Secure Communication Channels Using Atmosphere-Limited Line-of-Sight Terahertz Links

Zhaoji Fang, Hichem Guerboukha, Rabi Shrestha, Malachi Hornbuckle, Yasith Amarasinghe, and Daniel M. Mittleman, *Fellow, IEEE*

***Abstract*—Terahertz wireless links offer great promise for realizing physical-layer security due to the high directionality and the high path loss. In this work, we investigate the resilience against eavesdropping attacks in a directional terahertz link which exploits the attenuation due to the water vapor absorption resonances for enhanced security. The magnitude of the atmospheric attenuation can be controlled by tuning the carrier frequency relative to the peak of a water vapor absorption line. This idea can be used to thwart an eavesdropper by restricting the broadcast range of the signal. We develop a channel model for an eavesdropping scenario in which an attacker is located along a line-of-sight link. We explore through both experiments and calculations the performance of the terahertz channel, as well as the tradeoff between performance and security. Our results demonstrate the feasibility of limiting the broadcast range by making use of atmospheric conditions, paving the way for a simple yet powerful physical-layer security protocol for the terahertz range.**

***Index Terms*—Broadcast range, security, terahertz (THz) wireless communications, water vapor absorption.**

I. Introduction

TERAHERTZ radiation is promising for future generations of wireless communication technology due to the possibility of ultrahigh data rate and ultralow latency [1], [2]. Compared to the microwave signals used in conventional communication systems, terahertz signals are more directional for a given antenna aperture and attenuate faster with propagation range due to an increase in atmospheric attenuation in addition to the free space path loss, which (for fixed antenna gains) increases dramatically with frequency [3]. Because of these characteristics, terahertz wireless systems present new opportunities to engineer security and resilience against eavesdropping attacks. The issue of security in these future wireless systems has recently become an active research topic [4]–[12], as new vulnerabilities must be considered at these frequencies. For example, scattering a portion of the main lobe enables eavesdropping outside the narrow broadcast sector [4], [8], [10]. The unique characteristics of these broadcasts also enable new countermeasures; for example, by combining the high directionality with multiple-input and multiple-output (MIMO) technology, splitting the link into multiple non-line-of-sight propagation paths could minimize the size of an insecure region, preventing an eavesdropper from detecting the signals [13]. Another key characteristic of terahertz propagation is related to atmospheric attenuation [14]. This attenuation can be quite large, but is very strongly frequency-dependent, especially at frequencies that are close to the absorption resonances of the water vapor molecule [15]–[19]. Using this idea, researchers have proposed that additional security protocols which account for the range of the intended broadcast can render eavesdropping challenging, for an eavesdropper who is farther away [20]–[22].

In this work, we describe the first experimental investigation of this possibility with quantitative metrics for achievable security. In addition to power measurements, here we also measure the constellation diagram of the channel to demonstrate the performance of a practical communication system. We consider a threat model in which Alice (the transmitter) is sending a signal to Bob (the intended receiver) via a direct line-of-sight link. Meanwhile, Eve (an eavesdropper), located along the same optical axis, but farther away, attempts to intercept the signals that propagate past Bob [Fig. 1(a)]. This positioning can be advantageous for Eve, as it avoids the possibility that she may block some portion of Bob's signal and thereby raise an alarm [8], [23]. However, if Alice is aware of the possibility that Eve may be positioned behind Bob, we show that she can engineer the properties of her broadcast to counter Eve's attack. We build a channel model to evaluate the effectiveness of this strategy and its impact on the channel capacity as well as on the secrecy capacity of the link. Our experimental results, obtained using a humidity-controlled chamber, are in good agreement with this model.

II. Channel Loss

Our approach is based on computing both the free-space path loss (FSPL) and the loss due to water vapor absorption resonances (WVAL). In general, the WVAL grows faster than the FSPL after sufficient propagation distance. Taking both

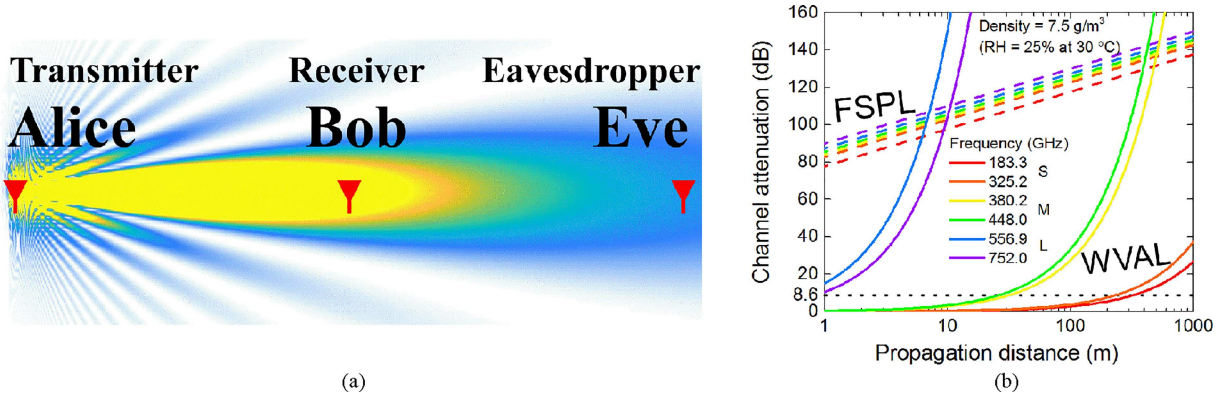
Manuscript received December 1, 2021; revised April 19, 2022; accepted May 13, 2022. Date of publication May 30, 2022; date of current version July 5, 2022. This work was supported in part by the US Air Force Research Laboratory's Information Directorate and in part by National Science Foundation. *(Corresponding author: Daniel M. Mittleman.)*

Zhaoji Fang, Hichem Guerboukha, Rabi Shrestha, Malachi Hornbuckle, and Daniel M. Mittleman are with Brown University, Providence, RI 02912 USA (e-mail: zhaoji_fang@brown.edu; hichem_guerboukha@brown.edu; rabi_shrestha@brown.edu; malachi_hornbuckle@brown.edu; daniel_mittleman@brown.edu).

Yasith Amarasinghe was with the Brown University, Providence, RI 02912 USA. He is now with the Institute of Microelectronics, A∗STAR, Singapore 138634 (e-mail: yasith_amarasinghe@alumni.brown.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TTHZ.2022.3178870.

Digital Object Identifier 10.1109/TTHZ.2022.3178870



(a) (b)

Fig. 1. (a) In the threat model, Alice is the transmitter, Bob the receiver, and Eve represents the eavesdropper. The yellow region represents the insecure region where SNR is high enough to build a successful link, whereas the blue represents the secure region where SNR is too low to eavesdrop. (b) Channel attenuation versus propagation distance with selected frequencies corresponding to the peaks of water vapor absorption lines, in an atmosphere with water vapor density of 7.5 g/m^3 (i.e., relative humidity of 25%) and temperature of 30 °C.

the FSPL and the WVAL into account, we demonstrate that Alice can manipulate the channel performance by tuning the carrier frequency of her transmission, relative to the frequency channel capacity, Alice can reduce the insecure region where eavesdropping is feasible. This data-rate-vs.-security tradeoff is a common feature of nearly all physical-layer security strategies [20], leading to an optimization challenge that must take into account other higher layer considerations such as the possibility of encryption, which are beyond the scope of this work. Nevertheless, our results provide key input to these considerations by offering a quantitative analysis of the tradeoff.

To evaluate the security of the channel, we consider the security model shown in Fig. 1(a). We assume that both Bob (receiver) and Eve (eavesdropper) are located at the peak of the main lobe from Alice's (transmitter) antenna and that Eve sits further from Alice than Bob (so $d_{\text{Eve}}/d_{\text{Bob}} > 1$). For simplicity, we ignore the blockage of the signal to Eve by Bob. Although models exist to account for such blockage, in our analysis their effect is merely to shift the results by the fraction of blocked radiation, so including these effects would distract from the main point of this discussion. We assume that Eve has the same detector as Bob. We also neglect atmospheric turbulence and scintillation effects [24], and assume that the atmospheric conditions are clear and uniform throughout the entire communication region [14], [25]. Thus, the channel performance for both Bob and Eve is determined by the output power of Alice's transmitter, the antenna gains, and the losses due to the channel which include both FSPL and WVAL. Both the FSPL and the WVAL depend on the distance and the selected carrier frequency of Alice's transmission. In Fig. 1(b), we evaluate several of the most prominent water vapor absorption lines in the range from 100 to 800 GHz to compare the FSPL and the WVAL. The FSPL is determined by the Friis transmission formula [26]:

$$\text{FSPL} = 20\left(\log d - \log f + \tfrac{1}{2}\log\tfrac{c^2}{A_r A_t}\right)(\text{dB}) \tag{1}$$

where A_r is the effective area of the receiver, A_t is the effective area of the transmitter, f is the frequency, c is the free-space light speed, and d is the distance of the wireless link. We note that A_r and A_t also depends on frequency. The slope of the FSPL is:

$$\frac{\partial \text{FSPL(dB)}}{\partial(\log d)} = 20\ \text{dB/decade} \tag{2}$$

Meanwhile, the WVAL grows exponentially as a function of the distance according to Beer's law [27]:

$$\text{WVAL} = e^{G_c(f)\cdot \text{RH}\cdot d} = 4.3 G_c(f)\cdot \text{RH}\cdot d\,(\text{dB}) \tag{3}$$

where $G_c(f)\cdot \text{RH}$ is the absorption coefficient, $G_c(f)$ following the van Vleck Weisskopf lineshape function around an absorption peak [28] and RH the relative humidity in the terahertz beam path. Note that for a broadband signal, an integration of $G_c(f)$ multiplied by the power spectrum of the signal is required to calculate the WVAL, assuming that the spectrum distortion is compensated by adaptive equalization filters at the receiver. In that case, the WVAL is less sensitive to the carrier frequency compared to the case narrowband signals. Additional frequency division multiplexing techniques are required to make the frequency tuning effective for security. The WVAL is calculated using the standard atmospheric ITU model, which has been shown to be reasonably accurate for frequencies below 500 GHz [18], [29]. Note that WVAL(dB) may not grow linearly as a function of the relative humidity for high humidity circumstances, which is beyond the scope of the experiment in this article [27]. The slope of the WVAL as a function of distance can be written as follows:

$$\frac{\partial \text{WVAL(dB)}}{\partial(\log d)} = \frac{\partial\left(10\log e^{\alpha d}\right)}{\partial(\log d)} = \frac{\text{WVAL}}{0.43}\,(\text{dB/decade}) \tag{4}$$

which is proportional to the WVAL itself on a log scale. Thus, the WVAL increases more rapidly with distance than the FSPL if the WVAL is greater than $0.43 \times 20 =$ 8.6 dB [dotted line in Fig. 1(b)].

We choose several most significant water vapor absorption peaks from 100 to 800 GHz to numerically illustrate FSPL and WVAL as a function of the propagation distance. As depicted in Fig. 1(b), the rise of WVAL is more significant than the rise of FSPL beyond the threshold of 8.6 dB. Such rise would enlarge the difference of channel loss between Bob and Eve, which enhances the security. The corresponding threshold distances

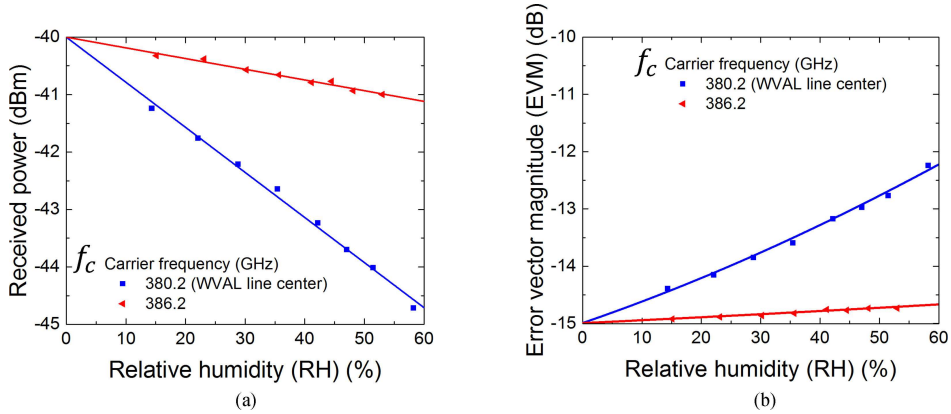


Fig. 2. Experimental results (dots) and fitted calculations (lines) of a 4-m line-of-sight wireless link inside a humidity chamber at 51.5 °C. (a) Received power decreases linearly as a function of the relative humidity of the atmosphere. This phenomenon results in a higher slope when transmitting closer to the WVAL line center. (b) EVM of the constellation diagram of QPSK modulation at a symbol rate of 3.8 GBaud also decreases linearly as a function of the relative humidity of the atmosphere.

range from ∼100 m for small intensity WVAL peaks (183.3 and 325.2 GHz), ∼10 m for medium intensity WVAL peaks (380.2 and 448.0 GHz), to ∼1 m for large intensity WVAL peaks (556.9 and 752.0 GHz). Depending on the range of communication distance for a specific application scenario, we can choose the communication system that operates around the corresponding WVAL line center to reach the desired security level. For our experiments, we employ a 4-m link, and therefore we choose to operate our link near the 380.2 GHz WVAL line center.

III. Channel Model

We now build a channel model to characterize the effect of WVAL and FSPL losses on the performance of the communication link. Before reaching either receiver, the terahertz signal is attenuated by both the FSPL and the WVAL. The received power of the signal P_{r} can be described as follows

$$P_{\mathrm{r}} = \frac{P}{\mathrm{WVAL}\cdot\mathrm{FSPL}} \tag{5}$$

For convenience, we include the antenna gain in the transmitted power from Alice P, and assume P is constant and independent of frequency. Based on [30], we propose a channel model which separate the total noise into sources from the transmitter and the receiver, ignoring the molecular noise [31], small scale fading [32], and interference from other users [33].

$$N = \frac{N_{\mathrm{Tx}}}{\mathrm{WVAL}\cdot\mathrm{FSPL}} + N_{\mathrm{Rx}} \tag{6}$$

N is the effective total noise power measured by the receiver. N_{Tx} and N_{Rx} are the effective noise powers originating from the transmitter and the receiver, respectively. Note that this noise model only accounts for the channel attenuation; that is, the antenna gain is included in N_{Tx} and N_{Rx}. We also assume all the noise is uncorrelated additive white Gaussian noise. Thus, the signal-to-noise ratio (SNR) at the receiver is derived as follows.

$$\mathrm{SNR} = \frac{P_{\mathrm{r}}}{N} = \frac{P}{N_{\mathrm{Tx}} + N_{\mathrm{Rx}}\cdot\mathrm{WVAL}\cdot\mathrm{FSPL}} \tag{7}$$

The introduction of the WVAL can greatly reduce the power of the received signal, especially for Eve since her distance from Alice is greater than d_{Bob}. Therefore, Alice can enhance the security of the wireless link by selecting her broadcast frequency appropriately. Her choice depends on d_{Bob} and d_{Eve}, as well as on the relative humidity and temperature of the environment. We show later in Fig. 5 that Alice's selection of a broadcast frequency involves a tradeoff between data rate and the secrecy capacity of the channel.

IV. Experimental Results

We next validated this channel model through experiment. In our experiment, the signal from Alice to Bob is transmitted through a line-of-sight terahertz wireless link inside a humidity chamber of the dimension $W \times D \times H = 1.8 \times 0.5 \times 0.5\mathrm{m}^3$ with a folded path to achieve a 4-m range. The chamber allows us to increase the temperature up to 51.5 °C and to vary the relative humidity from 14%–58%, with temperature fluctuation of ±0.5 °C and relative humidity fluctuation of ±1%. We use two 4-inch-diameter Teflon lenses inside the chamber to boost the overall channel gain. A pair of mixers are used to generate and detect terahertz signals with QPSK modulation at a symbol rate of up to 3.8 GBaud. In order to minimize the intersymbol interference due to signal distortion [34], root-raised cosine filters are used at both the transmitter and the receiver, and an adaptive equalization filter is used at the receiver. We use the error vector magnitude (EVM) of the constellation diagram as the metric for our measurements, since it provides a good estimation of the bit error rate (BER) of QPSK modulation when $\mathrm{EVM} < -10\mathrm{dB}$ [35]. Since we average a large number (10^5) of symbols, it is safe to assume that $\mathrm{EVM(dB)} = -\mathrm{SNR(dB)}$ [36].

In Fig. 2, we show the received power P_{r} and the QPSK EVM which both decay almost linearly as a function of the relative humidity (RH). This demonstrates that WVAL could have a significant effect for a 4-m terahertz link. The slope of the received power versus RH can be explained by a modified equation from (5):

$$P_{\mathrm{r}}\,(\mathrm{dBm}) = P(\mathrm{dBm}) - \mathrm{FSPL(dB)} - \underset{\mathrm{RH}=100\%}{\mathrm{WVAL(dB)}}\,\mathrm{RH} \tag{8}$$

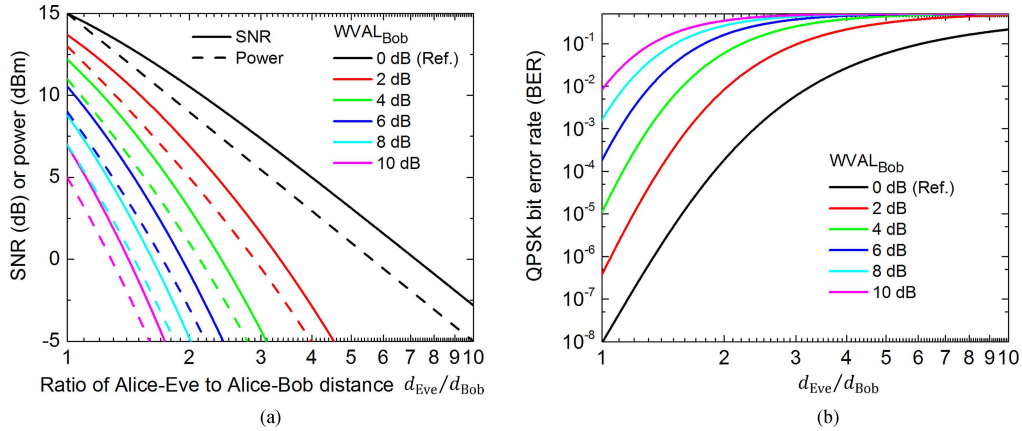


Fig. 3. Eavesdropping performance for Eve positioned behind Bob taking Alice as a reference, including (a) received power, signal-to-noise ratioSNR_{Eve}, and (b) bit error rate for QPSK modulation BER_{Eve}. We assume that the water vapor attenuation between Alice and Bob is tuned by changing the carrier frequency, and the output power of Alice is fixed. Note that we include WVAL $= 0$ dB as a reference for lower frequencies (radio or microwave), in which the water vapor attenuation could be ignored compared to the FSPL.

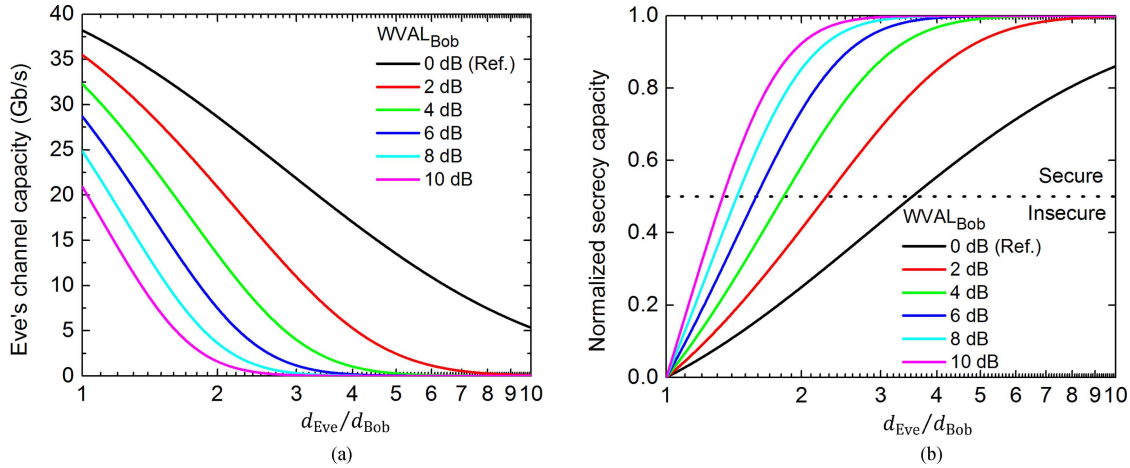


Fig. 4. Eavesdropping performance including (a) channel capacity and (b) normalized secrecy capacity.

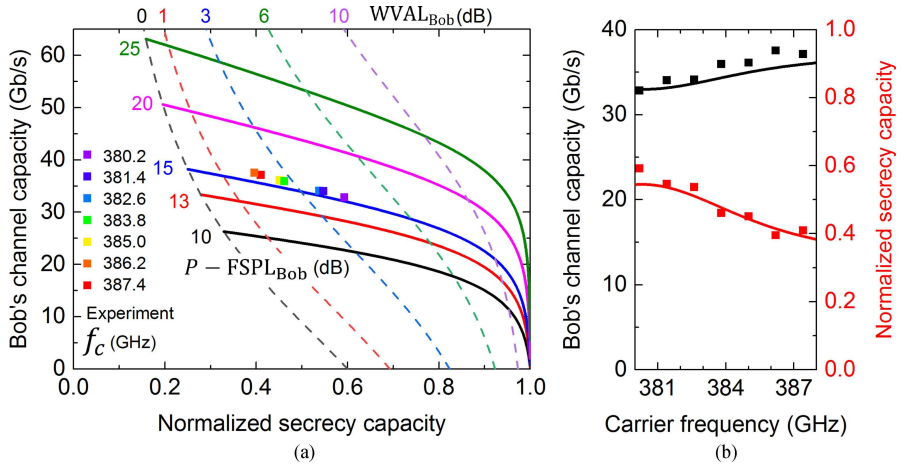


Fig. 5. (a) Tradeoff between the Alice-Bob channel capacity and the normalized secrecy capacity assuming $d_{\text{Eve}}/d_{\text{Bob}} = 2$. For the solid curves, we assume a fixed $P - \text{FSPL}_{\text{Bob}}$ and tune theWVAL_{Bob}, and for the dashed curves vice versa. The dots represent the experimental results of tuning the carrier frequency relative to the WVAL line at 380.2 GHz at RH $= 50\%$. (b) Dots represent the experimental measurements, while the curves represent the numerical calculations.

TABLE I
SLOPE OF POWER AND EVM VERSUS RH

f_c	∂P_r / ∂RH	∂EVM / ∂RH
380.2 GHz	−7.8 dB/100 %	−5.2 dB/100 %
386.2 GHz	−1.8 dB/100 %	−0.6 dB/100 %

where dBm is the power in dB with reference to 1 mW. As listed in Table I, the slope with carrier frequency f_c exactly at the WVAL line center (380.2 GHz) is much higher than the slope at $f_c = 386.2$ GHz, which is further away from the line center. Thus, the carrier frequency serves as a tunable parameter to vary the WVAL.

In Fig. 2(b), the slope of EVM versus RH is only around a half of the slope of power versus RH for both frequencies. We can understand this using a first-order approximation of (7) for WVAL close to 0 dB

$$\mathrm{EVM(dB)} = \underset{\mathrm{RH}=0}{\mathrm{EVM(dB)}} + \frac{N_{\mathrm{Rx}}\mathrm{FSPL}}{N_{\mathrm{Tx}}+N_{\mathrm{Rx}}\mathrm{FSPL}} \underset{\mathrm{RH}=100\%}{\mathrm{WVAL(dB)}}\,\mathrm{RH} \tag{9}$$

If $N_{\mathrm{Tx}} = 0$, the slope of EVM versus RH is the same as the slope of power versus RH. That is the case for most situations at lower frequencies (radio or microwave), in which the transmitter noise is usually low enough to be ignored, compared to the other source of noise (e.g., small-scale fading, interference of other nearby users, etc.) [30]. Here, the transmitter noise is not negligible using the current technology of terahertz mixers, resulting in a slope of EVM versus RH lower than the power slope. The difference in slopes allows us to estimate a value for the quantity $N_{\mathrm{Rx}} \cdot \mathrm{FSPL}/(N_{\mathrm{Tx}} + N_{\mathrm{Rx}} \cdot \mathrm{FSPL})$. By fitting the experimental data with (8-9), we get $N_{\mathrm{Tx}} : N_{\mathrm{Rx}} \cdot \mathrm{FSPL} \approx 1$. In other words, the impact of the transmitter noise and the receiver noise on EVM are comparable. On top of that, we can also estimate that the SNR of the output signal at the transmitter P/N_{Tx} is around 18 dB (i.e., 3 dB above $\mathrm{SNR}_{\mathrm{RH}=0}$).

V. LINK SECURITY

Next, we investigate numerically the impact of Alice's frequency tuning on link security. We evaluate an illustrative example situation, where we assume that Alice has a fixed constant output power for all frequencies, and Bob can achieve $P_r = 15$ dBm and SNR $= 15$ dB when WVAL $= 0$ dB (no water vapor). Using (5-7), we compute the effect on Eve's received power and SNR as a function of her distance from Alice. Note that the calculation does not depend on d_{Bob}. Fig. 3(a) shows that as she moves further from Alice, her power decreases, as does her SNR. Additionally, the slopes of SNR and power versus distance increase for increasing values of WVAL, which indicates that the rate of attenuation increases with WVAL. Similarly, Fig. 3(b) shows that Eve's BER increases faster as Alice increases the $\mathrm{WVAL}_{\mathrm{Bob}}$ by varying her broadcast frequency closer to the resonance line center.

We can also explore the enhancement of security by simulating Eve's channel capacity [37] and Bob's normalized secrecy capacity as defined in [8] as we do in Fig. 4. By increasing WVAL, the descent rate of Eve's channel capacity versus distance could be enhanced as depicted in Fig. 4(a), while the normalized security capacity increases more rapidly as demonstrated in Fig. 4(b). As in [8], we assume that the channel is secure when the normalized secrecy capacity is greater than an arbitrary value of 0.5 [dotted line in Fig. 4(b)]. By increasing the WVAL from 0 to 10 dB, the insecure range is reduced from 3.5 d_{Bob} to 1.3 d_{Bob}. At the same time, Bob's channel capacity is decreased from 38 to 21 Gbps. If Alice knows Bob's position, she can effectively vary her broadcast parameters such that eavesdropping fails at a given distance greater than Bob's. The threshold distance for secure communications can be reduced at the cost of Bob's channel capacity.

In Fig. 5, we parameterize the tradeoff between the channel capacity and the normalized secrecy capacity by considering an example case where the Alice-Eve distance is twice the Alice-Bob distance ($d_{\mathrm{Eve}}/d_{\mathrm{Bob}} = 2$). As depicted by the solid curves (assuming a fixed $P - \mathrm{FSPL}_{\mathrm{Bob}}$ and a tunable $\mathrm{WVAL}_{\mathrm{Bob}}$), a fairly modest sacrifice in channel capacity can produce a very significant improvement in normalized secrecy capacity, and therefore this approach to security is highly promising. The tradeoff is accomplished by varying the carrier frequency f_c close to the WVAL line at 380.2 GHz [dots in Fig. 5(a)]. The dynamic range of the tradeoff can be further improved at some of the WVAL lines at higher frequencies. Based on the requirement of normalized secrecy capacity for a specific application, Alice can decide the $\mathrm{WVAL}_{\mathrm{Bob}}$ [dashed curves in Fig. 5(a)] by choosing an appropriate f_c as well as and appropriate modulation scheme. For example, by varying the carrier frequency from 386.2 to 380.2 GHz, we increased the normalized secrecy capacity from 0.4 to 0.6, at the cost of channel capacity reduction from 38 to 33 Gbps (13% reduction). Our measured values for channel capacity and secrecy capacity match well with the channel model described above [Fig. 5(b)].

VI. CONCLUSION

We propose a physical-layer security protocol to restrict the range of the insecure region where an eavesdropper can successfully attack the channel. Our strategy relies on the intrinsic attenuation of the atmosphere, and a frequency tuning capability for Alice. Based on a threat model where Alice, Bob, and Eve are located along with a line-of-sight link, we demonstrate that the exponential growth of WVAL as a function of distance can be used to thwart Eve if she is outside the broadcast range. Alice can control this effect by tuning her carrier frequency relative to the peak of a nearby water vapor absorption line center. We explore the tradeoff between the channel capacity and the normalized secrecy capacity, which results from Alice's frequency tuning. For our experiment, we find that, at the cost of around 13% of the channel capacity, Alice can enhance the normalized secrecy capacity from 0.4 to 0.6. Our results demonstrate the feasibility of this simple and versatile approach to physical-layer security in terahertz wireless communications. In practical terahertz communication systems, besides the direction of the intended receiver for beamforming, the distance should also be taken into consideration to optimize the security of the broadcast through tuning the carrier frequency.

REFERENCES

[1] H. J. Song and T. Nagatsuma, "Present and future of terahertz communications," *IEEE Trans. Terahertz Sci. Technol.*, vol. 1, no. 1, pp. 256–263, Sep. 2011.

[2] K. Sengupta, T. Nagatsuma, and D. M. Mittleman, "Terahertz integrated electronic and hybrid electronic–photonic systems," *Nature Electron.*, vol. 1, pp. 622–635, 2018.

[3] J. Ma, R. Shrestha, L. Moeller, and D. M. Mittleman, "Invited article: Channel performance for indoor and outdoor terahertz wireless links," *APL Photon.*, vol. 3, 2018, Art. no. 051601.

[4] D. Steinmetzer, J. Chen, J. Classen, E. Knightly, and M. Hollick, "Eavesdropping with periscopes: Experimental security analysis of highly directional millimeter waves," in *Proc. IEEE Conf. Commun. Netw. Secur.*, 2015, pp. 335–343.

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

[6] Y. Zhu, L. Wang, K. K. Wong, and R. W. Heath, "Secure communications in millimeter wave ad hoc networks," *IEEE Trans. Wireless Commun.*, vol. 16, no. 5, pp. 3205–3217, May 2017.

[7] 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.*, vol. 17, no. 4, pp. 2675–2689, Apr. 2018.

[8] J. Ma *et al.*, "Security and eavesdropping in terahertz wireless links," *Nature,* vol. 563, pp. 89–93, 2018.

[9] Z. Liu, J. Liu, Y. Zeng, and J. Ma, "Covert wireless communication in IoT network: From AWGN channel to THz band," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3378–3388, Apr. 2020.

[10] T. Troha, T. Ostatnický, and P. Kužel, "Improving security in terahertz wireless links using beam symmetry of vortex and Gaussian beams," *Opt. Express,* vol. 29, pp. 30461–30472, 2021.

[11] C.-Y. Yeh, Y. Ghasempour, Y. Amarasinghe, D. M. Mittleman, and E. W. Knightly, "Security in terahertz WLANs with leaky wave antennas," in *Proc. 13th ACM Conf. Secur. Privacy Wireless Mobile Netw.*, 2020, pp. 317–327.

[12] C. Liaskos *et al.*, "A novel communication paradigm for high capacity and security via programmable indoor wireless environments in next generation wireless systems," *Ad Hoc Netw.,* vol. 87, pp. 1–16, 2019.

[13] V. Petrov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Exploiting multipath terahertz communications for physical layer security in beyond 5G networks," in *Proc. IEEE INFOCOM Conf. Comput. Commun. Workshops*, 2019, pp. 865–872.

[14] J. F. Federici, J. Ma, and L. Moeller, "Review of weather impact on outdoor terahertz wireless communication links," *Nano Commun. Netw.*, vol. 10, pp. 13–26, 2016.

[15] R. Wang, Y. Mei, X. Meng, and J. Ma, "Secrecy performance of terahertz wireless links in rain and snow," *Nano Commun. Netw.*, vol. 28, 2021, Art. no. 100350.

[16] Y. Yang, M. Mandehgar, and D. R. Grischkowsky, "Understanding THz pulse propagation in the atmosphere," *IEEE Trans. Terahertz Sci. Technol.*, vol. 2, no. 4, pp. 406–415, Jul. 2012.

[17] 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, Terahertz Waves,* vol. 36, pp. 97–129, 2015.

[18] 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. Terahertz Sci. Technol.*, vol. 8, no. 3, pp. 372–375, May 2018.

[19] R. Sczech, D. Stock, R. Bornemann, and P. Haring Bolívar, "Experimental evidence for cm propagation lengths of long-range guided terahertz radiation by thin layers of water," *Appl. Phys. Lett.,* vol. 103, 2013, Art. no. 031106.

[20] W. Gao, Y. Chen, C. Han, and Z. Chen, "Distance-Adaptive absorption-peak hopping (DA-APH) modulation for terahertz covert communications," in *Proc. IEEE Glob. Commun. Conf.*, 2019, pp. 1–6.

[21] Z. Fang and D. M. Mittleman, "Secure communication channels using atmosphere-limited line-of-sight terahertz links," in *Proc. 45th Int. Conf. Infrared, Millimeter, Terahertz Waves*, 2020, pp. 1–2.

[22] Z. Fang and D. M. Mittleman, "Physical-layer security using atmosphere-limited line-of-sight terahertz links," in *Proc. CLEO Sci. Innovations*, 2021, Paper JW1A.18.

[23] V. Petrov, M. Komarov, D. Moltchanov, J. M. Jornet, and Y. Koucheryavy, "Interference and SINR in millimeter wave and terahertz communication systems with blocking and directional antennas," *IEEE Trans. Wireless Commun.*, vol. 16, no. 3, pp. 1791–1808, Mar. 2017.

[24] M. Taherkhani, Z. G. Kashani, and R. A. Sadeghzadeh, "On the performance of THz wireless LOS links through random turbulence channels," *Nano Commun. Netw.,* vol. 23, 2020, Art. no. 100282.

[25] 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, Terahertz Waves,* vol. 39, pp. 505–508, 2018.

[26] J. A. Shaw, "Radiometry and the friis transmission equation," *Amer. J. Phys.*, vol. 81, pp. 33–37, 2013.

[27] Y. Yang, M. Mandehgar, and D. Grischkowsky, "Determination of the water vapor continuum absorption by THz-TDS and molecular response theory," *Opt. Exp.,* vol. 22, pp. 4388–4403, 2014.

[28] J. H. Van Vleck and V. F. Weisskopf, "On the shape of collision-broadened lines," *Rev. Modern Phys.,* vol. 17, 1945, Art. no. 227.

[29] "Attenuation by atmospheric gases," ITU-R Rec. P. 676-9, International Telecommunication Union, 2012.

[30] H. Suzuki, T. V. A. Tran, I. B. Collings, G. Daniels, and M. Hedley, "Transmitter noise effect on the performance of a MIMO-OFDM hardware implementation achieving improved coverage," *IEEE J. Sel. Areas Commun.*, vol. 26, no. 6, pp. 867–876, Aug. 2008.

[31] P. Boronin, D. Moltchanov, and Y. Koucheryavy, "A molecular noise model for THz channels," in *Proc. IEEE Int. Conf. Commun.*, 2015, pp. 1286–1291.

[32] E. N. Papasotiriou, A.-A. A. Boulogeorgos, K. Haneda, M. F. de Guzman, and A. Alexiou, "An experimentally validated fading model for THz wireless systems," *Sci. Rep.,* vol. 11, pp. 1–14, 2021.

[33] Z. Hossain, C. N. Mollica, J. F. Federici, and J. M. Jornet, "Stochastic interference modeling and experimental validation for pulse-based terahertz communication," *IEEE Trans. Wireless Commun.*, vol. 18, no. 8, pp. 4103–4115, Aug. 2019.

[34] I. Otung, *Digital Communications: Principles and Systems*, vol. 2. London: U.K.: Institution of Engineering and Technology, 2014.

[35] R. Schmogrow *et al.*, "Error vector magnitude as a performance measure for advanced modulation formats," *IEEE Photon. Technol. Lett.,* vol. 24, no. 1, pp. 61–63, Jan. 2012.

[36] R. A. Shafik, M. S. Rahman, and A. R. Islam, "On the extended relationships among EVM, BER and SNR as performance metrics," in *Proc. Int. Conf. Elect. Comput. Eng.*, 2006, pp. 408–411.

[37] J. M. Jornet and I. F. Akyildiz, "Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3211–3221, Oct. 2011.

Zhaoji Fang received the B.S. degree in electrical and information engineering from Beihang University, Beijing, China, in 2019. He is currently working toward the Ph.D. degree in electrical engineering with Brown University, Providence, RI, USA, under the direction of Dr. Daniel M. Mittleman.

His current research interests include terahertz wireless communication and technology.

Hichem Guerboukha received the B.Sc. degree in engineering physics, the M.Sc. degree in applied science, and the Ph.D. degree in engineering physics from Polytechnique Montreal, Montreal, QC, Canada, in 2014, 2015, and 2019, respectively.

He is a Postdoctoral Research Fellow with the School of Engineering, Brown University, Providence, RI, USA. His previous research included THz instrumentation and waveguides, THz computational imaging, and THz communications.

Dr. Guerboukha was the recipient of the 2015 Releve Étoile Louis-Berlinguet from Fonds de recherche – Nature et technologies. He received the Best M.Sc. Thesis Award and the Best Ph.D. Thesis Award from Polytechnique Montreal in 2015 and 2019, respectively. He is currently a FRQNT Postdoctoral Research Fellow and working on THz communications, antennas, and metamaterials.

Rabi Shrestha received the B.S. degree in electrical and computer engineering and the M.S. degree in electrical engineering from the University of Rochester, Rochester, NY, USA, in 2016 and 2017, respectively. He is currently working toward the Ph.D. degree in electrical engineering with Brown University, Providence, RI, USA, under the guidance of Prof. Daniel M. Mittleman.

His current research interests include terahertz wireless communication and technology.

Malachi Hornbuckle was born in Ann Arbor, MI, USA on April 30, 2000. He is currently working toward the B.S. degree in electrical engineering with Brown University, Providence, RI, USA.

He has held positions as an Undergraduate Research Assistant with the Bioeconomy Institute, Iowa State University and the Mittleman Lab at Brown University during the summers of 2019 and 2020, respectively. During the summer of 2021, he was an RF Design & Integration Intern at Wolfspeed.

Yasith Amarasinghe received the B.Sc. degree in electronic and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2016, and the Ph.D. degree in electrical engineering from the Brown University, Providence, RI, USA, in 2021, under the direction of Dr. Daniel M. Mittleman.

He has now joined the Institute of Microelectronics, A∗STAR in Singapore as a Research scientist. His current research interests include THz devices and systems, wireless communications and metamaterials.

Daniel M. Mittleman (Fellow, IEEE) received the B.S. degree in physics from the Massachusetts Institute of Technology, Cambridge, MA, USA, in 1988, and the M.S. and Ph.D. degrees in physics from the University of California, Berkeley, Berkeley, CA, USA, in 1990 and 1994, under the direction of Dr. Charles Shan.

He then joined the AT&T Bell Laboratories as a postdoctoral member of the technical staff, working first for Dr. Richard Freeman on a terawatt laser system, and then for Dr. Martin Nuss on terahertz spectroscopy and imaging. He joined the ECE Department with Rice University in September 1996. In 2015, he moved to the School of Engineering at Brown University. His research interests involve the science and technology of terahertz radiation.

Dr. Mittleman is a Fellow of the OSA, and the APS, and was a 2018 recipient of the Humboldt Research Award. He has recently completed a three-year term as Chair of the International Society for Infrared Millimeter and Terahertz Waves.