A Survey on Physical Layer Security for FSO Communication Systems

Wafaa Mohammed Ridha Shakir [1], Ruwaida A. Abdulkareem[2]
{inb.wfa@atu.edu.iq[1], engrawada8888@gmail.com[2]}

Department of Computer Systems, Technical Institute of Babylon, Al-Furat Al-Awsat Technical University, Babil 51015, Iraq[1,2]

Abstract. Physical layer security (PLS), which uses information-theoretic techniques to protect data secrecy, has recently received a lot of academic attention. As wireless communications progresses to 5G and beyond, physical layer security research faces new hurdles. Because existing Radio-Frequency (RF) networks are unable to meet increasing data rate demands, optical wireless communication (OWC) based on free-space optical (FSO) techniques has been proposed as a viable approach to overcome RF spectrum limitations. Because of the small coverage offered by the narrow optical beam and the fact that they work properly only in the presence of line-of-sight components, FSO networks are more secure and less sensitive to eavesdropping than RF networks. However, the presence of an aggressive eavesdropper may undermine the secrecy performance of FSO networks. This document summarises all of the research that has been done on physical layer security in free space optical networks. In addition, the study suggests a number of open problems in these networks in order to improve and optimise security performance.

Keywords: Physical layer security, free-space optical, secrecy metrics.

1 Introduction

The increased demand for high-data-rate services and applications has prompted researchers to concentrate their efforts on using the unregulated optical spectrum for communications to meet the traffic demands of 5G and beyond networks. RF networks are proving insufficient to meet the growing need for data rate services [1], so optical wireless communication (OWC) has arisen as a promising alternative or supplement to existing RF networks to meet the anticipated traffic demand. Free-space optical (FSO) is regarded as one of the most promising OWC techniques due to its merit criteria. Due to its extensive bandwidth, free licences, strong security, low implementation costs, and other appealing properties, FSO technology enables the realisation of many applications [2]. Another feature of FSO is that the transmission can only function successfully when LOS component is present. To put it another way, if the LOS component is lacking, the channel suffers greatly. As a result of the extremely directional optical beam of the laser transmitter diode and the fact that they only work properly in the presence of LOS components, FSO networks are more secure and less sensitive to eavesdropping as compared to RF networks. Security in FSO networks, on the other hand, remains a concern, especially when a wiretapper or eavesdropper is hidden at the same building's top as the main receiver [3]. An eavesdropper is a user who attempts to obtain confessional information from a legitimate user. This is primarily due to the laser beam

IMDC-IST 2021, September 07-09, Sakarya, Turkey

DOI 10.4108/eai.7-9-2021.2314809

spreading through the atmosphere, which causes the beam at the receiver to be substantially larger than the receiver size [4]. As a result, when the eavesdropper is in the divergence area of the transmitted optical beam, one possible eavesdropping occurs. By collecting radiated power across long FSO distances, the eavesdropper has a better chance of eavesdropping.

Using noise randomization, channel state information (CSI), and other resources (such as multiantenna and cooperative nodes), physical layer security (PLS) has emerged as a viable technique for minimising the amount of information received by eavesdroppers [5], [6]. In most wireless networks, the PL is utilised to facilitate reliable communication to approved destinations, while the top layers are used to protect and secure the communicated data [7]. The secrecy capacity measure was established by Wyner [8] to evaluate system secrecy performance. It was defined as the maximum source information that can be effectively recovered by the legitimate destination while keeping eavesdroppers as uninformed of this information as feasible. The eavesdroppers were believed to be completely aware to ensure an accurate evaluation [8].

Physical layer security techniques for FSO networks have the following advantages over cryptography approaches: Computing expense isn't a factor in physical layer security. Physical layer security, in contrast to traditional top-layer encryption systems, does not require a secret key because it relies on the properties of fading channels to ensure absolute secrecy [5]. As a result, safe and reliable communications can be established even if eavesdroppers (unauthorised smart devices) in FSO networks have powerful computer equipment. On the other hand, the security of computation-based encryption systems will be jeopardised if the eavesdroppers' equipment has enough processing power to solve challenging mathematical problems. Security in FSO systems is currently viewed as an open, demanding subject by the research community for all of these reasons.

We examine the research that has been done on securing FSO systems using PLS approaches in this work. Solutions offered in RF cannot be implemented in FSO systems due to the unique characteristics of this technology. As a result, a number of researchers have focused their efforts on how to improve the PLS in FSO systems by considering these factors. To our knowledge, only a small amount of research has looked into the security issue in FSO systems that use PLS approaches [9]. The aim of this study is to provide a extensive overview of PLS on FSO enablement technologies. The essential ideas for understanding PLS in FSO networks, as well as broader FSO systems for PLS model description, are first introduced. The key PLS performance measures of the FSO system are also defined. There is also some background information on these measurements. Second, we look at the PLS strategies that are often employed to improve secrecy performance. Then we go over some of the open difficulties in PLS for FSO systems, as well as some closing thoughts.

2 Fundamentals of Physical Layer Security in FSO Systems

The essential elements for comprehending PLS in FSO wireless communication systems are introduced in this section. The optical spectrum is used in FSO systems to deliver high data rates over long distances of up to ten kilometres between two stationary stations [10]. FSO lines have significantly more accessible bandwidth than RF links, resulting in higher data speeds. Because FSO systems operate at frequencies greater than 300 GHz, they do not require a licence. Because they use limited laser beams to transmit data, they are more secure than RF. They also

offer improved interference rejection and a high reuse factor, allowing the frequency to be reused multiple times. Eavesdroppers can obtain a version of the supplied data via atmospheric turbulences (AT), pointing error (PE), scattering channels, and laser-beam divergence, on the other hand [9].

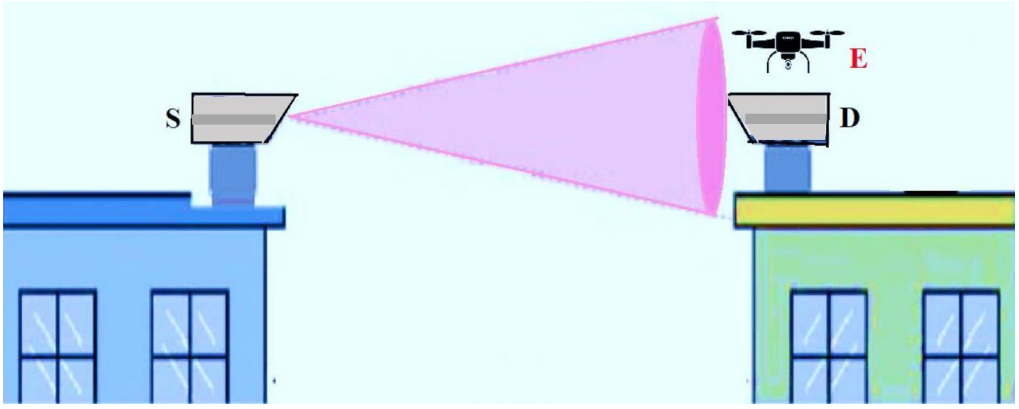

Fig. 1. FSO security communications over the physical layer.

2.1 The FSO System's General PLS Model

As illustrated in Fig. 1, the overall PLS for the FSO system is made up of three primary communication nodes. The FSO transmitter or source (S) node, the legitimate receiver or destination (D) node, and the eavesdropper (E) node are the first three nodes (also known as Eve). Laser diodes are commonly used as transmitters in FSO systems, and receivers must include photodetectors that can convert the received light intensity into an electrical signal. The legal channel is the FSO link between Alice and Bob, while the wiretap channel is Alice and Eve's FSO link. Alice sends confidential data to Bob across a legal FSO link in this system configuration. As a result, Alice's goal is to establish a communication route through which the secret information can be conveyed to Bob while assuring that the information is not intercepted by Eve. To accomplish secrecy in FSO wireless, PLS uses of specific features of the channel, such as fading, noise, and interference, among others. The availability of channel status information at all nodes is another crucial factor in the wiretap channel. CSI may be complete, partial, or even null at the nodes. Because the transmitter selects whether or not to broadcast and at what pace, CSI is critical from a security aspect. As a result, the system's secrecy performance will significantly enhance as a result of this fact.

The PLS for FSO systems, unlike its RF counterparts, is not yet mature, and its eavesdropping situations, which can be separated into active and passive eavesdropping, are currently being debated. When active eavesdropping is used, the eavesdropper may transmit jamming optical signals to legitimate receivers, clogging his receiver with unwanted noise [11]. Eve is supposed to passively intercept the genuine channel around Alice's transmitter [12], in the middle of the FSO connection [3], and near Bob's receiver [12]-[15] in the passive eavesdropping. This can also be applied to mixed RF-FSO relaying networks [16]-[17], where Eve is placed near Bob in the FSO link. In actuality, Eve's ability to intercept in the middle of the link is considerably hampered by the optical beamwidth of FSO systems, which is extremely tiny and invisible. As

a result, it's more realistic to limit the FSO channel, therefore modelling it as an FSO rather than a wiretap channel [17].

Eve is considered to be a fully passive eavesdropper positioned somewhere on or behind Bob's reception plane, attempting to tap the diverging optical beam's side lobs [17], [18]. This FSO over a wiretap channel model has also been used to improve secret-key rates (SKRs) in free-space quantum key distribution (QKD) systems [19], [20]. [12], [21] have also studied the correlated link channels.

2.2 PLS Performance Metrics for FSO Systems

The most often used secrecy performance measures in the literature are clarified in this section. The mean secrecy capacity (ASC), secrecy outage probability (SOP), and strictly positive secrecy capacity (SPSC) have closed-form formulas.

2.2.1 ASC

The mean secrecy capacity is one of the performance metrics for the free-space optical link in WOC. Data transmission is secure when the legitimate receiver's instantaneous SNR is much larger than the eavesdropper's SNR. As a result, the greatest data transfer rate that can be achieved without being hacked by an eavesdropper is defined as the mean secrecy capacity. The maximum achievable secrecy rate is denoted by (C_s) and may be defined as follows [22].

$$C_s(\gamma_{sd}; \gamma_{se}) = \max\{W \log_2(1+c\,\gamma_{sd}) - W \log_2(1+c\,\gamma_{se}); 0\} \quad (1)$$

where (γ_{sd}; γ_{se}) denote the electrical SNR of legitimate link (source to legal destination) and wiretap link (source to eavesdropper), and W denotes the bandwidth of the corresponding channel, and $\log_2(1+c\,\gamma_{sd}) = C_{sd}$ is main channel capacity, and $\log_2(1+c\,\gamma_{se}) = C_{se}$ is the wiretap capacity, respectively, while, c is a constant.

2.2.2 SOP

The possibility that the achievable secrecy capacity Cs falls below a predefined threshold rate Rs in information-theoretic security is described by SOP, a crucial parameter in physical layer security. In this case, the lawful channel's capacity is lower than the wiretap channel's, resulting in a security outage as defined by [22]:

$$SOP = P_r\{ C_s(\gamma_{sd}; \gamma_{se}) < R_s\} \quad (2)$$

where $P_r\{.\}$ denotes the probability, R_s is the threshold secrecy rate.

2.2.3 SPSC Probability

SPSC, is the probability which may be thought of as a special instance when the target secrecy rate, Rs = 0 [22]. Insecure communications, SPSC can be characterized the system performance, as the following of having precisely positive secrecy capacity

$$SPSC = P_r\{C_s > 0\} = P_r\{\gamma_{sd} > \gamma_{se}\} \quad (3)$$

3 Physical Layer Security Techniques in FSO Systems

Min and Jams suggested a physical layer architecture in [23] to improve security in single input single output (SISO) FSO communication utilizing deflectors of acousto-optic (AODs) and gratings of synthetic holographic, in which the transmitter distributes packets along distinct beam pathways between two legitimate peers. The authors showed in [23] that the radius and intensity of the transmitted optical beam have a direct impact on security and that these parameters may be modified by altering the AODs parameters under various turbulence strength conditions. Lopez-Martinez et al. [12] investigated FSO communication with an external eavesdropper from the point of view of PLS. The processes of eavesdropping and the influence of disturbance-induced variations were explored in [12]. When the eavesdropper is closer to the intended receiver, the combined beam divergence and fading on received radiation allows the eavesdropper to penetrate the genuine communication link. Furthermore, the authors obtained closed-form formulations of the SPSC as the performance measure in [12], which found that the eavesdropper may penetrate the communication when close to the transmitter. In [14], the authors provide experimental data on optical transmission through the FSO link at a safe wavelength using Tokyo FSO Testbed. With a 7.8-kilometer link, this testbed comprises of one sender terminal and two reception ports, of legal recipient. The purpose of the testbed was to investigate PLS security approaches (such as secure message transmission and secret key) in real-world FSO lines across Tokyo. Furthermore, under true fading conditions, the secrecy performance of such a testbed is calculated using secrecy rate, outage probability, and predicted code length [14]. In [24], the authors looked into the dangers to sensitive data provided over the FOS link in the presence of eavesdropping out of the laser beam, where the eavesdroppers pick up information through a Non-LOS scattering channel. The authors examined FSO communication secrecy using the orbital angular momentum multiplexing technique. As it has been shown in [24], this technique provides a high level of security under certain disturbance conditions. This approach, as demonstrated in [24], gives a high level of security under particular disturbance situations. Using OOK modulation and threshold detection, the authors constructed a closed-form formula for an ASC and lower bound of ASC of the FSO system that suffers from turbulence-induced fading in [25]. In another paper, the authors used the intensity-modulation/direct-detection (IM/DD) technique over Malaga-M turbulence to develop formulas for the FSO system [15]. Because of their higher turbulence resiliency, the authors of [26] used numerical simulations and experiment results to verify that Bessel-Gaussian beams with spatial light modulators can improve the FSO link in weak to medium turbulence conditions than their Laguerre-Gaussian counterparts in weak to medium turbulence conditions. [27] investigates throughput of MIMO under-attack of a multiple-apertures eavesdropper (MIMO-ME) for coherent FSO.Furthermore, to analyse the overall system performance across the turbulence fading channel, adaptive and fixed transmission rate techniques are examined depended on the availability of the CSI at the transmission side constrained by the probability of a secrecy outage [27]. The authors of [28] performed an experiment utilizing Bessel–Gaussian (BS) beams to emulate data transmission across an eavesdropping channel under various AT conditions. Even when the eavesdropper can perform optical beam-splitting attacks in the channel to compromise PLS, and even when the legitimate transmitter and receiver do not use a shared key for communications, this study focused on achieving secure FSO communication by exploiting the

noisy and degraded channel conditions [28]. Under diverse AT settings, the authors of [19] combine FSO with the secret key agreement (SKA) to identify information security concerns and achieve secret key rates high-speed communications via FSO link. Another study [29] fragmented optical data into small fragments in order to provide secure communication over an FSO link under varied air turbulence conditions. The authors of [4] looked at how the secrecy of the FSO link was affected by turbulence-induced fading channels with pointing errors. Under two different weather situations, the authors of [30] compare the effective secrecy throughput of legal links and multi eavesdroppers with multiple-input-multiple-output relay supported. When the transmitter instantaneous CSI of the legitimate channel is available, the effect of using multiple relays on EST performance was investigated using two mechanisms: adaptive scheme with selective relaying, and fixed rate with all-active relaying, when the instantaneous CSI is not available at the transmitter [30].A framework for the secrecy analysis of a terrestrial FSO link considering the eavesdropper's location, under misalignments and atmospheric turbulence conditions is established in [31]. From a security standpoint, the IM/DD FSO system with CV-QKD technique was investigated [31]. In various recent works of literature [33]-[36], the inherent benefits of employing FSO based on transmitter spatial diversity [32] have been extended to improve PLS in FSO. In addition, [37]-[39] explored the security implications of hybridization between FSO and RF link. The hybrid FSO/RF system's main idea is to send identical signals across both connections at the same time and combine the received signals using a single diversity combining technique to benefit both technologies [39]. In these aforementioned studies, it was assumed that only the RF link was attacked by the eavesdropper considering the high security of the FSO link and broadcasting nature of wireless RF channels, which makes the RF link vulnerable to eavesdropping attack. The hybrid FSO/RF systems differ greatly from mixed FSO-RF relay systems because the FSO connection is only part of the mixed FSO-RF relay system. The current research on the PLS of mixed FSO-RF systems [40]–[56] is primarily limited to the RF link alone attack by an eavesdropper, according to a complete open literature survey. Table 1 outlines the current research trends in PLS approaches in FSO systems that have been applied by various researchers in their studies.

Table 1. The PLS trends in FSO techniques.

System Type	Reference	Focus of the work	Contribution and Research Direction	Channel conditions	Metrics
SISO FSO	[23]	Enhancing the data security based on AOD.	Formulating a transmitter beam setting by varying AOD's parameters.	Various AT	Secondary GSM transmitting beam
	[12]	Evaluating the FSO link security in presence of the eavesdropper.	The mechanisms of eavesdropping based on the eavesdropper location and the effect of joint laser-beam divergence were stated.	Various AT	SPSC
	[14]	Emulating a typical scenario of PLS security of the real-field FSO link.	Real-life experimental FSO links was considered with the influence on the instantaneous secrecy rate and the code lengths is analysed.	Various AT	Secrecy rate, SOP, the code lengths

	[24]	Impact of eavesdropper's were studied.	Formulating the security metrics considering the visibility of the link and different positions of eavesdropper taking into account two-dimensional space around the laser beam.	Various AT	ASC, SOP
	[25]	Secure communication over FSO links suffering from turbulence-induced fading.	Apply OOK to enhance the secrecy in FSO link and various channel models.	Various AT	ASC
	[26]	Secure FSO communications based on Bessel-Gaussian orbital angular Momentum	This paper provides a proved of the superiority of Bessel-Gaussian beams over the Laguerre-Gaussian beams in resilience to AT effects based on ASC.	weak to medium AT	ASC
	[28]	Creating an experiment to emulating an optical wiretap channel to extended Wyner's wiretap channel model.	Achieve reliable secrecy over noisy communications over and degraded channel conditions.	Various AT	ASC
	[19]	Experimental investigations for eavesdropping risks of several kilo meters.	A secure high-speed key FSO link, with a practical representation of the wiretap channel model, is established	Various AT	Asymptotic key rate
	[29]	Enhancing the security of FSO link concerning the channel changes	A testbed to view and approve the FSO link between two buildings	In Lab AT	Intercept possibility
	[4]	Proposing a misalignment error model based on a non-orthogonal optical beam	A two-axis misalignment pointing error effect is modelled and the effect of such type of error is investigated on the security performance of the FSO link.	AT with PE	SOP, SPSC
	[31]	Ggeneralised misalignments model is considered of a terrestrial FSO link.	Taking the account of the drops on the system operation including the transceiver misalignments and other system performances.	AT with PE	SOP
MIMO-ME FSO	[27]	Characterized the MIMO-ME oertaion over coherent transmissions. .	In this paper, CSI on two schemes were considered.	AT with PE	EST

MIMO-FSO Relay	[30]	Evaluating the EST of MIMO with relay stations.	An adaptive scheme with selective relaying depending on CSI that is available in the sender is present.	AT foggy weather	EST
MISO-FSO	[36]	Enhancing the ASC via MISO schemes.	To decrease the fading effects in FSO channels, use spatial diversity at the transmitter.	generalized misalignment and AT	ASC
Hybrid FSO/RF	[39]	Analysing the PLS of hybrid FSO/RF scheme	Different system and channel parameters, are formulated with derivative security metrics for analysing the PLS.	AT with PE	ASC, SOP, SPSC
Mixed RF-FSO	[52]	Passive eavesdropper of secure dual-hop RF-FSO.	Assessment of the capabilities of the hyper-Gamma RF and G-G FSO mixed systems against malevolent passive eavesdropper assaults.	AT	ASC, SOP, SPSC

4 Research Issues in FSO Systems that are Still Unsolved

Despite the past literature, the issues that might be tackled in future research, these various recommendations and open issues will aid in development of the PLS in FSO schemes:

1- PLS evaluation in multiuser mixed FSO-RF scheme. The multiple users' optical signals are sent via FSO links from the relay node to the destination side via an RF link. The relay could be applied with a laser diode and capable of receiving and converting multiple optical signals into a radio frequency signal of another type. Studying PLS in multiuser mixed FSO-RF systems differs from studying PLS in single FSO link-based systems due to the specific features of such systems.

2- Increasing the secrecy rate in mixed FSO-RF systems by optimising relays beamforming. The distribution of RF and the distribution of genuine users and eavesdroppers may affect the optimization problem.

3- Investigating the PLS in hybrid RF/FSO schemes, in which many eavesdroppers can target either RF or FSO link, or both links at the same time. Data is sent over both links simultaneously in hybrid RF/FSO systems. As a result, from a security standpoint, it is critical to research and investigates this system model while several eavesdroppers target both links at the same time.

4- NOMA in FSO systems is an important open research area. Several recent studies have focused on using PLS to safeguard NOMA in RF networks, but no research has been done to date on PLS in NOMA-FSO. It is vital to optimise and analyse the PLS in NOMA-FSO based systems due to the unique properties of FSO systems.

5- A study of the security-reliability tradeoff in multiuser FSO user scheduling. In the literature, the multiuser FSO with opportunistic user scheduling systems is rarely researched and examined. Furthermore, trade-off analysis of reliable security for this type of FSO system has never been examined before, to the author's knowledge.

5 Conclusion

FSO provides many advantages over conventional existing radio or microwave techniques. FSO systems are more secure than transmitting radio systems due to the extremely directional optical beam, the limits of the eavesdropper location, and the practicality of its operating technique. The FSO, on the other hand, is particularly sensitive to atmospheric turbulence, and bad weather will result in FSO transmission interruptions and a significant reduction in overall system performance. Both the information-theoretic and security mechanisms components of FSO systems are addressed by the solutions given here. SISO FSO link-based systems, mixed FSO-RF, and hybrid FSO/RF systems were among the FSO systems examined. We also looked at how input signalling techniques, the FSO network's atmospheric turbulence parameters, the location of eavesdroppers, and the availability of CSI at the sending nodes all influence secrecy performance. Furthermore, we identified a number of outstanding research problems with significant potential for improving the security of current FSO systems.

References

[1] Yongpeng W., Khisti A., Xiao C., Caire G., Wong K-K., Gao X. A Survey of physical layer security techniques for 5G wireless networks and challenges ahead. IEEE Journal on Selected Areas in Communications. 2018; 36(4): 679-695.

[2] Shakir W.M.R. Performance analysis of the hybrid MMW RF/FSO transmission system. Wireless Personal Communications. 2019; 109(4): 2199-2211.

[3] Sun X., Djordjevic I. B. Physical-layer security in orbital angular momentum multiplexing free-space optical communications. IEEE Photonics Journal. 2016; 8(1): 1-10.

[4] Rubén B-R., García-Zambrana A., Castillo-Vázquez B., Qaraqe K. Secure communication for FSO links in the presence of eavesdropper with generic location and orientation Optics Express. 2019; 27(23): 34211-34229.

[5] Zhou X., Zhang Y., Song L. Physical layer security in wireless communications. CRC Press, 2016.

[6] Obeed M., Mesbah W. Efficient algorithms for physical layer security in two-way relay systems. Physical Communication. 2018; 28: 78–88.

[7] Massey J. L. An introduction to contemporary cryptology. Proceedings of the IEEE. 1988; 76(5):533–549.

[8] Wyner A. D. The wire-tap channel. Bell Labs Technical Journal. 1975; 54(8):1355–1387.

[9] Obeed M., Salhab A. M., Alouini M.-S, Zummo S. A. Survey on physical layer security in optical wireless communication systems. *Proceedings of Seventh International Conference on Communications and Networking (ComNet)*: 2018, Hammamet, Tunisia: 2018, p. 1-5,

[10] Kim I. I., Korevaar E. Availability of free-space optics (FSO) and hybrid FSO/RF systems. Optical Wireless Communications IV, E. Korevaar, ed., *Proceedings of SPIE*. 2001. Bellingham WA USA. 4530(1): p-84–95.

[11] Paul P., Bhatnagar M. R., Jaiswal A. Jamming in free space optical systems: mitigation and performance evaluation. IEEE transactions on communications. 2020; 68(3): 1631–1647.

[12] Lopez-Martinez F. J., Gomez G., Garrido-Balsells J. M. Physical layer security in free-space optical communications. IEEE Photonics Journal. 2015; 7(2).

[13] Endo H., Han T. S., Aoki T., Sasaki M. Numerical study on secrecy capacity and code length dependence of the performances in optical wiretap channels. IEEE Photonics Journal. 2015; 7(5): 1–18.

[14] Endo H., Fujiwara M., Kitamura M., Ito T., Toyoshima M., Takayama Y., et al. Free-space optical channel estimation for physical layer security. Optics express. 2016; 24(8): 8940–8955.

[15] Saber M. J., Sadough S. On secure free-space optical communications over Malaga turbulence channels. IEEE wireless communications letters. Lett. 2017; 6(2): 274–277.

[16] Pan X., Ran H., Pan G., Xie Y., Zhang J. On secrecy analysis of DF based dual hop mixed RF-FSO systems. IEEE Access. 2019; 7: 66725-66730.

[17] Pattanayak D. R., Dwivedi V. K., Karwal V. Physical layer security of a two-relay based mixed RF/FSO network in presence of multiple eavesdroppers. Optics communications. 2020; 463: 125429.
[18] Fujiwara M., Ito T., Kitamura M., Endo H., Tsuzuki O., Toyoshima M., et al. Free-space optical wiretap channel and experimental secret key agreement in 7.8 km terrestrial link. Optics express. 2018; 26(15): 19513–19523.
[19] Endo H., Fujiwara M., Kitamura M., Tsuzuki O., Ito T., Shimizu R., et al. Free-space optical secret key agreement. Optics express. 2018; 26(18): 23305–23332.
[20] Legre M., Huttner B. Quantum-enhanced physical layer cryptography: a new paradigm for free-space key distribution. *Proceedings of International Conference in Quantum Crypto. (QCRYPT)*. Cambridge, UK, Sept. 2017, p. 1–3.
[21] Ai Y., Mathur A., Verma G. D., Kong L., Cheffena M. Comprehensive physical layer security analysis of FSO communications over Málaga channels. IEEE Photonics Journal. 2020; 12(6): 1-17.
[22] Sánchez J.D.V. et.al. Survey on physical layer security for 5G wireless networks. Annals of Telecommunications. 2021; 76: 155–174.
[23] Eghbal M., Abouei J. Security enhancement in free-space optics using acousto-optic deflectors. IEEE/OSA Journal of Optical Communications and Networking. 2014; 6(8), 684–694.
[24] Zou D., Xu Z. Information security risks outside the laser beam in terrestrial free-space optical communication. IEEE Photonics Journal. 2016; 8(5): 1–9.
[25] Zhu J., Chen Y., Sasaki M. Average secrecy capacity of free-space optical communication systems with on-off keying modulation and threshold detection. *Proceedings of IEEE International Symposium on Information Theory and Its Applications (ISITA)*, 30 Oct.-2 Nov. 2016, Monterey, CA, USA, 2016, p. 616–620.
[26] Wang T.-L., Gargano J. A., Djordjevic I. B. Employing Bessel- Gaussian beams to improve physical-layer security in free-space optical communications. IEEE Photonics Journal. 2018; 10(5).
[27] Monteiro M. E. P., Revelator J. L., Souza R. D., Briante G. Maximum secrecy throughput of MIMOME FSO communications with outage constraints. IEEE Transactions on Wireless Communications. 2018; 17(5): 3487–3497.
[28] Wang T.-L., Djordjevic I. B. Physical-layer security of a binary data sequence transmitted with Bessel-Gaussian beams over an optical wiretap channel. IEEE Photonics Journal. 2018; 10(6).
[29] Huang Q., Liu D., Chen Y., Wang Y., Tan J., Chen W. et al. Secure free-space optical communication system based on data fragmentation multipath transmission technology. Optics Express. 2018; 26(10):13536–13542.
[30] Monteiro M. E. P. et al. Effective secrecy throughput analysis of relay-assisted free-space optical communication. Physical communication.2019; 35: 100731.
[31] Trinh, P. V., Carrasco-Casado, A., Pham, A. T., & Toyoshima, M. Secrecy analysis of FSO systems considering misalignments and eavesdroppers location. IEEE Transactions on communications. 2020; 68(12): 7810-7823.
[32] García-Zambrana A, Boluda-Ruiz R, Castillo-Vázquez C, Castillo-Vázquez B. Novel space-time trellis codes for free-space optical communications using transmit laser selection. Optics express. 2015;23(19):24195-211.
[33] Boluda-Ruiz R, García-Zambrana A, Castillo-Vázquez B, Castillo-Vázquez C. On the capacity of MISO FSO systems over gamma-gamma and misalignment fading channels. Optics express. 2015;23(17):22371-85.
[34] Boluda-Ruiz R, C. Castillo-Vázquez B, García-Zambrana A, Qaraqe K. On the average secrecy capacity for FSO wiretap channels with nonzero boresight pointing errors. *Proceedings of 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall)*, 2018, Chicago, IL, USA, 2018, p. 1–5.
[35] Boluda-Ruiz R, Tokgoz SC, Garcia-Zambrana A, Qaraqe K. Asymptotic average secrecy rate for MISO free-space optical wiretap channels. *Proceeding of 2019 IEEE 20th International Workshop on Signal Processing Advances in Wireless Communications (SPAWC)*. IEEE; 2019, p. 1–5.
[36] Boluda-Ruiz R, Tokgoz SC, Garcia-Zambrana A, Qaraqe K. Enhancing secrecy capacity in FSO links via MISO systems through turbulence-induced fading channels with misalignment errors. IEEE photonics journal. 2020; 12(4): 1–13.

[37] Ai Y, Mathur A, Lei H, Cheffena M, Ansari IS. Secrecy enhancement of RF backhaul system with parallel FSO communication link. Optics communications. 2020; 475:126193.
[38] Kafafy M, Fahmy Y, Khairy M, Abdallah M. Secure backhauling over adaptive parallel mmWave/FSO link. *2020 IEEE International Conference on Communications Workshops (ICC Workshops)*. IEEE; 2020. Dublin, Ireland, June, 2020, p 1-6.
[39] Shakir WMR. Physical layer security performance analysis of hybrid FSO/RF communication system. IEEE access. 2021;9:18948-61.
[40] Abd El-Malek AH, Salhab AM, Zummo SA, Alouini M. Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling. IEEE transactions on wireless communications. 2016;15(9):5904-18.
[41] Lei H., Dai Z., Ansari I. S., Park K. H., Pan G., Alouini M. S. On secrecy performance of mixed RF-FSO systems. IEEE Photonics Journal. 2017; 9 (4): 1–14.
[42] Abd El-Malek AH, Salhab AM, Zummo SA, Alouini M. Effect of RF interference on the security-reliability tradeoff analysis of multiuser mixed RF/FSO relay networks with power allocation. Journal of lightwave technology. 2017;35(9):1490-505.
[43] Yang L, Liu T, Chen J, Alouini M. Physical-layer security for mixed η-μ and M- distribution dual-hop RF/FSO systems. IEEE transactions on vehicular technology. 2018;67(12):12427-31.
[44] Lei H, Luo H, Park KH, Pan G, Ren Z, Alouini M. On secrecy performance of mixed RF-FSO systems with channel imperfection. IEEE Photonics Journal. 2018; 10(4): 1-13.
[45] Lei H, Dai Z, Park K, Lei W, Pan G, Alouini M. Secrecy outage analysis of mixed RF-FSO downlink SWIPT systems. IEEE transactions on communications. 2018; 66(12): 6384-95.
[46] Odeyemi KO, Owolawi P.A. Physical layer security in mixed RF/FSO system under multiple eavesdroppers collusion and non-collusion.Optical and Quantum Electronics. 2018; 50(7): 1-19.
[47] Saber MJ, Keshavarz A, Mazloum J, Sazdar AM, Piran MJ. Physical-layer security analysis of mixed SIMO SWIPT RF and FSO fixed-gain relaying systems. IEEE systems journal. 2019;13(3):2851-8.
[48] Ai Y, Mathur A, Cheffena M, Bhatnagar M, Lei H. Physical layer security of hybrid satellite-FSO cooperative systems. IEEE Photonics Journal. 2019; 11(1): 1–14.
[49] Lei H, Luo H, Park K, Ansari IS, Lei W, Pan G, et al. On secure mixed RF-FSO systems with TAS and imperfect CSI. IEEE transactions on communications. 2020;68(7):4461-75.
[50] Pan X, Ran H, Pan G, Xie Y. Zhang J. Secrecy analysis for multi-relaying RF-FSO systems with a multi-aperture destination. IEEE Photonics Journal. 2020; 12(2): 1-11.
[51] Pattanayak DR, Dwivedi VK, Karwal V, Ansari IS, Lei H, Alouini M., On the physical layer security of a decode and forward based mixed FSO/RF cooperative system. IEEE Wireless Communications. Letters. 2020; 9(7): 1031-1035.
[52] Pattanayak DR, Dwivedi VK, Karwal V. On the physical layer security of hybrid RF-FSO system in presence of multiple eavesdroppers and receiver diversity. Optics Communications. 2020; 477: 126334.
[53] Tubail D, El-Absi M, Salhab A, Ikki S, Zummo S, Kaiser T. Physical layer security of interference aligned mixed RF/unified-FSO relaying network. IET Communications. 2020; 14(14): 2282–2293.
[54] Wang Z, Shi W, Liu W, Zhao Y Kang K. Performance analysis of full duplex relay assisted mixed RF/FSO system. Optics Communications. 2020; 474: 126170.
[55] Islam S. et al. On secrecy performance of mixed generalized Gamma and Málaga RF-FSO variable gain relaying channel. IEEE Access. 2020; 8: 104127-104138.
[56] Sarker N. et al., Secrecy performance analysis of mixed Hyper-Gamma and Gamma-Gamma cooperative relaying system. IEEE Access. 2020; 8: 131273-131285.