Exploring physical layer security in underwater optical wireless communication: A concise overview

Dang Tien Sy[1*], Nguyen Van Thang[2], Cao Van Toan[1], Dang The Ngoc[2]

[1]Institute of Electronics, Academy of Military Science and Technology, 17 Hoang Sam, Cau Giay, Hanoi, Vietnam;
[2]Posts and Telecommunications Institute of Technology, Km10, Nguyen Trai, Ha Dong, Hanoi, Vietnam.
[*]Corresponding author: sydt.start18@gmail.com
Received 22 May 2024; Revised 30 Aug. 2024; Accepted 11 Oct. 2024; Published 25 Oct. 2024.
DOI: https://doi.org/10.54939/1859-1043.j.mst.98.2024.3-14

ABSTRACT

Underwater wireless optical communications are a developing alternative to meet the increasing need for high-speed connections in oceans and seas. Optical wireless communications (OWCs) are more secure and less susceptible to eavesdropping compared to acoustic communications or radio frequency (RF) communications due to their narrow optical beam coverage and reliance on line-of-sight components. Nevertheless, the existence of a hostile eavesdropper can compromise the level of confidentiality achieved by OWC networks. This article provides a concise overview of the latest research conducted on physical layer security (PLS) in underwater optical wireless communication (UOWC). Furthermore, this work presents the relevant unresolved matters, approaches for enhancing secrecy performance, and potential areas for further research.

Keywords: Physical layer security (PLS); Underwater Optical Wireless Communication (UOWC); Secrecy performance improvement techniques.

1. INTRODUCTION

Underwater optical wireless communication (UOWC) has garnered significant interest across military, industrial, and scientific domains due to its potential applications in tactical surveillance, environmental monitoring, and oceanographic research. While UOWC offers advantages over traditional acoustic methods, including increased bandwidth and enhanced security [1], it faces challenges such as limited communication range due to absorption, scattering, and turbulence [2]. The advent of 6G communications necessitates robust security solutions for UOWC systems. Conventional cryptography, based on computational security [3], may be vulnerable to future quantum computing advances [4]. Consequently, there is a growing emphasis on developing information-theoretic security and physical-layer security (PLS) approaches [5].

PLS encompasses both keyless and secret-key schemes. The keyless system, introduced by Wyner, involves confidential transmission via a wiretap channel [6]. The secret-key approach originated with Vernam's one-time-pad scheme, later proven secure by Shannon. Recent research has explored secret-key agreement (SKA) systems for wireless channels experiencing multipath scattering and fading [7]. Quantum key distribution (QKD) has emerged as an alternative ITS-proof method, utilizing quantum physics principles. QKD implementations include discrete-variable (DV-QKD) and continuous-variable (CV-QKD) schemes. Ongoing research focuses on improving QKD practicality through techniques such as differential-phase-shift-keying (DPSK) [8] and intensity modulation/direct detection (IM/DD) systems for both optical fiber [9] and free-space optical (FSO) systems [10]. These advancements aim to establish secure connections for terrestrial, aerial, and satellite-based platforms, potentially contributing to a future global quantum network [11].

This survey aims to provide a comprehensive overview of PLS and its applications in UOWC systems, addressing the current limitations in research scope [12]. It discusses fundamental

concepts such as PLS models, channel models, and performance metrics, as well as existing PLS techniques implemented for UOWC systems. Furthermore, the survey proposes and suggests several potential research directions for enhancing security in UOWC communications, contributing to the ongoing development of robust and efficient UOWC networks.

2. FUNDAMENTALS OF PLS IN UOWC SYSTEMS

PLS in UOWC exploits inherent properties of the physical layer to ensure secure data transmission without relying solely on higher-layer encryption. This approach leverages channel randomness, beamforming, artificial noise, and QKD to enhance security against eavesdroppers. UOWC systems utilize underwater channel characteristics such as turbulence, absorption, and scattering to create a unique security environment. Beamforming techniques concentrate optical signals towards intended receivers, while artificial noise addition confounds potential interceptors. QKD offers unconditional security by employing quantum mechanics principles for key generation and distribution. Additionally, PLS enables keyless security in UOWC systems by exploiting channel reciprocity and spatial correlation properties, thus eliminating the need for traditional key management processes.

2.1. Basic PLS Model of UOWC System

In the general PLS model for a UOWC system (figure 1), there are three main communication nodes: the transmitter node or source node of the legitimate user Alice (S), the receiver node or destination node of the legitimate user Bob (D), and the eavesdropping node of the illegitimate user Eve (E). The links in UOWC can be categorized into two primary types: line-of-sight (LOS) links and non-line-of-sight (NLOS) links [13].

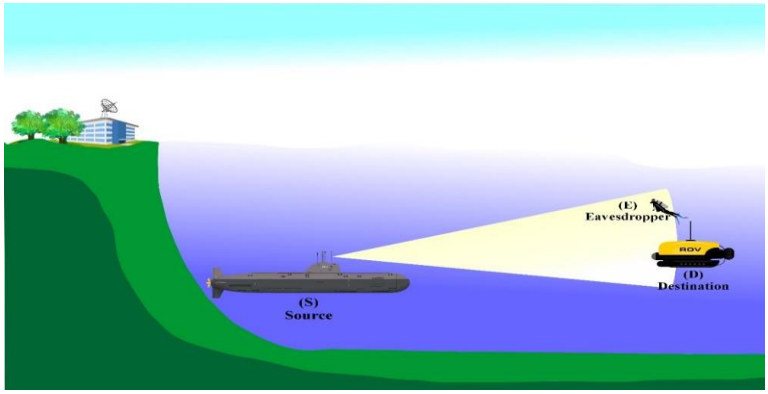


Figure 1. *A typical example of UOWC security communications over the physical layer.*

In this survey, we consider the case of LOS links is implemented and assume that the direct link between node S and node D is not blocked by obstacles, such as seamounts, submarines, marine life, etc. The received signal at node D can be expressed as:

$$y = hs + n \tag{1}$$

where s is the signal transmitted from the source node S, $\boldsymbol{n} \sim \boldsymbol{\mathcal{N}}(\mathbf{0}, \boldsymbol{\sigma_n^2})$ is the additive white Gaussian noise (AWGN) with zero mean and variance $\boldsymbol{\sigma_n^2}$.

2.2. Underwater Channel Model

We consider the channel to include three main effects: path loss h_{pl}, oceanic turbulence h_t, and beam spreading loss h_{bl}. The underwater channel coefficient can be expressed as:

$$h = h_{pl} h_{bl} h_t \tag{2}$$

2.2.1. Oceanic Propagation Loss

According to the characteristic properties of the aquatic environment, different geographical locations have different types of seawater, leading to varying attenuation of optical transmission in the underwater environment. The oceanic propagation loss can be determined as [14]:

$$h_{pl} \approx \left(\frac{D_R}{\theta_F}\right) d^{-2} \exp\left[-c_e \left(\frac{D_R}{\theta_F}\right)^{\rho} d^{1-\rho}\right] \tag{3}$$

where c_e is the light beam attenuation coefficient, whose value depends on the water type and depth [15]. The common values of c_e are mentioned in [54]. The parameters ρ, θ_F, D_R and d are the correction factor, divergence angle adjustment factor, receiver aperture diameter, and the transmission distance respectively.

2.2.2. Oceanic Turbulence

Ocean turbulence is a phenomenon caused by changes in water temperature and salinity, and its impact leads to fluctuations in the received power. The intensity of turbulence can be expressed through the refractive index along the water environment. In this study, we investigate the lognormal distribution. Following the approach in [16], the probability density function (PDF) of the ocean turbulence coefficient can be presented as:

$$f_{h_t}(h_t) = \frac{1}{h_t \sqrt{8\pi\sigma_t^2}} \exp\left[-\frac{(\ln(h_t) - 2\mu_t)^2}{8\sigma_t^2}\right] \tag{4}$$

where μ_t and σ_t^2 are the mean and variance of the log-amplitude coefficient, respectively. The relationship between the log-amplitude variance and the scintillation index is represented as $\sigma_t^2 = 0.25\ln(1+\sigma_R^2)$, where σ_R^2 is the Rytov variance, which is mentioned in [17].

2.2.3. Beam Spreading Loss

At a distance *d*, the attenuation of optical intensity due to the divergence property of the beam can be calculated by the Gaussian form [18] follows:

$$h_{bl}(r;D) \approx A_0 \exp\left(-\frac{2r^2}{\omega_L^2}\right) \tag{5}$$

where A_0 is the received power at $r = 0$, ω_L^2 is defined as the beam width at the destination, and r is the distance between the center of the beam at the receiver side and the position of the receiver.

2.3. PLS Performance Metrics for UOWC Systems

Prevalent metrics for assessing communication systems' secrecy performance include secrecy capacity (SC), average secrecy capacity and secrecy outage probability. These quantitative measures, expressible in closed-form mathematical formulations, enable evaluation of a system's confidentiality maintenance and eavesdropping resistance capabilities.

2.3.1. Average Secrecy Capacity (ASC)

ASC is a key metric for evaluating wireless communication system security in the presence of eavesdroppers. It quantifies the maximum achievable secrecy rate, defined in information theory:

$$C_s = \begin{cases} \log_2(1+\gamma_B) - \log_2(1+\gamma_E), & \gamma_B > \gamma_E \\ 0, & \text{other} \end{cases} \tag{6}$$

where γ_B and γ_E are the instantaneous SNRs of the legitimate receiver and the eavesdropper's receiver, respectively. ASC is mathematically defined as follows [19]:

$$ASC = E[C_s(\gamma_B, \gamma_E)] = \int_0^{\infty}\int_0^{\infty} C_s(\gamma_B, \gamma_E) f(\gamma_B, \gamma_E) d\gamma_B d\gamma_E \tag{7}$$

where $C_s(\gamma_B, \gamma_E)$ is the instantaneous secrecy capacity of the considered system and $f(\gamma_B, \gamma_E)$ is

the joint PDF.

2.3.2. Secrecy Outage Probability (SOP)

This is a security metric that measures the likelihood of a confidential message being intercepted by an eavesdropper. It occurs when the difference between the capacity of the legitimate communication link and the eavesdropping link, known as the secrecy capacity, falls below a predefined threshold rate (R_s). Mathematically, SOP is expressed as the probability that the secrecy capacity is in outage [20], represented by:

$$SOP = \Pr\{C_s(\gamma_B, \gamma_E) \le R_s\} \tag{8}$$

2.3.3. Some other metrics

In addition to the popular metrics mentioned in the previous section, some other metrics can be mentioned. In wiretapped communication models, strictly positive secrecy capacity (SPSC) plays a vital role in ensuring the feasibility of uninterrupted secure communication. The SPSC is a critical parameter that determines whether the system can maintain a positive secrecy capacity, which is essential for preventing the eavesdropper from intercepting and decoding the transmitted information. A positive secrecy capacity indicates that the main channel between the transmitter and the intended receiver has a higher capacity than the wiretap channel between the transmitter and the eavesdropper. The mathematical representation of SPSC [21] follows as:

$$SPSC = \Pr\{C_s(\gamma_B, \gamma_E) > 0\} \tag{9}$$

where C_s is the instantaneous secrecy capacity.

Secrecy throughput (ST) quantifies the rate of secure information transmission in a communication channel [22]. It is a crucial metric in information-theoretic security, measuring the volume of confidential data securely communicated over time in potentially compromised channels:

$$ST = R_s(1 - SOP) \tag{10}$$

Ergodic capacity represents the maximum achievable rate at which information can be reliably transmitted over a channel, averaged over all possible channel states, assuming that the channel is ergodic. The formula (11) is a probabilistic average and equal to Shannon capacity for an AWGN channel with SNR γ, given by $B\log_2(1+\gamma)$ and averaged over the distribution of γ [23]:

$$C = \int_0^\infty B\log_2(1+\gamma)\, p(\gamma) d\gamma \tag{11}$$

Intercept probability (IP) is a concept in wireless communication systems that refers to the probability of an eavesdropper successfully intercepting and decoding the transmitted information intended for a legitimate receiver [24]:

$$P_{IP} = \Pr(C_B < C_E) \tag{12}$$

where C_B and C_E are the secrecy capacity of the legitimate receiver and the eavesdropper's receiver, respectively.

In a UOWC system based on a quantum key distribution protocol, quantum bit error rate (QBER) is a measure of the errors that occur during the transmission of quantum bits (qubits). It represents the ratio of the number of erroneous bits to the total number of transmitted bits:

$$QBER = \frac{\Pr(error)}{\Pr(sift)} \tag{13}$$

where $\Pr(error)$ and $\Pr(sift)$ are probabilities of sift and error, respectively. Secret key rate (SKR) is a fundamental metric in quantum key distribution (QKD) that quantifies the rate at which secret key bits can be securely generated and shared between two communicating parties, often referred to as Alice and Bob [25]. For example, in the case of using the BB84 protocol, the SKR can be

calculated as:

$$SKR = 1 - (1 + f)\hbar(QBER) \quad (14)$$

where f is the reconciliation efficiency, $\hbar(QBER)$ is the entropy function representing the minimum amount of information that needs to be sent from Alice to Bob to correct Bob's key string.

3. RECENT UP-TO-DATE LITERATURE SURVEY ON PLS IN UOWC SYSTEMS

3.1. Summary of PLS trends in UOWC techniques

Current research on PLS in UOWC primarily focuses on three areas: (1) mixed/hybrid systems combining acoustic, radio, and optical wave communication technologies; (2) modulation techniques; and (3) quantum key distribution (QKD) as a potential solution. Studies have explored the relationships between factors such as channel models, transmission distance, signal power, and eavesdropper numbers. By delving into specific cases and results from recent research, we gain a comprehensive understanding of the current state and future directions of PLS techniques in UOWC (table 1).

Table 1. *The PLS trends in UOWC techniques.*

Ref	System Type	Main Focus	Channel Model	Metrics
[26]	NOMA-supported UOWC system	Security performance under inaccurate CSI conditions	Underwater channel with attenuation, scattering, air bubbles	SOP
[27]	UOWC system with SSE-OFDM modulation	Demonstrated SSE-OFDM in sediment-filled tank	14.2m long sediment-filled tank simulation	The signal-to-noise power ratio (OPR); SC
[28]	UOWC with 450 nm laser and DFT-S DMT modulation	Enhance UOWC security by two-level chaotic encryption	Water channels under various turbidity conditions	Security against brute-force attacks
[29]	Mixed RF/RIS and UOWC system	Impact of RIS elements on secrecy	RF and UOWC channels with Nakagami-m and mEGG distributions	ASC; SOP; SPSC
[30]	Air-to-underwater system with AF relaying	Minimize complexity and enhance security	RF with α-μ and UOWC with mixed EGG distributions	SOP; The probability of non-zero secrecy capacity
[20]	Dual-hop RF/UOWC system with an intermediate decode-and-forward (DF) relay node	Investigate PLS in a UOWC-RF network with multiple RF eavesdroppers.	UOWC with a mixture of exponential generalized Gamma turbulence with pointing error impairments. RF with κ-μ shadowed fading	SOP; SPSC; Effective secrecy throughput (EST)
[31]	A dual-hop mixed RF/UOWC system	Analyzing PLS under RF channel eavesdropping.	RF with generalized GG fading distribution. UOWC with mEGG fading/turbulence distribution	ASC; SOP; SPSC

[32]	A mixed RF/UOWC system using decode-and-forward and selection combining at the relay node	Analyze PLS performance under multiple RF eavesdroppers	RF with Nakagami-m distribution UOWC with mixture Exponential-Gamma distribution	SOP
[33]	An amplify-and-forward and energy harvesting-based mixed RF/UOWC system	Analyzing the PLS performance of the system in the presence of a single eavesdropper attacking the RF channel	RF with Nakagami-m fading UOWC with mixture Exponential-Gamma fading	SOP; IP
[34]	NOMA-based dual-hop hybrid RF-UOWC system	Power allocation optimization	RF with Rayleigh and AWGN; UOWC with mEGG and AWGN	Outage probability; Ergodic capacity
[35]	CVQKD system for trans-media communication	Establish trans-media CVQKD link	Atmospheric and seawater quantum channels	SOP
[36]	UOWC system with quantum technologies	Enhance underwater communication capabilities	Experimental setups for UOWC	Bit error rate (BER); Secure key generation
[37]	Secure underwater communications with QKD	Feasibility of quantum communication in maritime environment	Oceanic water types for quantum and classical channels	QBER; SKR
[38]	Quantum communication protocols in aquatic scenarios	Ultimate security through quantum technologies	LOS and reflective NLOS optical channel models	QBER; SKR
[39]	QKD system in underwater channels	QBER and SKR performance of BB84 protocol	Modified Beer–Lambert formula for path loss	QBER; SKR
[40]	Underwater QKD with polarization encoding	Enhance understanding and performance of underwater QKD	Underwater channel with background light analysis	QBER; SKR
[41]	Real-time underwater QKD system	Develop real-time quantum-secure underwater networks	Underwater System architecture	QBER

Research findings indicate that secrecy outage probability (SOP) improves with increased transmit power, legitimate SINR, LED numbers, and target data rates, while degrading under stronger underwater turbulence [26]. Optimal spectrum spread factors for maximizing secrecy capacity vary with OPR [27]. Chaotic encryption schemes have demonstrated enhanced PLS for high-speed, long-distance UOWC systems [28].

Secrecy performance is strongly influenced by relative SNRs, eavesdropper numbers, and detection techniques [32, 33]. QKD solutions have been analyzed for maximum transmission distances [35], with experimental demonstrations of quantum technologies for secure UOWC [36]. Studies have examined BER and key rates for various scenarios, including single-photon detection [36], orbital angular momentum (OAM) modulation, and decoy-state BB84 protocol. Results indicate the feasibility of secure underwater quantum communications under certain conditions

[37, 38], with differential phase shift (DPS) and coherent one-way (COW) protocols showing slightly better performance than BB84 and B92 [38].

3.2. Potential solutions for PLS in UOWC systems

3.2.1. PLS in UOWC systems based on the OCDMA technique

The concept of underwater mobile optical wireless code division multiple access (OCDMA) networks based on orthogonal optical codes (OOC) was introduced in [42]. This system employs optical base transceiver stations (OBTS) in a hexagonal cell configuration to extend communication coverage. An experimental model demonstrated the system's feasibility [42]. Further studies [43] explored the characteristics, potential, and challenges of these networks. BER performance evaluation [44] using 532 nm LEDs and Silicon APD detectors achieved a BER of 2.7 x 10^{-7} with a code length of 255 in clean water, confirming the system's viability for deployment.

The authors in [45] proposed an underwater wireless optical communications code-division multiple-access (UOWC/CDMA) system with multiple relay assistance, which implements the Chip Detect-and-Forward (CDF) technique to prevent the difficult multiuser decoding procedure. The performance analysis of a vertical UOWC link subject to multiple-access interference and background noise is considered. The security analysis focuses on the probability of eavesdropping on the user's code ($P_{correct}$) and how it varies with transmit power, number of users, and code parameters.

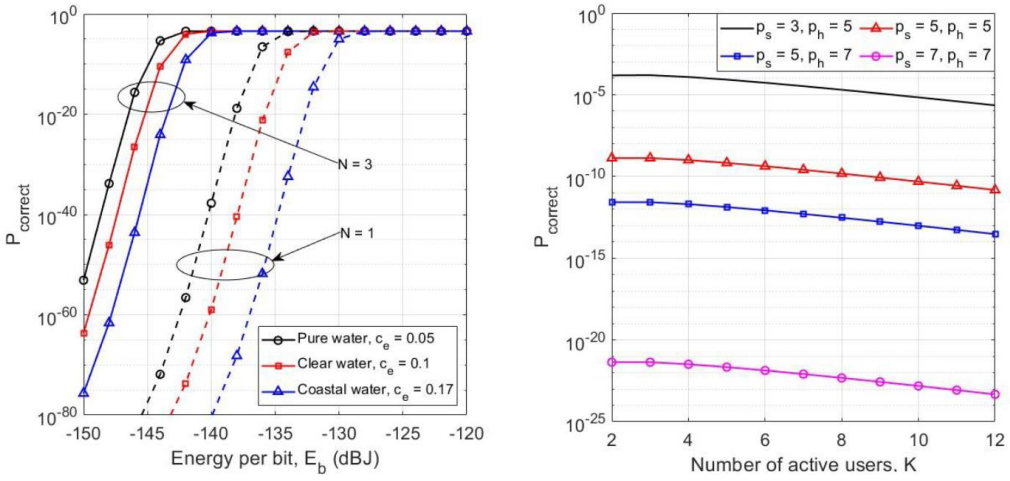


Figure 2. *Evaluation results of the security of UOWC/CDMA system [45].*

Figure 2 shows two figures: (1) $P_{correct}$ versus the transmitted power per bit E_b under different underwater propagation loss conditions; (2) The relationship between $P_{correct}$ and the number of active users k for different prime code parameters. Using relay transmission can help increase the achievable distance at a given BER. For example, with 4 users and a BER of 10^{-6}, the transmission distance increases from 3.5 to 5.2 km when the number of relays increases from 1 to 2. The results have demonstrated UOWC systems using CDMA is feasible and has an advantage over the ones using wavelength-division multiple-access.

3.2.2. PLS in UOWC systems applied QKD technique

QKD protocols have garnered significant attention due to their ability to provide unconditional security, contrasting with traditional encryption methods' reliance on computational complexity [46]. QKD systems, based on the "No-cloning" theorem, can detect eavesdropping through additional noise in quantum transmissions. QKD protocols are categorized into three families: DV-QKD, CV-QKD, and distributed phase reference coding (DPR-QKD) [47]. DV-QKD protocols,

including BB84, E91, and BBM92, are widely researched and implemented. Studies indicate that single-photon QKD can be effective at depths of 60-110 m in clear water [48], with practical experiments demonstrating feasibility for UOWC [36]. Performance analysis in turbulent underwater channels shows that secure QKD distances vary based on water type, atmospheric conditions, detector field of view, and aperture size [39].

CV-QKD addresses the limitations of single-photon detectors by employing homodyne detection with conventional photodiodes. Various CV-QKD schemes have been proposed, including Gaussian-modulated coherent state (GMCS), discrete-modulated coherent state (DMCS), two-way CV-QKD, unidimensional CV-QKD, squeezed-state CV-QKD, and entanglement-based CV-QKD protocols. Ongoing research focuses on improving security, efficiency, and practicality of these schemes. A novel CV-QKD scheme employing direct detection and intensity-modulated (IM) coherent light with moderate power was proposed, where the transmitted light is directly detected (DD). From an information-theoretic perspective, the secure key creation rate R_f, which represents the final key rate after error correction and privacy amplification, is given by:

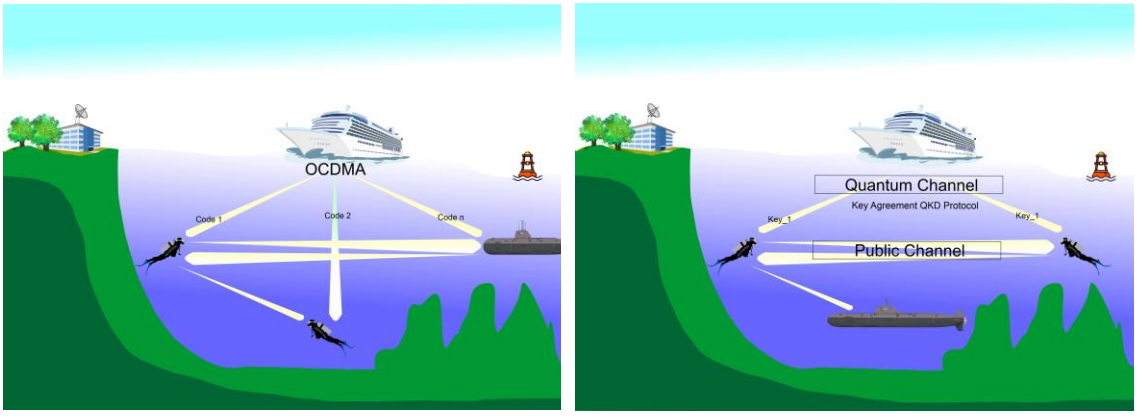
$$R_f = R_{AB} - R_{AE} \text{ or } R_{AB} - R_{BE} \quad (15)$$

where R_{AB}, R_{AE}, and R_{BE} are the mutual information between Alice and Bob, that between Alice and Eve, and that between Bob and Eve, respectively.

4. OPEN RESEARCH PROBLEMS FOR PLS IN UOWC SYSTEMS

The necessity to ensure communication security in the underwater environment has garnered significant attention from both network service providers and research laboratories, as the Internet of Underwater Things (IoUT) emerges as one of the pioneering technologies in the beyond 5G and future 6G network trends [49].

First, the solution of employing OCDMA technology for PLS in UOWC has been mentioned in the previous section. However, recent studies have only focused on the utilization of OOC codes, without providing evaluations and comparisons when using other types of optical codes belonging to unipolar, bipolar, or codes with ideal in-phase cross-correlation (e.g., Prime codes, Walsh-Hadamard codes, Modified Quadratic Congruence (MQC) codes [50],...). Furthermore, there have been no assessments of the system's security capabilities based on code length and code weight. Depending on the usage characteristics and the purpose of system deployment, the number of devices participating in the OCDMA-UOWC network can be small or large. Therefore, selecting the appropriate code type to achieve high system performance and security effectiveness is a crucial issue that requires further research and evaluation.



a) *A OCDMA-UOWC system concept* b) *A UOWC based on QKD system concept*

Figure 3. *Security scenario for UOWC systems.*

Second, the security solution for UOWC based on QKD is a novel approach, with only a few studies summarized in the previous section. Therefore, it is necessary to conduct more research on this solution due to its feasibility. The next research direction could be to propose and develop new QKD-UOWC models, combined with evaluating system performance and security effectiveness. For example, building a QKD-UOWC system using modulated signals such as BPSK (Binary Phase Shift Keying) or 8PSK (Octa-phase Shift Keying) [51], and assessing the system performance and security effectiveness of these systems. Additionally, studies utilizing the family of CV-QKD and DPR-QKD protocol codes are also a research direction to develop security using the QKD protocol, which is currently receiving significant attention.

Third, some potential research directions for PLS in UOWC include:

- Underwater channel modeling: One of the issues that researchers are currently focusing on is developing a more comprehensive UOWC channel model with accurate models describing ocean turbulence. Several different optical channel modeling distributions are used to describe the variation of the optical signal as it passes through the aquatic environment, such as Rayleigh distribution, Exponential distribution, Gamma-Gamma distribution, and optical bandwidth distribution [52]. To optimize the system performance and security effectiveness of UOWC, developing underwater channel modeling is an important research direction.
- Intelligent reflective surface (IRS) assisted UOWC system: IRS is an advanced technology that enables the design of wireless signal transmission in wireless networks. By intelligently adjusting the signal reflection through a large number of low-cost passive reflecting elements, IRS has the ability to flexibly change wireless channels to enhance communication performance. The authors in [53] have built and evaluated the performance of an IRS-assisted UOWC system, but the assessment of the security capability for this system is still open and needs to be further investigated.
- The mixed/hybrid UOWC systems: UOWC systems are almost impossible to completely replace systems using acoustic or RF communication technologies. Therefore, the idea of building mixed/hybrid RF/UOWC, Acoustic/UOWC, or FSO/UOWC systems using relays as signal forwarding nodes with amplify-and-forward or/and decode-and-forward techniques has been implemented and evaluated for performance [54] and PLS effectiveness [20]. The security issue for these systems still needs to be further studied due to their high practical application potential in the near future.

5. CONCLUSIONS

Underwater optical wireless communications (UOWC) are gaining increasing attention from scientists, commercial organizations, and military forces due to their practical applications and outstanding advantages in the fields of ocean science and maritime military. The diverse applications and characteristics of the deployment environment pose significant challenges, affecting the reliability of UOWC systems. To address this issue, improving system performance and security effectiveness for UOWC systems is a crucial problem that needs to be prioritized for research. Important factors that directly affect the performance and security of the UOWC system include the transmission environment and attack methods that have been mentioned. Specifically, research mainly focuses on eavesdropping attack methods and channel models, where many factors have also been built on which to calculate and evaluate system performance and security capabilities of the UOWC system. Current technical solutions for physical layer security are also summarized. In addition, our analysis has revealed a range of open research issues that hold considerable promise for strengthening the security posture of present-day UOWC systems. These identified challenges serve as compelling avenues for future research endeavors, as they have the potential to drive significant advancements in the field of UOWC security. By addressing these outstanding problems, researchers can work towards developing innovative solutions such as

QKD, OCDMA, IRS and mixed/hybrid RF/Acoustic/FSO/UOWC systems that enhance the resilience and robustness of UOWC systems in the face of diverse security threats.

REFERENCES

[1]. H. Kaushal and G. Kaddoum, *"Underwater optical wireless communication,"* IEEE Access, Vol 4, pp 1518–1547, (2016).

[2]. M.F. Ali et al., *"Recent Advances and Future Directions on Underwater Wireless Communications,"* Archives of Computational Methods in Engineering, pp 1-34, (2019).

[3]. W. Stallings, *"Cryptography and Network Security: Principles and Practice,"* 6th ed. Englewood Cliffs, NJ, USA: Prentice-Hall, (2013).

[4]. L. Gomes, *"Quantum computing: Both here and not here,"* IEEE Spectr., Vol 55, No 4, pp 42–47, Apr. (2018).

[5]. A. Mukherjee et al., *"Principles of physical layer security in multiuser wireless networks: A survey,"* IEEE Commun. Surveys Tuts., Vol 16, No 3, pp 1550–1573, 3rd Quart, (2014).

[6]. D. Wyner, *"The wire-tap channel,"* Bell Syst. Tech. J., Vol 54, No 8, pp 1355–1387, (1975).

[7]. J. Zhang et al., *"Key generation from wireless channels: A review,"* IEEE Access, Vol 4, pp 614–626, Mar. (2016).

[8]. T. Kukita, H. Takada, and K. Inoue, *"Macroscopic differential phase shift quantum key distribution using an optically pre-amplified receiver,"* Jpn. J. Appl. Phys., Vol 49, No 122801, (2010).

[9]. T. A. Eriksson et al., *"Secret key rates for intensity-modulated dual-threshold detection key distribution under individual beam splitting attacks,"* Opt. Express, Vol 26, No 16, pp 20409–20419, (2018).

[10]. P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng, and A. T. Pham, *"Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver,"* IEEE Access, Vol 6, pp 4159–4175, Feb. (2018).

[11]. H. Takenaka et al., *"Satellite-to-ground quantum-limited communication using a 50-kg-class microsatellite,"* Nature Photon., Vol 11, No 8, pp 502–508, (2017).

[12]. Y. Zou et al., *"A survey on wireless security: Technical challenges, recent advances, and future trends,"* Proc. of the IEEE, Vol 104, (2016).

[13]. Nasir Saeed et al., *"Underwater optical wireless communications, networking, and localization: A survey,"* Ad Hoc Networks, Vol 94, 101935, (2019).

[14]. Gabriel et al., *"Channel modeling for underwater optical communication,"* in 2011 IEEE GLOBECOM Workshops (GC Wkshps), pp 833–837, (2011).

[15]. T. J. Petzold, *"Volume Scattering Functions for selected ocean waters,"* La Jolla Ca Visibility Lab, Scripps Institute of Oceanography, San Diego, CA, SIO Ref. 72–78, (1927).

[16]. Khalighi et al., *"Fading reduction by aperture averaging and spatial diversity in optical wireless systems,"* Journal of Optical Communications and Networking 1(6), 580–59357, pp 7600–7608, (2009).

[17]. A. Huang et al., *"Error performance of underwater wireless optical communications with spatial diversity under turbulence channels,"* Appl. Opt., Vol 57, pp 7600–7608, (2018).

[18]. Gaofeng Pan, Jia Ye and Zhiguo Ding, *"Outage capacity optimization for free-space optical links with pointing errors,"* Journal of Lightwave Technology 25(7), 1702–1710, (2007).

[19]. L. Wang et al., *" On Secure VLC Systems with Spatially Random Terminals,"* IEEE Communications Letters, 21(3), 492-495, (2017).

[20]. Elmehdi Illi et al., *"Physical Layer Security of a Dual-Hop Regenerative Mixed RF/UOW System,"* IEEE Transactions on Sustainable Computing, Vol 6, (2018).

[21]. Sheikh Habibul Islam et al., *"On Secrecy Performance of Mixed Generalized Gamma and Málaga RF-FSO Variable Gain Relaying Channel,"* IEEE Access, Vol 8, pp 104127-104138, (2020).

[22]. Yingbin Liang, H. Vincent Poor and Shlomo Shamai, *"Information Theoretic Security,"* Foundations and Trends® in Communications and Information Theory, Vol 5, No 4–5, pp 355-580, (2009).

[23]. Goldsmith, A., *"Wireless communications,"* Cambridge university press, (2005).

[24]. Bloch, M., & Barros, J., *"Physical-layer security: From information theory to security engineering,"* Cambridge University Press, (2011).

[25]. Scarani et al., *"The security of practical quantum key distribution,"* Reviews of Modern Physics, 81(3), 1301, (2009).

[26]. Ambrish Kumar et al., *"Security Performance Analysis of a NOMA-Assisted Underwater VLC System*

Under Imprecise Channel Estimations," IEEE Access, Vol 10, (2022).
[27]. Jialiang Zhang, Guanjun Gao, Jie Zhang, and Yonggang Guo, *"Secure and noise-resistant underwater wireless optical communication based on spectrum spread and encrypted OFDM modulation,"* Optics Express, Vol 30, No 10 17140, (2022).
[28]. Ji Du et al., *"Experimental demonstration of 50-m/5-Gbps underwater optical wireless communication with low-complexity chaotic encryption,"* Optics Express, Vol 29, No 2, 783, (2021).
[29]. T Hossain et al., *"On the Physical Layer Security Performance over RIS-aided Dual-hop RF-UOWC Mixed Network,"* IEEE Transactions on Vehicular Technology, Vol 72, Issue 2, (2022).
[30]. Yi Lou et al., *"Physical-Layer Security for Two-Hop Air-to-Underwater Communication Systems With Fixed-Gain Amplify-and-Forward Relaying,"* CoRR, (2020).
[31]. Moloy Kumar Ghosh et al., *"Physical Layer Security in Mixed UOWC-RF Networks with Energy Harvesting Relay against Multiple Eavesdroppers,"* IEEE Open Journal of the Commutications Society, (2024).
[32]. A. S. M. Badrudduza et al., *"Security at the Physical Layer Over GG Fading and mEGG Turbulence Induced RF-UOWC Mixed System,"* IEEE Access, Vol 9, (2021).
[33]. Elmehdi Illi, Faissal El Bouanani, and Fouad Ayoub, *"Physical Layer Security of an Amplify-and-Forward Energy Harvesting-based mixed RF/UOW System,"* 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), (2019).
[34]. Ahmed Samir et al., *"Performance Analysis of Dual-Hop Hybrid RF-UOWC NOMA Systems,"* Sensors, (2022).
[35]. Ying Guo et al., *"Trans-Media Continuous-Variable Quantum Key Distribution via Untrusted Entanglement Source,"* IEEE Photonics Journal, Vol 13, No 2, (2021).
[36]. Lei Gai et al., *"Secure underwater optical communications based on quantum technologies,"* 19th International Conference on Optical Communications and Networks (ICOCN), (2021).
[37]. Jeffrey Uhlmann, Marco Lanzagorta, Salvador E. Venegas-Andraca, *"Quantum Communications in the Maritime Environment,"* OCEANS 2015 - MTS/IEEE Washington, (2016).
[38]. Tarantino, Silvia; Cozzolino, Daniele, Rottwitt, Karsten, Bacco, Davide, *"Feasibility of Quantum Communications in Aquatic Scenario,"* 2018 IEEE Photonics Conference, (2018).
[39]. Amir Hossein Fahim Raou, Fmajid Safari and Murat Uysal, *"Performance analysis of quantum key distribution in underwater turbulence channels,"* Journal of the Optical Society of America B, Vol 37, No 2, (2020).
[40]. Shi-Cheng Zhao et al., *"Performance of underwater quantum key distribution with polarization encoding,"* Journal of the Optical Society of America A, Vol 36, No 5, (2019).
[41]. Burak Kebapci et al., *" Real-Time Implementation of an Underwater Quantum Key Distribution System,"* 2022 Sixth Underwater Communications and Networking Conference (UComms), (2022).
[42]. Farhad Akhoundi, Jawad A. Salehi, and Arvin Tashakori, *"Cellular Underwater Wireless Optical CDMA Network: Performance Analysis and Implementation Concepts,"* IEEE Transactions on Communications, (2015).
[43]. Farhad Akhoundi et al., *"Cellular Underwater Wireless Optical CDMA Network: Potentials and Challenges,"* IEEE Access, Vol 4, (2016).
[44]. Mir Mehedi Al Hammadi and Md. Jahedul Islam, *"Performance Analysis of Underwater Wireless Optical CDMA System,"* 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT), (2018).
[45]. Nguyen Van Thang, Dang Tien Sy, and Pham Thi Thuy Hien, *"Physical Layer Security for Multihop Underwater Wireless Optical Communications Using Optical CDMA,"* Journal of Science and Technology on Information and Communications, No 03 (CS.01), pp 17-27, (2023).
[46]. Laszlo Gyongyosi, Laszlo Bacsardi and Sandor Imre, *"A Survey on Quantum Key Distribution,"* Infocommunications Journal, Vol XI, (2019).
[47]. Purva Sharma et al., *"Quantum Key Distribution Secured Optical Networks: A Survey,"* IEEE Open Journal of the Communications Society, Vol 2, (2021).
[48]. Shicheng Zhao et al., *"Experimental investigation of quantum key distribution over a water channel,"* Applied Optics, (2019).
[49]. Chien-Chi Kao, Yi-Shan Lin, Geng-De Wu, Chun-Ju Huang, *"A Study of Applications, Challenges, and Channel Models on the Internet of Underwater Things,"* 2017 International Conference on

Applied System Innovation (ICASI), (2017).
[50]. Zou Wei, H. M. H. Shalaby and H. Ghafouri-Shiraz, *"Modified Quadratic Congruence Codes for Fiber Bragg-Grating-Based Spectral-Amplitude-Coding Optical CDMA Systems,"* Journal of lightwave technology, Vol 19, (2001).
[51]. Ragini Verma, Anshul Jaiswal and Anh T. Pham, *"Design and Analysis of Octa-phase Shift Keying based Quantum Key Distribution System,"* IEEE Communications Letters, Vol 27, (2023).
[52]. Saeed, A., et al., *"Optical Wireless Communications: Principles and Practices,"* CRC Press, (2019).
[53]. Vu Tuan Lam, Do Trung Anh, N. Thang, Tien Dang Sy, Dang The Ngoc, *"Outage Performance of IRS-Assisted Underwater Optical Wireless Communication Systems over Combined Channel Model,"* 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Montreal, QC, Canada, (2023).
[54]. Hongjiang Lei et al., *"Performance Analysis of Dual-Hop RF-UWOC Systems,"* IEEE Photonics Journal, Vol 12, (2020).

TÓM TẮT

Bảo mật lớp vật lý trong truyền thông quang không dây dưới nước: Tổng quan ngắn gọn

Truyền thông quang không dây dưới nước là một giải pháp thay thế đang được phát triển để đáp ứng nhu cầu ngày càng tăng về kết nối tốc độ cao trong đại dương và biển cả. Truyền thông quang không dây (OWC) an toàn hơn và ít bị nghe trộm hơn so với truyền thông sóng âm hoặc truyền thông tần số vô tuyến (RF) do phạm vi chùm tia quang hẹp và phụ thuộc vào các thành phần trong tầm nhìn trực tiếp. Tuy nhiên, sự tồn tại của một kẻ nghe trộm tiềm tàng có thể làm tổn hại đến mức độ bảo mật đạt được bởi các mạng OWC. Bài báo này cung cấp một cái nhìn tổng quan ngắn gọn về các nghiên cứu mới nhất được thực hiện về bảo mật lớp vật lý (PLS) trong truyền thông quang không dây dưới nước (UOWC). Hơn nữa, công trình này trình bày các vấn đề chưa được giải quyết, các phương pháp để nâng cao hiệu suất bảo mật và các lĩnh vực tiềm năng để nghiên cứu sâu hơn.

Keywords: Bảo mật lớp vật lý (PLS); Truyền thông quang không dây dưới nước (UOWC); Kỹ thuật nâng cao hiệu năng bảo mật.