International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(18s) 2026 pp. 703-725
https://doi.org/10.70917/ijcisim-2026-4915
Article

Q-CARE-VLC: Quantum-Secured Vehicular Visible-Light Communication with Key-Continuity-Aware Handover for Smart-Ambulance Healthcare

Vivek Kumar1; Keshav Kumar[2*], Mohit Kumar Srivastava[3], Abhishek Rathour[4], Gaurav Sahu[5]

[1,2,4,5]Department of ECE, Pranveer Singh Institute of Technology, Kanpur-209305, UP, India
[1]rastogi0807@gmail.com, 2keshav@gyancity.com, 3mohit.srivastava@psit.ac.in, 4abhisheksrathour@gmail.com, 5sahugaurav12@gmail.com
* Corresponding author: Keshav Kumar

Abstract: Transmission of patient telemetry, diagnostic video, electronic health records, and emergency-control information from a moving ambulance requires simultaneous low latency, high reliability, and strong confidentiality. Vehicular visible-light communication (V-VLC) offers a directional high-rate optical channel, but classical key exchange remains exposed to long-term cryptanalytic risk, and quantum key distribution (QKD) is difficult to sustain under mobility because the quantum link is sensitive to range, background light, pointing error, and handover interruption. This paper proposes Q-CARE-VLC, a dual-plane quantum-secured V-VLC architecture for connected ambulances. The architecture combines a high-rate classical vehicle-to-infrastructure (V2I) VLC data plane with a co-aligned decoy-state BB84 quantum key plane, trusted roadside quantum-VLC units (QVUs), a hospital key orchestrator, a dual-aperture make-before-break quantum handover mechanism, and a priority-aware quantum-key buffer. A unified analytical model is developed for vehicular optical attenuation, atmospheric loss, pointing jitter, classical achievable rate, quantum bit error rate (QBER), asymptotic decoy-state secret-key rate (SKR), key-buffer dynamics, handover interruption, and deadline-constrained medical traffic. A quantum-key-aware handover and scheduling policy gives critical physiological traffic precedence while pre-acquiring keys from the next QVU before the active quantum session is released. Monte Carlo and time-slotted simulations over a 4-km urban emergency corridor, in which all schemes share one simulator and one physical-layer parameter set, show that at an aggregate key-refresh demand of 75 kb/s, Q-CARE-VLC maintains 100% quantum-secure service continuity compared with 80.16% for a static-buffer QKD baseline and 78.77% for break-before-make QKD. At 80 km/h the modeled handover interruption fraction falls from 6.25% to 0.42%. For a daytime clear-air link, the modeled SKR is 70.62 kb/s at 40 m and 13.96 kb/s at 80 m, while the classical VLC plane remains above 83 Mb/s at 80 m. Under an 80 Mb/s aggregate medical load, the proposed scheduler satisfies the 20-ms critical-traffic deadline in 100% of slots, whereas a direct-QKD/FIFO baseline reaches only 12.69%. The results are obtained from a calibrated simulation study rather than a hardware prototype, and they establish a vehicular-healthcare architecture in which quantum key generation, mobility management, and clinical traffic prioritization are co-designed rather than treated as independent functions.

Keywords: Connected healthcare, decoy-state BB84, handover, medical Internet of Things, optical wireless communication, quantum key distribution, quantum-secure networking, smart ambulance, vehicle-to-infrastructure (V2I), vehicular visible light communication

1. Introduction

Emergency medicine increasingly depends on data that must leave the ambulance before the patient reaches the hospital. Multi-lead electrocardiography, oxygen saturation, blood pressure, ventilator status, point-of-care imaging, body-camera or telemedicine video, and electronic patient records can support remote triage, specialist consultation, destination selection, and preparation of an emergency department. In a connected-ambulance model, communication

is therefore not a convenience layer; it becomes part of the clinical workflow. The network must provide sufficient throughput for heterogeneous medical streams, preserve low latency for life-critical telemetry, resist interception, and continue operating while the vehicle experiences rapid changes in geometry and channel quality.

Vehicular visible-light communication is attractive for this role because existing headlights, taillights, traffic lamps, and dedicated roadside luminaires can be used as optical transmitters. V-VLC has a large unlicensed spectrum, directional propagation, natural spatial reuse, and immunity to radio-frequency electromagnetic interference. Recent reviews emphasize, however, that outdoor optical channels are strongly shaped by source radiation pattern, receiver orientation, inter-vehicle geometry, weather, ambient illumination, and mobility [1]. Measurement- and ray-tracing-based studies have also shown that weather, lateral displacement, and non-line-of-sight reflections can materially change the usable link range [2]-[4]. Consequently, a healthcare-grade V-VLC system must be engineered around mobility and environmental variation rather than assuming an indoor Lambertian channel.

Security is equally important. Directionality reduces the spatial region from which a VLC waveform can be intercepted, but it does not make the data cryptographically secure. Recent vehicular work has therefore investigated visible-light-assisted authentication and physical-layer security [5]. These mechanisms address important attack surfaces, but they remain distinct from the problem of generating fresh cryptographic keys whose secrecy does not depend on the computational difficulty of a mathematical problem. QKD provides such keys by exploiting the measurement disturbance of nonorthogonal quantum states. Decoy-state BB84, in particular, permits practical weak-coherent-pulse transmitters while limiting photon-number-splitting attacks [6]-[9].

The difficulty is that QKD was historically developed for fixed fiber or free-space terminals. A moving ambulance creates additional problems: short optical dwell times, background-light variation, mechanical vibration, angular jitter, blockage by other vehicles, and frequent roadside-unit handovers. The feasibility of mobile QKD is nevertheless becoming more credible. A recent mobile-platform demonstration reported finite-key secure rates in the kilobit-per-second range for drone-to-drone, drone-to-vehicle, and vehicle-to-vehicle links [10], while recent daylight free-space QKD experiments have demonstrated practical metropolitan-scale key generation under substantial channel loss [11]. Earlier research also considered satellite QKD as a source of keys for vehicular VLC networks [12]. Field trials conducted within the AirQKD programme have gone further and delivered quantum-derived keys into a working V2I application [13], with an accompanying outage analysis for 6G-V2X links fed by free-space optical QKD [14]. These results motivate direct integration of a mobile quantum plane into road infrastructure, but they do not solve the key-continuity problem for safety-critical medical traffic.

Healthcare introduces a second mismatch. QKD research in medical communications has primarily focused on securing medical images or records over fixed fiber and free-space channels [15]. Vehicular networking research, in contrast, usually optimizes safety-message delivery, authentication, or V2X throughput rather than the quantum-key lifecycle of heterogeneous clinical flows. In an ambulance, a short outage of a video stream may be tolerable, whereas a key-starvation event that blocks encrypted arrhythmia telemetry or remote defibrillation-control data is not. A suitable architecture must therefore couple the quantum key buffer to the medical traffic scheduler and to mobility management.

This paper addresses that gap with Q-CARE-VLC, a dual-plane architecture in which the classical optical data link and the quantum key link are co-designed. Roadside quantum-VLC units provide both a broadband VLC transceiver and a narrowband weak-coherent quantum optical terminal. The ambulance carries a classical optical terminal, a dual-aperture quantum receiver/transmitter module, a medical edge gateway, and a secure key buffer. The hospital is connected to roadside units through an authenticated trusted backhaul or QKD-enabled metro network. The architecture uses make-before-break quantum handover: while medical data continue through the serving roadside unit, a standby quantum aperture acquires the next unit, authenticates it, and begins key generation before the current QKD session is released.

The paper does not assume that QKD itself authenticates network peers. A small pre-provisioned authentication secret or a quantum-resistant authentication mechanism is required to authenticate the classical discussion channel,

after which QKD-generated material can refresh authentication keys. Roadside quantum units are treated as trusted nodes in the baseline architecture. The security objective is therefore to provide information-theoretically generated symmetric key material for frequent rekeying of authenticated medical sessions, not to claim immunity against denial-of-service or compromise of a trusted roadside node.

The scope of the evaluation should be stated plainly. Q-CARE-VLC is assessed by a reproducible time-slotted simulation whose physical-layer parameters are drawn from published V-VLC and free-space QKD measurements; it is not a hardware demonstration. The acquisition and switching latencies used for the three mobility schemes are architectural assumptions chosen to expose the effect of pre-acquisition, and the secret-key rate is computed in the asymptotic decoy-state limit. All reported comparisons are therefore relative statements between schemes evaluated inside one simulator with one common physical-layer parameter set, and Section IX states explicitly which assumptions a hardware-in-the-loop study would have to replace.

The contributions are summarized as follows. First, a connected-ambulance architecture is introduced that jointly integrates vehicular VLC, roadside mobile QKD, medical traffic differentiation, a dual-aperture quantum terminal, and trusted hospital key orchestration. Second, a mobility-aware quantum channel and key-buffer model is developed, including atmospheric attenuation, pointing jitter, background counts, QBER, and decoy-state SKR. Third, a key-continuity-aware make-before-break handover mechanism is designed to pre-acquire the next roadside quantum link and to maintain a reserve of secret bits for emergency rekeying. Fourth, a medical traffic scheduler maps critical telemetry, interactive clinical media, and bulk records to different key-rotation and delay requirements, preserving critical service when the quantum buffer becomes scarce. Fifth, a reproducible simulation study evaluates link distance, weather, pointing error, vehicle speed, roadside-unit spacing, key demand, medical offered load, and intercept-resend attacks against common-implementation baselines. Sixth, closed-form expressions are given for the three network-level metrics used throughout the paper - handover interruption fraction, quantum-secure service continuity, and per-class deadline satisfaction - so that the reported numbers can be reproduced independently of the simulator.

The remainder of the paper is organized as follows. Section II reviews the most relevant V-VLC, QKD, and healthcare-security literature. Section III presents the Q-CARE-VLC architecture. Section IV formulates the classical and quantum channel models. Section V develops the key-buffer, handover, and medical scheduling mechanisms and states the Q-CARE-VLC control procedure as Algorithm 1. Section VI analyzes the security properties and assumptions. Section VII describes the simulation methodology and defines the performance metrics. Section VIII presents and discusses the numerical results. Section IX combines the complexity, deployment, and comparative positioning analysis, and Section X concludes the paper.

2. Related Work and Research Gap

A. Vehicular Visible-Light Communication

The recent IEEE Communications Surveys & Tutorials review by Dotreppe et al. [1] consolidates more than a decade of vehicular VLC channel research and highlights the need to account for photometric source behavior, mobility, environmental conditions, and receiver geometry. Karbalayghareh et al. [2] used non-sequential ray tracing to derive V2V channel and performance limits under multiple weather conditions, demonstrating that weather extinction and asymmetric vehicle-light patterns influence achievable range. Turan and Coleri [3] used real-world V-VLC measurements to build machine-learning channel models based on distance, ambient light, orientation, and turbulence, while later measurement-based work characterized reflected NLOS V-VLC paths [4]. These studies provide the physical basis for the mobility and weather terms adopted in this paper, but do not incorporate quantum key generation or medical traffic.

Security mechanisms for V2I links have also evolved beyond conventional credentials. De Vincenzi et al. [5] proposed a multi-channel multi-factor vehicle-authentication system in which a line-of-sight visual channel complements cryptographic credentials, reporting high authentication accuracy across lighting, speed, and weather

variations. This demonstrates the value of optical line-of-sight information for vehicular security. Q-CARE-VLC is complementary: visual and credential authentication can bootstrap a trusted association, while the quantum plane supplies fresh symmetric key material for the confidentiality and integrity protection of medical sessions.

B. Quantum Key Distribution for Optical and Mobile Links

BB84 established the principle of distributing secret bits by encoding nonorthogonal quantum states [6]. Practical weak-coherent transmitters require protection against multiphoton vulnerabilities; decoy-state methods address this by varying the mean photon number and estimating the single-photon yield [7], [8]. Security analyses have subsequently clarified practical attack surfaces, detector imperfections, authentication requirements, and finite-key effects [9].

Recent mobile experiments are especially important for the present work. Conrad et al. [10] demonstrated QKD on vehicle and drone platforms, showing that mobile quantum links are technically feasible but sensitive to platform imperfections. Zhang et al. [11] demonstrated daylight free-space QKD over a metropolitan-scale link, confirming that strong background illumination does not preclude operation when filtering and receiver design are adequate. For vehicular VLC specifically, Le et al. [12] investigated satellite-generated quantum keys distributed to vehicles through an optical architecture. These results motivate direct roadside quantum access, but they do not develop a healthcare-aware key-buffer and make-before-break handover architecture.

The closest infrastructure precedent is the AirQKD line of work. Fowler et al. [13] implemented a free-space optical QKD system inside a functioning V2I application, replacing conventional public-key material with quantum-derived symmetric keys and adding a zero-trust protocol so that spoofed messages from a compromised roadside device are rejected. Yuan et al. [14] complemented that demonstration with an outage analysis of a 6G-V2X link supplied by free-space optical QKD. Both works establish that quantum-derived keys can be delivered to a vehicle in practice. Neither, however, treats the secret-key supply as a buffered resource that must survive repeated roadside-cell crossings, and neither couples that supply to deadline-constrained clinical traffic - which is precisely the coupling that Q-CARE-VLC introduces.

C. Quantum Security for Healthcare and Network Integration

Medical data are unusually sensitive because confidentiality must often persist for many years, while emergency data may also be safety critical in real time. Mallick et al. [15] examined QKD-based protection of medical image transmission over fiber and free-space channels, illustrating the relevance of quantum keying to healthcare workloads. Zia-Ul-Mustafa et al. [16] reviewed the broader integration of QKD with visible-light communications. However, neither fixed healthcare links nor generic VLC-QKD studies address rapid roadside cell crossing, pointing, handover, key prefetch, and clinical traffic prioritization in a moving ambulance.

At the network level, QKD-secured optical systems require key management, trusted-node operation, routing, and authenticated control functions [17], while broader quantum-cryptography research emphasizes that practical security depends on implementation assumptions rather than the protocol name alone [18]. High-rate fiber QKD has demonstrated that key generation can reach very high rates in fixed links [19], and high-dimensional QKD has been demonstrated over deployed multicore fiber [20]; these advances are relevant to the hospital and backhaul side but do not remove the short-contact mobile-access bottleneck. Stavdas et al. investigated QKD integration with V2I communications and software-defined networking [21], providing a particularly relevant network precedent. Physical-layer VLC secrecy methods such as IRS-assisted anti-eavesdropping [22] represent a complementary classical-light security approach rather than a substitute for quantum-generated key material.

Table I positions Q-CARE-VLC against the most closely related studies and identifies, for each, the specific gap that the proposed architecture addresses.

TABLE I

POSITIONING OF Q-CARE-VLC RELATIVE TO CLOSELY RELATED RESEARCH

Work	Domain	Main focus	QKD	Mobility-aware key continuity	Gap addressed by Q-CARE-VLC
Karbalayghareh et al. [2]	V-VLC	V2V channel and weather modeling	No	No	Adds a quantum plane and key lifecycle
De Vincenzi et al. [5]	V2I security	Visual and credential authentication	No	No	Authentication as bootstrap; QKD for rekeying
Le et al. [12]	Vehicular VLC and QKD	Satellite-to-ground key distribution	Yes	No	Direct roadside QKD plus handover
Fowler et al. [13]	V2I FSO-QKD	Deployed quantum-derived V2I keys	Yes	No	Route-level buffered key continuity
Conrad et al. [10]	Mobile QKD	Vehicle and drone quantum links	Yes	No	Network architecture around mobile QKD
Mallick et al. [15]	Healthcare and QKD	Medical image protection	Yes	No	Vehicular mobility and deadline-aware scheduling
Q-CARE-VLC	**Vehicular healthcare**	**Roadside QKD, VLC, and key-aware handover**	**Yes**	**Yes**	**Dual-plane, key-buffered, make-before-break**

3. Q-CARE-VLC System Architecture

Fig. 1 shows the proposed architecture. The design separates bulk medical data transport from secret-key generation while keeping the two planes under a common mobility and security controller. This separation is essential because a high-rate optical data signal and a single-photon-level quantum signal have very different link budgets and receiver requirements. The classical plane can continue carrying encrypted packets using previously generated keys even when the instantaneous quantum link temporarily degrades, provided that the local key buffer remains above its safety threshold.

The connected ambulance contains four logical modules. The medical acquisition network receives data from body-area sensors, patient monitors, point-of-care devices, and telemedicine cameras. A medical edge gateway time-stamps, compresses, and classifies the traffic. A classical vehicular optical terminal uses a headlamp or roof-mounted transmitter and a narrow-field receiver for V2I data. A quantum optical terminal contains polarization and intensity control, narrow spectral filtering, timing recovery, single-photon detection, and two steerable apertures: one aperture maintains the active QKD session while the second performs pre-acquisition of the next QVU. Secret bits are delivered to a protected key buffer accessible only to the cryptographic session manager.

Each QVU combines a broadband VLC transceiver and a quantum terminal. The classical transmitter may be integrated with a traffic signal or dedicated roadside luminaire. The quantum channel uses a narrowband optical source and detection chain spectrally isolated from the broadband VLC waveform. A dichroic or narrowband filter separates the quantum wavelength from the classical optical carrier at the receiver. The QVU maintains an authenticated control

connection to the hospital key orchestrator through a trusted wired or optical backhaul. In a future deployment this backhaul may itself be QKD-enabled, but the present model requires only that the QVU-to-hospital key transfer be trusted and authenticated.

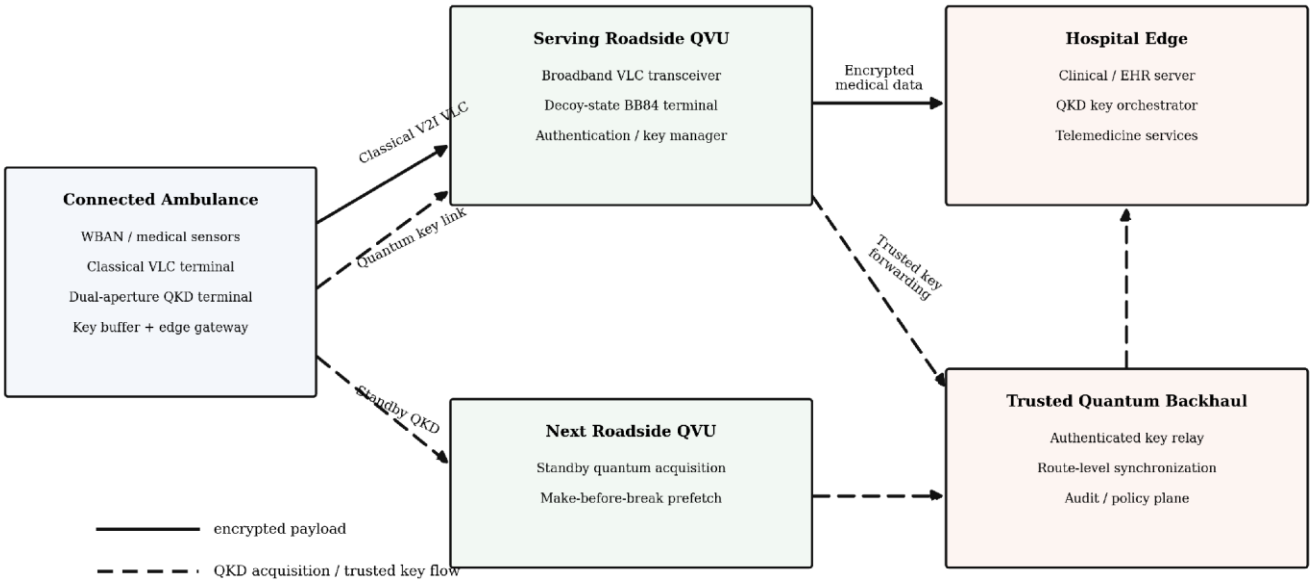

Fig. 1. Q-CARE-VLC dual-plane architecture.

The hospital edge terminates the medical application sessions and maintains a synchronized view of the ambulance key buffer. When a QVU generates a block of secret bits with the ambulance, the corresponding hospital-side key material is delivered through trusted-node key forwarding. Application encryption uses a standardized authenticated symmetric cipher such as AES-GCM. QKD bits are therefore used as high-grade session key material rather than as a one-time pad for the entire medical payload; this allows kilobit-per-second QKD links to secure tens or hundreds of megabits per second of medical data through frequent key rotation.

The most important architectural departure from conventional mobile QKD is the make-before-break procedure. As the ambulance approaches the geometric handover region, the mobility controller estimates the secret-key yield from both the serving and candidate QVUs. The standby quantum aperture begins timing acquisition, authentication, and decoy-state exchange with the next QVU while the serving link remains available. Secret bits from the candidate are admitted to the same logical key reservoir after key identifiers are synchronized with the hospital. The active data-plane handover is allowed only after the candidate quantum path is authenticated or the reserve buffer is sufficiently high to survive the predicted acquisition interval.

The architecture is intentionally compatible with established classical interfaces rather than defining an isolated security stack. The broadband optical access plane can be implemented within the short-range optical-wireless framework of IEEE 802.15.7 [23], while vehicular credential and message-security functions can interoperate with IEEE 1609.2 mechanisms [24]. Payload encryption uses the standardized Advanced Encryption Standard [25] in Galois/Counter Mode [26], with QKD material feeding session-key refresh rather than replacing the authenticated cipher. Medical-device traffic can be mapped from interoperable point-of-care interfaces such as the ISO/IEEE 11073 family [27] into the C1-C3 classes defined in Section IV-F.

4. System and Channel Model

A. Road Geometry and Mobility

Consider an urban emergency corridor of length L with roadside QVUs positioned at longitudinal coordinates x_j. The ambulance position at slot t is $x_a(t)$ and its instantaneous velocity is $v(t)$. A lateral and vertical offset $d_\perp$ accounts for mounting geometry between the vehicle optical terminal and the roadside terminal. The slant range to QVU j is

$$d_j(t) = \sqrt{\left[x_a(t) - x_j\right]^2 + d_\perp^2} \quad (1)$$

The active QVU set contains units satisfying $d_j(t) \le d_{cov}$ and the field-of-view constraints. Unlike an RF cell, coverage is also constrained by optical orientation, line-of-sight blockage, and received photon flux.

Because the quantum plane is the scarce resource, the time available for key accumulation at each roadside unit must be modeled explicitly. Neglecting acceleration over one cell, the contact time of QVU j at constant speed v is

$$\hat{T}_j(v) = \frac{2\sqrt{d_{cov}^2 - d_\perp^2}}{v} \quad (2)$$

which decreases hyperbolically with speed and directly bounds the number of secret bits that can be harvested during a single pass. Equation (2) is the reason an emergency vehicle, which may travel considerably faster than surrounding traffic, needs a route-aware prefetch policy rather than a purely reactive one.

B. Classical Vehicular VLC Channel

For the classical optical data plane, the direct-current channel gain follows standard optical-wireless Lambertian modeling [28], [29], multiplied by weather and pointing terms. For irradiance angle $\phi_j(t)$ and incidence angle $\psi_j(t)$,

$$h_{c,j}(t) = \frac{(m+1)A_{PD}}{2\pi d_j^2(t)} cos^m(\phi_j) \times T_s(\psi_j) g(\psi_j) cos(\psi_j) L_{atm,c} L_{p,c} \quad (3)$$

where A_{PD} is the photodetector area, $T_s(\cdot)$ is the optical filter gain, and $g(\cdot)$ is the concentrator gain. The Lambertian order is determined by the transmitter semi-angle $\Phi_{1/2}$ through

$$m = \frac{-ln2}{ln[cos(\Phi_{1/2})]} \quad (4)$$

The atmospheric factor uses Beer-Lambert attenuation

$$L_{atm,c}(d) = 10^{-\alpha_c d/10^4} \quad (5)$$

where α_c is expressed in dB/km and the 10^4 in the exponent converts the range from metres to kilometres while removing the decibel scaling. Pointing loss is represented by an angular-jitter-dependent factor $L_{p,c}$. The electrical signal-to-noise ratio of the intensity-modulated direct-detection link can then be written as

$$\gamma_{c,j} = \frac{\left(R_{PD} P_{opt} h_{c,j}\right)^2}{\sigma_n^2} \quad (6)$$

and an achievable-rate approximation for a real-valued optical multicarrier waveform is

$$C_j = \frac{B_c}{2} log_2\left(1 + \gamma_{c,j}\right) \quad (7)$$

The factor one-half accounts for the Hermitian symmetry required to generate a real optical OFDM waveform. Dynamic statistical V-VLC studies have shown that traffic density and changing inter-vehicle geometry materially alter optical path loss [30]; accordingly, the simulations use a calibrated vehicular link budget rather than an indoor received-power model.

C. Quantum Optical Channel

The quantum plane uses phase-randomized weak coherent pulses with signal intensity μ and one or more decoy intensities. The end-to-end transmittance is

$$\eta_j(t) = \eta_{tx}\eta_{rx}\eta_{det}\eta_{geo}\left[d_j(t)\right]\eta_{p,j}(t)\eta_{atm,q}\left[d_j(t)\right] \quad (8)$$

where η_{tx}, η_{rx}, and η_{det} are the transmitter, receiver, and detector efficiencies. For receiver aperture diameter D_r and far-field beam radius $w(d)$, a useful geometric approximation is

$$\eta_{geo}(d) = min\left\{1, \left[\frac{D_r}{2w(d)}\right]^2\right\} \quad (9)$$

Angular vibration produces a lateral pointing displacement of approximately $r_p = d\sigma_\theta$. The average pointing-coupling penalty is modeled as

$$\eta_p \simeq \left[1 + \frac{4\sigma_r^2}{w^2(d)}\right]^{-1}, \qquad \sigma_r = d\,\sigma_\theta \quad (10)$$

This form is deliberately simple enough for network simulation while retaining the principal sensitivity to angular jitter. In hardware validation it should be replaced by the measured pointing-error distribution of the optical terminal.

D. Decoy-State BB84 Secret-Key Model

Let Y_0 denote the background plus dark-count yield per emitted pulse. For signal intensity μ, the overall gain is approximated as

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \quad (11)$$

If e_d is the optical misalignment error, the signal-state QBER satisfies

$$E_\mu Q_\mu = \frac{1}{2}Y_0 + e_d(1 - e^{-\eta\mu}) \quad (12)$$

The single-photon gain Q_1 and single-photon error e_1 are estimated by the decoy-state procedure. For the asymptotic model used in the network-level study, the resulting secure rate is

$$R_{sec} = qf_{clk}max\{0,\ \ Q_1[1 - H_2(e_1)]\ \ - f_{EC}Q_\mu H_2\left(E_\mu\right)\} \quad (13)$$

where q is the basis-sifting factor, f_{clk} is the pulse repetition rate, f_{EC} is the error-correction inefficiency, and the binary entropy function is

$$H_2(x) = -xlog_2x - (1 - x)log_2(1 - x) \quad (14)$$

The outer maximum operator in (13) forces negative asymptotic key estimates to zero. A final experimental paper should replace the asymptotic term with a composable finite-key analysis based on the actual block length and failure probabilities. The present objective is to evaluate the network architecture under a conservative mobile-link budget.

E. Quantum-Key Buffer Dynamics

Let $B_k(t)$ denote the number of secret bits available in the synchronized ambulance-hospital key reservoir. During slot Δt, new QKD material is admitted at rate $R_{sec}(t)$, while cryptographic sessions consume $\kappa(t)$ bits for rekeying. The buffer evolves as

$$B_k(t+1) = min\{\, B_{max},\ max[0, B_k(t) - \kappa(t)\Delta t] + R_{sec}(t)\Delta t\} \quad (15)$$

A reserve threshold B_{res} is maintained for life-critical streams. When B_k falls below the lower threshold, Q-CARE-VLC does not terminate critical traffic. Instead, it preserves the critical rekey period and temporarily lengthens the permitted key-rotation interval of lower-priority media and record-transfer sessions within configured security policy bounds.

F. Medical Traffic Classes

Table II summarizes the three medical traffic classes and the delay and key-rotation targets assigned to each.

TABLE II

MEDICAL TRAFFIC CLASSES USED BY THE Q-CARE-VLC SCHEDULER

Class	Traffic type	Examples	Delay target	Priority	Key rotation
C1	Critical telemetry and control	ECG, SpO2, alarms, device commands	20 ms	Highest	Very frequent
C2	Interactive clinical media	Telemedicine video, ultrasound snapshots	120 ms	Medium	Frequent
C3	Clinical records and bulk transfer	EHR, logs, nonurgent files	500 ms	Lower	Adaptive

Table II captures the core healthcare design principle: confidentiality is required for all classes, but urgency and tolerated key-rotation delay are not identical. This allows the architecture to trade temporary postponement of lower-priority rekey events for uninterrupted C1 protection when the mobile quantum channel deteriorates.

5. Quantum-Key-Aware Handover and Medical Scheduling

A. Candidate QVU Prediction

The ambulance route, current velocity, and QVU map are available to the mobility controller. Cooperative VLC traffic-control studies have already shown the value of route- and infrastructure-aware optical vehicular coordination [31]. Q-CARE-VLC extends that principle to quantum-key continuity: for candidate unit j, the controller predicts an average classical rate $\hat{C}_j$, secret-key rate $\hat{R}_{q,j}$, contact time $\hat{T}_j$ from (2), and acquisition penalty $T_{acq,j}$ over a short horizon. A normalized handover score is

$$S_j = w_c \frac{\hat{C}_j}{C_{ref}} + w_q \frac{\hat{R}_{q,j}}{R_{q,ref}} + w_t \frac{\hat{T}_j}{T_{ref}} - w_a \frac{T_{acq,j}}{T_{a,ref}} \quad (16)$$

where C_{ref}, $R_{q,ref}$, T_{ref}, and $T_{a,ref}$ are normalizing constants and the weights can be configured by the emergency service operator. In the simulations the quantum and contact-time terms are emphasized whenever the key buffer is below its target level.

B. Make-Before-Break Quantum Handover

When the score of the next QVU exceeds that of the serving unit by a hysteresis margin Δ_{hys}, the standby optical aperture performs acquisition and authenticated QKD initialization. Because the serving quantum link is not released during this process, the main interruption occurs only during the final key-index synchronization and optical switch. For a corridor with uniform QVU spacing S_{QVU}, the vehicle crosses v/S_{QVU} cell boundaries per second, so the fraction of route time spent in a quantum-link interruption of duration T_{int} is

$$\Xi(v) = \frac{T_{int}\, v}{S_{QVU}} \quad (17)$$

Equation (17) makes the architectural benefit explicit: reducing T_{int} by pre-acquisition is equivalent to reducing the effective outage of the quantum plane by the same factor at every speed. The modeled residual interruption is 30 ms, compared with 180 ms for a static-buffer single-aperture design and 450 ms for a break-before-make direct-QKD design. These values are simulation assumptions chosen to expose the architectural effect; they are not claimed as measured hardware timings.

C. Key-Reserve Policy

The key manager defines $B_{low} < B_{tgt} < B_{max}$. If $B_k \geq B_{tgt}$, all streams use their nominal aggressive rekey schedule. For $B_{low} \leq B_k < B_{tgt}$, lower-priority key rotation is moderately relaxed and the candidate-QVU score is biased toward SKR. If $B_k < B_{low}$, C1 retains its nominal rekey period, C2 uses a bounded extended interval, and C3 key rotation is deferred until the buffer recovers. This policy converts the quantum channel from a hard availability constraint into a buffered security resource.

D. Priority Medical Scheduler

Let $Q_i(t)$ denote the queued bits for class i and D_i the deadline target. Q-CARE-VLC uses strict urgency ordering for the critical class and deadline-weighted service for the remaining classes. The scheduling weight is

$$W_i(t) = \frac{\omega_i Q_i(t)}{max[D_i - a_i(t), \varepsilon]} \quad (18)$$

where $a_i(t)$ is the age of the head-of-line data, ω_i is a class priority coefficient, and ε prevents division by zero. Packets with an expired clinical deadline can be discarded if they are stale and semantically useless, but C1 telemetry is configured with a retransmission and duplication policy rather than silent expiration. The scheduler consumes key identifiers atomically with packet-batch encryption so that a packet is never transmitted under an unconfirmed key epoch.

E. Q-CARE-VLC Control Procedure

The complete control loop is stated in Algorithm 1 and illustrated in Fig. 2. Algorithm 1 makes the ordering of the quantum and clinical decisions explicit, whereas Fig. 2 shows the two decision branches - insufficient buffer and unauthenticated candidate - that keep critical traffic protected when the quantum plane degrades.

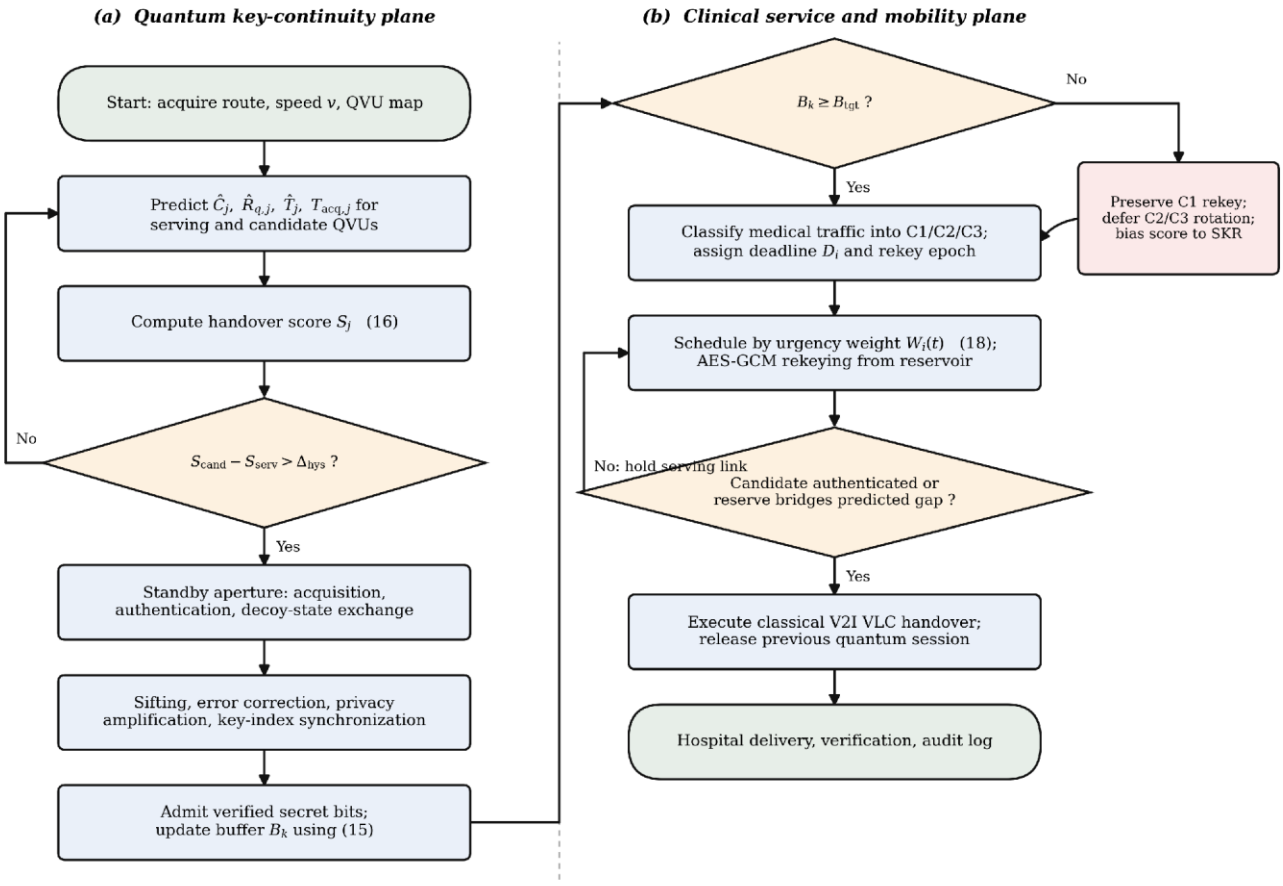

Fig. 2. Q-CARE-VLC operational flowchart. (a) Quantum key-continuity plane: candidate prediction, scoring, standby acquisition, and buffer admission. (b) Clinical service and mobility plane: reserve policy, traffic classification, deadline-weighted scheduling, and gated handover.

Algorithm 1 Q-CARE-VLC key-continuity-aware handover and scheduling

Input: route and QVU map; speed $v(t)$; channel state; buffer $B_k(t)$; thresholds $B_{low} < B_{tgt} < B_{max}$; deadlines $D_{1..3}$

Output: serving QVU assignment, admitted secret bits, and per-class transmission order

1: **while** ambulance has not reached the hospital **do**

2: measure $x_a(t)$, $v(t)$, and serving-link state; read $B_k(t)$

3: **for each** candidate QVU j in the coverage set **do**

4: predict $\hat{C}_j, \hat{R}_{q,j}, T_{acq,j}$; compute $\hat{T}_j$ by (2)

5: **if** $B_k(t) < B_{tgt}$ **then** raise w_q, w_t **end if**

6: evaluate the handover score S_j by (16)

7: **end for**

8: $c \leftarrow argmax_{j \neq serv} S_j$

9: **if** $S_c - S_{serv} > \Delta_{hys}$ **then**

10: start standby-aperture acquisition and authentication with QVU c

11: run decoy-state exchange, sifting, error correction, and privacy amplification

12: synchronize key indices with the hospital orchestrator

13: admit verified secret bits; update B_k by (15)

14: **end if**

15: classify arriving medical traffic into C1, C2, and C3; assign D_i and rekey epochs

16: **if** $B_k(t) < B_{low}$ **then**

17: keep the C1 rekey period; extend C2 within policy bounds; defer C3 rotation

18: **else if** $B_k(t) < B_{tgt}$ **then**

19: relax C3 rotation only

20: **end if**

21: compute $W_i(t)$ by (18); serve C1 first, then C2 and C3 by descending $W_i(t)$

22: encrypt each packet batch under a confirmed key epoch drawn from the reservoir

23: **if** QVU c is authenticated **or** $B_k(t) \geq \kappa T_{acq,c}$ **then**

24: execute the classical V2I VLC handover; release the previous quantum session

25: **else** retain the serving link for one more control interval **end if**

26: **end while**

6. Security Analysis

A. Passive Eavesdropping on the Classical VLC Plane

All medical payloads are encrypted and integrity protected with QKD-derived symmetric keys. Directional optical propagation reduces opportunistic collection but is not relied upon as the primary security control. Classical V-VLC can additionally employ physical-layer secrecy techniques, including RIS-assisted legitimate-link enhancement and eavesdropper suppression [32], but Q-CARE-VLC treats such mechanisms as complementary. An eavesdropper that records the classical waveform obtains ciphertext and metadata but not the fresh session key, assuming endpoint and trusted-node integrity.

B. Intercept-Resend on the Quantum Plane

An intercept-resend adversary measuring a fraction p_E of BB84 states introduces additional errors because measurements performed in the wrong basis disturb the states. An adversary who measures in a randomly chosen basis is wrong half the time and, when wrong, resends a state that the legitimate receiver decodes incorrectly with probability one-half, so the effective optical error becomes

$$e_q(p_E) = e_d + \frac{1}{4} p_E \quad (19)$$

The increase in QBER directly reduces the privacy-amplified SKR through (13) and ultimately forces the secure rate to zero when the estimated phase-error bound becomes too large. This behavior is evaluated in Section VIII-J.

C. Authentication, Replay, and Man-in-the-Middle Protection

QKD does not by itself authenticate the classical reconciliation channel. Q-CARE-VLC therefore assumes an initial authentication secret provisioned to the ambulance and the trusted emergency-service infrastructure, or a quantum-resistant signature or MAC bootstrap. Once the first QKD epoch succeeds, part of the new secret material is reserved for future information-theoretic or symmetric authentication. Key epoch identifiers, nonces, sequence numbers, and authenticated encryption prevent replay of previously valid medical ciphertext.

D. Trusted-Node and Availability Assumptions

Roadside QVUs are trusted in the baseline architecture because they participate in key forwarding toward the hospital. Compromise of a trusted QVU is therefore a system-security event rather than a quantum-channel attack. This trust and availability separation is consistent with broader 6G security roadmaps that distinguish confidentiality mechanisms from resilience and service availability [33]. The architecture can be extended toward end-to-end entanglement-based networking when practical quantum repeaters become available. Similarly, intense optical jamming or deliberate physical blockage can deny service; QKD detects secrecy degradation but cannot guarantee availability. An operational system should therefore retain an authenticated RF or 5G fallback for availability while maintaining the QKD-derived key state whenever possible.

7. Simulation Methodology

A. Simulator and Parameters

A time-slotted Python simulation was developed to evaluate both physical-link behavior and network-level key continuity. The purpose is not to claim an experimental prototype, but to test whether the proposed architecture produces internally consistent performance under realistic orders of magnitude drawn from current V-VLC and free-space QKD literature. All proposed and baseline schemes are evaluated in the same simulator and use identical physical channel parameters.

Table III lists the principal simulation parameters; every result in Section VIII uses these values unless the corresponding sweep variable is stated otherwise.

TABLE III

PRINCIPAL SIMULATION PARAMETERS

Parameter	Value or range
Road length	4 km nominal
QVU spacing S_{QVU}	100-240 m; 160 m nominal
Coverage radius d_{cov}	160 m
Ambulance speed v	30-130 km/h; 80 km/h nominal
Slant offset $d_{\perp}$	7 m
Classical bandwidth B_c	40 MHz
Quantum wavelength	narrowband visible (650-nm class)
QKD protocol	decoy-state BB84
Pulse rate f_{clk}	50 MHz
Signal intensity μ	0.5

Detector efficiency η_{det}	0.25
Day background yield Y_0	5×10^{-5} per gate
Night background yield Y_0	5×10^{-6} per gate
Intrinsic optical error e_d	1.5%
RMS pointing jitter σ_θ	0.5 mrad
Key buffer B_{max}	150 kbit
Initial buffer $B_k(0)$	50 kbit
Key-refresh demand κ	75 kb/s nominal
T_{int}: direct / static / proposed	450 / 180 / 30 ms
Deadlines D_1, D_2, D_3	20 / 120 / 500 ms

Three QKD mobility baselines are implemented. Direct-QKD uses a single quantum terminal, break-before-make handover, and fixed application rekey periods. Static-buffer QKD adds a larger local key buffer and a shorter acquisition delay but does not pre-acquire the next roadside unit. Q-CARE-VLC uses dual-aperture pre-acquisition, a predictive candidate score, and priority-aware key consumption. For medical queueing, a Direct-QKD/FIFO variant represents a system that does not prioritize critical traffic, whereas Static-buffer priority uses strict traffic priority without predictive key continuity.

B. Performance Metrics

Three network-level metrics are reported throughout Section VIII, and each is defined here so that the numbers can be reproduced independently. Quantum-secure service continuity is the fraction of the N_s simulated slots in which the reservoir can still satisfy the critical-class rekey demand,

$$\Theta = \frac{1}{N_s}\sum_{t=1}^{N_s} \quad 1\{B_k(t) \geq B_{res}\} \qquad (20)$$

where $1\{\cdot\}$ is the indicator function. Per-class deadline satisfaction is the fraction of class-i packets whose end-to-end delivery latency $\tau_{i,n}$ meets the clinical deadline,

$$\Psi_i = \frac{1}{N_i}\sum_{n=1}^{N_i} \quad 1\{\tau_{i,n} \leq D_i\} \quad (21)$$

and the secret-bit yield harvested during a single roadside-unit pass, used in Section VIII-H, follows from (2) as

$$Y_{pass}(v) = \frac{1}{v}\int_{-S_{QVU}/2}^{S_{QVU}/2} \quad R_{sec}(x)\,dx \quad (22)$$

The handover interruption fraction $\Xi(v)$ of (17) completes the metric set. Reporting Θ, Ψ_i, and Ξ together is deliberate: a scheme can protect the key reservoir while starving a traffic class, or meet deadlines while running the reservoir empty, and only the combination distinguishes the architectures.

8. Results and Discussion

A. Secret-Key Rate and QBER Versus Distance

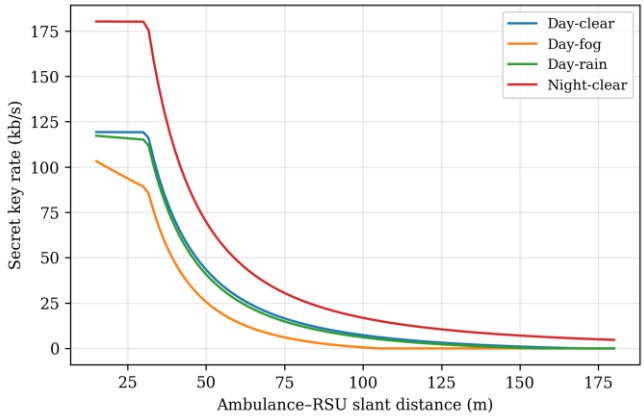

Fig. 3. Modeled decoy-state secret-key rate versus ambulance-QVU distance under representative background-light and weather conditions.

Fig. 3 shows that mobility-compatible QKD is fundamentally a short-range resource. In the daytime clear-air case, the modeled SKR decreases from 70.62 kb/s at 40 m to 13.96 kb/s at 80 m, 3.79 kb/s at 120 m, and 1.03 kb/s at 150 m. At night, the lower background yield materially improves the usable margin: the model produces 26.74 kb/s at 80 m, 11.47 kb/s at 120 m, and 7.08 kb/s at 150 m. The important design implication is that QVU spacing should be driven by quantum yield rather than only by the much longer classical VLC link budget. The architecture therefore accumulates keys near the center of each optical cell and consumes the reservoir while the vehicle traverses the lower-yield edges.

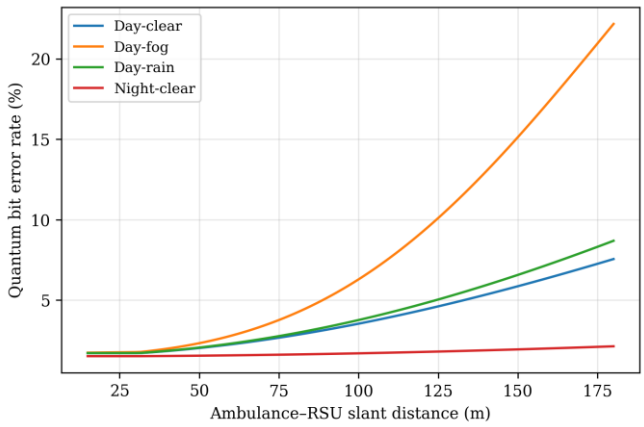

Fig. 4. QBER versus distance for the same quantum-channel scenarios.

The corresponding QBER behavior is shown in Fig. 4. For daytime clear conditions the QBER rises from 1.84% at 40 m to 2.82% at 80 m, 4.39% at 120 m, and 5.87% at 150 m. The increase results from the growing contribution of background and dark counts as signal detection probability falls. Night operation remains below 2% over much of the simulated range. These values are consistent with the architectural requirement that key generation be opportunistic and buffered rather than treated as a continuously high-rate channel.

B. Classical Medical Data Capacity

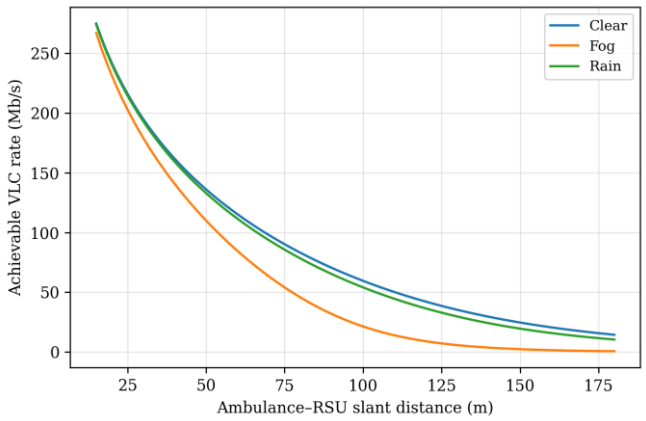

Fig. 5. Achievable classical vehicular VLC rate versus distance for representative weather attenuation.

Fig. 5 confirms the different operating scales of the two planes. In clear air, the modeled classical VLC rate is 83.11 Mb/s at 80 m, 42.16 Mb/s at 120 m, and 24.68 Mb/s at 150 m. Even a rain-like 5 dB/km attenuation produces only a moderate reduction over these short ranges. Heavy fog is more damaging: at 120 m the modeled rate falls to 9.02 Mb/s and at 150 m to 2.39 Mb/s. This separation supports the dual-plane design. The classical channel has enough capacity to carry compressed telemedicine media in ordinary conditions, whereas the quantum channel is the scarce resource that must be accumulated and managed.

C. Route-Level Key-Buffer Continuity

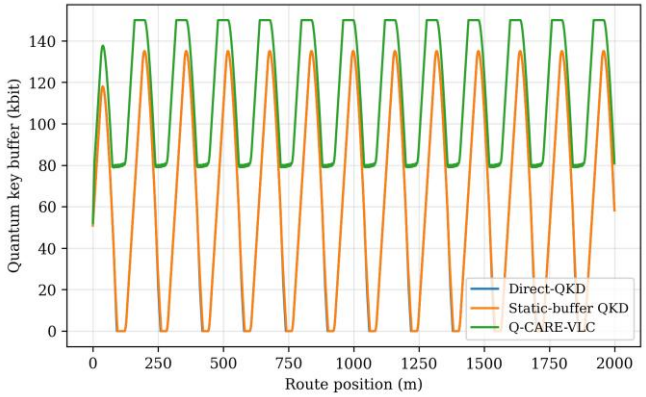

Fig. 6. Quantum-key buffer along a 2-km route at 80 km/h for direct QKD, static-buffer QKD, and Q-CARE-VLC.

Fig. 6 illustrates the mechanism that produces the continuity gain. Direct and static single-aperture schemes repeatedly deplete their buffers near cell edges because their average key inflow is close to the configured rekey demand and acquisition gaps prevent timely replenishment. Q-CARE-VLC prefetches from the next QVU in the overlap region and temporarily protects the critical-key budget when the buffer is low. Under the nominal 75-kb/s key demand over the steady-state portion of a 4-km route, Direct-QKD provides 78.77% quantum-secure service continuity and Static-buffer QKD provides 80.16%, while Q-CARE-VLC maintains 100%. The proposed scheme also preserves a modeled minimum buffer of approximately 79 kbit under this scenario, whereas both baselines reach zero.

D. Sensitivity to Key-Refresh Demand

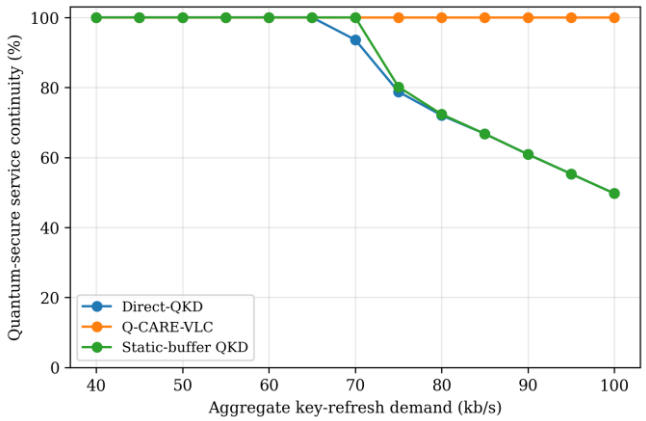

Fig. 7. Quantum-secure service continuity versus aggregate cryptographic key-refresh demand.

Fig. 7 separates a low-load regime from a key-starved regime. At 60 kb/s all schemes maintain full continuity because the average QKD inflow is sufficient. At 75 kb/s the direct and static baselines fall to 78.77% and 80.16%, respectively. At 90 kb/s both fixed-demand baselines are near 60.88%, whereas Q-CARE-VLC still protects the quantum-secure service by adapting noncritical rekey timing and using candidate-QVU prefetch. This result should not be interpreted as free key generation: the advantage comes from assigning the limited secret-bit supply according to clinical urgency instead of applying identical key-refresh behavior to every stream.

E. Handover Robustness Under Ambulance Speed

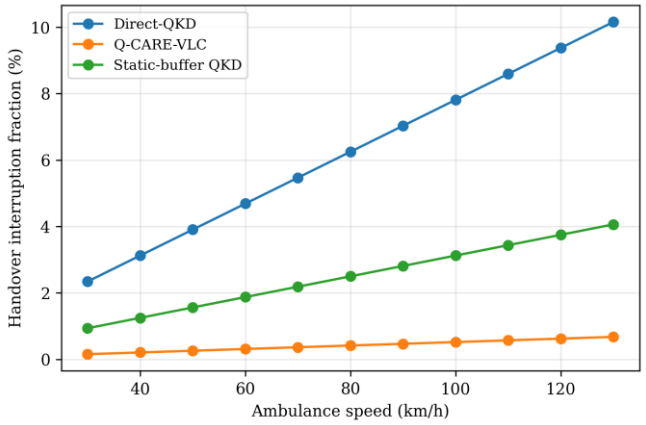

Fig. 8. Modeled handover interruption fraction versus ambulance speed.

The make-before-break mechanism becomes increasingly valuable at higher speed. With 160-m QVU spacing, the 450-ms acquisition assumption of Direct-QKD corresponds to a 6.25% interruption fraction at 80 km/h and 9.38% at 120 km/h. Static-buffer QKD reduces these values to 2.50% and 3.75%. Q-CARE-VLC, with 30-ms residual switching time after pre-acquisition, reduces the corresponding fractions to only 0.42% and 0.63%. These values follow directly from (17), and the linear growth of each curve with speed confirms that the simulator and the analytical expression agree. The result indicates that mobility should be handled in the quantum plane before the classical link is forced to change serving units.

F. Roadside-Unit Spacing

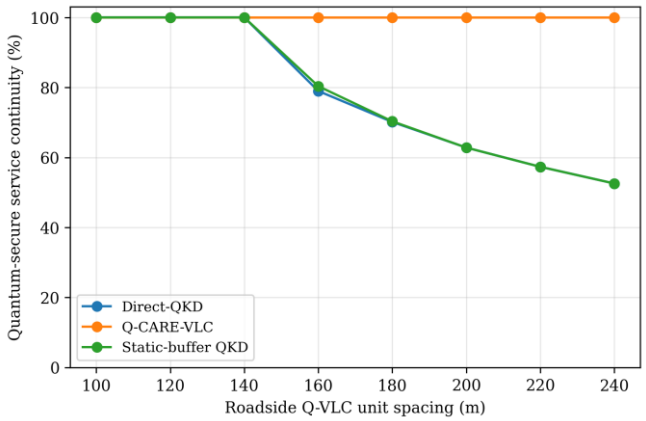

Fig. 9. Quantum-secure service continuity versus roadside QVU spacing.

Fig. 9 quantifies infrastructure-density sensitivity. At 120-m spacing all schemes have sufficient overlap and key opportunity to maintain continuity. At the nominal 160-m spacing, the direct and static baselines fall to roughly 79-80%, while Q-CARE-VLC remains continuous. At 200 m, the baseline continuity is approximately 62.81%, and at 240 m it drops to about 52.56%. The proposed scheme remains continuous in the modeled route because the dual-aperture overlap and adaptive buffer policy exploit the available high-rate regions more effectively. This result provides a planning insight: the value of predictive key accumulation increases sharply once infrastructure spacing approaches the quantum-link edge rather than the classical-link edge.

G. Pointing Jitter and Weather Robustness

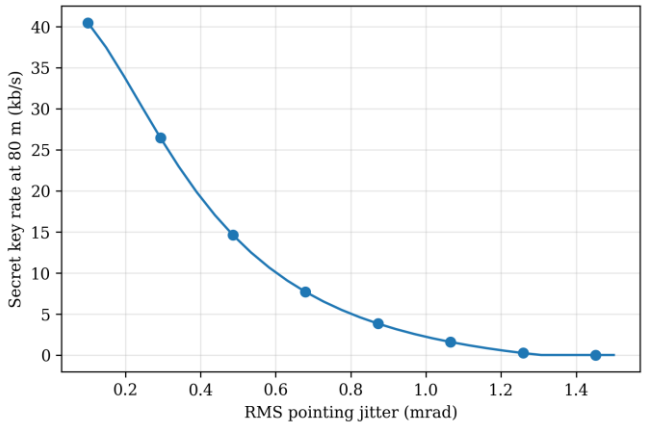

Fig. 10. Secret-key rate at 80 m versus RMS pointing jitter.

Mobile quantum optics are particularly sensitive to angular error. At 80 m, the modeled SKR is approximately 14.60 kb/s near 0.5 mrad RMS pointing jitter but only 2.04 kb/s near 1.0 mrad; at approximately 1.5 mrad the selected link budget no longer yields a positive secure rate. This result places active pointing and stabilization among the most important hardware requirements of the proposed architecture. It also motivates the dual-aperture design, because a standby aperture can spend more time on acquisition and tracking without interrupting the serving quantum path.

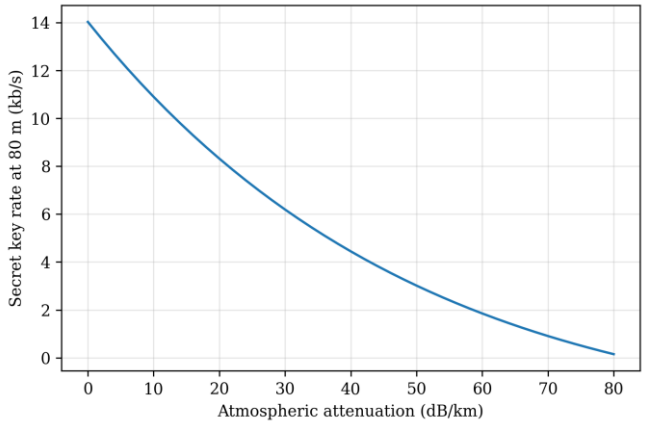

Fig. 11. Secret-key rate at 80 m versus atmospheric attenuation.

Atmospheric loss causes a similarly nonlinear degradation because lower photon detection probability increases the relative weight of background counts. At 80 m, increasing attenuation from 0 to 20 dB/km reduces the modeled SKR from roughly 14.03 to 8.32 kb/s; at 40 dB/km it falls to 4.44 kb/s, and at 80 dB/km it approaches 0.15 kb/s. The operational consequence is that severe fog should trigger a cross-technology availability mode in which classical RF or 5G carries the encrypted payload while the system conserves its QKD-derived key reserve until optical conditions recover.

H. Key Yield Per Roadside Contact

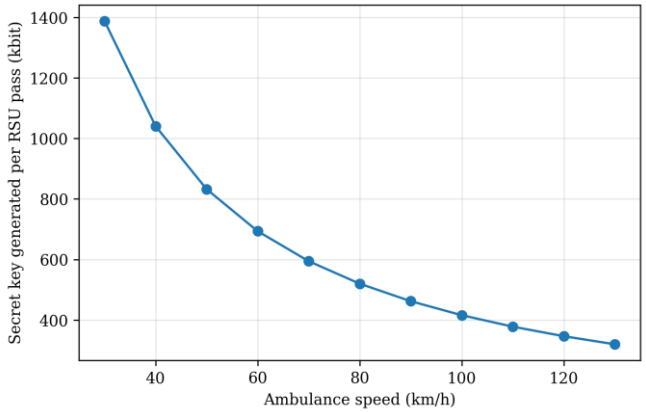

Fig. 12. Integrated secret-key yield during one 160-m QVU pass versus ambulance speed.

Fig. 12 expresses mobility in key-budget terms through the integral in (22). The integrated secret-bit yield per nominal QVU pass decreases from about 1.39 Mbit at 30 km/h to 0.694 Mbit at 60 km/h, 0.462 Mbit at 90 km/h, and 0.347 Mbit at 120 km/h. The inverse proportionality to speed predicted by (22) is reproduced almost exactly, since doubling the speed halves the harvested yield. Thus, even when instantaneous SKR is unchanged at a given position, a fast ambulance has less time to replenish its buffer. Route-aware prefetch and an explicit reserve are therefore necessary for emergency vehicles that may travel substantially faster than normal urban traffic.

I. Medical-Traffic Latency and Deadline Satisfaction

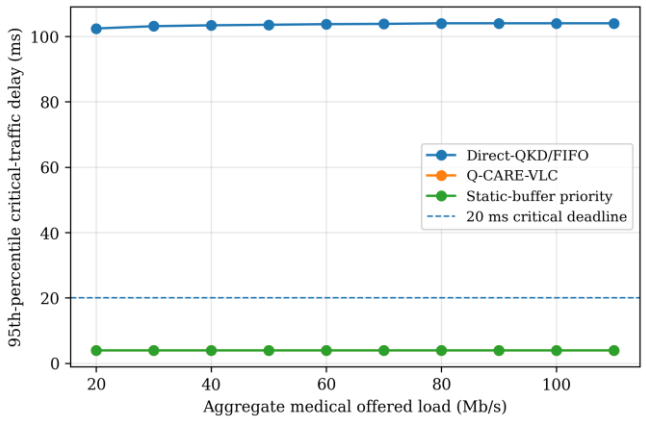

Fig. 13. 95th-percentile critical-traffic delay versus aggregate medical offered load.

The network architecture matters most when the physical channel is translated into a clinical quality-of-service metric. Fig. 13 shows the 95th-percentile delay of C1 traffic. At a 60 Mb/s aggregate load, Direct-QKD/FIFO reaches approximately 103.7 ms because key interruptions and non-priority queueing block critical telemetry. Static-buffer priority and Q-CARE-VLC both keep C1 near the 4-ms processing floor under the modeled capacity. At 80 and 100 Mb/s, Q-CARE-VLC continues to preserve the critical queue because C1 represents a small but high-value fraction of the total load, while congestion is absorbed primarily by C2 and C3.

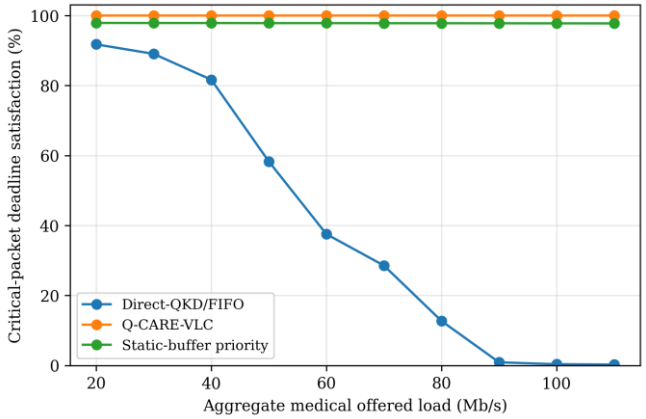

Fig. 14. Critical medical deadline satisfaction versus aggregate offered load.

Fig. 14 makes the safety effect explicit. At an 80 Mb/s aggregate medical load, the Direct-QKD/FIFO baseline satisfies the 20-ms C1 deadline in only 12.69% of simulated slots. Static-buffer priority reaches 97.78%, whereas Q-CARE-VLC reaches 100%. At 100 Mb/s, Direct-QKD/FIFO falls below 1%, Static-buffer priority remains near 97.75%, and Q-CARE-VLC continues to protect C1. The result does not imply that all traffic is congestion free: at 100 Mb/s, C2 deadline satisfaction is approximately 46.33% for Q-CARE-VLC because the scheduler intentionally sacrifices interactive-media timeliness before critical telemetry. This is the intended clinical behavior.

J. Intercept-Resend Response

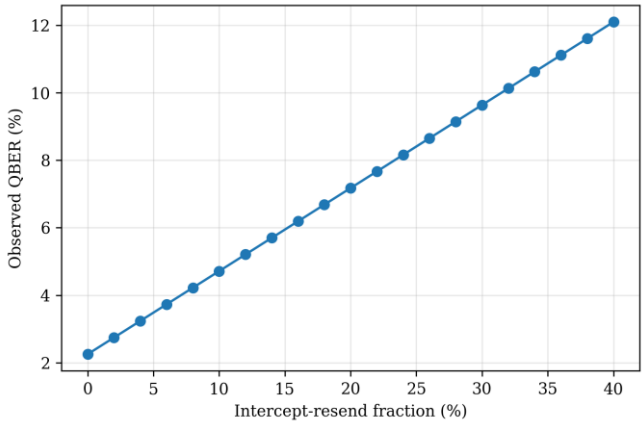

Fig. 15. QBER versus the fraction of quantum pulses exposed to an intercept-resend adversary.

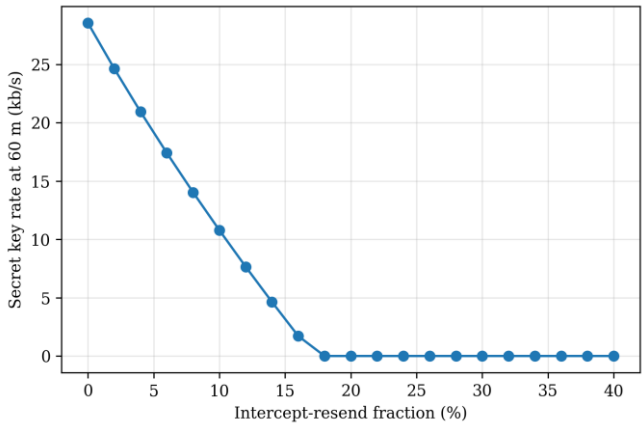

Fig. 16. Secret-key rate versus intercept-resend fraction for the representative 60-m quantum link.

Figs. 15 and 16 demonstrate the security response of the QKD plane. With no active interception, the representative 60-m link has a modeled QBER of approximately 2.25% and an SKR of 28.55 kb/s. As the intercept-resend fraction increases, QBER rises according to (19) and privacy amplification removes a larger share of the raw key. At a 10% intercept fraction the model produces about 4.71% QBER and 10.78 kb/s SKR; by 20% interception the QBER is about 7.18% and the selected asymptotic secure-rate expression yields no positive secret key. This behavior is qualitatively different from classical optical confidentiality: an adversary cannot copy arbitrary quantum states without changing the statistics used for key estimation.

K. Aggregate Comparison

Table IV consolidates the nominal operating point. Read together with (17), (20), and (21), it shows that the three metrics improve for the same architectural reason - the standby aperture removes the acquisition gap that would otherwise empty the reservoir precisely when the vehicle is furthest from both roadside units.

TABLE IV: NOMINAL SYSTEM-LEVEL COMPARISON AT 80 KM/H AND 75-KB/S KEY-REFRESH DEMAND

Scheme	**Quantum handover**	**Key policy**	**Continuity Θ (%)**	**Interruption Ξ (%)**	**C1 deadline Ψ_1 at 80 Mb/s**
Direct-QKD/FIFO	Break-before-make	No adaptive reserve	78.77	6.25	12.69%

Static-buffer priority	Single aperture, shorter gap	Static reserve	80.16	2.50	97.78%
Q-CARE-VLC	**Dual-aperture make-before-break**	**Priority-aware reserve**	**100.00**	**0.42**	**100%**

9. Conclusion

Q-CARE-VLC proposes a quantum-secured vehicular visible-light communication(VLC) architecture for connected ambulances and smart emergency healthcare. The framework deals with a basic mismatch between classical and quantum optical communications. The classical VLC channel can support tens to hundreds of megabits per second over realistic V2I distances, while the quantum key distribution (QKD) channel yields a significantly smaller and very fluctuating secret-key rate which is highly sensitive to distance, background illumination, atmospheric conditions and pointing errors. When QKD is assumed to be always available, key starvation and communication breaks even if the classical channel is working are caused. To address this problem, Q-CARE-VLC views quantum keys as a buffered network resource rather than a resource that has to be generated on-the-fly for each packet. The proposed architecture consists of a high-speed vehicular-VLC data plane, co-aligned deco-aligned state BB84 quantum channel, trusted roadside quantum-VLC units, a hospital key orchestrator, a dual-aperture quantum terminal, and a clinically aware key manager. The critical feature is a make-before-break quantum handover mechanism, which provides the establishment and authentication of the next roadside quantum link before the previous one is broken. During the period of overlap, new keys are gathered, and the key manager buffers keys for life-critical physiological telemetry, and relaxes rekeying requirements for less critical services in the event of a temporary degradation of the quantum channel. The proposed design is effective as illustrated in the results of the simulation. With daytime clear-air conditions, the secret-key link rate modeled is reduced by four orders of magnitude, from 70.62 kb/s at 40 m to 1.03 kb/s at 150 m, while the classical VLC link rate is still about 83.11 Mb/s at 80 m. The results showed that Q-CARE-VLC maintained 100% quantum secure communication continuity under the demand of 75kb/s aggregate key-refresh, outperforming direct break-before-make QKD (78.77%) and static-buffer QKD (80.16%). The handover interruption fraction was decreased from 6.25% to 0.42% at 80kmph. Moreover, last-mile users have 100% compliance with the critical medical traffic 20 ms deadlines for the offered load of 80 Mb/s in the face of a load of medical and non-critical traffic, such as video and medical records, absorbing congestion. In general, Q-CARE-VLC provides a system to jointly optimize mobility, cryptographic key management, and clinical service prioritization while guaranteeing key continuity. The architecture is a viable approach to deployable quantum secured emergency healthcare networks, and future avenues of research include hardware-in-the-loop validation and finite-key experimental characterization.

REFERENCES

1. G. M. Dotreppe, A. Mentens, J. Coosemans, P. Van den Bossche, and V. A. Jacobs, "Shedding light on vehicular communication: A review of the latest vehicular visible light communication channel models," *IEEE Commun. Surveys Tuts.*, early access, Jun. 2025, doi: 10.1109/COMST.2025.3576289.
2. M. Karbalayghareh, F. Miramirkhani, H. B. Eldeeb, R. C. Kizilirmak, S. M. Sait, and M. Uysal, "Channel modelling and performance limits of vehicular visible light communication systems," *IEEE Trans. Veh. Technol.*, vol. 69, no. 7, pp. 6891-6901, Jul. 2020.
3. B. Turan and S. Coleri, "Machine learning based channel modeling for vehicular visible light communication," *IEEE Trans. Veh. Technol.*, vol. 70, no. 10, pp. 9659-9672, Oct. 2021.
4. B. Turan, O. Narmanlioglu, O. N. Koc, E. Kar, S. Coleri, and M. Uysal, "Measurement based non-line-of-sight vehicular visible light communication channel characterization," *IEEE Trans. Veh. Technol.*, vol. 71, no. 9, pp. 10110-10114, Sep. 2022.
5. M. De Vincenzi *et al.*, "Vehicular communication security: Multi-channel and multi-factor authentication," *IEEE Trans. Veh. Technol.*, vol. 75, no. 2, pp. 1779-1792, Feb. 2026, doi: 10.1109/TVT.2025.3598113.
6. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comput., Syst. Signal Process.*, Bangalore, India, 1984, pp. 175-179.
7. H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," *Phys. Rev. Lett.*, vol. 94, no. 23, 2005, Art. no. 230504.

8. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A*, vol. 72, no. 1, 2005, Art. no. 012326.
9. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, pp. 1301-1350, Sep. 2009.
10. A. Conrad *et al.*, "Drone- and vehicle-based quantum key distribution," 2025, *arXiv:2505.17587*.
11. P. Zhang *et al.*, "Daylight quantum key distribution over free-space optics for future security networks," *J. Opt. Commun. Netw.*, vol. 17, no. 6, pp. B61-B70, Jun. 2025, doi: 10.1364/JOCN.553171.
12. H. T. Le, H. T. T. Pham, H.-C. Le, and N. T. Dang, "Satellite quantum key distribution for vehicular visible light communication networks," in *Proc. IEEE 8th Int. Conf. Commun. Electron. (ICCE)*, Phu Quoc Island, Vietnam, Jan. 2021, pp. 45-50, doi: 10.1109/ICCE48956.2021.9352118.
13. D. S. Fowler, C. Maple, and G. Epiphaniou, "A practical implementation of quantum-derived keys for secure vehicle-to-infrastructure communications," *Vehicles*, vol. 5, no. 4, pp. 1586-1604, Nov. 2023, doi: 10.3390/vehicles5040086.
14. H. Yuan, D. S. Fowler, C. Maple, and G. Epiphaniou, "Analysis of outage performance in a 6G-V2X communications system utilising free-space optical quantum key distribution," *IET Quantum Commun.*, vol. 4, no. 4, pp. 191-199, Dec. 2023, doi: 10.1049/qtc2.12067.
15. B. Mallick *et al.*, "Multi-channel multi-protocol quantum key distribution system for secure image transmission in healthcare," *IEEE Access*, vol. 13, pp. 62476-62505, 2025, doi: 10.1109/ACCESS.2025.3558294.
16. R. Zia-Ul-Mustafa, S. S. Boroujeni, C. Guerra-Yanez, Z. Ghassemlooy, H. Le Minh, and S. Zvanovec, "Quantum key distribution for visible light communications: A review," in *Proc. 13th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, 2022, pp. 589-594.
17. P. Sharma, A. Agrawal, V. Bhatia, S. Prakash, and A. K. Mishra, "Quantum key distribution secured optical networks: A survey," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 2049-2083, 2021.
18. S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012-1236, Dec. 2020.
19. W. Li *et al.*, "High-rate quantum key distribution exceeding 110 Mb s^{-1}," *Nature Photon.*, vol. 17, no. 5, pp. 416-421, May 2023, doi: 10.1038/s41566-023-01166-4.
20. M. Zahidy *et al.*, "Practical high-dimensional quantum key distribution protocol over deployed multicore fiber," *Nature Commun.*, vol. 15, 2024, Art. no. 1651, doi: 10.1038/s41467-024-45876-x.
21. A. Stavdas *et al.*, "Quantum key distribution for V2I communications with software-defined networking," *IET Quantum Commun.*, vol. 5, no. 1, pp. 38-45, Mar. 2024, doi: 10.1049/qtc2.12070.
22. C. Liu, L. Feng, J. Wang, H. Sun, R. Q. Hu, and H. Lu, "IRS-VLC physical layer security scheme: A dual-strategy against eavesdropping and attacks," *Appl. Opt.*, vol. 64, no. 3, pp. 703-711, Jan. 2025, doi: 10.1364/AO.540543.
23. *IEEE Standard for Local and Metropolitan Area Networks - Part 15.7: Short-Range Optical Wireless Communications*, IEEE Standard 802.15.7-2018, 2019.
24. *IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages*, IEEE Standard 1609.2-2022, 2023.
25. *Advanced Encryption Standard (AES)*, FIPS PUB 197, Nat. Inst. Standards Technol., Gaithersburg, MD, USA, 2023.
26. M. Dworkin, "Recommendation for block cipher modes of operation: Galois/Counter Mode (GCM) and GMAC," Nat. Inst. Standards Technol., Gaithersburg, MD, USA, NIST Special Publication 800-38D, 2007.
27. *Health Informatics - Point-of-Care Medical Device Communication - Part 10201: Domain Information Model*, ISO/IEEE Standard 11073-10201, 2004.
28. M. Uysal, C. Capsoni, Z. Ghassemlooy, A. Boucouvalas, and E. Udvary, Eds., *Optical Wireless Communications: An Emerging Technology*. Cham, Switzerland: Springer, 2016.
29. Z. Ghassemlooy, W. Popoola, and S. Rajbhandari, *Optical Wireless Communications: System and Channel Modelling With MATLAB*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2019.
30. F. M. Alsalami, Z. Ahmad, S. Zvanovec, P. A. Haigh, O. C. L. Haas, and S. Rajbhandari, "Statistical channel modelling of dynamic vehicular visible light communication system," *Veh. Commun.*, vol. 29, 2021, Art. no. 100339.
31. M. A. Vieira, M. Vieira, P. Louro, P. Vieira, and R. Fernandes, "Adaptive traffic control using cooperative communication through visible light," *SN Comput. Sci.*, vol. 5, no. 1, 2024, Art. no. 159, doi: 10.1007/s42979-023-02483-9.
32. X. Jing, Y. Wu, F. Yu, Y. Xu, and X. Wang, "Reconfigurable intelligent surface-aided security enhancement for vehicle-to-vehicle visible light communications," *Photonics*, vol. 11, no. 12, 2024, Art. no. 1151, doi: 10.3390/photonics11121151.
33. P. Porambage, G. Gur, D. P. M. Osorio, M. Liyanage, A. Gurtov, and M. Ylianttila, "The roadmap to 6G security and privacy," *IEEE Open J. Commun. Soc.*, vol. 2, pp. 1094-1122, 2021.
34. Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution system: Past, present, and future," *Appl. Phys. Rev.*, vol. 11, no. 1, 2024, Art. no. 011318, doi: 10.1063/5.0179566.