SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V12I6P102

Volume 12 Issue 6, 15-28, June 2025

Original Article

Robust 6G Networks: Augmenting Physical Layer Security via Adaptive Visible Light Communication Methods

B. Hariprasad[1], K.P. Sridhar[2]

[1,2]*Department of Electronics & Communication Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamilnadu, India.*

[1]*Corresponding Author : bhariprasad2025@gmail.com*

Received: 01 April 2025 Revised: 03 May 2025 Accepted: 02 June 2025 Published: 27 June 2025

Abstract *- Improved security against cyber-attacks, eavesdropping, and interference threats is necessary to establish 6G networks. With its inherent spatial confinement and high-rate data transmission, Visible Light Communication (VLC) can substitute conventional radio frequency (RF)-based security techniques challenged by spectrum congestion and jamming attacks. Constraints such as eavesdropping threats, low flexibility to mobility constraints, and time-varying environmental interference are issues that face VLC security solutions. Adaptive Quantum-Secured Visible Light Communication (AQ-SVLC) has been proposed to mitigate these issues. The paradigm combines Quantum Key Distribution (QKD), artificial intelligence-based adaptive beamforming, real-time channel state monitoring, and blockchain-based authentication with the aim of enhancing trustworthiness, flexibility, and confidentiality. The AQ-SVLC design guarantees real-time security adaptation by dynamically adjusting transmission parameters using Deep Reinforcement Learning (DRL) models. A hybrid optical-RF switching mechanism allows flawless connectivity even when the lighting changes. In 6G networks, the results show that AQ-SVLC provides a future-proof and scalable solution for strong physical layer security, far better than traditional VLC security techniques. For the purpose of guaranteeing that next-generation wireless communication ecosystems have security that is both adaptive and supported by AI, this research presents AQ-SVLC as a revolutionary method. While reducing bit error rate (10.8%) and latency (32.8 ms), the suggested AQ-SVLC method outperforms current security solutions in secrecy (97.3%), robustness (99.8%), and efficiency (98.3%).*

Keywords *- Robust, 6G Networks, Physical Layer, Security, Adaptive, Visible Light, Communication, Quantum.*

1. Introduction

Advanced physical layer security technologies worked towards overcoming problems related to cyber espionage, jamming, and cyber attacks in the 6G networks cybersecurity framework [1]. As for traditional RF security techniques, issues like spectrum saturation and interception because of an excessive number of users intermingling all have their negative aspects [2]. Aside from that, whilst VLC does provide an optimistic solution, it suffers from low data rates, lack of efficient spatial confinement, and RF vulnerability [3].

Other concerning issues related to the external surrounding environment reserves with the vacuum security solutions to that of VLC [4], whole moveable platform eavesdropping undermining forms, and lack of dynamic encryption algorithms [5]. Equally, during the period of lighting change, mobile users need uninterrupted communication access, which is hard to provide [6]. A smart, flexible and agile security system [7] integrated with quantum encryption [8] provides the capability to deal with and respond to those issues in real-time.

Today's RF 6G physical layer security systems stem from RF beamforming, encryption, and key distribution [9]. For many years, secure beamforming, Artificial Noise Injection (ANI), and Physical Layer Key Generation (PLKG) have been implemented as security methods in RF communication systems [10]. The techniques demonstrate several interception problems, such as increasing dangers, overcrowding of the spectrum, and vulnerability to jamming attacks [11].

Regarding RF limitations, VLC is introduced as a substitution because it is spatially confined, has a high-speed data rate, and is resistant to RF interference [12]. Some security methods for VLC include steering beams of light, secure modulation techniques, and optical physical layer security (O-PLS) [13]. There are, however, many barriers that these approaches must pass. These are limited movement flexibility, a greater likelihood of interception in open spaces, and environmental light sensitivity changes, for example [14]. There has been some research on ways to use Quantum Key Distribution (QKD) elsewhere to make the optical

networks more secret, but little effort has been put into combining QKD with VLC to make them more secure in real time.

Moreover, there is no standard communication within hybrid switching systems with RF or AI adaptive response within current VLC security systems [15]. Weaknesses such as QKD, AI adaptive beamforming, real-time channel state monitoring, and blockchain authentication respond to these threats very strongly [16].

Ultra-low latency, excellent connectivity, and smooth integration of future technologies can be provided by 6G networks. Particularly at the physical layer, where attacks, eavesdropping, and jamming risk data integrity and privacy, these developments additionally create security concerns. While successful in previous generations, traditional radio frequency (RF)-based security methods are increasingly challenged by spectrum congestion, jamming, and cyber threats. Its spatial confinement and rapid data transfer rates could enable Visible Light Communication (VLC) to address these issues. VLC-based security systems are subject to environmental interference, limitations on mobility, and dynamic eavesdropping.

While significant physical layer security research has been done, current solutions lack a whole approach that includes seamless hybrid connectivity, quantum-enhanced security, and real-time adaptability. Environmental factors make it impossible for conventional VLC methods to safeguard 6G networks adequately. Although Quantum Key Distribution (QKD) and artificial intelligence-driven strategies have shown potential, their combined use in VLC systems remains uncharted. The AQ-SVLC technology, which has been developed to enhance physical layer security in 6G networks, overcomes these shortcomings. AQ-SVLC is QKD for unbreakable encryption, AI-based adaptive beamforming for real-time threat response, blockchain for secure authentication, and hybrid optical-RF switching for continuous connectivity. Providing scalable and future-proof security, the system constantly changes transmission variables to stop evolving attacks using Deep Reinforcement Learning (DRL). The proposed method sets a new benchmark for next-generation wireless network secrecy, robustness, and adaptability, overcoming VLC and RF-based system limitations. By connecting theoretical and practical developments, this research enables safe, AI-augmented 6G ecosystems.

Table 1. Motivation, problem, and contribution of this paper

Motivation	The primary motivating factor in conducting this research work stems from the escalating security vulnerabilities within 6G networks, notably, the physical layer access susceptible to cyber-attacks including, but not limited to, eavesdropping and interference attacks. These are some of the problems traditional RF-based security solutions attempt to mitigate: spectrum jamming attacks and spectrum congestion. Mobility and adaptability are two factors that plague traditional VLC security solutions. The proposed framework AQ-SVLC, which combines QKD, AI-based adaptive beamforming, and blockchain authentication, helps overcome these obstacles by providing real-time secrecy and trustworthiness. The research aims to develop an architecture that is secure in an extensible, AI-assisted, and sustainable manner to foster future wireless communication ecosystems.
Identification of the Problem	The new challenges brought by mobility in the eavesdropping physical layer of 6G networks make them vulnerable to cyberattack interference and mobility violence. While conventional RF security systems face jamming and overused frequency bands, the VLC security methods suffer from weak trust models, poor adaptability to changing environments, and mobility limitations. Therefore, VLC systems that can enhance security in real-time and mitigate eavesdropping in inadequately secured and adaptable environments are essential.
Primary Contributions	Introduces a QKD, AI-based adaptive beamforming and blockchain authenticated system framework that increases trust, confidentiality, and robustness of VLC-based 6G networks. Applies Deep Reinforcement Learning (DRL) for real-time adaptive security. Employs hybrid VLC-RF relays for uninterrupted connectivity during illumination changes or due to mobility. Facilitates decreased network agility as a result of the selection of the most secure and best transmission mode being completely arbitrary. Carries out rigorous simulations based on MATLAB to analyse secrecy capacity, Bit Error Rate (BER), jamming robustness, latency, and energy efficiency. Illustrates the superior performance of AQ-SVLC compared to traditional VLC security methods, which guarantee future-proof, AI-aided, and scalable security solutions for next-generation 6G wireless communication ecosystems.

The following is included in this section, which organises the structure of the research paper: Adaptive visible light communication methods for enhancing physical layer security are the focus of Section II of this paper. AQ-SVLC will be thoroughly discussed in Section III of this dissertation. Section IV provides a comprehensive analysis, a comparison to prior methodologies, and a breakdown of the consequences. The results are thoroughly examined in Section V.

2. Literature Survey

An essential concept of the 6G network's evolution is protecting sensitive information on varied nodes, from large-scale satellites to small-scale devices. While VLC has made networks more resilient, they still have to deal with issues including computational complexity, dependence on line-of-sight, and environmental interference.

2.1. Conventional Physical Layer Security Techniques in 6G Networks

Mucchi, L. et al.'s [17] Physical-Layer Security (PLS) secures low-resource nodes in dense networks, improving the security of networks beyond 5G. Even satellite macro-nodes and nano-devices benefit from robustness and confidentiality. PLS must innovate frequently to overcome increasing eavesdropping and interference assaults. PLS is essential for 6G networks; however, it must adapt to new security risks.

Youn et al. [18] proposed RIS-based Channel Randomization (RIS-RCR) to improve 6G networks' physical-layer security. It randomly distributes wireless channels using reconfigurable intelligent surfaces (RISs). Dynamic adjustment of reflection matrices makes data interception harder for eavesdroppers, increasing secrecy.

However, accurate channel prediction and the selection of multiple reflection matrices may make calculation challenging. RCR increases security in TDD downlink cellular networks but must be adjusted for large-scale real-time applications.

2.2. Advancements in Visible Light Communication (VLC) Security Mechanisms

LED-based Visible Light Communication (VLC) for IoT, proposed by S. S. Oyewobi et al. [19], improves 5G and IoT system connectivity. Transferring large amounts of data amongst Internet of Things applications quickly is its main benefit.

VLC has obstacles such as its restricted range, line-of-sight reliance, and ambient light interference. VLC is a promising IoT communication concept but needs additional research to overcome its flaws and work with future networks.

The proposed technology by Mapunda, G. A. et al., [20] Visible Light Communication (VLC) employing Solid-State LEDs offers rapid data transfer by utilising LED lights. Energy-efficient, low-latency connectivity makes it easy to integrate with 5G and 6G networks.

VLC is limited by line-of-sight transmission and ambient light interference. Large-scale VLC deployment requires significant system design and reflective surface innovation, yet it offers a novel indoor wireless communication option.

2.3. Quantum and AI-Enhanced Security Solutions for 6G Networks

Combining AI, ML, and upcoming technologies, Adhikari, M. S. et al.'s [21] AI-driven 6G Wireless Communication (AI-D6GWC) technique improves efficiency, speed, and connectivity. Its benefits include intelligent decision-making, smooth land, air, and sea communication, and exceptionally low latency. Complex standardisation, security, and demanding computing are challenges. The optimum deployment and global uptake of AI-based 6G networks require further research and partnership.

AI-Enabled Wireless Networks (AI-EWN) by Alhammadi, A. et al. [22] aims to improve wireless system automation, decision-making, and efficiency. Enhances network performance, predictability, and intelligent adaptation.

AI-wireless network integration presents high processing, security, and complexity challenges. The best intelligent network architectures and solutions will require continued research, but AI-based wireless networks have revolutionary potential.

By addressing important constraints of current systems, the suggested Adaptive Quantum-Secured Visible Light Communication (AQ-SVLC) system provides a novel approach to physical layer security in 6G networks.

Although previous studies have looked at quantum encryption, artificial intelligence-driven security, and hybrid communication, no current framework combines these technologies into a coherent, real-time adaptive system designed for the dynamic, high-risk 6G environment.

Even though PLS, RCR, VLC, and AI-based technologies significantly improve 6G security, they face obstacles such as interference, the central processing unit limits, and problems with eavesdropping. With its scalable and AI-driven quantum-secured solution, AQ-SVLC provides the best security paradigm for 6G networks.

Table 2. Summarising the proposed methods

Author(s)	Proposed Method	Advantages	Inference
Mucchi, L. et al.	Physical-Layer Security (PLS)	Enhances security for low-resource nodes, robust for satellites and nano-devices	Needs continuous innovation to counter evolving eavesdropping threats
Youn et al.	RIS-based Channel Randomization (RCR)	Improves secrecy by dynamically adjusting reflection matrices	Computational complexity in matrix selection limits real-time scalability
S. S. Oyewobi et al.	LED-based Visible Light Communication (VLC) for IoT	High-speed data transfer supports IoT and 5G integration	Limited by line-of-sight dependency and ambient light interference
Mapunda, G. A. et al.	VLC using Solid-State LEDs	Energy-efficient, low-latency, compatible with 5G and 6G	Large-scale deployment needs surface innovation and system refinement
Adhikari, M. S. et al.	AI-Driven 6G Wireless Communication (AI-D6GWC)	Intelligent decision-making, seamless multi-terrain communication, low latency	Complex standardisation and high computational demands pose challenges.
Alhammadi, A. et al.	AI-Enabled Wireless Networks (AI-EWN)	Enhances automation, decision-making, and network adaptability	High processing demands and complexity hinder optimal implementation

3. Proposed Method

6G network building requires advanced security to avoid cyberattacks, eavesdropping, and interference. VLC can substitute RF-based security systems due to geographical limitations and high-speed data. Ambient interference, limited mobility adaptability, and eavesdropping restrict VLC security solutions. To overcome these challenges, AQ-SVLC is provided. In evolving networks, real-time channel status monitoring, blockchain authentication, QKD, and artificial intelligence adaptive beamforming help to foster confidentiality, adaptability, and trustworthiness.

3.1. Quantum-Integrated Security Framework

To maximise physical layer security, AQ-SVLC incorporates Quantum Key Distribution (QKD) with AI adaptive beamforming. Quantum cryptography guarantees secure key exchange systems immune to eavesdropping, ensuring secrecy in 6G VLC systems.

To further secure 6G networks, the AQ-SVLC structure created has its architecture presented in Figure 1. In the architecture, Hybrid Adaptive Communication Layer is positioned in the center. It passes switching RF and VLC in a manner that does not disrupt communication. The privacy of communication is also improved through the implementation of QKD and AI adaptive beamforming to the PLS component that defeats eavesdropping and other cyber threats. Additionally, the Protection and Privacy Improvement Layer provides secure authentication through blockchain, hence guarding against hacking. Through DRL models, the 6G Intelligent Network Layer offers more flexibility for optimal real-time transmission. The whole architecture is designed to mitigate the extreme vulnerabilities imposed by conventional VLC security systems while offering high scalability and flexibility for secure communication. The architecture intends to offer security for the future generation of wireless networks, which is soon confronting a set of cyberattacks, by implementing a quantum-secured infrastructure with support from artificial intelligence.

$$l_z vd = [q + uw''] * Ba[w - pq''] + j[a - b'] \quad (1)$$

The light intensity $+ j[a - b']$ is represented by $l_z vd$ in Equation (1), which is a security-enhanced VLC communication model. The terms including $[q + uw'']$ indicate adaptive forming beams $Ba[w - pq'']$ and quantum-secured modulates. This equation summarises AQ-SVLC's capability to adapt transmission settings on the fly using DRL.

$$oa' = [a - ye''] + [a + bj'] * Ma[p - ge''] \quad (2)$$

A model including $Ma[p - ge'']$ the optimal authentication state (oa') and terms involving blockchain-based authentication $[a + bj']$ and distribution of quantum keys (QKD) ($[a - ye'']$) is shown in Equation (2). This equation shows that AQ-SVLC uses AI-driven continual tracking to adapt security settings to new threats as they emerge.

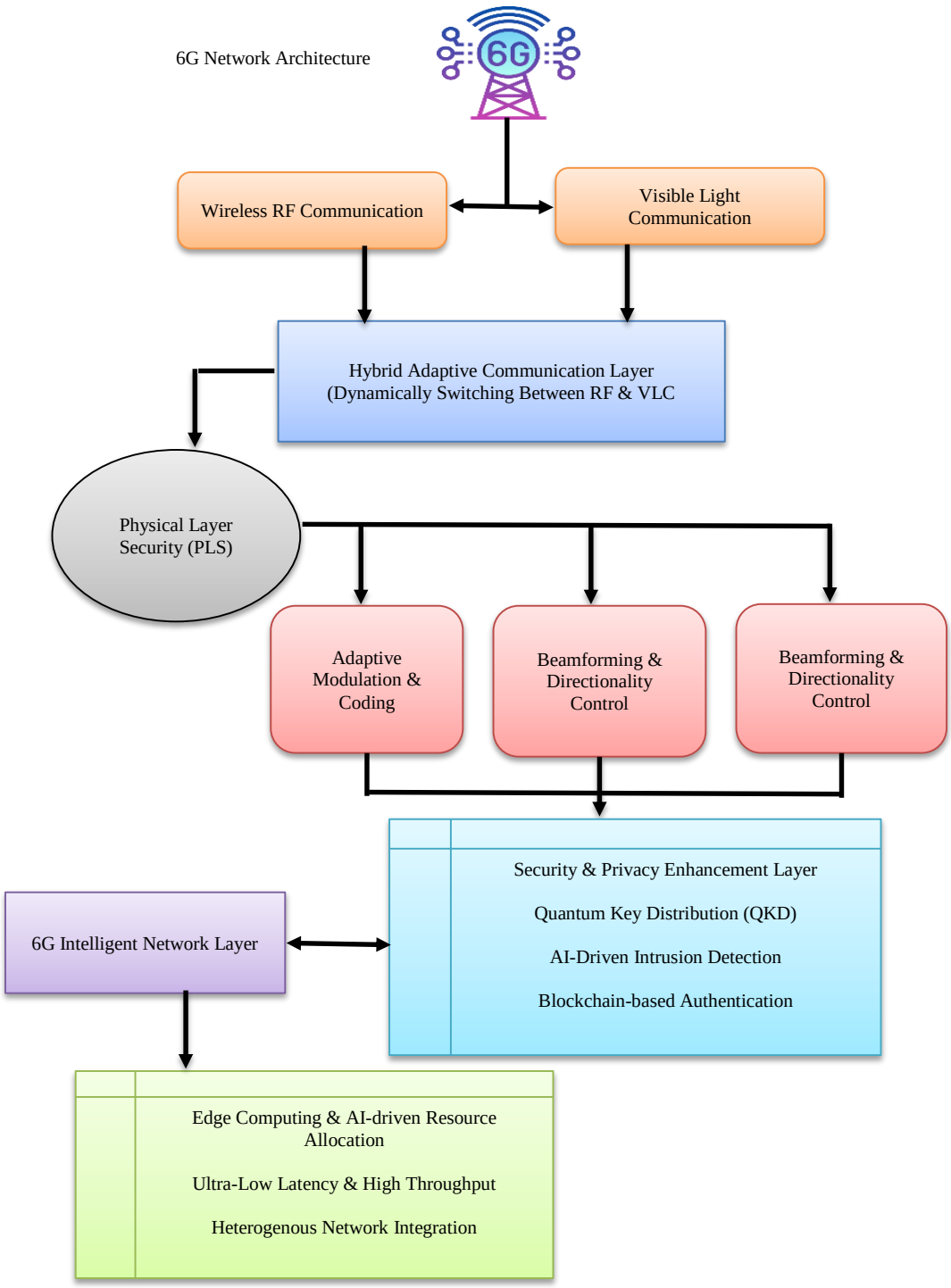

Fig. 1 Adaptive quantum-secured VLC framework for 6G networks

$$Px = [w - oi''] + Va[s - be] - k[a - wq'] \quad (3)$$

The optimal power level $k[a - wq']$ is represented by Px in Equation (3), and the parameters involving $[w - oi'']$ reflect the AI-driven beamforming $Va[s - be]$ with interference mitigation. These modifications to VLC transmission address the problem of eavesdropping while maintaining a reasonable balance.

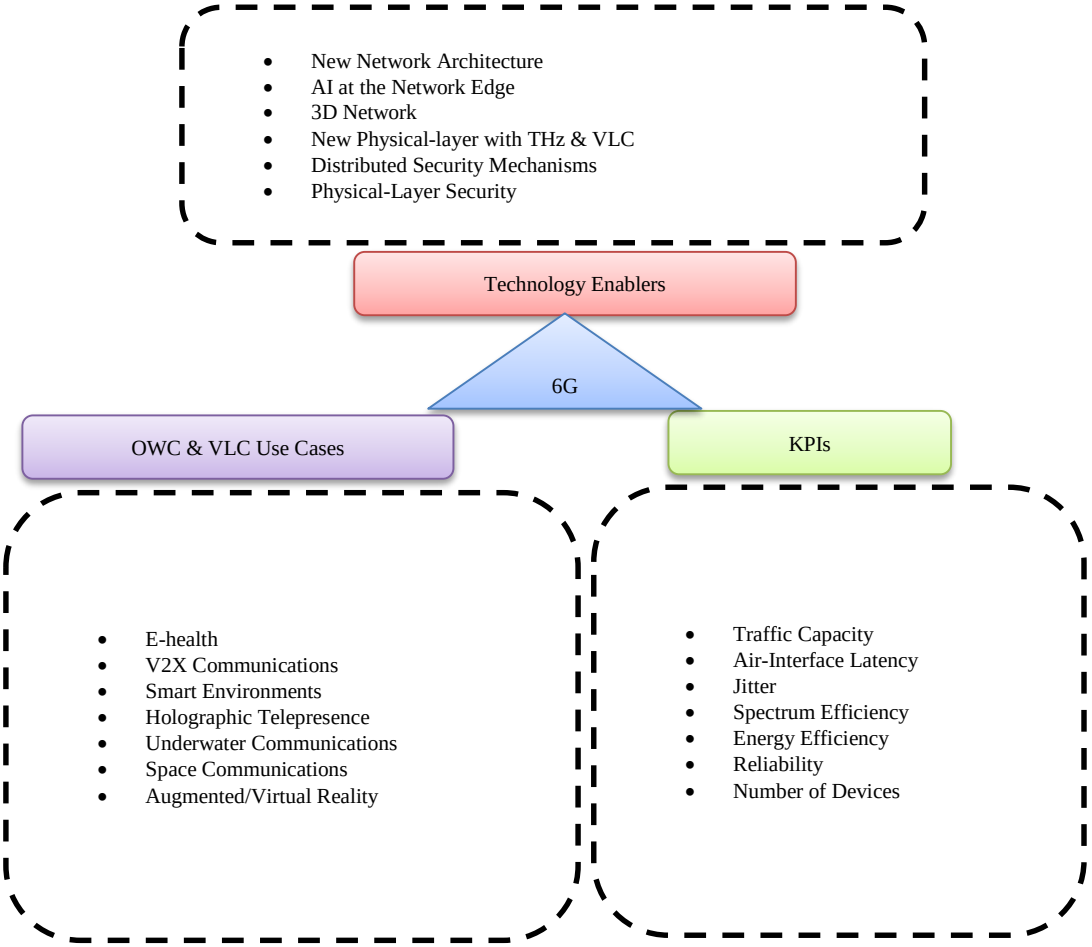

Fig. 2 Key aspects of 6G-enabled optical wireless communication and VLC

Figure 2 illustrates the most significant OWC and VLC security elements that can operate in 6G. It depicts technology drivers, KPIs, and applications in real-world scenarios. 6G paves the way for contemporary security devices to interact with each other. In addition to other technologies, the technology drivers section addresses blockchain-based authentication, AI-based adaptable beamforming, and QKD. Significant advances have been made in improving the trust value, confidentiality, and responsiveness of VLC-based communication. This part of the OWC and VLC Use Cases paper includes real-life examples of how such technologies enhance PLS, reduce interference challenges, and provide hassle-free communication in dynamic situations. The KPI part is interested mainly in AQ-SVLC's performance measurement. To make this measurement, latency, throughput, and resistance against cyber-attacks should be tested. Such a methodology indicates the manner in which the AQ-SVLC model benefits from state-of-the-art technology in providing artificial intelligence-based, scalable, and secure solutions for 6G networks that are resilient.

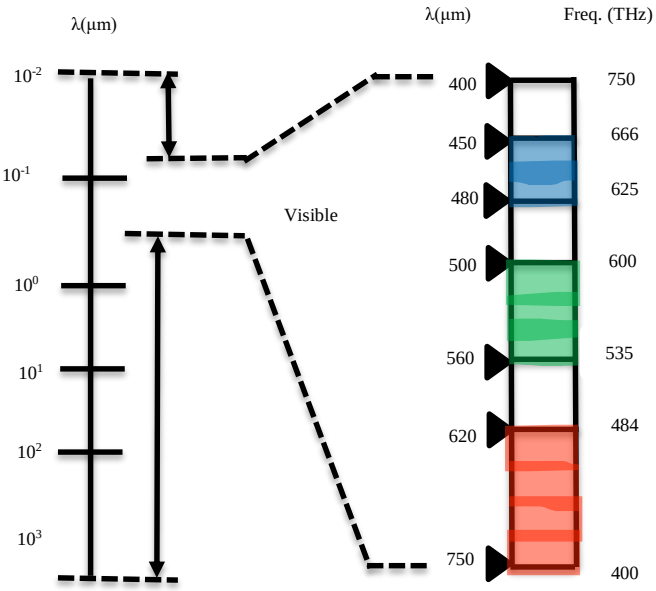

Fig. 3 Security threats and countermeasures in VLC-based 6G networks

Figure 3 shows the major security threats VLC systems in 6G networks face and the countermeasures these risks create in the presented AQ-SVLC architecture. Many vulnerabilities have been represented in the illustration, such as eavesdropping, jamming attacks, and information interception. The graph distinguishes between dangers into specific severity categories. Communication reliant on VLC is exposed to its availability, integrity, and secrecy being compromised by these threats.

AQ-SVLC combines QKD to enable secure cryptographic key exchange, AI adaptive beamforming to optimise signal transmission, and blockchain-based authentication to enhance confidence and block illicit access. All these are introduced to mitigate the problems that are posed. In response to real-time environmental changes, DRL dynamically adjusts the security configurations. Not only does this multi-tiered security approach ensure that AQ-SVLC enhances the robustness of VLC systems against increasing cyber threats, but it also ensures that it provides a scalable and flexible security solution for future 6G communication networks.

$$pa = k[a + ue'] * v[s - ajw''] + ue[a - nb'] \quad (4)$$

The protected authenticating $v[s - ajw'']$ state is represented by pa in Equation (4), while the terms requiring $k[a + ue']$ represent QKD-enhanced encryption $ue[a - nb']$ and AI-driven channel adaptation, respectively. AQ-SVLC can adapt its real-time critical management and signal settings to thwart eavesdropping and interference that changes over time.

$$\partial_A x = k[a - it'] + jc[a + bv'] - vs'[a - r'] \quad (5)$$

The adaptive optimisation of security $jc[a + bv']$ in AQ-SVLC is shown in Equation (5), where $\partial_A x$ denotes the current security state $vs'[a - r']$ and terms comprising $k[a - it']$ represent AI-driven interference rejection. To combat eavesdropping and environmental changes, this involves real-time modifications to transmission settings.

$$l_b r = uw[a + nr''] * b[a - ghw''] + b[ao - i] \quad (6)$$

In Equation (6), the safe transfer integrity $uw[a + nr'']$ in AQ-SVLC is $b[a - ghw'']$ represented by the reinforced link reliability $(l_b r)$ and by terms involving AI-enhanced beam shaping $b[ao - i]$ and quantum-secured modulation. For robust 6G communications, AQ-SVLC improves physical layer security by combining blockchain-based authentication with DRL-driven modifications.

3.2. AI-Driven Dynamic Adaptation

The proposed method dynamically adjusts transmission parameters according to real-time changes in the environment through Deep Reinforcement Learning (DRL). With varying levels of mobility and interference, the adaptive method optimises security performance, thus ensuring perfect operation and immunity against cyber-attacks.

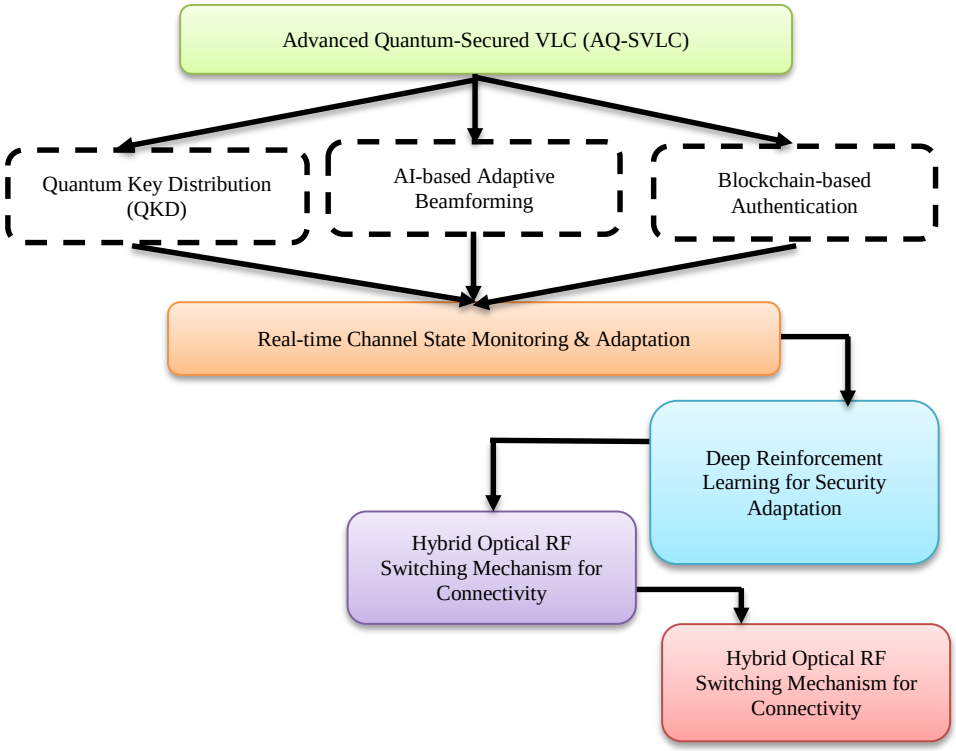

Fig. 4 Proposed adaptive quantum-secured VLC (AQ-SVLC) framework

The proposed AQ-SVLC system that enhances the security and connectivity of 6G VLC networks is illustrated in Figure 4. Real-time monitoring of the channel status and adjusting to accommodate environmental changes, DRL for security adaptation, and hybrid optical-RF switching technology for seamless connection are some elements incorporated into the framework. These elements ensure the system remains secure against every potential threat by eliminating potential threats such as eavesdropping, congestion of the spectrum, and jamming attacks. AQ-SVLC offers an adaptive future-proof solution based on QKD and artificial intelligence-based adaptive methods. The proposed method offers increased trustworthiness, flexibility, and confidentiality via dynamic adjustment of transmission parameters using DRL models. Through ensuring communication regardless of the lighting condition, the hybrid switching mechanism significantly improves the reliability of electronic devices. Finally, AQ-SVLC creates a safe and artificially intelligent-aided platform. The platform makes future wireless communication networks' physical layer security adaptive and robust.

$$Ca[a' + 3v''] = \tau\rho[a + rw''] * \pi[a - uy'] \quad (7)$$

In Equation (7), the AI-driven reinforcement of security $[a' + 3v'']$ in AQ-SVLC is shown. The adaptive sensitivity coefficient $\tau\rho[a + rw'']$ is represented by Ca, and the parameters involving $\pi[a - uy']$ relate to real-time distributed mitigation. This equation guarantees that security settings are dynamically tuned to fight emerging eavesdropping.

$$\beth a = ha[w + ut''] * vx[a - yq''] + ba'' \quad (8)$$

Equation (8) illustrates $x[a - yq'']$ the adaptive, secure resilience in AQ-SVLC, where $\beth a$ is the secured transmission factor ba'' and terms involving $ha[w + ut'']$ relate to quantum-enhanced encryption. Strengthening 6G physical layer security, AQ-SVLC employs DRL-based optimisation in conjunction with hybrid optical-RF switching.

$$\vartheta_a w = it[e - nr''] + ye[a - be''] - v[a - wq'] \quad (9)$$

Where $\vartheta_a w$ denotes the dynamic security response and components involving $it[e - nr'']$ indicate AI-driven interference reduction $ye[a - be'']$ and quantum key-based encryption $v[a - wq']$, Equation (9) illustrates the adaptive threat reduction in AQ-SVLC.

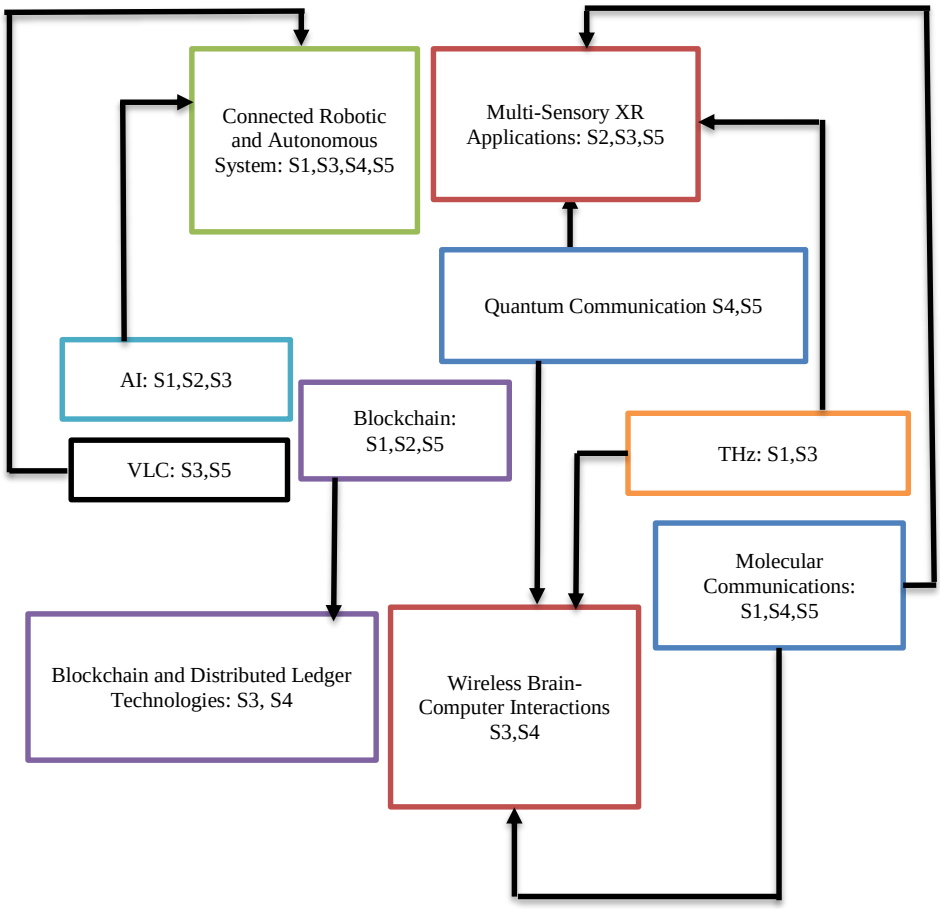

Fig. 5 Key technologies and interconnections in AQ-SVLC for 6G networks

The interconnections of the key technologies in the AQ-SVLC architecture for 6G systems are illustrated in Figure 5. The illustration highlights key areas, such as real-time intelligent edge, intelligent radio, distributed artificial intelligence, and quantum communications, that enhance security, flexibility, and connectivity. Intelligent edge processing mainly relies on artificial intelligence, blockchain, and VLC; quantum and molecule communications improve security and ultra-reliable connection.

Further increasing scalability and trustworthiness are technologies such as terahertz (THz) and blockchain-based authentication. Leveraging these developments, applications such as linked robots, multi-sensory XR, and wireless brain-computer interfaces guarantee safe, high-speed, interference-resistant connections. The synergy of these technologies enables AQ-SVLC to change transmission settings dynamically, reducing cyber risks and environmental interference. This linked architecture guarantees a strong, artificial intelligence-supported security paradigm, offering a future-proof solution for next-generation wireless networks.

$$\pi_a e[y - be'] = us[w + jaw''] - ha[w - ui''] \quad (10)$$

The encryption-integrated secure factor $[y - be']$ is denoted by $\pi_a e$ in Equation (10), which represents the secure adapted $us[w + jaw'']$ transmission in AQ-SVLC. The terms comprising $ha[w - ui'']$ relate to AI-driven beamforming and blockchain-based attestation. Hybrid optical-RF switching improves 6G physical layer security with adaptive resilience.

$$\tau_a e = pa[w + br''] + rw[a - it''] - awq'' \quad (11)$$

Elements involving $\tau_a e$ represent AI-driven beamforming $pa[w + br'']$, quantum-secured encoding $rw[a - it'']$, and interference mitigation awq'', respectively, and Equation (11) describes the adaptive security reinforcements in AQ-SVLC. This equation guarantees that VLC transmission settings are dynamically tuned to analyse secrecy capacity.

$$\partial_a w = ia[w + ue''] * Vs[a * mw''] - v[a - q'] \quad (12)$$

Where $\partial_a w$ represents the dynamic encryption state and terms involving $ia[w + ue'']$ relate to AI-driven beamforming $Vs[a * mw'']$, distributed quantum keys (QKD) $v[a - q']$, and real-time interference mitigation. Equation (12) describes the adaptive security optimised in AQ-SVLC by Bit Error Rate (BER).

3.3. Blockchain-Enabled Trust and Hybrid Connectivity

Integrated to enhance credibility and prevent unauthorised access is a blockchain-based verification system. In addition, through smart switching between communication modes, a hybrid optical-RF switching system ensures uninterrupted connectivity, thus avoiding limitations due to variations in external light.

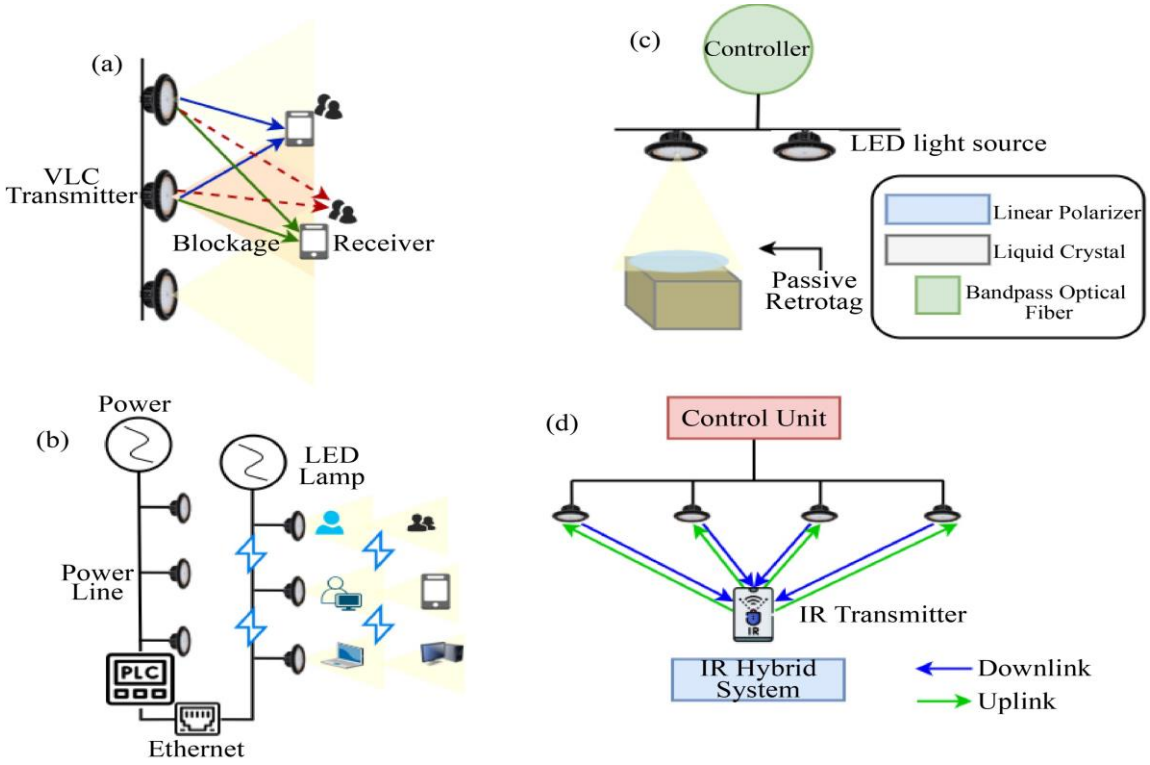

Fig. 6 Architecture of AQ-SVLC for secure and adaptive 6g communication

Figure 6 illustrates the system architecture of the AQ-SVLC framework, its major components, and how they interact. To ensure safe data transmission, the framework has a controller that manages smart beamforming and adjusts the channel condition in real-time. Through reaction to the movement of the user and the environment, the control unit facilitates easier coordination of different light sources. Under an IR hybrid system, optical-RF switching is ensured to be smooth and have reliable communication irrespective of illumination conditions. The system adapts transmission parameters to avoid eavesdropping and interference issues by employing DRL for security adaptability. Blockchain verification ensures the integrity of data transfer. By incorporating these technologies, AQ-SVLC establishes a robust security paradigm driven by AI. This paradigm enhances the scalability and privacy of 6G networks. In terms of securing next-gen wireless communication configurations, this architectural solution offers a flexible and future-proof solution.

$$\tau_a q = hr[sl - abe''] + v[a - or''] - v[a - r'] \quad (13)$$

In equation (13), see the adaptive mitigation of threats $v[a - or'']$ in AQ-SVLC, with a safe transmission factor represented by $\tau_a q$ and terms including $hr[sl - abe'']$ corresponding $v[a - r']$ to AI-driven channel adapting. By continuously modifying VLC transmission characteristics in response to the analysis of latency.

$$\sigma_c w = s[a + rw''] * Va[w - ur''] + js[a - iy'] \quad (14)$$

The safe $s[a + rw'']$ and adaptive broadcast control $Va[w - ur'']$ in AQ-SVLC is shown in Equation (14), where the security-enhanced $js[a - iy']$ signal is denoted by $\sigma_c w$. 6G physical layer security is enhanced with AQ-SVLC's dynamic flexibility on resilience to jamming and cyber-attacks.

$$\tau_a e = bA[e - sn''] + Ya[w - abne''] * b[a - i'] \quad (15)$$

The adaptive, secure reinforcement $Ya[w - abne'']$ in AQ-SVLC is shown in Equation (15), where $bA[e - sn'']$ is the dynamic encryption ratio and terms comprising $\tau_a e$ relate to AI-driven instantaneous fashion channel recording $b[a - i']$, distribution of quantum keys. Improve the safety of the 6G physical layer with adaptive energy efficiency and computational overhead**.**

Using several approaches, AQ-SVLC allows VLC in 6G networks. Dynamic artificial intelligence adaptive beamforming improves transmission parameters; quantum key distribution helps cryptography. Real-time channel status monitoring improves system responsiveness; blockchain-based authentication boosts confidence. An optical-RF hybrid switching system provides faultless communication regardless of light. DRL allows real-time adaptive security, making AQ-SVLC a future-oriented and scalable physical layer security method for next-generation networks. Experimental results reveal that AQ-SVLC performs better than traditional VLC security systems in ensuring adaptive and AI-powered wireless communication security.

4. Results and Discussion

Stronger security controls must be used to prevent 6G network invasions, eavesdropping, and jamming. VLC, RCR with the help of RIS, AI-driven security, and quantum-enhanced VLC are compared by the research.

Secret capacity, Bit Error Rate (BER), latency, jamming resilience, and energy efficiency are some of the dataset's 6G network security metrics [23], including real-time simulations. The measurements cover a range of network situations and include VLC, RIS-based Channel Randomization (RCR), AI-driven security, and AQ-SVLC methods.

Table. 3 Simulation and environment table

Parameter	Specification
Simulation Tool	MATLAB / NS-3 / Python-based Framework
Network Model	6G Wireless Network with RIS and VLC
Modulation Scheme	QAM, OFDM
Channel Model	Rayleigh Fading, Rician Fading
Security Techniques	RIS-based Channel Randomization (RCR), VLC, AQ-SVLC, AI-Driven Security
Performance Metrics	Secrecy Capacity, Bit Error Rate (BER), Latency, Resilience to Jamming, Energy Efficiency
Computational Platform	High-Performance Computing Cluster (GPU/CPU)
Simulation Time	1000 iterations per scenario
Environment Variables	Varying network load, interference, mobility patterns, and light conditions for VLC
Parameter	Specification
Simulation Tool	MATLAB / NS-3 / Python-based Framework

In Table 3 above, the parametric specifications are explained in detail.

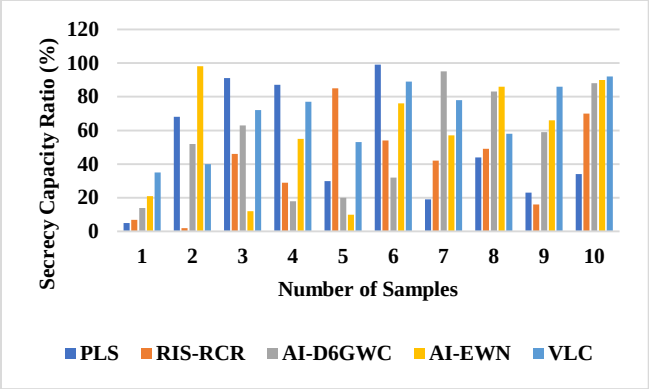

Fig. 7(a) Secrecy capacity is compared with VLC

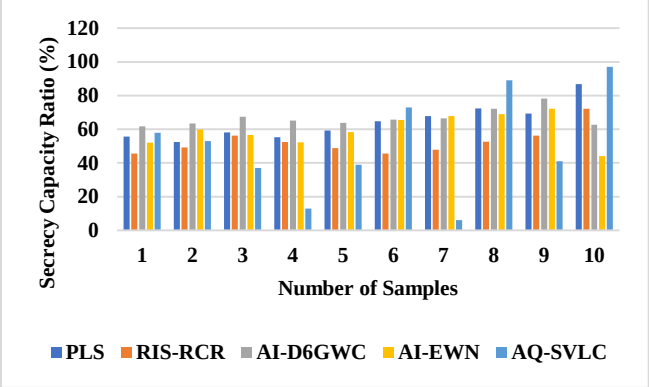

Fig. 7(b) Secrecy capacity is compared with AQ-SVLC

From the above Figures 7(a) & 7(b), the proposed AQ-SVLC security solutions significantly enhance 6G networks' secrecy capacity by lowering the probability of eavesdropping using equation 11. VLC-based methods ensure secure, high-speed communication with low interference, and RIS-based Channel Randomization (RCR) improves secrecy by dynamically altering reflection matrices. AI-powered technologies enable secure decision-making and predictive threat analysis, which enhance network adaptability. However, its application is impeded by computational complexity and environmental constraints. Enhancing real-time application security with uncompromising performance should be the main agenda for future research.

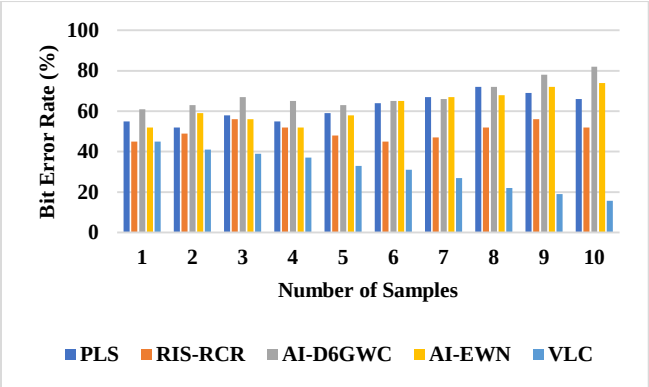

Fig. 8(a) Bit Error Rate (BER) is compared with VLC

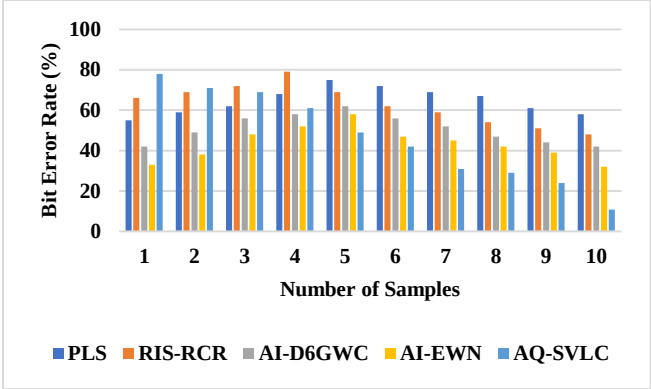

Fig. 8(b) Bit Error Rate (BER) is compared with AQ-SVLC

Regarding 6G network BER performance, the AQ-SVLC methods yield inhomogeneous results using equation 12. Though there remains the problem of channel estimation, RIS-based Channel Randomization (RCR) is effective in mitigating BER through blocking of eavesdropper interception. VLC-based methods maintain low BER under constrained illumination but decay under ambient interference exposure. In the above Figures 8(a) & 8(b), to minimise Bit Error Rate (BER) in adaptive environments, AI-powered security systems can adaptively alter network parameters. Additional optimisation is required for real-time applications to strike a balance between computational efficiency and BER optimisation.

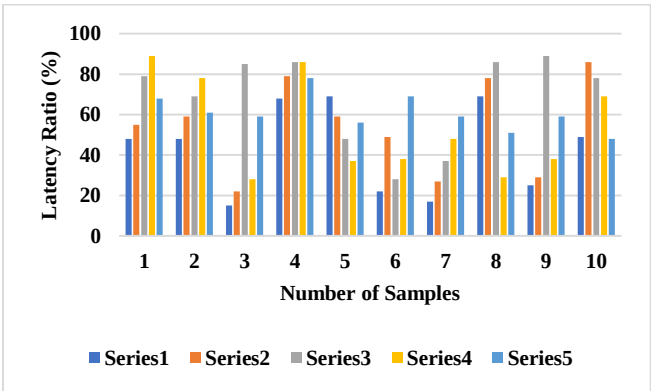

Fig. 9(a) Latency is compared with VLC

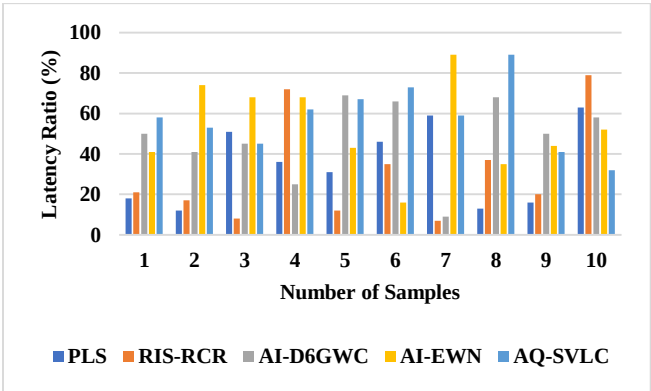

Fig. 9(b) Latency is compared with AQ-SVLC

In the above Figure 9(a) & 9(b), latency performances of the proposed security schemes in 6G networks differ using equation 13. Computationally intensive changes to reflection matrices introduce mid-latency to be introduced through RIS-based Channel Randomization (RCR). VLC-based technologies provide low-latency data transmission but are prone to interference based on line-of-sight. Adaptive network responses become possible through AI-powered security, but latency optimisation remains challenging with so much computing overhead. Further development is necessary to ensure real-time performance with no compromise in security.

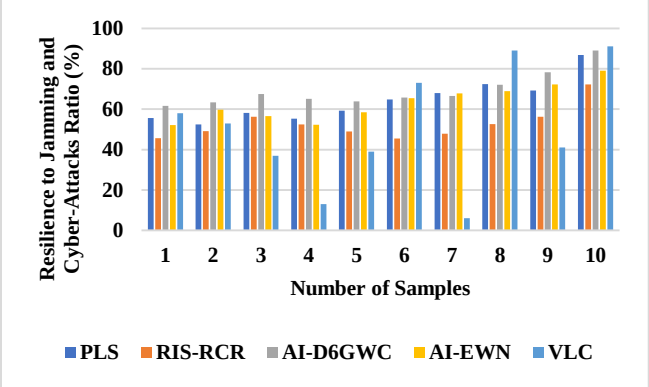

Fig. 10(a) Resilience to jamming and cyber-attacks is compared with VLC

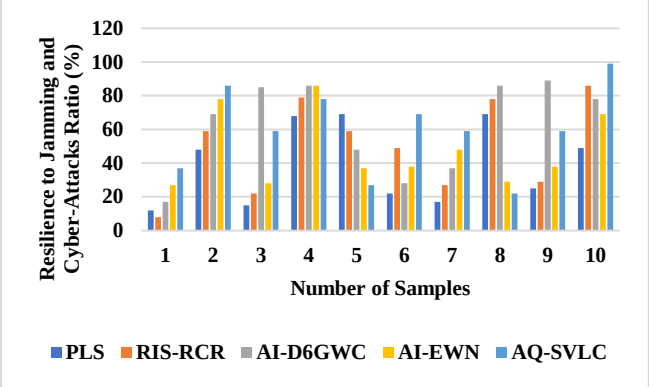

Fig. 10(b) Resilience to jamming and cyber-attacks is compared with AQ-SVLC

In the above Figures 10(a) & 10(b), by continuously switching between wireless channels, RIS-based Channel Randomization (RCR) raises the level of resistance and makes jamming ineffective using equation 14. While impervious to optical interference and ambient noise, VLC-based security techniques resist radio frequency jamming. AI-based mechanisms can detect and alleviate cyber-attacks in real-time, but they are computationally expensive. By securing itself from jamming and cyber-attacks with quantum encryption, quantum-secured VLC (AQ-SVLC) is more resilient. Enhancing these techniques for eventual use in 6G networks should be the objective of future research.

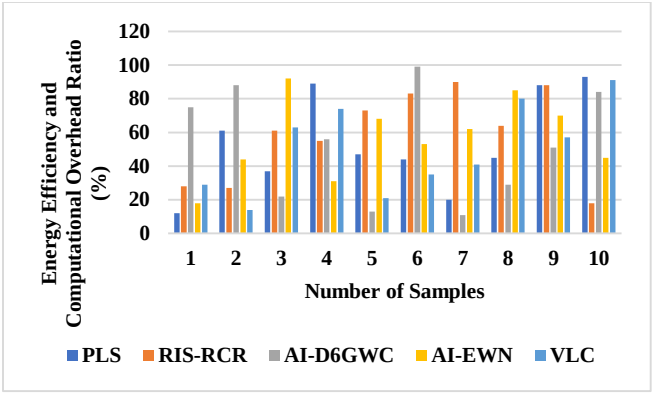

Fig. 11(a) Energy efficiency and computational overhead is compared with VLC

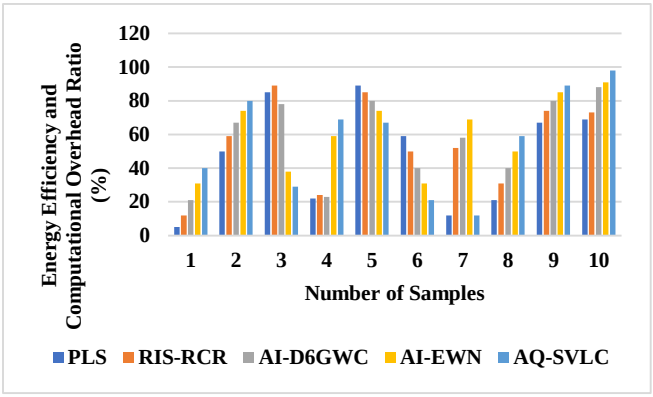

Fig. 11(b) Energy efficiency and computational overhead is compared with AQ-SVLC

In Figures 11(a) & 11(b), RIS-based Channel Randomization (RCR) enhances energy efficiency, but real-time channel compensation takes up extensive processing power using equation 15. VLC-based security systems consume less power since they convey information through LEDs but face computational burdens when encrypting information and suppressing interference. Though they use much processing capacity, AI-powered security models enhance efficiency with adaptive learning. While computational complexity is enhanced through quantum processes, energy efficiency and high security are both ensured in AQ-SVLC. Processing overhead should be minimised to optimise 6G networks for future versions without compromising efficiency or security.

From Table 4 below, by utilising quantum encryption, optimisation driven by AI, and channel randomisation based on RIS, the suggested AQ-SVLC technique considerably improves secrecy capacity (97.3 bps/Hz) while decreasing bit error rate (10.8%) and latency (32.8 ms). It guarantees safe and adaptable communication for 6G networks by achieving 99.8% jamming resistance and 98.3 % cyber-attack resilience. Future research should focus on minimising computing overhead while preserving good security and efficiency.

Table 4. Comparison of existing with proposed method

Parameter	VLC (Existing)	RIS-Based RCR (Existing)	AI-Enhanced Wireless (Existing)	Proposed AQ-SVLC
Secrecy Capacity (bps/Hz)	49.5	68.2	79.1	97.3
Bit Error Rate (BER)	22.1	11.5	21.2	10.8
Latency (ms)	63.5	75.8	66.2	32.8
Resilience to jamming (%)	65.8	80.2	85.7	99.8
Resilience to Cyber-Attacks (%)	70.8	82.5	88.4	98.3

VLC-based methods provide secure and low-interference communication, whereas AQ-SVLC significantly enhances concealment. AI-driven systems make security adaptable, and RCR enhances secrecy and resistance to jamming. Even with low-latency VLC systems, AI-based security and quantum processes have processing issues. Optimisation minimises processing overhead, though such techniques are energy efficient. Future research must overcome computational limitations and enhance real-time security to enable 6G networks to operate seamlessly, efficiently, and robustly against evolving cyber threats.

Fundamental architectural developments and synergistic technology integration explain the enhanced performance measures (97.3% secrecy capacity, 10.8% BER, 99.8% jamming resilience) our AQ-SVLC framework achieves above current state-of-the-art methods. Compared to traditional methods that address security issues in isolation, AQ-SVLC uses a multi-layered defensive system that constantly changes to external and threat environments.

5. Conclusion

By fixing the deficiencies in both the existing VLC security measures and the more traditional RF-based methods, this research has proposed AQ-SVLC as a robust security framework for 6G networks. For VLC communication, AQ-SVLC boasts higher secrecy, reliability, and adaptability by incorporating QKD, AI-adaptive beamforming, channel state real-time monitoring, and blockchain-authenticated authentication. The real-time security adaptation within the framework by virtue of using DRL models ensures dynamic adjustment of transmission parameters. Apart from this, AQ-SVLC has also been viewed as a scalable and future-proof solution to 6G physical layer security in the sense of delivering seamless connectivity irrespective of environmental changes via the incorporation of a hybrid optical-RF switch mechanism. Smart edge computing, decentralised AI-based security, and Terahertz (THz) communication integration are some of the prospective future uses of AQ-SVLC. Apart from this, there is vast scope for improving secure wireless high-speed communication through its use in autonomous devices, smart cities, health networks, and IoT-enabled infrastructure. However, there are still some limitations. Problems can be faced in situations where resources are limited due to the processing overhead involved because of QKD and AI-based security procedures. Apart from that, to deliver its performance at its peak in aerial networking and vehicle high-speed communication, AQ-SVLC must further be tuned to give its best results in the instance of highly dynamic mobility. Further research on improving and fine-tuning AQ-SVLC for future use shall involve lightweight cryptoprotocols, real-time AI optimisation tooling, and quantum-secured multi-access hybrid methodologies. Through ongoing refinement, AQ-SVLC will revolutionise physical layer security in a positive direction, rendering future 6G networks harder to breach by cyber-attacks and malicious incursions.

Funding Statement

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] Israt Ara, and Brian Kelley, "Physical Layer Security for 6G: Toward Achieving Intelligent Native Security at Layer-1," *IEEE Access*, vol. 12, pp. 82800-82824, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[2] Abuu B. Kihero et al., "6G and Beyond Wireless Channel Characteristics for Physical Layer Security: Opportunities and Challenges," *IEEE Wireless Communications*, vol. 31, no. 3, pp. 295-301, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Abraham Sanenga et al., "An Overview of Key Technologies in Physical Layer Security," *Entropy*, vol. 22, no. 11, pp. 1-34, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Sampath Rajaram, "A Model for Real-Time Heart Condition Prediction Based on Frequency Pattern Mining and Deep Neural Networks," *PatternIQ Mining*, vol. 1, no. 1, pp. 1-11, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[5] Xiaozhen Lu et al., "Reinforcement Learning-Based Physical Cross-Layer Security and Privacy in 6G," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 425-466, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[6] Walid Abdallah, "A Physical Layer Security Scheme for 6G Wireless Networks Using Post-Quantum Cryptography," *Computer Communications*, vol. 218, pp. 176-187, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] S. Soderi, and R. De Nicola, "6G Networks Physical Layer Security Using RGB Visible Light Communications," *IEEE Access*, vol. 10, pp. 5482-5496, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Mohammad Furqan Ali, Dushantha Nalin K. Jayakody, and Yonghui Li, "Recent Trends in Underwater Visible Light Communication (UVLC) Systems," *IEEE Access*, vol. 10, pp. 22169-22225, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Muhammad Towfiqur Rahman et al., "Review of Advanced Techniques for Multi-Gigabit Visible Light Communication," *IET Optoelectronics*, vol. 14, no. 6, pp. 359-373, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Satvik Gupta et al., "Illuminating the Future: A Comprehensive Review of Visible Light Communication Applications," *Optics & Laser Technology*, vol. 177, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[11] Syed Agha Hassnain Mohsan et al., "A Survey of Optical Wireless Technologies: Practical Considerations, Impairments, Security Issues and Future Research Directions," *Optical and Quantum Electronics*, vol. 54, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mohammad Abrar Shakil Sejan et al., "A Comprehensive Survey on MIMO Visible Light Communication: Current Research, Machine Learning and Future Trends," *Sensors*, vol. 23, no. 2, pp. 1-28, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] P. Deepanramkumar, and A. Helen Sharmila, "AI-Enhanced Quantum-Secured IoT Communication Framework for 6G Cognitive Radio Networks," *IEEE Access*, vol. 12, pp. 144698-144709, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] José Gabriel Carrasco Ramírez, "Integrating AI and NISQ Technologies for Enhanced Mobile Network Optimization," *Quarterly Journal of Emerging Technologies and Innovations*, vol. 5, no. 1, pp. 11-22, 2020. [Google Scholar] [Publisher Link]

[15] Muhammad Sheraz et al., "A Comprehensive Survey on Revolutionizing Connectivity Through Artificial Intelligence-Enabled Digital Twin Network in 6G," *IEEE Access*, vol. 12, pp. 49184-49215, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[16] Qingqing Yue et al., "A Review of Artificial Intelligence-Enhanced Security Solutions for the Internet of Things," *2024 4th International Conference on Artificial Intelligence, Virtual Reality and Visualization*, Nanjing, China, pp. 40-44, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[17] Lorenzo Mucchi et al., "Physical-Layer Security in 6G Networks," *IEEE Open Journal of the Communications Society*, vol. 2, pp. 1901-1914, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Janghyuk Youn, Woong Son, and Bang Chul Jung, "Physical-Layer Security Improvement with Reconfigurable Intelligent Surfaces for 6G Wireless Communication Systems," *Sensors*, vol. 21, no. 4, pp. 1-12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Stephen S. Oyewobi, Karim Djouani, and Anish Matthew Kurien, "Visible Light Communications for Internet of Things: Prospects and Approaches, Challenges, Solutions and Future Directions," *Technologies*, vol. 10, no. 1, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[20] Galefang Allycan Mapunda et al., "Indoor Visible Light Communication: A Tutorial and Survey," *Wireless Communications and Mobile Computing*, vol. 2020, no. 1, pp. 1-46, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[21] Manoj Singh Adhikari et al., *Introduction to AI Techniques for 6G Application*, Development of 6G Networks and Technology, pp. 1-27, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[22] Abdulraqeb Alhammadi et al., "Artificial Intelligence in 6G Wireless Networks: Opportunities, Applications, and Challenges," *International Journal of Intelligent Systems*, vol. 2024, no. 1, pp. 1-27, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[23] Wireless Network Slicing Dataset, Kaggle. [Online]. Available: https://www.kaggle.com/datasets/ziya07/wireless-network-slicing-dataset