

# Frequency Diversity for Ultra-Reliable and Secure Communications in Sub-THz Two-Ray Scenarios

Karl-Ludwig Besser and Eduard A. Jorswieck  
Institute for Communications Technology  
Technische Universität Braunschweig, Germany  
Email: {k.besser, e.jorswieck}@tu-bs.de

Justin P. Coon  
Department of Engineering Science  
University of Oxford, U. K.  
Email: justin.coon@eng.ox.ac.uk

**Abstract**—Ensuring a reliable and simultaneously secure transmission of data is one of the major challenges for wireless communication systems. This is especially difficult when no perfect channel state information (CSI) at the transmitter is available. In this work, we consider a two-ray ground reflection scenario with a passive eavesdropper. At the transmitter, there only exists limited knowledge about the channels to both the legitimate receiver and the eavesdropper. We propose a simple frequency diversity scheme which maximizes the worst-case secrecy capacity for the considered scenario. In particular, we show how to optimally adjust the frequency spacing between the used frequencies. Thereby, we can guarantee a certain secrecy rate at which data can be transmitted both reliably and securely for all locations of the receivers.

**Index Terms**—Ultra-reliable communications, Two-ray ground reflection, Frequency diversity, Physical Layer Security, Worst-case design

## I. INTRODUCTION

Emerging technologies like 6G enable many novel applications that rely on wireless communications technology to transmit sensitive information [1], [2]. This creates the need of techniques which allow both secure and ultra-reliable communications simultaneously [3], [4]. In particular, low outage probabilities below  $10^{-5}$  need to be assured [5], especially in scenarios where only limited channel state information (CSI) is available.

It has been observed that negative dependency between channel gains can significantly improve reliability [6] and secrecy [7]. The basic idea is to establish multi-link diversity and ensure that always one communication link is available, if the others fail. We will apply this idea in the following to develop a simple frequency diversity scheme that enables ultra-reliable and secure communications in two-ray ground reflection scenarios. In this two-ray model, it is assumed that only one significant multipath component exists in addition to a line-of-sight (LoS) connection. The second component is typically caused by a single reflection on a ground surface. This could occur in flat outdoor terrain [8], on large concrete areas, e.g., airports [9], and for a unmanned aerial vehicle (UAV) flying above water [10], [11]. It has also been observed that

the two-ray model can be appropriate for vehicle-to-vehicle (V2V) communication scenarios [12].

When varying the distance between transmitter and receiver, the relative phase of the two received signal components varies and they may interfere constructively or destructively. A destructive interference causes a drop of receive power, which in turn could cause an outage of the communication link. In order to mitigate drops of the signal power on one frequency, a second frequency can be used in parallel. The use of multiple frequencies in parallel to create diversity and improve the reliability in ground reflection scenarios has already been proposed in [6] and [13].

In this work, we include an additional passive eavesdropper at an unknown distance to the transmitter. The aim of this work is to show that the simple frequency diversity with two frequencies can be used to ensure a certain worst-case secrecy rate. This also corresponds to maximizing the zero-outage secrecy capacity (ZOSC) [14]. In particular, we optimize the frequency spacing such that the worst-case secrecy rate is maximized.

Our contributions are summarized as follows.

- We show that worst-case design of the secrecy rate can be done by only performing a worst-case design with respect to the legitimate receiver, i.e., it is independent of the eavesdropper's location. (Theorem 2)
- It is illustrated by numerical examples that a positive ZOSC can be achieved using the proposed scheme (Example 3).
- Additionally, we provide necessary and sufficient conditions whether a positive ZOSC is achievable (Section V).

The source code to reproduce all presented results and simulations is made publicly available at [15].

*Notation:* In order to simplify the notation, we will omit variables on which functions depend when their value is clear from the context, e.g., we will write  $f(x)$  instead of  $f(x, y)$  when the value of  $y$  is fixed.

Since the angular frequency  $\omega = 2\pi f$  is a simple scaling of the frequency  $f$ , we will treat them somewhat interchangeably. Especially for calculations, it is more convenient to use  $\omega$ , while  $f$  is relevant for actual system design. We will therefore use the frequency  $f$  for the numerical examples while expressing all formulas in terms of the angular frequency  $\omega$ .

The work of E. Jorswieck is partly supported by the Federal Ministry of Education and Research Germany (BMBF) as part of the 6G Research and Innovation Cluster 6G-RIC under Grant 16KISK020K. The work of J. Coon is supported by the EPSRC under grant number EP/T02612X/1.

## II. SYSTEM MODEL AND PROBLEM FORMULATION

Throughout this work, we consider a communication system where a transmitter (Alice) transmits data to a legitimate receiver (Bob). While the exact distance  $d_B$  between them is unknown, we have knowledge about an interval  $[d_{\min,B}, d_{\max,B}]$  of possible distances, i.e.,  $d_B \in [d_{\min,B}, d_{\max,B}]$ . This interval could be obtained, e.g., by a distance estimation with a given uncertainty, or it could stem from the scenario geometry. Additionally, an eavesdropper (Eve) is at an unknown distance  $d_E$  from the transmitter. However, there is a security perimeter around Alice such that the distance to the eavesdropper is at least  $d_{\min,E}$ , i.e.,  $d_E \geq d_{\min,E}$ . An overview of the considered scenario can be found in Figure 1.

The whole terrain is assumed to be flat such that the channels between all communication parties can be modeled by the two-ray ground reflection model [16], which is depicted in Figure 2. In this scenario, the transmitted signal is propagated via two separate paths to the receiver. First, there is a LoS propagation with path length  $\ell$ . Additionally, the signal is reflected by the ground, which leads to a second component which superimposes with the LoS component at the receiver. The total length of the second ray is  $\tilde{\ell} > \ell$ . From basic trigonometric considerations, the path lengths can be calculated as

$$\ell_u^2 = (h_{Tx} - h_{Rx,u})^2 + d_u^2 \quad (1)$$

$$\tilde{\ell}_u^2 = (h_{Tx} + h_{Rx,u})^2 + d_u^2, \quad (2)$$

where the index  $u \in \{B, E\}$  represents the receivers Bob and Eve.

In order to increase the reliability, a frequency diversity scheme with two frequencies,  $\omega_1 = 2\pi f_1$  and  $\omega_2 = \omega_1 + \Delta\omega$ , is used. The achievable rate  $R$  for a transmission over such a channel is given by

$$R = W \log_2 \left( 1 + \frac{P_s}{WN_0} \right), \quad (3)$$

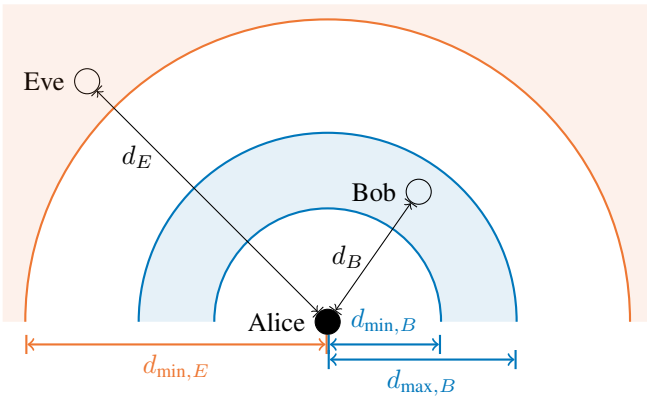


Figure 1. Geometric model of the considered communication scenario. The legitimate receiver (Bob) is at an unknown distance  $d_B$  from the transmitter, which is within the known interval  $[d_{\min,B}, d_{\max,B}]$ . Around the transmitter, there exists a safety perimeter at distance  $d_{\min,E}$ , such that potential eavesdroppers (Eve) are at least this far away from the transmitter, i.e.,  $d_E \geq d_{\min,E}$ .

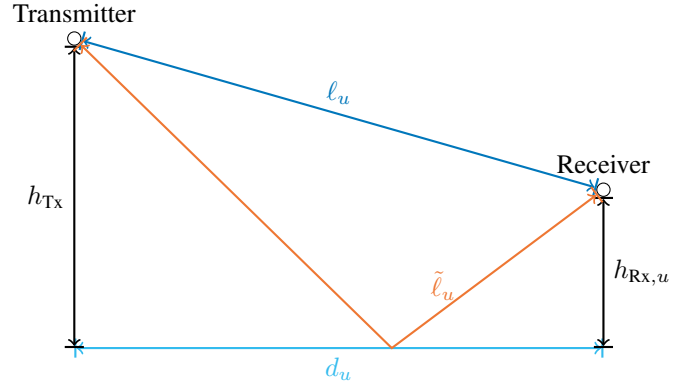


Figure 2. Geometrical model of the considered two-ray ground reflection scenario. The transmitter is placed at height  $h_{Tx}$  above the ground. The receiver  $u$  is located at height  $h_{Rx,u}$  at a (ground) distance  $d_u$  away from the transmitter. The LoS path and reflection path have lengths  $\ell_u$  and  $\tilde{\ell}_u$ , respectively.

where  $P_s$  is the received sum power,  $W$  is the total bandwidth, and  $N_0$  is the noise spectral density. Note that this formula is a narrow-band approximation which requires a small bandwidth  $W$  compared to the carrier frequency  $f_1$  [17, Chap. 5]. We will use this assumption throughout the work.

The secrecy capacity  $C_S$ , i.e., the highest rate at which one can transmit securely without any leaked information to the eavesdropper, is given by [18],

$$C_S = [R_B - R_E]^+, \quad (4)$$

where  $R_B$  and  $R_E$  represent the achievable rates to Bob and Eve, respectively.

### A. Problem Formulation

In the following, we want to consider the problem of optimally selecting the frequency spacing  $\Delta\omega$  such that the worst-case secrecy capacity is maximized. This worst-case design is especially useful in applications where an ultra-high reliability is required, since it provides a performance guarantee that even holds in the worst-case scenario. The exact problem statement is given as follows.

**Problem Statement 1.** Consider the described frequency diversity communication system with a passive eavesdropper. Since we only have limited knowledge about the distances between transmitter and receivers, we want to adjust the frequency spacing  $\Delta\omega$  such that the *worst-case secrecy capacity* with respect to the distances  $d_B$  and  $d_E$  is maximized, i.e.,

$$C_S^* = \max_{\Delta\omega} \min_{\substack{d_B \in [d_{\min,B}, d_{\max,B}] \\ d_E \geq d_{\min,E}}} C_S. \quad (5)$$

## III. WORST-CASE SECRECY RATE

In this section, we first analyze the inner part of (5), i.e., the worst-case secrecy capacity for given distance intervals.

In order to simplify the problem, we replace the exact minimum over all possible distance combinations by a lower

$$P_s(d, \Delta\omega; \omega_1, h_{\text{Tx}}, h_{\text{Rx}}, P_t) = \frac{P_t}{2} \left(\frac{c}{2}\right)^2 \left[ \left(\frac{1}{\omega_1^2} + \frac{1}{\omega_2^2}\right) \left(\frac{1}{\ell^2} + \frac{1}{\tilde{\ell}^2}\right) - \frac{2}{\ell\tilde{\ell}} \left( \frac{\cos\left(\frac{\omega_1}{c}(\tilde{\ell} - \ell)\right)}{\omega_1^2} + \frac{\cos\left(\frac{\omega_2}{c}(\tilde{\ell} - \ell)\right)}{\omega_2^2} \right) \right] \quad (7)$$

$$\underline{P}_s(d, \Delta\omega; \omega_1, h_{\text{Tx}}, h_{\text{Rx}}, P_t) = \frac{P_t}{2} \left(\frac{c}{2}\right)^2 \left[ \left(\frac{1}{\omega_1^2} + \frac{1}{\omega_2^2}\right) \left(\frac{1}{\ell^2} + \frac{1}{\tilde{\ell}^2}\right) - \frac{2}{\ell\tilde{\ell}} \sqrt{\left(\frac{1}{\omega_1^2}\right)^2 + \left(\frac{1}{\omega_2^2}\right)^2 + \frac{2 \cos\left(\frac{\Delta\omega}{c}(\tilde{\ell} - \ell)\right)}{\omega_1^2 \omega_2^2}} \right] \quad (8)$$

$$\overline{P}_s(d, \Delta\omega; \omega_1, h_{\text{Tx}}, h_{\text{Rx}}, P_t) = \frac{P_t}{2} \left(\frac{c}{2}\right)^2 \left(\frac{1}{\omega_1^2} + \frac{1}{\omega_2^2}\right) \left(\frac{1}{\ell} + \frac{1}{\tilde{\ell}}\right)^2 \quad (9)$$

bound. Since we are interested in worst-case design, we can still use this lower bound to give performance guarantees. In particular, we transform the problem by taking the individual worst-cases for Bob and Eve as

$$\min_{\substack{d_B \in [d_{\min, B}, d_{\max, B}] \\ d_E \geq d_{\min, E}}} C_S \geq \min_{d_B \in [d_{\min, B}, d_{\max, B}]} R_B - \max_{d_E \geq d_{\min, E}} R_E. \quad (6)$$

In the following, we will derive expressions for the individual worst-case rates. For this, we first investigate the receive power and next analyze the rate expressions.

#### A. Receive Power

The total received power  $P_s$  is given as the sum of the receive powers at frequencies  $\omega_1$  and  $\omega_2 = \omega_1 + \Delta\omega$ . For each frequency, the receive power is given according to the two-ray ground reflection model [16]. The resulting expression for the total received (sum) power  $P_s$  is shown in (7) at the top of this page, where  $c$  denotes the speed of light. The total transmit power  $P_t$  is equally distributed over the two frequencies. Note that the distance  $d$  and the transmitter and receiver heights  $h_{\text{Tx}}$  and  $h_{\text{Rx}}$  are influencing the receive power via the ray lengths  $\ell$  and  $\tilde{\ell}$ .

Since we are interested in worst-case design, we need worst-case bounds on  $P_s$ . For Bob, we use the lower bound  $\underline{P}_s$  from [19, Lem. 1], which is shown in (8) at the top of this page. Similarly, we need an upper bound as the worst-case for Eve. This upper bound  $\overline{P}_s$  is given in (9) at the top of this page. Therefore, the relation  $\underline{P}_s \leq P_s \leq \overline{P}_s$  holds.

*Example 1.* The receive power and its bounds are illustrated with the following numerical example. We set the parameters to  $f_1 = 2.4$  GHz,  $\Delta f = 250$  MHz,  $h_{\text{Tx}} = 10$  m, and  $h_{\text{Rx}} = 1.5$  m. For these values, Figure 3 shows the actual receive power  $P_s$  from (7), the lower bound  $\underline{P}_s$  from (8), and the upper bound  $\overline{P}_s$  from (9) over the distance  $d$  between transmitter and receiver. It can be seen that there occur drops in the receive power at certain distances where the LoS and the reflected component superimpose destructively at the receiver. The location of the drops can be influenced by the choice of the frequency spacing  $\Delta\omega$  [19]. Additionally, the receive power decreases overall with an increasing distance due to the higher path loss.

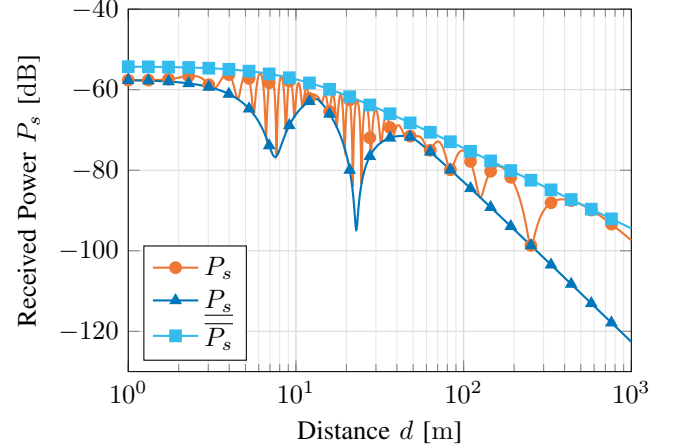


Figure 3. Total receive power for two frequencies with  $f_1 = 2.4$  GHz,  $\Delta f = 250$  MHz,  $h_{\text{Tx}} = 10$  m, and  $h_{\text{Rx}} = 1.5$  m. The actual value  $P_s$  from (7), the lower bound  $\underline{P}_s$  from (8), and the upper bound  $\overline{P}_s$  from (9) are shown. (Example 1)

#### B. Rate Bounds

With the expressions for the receive power, we can calculate the achievable rates according to (3). Since the rate is a strictly monotonically increasing function of the receive power, it is maximized (resp. minimized) when the power is maximized (resp. minimized).

1) *Bob:* The worst-case rate to Bob is given in the case when it is minimal, i.e., when the receive power at Bob is minimal. This problem has been studied in detail in [19], [20] and the solution can be found in [20, Thm. 2].

2) *Eve:* For Eve, the worst-case rate occurs when her receive power is maximal. In the following, we use the following upper bound for Eve's rate.

**Lemma 1** (Upper Bound for the Rate of the Eavesdropper). *For the described communication system with uncertainty about the distance between transmitter and the eavesdropper, we have*

$$\max_{d_E \geq d_{\min, E}} R_E \leq \overline{R}_E, \quad (10)$$

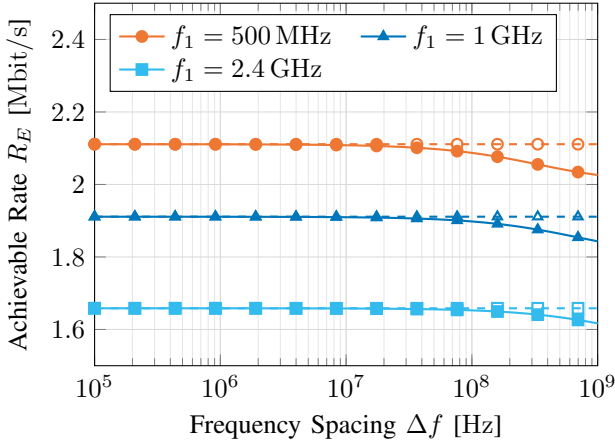


Figure 4. Worst-case achievable rate for Eve with  $d_{\min,E} = 100$  m,  $h_{Tx} = 10$  m,  $h_{Rx,E} = 1.5$  m, and  $W = 100$  kHz for different values of  $f_1$ . The solid lines indicate the rate when using  $\overline{P_s}$  for the rate calculation and the dashed lines show the upper bound  $\overline{R_E}$  from (11). (Example 2)

with

$$\overline{R_E} = W \log_2 \left( 1 + \frac{P_t}{WN_0} \left( \frac{c}{2} \right)^2 \frac{1}{\omega_1^2} \left( \frac{1}{\ell_E} + \frac{1}{\bar{\ell}_E} \right)^2 \right) \Big|_{d_E=d_{\min,E}} \quad (11)$$

*Proof.* From (9), it can be seen that the upper bound on the receive power is monotonically decreasing with the distance. Therefore, it is maximized at the minimum distance, which is  $d_{\min,E}$  in the case of the considered eavesdropper. This yields the worst-case for Eve

$$\max_{d_E \geq d_{\min,E}} R_E \leq W \log_2 \left( 1 + \frac{\overline{P_s}(d_{\min,E}, \Delta\omega)}{WN_0} \right). \quad (12)$$

Since we have that  $\omega_2 \geq \omega_1$ , this can be further bounded by

$$W \log_2 \left( 1 + \frac{\overline{P_s}(d_{\min,E}, \Delta\omega)}{WN_0} \right) \leq \overline{R_E}$$

which yields (10).  $\square$

**Remark 1.** The bound  $\overline{R_E}$  becomes tight for  $\Delta\omega \ll \omega_1$ , since  $\omega_1 \approx \omega_2$  holds in this case.

**Example 2.** For a numerical illustration of Lemma 1, we use the parameters  $d_{\min,E} = 100$  m,  $h_{Tx} = 10$  m,  $h_{Rx,E} = 1.5$  m, and  $W = 100$  kHz. Figure 4 shows both the right-hand side from (12) (solid lines) and the upper bound  $\overline{R_E}$  from (11) for different values of  $f_1$ . First, it can be seen that  $\overline{R_E}$  is indeed an upper bound on the worst-case rate of the eavesdropper. Second, we can also observe that  $\overline{R_E}$  approximates the right-hand side of (12) for  $\Delta\omega \ll \omega_1$ .

#### IV. OPTIMAL FREQUENCY SPACING

With Lemma 1 in Section III, we can replace (6) by

$$\min_{\substack{d_B \in [d_{\min,B}, d_{\max,B}] \\ d_E \geq d_{\min,E}}} C_S \geq \underline{C_S}$$

with

$$\underline{C_S} = \min_{d_B \in [d_{\min,B}, d_{\max,B}]} R_B - \overline{R_E}. \quad (13)$$

Since  $\overline{R_E}$  is independent of the frequency spacing  $\Delta\omega$ , it does not need to be considered in the outer optimization of (5). Instead, we obtain the new optimization problem

$$\underline{C_S}^* = \max_{\Delta\omega} \underline{C_S} = \max_{\Delta\omega} \min_{d_B \in [d_{\min,B}, d_{\max,B}]} R_B - \overline{R_E}, \quad (14)$$

whose solution provides a lower bound on the solution of (5).

In order to solve the optimization problem in (14), we need the following result from [19], which we restate in the following as Theorem 1. Additionally, we need the following definitions of  $\Delta\omega_\pi$  and  $\widetilde{\Delta\omega}$  from [19]

$$\Delta\omega_\pi(d) = \frac{\pi c}{\bar{\ell}(d) - \ell(d)} \quad (15)$$

$$\widetilde{\Delta\omega}(d) = \frac{2\pi c}{\bar{\ell}(d) - \ell(d)}. \quad (16)$$

**Theorem 1** ([19, Thm. 2]). *Consider the described communication system with only the legitimate receiver, where two frequencies  $\omega_1$  and  $\omega_2 = \omega_1 + \Delta\omega$  are used in parallel. The optimal frequency spacing  $\Delta\omega^*$  for maximizing the worst-case receive power  $\underline{P_s}$ , i.e.,*

$$\Delta\omega^* = \arg \max_{\Delta\omega} \min_{d \in [d_{\min}, d_{\max}]} \underline{P_s}(d, \Delta\omega),$$

is given by the intersection of  $\underline{P_s}(d_{\max}, \Delta\omega)$  and  $g(\Delta\omega)$  in the interval  $\Delta\omega \in [\Delta\omega_\pi(d_{\min}), \Delta\omega_\pi(d_{\max})]$ , if it exists, with

$$g(\Delta\omega) = \begin{cases} \underline{P_s}(d_{\min}, \Delta\omega) & \text{if } 0 < \Delta\omega < \widetilde{\Delta\omega}(d_{\min}) \\ \underline{P_s}(d_1, \Delta\omega) & \text{if } \widetilde{\Delta\omega}(d_{\min}) \leq \Delta\omega < \widetilde{\Delta\omega}(d_{\max}) \end{cases} \quad (17)$$

and  $\underline{P_s}(d_1, \Delta\omega)$  in (18) at the top of the next page. Otherwise, if no intersection exists, it is given by the maximum of  $\underline{P_s}(d_{\max}, \Delta\omega)$ , which is approximately located at

$$\Delta\omega^* \approx \frac{c\pi}{\bar{\ell}(d_{\max}) - \ell(d_{\max})} = \Delta\omega_\pi(d_{\max}). \quad (19)$$

This result now enables us to solve the optimization problem in (14) and determine the optimal frequency spacing for maximizing the worst-case secrecy rate as shown in the following theorem.

**Theorem 2** (Optimal Frequency Spacing for Worst-Case Design). *The optimal frequency spacing  $\Delta\omega^*$  which solves the optimization problem (14) is given by Theorem 1 ([19, Thm. 2]).*

*Proof.* As discussed in Section III, optimizing the rate is equivalent to optimizing the receive power due to the monotonic nature of the logarithm. Therefore, the max-min problem of  $R_B$  in (14) can be reformulated as a max-min problem of the receive power at Bob as

$$\max_{\Delta\omega} \min_{d_B \in [d_{\min,B}, d_{\max,B}]} R_B = W \log_2 \left( 1 + \frac{1}{WN_0} \max_{\Delta\omega} \min_{d_B \in [d_{\min,B}, d_{\max,B}]} \underline{P_s}(d_B, \Delta\omega) \right). \quad (20)$$

$$P_s(d_1, \Delta\omega) = \frac{P_t}{2} \left( \frac{c^2 \pi \Delta\omega}{2} \right)^2 \left( \frac{1}{\omega_1^2} + \frac{1}{\omega_2^2} \right) \left( \frac{1}{\sqrt{(c^2 \pi^2 - h_{Rx} h_{Tx} \Delta\omega^2)^2}} - \frac{1}{\sqrt{(c^2 \pi^2 + h_{Rx} h_{Tx} \Delta\omega^2)^2}} \right)^2 \quad (18)$$

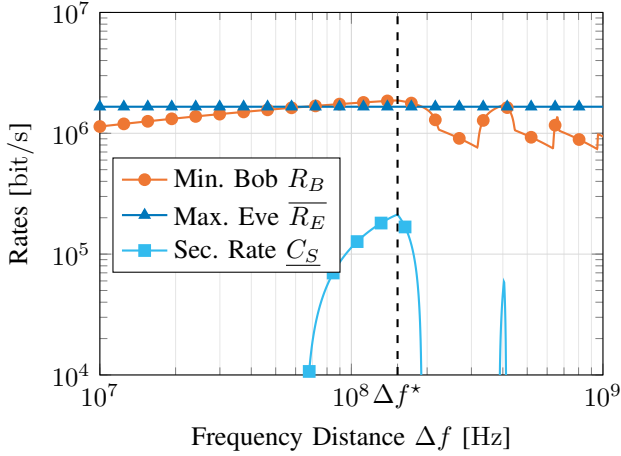


Figure 5. Worst-case rates to Bob and Eve together with the resulting secrecy rate  $C_S$  over a varying frequency spacing  $\Delta f$ . The system parameters are set to  $h_{Tx} = 10$  m,  $h_{Rx,B} = h_{Rx,E} = 1.5$  m,  $d_{min,B} = 20$  m,  $d_{max,B} = 30$  m,  $d_{min,E} = 100$  m,  $f_1 = 2.4$  GHz, and  $W = 100$  kHz. The optimal frequency distance  $\Delta f^* = 152$  MHz is found according to Theorem 2 by [19, Thm. 2]. (Example 3)

The solution  $\Delta\omega^*$  to the optimization problem of maximizing the minimum receive power  $\underline{P}_s$  is presented in Theorem 1 ([19, Thm. 2]).  $\square$

The main takeaway from Theorem 2 is that we can perform worst-case design of the secrecy rate by only considering the legitimate receiver. This is achieved by bounding the eavesdropper's performance by the constant  $\overline{R}_E$ . While the resulting secrecy rate  $C_S^*$  may be less than the solution  $C_S^*$  of the original problem (5), it still provides a worst-case bound that can always be achieved. Hence, by applying Theorem 2, we may underestimate the performance, however, we can give performance guarantees that will never be violated.

**Example 3.** For a numerical example, we again use the system parameters  $h_{Tx} = 10$  m,  $h_{Rx,B} = h_{Rx,E} = 1.5$  m,  $d_{min,B} = 20$  m,  $d_{max,B} = 30$  m,  $d_{min,E} = 100$  m,  $f_1 = 2.4$  GHz, and  $W = 100$  kHz. In Figure 5, we show the minimum rate  $\min_{d_B} R_B$  to Bob, the worst-case upper bound  $\overline{R}_E$  of Eve's rate, and the resulting worst-case secrecy rates  $\underline{C}_S$  over the frequency spacing  $\Delta f$ .

As described in Theorem 2, the optimal frequency spacing  $\Delta f^*$ , which maximizes both the minimum rate to Bob and the secrecy rate, is determined according to [19, Thm. 2]. For the given parameters, it is calculated to  $\Delta f^* = 152$  MHz. From this, it follows that the maximum worst-case secrecy rate is  $\underline{C}_S^* = 212$  kbit/s.

**Example 4 (Higher Frequency Example).** In order to show that the proposed scheme also works for higher frequency

bands, we now consider the following numerical example. The carrier frequency is set to  $f_1 = 30$  GHz, while the other system parameters are given as  $h_{Tx} = 5$  m,  $h_{Rx,B} = 1$  m,  $h_{Rx,E} = 1.5$  m,  $d_{min,B} = 40$  m,  $d_{max,B} = 50$  m,  $d_{min,E} = 100$  m, and  $W = 100$  kHz. Based on these parameters, the optimal frequency spacing is calculated according to Theorem 1 as  $\Delta f^* = 751$  MHz. The resulting maximum worst-case secrecy rate is then  $\underline{C}_S^* = 91.6$  kbit/s.

## V. POSITIVE ZERO-OUTAGE SECRECY RATE

For the parameters chosen in Example 3 and 4, the maximum worst-case secrecy rate is positive. This has the important implication that it is possible to transmit at a positive rate without any information leakage to an eavesdropper even in the worst-case, i.e., it is possible to achieve a positive ZOSC [14]. Additionally, it should be highlighted that the proposed scheme does *not* require perfect CSI at the transmitter but only limited knowledge about the receiver positions.

While the worst-case secrecy rate is positive for the parameters in Example 3, the immediate question arises whether this is always possible for all parameter choices. From the expressions of the receive power in (7)-(9), it can be seen that this is not the case, e.g., if the eavesdropper is closer to the transmitter than the legitimate receiver. It is therefore of interest to find simple conditions on the system parameters, which allow checking whether a positive ZOSC can be achieved, without having to solve the optimization problem in (14). Such simple conditions are presented in the following.

**Corollary 1** (Necessary condition for  $\underline{C}_S^* > 0$ ). *Consider the described communication system with  $\omega_1 \gg \Delta\omega$ . The relation*

$$\frac{1}{\ell_B^2} + \frac{1}{\tilde{\ell}_B^2} \Big|_{d_B=d_{max,B}} > \frac{1}{\ell_E^2} + \frac{1}{\tilde{\ell}_E^2} \Big|_{d_B=d_{min,E}} \quad (21)$$

*is a necessary condition for a positive ZOSC, i.e., for  $\underline{C}_S^* > 0$ .*

*Proof.* The proof can be found in Appendix A.  $\square$

In the other direction, we can also find a sufficient condition that a positive ZOSC can definitely be achieved.

**Corollary 2** (Sufficient condition for  $\underline{C}_S^* > 0$ ). *Consider the described communication system with  $\omega_1 \gg \Delta\omega$ . If*

$$\underline{P}_s(d_{max,B}, \Delta\omega_\pi(d_{min,B})) > \frac{P_t}{\omega_1^2} \left( \frac{c}{2} \right)^2 \left( \frac{1}{\ell_E} + \frac{1}{\tilde{\ell}_E} \right)^2 \Big|_{d_E=d_{min,E}} \quad (22)$$

*with*

$$\Delta\omega_\pi(d) = \frac{c\pi}{\tilde{\ell}(d) - \ell(d)} \quad (23)$$

*holds, we have  $\underline{C}_S^* > 0$ , and thus, a positive ZOSC is achievable.*

*Proof.* The proof can be found in Appendix B.  $\square$

*Remark 2.* It should be noted that there exists a gap between the necessary and sufficient conditions from Corollary 1 and 2, respectively. This means that there exist parameter choices for which condition (22) is not fulfilled but the solution to (14) is still positive. Similarly, there exist parameters such that condition (21) holds but we still get  $\underline{C}_S^* = 0$  as demonstrated in the following examples.

*Example 5.* For the parameters from Example 3, (22) holds true and we already know that a positive ZOSC can be achieved. The actual solution  $\underline{C}_S^*$  can be found in Example 3.

*Example 6.* For the next example, we consider the same parameter as in Example 3 with the only difference that  $d_{\min,E}$  is varied. With  $d_{\min,E} = 50$  m, the sufficient condition (22) from Corollary 2 is not fulfilled. Therefore, we do not automatically know whether a positive ZOSC can be achieved. However, the necessary condition (21) from Corollary 1 is fulfilled. Therefore, it is at least possible to have  $\underline{C}_S^* > 0$ . In fact, solving the optimization problem (14) yields the worst-case secrecy rate to be  $\underline{C}_S^* = 16.7$  kbit/s, i.e., a positive ZOSC is achievable. Similarly, when setting  $d_{\min,E}$  to  $d_{\min,E} = 40$  m, the necessary condition holds but the solution to (14) is  $\underline{C}_S^* = 0$  in this case. This example shows that there is a gap between the necessary and sufficient conditions from (21) and (22), respectively. When further reducing  $d_{\min,E}$ , e.g., to  $d_{\min,E} = 20$  m, condition (21) is not fulfilled, which directly implies that  $\underline{C}_S^* = 0$ .

## VI. CONCLUSION AND FUTURE WORK

In this work, we have investigated a simple frequency diversity system for maximizing the worst-case secrecy rate in a two-ray ground reflection scenario with limited CSI at the transmitter. We showed that the optimal frequency spacing for worst-case design is independent of the eavesdropper. The resulting worst-case secrecy rate corresponds to the ZOSC and can therefore always be guaranteed.

While we only considered an equal power split between the two used frequencies, this power allocation could also be optimized in future work. Furthermore, the use of additional frequencies could be considered.

### APPENDIX A PROOF OF COROLLARY 1

In order to prove Corollary 1, we show that the (logical) negation of (21), i.e.,

$$\frac{1}{\ell_B^2} + \frac{1}{\tilde{\ell}_B^2} \bigg|_{d_B=d_{\max,B}} \leq \frac{1}{\ell_E^2} + \frac{1}{\tilde{\ell}_E^2} \bigg|_{d_B=d_{\min,E}} \quad (24)$$

is a sufficient condition for  $\underline{C}_S^* = 0$ .

It is straightforward to see that the solution  $\underline{C}_S^*$  to (14) is zero, if  $\overline{R}_E \geq \max_{\Delta\omega} \min_{d_B} R_B$  holds.

As discussed in Section III, we will only compare the receive powers instead of the rate expressions in the following.

First, it follows from [19, Lem. 3] and [19, Lem. 2] that

$$\max_{\Delta\omega} \min_{d_B \in [d_{\min,B}, d_{\max,B}]} \underline{P}_s(d_B, \Delta\omega) \quad (25)$$

$$\leq \max_{\Delta\omega} \underline{P}_s(d_{\max,B}, \Delta\omega) \quad (26)$$

$$= \underline{P}_s(d_{\max,B}, \Delta\omega_\pi(d_{\max,B})) \quad (27)$$

with

$$\Delta\omega_\pi(d_{\max,B}) = \frac{c\pi}{\tilde{\ell}_B(d_{\max,B}) - \ell_B(d_{\max,B})}$$

where (27) holds for  $\omega_1 \gg \Delta\omega$  [19, Lem. 2].

Next, we compare these expressions with the receive power corresponding to  $\overline{R}_E$  from (11) (already omitting the common factors). If condition (24) holds, the following chain of inequalities also holds, which then implies  $\overline{R}_E \geq \max_{\Delta\omega} \min_{d_B} R_B$  and in turn  $\underline{C}_S^* = 0$ ,

$$\frac{2}{\omega_1^2} \left( \frac{1}{\ell_E} + \frac{1}{\tilde{\ell}_E} \right)^2 \bigg|_{d_E=d_{\min,E}} \stackrel{(a)}{\geq} \frac{2}{\omega_1^2} \left( \frac{1}{\ell_E^2} + \frac{1}{\tilde{\ell}_E^2} \right) \bigg|_{d_E=d_{\min,E}} \quad (28)$$

$$\stackrel{(b)}{\geq} \frac{2}{\omega_1^2} \left( \frac{1}{\ell_B^2} + \frac{1}{\tilde{\ell}_B^2} \right) \bigg|_{d_B=d_{\max,B}} \quad (29)$$

$$\stackrel{(c)}{\geq} \left( \frac{1}{\omega_1^2} + \frac{1}{\omega_2^2} \right) \left( \frac{1}{\ell_B^2} + \frac{1}{\tilde{\ell}_B^2} \right) \bigg|_{d_B=d_{\max,B}} \quad (30)$$

$$\stackrel{(d)}{\geq} \left( \frac{1}{\omega_1^2} + \frac{1}{\omega_2^2} \right) \left( \frac{1}{\ell_B^2} + \frac{1}{\tilde{\ell}_B^2} \right) - \frac{2}{\ell_B \tilde{\ell}_B} \left( \frac{1}{\omega_1^2} - \frac{1}{\omega_2^2} \right) \bigg|_{d_B=d_{\max,B}} \quad (31)$$

where (a) follows from the binomial expansion, and (c) and (d) follow from the fact that  $0 < \omega_1 \leq \omega_2$ . The left-hand side in the first line (28) corresponds to  $\overline{R}_E$  and the last line (31) corresponds to  $\underline{P}_s(d_{\max,B}, \frac{c\pi}{\tilde{\ell}_B - \ell_B} \big|_{d_B=d_{\max,B}})$  from (27). Thus, if inequality (b) holds, we have that  $\underline{C}_S^* = 0$ , i.e., condition (24) is a sufficient condition for  $\underline{C}_S^* = 0$ . From basic logical arguments, it follows that condition (21) from Corollary 1 is a necessary condition for  $\underline{C}_S^* > 0$ .

### APPENDIX B PROOF OF COROLLARY 2

First, it should be noted that the right-hand side of (22) is the receive power corresponding to  $\overline{R}_E$  from (11). Next, the left-hand side of (22) is the receive power of Bob at maximum distance  $d_B = d_{\max,B}$ , when the frequency spacing is set to  $\Delta\omega = \Delta\omega_\pi(d_{\min,B})$ . From [19, Thm. 2], it follows that

$$\max_{\Delta\omega} \min_{d_B \in [d_{\min,B}, d_{\max,B}]} \underline{P}_s(d_B, \Delta\omega) > \underline{P}_s(d_{\max,B}, \Delta\omega_\pi(d_{\min,B}))$$

Therefore, if condition (22) holds, it implies that

$$\max_{\Delta\omega} \min_{d_B \in [d_{\min,B}, d_{\max,B}]} \underline{P}_s(d_B, \Delta\omega) > \overline{R}_E,$$

which in turn implies that the solution to (14) is positive, i.e.,  $\underline{C}_S^* > 0$ .



# REFERENCES

- [1] G. Gui, M. Liu, F. Tang, N. Kato, and F. Adachi, "6G: Opening new horizons for integration of comfort, security, and intelligence," *IEEE Wireless Communications*, vol. 27, no. 5, pp. 126–132, Oct. 2020. DOI: [10.1109/MWC.001.1900516](https://doi.org/10.1109/MWC.001.1900516).
- [2] S. Dang, O. Amin, B. Shihada, and M.-S. Alouini, "What should 6G be?" *Nature Electronics*, vol. 3, no. 1, pp. 20–29, Jan. 2020. DOI: [10.1038/s41928-019-0355-6](https://doi.org/10.1038/s41928-019-0355-6).
- [3] W. Saad, M. Bennis, and M. Chen, "A vision of 6G wireless systems: Applications, trends, technologies, and open research problems," *IEEE Network*, vol. 34, no. 3, pp. 134–142, May 2020. DOI: [10.1109/MNET.001.1900287](https://doi.org/10.1109/MNET.001.1900287). arXiv: [1902.10265](https://arxiv.org/abs/1902.10265) [cs.IT].
- [4] J. Park, S. Samarakoon, H. Shiri, *et al.*, "Extreme ultra-reliable and low-latency communication," *Nature Electronics*, vol. 5, no. 3, pp. 133–141, Mar. 2022. DOI: [10.1038/s41928-022-00728-8](https://doi.org/10.1038/s41928-022-00728-8). arXiv: [2001.09683](https://arxiv.org/abs/2001.09683) [cs.IT].
- [5] M. Bennis, M. Debbah, and H. V. Poor, "Ultrareliable and low-latency wireless communication: Tail, risk, and scale," *Proceedings of the IEEE*, vol. 106, no. 10, pp. 1834–1853, Oct. 2018. DOI: [10.1109/JPROC.2018.2867029](https://doi.org/10.1109/JPROC.2018.2867029). arXiv: [1801.01270](https://arxiv.org/abs/1801.01270) [cs.IT].
- [6] F. Haber and M. Noorhashm, "Negatively correlated branches in frequency diversity systems to overcome multipath fading," *IEEE Transactions on Communications*, vol. 22, no. 2, pp. 180–190, Feb. 1974. DOI: [10.1109/TCOM.1974.1092173](https://doi.org/10.1109/TCOM.1974.1092173).
- [7] K.-L. Besser and E. A. Jorswieck, "Bounds on the secrecy outage probability for dependent fading channels," *IEEE Transactions on Communications*, vol. 69, no. 1, pp. 443–456, Jan. 2021. DOI: [10.1109/TCOMM.2020.3026654](https://doi.org/10.1109/TCOMM.2020.3026654). arXiv: [2004.06644](https://arxiv.org/abs/2004.06644) [cs.IT].
- [8] R. J. Weiler, M. Peter, W. Keusgen, A. Kortke, and M. Wisotzki, "Millimeter-wave channel sounding of outdoor ground reflections," in *2015 IEEE Radio and Wireless Symposium (RWS)*, IEEE, Jan. 2015, pp. 95–97. DOI: [10.1109/RWS.2015.7129712](https://doi.org/10.1109/RWS.2015.7129712).
- [9] J. Naganawa, K. Morioka, J. Honda, N. Kanada, N. Yonemoto, and Y. Sumiya, "Antenna configuration mitigating ground reflection fading on airport surface for AeroMACS," in *2017 IEEE Conference on Antenna Measurements & Applications (CAMA)*, IEEE, Dec. 2017. DOI: [10.1109/cama.2017.8273487](https://doi.org/10.1109/cama.2017.8273487).
- [10] D. W. Matolak and R. Sun, "Air-ground channel characterization for unmanned aircraft systems—part I: Methods, measurements, and models for over-water settings," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 1, pp. 26–44, Jan. 2017. DOI: [10.1109/tvt.2016.2530306](https://doi.org/10.1109/tvt.2016.2530306).
- [11] C.-C. Chiu, A.-H. Tsai, H.-P. Lin, C.-Y. Lee, and L.-C. Wang, "Channel modeling of air-to-ground signal measurement with two-ray ground-reflection model for UAV communication systems," in *2021 30th Wireless and Optical Communications Conference (WOCC)*, IEEE, Oct. 2021. DOI: [10.1109/wocc53213.2021.9603250](https://doi.org/10.1109/wocc53213.2021.9603250).
- [12] A. H. Farzamiyan, M. G. Gaitan, and R. Samano-Robles, "A multi-ray analysis of LOS V2V links for multiple antennas with ground reflection," in *2020 AEIT International Annual Conference (AEIT)*, IEEE, Sep. 2020. DOI: [10.23919/aeit50178.2020.9241147](https://doi.org/10.23919/aeit50178.2020.9241147).
- [13] H. Berger and J. E. Evans, "Diversity techniques for airborne communications in the presence of ground reflection multipath," Massachusetts Institute of Technology, Lincoln Laboratory, Tech. Rep. 1972-27, Sep. 8, 1972.
- [14] E. A. Jorswieck, P.-H. Lin, and K.-L. Besser, "On the zero-outage secrecy-capacity of dependent fading wiretap channels," *Entropy*, vol. 24, no. 1, 99, Jan. 2022. DOI: [10.3390/e24010099](https://doi.org/10.3390/e24010099).
- [15] K.-L. Besser, "Worst-case secrecy rate optimization for two-ray scenarios, Supplementary material." (2022), [Online]. Available: <https://github.com/klb2/two-ray-worst-case-secrecy>.
- [16] T. S. Rappaport, *Wireless Communications: Principles and Practice*, 2nd ed. Prentice Hall, 2002.
- [17] D. Tse and P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge University Press, 2005. DOI: [10.1017/CBO9780511807213](https://doi.org/10.1017/CBO9780511807213).
- [18] M. Bloch and J. Barros, *Physical-Layer Security*. Cambridge University Press, 2011. DOI: [10.1017/CBO9780511977985](https://doi.org/10.1017/CBO9780511977985).
- [19] K.-L. Besser, E. A. Jorswieck, and J. P. Coon, *A simple frequency diversity scheme for ultra-reliable communications in ground reflection scenarios*, Jun. 2022. arXiv: [2206.13459v1](https://arxiv.org/abs/2206.13459v1) [cs.IT].
- [20] K.-L. Besser, E. A. Jorswieck, and J. P. Coon, "Multi-user frequency assignment for ultra-reliable mmWave two-ray channels," in *20th International Symposium on Modeling and Optimization in Mobile, Ad hoc, and Wireless Networks (WiOpt) – RAWNET Workshop*, IEEE, Sep. 2022.