INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2026, VOL. 72, NO. 2, PP. 1–8
Manuscript received October 9, 2026; revised April 2026. doi: 10.24425/ijet.2026.157921

Detecting and responding to attacks and weather effects in hybrid FSO/RF systems using the Dempster-Schaffer theory with AI algorithms

Ali Khwayyir, Mahdi Nangir, and Javad Musevi Niya

***Abstract*—In this paper, a new intelligent switch for hybrid Free-Space Optical (FSO) RF communication is proposed for improved reliability and security in the presence of dynamic environmental changes and cyber-attack interferences. Using Dempster-Shafer Theory (DST) for reliable threat classification and ANN, KNN, and SVM for machine learning, an extraordinary real-time communication link selection is achieved. A broad training dataset (10,000 simulated samples), covering eavesdropping and jamming threats, fog and dust effects, was used to train and validate the network. Our work combines DST to combine evidence from multiple sources and make an accurate belief assignment for communication modes. In addition, the system exhibits a high claimed confidence, RF and FSO link beliefs around 0.88-0.89 and 0.82-0.83, respectively. The machine learning models have excellent performance on threat detection and mode classification. ANN, KNN, and SVM obtained accuracies of 0.99986, 0.99984, and 0.99930, respectively. All models achieved near-perfect AUC values, where most classes reach 1, meaning a better discriminative performance. Importantly, the performance of ANN was significantly outperformed by KNN and SVM in all metrics, demonstrating its robustness. This work provides an efficient and dynamic approach to keep the communication in difficult FSO/RF links secure and reliable, and brightens the path for future communication systems.**

***Keywords*—FSO/RF; DST; ANN; KNN; SVM**

I. Introduction

COMMUNICATIONS systems are the backbone of modern society, supporting a wide range of applications from daily communications to critical infrastructure. However, with the increasing demand for high data rates and reliable communications, Free-Space Optical (FSO) communication systems have emerged as a promising solution[1][2]. It offers a massive bandwidth of over 100 GHz, and high data rates ranging from 10 Gbps to 100 Gbps (with 1 Tbps achieved in laboratory conditions using multiplexing). This makes it a compelling alternative to traditional Radio Frequency (RF) solutions in some applications [3]. However, FSO systems are very dependent on atmospheric conditions such as fog, dust and other meteorological phenomena that not only reduce the signal but also severely degrade system performance–thus the reliability and availability. Meanwhile, RF systems are well-suited for inclement weather conditions but offer lower bandwidth and data rates than FSO. To mitigate this inherent limitation of both technologies, hybrid FSO/RF systems have emerged as a promising solution [4][5]. Such systems are intended to provide a reliable and high-performance communication in the very high bandwidth FSO channel under fair weather, which switches to a robust RF link when atmospheric effects result in the lower availability of the FSO connection. In addition to the environmental issues, modern communication systems are confronting various complicated security problems as well. This includes different types of malicious cyber-attacks, interference, intentional or unintentional, and would undermine the integrity, confidentiality and availability of communications. Traditional defense approaches are inadequate in identifying such threats. Such identification requires advanced tools capable of processing large amounts of data and filtering it, pointing out irregular behavior or trends as they take place [6][7]. The weather, and the most important one is fog and dust, also have severe impacts on the FSO link. Fog is microscopic water droplets, which causes scattering and adsorption of optical signal, the optical signal serious attenuation and short-term communications transmission distance before error rate island using a waterside perspective. Furthermore, dust particles in the free space will cause attenuation and scattering of the signal, which could degrade the performance of the optical link. The impacts of extreme conditions are fewer RF systems than in FSO, but the effect is present [8]. Dempster-Shafer Theory (DST) is a mathematical combination rule for dealing with uncertainty and information from diverse sources. In contrast to classical probability theory, which assumes it is necessary to make specific value assignments for the probabilities required, in DST, uncertainty can be expressed by beliefs and plausibility sets of hypotheses. This tolerance to handle incomplete or DST's capability handling fuzzy information makes it especially well-suited for threat detection situations where data may be incomplete, uncertain and conflicting [9][10]. In the last couple of years, artificial neural networks (ANN), a type of (KNN) and support vector machines (SVM), among others, have been used and have made significant progress due to AI techniques [11]. These algorithms (and some others) are particularly effective over a wide range of applications, e.g., pattern recognition in which the types of patterns are not known beforehand; classification problems with unknown classes of items to classify; and

All authors are with Faculty of Electrical and Computer Engineering, University of Tabriz, Tabriz, Iran (e-mail: nangir@tabrizu.ac.ir, corresponding author; ali_khwayyir@tabrizu.ac.ir; niya@tabrizu.ac.ir).

anomaly detection, where it is only known for sure that only known as good or bad examples. Complex data sets are the food and drink of these algorithms [12]. They can decipher the code of complex structures and expose what had been hidden relationships. It is very important in threat detection and performance improvement in a communication system. These algorithms can process complex data sets, discover hidden correlations and derive from experience.[13]. Although much work has been done in hybrid FSO/RF systems, threat detection, and weather effects, and individually in applications of DST as well as AI algorithms[14][15]. There still exists a big gap for comprehensive integration of these components to meet the complex problems that are the threat detection in weather impact communication environments. Figure. 1 Illustration of a hybrid FSO/RF system's architectural structure and threats and weather conditions, integrating advanced AI and classification technology. This paper attempts to fill such a void by proposing a new approach that combines the power of DST in evidence combination with the learning ability of AI algorithms (ANN, KNN, and SVM) to enhance threat detection for Hybrid FSO/RF systems impacted by fog and dust. The main contributions of this paper are as follows: (1) we propose an innovative approach to threat detection specifically designed for hybrid FSO/RF systems. In particular, we incorporate the brutal influence of fog and detritus. Employing the sharing information platform of Dempster-Shafer theory decision systems and ANN, KNN, and SVM algorithms, detection accuracy and reliability are enhanced. (2) To our knowledge, no previous work has looked at such systematic integration of Dempster-Shafer theory with ANN, KNN, and SVM algorithms for threat detection in the context of weather-impacted hybrid FSO/RF systems.

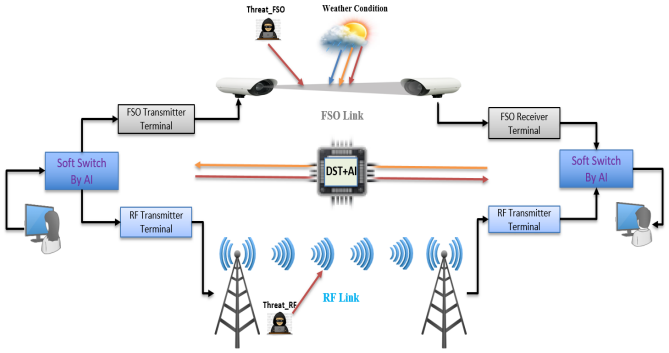

Fig. 1. FSO/RF hybrid system with DST and AI technology.

Such integration provides a unique ability to handle uncertainty and combine evidence from multiple sources (FSO-Threat data, RF-Threat data, weather sensor data such as Fog and Dust, Error point FSO data, and Quality factor FSO data), thereby improving detection decisions. (3) Harnessing the evidence fusion capabilities of DST and the learning and classification capabilities of AI algorithms, this approach aims to achieve higher detection accuracy and lower false alarm rates, compared to traditional methods that may not take into account uncertainty or changing environmental conditions. (4) This paper begins to set the stage for further research in the topic of intelligent and resilient communications systems, especially in challenging environments.

II. Methodology and Implementation

This section delineates the comprehensive methodology and intricate implementation details of an intelligent adaptive communication system designed to optimize Free-Space Optical (FSO) and Radio Frequency (RF) link performance under dynamic environmental conditions and security threats, as shown in Figure 2. The proposed work integrated a complex decision support system, which is based on the DST with advance machine learning techniques; these last algorithms are ANN, KNN and SVM [16]. This dual-use strategy enables dynamic link reclassification and makes autonomous decisions on intelligent cross-layering between a multitude of FSO and RF communications, as well as their cryptographically protected modalities. This paper details each stage of progress: from the first data collection, thoughtful preprocessing, to software deployment strategies that need change in real-time support of these small but important differences, with clearly explained mathematical derivations.

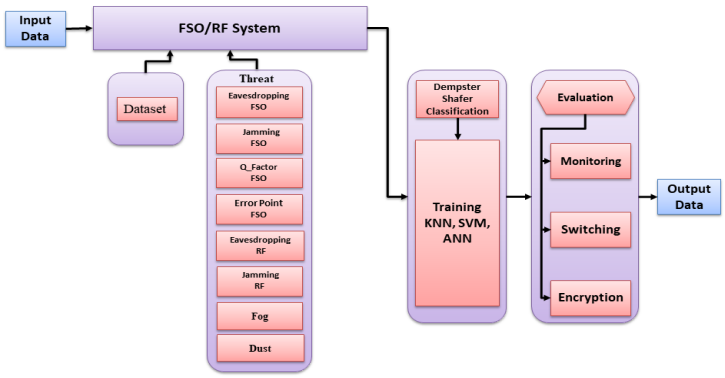

Fig. 2. Flow diagram of the proposed FSO-RF system model.

A. Data Acquisition and Characterization

The study focuses on 100,000 selected well-measured samples combined in a large-scale database, acquired from different weather stations. In this large pool of information, each instance holds environmental parameters, vital performance descriptive metrics for the communication link itself, and adds such information as is required to build a picture across all instances of link reliability and security posture. The system characteristics provided in this data set have been chosen to encompass a realistic representation of real-world operating conditions, so the statistics captured by the system can access invisible entities and thus make educated decisions about

optimal link selection and treatment strategies against security protocols. Key characteristics include:

- FSO Threat: A category for potential threats that affect the FSO link, such as No Threat, Eavesdropping, or Jamming.
- RF Threat: Threats that are confined to the RF link. Also sorted along these lines: No Threat, Eavesdropping, or Jamming.
- Fog: The level of mist and corresponding FSO link performance. Designations include Medium, High.
- Dust: The concentration of dust particles, which also affect FSO link quality lies between medium and High.
- Error Point FSO: An index showing how much error or otherwise the Communication link has reached, with categories like Very Good, Failure.
- Quality Factor FSO: Another performance indicator, measuring the overall quality factor of a link Example: Very Good, Good, Failure.
- Action: What mode of communication or action should be carried out according to the simulated circumstances, with choices being RF, FSO, CryptoFSO, CryptoRF.

This mixed type of data structure covering both the factors inside a particular environment and their security challenges guarantees that any model being trained is based on a mixed pool of cases. Such pools are far more varied (and conceivably more typical) than what yu'll find out in more general operational environments. With the cascading media generation method, all sorts of unpredictable atmospheric conditions and threat landscapes are produced, thus forming in *part a self-modifying, adaptable architecture whereby there can be communication systems which automatically adjust to resistance.

B. Dempster-Shafer Theory for Threat Classification and Estimation

The Dempster-Shafer Theory (DST) is often used as a theory about evidence, and is also a powerful mathematical guide for dealing with conditions of uncertainty and incomplete information. In this sense, it affords a very accurate view by allowing for the explicit representation of ignorance and combining evidence from different sources [17]. In the context of this intelligent communication system, DST is strategically employed to perform robust classification and estimation of the most appropriate communication link (e.g., direct FSO, cryptographically secured FSO, direct RF, cryptographically secured RF, or a state of inherent uncertainty) based on the real-time aggregation of observed environmental conditions and dynamic threat assessments.

C. Evidential Reasoning using Dempster-Shafer Theory

The initial classification and belief estimation were performed using Dempster-Shafer Theory, implemented in MATLAB. DST is employed to estimate belief levels for each action based on observed evidence[18]. The belief function $Bel : 2\Theta \rightarrow [0,1]$ quantifies the support assigned to a subset of hypotheses from a finite frame of discernment Θ={FSO,RF,CryptoFSO,CryptoRF, θ }.

1) Mass Function Formulation: FSO Threat Evidence (m_1):

$$m_1 = \begin{cases} \{\text{Crypto FSO}\}\text{:}0.9, \{\theta\} : 0.1 & \text{If FSO}_{\text{Threat}} = \text{"Eavesdropping"} \\ \{\text{RF}\}\text{:}0.9, \{\theta\} : 0.1 & \text{If FSO}_{\text{Threat}} = \text{"Jamming"} \\ \{\text{FSO}\}\text{:}0.9, \{\theta\} : 0.1, \{\theta\} : 1.0 & \text{If FSO}_{\text{Threat}} = \text{"Nan"} \\ \{\theta\} : 0.1 & \text{Otherwise.} \end{cases} \tag{1}$$

RF Threat Evidence (m_2):

$$m_2 = \begin{cases} \{\text{Crypto RF}\}\text{:}0.9, \{\theta\} : 0.1 & \text{If RF}_{\text{Threat}} = \text{"Eavesdropping"} \\ \{\text{FSO}\}\text{:}0.9, \{\theta\} : 0.1 & \text{If RF}_{\text{Threat}} = \text{"Jamming"} \\ \{\text{RF}\}\text{:}0.9, \{\theta\} : 0.1, \{\theta\} : 1.0 & \text{If RF}_{\text{Threat}} = \text{"Nan"} \\ \{\theta\} : 0.1 & \text{Otherwise.} \end{cases} \tag{2}$$

Environmental and Performance Evidence (m_3):

$$m_3 = \begin{cases} \{\text{FSO}\}\text{:}0.85, \{\theta\} : 0.15 & \text{If Fog=Moderate, Dust=Moderate,} \\ & \text{Error=Very Good, Quality} \neq \text{Failure} \\ \{\text{RF}\}\text{:}0.85, \{\theta\} : 0.15 & \text{Otherwise.} \end{cases} \tag{3}$$

Belief Fusion: The combined mass function was calculated recursively using Dempster's Rule [19]:

$$m_{\text{Belief Fusion}}(C) = \frac{1}{1-K} \sum_{A \cap B = C} m_1(A).m_2(B), \tag{4}$$
$$K = \sum_{A \cap B = \emptyset} m_1(A).m_2(B).$$

This process was repeated to integrate the third source (m_3), and the output decision and its belief value were stored in Dempster Shafer Classification Result Final.csv.

D. Machine Learning for Threat-Based Switching Prediction

1) Artificial Neural Network (ANN): ANN are non-linear computational models adept at learning complex relationships within data [20]. For this application, an ANN maps input features, including the FSO Threat , RF Threat , Fog , Dust , Error Point FSO, and Quality Factor FSO to the desired Action output. The core operation of a neuron involves a weighted sum of inputs (x_j) with a bias(b_i), followed by a non-linear activation function (f) [21].

$$y_i = f(\sum_{j=1}^{N} w_{ij} x_j + b_i), \tag{5}$$

where, w_{ij} are connection weights. The network is trained via backpropagation, an iterative process that adjusts weights and biases to minimize a loss function, such as cross-entropy for classification.

2) K-Nearest Neighbors (KNN): KNN is a non-parametric, instance-based algorithm that classifies new data points based on the majority class of their K closest neighbors. This approach is intuitive for real-time decision-making due to its direct reliance on data point proximity. For a new input vector x_q (comprising system parameters and threat indicators), the KNN algorithm computes its distance to all training samples x_i. A common metric is the Euclidean distance [22]:

$$d(x_q, x_i) = \sqrt{\sum_{j=1}^{D}(x_{qj} - x_{ij})^2}, \tag{6}$$

where D is the number of features. The Action for x_q is then determined by a majority vote among the 'Action' labels of its K nearest neighbors. The selection of an optimal K value is critical, typically determined through cross-validation to balance model bias and variance [23].

3) Support Vector Machines (SVM): SVM are powerful supervised learning models that construct an optimal hyperplane to separate data points of different classes in a high-dimensional space, maximizing the margin between them for enhanced generalization. For linearly separable data, the decision boundary is defined by $x - b = 0$. For non-linearly separable data, SVM employs kernel functions (e.g., Radial Basis Function) to implicitly map features into a higher-dimensional space where linear separation becomes feasible. The kernel trick allows computation of dot products in this space without explicit transformation [24][25]:

$$K(x_i, x_j) = \phi(x_i).\phi(x_j), \tag{7}$$

where, ϕ is the mapping function. SVM training involves solving a quadratic programming problem to find the optimal w and b. Its robustness to high-dimensional data and strong theoretical foundation make SVM well suited for the complex classification of communication modes (FSO, RF, CryptoFSO, CryptoRF) based on various threat and performance parameters, ultimately predicting the optimal "Action".

III. Results and Discussion

The method is based on a personal computer platform, of an Intel C i7-12650H (2.30 GHz, 16 CPUs), 16 GBD DDR5 RAM and NVIDIA GeForce RTX 4060 TI GPU, with MATLAB (R2023b). For classification purpose DST theory and ANN, KNN, and SVM intelligent models have been used to classify the threats and weather conditions affecting FSO and RF communication systems. This section aims to discuss the experimental results for various Machine Learning models, performance evaluations of those models with different metrics like Accuracy, Recall, Precision as well as false positive rate (FPR).

1) Classification Results Analysis and Discussion: The decision count by class shows that "FSO" is by far the most frequent decision, with 52,367 samples (out of 100,000) classified as FSO by the DST framework, followed by 29,441 as RF, 10,148 as CryptoFSO, and 8,044 as CryptoRF. (No samples were classified as "Theta" in this dataset.) In comparison, the baseline simulation (Enhanced FSO/RF) had 49,953 FSO decisions, 35,554 RF, 5,626 CryptoFSO and 8,867 CryptoRF as we note in Table 1, Thus the DST classifier tends more often to choose FSO (53% of decisions vs 50% baseline) while the baseline favored RF more often (36% vs 29%). This discrepancy reflects the DST evidence fusion favoring FSO when both systems are nominal.

TABLE I
Comparison of Decision Frequencies and Average Belief Values by Class

Decision Class	DST Count	Baseline Count	Avg Belief (DST)
FSO	52367	49953	0.851
RF	29441	35554	0.888
CryptoFSO	10148	5626	0.533
CryptoRF	8044	8867	0.574
Theta	0	0	0

Upon analyzing Figure 3, the RF link consistently exhibits the highest cumulative average belief, stabilizing at approximately 0.88-0.89. This underscores its frequent selection as the most reliable option under various conditions. The FSO link follows closely, with its cumulative average belief converging around 0.82-0.83, indicating strong confidence when environmental conditions are favorable. The encrypted modes, CryptoRF and CryptoFSO, show more moderate average beliefs, stabilizing at approximately 0.57-0.58 and 0.53-0.54, respectively. Notably, the 'Theta' (uncertainty) belief remains exceptionally low, stabilizing near 0, signifying the DST system's robust capability to render clear and high-confidence decisions with minimal ambiguity.

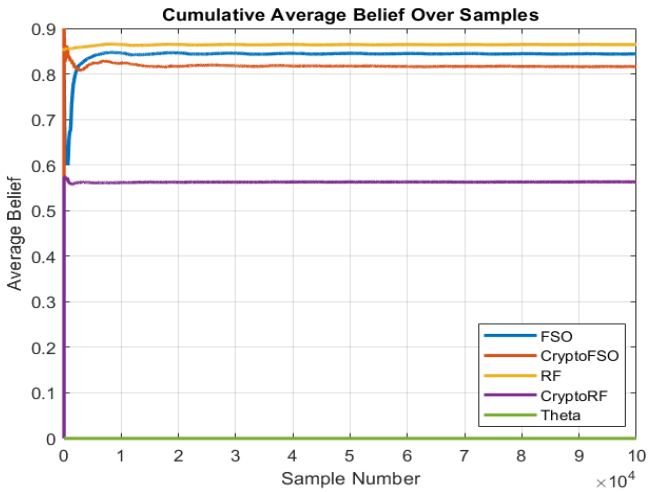

Fig. 3. Cumulative average belief.

These belief values are directly reflected in the decision frequencies presented in Figure 4. Across the 10,000 samples, the FSO link emerges as the most frequently chosen, accumulating approximately 5,100-5,200 decisions. The RF link is the second most frequent, with about 3,000-3,100 selections, affirming its critical role as a robust alternative.

The encrypted modes, CryptoRF and CryptoFSO, are selected less often, with cumulative counts of approximately

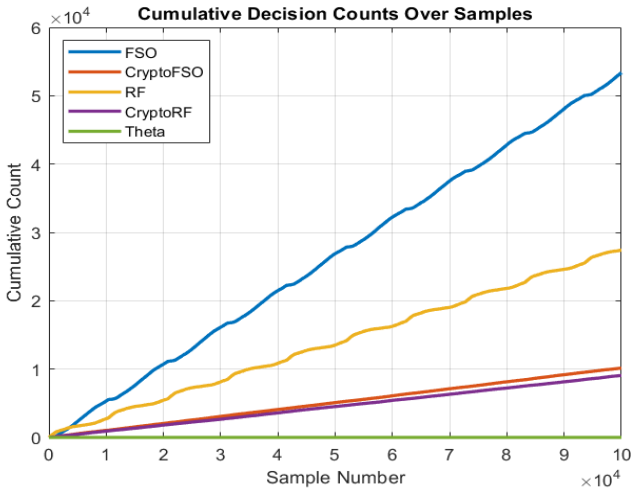

Fig. 4. Cumulative decision counts.

900-1,000 and 500-600, respectively, indicating their specific utility when security measures are necessitated by identified threats. The cumulative count for Theta remains negligible, reinforcing the system's consistent ability to make definitive classifications.

Average Belief per Decision and Dempster's Rule[26]. Figure 5, the 'Average Belief per Decision' bar chart, provides further insight into the system's confidence. This figure summarizes the mean confidence associated with each mode when it is selected as the primary action. The values presented in this figure are the result of Dempster's Rule of combination, which aggregates evidence from multiple sources to form a combined belief. For two mass functions, m_1 and m_2, over a frame of discernment θ , the combined mass $m_{1\oplus 2}(C)$ for any subset $(C) \subseteq \theta$ [27].

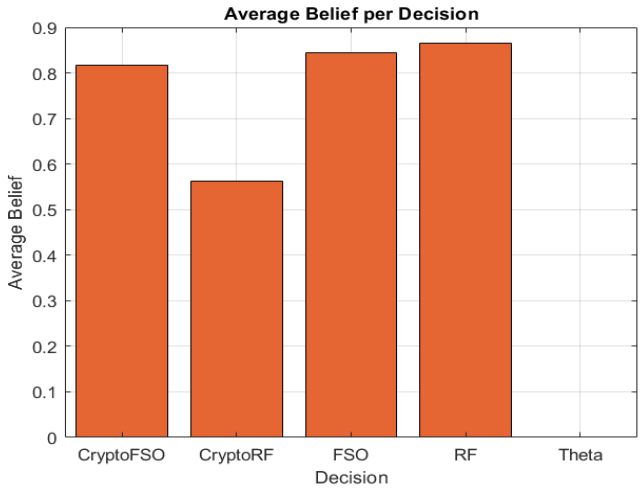

Fig. 5. Average belief per decision.

The RF link exhibits the highest average belief at approximately 0.89, closely followed by FSO at around 0.86, confirming that decisions to utilize these primary links are made with very high confidence. The encrypted modes, CryptoRF and CryptoFSO, show average beliefs of approximately 0.58 and 0.53, respectively, indicating a moderate yet sufficient level of confidence when these secure alternatives are chosen. Crucially, the average belief for Theta is effectively 0.00, unequivocally demonstrating that the system rarely, if ever, defaults to a state of complete uncertainty, even when evidence is complex.

A. Analysis of the performance results of threat detection algorithms

This section comprehensively analyzes the threat detection capabilities of Artificial Neural Networks (ANN), K-Nearest Neighbors (KNN), and Support Vector Machines (SVM) within the hybrid FSO/RF communication system [28]. Their performance in classifying communication modes (FSO, RF, CryptoFSO, and CryptoRF) is meticulously detailed through Confusion Matrix and Receiver Operating Characteristic (ROC) Curve analyses, complemented by a comparative assessment of key performance metrics.

1) Confusion Matrix Analysis: Confusion matrices provide a granular view of classifier performance, with diagonal elements representing correctly predicted instances for each communication mode and off-diagonal elements signifying misclassifications. All three confusion matrices, as we can see in the Figure 6 show remarkably high accuracy [29]. The ANN confusion matrices exhibits exceptional precision, correctly identifying 5074 CryptoFSO, 4022 CryptoRF, 26177 FSO, and 14720 RF instances, with only 7 FSO instances misclassified as RF. The KNN confusion matrices accurately classifies 2813 CryptoFSO, 4426 CryptoRF, 24976 FSO, and 17777 RF instances, noting only 5 CryptoRF misclassified as CryptoFSO and 3 as FSO. The SVM confusion matrices also performs robustly, correctly identifying 2813 CryptoFSO, 4426 CryptoRF, 24977 FSO, and 17749 RF instances, with 6 CryptoRF misclassified as CryptoFSO, 1 CryptoRF as FSO, and 28 RF as FSO.

Comparatively, the ANN model shows a slight edge in overall classification accuracy and minimizing misclassifications, suggesting superior generalization. While KNN and SVM also achieve outstanding results with very few errors, the ANN's ability to correctly classify a higher number of FSO and RF instances with fewer misclassifications indicates its marginally better performance for this dataset. All models, however, underscore the feasibility of accurately classifying communication modes for effective threat detection and intelligent switching.

2) Receiver Operating Characteristic (ROC) Curve Analysis: ROC curves (plotting True Positive Rate against False Positive Rate) and their Area under the Curve (AUC) quantify classifier performance[30]. The Figure 7 shows that ROC curves for ANN, KNN, and SVM consistently demonstrate exceptional performance. On the ANN ROC curves, the AUC (Area Under the Curve) for all classes (CryptoFSO, CryptoRF, FSO, and RF) is 1, indicating them as without distinction. On the KNN ROC curves, also for all classes, the AUC is equal to one, mirroring ANN's perfect discrimination capability yet again.

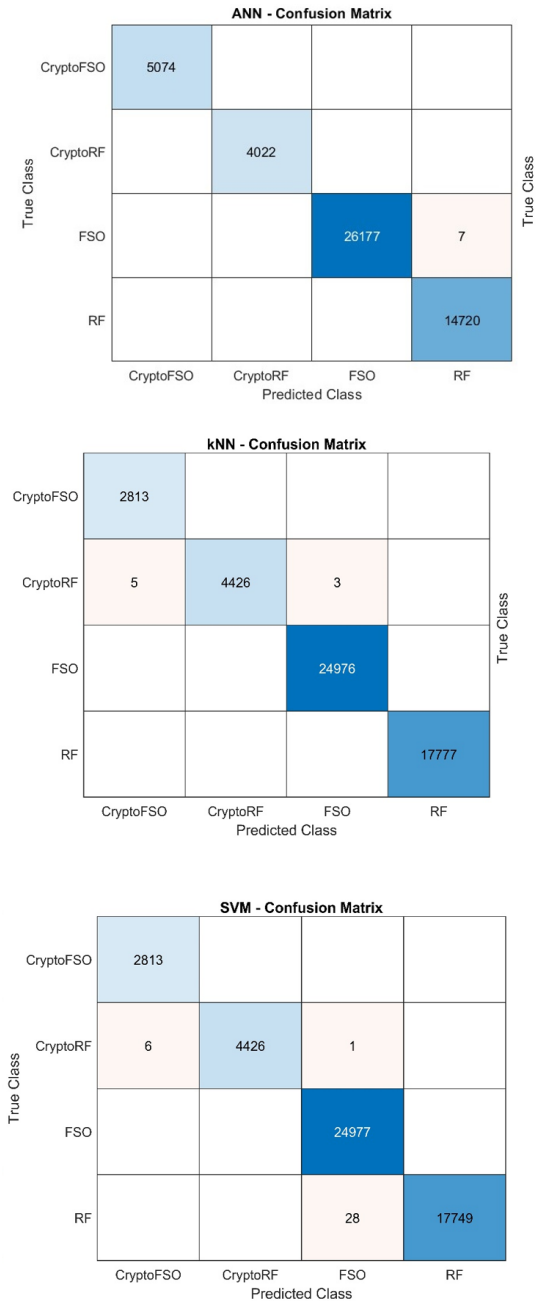

Fig. 6. Confusion Matrix Analysis (ANN, KNN, SVM).

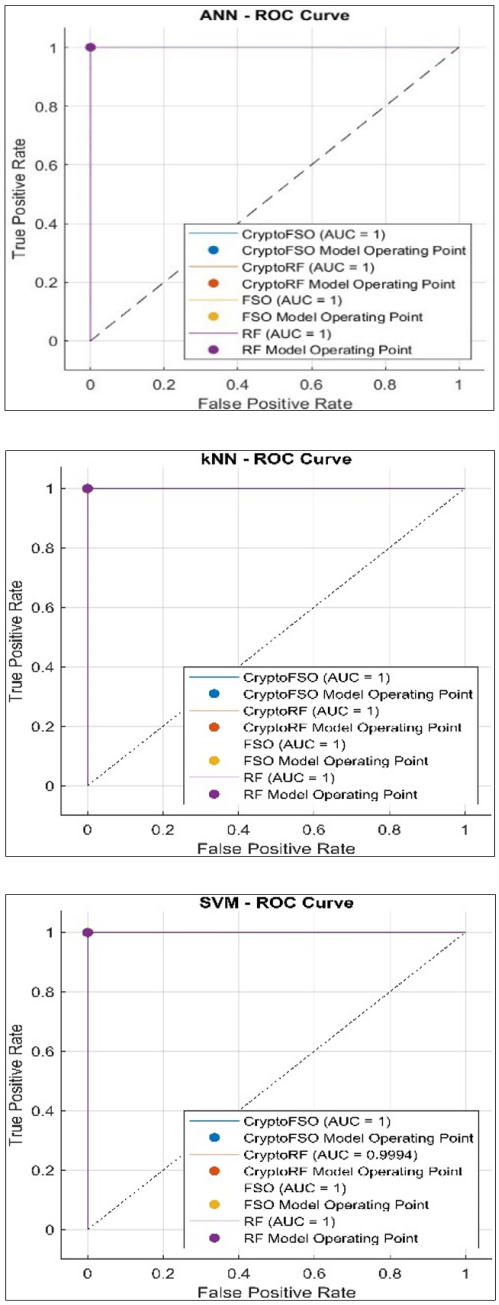

Fig. 7. Receiver Operating Characteristic (ROC) Analysis (ANN, KNN, SVM).

The SVM ROC curves have an AUC of 1 for Crypto FSO, FSO, and RF, while CryptoRF stands at 0.9994 to give high favorability ratings, which are exceptionally high values. For all classes across the three models, and in all cases, their operating points are still at or very near (0,1), indicate preferable performance for high true positive rates and minimal false positive rates In comparative terms, both ANN and KNN demonstrate perfect discriminative abilities with AUCs of 1 across all classes. The SVM, while performing exceptionally well, shows a minute deviation for the CryptoRF class. Overall, the ROC analysis confirms that all three algorithms are highly reliable for real-time intelligent switching, with ANN and KNN exhibiting marginally superior, albeit practically negligible, discriminative power in this specific application.

3) Analysis of Performance Metrics: Metrics are utilized to evaluate the performance of classification models in artificial intelligence and statistics. Each metric reflects a different aspect of a model's ability to correctly predict, whether in terms of accuracy, errors, or the balance between pros and cons [31]. The three algorithms in Table 2, show exceptional performance, with accuracy values consistently above 0.999. The Artificial Neural Network (ANN) exhibits the highest overall

performance across most metrics, including Accuracy 0.99986, Recall 0.99993, Specificity 0.99995, Precision 0.99988, and F1-score 0.99991. Its error rate 0.00014 and False Positive Rate 0.00005 are also the lowest. KNN follows closely, with marginally lower but still remarkably high metrics (e.g., F1-score of 0.99954). The SVM model, while highly effective with an accuracy of 0.99930, shows slightly lower values across most metrics than ANN and KNN. In conclusion, while all three machine learning algorithms are highly effective for threat detection and communication mode classification in the FSO/RF system, the ANN consistently outperforms KNN and SVM across most of the evaluated metrics, making it the most robust and reliable choice for this application.

TABLE II
COMPARATIVE PERFORMANCE METRICS OF ANN, KNN, AND SVM ALGORITHMS

Metric	ANN	KNN	SVM
Accuracy	0.99986	0.99984	0.99930
Error	0.00014	0.00016	0.00070
Recall	0.99993	0.99955	0.99921
Specificity	0.99995	0.99994	0.99968
Precision	0.99988	0.99953	0.99918
False Positive Rate	0.00005	0.00006	0.00032
F1-score	0.99991	0.99954	0.99919
Matthews Correlation Coefficient	0.99985	0.99949	0.99891
Kappa	0.99963	0.99957	0.99813

IV. CONCLUSIONS

This study presents an intelligent switching system for hybrid FSO and RF communication, utilizing Dempster-Shafer Theory (DST) for robust threat classification and advanced machine learning algorithms for real-time decision-making. Analysis of 10,000 simulation samples, covering environmental conditions (fog, dust) and threat scenarios (eavesdropping, jamming), conclusively demonstrates the system's effectiveness in optimizing communication link selection and ensuring resilient data transmission. DST proved instrumental in fusing evidence from FSO and RF threats, alongside FSO environmental factors, to derive precise belief assignments. The consistent convergence of cumulative average beliefs, with RF stabilizing at approximately 0.88- 0.89 and FSO at 0.82-0.83, highlights DST's capability to make high-confidence decisions with minimal uncertainty (Theta belief consistently near 0.01-0.02). The system's strong confidence in selecting primary FSO/RF links and adaptively transitioning to encrypted modes when security threats are present was further validated by average beliefs of 0.89 for RF and 0.86 for FSO decisions, and 0.58 for CryptoRF and 0.53 for CryptoFSO. Furthermore, the integration of (ANN, KNN, and SVM) significantly enhanced threat detection and real-time switching. Detailed analyses revealed exceptionally high classification accuracies across all algorithms. The ANN achieved an accuracy of 0.99986, KNN 0.99984, and SVM 0.99930. ROC curve analyses consistently yielded near-perfect AUC values, with most classes achieving an AUC of 1, underscoring the models' superior discriminative power and low false positive rates. The ANN consistently exhibited the highest overall performance across most metrics, including an F1-score of 0.99991, positioning it as the most robust and reliable choice. This research conclusively demonstrates that the proposed intelligent switching system, by synergistically combining DST with advanced machine learning, offers a highly effective and adaptive solution for maintaining secure and reliable communication in dynamic and challenging FSO/RF environments. Future work will explore the implementation of different classification methods and algorithms to achieve maximum detection accuracy and alternatives in FSO/RF systems.

REFERENCES

[1] F. P. Guiomar, M. A. Fernandes, J. L. Nascimento, V. Rodrigues, and P. P. Monteiro, "Coherent free-space optical communications: Opportunities and challenges," Journal of Lightwave Technology, vol. 40, no. 10, pp. 3173–3186, 2022. https://doi.org/10.1109/JLT.2022.3164736

[2] S. A. Al-Gailani et al., "A survey of free space optics (FSO) communication systems, links, and networks," IEEE Access, vol. 9, pp. 7353–7373, 2020. https://doi.org/10.1109/ACCESS.2020.3048049

[3] R. Ullah et al., "Beyond Fiber: Toward Terahertz Bandwidth in Free-Space Optical Communication," Sensors, vol. 25, no. 7, p. 2109, 2025. https://doi.org/10.3390/s25072109

[4] U. Darusalam, P. S. Priambodo, F. Y. Zulkifli, and E. T. Rahardjo, "The improvement of fiber-detection method to enhance the output of amplify-received relaying on FSO communications," International Journal of Electronics and Telecommunications, pp. 325–333, 2023. https://doi.org/10.24425/ijet.2023.144368

[5] H. Hassan, S. Althunibat, A. Al-Mbaideen, M. Hasna, and K. Qaraqe, "A Survey on Hybrid Free Space Optical and Radio Frequency Systems: Classification, Progress, Observations and Challenges," IEEE Access, 2025. https://doi.org/10.1109/ACCESS.2025.3558500

[6] S. S. Patil, C. Joseph, D. T. Varpe, and A. B. Raj, "A comprehensive review on security in free-space optical communication," Int. J. Eng. Res. Rev., vol. 12, no. 3, pp. 150–180, 2024. https://doi.org/10.5281/zenodo.13851700

[7] M. H. Khoshafa et al., "RIS-Assisted Physical Layer Security in Emerging RF and Optical Wireless Communication Systems: A Comprehensive Survey," arXiv preprint arXiv:2403.10412, 2024. https://doi.org/10.1109/comst.2024.3487112

[8] M. Mrabet and M. Sliti, "Performance analysis of FSO communications in desert environments," Optical and Quantum Electronics, vol. 56, no. 4, p. 659, 2024. https://doi.org/10.1007/s11082-024-06315-9

[9] T. Li, J. Sun, and L. Fei, "Dempster-Shafer theory in emergency management: a review," Natural Hazards, vol. 121, no. 6, pp. 6413–6440, 2025. https://doi.org/10.1007/s11069-024-07096-w

[10] G. Peng, J. T. ømmerås Selvik, E. B. Abrahamsen, and T. Markeset, "A novel operational risk assessment model based on evidence reasoning for multi-objective and dynamic operational scenarios," International Journal of System Assurance Engineering and Management, pp. 1–17, 2025. https://doi.org/10.1007/s13198-025-02750-3

[11] B. Dou et al., "Machine learning methods for small data challenges in molecular science," Chemical Reviews, vol. 123, no. 13, pp. 8736–8780, 2023. https://doi.org/10.1021/acs.chemrev.3c00189

[12] D. Ö. Kaya, Y. Koca, T. Ü. Kuzubaş, Ö. Kurtaş, İ. Demir, and G. Çetin, "Sex Determination Using Data Mining Methods Through Measurements of Ascender and Descender Parts of Letters," The Bulletin of Legal Medicine, vol. 29, no. 1, pp. 9–19, 2024. https://doi.org/10.17986/blm.1690

[13] D. Khairy, N. Alharbi, M. A. Amasha, M. F. Areed, S. Alkhalaf, and R. A. Abougalala, "Prediction of student exam performance using data mining classification algorithms," Education and Information Technologies, vol. 29, no. 16, pp. 21621–21645, 2024 https://doi.org/10.1007/s10639-024-12619-w

[14] S. R. Sabuj, M. S. Alam, M. Haider, M. A. Hossain, and A.-S. K. Pathan, "Low Altitude Satellite Constellation for Futuristic Aerial-Ground Communications.," CMES-Computer Modeling in Engineering and Sciences, vol. 136, no. 2, 2023. https://doi.org/10.32604/cmes.2023.024078

[15] R. Bopardikar, C. Joseph, and A. A. B. Raj, "A Review Paper on Hybrid RF/FSO System for Communication," International Journal of Engineering Research and Reviews, vol. 12, no. 3, pp. 90–115. https://doi.org/10.5281/zenodo.13848040

[16] A. Khwayyir, M. Nangir, and J. M. Niya, "Developing threat detection and weather impact techniques by AI algorithms to enhance the reliability of FSO/RF system," Opto-Electronics Review, pp. e155677–e155677, 2025. https://doi.org/10.24425/opelre.2025.155677

[17] F. Aragão and J. Alcântara, "Imprecise Belief Fusion Facing a DST benchmark problem," arXiv preprint arXiv:2408.08928, 2024. https://doi.org/10.48550/arXiv.2408.08928

[18] Y. Dong and Y. Zhou, "Hierarchical belief k-nearest neighbors for human activity recognition," in 2023 42nd Chinese Control Conference (CCC), IEEE, 2023, pp. 3109–3114. https://doi.org/10.23919/CCC58697.2023.10240988

[19] G. Bezirganyan, S. Sellami, L. Berti-Équille, and S. Fournier, "Multimodal Learning with Uncertainty Quantification based on Discounted Belief Fusion," arXiv preprint arXiv:2412.18024, 2024. https://doi.org/10.48550/arXiv.2412.18024

[20] P. Malik, A. Gehlot, R. Singh, L. R. Gupta, and A. K. Thakur, "A review on ANN based model for solar radiation and wind speed prediction with real-time data," Archives of Computational Methods in Engineering, vol. 29, no. 5, pp. 3183–3201, 2022. https://doi.org/10.1007/s11831-021-09687-3

[21] I. Ahmad, F. M'zoughi, P. Aboutalebi, I. Garrido, and A. J. Garrido, "A regressive machine-learning approach to the non-linear complex FAST model for hybrid floating offshore wind turbines with integrated oscillating water columns," Scientific Reports, vol. 13, no. 1, p. 1499, 2023. https://doi.org/10.1038/s41598-023-28703-z

[22] E. Zardini, E. Blanzieri, and D. Pastorello, "A quantum k-nearest neighbors algorithm based on the Euclidean distance estimation," Quantum Machine Intelligence, vol. 6, no. 1, p. 23, 2024. https://doi.org/10.48550/arXiv.2305.04287

[23] D. Ratnasari, "Comparison of performance of four distance metric algorithms in K-nearest neighbor method on diabetes patient data," Indonesian Journal of Data and Science, vol. 4, no. 2, pp. 97–108, 2023. https://doi.org/10.56705/ijodas.v4i2.71

[24] M. Tanveer, A. Tiwari, R. Choudhary, and M. A. Ganaie, "Large-scale pinball twin support vector machines," Machine Learning, vol. 111, no. 10, pp. 3525–3548, 2022. https://doi.org/10.1007/s10994-021-06061-z

[25] M. E. Paoletti, J. M. Haut, X. Tao, J. P. Miguel, and A. Plaza, "A new GPU implementation of support vector machines for fast hyperspectral image classification," Remote Sensing, vol. 12, no. 8, p. 1257, 2020. https://doi.org/10.3390/rs12081257

[26] Z. Liu, "A belief similarity measure for Dempster-Shafer evidence theory and application in decision making," Journal of Soft Computing and Decision Analytics, vol. 2, no. 1, pp. 213–224, 2024. https://doi.org/10.31181/jscda21202443

[27] F. Sebbak, M. R. Senouci, F. Benhammadi, M. Mataoui, and W. Cherifi, "Towards Cardinality-Aware Evidential Combination Rules in Dempster–Shafer Theory," KI-Künstliche Intelligenz, pp. 1–16, 2024. https://doi.org/10.1007/s13218-024-00859-4

[28] M. A. Amirabadi, S. A. Nezamalhosseini, M. H. Kahaei, and L. R. Chen, "A Survey on Machine and Deep Learning for Optical Communications," arXiv preprint arXiv:2412.17826, 2024. https://doi.org/10.48550/arXiv.2412.17826

[29] S. Abd Kadum, F. H. Najjar, H. M. Al-Jawahry, and F. Mohamed, "Eye Diseases Classification Based on Hybrid Feature Extraction Methods," in 2023 6th International Conference on Engineering Technology and its Applications (IICETA), IEEE, 2023, pp. 402–407. https://doi.org/10.1109/IICETA57613.2023.10351335

[30] J. Li, "Area under the ROC Curve has the most consistent evaluation for binary classification," PloS one, vol. 19, no. 12, p. e0316019, 2024. https://doi.org/10.48550/arXiv.2408.10193

[31] G. M. Foody, "Challenges in the real world use of classification accuracy metrics: From recall and precision to the Matthews correlation coefficient," Plos one, vol. 18, no. 10, p. e0291908, 2023. https://doi.org/10.1371/journal.pone.0291908