International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(16s) 2026 pp. 105-127
https://doi.org/10.70917/ijcisim-2026-4562
Article

An Efficient Secure Framework for Hybrid Li-Fi/Wi-Fi Transmission Systems

Charanjit Kaur[1]*, Mithilesh Kumar Dubey[2], Sudha Dubey[3]

[1] Department of Computer Sciences and Engineering, Lovely Professional University, Phagwara, Punjab – 144411, India.
Email: kj169987@gmail.com
[2] School of Computer Science and Engineering, Vellore Institute of Technology, Amaravati, Andhra Pradesh, India.
Email: mithileshkumar.dubey@vitap.ac.in
[3] Department of Sociology, Lovely Professional University, Phagwara, Punjab – 144411, India.
Email: sudha.sikhar25@gmail.com
Corresponding Author: Charanjit Kaur

Abstract: In the era of the Internet of Things (IoT), data on people, objects, and the environment flows are ever-increasing; light fidelity technology is one of the most creative but experimental futuristic networking techniques. To enhance the performance of complex narrowband Internet of Things (NB-IoT) systems, a recently developed hybrid network architecture that consists of Wi-Fi and Light Fidelity (Li-Fi) is investigated in this article. Feasibility studies show that it can significantly improve the availability, dependability, productivity, and safety of systems , while drastically reducing latency and bandwidth costs. The experimental results show that, compared with existing models, the hybrid model can effectively support multiple large data streams and also facilitate quick computing convergence. Simulation results demonstrate that 1) the performance of this scheme also outperforms traditional schemes in terms of throughput, speed, packet drop ratio, jitter and coverage range. The benefits of the proposed algorithm and other widely used algorithms in practical applications are compared in the conclusion, while some further improvements are also suggested.
Keywords: Wireless communication, Li-Fi, visible light communication, RSA, SHA-256 Hash, digital Signature.

1. Introduction

Due to the growing number of Internet of Things applications and smart environments, wireless data traffic has been increasing exponentially, which poses severe challenges for conventional Radio Frequency (RF)-based communication systems. Medium and short range radios such as Wi-Fi, although heavily in use suffers from spectrum congestion, interference, lack of sufficient bandwidth availability; radio based networks including Wi-Fi are under increasing security threats too owing to increased density of devices [1,2]. These constraints become particularly stringent in crowded indoor scenarios, industrial IoT and smart cities as well as mission-critical systems, where reliable and low-latency secure communication is fundamental [3,4].

The so-called Light Fidelity (Li-Fi), which also uses visible light communication (VLC), is considered a potential technology complementing the RF-based wireless systems. Due to its vast underlay spectrum, high data rate, and spatially confined properties, Li-Fi has been considered more bandwidth-efficient and physically secure than Wi-Fi [5–7]. Nevertheless, Li-Fi systems are limited by the line-of-sight dependence, limited coverage area and vulnerability to environmental factors like shadowing and blocking that hinder their direct operation [8, 9]. This has led to the hybrid Wi-Fi/Li-Fi communication architectures attracting attention, with the expectation of being a practical scheme that combines the wide coverage range of Wi-Fi with the advantages of high speed and security of Li-Fi [10–12].

However, despite the ongoing interest in hybrid Wi-Fi/Li-Fi networks, many issues have not been well-discussed. It is challenging to ensure secure data transmission between the RF and optical domains, given their disparate propagation and threat properties [13]. Several existing hybrid frameworks focus on throughput or load balance, and consider security as a secondary rather than a fundamental design concern [14, 15]. In addition, unified solutions that provide confidentiality, integrity, authentication , and non-repudiation over both media are still scarce. There is also performance deterioration in terms of packet loss, jitter, and throughput imbalance, with the increasing node density remaining a problem in the existing hybrid deployments [16, 17]. These challenges underline the necessity for a security-oriented hybrid communication system which will not sacrifice network efficiency. Motivated by these unaddressed needs, the aim of this paper is to propose and assess a secure hybrid Wi-Fi/Li-Fi communication model for the IoT context. In particular, this paper aims to integrate robust cryptographic techniques into a hybrid framework and assess their performance in terms of throughput, packet drop ratio, jitter, speed, and coverage range through simulation.

The main contribution of this work is the design of a secure hybrid Wi-Fi Li-Fi system using the Hybrid Communication Key (HCK) algorithm. The extended model integrates the RSA-based cypher of plaintext images, a self-designed image cypher, SHA-256 hash, and digital Signature into a single framework for end-to-end (confidentiality, integrity, authentication, nonrepudiation) security. Furthermore, a comprehensive analysis of the collected data on both security and performance measurements is used to study the hybrid network's performance, taking into account different node densities. Simulation results show that the proposed scheme achieves higher throughput, lower jitter, and a lower packet drop ratio, as well as better communication stability, than existing hybrid and Wi-Fi-only schemes.

The rest of the paper is structured as follows. The rest of this paper is organised as follows: Section 2 discusses existing work in the area of hybrid Wi-Fi/Li-Fi communication systems and presents the identified gap in the literature review. The Section 3, presents the secure hybrid scheme and the HCK method. The simulation setup and performance evaluation results are described in Section 4. A comparison of the results with related works is presented in Section 5, and concluding remarks are given in Section 6.

2. Literature review

Recently, a growing number of studies focus on hybrid Li-Fi/Wi-Fi networks as they are considered to be a doughty solution against the crowded spectrum and limited mobility and security in RF(Radio Frequency) or OW(Optical wireless) communication systems. Current literature may be roughly classified into hybrid network architectures, mobility and load-balancing techniques, security solutions, and performance enhancing methods.

2.1 Hybrid Li-Fi/Wi-Fi Network Architectures

Besjedica et al. [18] provided a detailed survey on the evolution of hybrid Li-Fi–Wi-Fi networks through systematic review to architectural designs, handover mechanisms and integration issues. The study also found that hybrid deployment improves both spectral efficiency and sum-rate over single-technology base stations. The primary merit is its extensive architectural categorization; however, it is not experimentally verified and does not give a quantitative evaluation of security.

Abdel-Razeq et al. [19] studied the indoor hybrid Wi-Fi/Li-Fi wireless networks based on architecture framework analysis, channel modeling and its state-of-the-art solutions. Their results indicated enhanced coverage continuity and reduced interference with combined optical and RF access. Despite the fact that the proposed work provides substantial theoretical and numerical observations, it lacks in its integration mechanism for mutual authentication and encryption for within hybrid cooperative overlay.

Ghali et al. [20] introduced an access-point allocation algorithm for dynamic heterogenous Li-Fi/Wi-Fi networks,in order to enhance QoS and energy effectiveness. The simulation results indicated the good throughput performance with low consumed energy for different user densities. However, it is not designed to deal with security or data integrity issues.

In a latter study, Ghali et al. [21] experimentally estimated the advantages of selective hybrid Wi-Fi/Li-Fi WLAN options for indoor environments and observed better throughput stability and power consumption efficient compared to Wi-Fi ones. Their work offers indoor performance verification, but security issues are not included in the evaluation. Li-Fi and Wi-Fi technologies are compared in Table 1, underlining their complementarity regarding spectrum exploitation, performance/coverage, mobility and security. The cross comparison drives the draft of hybrid Li-Fi/Wi-Fi architectures to effectively utilize both high-capacity optical links and stable RF connections.

Table 1. Updated comparison of Li-Fi and Wi-Fi technologies

Parameter	Li-Fi	Wi-Fi

Communication medium	Visible light spectrum (VLC)	Radio-frequency (RF) spectrum
Operating frequency	~400–800 THz	2.4 GHz, 5 GHz, 6 GHz
Available bandwidth	Very high and largely unlicensed	Limited and highly congested
Typical data rate	Very high (Gbps achievable in indoor LOS conditions)	Moderate to high (hundreds of Mbps to a few Gbps)
Interference	Immune to RF interference; sensitive to light blockage	Susceptible to RF interference in dense deployments
Line-of-sight (LOS) requirement	Required or partially required	Not required
Mobility support	Limited due to blockage and coverage constraints	Strong mobility support
Coverage range	Short range (typically room-level)	Medium to long range (tens of meters indoors)
Penetration through obstacles	Cannot penetrate opaque objects	Can penetrate walls and obstacles
Security characteristics	High spatial security due to confined light propagation	Vulnerable to eavesdropping and RF attacks
Energy efficiency	High when integrated with LED lighting	Moderate; depends on AP (Access Points) density
Deployment complexity	Requires lighting infrastructure alignment	Mature and widely deployed
Scalability in dense environments	High capacity for localized access	Performance degrades with congestion
Standardization	IEEE 802.15.7 and emerging VLC standards	IEEE 802.11 (a/b/g/n/ac/ax/be)
Role in hybrid networks	High-speed, secure local access	Broad coverage, mobility, and fallback connectivity

2.2 Mobility, Handover, and Load-Balancing Techniques

Wang et al. [22] represented a rate-stabilized and load-balanced handover management scheme in subway hybrid Li-Fi/Wi-Fi networks. It was concluded that the handover latency could be decreased and service continuity in high mobility environment could be increased. The key contribution of this work is that it provides security for mobility without giving an account of handover.

Farrag et al. [23] proposed a conditional most-correlated distribution independent-based load-balancing algorithm for hybrid Li-Fi/Wi Gig networks. The new algorithm performed the throughput enhancement and packet loss prevention with very low computational load. But the scheme trusts the network entities and does not consider adversary situations.

Chatterjee et al. [24] designed a mobility-adaptive blockage-handling scheme for multi-user, multi-cell hybrid Li-Fi/Wi-Fi networks based on freeform diversity receivers. The work showed that link reliability could be improved in the presence of user mobility and blockage. While significant physical-layer security gains were made, no attention was paid to higher-layer security mechanisms.

Su et al. [25] proposed an effective dynamic client association algorithm in Wi-Fi mesh networks based on EasyMesh. This augmented the throughput and load balancing, however it is modelled for RF alone and does not feature optical or hybrid Li-fi integration.

2.3 Security Mechanisms in Li-Fi and Wireless Networks

Msallam and Samet [26] studied security in Lifi, focusing on encryption techniques also investigated the physical layer aspects of secure optical communication. The survey pointed out the inherent space secure feature of Li-Fi but failed to cover hybrid Li-Fi/Wi-Fi system.

Liu et al. [27] developed an optical fingerprint-based authentication protocol for Li-Fi networks, and a high performance in terms of the authentication accuracy under different channel conditions was achieved. The method improves the device level security, but it is restricted to the stand alone Li-Fi systems.

Consideration to quantum key distribution in Li-Fi systems using FSO (free-space optics) and polarization modulation is also depicted by Ranjan and Sharma [28]. Their model showed improved privacy but is highly complex to implement and does not consider hybrid network coverage.

Dimmitt et al. [29] analysed the security features of powerline communication and Wi-Fi technologies for IoT application. The work exposed weaknesses in RF-based setups and did not consider optical or a combination of the two communication models.

Zabeeulla et al. [36] presented a hybrid network security modelling scheme for vehicular ad-hoc networks with an enhanced resistance to frequently occurring attacks. The framework yields useful results designed specifically for hybrid security modeling; however, it is only applicable to RF-based scenarios and cannot be used with Li-Fi or optical channels.

2.4 Performance Optimization and Emerging Approaches

Hybrid optical–RF distributed networks were optimized using advanced modulation techniques by Imam Sabitu and Malekmohammadi [30] to attain high data rate with bandwidth efficiency. The research concentrates solely on backhaul throughput and not end-user security.

Finally, Sinduja and Charles [31] combined deep learning with optimization to achieve load balancing in the clouds and demonstrated improved performance adaptability. However, the model was not verified in Li-Fi/Wi-Fi hybrid networks.

Iliyas et al. [32] introduced a trust-based symmetric game-theoretic model for physical-layer security in Wi-Fi transmission. The method enhanced the infallibility of routing, however a little restrictively to optical and hybrid communication.

Wang et al. [33] summarized potential solutions for advanced wireless connectivity and pointed out that inorder to help future networks forward, Li-Fi and hybrid architectures are the key enablers. The analysis is strategic but lacks actual performance assessment.

Chauhan and Jain [34] also talked about Li-Fi developments for future- generation wireless technology with focus on compatibility and safety. It is conceptual in the sense that there is no hybrid comparison.

Mohan et al. [35] introduce a hybrid optimization approach for congestion-free multipath routing and load balancing in IoT networks. It is successful in congestion control but does not address Li-Fi/Wi-Fi Hybrid systems explicitly.

Miranti et al. [37] studied mobility load balancin g algorithms for downlink LTE networks, and reached at enhanced user capacity. The work is related to dense network environment and it does not cover optical or hybrid communication.

Subhan et al. [38] provided a parametric study on the line-of-sight channel characteristics of Li-Fi networks, illustrating how distance and alignment affect data rates. Yet heterogenous integration was not taken into account with respect to Wi-Fi and security aspects.

The recent methods and findings of the studies (2023–2025) concerning hybrid Li-Fi/Wi-Fi, and other related wireless systems may be compared through Table 2 based on various experimental works in terms of constructed models as well as their benefits and drawbacks. The contrast shows that the majority of works concentrate on performance improvement or security reinforcement separately, which in return suggests the requirement for combined hybrid frameworks to concurrently take a target at security and network efficiency.

Table 2. Comparative analysis of recent hybrid Li-Fi/Wi-Fi studies highlighting method, results, advantages, and limitations

Method / Approach	Metrics Evaluated	Key Results	Advantages	Limitations	Year	Ref.
Survey of hybrid Li-Fi–Wi-Fi architectures	Throughput, spectral efficiency, mobility	Hybrid systems outperform standalone networks	Comprehensive taxonomy and trends	No experimental or security validation	2023	[18]
Architectural and channel modeling for indoor hybrids	Coverage, interference	Improved coverage continuity	Strong theoretical foundation	No authentication or encryption	2024	[19]
AP assignment strategy for QoS and energy efficiency	Throughput, energy efficiency	Stable throughput, reduced energy use	QoS-aware optimization	Security not addressed	2025	[20]
Experimental evaluation of indoor hybrid WLANs	Throughput, power efficiency	Higher performance than Wi-Fi-only	Realistic deployment analysis	No security evaluation	2025	[21]
Load-balanced handover management	Latency, handover cost	Reduced delay under mobility	Robust mobility support	Security during handover ignored	2023	[22]
Distribution-based load balancing	Packet loss, throughput	Improved reliability	Low computational complexity	Assumes trusted nodes	2023	[23]
Mobility-aware blockage management	Link reliability	Reduced blockage impact	Strong physical-layer design	Higher-layer security absent	2024	[24]
Dynamic client association (Wi-Fi mesh)	Throughput	Improved load distribution	Practical deployment	Optical links excluded	2025	[25]
Review of Li-Fi security techniques	Confidentiality	Enhanced spatial security	Security-focused analysis	No hybrid evaluation	2024	[26]
Optical fingerprint authentication for Li-Fi	Authentication accuracy	High authentication precision	Strong device security	Standalone Li-Fi only	2025	[27]

Quantum key distribution modeling for Li-Fi	Confidentiality	Improved encryption strength	Advanced security	High implementation complexity	2025	[28]
PLC vs Wi-Fi security comparison for IoT	Vulnerability analysis	Identified RF weaknesses	Comparative insight	No optical integration	2025	[29]
Optical–RF modulation optimization	Bandwidth efficiency	High data-rate support	Backhaul optimization	End-user security ignored	2025	[30]
Hybrid DL-based load balancing	Throughput, delay	Adaptive performance gains	Intelligent optimization	Not validated for Li-Fi/Wi-Fi	2025	[31]
Trust-based game-theoretic security model	Routing reliability	Improved trust handling	Security-centric framework	Optical channels excluded	2025	[32]
Review of advanced wireless connectivity	Scalability, coverage	Identified Li-Fi as future enabler	Strategic insights	No quantitative evaluation	2025	[33]
Conceptual study on Li-Fi integration	Compatibility	Highlighted integration potential	Forward-looking perspective	No benchmarking	2025	[34]
Hybrid optimization for IoT routing	Congestion, latency	Reduced congestion	Dense IoT applicability	Not Li-Fi/Wi-Fi specific	2025	[35]
Hybrid network security modeling (VANET)	Attack resistance	Improved security resilience	Structured security framework	RF-only environment	2023	[36]
Mobility load balancing for LTE	User capacity	Increased capacity	Dense-network relevance	Not optical–RF hybrid	2025	[37]
LOS channel evaluation for Li-Fi	Data rate vs distance	Performance degradation quantified	Accurate channel modeling	No Wi-Fi integration or security	2024	[38]

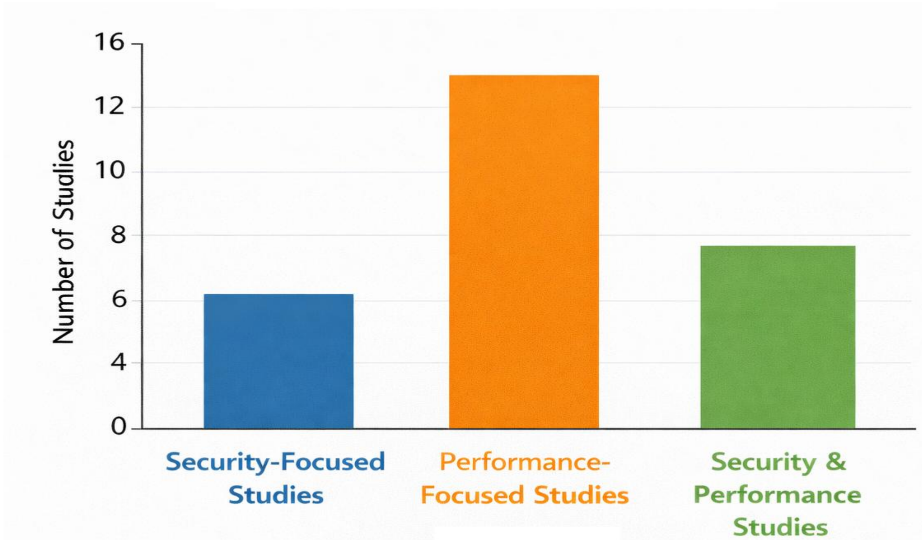


Figure 1. Distribution of existing hybrid Li-Fi/Wi-Fi studies based on security integration and performance evaluation focus.

Figure 1 depicts the most recent hybrid Li-Fi/Wi-Fi research distribution with respect to the main research concentration. The analysis reveals that the majority of studies focus on performance optimisation, less to security and only a few ones concern both security and performance in combination; which reflects clearly the gap in research.

2.5 Review Analysis and Research Gap

The literature survey indicates that hybrid Li-Fi/Wi-Fi networks yield improvement in throughput, coverage continuity, energy efficiency an mobility and blockage resilience over standalone systems. Performance-based research covers load balancing, handover optimization and channel modeling; while security-centric works improve the authentication and data confidentiality in isolated Li-Fi/RF networks.

But there is still a major unsolved problem: the majority of research treat performance optimization and security improvement as independent goals. There are limited number of integrated hybrid models in which security (confidentiality, integrity and authentication) and network performance metrics -throughput, packet drop ratio, jitter-speed and range are considered simultaneously. In addition, most existing works are based on symbolic or partial security model, and in hybrid deployment environment their evaluations are not comprehensive. Such constraints underscore the necessity for an integrated and secure hybrid Li-Fi/Wi-Fi framework that can jointly meet both performance and security needs.

3. Method

Research strategies are discussed regarding planned architecture.

a. Technique Used

The following are the important techniques used in the proposed methodology:

i. Encryption Techniques

Data encryption methods prioritise protecting certain data types. Text information is encrypted using RSA, a well-known public-key cryptosystem. In contrast, images go through a customised encryption process.

- RSA

The "Ronald Rivest, Adi Shamir, and Leonard Adleman" algorithm (developed in 1978) has been the standard ever since for public key encryption. RSA is the basis of many other encryption methodologies [39]. A commonly known public key cryptosystem is the RSA. It was the first scheme to be certified (in France) for both encryption and signing, and one of the most important early developments in public key cryptography [40]. In Figure 2, RSA is illustrated. It is the process of Encryption, Decryption and Key Generation.

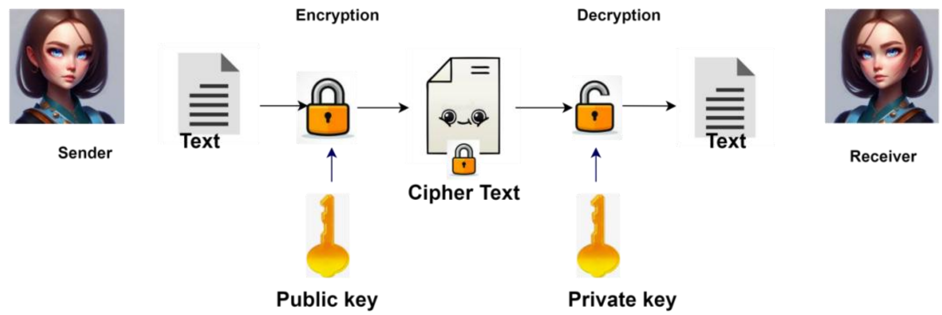


Figure 2. Proposed Methodology.

- Custom Encryption

"custom encryption for image data" refers to developing and deploying an original encryption technique or method to protect digital photographs(28). Rather than relying on pre-existing encryption methods like AES or RSA, this strategy requires a personalised method of picture encryption and decoding [41].

ii. SHA-256 Hash Algorithm

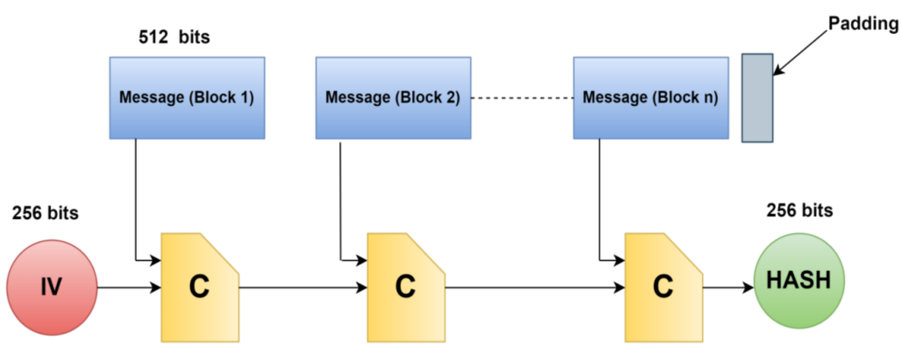


Figure 3. SHA-256 Hashing Algorithm.

SHA-256: The Secure Hash Algorithm 256-bit (SHA-256) belongs to the same family of cryptographic hash functions as SHA1, known as SHA2 [42]. It processes inputs of all lengths and returns a fixed-size (256-bit) hash. The 256-bit (32-byte) hash value generated by the SHA-256 algorithm is used [43].The original input cannot be derived by the hash result because SHA-256 is meant to be a one-way function. It is also collision-resistant, so that well-hashed different inputs will very unlikely to encounter the same resulting hash output. Applications include digital signatures, data integrity, and blockchain technology such as in Bitcoin. Figure 3 illustrates the SHS-256 hash function.

iii. Digital Signature

The established technology of cryptography for validating electronic documents and correspondence is the digital signature method. The sender's unique digital Signature can be verified by anyone who has the sender's public key, but this Signature is produced using their private key. Added to online chats and transactions , safe authentication can be ensured, as well as the integrity of data, with digital signatures that verify the file hasn't been altered since its creation. The equation (y r.r smod p) mod q = (gm mod p) mod q is used to write DSA signature verification; g(r) m y mod pq where (p;q); gm mo dp, m is the message and public key. The Signature is valid if the two sides of the equation are equal. The digital signature algorithm is presented in Figure 4.

b. Proposed Methodology

To exchange data over Li-Fi and Wi-Fi networks, the proposed method integrates essential security requirements with performance indicators, including throughput, jitter, and Packet Drop Ratio (PDR), in a secure hybrid architecture. This architecture has all the basic security concepts confidentiality, integrity, authentication and non repudiation integrated as a whole.

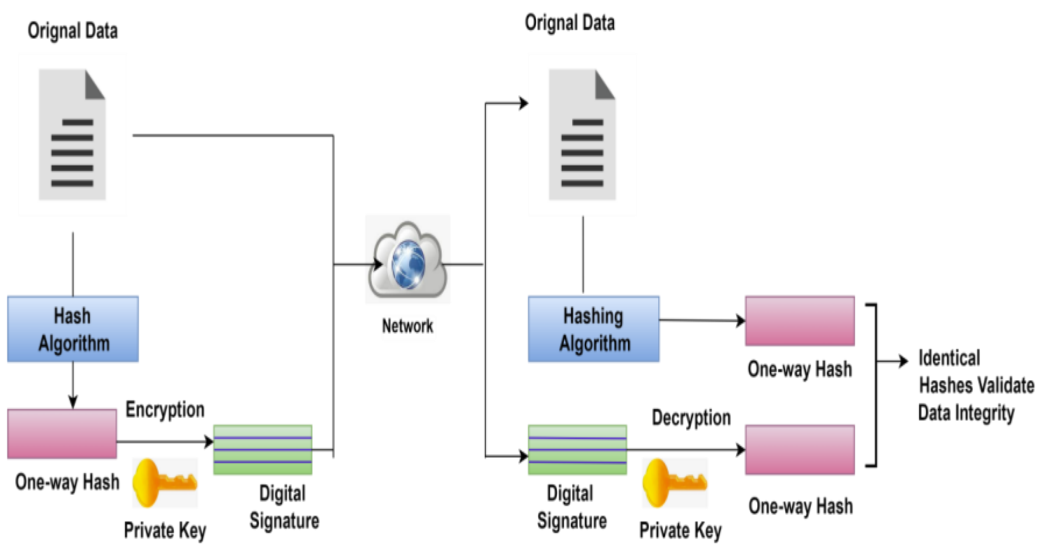


Figure 4. Digital Signature Algorithm.

Security Framework and Hybrid Communication Key (HCK) Implementation

The same security context can be extended over H-VLC/Wi-Fi communication due to the use of a common security architecture for such hybrid communication, which is based on the Hybrid Communication Key (HCK) in our proposed system. In this paper, HCK is not simply a cryptographic key, but an overall security system that encompasses encryption, hash functions, authentication, and non-repudiation across the optical network and RF environment. The transmitted data are first divided according to modality as either text or image. Text-based information is encrypted with the public key of recipient by RSA to guarantee privacy, and image data are also protected by a Custom Secure Image Transmission Algorithm (CSITA) that can realize lightweight but effective encryption for real-time exchange. After the encryption, a SHA-256 hash of the encrypted payload is created to protect against data tampering.

To secure authentication and non-repudiation, a sender computes a digital signature by signing the hash value with their own private key. This digital Signature ties the sender to exact data sent and thus prevents any kind of denial. At the receiver end, the digital Signature is verified with the public key and the hash is recomputed to ensure that it matches the transmitted checksum for data integrity.

Secured data are next transmitted over the hybrid Li-Fi/Wi-Fi system, with the Li- Fi mainly for short and high-data-rate links, while the Wi- Fi offers ubiquitous coverage and mobility support. The built-in HCK protocol ensures that the same security requirements—confidentiality, integrity, authentication, and non-repudiation—apply regardless of the underlying physical network.

This integrated security process provides transparent protection for diverse data types while maintaining network performance, rather than the traditional division between security and performance in current hybrid communication systems. Digital signatures enable identity authentication and verification of the integrity of online transactions by allowing detection of any modification to the data after transmission. Network graphs have been produced using the NetworkX library , where Wi-Fi nodes and super-nodes for Li-Fi are generated based on their features (type, bandwidth, and range). The probabilities of connections between nodes are set up as a model to emulate social interactions both in real life and at network scale.

The security layer combines password-based device authentication, SHA-256 hash model for integrity checks, digital Signatures for non-repudiation, RSA encryption algorithm for text data protection, and proprietary image encryption. Li-Fi nodes are shown as blue dots and Wi-Fi nodes in green for clear visualisation in a network diagram using a spring layout. Lastly, at the node level and lastly the data aggregated and store performance and security metrics for later post-processing and when constructing the dataset. Overall, the proposed method is a well-planned and effective means to slow down data transfer in Wi-Fi/Li-Fi networks.

A planned workflow of system development and security process es is illustrated in Figure 5. Taking everything into account, Xirrus Wi-Fi Inspector comes packed with straightforward and intuitive options for monitoring data transfers between Li-Fi and Wi-Fi networks in a secure working environment. A network graph is first constructed with the help of the NetworkX library or a similar tool. The nodes of Li-Fi and Wi-Fi are determined, connected together, and a probability link is assigned between them in this graph. The process is secured, to maintain confidentiality, integrity and non-repudiation via digital signatures, password-based authentication and SHA-256 hashing.

Network performance testing under these security provisions is also part of the process to verify reliable data transmission. A spring layout is applied for visualisation, and nodes are naturally colour-coded using blue for Wi-Fi, green for Li-Fi, and orange for hybrid nodes. Finally, to extensively evaluate network performance and security capabilities, datasets are generated that consider speed, range, packet drop ratio (PDR), jitter, and throughput.

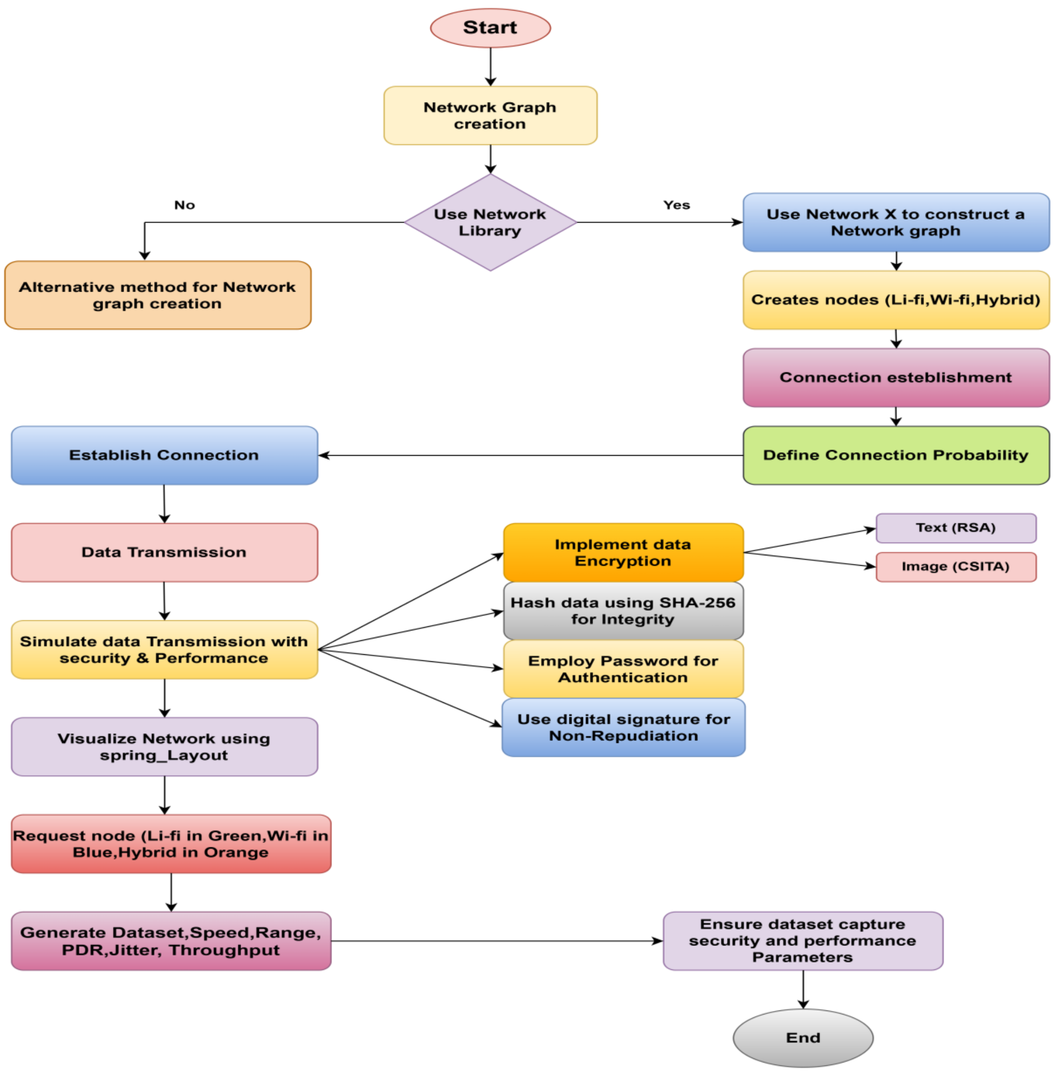


Figure 5. Proposed Methodology

c. *Proposed Algorithm*

This comprehensive algorithm uses simulation-based data transfer to assess the performance and security of wireless and hybrid networks.

Table 3. Algorithms

Algorithm: Hybrid Communication Key (HCK)
Step 1: Network Graph Creation Using NetworkX Library
Initialise an Empty Graph G
For each Li-Fi device:
Create a Node with Attributes (device type, speed, range)
Add the Node to the Graph G
For each Wi-Fi device:
Create a Node with Attributes (device type, speed, range)
Add the Node to the Graph G
Step 2: Connection Establishment
Define a connection *probability*
For Each Node in G:
For Each Other Node in G:
If the Nodes are of Different Types (Li-Fi and Wi-Fi):
Generate a Random Number Between 0 and 1 (connection attempts)
If communication attempt<=connection Probability
Create a Connection Between the Nodes
Step 3: Data Transmission
For Each Data Transmission:
a. If the Data Type is Text:
Encrypt the Data Using the RSA Algorithm
If the Data Type is Image:
Use Custom Encryption Method
b. Hash the Data Using SHA-256 for Integrity Checks
c. Use Passwords for Device Authentication
d. Apply Digital Signatures for Non-Repudiation
Step 4: Network Visualization
● Visualise the Network Using a Spring Layout
● Represent Li-Fi Nodes in Blue and Wi-Fi Nodes in Green
Step 5: Dataset Generation
Initialize an Empty Dataset
For each node in G:
● Generate Attributes (speed, range, PDR, jitter, throughput)
Add the Attributes to the Dataset

● Ensure the Dataset Captures Security and Performance Parameters

Algorithm: Custom Image Encryption
Step 1: Prepare the image If necessary, resize the image and convert it to grayscale. *Step 2: Create a Key* Use a chaotic map or pseudo-random generator to create a key matrix that is the same size as the image. *Step 3: Pixel Scrambling* Use the key to shuffle the pixel placements (both row-wise and column-wise). *Step 4: Value Encryption* Each pixel should be encrypted using bitwise XOR: Key $\oplus$ Pixel = Encrypted *Step 5:* Add Hash. Create a SHA-256 hash to verify the integrity of the image and include it in the image metadata. *Step 6: Save and Send* Send the encrypted matrix safely after converting it back to an image.

The simulation scenario aims to analyse the performance and security characteristics of the proposed hybrid Li-Fi/Wi-Fi network with diverse wireless network conditions. The main simulation parameters for setting up the network are listed in Table 4. Main simulation parameters for setting up the hybrid Li-Fi/Wi-Fi connected network, such as node density, simulation time, and connection probability, as well as properties of the network connectivity. These settings characterise the experimental conditions by which our approach is assessed.

Table 4: Simulation Parameters

Number of Nodes	*Simulation Time*	*Connections Probability*	*Average Node degree*	*Possible Connections*	*Actuel Connections*
10	0.41 Sec	80%	22.47	435	337

25	1.09 Sec	90.0%	59.63	2775	2236
50	1.10 Sec	74.89%	111.59	11175	8369
100	2.85 Sec	80.03%	269.20	44850	40380

For performance measurements and comparison, datasets are produced during the simulation by collecting node-level statistics for various data types. The properties of the generated datasets are reported in Table 5. Table 4 shows the details of simulation datasets, such as data type, number of records and dataset size and nodes performance (speed, jitter, range, packet drop ratio, etc.), which are used for processing. These datasets are applied to performance evaluation and benchmarking of the hybrid communication paradigm proposed.

Table 5. Dataset Details

Input Dataset Type	*No.of Records*	*Size*	*Node Parameters*
Text	61	1.2 Gb	Speed, Jitter, Range, PDR, Throughput
Image	221	75Mb	Speed, Jitter, Range, PDR, Throughput

The standard for the hybrid network connecting Wi-Fi and Li-Fi Performance

Performance Metric Definitions

Several typical network performance metrics are used in order to quantitatively assess the performance of the proposed secure hybrid Li-Fi/Wi-Fi architecture. Throughput refers to the average effective data delivery rate of the communication channel and is measured in bps (bits per second). It is calculated as the number of correctly received bits in the sum over the total simulation time. Packet Drop Ratio (PDR) is the fraction of lost data packets due to data transmission errors and expressed as a ratio of dropped packets to total number of transmitted packets. A smaller packet drop ratio represents higher transmission reliability.

Jitter is a variant of packet inter-arrival time and calculates as the mean deviation between two consecutive packet arrival times. Smaller jitter values prove a steadier and more predictable communication, what is crucial in *real time applications. The End-to-End Delay is determined as the average duration for a packet transferred from sender to receiver considering processing, transmission, and propagation trends. The rate refers to the effective data transmission speed, while distance represents the maximum range at which a signal can be reliably received at that speed. Together, these metrics provide a valuable balance between end-to-end security overhead and network performance in the face of different node densities and traffic loads. The effectiveness of a Wi-Fi and Li-Fi hybrid network can be assessed using several factors, including coverage. Numerous studies have examined the packet drop ratio, throughput (Mbps), jitter, range, and speed. These standards fall into the category of Figure 6.

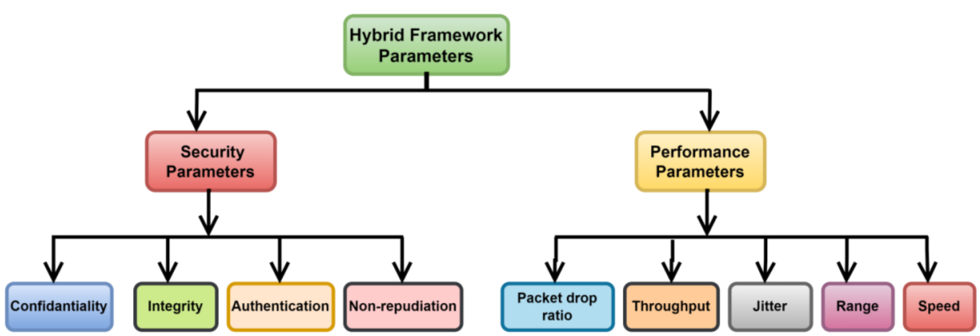


Figure 6. Performance Standards for hybrid Wi-Fi/Li-Fi networks.

4. Security Parameters

Fundamentals of information security include security standards like non-repudiation, confidentiality, integrity, and authentication:

A. Confidentiality:

Only those with permission can access information thanks to confidentiality. Data is shielded from unwanted access, exposure, or interception during transmission or storage by methods like encryption.

B. Integrity:

Integrity ensures that information is accurate, consistent, and unaltered during processing, storage, and transmission. Techniques like hash functions, checksums, and digital signatures are employed to confirm the accuracy and legitimacy of the data.

C. Authentication:

Verifying the identity of users, devices, or systems is known as authentication. It guarantees that organizations making access requests are authentic. Cryptographic techniques like digital certificates, biometric identifiers like fingerprints, and passwords are common approaches.

D. Non-repudiation:

People cannot deny their involvement in a communication or transaction or their actions. It guarantees that no one can contest the source, legitimacy, or receipt of data that has been transmitted. Non-repudiation is frequently enforced using audit logs and digital signatures [44]. These specifications are necessary to create safe systems and protect private data from abuse, tampering, and illegal access.

Table 6. Simulation Assumption

1.	*Network Topology*	This topology is static and has a set number of nodes, such as 30:10Li-fi,10 Wi-fi,10 Hybrid. For the worst-case stress test, all nodes have full mesh communication.
2.	*Data Type Simulate*	Three Data types: text, image, and Video, each having progressively higher transmission requirements.
3.	*Performance Metrics*	Speed, Jitter, Range, PDR, and Throughput were among the key metrics that the simulation focused on.
4.	*Security Assumption*	RSA is used for text encryption 2D chaotic Map or a custom secure image transmission algorithm (CSITA) is used to encrypt the image. A Hybrid AES+RSA encryption technique is used to encrypt video.
5.	*Simulation of DDoS Attack*	Flooding requests are sent to one randomly chosen node in order to examine network durability and Stress behaviour.
6.	*Environment*	Every Simulation is executed in a Python environment (such as Google Colab) without considering physical barriers or real-world signal interference.

5. Limitations of the simulation

While the simulated hybrid Li-Fi/Wi-Fi offers a useful insight, there are still many limitations. In addition, it fails to consider important environmental effects on the performance of Li-Fi channels (multipath and reflected surfaces) and lacks real-time modelling of the channel. A detailed security evaluation is not conducted, as encryption operations are modeled symbolically rather than implemented at the bit-by-bit level. One weakness of the model is that it does not have mobility and handover effect which are important in real hybrid networks for stationary nodes. Additionally, bandwidth is abstracted rather than modeled using real traffic scenarios, and the number of nodes involved in the computation is fixed and relatively small. Furthermore, hardware-level characteristics, such as processing delay and energy consumption, are not considered, which limits the generality of the simulation.

6. Performance Parameters

Throughput in a Network

Nevertheless, it has been proven that a simple RF-integration can be used to enhance the throughput performance of stand-alone Li-Fi systems with higher per user data rates and network efficiency. By allocating LAFs to semi-static users and WAF to mobile users, the hybrid architecture shows that the needs of users can efficiently be fulfilled. Compared to a Li-Fi-only network, an RF–Li-Fi hybrid network can significantly alleviate blockages and enhance overall system performance [45].

A. Speed: . Li-Fi is incredibly fast; in a typical context, it can reach speeds of up to 100 Gbps, while in a lab setting, it can reach speeds of up to 1 Gbps. Wi-Fi is 100 times slower than Li-Fi.

$$Speed = \frac{Data\ Size}{Transfer\ Time} \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Range:. A hybrid network that combines the advantages of Wi-Fi for more extensive and flexible connectivity, and Li-Fi for fast, localised communication, can offer optimal coverage and performance.

Packet Drop Ratio (PDR): The packet drop ratio, or PDR, is the proportion of dropped packets to all packets transmitted.

.

$$PDR = (\frac{pr}{pg})\times 100 \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Pr (number of dropped packets) and pg (total number of packets transmitted).D_{i+1} i

B. Jitter: Jitter is usually measured in milliseconds (ms). Network jitter can be quantified by determining the typical time interval between each packet sequence.

$$Jitter = \frac{1}{N-1}\sum_{i=1}^{N-1} |D_{i+1} - D_i| \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(3)$$

C. Average Throughput: The LiFi and WiFi APs' average throughput measurements are influenced by SNR, packet size, and physical layer rate. The following generic formula is then used to estimate the average throughput:

$$T_{Li\text{-}fi/Wi\text{-}fi} = (\frac{R}{t^2 - t^1})\times(\frac{8}{1000}) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots..(4)$$

Where t1 denotes the simulation start time, t2 is the simulation stop time, and R is the total number of packets the network has ever received.

Table 7. Simulation Basic

Language	*Library Versions*	*Computational Requirements*
Python 3.6	NetworkX (min 2.5)	CPU (1core)
	Matplotlib (min 3.3)	RAM (<=512 Mb)
	CSV (Stdlib)	Storage Min (CSV file<1Mb)
	Random (Stdlib)	

7. Results

Table 8. Simulation Parameters.

Simulation Parameters	Value
Area needed for a transmission room	10m,10m,5m
Quantity of LED lights	30
The LED lamps' height	3m

The device's height	1m
Power from LED emissions	55mW
View angle at the receiving end	750
Photodiode (l*b)	Approx1(cm*cm)

A transmission room constructed at a 10 m × 10 m × 5 m with the LED lights installed on walls at height of 3m and a receiver device placed at ground (at a high of H =1m) is introduced in simulation parameters listed in Table 8. The receiver is constructed with a field of view of 75° and each LED has an optical power emission of 55 mW. Active area of the photodiode that collects signals is $\sim 1\ cm^2$. These parameters provide controlled setting for system performance evaluation and easy evaluation of the communication ability and lighting condition.

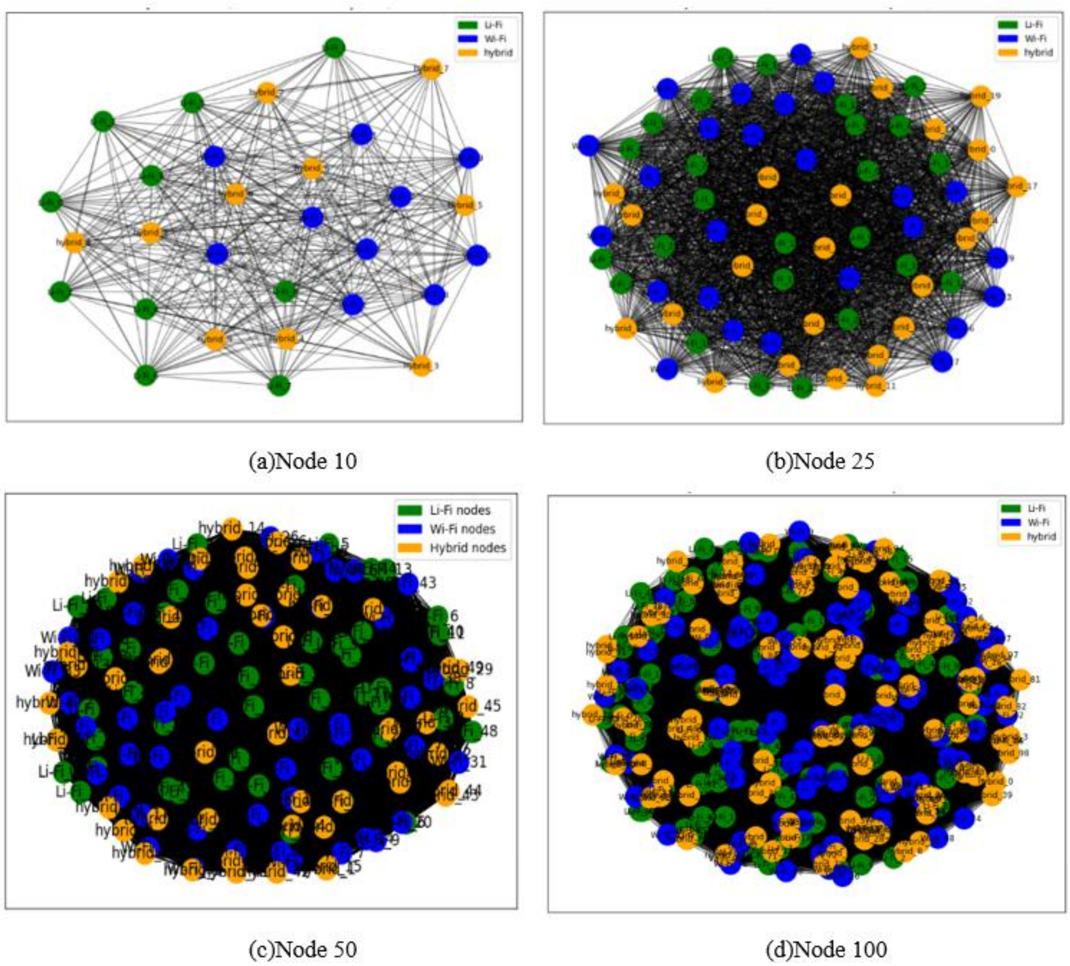
Simulation results based on the HCK algorithm.

The results of these simulations can be leveraged to guide the development and further enhancement of integrated Wi-Fi and Li-Fi systems, as well as to inform strategic decisions regarding potential use cases and their deployment . Specific parameters and performance measures can be assigned different weights in accordance with the specific objectives of the simulation. Many private nodes are shown in the simulation; blue refers to Li-Fi device nodes and green to Wi-Fi device nodes.

Node	Device_Type	Speed (Mbps)	Range (m)	Packet Drop Ratio	Jitter	Throughput (Mbps)
Wi-Fi_0	Wi-Fi	198.8557583	81.2890938	0.072498713	8.985806562	801.3458237
Wi-Fi_1	Wi-Fi	85.18086651	24.5103752	0.050632758	8.074922174	669.9410597
Wi-Fi_2	Wi-Fi	45.15645763	18.4273454	0.013202135	5.76064907	954.310664
Wi-Fi_3	Wi-Fi	85.17778593	84.4517386	0.090312551	1.111325825	299.9915173
Wi-Fi_4	Wi-Fi	173.9702394	49.9862918	0.075966558	4.961940838	688.9146639
Wi-Fi_5	Wi-Fi	862.9608998	33.1008107	0.030383335	8.410817531	985.0886813
Wi-Fi_6	Wi-Fi	508.6816949	25.1767052	0.032039413	4.77946181	100.6620701
Wi-Fi_7	Wi-Fi	268.157764	41.4801734	0.050216432	6.878909591	187.4781385
Wi-Fi_8	Wi-Fi	623.0436043	38.603723	0.023036455	8.801069093	650.17012
Wi-Fi_9	Wi-Fi	397.1725697	34.7269444	0.053199658	9.737831765	972.7509862
Wi-Fi_0 Li-Fi_0	hybrid	467.3404637	95.5105246	0.034520678	1.583809763	401.6338255
Wi-Fi_1 Li-Fi_1	hybrid	847.591416	85.6993373	0.093748481	1.073304716	619.9687283
Wi-Fi_2 Li-Fi_2	hybrid	207.3200376	97.9265111	0.065649079	7.194422128	639.1167447
Wi-Fi_3 Li-Fi_3	hybrid	330.122108	54.1031551	0.010439443	2.19717357	718.1807656
Wi-Fi_4 Li-Fi_4	hybrid	415.4670987	63.5686256	0.023630742	8.419426347	205.3323535
Wi-Fi_5 Li-Fi_5	hybrid	924.9856417	26.6453127	0.053889326	4.053444218	2.166999642
Wi-Fi_6 Li-Fi_6	hybrid	16.58682745	15.4813194	0.034866339	8.473343855	259.1152072
Wi-Fi_7 Li-Fi_7	hybrid	277.0644765	75.9171462	0.026028138	1.897140708	426.8821584
Wi-Fi_8 Li-Fi_8	hybrid	750.8876199	83.519745	0.046093455	2.76480453	613.4338855
Wi-Fi_9 Li-Fi_9	hybrid	142.0314583	37.3312917	0.020917858	6.348540869	897.636605

Figure 7. CSV File Report

The simulation here is modelling the performance of a reference heterogeneous wireless network with Wi-Fi, Li-Fi, and hybrid nodes, as the number of nodes increases. The network performs very well in terms of jitter, Packet Delivery Ratio (PDR) close to 100% and throughput close to the maximum supported speed in an event-free scenario, being better if only few nodes are involved (Figure a). In the case of 25 (b) and 50 (c) nodes, performance degrades as the network becomes larger due to interferences that reduce per-node throughput/PDR while increase jitter. The simulation highlights hybrid devices' advantages, which opportunistically switch from the Li-Fi to Wi-Fi and vice versa in order to avoid traffic jams, at the highest densities – 100 (d). When compared to a single-technology network, it is this adaptive nature of the network that will enable it to control jitter more efficiently, maintain throughput more stably, and reduce PDR degradation.



(a)Node 10 (b)Node 25

(c)Node 50 (d)Node 100

Figure 8. Simulation Graph (a,b,c,d)

Performance Metrics

The hybrid architecture performance is analyzed via various metrics, in security and efficiency aspects. The security metrics include, without limitation, integrity, non-repudiability and authenticity and confidentiality. Performance parameters include speed, packet drop ratio, jitter, throughput, and probability of range coverage. This section presents the relevant performance metrics and associated studies employed for the evaluation of hybrid solutions.

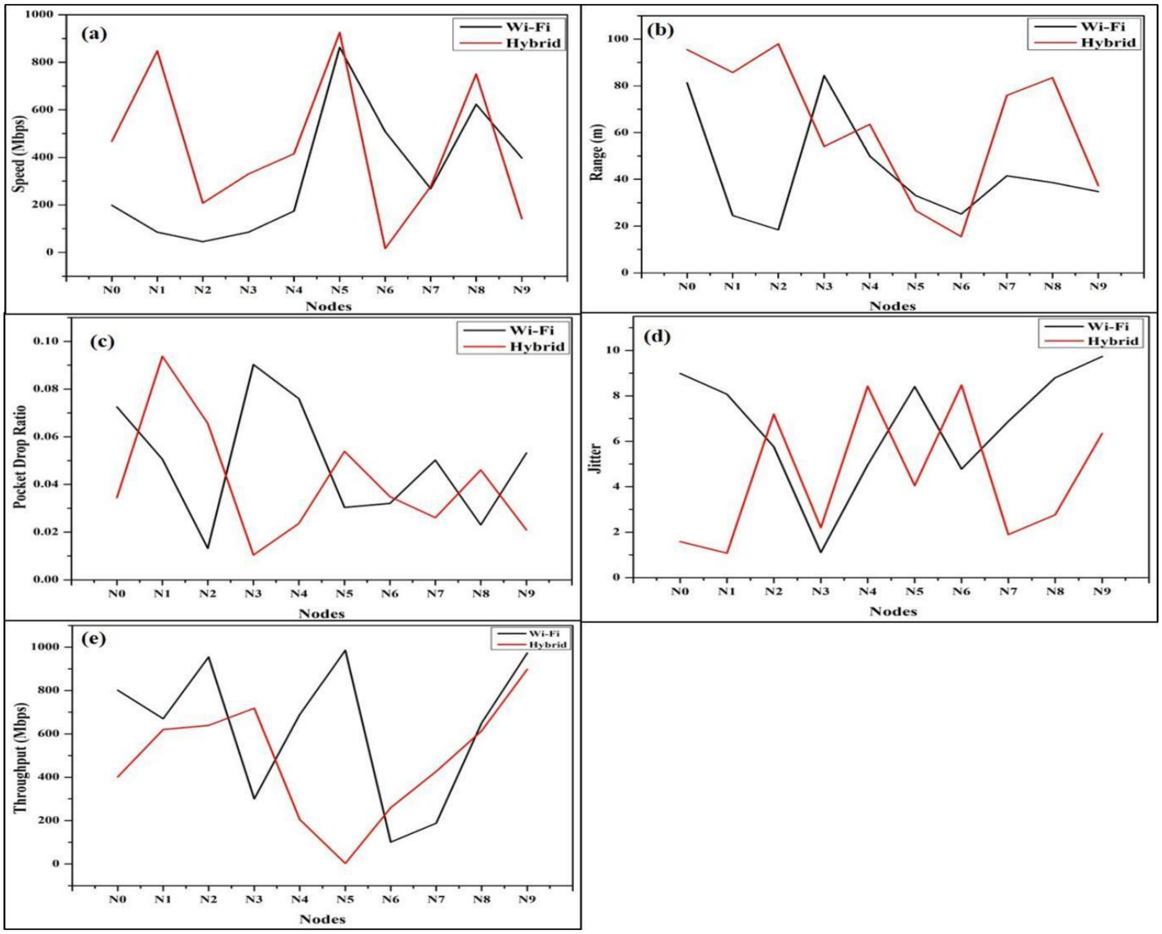


Figure 9. (a) Speed, (b) Range, (c) Packet Drop Ratio, (d) Jitter, and (e) Throughput of ten nodes based on the HCK algorithm.

In this set of graphs, ten nodes or measurement points are used to compare the performance of a hybrid network (represented by the red line) and a conventional Wi-Fi network (represented by the black line). In terms of stability and dependability, the hybrid system routinely performs better than the Wi-Fi-only system. A more stable connection is indicated by the hybrid network's notable significantly lower Packet Drop Ratio (c) and significantly lower Jitter (d). The hybrid network typically avoids the steep performance drops seen in the Wi-Fi network, leading to more constant data rates, even though the raw speed (a) and throughput (e) vary for both systems. Additionally, the hybrid network seems to maintain a superior effective Range (b) in the majority of scenarios.

9. Discussion

The output of the system (Wi-Fi and Li-Fi) with a few nodes (N0 - N9) is shown in Figure 7, which is fascinating for hybrid network design implement ation in the field. In general, the measured performance (speed, range packet drop ratio and jitter) metrics show how the hybrid scheme also provides significant improvement in some specific cases. For higher node-counts the hybrid is fastest, although depending on the speed many of them get closer or further from each other. Variations in coverage demonstrate the scope of the system for different ranges. While the jitter performance shows that communication has become more stable, packet loss ratio clearly demonstrates that hybrid is better able to combat data loss. Similar to throughput comparisons the advantages that may be obtained by using a hybrid system for data transmission are obvi ous as well.

These results demonstrate that the complementary features of the hybrid Wi-Fi Li-Fi system, which are a large coverage and flexibility (Wi-Fi) and high speed (Li-Fi), make it well-suited for low-latency, secure, high-throughput communications. The integrity, the authentication, confidentiality performance objectives and other related security requirements are some important factors that their optimal points can be obtained by optimising hybrid networks based on the suggested guidelines in this study to elaborate on the potential of hybrid architectures' utilisation in IoT or interconnected environments.

Table 9. A comparison of the suggested hybrid system's performance with that of hybrid systems from earlier studies.

References	Year	Algorithms	Throughput (Mbps)	Speed(mbps)
Ahmed et al. [46]	2019	Optimized Algorithm	72	-----
Wu et al. [47]	2020	Fuzzy Logic	400	-----
Ahmed et al. [48]	2020	RL	175	-----
Ahmed et al. [49]	2020	RL Method	110.69	-----
Ibraheem et al. [50]	2022	PSO Algorithm	725	-----
Proposed Work	*2024*	*HCK Algorithm*	*897.63*	*924.98*

The performance of the hybrid network proposed has been proven to have substantial potential improvement when comparing with pure Wi-Fi only system, and some other hybrid systems analyzed in this work. Throughput, jitter, packet drop ratio, speed and range are very important performance metrics to study how well the system performs in accomplishing the Wi-Fi's extended subscriber coverage along with flexibility and Li-Fi's high-speed requirement as well as low delay. This composite approach is especially suitable for mission critical Internet of Things and secure networking applications as it achieves optimal performance in data loss reduction, communication robustness as well as efficient data exchange across various multihop nodes. Comparing with other works, the presented model not only can achieve a greater throughput (897.63 Mbps) by using the HCK algorithm but is also better than both complex models, such as fuzzy logic and RL-based methods. However, apart from these merits, constraints of Li-Fi such as LOS based connectivity beginning and interference caused by the environments, have to be taken into account. However, this work provides strong evidence-based support for the continued optimisation and evolution of hybrid networking technology as it shows a hybrid architecture can indeed be capable to remain behind high performance, secure and scalable communication architectures.

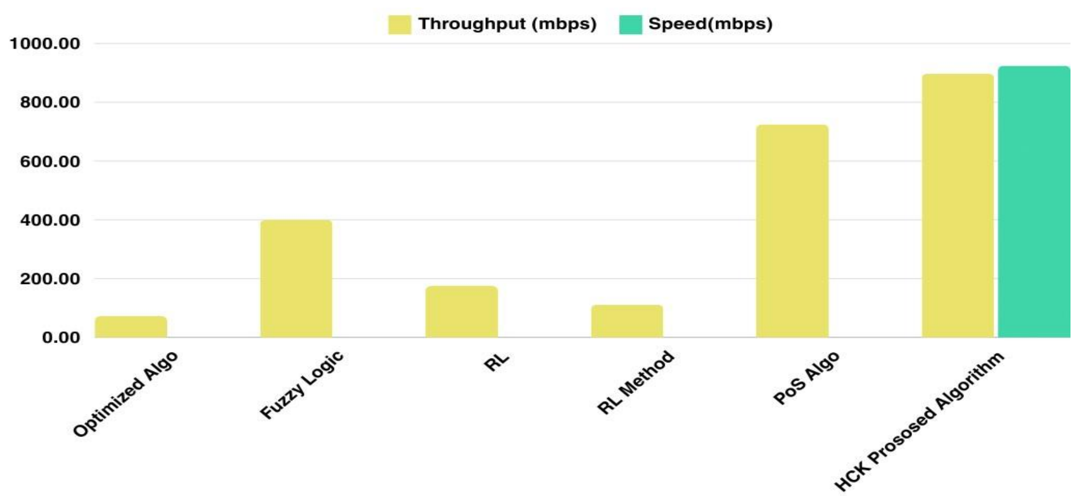


Figure 10. Comparison with Existing Algorithm

10. Conclusions & Future Work

Forward steps in communications systems have shown an increasing theme in a union of duplex communication between the radio-frequency (RF) wireless networks and light fidelity (Li-Fi) Major performance metrics including throughput, rate, dropping packet ratio, jitter and coverage probability are evaluated in this study to demonstrate the possibility and efficiency of harnessing the OW systems. The research findings show that hybrid Wi-Fi/Li-Fi architectures can exploit the complementary properties between Wi-Fi and Li-Fi for higher reliability, effectiveness and scalability according to a certain scenario.

The future work can study the new application fields and advanced optimization strategies as well as practical problems, including infrastructure cost, environmental limitations, standardization problem. Consideration of these factors is important in order to achieve the full potential of hybrid Wi-Fi/Li-Fi designs for future communication systems.

Authors Biography

Ms. Charanjit Kaur

PhD Scholar in the Department of Computer Applications, Lovely Professional University, Phagwara, Punjab, 144404. The scholar has published multiple papers and patents. She also has a patent granted in her name. Her area of interest is Networking.

Email: kj169987@gmail.com

Prof. (Dr.) Mithilesh Kumar Dubey

In the Department of Computer Applications, he holds the position of Professor at Lovely Professional University, Phagwara, Punjab, 144404. He has published multiple papers and patents in highly reputed journals. His area of interest is Artificial Intelligence, Machine learning, wireless networking, deep learning, federated learning, and security. He has more than 10 patents granted and copyrights in his name.

Email: Mithilesh.21436@lpu.co.in.

Author Contribution

Author 1: Writing, reviewing, and editing; project management; validation; and conceptualization.

Author 2: Guidance and Conceptualisation.

CONFLICTS OF INTEREST: The authors declare no conflict of interest

Appendix 1

S. No.	Abbreviation	Full Form
1	AES	Advanced Encryption Standard
2	AP	Access Point
3	CSITA	Custom Secure Image Transmission Algorithm

4	DNN	Deep Neural Network
5	DSA	Digital Signature Algorithm
6	HCK	Hybrid Communication Key
7	HLWNS	Hybrid Li-Fi and Wi-Fi Network System
8	IEEE	Institute of Electrical and Electronics Engineers
9	IoT	Internet of Things
10	Li-Fi	Light Fidelity
11	MAC	Medium Access Control
12	NB-IoT	Narrowband Internet of Things
13	OFDM	Orthogonal Frequency Division Multiplexing
14	OFDMA	Orthogonal Frequency Division Multiple Access
15	RF	Radio Frequency
16	RL	Reinforcement Learning
17	RSS	Received Signal Strength
18	SHA-256	Secure Hash Algorithm (256-bit)
19	SINR	Signal-to-Interference-plus-Noise Ratio
20	VLC	Visible Light Communication
21	Wi-Fi	Wireless Fidelity

All abbreviations and acronyms used in the manuscript are defined in Appendix A and are used consistently throughout the paper.

References

1. B. Anitha Vijayalakshmi1, "Integrating Li Fi for enhanced security in MANET data," Springer, pp. 1-8, 2024.
2. Olalere OE, & Dorasamy, N.. Perspectives on Digitisation and Economic Growth in India. Journal of Namibian Studies: History, Politics, Culture. 2024;40:464-99.
3. Toni Besjedica, Krešimir Fertalj, Vlatko Lipovac, and Ivona Zakarija, Evolution of Hybrid LiFi–WiFi Networks: A Survey. Sensors 2023, 23, 4252, pp. 1- 28.
4. K. N. R. Ali Ahmed Razzaq, "Improving the performance of IoT devices that use Wi-Fi," International Journal of Reconfigurable and Embedded Systems (IJRES), vol. 13, no. No. 3, pp. 748~- 757, November 2024.
5. R. K. 1, "Confidentiality Preserved Federated Learning for Indoor," MDPI, vol. 13, pp. 1-17, 2023.
6. Singh, PR, Singh, V. K., Yadav, R., & Chaurasia, S. N.. 6G networks for artificial intelligence-enabled smart cities applications: A scoping review. Telematics and Informatics Reports. 2023;9:100044.
7. Besjedica T, Fertalj, K., Lipovac, V., & Zakarija, I. Evolution of hybrid LiFi–WiFi networks: A survey. Sensors. 2023;23(9):4252.
8. Le DT, Tran, T. T., Dang, K. Q., Alkanhel, R., & Muthanna, A. Malware spreading model for routers in Wi-Fi networks. IEEE Access. 2022;10:61873-91.
9. G. L. X. Z. a. L. G. ChunChih Lin⇤, "RF Sensing-enabled Interference Mitigation for Wi-Fi-based IoT," in IEEE Conference on Communications and Network Security (CNS), 2024.
10. K. F. 2. Toni Besjedica 1, "Evolution of Hybrid LiFi–WiFi Networks: A Survey," MDPI, pp. 1-28, 2023.
11. K. U. V.Saravanan, "ADVANCEMENTS AND APPLICATIONS OF LI-FI TECHNOLOGY: AN IN-DEPTH EXPLORATION," in International Conference on Communication, Computing and Energy Efficient Technologies, 2024.

12. S. E. ,. I. IAIN LAU, "Hybrid mmWave-Li-Fi 5G Architecture for Reconfigurable Variable Latency and Data Rate Communications," IEEE Access, vol. 11, pp. 42850-42861, 2023.
13. Mohammed M. Ahmed , Satea H. Alnajjar . Cipher Text to Secure Li-Fi System Using Hybrid Encryption Algorithm.IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS 2025;6:210–220
14. Saman Nikkhah, Arman Alahyari, Adib Allahham, and Khaled Alawasa, Optimal Integration of Hybrid Energy Systems: A Security-Constrained Network Topology Reconfiguration.Energies 2023, 16, 2780
15. I. I. F. E. Nailal Elmangosh, "The Impact of Li-Fi Technology on Industrial Wireless Sensor Networks," in 2022 International Conference on Engineering & MIS (ICEMIS, 2022.
16. A Review of Security Methods in Light Fidelity Technology.Mohammed Majid Msallam1, Refik Samet.Proceedings of Engineering and Technology Innovation, vol. 27, 2024, pp. 01-1
17. J. Chakraborty1, "A Detailed Comparative Analysis of LiFi vs WiFi in Application of 5G Networks," Journal of Engineering Science and Technology Review, vol. 18, no. 3, pp. 126-136, 2025.
18. Besjedica, T., Fertalj, K., & Lipovac, V. (2023). Evolution of hybrid LiFi–WiFi networks: A survey. Sensors, 23(9), 4252. https://doi.org/10.3390/s23094252
19. Abdel-Razeq, S., Bany Salameh, H., & Mdardas, S. (2024). Indoor hybrid Wi-Fi/Li-Fi wireless networks (IHWLNets): Architecture, channel models, state of the art, and future directions. IEEE Communications Magazine, 62(9), 115–125. https://doi.org/10.1109/MCNA63144.2024.10703895
20. Ghali, M., Busson, A., & Begin, T. (2025). Lighting up dynamic networks: AP assignment strategy for QoS and energy efficiency in hybrid Li-Fi/Wi-Fi networks. In Proceedings of IEEE WiMob 2024. https://doi.org/10.1109/WIMOB61911.2024.10770534
21. Ghali, M., Busson, A., & Begin, T. (2025). Studying the benefits of hybrid Wi-Fi/Li-Fi networks for indoor WLANs. In Proceedings of IEEE ICC 2025. https://doi.org/10.1109/ICC52391.2025.11161091
22. Wang, X., Gan, C., Wu, S., Chen, Y., & Chen, Y. (2023). Rate-stabilized and load-balanced handover management for subway hybrid Li-Fi and Wi-Fi networks. Optics Communications, 529, 129890. https://doi.org/10.1016/j.optcom.2023.129890
23. Farrag, M., Al Ayidh, A., & Hussein, H. S. (2023). Conditional most-correlated distribution-based load-balancing scheme for hybrid Li-Fi/WiGig networks. Sensors, 24(1), 220. https://doi.org/10.3390/s24010220
24. Chatterjee, S., Sabui, D., & Roy, B. (2024). Mobility-aware blockage management of a multi-user multi-cell hybrid Li-Fi Wi-Fi system with freeform diversity receiver. Optics Communications, 552, 130487. https://doi.org/10.1016/j.optcom.2024.130487
25. Su, Y.-S., Chen, K.-L., Hsieh, M.-H., Yu, T., Li, C.-Y., & Tu, G.-H. (2025). PDCA: Practical dynamic client association in Wi-Fi mesh networks using EasyMesh. In Proceedings of IEEE ICC 2025. https://doi.org/10.1109/ICC52391.2025.11161355
26. Msallam, M. M., & Samet, R. (2024). A review of security methods in light fidelity technology. Proceedings of Engineering and Technology Innovation, 29, 13149. https://doi.org/10.46604/PETI.2024.13149
27. Liu, Z., Chen, X.-G., & Zhang, X. (2025). Optic fingerprint (OFP): Enhancing security in Li-Fi networks. In IEEE INFOCOM Workshops 2025. https://doi.org/10.1109/INFOCOMWKSHPS65812.2025.11152962
28. Ranjan, R., & Sharma, P. (2025). Simulation-based modeling of quantum key distribution in a Li-Fi system using free-space optics and polarization modulation. Journal of Optical Communications, 46(7), 1050–1064. https://doi.org/10.1515/joc-2025-0235
29. Dimmitt, J., Reith, M., & Neal, D. (2025). Security comparison of powerline communication and Wi-Fi technologies for the Internet of Things. In Proceedings of the European Conference on Information Warfare and Security (ECCWS 2025). https://doi.org/10.34190/eccws.24.1.3615
30. Imam Sabitu, R., & Malekmohammadi, A. (2025). Performance optimization of 120 Gbps–120 GHz hybrid MDM-FSO utilizing non-coherent modified duobinary modulations for optical wireless distributed networks. Applied Sciences, 15(7), 3659. https://doi.org/10.3390/app15073659
31. Infine Sinduja, V., & Charles, P. (2025). A hybrid approach using attention bidirectional GRU and weight-adaptive sparrow search optimization for cloud load balancing. The Scientific Temper, 16(5). https://doi.org/10.58414/scientifictemper.2025.16.5.12
32. Iliyas, S. M. M., Surputheen, M. M., & Shanavas, A. R. M. (2025). Trust-based symmetric game theory for physical layer security in Wi-Fi communication. The Scientific Temper, 16(5). https://doi.org/10.58414/scientifictemper.2025.16.5.03
33. Wang, J., Liu, L., & Wang, B. (2025). Preparing for what's next: Examining cutting-edge solutions for advanced wireless connectivity. In Proceedings of IEEE BMSB 2025. https://doi.org/10.1109/BMSB65076.2025.11165533
34. Chauhan, D., & Jain, J. K. (2025). Li-Fi for next-generation wireless communication. In Advances in Wireless Technologies and Telecommunication (AWTT). https://doi.org/10.4018/979-8-3693-8799-3.ch014
35. Mohan, M., Jackulin, T., Abuthahir, S. S., Sakthi, D. V., & Ayyasamy, K. (2025). Hybrid optimization model for congestion-free multipath routing and load balancing in IoT. Web Intelligence, 23(3), 1–14. https://doi.org/10.1177/24056456251325289
36. Zabeeulla, M., Singh, A., Sharma, S. K., & Chauhan, S. P. S. (2023). Design and modelling of a hybrid network security method for increasing security in vehicular ad-hoc networks. Measurement: Sensors, 29, 100878.

37. Miranti, M., Sari, L., Doris, M., Alam, S., & Surjati, I. (2025). User capacity optimization using mobility load balancing algorithms for downlink LTE networks. Jurnal Ecotipe, 12(1), 10–18. https://doi.org/10.33019/jurnalecotipe.v12i1.4532
38. Subhan, M., Raza, A., Qamar, F., Shahzadi, R., & Shahzad, A. (2024). Parametric evaluation of line-of-sight (LOS) channel in Li-Fi networks. Journal of Optical Communications, 45(10). https://doi.org/10.1515/joc-2024-0174
39. S. H. A. b. Mohammed M. Ahmed, "Cipher Text to Secure Li-Fi System Using Hybrid," IRAQI JOURNAL FOR COMPUTER SCIENCE AND MATHEMATICS, vol. 6, pp. 210-220, 2025.
40. R. Lakshman Naik1, "Development of hybrid weighted networks of RNN and DBN," Wireless Networks, vol. 31, p. 3625–3660, 2025.
41. R. Lakshman Naik1 · Sourabh Jain1 · Manjula Bairam. Development of hybrid weighted networks of RNN and DBN for facilitating the secure information system in cybersecurity using meta-heuristic improvement.Wireless Networks (2025) 31:3625–3660.
42. S. V. V. S. S. V. S V S N Murthy, "Li-Fi Technology for Visible Light Communication in Text and Audio Transmission," in 10th International Conference on Advanced Computing and Communication Systems (ICACCS), 2024.
43. R. A. B. P. M. L. R. DHANASEKARAN D, "Revolutionizing Data Transfer: Harnessing Li-Fi for Image and Text Transmission," in Proceedings of the Seventh International Conference on Electronics, Communication and Aerospace Technology (ICECA 2023), 2023.
44. G. J. V. J. S. R. B. DR. BRINDHA S, "Implementation Of Li-Fi Technology In Smart Classrooms," in Proc. of the 5th International Conference on Electrical, Communication and Computer Engineering (ICECCE), Kuala Lumpur, Malaysia, 2024.
45. H. A. Nahi, "Design and Implementation of a Holistic and Robust," LC INTERNATIONAL JOURNAL OF STEM, Vols. Volume-04, no. Issue-01, pp. 64-77, March 2023.
46. Ahmad R, & Srivastava, A. Optimized user association for indoor hybrid Li-Fi Wi-Fi network. 21st International Conference on Transparent Optical Networks (ICTON). 2019:1-5.
47. Wu X, & Haas, H. Load balancing for hybrid LiFi and WiFi networks: To tackle user mobility and light-path blockage. IEEE Transactions on Communications. 2019;68(3):1675-83.
48. F. T. ZAHRA, "LSTM-Based Jamming Detection and Forecasting,": LSTM-Based Jamming Detection and Forecasting Model, vol. 12, pp. 32944-32958, 2024.
49. Ahmad R, Soltani, M. D., Safari, M., Srivastava, A., & Das, A. Reinforcement learning based load balancing for hybrid LiFi WiFi networks. IEEE Access. 2020;8:132273-84.
50. Ibraheem EK, & Hamza, E. K.. Load Balancing Performance Optimization for LI-Fi/Wi-Fi HLR Access Points Using Particle Swarm Optimization and DL Algorithms. International Journal of Intelligent Engineering & Systems. 2022;15(6).