978-1-6654-1339-8/21/$31.00 ©2021 IEEE | DOI: 10.1109/DySPAN53946.2021.9677168

Jamming at Terahertz Frequencies: A Theoretical And Numerical Study

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

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

***Abstract*—Carrier frequencies in the terahertz (THz) range are being considered for future wireless communications. At such high frequency, THz links are more secure due to the need of using highly directional beams to counter free-space path loss. While previous studies have only considered eavesdropping threats to security, here we numerically investigate the susceptibility of THz links to physical layer jamming.**

Keywords—Wireless communications, terahertz physical-layer security,

I. INTRODUCTION

Intensive research in the future of communications systems is accelerating as 5G networks are beginning their global roll-out. Operating with large bandwidths in the terahertz (THz) frequency band is seen as a likely candidate to respond to the ever-increasing demand in data consumption [1-5]. At such high frequencies, high-gain antennas are necessary to overcome large free-space path loss. THz communications links are therefore highly directional [6,7]. This high directionality has attracted the attention of researchers in the context of physical layer security. Indeed, the use of narrow beams restricts the ability of eavesdropper to efficiently intercept the communication link [8-14]. However, the security of THz links during a jamming attack has not been addressed in prior research.

Jamming attacks are well known at lower frequencies and have been a concern since the beginning of the 20th century. In this paper, we numerically and theoretically address the security of THz links in the presence of a jammer. This paper is organized as follows. In Section II, we evaluate the effectiveness of a jamming attack based on a simple scenario where the jammer couples into the sidelobes of the receiver's antenna. Then, in Section III, we simulate the effect of single-tone jamming in the case of an incoherent on-off keying (OOK) communication link, when both the link and the jammer operate at the same center frequency. Finally, in Section IV, we compute the spectra when the jammer operates at a slightly detuned frequency from the link, a possibility that is not generally considered in studies of jamming attacks at lower frequencies.

II. EFFECTIVENESS OF THE JAMMING ATTACK

Fig. 1a depicts the schematic of the jamming scenario that we consider in the following. Alice (the transmitter) and Bob (the receiver) communicate through a direct line-of-sight link, while Mallory (the malicious jammer) is at an angle θ_M from their link and aims at one of the sidelobes of Bob's receiver. The effectiveness of Mallory's jamming depends on how well she can couple into Bob's antenna relative to how well Alice couples into the same antenna. This depends on a series of parameters and can be evaluated using Friis transmission. In general, the power originating from Alice that Bob measures is

$$P_B^A = P_A G_A^{\theta=0} G_B^{\theta=0} \left(\frac{\lambda}{4\pi R_{AB}}\right)^2 \quad (1)$$