AFRL-RI-RS-TR-2023-046

SECURE COMMUNICATION CHANNELS USING ATMOSPHERE-LIMITED LINE-OF-SIGHT TERAHERTZ LINKS

BROWN UNIVERSITY

MARCH 2023

FINAL TECHNICAL REPORT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

STINFO COPY

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE

■ **AIR FORCE MATERIEL COMMAND** ■ **UNITED STATES AIR FORCE** ■ **ROME, NY 13441**

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nations. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RI-RS-TR-2023-046 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

FOR THE CHIEF ENGINEER:

/ S /
NGWE THAWDER
Work Unit Manager

/ S /
GREGORY J. HADYNSKI
Assistant Technical Advisor
Computing & Communications Division
Information Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED	
		START DATE	END DATE
MARCH 2023	FINAL TECHNICAL REPORT	MAY 2019	SEPTEMBER 2022

4. TITLE AND SUBTITLE

SECURE COMMUNICATION CHANNELS USING ATMOSPHERE-LIMITED LINE-OF-SIGHT TERAHERTZ LINKS

5a. CONTRACT NUMBER	5b. GRANT NUMBER	5c. PROGRAM ELEMENT NUMBER
N/A	FA8750-19-1-0500	62788F
5d. PROJECT NUMBER	**5e. TASK NUMBER**	**5f. WORK UNIT NUMBER**
		R2SA

6. AUTHOR(S)

Daniel Mittleman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Brown University, Office of Sponsored Projects
Box 1929
Providence RI 02912

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)	11. SPONSOR/MONITOR'S REPORT NUMBER(S)
Air Force Research Laboratory/RITGA 525 Brooks Road Rome NY 13441-4505	AFRL/ RI	AFRL-RI-RS-TR-2023-046

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for Public Release; Distribution Unlimited. This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The objective of this research is to explore strategies for eavesdropping on terahertz wireless links. One eavesdropping option is to collect the signals that propagate past the receiver, avoiding the possibility of blocking the signal and raising an alarm. In that case, the eavesdropper is further from the transmitter than the receiver, resulting in increased transmission loss. Because of the strong distance dependence of transmission loss, it is possible to choose a carrier frequency such that the intended receiver (at a known range) can detect the signal, but an eavesdropper (at a greater distance) cannot. A second option for an eavesdropper is to rely on tapping into the side lobes of the transmitted signal, rather than the main lobe directed towards the intended receiver. To thwart this possibility, we develop a security scheme in which the eavesdropper has zero probability of intercept regardless of her ability to detect side lobe broadcasts. This scheme relies on the combination of a multi-channel broadcast together with a secure post-quantum encoding.

15. SUBJECT TERMS

Terahertz communications, ultrabroadband communications, atmospheric security, absolute security.

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES
a. REPORT	b. ABSTRACT	C. THIS PAGE		
U	U	U	SAR	35

19a. NAME OF RESPONSIBLE PERSON	19b. PHONE NUMBER *(Include area code)*
NGWE THAWDER	N/A

PREVIOUS EDITION IS OBSOLETE.

Table of Contents

1.0 SUMMARY 1

2.0 ATMOSPHERIC SECURITY IN THE TERAHERTZ BAND 2

2.1 INTRODUCTION 2

2.2 METHODS, ASSUMPTIONS, AND PROCEDURES 2

2.2.1 Bandwidth and spectrum 2

2.2.2 Security 3

2.2.3 Link security based on frequency tuning 5

2.3 RESULTS AND DISCUSSION 9

3.0 ABSOLUTE SECURITY IN BROADBAND WIRELESS LINKS 13

3.1 INTRODUCTION 13

3.2 METHODS, ASSUMPTIONS, AND PROCEDURES 14

3.3 RESULTS AND DISCUSSION 15

3.3.1. Antenna Configuration 15

3.3.2. Defining the Blind Region 15

3.3.3. Secure Encoding: Example 16

3.3.4. Increasing the Secure Communication Efficiency 18

3.3.5. Analysis of the security scheme 19

3.3.6. Experimental demonstrations 22

3.3.7. Contrast with zero forcing 25

4.0 CONCLUSIONS 26

5.0 REFERENCES 27

6.0 LIST OF ACRONYMS 30

List of Figures

1 Simulated atmospheric attenuation and free-space path loss. 2
2 Normalized secrecy capacity for the link described in the text 6
3 Normalized secrecy capacity with atmospheric absorption included 7
4 Experimental setup in the humidity chamber 9
5 Experimental measurements of EVM. 10
6 Bob's channel capacity and normalized secrecy capacity 12
7 An illustration of the absolute security scheme 13
8 Radiation patterns illustrating how the minima shift with frequency 20
9 Size of the blind region increases with bandwidth 21
10 Analysis of a horn antenna 21
11 Experimental realization of absolute security using widely spaced channels 23
12 The size of the blind region as a function of the number of OFDM channels 24

1.0 SUMMARY

Terahertz wireless links offer great potential for secure communications due to the narrow beam divergence, which makes eavesdropping more challenging. For these line-of-sight channels, it is hard for the eavesdropper to detect the terahertz beam without blocking the intended receiver. Several options remain for eavesdroppers. One such option is to collect the signals that propagate past the receiver, avoiding the possibility of blocking the signal and raising an alarm. In that case, the eavesdropper is further from the transmitter than the receiver, resulting in increased transmission loss. Because of the strong distance dependence of the main contributions to this transmission loss, it is possible to choose a carrier frequency such that the intended receiver (at a known range) can detect the signal, but an eavesdropper (at a greater distance) cannot. This frequency tuning relies on the well-established water vapor absorption resonances which are present to varying degrees in the atmosphere, depending on local humidity. In the first part of the project, we explored the engineering of a secure transmission link by exploiting this possibility. In this report, we refer to this first project as *atmospheric security*.

A second option for an eavesdropper is to rely on tapping into the side lobes of the transmitted signal, rather than the main lobe directed towards the intended receiver. Side lobes are typically weak compared to the main lobe (often down by ~15 dB or more), but an eavesdropper with a very sensitive receiver (or one who is much closer to the transmitter than the intended receiver) could still be able to receive enough signal to decode the transmission. To thwart this possibility, we developed the idea of *absolute security*, which indicates a security scheme in which the eavesdropper has zero probability of intercept regardless of her ability to detect side lobe broadcasts. This scheme relies on the combination of a multi-channel broadcast together with a secure post-quantum encoding. It overcomes the traditional bottlenecks in which security must be traded off against computational burden or data rate penalties. The second part of this project focused on developing and testing this absolute security scheme, both computationally and with over-the-air experiments. This second project is referred to here as *absolute security*.

2.0 ATMOSPHERIC SECURITY IN THE TERAHERTZ BAND

2.1 INTRODUCTION

Concerns about wireless security date back to Marconi, when critics pointed out that if wireless signals propagate in all directions, then an adversary can also receive them [1]. Over the last decade, there has been significant progress in the development of technologies to support wireless data transfer at frequencies of 100 GHz and up [2]. This has motivated growing interest in the use of these frequencies for secure and covert wireless links. These envisioned links could enable high-speed data transfer, and would exhibit resiliency against both unintended channel instabilities (e.g., blockage) and deliberate jamming or eavesdropping attacks. This first part of the project seeks to explore one of the most promising and intriguing methods for securing such links, using a technique which relies on the properties of the atmosphere in this spectral range. In particular, we show how one can optimize the security of a link by tuning the frequency of a broadcast near one of the strong, spectrally narrow, absorption lines that arise from ro-vibrational resonances in water vapor. This idea, which has no analog at the lower frequencies used in traditional networks, can offer significant advantages for improved link security.

2.2 METHODS, ASSUMPTIONS, AND PROCEDURES

2.2.1 Bandwidth and spectrum

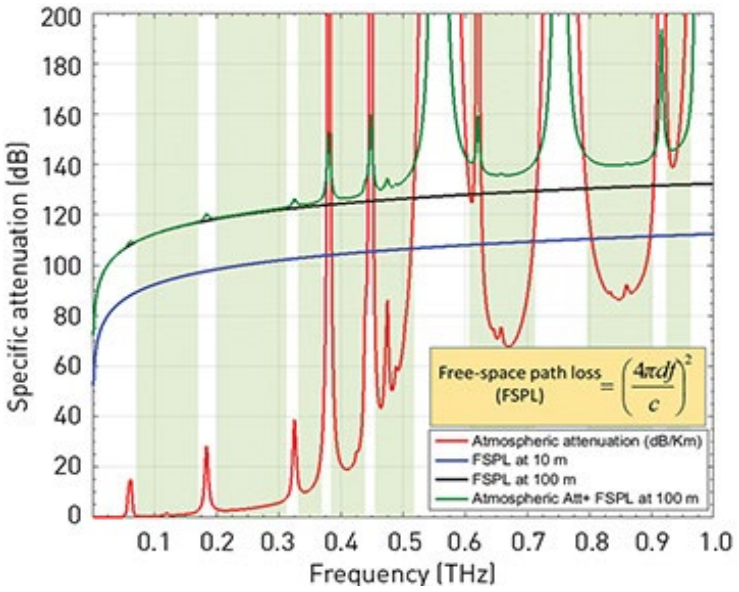

Figure 1. Simulated atmospheric attenuation and free-space path loss vs. frequency in the THz range, computed for a water vapor density of 7.5 g/m^3 at 15ºC (which corresponds to about 59% relative humidity). Adapted from [2].

One of the key motivating factors for the study of wireless systems above 100 GHz is the extremely large available bandwidth, with numerous continuous spectral windows of several tens of GHz, separated by relatively narrow atmospheric absorption bands, as illustrated in Fig. 1. In the range from 120 GHz to over 1000 GHz, the significant absorption lines are all due to water vapor.[1] Within the transmission windows between these narrow lines (indicated by the shaded light green regions in Fig. 1), the attenuation due to molecular absorption in the atmosphere is limited by the continuum background absorption. This background is commonly attributed to water dimers or other transient molecular species. At the frequencies of the resonances, the attenuation of a propagating wave can be quite large; in the windows between lines, the continuum absorption is considerably weaker, although it rises with frequency and can also be significant especially above 500 GHz. This attenuation (both the resonances and the continuum background) can be estimated using well-established models such as the ITU-R Recommendation P676-11, which is reasonably accurate up to at least 500 GHz [3].

If we assume that wireless systems would be designed to operate within the transmission bands, avoiding the sharp absorption lines, then this continuum absorption, along with the free-space path loss, determines the achievable range for a line-of-sight broadcast. Although this range is less than that of lower frequency microwave transmissions, it can still be on the order of tens to hundreds of meters, or even up to a few km (especially near the lower end of the spectral range). For example, the total propagation loss (atmospheric absorption + free-space path loss) is about 120 dB for propagation at 300 GHz over 100m distance, or about 140 dB for a distance of 1 km. To close this link, one can use high-gain (e.g., 50-60 dB) antennas for both the transmitter and receiver, which are readily available (e.g., a parabolic dish with diameter of 20 cm has a typical gain of 54 dB). A few examples of experimental verification of the feasibility of such long-range link demonstrations have been reported in the recent literature [4-6].

In general, the achievable broadcast distance depends on the specific value of the carrier frequency, the details of the transmission system (i.e., generated power, antenna gains), as well as atmospheric factors such as humidity. However, it is clear from Fig. 1 that, for broadcasts at frequencies within the atmospheric windows, the attenuation during propagation is dominated by the free-space path loss, especially for the windows that lie at lower frequencies than the first strong water vapor line (at 380.2 GHz). For the atmospheric windows at higher frequencies (e.g., the windows at 390-430 GHz, or 450-520 GHz), the continuum absorption becomes a more significant contributor to the overall link budget. In addition, if the carrier frequency of the broadcast approaches the frequency of an absorption line, then this situation can change dramatically, such that water vapor absorption becomes the overwhelmingly dominant contributor to the link budget. This is particularly true for the stronger absorption lines, such as those lying at 556.9 GHz and 752.0 GHz, but similar effects can also be observed for the lines at lower frequencies (e.g., 380.2 GHz).

2.2.2 Security

In addition to bandwidth, a second motivation for using terahertz links is the enhanced security and resilience against eavesdropping [7] and jamming [8] that they provide. As compared to

[1] We note that molecular oxygen (O_2) also exhibits absorption lines which can be large enough to have a significant impact, but all of these lines lie at frequencies below 120 GHz. Other molecular species exhibiting resonances in this spectral range (e.g., CO_2, ozone) are present in concentrations which are too low to play a significant role in wireless transmissions.

transmission systems operating at lower frequencies, terahertz wireless links are expected to present a more challenging environment for would-be attackers. This is a consequence of the higher directionality of these high-frequency broadcasts, which can easily exhibit directionality of 25-45 dBi or even higher (depending on frequency and on the antenna configuration) [9]. This higher directionality confines unauthorized users to be within the same narrow cone as the intended user if they wish to directly intercept the signal. As a result, it is commonly assumed that terahertz signals are more secure than broadcasts at lower frequencies, as this attempt to intercept the signal will inevitably be detected by the intended receiver. The reasoning behind this assumption is simple: a more directional transmission sends energy to a smaller range of locations, and so it is more difficult for Eve (an eavesdropper) to place a receiver that detects the signal broadcast by Alice (the transmitter) without blocking Bob (the intended recipient) and thereby raising an alarm. Similarly, a jamming signal would need to originate from within the narrow receiving cone angle of Bob's antenna in order to be effective at jamming Alice's intended transmissions. Since the equipment needed to collect, demodulate, and amplify terahertz signals is large and bulky, always larger than the detector collection aperture, blockage would always be a key concern for an eavesdropper who wishes to operate undetected.

These assertions about the enhanced security of directional links have been mentioned in the literature for a number of years. While this argument is reasonable for conventional eavesdropping attacks, it fails to consider alternative approaches which could circumvent the blockage problem and enable a successful attack. For example, one may consider a different approach for Eve. Rather than the conventional assumption that she must place a large bulky receiver within the narrow beam path [10-13], one may consider the possibility that she can place a smaller passive object in the beam which will scatter some of the transmitted radiation towards her receiver, which is located elsewhere [14]. The minimum size of an object that is required in order to scatter sufficient radiation at, e.g., a right angle to the intended beam path decreases with increasing frequency. As a result, this approach, which would be quite cumbersome for conventional microwave broadcasts, becomes more realistic in the terahertz range. This strategy affords Eve considerable additional flexibility, and can enable successful eavesdropping even at high frequencies with very directional beams.

We have recently reported the first experimental study of this effect at frequencies near or above 100 GHz [7]. We explored this scattering-based eavesdropping method through scale-model experiments, using low-gain antennas and a link with only a few meters of range. Our results demonstrate that an agile eavesdropper, with the freedom to carefully locate a scattering object within the beam path, can succeed in her attack, without being detected by Bob, at all frequencies up to at least 400 GHz. We also proposed a counter-measure in which Alice monitors the back-reflections of the channel, looking for changes that might result from Eve's attack. In our experiments, this counter-measure does indeed narrow the range of possible configurations in which Eve succeeds in her eavesdropping attack. However, not all of the possible attacks give rise to significant changes in the 180º back-scattered signal, so Eve can still implement a successful and undetected attack, particularly if she is aware of the details of the channel.

These findings [7] highlighted a previously unknown vulnerability to eavesdropping in highly directional point-to-point wireless links. It is important to note that, despite this new result, such links are still considerably more secure than conventional wireless broadcasts at lower frequencies, where the broadcast is more nearly omnidirectional. Thus, it is inevitable that future DOD systems

will exploit high-frequency directional links for secure transmissions. As a result, it is now critically important to explore all of the systemic vulnerabilities of such systems, and to develop effective strategies for optimizing their security and resilience against attacks.

2.2.3 Link security based on frequency tuning

The consideration of wireless link security at millimeter-wave and terahertz frequencies is still a field in its infancy, with many open questions remaining to be addressed. In the first part of this research program, we explored one such question, focusing on the efficacy of carrier frequency tuning relative to the frequency of a nearby water vapor resonance as a means for enhancing the security of a line-of-sight link.

For any point-to-point link in which the broadcast is highly directional, one obvious vulnerability originates from the possibility that the eavesdropper (or jammer) is located on the same line of sight as the transmission. Above, we discussed the possibility that the eavesdropper could intercede between Alice and Bob. However, one should also consider the possibility that Eve is situated directly behind Bob. In this case, she would still be in the line of sight of Alice's transmission, although farther away. Assuming that Bob does not entirely block the beam, Eve would still be able to harvest some of the transmitted signal, without being at risk of raising an alarm by blocking Bob's reception. Obviously, if Alice's transmission is not sufficiently narrow in angle, or if it exhibits significant side lobes, then there are even more locations where Eve could be situated (other than directly behind Bob on the line-of-sight path). This vulnerability opens the door to a potential eavesdropping threat which is distinct from the scattering-based attack discussed above.

As an illustrative example, we can envision a point-to-point transmission in which Alice broadcasts along a line of sight to Bob, at a distance of 100m. Unbeknownst to Alice and Bob, we imagine that Eve has located a receiver along this same line of sight, directly behind Bob, at a distance d from Alice (where $d > 100$m). We assume that Alice is using a carrier frequency of 300 GHz. We also assume for simplicity that Eve and Bob are employing receiver antennas with identical gain, and receivers with identical noise figures. In this situation, if we ignore the atmospheric absorption due to the water vapor continuum (as discussed above), then the only difference between Bob's link budget and Eve's link budget is the extra free-space path loss for Eve, due to the extra propagation distance $d_{extra} = d - 100$m. For example, if $d = 200$m, then this adds an extra 6 dB of loss to Eve's link.

One interesting question to consider is the impact that this extra distance has on Eve's ability to detect and decode Alice's transmission. To evaluate this, it is common to employ a parameter known as the *normalized secrecy capacity* [7] of the channel, defined as:

$$\overline{C}_s = \frac{\log_{10}\left(1+SNR_{Bob}\right) - \log_{10}\left(1+SNR_{Eve}\right)}{\log_{10}\left(1+SNR_{Bob}\right)}$$

where the signal-to-noise parameters for Bob and Eve SNR_{Bob} and SNR_{Eve} are expressed as linear (not log) ratios. This parameter subsumes the particular modulation and coding methods and characterizes the empirical limits of Bob and Eve's reception capabilities. It is equal to unity if Eve receives no signal (so the channel is perfectly secure), and zero if Eve and Bob receive the same

signal (i.e., her eavesdropping attack is guaranteed to succeed). Thus, from Alice and Bob's point of view, larger values are better (more secure), as they indicate that Eve's measurement has a lower SNR (and correspondingly, a higher bit error rate). For the purposes of this example, we assume that Alice uses amplitude-shift-keying (ASK) modulation, and that she has adjusted her transmitter's output power in order to guarantee that Bob has sufficient signal-to-noise to obtain a bit-error rate (BER) of 10^{-9}. With these assumptions, we can compute values for the normalized secrecy capacity as a function of d, the distance from Alice to Eve. This result is shown in Fig. 2, which shows the normalized secrecy capacity vs. Eve's distance, assuming that Bob is located at 100m from Alice, and that he receives Alice's broadcast with SNR corresponding to a bit error rate of 10^{-9}. In this example, we find that, if $d = 200$m, that $\bar{c}_s \approx 0.089$, which is a rather low value – in this case, Eve is likely to succeed in her attack. Indeed, in this example the normalized secrecy capacity remains below $\bar{c}_s = 0.5$ until Eve is more than 900m away. This value, indicated by the dashed line in Fig. 2, represents an arbitrary threshold which could be used to distinguish between a secure and non-secure channel. Evidently, the free-space path loss alone is not sufficient to guarantee the security of the channel.

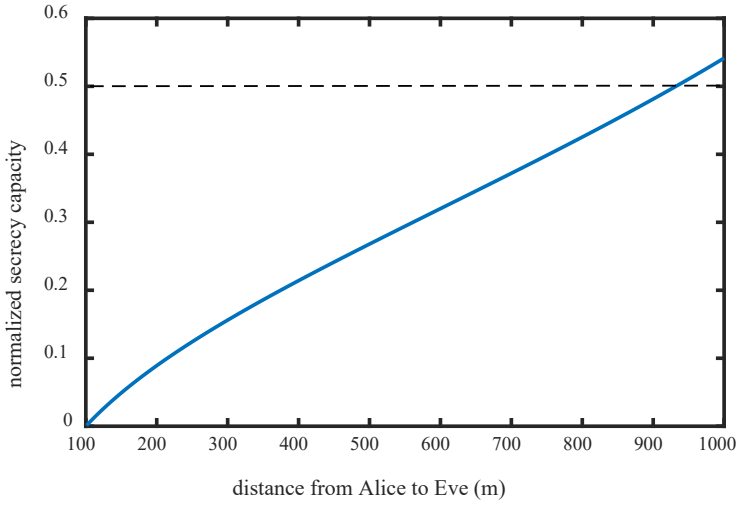

Figure 2. Normalized secrecy capacity for the link described in the text, computed as a function of distance between Alice and Eve.

The combination of higher directionality and the properties of the atmospheric attenuation suggests an interesting possibility for overcoming this intrinsic vulnerability. Suppose that Alice's transmitter has the capability to continuously tune the carrier frequency, in order to adjust the frequency offset between this carrier wave and the (fixed) frequency of a strong water vapor absorption line. With this capability, Alice could adjust her transmission to a chosen frequency, near a water vapor absorption line, in order to limit the distance over which the broadcast can be detected. Ideally, Bob would be close enough to be able to detect the signal. In contrast, Eve, located along the same line of sight as the transmission to Bob (but farther away), would not be able to detect the signal due to the extra atmospheric attenuation.

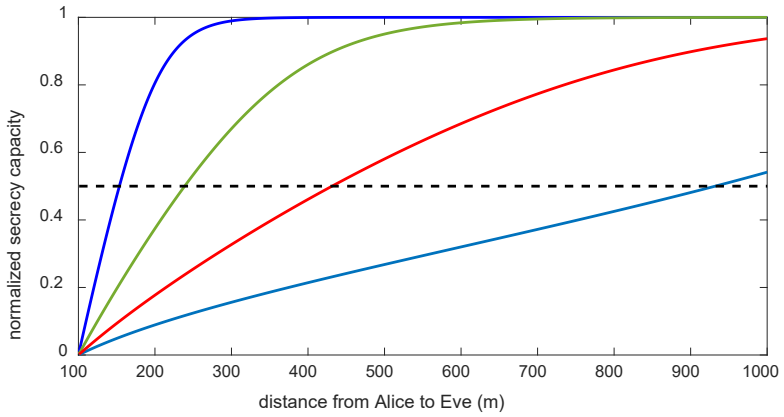

Figure 3. Normalized secrecy capacity for the link described in the text, in which attenuation of the signal due to atmospheric absorption is included in the upper three curves.

An illustration of the potential effectiveness of this strategy is shown in Fig. 3. Here, the normalized secrecy capacity is computed for the same assumptions as discussed above in the context of Fig. 2. In this plot, the lower (light blue) curve is the same as the curve in Fig. 2, showing the secrecy capacity as Eve's distance from Alice increases, which increases only very gradually due to the additional free-space path loss. The other three curves incorporate atmospheric loss in addition to the free-space path loss. This extra loss is included by a simple absorption coefficient

α which attenuates the signal according to Beer's Law: $\exp\left[-\alpha d\right]$ (with the red, green, and dark blue curves corresponding to increasing values of absorption coefficient, respectively). Clearly, since Eve is farther from Alice, her signal is attenuated by an additional factor of $\exp\left[-\alpha\left(d-100\right)\right]$, relative to Bob's signal. The calculation still assumes that Bob's SNR is constant, equal to the value necessary for a BER of 10^{-9}. In these cases, the secrecy capacity rises much more steeply with increasing distance; this extra atmospheric loss dramatically reduces the range of locations where Eve can situate her receiver in order to maintain a low (less than 0.5) value of $\overline{c}_s$.

Of course, the trade-off is that this extra attenuation also impacts Bob; with the assumption of constant SNR_{Bob}, we are implicitly assuming that Alice can not only tune the frequency of the transmission, but also that she correspondingly increases the output power of her transmitter, in order to compensate for the extra loss and maintain Bob's SNR. The three upper curves plotted in Fig. 3 represent three different values of α; for these three curves, Alice would need to increase her transmitter power by 1.3 dB (red curve), 4.3 dB (green curve), and 13 dB (dark blue curve), in order to satisfy this criterion.

We note that this simple illustration neglects several potentially significant complicating factors. For one, the absorption coefficient is assumed to be constant; in fact, it is strongly frequency-dependent near a resonance. As a result, a modulated signal, with a finite bandwidth, will be attenuated non-uniformly across its spectrum, resulting in distortions in the temporal shape of the

signal. For another, the signal would also be distorted by the phase response of the atmosphere – that is, the group velocity dispersion associated with the molecular resonance. In our proposed research discussed below, we will develop a more realistic model to include these effects in the analysis, as well as characterizing them through experimentation.

Despite the over-simplified nature of the example discussed here, it nevertheless makes a few important points. First, the idea of using frequency tuning to enhance link security appears to be feasible. Second, the key to implementing this strategy effectively lies in Alice's ability to tune the carrier frequency precisely, relative to a given water vapor absorption line, as well as tuning the output power of her transmitter. The idea is that she should aim for a frequency where the attenuation is just enough, neither too high nor too low, for the desired broadcast range. If Alice chooses a frequency that is too close to the water vapor resonance, then the signal will be too strongly attenuated, and she will not be able to compensate by increasing the broadcast power. In this case, neither Eve nor Bob will be able to detect the signal. Conversely, if Alice chooses a frequency that is too far from the resonance, then the signal will not be attenuated enough, and Eve will still be able to detect and decode the transmission, despite being farther away. Thus, the use of this counter-measure requires Alice to have accurate knowledge of the attenuation vs. frequency near the targeted water vapor absorption line, with the highest possible frequency resolution. Of course, these values depend sensitively on the weather conditions (temperature and humidity) at the time of the transmission. (We note that precipitation, e.g. rain or snow, presents an additional complication, as these weather conditions change the transmission characteristics of the atmosphere in complex and frequency-dependent ways, due to both absorption and scattering [15]. In this effort, we do not consider these complicating factors.)

Our experimental approach to study these questions is to employ a chamber for temperature and humidity control, which will enable experimental characterization of the channel in a scale-model system with well-controlled atmospheric conditions. We can then couple this chamber to a tunable transmitter and receiver system, based on mixers obtained from Virginia Diodes, in order to study the propagation of modulated signals with different carrier frequencies, and with different atmospheric conditions.

We note that the tuning range of the available measurement systems are collectively quite large, so that the experiments can in principle be carried out near any of the water vapor lines lying below 1 THz. However, there are some considerations which may suggest limiting the lines that are studied in this program. First, some of these lines are stronger than others. For the weaker ones, the path loss $(4\pi d/\lambda)^2$ may be much larger than the atmospheric attenuation, at a given range. Clearly, the path loss increases quadratically with propagation distance, while the resonant absorption increases exponentially, so the resonance must eventually become the dominant term. But, for a weak resonance, this distance could be larger than we can practically achieve, particularly given the low output power of typical sources. As is evident from Fig. 1, this is certainly the case for the lines at the low-frequency end of the spectrum (e.g., the water vapor line at 183.3 GHz). We instead focus on lines at higher frequencies (e.g., the line near 380 GHz). Lines at still higher frequency are even stronger (e.g., 556.9 GHz), and are even readily visible in short-range measurements with low-gain antennas. We note that it may not be necessary to exhaustively measure all of the lines, since a careful measurement of the effects near one absorption line should provide results which can easily be used to predict the analogous results near any of the other lines.

Attenuation due to the absorption of energy from the propagating beam is not the only issue. A second, more subtle issue is that of distortion of the signal due to dispersion [16]. Unlike conventional wireless systems at lower frequencies, the dispersion of signals in a terahertz link can arise from factors other than the effects of multi-path propagation. Although non-line-of-sight propagation is possible above 100 GHz in some cases [9], it is not generally expected to contribute substantially to a stochastic spread of arrival times, due to the limited number of possible low-loss paths connecting the transmitter and receiver. Rather, one should expect that the dominant dispersive effects arise due to the properties of the atmosphere, particularly for long-range transmissions. Any reasonably well-behaved resonance exhibits not only a peak in the imaginary part of the dielectric function, but also a dispersive line shape in the real part. In general, this dispersive line extends considerably farther from the line center than the peak in the imaginary part; in other words, the effects of dispersion can be significant even if the frequency of the transmitted signal is relatively far from the peak of the signal so that the attenuation is small. Thus, this effect will have a dramatic impact on the rate of data transmission, producing phase distortions and inter-symbol interference which will degrade the bit error rate (or, equivalently, limit the spectral bandwidth in which transmissions are possible). This effect will become more severe as the data rate increases, and also as the carrier frequency is tuned closer to the resonant absorption line. Thus, the frequency tuning scheme for enhanced security described above may limit the attainable data rate. If so, one could find that improved security will come at the cost of lower data rate. A key aspect of the proposed research is to quantify this effect by investigating the efficacy of automated channel equalization filters.

2.3 RESULTS AND DISCUSSION

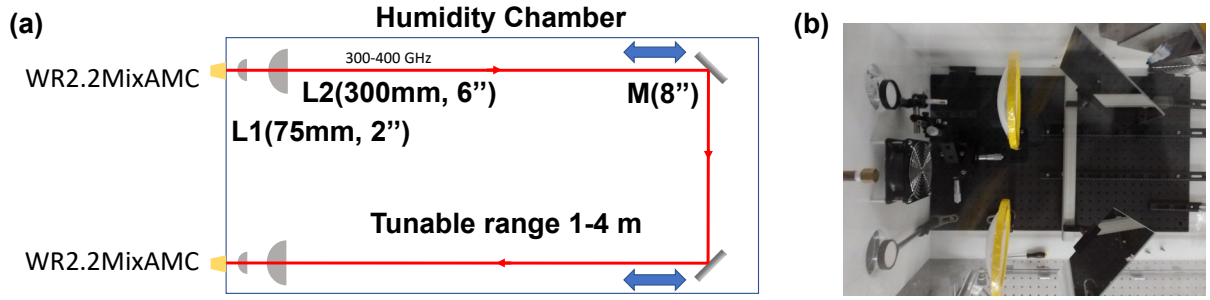

Figure 4. Experimental setup. (a) A schematic of the setup of the terahertz wireless link, allowing a tunable propagation range from 1-4 m. (b) A top-down photo of the interior of the chamber.

Fig. 4 shows the experimental setup of the terahertz wireless link inside a humidity chamber. The humidity chamber allows a tunable temperature from 5-51 °C. By attaching a heat insulation blanket outside the chamber, we diminished the heat transfer through the wall of the chamber to stabilize the temperature fluctuation down to ±0.5 °C. The dry air and the water vapor input of the chamber allows a tunable relative humidity from 5%-95% at room temperature (24 °C) and from

5%-68% at highest temperature (51 °C), corresponding to a tunable water vapor absorption loss from 0-3 dB at 380.2 GHz. We use 4 lenses (L1, L2) and 2 mirrors (M) to minimize the FSPL so that the link can be closed successfully at a propagation range of up to 4 m.

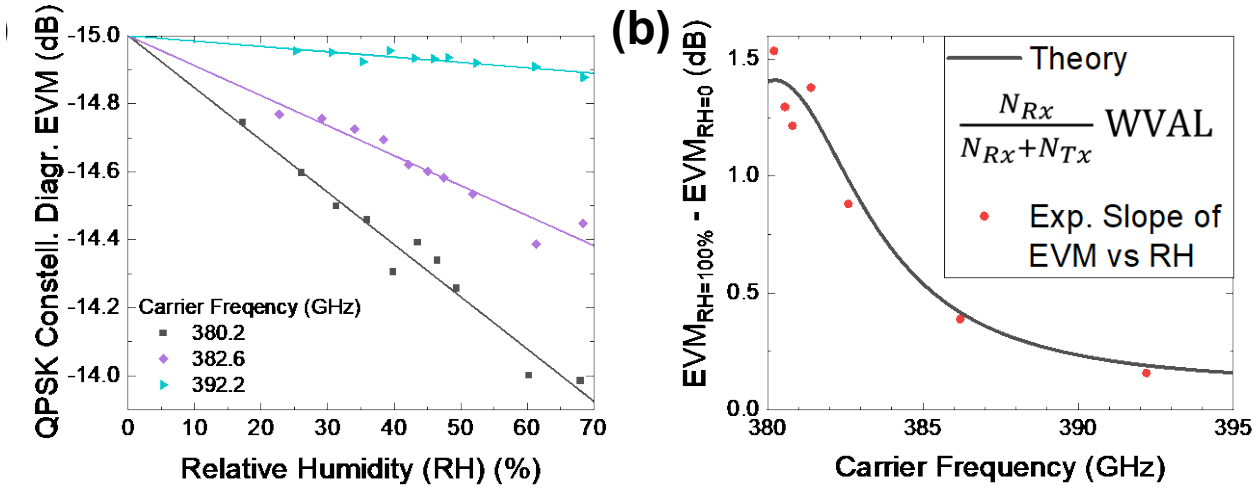

Figure 5. (a) Experimental measurement of EVM for the constellation diagram of QPSK modulation at a symbol rate of 1 GBaud for a 4 m link inside the humidity chamber at room temperature (T = 24 °C). (b) The slopes of EVM fitted in (a) plotted with the theoretical prediction from Eq. (3).

Fig. 5 shows some typical experimental results for the wireless link in the climate chamber. To present these results, we choose the error vector magnitude (EVM) of the constellation diagram as the metric of our measurement. The analytical expression of EVM is as follows:

$$\mathrm{EVM} = \frac{1}{\sqrt{\mathrm{SNR}}} = \sqrt{\frac{N_C \mathrm{WVAL}^2 + N_{Rx}\mathrm{WVAL} + N_{Tx}}{P\,/(\,\mathrm{FSPL}\,\times\,\mathrm{WVAL})}} \qquad (1)$$

Here, we define the two loss factors, both greater than unity, as:

$$\mathrm{FSPL} = \frac{c^2 d^2}{A_R A_T f^2} \quad \text{and} \quad \mathrm{WVAL} = e^{\mathrm{RH}\times \mathrm{G}(f) d} \qquad (2)$$

In these expressions, P is Alice's transmitting power, d is the propagation range, A_R and A_T are the transmitter and receiver antenna areas, RH is the relative humidity, and G(f) is the frequency-dependent atmospheric absorption. The SNR in Eq. (1) is the signal-to-noise ratio at the receiver. N_C, N_{Rx}, and N_{Tx} represent the effective AWGN noise at the receiver from the channel (C) [17], the receiver (Rx) and the transmitter (Tx), respectively. Under realistic conditions, the channel noise is negligible, so we generally set $N_C = 0$. If we further assume that the water vapor absorption

loss is small (so that WVAL ≈ 1 + a small correction), then Eq. (1) can be written in a linearized form. Expressed on a log scale, we find that the EVM should be expected to vary linearly as a function of relative humidity:

$$\mathrm{EVM_{RH}} - \mathrm{EVM_{RH=0}} = 10\log_{10}\frac{N_{Rx}\mathrm{WVAL} + N_{Tx}}{N_{Rx} + N_{Tx}} \approx \frac{N_{Rx}}{N_{Rx} + N_{Tx}}\,\mathrm{WVAL(dB)} \tag{3}$$

In Fig. 5(a), we show measurements of the EVM vs. humidity for several frequencies close to the water vapor line at 380.2 GHz. These values are normalized to extrapolate to a value of -15 dB at zero humidity, to remove the instrumental effect of frequency-dependent mixer gain. As expected, as we tune the carrier frequency further away from the water vapor absorption line center at 380.2 GHz, the change in humidity matters less, so the slope of EVM as a function of the relative humidity decreases. Linear fits to these data, following Eq. (3), are also shown, indicating good agreement with the model. These fits allow us to obtain a phenomenological value for the ratio of the noise terms, specifically $N_{Rx}: N_{Tx} = 1: 1.84$. Using this value, we can predict the slope of these EVM plots vs. frequency. This prediction is shown in Fig. 5(b), along with our measured results. These results validate our assumption that the noise parameters are approximately frequency-independent.

Next, we consider the trade-off in channel capacity with secrecy. As we have done previously [7], we define Bob's channel capacity c_{Bob} and the normalized secrecy capacity $\overline{c_s}$ as:

$$c_{\mathrm{Bob}} = 2B\log_2(1 + \mathrm{SNR_{Bob}}) \tag{4}$$

$$\overline{c_s} = \frac{c_s}{c_{\mathrm{Bob}}} = \frac{c_{\mathrm{Bob}} - c_{\mathrm{Eve}}}{c_{\mathrm{Bob}}} = \frac{\log(1 + \mathrm{SNR_{Bob}}) - \log(1 + \mathrm{SNR_{Eve}})}{\log(1 + \mathrm{SNR_{Bob}})} \in [0,1] \tag{5}$$

B is the bandwidth, and the signal-to-noise ratios for Bob and Eve are defined as usual. The factor of 2 in Eq. (4) arises because of the QPSK modulation (two subchannels including the in-phase (I) and quadrature (Q) components). To compute c_{Bob}, we use a zero-humidity SNR of 15 dB, roughly consistent with the extrapolated values from Fig. 5(a). Next, for illustrative purposes we assume that Eve is located behind Bob at a distance which is twice the Alice-Bob distance ($d_{\mathrm{Eve}}/d_{\mathrm{Bob}} = 2$). As depicted in Fig. 6(a), tuning the frequency closer to the water vapor absorption line center at 380.2 GHz increases the normalized secrecy capacity, with a cost of reduction of Bob's channel capacity. These curves are computed for room atmosphere, with T = 24 °C and RH = 68%. The solid curves in Fig. 6(b) assume different constant values for Alice's broadcast power P and a constant Alice-Bob distance (and therefore a constant $\mathrm{FSPL_{Bob}}$). These curves show that a modest sacrifice in channel capacity can produce a significant improvement in secrecy capacity, and therefore this approach to security is highly promising. The dashed curves in Fig. 6(b) show how much $\mathrm{WVAL_{Bob}}$ is needed, so that Alice can choose an appropriate carrier frequency. These results have now been published in the *IEEE Transactions on Terahertz Science and Technology* [18].

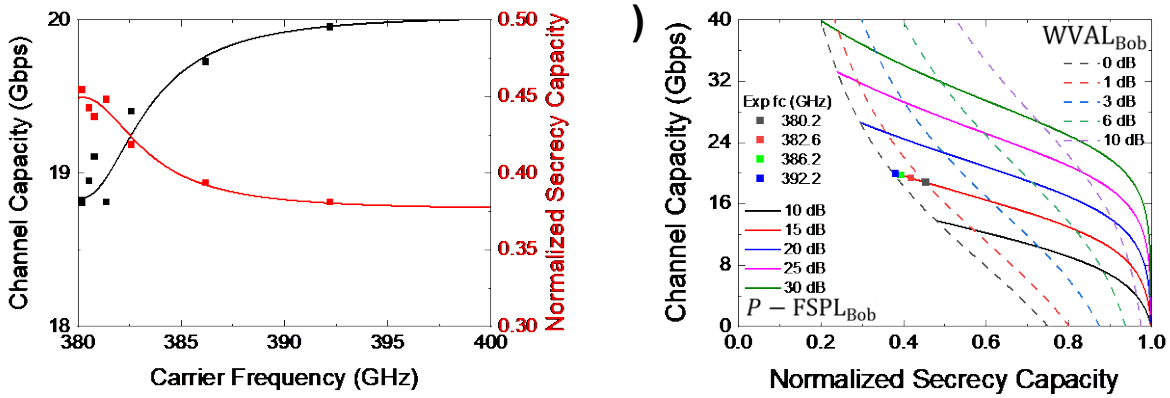

Figure 6. (a) Bob's channel capacity (black) and normalized secrecy capacity (red) as a function of the carrier frequency. (b) Bob's channel capacity vs. normalized secrecy capacity. The dots are the experimental results.

We have also completed the first version of a software package for predicting channel characteristics and secrecy capacity under given conditions of range and atmosphere. This can enable users to select the appropriate transmission carrier frequency in order to optimize the range/secrecy tradeoff for a given broadcast configuration. This code has been delivered to AFRL, and is currently being evaluated. We plan to continue to work with AFRL personnel to optimize the performance and ease of use of this package.

3.0 ABSOLUTE SECURITY IN BROADBAND WIRELESS LINKS

3.1 INTRODUCTION

Modern wireless technologies have now begun to employ higher frequencies, in the millimeter-wave [19-21] and terahertz ranges [7, 9, 22-24], which are likely to require the use of high-gain antennas to produce directional beams [9, 22, 25-27]. Although this directionality inhibits eavesdropping, successful attacks are still possible since most highly directional antennas exhibit side lobe emission which sends signals in many directions. Efforts to scramble the information contained in side lobes [28] can offer significant improvements, but even so, an eavesdropper (Eve) will always have a non-zero probability of intercepting and decoding the transmitted message between the sender (Alice) and the intended receiver (Bob). In essence, all such security schemes rely on assumptions about noise in Eve's measurement [29-32], or on her computational capabilities [33, 34]. Despite the fact that many of these security schemes are termed in the literature as exhibiting perfect security [30, 35, 36], it is clearly more favorable if Eve has *zero* probability of intercepting the message from Alice to Bob, regardless of assumptions.

In this project, we describe a new approach to realize what we term *absolute* security, which we define as security *with probability one*. Such a notion contrasts with common probabilistic security typically used in physical layer security discussions (including, e.g., Eq. (4) above), that relies on an SNR gap, and therefore holds merely in an average sense over noise realizations. In contrast, absolute security holds with probability one for *any* realization of the noise, even for the putative case, most favorable to Eve, in which her measurement is noiseless.

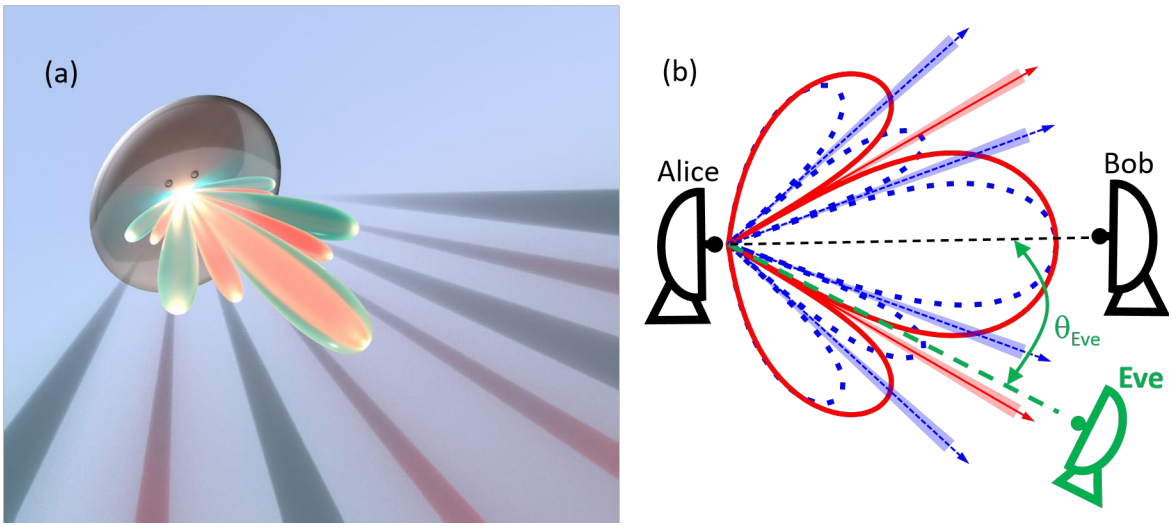

Figure 7. (a) An illustration of radiation patterns from a parabolic dish at two different frequencies, showing the main lobe and side lobes. (b) Schematic diagram showing Alice (the transmitter) broadcasting to Bob (the intended receiver), while (an eavesdropper) is located at θ_{Eve}.

Our approach to achieve absolute security relies on both the inherent properties of Alice's antenna and on an associated secure coding scheme. Many directional antennas, when driven over an ultrawide bandwidth, result in frequency-dependent minima as illustrated in Fig. 7. The minima of each pattern define angular regions where signals cannot be detected at a given frequency. Since any receiver has a minimum detectable signal threshold, radiation minima create regions in space where Eve cannot even detect the signal, regardless of the noise realization. This allow us to leverage recent developments in secure communications to thwart Eve as long as some frequencies are "blind" for her. As illustrated in Fig. 7(b), Eve may be able to detect one frequency (in this illustration, the blue one), but she is blind to the other one (the red one) because her location coincides with a minimum in that frequency's radiation pattern. Exploiting this idea enables Alice and Bob to establish a secure wireless link that cannot be broken by any adversary located in such a blind region of the broadcast space, even if she possesses arbitrarily powerful computational capabilities, even a quantum computer [37-39].

Our discussion here mostly focuses on the situation in which the eavesdropper is located not within the main lobe of Alice's transmission (as in the discussion of *atmospheric security* above), but rather within an engineered region of the broadcast sector that enables absolute security (the so-called "blind region", defined more rigorously below). We also describe a small modification to our method which allows us to provide absolute security even against eavesdroppers who are *not* in this blind region. Our method breaks the conventional paradigm for secure communications in which one faces a trade-off between data transmission rate and the degree of security: in our approach, increasing the transmission bandwidth (and therefore the achievable data rate) can *simultaneously* offer improved security. This method is therefore particularly well suited for future generations of wireless technology, which will exploit ultra-wideband channels in the millimeter-wave and terahertz regions of the spectrum [22].

3.2 METHODS, ASSUMPTIONS, AND PROCEDURES

To demonstrate our proposed method, we perform model-driven analysis for multiple antennas suitable for millimeter-wave and terahertz bands, as well as experimental measurement with over-the-air data transmissions. With model-driven analysis, we show how the blind region increases with a larger bandwidth, when the antenna features frequency-dependent minima, including phased arrays, parabolic dishes, and leaky wave antennas. We also show that not all antennas are suitable for our proposed method. Horn antennas, for example, do not exhibit pronounced minima, and thus increasing bandwidth does not enlarge the blind region. However, in the experiment, we show that the horn antenna can still be used for our method. By placing a beam block in front of the horn antenna, we create diffraction pattern and pronounced frequency-dependent minima. With three widely spaced frequencies (100, 200, and 400 GHz), we demonstrate a substantial blind region where Eve fails to detect at least one of the three modulated data streams and thus achieve absolute security.

3.3 RESULTS AND DISCUSSION

3.3.1. Antenna Configuration

For many antennas, the far-field radiation pattern exhibits minima in specific directions, which depend on the details of the antenna geometry and its excitation mechanism, as well as on the frequency of the radiation [40]. For example, two commonly employed antennas in high-frequency wireless links, a linear phased array [41, 42] and a center-fed parabolic dish [25], both exhibit pronounced minima at various angles, which shift with transmission frequency. Under the assumption (discussed further below) that Eve must avoid *all* of these minima, a transmission with multiple frequency bands creates a significant excluded region for Eve. To quantify this, we consider a transmission that uses a bandwidth B from f_L to f_H, centered on $f_C = (f_L + f_H)/2$, sliced uniformly into q frequency channels, each with bandwidth $w = (f_H - f_L)/q$. At location (r,θ), the received intensity S (in W/m^2) in the i^{th} frequency channel $[f_i - w/2, f_i + w/2]$ can then be written:

$$S(f_i) \propto \int_{f_i - w/2}^{f_i + w/2} P_T(f) \cdot \gamma(r, f) \cdot G(f, \theta)\, df \tag{6}$$

where $P_T(f)$ is the transmit power spectrum (in W/Hz) employed by Alice, $\gamma(r,f)$ is the distance- and frequency-dependent channel gain from the transmitter to the receiver and $G(f,\theta)$ is the antenna radiation pattern. For simplicity, we consider only one emission plane (H plane), although our results can readily be generalized to three dimensions.

3.3.2. Defining the Blind Region

For any receiver, there exists a minimum detectable signal threshold $\delta > 0$ (intensity per unit bandwidth), below which the receiver cannot detect a transmission. This threshold may depend on the receiver sensitivity, the receive antenna gain, the environmental noise floor, and the quantization of digital processing. The existence of this non-zero threshold δ implies that there are blind regions where, with probability one, Eve cannot detect the transmission. We define the blind region ($\boldsymbol{\Omega}$) for a transmission band $[f_L, f_H]$ as the set of locations (r_{Eve}, θ_{Eve}) where Eve is unable to detect signals in *at least one* of the q frequency channels. Specifically, we first define the blind region for the i^{th} frequency channel as the set of locations for which the signal intensity is below the detection threshold:

$$Z(f_i) = \left\{ (r_{Eve}, \theta_{Eve}) \middle| S(f_i) < \delta \cdot w \right\}. \tag{7}$$

The blind region for the total transmission band is then the union of blind regions for each subchannel:

$$\boldsymbol{\Omega} = \bigcup_{i=1}^{q} Z(f_i). \tag{8}$$

For each location in the blind region $\boldsymbol{\Omega}$, the number of missing frequency channels can vary from one up to all q of them. We therefore also define Γ as the number of subchannels for which $S(f_i) < \delta \cdot w$. Each possible location for Eve can therefore be characterized as either non-blind ($\Gamma = 0$) or Γ-blind ($1 \le \Gamma \le q$).

As the number of subchannels q increases, Alice's broadcast includes more signals at distinct frequencies with unique radiation patterns, each exhibiting minima in distinct directions. Thus, the percentage of angular locations θ_{Eve} that are within the blind region also increases.

We emphasize that the blind region defined here is not just a function of the antenna and broadcast frequencies. It also depends on the properties of Eve's receiver, through the parameter δ defined above. As a result, different assumptions about Eve's receiver capabilities will result in somewhat different blind regions. However, even in the hypothetical best case (for Eve) that her receiver is quantum-noise limited, her ability to detect Alice's broadcast is still limited by the thermal noise of the environment which she is observing. Of course, it is possible to detect signals that are well below the thermal background; this is commonly achieved, for example in astrophysical observations, by severely restricting the spectral bandwidth of the detection and/or extended signal averaging. However, Eve cannot employ these strategies if she wishes to decode a broadband high-data-rate transmission. Thus, the value of δ cannot be infinitesimal, regardless of how Eve detects signals. An important consequence of this conclusion is that we *need not require* that Eve's location must precisely coincide with the (mathematically infinitesimal) angular position of a minimum in an antenna radiation pattern; she only needs to be *close enough* to a minimum such that her received signal is small.

This consideration emphasizes the clear distinction between our proposal and the idea of extending conventional narrowband beam forming methods based on zero forcing to a broadband context [43, 44]. With zero-forcing, one can engineer an antenna (e.g., the signals applied to each element of a phased array) to force the broadcast wave amplitude to zero in a given direction at a given frequency. This would make it impossible for Eve to detect signals at that frequency, if she is located in that direction. But she would still be able to detect signals at other frequencies, since the zero is enforced in her direction only for one particular frequency. By contrast, with our method, Eve would fail to decode any of the frequency channels, not merely the one whose antenna pattern is forced to be zero at her location. Indeed, our approach does not require knowledge of Eve's location. Since the blind region defined by Eq. (8) is the *union* of minima over all frequency bands, it can quite realistically occupy a significant fraction of the total angular space. The approach described here scales favorably with increasing transmission bandwidth, while the exact opposite is true for security schemes based on zero forcing. It is also worth noting that zero-forcing only works for phased arrays; meanwhile, our approach has the advantage of working well for many antenna configurations, including for instance a conventional parabolic dish antenna, where zero-forcing techniques obviously cannot be applied.

It is the coordinated use of, on the one hand, the union of blind regions $\mathbf{\Omega}$ from frequency-dependent radiation patterns and, on the other hand, a secure coding scheme, that constitutes the core of our method's novelty. Unlike legacy methods relying on design of minima regions for security [36], the particular subset of frequencies that Eve can detect in any of the blind regions is irrelevant for our approach. This lack of dependence on the subset of detectable channels greatly expands the notion and, hence, footprint of the blind regions relative to traditional beam forming methods.

3.3.3. Secure Encoding: Example

In this section, we consider the first encoding scheme, which we denote as Scheme 1, assumes that Eve is within the blind region. We illustrate the ideas by using a simplified situation in which Alice wants to communicate securely with Bob using only $q = 3$ subchannels, at frequencies f_1, f_2, and f_3. The general idea can readily be scaled to a larger number of subchannels from known

constructions in the literature [45, 46]. In the encoding scheme considered here, we assume that Eve is within the blind region. Our scheme operates symbol-wise, so Alice must map her message into blocks, and then map each block into a symbol selected from a finite field of dimension greater than 2^q [46]. For ease of exposition, we consider here a prime field. The construction can be easily generalized to operation over extensions of the binary field. Because our simplified illustration employs $q = 3$ subchannels, our illustrative example employs the finite field F_{11} [45]. Alice first partitions her message (strings of bits) into blocks of length $\lceil \log_2(11) \rceil$, and then maps each block to a symbol of F_{11}. To transmit a single message symbol $M \in \mathsf{F}_{11}$ securely to Bob, Alice first generates two symbols $T_1, T_2 \in \mathsf{F}_{11}$ uniformly at random. Alice then generates three encoded symbols $X_1, X_2, X_3 \in \mathsf{F}_{11}$ using her message M and the two random symbols T_1 and T_2, given by:

$$\begin{aligned} X_1 &= M + T_1 + T_2 \\ X_2 &= M + 2T_1 + 4T_2 \\ X_3 &= M + 3T_1 + 9T_2 \end{aligned} \tag{9}$$

Each encoded symbol X_i is transmitted to Bob via the frequency band f_i. Since Bob is not in the blind region (i.e., his location has $\Gamma = 0$), he receives the three encoded symbols and is able to decode the message symbol M by means of a simple linear transform which inverts Eq. (9):

$$\begin{pmatrix} M \\ T_1 \\ T_2 \end{pmatrix} = \begin{pmatrix} 3 & 8 & 1 \\ 3 & 4 & 4 \\ 6 & 10 & 6 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} \tag{10}$$

However, since Eve is in the blind region, she can observe at most two encoded symbols from the set $\{X_1, X_2, X_3\}$ with probability one. We can show that, regardless of which two encoded symbols Eve detects, she cannot determine M. For instance, if Eve receives X_1 and X_2, then the mutual information between her observations and the message symbol M can be computed from the entropy as:

$$\begin{aligned} I(M; X_1, X_2) &= H(X_1, X_2) - H(X_1, X_2 \mid M) \\ &= H(X_1, X_2) - H(T_1 + T_2, 2T_1 + 4T_2) \\ &= H(X_1, X_2) - 2\log|\mathsf{F}_{11}| \\ &\le H(X_1) + H(X_2) - 2\log(11) = 0 \end{aligned} \tag{11}$$

This result follows directly from the definition of mutual information, and the fact that, conditioned on the messages, the only uncertainty about X_1 and X_2 is in the random variables $T_1 + T_2$ and $2T_1 + 4T_2$, which are independent and uniform. Thus, because there is zero mutual information between Eve's observation and Alice's message, Eve learns nothing about M; absolute security is guaranteed.

3.3.4. Increasing the Secure Communication Efficiency

We can define the secure communication efficiency in terms of the length of Alice's message. This efficiency η is the ratio between the size of the message and the number of bits needed to transmit it. Ideally, one would like this rate to be as close to $\eta = 1$ as possible. Generally, in previously proposed security schemes, this is not possible owing to the need to add redundancy to the transmission in order to guarantee security in the communication [29, 30, 47]. In the security scheme described above, by noting that Alice must send $q = 3$ encoded symbols to transmit the original message symbol, we see that the secure communication efficiency is $\eta = 1/3$. In general, the efficiency scales inversely with the number of frequency channels, $\eta \propto 1/q$.

It is easy to address this issue of the less-than-ideal efficiency of our approach, by making a small modification to the method, which we term Scheme 2: Alice can replace the $q - 1$ (in our example, two) random symbols with additional messages, M_2 and M_3, and then perform the same encoding as in Eq. (8), with the random symbols replaced by the additional messages. Alice can thus obtain an optimum secure communication efficiency of $\eta = 1$, regardless of the number of channels. That is, Alice replaces the random symbols, T_1 and T_2, with message symbols M_2 and M_3, and then transmits the three encoded symbols X_1, X_2, X_3 as defined in Eq. (9).

As before, Bob can decode all three message symbols through a linear transform; but, the secure communication efficiency issue is now solved, since now $q = 3$ encoded symbols are sent in order to retrieve $q = 3$ message symbols, i.e., $\eta = 1$. This scheme guarantees zero mutual information with any subset of message symbols, yet may potentially allow Eve to obtain information about linear combinations of the message symbols [46]. In order to implement this approach, Alice must ensure that the message symbols M_1, M_2, M_3 are uniformly distributed. The reason for this, intuitively, is that the message symbols themselves are performing the role of the random symbols T_1 and T_2. We note that there are known techniques described in the literature [48] which can be used to enforce this uniformity condition, so this requirement is not a significant impediment. Thus, although $I(M_1, M_2, M_3; X_1, X_2)$ may not be zero, it is nevertheless possible for Alice to guarantee that the mutual information between any individual message and any two transmitted symbols is zero. That is, for any distinct $i, j, k \in \{1, 2, 3\}$, it follows that

$$\begin{aligned} I\left(M_i; X_1, X_2\right) &= H\left(X_1, X_2\right) - H\left(X_1, X_2 \mid M_i\right) \\ &= H\left(X_1, X_2\right) - H\left(M_j + M_k, 2M_j + 4M_k\right) \\ &= H\left(X_1, X_2\right) - 2\log\left|\mathsf{F}_{11}\right| \\ &\le H\left(X_1\right) + H\left(X_2\right) - 2\log(11) = 0 \end{aligned} \tag{12}$$

We stress that the information that Eve *can* obtain in this situation (which involves only linear combinations of Alice's messages) is largely trivial, and cannot in general be used to decode or decipher any meaning.

A key and, to our knowledge, unique advantage of our method is that it provides improved security as the bandwidth of the transmission increases. Indeed, as q increases, Alice is afforded more bandwidth which, because of the $\eta = 1$ communication efficiency, increases the data rate in her link with Bob while simultaneously improving the security by expanding the size of the blind region $\boldsymbol{\Omega}$. This simultaneous improvement in security and data rate has never previously been realized in wireless systems.

3.3.5. Analysis of the security scheme

Next, we evaluate the absolute security approach using model-driven analysis. Since our method leverages antenna's frequency-dependent minima and coding to create blind regions, we examine the security performance when different types of antenna are employed. The first set of antennas features a fixed main lobe direction and frequency-dependent minima. The selected antennas in this category include a linear phased array and a parabolic dish. Next, we show that not all antennas are suitable for employing the proposed absolute security approach, especially for antennas without pronounced minima, such as the horn antenna.

3.3.5.1 Phased Array and Parabolic Dish

In this subsection, we consider two specific antenna geometries to provide concrete illustrations of the ideas that underlie our security protocol. One of these is a 16-element linear phased array, in which each element is a vertically polarized point dipole emitter, and the elements are spaced along a horizontal line by half of the center wavelength ($\lambda = 1.5$ mm in our simulations). The other is a parabolic dish antenna, with a diameter of 16 mm and a focal length of 10 mm, emitting vertically polarized radiation with a directional gain of 30.5 dBi at a frequency of 200 GHz. The phased array configuration is representative of steerable antennas that are commonly employed in today's millimeter-wave Wi-Fi and 5G standards, while the parabolic dish has often been employed in backhaul and other fixed broadband applications. In both cases, these antenna configurations scale naturally into the millimeter-wave and terahertz range, and have been employed for such high-frequency transmissions.

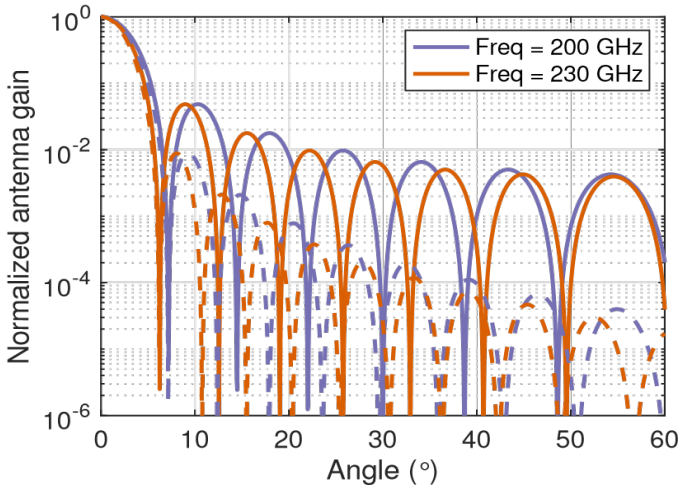

Figure 8. Radiation patterns illustrating how the pronounced minima shift with frequency (solid: phased array, dashed: parabolic dish).

Although radiation patterns are of course three-dimensional, for simplicity we illustrate the essential idea of our approach by only considering a two-dimensional slice (the horizontal plane which is orthogonal to the polarization axis, the H plane), for simplicity. Fig. 8 shows the radiation patterns of the two example antennas, at two different frequencies. In this figure, we observe that, even if Alice uses only the few frequency bands shown in these illustrations, many of Eve's possible locations are ruled out by the fact that she must avoid *all* of the minima of every frequency in Alice's transmission.

Using the phased array and the parabolic dish as described, we calculate the absolute secure angles according to Eq. (8) for a transmission with a center frequency of f_c = 200 GHz, a subchannel bandwidth of w = 1 GHz, and for several values of the parameter P_{AB} which describes Alice's transmit power to Bob. In particular, Alice's transmit power is parameterized by the intensity received by Bob, normalized to the detection threshold discussed above, $P_{AB} = S_{Bob}/(\delta \cdot w)$. For this calculation, Eve is assumed to be at the same distance from Alice as Bob, and Alice adjusts her transmit power so that Bob receives a fixed intensity level S_{Bob} at all frequencies from f_L to f_H.

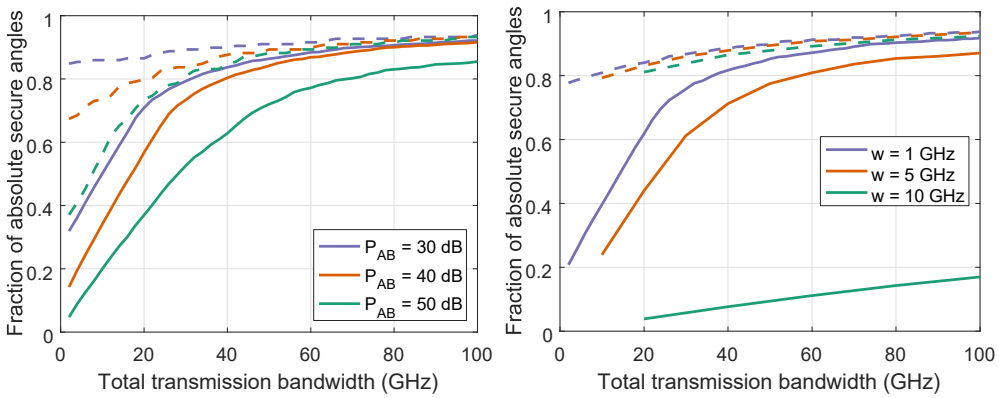

Figure 9. Size of the blind region vs. transmission bandwidth (solid: phased array, dashed: parabolic dish). Left: for several values of Alice's transmit power parameterized by P_{AB}. Right: for different values of subchannel bandwidth w.

Fig. 9(a) illustrates the size of the blind region increase as a function of total bandwidth B, assuming Alice transmits to Bob using the antenna main lobe. For an increasing transmitted bandwidth, as long as Eve is outside of the main antenna lobe (where Bob is located), she is increasingly likely to be within a blind region, i.e., at least one frequency channel is below her detection threshold ($\Gamma > 0$). In Fig. 9(a), the limiting value at large bandwidth is determined by the angular width of the main lobe of the antenna pattern, where Bob is located (and which, by definition, is never within the blind region).

The width of the subchannels also impacts the size of the blind region for a given bandwidth. Using the same setup as in Fig. 9(a) with a fixed transmit power parameterized by $P_{AB} = 35$ dB, Fig. 9(b) illustrates the blind region for different subchannel bandwidths w. Here, we observe that when the width of the subchannel is larger, it is harder to guarantee that the signal intensity across the subchannel is below the detection threshold, so the blind region is smaller.

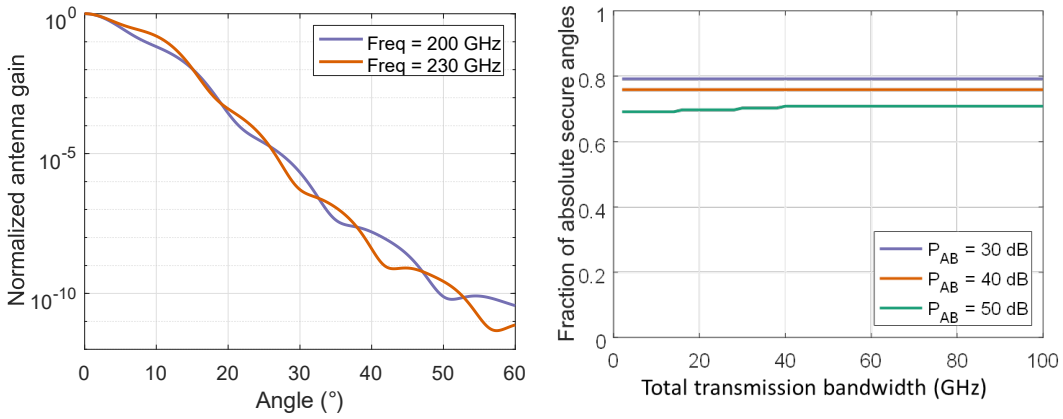

Figure 10. Analysis of a horn antenna. (a) The H-plane radiation pattern from a diagonal horn antenna, computed at two different frequencies. (b) The fraction of secure angles vs. transmission bandwidth, similar to Fig. 9, for the horn antenna.

3.3.5.2 Horn Antenna as a Counterexample

The schemes for implementing secure communications in the case where Eve is in the blind region ($\Gamma > 0$) rely on features of the radiation patterns inherent to the antenna used by Alice, specifically the fact that, in certain broadcast directions, these patterns exhibit pronounced minima (or even analytic zeros), due to destructive interference. It is important to realize that this is not a feature of all antennas. Here, we present a counterexample to illustrate this point: a diagonal horn antenna, another commonly employed design in millimeter-wave and terahertz systems.

As in the cases discussed above, the radiation pattern from this antenna, at a given frequency, is also amenable to direct calculation [43]. In the calculation, we employ a diagonal horn with a horn length of 20 mm and a diagonal aperture of 11 mm. Fig. 10(a) shows one such calculation, in which it is quite clear that the 'minima' between any two side lobes (or between the main lobe and first side lobes) are not very pronounced. Fig. 10(b) shows a blind region calculation analogous to the ones shown in Fig. 9(a), for this horn antenna. This result demonstrates that the blind region does not grow with increasing transmission bandwidth. Since there are no pronounced minima, there is no improvement with increasing spectral bandwidth. As a result, the creation of blind regions is ineffective, if this antenna is employed. Thus, the selection of antenna configuration is a key aspect of implementing the proposed security protocol for the blind region.

3.3.6. Experimental demonstrations

As noted, achieving absolute security requires that the broadcast antenna exhibit pronounced minima whose angular positions vary as a function of frequency. To illustrate the ease with which this can be accomplished, we assemble a link test bed using a horn antenna as the transmitter. Despite the lack of pronounced minima of horn antennas as observed in Fig. 10(a), it is still possible to demonstrate the feasibility of the absolute security system using a horn antenna, with suitable modification.

3.3.6.1 Widely spaced channels

As illustrated by the schematic in Fig. 11(a), we can place a focusing optic (a dielectric lens) in front of the horn, and focus its output onto a diffracting object, in this case a 4mm-wide metal beam block. The far-field diffraction pattern from this illuminated beam block exhibits a strong maximum on the optic axis (the main lobe, at $\theta = 0$) and a pronounced minimum due to destructive interference at a non-zero angle. Fig. 11(a) includes an illustration of the far-field radiation pattern of the setup at one of the three frequencies employed in the measurements (200 GHz), computed using finite element simulations. This clearly shows the pronounced minimum at a small angle, followed by a subsidiary maximum (first side lobe) at a larger angle on either side of the main lobe. We note that the first side lobes peak within 10 dB of the main lobe, for all three frequencies. Thus, an eavesdropper outside of the main lobe is easily able to detect signals in the individual side lobes, but cannot decode any information from signals at the angles of the minima. Because these three minima do not coincide with each other, they collectively form a substantial (though not complete) blind region for angles outside of the main lobe.

To demonstrate the blind region, we perform the experiments employing a frequency multiplier chain in order to generate modulated signals (on-off keying at 1 Gb/sec) at the three widely spaced frequencies (100, 200, and 400 GHz). The modulated data stream is broadcast from the emitter horn antenna, and the bit error rate is measured vs. angle. Fig. 11(b) shows the measured bit error

rates (BER) as a function of angle for each of the three frequencies. Eye diagrams are shown for a representative angle of θ =8.5° where an eavesdropper could be located. This configuration, using only three channels, creates blind regions for 1.6° < θ < 2.0° and θ > 3.4° (indicated by the orange bars along the horizontal axis).

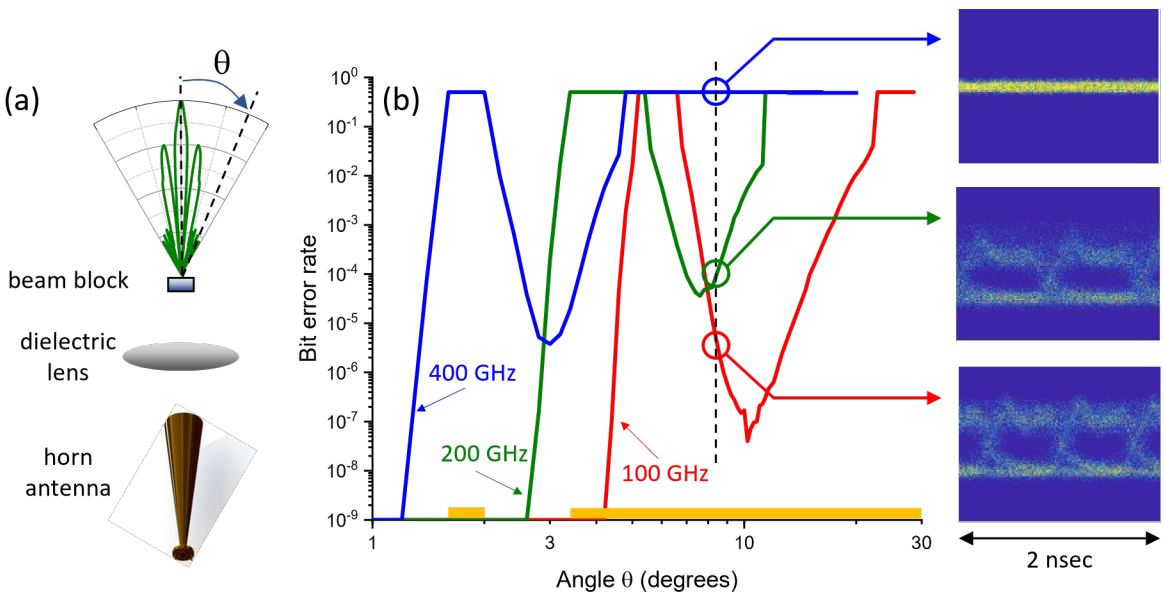

Figure 11. Experimental realization of absolute security using widely spaced channels. (a) A schematic of the experimental setup. (b) Bit error rate vs. angle for each of the three frequencies used in the experiments. Eye diagrams are shown for a representative angle.

At $\theta = 0^\circ$ (Bob's location), we find BER $< 10^{-9}$ at all three frequencies (note that this location is not shown in Fig. 11(b) because the horizontal axis is plotted on a log scale). As θ increases, each frequency band passes through the minimum of the radiation pattern, where the BER increases to 0.5 (i.e., it is impossible to tell the difference between a '0' and a '1'). As θ increases further, the first side lobe maximum is reached, and the BER again falls to a relatively low value, before once again increasing as the angle increases beyond the edge of the diffracted beam pattern. Eye diagrams for the three frequencies are shown for a representative angle of $\theta = 8.5^\circ$ where an eavesdropper could be located. The eye diagrams unambiguously demonstrate that an eavesdropper at this location receives information in only two of the three bands.

Based on the experiments, the blind regions (i.e., the angular locations where at least one frequency is below detection) are indicated by the orange bars along the horizontal axis in Fig. 11(b). This configuration, using only three channels, creates blind regions for $1.6^\circ < \theta < 2.0^\circ$ and $\theta > 3.4^\circ$. Even though only three channels are employed, we nevertheless induce a substantial (though not complete) blind region. These first results have been presented at the 2022 IEEE Conference on Communications and Network Security [49].

3.3.6.2 Adjacent channels

A second set of experiments have been performed at AFRL facilities by a Brown University PhD student who spent the summer of 2022 visiting the Information Directorate as a summer intern. Here, we present the results of those measurements. The goal of that measurement campaign was to establish the concept of a blind region using a more realistic point-to-point communication system. In contrast to the above table-top demonstration (which employed three very widely spaced and relatively narrow (~1 GHz) channels), these second set of measurements used a single continuous frequency band (roughly 195 – 205 GHz) which was subdivided into 41 adjacent channels of 0.240 GHz width to mimic an OFDM transmission system. Due to the limitations of the experimental apparatus, it was necessary to test each channel individually (rather than all at once), and then compile the results to represent a hypothetical multi-channel broadcast. We engineered a transmitter antenna configuration similar to that shown in Fig. 11(a) above, except that the diffraction pattern was formed using a metallic grating, in order to ensure that the radiation patterns of each channel exhibited several side lobes (not just one, as in the case of Fig. 11). We measured bit error rates and SNR for each of the 41 channels over a wide angular range. A given angular location is in the blind region if at least one of the employed channels exhibits a poor bit error rate (greater than 20% errors). Based on our measurements, we extract the size of the blind region as a function of the number of sub-channels included in a hypothetical multi-channel broadcast (ranging from just one, the center frequency at 200 GHz, all the way up to the entire 41-channel band). Fig. 12 shows how this blind region grows with the number of channels. This monotonic growth exhibits the same characteristic behavior as observed in our model calculations (see Fig. 9), and confirms the efficacy of the absolute security approach discussed above. We note that the step-like behavior observed here results from the fact that the broadcast power was not equal in all channels, due to the frequency-dependent efficiency of the multiplier chain used to produce the 200 GHz radiation. A modified calculation which accounts for this non-uniform broadcast power (not shown here) reproduces the step-like behavior of the growth of the blind region accurately. These results are currently being prepared for publication.

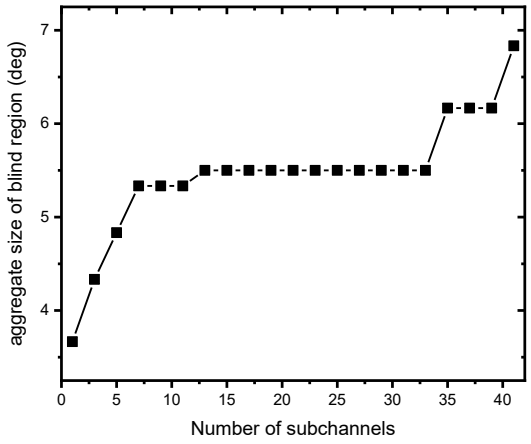

Figure 12. The size of the blind region as a function of the number of 0.24-GHz wide channels included in a hypothetical OFDM broadcast at 200 GHz.

3.3.7. Contrast with zero forcing

As a final comment on the absolute security scheme, we contrast our security scheme with a conventional method known as zero-forcing, in which a phased array is engineered to create a minima in the radiation pattern at a specific location in order to thwart an eavesdropper at that location. Our approach is quite distinct from this legacy approach, for several reasons. As detailed below, the blind region in our method is the union of minima over all frequency channels. Thus, we do not need to know the precise location of the eavesdropper, only whether she is located in this blind region (which can realistically encompass a large fraction of the full angular range). Moreover, unlike the case of zero forcing, if Eve fails to measure just one of the frequency channels in our approach, she is unable to decode any of them.

4.0 CONCLUSIONS

Terahertz communications will be an important element of future high-bandwidth wireless communication systems, in both the military and civilian sectors. The wide bandwidth enables new applications that cannot be supported by existing wireless systems. In addition, the directionality of these wireless links provides an inherent improvement in security. Nevertheless, important security threats still exist, including both those that are similar to the familiar threats present at lower frequencies and those that are not. The focus of this research has been to investigate two specific threat models, and to develop effective counter-measures that can readily be implemented without sacrificing reliability or data rate.

5.0 REFERENCES

[1] M. Raboy, *Marconi, the Man Who Networked the World*: Oxford University Press, 2016.

[2] H. Shams and A. Seeds, "Photonics, fiber, and THz wireless communication," *Opt. Photon. News,* **March 2017**, 25-31, 2017.

[3] J. F. O'Hara and D. R. Grischkowsky, "Comment on the veracity of the ITU-R recommendation for atmospheric attenuation at terahertz frequencies," *IEEE Trans. THz Sci. Technol.,* **8**, 372-375, 2018.

[4] C. Wang, B. Lu, C. Lin, Q. Chen, L. Miao, X. Deng, and J. Zhang, "0.34-THz Wireless Link Based on High-Order Modulation for Future Wireless Local Area Network Applications," *IEEE Trans. THz Sci. Technol.,* **4**, 75-85, 2014.

[5] I. Kallfass, F. Boes, T. Messinger, J. Antes, A. Inam, U. Lewark, A. Tessmann, and R. Henneberger, "64 Gbit/s Transmission over 850 m Fixed Wireless Link at 240 GHz Carrier Frequency," *J. Infrared Millimeter THz Waves,* **36**, 221-233, 2015.

[6] Z. Chen, B. Zhang, Y. Zhang, G. Yue, Y. Fan, and Y. Yuan, "220 GHz outdoor wireless communication system based on a Schottky-diode transceiver," *IEICE Electronics Express,* **13**, 20160282, 2016.

[7] J. Ma, R. S. 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**, 89-93, 2018.

[8] R. Shrestha, H. Guerboukha, Z. Fang, E. Knightly, and D. M. Mittleman, "Jamming a terahertz wireless link," *Nature Commun.,* **13**, 3045, 2022.

[9] J. Ma, R. Shrestha, L. Moeller, and D. M. Mittleman, "Channel performance of indoor and outdoor terahertz wireless links," *APL Photon.,* **3**, 051601, 2018.

[10] S. Vuppala, S. Biswas, and T. Ratnarajah, "An analysis on secure communications in millimeter/micro-wave hybrid networks," *IEEE Trans. Commun.,* **64**, 3507-3519, 2016.

[11] Y. Zhu, L. Wang, K.-K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.,* **16**, 3205-3217, 2017.

[12] M. Kim, E. Hwang, and J.-N. Kim, "Analysis of eavesdropping attack in mmWave-based WPANs with directional antennas," *Wireless Netw.,* **23**, 355-369, 2017.

[13] 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**, 2675-2689, 2018.

[14] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," presented at the Proc. IEEE Conf. Commun. Netw. Security (CNS), Florence, Italy, 2015.

[15] J. Ma, J. Adelberg, R. Shrestha, L. Moeller, and D. M. Mittleman, "The effect of snow on a terahertz wireless data link," *J. Infrared Millimeter THz Waves,* **39**, 505-508, 2018.

[16] Y. Yang, M. Mandehgar, and D. Grischkowsky, "THz-TDS characterization of the digital communication channels of the atmosphere and the enabled applications," *J. Infrared Millimeter THz Waves,* **36**, 97-129, 2015.

[17] P. Boronin, D. Moltchanov, and Y. Koucheryavy, "A molecular noise model for THz channels," presented at the IEEE International Conference on Communications (ICC), London UK, 2015.

[18] Z. Fang, M. Hornbuckle, and D. M. Mittleman, "Secure communication channels using atmosphere-limited line-of-sight terahertz links," *IEEE Trans. THz Sci. Technol.,* **12**, 363-369, 2022.

[19] R. Valkonen, "Compact 28-GHz phased array antenna for 5G access," presented at the IEEE/MTT-S International Microwave Symposium (IMS), 2018.
[20] S. Ullah, W.-H. Yeo, H. Kim, and H. Yoo, "Development of 60-GHz millimeter wave, electromagnetic bandgap ground planes for multiple-input multiple-output antenna applications," *Sci. Rep.,* **10**, 8541, 2020.
[21] 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.
[22] K. Sengupta, T. Nagatsuma, and D. M. Mittleman, "Terahertz integrated electronic and hybrid electronic–photonic systems," *Nature Electron.,* **1**, 622–635, 2018.
[23] A. Alexiou, S. Andreev, G. Fodor, and T. Nagatsuma, "THz communications: A catalyst for the wireless future," *IEEE Commun. Mag.,* **58**, 12-13, 2020.
[24] V. Petrov, T. Kürner, and I. Hosako, "IEEE 802.15.3d: First Standardization Efforts for Sub-Terahertz Band Communications toward 6G," *IEEE Commun. Mag.,* **58**, 28-33, 2020.
[25] C. Castro, R. Elschner, T. Merkle, C. Schubert, and R. Freund, "Experimental demonstrations of high-capacity THz-wireless transmission systems for beyond 5G," *IEEE Commun. Mag.,* **58**, 41-47, 2020.
[26] J. Federici and L. Moeller, "Review of terahertz and subterahertz wireless communications," *J. Appl. Phys.,* **107**, 111101, 2010.
[27] B. Peng, K. Guan, A. Kuter, S. Rey, M. Patzold, and T. Kürner, "Channel modeling and system concepts for future terahertz communications: Getting ready for advances beyond 5G," *IEEE Vehicular Tech. Mag.,* **15**, 136-143, 2020.
[28] X. Lu, S. Venkatesh, B. Tang, and K. Sengupta, "Space-time modulated 71-to-76 GHz mm-Wave transmitter array for physically secure directional wireless links," presented at the IEEE International Solid-State Circuits Conference (ISSCC), 2020.
[29] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.,* **54**, 1355-1387, 1975.
[30] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering*: Cambridge University Press, 2011.
[31] A. Cohen and A. Cohen, "Wiretap channel with causal state information and secure rate-limited feedback," *IEEE Trans. Commun.,* **64**, 1192-1203, 2016.
[32] A. Cohen, A. Cohen, and O. Gurewitz, "Secured data gathering protocol for IoT networks," presented at the International Symposium on Cyber Security Cryptography and Machine Learning, 2018.
[33] D. J. Bernstein, T. Lange, and C. Peters, "Attacking and defending the McEliece cryptosystem," presented at the 2nd International Workshop on Post-Quantum Cryptography, 2008.
[34] D. J. Bernstein, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*, D. J. Bernstein, J. Buchmann, and E. Dahmen, Eds.: Springer, 2009, pp. 1-14.
[35] Y. Liang, H. V. Poor, and S. Shamai, *Information Theoretic Security*: Now Publishers, Inc., 2009.
[36] X. Zhou, L. Song, and Y. Zhang, *Physical layer security in wireless communications*: CRC Press, 2013.
[37] A. Cohen, R. G. D'Oliveira, S. Salamatian, and M. Medard, "Network coding-based post-quantum cryptography," *IEEE J. Sel. Areas Info. Theory,* **2**, 49-64, 2021.

[38] S. Hallgren, "Fast quantum algorithms for computing the unit group and class group of a number field," presented at the 37th Annual ACM Symposium on Theory of Computing, 2005.
[39] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Rev.,* **41**, 303-332, 1999.
[40] C. A. Balanis, *Antenna Theory: Analysis and Design*: John Wiley & Sons, 2016.
[41] Y. Ghasempour, C. R. da Silva, C. Cordeiro, and E. W. Knightly, "IEEE 802.11ay: Next-generation 60 GHz communication for 100 Gb/s Wi-Fi," *IEEE Commun. Mag.,* **55**, 186-192, 2017.
[42] T. S. Rappaport, S. Sun, R. Mayzus, H. Zhao, Y. Azar, K. Wang, G. N. Wong, J. K. Schulz, M. Samimi, and F. Gutierrez, "Millimeter wave mobile communications for 5G cellular: It will work!," *IEEE Access,* **1**, 335 – 349, 2013.
[43] S. Cho, G. Chen, and J. P. Coon, "Zero-forcing beamforming for active and passive eavesdropper mitigation in visible light communication systems," *IEEE Trans. Info. Forensics Security,* **16**, 1495–1505, 2020.
[44] N. Anand, S.-J. Lee, and E. W. Knightly, "STROBE: Actively securing wireless communications using zero-forcing beamforming," presented at the Proceedings of IEEE INFOCOM, 2012.
[45] D. Silva and F. R. Kschischang, "Universal weakly secure network coding," presented at the IEEE Information Theory Workshop on Networking and Information Theory, 2009.
[46] A. Cohen, A. Cohen, M. Medard, and O. Gurewitz, "Secure multi-source multicast," *IEEE Trans. Commun.,* **67**, 708–723, 2018.
[47] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Lab. Tech. J.,* **63**, 2135–2157, 1984.
[48] M. Hayashi and R. Matsumoto, "Secure multiplex coding with dependent and non-uniform multiple messages," *IEEE Trans. Info. Theory,* **62**, 2355–2409, 2016.
[49] A. Cohen, R. G. L. D'Oliveira, C.-Y. Yeh, H. Guerboukha, R. Shrestha, Z. Fang, E. Knightly, M. Médard, and D. M. Mittleman, "Absolute security in high-frequency wireless links," presented at the IEEE Conference on Communications and Network Security (CNS), 2022.

6.0 LIST OF ACRONYMS

AFRL	Air Force Research Laboratory
ASK	amplitude shift keying
AWGN	additive white Gaussian noise
BER	bit error rate
dB	decibel
dBi	decibel relative to isotropic
DOD	Department of Defense
EVM	error vector magnitude
FSPL	free space path loss
Gb	gigabit
GHz	gigahertz
ITU-R	International Telecommunications Union – Radiocommunications Sector
OFDM	orthogonal frequency-division multiplexing
QPSK	quadrature phase-shift keying
RH	relative humidity
SNR	signal-to-noise ratio
THz	terahertz
WVAL	water vapor absorption loss