entropy

MDPI

Article

Sensing-Assisted Secure Communications over Correlated Rayleigh Fading Channels

Martin Mittelbach [1], Rafael F. Schaefer [1], Matthieu Bloch [2], Aylin Yener [3] and Onur Günlü [4,*]

[1] Chair of Information Theory and Machine Learning, Technische Universität Dresden, 01062 Dresden, Germany; martin.mittelbach@tu-dresden.de (M.M.); rafael.schaefer@tu-dresden.de (R.F.S.)
[2] School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA 30332, USA; matthieu.bloch@ece.gatech.edu
[3] Department of Electrical and Computer Engineering, The Ohio State University, Columbus, OH 43210, USA; yener@ece.osu.edu
[4] Information Theory and Security Laboratory (ITSL), Linköping University, 58183 Linköping, Sweden
* Correspondence: onur.gunlu@liu.se

Abstract: We consider a secure integrated sensing and communication (ISAC) scenario, where a signal is transmitted through a state-dependent wiretap channel with one legitimate receiver with which the transmitter communicates and one honest-but-curious target that the transmitter wants to sense. The secure ISAC channel is modeled as two state-dependent fast-fading channels with correlated Rayleigh fading coefficients and independent additive Gaussian noise components. Delayed channel outputs are fed back to the transmitter to improve the communication performance and to estimate the channel state sequence. We establish and illustrate an achievable secrecy-distortion region for degraded secure ISAC channels under correlated Rayleigh fading, for which we show that the signal-to-interference-plus-noise is not a sufficient statistic. We also evaluate the inner bound for a large set of parameters to derive practical design insights. The presented results include parameter ranges for which the secrecy capacity of a classical wiretap channel setup is surpassed and for which the channel capacity is approached. Thus, we illustrate for correlated Rayleigh fading cases that our secure ISAC methods can (i) eliminate the need for the legitimate receiver to have a statistical advantage over the eavesdropper and (ii) provide communication security with minimal rate penalty.

Keywords: secure integrated sensing and communications; physical layer security; secure feedbacked systems; sensing-assisted secure communications; correlated fading for the feedbacked wiretap channel; secure 6G

check for updates

Academic Editor: Mario Martinelli

Received: 25 January 2025
Revised: 14 February 2025
Accepted: 19 February 2025
Published: 21 February 2025
Corrected: 27 March 2026

Citation: Mittelbach, M.; Schaefer, R.F.; Bloch, M.; Yener, A.; Günlü, O. Sensing-Assisted Secure Communications over Correlated Rayleigh Fading Channels. *Entropy* **2025**, *27*, 225. https://doi.org/10.3390/e27030225

Correction Statement: This article has been republished with a minor change. The change does not affect the scientific content of the article and further details are available within the backmatter of the website version of this article.

Copyright: © 2025 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Integrating the digital and physical world, envisioned for future communication systems, requires a network to react to changes in real-time through sensing and communication [1]. An example is a millimeter wave (mmWave) integrated sensing and communication (ISAC) system that aims to sense a target by estimating relevant channel parameters to fine-tune the communication scheme [2,3]. There are multiple recent information-theoretic studies of ISAC that extend previous results, such as [4,5]. Focusing on vehicular radar applications for mmWave systems, an information-theoretic model is proposed in [6] for ISAC. In this model, encoded messages are sent over a state-dependent channel with generalized feedback such that the state is only known at the receiver and the feedback is used to improve communication and to estimate the channel state. The

rate-distortion region is characterized for independent and identically distributed (i.i.d.) channel states and memoryless ISAC channels with strictly causal channel output feedback. Subsequent works have considered multiple access channels [7], broadcast channels [6], transmitter actions [8], covert communications [9,10], and low-latency scenarios [11–13].

As a single modality is used to both communicate with a legitimate receiver and detect a target, the sensing signal may carry sensitive information about the message communicated, which may then be leaked to a target. Since the signal power at the sensed target impacts both the secrecy and sensing performance, there exists a tradeoff between the two [2,14–18]. This tradeoff is characterized in [14] for degraded and reversely-degraded ISAC channels, when the transmitter aims to reliably communicate with the legitimate receiver by using the ISAC channel, estimate the channel state by using the channel output feedback, and keep the message hidden from the target that acts as an eavesdropper. The results in [14] show that it is possible to surpass the secrecy capacity by using the channel output feedback for secure ISAC applications, which strongly contrasts with and significantly improves on classical physical layer security methods.

In this work, we establish an achievable rate region for stochastically degraded secure ISAC channels under bivariate Rayleigh fading by using a Gaussian channel input. Since closed form expressions for this rate region remain elusive, we derive integral expressions from the involved differential entropies, which are amenable to simplified and stable numerical evaluations. Based on the evaluation results, fundamental insights are presented, including, in particular, parameter ranges for which secure-ISAC rates greater than the secrecy capacity can be achieved and for which the channel capacity is approached. Moreover, we provide accurate approximations, which allow easy-to-compute numerical evaluations.

1.1. Main Contributions

A summary of the main contributions of this work is as follows:

- We establish an inner bound on the rate region for stochastically degraded secure ISAC channels under bivariate Rayleigh fading by employing a Gaussian input. Our formulation shows how channel-output feedback can be leveraged to significantly improve the secrecy rate, enabling the system to surpass classical secrecy capacity results.
- We derive integral expressions stemming from the involved differential entropies in the achievable rate region. These expressions are amenable to numerically stable and simplified evaluations, facilitating practical performance analysis.
- For some integral expressions in the achievable rate region, we provide closed form solutions in special cases, such as high SNR regime and uncorrelated fading, which significantly simplifies the numerical evaluations.
- We provide fundamental insights into sensing-assisted secure communication systems, including parameter regimes where the achievable secure-ISAC rates can exceed the secrecy capacity and where approaching the channel capacity (i.e., the maximum possible rate without a secrecy constraint) can be possible. We further present accurate approximations that enable straightforward numerical evaluations and guide system design.

1.2. Paper Organization

In Section 2, we define the system model and metrics used. In Section 3, we provide the secrecy-distortion regions for correlated fading additive Gaussian noise (AGN) ISAC channels. In Section 4, we evaluate the provided secrecy-distortion regions for Gaussian inputs, which constitutes an achievable rate region. In Section 5, we illustrate the achievable rate regions by numerical calculations and provide the fundamental insights gained from them. In Section 6, we conclude the paper.

1.3. Notation

Uppercase letters denote random variables, while their corresponding lowercase letters represent specific realizations. For a continuous random variable X, the probability density function (pdf) is denoted as $f_X(x)$ and the cumulative distribution function (cdf) is given by $F_X(x) = \Pr[X \leq x]$. Calligraphic letters, such as $\mathcal{X}$, indicate sets, with the cardinality of a set given by $|\mathcal{X}|$. X^n represents a sequence $X_1, X_2, \ldots, X_n$. We represent $\mathrm{cov}[\cdot,\cdot]$ as covariance and $\mathrm{var}[\cdot]$ as variance, respectively.

$$I_0(x) = \frac{1}{\pi}\int_0^{\pi} e^{x\cos(\phi)}\mathrm{d}\phi \tag{1}$$

denotes the zeroth-order modified Bessel function of the first kind ([19], 10.25.2, 10.32.1).

$$\mathrm{Ei}(z) = -\int_{-z}^{\infty} \frac{\exp(-t)}{t}\,\mathrm{d}t \tag{2}$$

represents the exponential integral function ([19], 6.2.5). $\gamma = 0.577216\ldots$ denotes Euler's constant ([19], 5.2.3). Moreover,

$$\mathrm{erfi}(y) = -\imath\,\mathrm{erf}(\imath y) = -\frac{2\imath}{\sqrt{\pi}}\int_0^{\imath y} \exp\left(-t^2\right)\mathrm{d}t \tag{3}$$

denotes the imaginary error function ([19], 7.2.1), and ${}_pF_q(a_1,\ldots,a_p;b_1,\ldots,b_q;z)$ represents the generalized hypergeometric function ([19], 16.2.1).

2. System Model and Problem Definition

We consider the secure ISAC model depicted in Figure 1, comprising one legitimate receiver, one state estimator, and an eavesdropper (Eve). The transmitter wants to transmit a uniformly distributed message M from the finite message set $\mathcal{M}$ through a fast fading additive Gaussian noise (AGN) secure ISAC channel, in which i.i.d. fading channel coefficients (S_1^n, S_2^n) are causally estimated by the receiver and eavesdropper, respectively. The fading coefficients $(S_{1,i}, S_{2,i})$ with non-negative real-valued alphabet $\mathcal{S}_1 \times \mathcal{S}_2$ are correlated according to a known joint pdf f_{S_1,S_2}, but their realizations are not known by the transmitter. For discussions about how to extend the results to include complex fading channel coefficients and noise components, see ([20], Section V-A).

Given M, the transmitter generates the channel inputs X^n by using encoding functions $\mathsf{Enc}_i(\cdot)$ such that $X_i = \mathsf{Enc}_i(M, Z^{i-1})$ for all $i = [1:n]$, where Z^{i-1} is the delayed channel output feedback. We impose an average power constraint on the subsequent transmitted symbols, i.e., we have

$$\frac{1}{n}\sum_{i=1}^{n}\mathbb{E}[X_i^2] \leq P$$

for all messages M, where $\mathbb{E}[\cdot]$ denotes expectation. The channel output for the legitimate receiver at time i is

$$Y_{1,i} = S_{1,i}X_i + N_{1,i}$$

where $N_{1,i}$ are i.i.d. Gaussian distributed with zero mean, variance $\sigma_{N_1}^2$, and independent of $(S_{1,i}, S_{2,i}, X_i)$. The legitimate receiver observes the sequences (Y_1^n, S_1^n) and estimates the transmitted message as $\widehat{M} = \mathsf{Dec}(Y_1^n, S_1^n)$, where $\mathsf{Dec}(\cdot)$ is a decoding function. Similarly, the channel output for the eavesdropper at time i is

$$Y_{2,i} = S_{2,i}X_i + N_{2,i}$$

where $N_{2,i}$ are i.i.d. Gaussian distributed with zero mean, variance $\sigma^2_{N_2}$, and independent of $(S_{1,i}, S_{2,i}, X_i, N_{1,i})$. The transmitted message M should be kept secret from the eavesdropper that observes (Y_2^n, S_2^n). Finally, the state estimator observes both the channel output feedback

$$Z_{i-1} = f(Y_{1,i-1}, Y_{2,i-1})$$

and the codeword symbol X_i to estimate the fading channel coefficients (S_1^n, S_2^n) as $\widehat{S_j^n} = \mathsf{Est}_j(X^n, Z^n)$ for $j = 1, 2$, where $\mathsf{Est}_j(\cdot,\cdot)$ is an estimation function with range $\mathcal{S}_j^n$.

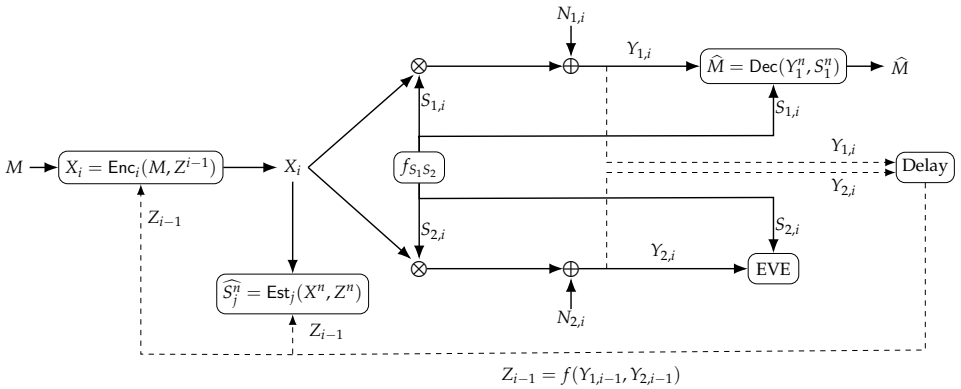


Figure 1. Secure ISAC model for $i = [1 : n]$ and $j = 1, 2$, for which the message M should be kept secret from the eavesdropper. We impose an average transmit power constraint on the channel input symbols X_i and assume independent AGN components $N_{1,i}$ and $N_{2,i}$. We principally consider perfect channel output feedback with unit symbol time delay, i.e., $Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1})$ such that the function $f(\cdot,\cdot)$ is the identity function.

For simplicity, we assume the deterministic processing function $f(\cdot,\cdot)$ is the identity function, so the channel output feedback is perfect, i.e., we have noiseless channel output feedback $Z_{i-1} = (Y_{1,i-1}, Y_{2,i-1})$. This simplification allows us to obtain fundamental insights into the optimal coding schemes and helps tackle the noisy feedback scenario, which is generally challenging; see, e.g., achievability results for wiretap channels with generalized output feedback in [21]. Note that the achievability proofs for wiretap channels generally require a local randomness source at the encoder, which is true also for the results given below. The randomness can be provided, e.g., by using hardware-intrinsic security primitives [22]. We next define the secrecy-distortion region for the secure correlated fast-fading ISAC problem.

Definition 1. *A secrecy-distortion tuple* (R, D_1, D_2) *is achievable for the secure correlated fast-fading ISAC problem if for any* $\epsilon > 0$*, there exist* $n \geq 1$*, one encoder-decoder pair, and two state estimators* $\mathsf{Est}_j(X^n, Y_j^n) = \widehat{S_j^n}$ *such that*

$$\Pr[M \neq \widehat{M}] \leq \epsilon \qquad (\textit{reliability}) \tag{4}$$

$$\log |\mathcal{M}| \geq n(R - \epsilon) \qquad (\textit{message rate}) \tag{5}$$

$$I(M; Y_2^n, S_2^n) \leq n\epsilon \qquad (\textit{secrecy}) \tag{6}$$

$$\mathbb{E}\left[d_j(S_j^n, \widehat{S_j^n})\right] \leq D_j + \epsilon \quad \textit{for } j = 1, 2 \qquad (\textit{distortions}) \tag{7}$$

where $d_j(\cdot,\cdot)$ *are averaged per-letter distortion metrics.*

The secrecy-distortion region $\mathcal{R}_{\text{S-ISAC}}$ *is the closure of the set of all achievable tuples for the secure correlated fast-fading ISAC problem under perfect channel output feedback.*

Since the transmitted message is independent of the channel state, the secrecy condition in (6) is equivalent to the inequality $I(M; Y_2^n | S_2^n) \leq n\epsilon$. Furthermore, there are ISAC models, such as in [23], that consider a practical application, in which only a part of the channel parameters are relevant for the transmitter. By not imposing the estimation of the exact channel state at the transmitter via adapting (7), one can extend our results for such practical settings.

3. Correlated Fading AGN ISAC Channel Secrecy-Distortion Regions

3.1. Secrecy-Distortion Region

We first provide the definition of a degraded ISAC channel; see also [6,14].

Definition 2. *An ISAC channel is* physically degraded *if X and (Y_2, S_2) are conditionally independent given (Y_1, S_1). Moreover, an ISAC channel is* stochastically degraded *if the joint probability distribution of (X, Y_1, S_1, Y_2, S_2) can be preserved by using a marginal probability distribution of (X, Y_1, S_1) such that the corresponding ISAC channel is physically degraded.*

Consider the secrecy-distortion region given in ([14], Theorem 1) for physically degraded secure ISAC channels with discrete-alphabet random variables and state estimators of the form $\mathsf{Est}_j(X^n, Y_1^n, Y_2^n) = \widehat{S_j^n}$. We evaluate the entropy terms in this rate region to characterize the secrecy-distortion region for the secure ISAC channel considered in this work.

The measures in the secrecy-distortion region in ([14], Theorem 1) remain valid for correlated fading channels with independent AGN components because of the following reasons:

(i) the outer bound applies to arbitrary random variables and does not assume any degradedness;
(ii) there is a discretization procedure to generalize the achievability proof to well-behaved continuous-alphabet random variables, such as the considered fading and noise distributions ([24] Remark 3.8); and
(iii) one can show that changing the estimator form does not change the entropy terms in the rate region, although achieved distortion levels might change since the estimators given in ([14], Theorem 1) should also be adapted.

Moreover, the state estimators considered in Definition 1 make the measures in ([14], Theorem 1) also valid for stochastically degraded channels, which follows because the constraints (4)–(7) in Definition 1 only depend on the marginal probability distributions of (X, Y_1, S_1) and (X, Y_2, S_2). This extension is important, as the practical secure ISAC model considered in this work is not physically degraded.

We next consider the secrecy-distortion region for stochastically degraded ISAC channels for our secure ISAC model. Below, expectations with subscripts of random variables indicate that we first calculate the argument of the expectation for fixed realization of the subscript and afterwards calculate the expectation with respect to the distribution of the subscript. Using ([15], Proposition 1), we obtain the following result.

Corollary 1. *The secrecy-distortion region for our secure ISAC model is the union w. r. t. all pdfs f_X of the rate-distortion tuples (R, D_1, D_2) satisfying*

$$R \leq \min \Big\{ \mathbb{E}_{S_1,S_2}\big[h(S_1X+N_1|S_2X+N_2)\big] - h(N_1) \tag{8a}$$

$$+ \mathbb{E}_X\big[h(S_1X+N_1|S_2)\big], \tag{8b}$$

$$\mathbb{E}_{S_1}\big[h(S_1X+N_1)\big] - h(N_1)\Big\}, \tag{8c}$$

$$D_j \geq \mathbb{E}[d_j(S_j,\widehat{S}_j))] \qquad \text{for } j=1,2 \tag{8d}$$

by using estimators of the form $\mathsf{Est}_j(X^n, Y_1^n, Y_2^n) = \widehat{S_j^n}$.

We provide a sufficient but not necessary condition to generate a stochastically degraded secure ISAC channel based on the stochastic ordering of the channel outputs Y_1 and Y_2.

Proposition 1. *The considered secure ISAC channel is stochastically degraded if* $S_1^2/\sigma_{N_1}^2$ *is* stochastically larger *than* $S_2^2/\sigma_{N_2}^2$*, i.e., if we have, for all* $s \geq 0$*,*

$$\bar{F}_{S_1^2}(s\,\sigma_{N_1}^2) \geq \bar{F}_{S_2^2}(s\,\sigma_{N_2}^2). \tag{9}$$

The proof of Proposition 1 follows from ([20], Lemma 3) after appropriate changes to account for the noise variances. For necessity discussions see ([25], Lemmas 1–4).

We next specify the correlated fast-fading distribution, for which we characterize an achievable secrecy-distortion region for stochastically degraded secure ISAC channels.

3.2. Bivariate Rayleigh Fading

Suppose the fading random variables (S_1, S_2) are distributed according to a bivariate Rayleigh fading distribution with pdf $f_{S_1S_2}(s_1, s_2)$ equal to

$$\frac{4s_1s_2}{\sigma_{S_1}^2\sigma_{S_2}^2(1-\rho^2)} \exp\left(-\frac{1}{1-\rho^2}\left(\frac{s_1^2}{\sigma_{S_1}^2}+\frac{s_2^2}{\sigma_{S_2}^2}\right)\right) I_0\left(\frac{2}{1-\rho^2}\sqrt{\rho^2\frac{s_1^2}{\sigma_{S_1}^2}\frac{s_2^2}{\sigma_{S_2}^2}}\right),\ s_1,s_2 \geq 0. \tag{10}$$

The parameters $\sigma_{S_1}^2$ and $\sigma_{S_2}^2$ in (10) are given as

$$\sigma_{S_j}^2 = \mathbb{E}\big[S_j^2\big], \quad j=1,2,$$

denoting (with a slight abuse of common notation) the second moments of S_1 and S_2. Furthermore, ρ^2, for $0 \leq \rho^2 < 1$, denotes the power correlation coefficient, i.e., we have

$$\mathrm{cor}(S_1^2, S_2^2) = \rho^2,$$

which is the Pearson correlation coefficient between S_1^2 and S_2^2. For later reference, we provide the marginal pdfs f_{S_1} and f_{S_2} of S_1 and S_2 as

$$f_{S_j}(s_j) = \frac{2\,s_j}{\sigma_{S_j}^2}\exp\left(-\frac{s_j^2}{\sigma_{S_j}^2}\right), \quad s_j \geq 0, \quad j=1,2, \tag{11}$$

as well as further moments

$$\mathbb{E}[S_j] = \sqrt{\frac{\pi}{4}\sigma_{S_j}^2},$$

$$\operatorname{var}[S_j] = \left(1 - \frac{\pi}{4}\right)\sigma_{S_j}^2,$$

$$\operatorname{cov}[S_1, S_2] = \sigma_{S_1}\sigma_{S_2}\left(E\left(\sqrt{\rho^2}\right) - \frac{1}{2}(1-\rho^2)K\left(\sqrt{\rho^2}\right) - \frac{\pi}{4}\right)$$

and

$$K(z) = \int_0^{\frac{\pi}{2}} \left(1 - z^2\sin^2(t)\right)^{-\frac{1}{2}} \mathrm{d}t, \tag{12}$$

$$E(z) = \int_0^{\frac{\pi}{2}} \left(1 - z^2\sin^2(t)\right)^{\frac{1}{2}} \mathrm{d}t \tag{13}$$

are the complete elliptic integrals of the first and second kind ([19], 19.2.4, 19.2.5, 19.2.8). Moreover, with the marginals (11) and basic transformations we obtain the complementary cdf of S_1^2 and S_2^2 as

$$\bar{F}_{S_j^2}(s_j) = \exp\left(-\frac{s_j}{\sigma_{S_j}^2}\right), \quad s_j \geq 0, \quad j = 1, 2. \tag{14}$$

Thus, for the bivariate Rayleigh distribution, the condition (9) on stochastic degradedness is equivalent to

$$\frac{\sigma_{S_2}^2}{\sigma_{N_2}^2} \leq \frac{\sigma_{S_1}^2}{\sigma_{N_1}^2}. \tag{15}$$

4. Achievable Rates for Gaussian Input

Given (8), the main goal is to find the maximum of its right-hand side with respect to the distribution f_X of the random variable X. However, this is a difficult optimization problem, so we instead provide an achievable rate for a Gaussian input X. Subsequently, we evaluate (8a)–(8c) for X being a zero-mean Gaussian random variable with positive variance P, where X is independent of (S_1, S_2, N_1, N_2).

4.1. Evaluation of Equation (8a)

Proposition 2. *Under the assumptions above, we have*

$$\mathbb{E}_{S_1,S_2}\left[h(S_1X + N_1 | S_2X + N_2)\right] - h(N_1) = \frac{1}{2}\int_0^\infty \log_2(1+s) f_S(s)\,\mathrm{d}s \tag{16}$$

where we have

$$f_S(s) = \sigma_1^2\sigma_2^2 \exp\left(\frac{\sigma_2^2}{2P(1-\rho^2)}\right) \exp\left(-\frac{\sigma_1^2 s + \sqrt{A(s)}}{2P(1-\rho^2)}\right) \times \left(\frac{1}{2P\sqrt{A(s)}} + \frac{\sigma_1^2 s + \sigma_2^2}{2PA(s)} + (1-\rho^2)\frac{\sigma_1^2 s + \sigma_2^2}{A(s)^{\frac{3}{2}}}\right) \tag{17}$$

with

$$A(s) = (\sigma_1^2 s)^2 + (2 - 4\rho^2)\sigma_1^2\sigma_2^2 s + (\sigma_2^2)^2, \tag{18}$$

$$\sigma_1^2 = \frac{\sigma_{N_1}^2}{\sigma_{S_1}^2}, \quad \sigma_2^2 = \frac{\sigma_{N_2}^2}{\sigma_{S_2}^2}. \tag{19}$$

Proof of Proposition 2. Fix $S_1 = s_1$ and $S_2 = s_2$ for some $s_1, s_2 \geq 0$. Then $(s_1X + N_1, s_2X + N_2)$ is jointly Gaussian with zero mean and covariance matrix

$$\begin{pmatrix} s_1^2 P + \sigma_{N_1}^2 & s_1 s_2 P \\ s_1 s_2 P & s_2^2 P + \sigma_{N_2}^2 \end{pmatrix} \tag{20}$$

since X, N_1, and N_2 are independent Gaussian random variables with positive variances P, $\sigma_{N_1}^2$, and $\sigma_{N_2}^2$. We have

$$\begin{aligned} h\big(s_1X + N_1 \,|\, s_2X + N_2\big) &= h\big(s_1X + N_1, s_2X + N_2\big) - h\big(s_2X + N_2\big) \\ &= \frac{1}{2}\log_2\left(2\pi e\sigma_{N_1}^2\right) + \frac{1}{2}\log_2\left(1 + \frac{s_1^2/\sigma_{N_1}^2}{s_2^2/\sigma_{N_2}^2 + 1/P}\right). \end{aligned} \tag{21}$$

Using (21), we can write

$$\mathbb{E}_{S_1,S_2}\big[h(S_1X + N_1|S_2X + N_2)\big] = h(N_1) + \frac{1}{2}\,\mathbb{E}_S\big[\log_2\left(1 + S\right)\big] \tag{22}$$

where the random variable S is given by

$$S = \frac{T_1}{T_2 + 1/P} \tag{23}$$

with $(T_1, T_2) = \left(S_1^2/\sigma_{N_1}^2, S_2^2/\sigma_{N_2}^2\right)$. Since S is a ratio of random variables, the pdf f_S of S has the following integral representation ([26], Equation 6.60):

$$f_S(s) = \int_{1/P}^{\infty} u f_{T_1,T_2}\left(su, u - 1/P\right) \mathrm{d}u, \quad s \geq 0 \tag{24}$$

where f_{T_1,T_2} is the joint pdf of (T_1, T_2) given by

$$f_{T_1,T_2}(t_1, t_2) = \frac{\sigma_1^2\sigma_2^2}{(1-\rho^2)} \exp\left(-\frac{1}{1-\rho^2}\left(\sigma_1^2 t_1 + \sigma_2^2 t_2\right)\right) I_0\left(\frac{2}{1-\rho^2}\sqrt{\rho^2\,\sigma_1^2 t_1\,\sigma_2^2 t_2}\right) \tag{25}$$

for $t_1, t_2 \geq 0$, where σ_1^2 and σ_2^2 are as specified in (19).

We substitute $\tilde{u} = (u - 1/P)$ in (24), plug it in (25), and then subsitute $v = \sqrt{\tilde{u}(\tilde{u} + 1/P)}$ to obtain

$$\begin{aligned} f_S(s) = \frac{\sigma_1^2\sigma_2^2}{1-\rho^2} \exp\left(\frac{\sigma_2^2}{2P(1-\rho^2)}\right) \exp\left(-\frac{\sigma_1^2 s}{2P(1-\rho^2)}\right) \\ \times \int_0^{\infty} \left[\frac{\theta v}{\sqrt{v^2 + \theta^2}} + v\right] \exp\left(-\alpha\sqrt{v^2 + \theta^2}\right) I_0\big(\beta v\big)\,\mathrm{d}v \end{aligned} \tag{26}$$

where we have

$$\alpha = \frac{\sigma_1^2 s + \sigma_2^2}{1-\rho^2}, \quad \beta = 2\frac{\sqrt{\rho^2\sigma_1^2\sigma_2^2\, s}}{1-\rho^2}, \quad \theta = \frac{1}{2P}. \tag{27}$$

Using this representation, we can directly apply ([27], Section 2.15.6.10) and ([27], Section 2.15.6.13). After collecting terms, we finally obtain the form of the density f_S given in (17), which completes the proof. □

In the case of uncorrelated fading ($\rho^2 = 0$) or for high SNR ($P \to \infty$), the representation given in Proposition 2 has the following closed form.

Corollary 2. *(i) For $\rho^2 = 0$, the density (17) simplifies to*

$$f_S(s) = \sigma_1^2\sigma_2^2 \exp\left(-\frac{\sigma_1^2 s}{P}\right)\left(\frac{1}{P(\sigma_1^2 s + \sigma_2^2)} + \frac{1}{(\sigma_1^2 s + \sigma_2^2)^2}\right) \tag{28}$$

resulting in

$$\begin{aligned}&\mathbb{E}_{S_1,S_2}\left[h(S_1X + N_1|S_2X + N_2)\right] - h(N_1)\\ &= \begin{cases} \dfrac{\sigma_2^2}{2\ln(2)(\sigma_1^2 - \sigma_2^2)}\left(\exp\left(\dfrac{\sigma_1^2}{P}\right)\mathrm{Ei}\left(-\dfrac{\sigma_1^2}{P}\right) - \exp\left(\dfrac{\sigma_2^2}{P}\right)\mathrm{Ei}\left(-\dfrac{\sigma_2^2}{P}\right)\right) & \text{if } \sigma_1^2 \neq \sigma_2^2 \\ \dfrac{1}{2\ln(2)}\left(1 + \left(\dfrac{\sigma_1^2}{P}\right)\exp\left(\dfrac{\sigma_1^2}{P}\right)\mathrm{Ei}\left(-\dfrac{\sigma_1^2}{P}\right)\right) & \text{if } \sigma_1^2 = \sigma_2^2 \end{cases}.\end{aligned} \tag{29}$$

(ii) For high SNR ($P \to \infty$), the density (17) simplifies to

$$\lim_{P\to\infty} f_S(s) = \sigma_1^2\sigma_2^2(1-\rho^2)\frac{\sigma_1^2 s + \sigma_2^2}{A(s)^{\frac{3}{2}}} \tag{30}$$

with $A(s)$ as in (18), which simplifies for $\sigma_1^2 = \sigma_2^2$ to

$$\lim_{P\to\infty} f_S(s) = \frac{(1-\rho^2)(s+1)}{\left(s^2 + (2-4\rho^2)s + 1\right)^{\frac{3}{2}}} \tag{31}$$

resulting in

$$\begin{aligned}&\mathbb{E}_{S_1,S_2}\left[h(S_1X + N_1|S_2X + N_2)\right] - h(N_1)\\ &\qquad = \frac{1}{4\sqrt{\rho^2}}\log_2\left(\frac{1+\sqrt{\rho^2}}{1-\sqrt{\rho^2}}\right) + \frac{1}{4}\log_2\left(1-\rho^2\right).\end{aligned} \tag{32}$$

Proof. *Proof of part (i)*: The density (28) follows by (17) for $\rho^2 = 0$. Plugging (28) into (16) and using the substitution $t = s + 1$, we obtain the equivalent integral

$$\int_1^\infty \frac{\sigma_1^2\sigma_2^2}{2}\exp\left(-\frac{\sigma_1^2}{P}(t-1)\right)\log_2(t)\left(\frac{\sigma_1^2(t-1) + \sigma_2^2 + P}{P(\sigma_1^2(t-1) + \sigma_2^2)^2}\right)\mathrm{d}t. \tag{33}$$

The antiderivative of the integrand in (33) for $\sigma_1^2 \neq \sigma_2^2$ is given by

$$\begin{aligned}&\frac{\sigma_2^2}{2\ln(2)(\sigma_1^2 - \sigma_2^2)}\left(\exp\left(\frac{\sigma_2^2}{P}\right)\mathrm{Ei}\left(-\frac{\sigma_1^2(t-1) + \sigma_2^2}{P}\right) - \exp\left(\frac{\sigma_1^2}{P}\right)\mathrm{Ei}\left(-\frac{\sigma_1^2}{P}t\right)\right)\\ &\qquad - \frac{\sigma_2^2}{2(\sigma_1^2(t-1) + \sigma_2^2)}\exp\left(-\frac{\sigma_1^2}{P}(t-1)\right)\log_2(t)\end{aligned} \tag{34}$$

which can be obtained by using, e. g., MATHEMATICA. The antiderivative can be directly verified by calculating the derivative of (34) and collecting the terms to re-obtain the integrand of (33). Evaluating (34) for the integration limits of (33), we obtain

$$t = 1: \quad -\frac{\sigma_2^2}{2\ln(2)(\sigma_1^2-\sigma_2^2)}\left(\exp\left(\frac{\sigma_1^2}{P}\right)\mathrm{Ei}\left(-\frac{\sigma_1^2}{P}\right)-\exp\left(\frac{\sigma_2^2}{P}\right)\mathrm{Ei}\left(-\frac{\sigma_2^2}{P}\right)\right), \tag{35}$$

$$t \to \infty: \quad 0. \tag{36}$$

Substracting (35) from (36) yields the first part of (29).

Similarly, for the antiderivative of the integrand in (33) for $\sigma_1^2 = \sigma_2^2$, we obtain

$$-\frac{1}{2\ln(2)\,t}\exp\left(-\frac{\sigma_1^2}{P}(t-1)\right)\left(1+\left(\frac{\sigma_1^2}{P}t\right)\exp\left(\frac{\sigma_1^2}{P}t\right)\mathrm{Ei}\left(-\frac{\sigma_1^2}{P}t\right)\right)-\frac{1}{2t}\log_2(t). \tag{37}$$

Evaluating (37) for the integration limits of (33), we obtain

$$t = 1: \quad -\frac{1}{2\ln(2)}\left(1+\left(\frac{\sigma_1^2}{P}\right)\exp\left(\frac{\sigma_1^2}{P}\right)\mathrm{Ei}\left(-\frac{\sigma_1^2}{P}\right)\right), \tag{38}$$

$$t \to \infty: \quad 0. \tag{39}$$

Substracting (38) from (39) yields the second part of (29).

Proof of part (ii): The densities (30) and (31) are directly obtained from (17) for $P \to \infty$ and $\sigma_1^2 = \sigma_2^2$. Plugging (31) into (16) and using the substitution $t = s + 1$, we obtain the equivalent integral

$$\int_1^\infty \frac{(1-\rho^2)\,t\log_2(t)}{2\left(t^2+4\rho^2(1-t)\right)^{\frac{3}{2}}}\,\mathrm{d}t. \tag{40}$$

The antiderivative of the integrand in (40) is given by

$$\begin{aligned}\frac{1}{4}\Bigg(\left(\frac{1}{\sqrt{\rho^2}}+\frac{(t-2)}{B(t)}\right)\log_2(t)-\frac{1}{\sqrt{\rho^2}}\log_2\left(\rho^2(2-t)+\sqrt{\rho^2}\,B(t)\right)\\ -\log_2\left(t-2\rho^2+B(t)\right)\Bigg)\end{aligned} \tag{41}$$

where we have $B(t) = \sqrt{t^2+4\rho^2(1-t)}$, and which can be directly verified by calculating the derivative of (41) and collecting the terms to re-obtain the integrand of (40). Evaluating (41) for the integration limits of (40), we obtain

$$t = 1: \quad \frac{1}{4}\left(\log_2\left(2(1-\rho^2)\right)+\frac{1}{\sqrt{\rho^2}}\log_2\left(\sqrt{\rho^2}\left(1+\sqrt{\rho^2}\right)\right)\right), \tag{42}$$

$$t \to \infty: \quad \frac{1}{4}\left(1+\log_2\left(\sqrt{\rho^2}\left(1-\sqrt{\rho^2}\right)\right)\right) \tag{43}$$

where we use L'Hôpital's rule to calculate the limit $t \to \infty$. Substracting (42) from (43) yields (32). □

4.2. Evaluation of Equation (8b)

First, we rewrite (8b) as

$$\mathbb{E}_X\left[h(S_1X+N_1|S_2)\right] = \mathbb{E}_X\left[h(S_1X+N_1,S_2)\right]-h(S_2). \tag{44}$$

Using the marginal pdf of S_2, we obtain

$$\begin{aligned} h(S_2) &= -\int_0^\infty f_{S_2}(s_2)\log_2\left(f_{S_2}(s_2)\right)\mathrm{d}s_2 \\ &= -2\log_2\left(\frac{2}{\sigma_{S_2}}\right)\int_0^\infty u\exp\left(-u^2\right)\mathrm{d}u - 2\int_0^\infty u\exp\left(-u^2\right)\log_2(u)\,\mathrm{d}u \\ &\quad + \frac{2}{\ln(2)}\int_0^\infty u^3\exp\left(-u^2\right)\mathrm{d}u \\ &= \frac{1}{\ln(2)}\left(1+\frac{\gamma}{2}\right) + \frac{1}{2}\log_2\left(\frac{\sigma_{S_2}^2}{4}\right) \end{aligned} \tag{45}$$

using the substitution $u = s_2/\sigma_{S_1}$ and the integral relations

$$\int_0^\infty u\exp(-u^2)\,\mathrm{d}u = \int_0^\infty u^3\exp(-u^2)\,\mathrm{d}u = \frac{1}{2} \tag{46}$$

and

$$\int_0^\infty u\exp(-u^2)\ln(u)\,\mathrm{d}u = -\frac{\gamma}{4}. \tag{47}$$

The evaluation of $\mathbb{E}_X\left[h(S_1X+N_1,S_2)\right]$ requires the following calculations. Let $Y_1(x) = xS_1 + N_1$. Then, the joint pdf of $\left(Y_1(x),S_2\right)$ is given for $x > 0$ by the convolution integral

$$f_{Y_1(x),S_2}(y_1,s_2) = \int_0^\infty \frac{1}{x} f_{S_1,S_2}\left(\frac{t}{x},s_2\right) f_{N_1}(y_1-t)\,\mathrm{d}t \tag{48}$$

for $-\infty < y_1 < \infty$ and $s_2 \geq 0$. Furthermore, we have

$$h(xS_1+N_1,S_2) = -\int_{y_1=-\infty}^{\infty}\int_{s_2=0}^{\infty} f_{Y_1(x),S_2}(y_1,s_2)\log_2\left(f_{Y_1(x),S_2}(y_1,s_2)\right)\mathrm{d}y_1\mathrm{d}s_2. \tag{49}$$

Due to symmetry, we obtain

$$\mathbb{E}_X\left[h(S_1X+N_1,S_2)\right] = 2\int_0^\infty h(xS_1+N_1,S_2)f_X(x)\,\mathrm{d}x. \tag{50}$$

As we can evaluate the convolution integral in (48) numerically, we rely on numerical calculations also for (49) and (50).

An upper bound of $\mathbb{E}_X\left[h(S_1X+N_1|S_2)\right]$, for which the numerical evaluation is much easier, is the following.

Proposition 3. *Under the assumptions above, we have*

$$\begin{aligned} \mathbb{E}_X\left[h(S_1X+N_1|S_2)\right] \;\leq\; & \frac{1}{2}\log_2\left(2(\pi\mathrm{e})^2\sigma_{S_1}^2\tilde{c}\,P\right) + \frac{\pi}{2\ln(2)}\,\mathrm{erfi}\left(\sqrt{\frac{\tilde{\sigma}_1^2}{2\tilde{c}\,P}}\right) + 1 \\ & - \frac{1}{\ln(2)}\left(\frac{\tilde{\sigma}_1^2}{2\tilde{c}\,P}\,{}_2F_2\left(1,1;\tfrac{3}{2},2;\frac{\tilde{\sigma}_1^2}{2\tilde{c}\,P}\right) + 1 + \gamma\right) \end{aligned} \tag{51}$$

with the parameters

$$\tilde{\sigma}_1^2 = \left(1-\frac{\pi}{4}\right)\frac{\sigma_{N_1}^2}{\sigma_{S_1}^2}, \tag{52}$$

$$\tilde{c} = \left(1 - \frac{\pi}{4}\right)^2 \left(1 - \operatorname{cor}[S_1, S_2]^2\right) \tag{53}$$

where we have

$$\operatorname{cor}[S_1, S_2] = \frac{\operatorname{cov}[S_1, S_2]}{\sqrt{\operatorname{var}[S_1]\operatorname{var}[S_2]}} = \left(1 - \frac{\pi}{4}\right)^{-1} \left(E\left(\sqrt{\rho^2}\right) - \frac{1}{2}(1-\rho^2)K\left(\sqrt{\rho^2}\right) - \frac{\pi}{4}\right) \tag{54}$$

with $K(\cdot)$ and $E(\cdot)$ the elliptic integrals given in (12) *and* (13)*, respectively.*

Proof of Proposition 3. Fix $X = x$ for some $x \in \mathbb{R}$. Then, the differential entropy $h\big(xS_1 + N_1, S_2\big)$ is bounded by

$$h\big(xS_1 + N_1, S_2\big) \leq \frac{1}{2}\log_2\left((2\pi\mathrm{e})^2\Big(\operatorname{var}\big[xS_1 + N_1\big]\operatorname{var}\big[S_2\big] - \operatorname{cov}\big[xS_1 + N_1, S_2\big]^2\Big)\right) \tag{55}$$

as a result of the differential entropy maximizing property of the Gaussian distribution with a given covariance matrix. Since S_1, S_2, and N_1 are independent, we have

$$\operatorname{var}\big[xS_1 + N_1\big] = x^2\operatorname{var}[S_1] + \operatorname{var}[N_1], \tag{56}$$

$$\operatorname{cov}\big[xS_1 + N_1, S_2\big] = x\operatorname{cov}\big[S_1, S_2\big]. \tag{57}$$

Inserting the definitions of $\operatorname{var}[S_1]$ and $\operatorname{cov}\big[S_1, S_2\big]$, we obtain

$$h\big(xS_1 + N_1, S_2\big) \leq a + \frac{1}{2}\log_2\left(\tilde{c}\,x^2 + \tilde{\sigma}_1^2\right) \tag{58}$$

where $\tilde{c}$ and $\tilde{\sigma}_1^2$ are as defined in (52), (53), and $a = \frac{1}{2}\log_2\left((2\pi\mathrm{e})^2\sigma_{S_1}^2\sigma_{S_2}^2\right)$. Due to the monotonicity of the integral and symmetry properties, we have

$$\begin{aligned}\mathbb{E}_X\big[h(S_1X + N_1|S_2)\big] &= \mathbb{E}_X\big[h(S_1X + N_1, S_2)\big] - h(S_2)\\ &\leq 2\int_0^\infty \left(a + \frac{1}{2}\log_2\left(\tilde{c}\,x^2 + \tilde{\sigma}_1^2\right)\right) f_X(x)\,\mathrm{d}x - h(S_2).\end{aligned} \tag{59}$$

To evaluate the integral, we use the substitution $u = x^2$, the correspondence ([28], 2.6.23.4) (please note that in ([28], 2.6.23.4), the sign before ${}_2F_2(\cdot;\cdot;\cdot)$ is incorrect), and the identities $\operatorname{erfi}(y) = -\imath\operatorname{erf}(\imath y)$ and $\frac{\sqrt{\pi}}{2z}\operatorname{erf}(z) = {}_1F_1\left(\frac{1}{2};\frac{3}{2};-z^2\right)$ ([19], 13.6.7). Applying the expression in (45) yields the bound for $\mathbb{E}_X\big[h(S_1X + N_1|S_2)\big]$ given in Proposition 3. □

The representation in Proposition 2 as a one-dimensional integral is particularly convenient for numerical evaluations and is used in Section 5.

4.3. Evaluation of Equation (8c)

Proposition 4. *Under the assumptions above, we have*

$$\mathbb{E}_{S_1}\big[h(S_1X + N_1)\big] - h(N_1) = -\frac{1}{2\ln(2)}\exp\left(\frac{1}{P}\right)\operatorname{Ei}\left(\frac{1}{P}\right). \tag{60}$$

Proof of Proposition 4. Fix $S_1 = s_1$ for some $s_1 \geq 0$. Then, $s_1X + N_1$ is a Gaussian random variable with zero mean and variance $s_1^2P + \sigma_{N_1}^2$ since X and N_1 are independent Gaussian random variables with positive variances P and $\sigma_{N_1}^2$. For the differential entropy $h\big(s_1X + N_1\big)$, we obtain

$$h\big(s_1X + N_1\big) = \frac{1}{2}\log_2\left(2\pi\mathrm{e}\sigma_{N_1}^2P\right) + \frac{1}{2}\log_2\left(\frac{s_1^2}{\sigma_{N_1}^2} + \frac{1}{P}\right). \tag{61}$$

Thus, we can write

$$\mathbb{E}_{S_1}\left[h(S_1X+N_1)\right] = h(N_1) + \frac{1}{2}\log_2\left(P\right) + \frac{1}{2}\,\mathbb{E}_{T_1}\left[\log_2\left(T_1 + 1/P\right)\right] \tag{62}$$

where $T_1 = S_1^2/\sigma_{N_1}^2$. With the marginal pdf of S_1 and basic density transformation, we obtain the pdf $f_{T_1}(t_1) = \exp(-t_1)$ for $t_1 \geq 0$ of the random variable T_1 such that we have

$$\begin{aligned}\mathbb{E}_{T_1}\left[\log_2\left(T_1 + 1/P\right)\right] &= \int_0^\infty \log_2\left(t_1 + 1/P\right)\exp(-t_1)\,\mathrm{d}t_1 \\ &= -\log_2(P) - \frac{1}{\ln(2)}\exp\left(\frac{1}{P}\right)\mathrm{Ei}\left(-\frac{1}{P}\right).\end{aligned} \tag{63}$$

The integral is solved using the substitution $u = (t_1 + 1/P)$ and integration by parts. Collecting the terms yields (60). □

5. Numerical Results and Discussions

We next evaluate the results of Section 4 numerically for interesting parameter regimes. To simplify notation, we denote the sum of (8a) and (8b) by R_α and the sum of (8a) and the upper bound (51) of (8b) by $R_{\alpha,\mathrm{ub}}$, respectively. Furthermore, we denote (8c) by R_β. With this notation, we have for the achievable rate in Section 4

$$R \leq \min\left\{R_\alpha, R_\beta\right\} \leq \min\left\{R_{\alpha,\mathrm{ub}}, R_\beta\right\}. \tag{64}$$

Based on the representation in (16)–(18) as a one-dimensional integral, we numerically evaluate (8a). Similarly, the upper bound in (51) is numerically evaluated, and the same applies to (8c) using (60). However, the numerical evaluation of (8b) is more involved. First, we numerically calculate the convolution integral in (48) on a sufficiently-dense grid for the variables y_1 and s_2. Then, we numerically calculate the differential entropy $h(xS_1 + N_1, S_2)$ using (49) based on an interpolated version of the density $f_{Y_1(x),S_2}(y_1, s_2)$. Repeating these calculations for a sufficiently dense set of values x, we numerically calculate $\mathbb{E}_X\left[h(S_1X + N_1, S_2)\right]$ using (50) and an interpolated version of the function $x \mapsto h(xS_1 + N_1, S_2)$. Combining with (45), we finally obtain (8b).

We consider a stochastically degraded secure ISAC channel, i. e., we assume that the chosen parameter values satisfy the inequality (15). Moreover, we assume that $\sigma_{N_1}^2 > \sigma_{N_2}^2$, which is the interesting regime where the corresponding wiretap channel without fading does not allow secure communication. The parameter sets satisfying these conditions for which we subsequently discuss the numerical results below are given in Table 1.

Table 1. Parameter sets for numerical calculations.

$\rho^2 \in \{0.01, 0.50, 0.81, 0.90\}$	
$\sigma_{N_1}^2 = 1$	$\sigma_{N_2}^2 = 0.50$
$\sigma_{S_1}^2 \in \{0.10, 0.50, 1.00\}$	$\sigma_{S_2}^2 = \sigma_{S_1}^2/10\sigma_{N_2}^2$

We compute the results for R_α, $R_{\alpha,\mathrm{ub}}$, and R_β as a function of the transmit power P for different values of the power correlation coefficient ρ^2. The corresponding curves are shown in Figures 2–5. For the row of subfigures in each figure, the parameter $\sigma_{S_1}^2$ is modified from left to right, whereas $\sigma_{N_1}^2 = 1$, $\sigma_{N_2}^2 = 0.5$, and $\sigma_{S_2}^2 = \sigma_{S_1}^2/10\sigma_{N_2}^2$ are fixed.

We next list our conclusions for a degraded secure ISAC channel with correlated Rayleigh fading for the parameter ranges given above, drawn from the computations mentioned above. From (60), we observe that R_β is only a function of the transmit power P

such that the curves of R_β are the same in all diagrams. From (16)–(18), we observe that (8a) as a summand of R_α and $R_{\alpha,\mathrm{ub}}$ is a function of ρ^2, P, and the parameter ratios $\sigma_{N_1}^2/\sigma_{S_1}^2$ and $\sigma_{N_2}^2/\sigma_{S_2}^2$. Similarly, the upper bound (51) as a summand of $R_{\alpha,\mathrm{ub}}$ is a function of ρ^2, P, $\sigma_{S_1}^2$, and $\sigma_{N_1}^2$ and it does not depend on $\sigma_{S_2}^2$ and $\sigma_{N_2}^2$.

The results show that $R_{\alpha,\mathrm{ub}}$ and R_α curves behave highly similar with a small constant gap. Thus, for most of the parameter constellations, the much-easier-to-calculate $R_{\alpha,\mathrm{ub}}$, instead of R_α, can be used to interpret the results.

Furthermore, we observe the following monotonicities: R_α increases for increasing parameters $\sigma_{S_1}^2$ and for decreasing parameters ρ^2. Moreover, we observe that increasing the power correlation ρ^2 from 0 to 0.50 has only a minor effect, whereas the impact of increasing ρ^2 from 0.50 to 0.81 is much stronger. This trend continues when ρ^2 further increases from 0.81 to 0.90.

The interesting regime in which the channel capacity is approached is when R_β determines the right-hand side of (8). Figures 2–5 show that the range of power P for which the channel capacity is approached stretches over all considered power values except when the power correlation coefficient ρ^2 is high combined with a low fading parameter $\sigma_{S_1}^2$, as can be observed in the leftmost diagrams of Figures 4 and 5. Thus, we observe that in the low power regime, channel capacity is always approached irrespective of the values of the remaining parameters.

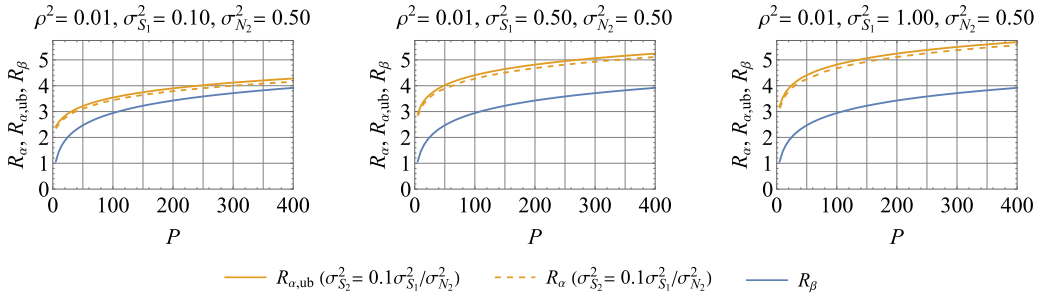


Figure 2. R_α, $R_{\alpha,\mathrm{ub}}$, and R_β for power correlation coefficient $\rho^2 = 0.01$.

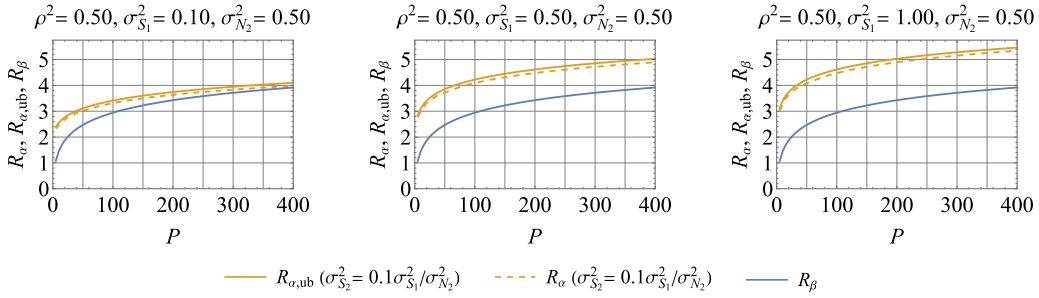


Figure 3. R_α, $R_{\alpha,\mathrm{ub}}$, and R_β for power correlation coefficient $\rho^2 = 0.50$.

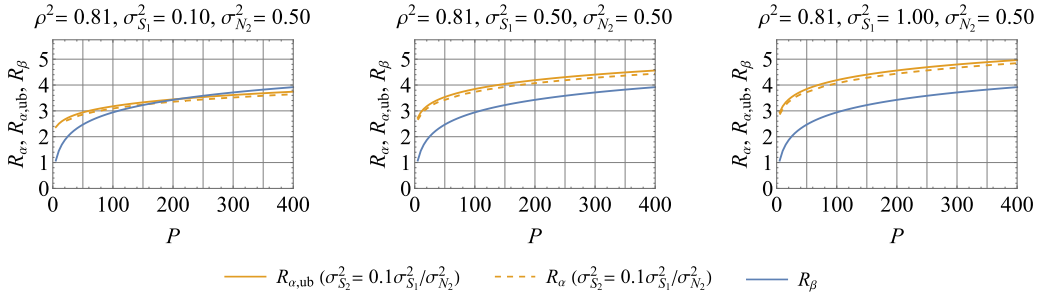


Figure 4. R_α, $R_{\alpha,\mathrm{ub}}$, and R_β for power correlation coefficient $\rho^2 = 0.81$.

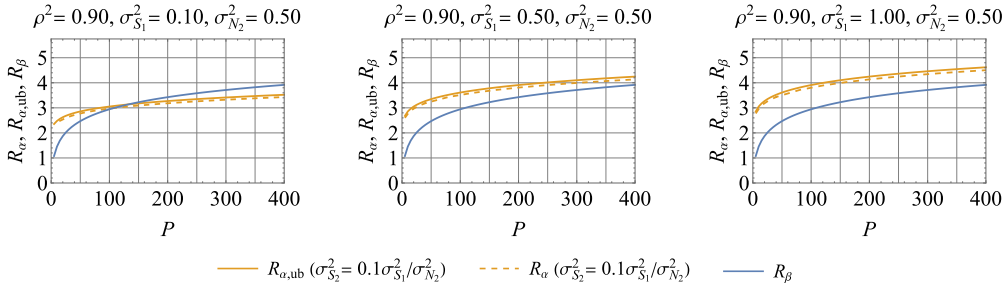


Figure 5. R_α, $R_{\alpha,\mathrm{ub}}$, and R_β for power correlation coefficient $\rho^2 = 0.90$.

6. Conclusions

We considered a new secure ISAC model for a state-dependent wiretap channel under correlated Rayleigh fading with channel output feedback. We derived and evaluated an achievable secrecy-distortion region and demonstrated conditions where the secrecy capacity can be surpassed, unlike classical physical layer security methods, which provides fundamental insights essential for designing optimal secure ISAC systems for future communication systems. We remark that extensions of our model to consider active attacks, as in, e.g., [29], and evaluations for more practical ISAC channel models, as in, e.g., [30], are also important for secure ISAC research.

Author Contributions: Conceptualization, M.M., R.F.S., M.B., A.Y. and O.G.; methodology, M.M., R.F.S. and O.G.; mathematical analysis, M.M., R.F.S., M.B. and O.G.; validation, M.M. and O.G.; writing—original draft preparation, M.M., R.F.S. and O.G.; writing—review and editing, M.B., A.Y. and O.G.; project management, M.B., A.Y. and O.G. All authors have read and agreed to this version of the manuscript.

Funding: This work has been supported by the German Federal Ministry of Education and Research (BMBF) through the research hub *6G-life* under grant 16KISK001K, the German Research Foundation (DFG) as part of Germany's Excellence Strategy—EXC 2050/1—Project ID 390696704—Cluster of Excellence *CeTI*, the U.S. National Science Foundation (NSF) under grant CCF 1955401 and grant CCF 2148400 as part of the Resilient and Intelligent NextG Systems (RINGS) Program, the U.S. Department of Transportation under grant 69A3552348327 for the CARMEN+ University Transportation Center, the ZENITH Research and Leadership Career Development Fund, and the ELLIIT funding endowed by the Swedish government.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Wild, T.; Braun, V.; Viswanathan, H. Joint Design of Communication and Sensing for Beyond 5G and 6G Systems. *IEEE Access* **2021**, *9*, 30845–30857. [CrossRef]
2. Wei, Z.; Liu, F.; Masouros, C.; Su, N.; Petropulu, A.P. Towards Multi-Functional 6G Wireless Networks: Integrating Sensing, Communication and Security. *IEEE Commun. Mag.* **2022**, *60*, 65–71. [CrossRef]
3. Fettweis, G.; Schlüter, M.; Thomä, R.; Boche, H.; Schotten, H.; Barreto, A.; Mueller, A.; Bilgic, A.; Hildebrand, C.; Schupke, D.; et al. Joint Communications & Sensing—Common Radio-Communications and Sensor Technology. *VDE Positionspapier* **2021**.
4. Zhang, W.; Vedantam, S.; Mitra, U. Joint Transmission and State Estimation: A Constrained Channel Coding Approach. *IEEE Trans. Inf. Theory* **2011**, *57*, 7084–7095. [CrossRef]
5. Wymeersch, H.; Shrestha, D.; de Lima, C.M.; Yajnanarayana, V.; Richerzhagen, B.; Keskin, M.F.; Schindhelm, K.; Ramirez, A.; Wolfgang, A.; de Guzman, M.F.; et al. Integration of Communication and Sensing in 6G: A Joint Industrial and Academic Perspective. In Proceedings of the IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications, Helsinki, Finland, 13–16 September 2021; pp. 1–7.
6. Ahmadipour, M.; Kobayashi, M.; Wigger, M.; Caire, G. An Information-Theoretic Approach to Joint Sensing and Communication. *IEEE Trans. Inf. Theory* **2024**, *70*, 1124–1146. [CrossRef]

7. Kobayashi, M.; Hamad, H.; Kramer, G.; Caire, G. Joint State Sensing and Communication over Memoryless Multiple Access Channels. In Proceedings of the IEEE International Symposium on Information Theory, Paris, France, 7–12 July 2019; pp. 270–274.
8. Welling, T.; Günlü, O.; Yener, A. Transmitter Actions for Secure Integrated Sensing and Communication. In Proceedings of the IEEE International Symposium on Information Theory, Athens, Greece, 7–12 July 2024; pp. 2580–2585.
9. Wang, S.Y.; Chang, M.C.; Bloch, M.R. Covert Joint Communication and Sensing under Variational Distance Constraint. In Proceedings of the Annual Conference on Information Sciences and Systems, Princeton, NJ, USA, 13–15 March 2024; pp. 1–6.
10. Wang, X.; Fei, Z.; Liu, P.; Zhang, J.A.; Wu, Q.; Wu, N. Sensing-Aided Covert Communications: Turning Interference Into Allies. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 10726–10739. [CrossRef]
11. Welling, T.; Günlü, O.; Yener, A. Low-latency Secure Integrated Sensing and Communication with Transmitter Actions. In Proceedings of the IEEE International Workshop on Signal Processing Advances in Wireless Communications, Lucca, Italy, 10–13 September 2024; pp. 351–355.
12. Günlü, O.; Bloch, M.; Schaefer, R.F.; Yener, A. Nonasymptotic Performance Limits of Low-Latency Secure Integrated Sensing and Communication Systems. In Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing, Seoul, Republic of Korea, 14–19 April 2024; pp. 12971–12975.
13. Nikbakht, H.; Wigger, M.; Shamai, S.; Poor, H.V. Integrated Sensing and Communication in the Finite Blocklength Regime. In Proceedings of the IEEE International Symposium on Information Theory, Athens, Greece, 7–12 July 2024; pp. 2790–2795.
14. Günlü, O.; Bloch, M.; Schaefer, R.F.; Yener, A. Secure Integrated Sensing and Communication. *IEEE J. Sel. Inf. Theory* **2023**, *4*, 40–53. [CrossRef]
15. Günlü, O.; Bloch, M.; Schaefer, R.F.; Yener, A. Secure Integrated Sensing and Communication for Binary Input Additive White Gaussian Noise Channels. In Proceedings of the IEEE International Symposium on Joint Communications & Sensing, Seefeld, Austria, 5–7 March 2023; pp. 1–6.
16. Ahmadipour, M.; Wigger, M.; Shamai, S. Integrated Communication and Receiver Sensing with Security Constraints on Message and State. In Proceedings of the IEEE International Symposium on Information Theory, Taipei, Taiwan, 25–30 June 2023; pp. 2738–2743.
17. Dong, F.; Liu, F.; Lu, S.; Xiong, Y. Secure ISAC Transmission With Random Signaling. In Proceedings of the IEEE GLOBECOM Workshops, Kuala Lumpur, Malaysia, 4–8 December 2023; pp. 407–412.
18. Su, N.; Liu, F.; Masouros, C. Sensing-Assisted Eavesdropper Estimation: An ISAC Breakthrough in Physical Layer Security. *IEEE Trans. Wirel. Commun.* **2024**, *23*, 3162–3174. [CrossRef]
19. Olver, F.W.J.; Lozier, D.W.; Boisvert, R.F.; Clark, C.W. (Eds.) *NIST Handbook of Mathematical Functions*; Cambridge University Press: Cambridge, UK, 2010.
20. Tse, D.; Yates, R. Fading Broadcast Channels with State Information at the Receivers. *IEEE Trans. Inf. Theory* **2012**, *58*, 3453–3471. [CrossRef]
21. Bassi, G.; Piantanida, P.; Shamai, S. The Wiretap Channel With Generalized Feedback: Secure Communication and Key Generation. *IEEE Trans. Inf. Theory* **2019**, *65*, 2213–2233. [CrossRef]
22. Günlü, O.; Schaefer, R.F. An Optimality Summary: Secret Key Agreement With Physical Unclonable Functions. *Entropy* **2021**, *23*, 16. [CrossRef] [PubMed]
23. Liu, Y.; Li, M.; Liu, A.; Ong, L.; Yener, A. Fundamental Limits of Multiple-Access Integrated Sensing and Communication Systems. *arXiv* **2023**, arXiv:2205.05328.
24. Gamal, A.E.; Kim, Y.H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011.
25. Lin, P.H.; Jorswieck, E. On the Fast Fading Gaussian Wiretap Channel with Statistical Channel State Information at the Transmitter. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 46–58. [CrossRef]
26. Papoulis, A.; Pillai, S.U. *Probability, Random Variables, and Stochastic Processes*, 4th ed.; McGraw-Hill: Boston, MA, USA, 2002.
27. Prudnikov, A.P.; Brychov, Y.A.; Marichev, O.I. *Integrals and Series, Volume 2: Special Functions*; Gordon and Breach Science: New York, NY, USA, 1986.
28. Prudnikov, A.P.; Brychov, Y.A.; Marichev, O.I. *Integrals and Series, Volume 1: Elementary Functions*; Gordon and Breach: New York, NY, USA, 1986.
29. Ge, Y.; Ching, P.C. Energy Efficiency for Proactive Eavesdropping in Cooperative Cognitive Radio Networks. *IEEE Int. Things J.* **2022**, *9*, 13443–13457. [CrossRef]
30. Xiong, B.; Zhang, Z.; Ge, Y.; Wang, H.; Jiang, H.; Wu, L.; Zhang, Z. Channel Modeling for Heterogeneous Vehicular ISAC System with Shared Clusters. In Proceedings of the IEEE Vehicular Technology Conference, Hong Kong, 10–13 October 2023; pp. 1–6.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.