The Security in Optical Wireless Communication: A Survey

XIAO ZHANG and GRIFFIN KLEVERING, Michigan State University, USA
XINYU LEI, Michigan Technological University, USA
YIWEN HU, LI XIAO, and GUAN-HUA TU, Michigan State University, USA

With the demand for economical and high-speed wireless services, Optical Wireless Communication (OWC) has attracted increasing attention in both research and the market. In the past decades, numerous optical-related techniques (e.g., LEDs, displays, cameras) and systems (e.g., VLC, LiFi, LiDAR) have been invented. OWC techniques, which are considered as a competitive mechanics in next-generation networks as an alternative to RF approaches, offer 10,000 times more bandwidth than conventional radio frequency (RF)-based wireless techniques (e.g., WiFi, LoRa, Bluetooth, LTE), as well as tremendous spatial reuse potential with even less interference. Because optical communications have a limited wavelength and travel in the line of sight (LoS) manner, the OWC is commonly thought as a secure wireless approach to confine light transmissions within physical bounds. However, in the real world, it is completely untrue. The privacy leakages and security risks broadly exist in the optical-related wireless applications including OWC networks. These threats and weaknesses have recently been the subject of several initial studies. However, they lack systematic analysis and are isolated. This survey first presents a general workflow of OWC systems, which consists of three stages: before signal emission (BSE), during signal propagation (DSP), and after signal receiving (ASV). For each stage, related risks are reviewed. Then, we summarize existing attacks in optical-related wireless applications and corresponding counter-attack solutions. Finally, we outline the future trends for improving OWC security.

CCS Concepts: • **General and reference** → **Surveys and overviews**; • **Security and privacy** → **Systems security;**

Additional Key Words and Phrases: Optical wireless communication, privacy leakage, physical layer attacks, counter-attack solutions, LoS, system security, optical camera communication

ACM Reference format:
Xiao Zhang, Griffin Klevering, Xinyu Lei, Yiwen Hu, Li Xiao, and Guan-Hua Tu. 2023. The Security in Optical Wireless Communication: A Survey. *ACM Comput. Surv.* 55, 14s, Article 329 (July 2023), 36 pages.
https://doi.org/10.1145/3594718

This work was partially supported by the U.S. National Science Foundation under Grants CNS-2226888, CCF-2007159, CNS-1815636, CNS-1814551, and CNS-2153393.
Authors' addresses: X. Zhang, G. Klevering, Y. Hu, L. Xiao, and G.-H. Tu, Computer Science and Engineering, 428 S. Shaw Lane, Room 3115, Engineering Building East Lansing, MI 48824-1226; emails: zhan1387@msu.edu, kleveri2@msu.edu, huyiwen3@msu.edu, lxiao@cse.msu.edu, ghtu@msu.edu; X. Lei, Rekhi Hall, 1400 Townsend Drive, Houghton, MI 49931; email: xinyulei@mtu.edu.

0360-0300/2023/07-ART329 $15.00
https://doi.org/10.1145/3594718

1 INTRODUCTION

The **radio frequency (RF)** used in wireless communications has drawbacks including limited low-frequency spectrum band (below 10 GHz), spectrum usage regulations, and severe interference among nearby RF access points. High-frequency RF band between 3 kHz and 300 GHz of the electromagnetic spectrum, such as millimeter and nanometer waves, has been explored for **fifth-generation (5G)** wireless communication. Nevertheless, using this RF band is regulated by local and international authorities strictly. However, there are no strict usage regulations of the optical spectrum. The optical spectrum also allows 10,000 times more bandwidth capacity than RF-based technology. **Optical Wireless Communication (OWC)** systems can provide high-data-rate services from a few nanometers to more than 10,000 km. Therefore, OWC would be a promising solution for the development of future high-density and high-capacity networks [1, 13, 25, 31, 45, 87, 92, 128, 151, 157, 159–161].

In recent years, optical wireless applications, which can be treated as part of OWC networks, have shown their success in many aspects such as remote sensing, vision recreation, high-speed communication LiFi, **Vehicle-to-Vehicle (V2V)** networks, and **Virtual Reality (VR)** the term abbreviation in this paper is listed in Table 1. In comparison with traditional RF-based wireless techniques (e.g., WiFi, Bluetooth, LTE), OWC takes the advantage of **Line-of-Sight (LoS)** propagation and visible to human eyes, and are able to provide secure communications and location-based services [58, 76, 88, 88, 155]. Because RF and optical signals propagate in distinct manners, OWCs may protect communication security by limiting communication to a specific physical space and increase throughput by massive spatial multiplexing for high-speed wireless services. However, as shown in Figure 1, in reality, this is not totally true. Security risks persist in three stages in OWC systems, from the traffic source to the sink. For the stage of **before signal emissions (BSE)**, researchers have investigated the security vulnerabilities such as modulation schemes [59, 77, 143, 168], coding schemes [21, 44, 154], channel hopping [10, 61, 133], and privacy leakage [43, 144, 156, 168]. **During the optical signal propagation (DSP)**, eavesdropping attacks [28, 33, 84, 90, 148] and message manipulation attacks [110, 124, 139, 154] can happen. Even with efficient protections in the first two early stages, risks still exist **after signal receiving (ASR)** such as multi-access risks [91, 115, 152, 163, 164] and replay attacks [12, 107, 124, 124, 139].

Despite rising interest in OWC systems and innovative optical wireless applications, existing investigations focus on specific goals with a wide range of scenarios and applications. The study into security and privacy risks for OWC networks is still in its early stages. Existing surveys are mostly for advanced OWC techniques and lack the study of security issues. This survey fills the gap by focusing on the three stages of OWC traffic from the Source to the Sink that have security issues, as depicted in Figure 1. Aside from presenting pertinent research of OWC security issues, we also examine the literature on emerging attacks in optical wireless applications, the most recent counter-attack techniques, and summarize the security problems mentioned in OWC network standards. Finally, we highlight the challenges in a variety of optical wireless services, as well as future research directions in secure OWC. We hope to present a comprehensive evaluation of security concerns in OWC networks and associated countermeasures, which will enlighten researchers on how to implement effective safeguards to fully release the great potential of optical wireless communication in practice.

Survey Organization: The following is how this survey is structured: We begin by presenting existing surveys, as well as related studies and our survey's perspective in Section 2. Next, we provide the background of OWC network as well as the comparison with traditional RF wireless techniques, and security concerns are discussed in OWC standard in Section 3. Furthermore, we study the security issues in three stages of OWC traffic in Section 4, Section 5, Section 6, respectively. Afterwards, we outline the novel attacks and protection techniques in Section 7. Then,

Table 1. Nomenclature

ASV	after signal receiving	NFV	network functions virtualization
BSE	before signal emission	NOMA	non-orthogonal multiple access
CSK	color shift keying	NLoS	none line of sight
DSP	during signal propagation	OOK	on off keying
DDoS	distributed denial of service	OCC	optical camera communication
FSOC	free space optical communication	OWC	optical wireless communication
LoS	line of sight	RF	radio frequency
LiFi	light fidelity	VLC	visible light communication
LiDAR	light detection and ranging	V2V	vehicle to vehicle
MIMO	multiple input multiple output	VPPM	variable pulse position modulation

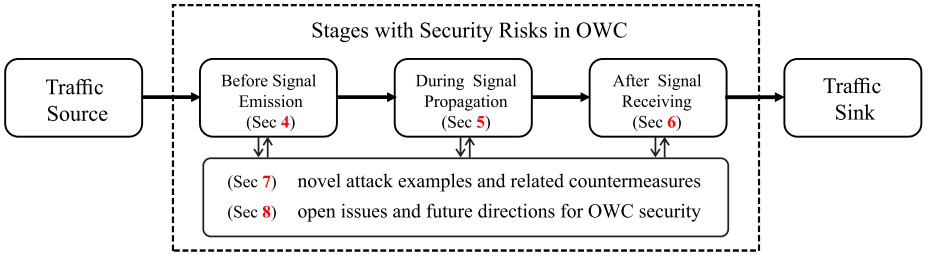

Fig. 1. The general flowchart of OWC traffic and stages with security risks in OWC.

in Section 8, we discuss open issues and future research directions. We conclude our survey in Section 9.

2 RELATED WORK AND OUR SURVEY POSITION

The studies on OWC network security and privacy concerns, as well as the related surveys, are still in their early stages. Existing research [11, 20, 28, 35, 89, 93, 106, 123, 148, 163, 168] on OWC and its security can be divided into four categories: (1) major emphasis on numerous OWC applications (e.g., V2V networks, LiFi systems, and OCC), (2) major emphasis on adopted techniques for specific goals (e.g., beamforming, dimming, MIMO, machine learning, and NFV), (3) major emphasis on network architecture and protocols (e.g., physical layer), and (4) major emphasis on attack types (e.g., jamming, eavesdropping, and spoofing). As detailed in Table 2, OWC security-related studies are divided into four categories and are focused on a certain application, attack, protocol, or technique.

The OWC **applications** are not new concepts, but they are still evolving. For example, the authors of Reference [31] gave a comprehensive study of current OWC applications and classified 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 numerous applications [6, 19, 22, 26, 32, 39, 46–48, 54, 57, 80, 82, 86, 109, 113, 114, 116, 137, 165] can be found in a multitude of places throughout our daily life, including homes, offices, cars, industry, terrestrial, undersea, and space. As a result, the security of these diverse applications should deliver secure and trustworthy services. Existing OWC security research focuses mostly on human-related applications. For instance, References [35, 89, 93, 106, 168] investigated the security of indoor VLC, LiFi, and smart lights, as shown in Table 2 and Figure 2.

Table 2. Some Related Surveys and Our Survey Position

Paper	Venue	Content main coverage			
		Applications	Attacks	Protocols	Techniques
Zhao [163]	18' IEEE Access				NOMA
Cho [28]	19' IEEE TIFS		jamming		beamform
Xiao [148]	19' IEEE ToComm	VLC	eavesdropping		AI/DL
Arfaoui [11]	20' IEEE Comm S&T	VLC		PHY layer	
Shaaban [123]	21' WILEY survey	VLC		PHY layer	
Memedi [93]	21' IEEE Comm S&T	V2X			hybrid net
Zhu [168]	17' ACM MobiCom	photograph	privacy		watermark
Cao [20]	19' ACM SIGSAC	LiDAR	adversarial		
Pan [106]	19' ACM MobiCom	QR code	eavesdropping		secure zone
Maiti [89]	19' ACM IMWUT	smart lights	privacy		
Cui [35]	20' ACM MobiCom	VLC	side-channel		
Our survey	covers all four aspects	✓	✓	✓	✓

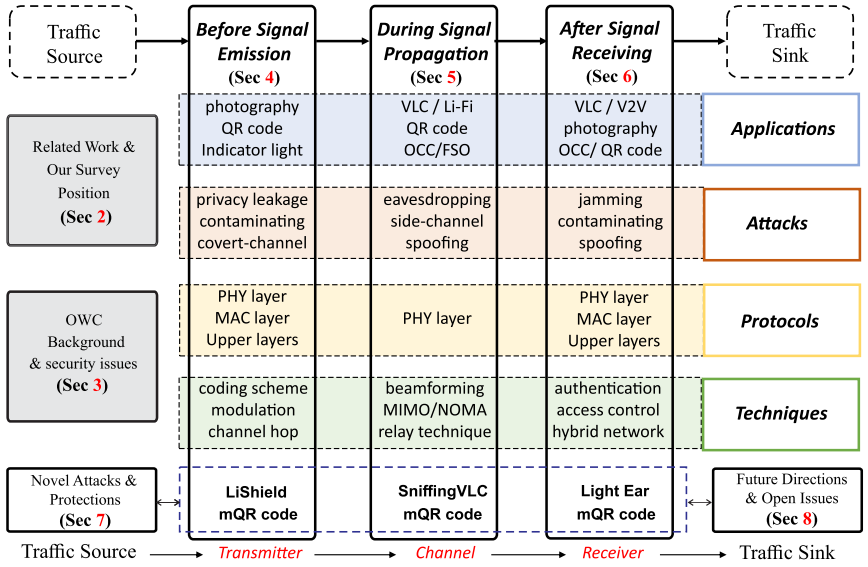

Fig. 2. Our survey covers all four aspects in secure OWC networks.

Given the specific **attack** types, the authors in References [119, 123] thoroughly described the many hazards in OWC networks, including jamming, polluting, eavesdropping, and spoofing. They also looked on corresponding PLS techniques for dealing with these attacks. For instance, to improve network secrecy, they advocated integrating different PLS approaches (beamforming, secure zones, friendly jamming, MIMO, and so on). As for specific attacks, the authors of References [34, 63, 65, 126] discussed jamming attack models and investigated the friendly jamming as the secure solution. Some novel attacks are listed in Table 2 and Figure 2 as well, including eavesdropping [148], privacy leakage [89, 168], side-channel attacks [35], covert-channel attacks, and so on.

Given the **protocols** and network architecture, the major distinction between OWC and RF-based wireless networks is their medium in the physical layer. The latest IEEE OWC network standard [1, 120] specifies the network architecture, which includes the PHY layer, MAC layer,

network layer, and application layer. There are various efforts that take into account the security issue on the PHY layer as well. As an example, the authors of References [98, 150] presented an overview of **PLS (physical layer security)** in VLC and LiFi systems. References [130, 151] investigated the PLS issues in multiple-users scenario in a 3D space. Some work also suggested viable solutions [24, 142] to improve the security performance in PHY layer of OWC, such as managing transmitter angle diversity, **MIMO (multiple-input-multiple-output)**, **NOMA (non-orthogonal multiple access)**, and so on. In addition to the physical layer, other papers [5, 17, 101, 119] examined security threats in the MAC layer of OWC networks.

Given the sophisticated **techniques** used in OWC (e.g., beamforming, dimming control, spectrum hopping, **AI/DL (artificial intelligence/deep learning)** approaches, spatial multiplexing, hybrid networking, and so on), the primary goal of these studies was to promote communication performance, including throughput, reliability, and security. For example, some studies [27, 28, 70, 71, 83, 100] have been done on adaptive beamforming algorithms to eliminate LoS signal blockages to provide smooth and stable communication services or to avoid signal leakages to eavesdroppers by innovative beamforming designs. Other advanced techniques for secure OWC are emerging, such as **RF/VL (radio frequency/visible light)** hybrid networks [11, 29, 97] and some [28, 93, 106, 148, 163, 168] are included in Table 2 and Figure 2.

However, there are security threats at every stage of the traffic flow, as seen in Figure 1. To the best of our knowledge, no prior investigation has systematically investigated the security of the OWC network in this rational manner. Instead of focusing on a single topic, our research covers all four categories (application, techniques, protocols, and attacks) and organizes them according to the OWC traffic flow. Figure 2 depicts the content coverage and our survey position. We expect that this survey will give a comprehensive review of security in OWC networks.

3 OWC BACKGROUND AND SECURITY VULNERABILITIES

In this section, we will first go through the characteristics and features of optical signals in this section. The network of OWCs is then compared to RF-based networks. We also present OWC network architecture as defined by the IEEE OWC standard [1]. Finally, we reveal the security flaws and vulnerabilities in OWC networks.

3.1 Source, Propagation, and Sink of Optical Signals

3.1.1 Modulated Signals as Source. Natural sunlight, starlight, lightning, man-made torches, candlelight, and modern illumination infrastructures can all be treated as light sources. Humans use light as a method of communication as well as a source of lighting, as evidenced by ancient Chinese beacon towers [68, 117]. New types of lamps (e.g., laser lamps, incandescent light bulbs, fluorescent lamps, LED lamps, Halide lamps, sodium lamps, mercury lamps, cold cathode tubes) suitable for diverse circumstances are becoming available as lighting technology progresses [145].

OOK: On–off keying modulation is the simplest form of **amplitude-shift keying (ASK)** modulation [1]. OOK is applied to RF carrier waves as well as optical communication systems. OOK represents digital data by the presence or absence of a carrier wave. Bit "1" is represented by the light being turned on, whereas bit "0" is represented by the light being turned off.

VPPM: Variable pulse position modulation is a new modulation technology that allows for simultaneous illumination, dimming control, and communication [1]. VPPM is intended for pulse-width-based light dimming and protects against intraframe flicker. In VPPM, the pulse amplitude is always constant, and the dimming is controlled by pulse width rather than amplitude.

CSK: Color-shift keying is a visible light communication intensity modulation described in the IEEE 802.15.7 standard that sends data invisibly by changing the color of red, green, and blue light emitting diodes [1]. The CSK symbol is produced by combining three color light sources from

the seven color bands indicated in the standard. The center wave length of the three color bands on xy color coordinates determines the three vertices of the CSK constellation triangle.

Other modulations: The standard offers six PHY modes to meet the various needs of applications. PHY I is intended for use outdoors with low data rate applications, with data speeds ranging from tens to hundreds of Mbps. PHY II is designed for indoor use with applications demanding a moderate data rate in the tens of Mbps. PHY I and PHY II both use OOK and VPPM modulation. As for PHY III, it is designed for CSK applications that use a variety of light sources and detectors and require data speeds in the tens of Mbps. To accomplish a relatively low data rate, PHY IV, PHY V, and PHY VI use different modulations with discrete light sources, diffused surfaces, or video displays. For example, **UFSOOK (undersampled frequency shift ON-OFF keying), Twinkle VPPM (Twinkle variable pulse position modulation), S2-PSK (spatial two-phase shift keying), HS-PSK (hybrid spatial phase shift keying), Offset-VPWM (offset variable pulse width modulation), RS-FSK (rolling shutter frequency shift keying), C-OOK (camera ON-OFF keying), CM-FSK (camera m-ary frequency shift keying), MPM (mirror pulse modulation), AQL (asynchronous quick link)**, and so on [1].

3.1.2 Line-of-sight Manner in Propagation. **Broad bandwidth.** The bandwidth of the optical spectrum is 10,000 times that of the RF spectrum [162]. The light resources cover a broad license-free spectrum that includes infrared, visible, and ultraviolet light. Optical wireless communication utilizes the light as the transmission medium for wireless communication. The broad frequency bandwidth in OWC provides the possibility of robust and secure multiple access. For example, in the broad optical spectrum, channel hopping methods will enjoy more hopping opportunities.

LoS Propagation. Because the light wavelengths are shorter than 700 nm, they can propagate in a **Line-of-Sight (LoS)** manner. Unlike radio frequency signals, optical signals propagate directly across the optical environment from the transmitter (light source) and finally arrive at the receiver side in Line-of-Sight travel path without passing through the obstacles as the RF signals. This inherent propagation feature eliminates signal leakage hazards and makes monitoring and controlling attackers in LoS travel pathways easier. Other than the LoS propagation property, three other properties can provide physical layer security: simple beamforming, broad bandwidth, and location-related information.

Location-related information. OWC systems give location-related information due to the LoS propagation property and the visibility of optical signals. For example, in addition to providing useful directional information to the ship, the lighthouse's location can be used to provide location-related services such as navigation. When compared to RF-based wireless communication, users can easily detect their own location as well as the transmitter's location, which is important for monitoring and inspecting attackers and leakages during communication operations.

3.1.3 Sink for Diverse Applications. There are various OWC technologies, as described in Reference [31], such as **VLC (Visible Light Communication), LiFi (Light Fidelity), OCC (Optical Camera Communication), FSOC (Free Space Optical Communication)**, and **LiDAR (Light Detection and Ranging)**. These OWC approaches have a wide range of applications as well [7, 72, 80, 112, 146]. For example, OWC techniques can be used in industry, transportation, workplaces, houses, malls, underwater, and space. Depending on the application type and the required data speed, communication type, and platform, different OWC techniques are employed. Security issues exist in a variety of applications. As a result, we classify OWC network risks according to various applications in the manner specified below.

Indoor vs. Outdoor: In indoor environments, attackers can conduct eavesdropping assaults in the transmitter's LoS zones without interfering with the process of OWC transfer from the transmitters to the genuine receivers. Although the walls can prevent optical signal leakage from

the indoor environment, the attacker can also steal critical data through its RF side channels. When opposed to indoor scenarios, outdoor conditions, such as sunlight, have considerable optical noise. However, because the OWC transmitter can generate weak RF signals while transmitting optical signals, the attacker can still use the RF side channel to conduct sniffing assaults.

Single-user vs. Multiple-users: OCC-based applications are prominent as one of OWC techniques because of the ubiquity of smartphones. For single user services, the majority of OCCs use **Device-to-Device (D2D)** communication. Despite the low risk of attacks on the user's receiver side, the eavesdropper can still access the optical channel in the same area, for example, to take images or record videos. Because of its inherent broadcast nature, the VLC is also suitable for allowing a large number of users to access the same optical wireless resource [163]. In the same enclosed physical space, unauthorized users and eavesdroppers will inevitably obtain raw optical signals from the open VLC channels.

Static vs. Mobile: The vast majority of indoor VLC systems are static OWC applications, with the transmitter and receiver remaining stationary during transmission. Other OWC applications in which the transmitter or receiver is mobile include **V2V (Vehicle-to-Vehicle)** or **V2I (Vehicle-to-Infrastructure)** communications. When opposed to static applications, mobility situations make it more difficult for attackers to carry out attacks due to the moving placements of the optical channels and the distorted optical signals.

Terrestrial vs. Underwater vs. Space: OWC devices can be used in underwater and space settings in addition to most terrestrial applications. In general, terrestrial attacks are less expensive than underwater and space attacks. Similarly, terrestrial attacks are less challenging than sea or space attacks. Furthermore, RF side-channel attacks for underwater OWC are useless because of the substantial distortion and interference caused by sea water.

High-speed applications vs. Quick link services: VLC and LiFi techniques are used to give high-speed services, whereas OCC provides quick link services. For example, indoor LiFi systems provide reliable and Mbps-speed access. OCC, however, offers low data rate services that can be used to provide quick link services for a large number of IoT devices. High-speed applications may necessitate more secure solutions than quick link services.

3.2 Comparison and Connection with RF Networks

3.2.1 Differences between Optical and RF Signals. **Wavelength and Bandwidth.** Optical radiation is electromagnetic radiation that has wavelengths ranging from 100 nanometers to one millimeter. The wavelength range that the human eye can detect is referred to as **visible radiation (VIS)** and ranges between 400 nm and 800 nm [31]. UV light is optical radiation having wavelengths less than 400 nanometers. **Infrared (IR)** radiation has wavelengths greater than 800 nm. Microwave (1 mm–1 m), VHF wave (1–10 m), LF wave (10–100 m), MF wave (100–1,000 m), LF wave (10 m–1 km), and VLF wave are all examples of RF wavelengths (100 m–10 km). The bandwidth of optical waves is around 30 PHz, which is 10,000 times greater than the bandwidth of radio waves (300 GHz).

Propagation. OWC necessitates a direct link between transmitter and receiver. Unlike RF transmissions, optical signals cannot flow through or around obstacles such as non-transparent objects. Light's LoS feature may provide a more secure physical layer than RF-based wireless communication. For RF signals, there are four propagation modes: (1) Free space propagation, (2) Direct modes (Line-of-Sight), (3) Surface modes (groundwave), and (4) Non-Line-of-Sight modes. Lower-frequency radio waves can pass through obstacles such as buildings and plants, but this is still considered a Line-of-Sight approach. Surface modes are radio transmissions with lower frequencies ranging from 30 to 3,000 kHz that travel as surface waves following the curvature of the Earth. Non-Line-of-Sight propagation modes include ionospheric modes, meteor scattering,

auroral backscatter, sporadic-E propagation, tropospheric scattering, rain scattering, airplane scattering, and lighting scattering.

Performance Underwater. The performance of optical and radio frequency waves for underwater wireless communication differs as well. Two mechanisms impede light transmission in water: absorption and scattering. As a result of scattering, the quantity of photons captured by the receiver is reduced. Furthermore, in a murky underwater environment, numerous photons may arrive with delays, resulting in **inter-symbol interference (ISI)** [122]. RF results in extremely poor performance for long distance underwater communications, especially over long distances, due to heavily influenced elements such as multi-path propagation, channel time changes, and strong signal attenuation (particularly the electromagnetic shielding effect in sea water). As a result, the RF systems are constrained by the associated short link range [30].

Energy Efficiency. When compared to an RF system, which necessitates energy-guzzling antennae and additional energy for cooling down, optical wireless communication uses the energy-efficient LED bulbs, and the consumed energy is not only for communication but also for the simultaneous lighting [55]. Thus, the OWC can provide considerable energy saving. Offloading traffic from RF networks to optical networks reduces overall power consumption [30].

3.2.2 Common Features between Optical and RF Networks. Despite their distinct physical properties, optical waves and radio frequency waves have several similarities: (1) They both have the same propagation speed in the air that is faster than audio waves; (2) they have the same upper layers in the network architecture with the exception of differences in the Physical layer and the Mac layer; (3) they are both essentially electromagnetic waves, transverse waves rather than longitudinal waves like sound waves; (4) the mmWave in the RF spectrum propagates in an LoS way, similar to optical waves; and (5) except for the **VL (visual light)** optical spectrum, other optical spectrum are likewise invisible, similar to RF waves.

3.3 OWC Architecture and Security in Standard

3.3.1 OWC Network Architecture. In contrast to RF-based wireless networks, the IEEE OWC standard [1] varies slightly from typical wireless networks in that optical transmissions cannot traverse obstacles such as walls. The PHY layer, which includes the light transceiver and its low-level control mechanism, and the MAC layer, which allows all types of transfers to access the physical channel, form an **OWPAN (Optical Wireless Personal Area Network)** device. Figure 3 depicts these layers in pictorial form.

The upper layers of OWPAN are also illustrated in Figure 3. The OWPAN has a network layer and an application layer. The network layer handles network configuration, manipulation, and message routing. The device's intended purpose is provided by the application layer. The standard defines two sublayers between the upper layers and the MAC layer: **LLC (logic link control)** and **SSCS (service-specific convergence sublayer)**, which serve as bridges from MAC to upper layers.

3.3.2 Security Discussed in Standard. Devices can be low-cost and have limited processing capability, available storage, and power consumption; it is not always assumed that they have a dependable computing platform with rich resources. Communications may involve brief partnerships between devices that have never worked together before and cannot rely on a permanent infrastructure being up at all times.

Because the development and maintenance of trust connections between devices should be handled with caution, these constraints limit the choice of cryptography algorithms, protocols, and influence the security architecture's design [1].

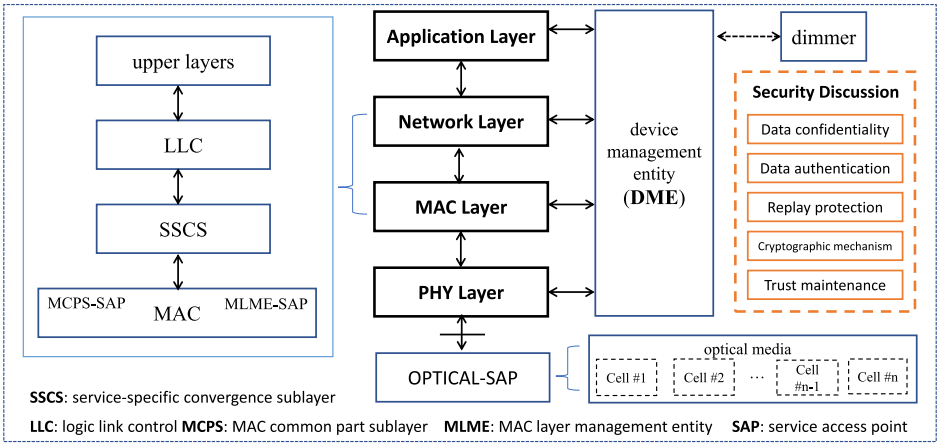

Fig. 3. The OWC network architecture and security discussion in IEEE standard [1].

Furthermore, battery life and cost limits can severely restrict the amount of security overhead that these networks can tolerate, whereas this is much less of an issue with bigger bandwidth networks. Because the majority of these security architectural components can be implemented at higher tiers, they are deemed outside the scope of this standard.

The cryptography mechanism provides particular combinations of the following security services: (a) data confidentiality: assurance that transmitted information is only disclosed to parties for whom it is intended; (b) data authenticity: assurance of the source of transmitted information (and, thereby, that information was not modified in transit); (c) replay protection: assurance that duplicate information is detected.

The actual frame protection given can be changed on a frame-by-frame basis, and it allows for variable levels of data authenticity to minimize security overhead in transmitted frames where necessary, as well as optional data confidentiality. Replay protection is always offered when nontrivial protection is necessary.

The usage of a key shared between two peer devices (i.e., link key) or a key shared among a group of devices (i.e., group key) is permitted for cryptographic frame protection. As a result, there is some flexibility and application-specific tradeoff between key storage and key maintenance costs. When a group key is used for peer-to-peer communication, it only protects against outsider devices and not against potentially malicious devices within the key-sharing group.

3.4 OWC Security Vulnerabilities

3.4.1 Risks in LoS and NLoS. Attackers must be inside the victim's **Line-of-Sight (LoS)** range to initiate an assault. This LoS propagation manner of the light blocks the majority of strikes that are not inside the LoS range. However, in both LoS and NLoS scenarios, there are still threats to the security of OWC.

Risks in LoS. There are several types of OWC techniques in general, such as **visible light communication (VLC), light fidelity (LiFi), optical camera communication (OCC), free-space optical communication (FSOC)**, and **light detection and ranging (LiDAR)** [31]. They are different for user cases, application categories, or technique requirements. The data-links in these OWC systems consist of: the transmitter, the optical propagation channel, and the receiver. If the attacker or hacker devices are in the LoS range of the data-link, then they still have the opportunities to steal or infer the user's privacy and relevant data by a verity of attacks. Due to

the fact that light signals can not penetrate through walls, we can prevent privacy leakage in the limited area or room with curtain covered windows compared with RF-based signals. However, due to the broadcast nature of OWC, the VLC channels are still facing the eavesdropping risks from unauthorized users accessing to the same room/area illuminated by the LED lamps. Typical threat scenarios are indoor public areas such as shopping malls, aircrafts, labs, sensitive meeting rooms, and so on.

Risks in NLoS. Modern Internet-enabled smart light devices, including LiFi, smartphones/tablets, smart lamps, and LEDs in display promise energy-efficient lighting and display function compared with traditional lamps and screens. However, these smart light devices or displays connected with the Internet also increase the risk of leakage of user's private information. These devices enable the fine-grained color and intensity emission that are utilized to carry local or public Internet data. However, if the attacker is in the range of light-emitting areas, then (s)he can capture the changing light with light sensor devices. Even if the attackers are not in range of the LoS of smart devices, they can still perform attacks. They can also install monitoring virus programs on these devices to create the new channel to steal the raw data from these "gateways." Besides the direct visible signals leakage, these smart electrical devices can generate undesigned RF signals when controlling the light signals, thus increasing the security risks as well. The light signals are propagated in LoS, however, all the light transmitted from the light source are not nearly paralleled. Except laser light sources, which can send out paralleling signals, other light sources such as our daily lamps are mostly the point light source with emissions to multiple directions. The attackers can capture optical signals in Non-Line-of-Sight areas and it is modifiable and high-cost to check the existence of attackers in NLoS paths. Even if we can improve the security level and authentic rules for indoor OWC networks, there still exists the risk of data leakage from side-channels such as the weak RF signals generated by transmitters in the process of optical signal controlling, such as turning on/off the lamps. These weak RF side-channel signals can be captured outside the walls due to RF signals can pass by obstacles and penetrate the walls.

3.4.2 Attack Types of OWC. To better study the security risks in OWC networks, we classify the attack types in four methods: attack goals, system structure, application scenarios, and channel types: (a) by attack goals (i.e., jamming, eavesdrop, spoofing, and **DDoS (Distributed Denial of Service)**-based OWC attacks), (b) by channel types (i.e., side-channel attacks and covert-channel attack), and (c) by system structure (i.e., transmitter side, channel side, and receiver side attacks).

(a) classified by attack goals

Jamming attacks. Jamming attacks are defined as the attacks where malicious nodes block legitimate communication by causing intentional interference in networks [49]. The jammers who attack OWC systems aim to prevent legitimate communications by adding optical noise and continuous signals to block the signal receiving at the receiver side. For example, the jammer knows the receiver's location and sends optical signals to the receiver to disturb or block the optical signals emitted from the transmitter, and thus the OWC system can not work and receive the data correctly. The one example of jamming attack is shown in Figure 4.

Eavesdropping attacks. Eavesdropping attacks are also known as sniffing attacks or snooping attacks. Eavesdroppers retrieve user information via optical channel or upper layers in the network. The eavesdropping attack typically happens under the usage of unsecured networks, such as public OWC connections in the shared LoS space. The eavesdropping in OWC and the optical privacy leakage are pervasive and normal. For example, the eavesdropper can easily take pictures of sensitive scenes/objects/people in the public area. Also, the eavesdropper can easily intercept the optical signals without the knowledge of the legitimate users given that the eavesdropper is

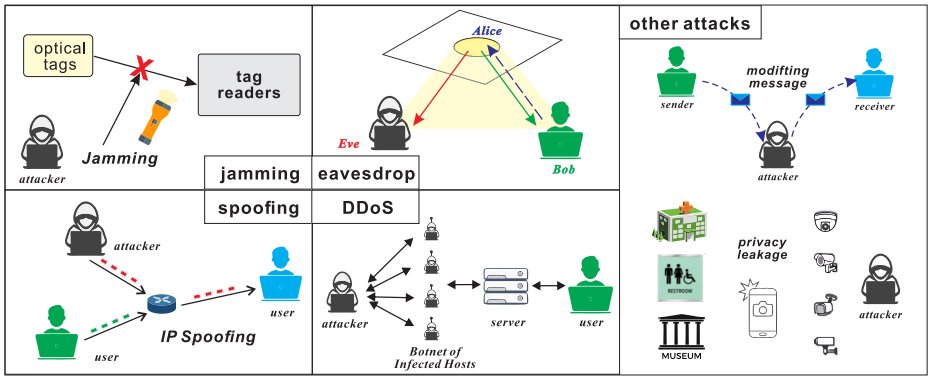

Fig. 4. Illustration of jamming, eavesdropping, spoofing, DDoS, and other attacks.

in the same LoS zone. The eavesdropper can perform eavesdropping attacks in the same room or outside of room via windows. One example of eavesdropping attack is shown in Figure 4.

Spoofing attacks. In the context of the network security, a spoofing attack means the situation where a person or program successfully identifies as another by falsifying data. For todays' OWC systems, how to guarantee the authenticity of the visible light signals from these light fixtures has become an urgent problem. The reason is that almost all these light fixtures are without protection and open to the access by almost every user. Thus, these transmitters in OWC network are subject to tampering and substitution attacks. As introduced in Reference [23], the attacker can easily replace an authentic LED by a rogue LED controlled by the attacker to inject spoofed optical signal into user's receiver. One example of spoofing attack is shown in Figure 4.

DDoS attacks. Denial-of-Service attacks are characterized by an explicit attempt by attackers to prevent legitimate use of a service. There are two general forms of DoS attacks: those that crash services and those that flood services. The most serious attacks are distributed. In OWC networks, the DDoS attacks can happen in both transmitter and receiver side, especially for duplex communication scenarios. For example, when the transmitter receives the response from multiple users, the attackers can flood traffic in the up link to crash the services of transmitter. On the other side, when the user receives the data from multiple transmitters, the attacker can also flood the traffic in the down link. One example of DDoS attack is shown in Figure 4.

Other attacks. Besides aforementioned attacks, the OWC systems are vulnerable to other attacks [123] such as message manipulation, reply attack, packet falsification, hijacking, membership falsification, and so on. The attacker's goal for message manipulation is to violate the integrity of a message and trick a victim receiver to accept the attacker's chosen message, while the sender/transmitter considers the original messages were delivered successfully. In replay attack, the valid data transmission is maliciously or fraudulently repeated or delayed in the network. Due to the property that optical signals can be intercepted in the middle of the transmitter and the receiver, the attacker can also perform massage manipulation and replay attack in OWC networks. Two examples of other attacks are shown in Figure 4.

(b) classified by channel types

We can also classify attacks by channel types of OWC attacks into side-channel attacks and covert-channel attacks as summarized in Reference [89]. **Side-channel attacks**: User's private data leaked through optical side-channels in a passive way. **Covert-channel attacks**: User's private data leaked through optical covert-channels in an active way.

Side-channel attacks. The side-channel attack mainly focuses on power consumption attack, electromagnetic field attack, and time attack. Power dissipation is one of the most powerful means

of attack, including simple power analysis attack **(SimplePower Analysis attacks, SPA)** and differential power analysis attack **(Differential Power Analysis attacks, DPA)**, compared with the traditional cryptanalysis, the means of attack effect is remarkable. In the OWC field, attackers infer the data or media content via capturing the changing light color and intensity. Most attacks even capture the images of the user's smartphone or screen to steal private data straightforward.

Covert-channel attacks. Unlike passively capturing users' private data, covert-channel attacks carefully control and operate the infrared light or other light unperceived by the human eyes of the smart bulb or screen of smart devices. This unperceived light to a human can be used as a "covert-channel" between the user's light device and the adversary device, which has infrared sensing ability. The attacker will install a software agent into the user's light device and then encode and transmit the private data over the covert-channel to the attacker. Besides, there are no authorizations for controlling lights on the victim's smartphone or smart bulbs. Any Trojan installed on a smart light-emitting device can act as a proxy for this type of attack. For example, the attacker can utilize a malicious infrared-equipped camera to inject or steal the private data to or from the air-gapped network. The covert-channel attack enables the victim's device as a gateway to leak the private data actively. The covert-channel could be one-way or two-way LoS data exfiltration or infiltration gateway. The covert-channel could be created by using the infrared spectrum due to human eyes cannot perceive infrared light. Moreover, the covert-channel can use visible light as well if the light signals are modulated in high-frequency or specific modulation scheme to make signal unperceived by victims. After private data transmission via the smart light-emitting device to the adversary device, the attacker executes the process of adversarial reconstruction. The attacker uses the infrared sensor to observe the victim's device. The reconstruction performance is related to the amount of signal attenuation and the optical channel noise.

(c) classified by system structure

Transmitter side. The attacker can perform attacks at transmitter or set the transmitter as attack object. The attacker can easily install the virus software/program at the transmitter due to the smart LED lamps are connected to the Internet. Thus, the attacker can conduct attacks such as message manipulation, reply attack, spoofing attack, DDoS attack, and other attacks at the transmitter side before the emission of the optical signals.

Channel side. Most attacks in OWC networks are conducted at the channel side. There are three types for the attacks at the channel side: (1) Attacker is between the transmitter and the receiver. For example, the attacker put a relay device in the middle of transmitter and the receiver and conduct replay attack, message manipulation attack, eavesdropping attacks, and so on. (2) Attacker is in the range of LoS zone of the transmitter. The attacker can perform eavesdropping attacks in this situation. (3) Attacker is in the range of NLoS zone of the transmitter. The attacker can perform sniffing attacks via RF side channel out of the LoS zone [35].

Receiver side. The attacker can also conduct attacks at the receiver side or set the receiver as the attack object. Due to the receivers in OWC networks are mostly the smart devices, such as the smartphone or **PD (Photo Diode)**-equipped MCU, the attacker can easily install virus software at the receiver and perform the replay attack, message manipulation here means tampering of message.

4 BEFORE SIGNAL EMISSION (BSE)

4.1 Security Risks of BSE in Diverse Applications

Certain applications have always had the security vulnerabilities at the BSE stage. We show three typical vulnerabilities: (1) photography, (2) bar / QR code, and (3) indicator light as shown in Figure 5.

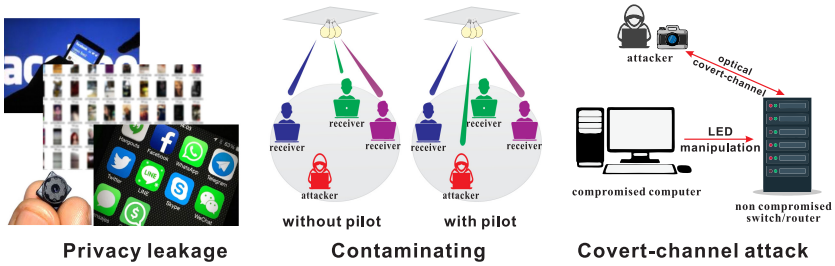

Fig. 5. The illustration of attacks happened in BSE (some pictures are from the Internet with redesign).

Photography. Consumer mobile devices with cameras, such as smartphones, tablets, drones, smart glasses, first-person recordings, and so on, are now ubiquitous. The proliferation of these cameras, combined with ubiquitous wireless access, is spawning a new wave of visual sensing applications, such as online video meeting, life-logging (vlog), live, photo-sharing social networks, and augmented reality applications [168]. Although camera-related applications create a more convenient and open environment that brings people closer together, they also raise privacy concerns at every moment. In our daily lives, optical signals involving sensitive scenarios, such as movie theaters, museums, government offices, dressing rooms, and so on, are naturally generated and emitted. As a result, if there is no physical shelter to stop the signal spread out, then these private circumstances automatically pose security risks at the stage before signal emission.

Bar/QR code. Barcodes are a universal technique that enables visual data representation utilizing a common series of lines, squares, or dots such as one-dimensional lines and spacing or two-dimensional dots to represent data [141]. They are popular machine-readable codes in our daily life. These optical tags function by embedding data in a 2D surface and spreading optical signals in public space, allowing reader equipment, such as smartphones, commercial cameras, and so on, to capture and decode encoded data rather than human-readable texts and images for more communicated data. However, because of the inherent nature of light, these visible codes can be captured by attackers and used to leak crucial and private data if they are private codes or intended at single user services, such as payment, access control, personal token, and so on [106].

Indicator light. Various studies over the past two decades have proven unique approaches for extracting information from victim devices using optical sensors (e.g., photo diodes, cameras) by leveraging the correlation between the optical side effects of the information and the device used to deliver the information [103]. Previous studies have examined the risks that a device's power indicator LED, with its linear response, may pose to the information given or processed by the device. Some research used preinstalled malware to create covert channels while modulating the user's data, which was subsequently leaked through the indication LEDs [52, 53]. Many applications in our daily lives are running on devices with LED indications, including the stereo, TV, computers, displays, cellphones, sweeper robots, wireless headsets, surveillance cameras, and so on. As a result, on these machines' side, the security risks exist before the optical signal emission.

4.2 Attacks Happened in BSE

The attacks happened in the BSE stage exist at the transmitter side, as shown below.

Snooping attack. It is reported more than 350 million photos/videos are uploaded to Facebook every day and over 40 billion photos and videos have been shared on the Instagram platform. These photos are mostly generated from mobile devices such as our smartphones. Although most people do not plan to photograph others who do not wish to be photographed, it does occur on a regular basis. Because these private photographs are freely shared online, it raises privacy concerns and

opens the door for attackers to obtain private information via **online social networks (OSN)** [64]. Many reports have revealed examples of users being fired as a result of sensitive images that they thought were private but were not. As illustrated in Face/off [64], certain instances illustrate the privacy problems that exist in our daily situations, allowing attackers in OSNs to view our private images: (1) the malicious tagger, (2) the silent uploader, (3) the group photographer, (4) the accidental over-sharer, and (5) the friendly stranger.

Contaminating. The goal of this assault is to pollute the communication channel estimate phase. The optical wireless communication is based on Line-of-Sight propagation manner and then it has the great potential for spacing multiplexing such as massive **MIMO (multiple input and multiple output)** technology [123]. Although MIMO can achieve high throughput with high efficiency of energy consumption and spectrum bandwidth, it increases the security risks. MIMO wireless technology, for example, is extremely vulnerable to pilot contamination attacks [142, 167]. The reason for this is that massive MIMO requires accurate **channel state information (CSI)** to pick optimal beamforming. During the channel training phase, a pilot-contamination attacker could undermine channel estimation by imitating and sending the identical pilot signals as normal users (LUs). As a result, the attacker may get an unfair advantage during the next communication phase [67]. In addition to massive MIMO, **NOMA (non-orthogonal multiple access)**, which can improve spectrum efficiency, is vulnerable to a pilot-contamination assault at the BSE stage [41].

Covert-channel attack. Several out-of-band covert channels have been developed in recent years, demonstrating the possibilities of leaking data out of computers without the requirement for network access. One of the earliest types of covert channels studied was electromagnetic radiation from the electrical devices such as keyboards, computers, embedded systems, and so on [74, 75, 140]. Other types of covert-channel attacks happening via both acoustic and thermal have also been studied [51, 56]. On the transmitter side, the attackers can preinstall the virus or program to modulate the signal (e.g., electromagnetic radiation, audio signals, or optical signals). Thus, the attackers can steal the vital data. One example of the optical covert-channel attack [50] takes advantage of the limitations of human visual perception to conceal sensitive data encoded in high frequency on the computer screen.

4.3 Security Protocols in BSE

The transmitter, which receives traffic from the Internet or LAN via the upper layer, is where the bulk of security flaws in the BSE stage are found. The MAC layer controls and divides the optical traffic between the various users. Finally, optical traffic with error correction, encryption, and different assigned resources is released by the PHY layer. The work of BSE and related security standards are outlined here.

PHY layer. Physical layer security in the information-theoretic approach, which covers topics such as trusted communication zones, artificial noise production, beamforming techniques, and PHY-based secret key generation, is the most established security-related study field in VLC [11, 15, 101]. The fascinating addition of **Physical Layer Security (PLS)** to cryptography-based security provides a second secrecy layer that is demonstrably impenetrable regardless of the computational capabilities of the attackers. PLS is a compelling substitute for simple standalone secrecy solutions for hardware- and/or energy-constrained systems, such as Internet of Things applications. Authors in Reference [101] designed a secure MIMO-VLC with adaptive emission controlling of cells in PHY layer.

MAC layer. For MAC-level security, the IEEE 802.15.7 standard employs symmetric-key cryptography. For example, the authors in Reference [101] proposed the modified **Rivest-Shamir-Adleman (RSA)** encrypting for media acess control. The standard does not include key creation and management processes. Frame protection is implemented as follows at the MAC

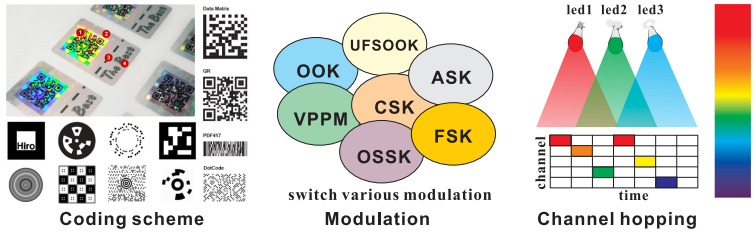

Fig. 6. The illustration of protections for BSE (some pictures are collected from the Internet with redesign).

level: For peer-to-peer communication, (1) a "link key" used solely by the peers is used; (2) for communication between a group of devices, a common "group key" is used. This technology allows for some flexibility and application-specific tradeoffs between the expenses of key maintenance and storage and the security it offers [1, 15]. Furthermore, the media switch protocol was proposed in the heterogeneous LiFi-WiFi system for supporting secure communication [11].

Upper layers. All wired and wireless networks, including VLC systems, are using the OSI protocol stack, which is composed of the **physical layer (PHY), media access layer (MAC)**, network layer, and other layers. Because the physical properties of light communication media are primarily represented in the two bottom layers, the PHY and MAC, most security work in OWC concentrates on these two layers. However, because different OWC applications do not typically use RF technology, a number of researchers are looking into several higher layer security protocols [15]. Turan and Ucar addressed and explored important security challenges affecting VANETs in their work. These issues were classified according to the layer they affected: application, system, and network. In addition, the authors suggested and investigated a "SecVL" protocol designed for secure data transmission in a hybrid VLC/DSRC configuration [93].

4.4 Protection Techniques in BSE

For security vulnerabilities that exist prior to optical emission at the transmitter side, the basic idea for protection is to make decoding the optical signals more difficult, such as encrypting QR codes, blurring or adding an optical shield to private scenes, friendly adding optical noises at the transmitter side to make attackers fail to decode the data. We show three kinds of protection techniques: (1) coding scheme, (2) modulation, and (3) channel hopping as shown in Figure 6.

Coding scheme. Optical codes or tags embed data into 2D images such as various bar codes and matrix codes. The security level at the BSE stage will be enhanced if the coding scheme uses encryption codes that only the receiver can decipher. As discussed in Reference [73], we can upgrade the coding scheme for QR code applications to improve security: (1) examine how difficult and expensive it is for altering the original code; and (2) integrate digital signatures into standards of QR codes to confirm the code's creator and then determine if updated QR codes are legitimate.

Modulation. Modulations used in OWC systems include OOK, PWM, PPM, VPPM, CDMA, OFDM, FSK, and others [16]. The complexity of modulation increases the difficulty of decoding them considering the eavesdropper with infinite computational power [59]. In addition to increasing the complexity of the modulation scheme, we may also add modulated optical noise to reduce the quality of the images to preserve privacy, as the frequency scrambling-based OOK modulation waveform in the LiShield [168]. In References [59, 66, 95], to improve the physical layer security at the BSE stage, the authors suggest using **optical space shift keying modulation (OSSK)**. In Reference [85], the authors propose to apply the **chaos-based constellation rotation (CCR)** method to **CSK (color shift keying)** modulation scheme. Because chaotic sequences are non-periodic and sensitive to the beginning value, the rotation pattern changes dynamically, making it impossible for eavesdroppers to recover information in real time in high-speed VLC systems.

Channel hopping. Channel hopping is a technique to switch the used spectrum band in communication. We may also transmit optical data using a channel-hopping technique that is only known by the receiver and the transmitter in a dynamic spectrum of color bands. Because of this, even if the attackers succeed in capturing the optical signals, they will not be able to properly decode the data. This type of security method makes use of the wide optical spectrum bandwidth. As discussed in Reference [8], the authors investigate the hyperchaotic baseband frequency hopping based optical orthogonal frequency-division multiplexing VLC system, which can enhance the security in VLC network at the stage of BSE. To increase the cost and difficulty of eavesdropping for attackers, they employ a four-tiered encryption strategy that incorporates chaotic frequency/time-domain scrambling of OFDM subcarriers.

5 DURING SIGNAL PROPAGATION (DSP)

5.1 Security Risks of DSP in Diverse Applications

The security risks in the DSP stage exist in numerous applications when the light propagates in the air. We list three classic vulnerabilities below.

VLC/LiFi. VLC systems have been designed and deployed for both indoor and outdoor use. A wide range of communication services are provided today via radio-based WLAN and **Personal Area Networks (PAN)**, and some indoor applications, such as LiFi indoor lighting, may be compatible with these networks [18, 54, 109]. VLC techniques are thought to perform better than conventional radio-based communication techniques in security, for instance. Optical signals are believed to offer a secure path for data transfer inside of a building because of their Line-of-Sight propagation, making the data impossible to capture from the outside. However, as shown in Reference [33], attackers inside the same physical zones and space can still readily spoof optical communications using open and public optical channels. Additionally, because of the shared nature of the optical medium, the attacker is also able to conduct denial-of-service (jamming) attacks.

Bar/QR code. As introduced in Section 4.1, the displayed Bar/QR codes at the transmitter side can be easily captured by anyone in the reading code zones while the optical signals are propagating. Machine-readable optical tags including barcodes and QR codes are widely utilized in daily life. The supermarket checkout systems made the barcode a commercial success. One of these matrix codes is the **QR (Quick Response)** code, which is widely utilized in a variety of applications such as mobile payments, social E-cards, electronic tickets, access control, and so on [136]. Some of these optical codes have encoded passive and static data that is accessible to the public, such as connections to commercial advertisements. The majority of these codes, however, pertain to private information, such as payment codes and access control IDs. If the attacker obtains these codes in the same zones without the authorized users realizing it, then he or she can act as though they are entering the building, checking out for a mobile payment, and other activities, as demonstrated in Reference [106].

OCC/FSOC. OCC, or optical wireless communication based on a camera, is a technology that is gaining popularity as smartphones and commercial cameras become more prevalent. **Free space optical communication (FSOC)** disperses optical signals in free space over a significant communication range. If the optical connection is not encrypted, then attacks will take place whether the users and the eavesdropper are inside or outside of a building. For instance, the attacker can easily track and decode the propagating optical signals using the most reliable and straightforward modulation OOK-based OCC/FSOC. Bar/QR code-based communication can be treated as one type of OCC. If the data embedding and decoding protocols are openly available, standardized, and used by many people, and if bar/QR code images captured by unauthorized users indicate optical data leakage via the optical channel.

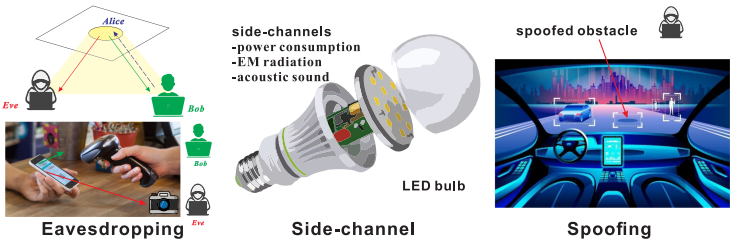

Fig. 7. The illustration of attacks happened in DSP (pictures are collected from the Internet with redesign).

5.2 Attacks Happened in DSP

If the optical signals are accessible to anyone without authentication and public to all, then attacks during the DSP phase can take place. We show three typical attacks below: (1) eavesdropping, (2) side-channel attack, and (3) spoofing attack.

Eavesdropping. VLC/LiFi is susceptible to eavesdropping even though it is more secure by nature, because light cannot pass through walls or objects and is blocked. Other than goal-based communication systems, other content-related lights, such as multimedia-visualization [89], would provide optical signals with a strong connection to private information. The attackers are able to determine the user's preferences for music and videos based on these easily captured LEDs. The attackers can easily eavesdrop on VLC not just from inside a room, but also from outside, or even from a flower pot next to a window, as shown in Reference [33].

Side-channel. In particular, the basic modulation OOK-based OWC transmitter emits an RF signal that can be seen as a side channel when it transmits optical traffic and results in data leakage through the walls [35]. In the aforementioned multimedia-visualization applications, the transmitter emits signals that go through the door and bounce off of surfaces, such as windows, walls, glasses, and other elements. These surfaces can also be regarded as side channels if they exhibit weakly reflected optical signals or other types of variation signals, including shape change.

Spoofing. Attackers can use an additional optical source to transmit the spoof signal to the receiver either with or without the real optical signals during optical signal propagation in free space. For example, the authors in [79] uses optical light to detect human postures as illustrated in Figure 7, there is an additional rogue LED on the ceiling in addition to the genuine LED light source. The same goes for created human shadows and light signals. Since the attack takes place at the signal level during signal propagation (i.e., the shadow) and no logical data is involved in the process, cryptography-based countermeasures are ineffective in this scenario [23].

5.3 Security Protocols of DSP

The optical channel and the PHY layer together account for the majority of the security flaws at the DSP stage. The work of DSP and related security protocols are outlined below.

OWC systems must be protected against eavesdropping, since OWC can transmit sensitive personal information. One simple method is to use WiFi-specific off-the-shelf security measures, such as the cryptographic-based MAC-layer security methods described in the IEEE 802.15.7 standard. Cryptography-based security approaches are efficient if the secret key is unknown to unwanted receivers and the computational capacity of the undesired receivers is limited. The scarcity of these strategies, as detailed in References [60, 102, 111, 149], comprises inefficient key distribution, key exposure potential, and decryption potential. Cryptograph techniques are therefore only conditionally secure. However, **physical layer security (PLS)** offers theoretically supported security

and is a workable strategy for protecting OWC systems. In mQR code [106], authors utilize the varied moiré pattern capturing at different spatial locations during the signal propagation state and propose PHY protocol to generate secure zones. The authors in Reference [127] utilize the **Reflective Intelligent Surface (RIS)** technology and proposed for active jamming protocol to block the eavesdropper during the optical signal propagation stage.

5.4 Protection Techniques in DSP

The fundamental concept of protection for security concerns that arise during optical signal propagation is to regulate the channel, such as by setting secure zones, beamforming, MIMO, and relaying to prevent eavesdropping. We show three kinds of protection techniques: (1) beamforming, MIMO/NOMA, and (3) relay in DSP stage below.

Beamforming. Beamforming technology manages the wireless signals to direct toward a specific receiving device. There is always a chance that someone could wiretap the information signal in the air in crowded, vast spaces, such as workplaces, libraries, and shopping centers. Beamforming techniques in OWC regulate the optical signals' **field of view (FOV)** to concentrate their emission zones and boost the transmitted signals' SNR. In contrast to RF signals, which have longer wavelengths, optical signals can more easily be controlled to produce paralleled optical beams. Thus, the hazards of data leakage can be eliminated and optical signals can be restricted to tiny zones used exclusively by receivers. By turning a non-convex optimization problem into a manageable quasi-convex search problem, for instance, the authors in Reference [100] constructed and solved the beamforming weight vector that maximized the feasible secrecy rate.

MIMO/NOMA. MIMO, abbreviated multiple-input, multiple-output, is a technique that uses several components on both the TX and RX sides to increase system capacity [129, 134]. Additionally, MIMO demonstrates its significant potential to improve wireless communication's concealment. Physical layer security is possible for OWC systems, thanks to MIMO transmission using multiple optical channels and spatial modulation techniques [96, 105, 129, 147]. To improve energy efficiency and confidentiality, MIMO can be used to deactivate some transmit units due to the various user services and broadcast nature of optical media. **Nonorthogonal Multiple Access (NOMA)**, one of the fundamental technologies for the next generation of communications, has drawn significant research interest worldwide [38, 40]. NOMA has the inherent ability to provide wide connection, which opens up the option of security management by allowing several users to share the same frequency or time resources while being segregated in the power domain or other domains.

Relay technique. Relaying is to receive, amplify, and forward the wireless signals with the relay to extend the communication range. Relaying-based mixed RF/FSOC systems have been researched for physical layer security. The FSO link is very susceptible to aiming errors and air turbulence despite its many benefits. The hybrid **radio frequency (RF)**-FSO system grabbed the interest of numerous researchers worldwide to overcome these problems [2, 3, 121]. Relaying methods are a practical way to enhance secure communication networks [42, 78, 104]. In the uplink scenario, data signals are transmitted from users to a relay node through an RF link, where they are converted to optical signals, multiplexed, and transferred to the data center via an FSO link. In the downlink scenario, information signals are delivered to the relay node via an FSO connection, where they are converted to RF signals and sent to users over an RF link.

6 AFTER SIGNAL RECEIVING

6.1 Security Risks of ASR in Diverse Applications

Here, we list three common vulnerabilities that may be found in applications at the ASR stage.

Fig. 8. The illustration of attacks in ASR (some pictures are collected from the Internet with redesign).

VLC. VLC is commonly thought to be a more secure wireless technology than RF-based wireless communication due to the unique physical propagation characteristics of optical signals [15]. However, VLC systems still hold many risks once a signal is picked up by a receiver. Jamming attacks can cause oversaturation of a signal and cause a receiver to not properly receive valid information. An attacker can conduct jamming attacks either through an additional light source or through hijacking an existing valid transmitter [15]. VLC systems are also vulnerable to replay attacks. An attacker can pick up an old signal and replay that signal to the receiver, masquerading it as a new signal. The receiver then uses this new signal, which can have potentially catastrophic effects on the system. Similarly, an attacker could receive a new signal and modify its data before propagating it to the receiver, causing the receiver to use malicious information [138].

Photography. With nearly everybody carrying at least some cameras on them at any given moment, security against illegal photo-taking has become much more difficult. Private photos can be taken from anywhere and spread online, where they will then be difficult to remove. How to address this problem is a relatively new topic. One novel solution to protect privacy could be found within facial recognition. By creating a central database of faces or by wearing clothing with some form of optical tag on it, people could pre-define their appearance in online shared photos. Upon a picture being taken with a cellphone, the cellphone will run it through the central database, which will analyze faces/tags present and determine who is in the photo. Upon the participants being identified, the system can protect their privacy, including facial blurring and restricting their names or other information from the post [37]. While this system will not protect from illegitimately taken photos by non-persons, it is an invaluable defense for people's privacy on the receiver side of picture-taking.

QR code. QR codes provide a significant security risk to OWC networks. QR codes are exceptionally easy to produce and be attached on objectives. They can easily be placed on stickers, shirts, posters, and so on [73]. Therefore, a malicious QR code can also be placed anywhere with no indication that it will have negative effects on a user. A scan of a malicious QR code by a user's cell phone could lead the unknowing user to a malicious website. This website could download malicious files onto a user's device without awareness. Similarly, it could inquire for login credentials or other private information. This process, also known as "phishing," could cause untold damage to victim's life, as the attacker now has full access to their account to a real website as well as their username and password combination, potentially allowing the attacker access into other websites [132].

6.2 Attacks Happened in ASR

The attacks happened in the ASR stage exist at the receiver side, as shown in Figure 8.

Jamming. Jamming attacks are a prevalent issue in OWC security. In a jamming attack, a malicious transceiver sends confounding light signals towards a valid receiver. The attack goal is to flood the receiver with a higher illumination than the valid signal being sent, introducing noise

in the signal. The BER of the received signal will be too high for the user to effectively utilize it. It is a denial of service attack for OWC systems. There are several ways an attacker can send a jamming signal. A standard undirected source could be used, but that would be detectable by the user. Thus, a highly directed transmitter is more desired, as it would be more difficult to pick up. Alternatively, the attacker could hijack part of the existing valid transmitter system [18]. However, jamming attacks are able to be detected to some extent. Using cooperative detective techniques and several cooperating LEDs can achieve 91% detection accuracy [108]. If they can be detected, then perhaps jamming signals can be less impactful on a system.

Contamination. Contamination attacks occur when valid data is contaminated with invalid data by an attacker such as attacks within optical codes/tags. Malicious barcode/QR codes can be devastating to a system, as they can link an unknowing user to a website to download software silently or steal login credentials. Malicious barcodes and QR codes can contaminate legitimate, normal barcodes and QR codes, making it challenging for users to determine which barcodes and QR codes to trust. In a barcode attack, a smaller barcode can be hidden and pasted onto a normal, legitimate QR code without users' awareness. Some phones are redirected to the normal QR code's website, while others will be brought to the malicious website. Thus, it makes the attack difficult for investigators to reproduce and helps the attack stay hidden [9, 36].

Spoofing. Spoofing attack is an issue in virtually all wireless communication systems. Spoofing attack happens when an adversary pretends to be a different valid entity, tricking the user to believe they are something else. As an example, packet falsification occurs when an attacker obtains a legitimate packet from a legitimate sender and changes its contents before sending it to the intended recipient. When the user receives the packet, he/she believes it is an unaltered packet from a valid sender and then uses the modified information, which could have disastrous results. Another similar type of attack is a replay attack, where an adversary saves an old message from a valid source. Instead of modifying this message, the adversary later sends the old message to the receiver. The receiver will interpret this old message as a new message from a valid sender and use its contents as though they are fresh. This would have similar repercussions as the packet falsification attack, as the receiver will use incorrect data as though it is new [138].

6.3 Security Protocols of ASR

The receiver, which will receive light signals from either legitimate senders, physical markers such as barcodes or QR codes, or malevolent entities, is the source of the bulk of security flaws in the ASR stage. The PHY layer receives transmissions and verifies the validity of the data; the MAC layer decrypts data and checks for problems; and ultimately, the application layer implements higher-level security mechanisms.

PHY layer. The physical layer is potentially the most unique aspect of OWC systems. Chaffing and winnowing can be used in the PHY layer. It involves the transmitter sending several fake packets to confuse potential eavesdropping receivers. The valid receiver, in turn, will figure out which packets are fake and ignore them, piecing together only the real packets [118]. Similarly, jamming also occurs on the PHY layer. Friendly jamming can harm an eavesdropping receiver by creating interference, thus making it difficult for them to listen in. Meanwhile, a valid user will suffer little to no adverse effects and only use the legitimate signals, as they will be able to ignore the interference [99]. The PHY layer will also provide some authentication. Using binary hypothesis testing and a sender's DC channel gain, OWC systems can deduce valid senders and invalid senders and ignore invalid communications [63].

MAC layer. The MAC layer, like that in RF systems, protects data integrity and confidentiality by using cryptography. Thus, it contains the details of key encryption and decryption. The receiver will decrypt received signals using symmetric key decryption, meaning both the transmitter and

receiver use the same key. Key generation, however, is done on higher levels [14]. Several cryptographic strategies have been modified to fit OWC communication, including Caesar cipher wheel encryption and quantum cryptography [4, 125]. Unfortunately, like many RF systems, some MAC headers are not encrypted, meaning any malicious receiver that picks up the signal could potentially learn confidential information [15].

Upper layers. The upper layers of the OSI contain many beneficial security protocols. The upper levels are responsible for symmetric key creation and management, which is essential to keep any wireless communication's integrity and confidentiality intact [14]. Additionally, the upper layers handle data manipulation such as stenography. After the receiver gets a message, the message is passed to the upper layers, which will then decode the hidden stenograhpic messages within. These stenographic messages will be undetectable to malicious receivers, ensuring secrecy [16]. QR code attacks can also be detected at upper layers. The future of QR code defense could rely on AI systems that can detect if a scanned QR code contains a malicious link. The link's URL will be analyzed and recognized by the AI system. The AI approach (dubbed barAI) can detect malicious barcodes with a success rate of 90.243% [9].

Comparisons of Security Protocols in BSE, DSP, and ASR. In BSE stage, the secure protocols focus on the improvement of transmitter itself with effective techniques in PHY, MAC, and upper layers. Similarly, the secure protocols at ASR stage focus on the enhancement at receiver itself about signal perception, demodulation, and media access authentication in PHY, MAC, and upper layers. In contrast, the goal of security protocols in DSP stage is to attack the attackers such as eavesdropper, jammer, and so on, via additional devices (e.g., RIS, interference unit) or functions (e.g., MIMO, moiré pattern) instead of enhancements at transmitter/receiver.

6.4 Protection Techniques in ASR

For security vulnerabilities that exist after optical signals receiving, the basic idea for protection is to enforce a proper authentication system to prevent rogue transmissions, provide strong access control to keep malicious entities from accessing important systems, utilizing hybrid RF/VLC networks to broadcast data on multiple channels. We show three protection techniques below: (1) authentication, (2) access control, and (3) hybrid networking in ASR stage.

Authentication. Authentication is a mandatory procedure of any wireless system, as it ensures that only allowable users operate a system. Currently, authentication on the PHY layer is done through feature-based authentication. A receiver looks at a sender's DC channel gain to use it as a fingerprint. A receiver can use a strategy called binary hypothesis testing to attempt to discern between valid transmitters and invalid transmitters. However, it is possible to happen for missed detections, accepting invalid signals as valid, false alarms, and declining valid signals. To avoid the aforementioned problems, a new method of separating the authentication process in two phases has been proposed. In the first phase (training), the valid transmitter sends to the receiver, and the receiver learns the specific features of the transmitter. In the second phase (testing), the valid transmitter and any attackers can send at the same time. Since the receiver knows the features of the valid sender, it will be able to authenticate the valid transmitter and ignore invalid signals [63].

Access control. One of the most unique characteristics of OWC is the dominance of Line-of-Sight signals. Unlike RF signals, OWC signals largely need to have a direct LoS between the transmitter and the receiver [15]. This gives the OWC system a great level of control over who accesses it. For a rogue transmitter to communicate with a valid receiver, it must be within the same room and, often visibly, projecting light towards it. Due to this, it can become difficult for a rogue transmitter to access a receiver without being detected [18]. This makes it one of the greatest defenses of the OWC receiver. Unfortunately, it is not perfect, as many different light sources in

one area can still create interference even if they are all legitimate and simply sending data to a variety of receivers. A single receiver may be able to pick up well over 30 transmitters, which will certainly result in channel interference [94].

Hybrid network. RF and VLC hybrid systems are incredibly valuable, since they can combine the wide range support of RF and the small range efficient transmission of VLC. A security strategy could be to transmit data over both optical and RF channels at the same time to one receiving device that can accept both. Thus, the receiver can aggregate both for the complete message. Eavesdroppers would need to be able to accept both as well, as if they can only receive one data type, then they will not be able to complete the message [11]. Similarly, this hybrid protection could extend to key generation as well. Encryption and decryption keys could be split into many pieces that are then sent over VLC transmitters. A valid receiver within all transmitter ranges will be able to piece the key together, where eavesdroppers who are out of range of any transmitters will not get that transmitter's respective part and remain unable to create the key. This key could then be used for further RF communication [15].

7 NOVEL ATTACKS AND PROTECTIONS

Following the analysis of the security concerns in the three stages (i.e., BSE, DSP, and ASR) of OWC traffic in Section 4, Section 5, and Section 6, we present detailed novel examples of attacks during these three stages and their related countermeasures in this section, as shown in Figures 1 and 2. We select Light Ear (attack in ASR) [89], SniffingVLC (attack in DSP) [35], and the camera-related privacy leakage in LiShield (attack in BSE) [168] and mQR code (attack in BSE, DSP, and ASR) [106] as the novel attack examples. We also report the related protections proposed in LiShield [168] and mQR code [106].

7.1 Novel Attacks

7.1.1 Light Ear [89]. In Light Ear, authors explore smart bulbs LIFX and Phillips Hue bulbs. They both support multimedia-visualization by apps such as Light DJ. When users turn on the multimedia-visualization system, smart bulbs will change or modify the brightness/color in real-time based on the feature of audio or video. In audio-based visualization, brightness change is used to reflect the ambient sound levels or output the music directly. For video-visualization, color and brightness are related to the primary color and brightness level of the current video frame. The adversary's goal is to passively infer medium content of target users by visually eavesdropping the output of smart bulbs.

As shown in Figure 9 (a), for the audio inference threat, there are two fundamental observations in the effect of sound on bulb brightness: (i) higher audio amplitudes make the bulb generate more brightness fluctuations; (ii) for a given song, it has a unique luminance-profile, which differs from other songs. The author designs the audio inference framework based on audio-visualizing light properties. It has four main steps: (a) the attacker within the LoS range of smart light captures the luminance-profile when the target user plays the audio files; (b) normalizing the luminance file to achieve invariant amplitude during similarity search; (c) create a reference library of different songs based on the normalized luminance file; (d) similarity search and song match. For the video inference threat, there are similar observations as audio inference threat: (i) RGB colors outcome from the bulb have a relation with the current frame of the video. (ii) For different video samples, they have specific RGB color-profiles. Compared with an audio-based threat, the video inference threat utilizes the color-profiles instead of luminance-profiles. The video inference framework is (a) capturing color-profile of different video samples; (b) normalizing the color and interpolation; (c) creating a video reference color-based library; and (d) running similarity search in library and video match.

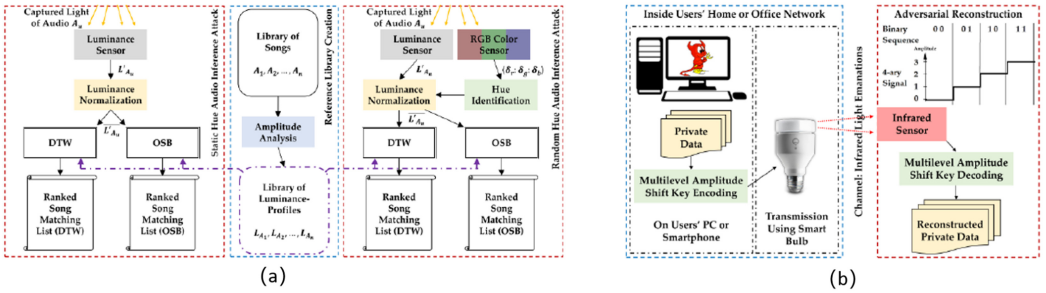

Fig. 9. (a) Audio/video inference attack framework; (b) Smart light-based covert-channel attack [89].

7.1.2 SniffingVLC [35]. As we introduced before, the optical signals in OWC could not propagate through blockages such as walls due to their extremely high frequency. This feature makes OWC more secure than RF-based wireless communication in indoor environment, because attackers have much difficulties to sniff data via optical channels. However, as investigated in Reference [35], even when the attackers are blocked with non-transparent walls, they can still steal the transmitted data from the indoor transmitter. The reason is that when the transmitter emits visible light, it also leaks "side channel signals" that can be captured by eavesdropper outside.

In OWC, intensity-based modulations are usually adopted, such as On-Off Keying modulation, in which On status denotes bit "1" and Off status denotes bit "0." The On/Off switching of the light source causes the change of current flow in the power line of the transmitter. This changing current at the transmitter could cause the a variable magnetic field in the air and this changing magnetic field can induce an electromotive force at the attackers' receiver. The authors in the paper conducted comprehensive field experiments with commercial devices. The results show that with the copper coil as the receiver, authors can simultaneously sniff multiple VLC transmissions even at 6.4 meters with one wall between transmitter and their sniffing devices.

7.2 Camera-related Privacy Leakage

7.2.1 LiShield [168]. Cameras are pervasive in today's consumer mobile devices such as tablet, smartphone, portable cameras, drones, smart glasses, and so on [158, 168]. These ubiquitous devices paired with pervasive wireless access increase the risk of the leakage of humans' privacy and sensitive object via maliciously capturing images or videos. Due to the easy process of photo-sharing applications such as Wechat, Facebook, Instagram, Twitter, there are bunch of photos/videos are and uploaded online with a simple one-time permission from the users. Privacy-sensitive scenes often occur in the enclosed indoor environment (e.g., theaters, hospitals, bathrooms, government office, dressing rooms). In LiShield, the attack goal is to passively take a photo of the private scene using a rolling shutter camera. They did the experiment based on multiple scenes such as the document, human face, glass, keys, and paint. The experimental setup is shown in the left of Figure 10.

7.2.2 mQR Code [106]. In mQR Code, the attacker wants to take a photo of the QR code shown on the victim's smartphone screen. Then, the attacker will present this snap QR code to the retail system for payment. The attacks mentioned in both papers (LiShield and mQR Code) are direct and do not infer private data from visible light. They can also be treated as side-channel attacks, because attackers steal private data in a passive way by capturing photos. The attack models in mQR code [106] are the forms of Replay attacks and **Synchronized Token Lifting and Spending**

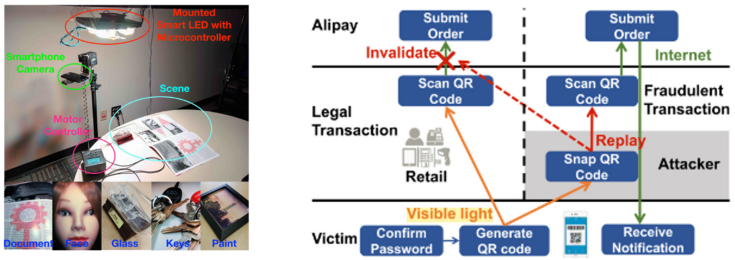

Fig. 10. Attacks in LiShield and QR-code based STLS attack process [106].

(STLS) attacks. The attacker secretly obtained the QR code from the victim's screen via the optical channel, especially visible light channels. The attack model is shown in the right of Figure 10.

7.3 Novel Protections

Covert-channel always requires additional software agents installed at the victim's device. It increases the difficulty of attack. As mentioned above, the side channel is the most popular attack modality, mainly for smartphone-based optical wireless communication such as screen-camera communication. We next introduce two novel privacy protection techniques: LiShield and mQR Code. These two secure solutions are both to interfere and obstruct the side-channels to prevent capturing images by cameras (especially cameras on smartphones).

7.3.1 LiShield [168]. The adversary model here is that the attacker wanted to take photos or videos of privacy-sensitive scenes that have only the consumer smartphones with rolling shutter cameras. (S)he can fully control the parameters of the camera, such as exposure times, rolling shutter sample rate, ISO setting, and so on. LiShield provides a similar illumination of standard and non-flicker office lighting. Due to the attackers not knowing the parameters of LiShield, the captured image will have blank strips or be overexposed, which causes distorted color. The distorted photographs prevent the disclosure of private information. However, the authorized user knows the LiShield parameters. Therefore, the authorized user can set the camera parameters to match the LiShield parameters to recover the clear picture or video without any strips or distortion.

However, there are some challenges here for LiShield: (1) if the attacker guesses the LiShield parameters by brute-force search, then the protection of LiShield will be invalid; (2) if the ambient light gets strong enough, then the On/Off of LiShield has no difference to attacker, since the brightness of the scene is dominated by the ambient light; (3) if the scene is static, then the attacker can record a video containing multiple frames to get rid of the strip effect, and so on. To address these problems, the author did preexperiments and had some observations: (1) there should be more than a single frequency for LiShield to ensure the robust protection; (2) LiShield should use a specific range of parameters to maximize the image quality degradation such as moderate duty cycle, high peak intensity, and long exposure time. Based on the observation and analysis, LiShield uses some countermeasures to these potential attacks, such as using frequency scrambling and illumination intensity randomization to combat the brute-force search, using barcode embedding to combat the online-delivery of the private image in the strong ambient light scene.

As for authorized users, LiShield should guarantee the good recovery of image whatever the static or dynamic scenes. To confirm the effectiveness of LiShield for disrupting the attacker and allowing the authorized users, LiShield designs barcode with multiple frequencies in each photo as well. The goal of the barcode is to encode the ratio of different frequencies. The ratio could be the digital information such as "no delivery" for images captured by attackers and "sharing

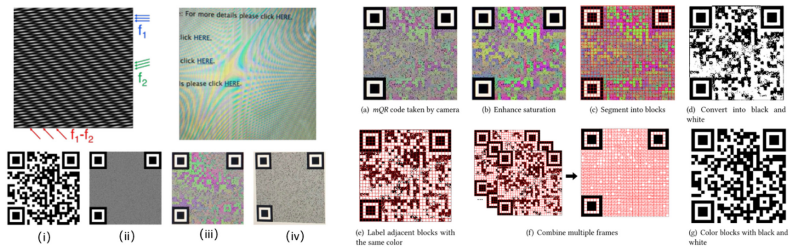

Fig. 11. mQR Code encrypt original QR code by exploiting nonlinearity of spatial frequency [106].

allowed" for images captured by authorized users. The barcode type depends on the light-medium of LiShield. It can be a monochrome barcode or an RGB barcode. LiShield adopts the multiple frequency pairs to improve the robustness and redundancy of the embedded barcode. The experiments show that using smart-LEDs and specific waveform successfully stops the privacy leakage in the indoor environment. The author implements and verifies the robustness and effectiveness of the LiShield system. Based on the analysis above, LiShield is one of the security solutions to combat the side-channel attacks, which prevents the capturing of private images in the LoS range of the victims.

7.3.2 mQR Code [106]. In the area of mathematics, physics, and engineering, the spatial frequency is characteristic of any structure that is periodic in space. The spatial frequency is a quantity that describes the frequency of the sinusoidal component of the unit length determined by the Fourier transform. The SI unit of spatial frequency is the number of cycles per meter. The authors of mQR Code use the **bi-dimensional (2D)** spatial structure, including a curvilinear pattern. It can be described in frequency and phase terms as follows:

$$m(x, y) = p(\phi(x, y)), \tag{1}$$

where $m(x, y)$ denotes the magnitude level at the location in 2D coordinate space, p is the periodic function of the frequency of the pattern, and $\phi(x, y)$ is the phase function denoting the angle of the pattern. There will be an additional visible layer (moiré pattern) generated when two optical spatial patterns overlap due to the nonlinear interaction of two patterns over the original image.

In mQR Code [106], the author developed a novel QR code, mQR Code, to combat the attacks in QR code-based screen camera communication. They explore the spatial frequency and exploit the nonlinearity of spatial frequency as the camouflage pattern of QR code. When the relative position of the screen containing QR code and the cashier scanner fits the designated relative position, including angle and distance, the cashier scanner can obtain the real QR code. It means the attacker can only get the camouflaged QR code image unless the pinhole camera is installed at the same place as the cashier scanner.

When we use cameras to take a picture of the spatial patterns, there will be a significant nonlinear effect on the display. Thus, the additional moire layer has repetitive curving lines that disrupt the captured image quality, as shown in the left of Figure 11. This prevents the QR code captured by the attacker. At the bottom left of Figure 11 are four pictures: (i) shows the original QR code, (ii) and (iii) are pictures taken at the wrong position, while (iv) is taken at the designated position, which can be used to recover the original QR code for users.

7.4 Other Directions for OWC Countermeasures

Wireless communication in our daily life is often protected against unauthorized wireless channel access, message modification, eavesdropping, and replay attacks. Authentication security services

verify an entity's identity and grant access to the wireless medium. Confidentiality services ensure that the contents of messages are understood only by the devices involved. Data integrity services ensure that data is not altered while in transit. Thus, VLC can be secured using three well-known security mechanisms: proximity-based protecting, steganographic protecting, and cryptographic protection [119]. These technologies provide security in fundamentally different ways: the choice of these solutions for a real-world deployment is dictated by the application's security requirements. Based on the analysis above, we list other OWC countermeasures below.

Create Secure Zone. Due to the LoS propagation of light medium and its broadcast nature, it is intuitively to protect optical signals within the limited space zones. The protected zone is defined by its center and the position of the **access point (AP)**, as well as a security radius, which is the minimum horizontal distance from the AP location to any potential eavesdroppers, and it employs motion sensors, which are already embedded into modern lighting equipment [123]. In Reference [69], the authors built an eavesdropper-free protected zone around APs to significantly enhance the secrecy performance of legitimate users. Similarly, the authors in Reference [81] conducted a security zone in the room with their proposed PLS approach based on beamforming for secure OWC.

Utilizing Hybrid Network Techniques. The link reliability is undoubtedly increased when there are two or more networks. In two-tier networks, which are created by VLC/WiFi, VLC/small cell, LiFi/WiFi, LiFi/small cell, VLC/macrocell, and LiFi/macrocell hybrid systems, transmitters and receivers are reliably connected. Optical wireless networks are very sensitive to obstacles. Consequently, the information cannot be hacked outside of the room. Therefore, all hybrid VLC/WiFi, VLC/small cell, LiFi/WiFi, LiFi/small cell, VLC/macrocell, RF/OCC, RF/OCC, and LiFi/macrocell systems improve the security level.

Channel-hopping Mechanism. A potent technique for maintaining the confidentiality of communications between a transmitter and receiver is channel hopping. By alternating the channel utilized by the transmitter and receiver on a regular basis, eavesdroppers will be unable to decode signals, since they will not know which channel is being used. One method to channel hop is use of a BFSK modulation scheme to randomly randomly hop channels. Although collisions with other light sources are still possible, the random hopping typically prevents them [62]. A similar idea is to use time-synchronized channel hopping to create a schedule that dictates which light sources use which channel during time slots. This ensures fairness between light sources and ensures that few channel collisions happen [135].

Authentication and Encryption. Authentication is traditionally done through feature-based detection. The receiver looks at the sender's channel gain to determine a fingerprint and discern whether that sender is valid or invalid. A recent innovation in authentication has been to use a training phase, where a receiver will learn about a valid sender, and a testing phase, where the sender will compare all transmissions to that valid sender [63]. Transmissions can easily be encrypted with a Caesar cipher system. This system converts text into a cipher using a cyclical array and a direct mapping of one letter to another. Although the text modification can be undone by the receiver, an attacker would be unable to undo the cipher without the right knowledge, protecting the data [4].

Proximity-based Protection. Proximity-based protection is likely OWC's strongest and most unique ability. Whereas RF waves can propagate through any medium, light waves are trapped within their environment; meaning, OWC communications are largely private within a single room or car, as they rely on line-of-sight to be received [119]. This makes it difficult for any eavesdropper to listen in, as they must physically be in the room with any transmitters. This is especially powerful compared to RF signals, which can be picked up from a wide radius around the transmitter, regardless of walls. Of course, it is not impossible for them to listen in. An attacker could view light from a variety of openings, such as windows, openings below doors, key holes,

and more, thus it is essential for any OWC system to keep secure areas enclosed to prevent these eavesdroppers [33].

Steganographic Protection. Steganography is the idea of hiding secret messages within another message. These hidden messages cannot be read by an eavesdropper unless the eavesdropper knows how to find and decode them, ensuring confidentiality [119]. One method of hiding these messages within OWC is through LuxSteg, which mixes steganographic messages with orthogonal codes and adds them to an overt signal modulated in a pulse position modulation scheme to create hidden messages [16]. A similar idea can be found in LiShield, which can hide barcodes within images that are invisible to the human eye. To assess whether an image can be posted or not, online systems can pick up these barcodes and read them [168].

Cryptographic Protection and Key Generation. Modern OWC systems employ cryptography at all layers of communication and rely on secret keys to encrypt communication [119]. Traditional OWC systems make use of symmetric keys that are made in the upper layers of the OSI through various methods [14]. One key generation and distribution method can be found in quantum cryptography. Through a quantum channel, a joint secret key can be established between two individuals and used for communication. Quantum channels can deter eavesdroppers through the use of protons. To measure a quantum channel, a proton must be measured and destroyed, making it impossible for eavesdroppers to listen, as the receiver will notice the missing proton. From this point, the parties can use quantum cryptography to keep the rest of their conversation secret [125].

Chaffing and Winnowing. Chaffing and winnowing is a unique way to ensure authenticity and integrity with shared keys but without encryption/decryption [119]. This process has two important steps: chaffing, the act of adding fake packets with fake MACs to a transmission, and winnowing, the act of removing packets with fake MACs [118]. Since the system makes use of shared keys, attackers cannot determine which packets are fake without the keys. Together, this sytem adds fake packets to confuse potential eavesdroppers, while the valid receiver knows which packets are faked due to the incorrect MACs. Chaffing and winnowing currently has a small presence in OWC and has great potential to grow in this topic.

8 OPEN ISSUES AND FUTURE DIRECTIONS

8.1 Applications: Optical-based V2X Networks

Among the numerical OWC-enabled applications, the optical based vehicle-to-everything networks are the most promising application in the near future. These systems have strict constraints for latency, collision avoidance, throughput, and reliability. To make the optical-based V2X into reality, there are some open issues and challenges that need to be addressed: (1) Current OWC V2X systems necessitate precise beam alignment and have a limited field of view, making them unsuitable for real-world vehicle scenarios in space; (2) Because of the bottleneck at camera-based receivers with rolling shutter frequency limitations, the broad light spectrum bandwidth is not completely utilized for high data rate; (3) Although OWC approaches are more energy-efficient than RF-based methods, directional resource allocation with adaptive communication ranges for many users at the transmitter side is critical and non-trivial for energy savings and green communication when multiple cars are involved; (4) Vehicle location and positioning are vital in a high-mobility environment for dynamic decentralized collaboration in vehicular network services such as critical information sharing and relaying.

For V2X networks, the future research directions about security can be foreseen as follows: (1) multi-to-multi access services and authentication; (2) jamming attacks from malicious light source in the same optical environment; (3) RF side-channel data leakage due to the ON/OFF switching at the transmitter side; (4) spoofing attacks by rogue vehicles for incorrect information sharing,

resulting in a deadly accident and injuries. In a nutshell, secure OWC approaches will pave the way for a bright future for V2X networks.

8.2 Attacks: Optical Code/Tag-related Attacks

Optical codes, such as one-dimensional bar codes, two-dimensional QR codes, and various varieties, are the most common and widely used in our everyday life, including mobile payment, e-health certificate, personal identification, access control, augmented reality, navigation, advertising, and so on [106, 131]. The majority of these optical codes are attached to the surface of products or shown on commercial screens such as smartphone and payment machine screens.

Despite the LoS propagation of these optical codes from transmitter to receiver, its nature broadcast characteristic allows attackers in the same physical optical environment to attack. There are still many open issues for optical codes with broader market and application scenarios: (1) optical code-related phishing, such as try to "fish" sensitive information from the victim [153]; (2) invisible optical code hijacking, in which a target victim optical code is illuminated with a specialized waveform that humans cannot perceive, but which destroys the decoding at camera [166]; (3) optical code manipulation attack, which is mentioned in barcode-in-barcode attack [36]; (4) optical code replacement attack, in which attackers print a new optical code with an included malicious link, such as the payment code on the salesperson side in Alipay/WechatPay, which has been reported many times in China; (5) modification attack of individual modules in optical code, which means the encoded content is modified solely by changing the color of specific modules of the optical codes reported in Reference [73].

8.3 Protocols: Security Risks in MAC Layer of OWC

The IEEE standard now covers a substantial portion of MAC security. The MAC layer focuses on security through cryptography while attempting not to bog down the rest of the system with high resources usage. It uses an AES counter block cipher to encrypt messages and uses an optional frame counter to attempt to discourage replay attacks [17]. This creates a strong baseline for MAC layer security for OWC, but it still has several weaknesses: (1) the IEEE standard only uses cryptographic encryption means to protect data, when there are many other options that could enhance security; (2) users can disable items like the frame counter, which would allow an uninformed user to severely lower security; (3) the MAC layer has no methods to detect and remove noise from malicious transmitters sending jamming signals; (4) MAC layer presently has no default support for asymmetric keys, which can be invaluable for wireless communication.

In the future, many solutions could be considered to enhance MAC security: (1) Steganographic messages, winnowing, and chaffing could be added as an optional feature to the IEEE standard to enhance security; (2) Research could be done in the area for having the MAC layer alternate between keys to keep attacks from attempting cryptographic attacks to solve keys; (3) Research could be done in having the MAC layer convert texting using a basic cipher before encryption to add an extra layer of security. While the current MAC layer is quite strong in the IEEE standard, there is great potential to become better and cover up its several weaknesses.

8.4 Techniques: AI-based OWC Networks

In several computer-related fields, **artificial intelligence (AI)** is a rapidly evolving field. It is undeniable that AI can boost OWC communications, but this potential has obviously largely gone untapped. Furthermore, there are a number of problems with using AI: (1) As AI is developed to make the transmitted optical signals clearer and easier to receive, it will also make it easier for eavesdroppers to access signals they should not; (2) AI frequently requires a significant amount of time to train, in which case the system must be solely dedicated to training that AI; (3) AI systems

could be very taxing on a communication system that does not really need them, making the cost not worth the benefit.

Despite the issues, however, there are myriad places AI could go: (1) AI detection could help clear up signals with a lot of noise; (2) AI could help a valid receiver determine where exactly a malicious transmitter could be; (3) AI could potentially read signals and determine jamming patterns to help the receiver detect and ignore malicious jammers; (4) AI could also help channel-hopping systems determine how to hop channels in a superior order while ensuring the fewest possible collisions; (5) It could be possible to do research to see whether an AI receiver could scan a space to look for obvious openings where light might escape and allow listeners in. In the OWC universe, AI appears to have untapped potential and has the ability to revolutionize OWC security.

9 CONCLUSION

In this article, we analyze the intrinsic security property of optical signals and the security risks in the OWC networks. Then, we creatively classify the security vulnerabilities and attacks in OWC networks in three stages: **before signal propagation (BSE), during signal propagation (DSP)**, and **after signal receiving (ASR)**. For each stage, we also discuss its related applications, countermeasures, and secure protocols. Furthermore, we present several novel attacks and secure solutions in OWC network covering these three stages. Then, we identified the future directions in secure solutions of optical wireless communication. Because of the rapid growth of OWC and its tremendous potential, more attention and effort are required in the field of OWC security and privacy. We believe that our survey would stimulate further investigation into OWC security.

REFERENCES

[1] 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.

[2] Ahmed H. Abd El-Malek, Anas M. Salhab, Salam A. Zummo, and Mohamed-Slim Alouini. 2016. Security-reliability trade-off analysis for multiuser SIMO mixed RF/FSO relay networks with opportunistic user scheduling. *IEEE Trans. Wirel. Commun.* 15, 9 (2016), 5904–5918.

[3] Ahmed H. Abd El-Malek, Anas M. Salhab, Salam A. Zummo, and Mohamed-Slim Alouini. 2017. Physical layer security enhancement in multiuser mixed RF/FSO relay networks under RF interference. In *IEEE Wireless Communications and Networking Conference (WCNC)*. IEEE, 1–6.

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

[5] Trio Adiono, Syifaul Fuada, Muhamad Luthfi, and Rosmianto Aji Saputro. 2017. MAC layer design for network-enabled visible light communication systems compliant with IEEE 802.15. 7. *EAI Endors. Trans. Energy Web* 4, 14 (2017).

[6] Yun Ai, Aashish Mathur, Michael Cheffena, Manav R. Bhatnagar, and Hongjiang Lei. 2019. Physical layer security of hybrid satellite-FSO cooperative systems. *IEEE Photon. J.* 11, 1 (2019), 1–14.

[7] Yun Ai, Aashish Mathur, Gyan Deep Verma, Long Kong, and Michael Cheffena. 2020. Comprehensive physical layer security analysis of FSO communications over Málaga channels. *IEEE Photon. J.* 12, 6 (2020), 1–17.

[8] Yahya M. Al-Moliki, Mohammed T. Alresheedi, and Yahya Al-Harthi. 2020. Improving availability and confidentiality via hyperchaotic baseband frequency hopping based on optical OFDM in VLC networks. *IEEE Access* 8 (2020).

[9] Mohammed S. Al-Zahrani, Heider A. M. Wahsheh, and Fawaz W. Alsaade. 2021. Secure real-time artificial intelligence system against malicious QR code links. *Secur. Commun. Netw.* 2021 (2021), 1–11.

[10] Jinyoung An and Wan-Young Chung. 2016. A novel indoor healthcare with time hopping-based visible light communication. In *IEEE 3rd World Forum on Internet of Things (WF-IoT)*. IEEE, 19–23.

[11] 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.

[12] Raed M. Bani-Hani, Yarub A. Wahsheh, and Mohammad B. Al-Sarhan. 2014. Secure QR code system. In *10th International Conference on Innovations in Information Technology (IIT)*. IEEE, 1–6.

[13] Rui Bian, Iman Tavakkolnia, and Harald Haas. 2019. 15.73 Gb/s visible light communication with off-the-shelf LEDs. *J. Lightw. Technol.* 37, 10 (2019), 2418–2424.
[14] Grzegorz Blinowski. 2015. Security issues in visible light communication systems. *IFAC-PapersOnLine* 48, 4 (2015).
[15] Grzegorz Blinowski. 2019. Security of visible light communication systems-a survey. *Phys. Commun.* 34 (2019), 246–260.
[16] Grzegorz Blinowski, Piotr Januszewski, Grzegorz Stepniak, and Krzysztof Szczypiorski. 2018. LuxSteg: First practical implementation of steganography in VLC. *IEEE Access* 6 (2018), 74366–74375.
[17] Grzegorz J. Blinowski. 2016. Practical aspects of physical and MAC layer security in visible light communication systems. *Int. J. Electron. Telecommun.* 62, 1 (2016), 7–13.
[18] Grzegorz J. Blinowski. 2017. The feasibility of launching rogue transmitter attacks in indoor visible light communication networks. *Wirel. Person. Commun.* 97, 4 (2017), 5325–5343.
[19] 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.
[20] Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z Morley Mao. 2019. Adversarial sensor attack on LiDAR-based perception in autonomous driving. In *ACM SIGSAC Conference on Computer and Communications Security*. 2267–2281.
[21] Zhen Che, Junbin Fang, Zoe Lin Jiang, Jin Li, Shancheng Zhao, Yongchun Zhong, and Zhe Chen. 2018. A physical-layer secure coding scheme for indoor visible light communication based on polar codes. *IEEE Photon. J.* 10, 5 (2018), 1–13.
[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.
[23] 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.
[24] Zhe Chen and Xin Wang. 2018. A method for improving physical layer security in visible light communication networks. In *IEEE Conference on Standards for Communications and Networking (CSCN)*. IEEE, 1–5.
[25] Nan Chi, Yingjun Zhou, Yiran Wei, and Fangchen Hu. 2020. Visible light communication in 6G: Advances, challenges, and prospects. *IEEE Vehic. Technol. Mag.* 15, 4 (2020), 93–102.
[26] 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.
[27] 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.
[28] 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.
[29] 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.
[30] Mostafa Zaman Chowdhury, Moh Khalid Hasan, Md Shahjalal, Md Tanvir Hossan, and Yeong Min Jang. 2020. Optical wireless hybrid networks: Trends, opportunities, challenges, and research directions. *IEEE Commun. Surv. Tutor.* 22, 2 (2020), 930–966.
[31] 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.
[32] Mostafa Zaman Chowdhury, Md Shahjalal, Moh Hasan, Yeong Min Jang et al. 2019. The role of optical wireless communication technologies in 5G/6G and IoT solutions: Prospects, directions, and challenges. *Appl. Sci.* 9, 20 (2019), 4367.
[33] 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 International Workshop on Visible Light Communications Systems*. 9–14.
[34] Jiska Classen, Daniel Steinmetzer, and Matthias Hollick. 2016. Opportunities and pitfalls in securing visible light communication on the physical layer. In *3rd Workshop on Visible Light Communication Systems*. 19–24.
[35] 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.
[36] Adrian Dabrowski, Katharina Krombholz, Johanna Ullrich, and Edgar R. Weippl. 2014. QR inception: Barcode-in-barcode attacks. In *4th ACM Workshop on Security and Privacy in Smartphones & Mobile Devices*. 3–10.

[37] Adrian Dabrowski, Edgar R. Weippl, and Isao Echizen. 2013. Framework based on privacy policy hiding for preventing unauthorized face image processing. In *IEEE International Conference on Systems, Man, and Cybernetics*. IEEE, 455–461.

[38] Linglong Dai, Bichai Wang, Zhiguo Ding, Zhaocheng Wang, Sheng Chen, and Lajos Hanzo. 2018. A survey of non-orthogonal multiple access for 5G. *IEEE Commun. Surv. Tutor.* 20, 3 (2018), 2294–2323.

[39] Svilen Dimitrov and Harald Haas. 2015. *Principles of LED Light Communications: Towards Networked Li-Fi*. Cambridge University Press.

[40] Zhiguo Ding, Xianfu Lei, George K. Karagiannidis, Robert Schober, Jinhong Yuan, and Vijay K. Bhargava. 2017. A survey on non-orthogonal multiple access for 5G networks: Research challenges and future trends. *IEEE J. Select. Areas Commun.* 35, 10 (2017), 2181–2195.

[41] Zhi-guo Ding, Mai Xu, Yan Chen, Mu-gen Peng, and H. Vincent Poor. 2018. Embracing non-orthogonalmultiple access in future wireless networks. *Front. Inf. Technol. Electron. Eng.* 19, 3 (2018), 322–339.

[42] Lun Dong, Zhu Han, Athina P. Petropulu, and H. Vincent Poor. 2009. Improving wireless physical layer security via cooperating relays. *IEEE Trans. Sig. Process.* 58, 3 (2009), 1875–1888.

[43] Meiya Dong, Jumin Zhao, Dengao Li, Biaokai Zhu, and Zhaobin Liu. 2018. CLOAK: visible touching and invisible protecting: Cloud privacy protection based on LSB and chaotic approach. In *6th International Conference on Advanced Cloud and Big Data (CBD)*. IEEE, 225–229.

[44] Wan Du, Jansen Christian Liando, and Mo Li. 2016. SoftLight: Adaptive visible light communication over screen-camera links. In *35th Annual IEEE International Conference on Computer Communications*. IEEE, 1–9.

[45] Monica Figueiredo, Luis Nero Alves, and Carlos Ribeiro. 2017. Lighting the wireless world: The promise and challenges of visible light communication. *IEEE Consum. Electron. Mag.* 6, 4 (2017), 28–37.

[46] Zabih Ghassemlooy, Shlomi Arnon, Murat Uysal, Zhengyuan Xu, and Julian Cheng. 2015. Emerging optical wireless communications-advances and challenges. *IEEE J. Select. Areas Commun.* 33, 9 (2015), 1738–1749.

[47] Zabih Ghassemlooy, Pengfei Luo, and Stanislav Zvanovec. 2016. Optical camera communications. In *Optical Wireless 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.

[49] 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.

[50] Mordechai Guri, Ofer Hasson, Gabi Kedma, and Yuval Elovici. 2016. An optical covert-channel to leak data through an air-gap. In *14th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 642–649.

[51] Mordechai Guri, Matan Monitz, Yisroel Mirski, and Yuval Elovici. 2015. BitWhisper: Covert signaling channel between air-gapped computers using thermal manipulations. In *IEEE 28th Computer Security Foundations Symposium*. IEEE, 276–289.

[52] Mordechai Guri, Boris Zadov, Dima Bykhovsky, and Yuval Elovici. 2019. CTRL-ALT-LED: Leaking data from air-gapped computers via keyboard LEDs. In *IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 1. IEEE, 801–810.

[53] Mordechai Guri, Boris Zadov, Andrey Daidakulov, and Yuval Elovici. 2018. xLED: Covert data exfiltration from air-gapped networks via switch and router LEDs. In *16th Annual Conference on Privacy, Security and Trust (PST)*. IEEE, 1–12.

[54] Harald Haas, Liang Yin, Yunlu Wang, and Cheng Chen. 2016. What is LiFi? *J. Lightw. Technol.* 34, 6 (2016), 1533–1544.

[55] M. A. Hadi. 2016. Wireless communication tends to smart technology Li-Fi and its comparison with Wi-Fi. *Amer. J. Eng. Res.* 5, 5 (2016), 40–47.

[56] Tzipora Halevi and Nitesh Saxena. 2012. A closer look at keyboard acoustic emanations: Random passwords, typing styles and decoding techniques. In *7th ACM Symposium on Information, Computer and Communications Security*. 89–90.

[57] Lajos Hanzo, Harald Haas, Sándor Imre, Dominic O'Brien, Markus Rupp, and Laszlo Gyongyosi. 2012. Wireless myths, realities, and futures: from 3G/4G to optical and quantum wireless. *Proc. IEEE* 100, Special Centennial Issue (2012), 1853–1888.

[58] Shinichiro Haruyama. 2020. Location-based services using visible light communication. In *Proceedings of SPIE-The International Society for Optical Engineering*, Vol. 11520. SPIE, 1152001–100.

[59] Osama Hassan, Erdal Panayirci, H. Vincent Poor, and Harald Haas. 2018. Physical-layer security for indoor visible light communications with space shift keying modulation. In *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6.

[60] Xiang He and Aylin Yener. 2009. Two-hop secure communication using an untrusted relay. *EURASIP J. Wirel. Commun. Netw.* 2009 (2009), 1–13.

[61] Wen-xin Hong, Jiong-qian Wang, and Wei-ze Li. 2019. CSK hopping pattern model for visible light communication networks. *Optic. Quant. Electron.* 51, 4 (2019), 1–17.
[62] Pan Hu, Liqun Li, Chunyi Peng, Guobin Shen, and Feng Zhao. 2013. Pharos: Enable physical analytics through visible light based indoor localization. In *12th ACM Workshop on Hot Topics in Networks*. 1–7.
[63] 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.
[64] Panagiotis Ilia, Iasonas Polakis, Elias Athanasopoulos, Federico Maggi, and Sotiris Ioannidis. 2015. Face/off: Preventing privacy leakage from photos in social networks. In *22nd ACM SIGSAC Conference on Computer and Communications Security*. 781–792.
[65] Susumu Ishihara, Reuben Vincent Rabsatt, and Mario Gerla. 2015. Improving reliability of platooning control messages using radio and visible light hybrid communication. In *IEEE Vehicular Networking Conference (VNC)*. IEEE, 96–103.
[66] Jeyadeepan Jeganathan, Ali Ghrayeb, Leszek Szczecinski, and Andres Ceron. 2009. Space shift keying modulation for MIMO channels. *IEEE Trans. Wirel. Commun.* 8, 7 (2009), 3692–3703.
[67] Dzevdan Kapetanovic, Gan Zheng, and Fredrik Rusek. 2015. Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks. *IEEE Commun. Mag.* 53, 6 (2015), 21–27.
[68] Latif Ullah Khan. 2017. Visible light communication: Applications, architecture, standardization and research challenges. *Digit. Commun. Netw.* 3, 2 (2017), 78–88.
[69] Ashish Khisti and Gregory W. Wornell. 2010. Secure transmission with multiple antennas–Part II: The MIMOME wiretap channel. *IEEE Trans. Inf. Theor.* 56, 11 (2010), 5515–5532.
[70] Sung-Man Kim. 2018. Visible light communication employing optical beamforming: A review. *Curr. Optics Photon.* 2, 4 (2018), 308–314.
[71] Sung-Man Kim and Seong-Min Kim. 2013. Performance improvement of visible light communications using optical beamforming. In *5th International Conference on Ubiquitous and Future Networks (ICUFN)*. IEEE, 362–365.
[72] 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.
[73] Katharina Krombholz, Peter Frühwirt, Peter Kieseberg, Ioannis Kapsalis, Markus Huber, and Edgar Weippl. 2014. QR code security: A survey of attacks and challenges for usable security. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 79–90.
[74] Markus Guenther Kuhn. 2002. *Compromising Emanations: Eavesdropping Risks of Computer Displays*. Ph.D. Dissertation. Citeseer, University of Cambridge, Computer Laboratory.
[75] Markus G. Kuhn and Ross J. Anderson. 1998. Soft tempest: Hidden data transmission using electromagnetic emanations. In *International Workshop on Information Hiding*. Springer, 124–142.
[76] Yong Up Lee. 2020. Secure visible light communication technique based on asymmetric data encryption for 6G communication service. *Electronics* 9, 11 (2020), 1847.
[77] Hongwei Li, Fasong Wang, Jiankang Zhang, and Chaowen Liu. 2018. Secrecy performance analysis of MISO visible light communication systems with spatial modulation. *Digit. Sig. Process.* 81 (2018), 116–128.
[78] Jiangyuan Li, Athina P. Petropulu, and Steven Weber. 2011. On cooperative relaying schemes for wireless physical layer security. *IEEE Trans. Sig. Process.* 59, 10 (2011), 4985–4997.
[79] Tianxing Li, Chuankai An, Zhao Tian, Andrew T. Campbell, and Xia Zhou. 2015. Human sensing using visible light communication. In *21st Annual International Conference on Mobile Computing and Networking*. 331–344.
[80] You Li and Javier Ibanez-Guzman. 2020. Lidar for autonomous driving: The principles, challenges, and trends for automotive LiDAR and perception systems. *IEEE Sig. Process. Mag.* 37, 4 (2020), 50–61.
[81] Shuang Liang, Zhiyi Fang, Geng Sun, and Jin Zhang. 2020. A physical layer security approach based on optical beamforming for indoor visible light communication. *IEEE Commun. Lett.* 24, 10 (2020), 2109–2113.
[82] Chi Lin, Yongda Yu, Jie Xiong, Yichuan Zhang, Lei Wang, Guowei Wu, and Zhongxuan Luo. 2021. Shrimp: A robust underwater visible light communication system. In *27th Annual International Conference on Mobile Computing and Networking*. 134–146.
[83] Xiaodong Liu, Yuhao Wang, Fuhui Zhou, Shuai Ma, Rose Qingyang Hu, and Derrick Wing Kwan Ng. 2020. Beamforming design for secure MISO visible light communication networks with SLIPT. *IEEE Trans. Commun.* 68, 12 (2020), 7795–7809.
[84] Xiangyu Liu, Xuetao Wei, Lei Guo, Yejun Liu, and Yufang Zhou. 2016. A new eavesdropping-resilient framework for indoor visible light communication. In *IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–6.
[85] Huaiyin Lu, Lin Zhang, and Xingcheng Liu. 2016. High-security colour shift keying modulation scheme with chaos-based constellation rotation for VLC system. In *10th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*. IEEE, 20–24.

[86] Hai-Han Lu, Chung-Yi Li, Hwan-Wei Chen, Chun-Ming Ho, Ming-Te Cheng, Zih-Yi Yang, and Chang-Kai Lu. 2016. A 56 Gb/s PAM4 VCSEL-based LiFi transmission with two-stage injection-locked technique. *IEEE Photon. J.* 9, 1 (2016), 1–8.

[87] Junhai Luo, Liying Fan, and Husheng Li. 2017. Indoor positioning systems based on visible light communication: State of the art. *IEEE Commun. Surv. Tutor.* 19, 4 (2017), 2871–2893.

[88] Shang Ma, Qiong Liu, and Phillip C.-Y. Sheu. 2017. FogLight: Visible light-enabled indoor localization system for low-power IoT devices. *IEEE Internet Things J.* 5, 1 (2017), 175–185.

[89] 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.

[90] Ignacio Marin-Garcia, Victor Guerra, and Rafael Perez-Jimenez. 2017. Study and validation of eavesdropping scenarios over a visible light communication channel. *Sensors* 17, 11 (2017), 2687.

[91] Hanaa Marshoud, Sami Muhaidat, Paschalis C. Sofotasios, Sajjad Hussain, Muhammad Ali Imran, and Bayan S. Sharif. 2018. Optical non-orthogonal multiple access for visible light communication. *IEEE Wirel. Commun.* 25, 2 (2018), 82–88.

[92] Luiz Eduardo Mendes Matheus, Alex Borges Vieira, Luiz F. M. Vieira, Marcos A. M. Vieira, and Omprakash Gnawali. 2019. Visible light communication: Concepts, applications and challenges. *IEEE Commun. Surv. Tutor.* 21, 4 (2019), 3204–3237.

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

[94] Agon Memedi, Christoph Sommer, and Falko Dressler. 2018. On the need for coordinated access control for vehicular visible light communication. In *14th Annual Conference on Wireless On-demand Network Systems and Services (WONS)*. IEEE, 121–124.

[95] Raed Mesleh, Hany Elgala, and Harald Haas. 2011. Optical spatial modulation. *J. Optic. Commun. Netw.* 3, 3 (2011), 234–244.

[96] Raed Y. Mesleh, Harald Haas, Sinan Sinanovic, Chang Wook Ahn, and Sangboh Yun. 2008. Spatial modulation. *IEEE Trans. Vehic. Technol.* 57, 4 (2008), 2228–2241.

[97] Syed Agha Hassnain Mohsan and Hussain Amjad. 2021. A comprehensive survey on hybrid wireless networks: Practical considerations, challenges, applications and research directions. *Optic. Quant. Electron.* 53, 9 (2021), 1–56.

[98] Ayman Mostafa. 2017. *Physical-layer Security for Visible-light Communication Systems*. Ph. D. Dissertation. University of British Columbia.

[99] Ayman Mostafa and Lutz Lampe. 2014. Securing visible light communications via friendly jamming. In *IEEE Globecom Workshops (GC Wkshps)*. IEEE, 524–529.

[100] Ayman Mostafa and Lutz Lampe. 2016. Optimal and robust beamforming for secure transmission in MISO visible-light communication links. *IEEE Trans. Sig. Process.* 64, 24 (2016), 6501–6516.

[101] Farag Ibrahim Khalifa Mousa, Noor Al Maadeed, Krishna Busawon, Ahmed Bouridane, and Richard Binns. 2017. Secure mimo visible light communication system based on user's location and encryption. *J. Lightw. Technol.* 35, 24 (2017), 5324–5334.

[102] Amitav Mukherjee, S. Ali A. Fakoorian, Jing Huang, and A. Lee Swindlehurst. 2014. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Commun. Surv. Tutor.* 16, 3 (2014), 1550–1573.

[103] Ben Nassi, Yaron Pirutin, Tomer Galor, Yuval Elovici, and Boris Zadov. 2021. Glowworm attack: Optical TEMPEST sound recovery via a device's power indicator LED. In *ACM SIGSAC Conference on Computer and Communications Security*. 1900–1914.

[104] Mohanad Obeed and Wessam Mesbah. 2019. Efficient algorithms for physical layer security in one-way relay systems. *Wirel. Netw.* 25, 3 (2019), 1327–1339.

[105] Frédérique Oggier and Babak Hassibi. 2011. The secrecy capacity of the MIMO wiretap channel. *IEEE Trans. Inf. Theor.* 57, 8 (2011), 4961–4972.

[106] 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.

[107] Hyeongmin Park, Taeeun Kim, Gaeul Kim, Wonyoung Jang, Kyungroul Lee, and Sun-Young Lee. 2019. Improvement of QR code access control system based on Lamport hash chain. In *International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*. Springer, 824–833.

[108] So-Hyun Park, Soyoung Joo, and Il-Gu Lee. 2022. Secure visible light communication system via cooperative attack detecting techniques. *IEEE Access* 10 (2022), 20473–20485.

[109] Parth H. Pathak, Xiaotao Feng, Pengfei Hu, and Prasant Mohapatra. 2015. Visible light communication, networking, and sensing: A survey, potential and challenges. *IEEE Commun. Surv. Tutor.* 17, 4 (2015), 2047–2077.

[110] Toni Perkovic, Mario Cagalj, Toni Mastelic, Nitesh Saxena, and Dinko Begusic. 2011. Secure initialization of multiple constrained wireless devices for an unaided user. *IEEE Trans. Mob. Comput.* 11, 2 (2011), 337–351.
[111] H. Vincent Poor and Rafael F. Schaefer. 2017. Wireless physical layer security. *Proc. Nat. Acad. Sci.* 114, 1 (2017), 19–26.
[112] Kun Qian, Yumeng Lu, Zheng Yang, Kai Zhang, Kehong Huang, Xinjun Cai, Chenshu Wu, and Yunhao Liu. 2021. AIRCODE: Hidden screen-camera communication on an invisible and inaudible dual channel. In *USENIX Symposium on Networked Systems Design and Implementation*. 457–470.
[113] 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.
[114] Yuchu Qin, Tuong Thuy Vu, and Yifang Ban. 2011. Toward an optimal algorithm for LiDAR waveform decomposition. *IEEE Geosci. Remote Sens. Lett.* 9, 3 (2011), 482–486.
[115] Junchao Qiu, Lin Zhang, Diyang Li, and Xingcheng Liu. 2016. High security chaotic multiple access scheme for visible light communication systems with advanced encryption standard interleaving. *Optic. Eng.* 55, 6 (2016), 066121.
[116] Arockia Bazil Raj and Arun K. Majumder. 2019. Historical perspective of free space optical communications: From the early dates to today's developments. *IET Commun.* 13, 16 (2019), 2405–2419.
[117] Saeed Ur Rehman, Shakir Ullah, Peter Han Joo Chong, Sira Yongchareon, and Dan Komosny. 2019. Visible light communication: A system perspective-overview and challenges. *Sensors* 19, 5 (2019), 1153.
[118] Ronald L. Rivest et al. 1998. Chaffing and winnowing: Confidentiality without encryption. *CryptoBytes (RSA Lab.)* 4, 1 (1998), 12–17.
[119] 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.
[120] Elham Sarbazi and Murat Uysal. 2013. PHY layer performance evaluation of the IEEE 802.15. 7 visible light communication standard. In *2nd International Workshop on Optical Wireless Communications (IWOW)*. IEEE, 35–39.
[121] Noor Ahmad Sarker, A. S. M. Badrudduza, S. M. Riazul Islam, Sheikh Habibul Islam, Imran Shafique Ansari, Milton Kumar Kundu, Mst Fateha Samad, Md Biplob Hossain, and Heejung Yu. 2020. Secrecy performance analysis of mixed hyper-gamma and gamma-gamma cooperative relaying system. *IEEE Access* 8 (2020), 131273–131285.
[122] Giuseppe Schirripa Spagnolo, Lorenzo Cozzella, and Fabio Leccese. 2020. Underwater optical wireless communications: Overview. *Sensors* 20, 8 (2020), 2261.
[123] 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.
[124] Rana Shaaban, Prakash Ranganathan, and Saleh Faruque. 2019. Visible light communication security vulnerabilities in multiuser network: Power distribution and signal to noise ratio analysis. In *Future of Information and Communication Conference*. Springer, 1–13.
[125] Ali Shahidinejad, Abouzar Azarpira, Toni Anwar, Otto Spaniol et al. 2014. Quantum cryptography coding system for optical wireless communication. *J. Optoelectron. Advan. Mater.* 16, 7-8 (2014).
[126] 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.
[127] Simone Soderi, Alessandro Brighente, Federico Turrin, and Mauro Conti. 2022. VLC Physical layer security through RIS-aided jamming receiver for 6G wireless networks. In *19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 370–378.
[128] Emilio Calvanese Strinati, Sergio Barbarossa, Jose Luis Gonzalez-Jimenez, Dimitri Ktenas, Nicolas Cassiau, Luc Maret, and Cedric Dehos. 2019. 6G: The next frontier: From holographic messaging to artificial intelligence using subterahertz and visible light communication. *IEEE Vehic. Technol. Mag.* 14, 3 (2019), 42–50.
[129] Nuğman Su, Erdal Panayirci, Mutlu Koca, and H. Vincent Poor. 2021. Spatial constellation design-based generalized space shift keying for physical layer security of multi-user MIMO communication systems. *IEEE Wirel. Commun. Lett.* 10, 8 (2021), 1785–1789.
[130] Nuğman Su, Erdal Panayirci, Mutlu Koca, Anil Yesilkaya, H. Vincent Poor, and Harald Haas. 2021. Physical layer security for multi-user MIMO visible light communication systems with generalized space shift keying. *IEEE Trans. Commun.* 69, 4 (2021), 2585–2598.
[131] Zishun Su, Qiaoling Zou, Xinying Wu, Junnan Ye, and Jianxin Cheng. 2021. Participant and strategy selection of health QR code product experience design during the COVID-19 pandemic in China: The information security perspective. *Discr. Dynam. Nat. Societ.* 2021 (2021).
[132] Sikiru Subairu, John Alhassan, Shafii Abdulhamid, and Joseph Ojeniyi. 2020. A review of detection methodologies for quick response code phishing attacks. In *2nd International Conference on Computer and Information Sciences (ICCIS)*. IEEE, 1–5.

[133] Rasool Tavakoli, Majid Nabi, Twan Basten, and Kees Goossens. 2015. Enhanced time-slotted channel hopping in WSNs using non-intrusive channel-quality estimation. In *IEEE 12th International Conference on Mobile Ad Hoc and Sensor Systems*. IEEE, 217–225.
[134] Emre Telatar. 1999. Capacity of multi-antenna gaussian channels. *Eur. Trans. Telecommun.* 10, 6 (1999), 585–595.
[135] Andrew Tinka, Thomas Watteyne, and Kris Pister. 2010. A decentralized scheduling algorithm for time synchronized channel hopping. In *International Conference on Ad Hoc Networks*. Springer, 201–216.
[136] Sumit Tiwari. 2016. An introduction to QR code technology. In *International Conference on Information Technology (ICIT)*. IEEE, 39–44.
[137] Dobroslav Tsonev, Stefan Videv, and Harald Haas. 2015. Towards a 100 Gb/s visible light wireless access network. *Optics Expr.* 23, 2 (2015), 1627–1637.
[138] Seyhan Ucar, Sinem Coleri Ergen, Oznur Ozkasap, Dobroslav Tsonev, and Harald Burchardt. 2016. SecVLC: Secure visible light communication for military vehicular networks. In *14th ACM International Symposium on Mobility Management and Wireless Access*. 123–129.
[139] Seyhan Ucar, Sinem Coleri Ergen, and Oznur Ozkasap. 2018. IEEE 802.11 p and visible light hybrid communication based secure autonomous platoon. *IEEE Trans. Vehic. Technol.* 67, 9 (2018), 8667–8681.
[140] Martin Vuagnoux and Sylvain Pasini. 2009. Compromising electromagnetic emanations of wired and wireless keyboards. In *USENIX Security Symposium*, Vol. 8. 1–16.
[141] Heider A. M. Wahsheh and Flaminia L. Luccio. 2020. Security and privacy of QR code applications: A comprehensive study, general guidelines and solutions. *Information* 11, 4 (2020), 217.
[142] Ning Wang, Pu Wang, Amir Alipour-Fanid, Long Jiao, and Kai Zeng. 2019. Physical-layer security of 5G wireless networks for IoT: Challenges and opportunities. *IEEE Internet Things J.* 6, 5 (2019), 8169–8181.
[143] Zhaocheng Wang, Qi Wang, Wei Huang, and Zhengyuan Xu. 2017. *Visible Light Communications: Modulation and Signal Processing*. John Wiley & Sons.
[144] Ning Wei, Ying Liu, Tingting Zhang, Jun Liang, and Daoai Wang. 2016. Hydrogenated TiO2 nanotube arrays with enhanced photoelectrochemical property for photocathodic protection under visible light. *Mater. Lett.* 185 (2016), 81–84.
[145] Y.-P. Wong, Shuhaidah Othman, Y.-L. Lau, S. Radu, and H.-Y. Chee. 2018. Loop-mediated isothermal amplification (LAMP): A versatile technique for detection of micro-organisms. *J. Appl. Microbiol.* 124, 3 (2018), 626–643.
[146] Xiping Wu, Mohammad Dehghani Soltani, Lai Zhou, Majid Safari, and Harald Haas. 2021. Hybrid LiFi and WiFi networks: A survey. *IEEE Commun. Surv. Tutor.* 23, 2 (2021), 1398–1420.
[147] Yongpeng Wu, Ashish Khisti, Chengshan Xiao, Giuseppe Caire, Kai-Kit Wong, and Xiqi Gao. 2018. A survey of physical layer security techniques for 5G wireless networks and challenges ahead. *IEEE J. Select. Areas Commun.* 36, 4 (2018), 679–695.
[148] Liang Xiao, Geyi Sheng, Sicong Liu, Huaiyu Dai, Mugen Peng, and Jian Song. 2019. Deep reinforcement learning-enabled secure visible light communication against eavesdropping. *IEEE Trans. Commun.* 67, 10 (2019), 6994–7005.
[149] Aylin Yener and Sennur Ulukus. 2015. Wireless physical-layer security: Lessons learned from information theory. *Proc. IEEE* 103, 10 (2015), 1814–1825.
[150] Anil Yesilkaya, Tezcan Cogalan, Serhat Erkucuk, Yalcin Sadi, Erdal Panayirci, Harald Haas, and H. Vincent Poor. 2020. Physical-layer security in visible light communications. In *2nd 6G Wireless Summit (6G SUMMIT)*. IEEE, 1–5.
[151] Liang Yin and Harald Haas. 2017. Physical-layer security in multiuser visible light communication networks. *IEEE J. Select. Areas Commun.* 36, 1 (2017), 162–174.
[152] Liang Yin, Wasiu O. Popoola, Xiping Wu, and Harald Haas. 2016. Performance evaluation of non-orthogonal multiple access in visible light communication. *IEEE Trans. Commun.* 64, 12 (2016), 5162–5175.
[153] Kelvin S. C. Yong, Kang Leng Chiew, and Choon Lin Tan. 2019. A survey of the QR code phishing: The current attacks and countermeasures. In *7th International Conference on Smart Computing & Communications (ICSCC)*. IEEE, 1–5.
[154] Bingsheng Zhang, Kui Ren, Guoliang Xing, Xinwen Fu, and Cong Wang. 2015. SBVLC: Secure barcode-based visible light communication for smartphones. *IEEE Trans. Mob. Comput.* 15, 2 (2015), 432–446.
[155] Chi Zhang and Xinyu Zhang. 2017. Pulsar: Towards ubiquitous visible light localization. In *23rd Annual International Conference on Mobile Computing and Networking*. 208–221.
[156] Lan Zhang, Kebin Liu, Xiang-Yang Li, Cihang Liu, Xuan Ding, and Yunhao Liu. 2016. Privacy-friendly photo capturing and sharing system. In *ACM International Joint Conference on Pervasive and Ubiquitous Computing*. 524–534.
[157] Xiao Zhang, Hanqing Guo, James Mariani, and Li Xiao. 2022. U-star: An underwater navigation system based on passive 3D optical identification tags. In *28th Annual International Conference on Mobile Computing and Networking*. 648–660.
[158] Xiao Zhang, Griffin Klevering, and Li Xiao. 2022. Exploring rolling shutter effect for motion tracking with objective identification. In *20th ACM Conference on Embedded Networked Sensor Systems*. 816–817.

[159] Xiao Zhang, James Mariani, Li Xiao, and Matt W. Mutka. 2022. LiFOD: Lighting extra data via fine-grained OWC dimming. In *19th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*. IEEE, 73–81.
[160] Xiao Zhang and Li Xiao. 2020. Effective subcarrier pairing for hybrid delivery in relay networks. In *IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 238–246.
[161] Xiao Zhang and Li Xiao. 2020. Lighting extra data via OWC dimming. In *Student Workshop*. 29–30.
[162] Xiao Zhang and Li Xiao. 2020. RainbowRow: Fast optical camera communication. In *IEEE 28th International Conference on Network Protocols (ICNP)*. IEEE, 1–6.
[163] 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.
[164] Xiang Zhao and Jinyong Sun. 2020. Physical-layer security for mobile users in NOMA-enabled visible light communication networks. *IEEE Access* 8 (2020), 205411–205423.
[165] Zhong Zheng, Lu Liu, and Weiwei Hu. 2017. Accuracy of ranging based on DMT visible light communication for indoor positioning. *IEEE Photon. Technol. Lett.* 29, 8 (2017), 679–682.
[166] Anfu Zhou, Guangyuan Su, Shilin Zhu, and HuaDong Ma. 2019. Invisible QR code hijacking using smart LED. *Proc. ACM Interact., Mob., Wear. Ubiq. Technol.* 3, 3 (2019), 1–23.
[167] Xiangyun Zhou, Behrouz Maham, and Are Hjorungnes. 2012. Pilot contamination for active eavesdropping. *IEEE Trans. Wirel. Commun.* 11, 3 (2012), 903–907.
[168] Shilin Zhu, Chi Zhang, and Xinyu Zhang. 2017. Automating visual privacy protection using a smart LED. In *23rd Annual International Conference on Mobile Computing and Networking*. 329–342.

Received 17 October 2022; revised 14 March 2023; accepted 23 March 2023