Abstract

Free Space Optical (FSO) Communication has been enjoying the limelight in recent years owing to its many strengths, such as the capability to deliver very high data rates, provide low latency, and offer large bandwidth and capacity, making it a top applicant for prime, real-time services such as video conferencing and financial transactions.

As FSO communication gains ground in the field of data transmission, it is imperative to identify and address the security connotations associated with it. One challenge to the security of FSO communication is jamming: an unlawful transmitter sends optical signals and interferes with the legitimate receiver, thus, limits its ability to decode the information. Another threat lies from an eavesdropper (Eve), which can place a wicked receiver within the line-of-sight to capture a fraction of transmitted optical power, attaining unsanctioned ingress to the data. This dissertation endeavors to analyze the viable menaces to the security of FSO communication, develop their mathematical models, and present their resilient solutions, accompanied by the quantified attestations of their performance in securing communication for the ever-evolving landscape of wireless communication.

In the first work, the mettle of optical space shift keying (OSSK) is tested in abating the jamming in an FSO network. The jamming noise is modeled as a function of the atmospheric turbulence (AT) observed by the optical jamming signal, as opposed to its general representation following Normal distribution. The work proposes employing the OSSK in a multiple-input-single-output (MISO) system to retaliate the jammer. Specifically, a closed-form average bit error rate (ABER) of a 2×1 MISO system encountering saturated AT (modeled by negative exponential distribution) and confronting the jamming and Gaussian noise, concurrently, is derived. Building on it,

coding gain and diversity order are studied.

The subsequent work focuses on an $N \times 1$ MISO-FSO system under attack from an optical jammer with a saturated AT and varying pointing error (PE). The efficacy of the transmit aperture selection technique, where the transmitter experiencing the maximum channel gain is selected for communication, is investigated in circumventing the cordial attack of optical jamming and Gaussian noise. The considered approach is compared with other methods such as repetitive coding (RC) and OSSK.

The following study examines the repercussions of jamming on an unmanned aerial vehicle (UAV) engaged in FSO communication with a ground station. The optical link deteriorates due to concurrent Gaussian noise and jamming, while the channel fading is modeled by GG distribution with PE, considering the Angle-of-Arrival and field-of-view (FoV) of mobile UAV. The work defines the optimal conditions for UAV under attack from a non-Gaussian and optical jammer.

The subsequent study introduces a novel system model giving center stage to the exacerbation caused by an Eve on an FSO network. The work proposes different solutions to abate, quantifying the efficacy of each strategy by evaluating the discrete-input-continuous-output memory-less channel (DCMC) capacity for authentic and eavesdropping channels. The channel is characterized by generic $\alpha - \mu$ distribution, zero and non-zero boresight PE, and partial band or broadband jamming noise. The devised strategies, which included deploying a friendly jammer and employing channel fading, are assessed by formulating the closed-form average secrecy capacity in both scenarios.

In essence, this research sheds a spotlight on the potential security issues in the FSO communication and contrives their resolutions by presenting diverse and resilient propositions for ensuring that this innovative technology meets the evolving demands of modern communication networks.