N_m} = \bar{\gamma}_{sm}, \quad \gamma_{se}(i) = \frac{Q[h_e(i)]^2}{N_e} = \frac{Q|h_e|^2}{N_e} = \gamma_{se}, \quad \bar{\gamma}_{se}(i) = \frac{QE[h_e(i)]^2}{N_e} = \frac{QE|h_e|^2}{N_e} = \bar{\gamma}_{se}.
\]

We have following marginal distributions for \( \gamma_{sm} \geq 0 \) and \( \gamma_{se} \geq 0 \), respectively as \( f(\gamma_{sm}) = \frac{1}{\gamma_{sm}} \exp\left(-\frac{\gamma_{sm}}{\gamma_{sm}}\right) \), and \( f(\gamma_{se}) = \frac{1}{\gamma_{se}} \exp\left(-\frac{\gamma_{se}}{\gamma_{se}}\right) \).

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?
3 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.

3.1 Related Works

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

\[ R_{s}^{\text{low}} = \max_{U \rightarrow (X,S) \rightarrow Y_{m} \rightarrow Y_{e}} I(U;Y_{m}) - \max \{ I(U;S), I(U;Y_{e}) \}, \]  

(6)

and

\[ R_{s}^{\text{up}} = \min \{ C_{m}, \max_{U \rightarrow (X,S) \rightarrow Y_{m} \rightarrow Y_{e}} [I(U;Y_{m}) - I(U;Y_{e})] \}, \]  

(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:

\[ C_{m} = \max_{U \rightarrow (X,S) \rightarrow Y_{m} \rightarrow Y_{e}} [I(U;Y_{m}) - I(U;S)]. \]  

(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. \( I(U_{e};Y_{m}) - I(U_{e};Y_{e}) = R_{e} \),
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 \( R_{e} \).

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

\[ I(U;S) \geq I(U;Y_{e}) \leftrightarrow \alpha \geq \alpha_{0} \text{ or } \alpha \leq \alpha_{-0}, \]
\[
(U; Y_e) \geq I(U; S) \iff \alpha_{-0} \leq \alpha \leq \alpha_0,
\]
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 Gaussian. We consider complex fading coefficients for both the main channel and the eavesdropper’s channel, as detailed in Section II.

### 3.2 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.

\[ C_s = \log \left(1 + \gamma_m\right), \quad \text{Corollary 1} \]

\[
\log \left[\frac{1+\gamma_m+\gamma_m'}{1+\gamma_s+\gamma_e}\right]^+, \quad \text{Corollary 2}
\]

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

**Proof** See Appendix A.

### 3.3 SCR analysis

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. This concept analysis is very important practically for all channels. 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 \( h_{sm} = h_{se} = 1 \). The SCR is analyzed for wiretap channel consisting of two point-to-point channels, i.e., the main channel (transmitter-to-legitimate receiver) and the eavesdropper channel (transmitter-to-eavesdropper). The relationships obtained in Theorem 2 are related to each other and collectively represent the SCR for the wiretap channel. 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.,

\[ G(d_m, d_e) \cdot \{d_m, d_e : C_s(d_m, d_e) > R_s\}, \]

where from theorem 1, with Corollaries 1 and 2 respectively we have

\[ C_s(d_m, d_e) = E_{\gamma_m} \left[\log(1 + \gamma_m)\right] \quad \text{and} \quad C_s(d_m, d_e) = E_{\gamma_m,\gamma_e,\gamma_m'} \left[\log \left(\frac{1+\gamma_s+\gamma_e}{1+\gamma_s+\gamma_e}\right)\right] \]

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 \( \bar{m}, \bar{e}, \bar{m}_s, \bar{m}_e \), \( \alpha (\alpha > 2 \text{ is the path loss exponent}) \) and \( R_s \), is given by.

For Corollary 1:

\[
d_m \leq \left( \frac{\pi^2 \bar{m}}{\pi^2 - 16 \ln \left( \frac{2R_s}{\sqrt{\pi}} \right)} \right)^{\frac{1}{\gamma}}.
\]

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:

\[
d_m \leq \left( \frac{\pi^2 \bar{m}}{\pi^2 - 16 \ln \left( \frac{2R_s}{\sqrt{\pi}} \right)} \right)^{\frac{1}{\gamma}}.
\]

\[
R_s \leq \frac{\sqrt{\pi}}{2} \left[ \left( 1 - \frac{1}{\bar{r}_m \bar{r}_e} \right) - \frac{1}{\bar{r}_m} \right] e^{\left( \frac{1 - 16}{\bar{r}_m} \right)} + e^{\left( \frac{d_m^\alpha (1 - 16)}{\bar{r}_m} \right)} + \frac{1}{1 - \frac{1}{\bar{r}_m} + \frac{1}{\bar{r}_e} - \frac{1}{\bar{r}_m \bar{r}_e}} - \frac{1}{\bar{r}_e} \right] e^{\left( \frac{1 - 16}{\bar{r}_e} \right)} + \left( 1 - \frac{1}{\bar{r}_m} - \frac{1}{\bar{r}_e} \right) \left[ e^{\left( \frac{1 - 16}{\bar{r}_e} \right)} \left( \frac{1 - 1}{\bar{r}_m} + \frac{1}{\bar{r}_e} \right) - \left( 1 - \frac{1}{\bar{r}_m} + \frac{1}{\bar{r}_e} \right) \left( \frac{1 - 16}{\bar{r}_m \bar{r}_e} \right) \right]
\]

\[
R_s \leq \frac{\sqrt{\pi}}{2} \left[ \left( 1 - \frac{1}{\bar{r}_m \bar{r}_e} \right) - \frac{1}{\bar{r}_m} \right] e^{\left( \frac{1 - 16}{\bar{r}_m} \right)} + e^{\left( \frac{d_m^\alpha (1 - 16)}{\bar{r}_m} \right)} + \frac{1}{1 - \frac{1}{\bar{r}_m} + \frac{1}{\bar{r}_e} - \frac{1}{\bar{r}_m \bar{r}_e}} - \frac{1}{\bar{r}_e} \right] e^{\left( \frac{1 - 16}{\bar{r}_e} \right)} + \left( 1 - \frac{1}{\bar{r}_m} - \frac{1}{\bar{r}_e} \right) \left[ e^{\left( \frac{1 - 16}{\bar{r}_e} \right)} \left( \frac{1 - 1}{\bar{r}_m} + \frac{1}{\bar{r}_e} \right) - \left( 1 - \frac{1}{\bar{r}_m} + \frac{1}{\bar{r}_e} \right) \left( \frac{1 - 16}{\bar{r}_m \bar{r}_e} \right) \right]
\]

Proof See Appendix B.

Remark Note that (i) the above results obtained for Rayleigh fading can be generalized similarly for other kinds of fading channels, accompanying with similar definitions, however, in other fading versions such as Rician, Nakagami, channels, etc., the corresponding computations will be different. (ii) Also, the SCR concept can be studied for wiretap multi-user channels such as wiretap multiple access channel.

4 Numerical Results

In this section, the numerical results are presented for the SCR to study how the SI affects the coverage region. In reference [13], the authors have been derived a closed-form expression for SCR in a Rayleigh fading WC without SI, where, the main channel
coefficients are correlated and the impact of channel correlation in different scenarios has been studied. In our work, the effect of SI on the SCR of the Rayleigh fading WC, not studied before for our intended channel, is investigated by finding expressions in terms of infinite series. 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.

Also, the trade-off between $d_m$ and $d_e$ has been indicated in Fig. 3. It is clearly seen that as $\gamma_{sm}$ increases, legitimate receiver is getting away from legitimate transmitter for a specified $d_e$. For example when $\gamma_m = 10dB, \gamma_e = 0dB, \gamma_{sm} = 10dB, \gamma_{se} = 0dB, \alpha = 3.52$
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.

5 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.

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:

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

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:

\[
I(U_m;Y_m) = H(h_m X + h_{sm} S + \eta_m) - H(h_m X + h_{sm} S + \eta_m | X + \alpha_m S) \\
= H(h_m X + h_{sm} S + \eta_m) + H(X + \alpha_m S) - H(h_m X + h_{sm} S + \eta_m, X + \alpha_m S) \\
= \log \left( \frac{2\pi e}{\det \text{cov}(h_m X + h_{sm} S + \eta_m, X + \alpha_m S)} \right) - \log \left( \frac{|h_m|^2 P + |h_{sm}|^2 Q + N_m}{P + \alpha_m^2 Q} \right) \\
\]

\[
= \log \left( \frac{\left( |h_m|^2 P + |h_{sm}|^2 Q + N_m \right)(P + \alpha_m^2 Q)}{PQ(|h_{sm}| - \alpha_m |h_m|^2 + N_m(P + \alpha_m^2 Q))} \right),
\]

and

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

Substituting (14) and (15) in \( C_m \) with corollary 1, we obtain:
\[ C_m(\alpha_m) = \log \left( \frac{P(\lvert h_m \rvert^2 P + \lvert h_{sm} \rvert^2 Q + N_m)}{PQ(\lvert h_{sm} \rvert - \alpha_m \lvert h_m \rvert)^2 + N_m(P + \alpha_m^2 Q)} \right). \]  

By maximizing \( C_m(\alpha_m) \) over \( \alpha_m \), for corollary 1, we get
\[ C_s = \max_{\alpha_m} C_m(\alpha_m) = \log \left( 1 + \frac{\lvert h_m \rvert^2 P}{N_m} \right) = \log \left( 1 + \gamma_m \right). \]  

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.
\[ f \ e^{-\xi t} \log (1 + \beta t) dt = \frac{1}{\xi} \left[ e^{\frac{\xi}{\beta}} Ei \left( -\left( \frac{\xi t + \frac{\xi}{\beta} \right) \right) - e^{-\xi t} \log (1 + \beta t) \right], \]  

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

\[ f \ e^{-\nu t} Ei(-(-\delta + \kappa t)) dt = \frac{1}{\nu} \left[ e^{\frac{\nu}{\kappa}} Ei \left( -\left( \frac{(\nu + \kappa)(\kappa t + \delta)}{k} \right) \right) - e^{\nu t} Ei(-(-\kappa t + \delta)) \right], \]  

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

where \( Ei(x) = -\int x^{-1} e^{-t} dt \). Also, \( Ei(-x) \) was approximated in [27] as follows:
\[ Ei(-x) = -4\sqrt{2} a_N a_I \sum_{n=1}^{N+1} \sum_{i=1}^{I+1} \sqrt{b_n} e^{-4b_n b_i x}, \]

where \( \theta_0 = 0 < \theta_1 < \cdots < \theta_{N+1} = \frac{\pi}{2} \), \( a_N = \frac{\theta_0 - \theta_{N+1}}{\pi}, \) \( b_n = \frac{\cos(\theta_{n-1}) - \cos(\theta_n)}{2(\theta_n - \theta_{n-1})} \), and for \( N = I = 1 \) we have: \( a_N = a_I = \frac{1}{4}, b_1 = \infty \) and \( b_2 = \frac{3}{\pi} \). Thus, \( Ei(-x) \) can be approximated as
\[ Ei(-x) \sim -\sqrt{\frac{\pi}{2}} e^{-(\frac{16}{\pi^2}) x}. \]  

**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
Now, using the derived distance and we have

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

(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:

\[ d_m \leq \left( \frac{\pi^2 \gamma_m}{\pi^2 - 16} \ln \left( \frac{2R_s}{\sqrt{\pi}} \right) \right)^{\frac{1}{2}}. \]  

(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

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

(26)

We have

\[ D_1 = \int_0^\infty \int_0^\infty \int_0^\infty \log \left( 1 + \frac{\gamma_m}{d_m^a + \gamma_{sm}} \right) \frac{1}{\gamma_{sm}} e^{-\frac{\gamma_m}{\gamma_{sm}}} \frac{1}{\gamma_{se}} e^{-\frac{\gamma_e}{\gamma_{se}}} \frac{1}{\gamma_{m}} e^{-\frac{\gamma_m}{\gamma_m}} d\gamma_{sm} d\gamma_{se} d\gamma_m, \]  

(27)

and

\[ D_2 = \int_0^\infty \int_0^\infty \int_0^\infty \log \left( 1 + \frac{\gamma_e}{d_e^a + \gamma_{se}} \right) \frac{1}{\gamma_{se}} e^{-\frac{\gamma_e}{\gamma_{se}}} \frac{1}{\gamma_{m}} e^{-\frac{\gamma_m}{\gamma_m}} \frac{1}{\gamma_{e}} e^{-\frac{\gamma_e}{\gamma_e}} d\gamma_{se} d\gamma_{e} d\gamma_m. \]  

(28)

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

\[ D_1 = \int_0^\infty e^{-\frac{\gamma_m}{\gamma_m}} (D_1'') d\gamma_m, \]  

(29)

where

\[ D_1'' = \int_0^\infty e^{-\frac{\gamma_e}{\gamma_{se}}} D_1' d\gamma_e \]  

and

\[ D_1' = \int_0^\infty \log \left( 1 + \frac{\gamma_e}{d_e^a + \gamma_{se}} \right) e^{-\frac{\gamma_{sm}}{\gamma_{sm}}} d\gamma_{sm} = \frac{1}{\gamma_{sm}} \ln \left( 1 + \frac{\gamma_m}{d_m^a} \right) + e^{-\frac{\gamma_m}{\gamma_m}} E_1 \left( \frac{1 + \frac{\gamma_m}{d_m^a}}{\gamma_{sm}} \right). \]  

So, we have

\[ D_1'' = j_1' + j_2', \]  

(30)

where

\[ j_1 = \int_0^\infty \frac{e^{-\frac{\gamma_e}{\gamma_{se}}}}{\gamma_{sm}} \ln \left( 1 + \frac{\gamma_m}{d_m^a} \right) d\gamma_e = \frac{\gamma_{sm}}{\gamma_{se}} \ln \left( 1 + \frac{\gamma_m}{d_m^a} \right) \left( 1 - e^{-\frac{\gamma_m}{\gamma_m}} \right), \]  

(31)

and
\[
\begin{align*}
 f'_2 &= \int_0^{\nu_m} \frac{\gamma_m e^{-\frac{\nu_m}{\gamma_m}}}{\gamma_m} E_1 \left( \frac{1 + \frac{\nu_m}{\gamma_m} \frac{1}{d_m}}{\gamma_m} \right) d\gamma_m = \frac{\nu_m}{\gamma_m} E_1 \left( \frac{1 + \frac{\nu_m}{\gamma_m}}{\gamma_m} \right). 
\end{align*}
\] (32)

Thus, by replacing (31) and (32) in (30) and then (29), we have
\[
D_1 = k'_1 - k'_2 + k'_3 - k'_4,
\] (33)

where by exploiting (19) and (21), we have
\[
k'_1 = \int_0^{\infty} e^{-\nu_m} \frac{1}{\gamma_m} \ln \left( 1 + \frac{\gamma_m}{d_m} \right) d\gamma_m = -e^{-\nu_m} E_i \left( -\frac{\nu_m}{\gamma_m} \right),
\] (34)

\[
k'_2 = \int_0^{\infty} e^{-\nu_m} \frac{1}{\gamma_m} \ln \left( 1 + \frac{\gamma_m}{d_m} \right) d\gamma_m = -\frac{\nu_m}{\gamma_m} E_i \left( -\frac{\nu_m}{\gamma_m} \right),
\] (35)

\[
k'_3 = \int_0^{\infty} e^{-\nu_m} \frac{1}{\gamma_m} \ln \left( 1 + \frac{\gamma_m}{d_m} \right) d\gamma_m = -\frac{1}{\gamma_m} \frac{d_m}{\gamma_m} E_i \left( -\frac{\nu_m}{\gamma_m} \right),
\] (36)

\[
k'_4 = \int_0^{\infty} e^{-\nu_m} \frac{1}{\gamma_m} \ln \left( 1 + \frac{\gamma_m}{d_m} \right) d\gamma_m = e^{-\nu_m} \frac{1}{\gamma_m} \left( \ln \left( 1 + \frac{\gamma_m}{d_m} \right) - e^{-\nu_m} \frac{1}{\gamma_m} \frac{d_m}{\gamma_m} E_i \left( -\frac{\nu_m}{\gamma_m} \right) \right).
\] (37)

Similarly, for \(D_2\), we have
\[
D_2 = \int_0^{\infty} e^{-\frac{\nu_m}{\gamma_m}} (D'_2) d\gamma_m,
\] (38)

where
\[
D'_2 = \int_0^{\infty} e^{-\frac{\nu_m}{\gamma_m}} (D'_2) d\gamma_m = \frac{\nu_m}{\gamma_m} E_i \left( \frac{1 + \frac{\nu_m}{\gamma_m}}{\gamma_m} \right).
\] (39)

where by exploiting (18) and (20), we have
\[
i'_1 = \int_0^{\infty} \frac{\gamma_m}{\gamma_m} e^{-\frac{\nu_m}{\gamma_m}} \ln \left( 1 + \frac{\gamma_m}{d_m} \right) d\gamma_m
\]
\[
= \frac{\gamma_m}{\gamma_m} \left[ e^{-\nu_m} E_i \left( -\frac{\nu_m}{\gamma_m} \right) - e^{-\nu_m} \ln \left( 1 + \frac{\gamma_m}{d_m} \right) - e^{-\nu_m} E_i \left( -\frac{\nu_m}{\gamma_m} \right) \right],
\] (40)
\[
\begin{align*}
\ell'_2 &= \frac{\gamma'_m}{\gamma_{se}} e^{\frac{\gamma_e}{\gamma_e}} e^{\frac{1 + \frac{\gamma_m}{\gamma_e}}{\gamma_{se}}} E_1 \left( \frac{1 + \frac{\gamma_m}{\gamma_e}}{\gamma_{se}} \right) d\gamma_e = -\frac{\gamma_{se} e^{\frac{\gamma_e}{\gamma_e}}}{\frac{1}{\gamma_e} - \frac{1}{\gamma_{se} d^e}} \left[ e^{\frac{\gamma_e}{\gamma_e}} \left( \frac{\gamma_m + d^e_e}{\gamma_e} \right) \right], \\
&\quad - e^{\frac{\gamma_e}{\gamma_e}} \left( \frac{1}{\gamma_{se}} \right) E_1 \left( \frac{1 + \frac{\gamma_m}{\gamma_e}}{\gamma_{se}} \right) - e^{\frac{\gamma_e}{\gamma_e}} \left( \frac{d^e_e}{\gamma_e} \right) + E_1 \left( -\frac{1}{\gamma_{se}} \right). \\
\end{align*}
\]  

(41)

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

\[
D_2 = d'_1 - d'_2 - d'_3 - d'_4 + d'_5 + d'_6 - d_7.
\]

(42)

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

\[
d'_1 = \int_0^{\infty} e^{\frac{\gamma_e}{\gamma_m}} e^{\frac{\gamma_e}{\gamma_e}} E_1 \left( \frac{\gamma_m + d^e_e}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left[ E_1 \left( -\frac{d^e_e}{\gamma_e} \right) - e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right) d^e_e \right],
\]

(43)

\[
d'_2 = \int_0^{\infty} e^{\frac{\gamma_e}{\gamma_m}} e^{\frac{\gamma_e}{\gamma_e}} \ln \left( 1 + \frac{\gamma_e}{d^e_e} \right) \gamma_e = -\frac{\gamma_e}{\gamma_{se} + \gamma_e} e^{\frac{\gamma_e}{\gamma_e}} \left( \frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right) E_1 \left( -d^e_e \left( \frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right) \right).
\]

(44)

\[
d'_3 = \int_0^{\infty} e^{\frac{\gamma_e}{\gamma_m}} e^{\frac{\gamma_e}{\gamma_e}} E_1 \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -d^e_e \left( \frac{1}{\gamma_m} + \frac{1}{\gamma_e} \right) \right).
\]

(45)

\[
d'_4 = \int_0^{\infty} e^{\frac{\gamma_e}{\gamma_m}} e^{\frac{\gamma_e}{\gamma_e}} \left( \frac{1}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e.
\]

(46)

\[
d'_5 = \int_0^{\infty} e^{\frac{\gamma_e}{\gamma_m}} e^{\frac{\gamma_e}{\gamma_e}} \left( \frac{1}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e.
\]

(47)

\[
d'_6 = \int_0^{\infty} e^{\frac{\gamma_e}{\gamma_m}} e^{\frac{\gamma_e}{\gamma_e}} \left( \frac{1}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e.
\]

(48)

\[
d'_7 = \int_0^{\infty} e^{\frac{\gamma_e}{\gamma_m}} e^{\frac{\gamma_e}{\gamma_e}} \left( \frac{1}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e = e^{\frac{\gamma_e}{\gamma_e}} \left( -\frac{d^e_e}{\gamma_e} \right) \gamma_e.
\]

(49)
Therefore, from (26), we have

\[ R_i \leq k'_1 - k'_2 + k'_3 - d'_4 - d'_2 - d'_3 - d'_4 + d'_3 + d'_6 - d'_7 \]

\[ = \frac{\tau_m e^{\frac{d_k}{\tau_m}} Ei \left(-\frac{d_k}{\tau_m}\right)}{\tau_m e^{\frac{d_k}{\tau_m}}} - \left(1 - \frac{\tau_m}{\tau_e + \frac{1}{\tau_m}}\right) \left(1 - \frac{1 - \frac{\tau_m}{\tau_e + \frac{d_k}{\tau_m}}}{\tau_m + \tau_e}\right) \]

\[ \cdot Ei \left(-\frac{\tau_m}{\tau_e + \frac{d_k}{\tau_m}}\right) \left(1 - \frac{1}{\tau_m + \tau_e}\right) \]

\[ + \left(1 - \frac{\tau_m}{\tau_e + \frac{d_k}{\tau_m}}\right) \left(1 - \frac{1}{\tau_e + \frac{d_k}{\tau_m}}\right) \left(1 - \frac{1}{\tau_m + \tau_e + \frac{d_k}{\tau_m}}\right) \]

\[ \cdot Ei \left(-\frac{\tau_m}{\tau_m + \tau_e + \frac{d_k}{\tau_m}}\right) \left(1 - \frac{1}{\tau_m + \tau_e + \frac{d_k}{\tau_m}}\right). \]

(50)

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

Funding This research does not have any financial support. The authors are with the Faculty of Engineering at the Ferdowsi University of Mashhad, Iran.

Data Availability and Materials Not available.

Code Availability Not available.

Declarations

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

Ethical Approval This article does not contain any studies of the others.

References

1. Schneier, B. (1998). Cryptographic design vulnerabilities. *Computer, 31*(9), 29–33.
2. Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal, 28*(4), 656–715.
3. Wyner, A. D. (1975). The wire-tap channel. *Bell System Technical Journal, 54*(8), 1355–1387.
4. Csiszár, I., & Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory, 24*(3), 339–348.
5. Leung-Yan-Cheong, S., & Hellman, M. (1978). The Gaussian wire-tap channel. *IEEE Transactions on Information Theory, 24*(4), 451–456.
6. Bloch, M., Barros, J., Rodrigues, M. R. D., & McLaughlin, S. W. (2008). Wireless information-theoretic security. *IEEE Transactions on Information Theory, 54*(6), 2515–2534.
7. Ai, Y., Kong, L., & Cheffena, M. (2019). Secrecy outage analysis of double shadowed Rician channels. *Electronics Letters, 55*(13), 765–767.
8. Li, J., & Petropulu, A. P. (2011). Ergodic secrecy rate for multiple-antenna wiretap channels with Rician fading. *IEEE Transactions on Information Forensics and Security, 6*(3), 861–867.
9. Liu, X. (2012). Probability of strictly positive secrecy capacity of the Rician-Rician fading channel. *IEEE Wireless Communications Letters*, 2(1), 50–53.

10. Omri, A., & Hasna, M. O. (2018). 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(6), 3822–3833.

11. Kong, L., & Kaddoum, G. (2018). On physical layer security over the fisher-snedecor wiretap fading channels. *IEEE Access*, 6, 39466–39472.

12. Badarneh, O. S., Sofotasios, P. C., Muhaidat, S., Cotton, S. L., Rabie K., & Al-Dhahir, N. (2018). 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.

13. Ghadi, F. R., & Hodtani, G. A. (2020). Copula-based analysis of physical layer security performances over correlated Rayleigh fading channels. *IEEE Transactions on Information Forensics and Security*, 16, 431–440.

14. Shannon, C. E. (1958). Channels with side information at the transmitter. *IBM Journal of Research and Development*, 2(4), 289–293.

15. Gelfand, S. I., & Pinsker, M. S. (1980). Coding for Channels with Random Parameters. *Probl. Contr. Inform. Theory*, 9(1), 19–31.

16. Cover, T. M., & Chiang, M. (2002). Duality between channel capacity and rate distortion with two-sided state information. *IEEE Transactions on Information Theory*, 48(6), 1629–1638.

17. Anzabi-Nezhad, N. S., Hodtani, G. A., & Kakhki, M. M. (2012). Information theoretic exemplification of the receiver re-cognition and a more general version for the costa theorem. *IEEE Communications Letters*, 17(1), 107–110.

18. Anzabi-Nezhad, N. S., Hodtani, G. A., & Kakhki, M. M. (2015). A new and more general capacity theorem for the gaussian channel with two-sided input-noise dependent state information. *arXiv preprint arXiv:1507.04924*.

19. Chen, Y., Han, A. J., & Vinck. (2008). Wiretap channel with side information. *IEEE Transactions on Information Theory*, 54(1), 395–402.

20. Chia, Y.-K., & El Gamal, A. (2012). Wiretap channel with causal state information. *IEEE Transactions on Information Theory*, 58(5), 2838–2849.

21. Liu, W., & Chen, B. (2007). 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.

22. Xu, P., Ding, Z., Dai, X., & Leung, K. K. (2013). A general framework of wiretap channel with helping interference and state information. *IEEE Transactions on Information Forensics and Security*, 9(2), 182–195.

23. Costa, M. (1983). Writing on dirty paper (Corresp.). *IEEE Transactions on Information Theory*, 29(3), 439–441.

24. Aggarwal, V., Bennatan, A., & Robert Calderbank, A. (2009). On maximizing coverage in gaussian relay channels. *IEEE Transactions on Information Theory*, 55(6), 2518–2536.

25. Alizadeh, A., & Hodtani, G. A. (2015). Analysis of capacity and coverage region for Rayleigh fading MIMO relay channel. *International Journal of Communication Systems*, 28(8), 1462–1474.

26. Jeffrey, A., & Zwillinger, D. (Eds.). (2007). *Table of integrals, series, and products*. Elsevier.

27. Alkheir, A. A., & Ibknahla, M. (2013). An accurate approximation of the exponential integral function using a sum of exponentials. *IEEE Communications Letters*, 17(7), 1364–1367.

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Saeid Pakravan received the B.Sc. degree in communication engineering from University of Birjand, Birjand, Iran, in 2014. He received the M.Sc. degree in communication engineering from Guilan University, Rasht, Iran, in 2017. He is currently Ph.D student in Ferdowsi university of Mashhad. His area research interests include information theory, channel coding and wireless communication and physical layer security.

Ghosheh Abed Hodtani received the B.Sc. degree in electronics engineering and the M.Sc. degree in communications engineering, both from Isfahan University of Technology, Isfahan, Iran, in 1985 and 1987, respectively. He joined Electrical Engineering Dept., at Ferdowsi University of Mashhad, Mashhad, Iran, in 1987. He decided to pursue his studies in 2005 and received the Ph.D. degree (with excellent grade) from Sharif University of Technology, Tehran, Iran, in 2008, and he is a professor in electrical engineering since 2016. His research interests are in multi-user information theory, communication theory, wireless communications, information-theoretic learning and signal processing. Prof. Hodtani is the author of a textbook on Electrical Circuits, the winner of the best paper award at IEEE ICT-2010 and a member of technical program and steering committees of Iran Workshop on Communication and Information Theory (IWCIT).