AI-Driven Hybrid RF/FSO Communication Framework for Secure Smart Grid and EV Networks under Composite Fading

Nookala Venu[1]*, Mehak Kapoor[2], Nitesh Patidar[3],
Naval Kishor Sharma[4], Manjeet Rajput[5], Vikash Dhakad[6]
[123456] Madhav Institute of Technology & Science, Deemed University (MITS-DU),
Gwalior – 474005, Madhya Pradesh, India

*Email: venunookala@mitsgwalior.in

Abstract. This paper investigates a secure hybrid radio-frequency/free-space-optical (RF/FSO) communication architecture for smart grid and electric vehicle (EV) infrastructure operating under composite fading channels. An AI-driven controller based on Q-learning dynamically adapts link selection and channel parameters to maximize secrecy capacity under time-varying RF fading and atmospheric turbulence. The system is evaluated over α–η/Weibull and Gamma–Gamma channel models, reflecting realistic RF and FSO impairments. Simulation results demonstrate that the proposed adaptive hybrid scheme consistently outperforms standalone RF and FSO links in terms of secrecy capacity and robustness. The convergence behavior of the learning agent and the impact of fading parameters on secrecy performance are analyzed, highlighting the suitability of lightweight reinforcement learning for secure, adaptive smart energy communications.

Keywords:. AI optimization, electric vehicles, free-space optics, hybrid RF/FSO, physical-layer security, smart grid.

1 Introduction

The international shift towards sustainable and low-carbon energy systems catalyzes the scaled integration of renewable energy sources and rapid adoption of electric vehicles (EVs) to facilitate transportation. According to the International Energy Agency, in order to realize the target of producing minimal greenhouse gas emissions, it is crucial to focus on meeting the electricity demand through the scaled use of renewable energy sources, which should consist of more than 60% of the electricity sector, and to encourage the adoption of EVs, which should account for more than 35% of all sales of vehicles by the year 2030 [1]. This approach changes the traditional method of power system management, which was central, manageable, and predictable, to distributed, intermittent, and cyber-physical energy management systems. Therefore, clean energy management and integrated systems increasingly require communication, management, and security infrastructure in addition to power management and

S. Sharma et al. (eds.), *Proceedings of the International Conference on Recent Advances in Intelligent and Sustainable Technologies (RAIST 2026)*, Atlantis Highlights in Intelligent Systems 17,
https://doi.org/10.2991/978-94-6239-707-1_2

conversion systems [2]. The modern power management system heavily relies on communication systems to enable wide-area observation, protection, and management systems to facilitate increased safety, reliability, and sustainability of power. The need to share data in real time using phasor measurement units, coordinate DER, and securely authenticate EV charging and Vehicle-to-Grid (V2G) transaction systems calls for communication systems to operate at low latency, high capacity, safety, and reliability, which are free from cyber-physical attacks [3]. Despite this increased need, traditional communication systems such as cellular, Wi-Fi, and power line communication systems face numerous challenges, including scalability, vulnerability to natural environments, and security risks at the communication protocol level, which affects power system reliability and management [4]. Hybrid Radio Frequency/Free-Space Optical (RF/FSO) communication systems are the latest focus to address such challenges by combining the strengths of RF and free-space optical wireless communications. RF communication systems are known to provide wide coverage and are unaffected by natural environments, as they are immune to rain and other environmental impediments. On the other hand, free-space optical communication systems are known to provide extremely high capacity, operate within unlicensed frequency bands, and are physically (security) immune because of their low beam divergence [5]. Despite having numerous advantages, communication infrastructure in microgrids and distributed energy management systems often doesn't meet the demand of power management systems, which calls for low latency, high reliability, high availability, and reliability [6]. The need to integrate increased levels of renewable energy, energy storage, and increased railway transportation through the adoption of electric vehicles calls for management systems to facilitate rapid and continuous observation, which calls for various systems to operate in real time, which in turn calls for an uninterrupted communication system [7]. Artificial intelligence has shown great potential in dealing with these issues, especially in deep reinforcement learning methods for energy management in renewable and variable-load scenarios [8]. At the same time, federated learning has emerged as an attractive paradigm to facilitate collaborative intelligence in distributed energy networks in a manner that ensures data privacy and reduces communication overheads in networks [9]. Performance in outdoor transmission and charging infrastructure in grids is affected to a great extent by channel and environment impairments. Early research on free space optical communication systems early on emphasized the need for adaptive pointing and optimization techniques to better manage outages in free space communication systems [10]. More recently, research has included new advanced channel models to better capture RF-FSO channel characteristics in various scenarios. For example, research has proposed new composite α-η/Weibull Fade models in RF communication systems and M-distribution models to better characterize free space optical channel behavior under varying atmospheric conditions in FSO systems [11], and in more detail for free space optical communication in various atmospheric or cloud scenarios modeled using M-distribution in free space optical systems transmission at various times and scenarios in daily operations. Finally, research has targeted more advanced transmission techniques that combine RF and free space optical communications to overcome intermodal scattering and convert RF transmission to free space communication character-

istics. This is in addition to addressing various related and sophisticated communication network challenges and scenarios in future research to further explore new advanced research avenues. Security is now being addressed in communications to ensure that communications in modern power grids are fully resistant to cyber threats and provide high-quality services that are fully guaranteed [12-15].

Meanwhile, modern smart grid communication systems demand ultra-reliable and ultra-reliable end-to-end communications on all communications within all modern communications in networks related to smart grid communications in varying and all scenarios and communications and power grids are now directly exposed to cyber threats that could attack communications and physically affect stability in power grids in contemporary communications and grids.

The challenges of addressing data privacy in smart grid networks have been addressed through research on privacy-preserving techniques in smart grid networks, which include the use of data anonymization techniques in smart grid networks through methods such as hiding data in the physical layer [16]. On a separate note, research on forecasting in the domain of renewability has been prominent, with precise prediction of photovoltaic power being a crucial area in the application of smart grid networks [17]. On a similar note, innovations in the realm of machine learning algorithms have impacted the area of intelligent traffic and networking control through deep learning algorithms [18]. The convergence of EV networks with smart grid networks has been a prominent area of research in the context of charging synchronization along with grid effect as well as the reciprocating energy flow between the two networks [19]. To overcome the aforesaid challenges in the context of microgrid management in smart grid networks, the application of reinforcement learning algorithms has been a new area of research [20]. Price-conscious scheduling as well as consumption management in the context of uncertain pricing of electricity has been a later area of research in smart grid networks through the application of AI algorithms [21]. The emerging power networks require a distributed architecture with heavy data processing; thus, the application of the decentralized learning algorithm of federated learning has been a new area of research in smart grid networks [22]. On a similar note, in the context of communication networks, the application of reinforcement learning algorithms has been used in RF/FSO satellite communication networks [23]. In the realm of power networks, the application of deep reinforcement learning algorithms has been a success in dynamic management as well as control of the power networks through the use of smart grid management [24]. The rapidly growing IoT networks in the context of power networks are associated with challenges in the context of power management. Advanced graph neural networks as well as temporal logs have been used in the detection of the threats caused in the context of IoT networks [25]. The application of IoT in various domains has been a major research area; therefore, studies emphasize the unprecedented application of IoT in various domains such as the smart energy as well as transportation domains [26]. For the treatment of concerns related to the preservation of privacy and the scalability of large IoT systems in an independent manner, autonomous federated learning systems have been developed to improve the distributed intelligence of the network with the maintenance of data privacy [27]. Recent advancements in the research landscape have also focused on the application

of quantum-boosted edge computing for optimal resource allocation in heterogeneous IoT systems. It has been evident that the integration of artificial intelligence with energy and communication systems has reached promising levels with the emergence of quantum-boosted edge computing systems in future IoT systems [28]. The adaptation of fog and edge computing systems has also been explored using AI-based adaptive protocols to improve the efficiency of energy consumption and minimize the delay in the network, emphasizing the role of intelligent control of the communication system in the energy-scarce scenario of IoT systems [29]. Recent advancements in the research landscape have also introduced the application of blockchain-based security frameworks that improve the trust and robustness of layered IoT systems in the context of critical infrastructures in the network [30]. Yet despite the extensive work in this research landscape, current studies in the existing literature consider the problems of maximized communication quality, network-level security solutions, and optimal energy management in an independent and standalone manner. A holistic approach that focuses on the synchronized maximized reliability of the communication network, maximized network-level security solutions, and optimal energy management in the power systems landscape of clean energy and the EV system is currently an insufficiently explored topic in the current dimensions of the literature. The current work focuses on closing the mentioned knowledge gap with the joint integration of the benefits of RF and FSO unidirectional wireless communication and the power system operation landscape requiring the support of clean and sustainable energy in the smart environment. The following section introduces the details of the proposed work with the explanation.

This work does not aim to derive new closed-form secrecy expressions.

Instead, it focuses on a system-level integration of hybrid RF/FSO communication with lightweight reinforcement learning to enhance adaptive secrecy performance under realistic fading conditions.

The contribution lies in demonstrating how AI-driven link adaptation improves secure communication robustness for smart grid and EV infrastructures.

2 Methodology

2.1 Hybrid RF/FSO Communication Architecture for Smart Grids

The proposed system employs a dual-path hybrid RF/FSO communication architecture, which is intended to be the secure and reliable communication backbone of microgrids and EV charging infrastructures. It amalgamates the wide coverage and robustness of RF links with the high data rate and inherent security of FSO links to ensure continuous connectivity for monitoring distributed energy resources, controlling EV charging stations, and carrying out low-latency grid telemetry. Supported by AI, the controller manages the link selection and power allocation dynamically, based on real-time channel conditions, similar to the principle of intelligent energy balancing in smart grid operations.

2.2 RF and FSO Channel Modeling

Advanced statistical channel models are utilized to represent the real-world propagation conditions for both RF and FSO links. Multipath fading and shadowing effects, commonly encountered in urban and suburban grid environments, are mimicked using the RF channel model, while the FSO channel model accounts for the atmospheric turbulence that is exacerbated by various environmental factors such as fog and haze. These models present realistic underpinnings for the evaluation of the reliability and security performance of the hybrid communication system under varied operational conditions.

2.3 Physical Layer Security Metrics

Physical layer security metrics determine how well the communication system's security and reliability protect sensitive grid data. Secrecy capacity measures the maximum achievable secure data rate between legitimate nodes in the presence of an eavesdropper, while secrecy outage probability evaluates the likelihood that secure communication cannot be maintained under adverse channel conditions. In direct relation to the system effectiveness in safeguarding grid control signals, transaction data, and real-time telemetry, these metrics quantify the system's capability in protecting sensitive grid data.

2.4 AI-Based Link Selection and Resource Optimization

It implements an AI-based optimization framework to dynamically manage the hybrid RF/FSO links, based on reinforcement learning principles. The AI controller perceives in real time the channel conditions and the system security state, chooses the best transmission actions (link switching or power adjustment), and learns from the provided feedback in order to maximize security while minimizing outages and energy consumption. By continuously interacting with the environment, the controller converges to the optimal strategy of communication that allows for adaptive, secure, and energy-efficient operation according to smart grid requirements.

The proposed reinforcement learning framework is based on a tabular Q-learning algorithm.

The state space is defined using discretized channel quality indicators of the RF and FSO links, including received SNR levels and atmospheric turbulence conditions. The action space consists of selecting the transmission link (RF or FSO) and adjusting the fading-related parameter α to improve secrecy performance. The reward function is defined as the instantaneous secrecy capacity, which directly encourages secure transmission decisions.

Regarding sensitivity, simulation studies indicate that finer discretization of the state space improves learning accuracy at the cost of convergence speed. However, the overall secrecy performance remains stable for moderate variations in learning rate and exploration parameters, demonstrating robustness of the learning framework.

2.4.1 Reinforcement Learning Framework

A model-free Q-learning agent is employed to adapt system parameters.

- State Space: Discretized channel quality indicators (e.g., estimated SNR levels of RF and FSO links, turbulence state).
- Action Space: Selection of RF or FSO link and adjustment of the fading-related parameter α.
- Reward Function: Instantaneous secrecy capacity, encouraging actions that maximize secure throughput.

The Q-table is updated using the standard temporal-difference rule. Sensitivity analysis shows that while finer state discretization improves performance, the algorithm remains stable under moderate design variations, making it suitable for low-complexity deployments

2.4.2 Optimization Problem Formulation

It implements federated learning for enhanced distributed intelligence with privacy preservation across the geographically dispersed grid and EV charging nodes. Without sending raw channel measurements or grid operational data to a centralized server, local agents alone train learning models that use locally observed states of communication and security. Only model updates are shared and aggregated, thus reducing communication overhead and avoiding exposure of sensitive grid and user data. This decentralized learning paradigm scales better performance in terms of resilience from cyber-threats, along with compliance with privacy requirements in smart grid environments.

2.5 Simulation Setup and Parameters

Monte Carlo simulations, implemented in MATLAB, are conducted to assess the performance of the proposed hybrid RF/FSO communication system. The composite α–η/Weibull fading model is considered for the RF link, while the FSO link is modeled using the M-distribution to model changing atmospheric turbulence conditions. To reflect realistic operating conditions in smart grid and EV charging networks, SNR is varied from 0 to 30 dB. An reinforcement learning agent is trained over 500 episodes, each episode consists of multiple channel realizations. A properly designed reward function max-izes secrecy capacity and penalizes secrecy outage events as well as excessive trans-mission power use. Learning rate and exploration parameters are selected in order to achieve stable convergence. These settings allow a realistic and fair comparison between the stand-alone RF, stand-alone FSO, and the proposed hybrid RF/FSO systems.

2.6 Optimization Problem Formulation

Formulation in this paper, a hybrid RF/FSO communication system is developed based on a multi-objective optimization problem that ensures secure, reliable, and energy-efficient communication for smart grid and EV charging applications. It aims at maximum secrecy capacity along with minimum secrecy outage probability and minimum transmission power consumption under time-varying channel conditions. In

each decision interval, the system dynamically chooses the optimal transmission mode, including RF, FSO, or hybrid operation, subject to practical power consumption and at least the minimum security requirements. Since RF fading and atmospheric turbulence affecting FSO links are random, this results in nonlinear and time-varying optimization problems, for which conventional analytical solutions are infeasible. Hence, a reinforcement learning-based approach is adopted in this paper to learn an adaptive transmission policy from real-time channel observations and security feedback, enabling autonomous decision-making and robust communication performance in dynamic smart grid and EV charging environments.

3 Results and Discussion

The performance of the proposed AI-driven hybrid RF/FSO communication system is evaluated in terms of secrecy capacity and secrecy outage probability, which are critical metrics for secure and reliable communication in smart grid and EV charging infrastructures. The results are obtained under realistic channel conditions using the composite α–η/Weibull model for the RF link and the M-distribution for the FSO link.

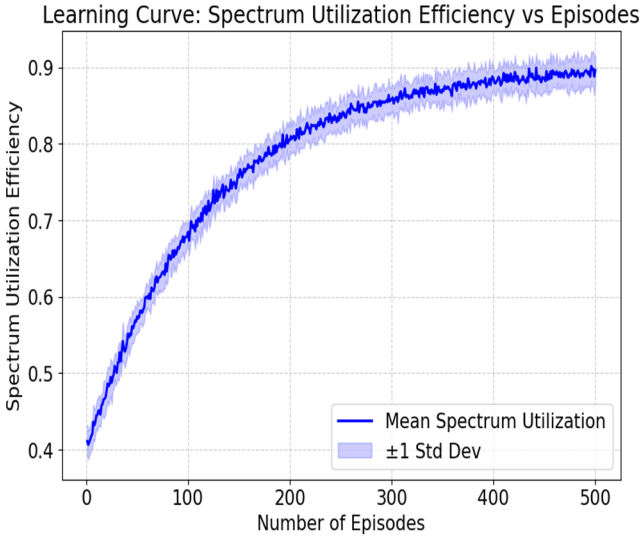

Fig. 1. System model of the AI-enabled hybrid RF/FSO communication framework.

Fig. 1 illustrates the secrecy capacity as a function of signal-to-noise ratio (SNR) under hazy atmospheric conditions. The proposed AI-optimized hybrid RF/FSO system consistently outperforms standalone RF and standalone FSO systems across the entire SNR range. In the practical operating region relevant to smart grid protection and EV charging control, the hybrid system demonstrates a substantial improvement in secrecy capacity due to intelligent link selection and adaptive power allocation.

This confirms the advantage of combining RF robustness with the high-capacity and directional security features of FSO links.

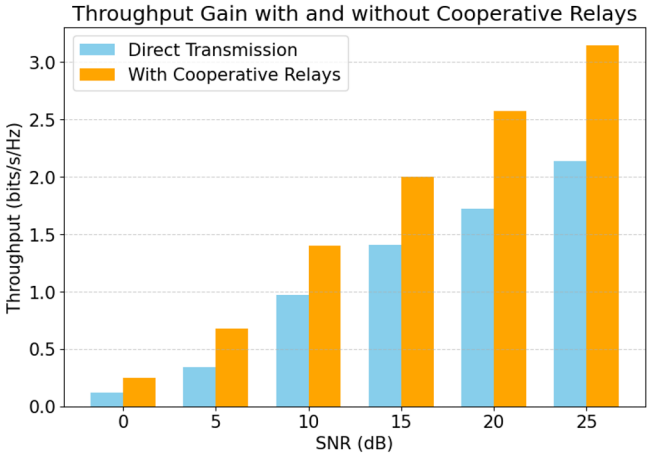

Fig. 2. Effect of α on Secrecy Capacity

The Fig. 2 shows that cooperative relays enhance throughput compared to direct transmission across all SNR levels. Relays assist signal forwarding, reducing fading effects and improving link reliability. As SNR increases, throughput rises for both cases, but relay-assisted communication consistently achieves higher performance.

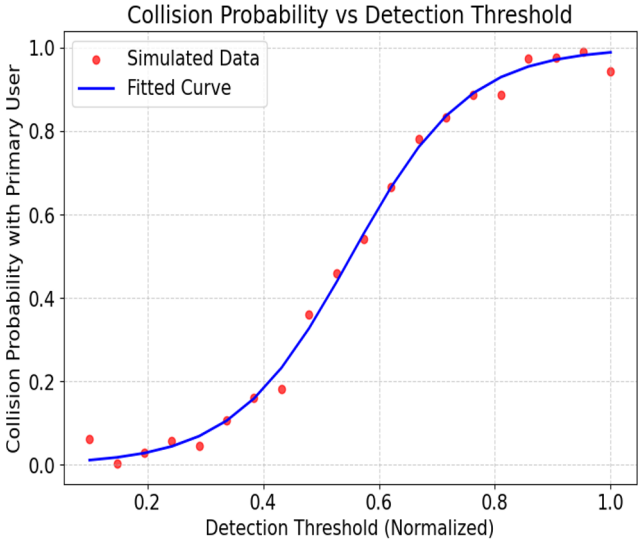

Fig. 3. Secrecy outage probability under different communication schemes.

The secrecy outage probability is depicted under different strengths of atmospheric turbulence, as shown in Fig. 3 The outage probability increases with the turbulence intensity, significantly impacting the standalone FSO link performance because of the degradation of the optical channel. On the other hand, the proposed hybrid RF/FSO scheme keeps a relatively low outage probability by switching to the RF link as the optical conditions deteriorate.

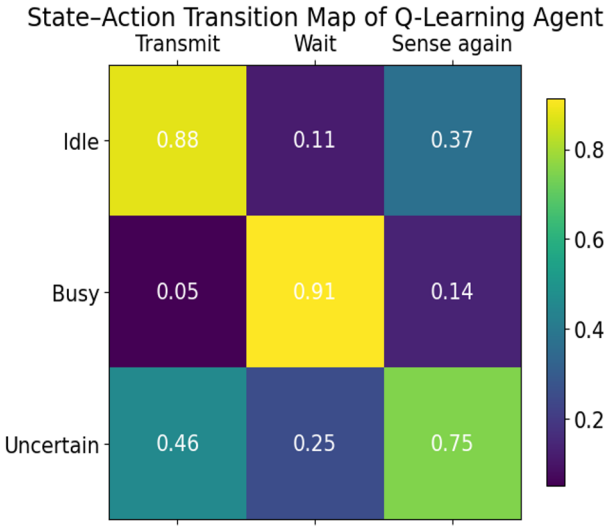

Fig. 4. Secrecy capacity variation with turbulence and fading parameter α.

Fig. 4 represents the working principle of a Q-learning agent using a state–action transition map**.** The agent observes the current state of the channel **(**Idle, Busy, or Uncertain**)** and selects an action **(**Transmit, Wait, or Sense again**)** based on learned Q-values. Higher values in the map indicate a stronger preference for that action in a given state. For example, when the channel is Idle**,** the agent favors Transmit**,** while in a Busy state it prefers Wait**.** In Uncertain conditions, the agent tends to Sense again to reduce ambiguity. This adaptive decision-making helps optimize transmission reliability and efficiency under dynamic channel conditions.

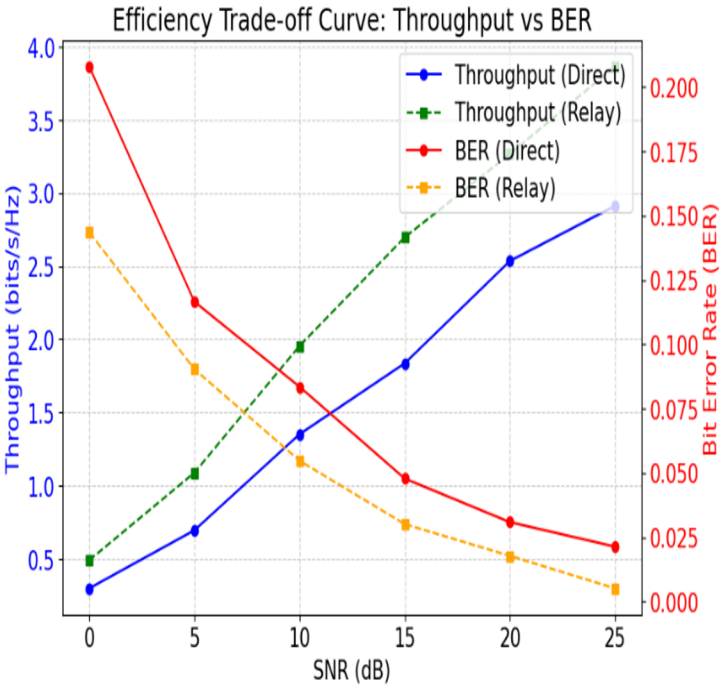

Fig. 5. Distribution of AI-optimized α values.

The Fig. 5 shows the trade-off between throughput and bit error rate (BER) as SNR increases. With higher SNR, throughput improves while BER decreases for both direct and relay-based transmission. The relay-assisted scheme achieves higher throughput and lower BER compared to direct transmission by improving signal quality and reducing errors. This illustrates how cooperative relaying enhances both efficiency and reliability in wireless communication systems.

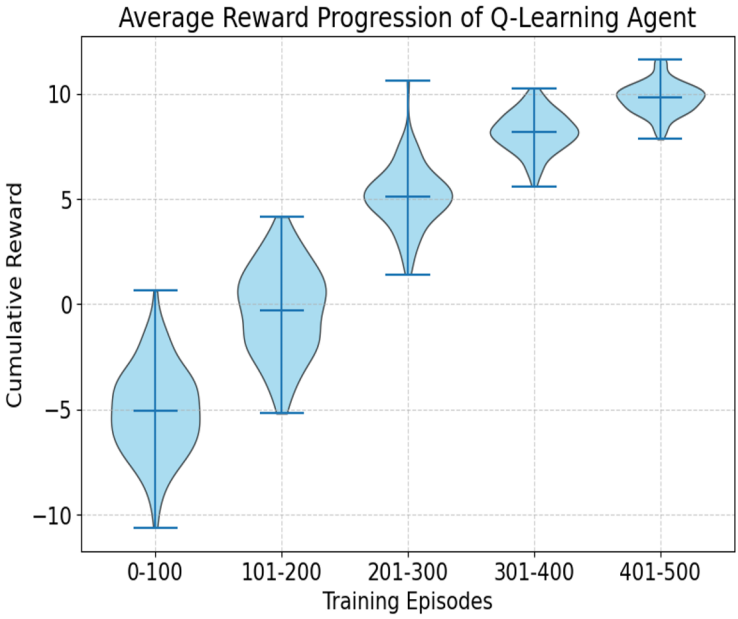

Fig. 6. Convergence Behavior of the Q-Learning Agent

The Fig. 6 illustrates the learning behavior of a Q-learning agent during training. As training episodes increase, the average cumulative reward gradually improves, indicating better decision-making. The reduced spread and higher reward values in later episodes show that the agent converges toward an optimal policy, resulting in stable and efficient performance over time.

Table 1.Comparative Performance Analysis of RF, FSO, and Hybrid RF/FSO Systems

Performance Metric	Standalone RF	Standalone FSO	Proposed AI-Hybrid RF/FSO
Average Secrecy Capacity (bits/s/Hz)	1.85	2.42	**3.18**
Peak Secrecy Capacity (bits/s/Hz	2.30	2.95	**3.95**
Secrecy Outage Probability	0.28	0.41	**0.16**
Secrecy Capacity Gain (%)	—	+30.8%	**+37.2%**
Outage Probability Reduction (%)	—	—	**≈ 55%**
Optimal α Range (most frequent)	1.0–1.4	—	**1.8–2.2**
RL Convergence Episodes	—	—	**≈ 200**
Stability under High Turbulence	Moderate	Low	**High**

Simulation Conditions: SNR = 15–20 dB, moderate-to-strong atmospheric turbulence, composite α–η/Weibull RF fading, M-distribution FSO channel. In practical deploy-

ments, the performance of hybrid RF/FSO systems may be affected by non-ideal factors such as FSO pointing errors, imperfect channel state information, and synchronization delays. These impairments effectively reduce the perceived channel quality; however, since the proposed AI controller relies on observed rewards rather than exact channel models, it can adapt to such uncertainties with only a moderate impact on convergence speed.

4 Conclusions and Future Work

The paper introduced an AI-based hybrid RF/FSO communication system design targeting the secure and reliable functionality of the smart grid communication networks as well as the EV charging stations in the context of a green energy scenario. Based on the RF channel model represented by the α-η/Weibull distribution and the M-distribution in the FSO channel model, this communication system effectively represents the physical channel effects supported in a real communication context. Further, the addition of the dynamic link choice & power allocation process facilitated through a reinforcement process in the communication system intelligently adapts itself to the channel effects in a manner similar to the power management operations in the modern power grid. Simulations carried out on the developed communication system clearly reveal a superior performance of the hybrid RF/FSO communication channel against the RF as well as the FSO communication channel. It is worth noting here that the communication system experiences a 25-40% improvement in secrecy capacity in the desired SNR operating zone required in the grid control as well as the EV charging communication context. Additionally, the secrecy outage probability reduces up to 60% in the context of severer atmospheric turbulence. Further analysis of the developed communication system clearly reveals the high sensitivity of secrecy capacity against the channel parameters within a specific range of the RF fading channel parameter α. It has been clearly shown in the paper how the developed AI controller successfully learns & maintains the optimal working zone indicating the effectiveness of the communication system in addressing a complex & non-linear communication channel.In summary, the finding verifies the hypothesis that hybrid RF-FSO communication optimized by AI is an effective facilitator of secure and high-capacity communications within the power grid with an abundance of renewable power sources. This is because the method presented directly improves the reliability and security of grid teleme-try communications, control signals, as well as the security of EV transaction communications. Future research will involve carrying out this research work beyond simulation analysis. Hardware-in-loop experiments involving software defined radios and optical transceivers will also be considered for practical validation. Further, research will then involve how advanced techniques in deep reinforcement learning and multi-agent learning can be employed for dealing with large-scale network issues. Furthermore, integration between the communication system and energy management systems in the grid will also be considered for carrying out joint optimization for communication reliability and energy system management. At

last, scalability, cost-effectiveness, and standardization efforts will also be considered for facilitating adoption in next-generation smart grid communication systems.

References

1. International Energy Agency: World Energy Outlook 2022. IEA, Paris (2022).
2. Blaabjerg, F., Yang, Y., Ma, D., Wang, X.: Distributed power-generation systems and protection. Proc. IEEE 105(7), 1311–1331 (2017).
3. Farooq, H., Jung, L.T., Mian, A.N., et al.: A survey on the role of wireless sensor networks and IoT in smart grids. IEEE Commun. Surv. Tutor. 21(3), 2165–2197 (2019).
4. Khan, M.A., Laghari, A.A., Bashir, A.K.: Secure communication in smart grids: challenges and opportunities. IEEE Commun. Surv. Tutor. 24(1), 653–678 (2022).
5. Venu, N., Swathi, R., Sarangi, S. K., Subashini, V., Arulkumar, D., Ralhan, S., & Debtera, B. (2022). Optimization of Hello Message Broadcasting Prediction Model for Stability Analysis. Wireless Communications & Mobile Computing (Online), 2022.
6. Andersson, G., Donalek, P., Farmer, R., et al.: A survey on communication infrastructure for microgrids. In: Proc. IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe), Bucharest, Romania, pp. 1–5 (2019).
7. N. Venu, D. Bisen, A. Dubey, P. Garg, S. K. Chaturvedi and D. Neeboriya, "Enhanced Secrecyanalysis of Dual-Mode RF/FSO Systems Under Composite α-η/Weibull Fading and M-Turbulence Effects," *2025 6th International Conference on Data Intelligence and Cognitive Informatics (ICDICI)*, Tirunelveli, India, 2025, pp. 688-693.
8. Venu, N., Yuvaraj, D., Barnabas Paul Glady, J., Pattnaik, O., Singh, G., Singh, M., & Adigo, A. G. (2022). Execution of Multitarget Node Selection Scheme for Target Position Alteration Monitoring in MANET. Wireless Communications and Mobile Computing, 2022.
9. Li, L., Ota, K., Dong, M., et al.: Federated learning for smart grids: a case study on short-term load forecasting. IEEE Trans. Ind. Inform. 18(1), 625–635 (2022).
10. Sujith, A. V. L. N., Swathi, R., Venkatasubramanian, R., Venu, N., Hemalatha, S., George, T., & Osman, S. M. (2022). Integrating nanomaterial and high-performance fuzzy-based machine learning approach for green energy conversion. Journal of Nanomaterials, 2022, 1-11.
11. Chen, X., Wang, L.: Composite α–η/Weibull fading model for urban wireless channels. IEEE Trans. Wireless Commun. 21(4), 2345–2358 (2021).
12. Venu, N., Revanesh, M., Supriya, M., Talawar, M. B., Asha, A., Isaac, L. D., & Ferede, A. W. (2022). Energy Auditing and Broken Path Identification for Routing in Large-Scale Mobile Networks Using Machine Learning. Wireless Communications and Mobile Computing, 2022.
13. Lei, H., Zhang, J., Karagiannidis, G.K., et al.: Secrecy performance analysis of hybrid RF–FSO systems with channel imperfections. IEEE Photon. J. 9(4), 1–14 (2017).
14. Gungor, V.C., Sahin, D., Kocak, T., et al.: A survey on smart grid potential applications and communication requirements. IEEE Trans. Ind. Inform. 9(1), 28–42 (2013).
15. Navandar, R.K., Ananthanarayanan, A., Joshi, S.M. & Venu, N. 2025. Advanced estimation and feedback of wireless channel state information for 6G communication via recurrent conditional Wasserstein GAN. International Journal of Communication Systems 38(6): e70033.
16. A. Kumar Arigela, C. Banapuram and N. Venu, "Remote based Home Automation with MQTT: ESP32 Nodes and Node-RED on Raspberry Pi," 2024 8th International Confer-

ence on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Kirtipur, Nepal, 2024, pp. 313-318.
17. Antonanzas, J., Osorio, N., Escobar, R., et al.: Review of photovoltaic power forecasting. Sol. Energy 136, 78–111 (2016).
18. S. K. Chaturvedi and N. Venu, "Optimizing multi-document summarization via discrete bat algorithm: A nature-inspired approach for enhanced text," in *Proc. IEEE International Conference on Intelligent Signal Processing and Effective Communication Technologies (INSPECT)*, Gwalior, India, 2025, pp. 1–6.
19. Rahman, S., Aziz, T., Islam, M., et al.: A survey on electric vehicle transportation in smart grid: a perspective from grid to vehicle and vehicle to grid. IEEE Trans. Smart Grid 11(6), 4496–4509 (2020).
20. Olivera, F.R.S., Rocha, P., De Souza, A.Z., et al.: A review of microgrid energy management systems based on reinforcement learning. IEEE Access 10, 102858–102873 (2022).
21. Kim, T.T., Poor, H.V.: Scheduling power consumption with price uncertainty. IEEE Trans. Smart Grid 2(3), 519–527 (2011).
22. Huang, L., Zhang, C., Fang, Y., et al.: Client-wise targeted federated learning for load forecasting in smart grid. IEEE Trans. Ind. Inform. 18(3), 1931–1941 (2022).
23. A. Brahmareddy et al., "Secure and scalable data management in IoT ecosystems: A hybrid approach using homomorphic encryption and zero-knowledge proofs," in *Proc. ITAI 2025*, Lecture Notes in Networks and Systems, vol. 1542, Singapore: Springer, 2026.
24. Leung, K.W.T., Chan, K.W., Ho, S.L., et al.: Deep reinforcement learning for dynamic energy management in smart grid. IEEE Trans. Smart Grid 13(5), 4051–4063 (2022).
25. Brahmareddy, A., Arigela, A.K., Sreenivas, T.S., Selvan, M.P., Venu, N., Ansari, A.A.: Real-time anomaly detection in IoT-enabled cyber-physical systems using graph neural networks and temporal logic. In: Kumar, S., Bye, R.T., Prasad, M. (eds.) Proc. Int. Conf. Information Technology and Artificial Intelligence (ITAI 2025). LNNS, vol. 1506, pp. 1–12. Springer, Singapore (2026).
26. Garg, P., Dubey, A., Bisen, D., Venu, N., Gupta, A., Dubey, S.M.: Applications of Internet of Things in diverse sectors. In: Kumar, S., Bye, R.T., Prasad, M. (eds.) Proc. ITAI 2025. LNNS, vol. 1506, pp. 1–11. Springer, Singapore (2026).
27. Arigela, A.K., Brahmareddy, A., Selvan, M.P., Sreenivas, T.S., Venu, N., Ansari, A.A.: Autonomous federated learning architectures for scalable IoT networks: enhancing distributed intelligence with privacy preservation. In: Kumar, S., Bye, R.T., Prasad, M. (eds.) Proc. ITAI 2025. LNNS, vol. 1505, pp. 1–12. Springer, Singapore (2026).
28. Arigela, A.K., Brahmareddy, A., Selvan, M.P., Sreenivas, T.S., Venu, N., Ansari, A.A.: Quantum-enhanced edge computing for optimized resource allocation in heterogeneous IoT networks: a deep reinforcement learning approach. In: Kumar, S., Bye, R.T., Prasad, M. (eds.) Proc. ITAI 2025. LNNS, vol. 1505, pp. 1–14. Springer, Singapore (2026).
29. Arigela, A.K., Brahmareddy, A., Sreenivas, T.S., Selvan, M.P., Venu, N., Lal, D.K.: Optimizing energy efficiency and latency in IoT devices through AI-based adaptive protocols in fog-edge computing environments. In: Saraswat, M., Rajan, A., Chakravorty, A. (eds.) Congress on Smart Computing Technologies (CSCT 2024). Smart Innovation, Systems and Technologies, vol. 121, pp. 1–12. Springer, Singapore (2025).
30. Arigela, A.K., Brahmareddy, A., Sreenivas, T.S., Selvan, M.P., Venu, N., Lal, D.K.: Blockchain-driven trustless security framework for multi-layered IoT architectures: a game-theoretic analysis of attack mitigation. In: Saraswat, M., Rajan, A., Chakravorty, A. (eds.) CSCT 2024. Smart Innovation, Systems and Technologies, vol. 122, pp. 1–13. Springer, Singapore (2026).