Jamming Threats And Countermeasures of the Terahertz OOK Mode in IEEE 802.15.3d

Hichem Guerboukha
School of Engineering
Brown University
Providence RI, USA
hichem_guerboukha@brown.edu

Rabi Shrestha
School of Engineering
Brown University
Providence RI, USA
rabi_shrestha@brown.edu

Zhaoji Fang
School of Engineering
Brown University
Providence RI, USA
zhaoji_fang@brown.edu

Josep M. Jornet
Department of Electrical and Computer Engineering
Northeastern University
j.jornet@northeastern.edu

Edward Knightly
Department of Electrical and Computer Engineering
Rice University
Houston TX, USA
knightly@rice.edu

Daniel M. Mittleman
School of Engineering
Brown University
Providence RI, USA
daniel_mittleman@brown.edu

2022 IEEE Future Networks World Forum (FNWF) | 978-1-6654-6250-1/22/$31.00 ©2022 IEEE | DOI: 10.1109/FNWF55208.2022.00077

***Abstract*—We unveil jamming threats of the OOK mode of the IEEE 802.15.3d. We discuss jamming effectiveness, asymmetric effect on the bits and beat jamming. We propose a low-weight coding scheme as a countermeasure.**

***Keywords*—Terahertz communications, physical layer security, jamming, low-weight coding**

I. Introduction

It is too early to exactly pinpoint what future communications systems of the sixth generation (6G) will look like. However, a recurrent theme is the use of frequencies in the terahertz (THz) band (>100 GHz) [1]. While 5G networks (operating <100GHz) are expected to reach peak data rates of ~20 Gbps [2], there are already experimental demonstrations at THz frequencies of transmission up to 300 Gbps [3], while the overall goal is to break the Tbps barrier [4]. In 2017, the first IEEE standard that covers the sub-THz band was approved: IEEE Std. 802.15.3d-2017, from 253 GHz to 322 GHz [5].

Operating at such high frequencies brings its own set of challenges. Free-space path loss in the THz range is extremely high and can reach ~80 dB at 300 GHz over a 1-m distance. High-gain antennas are required to counter these large propagation losses. Consequently, THz links are highly directional, and can have a pencil-like radiation pattern [6]. Of course, this is challenging because the user needs to be precisely localized [7], and the beam needs to be directed towards them in real-time [8]. However, having narrow links can also be beneficial from the point of view of physical-layer security.

Recent works have highlighted the inherent security of those highly directional beams to eavesdropping [9]. However, man-in-the-middle attacks are possible through the use of specially designed metasurfaces placed in the beam path [10]. Molecular absorption of water vapor can also be used to delimit an area beyond which an eavesdropper fails his attack [11].

Here, we are interested in another form of security attack at THz frequencies: jamming [12]. While jamming is a well-known type of attack at lower frequencies, there are substantial differences at THz frequencies. Indeed, while coherent detectors are universally adopted at lower frequencies, THz detectors often use incoherent On-off keying (OOK) modulation. This type of modulation is one of the two modes of the PHY layer of the IEEE 802.15.3d. It is “intended for simpler devices […] that are not able to utilize complex signals and thus rely on the amplitude information” [5].

In this work, we first begin by showing some of the peculiarities of jamming OOK-modulated THz data. In this work, we consider that Alice (the transmitter) and Bob (the receiver) are in a direct line-of-sight link while Mallory (the malicious jammer) aims at Bob’s receiver at an angle θ_M from the line-of-sight (Fig. 1a). We assume that Mallory uses a single-tone frequency unmodulated signal. We begin by investigating

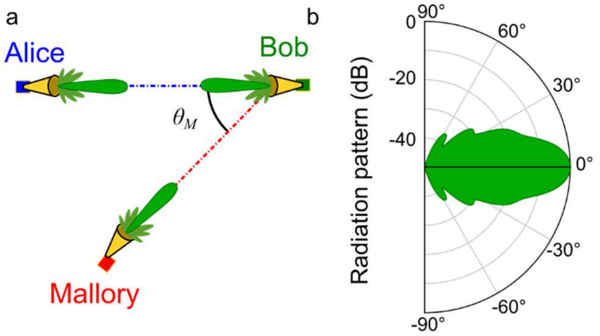

Fig 1. (a) Schematic of the jamming scenario we consider. (b) Radiation pattern of the Bob’s receiver, which is a horn antenna in our experiment

2770-7679/22/$31.00 ©2022 IEEE
DOI 10.1109/FNWF55208.2022.00077

the effectiveness of the attack based on Friis equation. Then, we show some intriguing phenomena that arise due to the use of incoherent detection. We show that the bits are asymmetrically affected by the jamming i.e., the bit 1 is more affected than the bit 0. Then, we show that the attack can be successful even if Mallory's single-tone is not at the same frequency as Alice's center frequency, an attack that we term "beat jamming". Finally, we discuss a countermeasure of this jamming attack that uses low-weight channel coding scheme [13].

II. Jamming Attack

A. Effectiveness of the Jamming Attack

Our jamming scenario is schematically depicted in Fig. 1a. We assume that Alice and Bob are in a direct point-to-point link, while Mallory aims at Bob receiver at an angle θ_M respective to the line-of-sight. In our experiment, Alice's transmitter is a photoconductive antenna excited by two detuned 1535-nm distributed feedback laser diode lasers. The difference in frequency between the two lasers is used to generate THz radiation through photomixing. We modulate the lasers using a fiber-coupled lithium niobate Mach-Zender modulator that we drive with a pulse pattern generator. Bob's receiver is a waveguide-coupled zero-bias Schottky diode followed by a low-pass filters to obtain the baseband signal between 0.1 MHz and 6 GHz. Mallory's transmitter is a frequency multiplier chain (multiplication factor of 16) driven by a RF oscillator. In the following experiments, Mallory uses a single-tone unmodulated signal.

The effectiveness of the jamming attack depends on how well Mallory's signal couples into Bob's antenna relative to how well Alice's does. Using Friis equation, this can be evaluated as the ratio of the measured powers originating from Mallory (P_B^M) and from Alice (P_B^A).

$$\frac{P_B^M}{P_B^A} = \frac{P_M}{P_A}\frac{G_M^{\theta=0}}{G_A^{\theta=0}}\frac{G_B^{\theta=\theta_M}}{G_B^{\theta=0}}\left(\frac{R_{AB}}{R_{MB}}\right)^{,2} \qquad (1)$$

where P_M and P_A are Mallory's and Alice's nominal power respectively, $G_M^{\theta=0}$ and $G_A^{\theta=0}$ are Mallory's and Alice's antenna gains in the front direction respectively, $G_B^{\theta=\theta_M}$ and $G_B^{\theta=0}$ are Bob's gain in the direction of Mallory (θ_M) and in the direction of Alice (0°) respectively, R_{MB} and R_{AB} are the distances from Mallory to Bob and from Alice to Bob respectively.

A successful jamming attack occurs when the ratio in (1) is maximized, and it is countered when it is minimized. To improve her attack, Mallory can 1) increase her power, 2) antenna gain and/or 3) reduce her distance to Bob. To counter the attack, Alice can 1) increase her power, 2) her antenna gain and/or reduce her distance to Bob. As for Bob, he can improve his defense by using an antenna with a more directional radiation pattern, such that $G_B^{\theta=0} \gg G_B^{\theta=\theta_M}$. For example, in our experiment, Bob's radiation pattern decreases by ~17 dB at $\theta_M = 22°$ (Fig. 1b). Therefore, Mallory must have enough power to counter these ~17 dB effective losses caused by her coupling at an angle into Bob's antenna.

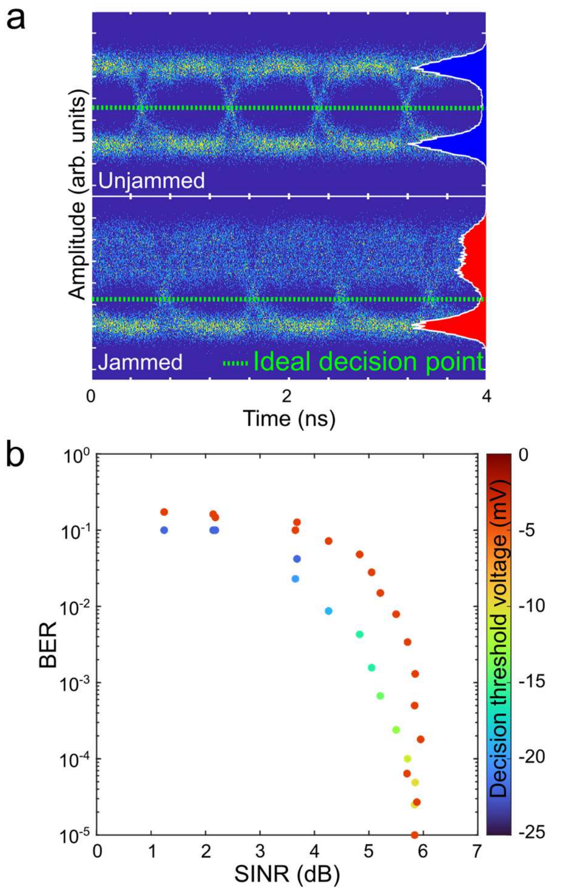

Fig 2. (a) Measured eye diagrams in the absence (top) and presence (bottom) of Mallory's jamming. The green dahsed lines correspond to the ideal decision threshold required to have the best BER. (b) BER as a function of the SINR when Mallory's jamming is introduced. The color of the dots correspond to the value of the decision threshold.

B. Asymmetric Effect on the Bits

As we mentioned before, we consider the PHY OOK Mode of the IEEE 802.15.3d. This mode is intended for low-complexity devices and uses incoherent detectors that are sensitive to the amplitude only. Typically, a Schottky diode followed by a low-pass filtering circuit is used. It is a power detector in the sense that it measures the square of the electric field. We consider that Mallory attempts to disrupt the signal with a single-tone signal at a frequency ν_M. The power incident on the Schottky diode is

$$|E_B(t)|^2 = |A_A u_A(t)\cos(2\pi\nu_A t) + A_M\cos(2\pi\nu_M t)|^2 + N(t), \qquad (2)$$

where A_A and A_M are the amplitudes of Alice and Mallory respectively. The first term in (2) is Alice's signal which consists of an OOK data $u_A(t)$ transmitted at a center frequency ν_A. The second term corresponds to Mallory's jamming, while the third term $N(t)$ is the noise expressed in power.

The incoherent detector followed by the low-pass filtering circuit demodulates the signal by removing the DC term and the high frequency term that can be found by expanding the square in (2):

$$|E_B(t)|^2 = \frac{A_A^2 u_A^2}{2} + A_A A_M u_A(t)\cos(2\pi\Delta\nu t) + N(t) \qquad (3)$$

where $\Delta\nu = |\nu_A - \nu_M|$ is the difference in frequency between Alice and Mallory. In Eq. 3, the first term corresponds to Alice's original data stream. It is a baseband signal centered at the 0 frequency. The second term is the effect of Mallory's jamming and consists of the product of the original data stream with a sinusoidal term oscillating at the beat frequency $\Delta\nu$.

Fig. 2a shows examples of measured eye diagrams in the presence and absence of Mallory's jamming. First, from the eye diagram it can be clearly observed that the jamming leaves the low bit (the "0") untouched and impacts the high bit (the "1") by increasing its error. This can be understood in light of (3) There, u_A denotes the data and can be seen as a rectangular function taking either a value of 0 (bit 0) or 1 (bit 1) in an OOK modulation format. From that equation, the jamming only appears when $u_a = 1$, whereas when $u_a = 0$, the equation is indistinguishable from the case without Mallory.

This asymmetric jamming has important consequences for Bob since it modifies the required value for error-free detection. Indeed, in a typical OOK scenario where noise affects both bits, the decision point is taken in-between the bit levels. However, here, because of the jamming, the bit 1 broadens, meaning that Bob must lower the value of his decision point to correctly retrieve the information. This is experimentally shown in Fig. 2b where we show the measured bit-error rate (BER) as a function of the signal-to-interference-plus-noise ratio (SINR). The colored dots correspond to values of the decision threshold. As can be seen, when the jamming level increases (i.e., decreasing SINR), the decision point must be monotonously lowered to retrieve better BER (monotonous change from red to blue dots), compared to the case without Mallory (red dots).

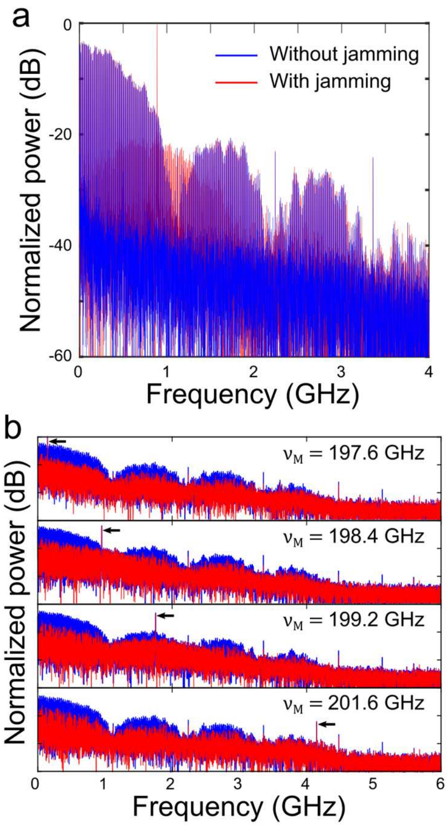

Fig 3. (a) Measured spectrum in the absence (blue) and presence (red) of Mallory's jamming. (b) Measrued spectrum (blue) and introduced interference (red) for different frequencies of Mallory's single-tone.

C. Beat Jamming

Another important threat appears when considering the spectral response of the jammed signal. By Fourier transform, the jamming term in (3) (the second term) becomes:

$$A_A A_M \Im\{u_A(t)\} * \Im\{\cos(2\pi\Delta\nu t)\} \qquad (4)$$

where $\Im\{\ldots\}$ is the Fourier transform, and $*$ is the convolution operator. In particular, $\Im\{\cos(2\pi\Delta\nu t)\}$ creates two Delta functions located at $\nu = \pm\Delta\nu$, where $\Delta\nu = |\nu_A - \nu_M|$ is the carrier frequency difference between Alice and Mallory. By the sifting property, these Delta functions translate the data spectrum $\Im\{u_A(t)\}$ to $\pm\Delta\nu$. The data spectrum itself consists of a wide bandwidth B determined by the modulation format, data rate, etc. This means that if the beat frequency is smaller than the bandwidth ($\Delta\nu < B$), then the effect of the jamming is to interfere with Alice's data by overlapping the jamming term to the data term. This is an important point, because it means that Bob cannot filter out the overlap term without removing parts of the data term.

Fig. 3a shows measured spectra with and without Mallory. In this experiment, Alice sends a 1 Gbps OOK data stream at a center frequency of 197.5 GHz (blue curve). This can be approximated as a sinc function where the first lobe ends at $B =$ 1 GHz. As for Mallory, she sends a single tone at 198.39 GHz, leading to a detuning $\Delta\nu = 0.89$ GHz (red curve). In the spectrum, we observe a Delta function centered at 0.89 GHz with a broad bandwidth corresponding to Alice's data. In this case, the jamming term overlaps Alice's spectrum and leads to a deterioration of the BER.

Fig. 3b shows different spectra measured when Mallory changes her frequency (while Alice transmits at 197.5 GHz). As Mallory increases her frequency, the Delta function she introduces (indicated by the black arrow) increases as well. When the beat frequency is large enough, she has no effect on the original signal because the overlap with the main lobe is minimal.

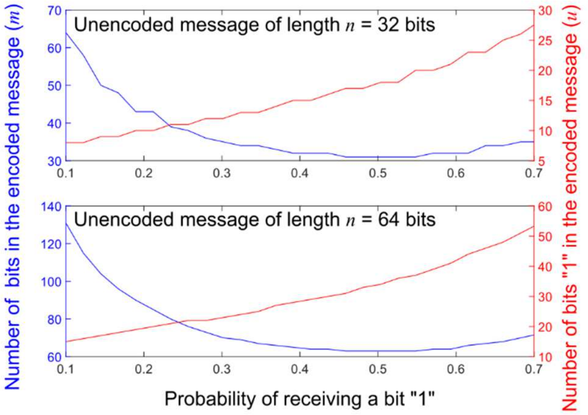

Fig 4. Low-weight coding scheme. Number of required bits in the encoded message (m) when considering a message of 32 bits (top) and 64 bits (bottom), and corresponding number of bits u that are logical "1"s.

D. Low-Weight Coding as a Jamming Countermeasure

To counter the effect of jamming, we propose to use a low-weight coding (LWC) scheme. LWC has been proposed in [13] to mitigate interference in time spread OOK in electromagnetic THz nanonetworks. At its heart, this technique recognizes that the interference appears only when the 1 bit is present, which is what we also observe in the asymmetric effect on the bits in (3). Instead of using error correction codes *after* transmission, the LWC technique designs the channel code – *before* transmission – to reduce the probability of having these errors. Typical channel codes use all potential codewords without consideration of their weight meaning that logical "0"s and "1"s are transmitted with overall equal probability. For a constant jamming, that would mean that half of the bits are affected by the jamming. The LWC technique proposes to *lower* the weight of the channel-code i.e., use more logical "0"s than logical "1"s to transmit information.

Of course, this would result in longer messages, thus reducing the effective information rate. As demonstrated in [13], it is possible to compute the probability of receiving a 1, for a given message. An unencoded message of length equal to n bits can be encoded into a message of $m < n$ bits in which the weight $u < m$ is the number of logical bits equal to "1". There are $\mathcal{W}(m,n) = m!/(m-u)!\,u!$ possible codewords, which means that to be able to encode all the possible messages of n bits into fix weight codewords, the inequality $\mathcal{W}(m,n) \geq 2^n$ must be respected. The probability of receiving a logical "1" is then $p_1 = u/m$, and can be injected into $\mathcal{W}(m,n) = 2^n$ to find the weight u and encoded message length m. Results of this calculation are shown in Fig. 4 for an uncoded message of length $n = 32$ bits (top) and $n = 64$ bits (bottom). For example, to achieve a probability of 20% of receiving a "1" when sending a message of $m = 64$ bits, it is necessary to encode the message with $n = 88$ bits with $u = 19$ of those bits being logical "1". From this, it appears evident that the LWC coding scheme can be used to reduce the interference on the high bit, and therefore reduce the jamming of the OOK data. Experimental demonstration is part of future work.

III. Conclusion

In conclusion, we have discussed the jamming vulnerabilities of the OOK mode of IEEE 802.15.3d. We showed that the efficiency of the attack can be calculated as the ratio of power of the jammer and the transmitter as measured by the receiver. Several parameters such as the antenna gains, nominal powers, distances can be used to increase or counter the attack. Next, we observed that the jamming attack asymmetrically affected more the bit 1 compared to the bit 0, and we showed that this is caused by the use of incoherent detectors. We also showed that the jammer does not need to be exactly at the center frequency of the signal to have significant jamming effect, an attack we termed "beat jamming". Finally, we proposed to use the low-weight coding scheme and introduce more zeros than 1 in order to reduce the effect of the jamming.

References

[1] M. Polese, J. M. Jornet, T. Melodia, and M. Zorzi, "Toward End-to-End, Full-Stack 6G Terahertz Networks," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 48–54, 2020, doi: 10.1109/MCOM.001.2000224.

[2] M. K. Afzal, Y. Bin Zikria, S. Mumtaz, A. Rayes, A. Al-Dulaimi, and M. Guizani, "Unlocking 5G Spectrum Potential for Intelligent IoT: Opportunities, Challenges, and Solutions," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 92–93, 2018, doi: 10.1109/MCOM.2018.8493125.

[3] S. Jia *et al.*, "2 × 300 Gbit/s Line Rate PS-64QAM-OFDM THz Photonic-Wireless Transmission," *J. Light. Technol.*, vol. 38, no. 17, pp. 4715–4721, 2020, doi: 10.1109/JLT.2020.2995702.

[4] T. Kürner, D.Mittleman, and T.Nagatsuma, *THz Communications: Paving the Way Towards Wireless Tbps*, vol. 234. 2022.

[5] V. Petrov, T. Kurner, and I. Hosako, "IEEE 802.15.3d: First Standardization Efforts for Sub-Terahertz Band Communications toward 6G," *IEEE Commun. Mag.*, vol. 58, no. 11, pp. 28–33, Nov. 2020, doi: 10.1109/MCOM.001.2000273.

[6] H. Guerboukha *et al.*, "Efficient leaky-wave antennas at terahertz frequencies generating highly directional beams," *Appl. Phys. Lett.*, vol. 117, no. 26, p. 261103, 2020, doi: 10.1063/5.0033126.

[7] Y. Ghasempour, R. Shrestha, A. Charous, E. Knightly, and D. M. Mittleman, "Single-shot link discovery for terahertz wireless networks," *Nat. Commun.*, vol. 11, no. 1, 2020, doi: 10.1038/s41467-020-15761-4.

[8] H. Guerboukha, K. Nallappan, and M. Skorobogatiy, "Toward real-time terahertz imaging," *Adv. Opt. Photonics*, vol. 10, no. 4, p. 843, 2018, doi: 10.1364/aop.10.000843.

[9] J. Ma *et al.*, "Security and eavesdropping in terahertz wireless links," *Nature*, vol. 563, no. 7729, pp. 89–93, Nov. 2018, doi: 10.1038/s41586-018-0609-x.

[10] Z. Shaikhanov, F. Hassan, H. Guerboukha, D. Mittleman, and E. Knightly, "Metasurface-in-the-Middle Attack: From Theory to Experiment," *WiSec 2022 - Proc. 15th ACM Conf. Secur. Priv. Wirel. Mob. Networks*, pp. 257–267, 2022, doi: 10.1145/3507657.3528549.

[11] Z. Fang, H. Guerboukha, R. Shrestha, M. Hornbuckle, Y. Amarasinghe, and D. M. Mittleman, "Secure Communication Channels Using Atmosphere-limited Line-of-sight Terahertz Links," *IEEE Trans. Terahertz Sci. Technol.*, 2022, doi: 10.1109/TTHZ.2022.3178870.

[12] R. Shrestha, H. Guerboukha, Z. Fang, E. Knightly, and D. M. Mittleman, "Jamming a terahertz wireless link," *Nat. Commun.*, vol. 13, no. 1, 2022, doi: 10.1038/s41467-022-30723-8.

[13] J. M. Jornet and I. F. Akyildiz, "Low-Weight Channel Coding for Interference Mitigation in Electromagnetic Nanonetworks in the Terahertz Band," in *2011 IEEE International Conference on Communications (ICC)*, Jun. 2011, pp. 1–6, doi: 10.1109/icc.2011.5962987.