# Secure Communications in Line-of-Sight Scenarios by Rotation-based Secret Key Generation

Thuy M. Pham, André N. Barreto, Miroslav Mitev, Maximilian Matthé, Gerhard Fettweis
Barkhausen Institut, Dresden, Germany
{minhthuy.pham, andre.nollbarreto, miroslav.mitev, maximilian.matthe, gerhard.fettweis}@barkhauseninstitut.org

***Abstract*—In this paper we evaluate the achievable rates of the physical layer security (PLS)-based secret key generation (SKG) in a line-of-sight (LoS) channel, which occurs with a high probability in unmanned aerial vehicle (UAV) communications. SKG is a promising technique for lightweight scalable key distribution, and, despite the mature theory of PLS, this technique remains to be seen in practical applications. Thus, modelling realistic scenarios is of particular interest. One of the reasons why SKG has not been used in practice is due to the deterministic properties of LoS channels. To overcome this problem, in this paper we propose the rotation of the device antennas as an entropy source, reflected by the channel phases, from which the keys are derived. Simulation results show that by utilizing rotation in LoS scenarios, a number of secret bits can be generated, also given the presence of an eavesdropper. It is also shown that by controlling the transmit power we can maximize the conditional mutual information.**

***Index Terms*—UAV, physical layer security, rotation, mutual information, entropy.**

## I. Introduction

The proliferation of wireless technologies and their widespread applications have led to an increasing interest in wireless physical-layer security (PLS) in recent years. Traditionally, network security relies on cryptography methods at the network layer. Since wireless networks operate in an open medium, these schemes are vulnerable to active attacks and eavesdropping. Additionally, encryption keys are difficult to distribute and manage due to the dynamic nature of wireless networks.

Generally, PLS can solve the key distribution problem either through keyless encryption using wiretap coding [1]–[4] or by means of channel-based secret key generation (SKG), which is lightweight and easily scalable. The keyless approach requires knowledge of the channel and noise of eavesdroppers, which cannot be obtained in most situations. Herein, we thus focus on SKG approach [5]–[9] which relies on the random characteristics of the wireless channel to generate secret keys. Its complexity is low and, more importantly, it is provably secure [5], [6]. The performance of this method however depends heavily on the dynamic nature of the channel. The SKG rates have been evaluated for particular Gaussian-distributed SISO and MIMO scenarios [10]–[12]. However, none of these consider line-of-sight (LoS) communication. In fact, as the security key is generated from the variations in the received signal, either in time or frequency, performing SKG in static or LoS scenarios (where variations are limited) is a challenging task.

In this paper, we investigate the possibility of applying the PLS key generation approach for line-of-sight scenarios in the context of unmanned aerial vehicle (UAV) communications. UAV communications have strong LoS components, which makes them vulnerable to channel prediction attacks [13]–[15]. It is also a well-known fact that the dominant component in LoS makes it difficult for key generation. To overcome this and introduce randomness to the system, we propose to employ the rotation of UAVs' antennas as a source of entropy. When multiple antennas are employed, this is reflected in random variations of the observed phases in the channels between pairs of antennas. Also notice that this approach could also be applied in any scenarios with LoS propagation.

Our main contributions are summarized as follows:

- To the best of the authors' knowledge, this is the first research on SKG that accounts for antenna rotations in a LoS scenario.
- We propose a novel approach that adds randomness to LoS scenarios by rotating antennas. In particular, we evaluate both 2D and 3D system models to arrive at rotation-based channels and, then, numerically estimate the mutual information (MI), which is a measure of the achievable secret key rate.
- We evaluate the performance of the system under different settings and observe that, even in the presence of an eavesdropper, there is a certain number of bits that can be secretly generated, and that this rate can be optimized by an appropriate power control.

*Notation*: Standard notations are used in this paper. Bold lower and upper case letters represent vectors and matrices, respectively. $\angle\underline{\mathbf{H}}$ defines the matrix containing the phases of the elements of $\mathbf{H}$, $I(.)$ represents the mutual information, and $\|.\|$ denotes the Frobenius norm.

## II. System Modelling and SKG Rates

### A. Assumptions

The following assumptions will be held throughout the paper. Far-field conditions are assumed, and signals propagate via plane waves. In addition, the carrier frequency $f$ and, consequently, the wavelength $\lambda$, are fixed and known; the radio link is interference-free and time invariant. We also consider that the noise follows a zero-mean Gaussian distribution. Moreover, the radio-frequency chain and signal processing are assumed ideal.

### B. 2D Modelling

For ease of representation, we start by a 2D system model with a single rotation axis. This analysis can later be easily extended to the 3D space, which is of course the real-life scenario, and a numerical analysis is performed for both cases.

In particular, we consider the communication model given in Fig. 1a. The model consists of two legitimate UAVs communicating with each other and an eavesdropper, placed on the top of a building, who tries to overhear the legitimate communication. We present the abstract model (c.f. Fig. 1b) as a 2D model of Alice, Bob and Eve, each of which has 2 antennas located at opposite direction from the center with a radius $\rho$. The center of each device also represents its rotation axis. Note that we assume that the antennas are perfect isotropic radiators, which is not a strong limitation, as the phase is the main observation parameter impacted by the rotation. The distances between pairs of antennas in the LoS paths are indicated by the variables $\ell$ and the channel coefficients are represented by the matrix $\mathbf{H}$ and coefficient $h$, which are detailed in the following.

Next, to estimate the eavesdropper's perspective we translate the centers of Alice's and Bob's antenna arrays (points $A$ and $B$ on Fig. 1b) on a coordinate system centered at point $E$, which is Eve's the rotation axis. i.e., $\mathbf{p}_A = [x_A, y_A]^T$ and $\mathbf{p}_B = [x_B, y_B]^T$, respectively. We also consider that the line running through both Eve's antennas represents the system's horizontal axis. It is assumed that Alice's and Bob's antennas rotate counterclockwise with the angles $\psi_A$ and $\psi_B$, respectively. We also assume that the distance between Bob and Alice $\|AB\| >> \rho$ and thus far field conditions holds.

From the Friis formula [16], we have:

$$P_r = P_t \; G_t \; G_r \; \left(\frac{\lambda}{4\pi \cdot \ell}\right)^2 \; K \tag{1}$$

where $P_t$ and $P_r$ are transmit and receive power, respectively; $G_t$ and $G_r$ are transmit and receive gain, respectively; $\ell$ is the distance and $K$ is polarization matching factor. Without loss of generality, we assume that: $P_t = 1, K = 1, G = 1$. Therefore, we can express the generic channel coefficient between an antenna pair as follows:

$$h \approx \exp\left(j \; \frac{2\pi}{\lambda} \; \ell\right) \in \mathbb{C}. \tag{2}$$

where $\ell/\lambda$ is the number of wavelengths in the generic $\ell$ path length. The computation of $\ell$ and, thus, of the phase of $h$ is detailed in the following.

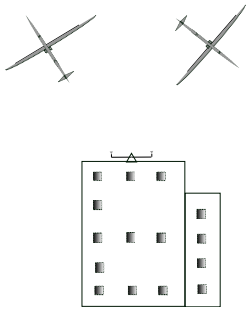
As mentioned above, we need to identify the position of the antennas after being rotated to arrive at distances between them, which is possible by means of rotation matrix detailed in what follows. Denoting by $\mathbf{p}$ the coordinates of a point in the 2D space, the rotation matrix [17] of a rotation angle $\psi$ can be expressed as

$$\mathbf{R} = \begin{bmatrix} \cos(\psi) & -\sin(\psi) \\ \sin(\psi) & \cos(\psi) \end{bmatrix} \in \mathbb{C}^{2\times 2}. \tag{3}$$

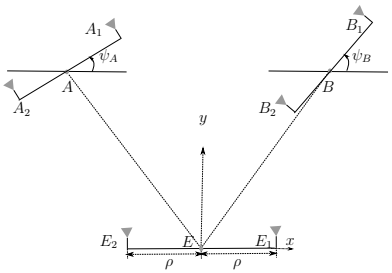
Thus, for instance, the position of the first antenna of Alice, i.e., $A_1$ is given by

$$\mathbf{p}_{A_1} = \mathbf{p}_A + \mathbf{p}_{A_1}^A \tag{4}$$

where $\mathbf{p}_{A_1}^A$ is the projected coordinate of $A_1$ on the coordinate system center at $A$ using the rotation matrix $\mathbf{R}$. We can continue in this fashion obtaining the remaining points and thus compute the distance between antennas and their channel coefficients as detailed in the following propositions.



(a) Application scenario




(b) Abstract representation

Fig. 1: System Model

Define $\Delta = y_B - y_A$ and $d = x_B - x_A$, the following proposition holds.

*Proposition* 1. The channel matrix between Alice and Bob is given by

$$\mathbf{H}_{AB} = \begin{bmatrix} h(\ell_{A_1B_1}) & h(\ell_{A_1B_2}) \\ h(\ell_{A_2B_1}) & h(\ell_{A_2B_2}) \end{bmatrix} \in \mathbb{C}^{2\times 2} \tag{5}$$

where

$$\begin{aligned} \ell^2_{A_1B_1} &= 2\rho^2 - 2\rho^2\cos(\psi_A - \psi_B) - 2\rho(\cos\psi_A - \cos\psi_B)d \\ &\quad - 2\rho(\sin\psi_A - \sin\psi_B)\Delta + d^2 + \Delta^2 \qquad (6) \\ \ell^2_{A_1B_2} &= 2\rho^2 + 2\rho^2\cos(\psi_A - \psi_B) - 2\rho(\cos\psi_A + \cos\psi_B)d \\ &\quad + 2\rho(\sin\psi_A + \sin\psi_B)\Delta + d^2 + \Delta^2 \qquad (7) \\ \ell^2_{A_2B_1} &= 2\rho^2 + 2\rho^2\cos(\psi_A - \psi_B) + 2\rho(\cos\psi_A - \cos\psi_B)d \\ &\quad - 2\rho(\sin\psi_A - \sin\psi_B)\Delta + d^2 + \Delta^2 \qquad (8) \\ \ell^2_{A_2B_2} &= 2\rho^2 - 2\rho^2\cos(\psi_A - \psi_B) + 2\rho(\cos\psi_A - \cos\psi_B)d \\ &\quad - 2\rho(\sin\psi_A - \sin\psi_B)\Delta + d^2 + \Delta^2. \qquad (9) \end{aligned}$$

The detailed proof of Proposition 1 is in the Appendix. Similarly, we can obtain the channel between Alice and Eve as shown in the following proposition.

*Proposition* 2. The channel matrix between Alice and Eve is given by

$$\mathbf{H}_{AE} = \begin{bmatrix} h(\ell_{A_1E_1}) & h(\ell_{A_1E_2}) \\ h(\ell_{A_2E_1}) & h(\ell_{A_2E_2}) \end{bmatrix} \in \mathbb{C}^{2\times 2} \tag{10}$$

where

$$\ell^2_{A_1E_1} = 2\rho^2 - 2\rho^2\cos\psi_A + 2\rho\cos\psi_A x_A + 2\rho\sin\psi_A y_A - 2\rho x_A + x_A^2 + y_A^2 \tag{11}$$

$$\ell^2_{A_1E_2} = 2\rho^2 + 2\rho^2\cos\psi_A + 2\rho\cos\psi_A x_A + 2\rho\sin\psi_A y_A + 2\rho x_A + x_A^2 + y_A^2 \tag{12}$$

$$\ell^2_{A_2E_1} = 2\rho^2 + 2\rho^2\cos\psi_A - 2\rho\cos\psi_A x_A - 2\rho\sin\psi_A y_A - 2\rho x_A + x_A^2 + y_A^2 \tag{13}$$

$$\ell^2_{A_2E_2} = 2\rho^2 - 2\rho^2\cos\psi_A - 2\rho\cos\psi_A x_A - 2\rho\sin\psi_A y_A + 2\rho x_A + x_A^2 + y_A^2. \tag{14}$$

A proof of Proposition 2 is similar to that of the Appendix and is thus skipped as it is easy to derive. In a similar fashion, $\mathbf{H}_{BE}$ can be calculated, which represents the channel between Bob and Eve.

### C. Extension to 3D Model

We can extend the result to 3D as follows. Considering multiple rotations of a 3D model, we have a rotation of $\psi$ around the $z$-axis, $\theta$ around the $y$-axis and a $\phi$ around the $x$-axis. The resulting rotation matrix is thus given in (15) [17]. The remaining derivation of the channel model will be similar to that of 2D and thus skipped for the sake of brevity.

### D. SKG Rates

We presume that the channel coefficients between every pair of antennas can be estimated using orthogonal pilots transmitted by the different antennas. The shared secret between Alice and Bob is obtained through measurements of the channel phase only, as the amplitude component is approximately the same for all elements in a given channel matrix. In particular, the phases observed at Alice, Bob, and Eve are given by

$$\hat{\mathbf{H}}_A = \angle\underline{\mathbf{H}_{AB} + \mathbf{N}_A} \tag{16}$$

$$\hat{\mathbf{H}}_B = \angle\underline{\mathbf{H}_{AB} + \mathbf{N}_B} \tag{17}$$

$$\hat{\mathbf{H}}_{AE} = \angle\underline{\mathbf{H}_{AE} + \mathbf{N}_{AE}} \tag{18}$$

$$\hat{\mathbf{H}}_{BE} = \angle\underline{\mathbf{H}_{BE} + \mathbf{N}_{BE}} \tag{19}$$

where $\mathbf{N}_A, \mathbf{N}_B, \mathbf{N}_{AE}, \mathbf{N}_{BE}$ represent the noise components measured at the corresponding receivers, which are modelled as independent complex zero-mean Gaussian variables. Notice that the noise variables represent the measurement error of the complex channel gain coefficients, and that the noise of the measured phase will have a different distribution, similar to the one observed for the phase of Rician fading [18]. The analytical derivation of the joint probability function (PDF) of all the phases, including noise components, is, however, still an open question.

The achievable SKG rate is thus given by [6]:

$$C = \min\left(I(\hat{\mathbf{H}}_A;\hat{\mathbf{H}}_B), I(\hat{\mathbf{H}}_A;\hat{\mathbf{H}}_B|\hat{\mathbf{H}}_{AE},\hat{\mathbf{H}}_{BE})\right). \tag{20}$$

It is worth noting that if Eve has only partial information of the system, e.g., can only measure $H_{AE}$, (20) reduces to

$$C = \min\left(I(\hat{\mathbf{H}}_A;\hat{\mathbf{H}}_B), I(\hat{\mathbf{H}}_A;\hat{\mathbf{H}}_B|\hat{\mathbf{H}}_{AE})\right). \tag{21}$$

As can been seen in Propositions 1 and 2, the measured phases are dependent among each other, and, thus, an analytical evaluation is quite involved. Therefore, to investigate the number of secret bits that can be extracted from the phase randomness we perform numerical evaluation. Specifically, we utilize the Non-parametric Entropy Estimation Toolbox (NPEET) [19], which allows for mutual-information (MI) estimation in complex systems, including the conditional MI (CMI).

## III. Numerical Results

This section numerically evaluates the performance of the proposed approach. In the following simulations, the rotation angles $\psi_A$ and $\psi_B$ have uniform distribution, i.e., $\psi_A \sim \mathcal{U}[0,\pi]$ and $\psi_B \sim \mathcal{U}[0,\pi]$. For simplicity, we also place the centers of antenna array of Alice and Bob at $[-d/2, d/2]^T$ and $[d/2, d/2]^T$, respectively, and, thus, $d$ is the distance between Alice and Bob. In addition, we assume that Alice, Bob, and Eve have the same signal-to-noise ratio (SNR) and the radius $\rho$ is equal to a wavelength. Other simulation parameters are specified for each setting.

In the first experiment, we study the behavior of the MI estimation between Alice and Bob in a 2D scenario. In particular, we fix the number of angle realizations at $1800$, where for each angle we simulate a different number of noise realizations. In addition, we consider two cases in which Eve can fully or partially obtain information from Alice and Bob. In the current context, these correspond to two different extreme scenarios. Since we assume that Alice, Bob and Eve are all subject to the same SNR, the full information means that the distances between Alice and Eve, and between Bob and Eve are the same. Partial information is another extreme case in which Eve can only measure the channel from Alice. This is equivalent to Eve being very far away from Bob, and close to Alice, or there is no direct link from Eve to Bob. In reality we will probably have something in between, with the links from Alice to Eve and from Bob to Eve being unbalanced, and with Eve's observations being dominated by the strongest of them.

As depicted in Fig. 2, the MI increases proportionally to the SNR. It is expected that, as the SNR increases, Alice and Bob will tend to observe exactly the same channel, and, hence, the MI will tend to infinity. However, the measurable MI is limited by the number of realizations, and, beyond a certain SNR, the estimates become unreliable and the MI plateaus. Interestingly, the SKG rate, i.e., the CMI peaks at certain point and then decreases at higher SNR. Intuitively, this phenomenon can stem from the following fact. As can be easily derived from the system model in Fig. 1, if Eve can correctly estimate the angles of arrival from Alice and from Bob, she will also be able to derive the angles between Alice and Bob, and, hence, the channel coefficients between them. To achieve that, however, she needs a very high SNR. This means that increasing the

$$\mathbf{R} = \begin{bmatrix} \cos\psi\cos\theta & \cos\psi\sin\theta\sin\phi - \sin\psi\cos\phi & \cos\psi\sin\theta\cos\phi + \sin\psi\sin\phi \\ \sin\psi\cos\theta & \sin\psi\sin\theta\sin\phi + \cos\psi\cos\phi & \sin\phi\sin\theta\cos\phi - \cos\psi\sin\phi \\ -\sin\theta & \cos\theta\sin\phi & \cos\theta\cos\phi \end{bmatrix} \in \mathbb{C}^{3\times 3} \tag{15}$$

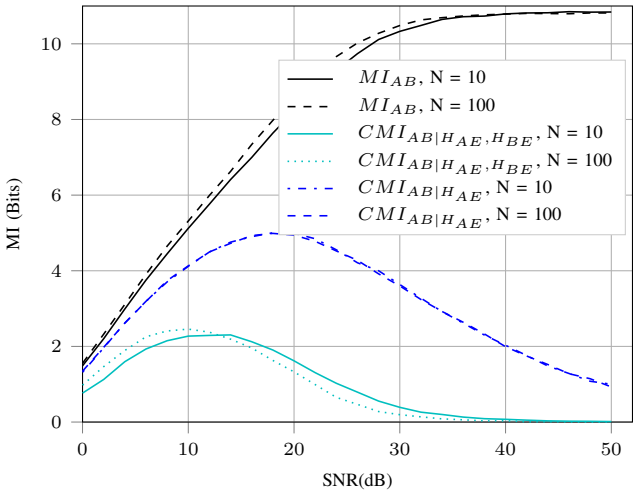
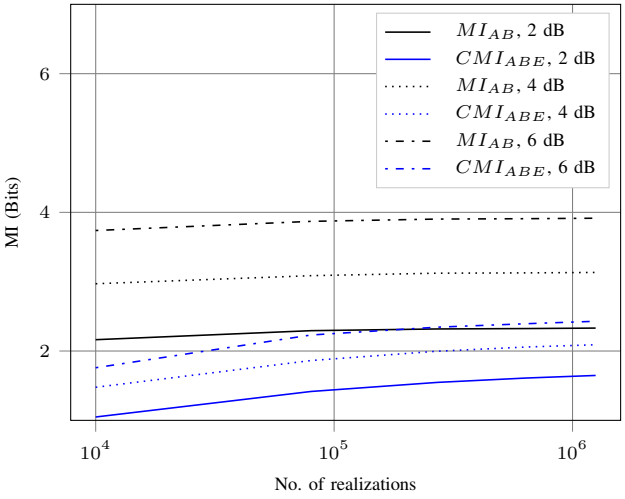


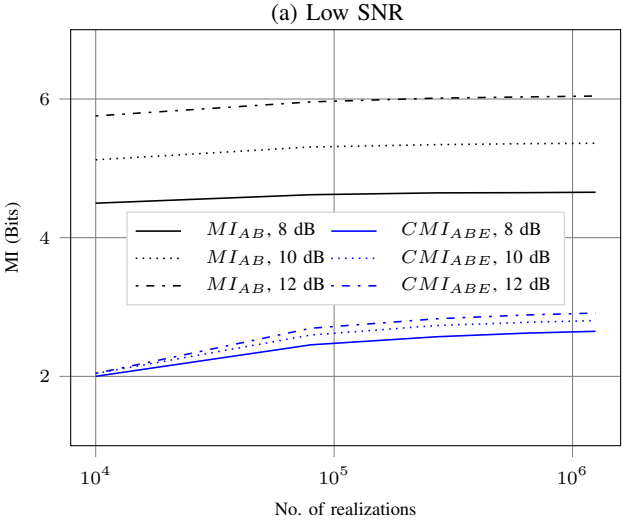

Fig. 2: MI evaluation with varying number of noise realizations $N$. The number of angle rotations is fixed at 1800. The distance between Alice and Bob is $d = 10$ m and the operating frequency $f = 3$ GHz.

SNR beyond a certain point helps not only the legitimate users, but also the eavesdropper. Thus, by controlling the transmit power, Alice and Bob can maximize the achievable SKG rate, taking into account also the eavesdropper's presence. To show the effect of channel information obtained by Eve on the SKG rate, we consider in Fig. 2 two cases, i.e., when Eve measures only a single channel, $H_{AE}$, and when she measures both $H_{AE}$ and $H_{BE}$. As discussed above, increasing the SNR over a certain threshold brings more information to Eve which leads to a decrease in the CMI. If Eve has access to both $H_{AE}$ and $H_{BE}$, it is observed that Alice and Bob must greatly decrease their SNR, e.g., to approximately 10 dB, in order to limit the leakage to Eve. However, if she has limited channel information, e.g., only $H_{AE}$, the legitimate users can afford increasing their SNR, for instance, up to 20 dB to achieve higher SKG rates. As can be also seen from Fig. 2, the number of noise realizations has minimal impact on the MI. This behavior is expected since the rotation plays a major role in creating the randomness of the system, as shown in the following simulation. Hereinafter we consider the worst-case scenarios in which Eve has access to the full channel information of Alice and Bob and evaluate the mutual information in the relevant SNR regimes, i.e., low and medium SNR.

Next, we change the number of channel realizations to study the convergence of our evaluation. Note that we fix the number of noise realizations to 10 and vary the number of random rotations. As can be seen from Fig. 3a, the MI estimation can converge very fast at low SNR. However, in higher SNRs, i.e., Fig. 3b, a higher number of iterations is required to guarantee the convergence. We also notice that the gap between the MI of Alice's and Bob's measurements, $I(\hat{\mathbf{H}}_A; \hat{\mathbf{H}}_B)$ and that of the conditional MI given Eve's observations, $I(\hat{\mathbf{H}}_A; \hat{\mathbf{H}}_B | \hat{\mathbf{H}}_E)$, will widen if we keep increasing the SNR, which matches with our aforementioned observations.




(a) Low SNR

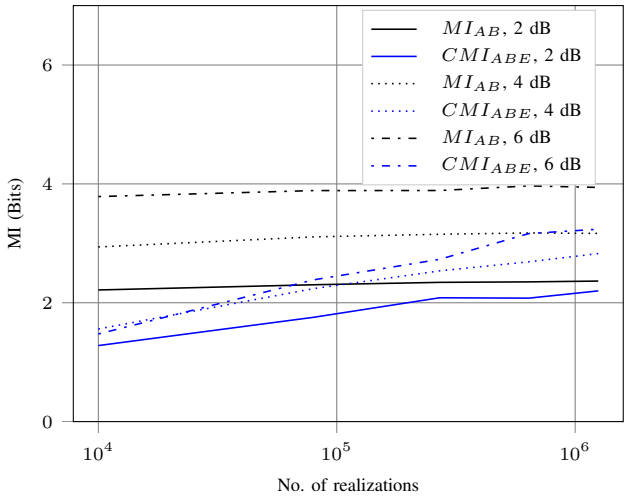



(b) Medium SNR

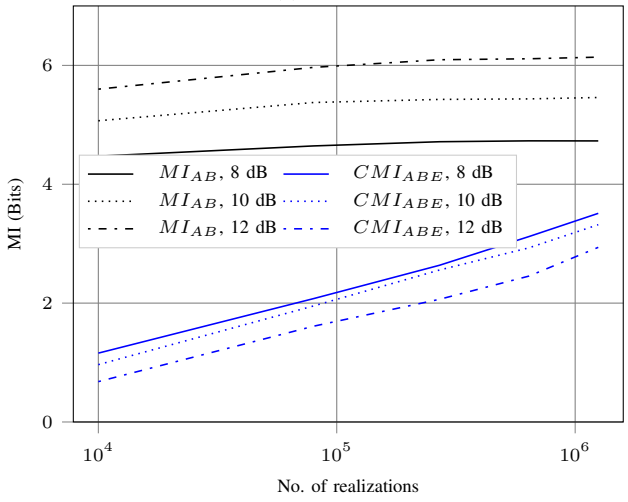
Fig. 3: Convergence behavior of 2D system. The distance between Alice and Bob is $d = 10$ m and the operating frequency $f = 10$ GHz.

The analysis in 2D is a good case study to understand the basic concept of this approach, but, obviously, in reality the devices move and rotate in a 3D space. Therefore, in the following investigations a 3D model is considered. Note

that each of the rotation angles will have uniform distribution in $\mathcal{U}[0, 2\pi]$. Unsurprisingly, we have a similar observation, i.e., the MI estimation converges faster at low SNR and much slower for higher SNR values (c.f. Fig. 4). This is consistent with what we observe in the preceding experiments. Noticeably, even at low SNR, the 3D model requires more channel realizations to converge, as compared to the 2D model. This may be explained by the fact that the system has more degrees of freedom and thus needs more channel realizations to sufficiently convey the information.




(a) Low SNR




(b) Medium SNR

Fig. 4: Convergence behavior of 3D system. The distance between Alice and Bob is $d = 10$ m and the operating frequency $f = 10$ GHz.

Finally, we compare the MI of the 2D and 3D systems under different SNRs. As shown in Fig. 5, the MI and CMI of the 3D model show some improvements over that of 2D, which is due to the higher number of degrees of freedom. However, it is very probable that the rotations are always bounded which has led to incremental improvement and thus needs further study to significantly enhance the MI if an application requires

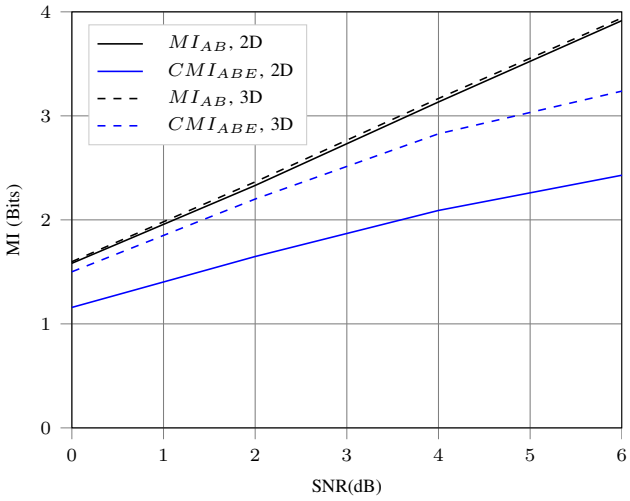



Fig. 5: Mutual information comparison of 2D and 3D models. The distance between Alice and Bob is $d = 10$m and the operating frequency $f = 10$GHz.

higher value of key capacity. Note that in the simulations we are still considering only two antennas also for the 3D model, which explains the little difference between the MI in 2D and 3D models. The use of more antennas is needed in order to capture all degrees of freedom provided by the rotation over three different axes, and we expect to observe a larger difference when more antennas are considered. However, due to computational constraints in the numerical analysis, an investigation with more antennas was not performed yet. We can also notice that the conditional MI improves in 3D over the one in 2D. This is justified by the fact that it is harder for the eavesdropper to extract the information of the channel between Alice and Bob with only two antennas in a 3D scenario.

It should also be noticed that although the achievable SKG rates are apparently low, the temporal aspect was not yet considered. We have so far analyzed the number of secret bits that can be generated from a single realization of random rotations. In a real-life scenario, UAVs are constantly moving, and the angles will also change randomly, which, in turn, will allow more bits to be generated over time.

## IV. Conclusion

We have modelled and evaluated the SKG based on channel properties in the context of UAV communications, in which line-of-sight propagation is expected. In particular, we have added the rotation of the antennas as a source of randomness and modelled the system in both 2D, for understanding, and 3D, which better represents a real-life system. The SKG rate is bounded by the mutual information between the channel observations at Alice and Bob, conditioned on Eve's observations. We have performed numerical evaluations of the MI in case the eavesdropper has partial or full channel information of Alice and Bob, and have shown that when an eavesdropper is present, Alice and Bob should carefully adjust their transmit power, as increasing the SNR will also improve the estimate

at Eve and decrease the achievable SKG rate. We have also noticed that the current MI estimation is computationally expensive, especially for high SNR. Furthermore, it was observed that the 3D model shows improvement in the key capacity compared to that of the 2D model, and therefore our approach to find the achievable SKG rates in realistic scenarios is of great importance to make SKG approach feasible for practical applications. In future works, the analysis will be extended to a larger number of antennas and to a time-varying scenario.

## ACKNOWLEDGEMENT

This work is financed by the Saxon State government out of the State budget approved by the Saxon State Parliament. We also thank Dr. Marco Zoli and Dr. Tom Hößler for their initial study on this topic.

## APPENDIX

Recall that $\mathbf{p}_{A_1}^A = \mathbf{R}\mathbf{p}_{A_1}^0$, where $\mathbf{p}_{A_1}^0 = [\rho, 0]^T$, thus

$$\mathbf{p}_{A_1} = \mathbf{p}_A + \mathbf{p}_{A_1}^A = \mathbf{p}_A + \mathbf{R}\mathbf{p}_{A_1}^0 = \begin{bmatrix} \rho\cos\psi_A + x_A \\ \rho\sin\psi_A + y_A \end{bmatrix}. \quad (22)$$

Similarly we obtain

$$\mathbf{p}_{A_2} = \mathbf{p}_A + \mathbf{p}_{A_2}^A = \begin{bmatrix} -\rho\cos\psi_A + x_A \\ -\rho\sin\psi_A + y_A \end{bmatrix}. \quad (23)$$

Continue in this fashion, we achieve

$$\mathbf{p}_{B_1} = \begin{bmatrix} \rho\cos\psi_B + x_B \\ \rho\sin\psi_B + y_B \end{bmatrix} \quad (24)$$

$$\mathbf{p}_{B_2} = \begin{bmatrix} -\rho\cos\psi_B + x_B \\ -\rho\sin\psi_B + y_B \end{bmatrix}. \quad (25)$$

As a consequence, we can evaluate the distance between those points of interest as follows:

$$\begin{aligned} \ell_{A_1B_1}^2 &= \|\mathbf{p}_{A_1} - \mathbf{p}_{B_1}\|^2 && (26)\\ &= (\rho\cos\psi_A - \rho\cos\psi_B + x_A - x_B)^2 \\ &+ (\rho\sin\psi_A - \rho\sin\psi_B + y_A - y_B)^2 && (27)\\ &= \rho^2(\cos^2\psi_A + \sin^2\psi_A) + \rho^2(\cos^2\psi_B + \sin^2\psi_B) \\ &- 2\rho^2(\cos\psi_A\cos\psi_B + \sin\psi_A\sin\psi_B) \\ &+ 2\rho(\cos\psi_A - \cos\psi_B)(x_A - x_B) \\ &+ 2\rho(\sin\psi_A - \sin\psi_B)(y_A - y_B) \\ &+ (x_A - x_B)^2 + (y_A - y_B)^2. && (28) \end{aligned}$$

By definition, we have the following trigonometric properties

$$\cos^2\alpha + \sin^2\alpha = 1 \quad (29)$$

$$\cos\alpha\cos\beta + \sin\alpha\sin\beta = \cos(\alpha - \beta). \quad (30)$$

Combining (29) and (30) with (28), we thus get

$$\begin{aligned} \ell_{A_1B_1}^2 &= 2\rho^2 - 2\rho^2\cos(\psi_A - \psi_B) - 2\rho(\cos\psi_A - \cos\psi_B)d \\ &- 2\rho(\sin\psi_A - \sin\psi_B)\Delta + d^2 + \Delta^2. && (31) \end{aligned}$$

Repeat the steps above, we obtain

$$\begin{aligned} \ell_{A_1B_2}^2 &= \|\mathbf{p}_{A_1} - \mathbf{p}_{B_2}\|^2 && (32)\\ &= 2\rho^2 + 2\rho^2\cos(\psi_A - \psi_B) - 2\rho(\cos\psi_A + \cos\psi_B)d \\ &+ 2\rho(\sin\psi_A + \sin\psi_B)\Delta + d^2 + \Delta^2 && (33)\\ \ell_{A_2B_1}^2 &= \|\mathbf{p}_{A_2} - \mathbf{p}_{B_1}\|^2 && (34)\\ &= 2\rho^2 + 2\rho^2\cos(\psi_A - \psi_B) + 2\rho(\cos\psi_A - \cos\psi_B)d \\ &- 2\rho(\sin\psi_A - \sin\psi_B)\Delta + d^2 + \Delta^2 && (35)\\ \ell_{A_2B_2}^2 &= \|\mathbf{p}_{A_2} - \mathbf{p}_{B_2}\|^2 && (36)\\ &= 2\rho^2 - 2\rho^2\cos(\psi_A - \psi_B) + 2\rho(\cos\psi_A - \cos\psi_B)d \\ &- 2\rho(\sin\psi_A - \sin\psi_B)\Delta + d^2 + \Delta^2 && (37) \end{aligned}$$

which completes the proof.

## REFERENCES

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

[2] A. Carleial and M. Hellman, "A note on Wyner's wiretap channel (corresp.)," *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 387–390, May 1977.

[3] C. Mitrpant, A. J. H. Vinck, and Yuan Luo, "An achievable region for the Gaussian wiretap channel with side information," *IEEE Trans. Inf. Theory*, vol. 52, no. 5, pp. 2181–2190, May 2006.

[4] P. K. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.

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

[6] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[7] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Trans. Commun.*, vol. 43, no. 1, pp. 3–6, Jan. 1995.

[8] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[9] M. Mitev, A. Chorti, M. Reed, and L. Musavian, "Authenticated secret key generation in delay-constrained wireless systems," *EURASIP Journal on Wireless Communications and Networking*, 2020.

[10] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE ISIT*, 2006, pp. 2593–2597.

[11] E. A. Jorswieck, A. Wolf, and S. Engelmann, "Secret key generation from reciprocal spatially correlated MIMO channels," in *Proc. IEEE Globecom Workshops*, 2013, pp. 1245–1250.

[12] M. Mitev, A. Chorti, E. V. Belmega, and H. V. Poor, "Protecting physical layer secret key generation from active attacks," *Entropy*, vol. 23, no. 8, 2021.

[13] Y. Zeng, R. Zhang, and T. J. Lim, "Wireless communications with unmanned aerial vehicles: opportunities and challenges," *IEEE Commun. Mag.*, vol. 54, no. 5, pp. 36–42, May 2016.

[14] X. Sun *et al.*, "Physical layer security in UAV systems: Challenges and opportunities," *IEEE Wireless Commun.*, vol. 26, no. 5, pp. 40–47, Oct. 2019.

[15] Y. Zhou *et al.*, "Robust trajectory and transmit power optimization for secure UAV-enabled cognitive radio networks," *IEEE Trans. Commun.*, vol. 68, no. 7, pp. 4022–4034, Jul. 2020.

[16] H. Friis, "A note on a simple transmission formula," *in Proc. IRE*, vol. 34, no. 5, pp. 254–256, 1946.

[17] E. Weisstein, *CRC Concise Encyclopedia of Mathematics*. CRC Press, 2002.

[18] Z. Luo, Y. Zhan, and E. Jonckheere, "Analysis on functions and characteristics of the Rician phase distribution," in *Proc. IEEE ICCC*, 2020, pp. 306–311.

[19] A. Kraskov, H. Stögbauer, and P. Grassberger, "Estimating mutual information," *Phys. Rev. E*, vol. 69, p. 066138, Jun. 2004.