IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

Enhanced Reinforcement Learning with Optimization for the Threat Detection in VLC Networks-based 5G

Vijayakumari K[1] Anusudha K[2]

Research Scholar, Department of Electronics Engineering, Pondicherry University, Pondicherry[1]

Associate Professor, Department of Electronics Engineering, Pondicherry University, Pondicherry[2]

Abstract: Visible Light Communication (VLC) offers significant bandwidth, energy efficiency, and resistance to electromagnetic interference, making it a promising addition to 5G technology. However, due to its broadcast nature and dependence on Line-of-Sight (LoS), it is vulnerable to threats such as eavesdropping, spoofing, and jamming. The unique characteristics of optical signals, background noise, and the need for real-time, low-latency communication make threat detection in VLC-based 5G networks challenging. Therefore, this research identifies threats in VLC-based 5G networks using a novel intelligent, machine-learning-based optimization approach. Threat data are collected from the benchmark VLCdata dataset and preprocessed using the Discrete Wavelet Transform (DWT) denoising technique. Feature extraction is then performed using the Hough Transform (HT). Finally, threats are detected using the proposed Enhanced Reinforcement Learning (ERL) model, in which the Builder Optimization Algorithm (BOA) is employed to optimize the reinforcement learning parameters. The optimization process aims to maximize detection accuracy. Experimental results demonstrate that the proposed ERL-BOA model outperforms existing approaches across multiple performance measures. Specifically, it achieves 8.76% higher accuracy and 4.17% higher F1-score than existing methods, demonstrating its effectiveness for intelligent threat detection in VLC-based 5G networks.

Keywords: Visible Light Communication Networks; 5G; Discrete Wavelet Transform (DWT) Denoising; Hough Transform; Enhanced Reinforcement Learning; Builder Optimization Algorithm.

I. INTRODUCTION

Fifth-generation (5G) wireless communication technologies are transforming connectivity around the world and creating an avenue to new applications through the provision of incredibly fast information rates, low latency, and extensive device connection [1]. As a reaction to the increasing need of spectrum and even bandwidth, VLC has become a potential affiliate of Radio Frequency (RF) systems [2]. VLC utilizes the visible light spectrum to provide illumination and transmit information using Light-Emitting Diodes (LEDs) (LEDs can be used to both illuminate and to transmit information) [3]. VLC is highly preferred to be combined with 5G structures because of its extensive, uncontrolled bandwidth, the physical layer security, and electromagnetic interference immunity [4]. Nonetheless, both the transmission capability of VLC channels and the direct-view capabilities come with vulnerabilities that can subject the framework to a number of threats that could interfere with its reliability, confidentiality, and integrity [5].

Because of the intricate and, at the same time, the evolving character of these frameworks, threat detection in 5G networks, based on VLC methodology, has turned into a significant research field [6]. VLC channels are particularly vulnerable to eavesdropping, jamming, signal interception, and spoofing attacks, and these attacks can seriously compromise effectiveness and threaten user security [7]. Additionally, the diversity of 5G structures complicates the safe information transfer process of information since they unite VLC and RF with millimeter waves and fiber backhaul [8]. Similar vulnerabilities of VLC are sometimes not sufficiently controlled by the conventional security applications, which were initially developed in RF-oriented contexts [9]. This is due to the fact that realization of sound security in such hybrid communications environments is compromised by factors such as the possibility of high false detection rates, inflexibility, and slower response time to malicious activity [10]. These security challenges will be crucial to establishing both reliable and robust communication methodologies because VLC is expected to form a significant part of future 6G and IoT systems [11].

To address them, VLC-oriented 5G threat detection should involve sophisticated methods that could be used to detect any abnormality rapidly, adapt to changing network dynamics, and manage risks effectively [12]. More and more research is underway on the potential of machine learning and optimization-based approaches to boost detection accuracy and

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026
DOI: 10.17148/IJIREEICE.2026.14817

minimize false alarms and adapt to changing threats [13]. This is done to keep the specificity high in order to reduce false positives and enhance the sensitivity in identifying actual threats by using data-driven insights [14]. Further, in order to ensure that security measures may be applied to a variety of VLC applications, such as indoor wireless access, vehicle communication, as well as critical infrastructure, efficient threat detection frameworks should balance computational needs with scalability [15]. In order to provide secure, reliable, as well as sustainable next-generation communication infrastructures, it is imperative that robust and intelligent threat detection frameworks for VLC be established in 5G networks. The general model for detecting threats in VLC-oriented 5G networks is diagrammatically portrayed in Figure 1.

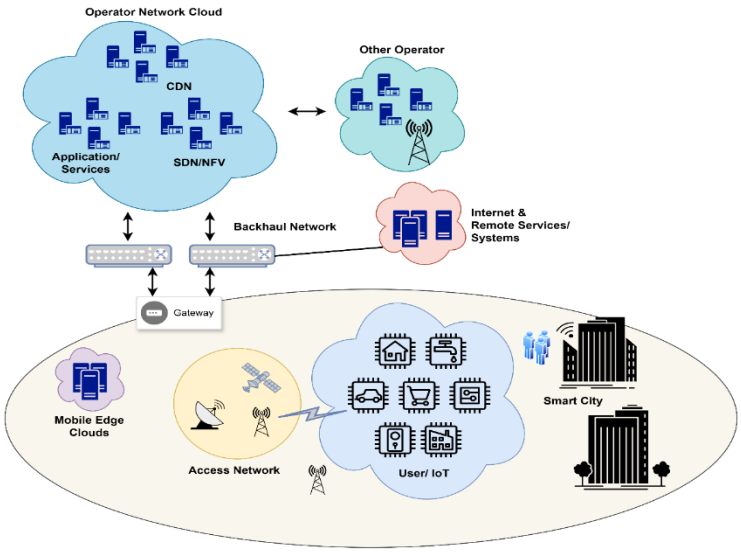

Figure 1. General model for detecting threats in VLC-oriented 5G Networks

The paper contribution is as below.

- To detect the threats in VLC networks-based 5G using novel intelligent machine learning-based optimization concept.
- To perform the pre-processing using the DWT Denoising approach and to extract the features by the HT method.
- To detect the threats by the novel ERL model, where the parameter tuning in RL is accomplished using the BOA algorithm that in turn returns the accuracy maximization as the objective function.

The paper organization is as follows. Section 1 is the introduction of threat detection models in VLC networks-based 5G. Section 2 is literature survey. Section 3 is proposed methodology with proposed model, dataset description, pre-processing by DWT, feature extraction by HT, detection by novel ERL and BOA algorithm. Section 4 is results and analysis. Section 5 is conclusion.

A. Motivation

There are now more opportunities for quick, low-latency, as well as energy-efficient information transport thanks to the quick deployment of 5G networks as well as VLC. Yet, due to its broadcasting nature, potential for eavesdropping, as well as susceptibility to signal interference, integrating VLC into 5G poses unique security challenges. In these dynamic situations, it is difficult for traditional threat detection techniques to strike a balance among accuracy, scalability, as well as instantaneous flexibility. In order to effectively handle new physical as well as cyber threats in VLC-enabled 5G networks, there exists an immediate need for intelligent, optimization-concentrated methods. In response to these challenges, the proposed ERL-BOA method combines state-of-the-art RL with bio-inspired optimization to provide robust, accurate, as well as effective threat identification, ensuring safe, reliable, and trustworthy communication for next 5G VLC frameworks.

II. RELATED WORK

The bio-inspired optimization methods used for VLC frameworks were thoroughly examined in this study [16]. With an emphasis on channel modelling, resource allocation, as well as energy efficiency, the researchers examined algorithms such as genetic algorithms, particle swarm optimization, ant colony optimization, as well as other evolutionary techniques created for VLC problems. The investigation highlighted how these techniques improved adaptability as well as durability in complex VLC environments. By categorizing algorithms based on performance gains as well as issue

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

regions, the research offered value. However, the paper highlighted that a number of methods have scaling issues as well as high computing demands, requiring more study for useful VLC applications in real-time.

This study proposed energy-efficient precoding methods of multi-user precoding VLC framework where privacy of delivery of the private messages had to be ensured [17]. The authors have developed an optimization methodology in which the optimization reduced the inter-user interference and balanced the information privacy and power economy. The technique according to the simulation results made communication safe on VLC channels and consumed less power. It had a primary advantage with its combined focus on both safety and energy consumption. Nevertheless, the model was more complex as the number of users grew, which emphasizes the necessity to work out more scalable precoding solutions.

The authors have introduced a new method that involved the application of distinct optical signal patterns to enhance security in VLC schemes [18] and this was referred to as Optic Fingerprint. The framework offered an additional level of authentication that also produced unique fingerprints to both anti-spoofing and anti-eavesdropping attempts. This research showed the degree to which fingerprinting was effective in offering secure information transfer within VLC without any increase in its design. It had the advantage of merging high identity verification with the signal integrity. But it may also be subject to device variability and ambient noise, which may compromise the accuracy of fingerprints, and adaptive calibration methods are necessary in practice.

This article discussed Automotive VLC (A-VLC) through the analysis of some of the techniques and devices that enabled car communication using visible light [19]. The researchers tested LEDs, photo detectors, and mixed VLC/RF structures as reliable options of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. This work showed how VLC may offer low-latency, high-bandwidth alternatives in congested RF channels in intelligent transportation systems. Safety applications and reduced RF interference were some of the advantages. However, the structure was limited by the weather conditions and visibility conditions besides installation expenses.

The authors presented NeoCommLight, VLC framework aimed at RF-restricted settings, including the Neonatal Intensive Care Unit (NICU) [20]. The approach minimized electromagnetic interference that could damage sensitive medical devices that used visible light as the main paradigm of communication. The framework was based on energy conservation and safety in addition to providing reliable and low-latency information transport. Its primary contribution was the increase of the VLC applications in the medical sector. Its application has both mobility and coverage area drawbacks, however, which may make it incapable of scaling beyond a few contexts.

In order to increase the capacity of VLC frameworks, this research proposed a uniformly distributed constellation codebook architecture [21]. This technique reduced symbol error rates as well as increased information throughput by optimizing constellation mapping. The method ensured better bandwidth utilization, which was crucial for VLC frameworks with large capacities. The advantage was in striking a balance among error performance as well as spectral effectiveness. However, issues with hardware execution still presented a problem, requiring more research into effective codebook design strategies. Some of the features and challenges of existing threat detection models in VLC networks-based 5G are shown below in Table 1.

Table 1 Features and challenges of existing threat detection models in VLC networks-based 5G

Citation	Methodology	Features	Challenges
[22]	VLC/RF networks utilizing NOMA	Ensures reliable hybrid communication	May limit delay in dynamic frameworks
[23]	DRL-oriented technique	Scalable in dynamic environments	Limits from convergence problems
[24]	Successive Light Interference Cancellation and Allocation (SLICA) algorithm	Enhances data throughput	Lessened in mobility conditions
[25]	Mixed RF-VLC relaying	Enhances reliability in fast mobility	Effectiveness may degrade in complex handover conditions
[26]	Probabilistic constellation shaping	Improve data rate	Complex receiver model
[27]	Hybrid FiWi using FSO, VLC, and mm-waves	Helps in multi-technology integration	More infrastructure complexity

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

III. PROPOSED METHODOLOGY

A. Proposed Model

The proposed threat detection in VLC networks-based 5G is composed of numerous phases such as data collection, pre-processing, feature extraction and detection. The VLCdata standard benchmark dataset is used to collect the information on the threats to VLC networks. The DWT Denoising technique is used to pre-process the gathered information. This pre-processed information is subjected to feature extraction using the HT approach. Finally, the novel ERL method performs the task of identifying risks from these derived attributes. The RL parameters are adjusted using BOA, a nature-inspired optimization technique. Accuracy maximization describes the ultimate objective function for the entire procedure. The overall proposed model of threat detection in VLC networks-based 5G is displayed in Figure 2 below.

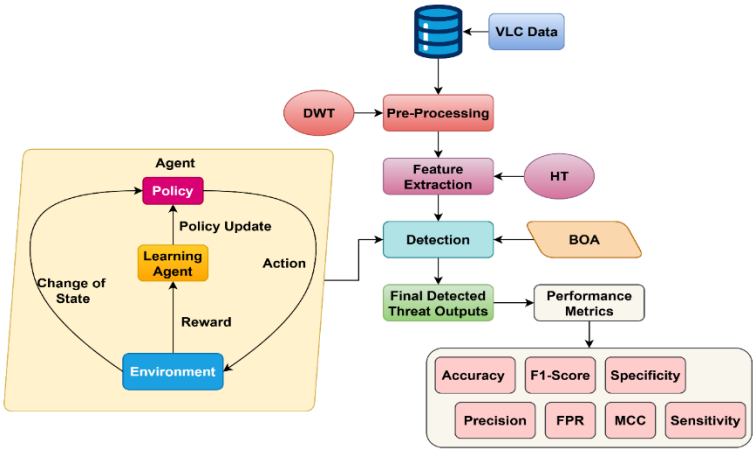

Figure 2. Overall Proposed model of Threat Detection in VLC Networks-based 5G

B. Dataset description

A publicly available benchmark for evaluating threat detection as well as intrusion prevention in VLC frameworks using 5G devices is the VLCdata dataset. It contains instances of both normal as well as malicious data generated beneath a range of VLC networking circumstances, including varying network loads, modulation methods, and lighting levels. Physical layer measures (Signal-to-Noise Ratio (SNR) received optical power, Bit Error Rate (BER)), traffic information (packet size, inter-arrival time, throughput), as well as attack-associated signatures (Denial of Service (DoS) floods, jamming, spoofing, and replay patterns) are among the feature groups that make up the dataset. By combining labelled benign as well as adversarial instances, VLCdata enables both supervised and unsupervised learning techniques for intrusion detection. It is particularly suitable for training and verifying machine learning as well as deep learning methods aimed at enhancing the security and resilience of VLC-oriented 5G communication frameworks because of its wide range of temporal and statistical features.

C. Pre-processing by DWT

In 5G frameworks focused on VLC Networks, pre-processing is crucial to increasing the accuracy as well as reliability associated with threat recognition. Due to variations in illumination, modulation, as well as device effectiveness, raw VLC traffic information sometimes contains noise, missing values, duplicate data, and inconsistent scales. Pre-processing techniques ensure that traffic metrics (such as packet size, jitter, as well as throughput) and physical layer characteristics (such as SNR, BER, and optical power) are consistently described for learning methods. Approaches for feature selection as well as dimensionality reduction can eliminate irrelevant characteristics while maintaining key attack patterns. By reducing computing burden, increasing classifier effectiveness, as well as enhancing method generalization, these steps eventually enable accurate and trustworthy real-time threat detection on 5G frameworks powered by VLC. Ambient optical noise, channel fluctuations, as well as device flaws often interfere with traffic and physical layer signals in VLC Networks-enabled 5G. This noise can reduce the quality of characteristics that are retrieved and make machine learning methods less efficient at detecting threats. DWT denoising is used as an effective pre-processing technique to address this. Through various resolution levels k, the DWT decomposes a signal $y(u)$ into detail coefficients E_k (high-frequency elements) as well as approximation coefficients B_k (low-frequency elements):

$$y(u) = \sum_l B_k(l)\phi_{k,l}(u) + \sum_k \sum_l E_k(l)\psi_{k,l}(u) \quad (1)$$

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

Here, the scaling function (low-pass filter) is shown by $\phi_{k,l}(u)$, the wavelet function (high-pass filter) is shown by $\psi_{k,l}(u)$, signal trends are captured by $B_k(l)$ and noise as well as rapid changes are captured by $E_k(l)$ respectively. The following actions are taken in order to denoise: Wavelet filters are used to separate the input VLC traffic signal into multi-level coefficients B_k and E_k. Noise-dominated high-frequency coefficients are reduced using a threshold function U:

$$E'_k(l) = \begin{cases} SGN\big(E_k(l)\big) \cdot (|E_k(l)| - U), & |E_k(l)| > U \\ 0, & |E_k(l)| \le U \end{cases} \quad (2)$$

This is referred to as "soft-thresholding." The inverse DWT yields the reconstructed denoised signal $\hat{y}(u)$:

$$\hat{y}(u) = \sum_l B_k(l)\phi_{k,l}(u) + \sum_k \sum_l E'_k(l)\psi_{k,l}(u) \quad (3)$$

By retaining significant approximation coefficients as well as removing noise-dominated features, DWT reduces irrelevant noise while maintaining critical traffic and attack-associated patterns. This improves the quality related to derived characteristics such as anomaly signals, modulation patterns, as well as packet-level measures. Consequently, in real-time VLC-5G threat detection scenarios, the cleaned dataset enables machine learning methods to achieve increased generalization, decreased false positives, as well as higher detection precision.

D. Feature extraction by HT

Feature extraction describes a crucial pre-processing step for effective threat identification in VLC Networks-based 5G since it transforms unprocessed optical as well as traffic signals into meaningful descriptions suitable for machine learning. Physical-layer features such as SNR, BER, received optical power, and modulation methods, as well as network-level measurements such as packet inter-arrival time, throughput, and jitter, may be included in VLC settings. It is possible to identify among malicious as well as benign traffic behaviors, including replay, spoofing, jamming, and Denial-of-Service (DoS) attacks, by extracting these distinguishing traits. To reduce dimensionality while maintaining attack-associated patterns, sophisticated techniques are applied. With VLC-enabled 5G frameworks, this technique increases classifier efficacy, lowers computing burden, as well as ensures accurate real-time threat detection.

Determining anomalous traffic or malicious patterns in high-dimensional signal or traffic data in 5G networks with VLC often requires that hidden structures in the high-dimensional data be revealed. Transforming the signal domain point of information into a parameter domain, the HT can be used to describe an effective feature extraction framework which simplifies recognizing structured patterns like synchronized packet timings, periodic bursts, or modulation anomalies that may represent a threat (e.g. replay or jamming attacks). The general line equation may be used to transform points in the information space (y, z) into a parameter space in order to describe a signal:

$$z = ny + d \quad (4)$$

In the Hough space, this is shown as:

$$\rho = y\cos\theta + z\sin\theta \quad (5)$$

Here, the orientation angle associated with the line is shown by θ and the perpendicular distance from the origin to the line is shown by ρ respectively. In the Hough parameter space, each point (y, z) in the signal domain relates to a sinusoidal curve. Curve groups that overlap indicate the presence of ordered patterns that can be recognized as features. HT can be used in VLC-5G threat detection to: Recognize recurring or coordinated traffic spikes that point to flooding or DoS attempts; identify recurring modulation irregularities linked to jamming or spoofing; and examine geometric correlations in packet arrival times or variations in optical power to help differentiate between benign and malicious activity. By converting raw VLC signals as well as traffic traces into geometric characteristics, the HT reduces noisy variability as well as improves structural patterns that are essential for machine learning classifiers. In 5G frameworks that use VLC, this enhances the accuracy as well as robustness of the intrusion detection system (IDS).

E. Detection by Novel ERL

As detection allows the rapid discovery of malicious activity within both optical and traffic information streams, it is critical to defending VLC Networks-oriented 5G. VLC is sensitive to ambient light, has a limited range, and is Line-of-Sight (LoS)-dependent, in which case, attackers can exploit vulnerabilities with the help of a replica, spoofing, jamming, or DoS attacks. Detection techniques use machine learning and the deep learning classifiers. These classifiers are trained based on extracted features, such as statistics of the traffic (packet timing, throughput, jitter) and physical-layer statistics

DOI: 10.17148/IJIREEICE.2026.14817

(SNR, BER, received optical power). Detection architectures provide the basis of on-demand intrusion prevention as they differentiate between normal communication activities and strange or malicious activities. This procedure enhances network strength, privacy, and integrity of information, and reliable implementation of 5G structures with VLC in the smart cities and the critical infrastructures.

Since RL can be modified to suit different environments, it presents tremendous benefits in terms of detecting threats in VLC Networks based on 5G. In contrast to the unchanging detection, RL refines its decision-making process constantly by interacting with the network, allowing prompt adaptability to new or changing attack techniques including DoS, spoofing, or jamming. Since it balances not only accuracy but also False Alarm Rates (FARs) and reduces computing requirements, its incentive-based approach allows to optimize detection processes. Additionally, due to a combination of adaptive choices in the set of relevant information and the enhancement of detection methods without full retraining, RL can cope with the numerous peculiarities of VLC-5G traffic. Due to its flexibility, RL could excellently work in time-intensive and resource-induced VLC contexts, boosting the performance of intrusion detection, provision of strong security, and superior Quality-of-Service (QoS) in future communication systems.

Although it is extremely adaptable, RL possesses several drawbacks as far as threat detection within 5G VLC frameworks is concerned. The high cost of computation and complex training process are the biggest drawbacks of RL since it typically involves a lot of interaction information besides being costly in terms of repetitiveness before discovering the best detection rules. It is neither the most suitable choice when real-time VLC-5G scenarios that have strict latency requirements are needed nor might require numerous resources. Moreover, RL designed methods often fail on both instability and convergence, particularly in dynamic VLC systems subject to changing motion and lighting conditions. Another issue that decreases the ability to generalize to unknown threats is overfitting to a certain pattern of attacks. In addition, it is not easy to develop a functional mechanism of rewards; an ill-defined reward system can result in biased learning or unintended detection processes, which threaten the security integrity.

ERL is much better in terms of threat detection in VLC frameworks-oriented 5G, as it overcomes the key disadvantages inherent in the traditional RL. ERL is also found to converge faster and be more stable in very dynamic VLC scenarios due to a combination of advanced methods such as experience replay, hybrid exploration-exploitation methods and adaptive reward shaping methods. Its ability to strike a balance between real-time learning and long-term policy enhancement will guarantee improved detection of a variety of threats, such as replay and spoofing and jammer attacks. Using feature extraction or ensemble rules improves generalization to new attacks and increases robustness to changing adversarial strategies, ERL. Moreover, its effectiveness in resource-constrained environments as compared to classical RL decreases computation. These advancements will allow ERL to provide powerful, scalable, and even real-time threat detection in future VLC-5G systems.

Conventional static detection techniques are minimal effective in the rapidly varying environment of VLC frameworks-oriented 5G, which is characterized by shifting light levels, fluctuating optical power, as well as distinct traffic patterns. By continuously interacting with the framework to learn the optimal detection techniques, ERL provides a versatile solution for real-time threat identification. The environment in ERL is described by a Markov Decision Process (MDP), which is defined by the following tuple:

$$N = (T, B, Q, S, \gamma) \tag{6}$$

Here, the discount factor is shown by $\gamma \in [0,1]$, reward function is shown by $S(t, b)$, state transition probability is shown by $Q(t'|t, b)$, group of actions (e.g., categorize as benign, detect spoofing, jamming and replay) is shown by B and the group of states (e.g., SNR, packet delay, traffic statistics and BER) is shown by T respectively. The goal is to increase the expected total reward:

$$R^*(t, b) = \underbrace{max}_{\pi} F[\sum_{u=0}^{\infty} \gamma^u S(t_u, b_u) \,|t_0 = t, b_0 = b, \pi] \tag{7}$$

Here, the detection strategy is denoted by π. ERL enhancements include Experience Replay, which uses prior experiences (t, b, s, t') to stabilize the training procedure. By dynamically altering incentives, adaptive reward shaping discourages false alarms as well as encourages precise danger detection.

$$S(t, b) = \alpha \cdot TP - \beta \cdot FP - \delta \cdot FN \tag{8}$$

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

Here, the variables α, β, and δ are changeable. In order to improve generalization against unknown attacks, multiple detection algorithms are used. ERL adjusts its policy during training using a gradient-oriented technique:

$$\theta \leftarrow \theta + \eta \nabla_{\theta} F[S(t,b)] \tag{9}$$

Here, η stands for the learning rate as well as θ for the policy parameters. By combining ensemble decision-making with adaptive learning, ERL achieves robust as well as scalable threat detection in VLC-5G. Even in contexts with lessened resources, it maintains low False Positive Rates (FPRs) as well as better detection accuracy while flexibly adapting to new attack patterns such as jamming or spoofing.

F. BOA Algorithm

For 5G networks on the basis of VLC, optimization is essential for improving the effectiveness as well as reliability of threat detection. Traditional detection methods may have effectiveness constraints due to the complex nature of VLC situations, which are especially impacted by changes in traffic, noise, as well as illumination. Optimization techniques aid in selecting the major distinctive characteristics, fine-tuning method parameters, as well as weighing the trade-offs between computing costs, FPRs, and detection accuracy. Metaheuristic methods allow classifiers to be dynamically adjusted, ensuring that they are resilient to a variety of threats, including DOS, spoofing, as well as jamming. By incorporating optimization into detection methodologies, VLC-5G frameworks may achieve better detection accuracy, faster convergence, as well as scalable effectiveness, enabling safe and instantaneous communications.

Human building techniques serve as a motivation for BOA. The BOA mimics the two primary strategies used by builders: (i) making major structural changes in accordance with the model, as well as (ii) making alterations to enhance details and aesthetic appeal. Exploration as well as exploitation are the two phases of the algorithm's operation. While the exploitation step improves these solutions to increase effectiveness, the exploration phase allows BOA to find potential solutions.

BOA describes a population-based metaheuristic in which every member of the population defines a potential building format in the search space. Each structure's configuration is determined by a set of design factors. Every structure has a vector representation in mathematics, and every vector element corresponds to a certain design parameter. To encourage variation in the early solutions, entire structures' placements are chosen at random inside the search space at the start of the BOA procedure. In order to optimally distribute buildings throughout the feasible region, this configuration follows a predetermined equation, as given in Eq. (10).

$$y_{j,e} = LB_e + s \cdot (UB_e - LB_e) \tag{10}$$

Here, Y_j denotes the j^{th} structure (developed solution), $y_{j,e}$ denotes its e^{th} model parameter, O describes the total number of structures, n describes the number of model parameters, s describes a random value between 0 and 1, and LB_e and UB_e represents the lowest as well as maximum limits associated with the e^{th} design parameter, respectively. Each BOA format represents a complete group of decision variables, resulting in a population matrix as shown in Eq. (11).

$$Y = \begin{bmatrix} Y_1 \\ \vdots \\ Y_j \\ \vdots \\ Y_O \end{bmatrix}_{O \times n} = \begin{bmatrix} y_{1,1} & \cdots & y_{1,e} & \cdots & y_{1,n} \\ \vdots & \ddots & \vdots & \iddots & \vdots \\ y_{j,1} & \cdots & y_{j,e} & \cdots & y_{j,n} \\ \vdots & \iddots & \vdots & \ddots & \vdots \\ y_{O,1} & \cdots & y_{O,e} & \cdots & y_{O,n} \end{bmatrix}_{O \times n} \tag{11}$$

In this case, Y stands for the BOA population matrix. A fitness function that measures each candidate format's conformity to the ideal model is used for evaluation. As seen in Eq. (12), the values related to the fitness function for the entire population are maintained in a vector.

$$G = \begin{bmatrix} G_1 \\ \vdots \\ G_j \\ \vdots \\ G_O \end{bmatrix}_{O \times 1} = \begin{bmatrix} G(Y_1) \\ \vdots \\ G(Y_j) \\ \vdots \\ G(Y_O) \end{bmatrix}_{O \times 1} \tag{12}$$

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

Here, G stands for the vector of fitness function values and G_j for the j^{th} structure's fitness function value. The best optimized format is identified as the model having the greatest favorable fitness function value. In order to explore different regions associated with the search space, candidate structures undergo significant changes throughout the exploration stage. The model configurations with better fitness function values serve as standards for major changes for all structures in the population. Eq. (13) is used to determine the set of potential modifications for each format.

$$DN_j = \{Y_l | G_l \leq G_j\} \tag{13}$$

Here, Y_l denotes a model setup having a greater fitness function value than the j^{th} format, and DN_j denotes the set of possible changes for the j^{th} format. Out of these potential models, an alteration is selected at random, as well as the related format's position is updated using a mathematical method based on generic structural variations in construction, as shown in Eq. (14). The modification is accepted in accordance with Eq. (15) if the updated configuration improves the fitness function.

$$y_{j,k}^{Q1} = y_{j,k} + J \cdot \cos\left(\frac{\pi}{2}s\right) \cdot \left(TN_{j,k} - J \cdot y_{j,k}\right) \tag{14}$$

$$Y_j = \begin{cases} Y_j^{Q1}, & G_j^{Q1} < G_j \\ Y_j, & otherwise \end{cases} \tag{15}$$

Here, Y_j^{Q1} describes the updated format in the first stage of BOA, $y_{j,k}^{Q1}$ describes its k^{th} model parameter, G_j^{Q1} describes the updated fitness function value, TN_j describes the chosen modification reference, $TN_{j,k}$ describes its k^{th} parameter, s describes a random value within [0−1], and J describes a random count selected from the group {1,2}. The exploitation stage, as used in BOA, defines the phase of exploitation where little modifications are done in near proximity to the current formats in order to maximize their configurations. Eq. (16) is used to find the optimal positions for structures, and Eq. (17) is used to approve the alterations if they enhance the fitness function.

$$y_{j,k}^{Q2} = y_{j,k} + \left(1 - 2 \cdot \cos\left(\frac{\pi}{2}s\right)\right)\frac{(UB_k - LB_k)}{u} \tag{16}$$

$$Y_j = \begin{cases} Y_j^{Q2}, & G_j^{Q2} < G_j \\ Y_j, & otherwise \end{cases} \tag{17}$$

Here, Y_j^{Q2} shows the second stage's improved format, $y_{j,k}^{Q2}$ describes its k^{th} model parameter, G_j^{Q2} describes the updated fitness function value, s describes a random count between 0 and 1, and u describes the count of iterations. BOA effectively balances local exploitation and global exploration by combining these two stages, which enables it to effectively optimize difficult model problems. The pseudocode of BOA is displayed in Algorithm 1 below. The proposed ERL-BOA model for the VLC Networks-based 5G is portrayed in Figure 3.

Algorithm 1: *BOA*

Start

Input fitness function $G(Y)$*, population size* O*, problem dimension* n*, lower as well as upper bounds and maximum iterations [extracted features of the proposed threat detection in VLC networks-based 5G model]*

Output best solution Y_{Best} *and optimal objective value* $G(Y_{Best})$ *[accuracy maximization of the proposed threat detection in VLC networks-based 5G model]*

For every structure $j = 1,2,\cdots,O$ *and dimension* $e = 1,2,\cdots,n$

$$y_{j,e} = LB_e + s \cdot (UB_e - LB_e)$$

Form initial population $Y = [Y_1;\ Y_2;\ \cdots;\ Y_O]$

$$G = \begin{bmatrix} G_1 \\ \vdots \\ G_j \\ \vdots \\ G_O \end{bmatrix}_{O\times 1} = \begin{bmatrix} G(Y_1) \\ \vdots \\ G(Y_j) \\ \vdots \\ G(Y_O) \end{bmatrix}_{O\times 1}$$

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

For $u = 1$ *to* U_{Max}

For every format Y_j

$$DN_j = \{Y_l | G_l \leq G_j\}$$

Select one superior method $TN_j \in DN_j$ *in a random manner*

$$y_{j,k}^{Q1} = y_{j,k} + J \cdot cos\left(\frac{\pi}{2}s\right) \cdot \left(TN_{j,k} - J \cdot y_{j,k}\right)$$

$$y_{j,k}^{Q2} = y_{j,k} + \left(1 - 2 \cdot cos\left(\frac{\pi}{2}s\right)\right)\frac{(UB_k - LB_k)}{u}$$

End for

End for

End for

Update global best solution [maximized accuracy value of the proposed threat detection in VLC networks-based 5G model]

Stop

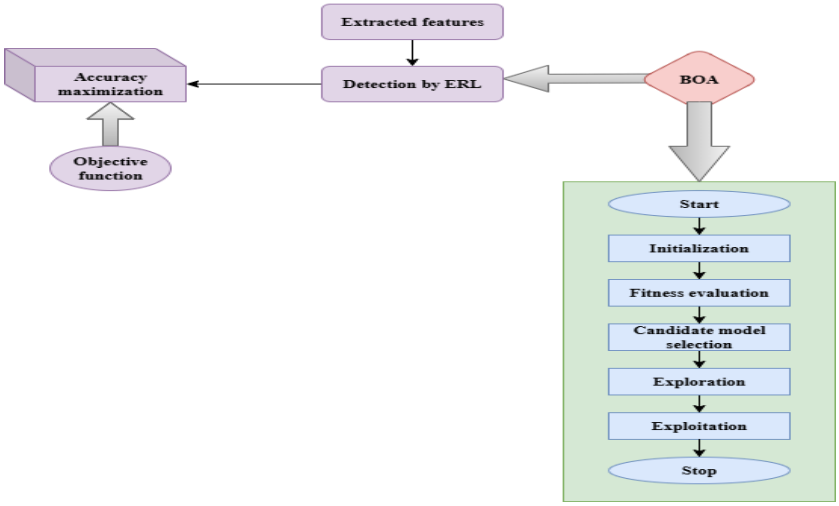

Figure 3. Proposed ERL-BOA model for the VLC Networks-based 5G

IV. RESULTS AND ANALYSIS

A. Experimental Setup

The proposed ERL-BOA for the VLC networks-based 5G model was implemented in MATLAB and the findings were discussed. The population size was 10 and 200 number of iterations were considered. The proposed ERL-BOA was compared with numerous models like DRL, SLICA, PCS and FiWi with respect to analysis such as accuracy, F1 Score, specificity, FPR, precision, Matthew's Correlation Coefficient (MCC) and sensitivity to prove the superiority of the developed VLC networks-based 5G model.

B. Accuracy analysis

According to the evaluation of threat detection accuracy in VLC Networks-backed 5G, the proposed ERL-BOA technique accomplishes better than existing techniques such as DRL, SLICA, PCS, as well as FiWi in a variety of iterations as in Figure 4. The entire methods exhibit a consistent improvement in accuracy among 20 and 200 iterations, indicating effective learning as the number of iterations rises. However, starting at 90.30% at 20 iterations as well as rising to an astounding 99.06% at 200 iterations, the proposed ERL-BOA continuously outperforms the others. By contrast, after 200 iterations, SLICA as well as PCS achieve 87.90% and 85.79%, respectively, while DRL shows a slight increase from 86.12% to 91.08%. With an accuracy gain of only 83.88%, FiWi exhibits the minimal enhancement. This work confirms that ERL-BOA more effectively integrates learning as well as optimization, resulting in faster convergence and higher

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026
DOI: 10.17148/IJIREEICE.2026.14817

detection accuracy for novel 5G VLC risks. The proposed ERL-BOA for the VLC networks-based 5G model in terms of accuracy is 8.76%, 12.70%, 15.47% and 18.10% better than DRL, SLICA, PCS and FiWi respectively.

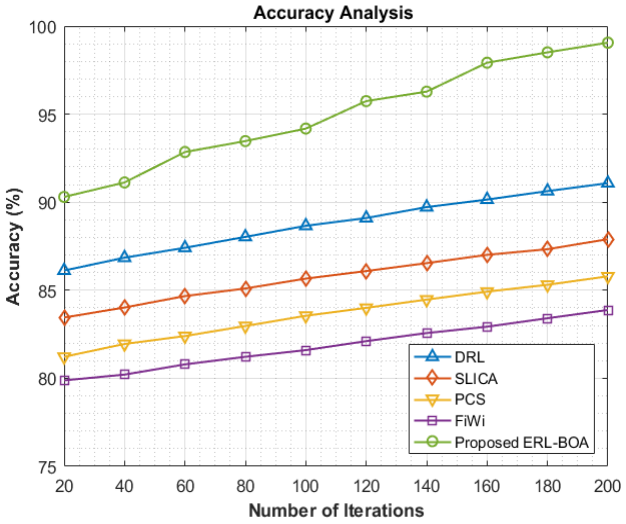

Figure 4. Accuracy analysis

C. F1 Score analysis

The assessment of the F1 score for threat detection in 5G powered by VLC frameworks highlights the recommended ERL-BOA technique's consistent advantage over conventional approaches as in Figure 5. Every technique shows steady, incremental progress over 20–200 iterations, indicating improved memory as well as accuracy balance with more training. While SLICA as well as PCS achieve scores of 85.69% and 83.05%, respectively, DRL exhibits relatively higher F1 scores within the existing methods, rising from 84.25% at 20 iterations to 89.30% at 200 iterations. After 200 rounds, FiWi displays the minimal improvement, increasing marginally to 81.45%. By contrast, the proposed ERL-BOA accomplishes significantly better than its counterparts, starting at 86.70% as well as rising steadily to 93.02%. These results confirm its potency as well as efficacy in achieving enhanced detection reliability in 5G environments with dynamic VLC support. The F1 Score associated with the proposed ERL-BOA for the 5G method on the basis of VLC frameworks is 4.17%, 8.55%, 12% and 14.21% higher than that of DRL, SLICA, PCS, as well as FiWi, respectively.

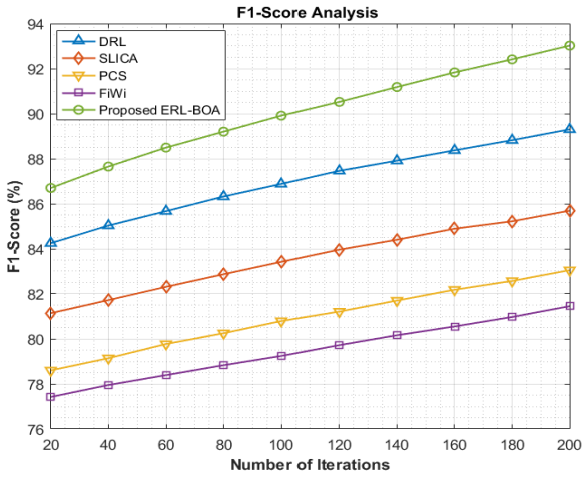

Figure 5. F1 Score analysis

D. Specificity analysis

The proposed ERL-BOA approach steadily surpasses existing methods in correctly recognizing non-threat instances, according to the specificity study for threat detection in VLC frameworks-oriented 5G as in Figure 6. The performance difference remains noticeable even if entire methods exhibit a gradual improvement in specificity as the number of repetitions rises. DRL performs exceptionally well, rising from 88.32% at 20 iterations to 91.63% at 200. SLICA comes

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

in second, reaching 89.30% at 200 iterations. PCS as well as FiWi achieve final results of 87.25% and 86.00%, respectively, indicating somewhat lesser gains. Better progress is demonstrated by the proposed ERL-BOA, which starts at 90.46% as well as reaches 94.28% after 200 iterations. This illustrates how it might lower false positives, hence increasing the trustworthiness as well as dependability of 5G VLC threat detection frameworks. For the 5G strategy on the basis of VLC networks, the specificity associated with the proposed ERL-BOA is 2.89%, 5.58%, 8.06% and 9.63% higher than those of DRL, SLICA, PCS, as well as FiWi, respectively.

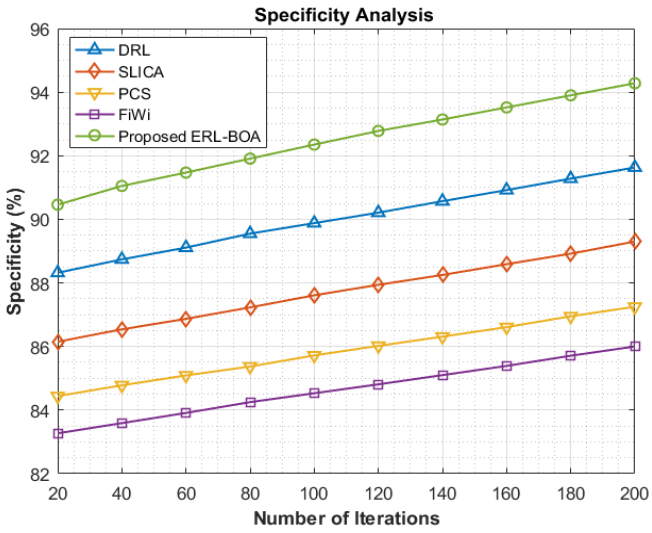

Figure 6. Specificity analysis

E. FPR analysis

The proposed ERL-BOA method's strong potential to lower false threat identifications is demonstrated by the FPR evaluation for threat identification in VLC frameworks-driven 5G as in Figure 7. The entire methods show a decreasing trend in FPR over the course of the iterations, suggesting that accuracy improves with more training. PCS as well as SLICA lag at 12.5% and 10.85%, respectively, while FiWi has the highest FPR values, dropping from 16.73% after 20 iterations to 13.72% after 200 iterations. DRL performs better, falling from 12.15% to 8.92% during the similar time period. Starting with a low FPR of 9.54% as well as steadily decreasing to just 5.18% after 200 iterations, the proposed ERL-BOA far outperforms the others. This notable decrease shows that it can reduce false alerts, enhancing reliability in real-world 5G VLC threat detection scenarios. The FPR associated with the proposed ERL-BOA in the 5G approach on the basis of VLC frameworks is greater than that of DRL, SLICA, PCS, as well as FiWi by 41.93%, 52.26%, 58.73% and 62.24%, respectively.

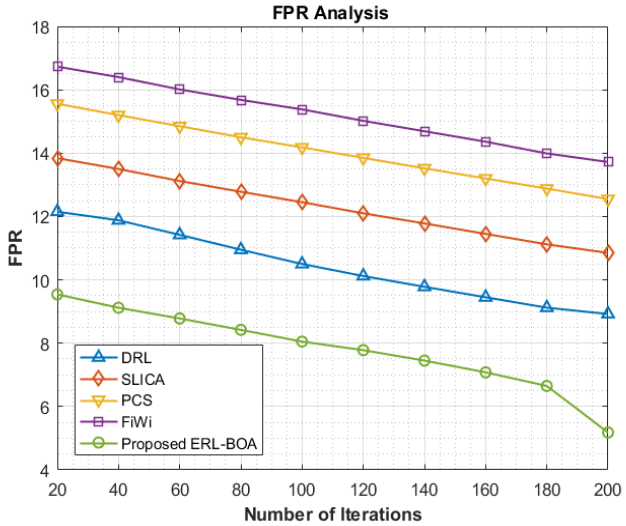

Figure 7. FPR analysis

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

F. Precision analysis

The precision evaluation for threat detection in 5G frameworks using VLC demonstrates that the proposed ERL-BOA technique consistently yields improved outcomes in correctly identifying real threats while lowering classification errors as in Figure 8. Precision values for entire methods progressively grow with more iterations, showing steady enhancement with continued training. DRL performs the best among the baseline approaches, rising from 85.42% at 20 iterations to 89.32% at 200 iterations. While PCS as well as FiWi show comparatively lesser accuracy, ending at 83.40% and 81.92%, respectively, SLICA continues to make steady progress, reaching 85.60% at the final iteration. By contrast, the proposed ERL-BOA significantly outperforms its rivals, starting at 87.66% as well as increasing to 92.58% after 200 iterations. This demonstrates how well it reduces false positives, ensuring reliable as well as efficient detection on 5G frameworks with VLC support. In the 5G network employing VLC, the precision associated with the proposed ERL-BOA is 3.65%, 8.15%, 11.01% and 13.01% greater than that of DRL, SLICA, PCS, as well as FiWi, respectively.

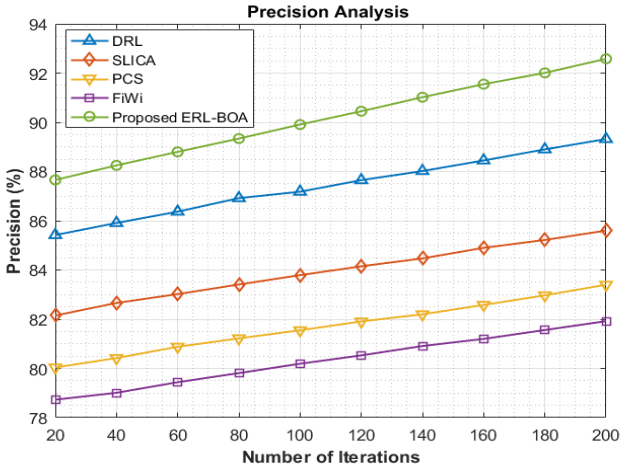

Figure 8. Precision analysis

G. MCC analysis

When compared to existing methods, the proposed ERL-BOA method significantly outperforms them in the MCC analysis for threat identification in VLC frameworks-oriented 5G as in Figure 9. With each cycle, MCC values for entire approaches increase progressively, suggesting a better balance among false positives as well as real positives. PCS as well as SLICA achieve moderate gains, reaching 71.30% and 74.68%, respectively, whereas FiWi exhibits the least effectiveness, rising from 65.40% at 20 iterations to 69.38% at 200 iterations. Over the course of the iterations, DRL rises from 72.35% to 77.92%, above the baselines. After 200 cycles, the recommended ERL-BOA exhibits a noticeable improvement, rising from 75.68% to 84.40%. This sophisticated MCC demonstrates that ERL-BOA maintains higher consistency as well as dependability in threat categorization, ensuring robust effectiveness in complex 5G VLC scenarios. The MCC associated with the proposed ERL-BOA in the 5G framework using VLC is 8.32%, 13.02%, 18.37% and 21.65% greater than that of DRL, SLICA, PCS, as well as FiWi, respectively.

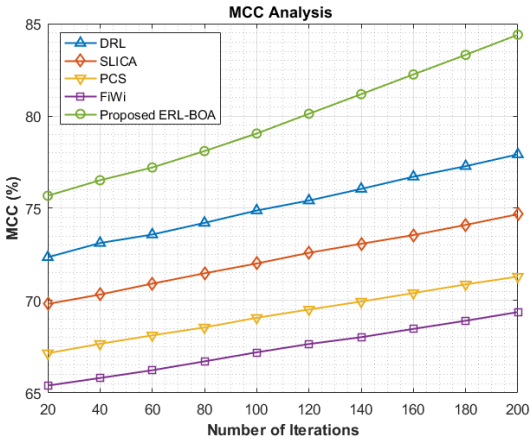

Figure 9. MCC analysis

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.021 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 8, August 2026

DOI: 10.17148/IJIREEICE.2026.14817

H. Sensitivity analysis

The improved capacity related to the proposed ERL-BOA method to accurately identify real threats is highlighted by the sensitivity evaluation for threat detection in VLC frameworks-based 5G as in Figure 10. With additional iterations, entire methods show a progressive increase in sensitivity, underscoring the benefit of extended training. DRL achieves the highest sensitivity within the baseline techniques, increasing from 83.42% at 20 iterations to 88.55% at 200 iterations. FiWi continues to be the least, ending at 80.89%, while SLICA as well as PCS see modest gains, reaching 84.80% and 82.40%, respectively. By contrast, after 200 iterations, the proposed ERL-BOA exhibits a significant enhancement, rising from 85.76% to 92.58%. This ongoing development confirms its effectiveness in reducing false negatives as well as enhancing detection reliability, making it perfect for protecting dynamic VLC-capable 5G setups. In the 5G network with VLC, the sensitivity associated with the proposed ERL-BOA is 4.55%, 9.17%, 12.35% and 14.45% more than that of DRL, SLICA, PCS, as well as FiWi, respectively.

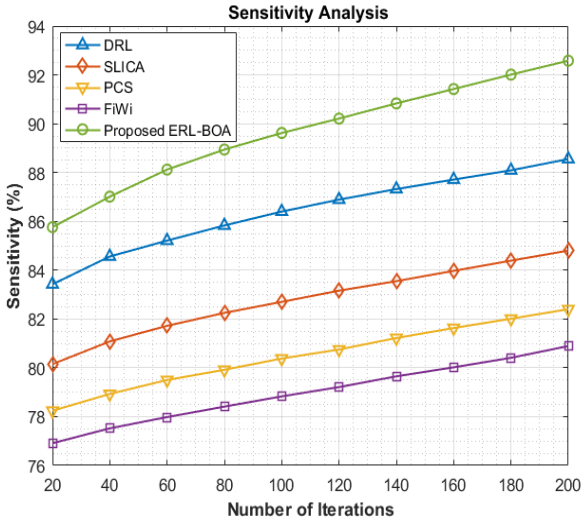

Figure 10. Sensitivity analysis

V. DISCUSSION

The benefits associated with the proposed ERL-BOA approach are evident from the comprehensive evaluation of threat detection in VLC frameworks using 5G in terms of a number of performance measures, including accuracy, F1 score, specificity, FPR, precision, MCC, as well as sensitivity. ERL-BOA consistently achieves higher values, indicating faster convergence as well as greater generalization, even though all of the existing methods, including DRL, SLICA, PCS, and FiWi, show increasing improvements with more iterations. Significant improvements in MCC as well as significant drops in FPR highlight its ability to balance accurate and inaccurate classifications, and high sensitivity ensures reliable detection of actual threats. ERL-BOA demonstrates notable efficacy gains above baselines, confirming its ability to more effectively combine learning and optimization. These findings support ERL-BOA as a viable technique for enhancing future 5G VLC threat detection framework's effectiveness, dependability, as well as trustworthiness.

VI. CONCLUSION

This research used a novel intelligent optimization strategy with a machine learning foundation to identify hazards in 5G frameworks on the basis of VLC. The VLCdata standard benchmark dataset was used to collect information on risks to VLC frameworks. The DWT Denoising technique was used to process the collected information. From this pre-processed information, features were extracted using the HT approach. Finally, the threats from these extracted characteristics were identified using the new ERL method. For adjusting the RL settings, BOA, a nature-inspired optimization technique, was taken into consideration. Maximizing accuracy determined the ultimate objective function for the whole procedure. In comparison to other conventional methods, the experimental investigation demonstrated the superiority associated with the suggested ERL-BOA method in detecting threats in VLC networks inside 5G across a number of parameters. For the VLC frameworks-oriented 5G method, the proposed ERL-BOA accomplished 8.76% better in accuracy as well as 4.17% better in F1 Score than the remaining approaches currently in use.

Data availability statement: The datasets generated during and/or analyzed during the current study are available in the [Zenodo] repository, [https://zenodo.org/records/15121418?utm_source]

DOI: 10.17148/IJIREEICE.2026.14817

REFERENCES

[1] Bin Chen, "A machine learning based approach for 5G network security monitoring", Applied Mathematics and Nonlinear Sciences, vol. 9, no. 1, January 2024.

[2] Sandeep Pirbhulal, Habtamu Abie, Martin Jullum, Didrik Nielsen, and Anders Loland, "AI/ML for 5G and Beyond Cybersecurity", 2024.

[3] Mohamed Amine Arfaoui, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghrayeb, Chadi Assi, Majid Safari, Harald Haas,"Physical Layer Security for Visible Light Communication Systems: A Survey", May 2019.

[4] Prokash Sikder, M. T. Rahman and A. S. M. Bakibillah,"Advancements and Challenges of Visible Light Communication in Intelligent Transportation Systems: A Comprehensive Review", Photonics, vol. 12, no. 3, 2025.

[5] S. Sherlin, "A comprehensive review of visible light communication (VLC)", i-manager s Journal on Communication Engineering and Systems, vol. 12, no. 2, January 2023.

[6] Anitha Vijayalakshmi, Mritha Ramalingam, M. K. Nagarajan and Arokiya Prasad, "Exploring innovations and opportunities in visible light communication for 5G-enabled industrial IoT systems", Journal of Optics, May 2025.

[7] Jupeng Ding, Chih-Lin I, Jintao Wang, and Hui Yang, "On the Performance of Non-Lambertian Relay-Assisted 6G Visible Light Communication Applications", Photonics, vol. 12, no. 6, May 2025.

[8] Arun Kumar, T.D.N.S.S Sarveswara Rao, Gireesh Babu C.N and Nishant Gaur, "Analysis of PAPR reduction algorithms for optical OFDM 5G radio waveform system for visible light communication", Journal of Optical Communications, January 2025.

[9] Tomas P V Andrade, Celso Henrique de Souza Lopes, Letícia Carneiro Souza and Arismar Cerqueira Sodré Junior, "Demonstration of a Hybrid B5G System Integrating VLC and RF-Based Technologies with Access Networks", Applied Sciences, vol. 15, no. 2, January 2025.

[10] Monica Bhutani, Bharat Singh, Ashutosh Gupta and K. Sudha, "Visible Light Communication Technologies: A Review of IEEE 802.15.7 and Its Role in Next-Generation Networks", International Journal of Communication Systems, vol. 38, no. 11, June 2025.

[11] Jupeng Ding, Jintao Wang, Chih-Lin I and Hui Yang, "Performance Comparison of Lambertian and Non-Lambertian Drone Visible Light Communications for 6G Aerial Vehicular Networks", Applied Sciences, vol. 15, no. 11, May 2025.

[12] Anitha Jebamani Soundararaj, Godfrey Winster Sathianesan, “Task offloading scheme in Mobile Augmented Reality using hybrid Monte Carlo tree search (HMCTS)", Alexandria Engineering Journal, vol. 108, pp. 611-625, 2024.

[13] Samson S Arivumani and Nagarajan M, "Adaptive convolutional-LSTM neural network with NADAM optimization for intrusion detection in underwater IoT wireless sensor networks", Engineering Research Express, vol. 6, September 2024.

[14] Rekha, V., Samuel Manoharan, J., Hemalatha, R. & Saravanan D. "Deep Learning Models for Muliple Face Mask Detection under a complex big data environment", Procedia Computer Science, vol. 215, pp. 706-712, 2022.

[15] J. Samuel Manoharan, G. Vijayasekaran, I. Gugan, and P. Nirmala Priyadharshini, "Adaptive forest fire optimization algorithm for enhanced energy efficiency and scalability in wireless sensor networks", Ain Shams Engineering Journal, vol. 16, no. 7, July 2025.

[16] Martin Dratnal, Lukas Danys & Radek Martinek, "Bio-inspired optimization methods for visible light communication: a comprehensive review", Artificial Intelligence Review, vol. 58, no. 246, May 2025.

[17] Son T. Duong, Thanh V. Pham, Chuyen T. Nguyen, Anh T. Pham, "Energy-Efficient Precoding Designs for Multi-User Visible Light Communication Systems with Confidential Messages", Information Theory, September 2023.

[18] Chen Xuanbang, Liu Ziqi, Zhang Xun, Wang Yuhao, Shi Dayu, Liu Xiaodong,"Optic Fingerprint: Enhancing Security in Visible Light Communication Networks", Signal Processing, April 2024.

[19] L. Cheng, Y. Wu, C. Xu, K. Ashraf, and A. Ashok, "Automotive Visible-Light Communication: Alternative Devices and Systems," Tsinghua Science and Technology, vol. 28, no. 4, pp. 719-728, August 2023.

[20] G. D. H. Niranga, A. R. Devidas and M. V. Ramesh, "NeoCommLight: A Visible Light Communication System for RF-Restricted NICUs," IEEE Access, vol. 12, pp. 12827-12842, 2024.

[21] L. Yu et al., "Uniform-Distributed Constellation Codebook Design for High-Capacity Visible Light Communications," IEEE Communications Letters, vol. 27, no. 11, pp. 2993-2997, Nov. 2023.

[22] K. G. Rallis et al., "Energy Efficient Cooperative Communications in Aggregated VLC/RF Networks With NOMA," IEEE Transactions on Communications, vol. 71, no. 9, pp. 5408-5419, Sept. 2023.

[23] T. Verma, A. Raza, S. Shrivastava, A. Kumar, D. P. Kothari, and U. D. Dwivedi, "A Novel On-Policy DRL-Based Approach for Resource Allocation in Hybrid RF/VLC Systems," IEEE Transactions on Consumer Electronics, vol. 71, no. 1, pp. 550-560, Feb. 2025.

[24] H. Sharma and R. K. Jha, "Successive Light Interference Cancellation and Allocation (SLICA) Algorithm for Indoor VLC System: A Backbone for 6G Network," IEEE Access, vol. 11, pp. 12623-12635, 2023.

DOI: 10.17148/IJIREEICE.2026.14817

[25] R. Singh, I. Ahmad and J. Huusko, "Mixed RF-VLC Relaying Systems for High-Speed Rail Communication," IEEE Photonics Journal, vol. 15, no. 5, pp. 1-12, Oct. 2023.

[26] A. Kafizov, A. Elzanaty and M. -S. Alouini, "Probabilistic Constellation Shaping for Enhancing Spectral Efficiency in NOMA VLC Systems," IEEE Transactions on Wireless Communications, vol. 23, no. 8, pp. 9958-9971, Aug. 2024.

[27] C. H. de Souza Lopes, T. P. V. Andrade, L. A. M. Pereira, A. Bogoni, E. Conforti and A. C. Sodré, "Implementation of a Hybrid FiWi System Using FSO, VLC and mm-Waves Toward 6G Applications," IEEE Photonics Technology Letters, vol. 35, no. 24, pp. 1403-1406, 15 Dec.15, 2023.