Secrecy performance analysis of a IRS-assisted underwater optical wireless communication system

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, 96A Tran Phu, Ha Dong, Hanoi, Vietnam.
[*]Corresponding author: sydt.start18@gmail.com
Received 07 Mar. 2024; Revised 14 May 2024; Accepted 12 Jun. 2024; Published 25 Jun. 2024.
DOI: https://doi.org/10.54939/1859-1043.j.mst.96.2024.21-29

ABSTRACT

In response to the dearth of radio frequency (RF) equivalents, there has been a recent surge in interest in optical wireless communication in underwater environments. To ensure a strong line-of-sight (LOS) connection, the intelligent reflecting surface (IRS) is installed to create a virtual LOS. Then, the first part of this study looks into the security of underwater optical wireless communication (UOWC) in relation to a number of real-world phenomena, including oceanic propagation loss, oceanic turbulence, and IRS-induced geometric loss. Then, a wiretap channel with three authorized users - a reputable broadcaster named Alice (the submarine), a law-abiding user named Bob, and an eavesdropper named Eve - is examined over turbulent channels that exhibit the Log-normal distribution. Furthermore, our study derives the closed-form formulas for the secrecy performance measures, secrecy outage probability, and secrecy throughput. Finally, the numerical results show how the impact of oceanic turbulence-induced fading and distance between Bob's and Eve's positions on the secrecy system performance.

Keywords: Physical layer security (PLS); Underwater Optical Wireless Communication (UOWC); IRS-Assisted UOWC system; Intelligent Reflecting Surface (IRS).

1. INTRODUCTION

The performance requirements of underwater communication are rising in tandem with the growing number of underwater activities, including navigation, fisheries, undersea oil exploration, and oceanic military operations. Currently, underwater radio frequency (RF), underwater acoustic, and underwater optical wireless communication (UOWC) are the most widely utilized underwater wireless communication techniques [1]. Signal attenuation, which results from high water conductivity at high frequencies, restricts the ability of radio-frequency waves to propagate in water. Although the bandwidth of acoustic waves is constrained, they can carry data over greater distances. Because of its high transmission bandwidth, security, and efficiency, UOWC is seen as an effective option [2]. However, underwater passageways are so complicated, it has a lot of difficulties. One major worry with UOWC is the obstructions, like sea mountains and marine life, e.g., ocean animals, which have the potential to totally block the optical links. Using the sea surface to enable reflecting communication is one way to address this problem [3]. This solution's primary flaw is its inability to fully reflect the signal to the receiver. Intelligent reflecting surfaces (IRS) have surfaced as a viable means of circumventing obstructions and extending the reach of communication [4, 5]. It works well for designing and planning maritime networks when IRS is mounted on already-existing infrastructure, such as ships, buoys, lighthouses, etc. In addition to the flexible deployment, less complex hardware is needed in comparison to traditional relay nodes. Therefore, the combination of UOWC and IRS is a promising technology to enable a new chapter for the next generation in the underwater environment.

A small amount of research has been done on privacy and security, despite extensive literature research on the design, performance analysis, and viability of UOWC-based IRS systems. Since

the beam footprint at the receiver in an UOWC is sufficiently small, it is difficult for malevolent users to eavesdrop on communications because of the relatively short link ranges (a few dozen meters to a few hundred). On the other hand, transmission distances in the UOWC scenario are typically several hundred meters or longer. The beam footprint at the receiver plane can, therefore, have a radius of several meters. An eavesdropper (Eve) may be in the beam footprint without the legitimate party noticing, which presents a serious security risk. Key-based cryptography is used at the upper levels of the OSI model to carry out traditional security procedures.

As part of potential security research directions, physical layer (PHY) security is becoming increasingly popular as a new way to stop eavesdropping without requiring advanced data encryption methods. A few studies have examined the secrecy performance of FSO-based SatCom in the literature in this area [6-9]. A series of studies have highlighted the security vulnerabilities in underwater wireless optical communications (UWOC). In [6] and [7], both underscore the potential for information leakage and eavesdropping in UWOC systems, with Kong's work demonstrating successful tapping of a 5-MHz signal at various underwater distances. These findings are further supported by [8] and [9], who emphasize the need for efficient and reliable security mechanisms in underwater wireless communication networks (UWCNs). The unique characteristics of the underwater acoustic communication channel, such as high bit error rates and large propagation delays, further intensify these security challenges.

In contrast to these previous studies, this one examines an all-optical underwater communication wiretap channel. We consider a wiretap channel, as illustrated in Fig. 1, that consists of a legitimate submarine (Alice), a validly received submarine (Bob), and an eavesdropper (Eve), such as a diver or small autonomous underwater vehicle (AUV) outfitted with a base station that may travel within the beam footprint area. Next, we derive new closed-form expressions for the secrecy outage probability (SOP) and secrecy throughput (ST), taking into account oceanic propagation loss, oceanic turbulence, and IRS-induced geometric loss.

Overall, in turbulence settings, as confirmed in [5], the log-normal distribution shows a superior fit to the experimental data compared to the other models in the literature. Numerous simulations were conducted to demonstrate the impact of various system and environmental factors on the secrecy performance of the IRS-assisted UOWC system.

2. SYSTEM AND CHANNEL MODELS

An IRS-assisted UOWC system, comprised of a source node (S - Alice) placed on a submarine or AUV, an IRS-based relay node (R) placed on a ship or fixed floating station on the sea surface, and a destination node (D - Bob) placed on a remotely operated underwater vehicle (ROUV) in deep under sea water is proposed. Assume that from node S, we cannot see node D because between these two nodes is blocked by the sea mountain. So, there is no direct link between node S and node D. An intelligent reflecting surface is implemented on a buoy or a boat’s hull to ensure the communication link between node S and node D. The specific scenario is shown in figure 1, the appearance of the eavesdropper is described as trying to approach node D to obtain a reflective optical signal from IRS on node R to node D. The end-to-end communication process is conducted in the presence of a potential eavesdropper, designated as node E (Eve). It is hypothesized that the eavesdropper is either a diver or an underwater vehicle strategically positioned near node D to facilitate the interception and collection of the transmitted signals for unauthorized access.

In case each optical IRS has perfect phase compensation, the received signal at node D can be described as follows:

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

where s is the transmitted signal from source node S, h denotes the oceanic channel coefficient,

and $n \sim N(0, \sigma_n^2)$ is the additive white Gaussian noise (AWGN) with zero mean and variance of σ_n^2.

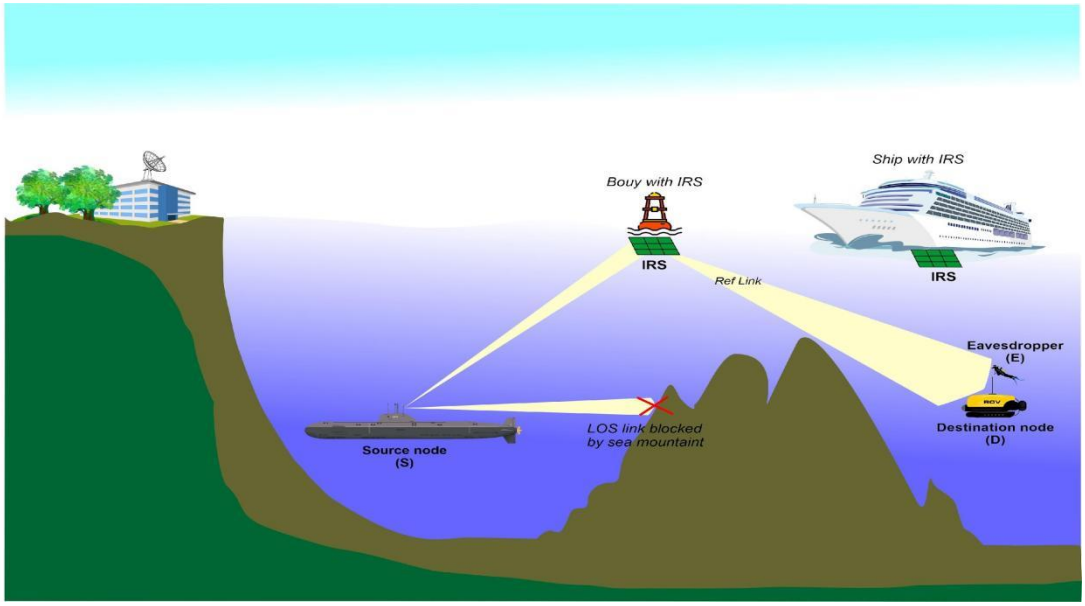

Figure 1. *An IRS-UOWC system model.*

Considering the oceanic channel consists of three components: oceanic propagation loss, oceanic turbulence, and IRS-induced geometric loss. The oceanic channel coefficient, h_U [1], can be expressed as:

$$h_U = h_p h_t h_{IRS}, \tag{2}$$

where h_p is the oceanic propagation loss and can be considered as constant in a bit duration while h_t and h_{IRS} are random variables due to the effect of turbulence and vibration.

The value of oceanic propagation loss major depends on the types of oceanic water and the link transmission distance between the source node and destination node d. Typically, some water type are considered including pure sea, clear ocean, coastal water and harbor [5, 10, 11], so h_p can be determined as:

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

where c_e denotes the beam extinction coefficient [5]. ρ, θ_F and D_R are correction coefficient, full optical divergence angle, and receiver aperture diameter, respectively.

Besides, one of the important effects cannot be ignored when implementing UOWC that is oceanic turbulence. The phenomenon of oceanic turbulence arises from changes in water temperature and salinity, leading to variations in the received power. The strength of this turbulence can be measured through the refractive index of the water.

In this research, we aim to utilize the log-normal distribution to model oceanic turbulence, and

[1] The subscript 'U' is used to denote Bob and Eves as users in general. When necessary, the subscript 'B' is used to refer to Bob while 'E' is used to refer to Eve.

the probability density function (PDF) and the cumulative distribution function (CDF) are represented by:

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

$$F_{h_t}(h_t) = \frac{1}{2}\text{erfc}\left(-\frac{\ln(h_t) - 2\mu_t}{\sqrt{8\sigma_t^2}}\right), \tag{5}$$

where μ_t and σ_t^2 represent, respectively, the log-amplitude coefficient's mean and variance. The fading amplitude is normalized and represented as $E[h_t] = 1$, which suggests that $\mu_t = -\sigma_t^2$, adheres to the constraint. This normalization ensures that the fading coefficient does not change the average power value. The correlation between log-amplitude variance and the scintillation index is given by $\sigma_t^2 = 0.25\ln\left(1+\sigma_R^2\right)$, where σ_R^2 is the Rytov variance and can be refereed from [12].

Besides, one of the technological breakthroughs deployed in this research is the IRS. Therefore, the influence of IRS, specifically the beam attenuation when transmitted through IRS is investigated in this work. Since the direct link is obstructed by sea mountains or occlusion, the IRS is installed in the buoy or ship in the system under consideration in order to reflect the optical signal from a submarine to another submarine. It is impractical to presume that node D's initial placement is in the middle of the beam footprint due to the movement of the IRS caused by waves on the ocean's surface and/or undersea mobility.

As a matter of fact, the wave on the ocean's surface causes the buoy or ship to move easily, which causes an alignment error between the targeted submarine's receiver and the reflected beam at the IRS. The fraction of gathered power at the targeted submarine with an aperture radius of D_t can be roughly calculated using the Gaussian beam profile as:

$$h_{irs} \approx A_0 \exp\left(-\frac{2u^2}{tw_L^2}\right)\exp\left(-\frac{2d_E^2}{tw_L^2}\right), \tag{6}$$

where u denotes the misalignment between the center of the beam footprint from IRS and the center of their detector. $A_0 = \left[\exp(v)\right]^2$, $t = \dfrac{\sqrt{\pi}erf(v)}{2v\exp\left(-v^2\right)\cos^2(\theta_{rl})}$, $v = \dfrac{\sqrt{2}\cos(\theta_{rl})D_t}{w_L}$, and θ_{rl} is the angle between the reflected beam and the normal vector of the lens at the target's submarine. Besides, $w_L = w_u\sqrt{\left(1-\dfrac{d_2}{F_0}\right)+\left(\dfrac{\lambda d_2}{\pi w_u^2}\right)}$ is the optical beam waist at the destination's detector with F_0 denoted the radius of curvature and d_2 is the link length from IRS to the destination while d_1 is a transmission distance from source to the IRS. Furthermore, d_E is the distance between Eve's and Bob's location on the receiver plane.

3. SECRECY PERFORMANCE ANALYSIS

The secrecy performance of the IRS-assisted UOWC system is examined over the given fading channel in this section. Two important secure metrics that are derived in a closed-form expression are the secrecy outage probability (SOP) and secrecy throughput (ST).

3.1. Secrecy Outage Probability (SOP)

SOP is one of the fundamental secrecy benchmarks, which shows the level of privacy in any communication system. It is defined as the probability that instantaneous secrecy capacity falls below a target secrecy rate, denoted R_s, and can be expressed as:

$$\begin{aligned} \mathrm{SOP} &= \Pr\{C_s(\gamma_B,\gamma_E) \le R_s\} \\ &= \Pr\left[\log_2\left(\frac{1+4\bar{\gamma}_B h_B^2}{1+4\bar{\gamma}_E h_E^2}\right) < R_s\right] \\ &= \int_0^\infty F_{h_B}\left(\sqrt{\frac{2^{R_s}\left(1+4\bar{\gamma}_E h_E^2\right)-1}{4\bar{\gamma}_B}}\right) f_{h_E}\left(h_E\right) dh_E \end{aligned} \quad , \tag{7}$$

Since an exact closed-form expression for (7) is difficult to obtain, we aim at deriving a lower bound for the SOP. Specifically, as $\frac{2^{R_s}\left(1+4\bar{\gamma}_E h_E^2\right)-1}{4\bar{\gamma}_B} > \frac{2^{R_s}\bar{\gamma}_E h_E^2}{\bar{\gamma}_B}$, a lower bound for (7) can be determined as:

$$\begin{aligned} \mathrm{SOP}_{\mathrm{LB}} &= \int_0^\infty F_{h_B}\left(2^{\frac{R_s}{2}}\sqrt{\frac{\bar{\gamma}_E}{\bar{\gamma}_B}}h_E\right) f_{h_E}\left(h_E\right) dh_E \\ &= \int_0^\infty \frac{1}{2\sqrt{8\pi\sigma_t^2}\,h_E} \exp\left[-\frac{\left(\ln\left(\frac{h_E}{h_a h_{ris}}\right)-2\mu_t\right)^2}{8\sigma_t^2}\right] \\ &\quad \times \mathrm{erfc}\left[-\frac{1}{\sqrt{8\sigma_t^2}}\left(\ln\left(2^{\frac{R_s}{2}}\sqrt{\frac{\bar{\gamma}_E}{\bar{\gamma}_B}}\frac{h_E}{h_a h_{ris}}\right)-2\mu_t\right)\right] dh_E \end{aligned} \quad , \tag{8}$$

To obtain the approximation of (8), the Gauss-Hermit quadrature method can be applied. Particularly, by making the change of variable $z = \frac{\ln\left(\frac{h_E}{h_a h_{ris}}\right)-2\mu_t}{\sqrt{8\sigma_t^2}}$, and then (8) is written in the form of $\int_{-\infty}^{\infty} \exp\left(-z^2\right) g\left(z\right) dz$ in which $g\left(z\right)$ is a function of the variable z [5]. Form this step, we can utilize the Gauss-Hermit quadrature as follow $\int_{-\infty}^{\infty} \exp\left(-z^2\right) g\left(z\right) dz \approx \sum_{i=1}^{N} w_i g\left(x_i\right)$; then, the closed-form expression of $\mathrm{SOP}_{\mathrm{LB}}$ can be derived as:

$$\mathrm{SOP}_{\mathrm{LB}} = \sum_{i=1}^{n} \frac{1}{2\sqrt{\pi}} w_i \mathrm{erfc}\left[-\frac{1}{\sqrt{8\sigma_t^2}}\left(\ln\left(2^{\frac{R_s}{2}}\sqrt{\frac{\bar{\gamma}_E}{\bar{\gamma}_B}}\exp\left(2\mu_t + z_i\sqrt{8\sigma_t^2}\right)\right)-2\mu_t\right)\right], \tag{9}$$

3.2. Secrecy Throughput (ST)

This parameter provides a significance for both reliability an secrecy of the system. It shows the multiplication of target secrecy rate with the probability of simultaneous guarantee of both reliability and secrecy constraint and can be written as:

$$\mathrm{ST} = R_s(1-\mathrm{SOP}_{\mathrm{LB}}), \tag{10}$$

4. NUMERICAL RESULTS

Table 1. *System parameters.*

Name	Symbol	Value
Optical wavelength	λ	450 nm
Transmission distance	d_{total}	30 m
Aperture radius	D_t	10 cm
Beam extinction coefficient	c_e	0.17
Correction coefficient	ρ	0.13
Full optical divergence angle	θ_F	$\pi/30$
Gaussian noise variance	σ_n^2	10^{-14}
IRS jitter	σ_{irs}^2	10^{-4}
IRS size	D_{irs}	10 cm
Transmitted power	P_t	20 dBm
Target secrecy rate	R_s	0.5

The impact of the system parameters on the secrecy performance is demonstrated in this part through the presentation of simulation data. The simulation parameters are listed in table 1 unless otherwise specified. Simulation programs using MATLAB® are also provided to validate the analytical results. Using the system parameters outlined in table 1, the simulation is done by using a discrete-event simulator.

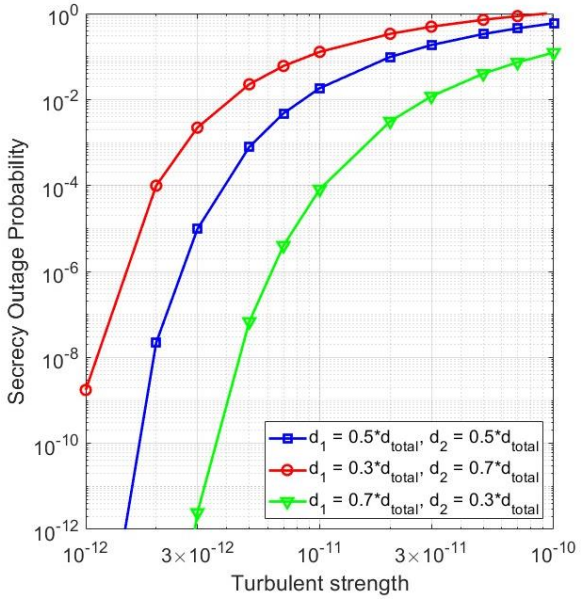

Figure 2. *SOP versus the impact of the turbulence strength with implementing different buoy-installed IRS positions.*

First, it depicts the secrecy outage performance by implementing different buoy-installed IRS positions over the range of the turbulence strength from 10^{-12} to 10^{-10} as shown in Fig. 2. Once the optical beam reaches the IRS surface, the value of the virtual divergence angle indicates the IRS position.

This resulted in the distance ratio between the source and IRS, denoted as d_1, and the destination and IRS, denoted as d_2, a crucial metric that must be examined to determine the current state of the evaluated system's secrecy outage likelihood. Unsurprisingly, secrecy outage probability increases with higher turbulence strength. One noteworthy finding from the analysis is that system security performs better when IRS is positioned close to the destination.

For example, from this result, we can easily observe that the SOP can reach 10^{-4} under the turbulent strength of $C_n^2 = 2.017\times10^{-12}$, $C_n^2 = 3.983\times10^{-12}$, and $C_n^2 = 1.043\times10^{-11}$ corresponding to the ratio of $d_1/d_{total} = 0.3$, $d_1/d_{total} = 0.5$, and $d_1/d_{total} = 0.7$.

Next, we explore in Fig. 3 the impact of the distance between Eve's and Bob's positions, denoted as d_E, on the SOP with two different total transmission distances of 50 m and 100 m, and two cases of oceanic environment conditions with the turbulence strength of 10^{-10} and 10^{-11}. From the figure, in fact, we can see that the farther distance of d_E, the more reliable the system becomes, meaning security is significantly increased. The reason behind this can be found in Eq. (6); If the distance between Eve's and Bob's location is longer, the effect of geometric loss increased.

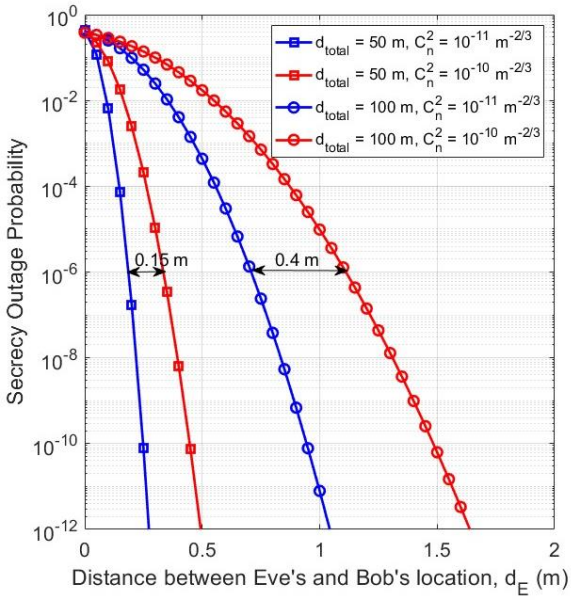

Figure 3. *The relationship between SOP and distance between Bob and Eve, d_E, with the two cases of the total transmission distance of 50 m and 100 m, and the considered turbulence strength of 10^{-10} and 10^{-11}.*

Additionally, as discussed in the previous results, the total transmission distance of the underwater optical communication system supported by IRS has a strong influence on the SOP. In this result, we can see that for the same value of total distance, d_{total} of 50 m or 100 m, the oceanic turbulence clearly shows an influence in the case that the total propagation distance is long, $d_{total} = 100$ m, instead of short $d_{total} = 50$ m.

For instance, to achieve the target SOP of 10^{-6}, a total system transmission distance of 50 m, in more unfavorable cases (such as stronger turbulent conditions), the legitimate receiver needs to be

0.15 meters further away from the eavesdropper while this distance will increase to 0.4 m in case the communication distance is 100 m.

Finally, we illustrate the secrecy throughput (ST) with respect to the target secrecy rate, denoted as R_s, in different oceanic turbulence conditions, denoted as C_n^2, and the different distance between Eve's and Bob's locations, denoted as d_E, as shown in Fig. 4. Based on the derivation in Eq. (10), we observed that the ST is improved by increasing the target secrecy rate because it can mitigate the influence of the turbulence strength as well as the Eve's positions.

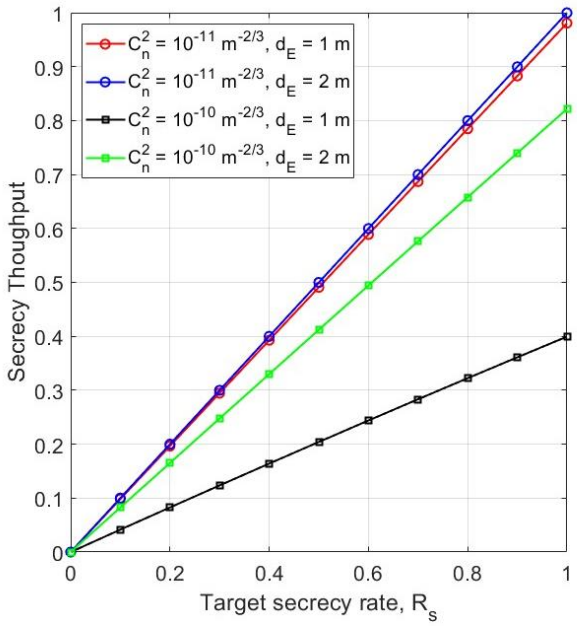

Figure 4. *Secrecy throughput versus the target secrecy rate in different turbulence conditions and different distances between Eve's and Bob's locations.*

However this only seems to be true under moderate turbulence $C_n^2 = 10^{-11}$, ST does not seem to improve when Eve is away from Bob, while ST improves significantly under strong ocean turbulence $C_n^2 = 10^{-12}$ under the same conditions when Eve moves 1 m further away from Bob.

5. CONCLUSIONS

In this article, we examined the PHY security concerns for the IRS-based UOWC system, taking into account physical layer impairments including oceanic propagation loss, oceanic turbulence, and IRS-induced geometric loss. Specifically, the log-normal distribution is used to model oceanic turbulence, considering the impact of the relative positions of Bob and Eve on the secrecy performance of UOWC systems. Furthermore, this study derives the secrecy outage probability and secrecy throughput in closed-form expressions. The numerical results highlight the impact of Eve's position on secrecy performance and show the severe effect of turbulence strength.

Acknowledgments: The work of Nguyen Van Thang was supported by the Posts and Telecommunications Institute of Technology (Vietnam) under Grant No. 15-2024-HV-VT1.

REFERENCES

[1]. Hassan, W., Sabril, M.S., Jasman, F, *"Experimental study of light wave propagation for underwater optical wireless communication (UOWC),"* J. Commun. 17(1), 23–29, (2022).

[2]. Lian, J., Gao, Y., Wu, P., et al.: *"Orthogonal frequency division multiplexing techniques comparison for underwater optical wireless communication systems,"* Sensors 19(1), 160–179, (2019).

[3]. M. F. Ali, D. N. K. Jayakody, and Y. Li, *"Recent trends in underwater visible light communication (uvlc) systems,"* IEEE Access, vol. 10, pp. 22169–22225, (2022).
[4]. R. P. Naik and W.-Y. Chung, *"Evaluation of reconfigurable intelligent surface-assisted underwater wireless optical communication system,"* Journal of Lightwave Technology, vol. 40, no. 13, pp. 4257–4267, (2022).
[5]. Tuan-Lam Vu, Trung-Anh Do, Thang. V. Nguyen, Tien-Sy Dang, and Ngoc T. Dang, *"Outage Performance of IRS-Assisted Underwater Optical Wireless Communication Systems over Combined Channel Model,"* In the Proc. of the IEEE 19th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Montreal, Canada, pp. 318-323, (2023).
[6]. Meiwei Kong, Jiongliang Wang, Yifei Chen, Tariq Ali, Rohail Sarwar, Yang Qiu, Shilian Wang, Jun Han, and Jing Xu, *"Security weaknesses of underwater wireless optical communication,"* Opt. Express 25, 21509-21518, (2017).
[7]. M. C. Domingo, *"Securing underwater wireless communication Networks,"* in IEEE Wireless Communications, vol. 18, no. 1, pp. 22-28, (2011).
[8]. Waqas Aman and Saif Al-Kuwari and Ambrish Kumar and Muhammad Mahboob Ur Rahman and Muhammad Muzzammil, *"Underwater and Air-Water Wireless Communication: State-of-the-art, Channel Characteristics, Security, and Open Problems,"* arXiv, (2022).
[9]. Kasture, Suraj S. and Nikhil Gudpelliwar. *"Securing Underwater Wireless Communication Networks-Literature Review,"* International Journal of Scientific & Engineering Research, Volume 4, Issue 12, (2013).
[10]. M. Elamassie, S. M. Sait and M. Uysal, *"Effect of Sea Waves on Vertical Underwater Visible Light Communication Links,"* in IEEE Journal of Oceanic Engineering, vol. 48, no. 2, pp. 515-525, (2023).
[11]. I. C. Ijeh, M. A. Khalighi, M. Elamassie, S. Hranilovic and M. Uysal, *"Outage probability analysis of a vertical underwater wireless optical link subject to oceanic turbulence and pointing errors,"* in Journal of Optical Communications and Networking, vol. 14, no. 6, pp. 439-453, (2022).
[12]. A. Huang, L. Tao, C. Wang, and L. Zhang, *"Error performance of underwater wireless optical communications with spatial diversity under turbulence channels,"* Appl. Opt., vol. 57, pp. 7600–7608, (2018).

TÓM TẮT

Phân tích hiệu năng bảo mật của hệ thống truyền thông quang không dây dưới nước hỗ trợ bởi bề mặt phản xạ thông minh

Để giải quyết vấn đề dần khan hiếm tài nguyên tần số vô tuyến (RF) cho hoạt động thông tin liên lạc dưới nước, truyền thông quang không dây dưới nước (UOWC) gần đây đã dành được sự quan tâm rất lớn. Trong môi trường dưới nước phức tạp, nhiều vật cản, bề mặt phản xạ thông minh (IRS) đã được sử dụng để tạo liên kết LOS ảo, hỗ trợ kết nối truyền thông ổn định. Nghiên cứu này đã tiến hành xem xét tính bảo mật của hệ thống UOWC hỗ trợ bởi IRS trong môi trường truyền thông dưới nước thực tế, bao gồm suy hao lan truyền trong đại dương, nhiễu loạn đại dương và suy hao hình học do IRS gây ra. Một hệ thống truyền thông giữa hai người dùng hợp pháp là Alice (tàu ngầm) và Bob (tàu do thám) đã được thiết lập, với mô hình kênh truyền là kênh hỗn loạn theo phân phối Log-normal. Xét sự can thiệp của một kẻ nghe lén là Eve, nghiên cứu đưa ra công thức dạng đóng cho thước đo hiệu quả bảo mật, xác suất ngừng bảo mật và thông lượng bảo mật. Kết quả mô phỏng cho thấy tác động của fading do nhiễu loạn đại dương và khoảng cách giữa vị trí của Bob - Eve đối với hiệu quả bảo mật của hệ thống.

Từ khoá: Truyền thông quang không dây dưới nước UOWC; Bề mặt phản xạ thông minh IRS; Bảo mật lớp vật lý; Hệ thống IRS-UOWC.