LETTER

https://doi.org/10.1038/s41586-018-0609-x

Security and eavesdropping in terahertz wireless links

Jianjun Ma[1], Rabi Shrestha[1], Jacob Adelberg[1], Chia-Yi Yeh[2], Zahed Hossain[3], Edward Knightly[2], Josep Miquel Jornet[3] & Daniel M. Mittleman[1]*

Resiliency against eavesdropping and other security threats has become one of the key design considerations for communication systems. As wireless systems become ubiquitous, there is an increasing need for security protocols at all levels, including software (such as encryption), hardware (such as trusted platform modules) and the physical layer (such as wave-front engineering)[1–5]. With the inevitable shift to higher carrier frequencies, especially in the terahertz range (above 100 gigahertz), an important consideration is the decreased angular divergence (that is, the increased directionality) of transmitted signals, owing to the reduced effects of diffraction on waves with shorter wavelengths. In recent years, research on wireless devices[6–8] and systems[9–11] that operate at terahertz frequencies has ramped up markedly. These high-frequency, narrow-angle broadcasts present a more challenging environment for eavesdroppers compared to the wide-area broadcasts used at lower frequencies[12,13]. However, despite the widespread assumption of improved security for high-frequency wireless data links[14–16], the possibility of terahertz eavesdropping has not yet been characterized. A few recent studies have considered the issue at lower frequencies[5,12,13,17,18], but generally with the idea that the eavesdropper's antenna must be located within the broadcast sector of the transmitting antenna, leading to the conclusion that eavesdropping becomes essentially impossible when the transmitted signal has sufficiently high directionality[15]. Here we demonstrate that, contrary to this expectation, an eavesdropper can intercept signals in line-of-sight transmissions, even when they are transmitted at high frequencies with narrow beams. The eavesdropper's techniques are different from those for lower-frequency transmissions, as they involve placing an object in the path of the transmission to scatter radiation towards the eavesdropper. We also discuss one counter-measure for this eavesdropping technique, which involves characterizing the backscatter of the channel. We show that this counter-measure can be used to detect some, although not all, eavesdroppers. Our work highlights the importance of physical-layer security in terahertz wireless networks and the need for transceiver designs that incorporate new counter-measures.

Wireless networking is on the cusp of a revolution. For more than 100 years, wireless links have relied on wide-angle broadcasts, using transmit and receive antennas with gains that are relatively insensitive to the angle of emission or reception (and therefore with relatively low directivity). With the roll-out of 5G cellular mobile communications systems, this approach will soon change to an entirely new one, in which highly directional (and steerable) antennas provide links that are more like directed beams than like omnidirectional broadcasts[2,19]. This change is an unavoidable consequence of the move to higher carrier frequencies, a necessary step for increased bandwidth and higher rates of data transfer. There are numerous advantages to using more directional channels, including improved data security. Here, we focus on the new challenges faced by an eavesdropper when communication channels become directional[5,18], with a beam divergence angle much smaller than that used by existing mobile networks, which often use 120° sectors[20].

Security mechanisms are available at every layer of a network, and can be used jointly across layers for redundancy or in a subset of layers when resources are constrained. These mechanisms can take many forms, including encryption and authentication at the upper layers[2,3], as well as physical-layer techniques such as wave-front engineering, near-field antenna modulation and polarization multiplexing[4,5,21,22]. Physical-layer approaches have some advantages: they do not require a shared private key, they use little or no additional computing resources[23] and they do not rely on the assumption that the attacker has limited computational power. In the terahertz frequency range, numerous researchers have envisioned the need for physical-layer security[14–16,24]. Highly directional beams and increased atmospheric attenuation will confine unauthorized users to be on the same narrow path as the intended user if they wish to intercept the signal. As a result, it is often assumed that terahertz signals are more secure than lower-frequency signals: a more directional transmission sends energy to a smaller range of locations, so it is more difficult for an eavesdropper to place a receiver that detects the signal without blocking the intended recipient and thereby raising an alarm. The equipment needed to collect, demodulate and amplify terahertz signals is large (always larger than the aperture of the detector) and bulky, so blockage would always be a concern.

Although this argument is reasonable for conventional eavesdropping attacks, it does not consider alternative approaches that could circumvent the blockage problem and enable a successful attack. In our measurements, we consider a different approach for the eavesdropper (Eve). Rather than adopting the conventional assumption that Eve must place a large bulky receiver within the narrow beam path[5,13,17,18], we instead consider the possibility that she can place a smaller passive object in the beam that will scatter some of the transmitted radiation towards her receiver, which is located elsewhere[12]. This set-up affords Eve considerable additional flexibility, and can enable successful eavesdropping even at high frequencies with very directional beams.

We assume a line-of-sight configuration connecting a single transmitter (Alice) and a single receiver (Bob), as is standard for a highly directional millimetre-wave or terahertz wireless link through the air[25–27] (see Methods section 'Radiation patterns for directional horn antennas'). In our scale model data link (Fig. 1), we position objects at various locations in the beam between Alice and Bob, and evaluate the signal strength and bit error rate detected by Eve at various receiver locations. Eve's goal is to choose a scattering object, and its location, in such a way that the signal measured by Bob is not attenuated too much (otherwise, Bob might detect the attack) and the signal that she measures is large enough for her to intercept the communication. This corresponds to a successful eavesdropping configuration. To quantify

[1]School of Engineering, Brown University, Providence, RI, USA. [2]Department of Electrical and Computer Engineering, Rice University, Houston, TX, USA. [3]Department of Electrical Engineering, University at Buffalo, The State University of New York, Buffalo, NY, USA. *e-mail: daniel_mittleman@brown.edu

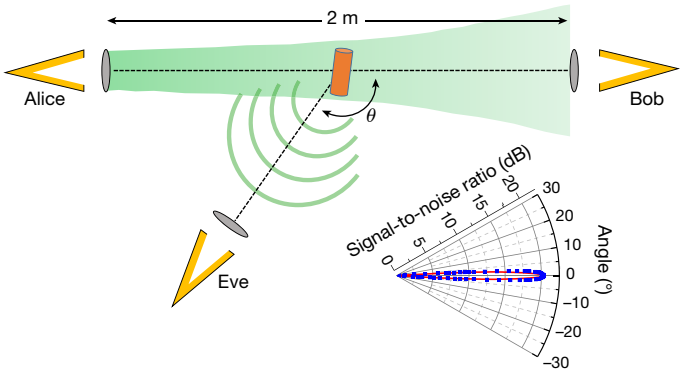

Fig. 1 | Schematic of a line-of-sight transmission channel with an eavesdropper. The schematic of the experiment shows a line-of-sight transmission channel between Alice (the transmitter) and Bob (the receiver). The inset shows the measured (blue) and computed (red) angular distribution of radiation emitted by our transmitter for the horn antenna and dielectric lens combination used in our measurements at a frequency of 200 GHz. These data indicate a high directivity of 34 dBi (decibels above isotropic) and no measurable side lobes. The results are similar for the other frequencies that we used in this work. The schematic also illustrates the eavesdropper's (Eve's) strategy: place a small (compared to the beam size) object (orange cylinder), which passively scatters radiation to a receiver located elsewhere, at an angle θ relative to the initial propagation axis of the beam. In our measurements, the receiver used by Eve is identical to that used by Bob and has identical angular sensitivity to the radiation pattern of the transmitter (Alice).

these statements, we define the attenuation of Bob's signal due to the scattering object, which we refer to as the blockage, as:

$$b = 1 - \frac{\mathrm{SNR}_{\mathrm{Bob}}^{\mathrm{object}}}{\mathrm{SNR}_{\mathrm{Bob}}^{\mathrm{no\ object}}}$$

where SNR represents the signal-to-noise ratio on a linear scale. A value of $b = 0.5$ would correspond to a situation in which Eve's scattering object is blocking half of Bob's signal. This arbitrary value may be considered a threshold beyond which Bob is certain to be aware of the change in the characteristics of his line-of-sight channel. Further, as a small modification to the conventional approach[28], we define a normalized secrecy capacity, which relates the strength of Eve's signal to Bob's signal:

$$\bar{c}_s = \frac{\log(1+\mathrm{SNR}_{\mathrm{Bob}}) - \log(1+\mathrm{SNR}_{\mathrm{Eve}})}{\log(1+\mathrm{SNR}_{\mathrm{Bob}})}$$

This quantity incorporates the particular modulation and coding methods used and characterizes the empirical limits of Bob's and Eve's reception capabilities. It is equal to unity if Eve receives no signal and to zero if Eve and Bob receive the same signal. In general, a threshold value for $\bar{c}_s$ is not easy to define, because Eve's ability to decode a signal depends on additional factors, including the modulation scheme and the absolute power level. In an information-theoretic sense, secure transmission is possible under certain circumstances even if $\bar{c}_s < 0$[29]. Thus, this quantity is not a perfect metric for defining the security of a channel. However, it is reasonable to assume that networks would be designed to strive to maximize $\bar{c}_s$, to minimize the likelihood of a successful eavesdropping attack[5]. To frame our discussion, we use an illustrative value of $\bar{c}_s = 0.5$ as an arbitrary threshold, below which we presume that eavesdropping is feasible. Both b and $\bar{c}_s$ depend on the size, shape, composition and location of the object placed in the beam path, and the carrier frequency. We find that for any frequency, Eve can always find a successful configuration that permits her to eavesdrop undetected, in the absence of any counter-measures.

To illustrate this point, we show in Fig. 2 the measured values of b and $\bar{c}_s$ for a set of scattering objects. These long cylindrical metal pipes

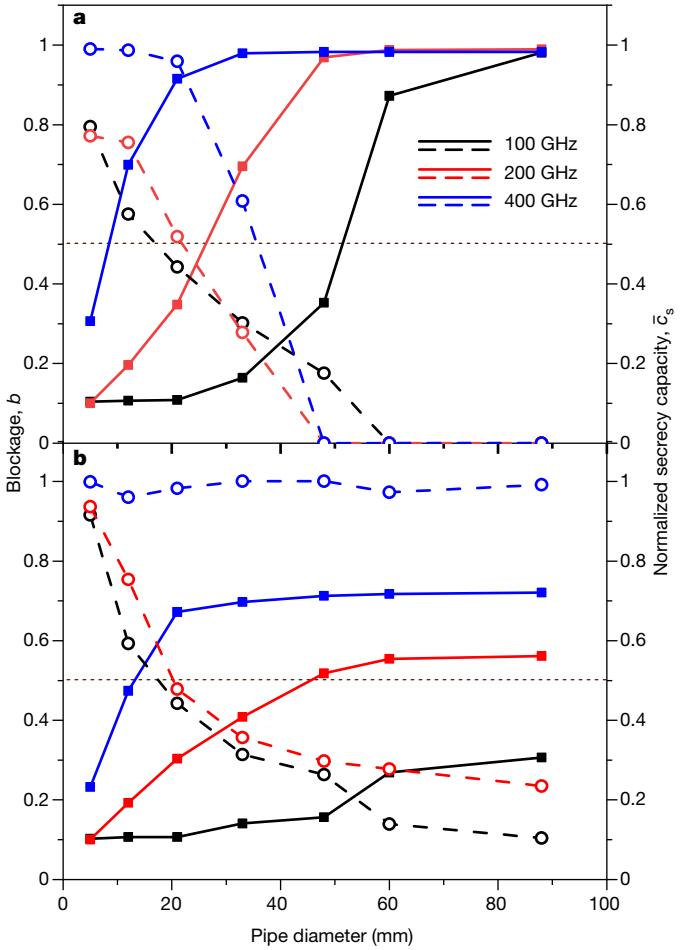

Fig. 2 | Measured blockage and secrecy capacity for eavesdropping attacks using metal cylinders. a, The blockage b (filled squares connected by solid lines; left axis) and normalized secrecy capacity $\bar{c}_s$ (open circles connected by dashed lines; right axis) as a function of the size of the metal pipe placed along the centre line of the transmission channel between Alice and Bob, for three different carrier frequencies. These values are measured with Eve located at an angle of $\theta = 160°$ (θ is defined in Fig. 1) and with the same total transmission path length as the distance from Alice to Bob (2 m). The blockage increases with the size of the object, owing to shadowing. In addition, for a given size, the blockage increases with frequency, because higher frequencies diffract less. Here, negative values of $\bar{c}_s$ are plotted as zero. **b**, The same as **a**, except with the scattering object moved off the centre line by a distance equal to the radius of the cylinder. This has the effect of decreasing the blockage substantially, making a successful eavesdropping attack easier. In **a** and **b**, the dashed horizontal lines indicate blockages or secrecy capacities of 0.5; a reasonable (but arbitrary) criterion for successful eavesdropping is that $b < 0.5$ and $\bar{c}_s < 0.5$. By this criterion, Eve succeeds in 10 of the 42 configurations that we measured.

of various diameters are inserted into the beam path along an axis parallel to the polarization direction of the beam. In Fig. 2a, the objects are situated on the line-of-sight transmission axis, so that they cast a direct shadow on the aperture of Bob's receiver[30]. Unsurprisingly, the value of b therefore increases with the size of the scattering object. We also observe a roughly opposite trend for $\bar{c}_s$: a larger scattering object directs more signal to Eve, so the secrecy capacity decreases.

For any realistic line-of-sight millimetre-wave or terahertz data link, even if the beam is highly directional, it is likely that the size of the beam when it reaches the receiver will exceed the aperture of the receiver. This is necessary to provide some margin of error for beam steering and for channel fluctuations such as atmospheric scintillation[31]. Therefore, it is possible that a scattering object could intercept a portion of the beam but not cast a shadow on the receiver. To illustrate this

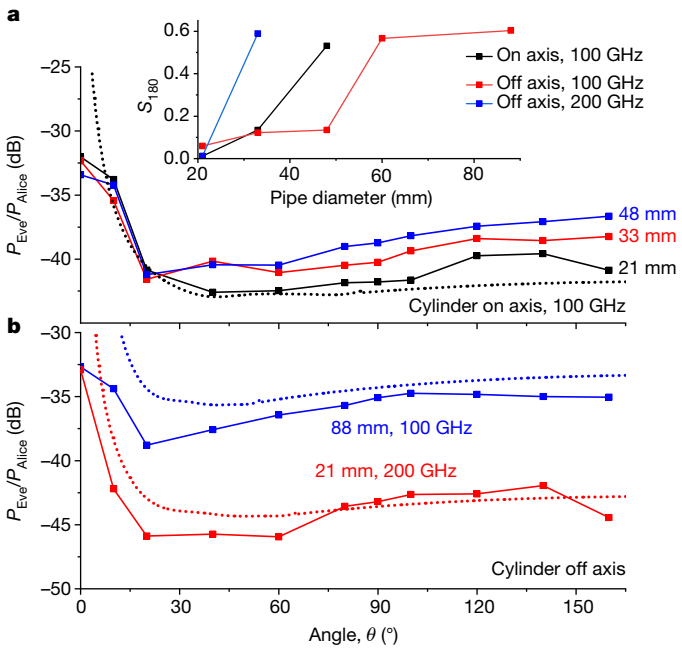

Fig. 3 | Angular distribution of power received by Eve, using metal cylinders. a, The received power ratio for Eve (the power received by Eve, P_{Eve}, normalized by the power transmitted by Alice, P_{Alice}), for different angular locations of her receiver, for all three of the configurations identified in Fig. 2a as resulting in successful eavesdropping attacks (metal cylinders located on the transmission axis; carrier frequency of 100 GHz). The labels in the main panel (21 mm, 33 mm and 48 mm) indicate the diameters of the cylinders. This result illustrates the increased power of the scattered signal with increasing cylinder diameter. The black dotted curve shows the results of ab initio numerical computations of the strength of the scattered signal for the 21-mm-diameter cylinder. **b**, Similar to **a**, showing two typical results for the seven successful-eavesdropping situations identified in Fig. 2b (in which the cylinder is moved off axis). As in **a**, the dotted curves show the corresponding computational results. The inset in **a** shows the back-scatter parameter S_{180} for all ten successful-eavesdropping configurations identified in Fig. 2. Assuming a criterion of $S_{180} > 0.5$ for the detection of potential eavesdropping, our proposed counter-measure identifies four of the ten attacks.

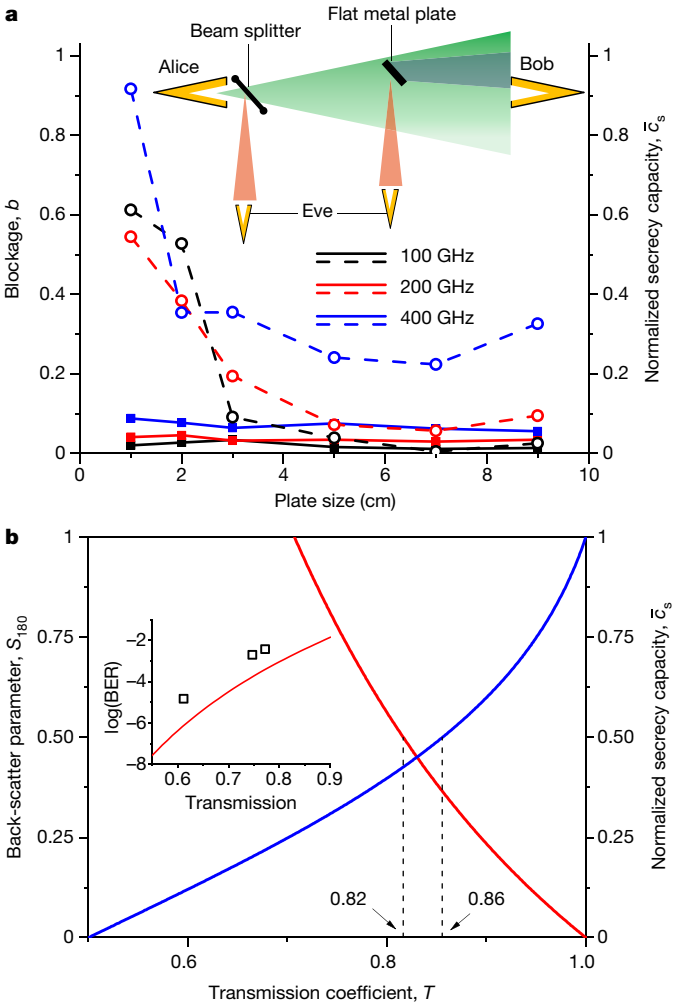

Fig. 4 | Measured blockage and secrecy capacity for eavesdropping attacks using flat objects. a, The blockage b (filled squares connected by solid lines; left axis) and normalized secrecy capacity $\bar{c}_s$ (open circles connected by dashed lines; right axis) for square planar metal reflectors of various sizes, for three different carrier frequencies. Here, the objects are placed off axis, similar to Fig. 2b. They are arranged to generate specular reflection to Eve's receiver, which is located at 90° to the axis of transmission. Unlike the case of the cylindrical objects, eavesdropping is possible ($b < 0.5$ and $\bar{c}_s < 0.5$), even at 400 GHz, for all but the smallest of the objects. The inset shows a schematic of the set-up for this form of attack, and for an attack using a beam splitter placed close to Alice (where the diameter of the beam is smallest), so as to encompass the entire transmitted beam. **b**, Values of the back-scatter parameter S_{180} (red; left axis) and $\bar{c}_s$ (blue; right axis) computed for the values of the transmission coefficient T of the beam splitter for which $b < 0.5$. There is a range of values for which S_{180} and $\bar{c}_s$ are both less than 0.5 (between the vertical dashed lines); a successful and undetected attack is possible in this range. If the back-scatter counter-measure is not used, then Eve can implement a successful attack for any value of T between 0.5 and 0.86, to obtain arbitrarily low secrecy capacity. The inset shows the measured (open squares) and calculated (solid line) bit error rate (BER) for Eve, under the assumption that Bob has a bit error rate of 10^{-9}. The experimental data were obtained using a few custom-made beam splitters (see Methods section 'The beam-splitter attack').

point, we repeat the experiments of Fig. 2a, except that we move the cylindrical objects off the centre line to minimize blockage due to direct shadowing. As a result, the values of b are reduced considerably (Fig. 2b), so that Bob may not notice the effect of the object in some cases. For the lower frequencies, the secrecy capacity is also quite low for larger objects, because they still scatter a substantial amount of power. Eve is much more readily able to implement a successful attack ($b < 0.5$ and $\bar{c}_s < 0.5$) with an off-centre object.

From Eve's point of view, cylindrical objects are advantageous because they scatter radiation over a wide range of angles. Whereas Fig. 2 depicts results for one particular location of Eve's receiver, Fig. 3 shows Eve's received power as a function of the angular location, for a few of the situations that satisfy both $b < 0.5$ and $\bar{c}_s < 0.5$. The dashed curves show a few examples of predicted values corresponding to the measured situations. These calculations use an ab initio model to compute the diffracted field from a perfectly smooth cylindrical conductor, under illumination from a point source[32] (see Methods section 'Diffracted field from a uniform metal cylinder'). As indicated by the measurements and calculations, Eve has the freedom to place her receiver in many different locations, without sacrificing signal strength.

The wide-angle scattering of a cylindrical object can also be used to develop a new type of physical-layer counter-measure[2]. A cylindrical object scatters some radiation at 180°, back towards the transmitter (Alice)[33]. It can also block radiation reflected from Bob's receiver, which would otherwise have returned to Alice. If Alice can measure these incoming signals and distinguish them from the variable back-scatter off mobile objects or the environment, then any change, either an increase or a decrease, would be a sign of a possible attack. The effectiveness of this strategy relies on the assumption that Alice has previously characterized the back-scatter of the channel before any attempted attack by Eve—a rather strong assumption. Nevertheless, when combined with other, more conventional eavesdropping counter-measures[2–5], this approach can provide an additional level

of security. We define the success of this counter-measure through a back-scatter parameter:

$$S_{180} = \left| 1 - \frac{\mathrm{SNR}_{\mathrm{Alice}}^{\mathrm{no\ object}}}{\mathrm{SNR}_{\mathrm{Alice}}^{\mathrm{object}}} \right|$$

If the object placed in the beam by Eve causes no change in the back-scattered signal, then $S_{180} = 0$ and the counter-measure has failed. But a larger value, greater than some pre-determined threshold (for example, $S_{180} > 0.5$), could be regarded as a warning of possible eavesdropping. In the inset in Fig. 3a we show measured values of S_{180} for all of the conditions for which both $b < 0.5$ and $\bar{c}_s < 0.5$ (see Methods section 'Measurement of S_{180}'). These measurements indicate that some, but not all, of Eve's attacks are detected by this counter-measure.

A second disadvantage for Eve is that, because the scattered radiation is dispersed in all directions, the power collected in a small receiver aperture is relatively low. Consequently, for example, at 400 GHz even the largest of our metal cylinders does not scatter enough radiation to permit Eve to decode the signal ($\bar{c}_s$ is nearly unity for all measurements at this frequency). An alternative for Eve is to use objects that scatter more selectively. Although this limits Eve's freedom of location considerably, it also increases her signal strength substantially. Instead of cylinders, we consider a set of square planar metal reflectors, which direct a portion of Alice's transmitted beam at 90° to the original propagation direction by specular reflection. When placed on the transmission axis, these plates block a substantial portion of Bob's signal. However, when moved off axis (Fig. 4a), the blockage drops to nearly zero, while the secrecy capacity remains low at all frequencies. Moreover, because these objects generate little back-scatter towards Alice, we find that S_{180} is small except for the largest plates, which block radiation reflected by Bob back towards Alice. For instance, for all of the measurements at 400 GHz, we find $S_{180} < 0.2$. As an extreme case, we imagine that Eve has the capacity to fabricate a lossless beam splitter, which is large enough to encompass the entire beam generated by Alice and which can be engineered to split off any desired fraction of the power in the transmitted beam. Figure 4b demonstrates that this type of attack is always effective if the transmittance of the beam splitter is chosen correctly (see Methods section 'The beam-splitter attack'). Moreover, if Alice cannot measure back-scattered signals (and is therefore unable to use the associated counter-measure), then the beam-splitter attack becomes even more devastating: Eve can readily obtain a bit error rate that is nearly as good as Bob's.

Our results demonstrate that a narrow pencil-like beam does not guarantee immunity from eavesdropping. Although this claim has often been cited as one of the advantages of using millimetre or terahertz waves, our analysis reveals that an agile eavesdropper can always succeed in implementing an undetected attack, unless counter-measures are used. Traditional counter-measures such as those that rely on beam forming[5,21,24] or on more advanced multiplexing schemes[22] may be less effective against these attacks, because the portion of the wave front that is sampled by Eve is almost coincident with that intended for Bob. On the other hand, our new counter-measure requires Alice to use a transceiver, not merely a transmitter. Thus, to incorporate security into a directional wireless link, systems will require new physical-layer components and new protocols for channel estimation. For our measurements, the transmitter-to-receiver distance is considerably less than what is often envisioned for line-of-sight terahertz links for backhaul applications. Nevertheless, our results apply equally well to communication over a longer range, by scaling the transmitter and receiver gain (see Methods section 'Radiation patterns for directional horn antennas'). Our results also demonstrate the ease with which line-of-sight communications can be diverted, which could have implications other than for eavesdropping, such as for distributing signals to multiple receivers in a network.

Online content

Any methods, additional references, Nature Research reporting summaries, source data, statements of data availability and associated accession codes are available at https://doi.org/10.1038/s41586-018-0609-x.

Received: 27 April; Accepted: 9 August 2018;
Published online 15 October 2018.

1. Shiu, Y.-S., Chang, S. Y., Wu, H.-C., Huang, S. C.-H. & Chen, H.-H. Physical layer security in wireless networks: a tutorial. *IEEE Wirel. Commun.* **18**, 66–74 (2011).
2. Yang, N. et al. Safeguarding 5G wireless communication networks using physical layer security. *IEEE Commun. Mag.* **53**, 20–27 (2015).
3. Zou, Y., Zhu, J., Wang, X. & Hanzo, L. A survey on wireless security: technical challenges, recent advances, and future trends. *Proc. IEEE* **104**, 1727–1765 (2016).
4. Sun, L. & Du, Q. Physical layer security with its application in 5G networks: a review. *China Commun.* **14**, 1–14 (2017).
5. Ju, Y., Wang, H.-M., Zheng, T.-X., Yin, Q. & Lee, M. H. Safeguarding millimeter wave communications against randomly located eavesdroppers. *IEEE Trans. Wirel. Commun.* **17**, 2675–2689 (2018).
6. Gao, W. et al. High-contrast terahertz wave modulation by gated graphene enhanced by extraordinary transmission through ring apertures. *Nano Lett.* **14**, 1242–1248 (2014).
7. Karl, N. J., McKinney, R. W., Monnai, Y., Mendis, R. & Mittleman, D. M. Frequency-division multiplexing in the terahertz range using a leaky-wave antenna. *Nat. Photon.* **9**, 717–720 (2015).
8. Reichel, K. S., Mendis, R. & Mittleman, D. M. A broadband terahertz waveguide T-junction variable power splitter. *Sci. Rep.* **6**, 28925 (2016).
9. Hermelo, M. F., Shih, P.-T. B., Steeg, M., Ng'oma, A. & Stöhr, A. Spectral efficient 64-QAM-OFDM terahertz communication link. *Opt. Express* **25**, 19360–19370 (2017).
10. Ma, J., Karl, N. J., Bretin, S., Ducournau, G. & Mittleman, D. M. Frequency-division multiplexer and demultiplexer for terahertz wireless links. *Nat. Commun.* **8**, 729 (2017).
11. Ma, J., Shrestha, R., Moeller, L. & Mittleman, D. M. Channel performance of indoor and outdoor terahertz wireless links. *APL Photon.* **3**, 051601 (2018).
12. Steinmetzer, D., Chen, J., Classen, J., Knightly, E. & Hollick, M. Eavesdropping with periscopes: experimental security analysis of highly directional millimeter waves. In *Proc. IEEE Conf. Commun. Netw. Security (CNS)* 335–343 (IEEE, 2015).
13. Zhu, Y., Wang, L., Wong, K.-K. & Heath, R. W. Secure communications in millimeter wave ad hoc networks. *IEEE Trans. Wirel. Commun.* **16**, 3205–3217 (2017).
14. Federici, J. & Moeller, L. Review of terahertz and subterahertz wireless communications. *J. Appl. Phys.* **107**, 111101 (2010).
15. Akyildiz, I. F., Jornet, J. M. & Han, C. Terahertz band: next frontier for wireless communications. *Phys. Commun.* **12**, 16–32 (2014).
16. Kürner, T. & Priebe, S. Towards THz communications – status in research, standardization and regulation. *J. Infrared Millim. THz Waves* **35**, 53–62 (2014).
17. Vuppala, S., Biswas, S. & Ratnarajah, T. An analysis on secure communications in millimeter/micro-wave hybrid networks. *IEEE Trans. Commun.* **64**, 3507–3519 (2016).
18. Kim, M., Hwang, E. & Kim, J.-N. Analysis of eavesdropping attack in mmWave-based WPANs with directional antennas. *Wirel. Netw.* **23**, 355–369 (2017).
19. Pierpoint, M. & Rebeiz, G. M. Paving the way for 5G realization and mmWave communication systems. *Mirowave J.* **59**, 106–108 (2016).
20. Xu, J. et al. Statistical analysis of path losses for sectorized wireless networks. *IEEE Trans. Commun.* **65**, 1828–1838 (2017).
21. Babakhani, A., Rutledge, D. B. & Hajimiri, A. Transmitter architectures based on near-field direct antenna modulation. *IEEE J. Solid-State Circuits* **43**, 2674–2692 (2008).
22. Djordjevic, I. B. Multidimensional OAM-based secure high-speed wireless communications. *IEEE Access* **5**, 16416–16428 (2017).
23. Rifà-Pous, H. & Herrera-Joancomarti, J. Computational and energy costs of cryptographic algorithms on handheld devices. *Future Internet* **3**, 31–48 (2011).
24. Headland, D., Monnai, Y., Abbott, D., Fumeaux, C. & Withayachumnankul, W. Tutorial: terahertz beamforming, from concept to realizations. *APL Photon.* **3**, 051101 (2018).
25. Song, H.-J. & Nagatsuma, T. Present and future of terahertz communications. *IEEE Trans. THz Sci. Technol.* **1**, 256–263 (2011).
26. Koenig, S. et al. Wireless sub-THz communication system with high data rate. *Nat. Photon.* **7**, 977–981 (2013).
27. Ducournau, G. et al. Ultrawide-bandwidth single-channel 0.4-THz wireless link combining broadband quasi-optic photomixer and coherent detection. *IEEE Trans. THz Sci. Technol.* **4**, 328–337 (2014).
28. Barros, J. & Rodrigues, M. R. D. Secrecy capacity of wireless channels. In *Proc. IEEE Symp. Inform. Theory* 356–360 (IEEE, 2006).
29. Csiszár, I. & Körner, J. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory* **24**, 339–348 (1978).
30. Petrov, V., Komarov, M., Moltchanov, D., Jornet, J. M. & Koucheryavy, Y. Interference and SINR in millimeter wave and terahertz communication systems with blocking and directional antennas. *IEEE Trans. Wirel. Commun.* **16**, 1791–1808 (2017).
31. Ma, J., Moeller, L. & Federici, J. F. Experimental comparison of terahertz and infrared signaling in controlled atmospheric turbulence. *J. Infrared Millimeter THz Waves* **36**, 130–143 (2015).

32. Kouyoumjian, R. G. & Pathak, P. H. A uniform geometrical theory of diffraction for an edge in a perfectly conducting surface. *Proc. IEEE* **62**, 1448–1461 (1974).
33. Dorney, T. D., Symes, W. W., Baraniuk, R. G. & Mittleman, D. M. Terahertz multistatic reflection imaging. *J. Opt. Soc. Am. A* **19**, 1432–1442 (2002).

Acknowledgements This work was funded in part by the US National Science Foundation, the US Army Research Office and the W. M. Keck Foundation.

Reviewer information *Nature* thanks K.-Y. Lam and the other anonymous reviewer(s) for their contribution to the peer review of this work.

Author contributions D.M.M. and E.K. conceived the experiments. J.M., R.S. and J.A. performed the measurements. Z.H. and J.M.J. performed the computations shown as dotted lines in Fig. 3. D.M.M., E.K. and C.-Y.Y. analysed and interpreted the data. All authors contributed to the writing of the manuscript.

Competing interests The authors declare no competing interests.

Additional information
Extended data is available for this paper at https://doi.org/10.1038/s41586-018-0609-x.
Reprints and permissions information is available at http://www.nature.com/reprints.
Correspondence and requests for materials should be addressed to D.M.M.
Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

METHODS

Radiation patterns for directional horn antennas. Our transmitter consists of a waveguide-coupled horn antenna together with a dielectric lens (diameter, 5 cm; focal length, 7.5 cm). In Fig. 1, we show the measured radiation pattern for the 200-GHz transmitter (WR-5.1 conical horn) used in our measurements, as well as a computed antenna pattern using a finite-element solver. For this configuration, the measured far-field beam pattern has a directivity of 34 dBi, which corresponds to an angular full-width of about 4°. The radiation patterns for the 100-GHz and 400-GHz measurements are similar; these transmitters also use horn antennas (WR-8 conical horn and WR-2.2 diagonal horn, respectively), coupled to the same dielectric lens. The measured directivities are shown in Extended Data Table 1. As might be anticipated from simple diffraction arguments, higher frequencies produce narrower beams. Yet, even for our narrowest beam, the diameter of the beam when it reaches Bob is still twice as large as the aperture of his receiver.

Our detection system, which we use for Bob's and Eve's measurements, uses the same type of lens and horn as used for the transmitter and therefore has similar angular sensitivity. For bit error rate (BER) measurements, the transmitter signal is modulated with a pulse-pattern generator using amplitude shift keying, with a bit rate of 1 Gb s^{-1}. The detected signal is amplified and analysed in real time using a BER tester. Other specifications of our transmitter and receiver equipment are given in Extended Data Table 1, with more details in ref. [10].

Our measurement set-up is a scale model of a typically envisioned terahertz wireless link—our transmitter–receiver distance is only 2 m. Our work is not intended to emulate a real system, which would require a transmitter–receiver distance of tens or hundreds of metres. In part, this is due to the limitations of our measurement apparatus. A system designed for longer distances would probably use a higher-power transmitter, higher-gain antennas and/or a more sensitive receiver. For example, a system operating at 220 GHz was used previously[34] to achieve a data transmission rate of 3.5 Gb s^{-1} using a transmitter antenna with a gain exceeding 50 dBi. This enhanced link budget enables a scaling of the broadcast distance to 200 m. If we assume that Eve's detector sensitivity scales in the same way as Bob's, then this scaling would not only enhance Bob's ability to detect signals at larger distances but also equally enhance Eve's ability. In more complex wireless links, such as those that use multiple inputs and multiple outputs (MIMO), the issue of scaling is more subtle and requires a more detailed consideration[35]. However, for the single-transmitter, single-receiver link discussed here, a scale-model approach is valid, on the basis of the linearity of the Friis equation. Our results should apply equally well to any line-of-sight link at any range.

Measurement of S_{180}. The data shown in Fig. 2 can be used to select a limited number of configurations for further investigation. Using the criteria that b and $\bar{c}_s$ must both be less than 0.5, we down-select from the 42 different measurements displayed in Fig. 2. The remaining ten points are a representative set of configurations that illustrate successful eavesdropping situations. Eight of these are at the lowest frequency of 100 GHz and the remaining two are at 200 GHz. We measured the back-scatter parameter S_{180} for each of these ten situations; the results are shown in the inset of Fig. 3a.

These measurements are limited in the sense that we have only one receiver for detecting signals. This makes it challenging to characterize back-scattered signals that might be received by Alice, because one of the main sources of back-scattered signals is Bob's receiver. If Bob's receiver generates a back-scattered signal, then it cannot also be used to measure this signal at Alice's location. Of course, a real transmission channel may have other sources of scattering, but in our controlled laboratory environment we worked to eliminate these. To make a measurement that illustrates the point of this potentially valuable counter-measure, we created a mock-up of Bob's receiver rig using highly reflective metal tape, configured to simulate a receiver at Bob's location. We can then move our receiver to a location close to Alice and measure back-scattered signals from the mock-up. This mock-up probably does not accurately reproduce the reflections that would come from an actual receiver, but this is not relevant; any given receiver configuration will give rise to a unique pattern of reflected waves, which will also depend strongly on frequency. Our approach is intended to illustrate the potential value of using back-scatter as a counter-measure in the case of a typical receiver; the details will change depending on the receiver configuration, mounting hardware, channel distance and so on. We also recognize that Alice would need to carefully characterize her transmission channel to Bob, before any eavesdropping attack, for this counter-measure to be useful. Any changes in Bob's receiver configuration or other aspects of the channel would require a recalibration of the back-scattered signal at Alice's location. This may seem challenging, but existing 4G LTE protocols already include a channel-sounding measurement every 20 ms; this is expected to decrease to 1 ms in 5G systems.

An additional measurement challenge in our experiment is that our transmitter (Alice) is not able to also detect received signals. Therefore, we cannot measure signals in exactly the back-scattered direction (180°). Instead, we place our receiver as close as possible to this direction, limited by the size of the equipment. The measured values of S_{180} reported in Fig. 3 were obtained at an angle of about 175° and are therefore only approximate values. Nonetheless, they illustrate the key points of our discussion.

Diffracted field from a uniform metal cylinder. The three dotted curves shown in Fig. 3 were computed using an ab initio model for diffraction from a uniform cylinder made of a perfectly conducting metal[28]. In brief, if Eve is not located in the geometric shadow of the cylinder, then the power received by Eve (in units of decibels) is

$$P_{\mathrm{Eve}} = P_{\mathrm{Alice}} + G_{\mathrm{tx}} + G_{\mathrm{rx}} + 20\log|R_{\mathrm{D}}| - 20\log\left[\frac{4\pi(d_{\mathrm{i}} + d_{\mathrm{r}})}{\lambda}\right]$$

where P_{Alice} is the power transmitted by Alice, G_{tx} and G_{rx} are the gains of the transmitter and receiver, respectively, d_{i} and d_{r} are the propagation distances from the transmitter to the specular surface reflection point on the cylinder and from that point to Eve's receiver, respectively (so that their sum is the total propagation distance for a ray detected by Eve), and λ is the wavelength of the radiation. The factor R_{D} accounts for the strength of the diffracted signal. In a coordinate system centred on the central axis of the cylinder, it is given by

$$R_{\mathrm{D}} = -\exp\left(-i\frac{\pi}{4}\right)\sqrt{\frac{-4}{\xi}}\exp\left(-i\frac{\xi^3}{12}\right)\left[\frac{-F(X)}{2\xi\sqrt{\pi}} + p(\xi)\right]$$

where $\xi = -2(ka/2)X^{1/3}$, $X = 2kd_{\mathrm{i}}\cos^2(\phi)$, k is the free-space wavevector and a is the radius of the cylinder. The angle ϕ is the difference between the angle at which Eve's receiver is located and the angle of the point on the surface of the cylinder that corresponds to the specular surface reflection, both measured relative to the line from the transmitter through the centre of the cylinder. The function F is defined as

$$F(x) = 2i\sqrt{x}\,\mathrm{e}^{ix}\int_{\sqrt{x}}^{\infty}\mathrm{e}^{ju^2}\mathrm{d}u$$

and the function p is the Fock scattering function, which is defined in appendix F of ref. [36].

The beam-splitter attack. In the context of Fig. 4, we envision that Eve has the freedom to create an ideal lossless thin-film beam splitter and place it in the transmission channel at a location where the beam is small enough so that it does not illuminate the edge of the beam splitter (that is, close to Alice), as shown in the inset in Fig. 4a. This placement eliminates any edge-scattering effects. Therefore, the only effect of the beam splitter is to redirect a portion of the transmitted power towards Eve, with the remaining power continuing to Bob, undistorted. We further imagine that Eve has the freedom to choose the power-transmission coefficient of the beam splitter T to be any value between 0 and 1. In this case, we can compute directly the three relevant parameters discussed in the text. First, the blockage is given by $b = 1 - T$. From this result, we conclude that Eve must choose $T > 0.5$, or else the blockage would be too high. Second, the back-scatter parameter S_{180} is found by noting that the signal-to-noise ratio of a back-reflected signal measured by Alice is reduced by a factor of T^2 when the beam splitter is inserted (because such signals must pass through the beam splitter twice to reach Alice, once in each direction). Thus, $S_{180} = |1 - 1/T^2|$. Third, to compute the normalized secrecy capacity, we note that Eve's signal-to-noise ratio ($\mathrm{SNR_{Eve}}$) is given by the product of $1 - T$ and the transmitter power, or

$$\mathrm{SNR_{Eve}} = \frac{1-T}{T}\mathrm{SNR_{Bob}} \tag{1}$$

where $\mathrm{SNR_{Bob}}$ is the signal-to-noise ratio measured by Bob with the beam splitter in place. The normalized secrecy capacity is therefore

$$\bar{c}_{\mathrm{s}} = 1 - \frac{\log[1 + \mathrm{SNR_{Bob}}(1-T)/T]}{\log(1 + \mathrm{SNR_{Bob}})}$$

To proceed with this analysis and compute the value of $\bar{c}_{\mathrm{s}}$ that results when Eve uses a beam splitter with a particular value of T, we must make an assumption about Bob's signal-to-noise ratio. For the purpose of illustration, we assume that Bob is receiving sufficient signal (with the beam splitter in place) to be able to achieve a BER of 10^{-9} (that is, an error-free signal). For amplitude-shift-keying modulation, the BER is related to the signal-to-noise ratio (SNR) by

$$\mathrm{BER} = \frac{1}{4}\mathrm{e}^{-\mathrm{SNR}/4}\mathrm{erfc}\left(\sqrt{\frac{\mathrm{SNR}}{2}}\right) \tag{2}$$

where $\mathrm{erfc}(x)$ is the complimentary error function and the signal-to-noise ratio is expressed as a linear ratio (not in decibels). To achieve $\mathrm{BER_{Bob}} = 10^{-9}$, a signal-to-noise ratio of about 23.3 is required.

Using this assumed value for SNR_{Bob}, we can compute $\bar{c}_s$ and S_{180} for T between 0.5 and 1 (Fig. 4b). These calculations show that there is a narrow range of T for which all three criteria are satisfied: $b < 0.5$, $\bar{c}_s < 0.5$ and $S_{180} < 0.5$. In particular, the criterion on S_{180} is satisfied for $T > \sqrt{2/3} \approx 0.82$ and the criterion on $\bar{c}_s$ is satisfied for

$$T < \frac{SNR_{Bob}}{\sqrt{1+SNR_{Bob}}+SNR_{Bob}-1} \approx 0.86$$

This quantity is not a very strong function of SNR_{Bob}. To reduce it from 0.86 to $\sqrt{2/3}$, SNR_{Bob} would need to be diminished considerably, from about 23.3 to about 10.9. This would eliminate the range of T for which eavesdropping is possible, but at the expense of increasing BER_{Bob} by nearly four orders of magnitude. Thus, under the assumptions that we have made for parameter thresholds, Alice and Bob can prevent a successful beam-splitter attack only by operating at greatly reduced BER and by using both blockage and back-scatter as detection counter-measures.

With the same assumption of $BER_{Bob} = 10^{-9}$, we can use equations (1) and (2) to compute the BER that Eve can achieve (BER_{Eve}) when she uses a beam-splitter attack (Fig. 4b inset, solid red line). Doing so indicates that BER_{Eve} improves continuously as T decreases. If Eve is restricted to the range of T mentioned above, then the optimal value of BER_{Eve} is achieved for $T = \sqrt{2/3}$ and is 1.5×10^{-3}. Although this value may be sufficient to decode information, Eve can do much better with a smaller value of T. If the back-scatter counter-measure proposed here is not used, then Eve can use any beam splitter with $T > 0.5$, enabling her to implement an attack with a secrecy capacity arbitrarily close to zero and thus achieve a BER essentially equal to that of Bob.

The above analysis assumes that the transmitter produces zero side lobes. Although small, the side lobes cannot be exactly zero. Therefore, in the beam-splitter configuration depicted in the inset of Fig. 4a, Eve would measure not only the signal from the beam splitter but also a small contribution from side lobes, which would effectively degrade her BER through added interference. The inset of Fig. 4b also contains a few measured data points (open squares), which quantify this effect. The data reproduce the predicted trend in BER_{Eve}, but with a slightly worse BER than predicted. This is presumably due to the effect of side-lobe interference, which amounts to an extra roughly 3 dB of noise.

To make these measurements, we fabricated a few large-aperture beam splitters (no such devices are commercially available for these frequencies). To avoid etalon effects, which could introduce substantial phase distortion that would artificially decrease the BER, we fabricated the beam splitters on very thin low-loss polyethylene substrates[37]. These substrates were stretched across a circular metal frame with a large enough diameter to encompass the beam at the output of Alice's transmitter without much scattering from the frame. The polyethylene films were then coated with a thin metal layer, using a metallic spray paint. The paint adhered well to the surface and coated it uniformly. By varying the thickness of this metal layer, we fabricated beam splitters with different values of T, which were determined experimentally.

Data availability

The data that support the findings of this study are available from the corresponding author on reasonable request.

34. Chen, Z. et al. 220 GHz outdoor wireless communication system based on a Schottky diode transceiver. *IEICE Electron. Express* **13**, 1–9 (2016).
35. Yeh, C.-Y. & Knightly, E. W. Feasibility of passive eavesdropping in massive MIMO: an experimental approach. In *Proc. IEEE Conf. Commun. Netw. Security (CNS)* 1–9 (IEEE, 2018).
36. McNamara, D. A., Pistorius, C. W. I. & Malherbe, J. A. G. *Introduction to the Uniform Geometrical Theory of Diffraction* (Artech House, Boston, 1990).
37. Ung, B. S.-Y. et al. Low-cost ultra-thin broadband terahertz beam-splitter. *Opt. Express* **20**, 4968–4978 (2012).

Extended Data Table 1 | Specifications for the terahertz wireless communication system

Carrier Frequency	100 GHz	200 GHz	400 GHz
IF frequency	1 GHz		
LO frequency	12.25 GHz		
PRBS	$2^7 - 1$		
Max. Tx output power	24 dBm	20 dBm	10 dBm
Tx/Rx antenna gain	21 dB	21 dB	26 dB
Tx beam directivity (angular full-width)	28 dBi (7.8º)	34 dBi (4º)	42 dBi (1.6º)
Detector responsivity	2400 V/W	6200 V/W	1700 V/W
Detector NEP	3 pW/√Hz	3 pW/√Hz	1.9 pW/√Hz
Tx/Rx polarization	vertical		