Network and Information Security in Wireless Optical Network

E.A. Okorie; H.U. Anyaragbu
Department of Computer Science, Faculty of Natural and Applied Sciences,
Tansian University Umunya Anambra State, Nigeria

Abstract

The increasingly growing demand for cost-effective and high-speed wireless communication services has led to significant interest in Optical Wireless Communication (OWC) within the research communities and market. Over the past decades, the numerous optical-related technologies (e.g., LEDs, displays, cameras) and systems (e.g., VLC, LiFi, LiDAR) have been developed. OWC technologies, regarded as competitive mechanism for next-generation networks and a viable alternative to radio frequency (RF)-based approaches, provide a bandwidth capacity 10,000 times greater than conventional RF-based wireless technologies (e.g., WiFi, LoRa, Bluetooth, LTE). Additionally, OWC offers substantial potential for spatial reuse with minimal interference. Due to its reliance on limited wavelengths and line-of-sight (LoS) transmission, OWC is often perceived as a secure wireless communication method, capable of confining signal transmissions within physical boundaries. However, in practical scenarios, this assumption is inaccurate. Privacy breaches and security vulnerabilities are prevalent across optical-related wireless applications, including OWC networks. While initial studies have begun to address these issues, they often lack systematic analysis and remain fragmented. This paper provides a board-wide review of security challenges in contemporary OWC networks. It systematically identifies and examines the primary vulnerabilities in current and emerging optical communication systems and delineates potential attack methods that exploit these weaknesses. Finally, it highlights future directions for enhancing the security of OWC technologies.

Keywords: wireless communication, optical netwrork security, radio frequency, light

I. Introduction

1.1 Defining Optical Wireless Communication (OWC)

Optical Wireless Communication (OWC) is a wireless technology which employs light waves and optoelectronic components for data transmission [1]. Unlike traditional optical connectivity methods, OWC does not rely on physical optical fibers. Instead, i utilizes free space as transmission medium and operates within the following light spectrums:

- Visible light spectrum: 380 nanometers (nm) to
700 nm.
- Infrared (IR) spectrum: 750 nm to 1 millimeter (mm).
- Ultraviolet (UV) spectrum 10 nm to 400 nm.

OWC systems consist of several key components for data transmission, including an encoder, modulator, source, and transmitter optics. Light-emitting semiconductor devices, such as light-emitting diodes (LEDs) and laser diodes, serve as the light sources. These devices typically mounted on ceilings or integrated into roofs alongside transmitter optics, ensuring compliance with established eye and skin safety standards. The data signal is embedded within a carrier signal through advanced modulation techniques, such as:

- Intensity modulation with direct detection,
- Pulse amplitude modulation,
- Pulse position modulation,
- Carrierless amplitude and phase modulation, and
- Orthogonal frequency-division multiplexing.

Once the transmitter convert the data into optical signals, the modulated light propagates through the free space channel. OWC systems employ various components for signal reception, including a photodetector—such as a photodiode or an avalanche photodiode—capable of detecting incoming light signals, an amplifier to improve signal quality, a demodulator to retrieve the original data, and decoder to process the signal [1].

DOI: https://doi.org/10.5281/zenodo.18410334

For effective signal reception, the receiver must maintain a wide field of view to capture the optical signal and be sufficiently flat to enhance spectral efficiency through an optimized detection area. Upon receiving the optical signal from the transmitter, the receiver demodulates and decodes it to reconstruct the original data.

1.2. Significance of Optical Wireless Communication (OWC)

Optical Wireless Communication (OWC) offers numerous advantages, which include the following[2]:

a) High Available Bandwidth

Unlike radio frequency (RF) spectra, the OWC spectrum is both unregulated and unlicensed, theoretically allowing access to bandwidths in the petahertz range. The visible light and infrared (IR) spectra typically provide bandwidths in the range of several hundred terahertz, while the ultraviolet (UV) spectrum offers comparable bandwidth. However, UV is less frequently utilized due to its higher absorption and scattering properties. Although current technological standards and devices cannot fully exploit these high frequencies due to technical limitations and safety considerations, the optical spectrum remains relatively uncongested. This lack of congestion positions OWC as a promising enabler of higher data rates in future sixth-generation (6G) networks.

b) Standardized Technology

OWC predominantly operates within the visible light spectrum and selected portions of the IR spectrum. The use of the UVC band is gradually emerging, particularly for solid-state devices, underwater communication, and wireless communication systems with a wide field of view. Depending on the type of light source employed, OWC can be categorized into several technologies, including:

I. Visible Light Communication (VLC),
II. Infrared (IR) communication, and
III. Free-Space Optical Communication (FSO).

These technologies have been subject to varying levels of standardization by regulatory bodies. Enterprises typically deploy VLC and IR communication systems for indoor applications, whereas FSO is primarily utilized for outdoor scenarios where laying cables is impractical

c) Electromagnetic Interference (EMI) Immunity

The majority of electromagnetic interference (EMI) occurs within the radio frequency (RF) spectrum, commonly referred to as radio frequency interference (RFI). In contrast, Optical Wireless Communication (OWC) is immune to EMI, a characteristic not shared by standard wireless networks. Light's inability to penetrate solid barriers, such as walls, eliminate the possibility of interference even in adjacent rooms utilizing same networking frequencies. While near-field electronic devices in the same room may generate EMI, such interference predominantly affects lower frequencies and does not impact the higher frequencies employed by OWC.

d) Enhanced Security

OWC's small cell sizes significantly enhance security by restricting signal transmission to specific physical areas. The reduced likelihood of eavesdropping arises
from limited access to enterprise premises, and the confinement of optical signals further mitigates this risk. Unlike RF signals, which can penetrate walls, OWC transmissions are confined to line-of-sight (LoS) communication, making it more challenging for malicious actors to intercept network signals. Additionally, the use of highly directional beam ensures that data transmission is targeted solely to intended receivers within the LoS, further bolstering network security.

e) Spot Diffusion for Enhanced Performance

To improve performance of OWC systems, enterprises can adopt advanced link designs, such as multiple-input, multiple-output (MIMO) technology. One widely utilized approach involves the use of a multispot diffusing transmitter. This design direct optical signal beams to multiple locations within a room, reducing the necessity for precise alignment between the transmitter and receiver. As a result, the system becomes more user-friendly, offering improved mobility and shadow immunity in enterprise environments.

f) Low Implementation Cost

DOI: https://doi.org/10.5281/zenodo.18410334

The implementation of Optical Wireless Communication (OWC) systems offers a cost-effective alternative to traditional networking infrastructure. The process of laying cables across an enterprise can be prohibitively expensive, often requiring substantial financial investment. In contrast, OWC operates on an unregulated optical spectrum, eliminating the licensing fees associated with radio frequency (RF) spectrum usage. Furthermore, enterprises can

reduce expenses by utilizing light-emitting diodes (LEDs) and laser diodes in place of conventional networking devices. Since the early 2000s, the adoption of LEDs and laser diodes in residential and commercial applications has increased significantly, driven by their energy efficiency and adaptability. These components consume relatively low amounts of electrical power during operation, resulting in reduced installation and operational costs over time.

g) Hybrid Networking

The integration of optical fibers with OWC networking components enables the creation of hybrid networks, which combines the advantages of both technologies. Such networks involve deploying multiple OWC access points across an enterprise—often in separate rooms—and interconnecting them through optical fibers. Hybrid networks support both line-of-sight

(LoS) and non-line-of-sight (non-LoS) communication modes, enhancing flexibility and scalability. The varying degrees of directionalities between transmitters and network devices facilitate on-site
mobility, multipoint communication, and improved data transmission rates.

1.3 . Challenges of OWC

Despite the numerous advantages offered by OWC, the technology faces several limitations, including[3]:

1.3.1 Short Range

The range of OWC systems is constrained by eye and skin safety regulations, which impose strict limits on the permissible transmitter power. As a result, low-power optical transmitters are typically effective only within a single room. The inability of visible and infrared (IR) light to penetrate solid barriers prevents OWC systems from transmitting data between rooms. Consequently, the operational range of OWC is restricted to a few meters, limiting its scalability in enterprises with outdoor spaces or indoor facilities featuring large rooms and expansive halls.

1.3.2 Line-of-Sight (LOS) Maintenance

For optimal Optical Wireless Communication (OWC), it is crucial that the transmitter and receiver maintain a direct line-of-sight (LOS). Misalignment between transmitter and receiver, known as pointing error loss, can occur when environmental factors, such as on-site mobility and varying seating arrangement, prevent multiple client devices from maintaining proper alignment. To mitigate this issue, transmitters are commonly mounted on the ceiling to create a broader radiation pattern, ensuring that receivers remain within the field of view. However, this configuration may lead to multipath dispersion, where reflection from walls and other surfaces cause signal degradation. This phenomenon results in a diminished signal-to-noise ratio (SNR) and can induce inter symbol interference (ISI).

1.3.4 Multipath Dispersion

Obstructions such as walls, ceilings, and furniture can block or shadow the client device, contributing to multipath dispersion. In this scenario, the transmitted signal follows multiple paths to reach the receiver, with some component taking the original LOS path, while others are reflected or scattered off surrounding surfaces. Consequently, the signal component arrive at the receiver at different times, creating propagation delays. This delay, along with multipath dispersion, causes channel distortion and further exacerbates ISI.

1.3.5 Intersymbol Interference (ISI)

Although electromagnetic interference (EMI) is absent in OWC systems, a similar effect, referred to as ISI, can occur. ISI arises when one symbol or information bit overlaps with successive symbols due to multipath dispersion or signal delays. The overlap results in data corruption, leading to a degradation of the quality of the received signal. To reduce the impact of ISI,
advanced link design and precise beam directionality techniques can be employed in OWC networks.

1.3.6 Atmospheric Susceptibility

DOI: https://doi.org/10.5281/zenodo.18410334

OWC systems are susceptible to atmospheric disturbances, such as natural sunlight and various artificial light sources, which introduce shot noise, commonly known as light noise. Additionally, temperature and pressure fluctuations can cause atmospheric turbulence, resulting in several effects, including signal absorption, scattering, refraction, and attenuation. These factors can significantly affect the performance and reliability of OWC systems, especially in outdoor environments.

1.3.7 Fluctuations and Signal Performance

Fluctuations in environmental conditions, such as changes in temperature or atmospheric pressure, can significantly impact the amplitude, phase, and also intensity of the OWC signal. These variations may result in signal flickering or an increased error rate. Consequently, outdoor OWC systems, such as Free-Space Optical (FSO) communication, are less suitable for deployment in regions prone to frequent weather changes due to the susceptibility of these systems to such fluctuations.

1.3.8 Optoelectronic Errors

OWC networks are particularly vulnerable to performance degradation arising from the limitation of optoelectronic devices. Components such as LEDs, laser diodes, and the photodetectors exhibit heightened sensitivity to temperature variations and are subject to a finite operational lifespan. For instance, LEDs used in Light Fidelity (Li-Fi)—a wireless OWC technology that transmits data using light—are prone to optical feedback and environmental pollution. On the receiver side, photodiodes, while offering large detection areas, have a limited spectral range, and issues such as high dark currents and capacitance can impair signal quality and network connectivity.

1.3.9 Regular Replacements

The lifetime maintenance costs for OWC network devices are typically higher than those associated with optical fiber networks. LEDs and laser diodes generally have an operational lifespan ranging from two to five years, whereas optical fibers can last up to 40 years. Consequently, OWC networks in enterprise settings may require more frequent maintenance and device replacements, typically every three to four years. As such, OWC is better suited for applications where regular maintenance is common, such as in vehicle networks, traffic lights, and the Internet of Things (IoT) systems.

2. A review of Related Works

Research on Optical Wireless Communication (OWC) network security and privacy concerns, as well as related surveys, remains in the early stages of development. The existing body of work [4, 5, 6, 7, 8, 9, 10] on OWC security can be categorized into four main areas:

(1) a focus on various OWC applications (e.g., Vehicle-to-Vehicle (V2V) networks, Light Fidelity (LiFi) systems, and Optical Camera Communication (OCC));

(2) a focus on specific techniques adopted for particular objectives (e.g., beamforming, dimming, Multiple Input Multiple Output (MIMO), machine learning, and Network Function Virtualization (NFV));

(3) a focus on network architecture and protocols (e.g., the physical layer); and

(4) a focus on attack types (e.g., jamming, eavesdropping, and spoofing). As summarized in Table 2, OWC security-related studies are organized into these four categories, each concentrating on particular applications, attacks, protocols, or techniques.

While OWC applications are not entirely new concepts, they continue to evolve. For instance, the authors of Reference [11] provided an extensive study on current OWC applications, classifying them into five categories: Visible Light Communication (VLC), Light Fidelity (LiFi), Optical Camera Communication (OCC), Free Space Optical Communication (FSOC), and Light Detection and Ranging (LiDAR). These diverse applications [12, 13, 14, 15–17, 18, 19] are increasingly integrated into everyday life, spanning various environments, such as homes, offices, vehicles, industrial settings, terrestrial, undersea, and space-based applications. Consequently, the security of these varied applications is essential to ensure the delivery of secure and reliable services. Existing research on OWC security predominantly focuses on applications involving human interaction. For example, References [20, 21, 22] examined the security of indoor VLC, LiFi, and smart lighting systems, as depicted in Figure 1.

DOI: https://doi.org/10.5281/zenodo.18410334

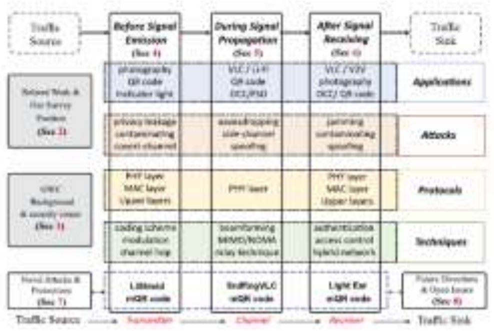

Figure 1: an overview of the 4 aspects of a secure OWC network[9]

Given the specific types of attacks, the authors in References [23] provide an in-depth analysis of various threats in Optical Wireless Communication (OWC) networks, including jamming, pollution, eavesdropping, and spoofing. They also explore the corresponding Physical Layer Security (PLS) techniques for mitigating these attacks. For example, to enhance network secrecy, they recommend integrating multiple PLS approaches, such as beamforming, secure zones, friendly jamming, and Multiple Input Multiple Output (MIMO) technologies. Regarding specific attacks, the authors of References [24, 25] examined jamming attack models and investigated the potential of friendly jamming as a secure countermeasure. Additionally, several novel attacks are highlighted in Figure 1, including eavesdropping [9], privacy leakage [26], side-channel attacks [35], and covert-channel attacks.

Given the advanced techniques employed in OWC, such as beamforming, dimming control, spectrum hopping, artificial intelligence/deep learning (AI/DL) approaches, spatial multiplexing, and hybrid networking, the primary objective of these studies has been to improve communication performance, encompassing throughput, reliability, and security. For instance, some studies [27, 28] focus on adaptive beamforming algorithms designed to mitigate Line-of-Sight (LoS) signal blockages, ensuring smooth and also stable communication services, or to prevent signal leakage to eavesdroppers through innovative beamforming designs. Other emerging techniques for securing OWC systems include Radio Frequency/Visible Light (RF/VL) hybrid networks [3, 29], as outlined in Figure 1.

However, security threats can arise at every given stage of the traffic flow, as illustrated in Figure 1. To the best of our knowledge, no previous study has systematically examined the security of OWC networks in such a structured manner. Rather than focusing on a single aspect, our research spans all four categories (applications, techniques, protocols, and attacks) and organizes them according to OWC traffic flow. Figure 2 illustrates the scope of our contents coverage and the position of our survey within this context. We anticipate that these survey will provide a comprehensive review of security within OWC networks.

3. **OWC Architecture and Security Standards**

3.1 **OWC Network Architecture**

Unlike RF-based wireless networks, the IEEE Optical Wireless Communication (OWC) standard [30] introduces some distinctions, particularly in the inability of optical transmissions to penetrate obstacles such as walls. The OWC architecture is composed of the Physical (PHY) layer, which encompasses the light transceiver and low-level control mechanisms, and the

Medium Access Control (MAC) layer, which facilitates various types of data transfers over the physical channel, forming the Optical Wireless Personal Area Network (OWPAN) device. Figure 2 illustrates these layers in a diagrammatic format.

The upper layers of the OWPAN are also depicted in Figure 3. The OWPAN includes a network layer and application layer. The network layer is responsible for network configuration, management, and message routings. The application layer, on the other hand, defines the device's intended functionality. Between the upper layers and the MAC layer, the standard specifies two sublayers: the Logical Link Control (LLC) and the Service-Specific Convergence Sublayer (SSCS), which serve as intermediaries between the MAC layer and the upper layers.

DOI: https://doi.org/10.5281/zenodo.18410334

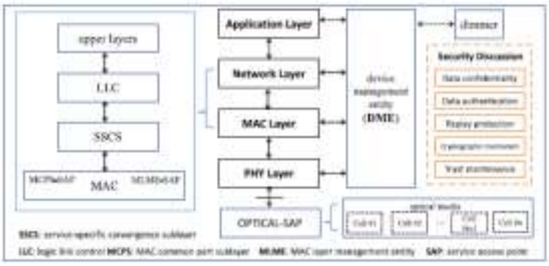

Figure 2: The OWC network architecture and security discussion in IEEE standard[30]

3.2 Mechanisms of Wireless Security

Wireless network security is a critical subset of network security that focuses on the design, implementation, and maintenance of security protocols to protect wireless computer networks from unauthorized access and potential breaches. This discipline aims to ensure the confidentiality, integrity, and also availability of wireless networks and their resources. Effective security measures are essential to prevent threats such as data interception, theft, and denial-of-service attacks.

Wireless security operates by establishing multiple layers of defense through a combinations of encryption, authentication, access control, device security, and intrusion detection systems. The process begins with the activation of encryption protocols such as WPA2 or WPA3, which serve to obscure data transmissions, rendering them unreadable to unauthorized parties even in the event of interception.

Upon attempting to connect to the network, users or devices are required to authenticate their identities, typically through the input of a password, to verify the legitimacy of the connection request. Subsequently, access control mechanisms define which users or devices are authorized to access the network and extent of their access privileges, determined by factors such as user roles, device types, and specific access rights.

Further security measures involve protecting network devices through the installation and maintenance of

antivirus software, regular updates to operating systems, and restricting the use of administrator

privileges to mitigate the risk of unauthorized access. Intrusion Detection and Prevention Systems (IDPS), along with other monitoring tools, play a crucial role in detecting and responding to anomalous activities or security breaches. These systems continuously monitor the network for unauthorized access attempts, malware, and other threats, providing real-time protection.

3.2.1 Overview of Potential Security Issues and Attack Methods Targeting Optical Networks

Optical networks are susceptible to a variety of security breaches or attacks, which are typically aimed at disrupting network services or gaining unauthorized access to the transmitted data, such as through eavesdropping [30]. Depending on the objectives of the attack, security breaches may lead to financial losses for clients or cause widespread service disruptions, which can result in significant data and revenue losses. Consequently, a comprehensive understanding of the vulnerabilities and attack methods is essential for the development of effective security solutions tailored to optical networks.

3.2.2 Classification of OWC Risks

Various Optical Wireless Communication (OWC) technologies, as outlined in Reference [31], include Visible Light Communication (VLC), Light Fidelity (LiFi), Optical Camera Communication (OCC), Free Space Optical Communication (FSOC), and the Light Detection and Ranging (LiDAR). These OWC technologies are employed across a broad spectrum of applications [32,]. For instance, OWC techniques find usage in diverse environments such as industrial settings, transportation systems, workplaces, residential areas, shopping malls, underwater locations, and outer space. The specific choice of OWC technology depends on the requirements of the application, including factors such as data speed, communication type, and the platform utilized. Given the varied nature of these applications, security challenges arise in each context. As such, OWC network risks can be categorized according to the specific application scenarios, as outlined below.

1. **Indoor vs. Outdoor Environments:** In indoor settings, attackers can perform eavesdropping attacks within the line-of-sight (LoS) zones of the transmitter, without disrupting the optical wireless communication (OWC) process between the transmitters and legitimate receivers. While walls may block optical signal leakage in indoor environments,

DOI: https://doi.org/10.5281/zenodo.18410334

attackers can still exploit radio frequency (RF) side channels to intercept critical data. In contrast, outdoor conditions, particularly sunlight, introduce significant optical noise. However, even in such environments, the OWC transmitter's ability to emit weak RF signals during
optical signal transmission provides attackers with the opportunity to conduct sniffing attacks through the RF side channel.

2. **Single-user vs. Multiple-users:** Optical Camera Communication (OCC)-based applications have gained prominence, particularly due to the widespread use of smartphones. In single-user services, the majority of OCCs rely on Device-to-Device (D2D) communication. Despite the relatively low risk of attacks on the receiver side, eavesdroppers within the same vicinity can still access the optical channel by capturing images or recording videos. Furthermore, due to the inherent broadcast nature of Visible Light Communication (VLC), it facilitates access for multiple users to the same optical wireless resource [33]. In such environments, unauthorized users and eavesdroppers are likely to intercept raw optical signals from open VLC channels.

3. **Static vs. Mobile:** Most indoor VLC systems are static OWC applications, wherein both the transmitter and receiver remain stationary during transmission. However, some OWC applications, such as Vehicle-to-Vehicle (V2V) or Vehicle-to-Infrastructure (V2I) communications, involve mobility, with either the transmitter or receiver in motion. Compared to static applications, mobility complicates attacks, as the optical channels' positions change, and the optical signals become distorted, making it more difficult even for attackers to conduct successful attacks.

4. **Terrestrial vs. Underwater vs. Space:** OWC devices are applicable not only in terrestrial environments but also in underwater and space settings. Generally, attacks on terrestrial OWC systems are less costly and less challenging than those targeting underwater or space-based OWC systems. Additionally, RF side-channel attacks are ineffective for underwater OWC systems due to the substantial distortions and interference introduced by seawater.

5. **High-speed Applications vs. Quick-link Services:** VLC and LiFi techniques are primarily used to deliver high-speed service, while OCC is typically employed for quick-link services. For example, indoor LiFi systems offer reliable, high-speed internet access with Mbps-level throughput. In contrast, OCC provides lower data rate services, which are particularly suited for quick-link connections involving a large number of Internet of Things (IoT) devices. High-speed applications often demand big robust security solutions compared to quick-link services.

3.3 OWC Security Vulnerabilities

3.3.1 Risks in Line-of-Sight (LoS) and Non-Line-of-Sight (NLoS): Attackers must typically be within the
victim's Line-of-Sight (LoS) to initiate an attack. The optical propagation of light in LoS communication inherently limits the range of potential strikes, preventing attacks from outside the LoS. However, threats to the security of Optical Wireless Communication (OWC) systems persist in both LoS and Non-Line-of-Sight (NLoS) scenarios.

3.3.2 Risks in LoS: OWC encompasses several techniques, including Visible Light Communication (VLC), Light Fidelity (LiFi), Optical Camera Communication (OCC), Free-Space Optical Communication (FSOC), and the Light Detection and Ranging (LiDAR) [11]. Each of these techniques is suited for specific use cases, application categories, or technical requirements. The data links in these systems typically consist of the transmitter, optical propagation channel, and receiver. If an attacker or malicious device is within the LoS range of the data link, there remains an opportunity to intercept or infers the user's privacy and relevant data through various attack methods. While light signals cannot penetrate walls, offering some protection against privacy breaches within confined spaces—such as rooms with curtain-covered windows—compared to RF-based signals, the broadcast nature of OWC still exposes VLC channels to eavesdropping risks. Unauthorized users within the same room or area illuminated by LED lamps may gain access to the signals. Such threats are particularly prevalent in

DOI: https://doi.org/10.5281/zenodo.18410334

indoor public spaces, such as shopping malls, airplanes, laboratories, and sensitive meeting rooms.

3.3.3 Risks in NLoS: The advent of Internet-enabled smart lighting devices, such as LiFi, smartphones, tablets, smart lamps, and also LED displays, has introduced energy-efficient lighting and display options that outperform traditional lamps and screens. However, these devices, when connected to the

Internet, increases the risk of private user information leakage. These smart devices enable precise control of color and intensity emissions, which are utilized to carry local or public Internet data. If an attacker is within the range of the light-emitting areas, they can also capture the fluctuating light signals using light sensor devices. Even in the absence of direct LoS to the smart devices, attackers can still perform covert attacks. They install monitoring software or viruses on these devices to create new channels for data exfiltration. In addition to the potential leakage of visible light signals, these smart devices may inadvertently generate undesired RF signals when controlling the light signal, further exacerbating security high risks.

3.4 Attack Types in OWC

To effectively analyze the security risks within Optical Wireless Communication (OWC) networks, we
categorize attack types using four different methods: attack goals, system structure, application scenarios, and channel types. These methods are outlined as follows: (a) classification by attack goals (including jamming, eavesdropping, spoofing, and Distributed Denial of Service (DDoS)-based OWC attacks); (b) classification by channel types (including side-channel attacks and covert-channel attacks); and (c) classification by system structure (including attacks targeting the transmitter side, channel side, and the receiver side).

(a) Classification by Attack Goals

Jamming Attacks: Jamming attacks refer to intentional actions by malicious nodes that disrupt legitimate communication by introducing interference into the network [17]. In the context of OWC systems, jammers aim to prevent normal communication by adding optical noise or continuous signal to obstruct signal reception at the receiver side. For instance, a jammer may identify the location of the receiver and transmit optical signals to disturb or block the signals emitted from the transmitter. As a result, the OWC system fails to function correctly and cannot receive data as intended. An example of a jamming attack is illustrated in Figure 3.

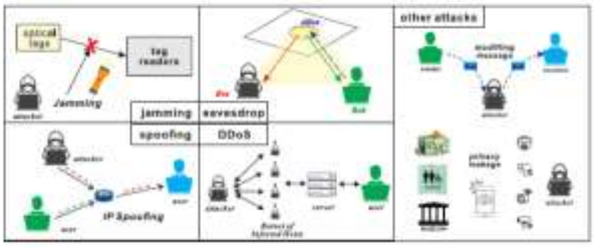

Figure 3: Illustration of jamming, eavesdroping, spoofing, DDoS and other attacks[17]

Eavesdropping Attacks: Eavesdropping attacks, also referred to as sniffing or snooping attacks, involve unauthorized access to user information via optical channels or higher network layers. These attacks typically occur when unsecured networks, such as public OWC connections, are used in shared Line-of-Sight (LoS) spaces. Eavesdropping and optical privacy leakage are prevalent and challenging to prevent. For instance, an eavesdropper may capture images of sensitive scenes, objects, or individuals in public areas or intercept optical signals without the knowledge of legitimate users, provided they are within the same LoS zone. Eavesdropping attacks can also occur from outside a room, such as through windows. An example of an eavesdropping attack is depicted in Figure 3.

Spoofing Attack: In network security, spoofing attacks occur when an individual or program masquerades as another entity by falsifying data. For modern OWC systems, ensuring the authenticity of visible light signals from light fixtures is a significant
concern. Most light fixtures lack protective measures, making them accessible to virtually any
user. Consequently, transmitters in OWC networks are vulnerable to tampering and substitution attacks. As described in Reference [35], an attacker can easily replace a legitimate LED with a rogue LED under their control to

DOI: https://doi.org/10.5281/zenodo.18410334

inject spoofed optical signals into a user's receiver. An example of a spoofing attack is illustrated in Figure 3.

DDoS Attacks: Denial-of-Service (DoS) attacks involve deliberate attempts by attackers to disrupt legitimate service usage. DoS attacks can take two primary forms: crashing services or flooding services with traffic. Distributed Denial-of-Service (DDoS) attacks are particularly severe and may target both transmitter and receiver sides in OWC networks, especially in duplex communication scenarios. For example, on the uplink, attackers may overwhelm the transmitter with responses from multiple users, causing a service crash. Conversely, on the downlink, attackers may flood traffic to disrupt the user's ability to receive data from multiple transmitters. An example of a DDoS attack is provided in Figure 3.

(b) Classified by Channel Types

OWC attacks can also be categorized based on channel types, specifically into **side-channel attacks** and **covert-channel attacks**, as summarized in Reference [6].

Side-Channel Attacks: Side-channel attacks exploit optical side-channels to passively extract a user's private data. These attacks often target power consumption, electromagnetic fields, or time-based vulnerabilities. For instance, power dissipation provides a significant avenue for attack, including Simple Power Analysis (SPA) and the Differential Power Analysis (DPA) techniques. Compared to traditional cryptanalysis, these methods yield notable results. In the context of OWC, attackers may infer transmitted data or media content by analyzing variations in light color and intensity. In some cases, attackers may capture image of a user's smartphone or screen to directly obtain sensitive information.

Covert-Channel Attacks: Covert-channel attacks differ from side-channel attacks in that they actively manipulate optical covert-channels to extract user data. These attacks utilize unperceived light, such as infrared, emitted by smart bulbs or screens. The covert-channel acts as a hidden communication pathway between a user's device and an adversary's device equipped with infrared sensing capabilities.

Attackers may install malicious software agents on the victim's smart device to encode and the transmit private data through the covert-channel. This method does not require authorization to control the light-emitting devices, allowing any Trojan installed on the victim's device to facilitate the attack. Take for example, an attacker might use a malicious infrared-
equipped camera to steal or inject private data across an air-gapped network. The covert-channel attack effectively turns the victim's device into a gateway for active data leakage. These channels can function as one-way or two-way Line-of-Sight (LoS) data exfiltration or infiltration pathways. Infrared light is often employed due to its imperceptibility to the human eye, but visible light may also be used if modulated at high frequencies or with specific schemes to remain unnoticed by the victim. Once private data is transmitted from the smart light-emitting device to the adversary's device, the attacker executes a processes of adversarial reconstruction. This involves using infrared sensors to observe the victim's device. The success of reconstruction depends on factors like as signal attenuation and the level of noise in the optical channel.

(c) Classified by System Structure

Attacks in OWC networks can be categorized based on the system structure into **transmitter side**, **channel side**, and **the receiver side**.

Transmitter Side: At the transmitter side, the attackers can target the transmitter directly or use it as an attack vector. Since smart LED lamps are often connected to the internet, attackers can exploit this connectivity to install malicious software or programs on the transmitter. This allows them to execute various attacks, such as message manipulation, replay attacks, spoofing attacks, the Distributed Denial of Service (DDoS) attacks, and other forms of interference. These attacks occur before the optical signals are emitted, compromising the integrity and security of the transmitted data.

Channel Side: The channel side is the most frequent target for attacks in OWC networks, which can be categorized into three scenarios:

1. **Attacker Positioned Between Transmitter and Receiver:** In this setup, the attacker places a relay device between the transmitter and receiver, enabling them to execute replay attacks, message manipulation attacks, eavesdropping attacks, and other forms of interference.

DOI: https://doi.org/10.5281/zenodo.18410334

2. **Attacker Within the Line-of-Sight (LoS) Zone of the Transmitter:** When the attacker is within the LoS zone, they can easily conduct eavesdropping attacks by intercepting the optical signals transmitted directly between the transmitter and receiver.
3. **Attacker Within the Non-Line-of-Sight (NLoS) Zone of the Transmitter:** In this scenario, the attacker, located outside the LoS zone, can exploit RF side channels to conduct sniffing attacks and capture transmitted data.

Receiver Side: The receiver side is another critical point of vulnerability in OWC networks, often involving smart devices such as smartphones or Photo Diode (PD)-equipped microcontroller units (MCUs).

Attackers can install malicious software on these devices to conduct replay attacks and manipulate messages, which entails tampering with transmitted or received data. This compromises the security and reliability of the receiver and can lead to unauthorized access or data corruption.

4.0 Other Directions for OWC Countermeasures

Wireless communication in our daily life is typically protected against unauthorized access, message modification, eavesdropping, and replay attacks. Key security mechanisms include:

- **Authentication Services**: Verifying an entity's identity to grant access.
- **Confidentiality Services**: Ensuring message content is understood only by intended devices.
- **Data Integrity Services**: Preventing alteration of data in transit.

For Visible Light Communication (VLC), three primary security mechanisms provide protection:

1. **Proximity-based Protection**: Leveraging physical location to restrict access.
2. **Steganographic Protection**: Embedding data in non-obvious formats for concealment.
3. **Cryptographic Protection**: Encrypting data for secure transmission.

These mechanisms are chosen based on application-specific security needs. Building on this, several additional countermeasures for Optical Wireless Communication (OWC) are discussed below.

4.1 Create Secure Zones

Given the line-of-sight (LoS) nature and broadcast characteristics of the optical signals, creating secure zones is an intuitive countermeasure.

- **Protected Zones**: Defined by the access point (AP) location, with a security radius representing the minimum distance to potential eavesdroppers.
- **Implementation**: Motion sensors embedded in modern lighting equipment can enforce these zones.

4.2 Utilizing Hybrid Network Techniques

Reliability and security improve in hybrid systems, combining different network types, such as:

- **VLC/WiFi**
- **LiFi/WiFi**
- **VLC/small cell**
- **LiFi/small cell**

Hybrid system mitigate vulnerabilities of individual technologies. For instance, optical networks are sensitive to obstacles, limiting signal hacking to within a room. Hybrid networks enhance security by ensuring reliable connections between transmitters and receivers.

4.3 Channel-Hopping Mechanis

Channel hopping protects the confidentiality of communications by frequently changing the transmission channel.

- **Eavesdropper Countermeasure**: Prevents decoding of signals by keeping channel usage unpredictable.
- **Implementation Techniques**:

1. **Frequency-Hopping (BFSK Modulation)**: Randomly switches between channels.
2. **Time-Synchronized Channel Hopping**: Allocates channels to light sources based on a predefined time schedule to ensure fairness and reduce collisions.

- **Benefits**: Random hopping limits channel collisions and improves security.

These countermeasures, when combined with traditional security mechanisms, significantly enhance the resilience of OWC networks.

4.4 Authentication and Encryption

Authentication in OWC systems is often achieved through the feature-based detection.

DOI: https://doi.org/10.5281/zenodo.18410334

The receiver evaluates the sender’s **channel gain** to create a fingerprint, determining whether the sender is valid or invalid.

- **Recent Advances**:
  - **Training Phase**: The receiver learns about the valid sender during training.
  - **Testing Phase**: Transmissions are compared against the valid sender’s profile.

Encryption can be implemented using a **Caesar cipher system**, which:

- Converts text into a cipher using a cyclical array and direct letter-to-letter mapping.
- Prevents attackers from decoding the data without the appropriate knowledge.
- Reference [37]: Highlights its simplicity and security benefits.

4.5 Proximity-based Protection

Proximity-based protection is one of OWC's strongest and the most unique features. Unlike RF signals that propagate through walls and can be intercepted from a distance, light waves are confined to the physical environment, ensuring privacy within a room or car.

- **Key Strengths**:
  - **Line-of-Sight (LoS)**: Communication relies on direct visibility between transmitter and receiver, making interception difficult.
  - **Limited Propagation**: Signals remain confined to a single room, enhancing security.
- **Vulnerabilities**:
  - Attackers could exploit openings such as windows, gaps below doors, or keyholes to intercept light signals.

4.

- **Mitigation**: Keeping secure areas enclosed is critical to prevent eavesdropping.

5.

- Reference [38]: Illustrate the comparative advantage over RF signals and the necessity for physical security measures.

4.6 Steganographic Protection

Steganography involves embedding secret/hidden messages within another message, ensuring confidentiality. The hidden messages can only be read by someone who knows how to locate and decode them.

- **Techniques in OWC**:
  - **LuxSteg**:Combines steganographic messages with orthogonal codes, integrating them into overt signals modulated through pulse position modulation. This technique creates hidden messages invisible to unauthorized parties.
  - **LiShield**: Hides barcodes within images, undetectable to the human eye but readable by online systems. These barcodes help determine if an image can be posted.
  - Reference [39]: Demonstrate practical applications of steganography in OWC systems.

These mechanisms, combined with encryption and physical security, significantly enhance the confidentiality and integrity of OWC communications.

4.7 Cryptographic Protection and Key Generation

Modern Optical Wireless Communication (OWC) systems implement cryptography across all communication layers, primarily relying on secret keys for encryption [40].

- **Symmetric Keys**:

1.Generated at upper layers of the OSI model using traditional methods [40].

- **Quantum Cryptography**:

1. Utilizes **quantum channels** to establish joint secret key between two parties for secure communication.
2. **Key Features**:
   - Protons serve as carriers; any attempt to measure or intercept a proton results in its destruction.
   - This alerts the receiver to potential eavesdropping attempts.
3. Once established, the quantum key secures subsequent communication.

   Reference [41]: Demonstrates the potential of quantum cryptography to deter eavesdroppers.

4.8 Chaffing and Winnowing

Chaffing and winnowing is an innovative method for ensuring **authenticity** and **integrity** without traditional encryption or decryption [42].

- **How It Works**:

1. **Chaffing**: Fake packets with also fake MACs are added to a transmission.
2. **Winnowing**: The receiver identifies and removes these fake packets based on their invalid MACs.

- **Security Benefits**:
  - Relies on **shared keys** to distinguish fake packets, making it impossible for attackers to discern legitimate packets without the correct key.

DOI: https://doi.org/10.5281/zenodo.18410334

- Adds confusion for eavesdroppers while ensuring the receiver processes only valid packets.

- **Potential for Growth**:
  - Currently underutilized in OWC systems but has significant potential for future applications.
  - Reference [118]: Highlights its simplicity and effectiveness in safeguarding communications.

5.0 Conclusions

Optical networks are susceptible various attacks, such as **eavesdropping** and the **service disruptions**, which can result in substantial **data** or **revenue losses**.

- **Emerging Vulnerabilities**:
  - The shift toward **software-programmable** and the **flexible node architectures** introduces new security risks.
  - These vulnerabilities must be proactively addressed during the design and operational phases of optical networks.

This analysis emphasizes the importance of identifying and mitigating potential security issues in current and the future OWC systems, offering insight into various attack methods and countermeasures to enhance network resilience.

References

[1] Xiao Zhang, Griffin Klevering, Li Xiao, The Security in Optical Wireless Communication: A Survey Article in ACM Computing Surveys · April 2023 DOI: 10.1145/3594718

[2] Xiao Zhang, Griffin Klevering, Li Xiao, The Security in Optical Wireless Communication: A Survey Article in ACM Computing Surveys · April 2023 DOI: 10.1145/3594718

[3] Mohamed Amine Arfaoui, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghrayeb, Majid Safari, Chadi M. Assi, and Harald Haas. 2020. Physical layer security for visible light communication systems: A survey. *IEEE Commun. Surv. Tutor.* 22, 3 (2020), 1887–1908.

[4] Sunghwan Cho, Gaojie Chen, and Justin P. Coon. 2019. Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems. *IEEE Trans. Inf. Forens. Secur.* 14, 10 (2019), 2633–2648.

[5] Minhao Cui, Yuda Feng, Qing Wang, and Jie Xiong. 2020. Sniffing visible light communication through walls. In *26th Annual International Conference on Mobile Computing and Networking*. 1–14.

[6]Anindya Maiti and Murtuza Jadliwala. 2019. Light ears: Information leakage via smart lights. *Proc. ACM Interact., Mob., Wear. Ubiq. Technol.* 3, 3 (2019), 1–27.

[7]Hao Pan, Yi-Chao Chen, Lanqing Yang, Guangtao Xue, Chuang-Wen You, and Xiaoyu Ji. 2019. mQRCode: Secure QR code using nonlinearity of spatial frequency in light. In *25th Annual International Conference on Mobile Computing and Networking*. 1–18.

[8]Rana Shaaban and Saleh Faruque. 2021. An enhanced indoor visible light communication physical-layer security scheme for 5G networks: Survey, security challenges, and channel analysis secrecy performance. *Int. J. Commun. Syst.* 34, 4 (2021), e4726.

[9] Liang Xiao, Geyi Sheng, Sicong Liu, Huaiyu Dai, Mugen Peng, and Jian Song. 2019. Deep reinforcement learningenabled secure visible light communication against eavesdropping. *IEEE Trans. Commun.* 67, 10 (2019), 6994–7005.

[10] Xiang Zhao, Hongbin Chen, and Jinyong Sun. 2018. On physical-layer security in multiuser visible light communication. systems with non-orthogonal multiple access. *IEEE Access* 6 (2018), 34004–34017.

[11] Mostafa Zaman Chowdhury, Md Tanvir Hossan, Amirul Islam, and Yeong Min Jang. 2018. A comparative survey of optical wireless technologies: Architectures and applications. *IEEE Access* 6 (2018), 9819–9840.

[22] Haoshuo Chen, Henrie PA van den Boom, Eduward Tangdiongga, and Ton Koonen. 2012. 30-Gb/s bidirectional transparent optical transmission with an MMF access and an indoor optical wireless link. *IEEE Photon. Technol. Lett.* 24, 7 (2012), 572–574.

[12] Yu-Chieh Chi, Dan-Hua Hsieh, Chung-Yu Lin, Hsiang-Yu Chen, Chia-Yen Huang, Jr-Hau He, Boon Ooi, Steven P. DenBaars, Shuji Nakamura, Hao-Chung Kuo et al. 2015. Phosphorous diffuser diverged blue laser diode for indoor lighting and communication. *Sci. Rep.* 5, 1 (2015), 1–9.

[13] Mostafa Zaman Chowdhury, Md Shahjalal, Moh Hasan, Yeong Min Jang et al.

DOI: https://doi.org/10.5281/zenodo.18410334

2019. The role of optical wireless communication technologies in 5G/6G and IoT solutions: Prospects, directions, and challenges. *Appl. Sci.* 9, 20 (2019), 4367.

[14] ZabihGhassemlooy, Pengfei Luo, and Stanislav Zvanovec. 2016. Optical camera communications. In *OpticalWireless Communications*. Springer, 547–568.

[48] Yuki Goto, Isamu Takai, Takaya Yamazato, Hiraku Okada, Toshiaki Fujii, Shoji Kawahito, Shintaro Arai, Tomohiro Yendo, and Koji Kamakura. 2016. A new automotive VLC system using optical communication image sensor. *IEEE Photon. J.* 8, 3 (2016), 1–17.

[15] Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti-jamming techniques in wireless networks: A survey. *Int. J. Ad Hoc Ubiq. Comput.* 17, 4 (2014), 197–215.

[16]Chi Lin, Yongda Yu, Jie Xiong, Yichuan Zhang, LeiWang, GuoweiWu, and Zhongxuan Luo. 2021. Shrimp: A robust underwater visible light communication system. In *27th Annual International Conference on Mobile Computing and Networking*. 134–146.

[17] Heng Qin, Yong Zuo, Dong Zhang, Yinghui Li, and Jian Wu. 2017. Received response based heuristic LDPC code for short-range non-line-of-sight ultraviolet communication. *Optics Expr.* 25, 5 (2017), 5018–5030.

[18] Minhao Cui, Yuda Feng, Qing Wang, and Jie Xiong. 2020. Sniffing visible light communication through walls. In *26th Annual International Conference on Mobile Computing and Networking*. 1–14.

[19] Agon Memedi and Falko Dressler. 2020. Vehicular visible light communications: A survey. *IEEE Commun. Surv. Tutor.* 23, 1 (2020), 161–181.

[20] Hao Pan, Yi-Chao Chen, Lanqing Yang, Guangtao Xue, Chuang-Wen You, and Xiaoyu Ji. 2019. mQRCode: Secure QR code using nonlinearity of spatial frequency in light. In *25th Annual International Conference on Mobile Computing and Networking*. 1–18.

[21] Christian Rohner, Shahid Raza, Daniele Puccinelli, and Thiemo Voigt. 2015. Security in visible light communication: Novel challenges and opportunities. *Sensors Transd. J.* 192, 9 (2015), 9–15.

[22] Aneeqa Ijaz, Muhammad Mahboob Ur Rahman, and Octavia A. Dobre. 2019. On safeguarding visible light communication systems against attacks by active adversaries. *IEEE Photon. Technol. Lett.* 32, 1 (2019), 11–14.

[23] Maha Sliti,Walid Abdallah, and Noureddine Boudriga. 2018. Jamming attack detection in optical UAV networks. In *20th International Conference on Transparent Optical Networks (ICTON)*. IEEE, 1–5.

[24] Anindya Maiti and Murtuza Jadliwala. 2019. Light ears: Information leakage via smart lights. *Proc. ACM Interact., Mob., Wear. Ubiq. Technol.* 3, 3 (2019), 1–27.

[25] Sunghwan Cho, Gaojie Chen, and Justin P. Coon. 2018. Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers. *IEEE Trans. Wirel. Commun.* 17, 5 (2018), 2918–2931.

[26] Sunghwan Cho, Gaojie Chen, and Justin P. Coon. 2019. Enhancement of physical layer security with simultaneous beamforming and jamming for visible light communication systems. *IEEE Trans. Inf. Forens. Secur.* 14, 10 (2019), 2633–2648.

[27] Mohamed Amine Arfaoui, Mohammad Dehghani Soltani, Iman Tavakkolnia, Ali Ghrayeb, Majid Safari, Chadi M. Assi, and Harald Haas. 2020. Physical layer security for visible light communication systems: A survey. IEEE Commun. Surv. Tutor. 22, 3 (2020), 1887–1908.

[28] Mostafa Zaman Chowdhury, Moh Khalid Hasan, Md Shahjalal, Md Tanvir Hossan, and Yeong Min Jang. 2018. Optical wireless hybrid networks for 5G and beyond communications. In *International Conference on Information and Communication Technology Convergence (ICTC)*. IEEE, 709–712.

[29] IEEE. 2019. IEEE standard for local and metropolitan area networks–part 15.7: Short-range optical wireless communications. *IEEE Std 802.15.7-2018 (Revision of IEEE Std 802.15.7-2011)* (2019), 1–407.

[30] Mostafa Zaman Chowdhury, Md Tanvir Hossan, Amirul Islam, and Yeong Min Jang. 2018. A comparative survey of optical wireless technologies: Architectures and applications. *IEEE Access* 6 (2018), 9819–9840

DOI: https://doi.org/10.5281/zenodo.18410334

[31] Aleksandra Kostic-Ljubisavljevic and Branka Mikavica. 2021. Challenges and opportunities of VLC application in intelligent transportation systems. In *Encyclopedia of Information Science and Technology, Fifth Edition*. IGI Global, 1051–1064.

[34] Xiang Zhao, Hongbin Chen, and Jinyong Sun. 2018. On physical-layer security in multiuser visible light communication systems with non-orthogonal multiple access. *IEEE Access* 6 (2018), 34004–34017.

[35]Kanika Grover, Alvin Lim, and Qing Yang. 2014. Jamming and anti-jamming techniques in wireless networks: A survey. *Int. J. Ad Hoc Ubiq. Comput.* 17, 4 (2014), 197–215..

[36] Jian Chen and Tao Shu. 2021. Spoofing Detection for indoor visible light systems with redundant orthogonal encoding. In *IEEE International Conference on Communications*. IEEE, 1–6.

[37] Anindya Maiti and Murtuza Jadliwala. 2019. Light ears: Information leakage via smart lights. *Proc. ACM Interact., Mob., Wear. Ubiq. Technol.* 3, 3 (2019), 1–27.

[38] Sabrina Abedin, Tasfia Tasbin, and Avijit Hira. 2017. Optical wireless data transmission with enhanced substitution caesar cipherWHEEL encryption. In *International Conference on Electrical, Computer and Communication Engineering (ECCE)*. IEEE, 552–556.

[39] Jiska Classen, Joe Chen, Daniel Steinmetzer, Matthias Hollick, and Edward Knightly. 2015. The spy next door: Eavesdropping on high throughput visible light communications. In *2nd InternationalWorkshop on Visible Light Communications Systems*. 9–14.

[40] Grzegorz Blinowski, Piotr Januszewski, Grzegorz Stepniak, and Krzysztof Szczypiorski. 2018. LuxSteg: First practical implementation of steganography in VLC. *IEEE Access* 6 (2018), 74366–74375.

[41] A. C. Boucouvalas, Periklis Chatzimisios, Zabih Ghassemlooy, Murat Uysal, and Konstantinos Yiannopoulos. 2015. Standards for indoor optical wireless communications. *IEEE Commun. Mag.* 53, 3 (2015), 24–31.

[42] Ronald L. Rivest et al. 1998. Chaffing and winnowing: Confidentiality without encryption. *CryptoBytes (RSA Lab.)* 4, 1 (1998), 12–17.

DOI: https://doi.org/10.5281/zenodo.18410334