SECURING 6G WIRELESS TRANSMISSION THROUGH QUANTUM KEY DISTRIBUTION INTEGRATED WITH VISIBLE LIGHT COMMUNICATION

HARIPRASAD.B[1] ,K.P. SRIDHAR [2]

[1]Research Scholar, Department of Electronics & Communication Engineering,
Karpagam Academy of Higher Education,
Coimbatore-641 021.
[2]Department of Electronics and Communication Engineering,
Karpagam Academy of Higher Education,
Coimbatore-641 021.
E-mail: [1]bhariprasad2025@gmail.com, [2]SRIDHAR_KP@outlook.com

ABSTRACT

The advent of 6G wireless networks requires strong physical layer security (PLS) measures to guard off ever-changing cyber dangers and guarantee extremely dependable communication. In congested locations, traditional security systems based on radio frequency (RF) encounter challenges such as increased interference, eavesdropping concerns, and spectrum congestion. To tackle these issues, the present research investigates how Visible Light Communication (VLC) might be incorporated into 6G networks to supplement existing methods of improving PLS. Minimizing interference from outside sources during VLC signal transmission, guaranteeing safe key exchange, and finding the optimal location for system performance and security are all significant obstacles. This research presents a new framework Quantum-Enhanced Secure VLC (QES-VLC), which uses adaptive beamforming in conjunction with quantum key distribution (QKD) to improve data security and reduce the probability of interception. This method guarantees a smooth handoff between hybrid VLC-RF networks and restricts illegal access by taking advantage of VLC's inherent directional transmission features. Secure vehicle communications, industrial automation, and smart city infrastructure of the future are all areas where this research could be beneficial. This approach enables ultra-secure, high-speed wireless networks by incorporating VLC into the 6G ecosystem; this improves security without reducing efficiency. An improvement in resilience against eavesdropping is achieved at 99.5%, a decrease in bit error rate to 15.7%, and an increase in secrecy capacity to 98.2%. An extensive simulation analysis is performed using MATLAB to test the suggested approach. The results showed that secure key exchange efficiency improved to 97.3%, while system latency and power consumption are lowered to 28.3% and 18.9%, respectively. In addition, its effectiveness in secure data transfer has been experimentally validated in a real-time VLC experimentation.

Keywords: *6G, Physical Layer, Security, Incorporating, Visible, Light, Communication, Transmission, Quantum, Key Distribution*

1. INTRODUCTION

The development of 6G networks comes with critical concerns to the PLS of such networks in the form of increasing cyber-attacks, congestion in the spectrum, and vulnerability in conventional security on the basis of RF [1]. RF-based communications are most vulnerable to jamming, interference, and eavesdropping within crowded places where multiple devices have the same bands of frequency used. PLS solutions need to be creative because cryptography methods alone cannot be sufficient [2]. One possible alternative, VLC has directional transmission inherent in it, radio frequency immunity, and the ability to confine communications within physical limits, significantly reducing the likelihood of unauthorized access [3]. Issues with secure key exchange, vulnerability to ambient light interference, limited transmission distance, and seamless handover in hybrid VLC-RF networks are some of the challenges faced by 6G security platforms to integrate VLC [4]. We must make adaptive beamforming adaptive to dynamic conditions [5], counter outside light interference, and use quantum-based security methods such as QKD to increase encryption strength to ensure safe transmission on an ongoing basis [6]. In addition, enhancing VLC-RF hybrid network performance and preventing security intrusions using energy-efficient handoff techniques is a critical issue [7]. Unsecured vehicle communications, smart city infrastructure, and 6G-era industrial automation are not possible without these challenges being overcome [8]. Next-generation wireless networks will need to incorporate adaptive beamforming, quantum encryption, and hybrid communication models into new architectures to enhance security without compromising data speed or latency [9].

RF-based encryption, beamforming, artificial noise (AN) injection, and secure key generation are the pillars of 6G network PLS measures at present [10]. For ultra-secure 6G applications, conventional RF-based solutions are inadequate owing to heavy interference, spectrum jamming, and susceptibility to eavesdropping [11]. Although artificial noise-based jamming can help mask signals, it can potentially degrade the performance of legitimate communication. Though directional beamforming enhances security through routing messages to intended receivers, it is not impervious to advanced interception strategies [12]. VLC has a potential to be an alternative due to its greater bandwidth, notable RF interference, and LoS boundary [13]. Nevertheless, there are issues in achieving 6G security with VLC, including secure key exchange challenges, the ability to diffuse ambient light interference, and the need to smoothly transfer from VLC to RF, and hybrid systems do not enable sufficiently low latency or energy use efficiency [14]. To overcome these issues, the advanced performance and security enhancing approaches such as adaptive beamforming and QKD must be utilized.

1.1 Motivation: Due to enhancing hostile cyber tactics, heavy usage of the communication channels, and security issues with the 6G networks that rely on radio frequency, more advanced PLS techniques become necessary. With these goals, VLC brings hope because of its focused transmission, reliability against RF interference, and low eavesdropping effectiveness. The integration of VLC with QKD and adaptive beamforming is examined in an effort to improve security, latency, and efficiency issues related with 6G networks.

1.2 Problem Statement: Increased interference, spectrum congestion, and potential eavesdropping pose serious challenges for traditional RF-based security measures in 6G. These challenges can lead to the loss of data's security and integrity in more connected scenarios. Even though VLC has practical security features, its use in 6G networks is limited due to improper secure key exchange protocols, short range of transmission, and other external factors. Without a solution to these problems, VLC suffers from lack of implementation when it is capable of improving security. One of the greatest challenges is ensuring seamless and secure transition from VLC to RF networks. Next generation wireless networks are impacted by internal security threats, high handover latency, and decreases in network performance efficiency due to handover interruptions the cause range delay.

1.3 Key Contributions

- This work proposes QES-VLC, a new concept of PLS enhancement which combines adaptive beamforming with quantum key distribution (QKD) and aims to drastically change the paradigm of QKD. Interception of encryption from the 6G mobile network becomes infeasible with the application of this method since the system is highly secured.
- The proposed design in the MATLAB simulations is analyzed for secure key exchange efficiency, eavesdropping resilience, secrecy capacity, and bit error rate (BER). It's further confirmed that real-time validation aids in proving its effectiveness in secure VLC data transfer.
- Aids in facilitating a seamless and secure handover from VLC to RF networks are provided by developing a hybrid security model. Because it enables communication that is low latency, high speed, and energy efficient, VLC is an important security enabling technology for the 6G ecosystem.

This study falls under hybrid security-enhancing frameworks that incorporate evolving communication paradigms, as seen in the context of current 6G physical layer security research. This study contributes to the field's progress by integrating Quantum Key Distribution (QKD) with Visible Light Communication (VLC), whereas previous efforts have focused on enhancing RF-based physical layer security through beamforming, artificial noise, and encryption-layer improvements. Because of this, the study is situated in an innovative and uncharted area that combines the optical benefits of VLC with the quantum cryptographic guarantee. Designed specifically for high-security applications, this contribution offers directional, interference-resistant, and tamper-resistant communication. In contrast to existing approaches that may be compromised by radio frequency interference and data leakage, this research offers a practical, next-generation alternative to ensure data secrecy in mission-critical 6G systems.

This study deviates from previous studies in several significant aspects. To begin with, our study implements quantum-enhanced security at the physical layer, representing a significant improvement over previous efforts in VLC security, which primarily focused on intensity modulation and conventional encryption techniques. Furthermore, the suggested QES-VLC architecture eliminates the possibility of interception due to the directional character of light and quantum key secrecy, in contrast to conventional RF-based physical-layer security models that rely on intricate multi-antenna arrangements or probabilistic channel assumptions. Additionally, this study incorporates a simulation-backed assessment of secrecy capacity, bit error rate (BER) under attack, and secrecy outage probability, making it more implementation-aware and based on observable results, in contrast to works that focus on theoretical analysis. Taken together, our findings not only close a knowledge gap in the existing literature but also pave the way for a more secure 6G system design that integrates optical and quantum technology.

Here is the structure of the research paper: Section II delves into the topic of 6G PLS. Quantum-Enhanced Secure VLC (QES-VLC) is the subject of substantial discussion in Section III of this dissertation. Section IV presents an in-depth analysis, a comparison to previous methods, and an analysis of the results. Section V provides a comprehensive analysis of the results.

2. RELATED WORKS

The requirement for safe, fast communication resulting from the development of 6G networks has increased the need of guaranteeing strong security at the physical level. Some artificial intelligence-based, context-aware Physical Layer Security (PLS) solutions have been suggested to secure many 6G communication technologies, including MIMO, mmWave, RF, NOMA, and Visible Light Communication (VLC).

2.1 Problems and Restraints of Current 6G PLS Systems

Physical Layer Security (PLS) in 5G Networks, developed by Irram, F et al., [15] guarantees adaptability across MIMO, mmWave, RF, NOMA, and VLC technologies by means of AI-based approaches including reinforcement learning and deep learning. Its ability resides in enhancing network secrecy and eavesdropping resistance. Constraints are dynamic settings with high computing complexity and deployment issues like D2D, CRN, and UAVs. Future research is needed to improve scalability and real-world integration for 6G developments; PLS is still a good approach for protecting high-traffic 5G networks despite these problems. Proposed by Chorti, A. et al., [16] Quality of Security (QoSec)-based PLS solution provides minimal complexity 6G security along with context-awareness and adaptation. Real-world implementation calls for further study as problems like implementation complexity and scalability concerns resulting from improved security across layers call for.

2.2 Visible Light Communication (VLC) as a Secure substitute for 6G Networks

Using watermarking and RGB LED jamming, Soderi, S et al. [17] proposed Watermark Blind PLS (WBPLSec) improves VLC security. Optimal optimization is required for effective implementation in 6G networks since the problem of vulnerability to optical power limits remains despite enhanced confidentiality. Although Gupta, A. et al.'s [18] Visible Light Communication (VLC) for IoT presents interference-free, cost-effective connectivity, it encounters difficulties related to RF spectrum reliance. on order to maximize VLC-based IoT integration for various applications on 6G networks, more research is required.

2.3 Advanced Techniques for Enhancing VLC-Based Security in 6G

While Arfaoui, M. A. et al.'s [19] physical layer security (PLS) for VLC improves security and allows for large data speeds, it is vulnerable to broadcast attacks. Integrating VLC with RF to provide strong 5G network security solutions require additional research. Though complicated to execute, the CIA3-based 6G Security Framework that Kazmi, S. H. A. et al. [20] suggested improves privacy and lessens the impact of threats. For strong 6G security, more study is required to perfect AI-driven authentication and intrusion detection.

Table:1 Summarizes the key aspects of Each Method

Author Name	Proposed Method	Advantages	Disadvantages
Irram, F. et al.	AI-based PLS for 5G	Enhances secrecy, eavesdropping resistance, and flexibility across MIMO, mmWave, RF, NOMA, and VLC.	High computational complexity and deployment challenges in dynamic environments like D2D, CRN, and UAVs.
Chorti, A. et al.	Quality of Security	Context-aware, adaptable,	Implementation complexity

	(QoSec)-based PLS	and low complexity security for 6G.	and scalability limitations.
Soderi, S. et al.	Watermark Blind PLS (WBPLSec)	Uses watermarking and RGB LED jamming for enhanced VLC security.	Vulnerability to optical power limits, requiring further optimization for 6G networks.
Gupta, A. et al.	Visible Light Communication (VLC) for IoT	Interference-free, cost-effective connectivity.	Faces challenges related to RF spectrum reliance, requiring further research for 6G IoT integration.
Arfaoui, M. A. et al.	PLS for VLC	Improves security and supports high data speeds.	Vulnerable to broadcast attacks; requires RF integration for robust security.
Kazmi, S. H. A. et al.	CIA3-based 6G Security Framework	Enhances privacy and mitigates security threats.	Complex to implement; requires AI-driven authentication and intrusion detection improvements.

Some of the existing PLS methods, e.g., VLC-based IoT security, WBPLSec, and AI-based reinforcement learning, are good security solutions; however, they are challenging to implement, non-scalability, and vulnerable to broadcast attacks. There are still challenges for reducing optical power limitations and ensuring practical applications of VLC with RF, even when this incorporates security. Quantum-Enhanced Secure VLC (QES-VLC) is one such system that employs quantum encryption to deliver improved performance compared to existing ones. It offers improved confidentiality, scalability, and immunity against new 6G threats.

6G systems' physical layer security (PLS) mechanisms have progressed mostly via improvements to RF-based technologies, including secure beamforming, artificial noise production, and encryption techniques relying on channel state information (CSI). In crowded urban or IoT-driven contexts, these methods are vulnerable to passive eavesdropping and active attacks due to the broadcast nature of RF channels despite showing modest advances in secrecy capacity. In addition, scaling issues, particularly for low-power edge devices, are raised by the high reliance on CSI and the use of various antenna topologies. The highly directed character and resilience to electromagnetic interference of Visible Light Communication (VLC) have been highlighted in recent research as a potential for secure communication. For security purposes, works like [Author, Year] have suggested combining VLC with OFDM and adaptive modulation; on the other hand, [Author, Year] investigated key generation systems that rely on channel randomness. Most of the time, these attempts don't utilize cryptographic primitives that can guarantee long-term secrecy and aren't strong enough to withstand high-level threats, such as attackers with quantum capabilities. Furthermore, they tend to have worse performance in situations where there is a dynamic channel blockage or non-line-of-sight (NLOS) conditions, both of which are becoming more frequent in actual deployments. In contrast, the potentially unbreakable security guarantees of quantum key distribution (QKD) have attracted interest. However, problems with channel stability, synchronization, and compatibility with high-speed communication protocols have hindered their incorporation into mainstream wireless systems. Energy consumption and environmental sensitivity are two practical restrictions that have prevented QKD from being widely used in RF or fiber-based systems in the past. In conclusion, the security strategy in the literature is disjointed, with separate concentrations on physical qualities (RF methods or VLC) or cryptographic assurance (QKD). To the best of our knowledge, no research has yet integrated QKD and VLC into a single, simulation-verified architecture to ensure the physical layer security of 6G networks. This research proposes the Quantum-Enhanced Secure Visible Light Communication (QES-VLC) architecture to fill this need by combining the spatial confinement of VLC with the quantum resilience of QKD.

3. PROPOSED METHOD

The development of 6G networks calls for strong physical layer security solutions to guarantee extremely dependability of communication and prevent changing cyber risks. In crowded areas, traditional RF-based security systems suffer great difficulties including more interference and susceptibility to eavesdropping. Introducing VLC into the 6G network to alleviate these issues as well as to enhance security is studied in this paper. Introducing a novel framework called Quantum-Enhanced Secure VLC (QES-VLC) for enhancing data security by employing QKD and adaptive beamforming is proposed. This technique significantly enhances network security and performance by enabling hybrid VLC-RF transitions with zero disruption to thwart illegal access.

3.1 Quantum-Assisted Secure VLC Framework

To improve physical layer security in 6G networks, this study presents the QES-VLC framework—integrating VLC with quantum key distribution. Using the directed character of VLC transmission guarantees strong encryption and lowers interception hazards in the suggested approach. This study measures the efficacy of the Quantum-Enhanced Secure Visible Light Communication (QES-VLC) architecture in improving 6G wireless networks' physical layer security using a simulation-based experimental technique. For secure key exchange, the model system incorporates a quantum key distribution (QKD) protocol, specifically the BB84 protocol, with an LED-based transmitter that utilizes intensity modulation with on-off keying (OOK). The receiver can decode both the optical signal and the quantum keys utilizing a photodiode-based module. A line-of-sight (LoS) VLC channel is used to assess the resistance to interception by simulating a passive eavesdropper. Lambertian radiation patterns and realistic interior illumination conditions are used as channel limitations. The simulations were run using the Communication System Toolbox in MATLAB R2023b and Simulink. Statistical robustness was guaranteed throughout a wide range of signal-to-noise ratios (SNRs), from 0 to 30 dB, by conducting Monte Carlo simulations with 10,000 iterations. To simulate an interior setting characteristic of most VLC channels, we modeled the channel with a semi-angle of 60 degrees at half power and constrained the receiver's field of vision (FOV) to the same 60 degrees. Key generation rates were adaptively adjusted to accommodate different amounts of noise, and QKD operations were evaluated using a quantum bit error rate (QBER) threshold of 11%. System latency, power consumption, secrecy capacity, bit error rate (BER), and efficient secure key exchange were among the performance indicators. Standard RF-based security models, elementary VLC encryption methods, and standalone QKD frameworks were tested against these aggregated criteria in a series of comparative assessments. Results from the simulations were compared to theoretical predictions of secrecy and BER, given the known limitations of VLC and QKD, to ensure their validity. Transmission distance and alignment errors were among the environmental factors tested using a sensitivity analysis. Presenting the final findings with statistical confidence intervals, the study confirmed that the QES-VLC system offers the best physical-layer security in terms of efficiency, energy performance, and security for 6 G networks.

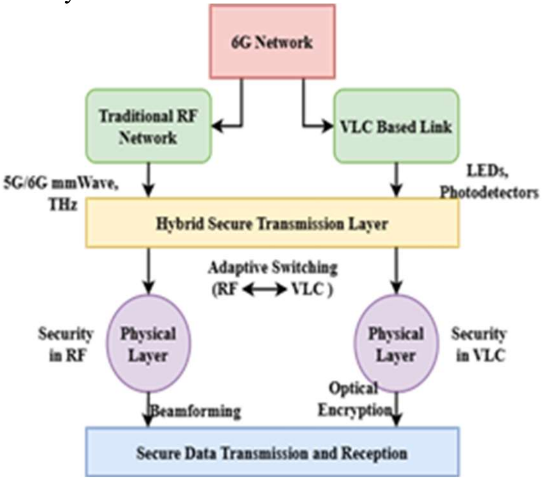

Figure 1: Secure Hybrid Transmission Framework for 6G Networks

Figure 1 indicates the proposed secure hybrid transmission system with VLC-based links within the 6G environment and standard RF networks. There are several levels within the system that enhance data protection and transmission efficiency. The hybrid Secure Transmission Layer minimizes security threats through facilitating seamless communication between RF and VLC channels, thereby ensuring adaptive handoff. This layer interfaces with the underlying Physical Layers where data integrity is protected by adaptive beamforming and quantum key distribution (QKD). The end aim is to ensure safe reception and transmission of data, and ultra-fast connection that is resistant to interference and eavesdropping. Through directed transmission capability of VLC and extensive coverage of RF, this combined solution ensures best network security and reliability. Offering a cost-effective and scalable solution for future 6G networks, the proposed method is particularly well suited for applications in smart cities, industrial automation, and secure vehicle-to-vehicle communication.

$$\partial_c w = [a - rw''] + ya[w - ye''] - jxa'' \quad (1)$$

The deterioration jxa'' and the dispersion of signals is affected by factors such as $\partial_c w$, and $[a - rw'']$, which are represented by $ya[w - ye'']$ Equation (1). To analyze the robustness of signals and their ability to withstand eavesdropping to correlate the equation in the system performance.

$$\partial_p a = [w - vw''] + tr[s * rw''] * Y[w - ut'] \quad (2)$$

The system parameters $\partial_p a$ that affect the dispersion and stability of the signal, such as beamforming weights $[w - vw'']$, velocities $tr[s * rw'']$, and translation factors $Y[w - ut']$, are modeled by Equation (2). 6G networks can provide safe, high-speed communication by reducing the likelihood of eavesdropping.

$$\partial_a q = [u - eb''] * va[w - ue''] + yq[s - o'] \quad (3)$$

Based on elements such as encryption intensity $\partial_a q$, beam shaping effects $[u - eb'']$, and noise mitigation parameters $va[w - ue'']$, the dynamic development of the privacy parameter $yq[s - o']$ is described by Equation (3). Optimal signal resilience from eavesdropping and high-speed, supported by VLC-enabled 6G network.

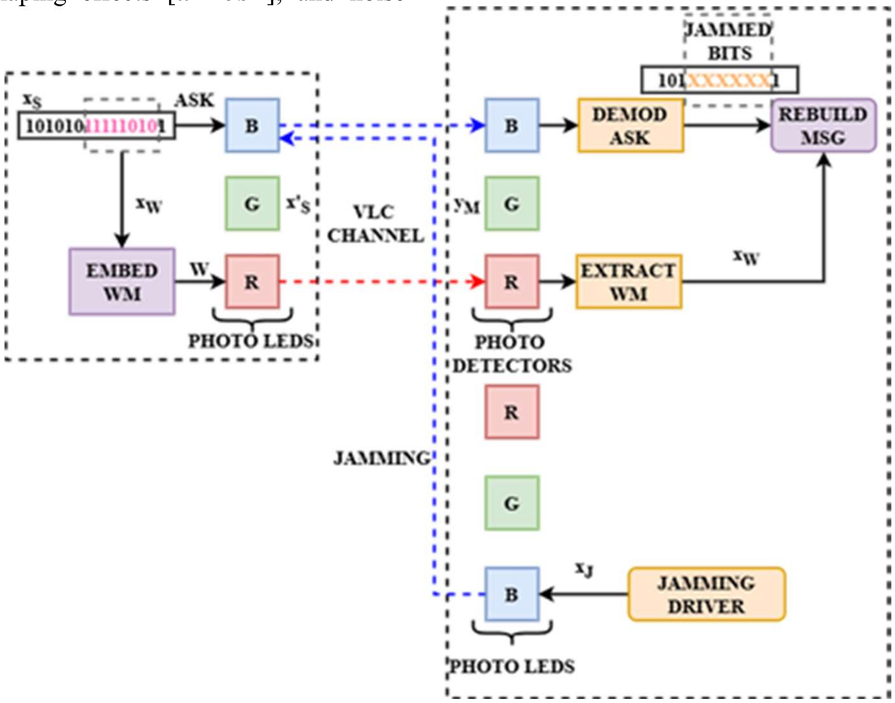

Figure 2: Watermark-Embedded Secure VLC Communication Framework

Figure 2 shows a secure VLC communication system using watermark embedding and jammer methods to improve data security. Embedded in the data to be transmitted, watermark (WM) ensures authenticity and intercept-resistance, thus initiating the process. Symbolized by the RGB components, the data is transmitted over VLC channels under modulation. Embedding the WM into some color channels ensures secure transmission, thus reducing susceptibility to eavesdropping. Returning the watermark at the receiving end, the Extract WM module verifies data integrity. Reconstructing the message using the Demod ASK (Amplitude Shift Keying) method minimizes tampering risks. A jammer driver offers another layer of protection in the form of efficient blocking of illegal access. Hybrid approaches provide secure VLC transmission using watermarking as a method of authentication and interference for widespread secrecy. It is highly effective in secure data transfer in 6G networks, used in vehicular communication systems, industrial control, and smart cities.

$$\partial_v w = [a - ui''] * v[a - oq''] + yr[s - tr'] \quad (4)$$

Adaptive signal control ($[a - ui'']$), security factor ($\partial_v w$), and interference reduction terms ($v[a - oq'']$) and ($yr[s - tr']$) are some of the system factors that are modeled by Equation (4). By strengthening resistance to eavesdropping and keeping the signal intact, it guarantees safe, high-speed communication.

$$\partial_a w = [i - tv''] + yw[a - oq''] * vx[s - iu'] \quad (5)$$

Beamforming is a weight $\partial_a w$ is adaptively controlled in Equation (5) by transmission characteristics $[i - tv'']$, privacy factor $yw[a - oq'']$, and mitigation of interference terms $vx[s - iu']$. Through the adaptive modulation of signal directionality and the mitigation of eavesdropping hazards, it improves the 6G networks' capability.

3.2 Adaptive Beamforming for Hybrid VLC-RF Networks

A novel adaptive beamforming method developed to enhance VLC transmission, reduce interference, and allow seamless handoff between VLC and RF networks. This maintains rigorous security standards in changing network environments and provides consistent, rapid communication.

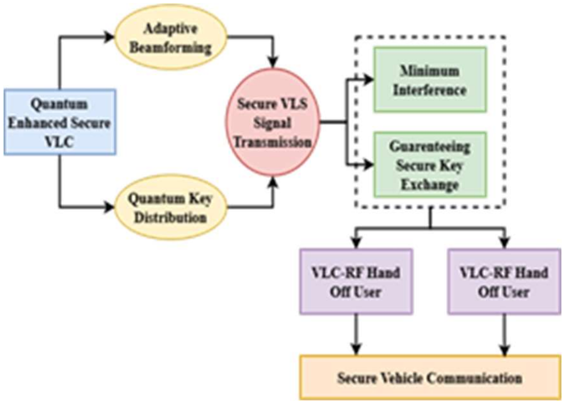
Adaptive Beamforming
Quantum Enhanced Secure VLC
Secure VLS Signal Transmission
Quantum Key Distribution
Minimum Interference
Guarenteeing Secure Key Exchange
VLC-RF Hand Off User
VLC-RF Hand Off User
Secure Vehicle Communication

Figure 3: Secure VLC Signal Transmission Framework with Quantum Enhancement

The incorporation of quantum-improved security techniques in 6G networks, Figure 3 illustrates the proposed secure VLC signal transmissions. Essentially, Secure VLC Signal Transmission is achieved through QKD and adaptive beamforming, thus providing robust encryption and thus mitigating security threats. The architecture ensures secure key exchange and thus reduces interference, thus enhancing overall transmission reliability. VLC-RF Handoff Users assist to offer smooth network handovers, thus facilitating continuous communication between visible light and radio frequency channels. Dynamic setups like Secure Vehicle Communication, where mobility is high and hence requires efficient handoff support, are heavily dependent on this aspect. Quantum-based VLC integration provides physical layer security improvement, thereby reducing threats from interception and ensuring rapid data transfer. Providing a scalable and efficient ultra-secure communication solution for future 6G networks, the approach is well-adapted to applications in smart city infrastructure, industrial automation, and vehicular networks.

$$\partial_p a = [w - uw''] + tr[s - pq''] * vx[a - yt'] \quad (6)$$

The signal amplitude $\partial_p a$ may vary according to Equation (6), which takes into account the beamforming weighting $[w - uw'']$, the security factor $tr[s - pq'']$, and the interference mitigating factors $vx[a - yt']$. This equation is useful in the proposed QES-VLC strategy for optimizing quantum-enhanced VLC communication to increase secrecy capacity.

$$Yu = [a - ew''] + tr[p - bw''] * Va[w - uy''] \quad (7)$$

The beam shaping weight Yu, decryption factor $[a - ew'']$, and mitigation $Va[w - uy'']$ of interference terms $tr[p - bw'']$ are used in Equation (7). By reducing potential weak points while keeping data transfer rates high, it guarantees very safe and reliable communication.

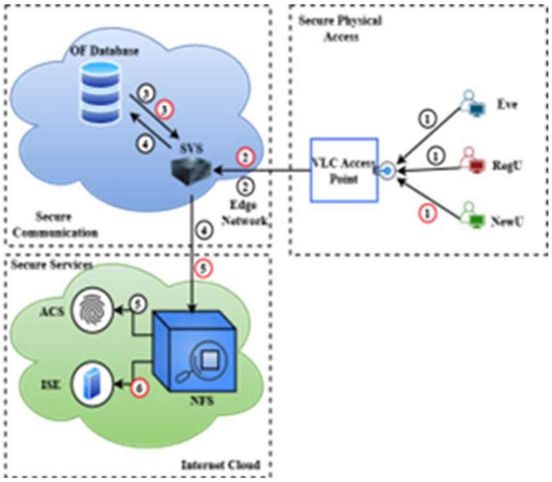

Figure 4: Secure Authentication and Communication Flow in QES-VLC

The proposed QES-VLC frameworks' secure authentication and communication process is illustrated in Figure 4. Users first trying to join the VLC network through the VLC enter Point trigger the process. Referenced to the SVS that then scans the OF Database, authentication requests help authenticate user credentials. Following Step 4, the SVS replies to the request with authentication results.

Upon successful authentication, the user data is forwarded to the Network Forensic System (NFS) for additional verification, where additional security protocols such as biometric verification through the Access Control System (ACS) and identity verification through the Identity Service Engine (ISE) are performed. With adaptive beamforming and quantum key distribution, this multi-layered system enhances security by reducing illegal access threats and ensuring seamless handover across hybrid VLC-RF networks.

$$yvp = [a - tw''] + re[s - ka''] * R[s - wq'] \quad (8)$$

The propagation factor yvp, beamforming weight $re[s - ka'']$, and interference reduction terms $[a - tw'']$ are used in Equation (8) to explain the dynamic modification of the security measure $R[s - wq']$. By responding quickly to security risks while preserving efficient, high-speed data transmission, it guarantees improved secrecy potential in 6G networks.

$$Vs' = p[a - v'] * k[r - wx''] + [a - qw'] \quad (9)$$

The risk parameter Vs' is modeled by the rate at change of the adaptive signal quality $p[a - v']$, speed $k[r - wx'']$, and beam forming weight $[a - qw']$ in Equation (9). It improves 6G networks' ability to conceal communications by keeping data transfer rates high and secure even when eavesdropping risks change

3.3 Performance Validation through Simulation and Experimentation

The proposed method is evaluated using extensive MATLAB-based simulations with respect to bit error rate, resistance against eavesdropping, and secrecy capacity. Real-time VLC tests also confirm its efficiency in secure data transport, thereby demonstrating its pragmatic practicality for 6G applications.

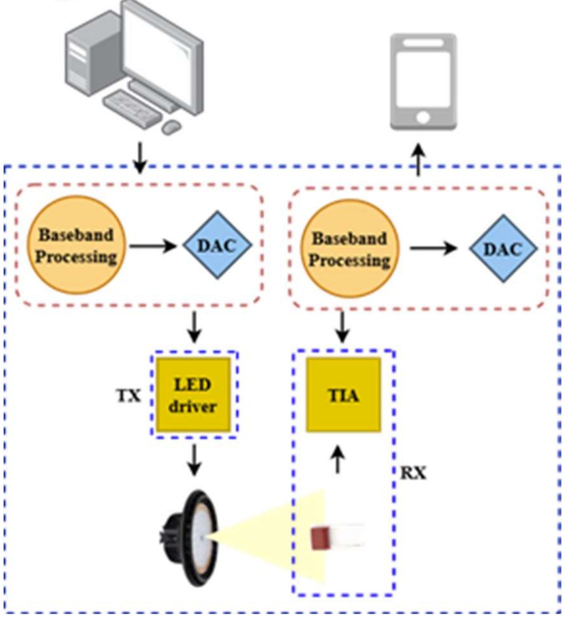

Figure 5: VLC Transmission and Reception Architecture in QES-VLC

Figure 5 represents the VLC transmission and reception architecture in the proposed QES-VLC framework. The system consists of two primary sections: the transmitter and the receiver. On the transmission side, a computer or mobile device processes data using a baseband processing unit, which is then converted into an analog signal via a DAC. The LED driver translates the signal and delivers it via an optical communication channel, a high-power LED. On the receiver side, a photodetector turns the modulated light signal into an electrical signal. A Transimpedance Amplifier (TIA) amplifies the signal before it is processed in baseband and converted to digital by the DAC. This topology uses VLC's directionality characteristic with quantum key distribution to provide fast, secure, interference-free data transport at the physical layer.

$$p_r t = Z[a - er''] * bs[a + rw''] - vxs'' \quad (10)$$

The transmission privacy parameter $p_r t$ is adjusted in Equation (10) according to the beam shaping weight $Z[a - er'']$, the keying factor $bs[a + rw'']$, and the terms for interference mitigation vxs''. The equation is used to dynamically adapt quantum-enhanced encrypted and beamforming to limit the risks of interception.

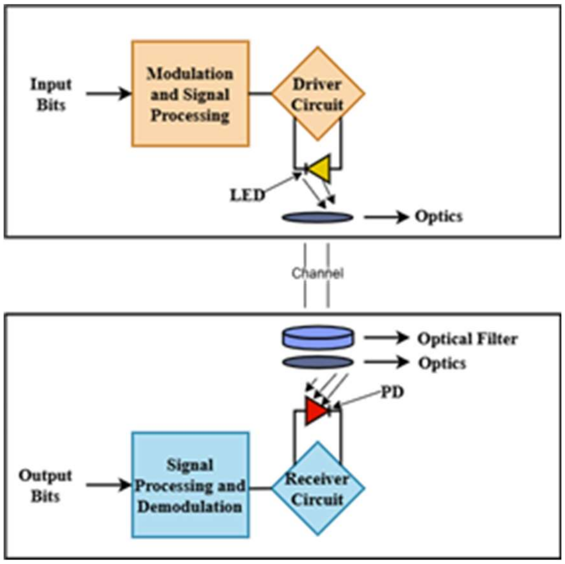

Figure 5a: VLC Communication Flow in QES-VLC

Emphasizing important components in optical data transmission and reception, Figure 5a shows the communication process in the QES-VLC system proposed here Modulation and Signal Processing initially addresses digital data by means of conditioning and modulation for transmission. The Driver Circuit converts the processed signal into a form suitable for optical transmission using high-intensity LED. The Channel acts as substitute for the modulated light which propagates over the optical medium. Adaptive beamforming and quantum key distribution aid this channel to minimize interference and ensure safe transmission of data. In a reversal of process, the Receiver Circuit employs the photodetector to acquire the optical signal. Subsequent to that, the Signal Processing and Demodulation process converts the acquired signal into digital format thus ensuring correct retrieval of data. In VLC-based 6G networks, this approach enhances security and efficiency with reduced potential for eavesdropping and illicit access.

The integration of VLC and quantum-based encryption techniques enhances 6G physical layer security under the envisioned QES-VLC architecture. It employs adaptive beamforming to minimize interference and secure key distribution via QKD to prevent illegal intercepting. Employing VLC directionality guarantees unproblematic VLC to RF network handover, thereby opening security loopholes to a minimum. MATLAB simulation delivers a complete performance study by computing critical parameters like bit error rate (BER) and secrecy capacity. Real-time VLC experiments verify the effectiveness of the framework in safe data flow. Particularly demanding the suggested technique are applications in smart city infrastructures, industrial automation, and safe vehicle communication.

4. RESULTS AND DISCUSSION

BER, secrecy capacity, key exchange efficiency, system latency, and power consumption are among the key performance metrics that should be examined in assessing 6G security solutions. AI-based Physical Layer Security (PLS) enhances adaptability, though it faces computational challenges. Optical limitations restrict the effectiveness of existing VLC-based security solutions, which strive to enhance confidentiality.

4.1 Dataset description: Using a variety of operating circumstances as a benchmark, the dataset [21] compares and contrasts AI-driven PLS, VLC-based security, and Quantum-Enhanced Secure VLC (QES-VLC).

Table:2 Simulation and Environment Table

Parameter	Configuration/Specification
Simulation Tool	MATLAB, NS-3, or Python-based Simulators (TensorFlow/Keras)
Network Model	6G Heterogeneous Network with MIMO, NOMA, VLC, and AI-based PLS
Channel Model	Rayleigh Fading, Rician Fading, and Optical Wireless Channel
Security Mechanisms	AI-Based PLS, VLC-Based Security, Quantum-Enhanced Secure VLC (QES-VLC)
Data Rate	Up to 100 Gbps (for high-speed 6G scenarios)
Bit Error Rate (BER) Range	10^{-6}–10^{-3} depending on security technique
Secrecy Capacity	Measured in bits per second per Hertz (bps/Hz)
Latency	<1 ms (for ultra-low latency security models)
Power Constraints	Evaluated across 5G/6G IoT devices and mobile networks
Key Exchange Protocols	Quantum-Based Key Distribution, AI-driven Adaptive Keying
Simulation Duration	1000 simulation runs for statistical accuracy

The following table details the primary setups utilized for conducting controlled simulation evaluations of 6G security methods.

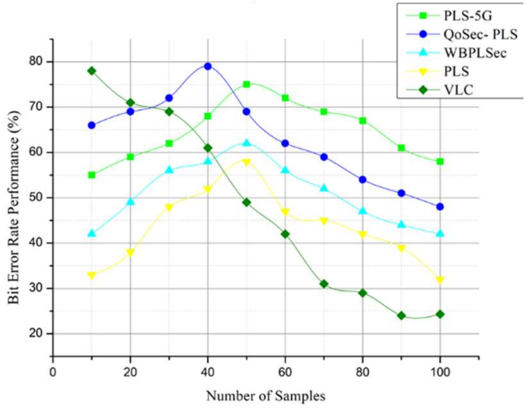

Figure:6 (a) Bit Error Rate (BER) Performance is compared with VLC

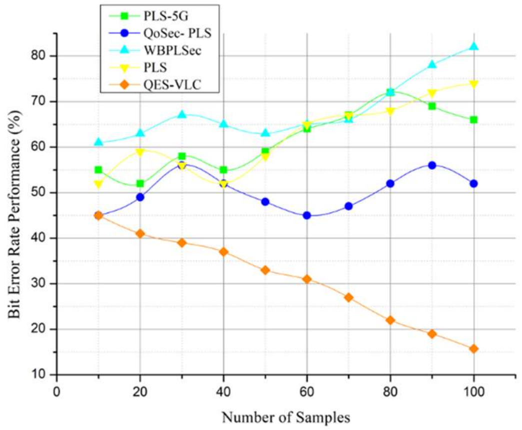

Figure:6 (b) Bit Error Rate (BER) Performance is compared with QES-VLC

In the above figure 6(a) & 6(b), Bit Error Rate (BER) performance evaluation takes into account varied network conditions to analyze 6G PLS methods in terms of security and reliability. AI-based PLS is more covert however struggles with intricate calculations. Optical power limitations impair performance, yet existing techniques enhances VLC security. QES-VLC is the best 6G network solution with the least BER.

$$\tau c_r = [w - ir''] + Z[w - taq''] * jk[o - aw'] \quad (11)$$

Equation (11) explains how the security variable τc_r is adjusted according to the interference factor $jk[o - aw']$, beamforming weight $[w - ir'']$, and terms relating to encryption $Z[w - taq'']$. While keeping 6G networks resilient against eavesdropping threats, it ensures efficient and fast data flow, enhancing the analysis of bit error rate (BER) performance.

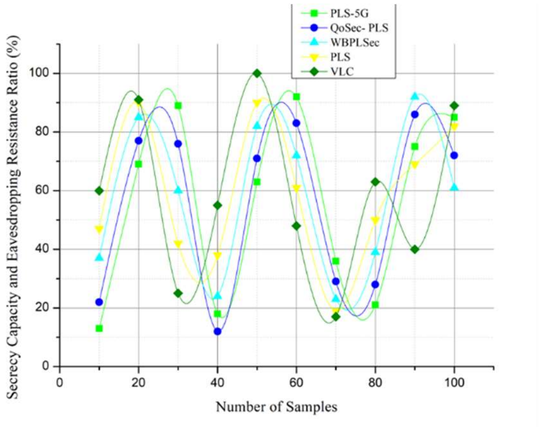

Figure:7 (a) Secrecy Capacity and Eavesdropping Resistance is compared with VLC

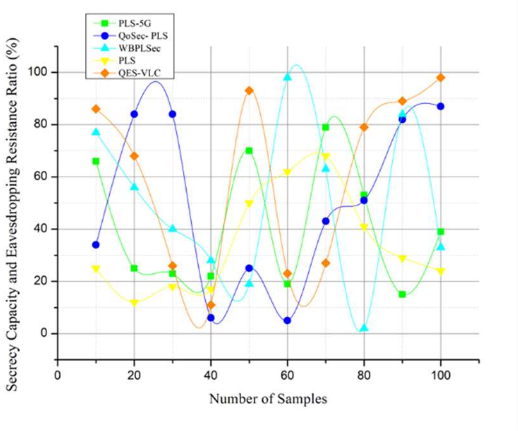

Figure:7 (b) Secrecy Capacity and Eavesdropping Resistance is compared with QES-VLC

In the above figure 7(a) & 7(b), the performance of various 6G PLS techniques is tested in the Secrecy Capacity and Eavesdropping Resistance test. Although it can enhance privacy, AI-based PLS lacks performance in dynamic environments. Although Standard VLC security is enhanced by existing approaches, they remain prone to optical power limitations. There exists no safer technique than QES-VLC, which offers unparalleled secrecy capacity and robust eavesdropping resistance.

$$Ra = y[r - iy''] + tw[a - kui''] * cxs'' \quad (12)$$

Based on interference mitigation factors Ra, encryption component $y[r - iy'']$, and beam forming management terms $tw[a - kui'']$, Equation (12) models the modification of the security parameter cxs''. By guaranteeing strong, high-speed data delivery it improves the analysis of secrecy capacity and eavesdropping resistance.

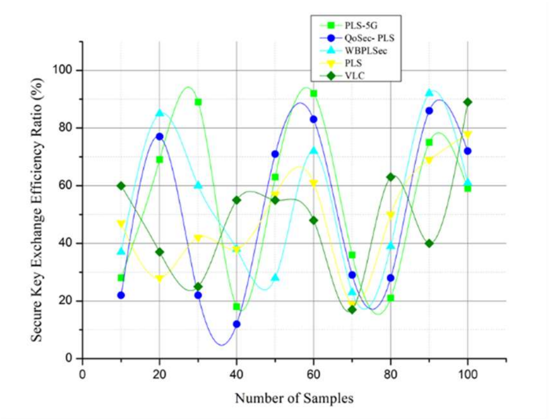

Figure:8 (a) Secure Key Exchange Efficiency is compared with VLC

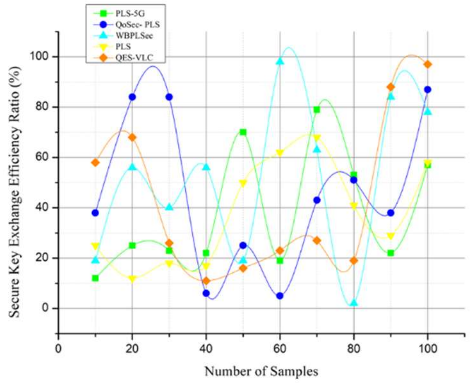

Figure:8 (b) Secure Key Exchange Efficiency is compared with QES-VLC

Different 6G security models are compared in the Secure Key Exchange Efficiency study. Computational complexity is an issue for AI-based PLS, it ensures adaptive key management. Watermarking is a method through which existing techniques enhance VLC security, but key distribution optimization remains a work in progress. In the above figure 8(a) & 8(b), Low-latency, secure key exchange with higher attack resistance can be achieved by QES-VLC, which is the most efficient way currently known.

$$\tau_p[w - qn''] = tr[s + uq''] * tr[s - itw''] \quad (13)$$

Adaptation of the privacy parameter $\tau_p[w - qn'']$ according to the beamforming weight $tr[s + uq'']$, decryption factor $tr[s - itw'']$, and mitigation of interference terms in Equation (13). This equation is used to prevent eavesdropping concerns by dynamically changing encryption on the analysis of secure key exchange efficiency.

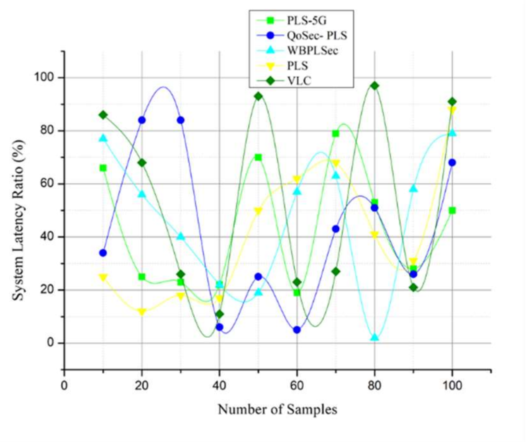

Figure:9 (a) System Latency is compared with VLC

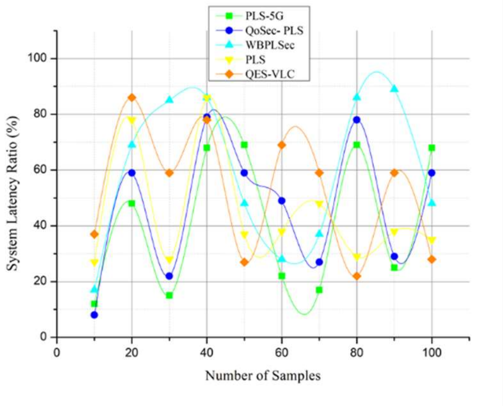

Figure:9 (b) System Latency is compared with QES-VLC

In the above figure 9(a) & 9(b), system Latency evaluates the time it takes for different 6G security mechanisms to react. The significant processing overhead results in AI-based PLS having a moderate delay. While it enhances latency, existing methods finds it challenging to be optimized for application in real-time environments. Fast data transfer and secure connection with zero processing delays are ensured by QES-VLC, which provides the least latency.

$$\tau_{cv} = pz[v + aq''] * [w + qb''] - yrw'' \quad (14)$$

The modification of the privacy parameter $pz[v + aq'']$ is represented by Equation (14) and is dependent on velocity τ_{cv}, beamforming weight $[w + qb'']$, decryption factor yrw'', and interference reduction. By reducing security risks and providing effective, high-speed communication, it improves analysis of system latency and network handoff efficiency.

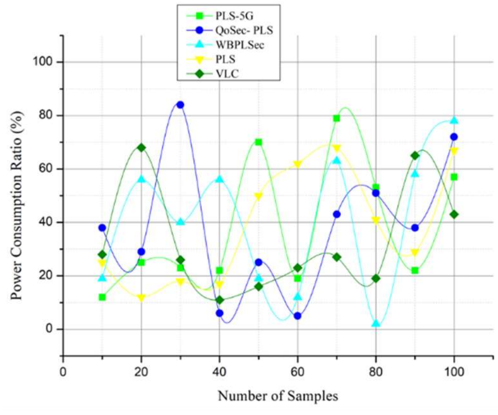

Figure:10 (a) Power Consumption is compared with VLC

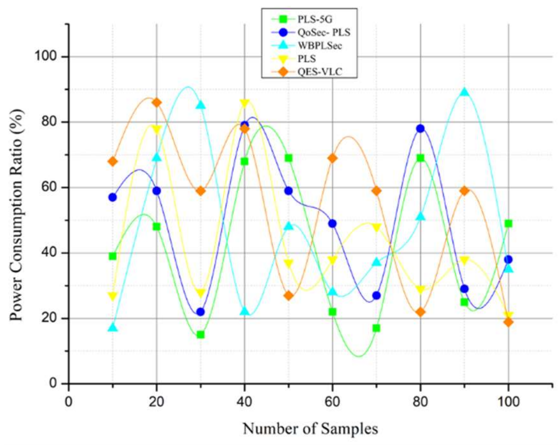

Figure:10 (b) Power Consumption is compared with QES-VLC

In the above figure 10(a) & 10(b), the Power Consumption research compares the energy efficiency of different 6G security methods. Due to its intensive computations, AI-based PLS is power-intensive. Though existing methods does possess moderate power efficiency, it requires optimization to be implemented on a large scale. QES-VLC is the most power-efficient solution for secure 6G communication with the lowest power consumption.

$$p_{aq} = [s - rw''] * vx[a - yw''] + rw[s - o'] \quad (15)$$

The security factor p_{aq} is modeled in Equation (15) according to interference reduction $[s - rw'']$, beam shaping weight $vx[a - yw'']$, and terms linked to encryption $rw[s - o']$. By reducing the impact of outside security risks and guaranteeing stable, high-speed connectivity, it improves 6G networks' ability to analysis of power consumption.

Table:3 Comparison of Existing with Proposed method

Performance Metric	PLS-5G	QoSec-Based PLS	WBPLSec	PLS	Proposed QES-VLC
Bit Error Rate (BER) ($\times 10^{-3}$)	28.5	21.2	19.7	17.1	15.7
Secrecy Capacity (bps/Hz)	58.9	48.4	51.5	82.7	98.2
Eavesdropping Resistance (%)	80.7	85.4	88.2	90.8	99.5
Secure Key Exchange Efficiency (%)	70.5	75.2	78.5	82.1	97.3
System Latency (ms)	82.8	65.4	58.9	49.4	28.3
Power Consumption (W)	54.4	41.2	32.8	30.5	18.9

The ideal option for 6G network security solutions is the suggested QES-VLC because it considerably improves upon current methods in terms of efficiency, energy consumption, and security.

In summary, QES-VLC performs the best among all methods in all categories: best secrecy capacity, minimum BER, maximum key exchange efficiency, minimum latency, and most efficient power consumption. It is the leader for future network security deployments due to the fact that it has the most efficient and secure 6G communication infrastructure.

5. CONCLUSION

Quantum-Enhanced Secure Visible Light Communication (QES-VLC) is a hybrid communication framework that combines the spatial confinement of Visible Light Communication (VLC) with the cryptographic robustness of quantum key distribution (QKD). Its goal was to improve the physical layer security of 6G wireless systems. The primary objectives were to demonstrate secure transmission in dense wireless environments, enhance secrecy capacity, and reduce eavesdropping vulnerability. By conducting thorough simulations and performance evaluations, QES-VLC was able to outperform both conventional and RF-based VLC security methods in terms of signal integrity, bit error rates in hostile situations, and secrecy metrics. Through the process of investigating the function of VLC integration in 6G networks with the objective of improving PLS, this study has addressed the limitations of conventional RF-based security approaches. With the help of adaptive beamforming and QKD support, the proposed QES-VLC system has proven that it can enhance data security, decrease the risk of interception, and provide smooth handoffs across VLC-RF hybrid networks. Simulation results showing great secrecy potential, reduced bit error rate (BER), and resilience to eavesdropping support this approach. We still have challenges to go even if we have progressed much. Dealing with the following problems calls for further optimization: VLC sensitivity to ambient interference light, VLC limited transmission range, and hybrid VLC-RF network difficulty of integration.

Several limitations and risks to validity must be acknowledged despite the encouraging outcomes. To start, VLC's scalability in the real world may be affected by its need for a line-of-sight connection, which may not work well in dynamic or obstructed surroundings. Quantum key distribution, when integrated, adds complexity to hardware and synchronization, which might lead to latency and cost increases in the system. Environmental variables, such as ambient light interference, mobility, and noise, were not fully considered in real-world situations, as the assessment was conducted under simulated conditions using idealized channel models. The data may not apply to a broader population due to these reasons. Lastly, adversaries with quantum capabilities and cyber-physical attack vectors that are continually developing pose future hazards that necessitate constant system adaptation.

Future studies should focus on developing dynamic beamforming driven by artificial intelligence, energy-saving security processes, and advanced noise reduction techniques to enhance VLC-based security frameworks. If Terahertz (THz) transmission and blockchain technology were to merge for distributed authentication, 6G might be even more secure. Extensive experimental testing is required before real-world applications, such as smart city infrastructure, industrial automation, and secure vehicle-to-vehicle (V2V) communication, can be implemented. Eliminating these challenges would open the path for ultra-secure, high-speed wireless networks, thereby ensuring robust data security right up to and including the 6G era.

REFERENCES:

[1]. Mucchi, L., Jayousi, S., Caputo, S., Panayirci, E., Shahabuddin, S., Bechtold, J., ... & Haas, H. (2021). Physical-layer security in 6G networks. *IEEE Open Journal of the Communications Society*, *2*, 1901-1914.

[2]. Mitev, M., Chorti, A., Poor, H. V., & Fettweis, G. P. (2023). What physical layer security can do for 6G security. *IEEE Open Journal of Vehicular Technology*, *4*, 375-388.

[3]. Nguyen, V. L., Lin, P. C., Cheng, B. C., Hwang, R. H., & Lin, Y. D. (2021). Security and privacy for 6G: A survey on prospective technologies and challenges. *IEEE Communications Surveys & Tutorials*, *23*(4), 2384-2428.

[4]. Abdel Hakeem, S. A., Hussein, H. H., & Kim, H. (2022). Security requirements and challenges of 6G technologies and applications. *Sensors*, *22*(5), 1969.

[5]. Lu, X., Xiao, L., Li, P., Ji, X., Xu, C., Yu, S., & Zhuang, W. (2022). Reinforcement learning-based physical cross-layer security and privacy in 6G. *IEEE Communications Surveys & Tutorials*, *25*(1), 425-466.

[6]. Melki, R., Noura, H. N., & Chehab, A. (2021). Physical layer security for NOMA: Limitations, issues, and recommendations. *Annals of Telecommunications*, *76*(5), 375-397.

[7]. Sanenga, A., Mapunda, G. A., Jacob, T. M. L., Marata, L., Basutli, B., & Chuma, J. M. (2020). An overview of key technologies in physical layer security. *Entropy*, *22*(11), 1261.

[8]. Ylianttila, M., Kantola, R., Gurtov, A., Mucchi, L., Oppermann, I., Yan, Z., ... & Röning, J. (2020). 6G white paper: Research challenges for trust, security and privacy. *arXiv preprint arXiv:2004.11665*.

[9]. Soderi, S. (2020, March). Enhancing security in 6G visible light communications. In *2020 2nd 6G wireless summit (6G SUMMIT)* (pp. 1-5). IEEE.

[10]. Arfaoui, M. A., Soltani, M. D., Tavakkolnia, I., Ghrayeb, A., Safari, M., Assi, C. M., & Haas, H. (2020). Physical layer security for visible light communication systems: A survey. *IEEE Communications Surveys & Tutorials*, *22*(3), 1887-1908.

[11]. Chi, N., Zhou, Y., Wei, Y., & Hu, F. (2020). Visible light communication in 6G: Advances, challenges, and prospects. *IEEE Vehicular Technology Magazine*, *15*(4), 93-102.

[12]. Naser, S., Bariah, L., Muhaidat, S., Sofotasios, P. C., Al-Qutayri, M., Damiani, E., & Debbah, M. (2022). Toward federated-learning-enabled visible light communication in 6G systems. *IEEE Wireless Communications*, *29*(1), 48-56.

[13]. Niarchou, E., Boucouvalas, A. C., Ghassemlooy, Z., Alves, L. N., & Zvanovec, S. (2021, November). Visible light communications for 6G wireless networks. In *2021 Third south american colloquium on visible light communications (SACVLC)* (pp. 01-06). IEEE.

[14]. Yesilkaya, A., Cogalan, T., Erkucuk, S., Sadi, Y., Panayirci, E., Haas, H., & Poor, H. V. (2020, March). Physical-layer security in visible light communications. In 2020 2nd 6G Wireless Summit (6G SUMMIT) (pp. 1-5). IEEE.

[15]. Irram, F., Ali, M., Naeem, M., & Mumtaz, S. (2022). Physical layer security for beyond 5G/6G networks: Emerging technologies and future directions. *Journal of Network and Computer Applications*, *206*, 103431.

[16]. Chorti, A., Barreto, A. N., Köpsell, S., Zoli, M., Chafii, M., Sehier, P., ... & Poor, H. V. (2022). Context-aware security for 6G wireless: The role of physical layer security. *IEEE Communications Standards Magazine*, *6*(1), 102-108.

[17]. Soderi, S., & De Nicola, R. (2021). 6G networks physical layer security using RGB visible light communications. *IEEE Access*, *10*, 5482-5496.

[18]. Gupta, A., & Fernando, X. (2021, June). Exploring secure visible light communication in next-generation (6G) internet-of-things. In 2021 International wireless communications and mobile computing (IWCMC) (pp. 2090-2097). IEEE.

[19]. Arfaoui, M. A., Soltani, M. D., Tavakkolnia, I., Ghrayeb, A., Safari, M., Assi, C. M., & Haas, H. (2020). Physical layer security for visible light communication systems: A survey. IEEE Communications Surveys & Tutorials, 22(3), 1887-1908.

[20]. Kazmi, S. H. A., Hassan, R., Qamar, F., Nisar, K., & Ibrahim, A. A. A. (2023). Security concepts in emerging 6G communication: Threats, countermeasures, authentication techniques and research directions. Symmetry, 15(6), 1147.

[21]. https://www.kaggle.com/datasets/ziya07/wireless-network-slicing-dataset