OPTICAL WIRELESS COMMUNICATION FROM INFORMATION SECURITY PERSPECTIVES

Engineering Case Studies

Zixian Wei, Rui Deng, Binbin Zhu, Chen Chen, Yanbing Yang, and Changyuan Yu

Point-to-point optical wireless communication (OWC) systems and derived point-to-multipoint optical Internet of Things (O-IoT) broadcasting networks can serve as a secure and reliable means for information protection, emergency communication, and confidentiality management within localized environments. Meanwhile, they may also act as potential tools for covert eavesdropping, weak signal detection, or latent surveillance. We summarize recent advances and potential progress in physical-layer security (PLS) of OWC. Furthermore, several case studies are presented, covering a broad spectral range from ultraviolet to near-infrared (NIR), to illustrate how system-level OWC architectures can enable or defend against optical attacks, interception, and confidential transmission. These cases involve both hardware- and software-defined implementations, including photon counting, digital signal processing, and protocol design, highlighting practical approaches for optical information security management, covert transmission, eavesdropping, and weak signal detection. The discussed methods provide complementary solutions for the design and deployment of secure LANs in the emerging information security era.

Digital Object Identifier 10.1109/MVT.2026.3710587

Introduction

With the evolution from 5G to 6G, the world is entering an era of intelligent and ubiquitous connectivity between humans and machines, as well as among massive numbers of interconnected devices at the network edge. The large-scale integration of edge devices and consumer

electronics, widespread adoption of generative artificial intelligence applications, and an unprecedented surge in network traffic have jointly made wireless access bandwidth, data privacy, and confidentiality concerns among users, network designers, and administrators [1]. Compared with conventional radio frequency (RF)-based near-field wireless communication systems, OWC and the O-IoT, along with their wavelength-specific branches such as visible light communication (VLC), ultraviolet communication, and infrared communication (IRC), have attracted extensive attention due to their unique advantages, including license-free spectrum usage, extremely high potential data rates, and inherent immunity to electromagnetic interference (EMI) [2]. It is estimated that tens of billions of light-emitting diodes (LEDs) are deployed worldwide, which can be rapidly integrated with other smart terminals to form a vast OWC network. Such networks have the potential to meet wireless connectivity demands in indoor networks, the IoT, vehicular networks, and industrial Internets, providing a promising alternative for secure information delivery. On one hand, many previous works were based on the numerical analysis of secrecy capacity theory, ignoring the engineering perspective. The following work is also rooted in classical PLS principles and aligns with recent IEEE 802.15.7 standard discussions [3].

Additionally, traditional security mechanisms are primarily implemented at the upper layers of the network stack, relying on access control, password protection, and end-to-end encryption. These approaches are generally considered secure if the eavesdropper's computational and storage capabilities remain within practical limits. However, recently, the open and densely interconnected wireless environments, coupled with the ubiquitous deployment of distributed computing resources, have posed significant challenges to conventional encryption schemes. To address these issues, PLS over OWC has emerged as an effective complement to traditional cryptographic methods. By exploiting the inherent characteristics of optical free-space channels, PLS can obscure confidential information from unauthorized receivers without relying on computational assumptions [4]. In the ongoing commercialization of OWC technologies, both security and antisecurity aspects have been widely discussed.

Near-Field Optical Access and Security

With the large-scale adoption of edge computing, researchers aim to reduce the computational burden on cloud servers and minimize the transmission overhead caused by redundant data. Consequently, modern edge devices are increasingly expected to support local high-speed data exchange, computation, and encryption processing. As sensing, communication, and computing terminals, these edge devices must continuously acquire, exchange, and process physical world data. As a near-field communication technology that can be seamlessly integrated with lighting infrastructures, OWC provides an energy-efficient solution for establishing localized high-speed data links. Owing to its low power consumption and compatibility with existing illumination systems, OWC has been increasingly adopted by a wide range of edge devices.

On the other hand, edge nodes in near-field IoT networks and lightweight consumer electronic products are often constrained by limited computational resources and power budgets, making it impractical to employ complex encryption or authentication mechanisms. Meanwhile, conventional Wi-Fi or RF-based transmissions inherently face the risk of information leakage due to their broadcast nature. By deploying OWC, O-IoT, or heterogeneous optical–radio hybrid networks, these vulnerabilities can be effectively mitigated, creating secure, interference-resistant, and interception-resilient information space. In practical implementations, a simple opaque physical barrier can serve as an effective spatial delimiter to confine communication within a designated region, essentially forming an optical information enclosure. When combined with multidimensional PLS configurations, such systems exhibit desirable features including covert transmission, distributed predeployment capability, and enhanced resistance to detection and interception.

Light Attack Technology

Eavesdropping can be carried out by many tools. Conventional electronic interception is often relatively easy to detect and, from a practical standpoint, may incur significant operational difficulty and risk. By contrast, optical attack techniques exploit the measurement of extremely weak light signals to extract information in specific scenarios. Such optical attack techniques can be used to recover voice, data, and image content, and they offer several practical advantages, including immunity to EMI, resistance to RF-based jamming, and a high degree of stealth that makes them difficult to detect. Rapidly developing examples include fiber tap and optical cable attacks, fiber-optic voice eavesdropping, laser-based eavesdropping, and optical wireless monitoring. We mainly discuss and demonstrate the technological developments for the last application scenario.

Unlike RF attacks, optical-based methods exploit ubiquitous physical resources in daily life. For example, ordinary illumination or otherwise imperceptible light can carry rich information and silently leak sensitive signals when combined with local sensors or sensor networks. The maturation of these techniques therefore presents renewed challenges to confidentiality protection. It is thus essential to develop methods for detection and localization of optical intrusion (e.g.,

monitoring based on anomalous light signatures and visible light attack detection) and to deploy isolation and secure monitoring systems. Similar topics have become research priorities in many countries. We focus on attacker scenarios and the evolving technical landscape of optical eavesdropping.

In this work, we examine OWC and O-IoT from an information security perspective, highlighting their implications through practical engineering deployment cases in the era of pervasive data confidentiality. Compared with traditional RF channels, optical carriers, particularly those based on ubiquitous illumination, offer a much higher degree of concealment when used for data encryption, signal interception, or eavesdropping. In certain scenarios, optical eavesdropping devices can be integrated directly into lighting drivers, making the attack system visually indistinguishable from standard infrastructure and thus difficult to detect by end users. Techniques such as visible light eavesdropping and weak optical signal detection remain largely underexplored yet present emerging risks in consumer electronic products with increasingly embedded photonic technologies. We summarize that photon counting receivers outperform traditional avalanche photodiode (APD) devices in weak light secure communication, and consumers need to be aware that spectrum monitoring and physical isolation serve as effective defense approaches.

PLS Over Optical Channels

Spatial-Domain PLS

Exploiting spatial relationships or programmable manipulation of the physical properties of optical beams provides an effective pathway toward realizing PLS. For example, a multiuser single-pixel imaging (SPI)-based encryption and authentication framework has been proposed in conjunction with orthogonal frequency division multiplexing (OFDM)-assisted key management. Within this framework, regional and global encryption operations are first performed to generate a composite intensity sequence, which is then transmitted to multiple users while simultaneously producing corresponding user-specific keys. Integrating direct key management with indirect image encryption yields a multiuser computational imaging-based encryption and authentication scheme [5]. In addition, spatiotemporal control over the full degrees of freedom of polarized light has been demonstrated as an effective means to realize spatial-domain PLS in OWC [6].

Frequency-Domain PLS

The color domain, or more generally the frequency domain, inherently provides multichannel transmission capabilities, which can be naturally integrated with a wide range of PLS schemes. This is primarily because an eavesdropper faces significant challenges in simultaneously and synchronously acquiring information across multiple frequency channels [7]. From the receiver perspective, PLS can be further enhanced by carefully selecting detector materials and employing structure-level engineering to exploit the remarkable wavelength-dependent temporal responses of photodetectors [8]. For example, a dual-band photodetector with highly selective responsivities in distinct spectral bands has been developed as an optical signal receiver for PLS in VLC and IRC, where reconfigurable encryption relationships based on geometric arithmetic are employed [9].

Digital-Domain PLS

Digital-domain PLS techniques currently represent the most widely adopted class of solutions, including artificial noise injection, chaos-based encryption schemes, and various digital signal processing (DSP) approaches [7], [10]. These methods remain effective for OWC systems equipped with sufficient computational capabilities. However, for low-power O-IoT operating with limited clock rates, deploying computationally intensive PLS encryption schemes at edge nodes is often impractical. Motivated by the low design and operational cost characteristics of near-field communication, lightweight digital-domain PLS solutions are proposed for mass-produced mobile devices in edge IoT scenarios. Such approaches leverage existing general-purpose modules available on mobile platforms, requiring neither additional dedicated hardware components nor modifications to current hardware architecture.

Protocols in Medium Access Control-Layer Security

Medium access control (MAC)-layer security over the free-space optical channel plays a vital role in safeguarding data confidentiality and integrity, complementing the strong inherent protection provided by the directional nature of light. Beyond managing access, synchronization, and mobility, the OWC MAC layer incorporates protocols for secure key generation, distribution, and encryption, thereby preventing unauthorized access in environments where physical isolation may be insufficient [11]. By integrating encryption and error detection mechanisms, the MAC layer ensures both data privacy and transmission integrity. Importantly, MAC-layer security not only enhances PLS but also improves OWC system efficiency by reducing the dependence on complex upper-layer encryption, leading to higher throughput. It is particularly crucial for sensitive or mission-critical applications where secure and reliable OWC is essential, by combining PLS and MAC-layer security to form a dual protection framework. Overall, MAC-layer security ensures that only authorized devices can access and exchange information, reinforcing a multilayered defense architecture in OWC networks.

Engineering Cases of Confidentiality Management

Classified Factory: Architecture and Traffic Control

Figure 1 presents our engineerable solution of a physically confined high-security OWC architecture designed specifically for sensitive areas within smart factories. The full-duplex (FDX) system leverages a VLC downlink with 100 MHz modulation bandwidth and 10 Mb/s/100 Mb/s/1 Gb/s data streams and an IRC uplink to provide completely EMI-free networking while ensuring that wireless signals cannot escape the designated secure zone, thereby achieving true PLS for confidential R&D laboratories, precision assembly lines, or classified production areas.

First, a unified software-defined control and visualization platform, as shown in Figure 1, centrally manages the entire optical wireless network traffic. This platform integrates real-time link monitoring, adaptive quality of service (QoS) scheduling, automatic fault detection and failover, and emergency early-warning and priority-switching mechanisms, as well as comprehensive security functions including end-to-end data encryption, multifactor authentication, detailed access logging, and role-based jurisdiction control. Administrators can monitor optical link quality, security events, and traffic statistics through an intuitive graphical dashboard, ensuring full situational awareness and rapid response capability across the factory's sensitive zones.

The physical layer architecture forms a secure end-to-end data path that begins at the external Internet or campus LAN, passes through a hardened routing gateway and firewall, and reaches a central server via network cabling. The main switch adopts an RJ45 interface, with dimensions of 550 mm × 320 mm × 780 mm, a weight of 10 kg, and a handover latency below 5 ms. From the server, a DC power-and-data trunk feeds front-end industrial power line communications (PLCs) that act as edge gateways for the optical wireless segment. These PLCs distribute both power and Ethernet traffic to multiple area-confined access nodes strategically placed inside the restricted zones. Downlink is primarily carried by high-brightness LED luminaires that simultaneously provide workspace illumination and visible light data transmission. The Li-Fi headlamp operates at 38 V input voltage and 20 W power, delivering a 5-Mb/s communication rate with a maximum coverage height of 8 m. The transmitted light beams are directed and collimated to create sharp geometric boundaries, guaranteeing zero signal leakage beyond the authorized physical area. Uplink channels predominantly use IR emitters and receivers to avoid interference from ambient light and to further enhance security, especially for mobile terminals such as robotic arms, automated guided vehicles (AGVs), handheld devices, and others equipped with integrated visible light receivers and IR transmitters.

The pictures at the bottom of Figure 1 showcase the actual hardware prototypes successfully developed and validated in real factory environments, including a ceiling-mounted FDX LED as standard factory lighting with an injected current 700 mA, a compact high-sensitivity FDX receiver module, a rugged front-end PLC responsible for protocol conversion and local coordination, and a back-end PLC that orchestrates the entire system and interfaces with the unified management platform. The measured performances in the factory environment are 10–100 Mb/s with bit error rate (BER) < 10^{-6} for VLC downlink and 1–10 Mb/s with BER < 10^{-5} for IR uplink. These data rates satisfy the demands of industrial control, AGV communication, and real-time monitoring, while the low BER ensures reliable transmission under

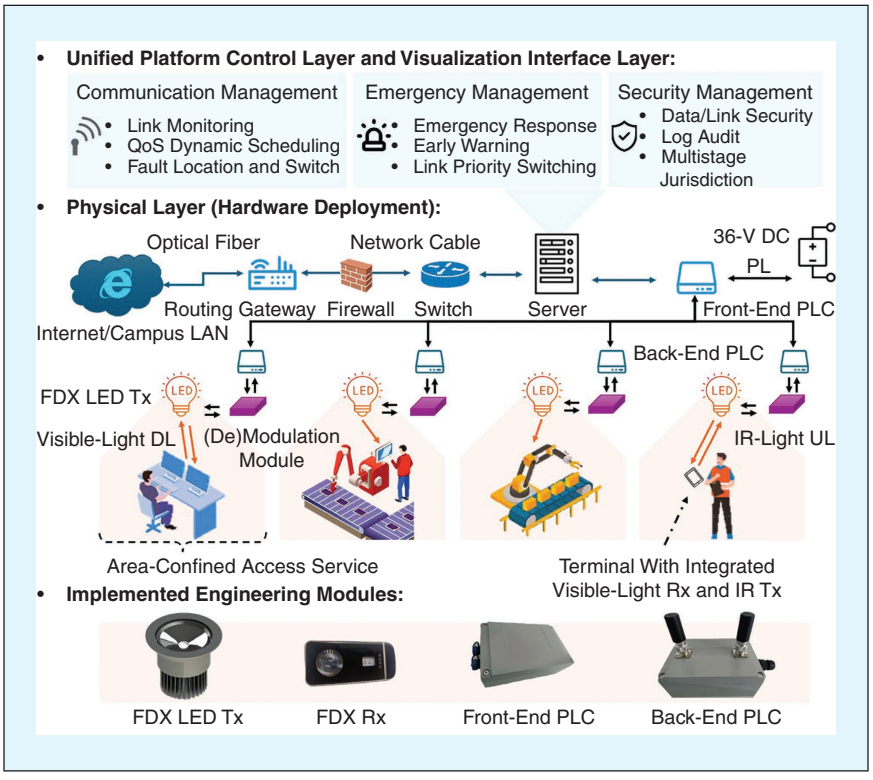

FIGURE 1 A schematic of the overall architecture and prototype implementation of a secure intrafactory wireless optical communication system for area-confined sensitive zones in smart manufacturing environments. Software security architecture and functions, overall hardware system framework, and hardware modules' photos on our proposed engineering case, respectively. DL: down link; FDX: full duplex; PLC: power line communication; PL: power line; Rx: receiver; Tx: transmitter; UL: uplink.

EMI-free and area-confined conditions. Together, these components deliver an industrially practical solution and demonstrate a secure, high-reliability optical wireless networking exclusively within the intended sensitive areas of modern smart factories.

Underground Tunnel: Integrating Power Lines and OWC

In underground tunnel development for subway systems or mineral resource extraction, RF communication faces significant challenges. These tunnels, often extending deep beneath the surface, exhibit weak signal propagation due to dense rock formations, surface absorptions, high humidity, and EMI from machinery, making Wi-Fi or cellular networks unreliable and prone to outages. Moreover, the harsh, variable environment, characterized by dust, vibrations, and limited accessibility, renders the installation of dedicated cabling impractical and costly as it requires extensive drilling, maintenance, and potential disruptions to ongoing operations. This RF communication shortfall not only hampers real-time monitoring, worker safety coordination, and equipment automation but also poses risks in emergency scenarios where reliable data transmission is critical. Therefore, we modified the solution in Figure 1 and applied it to this scenario.

Integrating PLC with VLC offers a transformative solution that simplifies deployment while merging multiple functionalities into a unified network [4]. By leveraging existing power infrastructure for both electricity distribution and PLC, combined with LED-based illumination that doubles as VLC transmitters, this approach eliminates the need for separate cabling deployment. The result is a seamless fusion of illumination, data transmission, and secure connectivity, where light signals are confined to line-of-sight (LoS) paths, inherently providing PLS that prevents eavesdropping from outside the tunnel sections. Furthermore, a centralized management platform enables unified traffic control, multiuser access prioritization, and end-to-end encryption, making it an exemplary case for encrypted OWC applications in confined, high-stakes environments like mining tunnels.

Indoor Optical IoT: Integrating RF and OWC

In large-scale indoor IoT deployments, hundreds or thousands of sensors, actuators, and mobile devices need reliable, low-latency connectivity while maintaining strict information confidentiality. Pure RF solutions easily suffer from interference and spectrum congestion, whereas standalone OWC is limited by LoS requirements and struggles to serve highly mobile or shadowed terminals. A hybrid RF–OWC architecture elegantly resolves these contradictions by combining the non-LoS (nLoS) broadcast capability of RF with the high bandwidth and inherent PLS of directional optical links, creating a scalable O-IoT ecosystem that supports massive device access without compromising security.

The core lies in a physically enhanced encryption mechanism that exploits the complementary nature of the two mediums. Omnidirectional RF channels are used as the primary medium for encrypted payload transmission, offering seamless coverage to all users and sensors regardless of orientation or minor blockages. Simultaneously, highly directional optical beams deliver short-lived session keys or decryption tokens exclusively to authorized terminals located within the illuminated zone. Only devices that correctly receive the optical key, possible solely when they are physically present in the intended area and properly aligned, can decrypt the RF payload. Eavesdroppers capturing only the RF signal, even if located nearby, remain unable to reconstruct the original information without the corresponding optical key, achieving a practical "light-as-key" security model that combines the convenience of RF coverage with light's natural spatial confinement and provides a compelling, deployment-ready use case for secure O-IoT networks. Furthermore, lightweight and real-time optical intrusion detection protocols will be designed specifically for resource-constrained edge O-IoT nodes. Such protocols can detect abnormal optical signals, spectral anomalies, and potential eavesdropping behaviors with low computational complexity, enabling distributed and proactive security monitoring for large-scale optical wireless networks.

Emergency Voice Encrypted Communication

In high-risk industrial environments such as petrochemical plants, underground mines, and large-scale manufacturing facilities, frontline workers must always carry personal lighting equipment, such as headlamps or handheld torches, for safety and operational needs. In Figure 2, we have developed a compact, retrofittable module that seamlessly integrates into these existing illumination devices, adding fully digital-domain encrypted voice communication capability without increasing weight, volume, or operational burden. Under normal conditions, the device functions as a standard high-brightness LED light source. However, in emergency situations when RF systems fail due to interference, explosion-proof restrictions, or infrastructure damage, it instantly transforms the same LED into a directional secure voice transmission. By modulating encrypted voice packets onto the illumination beam, nearby colleagues within the light cone can receive and decode the audio in real time through compact receivers embedded in their own headlamps or safety helmets, as shown in Figure 2. This "voice-over-light" mechanism provides a completely independent and inherently confidential emergency communication channel that leverages equipment workers already

carry, offering a life-saving fallback layer with zero additional wearable load.

Eavesdropping or Light Attack Engineering Cases

Although OWC is widely celebrated for its PLS, the same optical channel can be weaponized in the opposite direction to create an extremely stealthy eavesdropping vector that is nearly impossible to detect using conventional countermeasures. Here we will discuss typical light attack cases, including one of our own engineering implementation examples. Overall, in this section, the purpose of illustrating these optical attack scenarios is strictly for security vulnerability assessment and defensive system design, rather than providing operational guidance. Identifying such hidden risks will promote the development of effective countermeasures, such as optical monitoring, spectral anomaly detection, and secure lighting control in future OWCs.

Visible Light Long-Reach Eavesdropping

Figure 3 presents a fully functional prototype that demonstrates the feasibility and alarming stealth of visible light side-channel eavesdropping using daily indoor illumination. By embedding a miniature eavesdropping payload into an LED ceiling lamp equipped with a microprogrammed control unit and driver, the system transforms normal room lighting with ~30 W launched optical power into a clandestine optical transmitter capable of exfiltrating high-quality speech without any perceptible change in illumination or detectable radio emissions. Here we explicitly define the attacker's capabilities with feasible eavesdropping distance up to 50 m, telescope-based optical reception, LoS requirement, narrowband spectral filtering, and basic synchronization. Furthermore, we assume that the eavesdropping victim is unaware of the existence of light attacks.

Figure 3 details the DSP chain at the covert transmitter side. Ambient speech inside the target room is first captured by a concealed microphone integrated within the lamp. The analog audio signal undergoes A/D conversion, digital buffering, and real-time low-bitrate compression encoding. A modulation and current-control block then superimposes the encoded bitstream onto the LED drive current at flicker frequencies ≥2 kHz, ensuring no observable flickering while preserving full illumination functionality. The modulated light is broadcast omnidirectionally through the existing diffuser, effectively turning the entire luminous flux into a covert data carrier. Figure 3 illustrates the corresponding receiver architecture and experimental deployment. Outdoor experiments were conducted at standoff distances of 50 m and extended to over 100 m under clear LoS conditions. The receiver front end consists of a commercial telescope as optical antenna coupled to an APD module (Hamamatsu, C12702-11, 100 MHz, 5-V driven voltage). The spectral response range is 320–1,100 nm, and the peak sensitivity wavelength is >800 nm. The sensitivity is generally lower than 0.3 A/W in the commonly used blue light range. The signal passes through a transimpedance amplifier (TIA), bandpass filtering, and A/D conversion before demodulation and audio reconstruction.

Figure 2 Real-time voice communication between staff and the back-end command center is achieved through emergency lighting equipment as the access point. The figure includes photos of the main components for practical emergency deployment. (a) A smart helmet. (b) A Li-Fi LED access point. (c) An emergency flashlight. (d) An illustration of the actual deployment. The black line represents the power line for Li-Fi LED at different locations.

Figure 3 shows several commercial visible light receiver prototypes, where we used a compact APD receiver with integrated TIA and digitizer as an example case. The complete outdoor receiving station comprises a telescope, APD head, real-time evaluation board, and noise-canceling headphones for immediate playback. The bottom left waveforms in Figure 3 compare the recovered speech before transmitting and after the final D/A stage. The waveform before transmitter (Tx) A/D conversion represents the ideal clean digital baseband signal. The waveform after receiver (Rx) D/A conversion and optical transmission shows minor distortions caused by finite circuit bandwidth, analog filtering, thermal noise, and mild nonlinearity during electro-optical conversion. Despite these practical impairments, the recovered signal

maintains high fidelity and intelligibility at 50 m. The eye diagram is shown at 5 Mb/s with non-return-to-zero on-off keying modulation format at 30-m range.

This prototype conclusively demonstrates that a low-cost, physically indistinguishable modification of widely deployed LED lighting can establish a persistent, high-fidelity optical covert channel immune to RF jamming, Wi-Fi shutdown, or spectrum monitoring. Because the attack leverages the very light required for normal room functionality and produces no anomalous electromagnetic signature, conventional countermeasures, such as RF bug sweeps, Faraday shielding, or network isolation, are rendered ineffective. To take measures against light eavesdropping, the defender should configure some capabilities including optical spectrum monitoring, abnormal flicker detection, secure LED driver design, physical isolation, and link-level authentication.

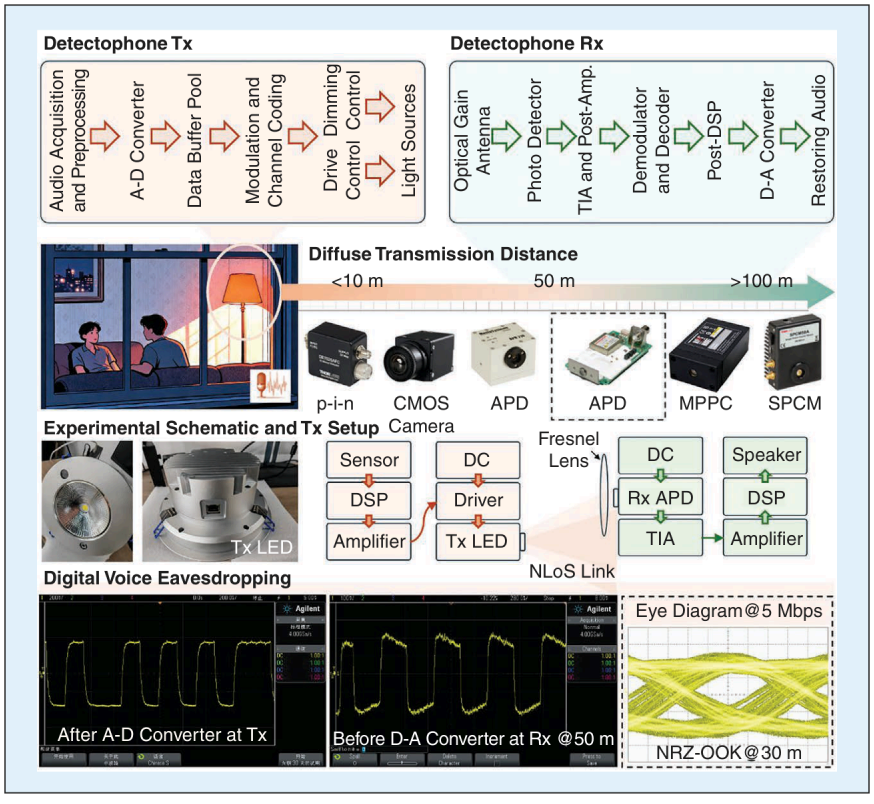

Figure 3 An engineering prototype of a covert visible light eavesdropping system exploiting compromised LED lighting infrastructure. The transmitter and receiver DSP of the detectophone are shown. Different visible light receiver types can cover different diffuse transmission distances. The photon counting modules, such as multipixel photon counters (MPPCs) (Hamamatsu) and single-photon counting modules (SPCMs) (Thorlabs), can detect diffuse transmission signals at the level of several hundred meters. Avalanche photodiode (APD) modules can usually detect tens of meters of transmitted signals. The experimental schematic is used to show the physical layout of the overall eavesdropping system, and Tx LED modules with different angles are embedded. As an engineering example, we show the waveform comparison between voice transmission and eavesdropping reception under 50-m transmission distance and show the eye diagram at 5-Mb/s non-return-to-zero on-off keying (NRZ-OOK) format using an APD module (Hamamatsu, C12702-11, 100 MHz). TIA: transimpedance amplifier.

Weak Light Signal Receiver

Silicon-based photodetectors, represented by positive-intrinsic-negative (p-i-n) and APD, remain the most widely adopted receivers in VLC due to their maturity, cost efficiency, and compatibility with consumer electronics. When operating in extremely low-light or photon-starved regimes, conventional p-i-n and APD receivers become inadequate. Single-photon avalanche diodes (SPADs) enable single-photon sensitivity with excellent timing resolution, making them suitable for ultra-low-power VLC eavesdropping, covert communication, and PLS monitoring. Single-photon counting modules (SPCMs) integrate SPADs with quenching and counting electronics, providing turnkey solutions for laboratory and proof-of-concept systems where stability and ease of use are prioritized.

For applications requiring both high sensitivity and wider dynamic range, silicon photomultipliers (SiPMs), also known as multipixel photon counters (MPPCs) in Hamamatsu implementations, combine arrays of micro-SPADs to enable photon-number-resolving detection. These devices are well suited for secure OWC and O-IoT scenarios where weak signal detection and spatial or spectral diversity are required. We summarize and compare these four typical visible light weak light receivers in Table 1.

Laser Microphone or Optical Vibrometry

Optical vibrometry, commonly referred to as the laser microphone, remains the most classic and widely recognized form of optical eavesdropping. From standoff distances of several tens to hundreds of meters, an attacker directs an invisible infrared laser beam toward everyday objects inside the target room that are visible from the outside. Acoustic waves generated by indoor speech induce micrometer-scale mechanical vibrations on the object's surface, which in turn modulate the phase or intensity of the reflected laser light. By collecting the backscattered beam with a telescopic receiver and applying coherent detection techniques such as self-mixing interferometry or homodyne demodulation, the attacker can faithfully reconstruct intelligible

TABLE 1 *A comparison of SPAD, SPCM, SiPM, and MPPC in visible light weak light detection.*

*Parameter**	*SPAD*	*SPCM*	*SiPM*	*MPPC*
Basic structure	Single avalanche diode operated in Geiger mode	Integrated SPAD + quenching + counting electronics	Array of micro-SPAD cells connected in parallel	Same as SiPM (Hamamatsu implementation of SiPM)
Spectral range	~350–1,000 nm	~350–900 nm	~320–900 nm	~320–900 nm
Quantum efficiency	40%–70% (at ~500–600 nm)	50%–70%	30%–60%	30%–60%
Gain	~10^6–10^7 (Geiger mode avalanche)	~10^6–10^7	~10^5–10^6 (sum of microcells)	~10^5–10^6
Dark count rate	10–1,000 cps (depending on area and temperature)	25–250 cps	10^4–10^6 cps/mm^2	10^4–10^6 cps/mm^2
Timing resolution	20–100 ps	50–350 ps	100–300 ps	100–300 ps
Dynamic range	Limited (single-photon level)	Limited	Wide (counts multiple photons simultaneously)	Wide
Photon number resolution	No (binary output)	No (binary output)	Yes (analog sum of microcells)	Yes (analog sum of microcells)
Afterpulsing probability	0.1%–5%	0.1%–5%	<1%	<1%
Operation mode	Single-photon detection; gated or free running	Plug-and-play single-photon counting	Analog output proportional to photon number	Analog output proportional to photon number
Temperature sensitivity	High (requires cooling for low noise)	Moderate (thermoelectrically cooled)	Moderate	Moderate
Advantages	Ultrahigh sensitivity, low jitter	Turnkey single-photon detection	High dynamic range, photon number resolving	Compact, cost-effective SiPM version
Limitations	Low count rate, limited dynamic range	Bulky, high cost	Higher dark noise, moderate timing	Similar to SiPM

*All values are typical performance parameters of commercial single-photon detectors and silicon photomultipliers, which are consistent with manufacturer datasheets and the related literature.

conversations with remarkable clarity. Because the method produces no radio emissions and requires only an unobstructed LoS path, it evades conventional RF countermeasures and continues to pose a persistent, stealthy threat in both intelligence and commercial espionage scenarios.

Subcutaneous Eavesdropping

One emerging and highly covert application of OWC in eavesdropping involves integrating it with multimedia acquisition and subdermal storage, effectively creating a biohybrid system for discreet data logging. Wearable devices equipped with sensors passively or actively capture ambient speech, audio signals, or even low-resolution video feeds from the environment. The collected multimedia data are then modulated onto an NIR beam emitted by the wearable device, which penetrates the skin and underlying tissues, exploiting the biological window of NIR (700–900 nm) with low tissue absorption, allowing transmission depths of several millimeters to centimeters depending on tissue type. Beneath the skin, an implantable photodetector array coupled with a miniaturized storage chip receives and demodulates the optical signal and securely records the data without any external radio emissions or detectable surface activity. This approach not only ensures electromagnetic silence to evade RF detection but also leverages the body's own opacity as a natural barrier, making the system ideal for high-stakes scenarios like undercover operations, medical monitoring, or illicit espionage where traditional wearables might be compromised or confiscated. Early prototypes demonstrated in biomedical optics have achieved data rates up to 10 Mb/s for subdermal optical links, with potential for PLS to further enhance confidentiality [12].

Further optimizations will be conducted to improve the miniaturization, power efficiency, and achievable data rate of subdermal optical communication links. By utilizing high-efficiency microlight sources, low-noise compact photodetectors, and the low-absorption biological window in the NIR band, more robust and higher-speed implantable optical transmission can be realized.

Techniques to Enhance the Detection of Weak Light Signals

In this section, we briefly describe four emerging weak light detection enhancement techniques in addition to traditional optical front-end enhancements, such as compound parabolic concentrators and narrowband optical filters, and diversity techniques in the temporal or spatial domains.

Photon Counting

Photon counting techniques, represented by SPAD and SPCM, detect and process individual photon arrival events, making them particularly effective in photon-starved OWC scenarios. By exploiting the statistical properties of photon arrivals, such receivers enable reliable data recovery at extremely low optical power levels, where conventional intensity-based detection fails [13]. SiPM is not a strict single-photon counting device, but it operates on photon counting principles, providing photon-number-resolving capability.

To compare the advantages of photon counting-based visible light OWC detection schemes with traditional APD-based solutions, we conducted a series of experiments. Specific experimental details are omitted here. Under indoor conditions, as shown in Figure 4, receivers based on SiPM or SPAD often exhibit higher sensitivity, extending detection distances to the hundreds of meters. For example, under the same Mb/s-level transmission rate and hard-decision forward error correction threshold, compared with the two similar configuration schemes of LED transmitter, APD and SiPM, the latter can improve the receiving sensitivity of ~35 dB and the transmission distance of ~20 m. However, due to limitations in both modulation bandwidth and signal-to-noise ratio, their communication rates are currently relatively limited, although still sufficient to cover the range of voice-oriented OWC.

Reconfigurable Retroreflector

Reconfigurable microelectromechanical systems (MEMS)-based retroreflectors enhance weak optical

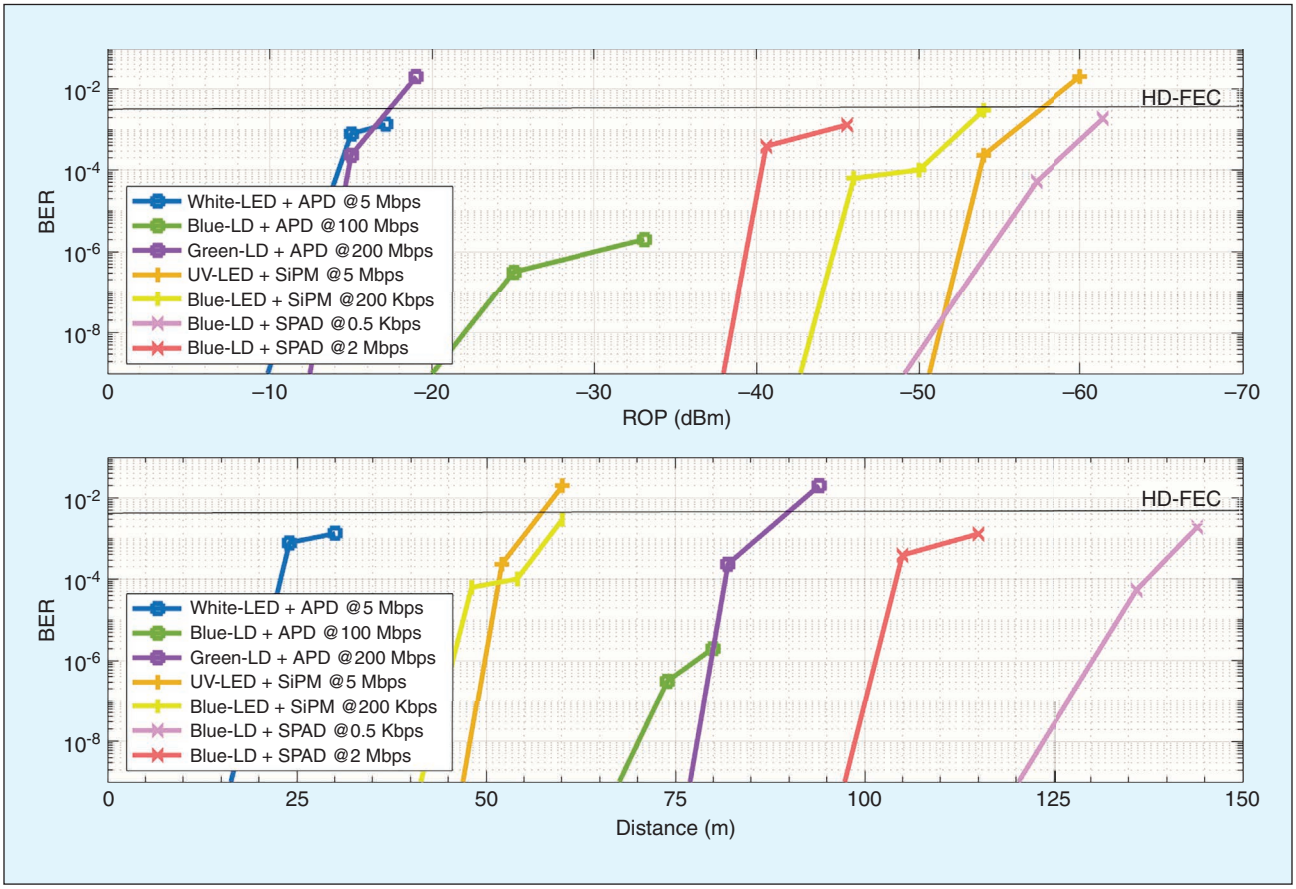

FIGURE 4 The BER performances of different transmitters and receivers at different received optical powers (ROPs) and transmitting distances. Within the hard-decision forward error correction (HD-FEC) of 3.8×10^{-3}, the OWC scheme based on a traditional APD was compared with that based on photon counting (SiPM and SPAD), and the latter can improve sensitivity and link distance. All experiments employ NRZ-OOK modulation format under identical ambient light conditions, without adopting any source or channel coding schemes. For the seven total control groups, the receiver models from top to bottom are APD 1 (Hamamatsu, C12702-11, 100 MHz), APD 2/3 (MenloSystems APD210, 1 GHz), SiPM 4/5 (JAMP-TP6050-SMT, Joinbon), and SPAD 6/7 (Thorlabs, SPCM20, 25-Hz dark count rate). In addition, the blue LD is 450 nm LD (Thorlabs, PL450B), the green LD is 520 nm LD (Thorlabs, L520P50), and the white LED and UV LED are commercial LEDs. LD: laser diode.

links by actively reflecting incident light back toward the transmitter with minimal angular dispersion. This approach enables efficient two-way or directed communication without active optical emission at the remote node, improving link budget and sensitivity in low-power or energy-constrained OWCs [14]. Similarly, active reconfigurable metasurfaces or optical intelligent reflecting surfaces (IRSs) can also be used as a new tool to enhance sensitivity during channel propagation. By dynamically adjusting the phase and reflection direction of optical waves in a programmable manner, optical IRSs can further enhance link gain, mitigate blockage effects, and improve weak signal reception performance for energy-constrained OWC systems.

Beamforming

Optical beamforming concentrates transmitted or received optical energy in specific spatial directions, increasing the effective optical power density at the receiver. An optical phased array-based beam steering or forming is a typical example. By reducing spatial spreading and suppressing off-axis interference, beamforming improves detection sensitivity and robustness in weak signal and long-distance links.

Computational Optics

Computational optics enhances weak light detection by jointly optimizing optical system and DSP design. Through techniques such as computational SPI, temporal ghost imaging [5], [15], inverse reconstruction, and model-based signal recovery, it enables reliable extraction of communication signals from noisy, distorted, or low-photon-count optical measurements.

Conclusions

From an information security perspective, this work provides a detailed discussion on optical PLS and attack techniques within the frameworks of OWC. The proposed PLS strategies span both the physical and digital domains and are exemplified through an engineering case study involving a hybrid PLC–VLC deployment. Before weak light signal detection toolkits become ubiquitous in consumer electronics, OWC and O-IoT systems inherently maintain advantages in local information security and data flow management owing to their spatial confinement and LoS properties. Additionally, optical attack technologies leverage diverse weak signal detection principles enabling high-stealth and high-precision eavesdropping. As the LED-based lighting industry and photonics-enabled sensors in consumer electronics continue to advance and proliferate, optical eavesdropping and O-IoT monitoring are emerging as new forms of information interception. Consequently, the consumer electronics sector must recognize the potential security and confidentiality risks associated with these techniques and take proactive measures by enhancing awareness and deploying corresponding optical monitoring and detection tools.

Acknowledgment

This work was supported by the RGC Junior Research Fellow Scheme (JRFS2526-5S09), the Hong Kong Research Grants Council (GRF15236424 and GRF15231923), the State Key Laboratory of Photonics and Communications Open Project Fund (2026QZKF01), the Key Laboratory of Photonic-Electronic Integration and Communication-Sensing Convergence Open Project Fund (PICCSC202608), and the Sixth Batch of Leading Scientific Research Projects of China National Nuclear Corporation (CNNC-LCKY-2025-085).

Author Information

Zixian Wei (zixian.wei@polyu.edu.hk) is with The Hong Kong Polytechnic University, Hong Kong SAR, China.

Rui Deng (r.deng@hccl-tech.com) is with Shenzhen Hua Chuang Chip Lighting Technology Co., Ltd., Shenzhen 518017, China.

Binbin Zhu (binbin.zhu@hccl-tech.com) is with Shenzhen Hua Chuang Chip Lighting Technology Co., Ltd., Shenzhen 518017, China.

Chen Chen (c.chen@cqu.edu.cn) is with Chongqing University, ChongQing 400044, China.

Yanbing Yang (yangyanbing@scu.edu.cn) is with Sichuan University, Chengdu 610065, China.

Changyuan Yu (changyuan.yu@polyu.edu.hk) is with The Hong Kong Polytechnic University, Hong Kong SAR, China.

References

[1] A. Chorti et al., "Context-aware security for 6G wireless: The role of physical layer security," *IEEE Commun. Standards Mag.*, vol. 6, no. 1, pp. 102–108, Mar. 2022, doi: 10.1109/MCOMSTD.0001.2000082.

[2] Z. Wei, Z. Wang, J. Zhang, Q. Li, J. Zhang, and H. Y. Fu, "Evolution of optical wireless communication for B5G/6G," *Prog. Quantum Electron.*, vol. 83, May 2022, Art. no. 100398, doi: 10.1016/j.pquantelec.2022.100398.

[3] W. Jin-Yuan et al., "Physical-layer security for indoor visible light communications: Secrecy capacity analysis," *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6423–6436, Dec. 2018, doi: 10.1109/TCOMM.2018.2859943.

[4] V. Jungnickel et al., "LiFi for Industrial wireless applications," in *Proc. Opt. Fiber Commun. Conf. (OFC)*, 2020, pp. 1–3.

[5] H. Zeng et al., "Multiuser computational imaging encryption and authentication with OFDM-assisted key management," *Adv. Photon. Nexus*, vol. 3, no. 5, 2024, Art. no. 056016, doi: 10.1117/1.APN.3.5.056016.

[6] J. Lv et al., "Spatiotemporally modulated full-polarized light emission for multiplexed optical encryption," *Nature Commun.*, vol. 15, no. 1, 2024, Art. no. 8257, doi: 10.1038/s41467-024-52358-7.

[7] S. Soderi and R. De Nicola, "6G networks physical layer security using RGB visible light communications," *IEEE Access*, vol. 10, pp. 5482–5496, 2022, doi: 10.1109/ACCESS.2021.3139456.

[8] J. Wu, R. Zhang, S. Yao, Z. Hou, and C.-Z. Ning, "High-gain PMMA-modified graphene photodetectors for dual-wavelength secure communication utilizing distinct temporal photoresponses," *Adv. Sci.*, vol. 13, no. 25, 2025, Art. no. 2501294.

[9] Z. Wang et al., "High speed dual-band photodetector for dual-channel optical communications in wavelength division multiplexing and security enhancement," *Adv. Funct. Mater.*, vol. 34, no. 17, 2024, Art. no. 2310911.

[10] A. Yesilkaya et al., "Physical-layer security in visible light communications," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5, doi: 10.1109/6GSUMMIT49458.2020.9083799.
[11] S. Parvaneh, M. Erol-Kantarci, and M. Uysal, "MAC layer performance of the IEEE 802.15.7 visible light communication standard," *Trans. Emerg. Telecommun. Technol.*, vol. 27, no. 5, pp. 662–674, 2016.
[12] J. J. D. McKendry, E. Gu, N. McAlinden, N. Laurand, K. Mathieson, and M. D. Dawson, "Micro-LEDs for biomedical applications," *Semicond. Semimetals*, vol. 106, pp. 57–94, 2021.
[13] Y. Si, T. Wen, J. Huang, L. Zhang, R. Shu, and J. Wang, "500 Mbps high-speed high-sensitivity photon-counting communication demonstration system," *Opt. Express*, vol. 33, no. 3, pp. 5713–5726, 2025, doi: 10.1364/OE.546097.
[14] L. Liu, X. Tang, Z. Chen, Y. Li, and H. Y. Fu, "Full-duplex modulating retroreflector based UWOC system using MEMS grating modulator and SiPM," *Opt. Laser Technol.*, vol. 182, Apr. 2025, Art. no. 112163, doi: 10.1016/j.optlastec.2024.112163.
[15] X. Chen, M. Jin, R. Lin, G. Zhou, X. Cui, and P. Tian, "Visible light communication based on computational temporal ghost imaging and micro-LED-based detector," *Opt. Lasers Eng.*, vol. 152, May 2022, Art. no. 106956, doi: 10.1016/j.optlaseng.2022.106956.

VT