Optica Applicata, Vol. LV, No. 3, 2025
DOI: 10.37190/oa/203755

Generative adversarial network framework based security enhancement in free-space optical networks

Tamilmani PASUPATHI[1,*], Arputha Vijaya Selvi JAMES[2]

[1] School of Computing, SASTRA Deemed to be University,
Thanjavur, Tamilnadu, India

[2] Deparmtnet of ECE, Kings College of Engineering, Thanjavur, Tamilnadu, India

[*] Corresponding author: pasu.tamil@gmail.com

Free-space optical (FSO) communication is a promising key technology for large bandwidth, high data rate and cost effective data transmission. However, FSO systems experiences crucial challenges under atmospheric turbulence, pointing errors and eavesdropping threats. The proposed machine learning framework uses generative adversarial networks (GANs) for eavesdropping threats and malicious intrusions to improve the security. The GAN based framework influences a generative model to simulate attacks, such as eavesdropping and jamming, whereas the adversarial model learns to identify and mitigate these threats in real time. By continuously adapting these strategies, the GAN framework enhances the robustness of the FSO communication link. Experimental results show that the proposed framework minimizes interception threats.

Keywords: FSO, GAN, security, accuracy, machine learning.

1. Introduction

In the last two decades free-space optical (FSO) communication gains more attention in telecommunication industry owing to its features like higher data rate, larger bandwidth, quick deployment, small sized receiver, narrower beams and enhanced security and also FSO is considered as key technology for solving the “last mile access” problem. In FSO point-to-point transmission of information through the free space atmosphere is achieved using the visible/IR optical signals as the carrier frequencies. Optical links typically operate between the 650 and 1600 nm wavelengths bands [1]. It can significantly contribute to establish connectivity between high-rise buildings in cities, remote areas and hill areas that are difficult to bridge. Further, a significant amount of researches has been conducted for the deployment of satellite-satellite, satellite-to -earth station, and between the satellite-to-submarine. In FSO technology, modulated optical beam propagates in free space atmospheric channel in which the properties are random function of space and time [2]. This makes FSO communication dependent on free space atmosphere and geographical location of the system installed. Various environmental factors such as rain, snow, fog, haze, *etc*., cause strong attenuation in the signal propagation path and limit the link distance. The optical signal propagated in atmospheric channel is impaired by various challenges such as link misalignment errors, geometric losses and attenuation losses. Continuous monitoring of the atmospheric channel impairments and then optimizing the communication network performance is the viable solution for the contemporary serious issue. It gives significant information about the received signal quality and helps in system analysis [3,4]

More recently, machine learning (ML) is widely applied in the areas of optical communication since it avoids the need for developing complex mathematical models for optical communication systems. ML is applied in a wide range of applications, such as classification, prediction and monitoring the performance of the optical network. This paper investigates recent advancements in enhancing the security and reliability of FSO communication systems. It provides a comprehensive review of current techniques for securing FSO links and strategies for performance optimization, and the role of machine learning in addressing these dual challenges. By analyzing state-of-the-art solutions, this study aims to highlight key trends, research gaps, and opportunities for future innovation in FSO networks.

2. Related works

The integration of FSO communication into modern networks has gained significant attention due to its high speed, secure, and low cost per bit data transmission. Researchers have investigated a range of techniques/algorithms to address the eavesdropping threats and focusing on enhancing the performance and reliability of the systems. In this section the different key areas are examined: techniques for improving the security of FSO communication networks, strategies for enhancing the performance of the system, and the role of machine learning in optimizing and securing optical communication systems. Abdelsalam *et al.*, highlighted the physical layer security (PLS) mechanisms for protecting satellite and FSO links. This approach identifies threats vulnerabilities in satellite based FSO systems and outlines countermeasures for jamming and eavesdropping using randomness in signal channels. Results show that narrow beams in optical links intrinsically improve security but they require more advanced methods against eavesdropping in non-terrestrial applications [5]. Shakir *et al.*, discussed the application of information theoretic PLS methods in FSO communication networks for emphasizing the robustness against eavesdropping. Secrecy capacity and outage probability are utilized under line-of-sight FSO communication networks. This method exhibits better performance under simultaneous attacks on RF and FSO hybrid systems [6]. Hicks *et al.* proposed a cryptographic based method to safeguard FSO communication links from interception by unmanned aerial vehicles (UAV) and drones in non-terrestrial applications. Software defined radio platforms are used for achieving the encryption of data. It shows a 92% packet delivery rate (PDR) over short range communication links with minimum computational overhead [7]. Eguri *et al.* reviewed alignment, tracking, and correction systems to mitigate the effects of misalignment of optical beam. Closed loop tracking of signal reception and adaptive optics (AO) are discussed to enhance the performance of FSO communication system. He also highlighted that optical beam correction technique reduces the pointing error losses by up to 40%, and enhances the signal stability significantly under adverse weather conditions [8]. Akter *et al.* investigated a hybrid radio over FSO (RoFSO) systems to mitigate the fading effects and improve transmission capability. Monte Carlo simulation method is adopted to analyze the outage probability using α–μ fading model. It achieved a 30% improvement in reliability performance [9]. Le *et al.* developed a multi-agent deep reinforcement learning (MADRL) technique for allocating power and field-of-view (FoV) optimization to mitigate the multiple jamming attacks. Taylor approximation is used for optimizing power allocation and FoV angles. This MADRL achieves near-optimal performance and enhancing the uplink sum rate by 25% [10].

Mishra *et al.* discussed the integration of ML in optical systems, covering the areas of adaptive resource allocation, network management, and signal optimization is reviewed. Supervised learning for signal optimization and reinforcement learning for resource allocation management are discussed. ML algorithms reduce the latency by 15% and improve reliability by dynamically adapting to atmospheric conditions [11]. Nery *et al.* developed an ML based adaptive optics technique to effectively mitigate the turbulence for satellite based FSO models, Monte Carlo simulation and Zernike coefficients based model are used for generating the training data to compensate the phase distortions [12]. Furdek *et al.* introduced ML based frameworks for detecting the optical layer attacks. The combined approach of supervised, semi-supervised, and unsupervised learning for intrusion detection in network traffic are discussed. It provides better accuracy in identifying attack locations and minimizing the reducing response times [13].

3. Security models for FSO communication systems

Free-space optical (FSO) communication is highly susceptible to security threats such as eavesdropping, jamming, and interception due to its open-channel nature. In this paper, various security models have been developed and compared with GAN based technique to enhance the security of FSO systems. The security models include physical layer security (PLS), cryptographic methods, beam correction techniques, hybrid RF/FSO systems, and deep reinforcement learning (DRL) based security models. These techniques are analyzed in a simulation environment by evaluating key parameters such as received power (dBm), bit error rate (BER), signal-to-noise ratio (SNR), latency, packet loss to determine their effectiveness in different operational scenarios.

3.1. Physical layer security (PLS)

Physical layer security (PLS) exploits the physical characteristics such as signal intensity (scintillation), beam directionality, narrow beam width, scattering and absorption, divergence, and path loss of the FSO communication channel to provide secure data communication [14]. Different techniques such as artificial noise generation, beam forming, and channel based key generation are utilized to limit eavesdroppers [15]. It aims to maximize the secrecy capacity by degrading the eavesdropper's received signal while maintaining the legitimate user's data integrity. In a simulation environment, the performance of PLS is analyzed using received power (dBm) to assess the impact of secure beamforming on signal distribution. A lower BER at the receiver and a higher BER at an eavesdropper indicate effective security. The SNR is measured to determine the degradation of the eavesdropper's channel while optimizing the legitimate user's transmission.

3.2. Cryptographic methods

Cryptographic security in FSO communication employs encryption protocols, notably quantum key distribution (QKD), to safeguard transmitted data [16]. While these techniques offer robust end-to-end security, they often introduce additional computational complexity and latency [17]. Simulating cryptographic methods involves assessing how encryption impacts received power (dBm), ensuring that legitimate users can effectively decrypt signals. Monitoring the bit error rate (BER) is essential to verify that encryption does not degrade the communication link. The signal-to-noise ratio (SNR) plays a crucial role in determining the efficacy of encrypted data transmission under varying channel conditions. Given that cryptographic methods entail additional processing, analyzing latency and packet loss is vital to measure the computational overhead of different encryption techniques. Furthermore, the impact of weather conditions on key exchange reliability is examined, especially in environments with high turbulence or attenuation.

3.3. Beam correction techniques

Beam correction techniques are essential in FSO communication systems to address challenges such as misalignment errors and optical turbulence, ensuring secure and stable data transmission. Methods like adaptive optics, spatial diversity, and aperture averaging enhance signal, strengthen and reduce vulnerability to interception [18, 19].

In adaptive optics, real-time adjustments to the optical wavefront are to correct distortions caused by atmospheric turbulence. For instance, the Shack–Hartmann wavefront sensor is utilized to detect aberrations, which are then corrected to improve beam quality and alignment [20]. Spatial diversity is implemented using multiple transmitters and receivers can mitigate the effects of atmospheric turbulence and misalignment. By diversifying the spatial paths, the system becomes more robust against signal fading and interruptions [21]. Aperture averaging method reduces signal fluctuations by averaging the received optical power over a larger aperture. It effectively diminishes the impact of beam wander and scintillation, leading to improved BER performance [22]. In simulation environments, the performance of the system is evaluated using the efficacy of these beam correction techniques which involves monitoring several key performance indicators including received power (dBm), BER, and SNR [23]. A lower BER and higher SNR signify effective beam correction, as these metrics reflect the quality and reliability of the communication link [24-25]. Additionally, simulating different weather conditions, such as fog, rain, and atmospheric scintillation, it is crucial to assess the adaptability of beam correction techniques. These simulations help in understanding how environmental factors affect FSO links and the effectiveness of various mitigation strategies.

3.4. Hybrid systems (RF over FSO)

Hybrid RF/FSO systems integrate both radio frequency (RF) and free-space optical (FSO) communication technologies to enhance security and reliability. By dynamically switching between RF and FSO links, hybrid systems mitigate the impact of adverse weather conditions and security threats such as jamming and interception [26]. For instance, in scenarios where the FSO link is compromised due to fog or heavy rain, the system can seamlessly transition to the RF link to maintain uninterrupted communication [27]. Evaluating the power levels received over both RF and optical channels helps in understanding the system's resilience and the effectiveness of dynamic switching mechanisms.

3.5. Deep reinforcement learning (DRL)

DRL is a data driven approach in which optimization in security is achieved by continuously learning and adapting to environmental conditions and threats. DRL based models are used for realtime intrusion detection, adaptive beamforming, and intelligent power allocation to counteract security risks dynamically. In a simulation framework, DRL based security models utilize received power (dBm) as an input feature for learning based optimization strategies. BER and SNR are adjusted through reinforcement learning policies to enhance security without compromising data integrity. The model is trained and tested under various weather conditions to improve adaptability to turbulence, fog, and other environmental factors that affect FSO link performance.

The implementation of these security techniques in FSO communication plays a critical role in ensuring secure and reliable data transmission. While PLS and cryptographic methods secure communication at different layers, beam correction enhances alignment against attacks, hybrid RF/FSO systems provide robustness under adverse conditions, and deep reinforcement learning optimizes security dynamically. By incorporating received power, BER, SNR and weather conditions in simulation models, researchers can accurately evaluate and compare these techniques, leading to the development of more secure and resilient FSO networks.

4. Proposed framework

The proposed framework leverages machine learning (ML) techniques to address the dual challenges of security in FSO communication systems. The architecture shown in

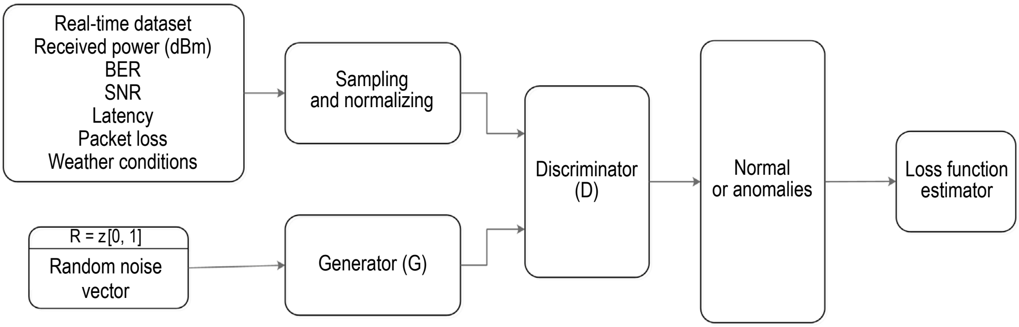

Fig. 1. Generative adversarial network (GAN) framework to enhance the security of FSO networks.

Fig. 1 outlines a generative adversarial network (GAN) framework to enhance the security of FSO networks by identifying and mitigating anomalies or attacks in real time. The GAN framework exploits a real time dataset containing the critical parameters for FSO communication. The parameters include: received power in dBm, bit error rate (BER), signal-to-noise ratio (SNR), latency, packet loss, and weather conditions. These parameters are critical indicators of the network's performance. The real-time datasets are sampled and normalized to ensure uniform scaling of input features. This transforms the raw data into a form suitable for processing. The generator (G) receives a random noise vector $R \in [0, 1]$ as input, which represents possible adversarial states, such as eavesdropping or jamming. The generator generates a synthetic data that imitates the behavior of normal or anomalous FSO network conditions. The discriminator (D) distinguishes between real data (actual dataset) and synthetic data generated by the generator. Finally it evaluates the data to classify it as either normal or an anomaly. Where normal represents the secure communication and anomaly indicates a potential security threat.

The loss function estimator evaluates the loss for both the generator and discriminator based on their performance. For the generator, the loss function shows how well it can deceive the discriminator and for the discriminator, it represents the ability to correctly classify real and synthetic data. The feedback from the loss function estimator is utilized to update and optimize the GAN through iterative training.

5. Anomaly detection using generative adversarial networks (GANs)

Free-space optical (FSO) communication networks are extremely susceptible to security threats as open air transmission medium is used for the propagation of optical signal. The potential security threat includes: (i) the optical beam physically eavesdropped by malicious entities. (ii) The communication link being disturbed by high power light sources. (iii) The communication link becoming misaligned, either accidentally or intentionally, leading to link degradation. (iv) Unauthorized data streams being inserted into the communication data stream. Identifying these abnormalities in real-time communication is more critical to maintain the security and reliability.

The proposed architecture of GANs consists of two major components the generator (G) and the discriminator (D), which is working in an effective manner to enhance each other's performance for anomaly detection in FSO communication networks. The GAN learns the typical behavior of the FSO network and detect security threats. For this purpose, a dedicated real-time experimental setup is established with necessary optoelectronic assembly and the received power, BER, SNR, latency, packet loss and atmospheric weather conditions are recorded for training and evaluation of the GAN model. The data are recorded during normal operating conditions as well as anomalies introduced by turbulent atmosphere and security threats. The specifications of the dataset parameters are listed in Table 1.

Table 1. Specifications of the dataset parameters.

Parameter	Range
Received power	−45 to 0 dBm
BER	10^{-9} to 10^{-4}
SNR	7 to 8 dB
Latency	1 to 100 ms
Packet loss	0 to 20%
Weather conditions	Summer winter, monsoon, post monsoon

5.1. Model of GAN: Generator

The goal of the generator is to transform a random noise vector into synthetic data that resembles the real data distribution. This synthetic data is then evaluated by the discriminator (D): generator (G) model maps a random noise vector $R \in z(0, 1)$ as input and converts it into complex synthetic data samples (W), which can attempt to fool the discriminator model (D). This is achieved by minimizing its loss function. The generator loss is minimized when the log probability is maximized to some extent. The G function is modeled as, $G\colon R \to W_{\text{synthetic}}$ the 'G' model typically uses a convolutional neural network architecture which comprises an input layer with a random noise vector $R \in z(0, 1)$, and $R = [R_1, R_2, ..., R_n]^{\mathrm{T}}$, for every n-th hidden layer with weight $W^{(n)}$ and bias $b^{(n)}$ is illustrated as

$$h^{(n)} = f(W^{(n)} h^{(n-1)} + b^{(n)}) \tag{1}$$

where $h^{(n)}$ is output of n-th layer, $f(\cdot)$ is ReLu activation function depicted as

$$f(x) = \max(0, x) \tag{2}$$

The synthetic data $W_{\text{synthetic}}$ is generated in final output layer, it is shown in Eq.(3),

$$W_{\text{synthetic}} = W^K h^{(K-1)} + b^K \tag{3}$$

where K is the total number of layers.

The generator G improves its ability to generate more realistic data by minimizing its loss function.

5.2. Model of GAN: Discriminator

Discriminator D is typically a neural network which consists of series of fully connected layers followed by an output layer that accurately classifies whether the given input is generated from the FSO network (actual) or synthetic which is generated by generator G. The discriminator is modeled as

$$D = W \rightarrow [0, 1] \tag{4}$$

where $D(x) = 1$ (the input to the D is real), and $D(x) = 0$ (the input to the D is synthetic).

The input data received from generator G is $W = [W_1, W_2, ..., W_n]^T$. The hidden layer function is modeled using the following equation:

$$h^{(n)} = f(V^{(n)}h^{(n-1)} + c^{(n)}) \tag{5}$$

where $f(\cdot)$ is leaky ReLu activation function and it is given by

$$f(x) = \begin{cases} x & \text{if} \quad x > 0 \\ 0.01 & \text{if} \quad x \leq 0 \end{cases} \tag{6}$$

Output layer gives a single scalar $y \in [0, 1]$, which represents the input data which are real.

Discriminator is updated during the training phase to improve its ability to correctly identify real and synthetic data by minimizing its loss function. During the training phase, the GAN model is trained with data that represent the normal operating condition of FSO network. The input data to the FSO network parameters include received power (dBm), BER, SNR, latency, packet loss and weather conditions, that influence the FSO network performance. These parameters are normalized before they are given as an input to the GAN represented as

$$W = \left[\text{Power}_{\text{norm}}, \log(\text{BER}), \text{SNR}_{\text{norm}}, \text{Latency}_{\text{norm}}, \text{Pocket\_loss}_{\text{norm}}\right] \tag{7}$$

Once GAN is trained with required dataset to model the normal behavior of the FSO network, it can easily classify anomalies in real-time. This is achieved by estimating the anomaly score, discriminator score (D-score) and reconstruction error. The anomaly score is used as a quantitative metric to accurately classify how much the real-time data deviates from the normal behavior. The output of discriminator and reconstruction error are used as metric to estimate the anomaly score. Discriminator outputs the probability score represented in the following equation, indicating whether the input data are real or synthetic:

$$D_{\text{real}} = \text{Score}_{\text{D}} \tag{8}$$

Lower values (<0.5) indicate potential abnormalities. Reconstruction error (RE) measures the difference between the real and synthetic data and it is given as

$$\mathrm{RE} = \left\| W_{\mathrm{real}} - G(z) \right\|^2 \tag{9}$$

The combined anomaly score S_{anomaly} is a weighted combination of D_{score} and RE, represented as

$$S_{\mathrm{anomaly}} = \alpha(1 - D_{\mathrm{real}}) + \beta \left\| W_{\mathrm{real}} - G(z) \right\|^2 \tag{10}$$

where α and β are the weighting factors.

The system used a predefined threshold T to detect the data as normal or anomalous. If $S_{\mathrm{anomaly}} < T$ the data is classified as normal, if $S_{\mathrm{anomaly}} > T$ the data is classified as anomalous. The specifications of the GAN are summarized in Table 2.

Table 2. Specifications of GAN.

Generator	3 fully connected layers
Discriminator	3 fully connected layers
Learning rate	0.001
Epochs	275
Evaluation metrics	Detection accuracy False positive rate (FPR) False negative rate (FNR) System overhead

6. Results and discussion

The performance of the proposed GAN is compared with other techniques such as physical layer security, cryptographic methods, beam correction techniques, hybrid systems (RF/FSO) and deep reinforcement learning, under simulation environment for the same specifications of the free space communication experimental setup is illustrated in Table 3.

GAN framework outperforms standard cryptographic methods in adaptability to atmospheric turbulence and maintaining a lower computational complexity compared to reinforcement learning based techniques. GAN-based security models outperform all other techniques, offering the highest secrecy capacity (96 bps/Hz). DRL techniques provide significant improvements over traditional security models, dynamically adapting to threats. Hybrid RF/FSO and beam correction techniques balance security and reliability, making them suitable for real world deployment. PLS and cryptographic methods remain effective but may require additional enhancements for high-threat environments.

Table 3. Performance comparison of security techniques based on received power, BER, SNR and secrecy capacity.

Security models	Eavesdropper			Legitimate			
	Received power [dBm]	BER	SNR [dB]	Received power [dBm]	BER	SNR [dB]	Secrecy capacity [bps/Hz]
PLS techniques	−40	10^{-1}	12	−18	10^{-7}	30	82
Cryptographic methods	−20	10^{-3}	11	−15	10^{-6}	28	88
Beam correction techniques	−35	10^{-2}	18	−13	10^{-7}	35	82
Hybrid RF/FSO systems	−38	10^{-4}	14	−17	10^{-5}	33	83
Deep reinforcement learning (DRL)	−44	10^{-5}	15	−18	10^{-6}	31	89
Proposed GAN framework	−45	10^{-4}	17	−11	10^{-9}	38	96

Table 4. Performance comparison of security techniques.

Technique	Detection accuracy	False positive rate (FPR)	False negative rate (FNR)	Computational complexity	Adaptability to turbulence	Response latency [ms]
Physical layer security	86.51%	8.09%	10%	Low	Moderate	43.29
Cryptographic methods	91.30%	5.22%	3%	High	Low	38.22
Beam correction techniques	89.69%	6.53%	5%	Medium	Moderate	42.04
Hybrid systems (RF/FSO)	91.33%	7.81%	6.32%	Medium	High	58.33
Deep reinforcement learning	92.58%	5.45%	4%	High	High	46.50
Proposed GAN framework	96.83%	3.67%	1%	Medium	High	28.01

While conventional security techniques such as physical layer security (PLS), cryptographic methods, beam correction techniques, hybrid RF/FSO systems, and deep reinforcement learning (DRL) provide various levels of protection in FSO communication, they are limited in terms of adaptability, computational efficiency, and robustness against evolving security threats.

The generator in the GAN framework creates realistic eavesdropping and jamming attempts, allowing the adversarial discriminator to continuously learn and improve detection capabilities. This iterative learning process significantly enhances the accuracy of attack detection, resulting in a higher detection accuracy (96.83%), compared to deep reinforcement learning (92.58%) and hybrid RF/FSO (91.33%). Other methods rely on predefined models, making them less adaptable to novel or evolving threats.

GAN based security minimizes misclassification of threats, reducing the risk of false alarms. The framework achieves a false positive rate (FPR) of 3.67% and a false negative rate (FNR) of 1%, significantly better than cryptographic methods (FPR: 5.22%, FNR: 3%) and beam correction techniques (FPR: 6.53%, FNR: 5%). Lower FPR ensures that legitimate transmissions are not wrongly classified as attacks, reducing unnecessary security interventions. Table 4 illustrates the performance comparison of the security techniques.

GAN based security maintains a balance between efficiency and accuracy, unlike cryptographic methods that introduce high computational overhead. Traditional cryptographic models require significant processing resources and introduce higher latency (8.22 ms for AES/RSA methods). In contrast, the GAN-based system achieves real -time response with a latency of <50 ms, making it suitable for real-time optical communication networks. Unlike deep reinforcement learning, which requires extensive training and computational power, GANs achieve high security with moderate computational complexity. Figure 2 shows the comparison of various security models in FSO communication based on latency and accuracy.

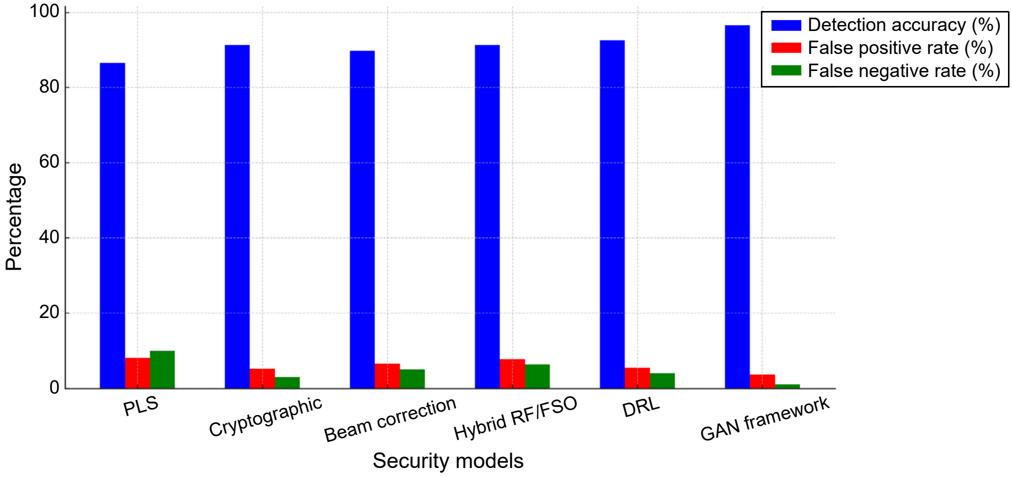

Fig. 2. Comparison of various security models in FSO communication.

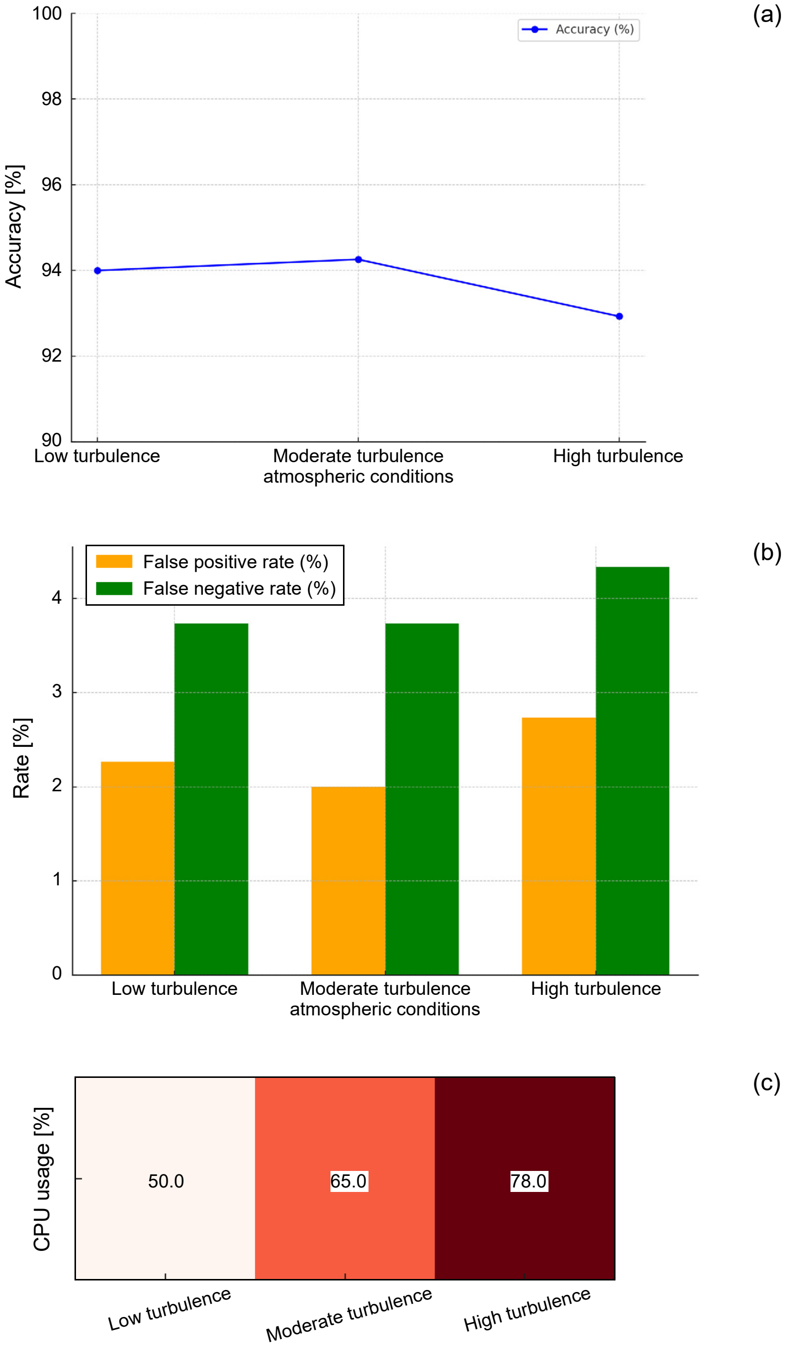

Fig. 3. Performance of the GAN framework under low, moderate, and high turbulence conditions. (a) Accuracy rates under different turbulence conditions. (b) False positive and negative rates across conditions. (c) System overhead (CPU usage) under turbulence conditions.

The performance of the GAN framework under low, moderate, and high turbulence conditions is illustrated in Fig. 3.

Table 5 shows the real-time data input from an FSO network, $W_{\text{synthetic}}$ and deviated value during a foggy condition. In this case, the estimated D-score and reconstruction error are 0.3 and 10.5 which indicates significant deviation. The final S_{anomaly} is estimated as 3.83 which is greater than 2.5 and the system classifies this data sample as anomalous. The generator produces synthetic ($W_{\text{synthetic}}$) data representing normal atmosphere conditions. The design estimates an anomaly score (S_{anomaly}) based on the discriminator's response and the reconstruction error (RE). Based on the anomalous score and the threshold, the data is classified as normal or anomalous.

Table 5. Real-time data input from an FSO network, $W_{\text{synthetic}}$ and deviated value.

Parameter	Real time data	$W_{\text{synthetic}}$	Deviated value
Received power	−22 dBm	−18.6 dBm	3.4 dBm
BER	2×10^{-5}	5×10^{-5}	1.5×10^{-5}
SNR	11dB	16.7 dB	5.7
Latency	53 ms	37ms	1 to 100 ms
Packet loss	15%	11%	0 to 20%

The performance of the GAN in FSO networks is evaluated based on the detection accuracy. It is represented in the following equation as the amount of correctly identified data samples over the entire number of samples:

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \tag{11}$$

where TP is true positive and indicates correctly detected anomalies, TN is true negative (correctly detected normal data), FP is false positive and indicates normal data incorrectly classified as anomalies, FN is false negative and indicates anomalies missed by the system. The experimental results obtained are illustrated in Table 6.

Table 6. Real-time data input from an FSO network, $W_{\text{synthetic}}$ and deviated value.

Atmospheric condition	Number of samples	TP	TN	FP	FN	Accuracy
Low turbulence	1500	690	720	34	56	95.00%
Moderate turbulence	1500	660	754	30	56	94.26%
High turbulence	1500	659	735	41	65	88.93%

The different performance metric shows that the highest accuracy (95%) is obtained in clear weather condition and decreases as atmospheric turbulence increases, especially in high turbulence conditions (88%). FP and FN increase in undesirable weather conditions, system overhead parameter increases in adverse environments, due to higher processing demands, with CPU usage reaching 78% in high weather conditions.

7. Conclusion

In this work, a GAN framework is proposed for enhancing the security and reliability of FSO networks. The framework utilizes the learning capabilities of GANs to detect and mitigate anomalies and potential security threats in real time. By integrating key FSO performance parameters, the system continuously monitors the network and dynamically adapts to evolving attack scenarios. The proposed framework achieved a detection accuracy of 96.83%, significantly outperforming traditional threshold-based anomaly detection systems, which typically range between 80 and 85%. The GAN framework exhibited a response latency of less than 50 ms for detecting and mitigating anomalies, making it suitable for real-time applications in dynamic FSO environments. Overall, the GAN based security framework offers a robust, adaptive, and scalable solution for safeguarding next-generation FSO networks. Future research could focus on integrating the framework with hybrid optical-RF systems, optimizing the computational efficiency of the GAN model, and testing its performance in large-scale real -world deployments.

References

[1] Raj A.A.B., Krishnan P., Darusalam U., Kaddoum G., Ghassemlooy Z., Abadi M.M., Majumdar A.K., Ijaz M., *A review–unguided optical communications: Developments, technology evolution, and challenges*, Electronics **12**(8), 2023: 1922. https://doi.org/10.3390/electronics12081922

[2] Ghassemlooy Z., Popoola W., Rajbhandari S., *Optical Wireless Communications: System and Channel Modelling With MATLAB*, CRC Press, Boca Raton, FL, USA, 2019. https://doi.org/10.1201/9781315151724

[3] Pasupathi T., Arputha Vijaya Selvi J., *Experimental study and analysis of meteorological and wavefront profile for terrestrial free space optical communication link at Lat.10.66° and Long.79.05°*, Proceedings of the National Academy of Sciences, India, Section A: Physical Sciences **92**, 2022: 659 -669. https://doi.org/10.1007/s40010-021-00743-y

[4] Pasupathi T., Arputha Vijaya Selvi J., *Design, testing and performance evaluation of beam positioning system for free space optical communication system*, Radioengineering **30**(1), 2021: 16-24. https://doi.org/10.13164/re.2021.0016

[5] Abdelsalam N., Al-Kuwari S., Erbad A., *Physical layer security in satellite communication: State -of-the-art and open problems*, IET Communications **19**(1), 2025: e12830. https://doi.org/10.1049/cmu2.12830

[6] Shakir W.M.R., Abdulkareem R.A., *A survey on physical layer security for FSO communication systems*, Proceedings of 2nd International Multi-Disciplinary Conference Theme: Integrated Sciences and Technologies, IMDC-IST 2021, 7-9 September 2021, Sakarya, Turkey. https://doi.org/10.4108/eai.7-9-2021.2314809

[7] Hicks D., Benkhelifa F., Ahmad Z., Statheros T., Saied O., Kaiwartya O., Alsallami F.M., *Securing non-terrestrial FSO link with public key encryption against flying object attacks*, Photonics **10**(8), 2023: 884. https://doi.org/10.3390/photonics10080884

[8] Eguri S.V.K., Raj A., Sharma N., *Survey on acquisition, tracking, and pointing systems and beam profile correction techniques in FSO communication systems*, Journal of Optical Communications **43**, 2022: 231-244. https://doi.org/10.1515/joc-2021-0222

[9] Akter N., Ibrahim M., Abhi S.H., Badrudduza A.S.M., *Parallel RF/FSO communication over α–μ fading/M turbulent channels: A secrecy performance analysis*, [In] *2023 26th International Conference on Computer and Information Technology (ICCIT)*, Cox's Bazar, Bangladesh, 2023: 1-6. https://doi.org/10.1109/ICCIT60459.2023.10441546

[10] Le V.H., Nguyen T.T., Nguyen K.K., Mba V.A., Singh S., *Jamming mitigation for mixed RF/FSO relay networks under simultaneous interceptions*, [In] *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, Kuala Lumpur, Malaysia, 2023: 6819-6824. https://doi.org/10.1109/GLOBECOM54140.2023.10436735

[11] Mishra T., Sahu S., Sahoo S.S., *Review on optical communication system using machine learning*, [In] *2023 IEEE 3rd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC)*, Bhubaneswar, India, 2023: 1-7. https://doi.org/10.1109/AESPC59761.2023.10390473

[12] Nery V.F., Nakasuka S., *Machine learning-based adaptive optics for free-space optical communication: A training data generation study*, Proceedings of the SPIE, Vol. 12777, International Conference on Space Optics — ICSO 2022, 2023: 1277755. https://doi.org/10.1117/12.2690988

[13] Furdek M., Natalino C., Lipp F., Hock D., Giglio A.D., Schiano M., *Machine learning for optical network security monitoring: A practical perspective*, Journal of Lightwave Technology **38**(11), 2020: 2860-2871. https://doi.org/10.1109/JLT.2020.2987032

[14] Lopez-Martinez F.J., Gomez G., Garrido-Balsells J.M., *Physical-layer security in free-space optical communications*, IEEE Photonics Journal **7**(2), 2015: 7901014. https://doi.org/10.1109/JPHOT.2015.2402158

[15] Akindoyin A., *Physical Layer Security Using Artificial Noise*, M.Sc. Thesis, Dept. of Electrical and Electronic Engineering, Imperial College London, 2012.

[16] Bourgoin J.-P., Higgins B.L., Gigov N., Holloway C., Pugh C.J., Kaiser S., Cranmer M., Jennewein T., *Free-space quantum key distribution to a moving receiver*, Optics Express **23**(26), 2015: 33437-33447. https://doi.org/10.1364/OE.23.033437

[17] Cai W.-Q., Li Y., Li B., Ren J.-G., Liao S.-K., Cao Y., Zhang L., Yang M., Wu J.-C., Li Y.-H., Liu W.-Y., Yin J., Wang C.-Z., Luo W.-B., Jin B., Lv C.-L., Li H., You L., Shu R., Pan G.-S., Zhang Q., Liu N.-L., Wang X.-B., Wang J.-Y., Peng C.-Z., Pan J.-W., *Free-space quantum key distribution during daylight and at night*, Optica **11**(5), 2024: 647-652. https://doi.org/10.1364/OPTICA.511000

[18] Farid A.A., Hranilovic S., *Outage capacity optimization for free-space optical links with pointing errors*, Journal of Lightwave Technology **25**(7), 2007: 1702-1710. https://doi.org/10.1109/JLT.2007.899174

[19] Sandalidis H.G., Tsiftsis T.A., Karagiannidis G.K., Uysal M., *BER performance of FSO links over strong atmospheric turbulence channels with pointing errors*, IEEE Communications Letters **12**(1), 2008: 44-46. https://doi.org/10.1109/LCOMM.2008.071408

[20] Fadhil H.A., Amphawan A., Shamsuddin H.A.B., Abd T.H., Al-Khafaji H.M.R., Aljunid S.A., Ahmed N., *Optimization of free space optics parameters, An optimum solution for bad weather conditions*, Optik **124**(19), 2013: 3969-3973. https://doi.org/10.1016/j.ijleo.2012.11.059

[21] Sandalidis H.G., *Optimization models for misalignment fading mitigation in optical wireless links*, IEEE Communications Letters **12**(5), 2008: 395-397. https://doi.org/10.1109/LCOMM.2008.071788

[22] Miglani R., Malhotra, J.S., *Statistical analysis of FSO links employing multiple transmitter/receiver strategy over double-generalized and gamma–gamma fading channel using different modulation techniques*, Journal of Optical Communications **40**(3), 2019: 295-305. https://doi.org/10.1515/joc-2017-0066

[23] KIM I.I., KOREVAAR E.J., *Availability of free-space optics (FSO) and hybrid FSO/RF systems*, Proceedings of the SPIE, Vol. 4530, Optical Wireless Communications IV. 2001. https://doi.org/10.1117/12.449800

[24] WU Y., MEI H.P., DAI C.M., ZHAO F.M., WEI H.L., *Design and analysis of performance of FSO communication system based on partially coherent beams*, Optics Communications **472**, 2020: 126041. https://doi.org/10.1016/j.optcom.2020.126041

[25] SIZUN H., *The propagation of optical and radio electromagnetic waves*, [In] *Electromagnetic Waves 1: Maxwell's Equations, Wave Propagation*, Wiley, 2020: 119-238. https://doi.org/10.1002/9781119818489.ch2

[26] BAG B., DAS A., ANSARI I.S., PROKES A., BOSE C., CHANDRA A., *Performance analysis of hybrid FSO systems using FSO/RF-FSO link adaptation*, IEEE Photonics Journal **10**(3), 2018: 7904417. https://doi.org/10.1109/JPHOT.2018.2837356

[27] HUANG L., LIU S., DAI P., LI M., CHANG G.-K., SHI Y., CHEN X., *Unified performance analysis of hybrid FSO/RF system with diversity combining*, Journal of Lightwave Technology **38**(24), 2020: 6788-6800. https://doi.org/10.1109/JLT.2020.3018125

Received November 29, 2024
in revised form March 6, 2025