Research Article | Vol. 29, No. 19 / 13 Sep 2021 / Optics Express 30461
Optics EXPRESS

Improving security in terahertz wireless links using beam symmetry of vortex and Gaussian beams

TINKARA TROHA,[1] TOMÁŠ OSTATNICKÝ,[2] AND PETR KUŽEL[1,*]

[1] *Institute of Physics of the Czech Academy of Sciences, Na Slovance 1999/2, 182 00 Prague 8, Czech Republic*
[2] *Faculty of Mathematics and Physics, Charles University in Prague, Ke Karlovu 3, 121 16 Prague 2, Czech Republic*
[*] *kuzelp@fzu.cz*

Abstract: We present an effective way to improve the security of a point-to-point terahertz wireless link on a physical layer supported by numerical calculations in the frame of Fourier optics. The improvement is based on original countermeasures which exploit three independent degrees of freedom of the carrier wave: its intensity and azimuthal and radial symmetry. When the transmission line is intercepted, the light beam is subject to changes in either of the three degrees of freedom. We propose a strategy to measure these changes and they are quantified by a single eavesdropping parameter that is shown to be correlated to the secrecy capacity of the transmission. Consequently, its excessive value serves as an indication of the beam interception. We consider the carrier wave in the form of Gaussian and vortex beams. Comparison between the two reveals that vortex beam ensures a even higher level of security.

1. Introduction

Wireless communication technology has become an indispensable part of today's society. One of its main concerns is to provide secure transmission of information which means to prevent its revelation to any unauthorized person. Security of communication is ensured on many levels by security protocols [1–3] some of which provide the integrity of the information content itself (encryption) and some are related to the transport mechanism. In this study we are concerned about the latter: avoiding an information leakage from the volume between the transmitter and the receiver. The increasing data traffic directed the development of wireless communications towards higher carrier frequencies, i.e., to terahertz (THz) spectral range [4–10], where higher data rates are achievable. In particular, the THz spectral region seems to be more suitable for achieving wireless Terabit-per-second transfer rates than microwaves (<100 GHz) and far/mid-infrared waves (> 10 THz) [10]. Compared to radio frequencies and microwaves, THz-frequency radiation can be collimated to a highly directional beam whose energy can be almost completely enclosed (radius of tens of centimeters) between transmitting and receiving antennae; therefore, in the case of eavesdropping attack, an eavesdropper has to intercept the beam somewhere in the line. This limits the available positions of interception device; therefore, it was generally believed that higher transmission frequencies would lead to a higher level of security [6,10–12].

Recent discoveries of new approaches to the THz generation, detection and wave manipulation can be applied to improve the existing schemes of signal transfer and processing. For example, a significant advancement in the generation and detection of the vortex beams in the THz spectral range has been achieved [13–16], allowing phase and shape modulation of the radiation that can be used to improve the security.

One of the first investigations showing that, despite the high directionality of THz wireless links, the security on the physical (i.e., propagation) layer is not guaranteed, was done by the

#433606 https://doi.org/10.1364/OE.433606
Journal © 2021 Received 7 Jun 2021; revised 26 Aug 2021; accepted 27 Aug 2021; published 7 Sep 2021

Optics EXPRESS

group of D. Mittleman [17]. In their scenario an eavesdropper puts an object inside the beam path achieving that the portion of light is scattered in another direction where the eavesdropper's detection system is located. They proposed a strategy based on the measurement of the beam intensity to detect a possible interception: it has been shown experimentally, however, that the attacker can overreach this strategy even in the frequency range of 100-400 GHz.

In this paper we theoretically study scattering geometries of line-of-sight wireless link similar to those discussed in Ref. 17 in order to find out new schemes to increase the security. As a theoretical work, this paper does not have ambition to present complete technical solutions of the wireless security; it proposes principles and concepts how to exploit properties of THz beams to improve the security countermeasures on the physical layer. We take the advantage of the high symmetry of collimated electromagnetic beams, where the presence of an interception object can be found from a symmetry breaking of the received signal. We propose advanced approaches to significantly improve the chances to detect the attempts of THz beam eavesdropping consisting of countermeasures of the transmitted light power at specifically chosen points within the lateral profile of the beam and by using vortex beams instead of common Gaussian beams. Indeed, the phase vorticity and the donut-like profile of the vortex beam intensity help in identifying the eavesdropper's attack since they lead to a higher distortion of the beam which is a subject of scattering compared to a Gaussian beam. We discuss also how the symmetry-protected zero intensity in the center of the vortex beam can help in rising warnings against eavesdropping. The proposed additional measurements can be used, e.g., to ensure no signal interception during the transmission of the encryption key; the safely encrypted data then can be securely sent at high speed without additional countermeasures.

2. Security of wireless links

In this work we take advantage of some quasi-optical properties of THz beams which are routinely used in the THz laboratories. Indeed, compared to radiofrequencies, THz radiation can be easily transformed in space using far-infrared optics and it can propagate as a collimated beam over large distances. We consider a line-of-sight wireless link between transmitter (Alice) and receiver (Bob) as shown in Fig. 1 for communications over distances between tens to hundreds of meters. Both Alice and Bob wish to communicate securely, i.e., the transmitted data cannot be decrypted by a third party (Eve in Fig. 1). Following Ref. 17, we aim here at increasing the transmission security by preventing Eve's interception directly on the physical layer of communication.

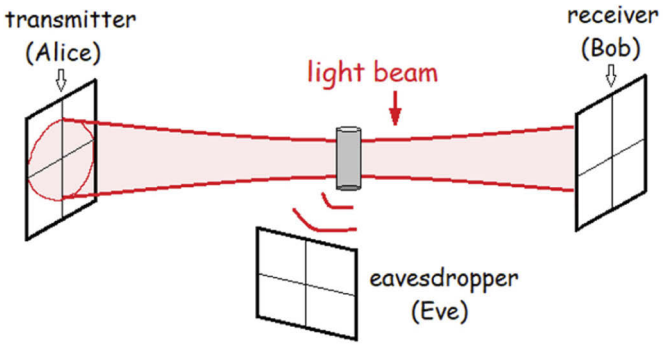

Fig. 1. Sketch of eavesdropping geometry. Alice sends the signal in a direct line towards Bob. Eve inserts a metallic object into the beam path and locates her detector somewhere outside the beam path.

The communication between Alice and Bob is never 100% secret provided that Eve is able to collect radiation scattered by random obstacles or by an artificial object intentionally placed

Optics EXPRESS

into the beam path. The presence of noise (background radiation, detector noise, atmospheric conditions) naturally causes errors in a decoded data stream: the larger signal-to-noise ratio (SNR = transmitted power over the noise level), the lower bit error rate (BER) [17]. Alice usually supports a bit error correction protocol which enables Bob (and potentially Eve) to identify and correct the data. The objective is then to ensure that Eve's BER is much higher than Bob's BER such that she is not able to gain the full transmitted information.

In principle the wireless link can be always intercepted. The only possibility to avoid the information leakage on the physical layer is therefore to stop the transmission as soon as an attack is registered. For this purpose, Bob analyzes properties of the received signal and tries to identify the presence of Eve and, more importantly, he stops the communication at the moment when Eve potentially achieves the BER low enough for a successful attack.

We will define several countermeasures for Bob and we will combine them into a single parameter for the purpose of the signal analysis and to estimate the level of the link security. This parameter will be then compared to Eve's ability to eavesdrop: this ability relies on the particular BERs, which in turn depend on Bob's and Eve's SNR, and it is defined as the secrecy capacity c_s [17]:

$$c_s = 1 - \frac{\log(1 + \mathrm{SNR_{Eve}})}{\log(1 + \mathrm{SNR_{Bob}})}. \tag{1}$$

In correspondence to Ref. 17, we set that eavesdropping is possible when c_s<0.5. Bob's SNR can be assumed $\mathrm{SNR_{Bob}} = 23.3$, which corresponds to the bit error rate of 10^{-9} [17]. However, the value of c_s depends also on the intensity of Eve's signal and on the noise level of her detection system. The latter quantity is determined by the quality of her detector; here we assume that Eve can achieve two times lower noise level compared to Bob. The threshold condition $c_s = 0.5$ is rather demanding for the signal decoding by Eve since it corresponds to $\mathrm{SNR_{Eve}} = 4$ (or $\mathrm{BER} = 4 \times 10^{-3}$). Conventionally a BER worse than 10^{-3} will not allow for forward error correction.

The most straightforward control for eavesdropping is the measurement of the optical power on Bob's detector. Its value may fluctuate due to several reasons; in this study the changes in optical power are a consequence of the interception of the beam by an object. We describe this with the blockage b, defined in [17] as

$$b = 1 - \frac{\mathrm{SNR_{Bob}^{object}}}{\mathrm{SNR_{Bob}^{no\ object}}} \tag{2}$$

This parameter could be a sufficient countermeasure if Bob collects most of the power transmitted by Alice: any decrease in the signal then reveals a possible interception and Bob might assume that Eve is able to gain the missing part of the power. We consider here that Bob's antenna is not large enough to cover the whole beam profile, so that the attack is possible even if the blockage measured by Bob is close to zero as demonstrated in Ref. 17. We therefore need to propose additional countermeasures to ensure higher level of security.

3. Additional countermeasures and vortex beam wireless link

Optical radiation allows transmission of energy within peer-to-peer connections by the use of spatially narrow collimated beams. So far, the most common is the Gaussian optical beam [18]; a laterally confined light wave with a Gaussian distribution of intensity in the cross-section plane, as illustrated in Fig. 2(a). During the propagation the beam radius w is changing (beam convergence/divergence) whereas its cross section retains the same shape. The narrowest point of the beam is called the beam waist (w_0).

In this paper we propose another type of the beam to be used for the transmission of information, that is Laguerre-Gaussian light beam [19] (also called vortex beam). Vortex beams exhibit

Optics EXPRESS

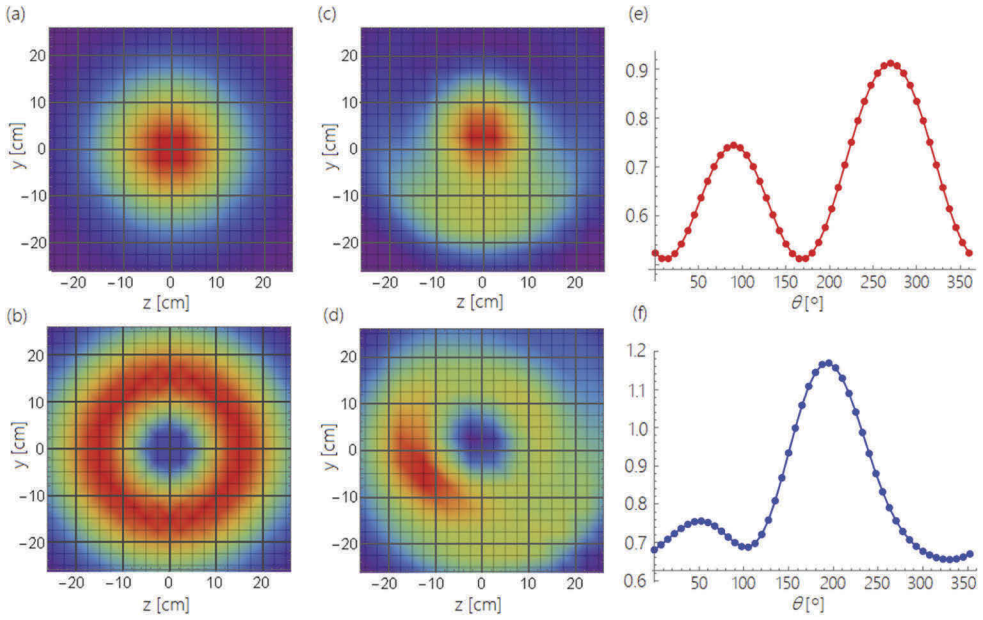

Fig. 2. Light intensity profile at Bob's detector for freely propagating (a) Gaussian and (b) vortex beam. The vacuum wavelength of radiation is $\lambda = 1$ mm, the beam waist radius is $w_0 = 20$ cm and Bob's detector is at $d = 50$ m away from the waist. (c) Changes in the Gaussian beam profile and (d) vortex beam profile when intercepted with a circular mirror positioned off-axis. In this example, the mirror with radius $a = 8$ cm is placed inside the beam in the waist position at an angle of 45° with respect to the beam propagation direction (x-axis). The mirror is displaced from the beam center in y-direction by 7.5 cm; (e) The intensity profile as a function of the azimuthal angle θ, defined as $\tan\theta = y/z$ with the fixed radial component $R = \sqrt{y^2 + z^2}$. For Gaussian beam, $R_G = 12.6$ cm, and (f) for vortex beam, $R_V = 15.2$ cm.

some different properties compared to Gaussian beams. They have a donut like distribution of intensity in the cross-section with the zero intensity in the beam center, see Fig. 2(b). Compared to Gaussian beams the vortex beams with similar parameters reveal spatially wider intensity distribution in the cross section and they are more divergent. See also Supplement 1.

We consider, similarly as in previous experimental work [17] and following Fig. 1, the scattering on an intercepting object represented by a metallic cylinder or a circular mirror, both causing not only a drop of the total optical power but also a change of the light intensity profile at Bob's detector. These changes are illustrated for the Gaussian (Fig. 2(c)) and vortex (Fig. 2(d)) beams for the case of a mirror located off the beam axis. The idea is to measure these distortions and use them to define Bob's countermeasures which serve as a warning against eavesdropping.

To analyze the changes of the beam properties on Bob's detector, we propose several countermeasures. For this purpose, we identify independent degrees of freedom of the beam on Bob's detector: 1. total power, 2. angular intensity distribution, 3. radial intensity distribution, and 4. polarization. Changes in the polarization are of a minor importance and therefore we concentrate on the remaining three points. We define a separate countermeasure for each of the degrees of freedom based merely on measurements that Bob can carry out on his own, defining a three-dimensional space in which we classify the integrity of the detected beam. Finally, we define a boundary beyond which the beam reveals inacceptable changes, and the transmission is not considered as secure.

Optics EXPRESS

In order to be able to characterize the angular and radial intensity distributions, we propose the following detection geometry. We assume Bob sets up his detection system to be able to measure signal-to-noise ratio $\mathrm{SNR_k}$ at some distinct control points within the beam profile. These points may be chosen in various ways; however, based on our analysis, we propose to use one point in the beam center, referred as "0" in the following, and 6 equidistant points ($k = 1..6$) lying on a circle with radius R as shown in Fig. 3. Due to the different intensity profiles of the two beams, we choose the radius R_G for the Gaussian beam at the half width at half maximum (HWHM) of the light intensity profile, and R_v for the vortex beam at the maximum of the donut-like intensity profile. We also assume that Bob performs a reference measurement with well aligned setup, in good atmospheric conditions and without eavesdropping, denoted $\mathrm{SNR_{ref}}$ for the points on a circle and $\mathrm{SNR_{ref,0}}$ for the central point (Fig. 3).

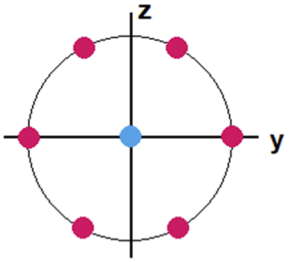

Fig. 3. Bob's detection configuration; light intensity is measured at six equidistant positions lying on a circle around a beam center (denoted by red circles) and in the beam center (blue circle). The distance from the center of the detector to each point is R; for Gaussian beam $R_\mathrm{G} = 12.6$ cm, and for vortex beam it is $R_\mathrm{V} = 15.2$ cm.

1. *Transmitted power*. The countermeasure related to this degree of freedom is the blockage. Since Bob's distance to Alice can be arbitrary, he has rarely the possibility to detect the power of the whole beam due to its divergence; however, in our scheme he may check its intensity at the control points. The blockage b following the definition (2) would be equal to an average value of the blockages measured by control detectors:

$$b = 1 - \frac{\mathrm{ave(SNR_k)}}{\mathrm{SNR_{ref}}}. \tag{3}$$

2. *Angular intensity distribution*. Beam symmetry breaking by an intercepting object can naturally lead to the intensity redistribution on a circle at a constant distance from the beam center. This redistribution turns into nonzero differences between measured SNR_k in the control points $k = 1..6$. Hence, we define a second test parameter η as

$$\eta = 1 - \frac{\min(\mathrm{SNR}_k)}{\max(\mathrm{SNR}_k)}, \tag{4}$$

where $\max(\mathrm{SNR}_k)$ and $\min(\mathrm{SNR}_k)$ are the maximum and minimum values among signal-to-noise ratios at the control positions. When $\max(\mathrm{SNR}_k) = \min(\mathrm{SNR}_k)$, one finds $\eta = 0$ (the symmetry is not broken), whereas the non-zero value of η is a fingerprint of the beam interception. The value of η is independent of typical changes in atmospheric conditions like fog or rain, which mainly result in the change of the total intensity but do not distort significantly the shape of the beam. While the positions of the control points following Fig. 3 are selected by Bob, the orientation of the intercepting object in the yz plane is chosen by Eve independently: it means that the respective orientation may be favorable for Bob (i.e., lower value of $\min(\mathrm{SNR}_k)$) or unfavorable for him (higher value of $\min(\mathrm{SNR}_k)$). This can be controlled neither by Bob nor by Eve. Therefore, we

Optics EXPRESS

will analyze here the value $\eta_{\min}$ calculated as the minimum value over all the orientations of the object, i.e., we consider the least favorable orientation for Bob's countermeasure.

3. Radial intensity distribution. Another way of the beam distortion by an intercepting object is the change in the radial coordinate. Bob can select only a limited number of control points, so for the Gaussian beam we propose the last countermeasure based only on a two-point measurement of the SNR on the beam axis and at one fixed radius:

$$\eta_{0,\mathrm{Gauss}} = \left| 1 - \frac{2\mathrm{ave}(\mathrm{SNR}_k)}{\mathrm{SNR}_0} \right| , \tag{5}$$

and $\eta_{0,\mathrm{Gauss}} = 1$ for $\mathrm{SNR}_0 < \mathrm{ave}(\mathrm{SNR}_k)$. In the case there is no deformation, $\mathrm{ave}(\mathrm{SNR}_k)/\mathrm{SNR}_0 = 1/2$ due to the selected radius at which the control points are placed and then $\eta_{0,\mathrm{Gauss}} = 0$.

For the vortex beam, however, the above definition makes no sense due to the symmetry-protected zero intensity in the beam center which is not influenced by spatially homogeneous environmental conditions. Therefore, an increase of the signal in the beam center may serve as an indication of the attack and can complement the symmetry-related parameter η and thus strenghen the role of the beam symmetry in the countermeasures. We thus introduce a third test parameter η_0 for the vortex beam as

$$\eta_{0,\mathrm{vortex}} = \frac{\mathrm{SNR}_0}{\mathrm{SNR}_0 + 4} , \tag{6}$$

Equation (6) was chosen to fulfil the following requirements: it is a monotonous function with values between 0 and 1 and the threshold value of 0.5 is reached for $\mathrm{SNR}_0 = 4$; this is in analogy with the threshold value of the secrecy capacity that allows eavesdropping, $c_s = 0.5$, which is achieved for $\mathrm{SNR}_{\mathrm{Eve}} = 4$, see Eq. (1).

The countermeasures expressed by means of b, η, and η_0 provide information about the changes in the transmitted intensity and beam spatial profile. All three parameters may acquire values between 0 and 1 and their values of 0.5 are set here as individual eavesdropping thresholds. The transmission process can be even more conveniently characterized by a single countermeasure parameter $p(b, \eta, \eta_0)$, entirely determined by Bob's measurements. Its increasing value can be assigned to an increasing probability of eavesdropping; if it reaches a defined threshold value a trigger for stopping the information flow between Alice and Bob can be raised. Many particular forms of p can be considered, and final implementation will depend on the particular experimental realization of the transmission setup, e.g., $p = p[(\alpha b)^n + (\beta\eta)^n + (\gamma\eta_0)^n]$, where α, β, γ define the weights of individual countermeasure parameters and n defines the metrics. In the ideal case p would perfectly reflect the secrecy capacity, i.e., $p = 1 - c_s$. For the purpose of our paper, we consider equal weights of the parameters; we introduce $\rho_{(n)} = \sqrt[n]{b^n + \eta^n + \eta_0^n}$ as a factor mapping the individual eavesdropping parameters into a single value according to the chosen metrics n and we define

$$p_{(n)} = \rho_{(n)} \sqrt[n]{\frac{3(2^n - 1) + 2}{3(2^n - 1) + 2^{n+1}\rho_{(n)}^n}} . \tag{7}$$

Here the n^{th} root expression is used just for normalization: the values of $p_{(n)}$ are confined between 0 and 1 and the eavesdropping threshold value is set to 0.5, i.e., $\rho_{(n)} = 0.5$ yields $p_{(n)} = 0.5$. In other words, if any individual countermeasure parameter (b, η or η_0) reaches the value of 0.5, the eavesdropping alarm will switch on (since $p \geq 0.5$); a parameter with a value significantly lower than 0.5 loses its importance more or less rapidly (depending on the metrics n). In this work we choose a particular value of $n = 4$ to carry out our calculations. In realistic implementation the appropriate value of n may be chosen depending on the practical experience with a particular wireless connection. Note that Bob's experimental errors related to disturbances in the transmission (due to, e.g., atmospheric conditions causing beam attenuation, fluctuations

Optics EXPRESS

in the beam properties or beam-pointing jitter) will appear as small additional contributions to individual eavesdropping parameters. The formula (7) is set up to be rather insensitive to changes in the values of parameters which are otherwise small (i.e., non-affected by the eavesdropping). Moreover, the choice of the threshold value of $p = 0.5$ means that there is enough space for natural beam distorsion which will not be in turn interpreted as Eve's attack and the method therefore should be applicable to realistic atmospheric conditions.

4. Results

In our model of a line-of-sight wireless link we calculate the spatial electromagnetic field distribution at Bob's and Eve's detector by means of Fourier optics (see Supplement 1 where details of the calculations are described). The numerical calculations are performed for selected values of the distance and beam diameter; however, they can be easily appropriately rescaled, providing a more general character to the results. Here we assume the distance between Bob and Alice is $2d = 100$ m (see Fig. 4 (a)). The light beam with frequency 300 GHz (vacuum wavelength $\lambda = 1$ mm) is polarized in the z-direction. The beam waist lies in the center of the line between Alice and Bob and the waist radius is relatively large: $w_0 = 20$ cm in order to achieve low beam divergence. The detection system of Bob consists of seven equal square detectors with the size of 5×5 cm^2. Eve inserts a circular mirror into the beam waist to deflect a part of its power in a direction perpendicular to the beam axis (Fig. 4 (b)) towards her detector with the size of 50×50 cm^2. Note that the Raileigh parameter of the beam $z_R = \pi w_0^2/\lambda$ exceeds the distance between Bob and Alice; therefore, the essential results remain valid if the object inserted by Eve is somewhat shifted along the beam. All the results also remain valid if the wavelength (frequency) is changed and all the dimensions are appropriately scaled.

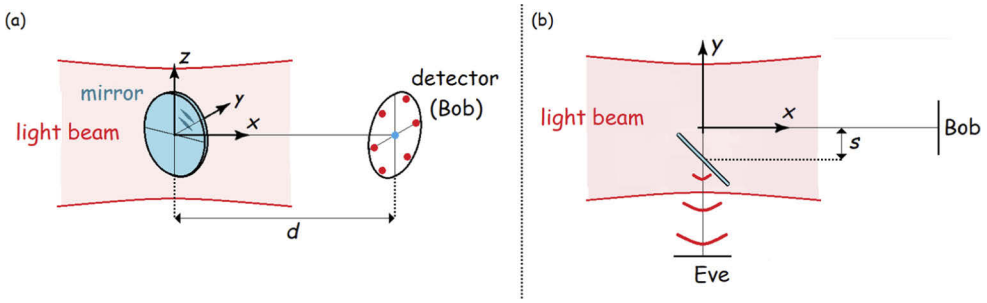

Fig. 4. Definition of the geometry and of the coordinate system. (a) The light propagates in the x-direction and it is polarized in the z-direction. Bob's detector lies in the yz-plane. Eve puts a circular mirror into the beam waist. (b) View from above: The center of the mirror is displaced from the beam axis in the y-direction by a variable distance s and it is oriented at 45° with respect to the beam propagation direction.

We calculate Bob's particular countermeasures and use them to evaluate the overall countermeasure parameter p. Based on the calculated power detected by Eve, we also evaluate the secrecy capacity and compare it to p in order to check our ability to reveal a possible attack. The resulting comparison of Bob's countermeasure parameter p with the secrecy capacity c_s is shown in graphs in Fig. 5 for the mirror radii between 6 cm and 13 cm. Additional situation is considered in Fig. 5(f) where we show the secrecy capacity and the parameter p versus the displacement of a scattering object represented by a metallic rod with the radius $a = 5$ cm. In this case, Eve's detector covers a larger solid angle as compared to the beam deflected by a mirror since the metallic rod scatters the radiation to various directions in contrast to mirrors. We considered in our calculations that the signal is collected from an azimuthal angle of 1 rad.

Optics EXPRESS

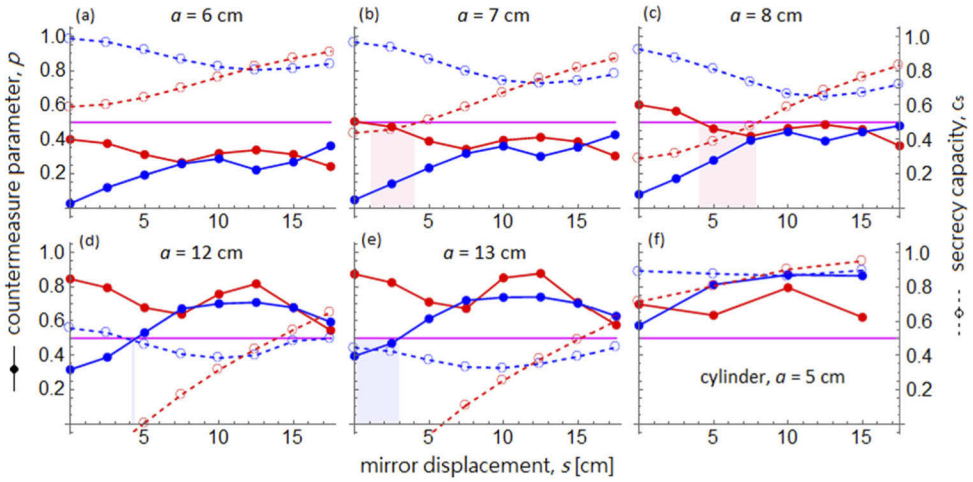

Fig. 5. Eavesdropping parameter p (filled circles) and secrecy capacity c_s (empty circles) as a function of the displacement s of the mirror from the beam axis. Mirror radius is (a) $a = 6$ cm, (b) $a = 7$ cm, (c) $a = 8$ cm, (d) $a = 12$ cm, and (e) $a = 13$ cm. Red color corresponds to the Gaussian beam and blue to the vortex beam. The intervals where Eve can successfully eavesdrop, i.e., she is not revealed by Bob's countermeasures with the selected threshold (c_s<0.5 and p<0.5), are labeled light red (for the Gaussian beam) or light blue (for the vortex beam). (f) A metallic cylinder with radius a = 5 cm is considered as an intercepting object.

To define the secrecy of Alice's transmission to Bob, we set the threshold for the secrecy capacity c_s to 0.5 in accordance with Ref. 17. The transmission is secure whenever c_s>0.5 and insecure for c_s<0.5. Bob's countermeasure parameter p is then an estimate of the transmission security and Bob can set his own threshold above which the transmission is stopped: for the sake of simplicity, we set the threshold value $p = 0.5$. Successful eavesdropping (i.e., disregarded by Bob) then occurs when both c_s and p<0.5.

For the Gaussian beam, it follows from Fig. 5(a) that the mirror radius of 6 cm does not provide enough signal for Eve to have even a possibility to eavesdrop. Expectedly, the secrecy capacity is the smallest when the mirror is placed on the beam axis and increases with increasing mirror displacement: this observation defines a general rule that c_s reaches its minimum at the point when Eve blocks the maximum of the transmitted signal. We see that the countermeasure parameter p is below the threshold, $p < 0.5$, in the entire range of displacements which means that it reflects a realistic situation, Eve's inability to eavesdrop. When a larger mirror is used (radius $a = 7$ cm, Fig. 5(b)), c_s drops below the threshold and a range of mirror displacements appears (1 cm < s < 4 cm), where successful eavesdropping is possible (labeled light red in Fig. 5(b)). Upon further increase of the mirror size, the interval which allows successful eavesdropping shifts to larger displacements ($a = 8$ cm, Fig. 5(c)) and eventually disappears (Fig. 5(d-e)).

Eavesdropping on a vortex beam (with the same waist size as the Gaussian beam considered above) requires larger objects since the power distribution in the vortex beam is more delocalized. From Fig. 5 we read that the transmission is unsecure (c_s<0.5) only when the mirror radius is at least 12 cm (Fig. 5(d,e)). For $a = 12$ cm, Fig. 5(d), the values of the parameter p allow Bob to recognize the attack with the chosen countermeasure threshold of 0.5. On the other hand, upon further increase of the mirror size ($a = 13$ cm, Fig. 5(e)), a range of mirror displacements appears (0 cm < s < 3 cm, labeled light blue) where successful eavesdropping is possible.

Optics EXPRESS

5. Discussion

Analyzing the results in Fig. 5, we may conclude that the countermeasure parameter p behaves as we required: p may be used to estimate the secrecy capacity $c_s \approx 1 - p$, and, consequently, the secrecy of communication can be estimated based on Bob's measurements. At small mirror displacements a large contribution to the countermeasure parameter p comes from the blockage (see Fig. 6 and Supplement 1) as Eve's ability to gain information from the wireless link is proportional to the power redirected to her detector. It is probable, however, that Bob cannot cover the whole transmitted beam by his detector and therefore he should not rely only upon the blockage analysis as already shown in Ref. 17.

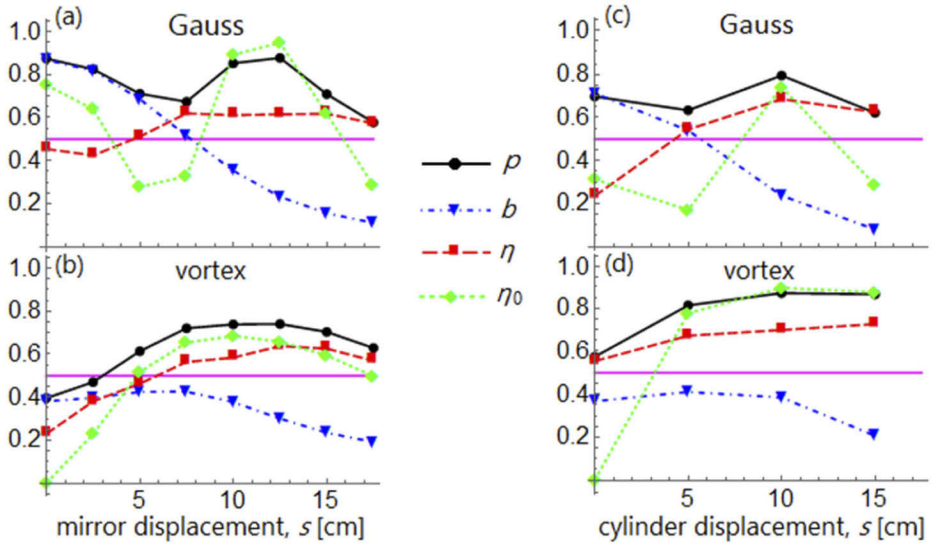

Fig. 6. Behavior of individual countermeasure parameters that contribute to the overall eavesdropping parameter p (black circles) as a function of the interception object displacement s. Blue triangles: blockage b; red squares: angular symmetry breaking parameter η; green diamonds: radial symmetry breaking parameter η_0. Interceptions objects: circular mirror with the radius $a = 13$ cm in a Gaussian beam (a) and vortex beam (b); metallic cylinder with radius $a = 5$ cm, in a Gaussian beam (c) and vortex beam (d).

It is natural that Eve will try to put a scattering object or a mirror in such position to be able to reach good enough SNR and, at the same time, not to cast a direct shadow on Bob's detector. Although in this case the blockage is decreased, it is balanced by an increase of the remaining two countermeasures due to the breaking of the beam symmetry. This scenario is clearly demonstrated in Fig. 6 where we show separate values of the individual countermeasures. The complementary symmetry-breaking measures η and η_0 clearly increase the reliability of revealing Eve's attack.

From Fig. 5 we can read out that the countermeasure control parameter p is not too far from the threshold 0.5 in all the eavesdropping regions. We have chosen this value as an example and Bob can change it to a lower value to completely avoid the possibility of an attack. On the other hand, the selected value should not be too small in order to avoid frequent interruptions of the communication due to some natural fluctuations. We observe in Fig. 5 that, e.g., decreasing the threshold value to $p = 0.4$ would be sufficient to prevent Eve's attack with only a few "false alarms" for vortex beams in the case of highly off-center positioned medium sized mirror (Fig. 5(c), region of c_s>0.5 and p>0.4). Unjustified interruptions in the case of off-centered mirrors would be, however, more frequent in the case of Gaussian beams (Fig. 5(b-c)). We imposed a trial value

Optics EXPRESS

c_s = 0.5 of acceptable security capacity (Eve's SNR = 4 or BER $\approx 4 \times 10^{-3}$); depending on experimental conditions one may set as acceptable BER = 1×10^{-3} ($c_s \approx 0.4$; Eve's SNR $\approx$ 5.7), at which it would be still challenging for Eve to decode a part of the transmitted information. Then the countermeasure threshold of $p = 0.5$, would be largely sufficient for the vortex beam in any considered situation. On the other hand, in order to achieve secure communication based on Gaussian beams using the countermeasure threshold of $p = 0.5$, we infer from Fig. 5(c) the required BER = 0.4×10^{-3} ($c_s \approx 0.35$; Eve's SNR $\approx$ 7). From this point of view the use of the vortex beam instead of the Gaussian beam multiplies Eve's BER by a factor of ~2.5 in the potentially critical situations. Redefinition of the threshold values and setting the proper power n in Eq. (7) then requires a practical testing of a particular transmission setup and cannot be set from a theoretical analysis which may underestimate some of the real experimental parameters. The above discussion shows, indeed, that introduction of the additional countermeasures leads to an increased security and only minor corrections of some parameters in our general formulae are needed for practical use.

If a metallic cylinder is used to intercept the beam (Fig. 5(f)), expectedly, its dimensions should be very large for the practical use by Eve since the light scattering is poorly directional and, consequently, it is much less efficient for eavesdropping than specular reflection. Indeed, Eve's SNR in the scattering case remains much lower as already pointed out in Ref. 17. This case illustrates quite well the feature of false alarms. In Fig. 5(f) we observe that the parameter p reaches values well above 0.5; here, the broken beam symmetry due to the introduction of a large object provides the dominant contribution, cf. Figure 6(c-d). In fact, Bob cannot a priori know which signal interception method will be applied by Eve; consequently, he tunes his countermeasure system to be quite sensitive to the signal drop and beam symmetry breaking in order to handle the most efficient interception cases. As a result, the interception by scattering can hardly lead to a successful attack (c_s largely exceeds 0.5 as observed in Fig. 5(f)) but it can lead quite often to false alarms (p>0.5), i.e., hinder a communication without decreasing its security.

Comparison of the performance of the Gaussian and vortex beams leads to the conclusion that the vortex beams provide better security, namely at least twice higher threshold value of Eve's BER when we consider the transmission as secure. This is a direct consequence of the fact that the vortex beams are donut-like with low energy density in the center: any attack using a small mirror then requires interception of a portion of the high-intensity part of the beam and, in turn, its large symmetry breaking. On the other hand, when trying not to break the symmetry, a large mirror (comparable in size with the beam cross section and with Bob's antenna dimensions) is necessary as seen in Fig. 5(e). In this case other security checks may be implemented (e.g., visual inspection of the beam trajectory).

Bob's detection points were chosen at characteristic natural distance from the beam center (HWHM or maximum intensity for Gaussian and vortex beam, respectively). This distance can be varied in a real experiment either because of a change of the beam diameter due to some external conditions or as a result of the displacement of Bob's detection system along the beam path. We calculated that for small changes of this radial distance (up to 25% with respect to the original distance) the results remain practically the same (an example of such calculation is shown in Supplement 1). The detection geometry is thus quite robust from this point of view.

We also studied the possible influence of the beam pointing of the transmitted beam. In our simulations we shifted the Bob's detection system in the z- or y-direction by units of per cent of the beam diameter. The changes in the eavesdropping parameter are quite minor in this case and confirm our explanation of the properties of the function p defined by Eq. (7). The data relative to these calculations are provided in Supplement 1.

In our theoretical analysis, we considered that Bob performs his measurements at several distinct points across the beam while real applications will allow only measurements over an area

Optics EXPRESS

of a finite size. This is not, however, a disadvantage: our analysis suggests the principle based on the detection of the modified beam parameters related to independent degrees of freedom; this will be still possible with a receiver divided into several equally sized segments. The spatial resolution of the measurements may be decreased in such a case but there is still a room for modifications of free parameters (p, c_s or Bob's SNR) to acquire high level of security.

6. Conclusion

We analyze on the physical layer the possibility of ensuring secure point-to-point transmission of information between Alice and Bob using a terahertz wireless link over the distance of several hundred meters. We consider a highly directional beam which is the subject of eavesdropping. We define Bob's strategy to characterize modifications of the transmitted beam due to Eve's intrusion, which is based on a seven-point measurement of the local radiation density. Three countermeasures are then evaluated from the measured values, each of them expresses a change of the beam properties in a distinct degree of freedom. These three countermeasures are finally combined into a single parameter p whose value lies in the range between 0 and 1 and which reveals the amount of the risk of the eavesdropping attack. The proposed method allows scaling of the wireless link geometry and fine tuning of the countermeasure parameter by four independent constants thus providing a rather general working concept, which can be adapted to particular requirements by the link users and the environmental conditions.

By performing Fourier optics calculations with a Gaussian and a vortex beam, we show that the proposed strategy is viable and we demonstrate that the parameter p is suitable for estimating the level of security. It can be used as a threshold parameter for the communication interruption. Compared to the pioneering work in Ref. 17, the definition of additional measures besides the single blockage parameter, related to the beam symmetry, allows us to recognize an attack with high success rate: our analysis shows that the proposed tests of the beam symmetry play a crucial role. High reliability of the proposed strategy is demonstrated even though we consider that Eve can cover much larger detection area and has half as low noise level compared to Bob. We also propose the use of vortex beams in order to further increase security and we verify that they provide a lower risk of an attack – Eve's bit error rate is typically increased by a factor of 2.

Funding. Ministerstvo Školství, Mládeže a Tělovýchovy (SOLID21-CZ.02.1.01/0.0/0.0/16_019/0000760); Grantová Agentura České Republiky (19-28375X).

Acknowledgment. This work was supported by the Czech Science Foundation (Project No. 19-28375X) and by the Operational Programme "Research, Development and Education" financed by European Structural and Investment Funds and the Czech Ministry of Education, Youth and Sports (Project No. SOLID21-CZ.02.1.01/0.0/0.0/16_019/0000760).

Disclosures. The authors declare no conflicts of interest.

Data availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

Supplemental document. See Supplement 1 for supporting content.

References

1. Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: technical challenges, recent advances, and future trends," Proc. IEEE **104**(9), 1727–1765 (2016).
2. L. Sun and Q. Du, "Physical layer security with its application in 5G networks: a review," China Commun. **14**(12), 1–14 (2017).
3. Y. Ju, H.-M. Wang, T.-X. Zheng, Q. Yin, and M. H. Lee, "Safeguarding millimeter wave communications against randomly located eavesdroppers," IEEE Trans. Wireless Commun. **17**(4), 2675–2689 (2018).
4. T. S. Rappaport, Y. Xing, O. Kanhere, S. Ju, A. Madanayake, S. Mandal, A. Alkhateeb, and G. C. Trichopoulos, "Wireless Communications and Applications Above 100 GHz: Opportunities and Challenges for 6G and Beyond," IEEE Access **7**, 78729–78757 (2019).
5. J. Federici and L. Moeller, "Review of terahertz and subterahertz wireless communications," J. Appl. Phys. **107**(11), 111101 (2010).

Optics EXPRESS

6. R. Piesiewicz, T. Kleine-Ostmann, N. Krumbholz, D. Mittleman, M. Koch, J. Schoebel, and T. Kurner, "Short-range ultra-broadband terahertz communications: concepts and perspectives," IEEE Antennas Propag. Mag. **49**(6), 24–39 (2007).
7. K.-C. Huang and Z. Wang, "Terahertz terabit wireless communication," IEEE Microwave **12**, 108–116 (2011).
8. T. Kürner and S. Priebe, "Towards THz communications – status in research, standardization and regulation," J. Infrared Milli. Terahz Waves **35**(1), 53–62 (2014).
9. T. Kleine-Ostmann and T. Nagatsuma, "A review on terahertz communications research," J. Infrared Milli. Terahz Waves **32**(2), 143–171 (2011).
10. I. F. Akyildiz, J. M. Jornet, and C. Han, "Terahertz band: Next frontier for wireless communications," Phys. Commun. **12**, 16–32 (2014).
11. T. Rappaport, Y. Xing, G. R. MacCartney Jr., A. F. Molisch, E. Mellios, and J. Zhang, "Overview of millimeter wave communications for fifth-generation (5G) wireless networks-with a focus on propagation models," IEEE Trans. Antennas Propag. **65**(12), 6213–6230 (2017).
12. J. Harvey, M. B. Steer, and T. S. Rappaport, "Exploiting high millimeter wave bands for military communications, applications, and design," IEEE Access **7**, 52350–52359 (2019).
13. R. Arikawa, S. Morimoto, and K. Tanaka, "Focusing light with orbital angular momentum by circular array antenna," Opt. Express **25**(12), 13728–13735 (2017).
14. R. Imai, N. Kanda, T. Higuchi, K. Konishi, and M. Kuwata-Gonokami, "Generation of broadband terahertz vortex beams," Opt. Lett. **39**(13), 3714–3717 (2014).
15. Q. Lin, S. Zheng, Q. Song, X. Zeng, Y. Cai, Y. Li, Z. Chen, L. Zha, X. Pan, and S. Xu, "Generation of terahertz vortex pulses without any need of manipulation in the terahertz region," Opt. Lett. **44**(4), 887–890 (2019).
16. A. A. Sirenko, P. Marsik, C. Bernhard, T. N. Stanislavchuk, V. Kiryukhin, and S.-W. Cheong, "THz vortex beam as a spectroscopic probe of magnetic excitations," Phys. Rev. Lett. **122**(23), 237401 (2019).
17. J. Ma, R. Shrestha, J. Adelberg, C.-Y. Yeh, Z. Hossain, E. Knightly, J. M. Jornet, and D. M. Mittleman, "Security and eavesdropping in terahertz wireless links," Nature **563**(7729), 89–93 (2018).
18. A. Yariv and P. Yeh, *Optical waves in crystals* (Wiley, 1984), Chap. 2.
19. L. Allen, M. W. Beijersbergen R, J. C. Spreeuw, and J. P. Woerdman, "Orbital angular momentum of light and the transformation of Laguerre-Gaussian laser modes," Phys. Rev. A **45**(11), 8185–8189 (1992).