Impact of Realistic Propagation Conditions on Reciprocity-Based Secret-Key Capacity

François Rottenberg*†, Philippe De Doncker†, François Horlin† and Jérôme Louveaux*
*ICTEAM institute, Université catholique de Louvain, Belgium
†OPERA department, Université libre de Bruxelles, Belgium

***Abstract*—Secret-key generation exploiting the channel reciprocity between two legitimate parties is an interesting alternative solution to cryptographic primitives for key distribution in wireless systems as it does not rely on an access infrastructure and provides information-theoretic security. Many works in the literature assume that the eavesdropper gets no side information about the key from her observations provided that: (i) it is spaced more than a wavelength away from a legitimate party and (ii) the channel is rich enough in scattering. In this paper, we show that this condition is not always verified under realistic propagation conditions and we study the resulting secret-key capacity.**

***Index Terms*—Secret-key capacity, channel reciprocity, propagation.**

I. Introduction

The secrecy-capacity is defined as the number of bits per channel use that can be reliably transmitted to a legitimate receiver (Bob) while guaranteeing a negligible information leakage to the eavesdropper (Eve). The seminal work of Wyner [1] and its extension to more general channels [2] have shown that a "physical advantage" at Bob with respect to Eve is required to guarantee a larger-than-zero secrecy capacity. This "physical advantage" implies that Eve channel has to be noisier, which might not be always verified in practice [3].

Later, the works of [4], [5] have shown that the pessimistic limitation of requiring an advantage over the eavesdropper can be overcome by using stronger communication schemes that are not restricted to one-way rate-limited communications [3]. Maurer [4] and Ahlswede and Csiszár [5] were the first to analyze the problem of generating a secret key from correlated observations. In the source model (see Fig. 1), two legitimate parties (Alice and Bob) and one illegitimate party (Eve) observe the realizations of a discrete memoryless source. From their observations, Alice and Bob have to distill an identical key that remains secret from Eve. Moreover, Alice and Bob have access to a public error-free authenticated channel with unlimited capacity. This helps them to agree a common key with the limitation that Eve also can listen to it. Upper and lower bounds for the secret-key capacity, defined as the number of secret bits that can be generated per observation of the source, were derived in [4], [5]. Their results show that positive secret-key rates are achievable even if the channel from Alice to Bob is not degraded with respect to the channel from Alice to Eve.

A practical source of common randomness at Alice and Bob consists of the wireless channel reciprocity, which implies that the propagation channel from Alice to Bob and from Bob to Alice is identical if both are measured within the same channel coherence time and at the same frequency. At each coherence time, Alice and Bob can repeatedly sample the channel by sending each other a pilot symbol so as to obtain a set of N highly correlated observations and finally start a key-distillation procedure. The vast majority of works in the literature considers that Eve gets no side information about the key from her observations, which consist of the pilots transmitted by Alice and Bob [6]–[10]. Often, this assumption is justified by the fact that: (i) Eve is supposed to be separated from Bob and Alice by more than one wavelength (otherwise she could be easily detected) and (ii) the channel environment is supposed to be rich enough in scattering implying that the fading process of the channels at the different antennas can be considered independent. The assumption of rapid decorrelation in space has been further validated through measurement campaigns [6], [8], [11]–[13]. Moreover, this assumption is convenient as it drastically simplifies the problem of secret-key generation. Indeed, the secret-key capacity simply becomes equal to the mutual information between Alice and Bob since Eve cannot learn anything about the key from her channel observations. This implies that Eve can only learn about the secret-key from the discussion over the public channel.

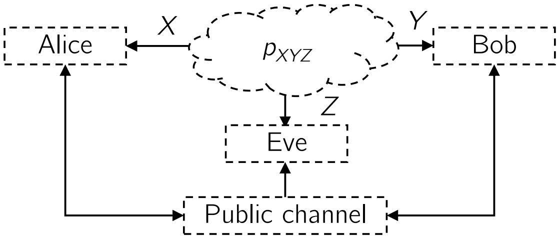

Fig. 1: Source model for secret-key agreement.

However, it often occurs in practical scenarios that scatterers are clustered with small angular spread rather than being uniformly distributed, which leads to much longer spatial decorrelation length. There exist only a small number of works that have considered the impact of potential spatial correlation at Eve's side. For instance, ref. [14] studied the impact of channel sparsity, inducing correlated eavesdropping, on the secret-key capacity. However, no advanced physical characterization of the propagation environment was considered. In [15], correlation of

978-1-5386-8110-7/19/$31.00 © 2019 IEEE

the eavesdropper channel is taken into account but the spatial and time correlation of the channel is modeled according to Jakes Doppler model, which again assumes a rich scattering environment and leads to decorrelation in space after only a few wavelengths. In [16], experiments are conducted indoor to evaluate the correlation of the eavesdropper's observations and its impact on the secret-key capacity. The work of [17] uses a similar indoor experimental approach and propose results of cross-correlation, mutual information and secret-key rates, which are dependent on the eavesdropper's position. Still, [16], [17] are only experimentally-based and were performed in an indoor environment. No advanced propagation model is proposed to characterize the spatial correlation arising for any given particular environment. Moreover, no analytical expressions was proposed on how such a propagation environment would affect the secret-key capacity.

In the light of these limitations, we feel that a theoretical analysis of the impact of realistic propagation environments on the secret-key capacity is still missing in the literature. In this paper, as opposed to many works in the literature, we characterize the secret-key capacity without making the simplifying assumption of a rich scattering environment, which are likely to arise in 5G deployments relying directive transmission such as massive MIMO and millimeter wave communications. The obtained lower and upper bounds for the secret-key capacity take into account the impact of realistic propagation environments, which controls the spatial decorrelation of Eve. Eve is also allowed to have a more powerful receiver than Alice and Bob, resulting in a larger signal-to-noise ratio (SNR). We show that, under typical propagation conditions drawn from 3GPP models [18], many evaluations of the secret-key capacity, relying on a rich scattering assumption, are too optimistic as they underestimate the information available at Eve's side. In practice, privacy amplification, *i.e.*, reducing the key size using universal hashing, should be used to remove the information Eve has learned about the key not only from public discussion but also from her correlated observations [3]. This work quantitatively evaluates this loss of capacity.

Notations: Vectors and matrices are denoted by bold lowercase and uppercase letters, respectively (resp.). Non bold uppercase letter refers to a random variable. The vector notation $\vec{r}$ refers to a 3D position. Superscripts *, ^{T} and ^{H} stand for conjugate, transpose and Hermitian transpose operators. The symbols tr, $\mathbb{E}$, $\Im$ and $\Re$ denote the trace, expectation, imaginary and real parts, respectively. $\jmath$ is the imaginary unit. The norm $\|\mathbf{A}\|$ is the Frobenius norm. $|\mathbf{A}|$ is the determinant of matrix $\mathbf{A}$. $\mathbf{I}_n$ denotes the identity matrix of order n. $\delta(t)$ is the Dirac delta.

II. Transmission Model

We assume that Alice and Bob extract a common key from observations of their shared channel H, assumed to be reciprocal. The channel H is estimated based on the transmission of *a priori* known pilots by Alice and Bob. We consider that the channel remains invariant during the transmission of each pilot symbol. Assuming a narrowband channel, the estimates of H at Alice's and Bob's sides, respectively denoted by X and Y, are given by

$$X = H + W_X, \; Y = H + W_Y,$$

where the additive noise samples W_X and W_Y are modeled as zero mean circularly-symmetric complex Gaussian (ZMCSCG) with variance σ_X^2 and σ_Y^2 respectively.

The strategy of Eve consists in going as close as possible from Bob's antenna[1]. Then, Eve estimates her channel H_Z between Alice's antenna and hers by intercepting the pilots sent from Alice to Bob. Since Eve is close to Bob, the channel from Alice to Eve will be spatially correlated with H while the channel between Bob and Eve will experience a negligible correlation with H. Therefore, we neglect the pilot sent by Bob and received by Eve in the following as she cannot get any useful information from it. We define the channel estimate of Eve as

$$Z = H_Z + W_Z,$$

where W_Z is modeled as ZMCSCG with variance σ_Z^2. If Alice and Bob transmit a pilot of equal power and Alice, Bob and Eve use a similar receiver, one could expect a situation of equal noise variance $\sigma_X^2 = \sigma_Y^2 = \sigma_Z^2$. On the other hand, Eve could use a more powerful receiver than Alice and/or Bob by having, *e.g.*, a larger antenna size, a multi-antenna receiver or an amplifier with lower noise figure. This would result in a lower noise variance σ_Z^2 and a higher SNR. Moreover, a different pilot power transmitted by Alice and Bob will induce variations in their noise variance.

We consider a memoryless source model for secret-key agreement [3], [5] as shown in Fig. 1. This implies that Alice, Bob and Eve observes n independent and identically distributed (i.i.d.) repetitions of the random variables measurements X, Y and Z, giving $X^n = (X_1, ..., X_n)$, $Y^n = (Y_1, ..., Y_n)$ and $Z^n = (Z_1, ..., Z_n)$. Moreover, a noiseless authenticated public channel of unlimited capacity is available for communication. All parties have access to the public channel.

III. Channel Model

In this section, we aim at providing a realistic model of the channel H and H_Z with particular emphasis on their correlation in time and space. The assumption of i.i.d. repeated measurements X^n, Y^n, Z^n is well fulfilled in practice if the measurements of the channel are repeated in time with a sampling period that is large compared to the coherence time of the channel. This time can be related to the degree of mobility of Alice, Bob, Eve and the scattering environment. In this paper, we assume that Bob and Eve and scatterers are fixed while Alice is moving. This can model a typical situation where Bob is a base station and Alice is a user terminal. This implies that H and H_Z change over time, which leads to channel decorrelation in time. Alice is also assume to be in a non line-of-sight (LOS) situation.

[1] Note that all of the following is symmetrical if Eve gets close to Alice instead of Bob.

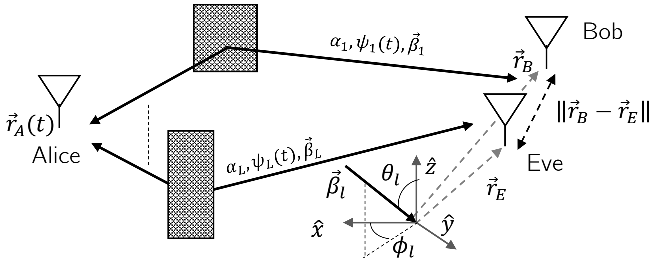

Fig. 2: Non-LOS channel propagation model: Eve gets close to Bob to increase the spatial correlation between the channel from Alice to her antenna $H_Z(t)$ and the channel from Alice to Bob $H(t)$. Scatterers, Bob and Eve are static but Alice is moving.

As opposed to previous approaches [7]–[10], we do not consider a uniform distribution of scatterers in angle. Instead, we consider a model where the channels H and H_Z can be described by the combination of L paths, as shown in Fig. 2. The l-th path is characterized by an azimuth angle ϕ_l and elevation angle θ_l at Bob and Eve side. Bob and Eve belong to a local area, situated in the far field from scatterers, so that the angles are identical at Bob and Eve. Moreover they are assumed to remain constant in time over the n measurements. The mobility of Alice induces a phase drift of each multipath component, common at Bob and Eve, that we denote by $\psi_l(t)$. Bob and Eve (fixed) positions are denoted by $\vec{r}_B \in \mathbb{R}^{3\times 1}$ and $\vec{r}_E \in \mathbb{R}^{3\times 1}$ respectively in their local area coordinate system. Alice, Bob and Eve are each equipped with a single isotropic antenna. Under previous assumptions, the narrowband multipath channels H and H_Z at time t can be modeled as [19]

$$H(t) = \sum_{l=1}^{L} \alpha_l e^{\jmath\psi_l(t)} e^{-\jmath\vec{\beta}_l\cdot\vec{r}_B}$$

$$H_Z(t) = \sum_{l=1}^{L} \alpha_l e^{\jmath\psi_l(t)} e^{-\jmath\vec{\beta}_l\cdot\vec{r}_E},$$

where $\vec{\beta}_l \in \mathbb{R}^{3\times 1}$ is the wave vector associated to path l at Bob/Eve side, which is directly related to the carrier wavelength λ and points in direction (ϕ_l, θ_l). α_l is the complex gain of path l.

In the following, in accordance with conventional approaches in the propagation literature [20], we consider multipath components as stochastic. Moreover, we assume uncorrelated scatterers with a uniformly distributed phase in $[0, 2\pi]$ so that $\mathbb{E}(\alpha_l) = 0$ and $\mathbb{E}(\alpha_l\alpha_{l'}^*) = p_l\delta_{l-l'}$ with $p_l = \mathbb{E}(|\alpha_l|^2)$. We also define $p = \mathbb{E}(|H(t)|^2) = \mathbb{E}(|H_Z(t)|^2) = \sum_l p_l$ as the average power of scattered paths. Non LOS measurement campaigns have shown that the channels $H(t)$ and $H_Z(t)$ can be accurately modeled with a zero-mean Gaussian distribution, especially for large values of L. Therefore, we assume that the random vector $(H(t), H_Z(t))^T$ follows a joint circularly symmetric Gaussian distribution with zero mean and covariance matrix given by

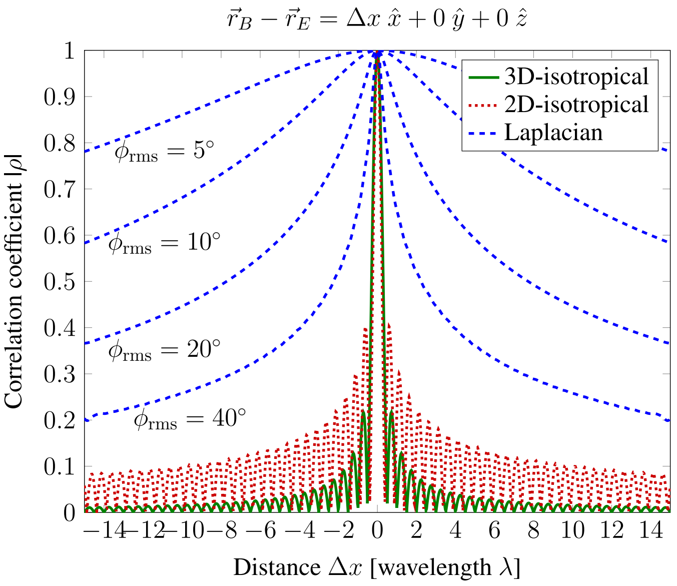

Fig. 3: Correlation coefficient $|\rho|$ as a function of the distance $\Delta x = \|\vec{r}_B - \vec{r}_E\|$ along the $\hat{x}$ axis. Three types of angular distributions are considered: (i) 3D-isotropic, $\rho = \text{sinc}\left(\frac{2\pi\Delta x}{\lambda}\right)$, (ii) 2-D isotropic, $\rho = J_0\left(\frac{2\pi\Delta x}{\lambda}\right)$ and (iii) $\rho =$ (2) with $f(\Omega)$ a Laplacian distribution with elevation spread $\theta_{\text{rms}} = 5°$ and different angular spreads ϕ_{rms}.

$$\mathbb{E}\begin{pmatrix} H(t) \\ H_Z(t) \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, \ \mathbf{C}_{HH_Z} = p\begin{pmatrix} 1 & \rho \\ \rho^* & 1 \end{pmatrix}.$$

We now study the spatial correlation coefficient ρ between $H(t)$ and $H_Z(t)$. Under previous assumptions, we can write

$$\rho = \frac{1}{p}\mathbb{E}\left[H(t)H_Z^*(t)\right] = \frac{1}{p}\sum_{l=1}^{L} p_l e^{-\jmath\vec{\beta}_l\cdot(\vec{r}_B - \vec{r}_E)}. \qquad (1)$$

Defining the normalized angular power density function $f(\Omega)$ at Bob and Eve (per steradian) as [20]

$$f(\Omega) = \frac{1}{p}\sum_{l=1}^{L} p_l\delta\left(\Omega - \Omega_l\right)$$

$$\delta\left(\Omega - \Omega_l\right) = \frac{1}{\sin\theta_l}\delta\left(\phi - \phi_l\right)\delta\left(\theta - \theta_l\right),$$

we can rewrite (1) as

$$\rho = \int_{\Omega} f(\Omega) e^{-\jmath\vec{\beta}\cdot(\vec{r}_B - \vec{r}_E)} d\Omega, \qquad (2)$$

where the differential $d\Omega$ can be formulated in spherical coordinates as $d\Omega = \sin\theta d\theta d\phi$. Note that the wave vector $\vec{\beta}$ depend on Ω through the angles (ϕ, θ). Since $p = \sum_{l=1}^{L} p_l$, we have $\int_{\Omega} f(\Omega) d\Omega = 1$ so that $0 \leq |\rho| \leq 1$.

The formulation (2) in terms of $f(\Omega)$ is convenient as it allows to represent both specular components and continuous spectrum, which can occur in the case of diffuse scattering. Typically, the value of ρ will decrease as (i) the distance of Eve with respect to Bob $\|\vec{r}_B - \vec{r}_E\|$ increases and/or (ii) as the distribution $f(\Omega)$ gets uniform over (ϕ, θ). The worst-case in terms of secrecy occurs in the extreme case $f(\Omega) = \delta(\Omega - \Omega_1)$ (only one incoming direction for the scattered paths) implying that $|\rho| = 1$. The opposite extreme case is an isotropic distribution over azimuth and elevation (3D-isotropic), *i.e.*, $f(\Omega) = \frac{1}{4\pi}$, which leads to the well-known result [21, p. 49]

$$\rho = \operatorname{sinc}\left(\frac{2\pi\|\vec{r}_B - \vec{r}_E\|}{\lambda}\right), \tag{3}$$

where $\operatorname{sinc}(x) = \sin x/x$. This shows that ρ becomes negligible after a few λ. Similarly, if scattered paths are coming from a fixed horizontal elevation $\theta = \pi/2$ but are uniformly distributed in azimuth (2D-isotropic), *i.e.*, $f(\Omega) = \frac{1}{2\pi}\delta(\theta - \pi/2)$, we get another well-known result [22]

$$\rho = J_0\left(\frac{2\pi d}{\lambda}\right),$$

where $J_0(.)$ is the zero-order Bessel function and d is the distance between Eve and Bob in the horizontal plane. Here again, ρ becomes negligible if d is larger than a few λ. This was the justification of many works suggesting that Eve does not get any useful information about H from Z as soon as she is a few centimeters away from Bob for conventional radio-frequency bands [6]–[10]. This implies that Eve can only learn about H and thus the secret-key from the public discussion between Alice and Bob.

In this paper, we do not make this assumption, which can be too optimistic in terms of secrecy. In practice, the decay of ρ as a function of $\|\vec{r}_B - \vec{r}_E\|$ will depend on the scattering environment, which is often far from being uniformly distributed in angle but rather clustered with specific angular spreads. As an example, we compare in Fig. 3 the decay of ρ as a function of the distance between Eve and Bob, along the $\hat{x}$ axis ($\phi = 0$ and $\theta = \pi/2$), and different angular distributions. In addition to the previously described 3D- and 2D-isotropic distributions, we also consider a more realistic Laplacian distribution in azimuth and elevation, centered in $(\phi, \theta) = (0, \pi/2)$, which is a common model for a base station [23]

$$f(\Omega) = \gamma e^{-\sqrt{2}\frac{|\phi|}{\phi_{\text{rms}}}} \frac{1}{\sin\theta} e^{-\sqrt{2}\frac{|\theta - \pi/2|}{\theta_{\text{rms}}}},$$

where ϕ_{rms} and θ_{rms} are the azimuth and elevation angular spreads respectively and γ is a normalization constant. According to recent 3GPP standard channel models [18], typical values of ϕ_{rms} range around 40° for an indoor office, in $[1°, 10°]$ for a rural environment and in $[10°, 40°]$ for an urban micro/macro cell environment while a typical value for the elevation angular spread is $\theta_{\text{rms}} = 5°$. We can clearly see in Fig. 3 that the 3D- and 2D-isotropic distributions underestimate the spatial correlation between Bob and Eve. In other words, considering these models overestimates the secret-key capacity in scenarios of practical relevance. For a typical cellular carrier frequency of 1 GHz, $\lambda = 30$ cm and Eve could be placed at $10\lambda = 3$ m while still having a significant correlation with H. Moreover, as explained earlier, Eve could also use a more powerful receiver than Alice and Bob resulting in a lower noise variance σ_Z^2.

IV. Secret-Key Capacity

The secret-key capacity $S(X;Y||Z)$ is defined as the maximum rate at which Alice and Bob can agree on a secret-key while keeping the rate at which Eve obtains information about the key arbitrarily small for sufficiently large n. Moreover, Alice and Bob should agree on a common key with high probability and the key should approach the uniform distribution. We refer to [3]–[5] for a formal definition.

As explained above, we consider that Eve gets useful information from her observation Z over H. This implies that the secret-key capacity is not simply equal to $I(X;Y)$, as opposed to many previous works. Finding the general expression of the secret-key capacity for a given distribution of X, Y, Z is still an open problem. From [4], [5] [3, Prop. 5.4], the secret-key capacity, expressed in the number of generated secret bits per channel observation, can be lower and upper bounded as follows

$$S(X;Y||Z) \geq I(X;Y) - \min\left[I(X;Z), I(Y;Z)\right] \tag{4}$$

$$S(X;Y||Z) \leq \min\left[I(X;Y), I(X;Y|Z)\right]. \tag{5}$$

The lower bound (4) implies that if Eve has less information about Y than Alice or respectively about X than Bob, such a difference can be leveraged for secrecy [4]. Moreover, this rate can be achieved with one-way communication. On the other hand, the upper bound (5) implies that the secret-key rate cannot exceed the mutual information between Alice and Bob. Moreover, the secret-key rate cannot be higher than the mutual information between Alice and Bob if they happened to learn Eve's observation Z.

In particular cases, the lower and upper bounds can become tight [3]–[5]. In the next subsections, we evaluate the lower and upper bounds of (4) and (5), and their simplification in the cases where the bounds become tight. To do this, we use the fact that, from the system model detailed in previous sections, the random variables X, Y and Z are jointly circularly symmetric Gaussian distributed. This implies that the entropy of these random variables only depend on their covariance, which is equivalent to their correlation given their zero mean. The entropy of a circularly symmetric Gaussian with covariance $\mathbf{C}$ is $\log_2(|\pi e \mathbf{C}|)$, where e is the Euler number.

A. Lower Bound

The random variables X and Y are jointly Gaussian distributed with covariance

$$\mathbf{C}_{XY} = \begin{pmatrix} p + \sigma_X^2 & p \\ p & p + \sigma_Y^2 \end{pmatrix}.$$

From this distribution, we find

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(XY) \\ &= \log_2\left(1 + \frac{p^2}{(p + \sigma_X^2)(p + \sigma_Y^2) - p^2}\right). \end{aligned} \tag{6}$$

Moreover, X and Z are jointly Gaussian with covariance

$$\mathbf{C}_{XZ} = \begin{pmatrix} p + \sigma_X^2 & \rho p \\ \rho^* p & p + \sigma_Z^2 \end{pmatrix}.$$

This leads to the mutual information

$$I(X;Z) = \log_2 \left(1 + \frac{|\rho p|^2}{(p+\sigma_X^2)(p+\sigma_Z^2) - |\rho p|^2} \right).$$

Using a similar methodology for Y, we find

$$I(Y;Z) = \log_2 \left(1 + \frac{|\rho p|^2}{(p+\sigma_Y^2)(p+\sigma_Z^2) - |\rho p|^2} \right).$$

In the end, we find that the lower bound in (4) is equal to

$$S(X;Y||Z) \geq \log_2 \left(\frac{1 + \frac{p^2}{(p+\sigma_X^2)(p+\sigma_Y^2)-p^2}}{1 + \frac{|\rho p|^2}{(p+\max(\sigma_X^2,\sigma_Y^2))(p+\sigma_Z^2)-|\rho p|^2}} \right).$$

As soon as $|\rho| < 1$, $S(X;Y||Z)$ is unbounded and goes to infinity as $p \to +\infty$. Indeed, as $p \to +\infty$, $I(X;Y) \to +\infty$ while $I(X;Z)$ and $I(Y;Z)$ converge to $\log_2 \left(1 + \frac{|\rho|^2}{1-|\rho|^2}\right)$, which is bounded for $|\rho| < 1$. Note that the lower bound is not restricted to be positive (as will be shown in Section V), in which case it becomes useless. We can find the condition on the minimum noise variance at Eve σ_Z^2 for having a larger-than-zero lower bound

$$\sigma_Z^2 > p(|\rho|^2 - 1) + |\rho|^2 \min(\sigma_X^2, \sigma_Y^2). \tag{7}$$

In the worst-case, $|\rho| = 1$ and σ_Z^2 has to be larger than the minimum of the noise variances of Alice and Bob. We can invert (7) to find the maximal correlation coefficient $|\rho|^2$ to have a larger-than-zero lower bound

$$|\rho|^2 < \frac{p + \sigma_Z^2}{p + \min(\sigma_X^2, \sigma_Y^2)}.$$

From the definition of ρ in (2) and for a given propagation environment inducing a specific angular power distribution $f(\Omega)$, the last equation can be related to the minimal admissible distance $\|\vec{r}_B - \vec{r}_E\|$ between Eve and Bob.

B. Upper Bound

To evaluate the upper bound in (5), we only need to evaluate $I(X;Y|Z)$ as we already evaluated the expression $I(X;Y)$. To do this, first note that X, Y and Z are jointly Gaussian distributed with covariance matrix

$$\mathbf{C}_{XYZ} = \begin{pmatrix} p+\sigma_X^2 & p & \rho p \\ p & p+\sigma_Y^2 & \rho p \\ \rho^* p & \rho^* p & p+\sigma_Z^2 \end{pmatrix},$$

which gives

$$\begin{aligned} I(X;Y|Z) &= H(XZ) + H(YZ) - H(Z) - H(XYZ) \\ &= \log_2 \left(\frac{|\mathbf{C}_{XZ}||\mathbf{C}_{YZ}|}{(p+\sigma_Z^2)|\mathbf{C}_{XYZ}|} \right). \end{aligned}$$

The upper bound is then given by the minimum of $I(X;Y|Z)$ and $I(X;Y)$. It is possible to show that the condition $I(X;Y|Z) \leq I(X;Y)$ is always verified under the assumptions of our channel model (see [24] for the proof) and thus

$$S(X;Y||Z) \leq \log_2 \left(\frac{|\mathbf{C}_{XZ}||\mathbf{C}_{YZ}|}{(p+\sigma_Z^2)|\mathbf{C}_{XYZ}|} \right).$$

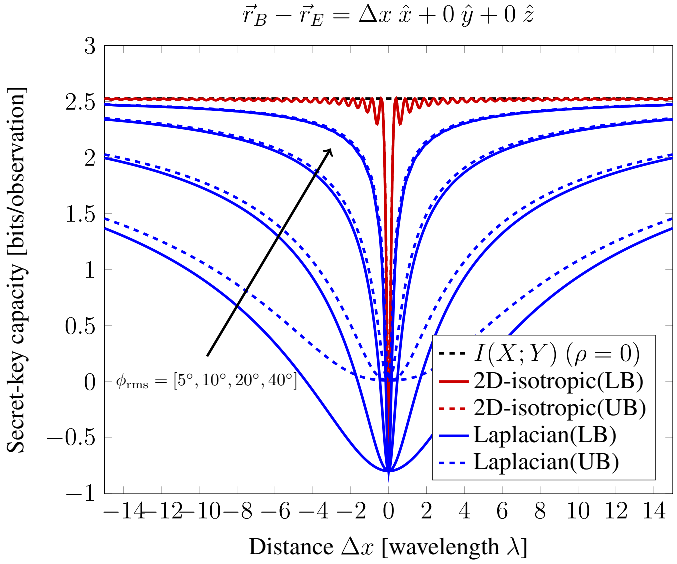

Fig. 4: Lower bound (LB) and upper bound (UB) for secret-key capacity as a function of propagation environments considered in Fig. 3. The curve $I(X,Y)$ corresponds to the case of independent observations at Eve ($\rho = 0$).

One should note that the situation $I(X;Y|Z) > I(X;Y)$ could be possible in another context. This would imply that the knowledge of Eve's observation could help Alice and Bob to generate secrecy. We refer to [25] for an analysis of the quantity $I(X;Y|Z) - I(X;Y)$ and to [5] for its implication in terms of secrecy.

C. Tight Bound

In our context, three particular cases can be distinguished.

1) $\rho = 0$, Eve does not learn anything about H from Z, which becomes independent from X and Y. This leads to the trivial result $S(X;Y||Z) = I(X;Y)$, given in (6) and as considered in [7]–[10].

2) $\sigma_Y^2 = 0$, $Y = H$, this implies that $X \to Y \to Z$ forms a Markov chain, which leads to $I(X;Y|Z) = I(X;Y) - I(X;Z)$ [3, Corol. 4.1] and

$$S(X;Y||Z) = \log_2 \left(\frac{1 + \frac{p}{\sigma_X^2}}{1 + \frac{|\rho p|^2}{(p+\sigma_X^2)(p+\sigma_Z^2)-|\rho p|^2}} \right).$$

3) $\sigma_X^2 = 0$, $X = H$, symmetrically as in 2), we find

$$S(X;Y||Z) = \log_2 \left(\frac{1 + \frac{p}{\sigma_Y^2}}{1 + \frac{|\rho p|^2}{(p+\sigma_Y^2)(p+\sigma_Z^2)-|\rho p|^2}} \right).$$

Cases 2) and 3) let us expect that the bounds become tight as the receiver of Alice or Bob is significantly noisier than the one of the other.

V. Numerical Validation

We evaluate numerically the secret-key capacity in Fig. 4 based on the formulas derived in Section IV for the lower/upper bounds (LB/UB) and relying on the channel models derived in

Section III. We consider the same angular distributions as in Fig. 3. We recall that an angular Laplacian distribution is an accurate model for a base station with varying angular spreads as a function of the propagation environment. We consider signal-to-noise ratios $p/\sigma_X^2 = p/\sigma_Y^2 = 10$ dB at Alice and Bob while Eve is allowed to have a more power receiver that achieves $p/\sigma_Z^2 = 20$ dB. For a given angular spread, Fig. 4 gives the admissible distance between Bob and Eve to achieve a given secret-key capacity.

Here again, we see that the general assumption of considering that Eve's observations Z are independent of X and Y ($\rho = 0$) is well verified if scatterers are 2D-isotropic distributed and if Eve is more than a wavelength away from Bob. However, for practical angular spreads at the base station, this assumption is typically not valid and too optimistic. This implies that lower secret-key rates are achievable in practice and privacy amplification should compensate for the information that Eves learns about the key not only from public discussion but also from her observations.

VI. Conclusion

In this paper, we have studied the secret-key capacity based on the principle of channel reciprocity. We have shown that the assumption of full decorrelation of Eve's observations with respect to Alice and Bob is not always verified and critically depends on the propagation environment. Our simulation results show that, for practical propagation environments, the correlation of Eve's observations is non negligible implying a potentially significant reduction of the secret-key capacity.

Acknowledgment

The research reported herein was partly funded by the Fonds National de la Recherche Scientifique (F.R.S.-FNRS).

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] M. Bloch and J. Barros, *Physical-layer security: from information theory to security engineering*. Cambridge University Press, 2011.

[4] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[5] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[6] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust Key Generation from Signal Envelopes in Wireless Networks," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 401–410. [Online]. Available: http://doi.acm.org/10.1145/1315245.1315295

[7] T. F. Wong, M. Bloch, and J. M. Shea, "Secret sharing over fast-fading MIMO wiretap channels," *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, no. 1, p. 506973, 2009.

[8] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-Theoretically Secret Key Generation for Fading Wireless Channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 2, pp. 240–254, June 2010.

[9] C. Chen and M. A. Jensen, "Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients," *IEEE Transactions on Mobile Computing*, vol. 10, no. 2, pp. 205–215, Feb 2011.

[10] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *2013 IEEE Globecom Workshops (GC Wkshps)*, Dec 2013, pp. 1245–1250.

[11] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139. [Online]. Available: http://doi.acm.org/10.1145/1409944.1409960

[12] M. Ghoreishi Madiseh, S. He, M. L. Mcguire, S. W. Neville, and X. Dong, "Verification of Secret Key Generation from UWB Channel Observations," in *2009 IEEE International Conference on Communications*, June 2009, pp. 1–5.

[13] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental Study on Key Generation for Physical Layer Security in Wireless Communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[14] T. Chou, S. C. Draper, and A. M. Sayeed, "Impact of channel sparsity and correlated eavesdropping on secret key generation from multipath channel randomness," in *2010 IEEE International Symposium on Information Theory*, June 2010, pp. 2518–2522.

[15] J. Zhang, B. He, T. Q. Duong, and R. Woods, "On the Key Generation From Correlated Wireless Channels," *IEEE Communications Letters*, vol. 21, no. 4, pp. 961–964, April 2017.

[16] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "Experimental aspects of secret key generation in indoor wireless environments," in *2013 IEEE 14th Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*, 2013, pp. 669–673.

[17] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The Passive Eavesdropper Affects My Channel: Secret-Key Rates under Real-World Conditions," in *2016 IEEE Globecom Workshops (GC Wkshps)*, 2016, pp. 1–6.

[18] "3GPP TR 38.901 v15.0.0," Tech. Rep., 2018.

[19] A. F. Molisch, *Wireless communications*. John Wiley & Sons, 2012, vol. 34.

[20] G. D. Durgin, *Space-time wireless channels*. Prentice Hall Professional, 2003.

[21] D. H. Johnson and D. E. Dudgeon, *Array signal processing: concepts and techniques*.

[22] G. L. Stüber and G. L. Stèuber, *Principles of mobile communication*. Springer, 1996, vol. 2.

[23] K. I. Pedersen, P. E. Mogensen, and B. H. Fleury, "Power azimuth spectrum in outdoor environments," *Electronics Letters*, vol. 33, no. 18, pp. 1583–1584, Aug 1997.

[24] F. Rottenberg, T.-H. Nguyen, J.-M. Dricot, F. Horlin, and J. Louveaux, "CSI-based versus RSS-based Secret-Key Generation under Correlated Eavesdropping," *arXiv preprint arXiv:2006.12049*, 2020.

[25] R. W. Yeung, "A new outlook on Shannon's information measures," *IEEE Transactions on Information Theory*, vol. 37, no. 3, pp. 466–474, May 1991.