Superposition Modulation for Physical Layer Security in Water-to-Air Visible Light Communication Systems

Qingqing Hu, Nuo Huang, and Chen Gong, *Senior Member, IEEE*

***Abstract*—In this paper, we propose a physical layer security (PLS) scheme based on superposition modulation for water-to-air (W2A) visible light communication (VLC). We characterize the high correlation between W2A and air-to-water (A2W) link gains from ray tracing simulation and experiments. The proposed scheme selects the modulation order and superposition parameter based on the high correlation between the W2A and A2W link gains. The scheme performance is studied by exploring its immunity against different types of attacks. Based on the link gains from real measurements, it is shown that under random attack Eve's SER exceeds 0.77 when Eve's signal-to-noise ratio (SNR) varies from 5 dB to 30 dB, and under correlated attack Eve's SER decreases only for a high correlation coefficient when Eve is close enough to Bob, which is unrealistic for eavesdropping. In addition, the entropy of potential set under post-processing attack is derived. For intelligent attack, two unsupervised algorithms, namely K-means clustering and expectation maximization (EM) algorithm, are adopted for modulation identification. The distributions of Eve' SER under all four attacks are investigated based on the measured link gains in the laboratory environment, which demonstrates that intelligent attack with K-means clustering possesses the highest eavesdropping capability. However, more numerical results show that for intelligent attack with K-means clustering under wavy water surface, the proportion of the case where Eve has a higher SER than Bob is lower than 0.5 only when Eve lies between Alice and Bob with small horizontal distance, which is unrealistic for eavesdropping operation.**

***Index Terms*—Physical layer security, water-to-air, visible light communication, superposition modulation, attacks.**

I. Introduction

RECENTLY, there has been a growing interest in developing air/water cross boundary communication technologies, as communicating across the ocean directly enables a variety of potential oceanographic and commercial applications [1]. However, the direct water/air cross-boundary communication faces many challenges [2]. For example, radio frequency (RF) wave experiences significant signal absorption [3] in water and the low speed of acoustic wave drastically reduces the data rate [4]. Therefore, visible light communication (VLC) has been considered as an attractive alternative for air/water cross boundary communication, due to its high transmission bandwidth and data rate under short-to-medium distance [5], [6].

Compared to laser diode (LD), light-emitting diode (LED) with a high divergence angle can alleviate the requirement of strict alignment and have a relatively low price, which facilitates mass deployments in the network. Due to inherent semi-broadcast nature of VLC channels, the information may be eavesdropped by unauthorized terminals under LED coverage [7]. In our previous work [8], we explored the secrecy performance for water-to-air (W2A) VLC via both simulation and experiment, which indicates that water surface fluctuations can cause information leakage.

On the other hand, to ensure the secrecy of information transmission, physical layer security (PLS) approaches against passive eavesdropper can be divided into signal-to-interference-plus-noise ratio (SINR)-based and complexity-based ones. The SINR-based (key-less) approaches mainly include channel coding, channel-based adaptation and injection of artificial noise [9], [10], [11], which can practically achieve perfect secrecy [12]. The complexity-based (key) approaches extract random keys from the legitimate channel to encipher data at the upper layers [13], [14], which is being increasingly challenged with the rapid development of computational power [15]. Existing physical layer security schemes for VLC systems mainly focused on beamforming [16], [17] or artificial noise generation [18], [19] with multiple LEDs in indoor static channels, which cannot be directly applied to dynamic W2A scenarios. To the best of the authors' knowledge, the security scheme for W2A-VLC has not been systematically investigated in previous studies.

In W2A-VLC systems, random fluctuation of water surface leads to the variation of channel gain, which provides a source of randomness. Therefore, the channel-based adaptation approach is considered in this work. Without the need for extra frequency and space resources (e.g., multiple subcarriers in [20] and multiple antennas in [21]), we propose a low-complexity

Manuscript received 3 November 2022; revised 2 January 2023; accepted 24 January 2023. Date of publication 27 January 2023; date of current version 16 May 2023. This work was supported in part by the National Natural Science Foundation of China under Grants 62171428 and 62101526, in part by the Key Program of National Natural Science Foundation of China under Grant 61631018, in part by the Key Research Program of Frontier Sciences of CAS under Grant QYZDY-SSW-JSC003, and in part by the Fundamental Research Funds for the Central Universities under Grant KY2100000118. *(Corresponding authors: Nuo Huang; Chen Gong.)*

The authors are with the Key Laboratory of Wireless-Optical Communications, Chinese Academy of Sciences, School of Information Science and Technology, University of Science and Technology of China, Hefei 230052, China (e-mail: ruixihu@mail.ustc.edu.cn; huangnuo@ustc.edu.cn; cgong821@ustc.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/JLT.2023.3240180.

Digital Object Identifier 10.1109/JLT.2023.3240180

and resource-constrained PLS scheme based on superposition modulation for W2A-VLC systems, which achieves secrecy based on channel randomness, the correlation between W2A and air-to-water (A2W) links, and signal diversity of superposition modulation. Firstly, to explore the feasibility of using channel correlation for security design, the correlation between W2A and A2W links is investigated by ray tracing simulation and experiment, which verifies that channel state information (CSI) can be obtained by performing implicit feedback in coherence time interval and be kept secret between Alice and Bob. Based on the high correlation in terms of the channel gain, the proposed scheme is performed in two steps. During the first step, the legitimate receiver Bob transmits the pilot signal at each coherent time, while underwater transmitter Alice estimates the A2W channel gain and calculates the W2A channel gain. Then, Alice selects the signal modulation order and superposition parameter based on the probed channel gain. The selection strategy for superposition parameters is to maximize the detection error probability of Eve under the premise that Bob's symbol error rate (SER) is lower than a certain threshold. Moreover, we consider four different attack models, and accordingly analyze Eve's SER for both random and correlated attacks. It is shown that under random attack Eve's SER exceeds 0.77 when Eve's signal-to-noise ratio (SNR) varies from 5 dB to 30 dB, and under correlated attack Eve's SER decreases only under a high correlation coefficient when Eve is close enough to Bob, which is unrealistic for eavesdropping. In addition, the entropy of potential set under the post-processing attack is derived and the complexity of successful cracking increases with the modulation set size. Finally, we consider intelligent attack with two unsupervised algorithms, namely K-means clustering and expectation maximization (EM) algorithm, for modulation identification. The secrecy performance of the proposed modulation is evaluated based on the measured link gains in the laboratory environment. It is demonstrated that intelligent attack with K-means clustering possesses the highest eavesdropping capability. The contributions of this paper can be summarized comprehensively as follows:

1) We propose a PLS scheme against passive eavesdropper for dynamic W2A-VLC scenarios, which has not been systematically investigated in previous studies. The proposed security scheme achieves secrecy based on channel randomness, the correlation between W2A and A2W links, and signal diversity of superposition modulation, which is a channel-based adaptation approach without the need for extra frequency and space resources.
2) We investigate the correlation between W2A and A2W links by ray tracing simulation and experiment, which validates the feasibility of implicit feedback for CSI in coherence time interval and achieves the confidentiality between Alice and Bob using the CSI-based security scheme.
3) We explore the secrecy performance of the proposed security scheme by analyzing Eve's SER under four different attacks. We optimize the superposition parameter to maximize the detection error probability of Eve while considering the cases of accurate CSI known or unknown by Alice.
4) We adopt the measured link gains from the experimental results to evaluate the secrecy performance of the proposed security scheme. It is demonstrated that the probabilities of Eve's SER higher than Bob's exceed 0.9 for random, correlated, and post-processing attacks. For K-means-based intelligent attack, the insecure region of Eve's SER higher than Bob's with probability lower than 0.5 is only located between Alice and Bob with small horizontal distance, which is unrealistic for eavesdropping operation.

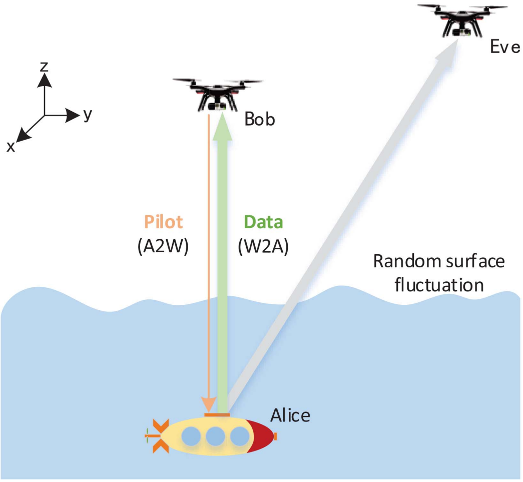


Fig. 1. Illustration of the considered W2A-VLC system.

The remainder of this paper is organized as follows. In Section II, we introduce the W2A-VLC system model and investigate the correlation of W2A and A2W link gains via both ray tracing simulation and experiment. In Section III, we propose a PLS scheme by adopting superposition modulation based on high correlation between the W2A and A2W link gains, and investigate the demodulating performance. In Section IV, we study the scheme performance by exploring its immunity against different types of attacks, namely, random attack, correlated attack, post-processing attack and intelligent attack. In Section V, we optimize the superposition parameter to maximize the detection error probability of Eve. In Section VI, we numerically evaluate Eve' SER under all four attacks based on the measured link gains in the laboratory environment, compare the SER distributions for Bob and Eve, and characterize the insecure region. Finally, we conclude this work in Section VII.

II. System Model

A. System Model

We consider a W2A-VLC system as shown in Fig. 1. An underwater submarine (transmitter Alice) adopts visible light beam to communicate with an unmanned aerial vehicle (legitimate receiver Bob) in the air, while an unmanned aerial vehicle (passive eavesdropper Eve) tries to intercept the information from Alice. The W2A-VLC system can be adopted for underwater rescue, underwater resource exploration and several other missions. Due to random fluctuation of water surface, the channel gain between Alice and Bob varies randomly with time. From our previous experiment in [8], adopting direct current (DC)-blockage avalanche photodiode (APD) receivers, the channels Alice-Bob and Alice-Eve in the electrical domain are considered to be lognormal block fading under laboratory condition. The received signals at Bob and Eve are given by

$$y_B = h_B x + n_B, \quad y_E = h_E x + n_E, \tag{1}$$

where x is the transmitted symbol with average energy E_s; h_B and h_E are channel gains; n_B (n_E) is the additive white Gaussian noise (AWGN) with zero mean and variance N_B (N_E). The electrical-domain SNR can be expressed as $snr_B = \frac{E_s {h_B}^2}{N_B}$ and $snr_E = \frac{E_s {h_E}^2}{N_E}$.

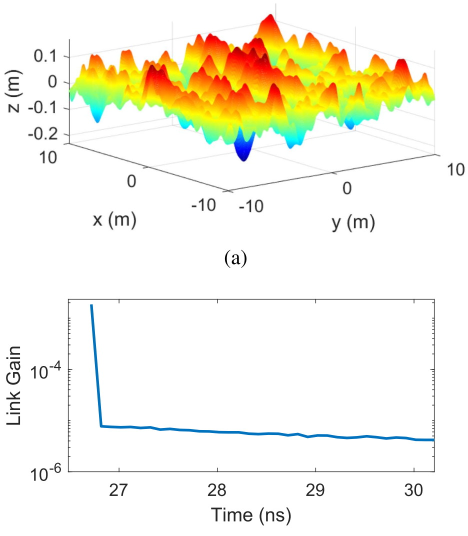
B. Correlation of W2A and A2W Link Gains in Monte Carlo Simulations

For Alice, to obtain the CSI and adapt the transmission parameters according to the fading channel for security scheme design, there are two typical feedback mechanisms: implicit feedback and explicit feedback [22]. In explicit feedback, Alice first sends a training frame to Bob, then Bob performs channel estimation and sends back the CSI to Alice. However, the feedback information can be eavesdropped by Eve, threatening the communication security. In implicit feedback, Alice implicitly obtains the CSI of W2A link by estimating the A2W link, assuming that W2A and A2W links are perfectly or partially reciprocal. Such method reduces the feedback delay and is robust to interception since the exchanged information does not contain CSI.

In this subsection, we consider implicit feedback and investigate the correlation of W2A and A2W link gains using Monte Carlo simulations. Assume that Alice and Bob are located at (0, 0, −5) m and (0, 0, 3) m, respectively. The fields of view (FOVs) of Alice and Bob are both 45 degrees, and Pierson-Moscowitz spectrum is adopted to model the sea surface under wind speed 3 m/s [23]. We consider visible light of wavelength 525 nm and clear oceanic water corresponding to Jerlov type IB water [24].

The water surface in Monte Carlo simulation is shown in Fig. 2(a). The channel impulse response in Fig. 2(b) shows that most received photons arrive at the receiver within the order of nanoseconds. Therefore, the temporal dispersion caused by scattering can be neglected if the transmission symbol rate is lower than Gbps. Fig. 3(a) shows that WA2 and A2W link gains vary with random fluctuations of the water surface. From Fig. 3(b), the relation between the W2A link gain h_B and A2W link gain h_A can be fitted by a straight line (i.e., $h_B = c \cdot h_A$), and the correlation coefficient is 0.9960, which indicates that the channel is highly reciprocal in terms of the channel gain. There exists a constant ratio c between the W2A and A2W link gains, since different beam divergence angles in the W2A and A2W links result in different optical power densities.

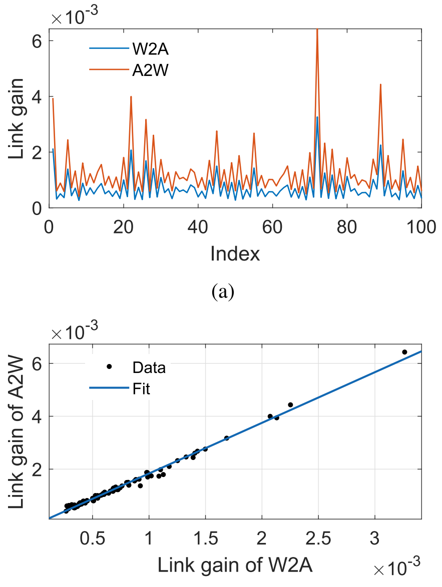
As shown in Fig. 4(a), the W2A and A2W links exhibit high correlation coefficients for different Bob's heights. Besides, it is seen from Fig. 4(b) that as the horizontal distance offset of Eve with respect to Bob increases, the correlation coefficient decreases rapidly, which indicates that the Alice-Eve channel is not correlated with the Alice-Bob channel when Eve is far away from Bob.



(a)

(b)

Fig. 2. (a) The simulated water surface and (b) the channel impulse response.



(a)

(b)

Fig. 3. (a) The gains of W2A and A2W links and (b) the fitted line of the relation between W2A and A2W link gains.

C. Experimental Investigation and Parameter Measurements

A W2A-VLC system is established to experimentally investigate the correlation of W2A and A2W link gains, and measure the distribution parameters of channel gain, as shown in Fig. 5. A green LED (LED1, Cree XP-E, 520∼535 nm) and an APD (APD1, Hamamatsu C10508-01) are placed under depth 0.2 m as the transmitter Alice with coordinate (0, 0, −0.2) m. In the same

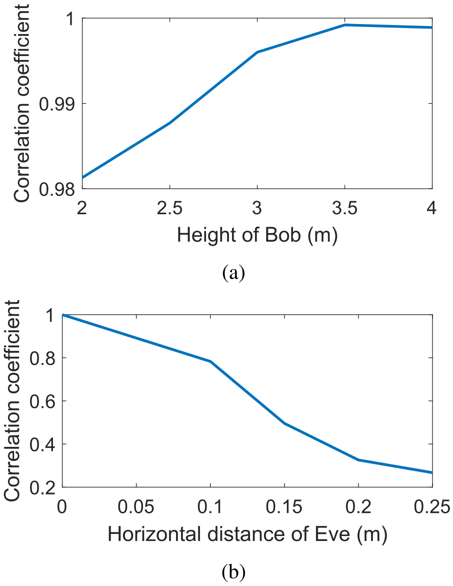


Fig. 4. The correlation coefficients versus (a) Bob's height and (b) Eve's horizontal distance.

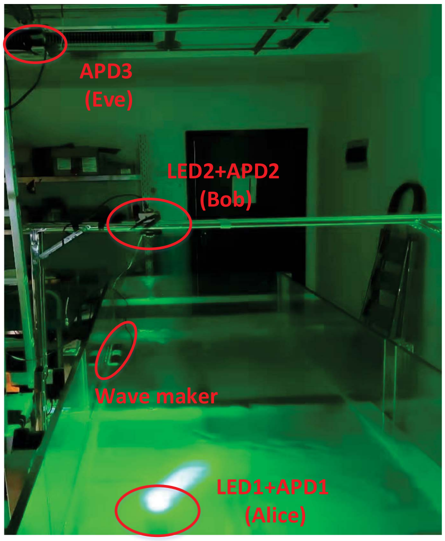


Fig. 5. The experimental system of W2A-VLC.

way, LED2 (Cree XP-E, 520∼535 nm) and APD2 (Hamamatsu C10508-01) are placed directly above Alice at (0, 0, 0.7) m as the legitimated receiver Bob. APD3 (Hamamatsu C10508-01) acts as the eavesdropper Eve. A wave generator (Yujang CX-W3) is placed in a water tank to generate wave. In our experimental environment, the generated water waves in the tank can be considered as irregularly small waves. An arbitrary waveform generator (AWG, RigolDG5252) is adopted to generate sinusoidal waves ($V\text{pp} = 5$ V) of frequencies 100 kHz and 200 kHz for driving LED1 and LED2, respectively. The received signals are sampled by a data collector (ART PCIE8584) with sampling rate 1 MSa/s for offline signal processing. The channel gains of Bob and Eve can be extracted by using the signal processing method in [4]. Besides, considering different responses of APD2 and APD3, we normalize their corresponding channel gains via the received signal amplitudes from the same LED under the same transmission distance to compare the channel gains accurately.

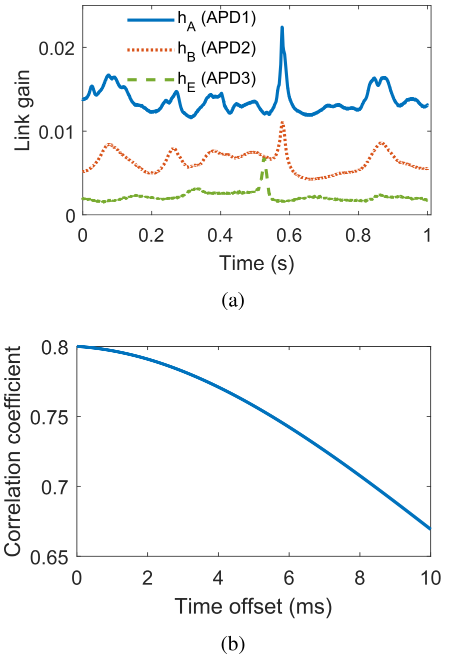
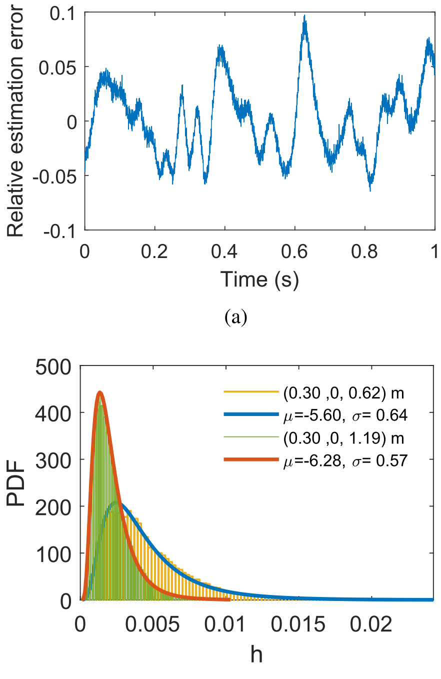


Fig. 6. (a) Gains of Bob-to-Alice, Alice-to-Bob, and Alice-to-Eve links and (b) correlation coefficients of Bob-to-Alice and Alice-to-Bob link gains versus time offset.

In the experiment, LED1 and APD2 form a W2A link, while LED2 and APD1 form an A2W link between Alice and Bob. Due to the size limitation of devices, the horizontal distance between the W2A and A2W links is 2 cm. Fig. 6(a) shows the variations of A2W link gain h_A, W2A link gain h_B and eavesdropping link gain h_E with the time. The correlation coefficient between h_A and h_B is 0.80, while the correlation coefficient between h_B and h_E is 0.13 when Eve is located at (0.3, 0, 1.19) m. Due to the horizontal distance between the W2A and A2W links as well as the discrepancy between the divergence angle of LED and FOV of APD, the correlation coefficient between h_A and h_B is reduced compared with the simulation results in Section II-B. The results indicate that the device integration and matched FOV/divergence angle are required to achieve high correlation between W2A and A2W links. The small correlation coefficient between h_B and h_E implies that the Alice-Eve channel is not correlated with the Alice-Bob channel. Fig. 6(b) shows the correlation coefficient between $h_A(t)$ and $h_B(t-\tau)$ versus the time offset τ. It is seen that the correlation coefficient drops slightly to 0.79 as the time offset increases to 2 ms, which indicates the feasibility of channel estimation in coherence time interval. Alice can estimate h_B from h_A based on the linear correlation between h_A and h_B. Let $\hat{h}_B$ denote the estimate of h_B based on h_A. The estimation error of h_B is $h_B - \hat{h}_B$, and the relative estimation error is $(h_B - \hat{h}_B)/h_B$, as shown in Fig. 7(a). In Fig. 7(b), the probability density functions (PDFs) of channel gain can be well fitted by the lognormal distribution with parameters μ and σ, when Eve is located at (0.3, 0, 0.62) m and (0.3, 0, 1.19)



(a)

(b)

Fig. 7. (a) Relative estimation error of W2A-link gain and (b) PDF of Eve's channel gain.

m. These distribution parameters will be used in the following simulations.

III. The Proposed Security Scheme

After verifying the high correlation between the W2A and A2W link gains, we propose a PLS scheme by adopting superposition modulation. The proposed scheme is performed through two steps during each coherent time interval. In the first step, Alice obtains A2W channel gain h_A from the pilot signal transmitted by Bob, and estimates W2A channel gain as $\hat{h}_B$ based on the high correlation between h_A and h_B. In the second step, Alice alters the signal modulation order and the superposition parameter according to $\hat{h}_B$, and sends the information signal back to Bob together with pilots. Bob obtains the W2A channel gain h_B from the pilot transmitted by Alice, and then selects the modulation parameters based on h_B to demodulate the received signal. The W2A channel gain and modulation parameters are kept secret between Alice and Bob. The selection strategy of modulation parameters is designed to maximize the detection error probability of Eve, which will be presented in Section V. The proposed scheme achieves secrecy based on channel randomness, the correlation between W2A and A2W links, and signal diversity of superposition modulation for W2A-VLC systems.

A. Superposition Modulation

The principle of superposition modulation is shown in Fig. 8. A binary data stream is first split into M parallel binary data streams. All information bits $b_m \in \{0, 1\}$ are mapped into binary antipodal symbols $d_m \in \{+1, -1\}$. Afterward, symbols $\{d_m\}$ are weighted by a set of factors $\{\alpha_m\}$, and modulated via linear superposition as follows [25],

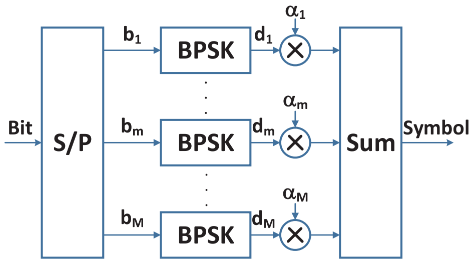


Fig. 8. The schematic diagram of the superposition modulation.

$$x = \sum_{m=1}^{M} \alpha_m d_m = \sum_{m=1}^{M} \alpha_m (-1)^{b_m}. \tag{2}$$

One special case of $M = 1$ corresponds to 2-PAM signal without superposition and DC component. The transmitted alternating current (AC) 2^M-PAM ($M > 1$) with superposition parameter ρ can be generated by superimposing equally spaced $2^{(M-1)}$-PAM signal $\{2^{(M-1)} - 1, 2^{(M-1)} - 3, \ldots, -2^{(M-1)} + 1\}$ and 2-PAM signal $\{+\rho, -\rho\}$, i.e, weight factors $\alpha_m = 2^{m-1}$ for $m \in \{1, 2, \ldots, M-1\}$ and $\alpha_M = \rho$.

B. Demodulation Performance

In this subsection, we derive the SERs of Bob and Eve after demodulation. Assume that Bob knows modulation order m and superposition parameter ρ, while Eve knows m but not ρ. Note that inaccurate information about modulation order m leads to Eve's SER of one. Eve adopts detection thresholds of equally spaced PAM signals for symbol decision.

1) SER of 4-PAM Signal: First we consider 4-PAM signal with superposition parameter ρ. The transmitted AC 4-PAM signal is generated by superimposing 2-PAM signal $\{+1, -1\}$ and 2-PAM signal $\{+\rho, -\rho\}$, which can be expressed as $x = \{\pm(\rho+1), \pm(\rho-1)\} \times \sqrt{\frac{E_s}{\rho^2+1}}$ with $\rho \geq 2$, where E_s is the average symbol energy. With the received signal y given in (1), the demodulation SER can be derived as

$$\begin{aligned} P_e &= 1 - \frac{1}{4} \\ &\times \begin{pmatrix} P\left(y > h\rho' \sqrt{\frac{E_s}{\rho'^2+1}} \,\middle|\, x = (\rho+1)\sqrt{\frac{E_s}{\rho^2+1}}\right) \\ + P\left(0 < y < h\rho' \sqrt{\frac{E_s}{\rho'^2+1}} \,\middle|\, x = (\rho-1)\sqrt{\frac{E_s}{\rho^2+1}}\right) \\ + P\left(-h\rho' \sqrt{\frac{E_s}{\rho'^2+1}} < y < 0 \,\middle|\, x = (-\rho+1)\sqrt{\frac{E_s}{\rho^2+1}}\right) \\ + P\left(y < -h\rho' \sqrt{\frac{E_s}{\rho'^2+1}} \,\middle|\, x = (-\rho-1)\sqrt{\frac{E_s}{\rho^2+1}}\right) \end{pmatrix} \\ &= \frac{1}{2} - \frac{1}{2} Q\left(\rho' \sqrt{\frac{snr}{\rho'^2+1}} - (\rho+1)\sqrt{\frac{snr}{\rho^2+1}}\right) \end{aligned}$$

$$+\frac{1}{2}Q\left(\rho'\sqrt{\frac{snr}{\rho'^2+1}}-(\rho-1)\sqrt{\frac{snr}{\rho^2+1}}\right)$$
$$+\frac{1}{2}Q\left((\rho-1)\sqrt{\frac{snr}{\rho^2+1}}\right), \qquad (3)$$

where ρ' is the superposition parameter adopted by the receiver for symbol detection ($\rho' = \rho$ for Bob and $\rho' = 2$ for Eve), and $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-t^2/2}dt$ is the tail probability of the standard normal distribution.

2) SER of 8-PAM Signal: The transmitted 8-PAM signal with superposition parameter ρ is generated by superimposing 4-PAM signal $\{+3, +1, -1, -3\}$ and 2-PAM signal $\{+\rho, -\rho\}$, which can be expressed as $\{\pm(\rho+3), \pm(\rho+1), \pm(\rho-1), \pm(\rho-3)\} \times \sqrt{\frac{E_s}{(\rho^2+5)}}$ with $\rho \geq 4$. The demodulation SER can be derived as

$$P_e = \frac{1}{4} - \frac{1}{4}Q\left((\rho'+2)\sqrt{\frac{snr}{(\rho'^2+5)}}-(\rho+3)\sqrt{\frac{snr}{(\rho^2+5)}}\right)$$
$$+\frac{1}{4}Q\left((\rho'+2)\sqrt{\frac{snr}{(\rho'^2+5)}}-(\rho+1)\sqrt{\frac{snr}{(\rho^2+5)}}\right)$$
$$+\frac{1}{4}Q\left(-\rho'\sqrt{\frac{snr}{(\rho'^2+5)}}+(\rho+1)\sqrt{\frac{snr}{(\rho^2+5)}}\right)$$
$$+\frac{1}{4}Q\left(\rho'\sqrt{\frac{snr}{(\rho'^2+5)}}-(\rho-1)\sqrt{\frac{snr}{(\rho^2+5)}}\right)$$
$$+\frac{1}{4}Q\left((2-\rho')\sqrt{\frac{snr}{(\rho'^2+5)}}+(\rho-1)\sqrt{\frac{snr}{(\rho^2+5)}}\right)$$
$$+\frac{1}{4}Q\left((\rho'-2)\sqrt{\frac{snr}{(\rho'^2+5)}}-(\rho-3)\sqrt{\frac{snr}{(\rho^2+5)}}\right)$$
$$+\frac{1}{4}Q\left((\rho-3)\sqrt{\frac{snr}{(\rho^2+5)}}\right), \qquad (4)$$

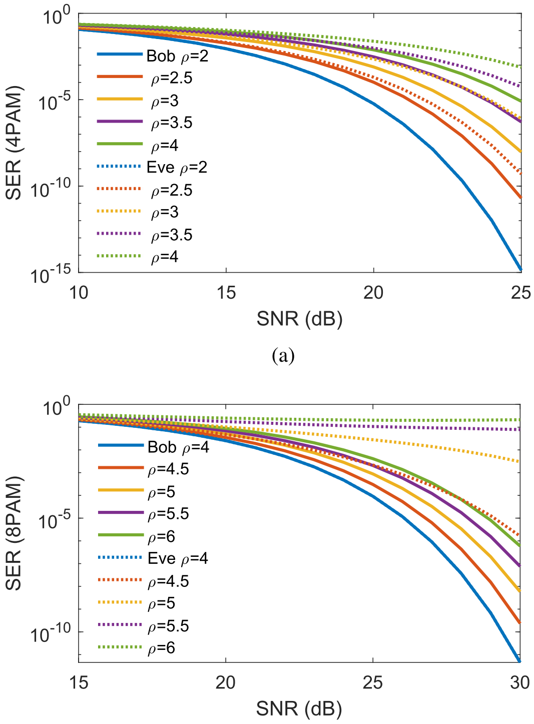
where $\rho' = \rho$ for Bob and $\rho' = 4$ for Eve,.

3) SER Comparison: The SER comparison of Bob and Eve is shown in Fig. 9. It is seen that Eve has a larger SER than Bob under the same SNR and superposition parameter ρ, except for equally spaced 4-PAM signal ($\rho = 2$) or 8-PAM signal ($\rho = 4$) with identical SER. As superposition parameter ρ increases, the SER of Eve increases rapidly, which indicates that a larger superposition parameter ρ can reduce the successful detection probability of Eve significantly.

Except for changing the modulation order, the superposition scheme changes the constellation diagram more diversely. Since the modulation parameters vary randomly with Bob's channel, the cracking can be more difficult and the successful detection probability of Eve can be reduced.

IV. Attack Models

In this section, four different attack types of Eve are considered, namely random attack, correlated attack, post-processing attack and intelligent attack. Eve's demodulation performance is analyzed under the four attack types.



(a)

(b)

Fig. 9. Bob's and Eve's SERs versus SNR (a) for 4-PAM signal and (b) for 8-PAM signal.

A. Random Attack

Random attack corresponds to the case when Eve has no knowledge on the CSI of Alice-Bob channel and performs random demodulation. We consider the following two methods of random demodulation.

1) Method 1: In the first random demodulation method, Eve chooses the SNR of legitimate channel randomly and adopts the corresponding modulation type to demodulate the received signal. Let $P_s = 1 - P_e$ denote the probability of correct demodulation when Eve adopts superposition parameter ρ_E to demodulate signals with ρ_B, where the SERs of Eve for 4-PAM and 8-PAM signals are given in (3) and (4) with $\rho = \rho_B$ and $\rho' = \rho_E$. For the 2-PAM signal, there is no superposition parameter, and we have $P_s = Q(-\sqrt{snr_E})$. Let m be the modulation order index corresponding to 2^m-PAM, snr_U^m and snr_L^m be the lower and upper bounds of SNR for the modulation order index m, respectively.

The average demodulation SER of Eve can be written in (5), shown at the bottom of next page. where $\rho_B(snr_B)$ denotes the mapping from snr_B to ρ_B that we will explore later; M is the maximum modulation order index; snr' is the SNR chosen randomly by Eve, following a uniform distribution $f(snr') = \frac{1}{snr'_U - snr'_L}$. Since the W2A link gain h_B follows the lognormal distribution with parameters u_1 and σ_1, Bob's SNR $snr_B = \frac{E_s {h_B}^2}{N_B}$ follows the lognormal distribution with parameters $u =$

$2u_1 + \ln(\frac{E_s}{N_B})$ and $\sigma^2 = 4{\sigma_1}^2$, i.e., its PDF is given by

$$f\left(snr_B\right) = \frac{1}{snr_B\sigma\sqrt{2\pi}} \exp\left(\frac{-\left(\ln\left(snr_B\right) - u\right)^2}{2\sigma^2}\right). \tag{6}$$

2) Method 2: In the second random demodulation method, Eve chooses the modulation order and constellation point index randomly, where the average SER is given by

$$SER_{rnd2} = 1 - \sum_{m=1}^{M}\left(\frac{1}{M} \times \frac{1}{2^m} \times \int_{snr_L^m}^{snr_U^m} f\left(snr_B\right) dsnr_B\right). \tag{7}$$

B. Correlated Attack

Correlated attack corresponds to the case when the channels of Eve and Bob are correlated, Eve estimates the modulation type based on its own channel gain. The joint distribution of Bob and Eve's SNR is a bivariate lognormal distribution with PDF given by

$$\begin{aligned} f\left(snr_B, snr_E\right) = &\frac{1}{2\pi snr_B snr_E \sigma_B \sigma_E \sqrt{1-r^2}} \\ &\times \exp\left\{-\frac{1}{2\left(1-r^2\right)}\left[\begin{array}{c}\left(\frac{\ln(snr_B)-u_B}{\sigma_B}\right)^2 + \left(\frac{\ln(snr_E)-u_E}{\sigma_E}\right)^2 \\ -2r\left(\frac{\ln(snr_B)-u_B}{\sigma_B}\right)\left(\frac{\ln(snr_E)-u_E}{\sigma_E}\right)\end{array}\right]\right\}, \end{aligned} \tag{8}$$

where r is the correlation coefficient between $\ln(snr_B)$ and $\ln(snr_E)$. The average SER can be written in (9), shown at the bottom of this page.

C. Post-Processing Attack

Post-processing attack corresponds to the case when Eve searches the potential set of transmitted symbols, which is similar to brute force search attacks on secret keys [26]. Assume that post-processing attack has sufficient capability to store and process all received signals.

The transmitted symbol $x_{m,\rho,k}$ is given by

$$x_{m,\rho,k} = \begin{cases} \left(-\rho - 2^{m-1} + 2\,k - 1\right)\sqrt{\frac{E_s}{\rho^2 + \frac{1}{3} \times 2^{2\,m-2} - \frac{1}{3}}}, \\ \quad k \in \left\{1, 2, \ldots, 2^{m-1}\right\} \\ \left(\rho - 3 \times 2^{m-1} + 2\,k - 1\right)\sqrt{\frac{E_s}{\rho^2 + \frac{1}{3} \times 2^{2\,m-2} - \frac{1}{3}}}, \\ \quad k \in \left\{2^{m-1} + 1, 2^{m-1} + 2, \ldots, 2^m\right\}, \end{cases} \tag{10}$$

where k is the constellation point index for 2^m-PAM signal with superposition parameter ρ. We use binary indicator $I_{m,\rho,k} = 1$ to represent that the symbol with modulation order m, superposition parameter ρ and constellation point index k is detected as the transmitted symbol. The potential set of transmitted symbols can be expressed as $\{x_{m,\rho,k} | I_{m,\rho,k} = 1\}$. Denoting the actually transmitted symbol by x_{m^*,ρ^*,k^*}, the received signal at Eve is $y_{m^*,\rho^*,k^*} = h_E x_{m^*,\rho^*,k^*} + n_E$, and the binary indicator is computed as

$$I_{m,\rho,k} = \begin{cases} 1, \text{when } y_{m^*,\rho^*,k^*} \in \left[\begin{array}{l}\frac{h_E}{2}\left(x_{m,\rho,k} + x_{m,\rho,k-1}\right), \\ \frac{h_E}{2}\left(x_{m,\rho,k} + x_{m,\rho,k+1}\right)\end{array}\right) \\ \quad \text{for } k \in \left\{2, 3, \ldots, 2^m - 1\right\}, \\ y_{m^*,\rho^*,k^*} \geq \frac{h_E}{2}\left(x_{m,\rho,k} + x_{m,\rho,k-1}\right) \text{ for } k = 2^m, \\ y_{m^*,\rho^*,k^*} < \frac{h_E}{2}\left(x_{m,\rho,k} + x_{m,\rho,k+1}\right) \text{ for } k = 1; \\ 0, \text{Otherwise.} \end{cases} \tag{11}$$

The conditional probability of $I_{m,\rho,k} = 1$ given transmitted symbol x_{m^*,ρ^*,k^*} can be written as

$$\begin{aligned} &P\left(I_{m,\rho,k} = 1 | x_{m^*,\rho^*,k^*}\right) = \\ &\begin{cases} 1 - Q\left(\left(\frac{h_E}{2}\left(x_{m,\rho,k} + x_{m,\rho,k+1}\right) - h_E x_{m^*,\rho^*,k^*}\right) / \sqrt{N_E}\right) \\ - Q\left(\left(-\frac{h_E}{2}\left(x_{m,\rho,k} + x_{m,\rho,k-1}\right) + h_E x_{m^*,\rho^*,k^*}\right) / \sqrt{N_E}\right), \\ \quad k \in \left\{2, 3, \ldots,\ 2^m - 1\right\}; \\ Q\left(\left(\frac{h_E}{2}\left(x_{m,\rho,k} + x_{m,\rho,k-1}\right) - h_E x_{m^*,\rho^*,k^*}\right) / \sqrt{N_E}\right), \\ \quad k = 2^m; \\ Q\left(-\left(\frac{h_E}{2}\left(x_{m,\rho,k} + x_{m,\rho,k+1}\right) + h_E x_{m^*,\rho^*,k^*}\right) / \sqrt{N_E}\right), \\ \quad k = 1; \\ 0, \quad \text{Otherwise.} \end{cases} \end{aligned} \tag{12}$$

The post-processing attack can reduce the uncertainty of potential transmitted symbol set, which can be characterized by comparing the entropy of transmitted message with that of the potential set in post-processing attack. Assume that Alice chooses the modulation type of modulation order index m and superposition parameter ρ with probability

$$q\left(m, \rho\right) = \int_{snr_L(m,\rho)}^{snr_U(m,\rho)} f\left(snr_B\right) dsnr_B, \tag{13}$$

$$SER_{rnd1} = 1 - \sum_{m=1}^{M}\left(\int\limits_{snr_L^m}^{snr_U^m}\int\limits_{snr_L^m}^{snr_U^m}\left(P_s\left(snr_E, \rho_B\left(snr_B\right), \rho_E\left(snr'\right)\right) \times f\left(snr_B\right) f\left(snr'\right) dsnr_B dsnr'\right)\right). \tag{5}$$

$$SER_{cor} = 1 - \sum_{m=1}^{M}\left(\int\limits_{snr_L^m}^{snr_U^m}\int\limits_{snr_L^m}^{snr_U^m}\left(P_s\left(snr_E, \rho_B\left(snr_B\right), \rho_E\left(snr_E\right)\right) \times f\left(snr_B, snr_E\right) dsnr_B dsnr_E\right)\right). \tag{9}$$

where $snr_L(m,\rho)$ and $snr_U(m,\rho)$ are the lower and upper bounds of SNR for choosing the modulation order m and superposition parameter ρ, respectively. Each symbol of this modulation type have equal probability $(q(m,\rho)/2^m)$ to be transmitted. Assume the range of ρ for given m is $[\rho_1(m), \rho_2(m)]$. The entropy can be calculated as

$$\begin{aligned} H_A &= -\sum_{m=1}^{M}\sum_{\rho=\rho_1(m)}^{\rho_2(m)} \frac{q(m,\rho)}{2^m} \times 2^m \log_2\left(\frac{q(m,\rho)}{2^m}\right) \\ &= -\sum_{m=1}^{M}\sum_{\rho=\rho_1(m)}^{\rho_2(m)} q(m,\rho)\log_2\left(\frac{q(m,\rho)}{2^m}\right) \end{aligned} \tag{14}$$

Note that among all symbols with modulation order index m and superposition parameter ρ, only one candidate symbol belongs to the potential set, i.e., we have $I_{m,\rho} = \sum_{k=1}^{2^m} I_{m,\rho,k} = 1$. Then, the entropy of potential set in the post-processing attack can be written as

$$\begin{aligned} H_E &= -\sum_{m=1}^{M}\sum_{\rho=\rho_1(m)}^{\rho_2(m)} \frac{q(m,\rho)}{I_{m,\rho}} \times I_{m,\rho} \log_2\left(\frac{q(m,\rho)}{I_{m,\rho}}\right) \\ &= -\sum_{m=1}^{M}\sum_{\rho=\rho_1(m)}^{\rho_2(m)} q(m,\rho)\log_2\left(q(m,\rho)\right) \end{aligned} \tag{15}$$

Assuming that the transmitted symbol is x_{m^*,ρ^*,k^*} and Eve uniformly choose a symbol in the potential set as the decision of the transmitted symbol, the SER is given by

$$\begin{aligned} SER_{ppr} &= 1 - \frac{1}{\sum_{m=1}^{M}\sum_{\rho=\rho_1(m)}^{\rho_2(m)} I_{m,\rho}} \\ &\quad \times P\left(I_{m^*,\rho^*,k^*} = 1 \left| x_{m^*,\rho^*,k^*}\right.\right) \\ &= 1 - \frac{1}{N_t} \times P\left(I_{m^*,\rho^*,k^*} = 1 \left| x_{m^*,\rho^*,k^*}\right.\right), \end{aligned} \tag{16}$$

where N_t is the number of all modulation types $\{(m,\rho)\}$.

D. Intelligent Attack

Intelligent attack corresponds to the case when Eve adopts modulation classification methods to identify the modulation type and classify the symbols. Due to irregular PAM signals, some traditional modulation classification methods, such as maximum likelihood, Kolmogorov-Smirnov test and high-order statistics [27], are not suitable since these methods perform symbol decisions from a finite set of known candidates. In this work, both modulation order and constellation position need to be estimated. However, supervised learning techniques, such as K-nearest neighbour, support vector machine and artificial neural network, require training data and labels to optimize the classification model, which is unrealistic for eavesdroppers. Therefore, we consider the unsupervised algorithms in this section, including K-means clustering and EM algorithm. The intelligent attack is performed as follows. Firstly, the modulation order (i.e., clustering number 2^m) is determined by Silhouette score, which takes values in $[-1, 1]$ and is adopted to evaluate the quality of clustering (Specifically, Silhouette score being 1 represents that the data can be well separated) [28]. Secondly, we estimate the constellation locations and calculate the SER.

1) K-Means Clustering: The received signal after channel gain normalization can be expressed as

$$r_n = x_n + w_n, \quad n \in \{1, 2, \ldots, N\}, \tag{17}$$

where x_n is nth transmitted symbol, and w_n is AWGN with zero mean and variance σ^2. Let $\mathcal{A} = \{a_1, a_2, \ldots, a_{2^m}\}$ denote the constellation set for a given modulation order index m, and $\boldsymbol{x} = [x_1, x_2, \ldots, x_N]^T$ denote the transmitted symbol vector. The optimization problem of K-means algorithm can be written as

$$\min_{\mathcal{C}} \sum_{k=1}^{2^m}\sum_{n\in\mathcal{C}_k} (r_n - a_k)^2, \tag{18}$$

where K-means clustering aims to partition the N received signals into 2^m sets, i.e, $\mathcal{C} = \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{2^m}\}$ and $\mathcal{C}_k \triangleq \{n|\hat{x}_n = a_k\}$. The optimization problem (18) is non-convex and can be solved by a two-step iterative method. In the first step, we fix the constellation set $\mathcal{A}$ and estimate the transmitted symbol as

$$\hat{x}_n = \arg\min_{a_k\in\mathcal{A}} \left(|r_n - a_k|\right). \tag{19}$$

In the second step, we update $\mathcal{A}$ with fixed $\boldsymbol{x}$. The updated constellation symbol a_k is expressed as

$$a_k = \frac{1}{|\mathcal{C}_k|}\sum_{l\in\mathcal{C}_k} r_l. \tag{20}$$

2) EM Algorithm: The observed signals are combinations of several Gaussian distributions with different mean values (constellation points), which can be modeled as Gaussian mixture model (GMM) given by

$$f\left(r_n \left|\boldsymbol{\theta}\right.\right) = \sum_{k=1}^{2^m} \alpha_k \frac{1}{\sqrt{2\pi{\sigma_k}^2}} \exp\left(-\frac{(r_n - u_k)^2}{2{\sigma_k}^2}\right), \tag{21}$$

where the unknown parameter matrx is $\boldsymbol{\Theta} = [\boldsymbol{\theta_1}, \boldsymbol{\theta_2}, \ldots, \boldsymbol{\theta_{2^m}}]$, and $\boldsymbol{\theta_k} = [\alpha_k, u_k, {\sigma_k}^2]^T$. The logarithmic likelihood function is

$$\log f\left(\boldsymbol{r}\left|\boldsymbol{\theta}\right.\right) = \sum_{n=1}^{N}\log\left(\sum_{k=1}^{2^m}\alpha_k\frac{1}{\sqrt{2\pi{\sigma_k}^2}}\exp\left(-\frac{(r_n - u_k)^2}{2{\sigma_k}^2}\right)\right). \tag{22}$$

EM algorithm is an iterative method for approximately obtaining ML estimates of parameters. The detailed iterative process can be found in [29], which is standard and thus omitted here.

After using K-means and EM methods, the detection SER can be obtained as the performance metric.

E. Computational Complexity of Attack Types

For both two methods of random attack and correlated attack, Eve estimates the modulation type randomly or based on its own channel gain, and demodulates each received symbol. The computational complexity is $O(n)$ for n received symbols. For post-processing attack, Eve searches a potential set of transmitted symbols in all modulation types for each received symbol, with a computational complexity of $O(N_t n)$, where N_t is the number of all modulation types $\{(m,\rho)\}$. For K-means method of intelligent attack, Eve computes distance between each of n symbols and K cluster centers with a complexity of $O(Kn)$ at each iteration, and thus with a total computational complexity of $O(KTn)$ after T iterations. For EM method of intelligent attack, Eve computes each weight $w_{i,k}$ of the ith received symbol in the kth cluster at each iteration, where $i \in \{1,2,\ldots,n\}$ and $k \in \{1,2,\ldots,K\}$. Therefore, the computational complexity is $O(KTn)$ after T iterations.

V. Superposition Parameter Optimization

Since Eve is a passive eavesdropper, Alice cannot get any CSI of Alice-Eve channel and can only alter the modulation parameters according to the CSI of Alice-Bob channel. One selection strategy for superposition parameter ρ_B is to maximize the detection error probability of Eve given that Bob's SER is lower than a certain threshold.

For random and correlated attacks, if Eve selects the correct parameter to demodulate (i.e., $\rho_B = \rho_E$), a lower bound on SER can be written as

$$SER_L = 1 - \sum_{m=1}^{M} \left(\int_{snr_L^m}^{snr_U^m} P_s\left(snr_E, \rho_B\left(snr_B\right), \rho_B\left(snr_B\right)\right) f\left(snr_B\right) dsnr_B \right), \tag{23}$$

where ρ_B is a function of snr_B. We aim to maximize SER_L with respect to ρ_B, i.e.,

$$\max_{\rho_B} SER_L \Leftrightarrow \min_{\rho_B} P_s\left(snr_E, \rho_B\left(snr_B\right), \rho_B\left(snr_B\right)\right). \tag{24}$$

Theorem 1: The probability P_s of correct demodulation decreases monotonically as ρ_B increases when $\rho_B \geq 2$ for 4-PAM and $\rho_B \geq 4$ for 8-PAM.

Proof: See Appendix A.

Based on Theorem 1, problem (24) is equivalent to

$$\min_{\rho_B} P_s\left(snr_E, \rho_B\left(snr_B\right), \rho_B\left(snr_B\right)\right) \Leftrightarrow \max \rho_B. \tag{25}$$

Hence, Alice selects the maximum superposition parameter ρ_B based on snr_B, subject to the constraint that Bob's SER is lower than a certain threshold. Considering whether Alice has an accurate snr_B of W2A link, the constraint can be divided into the following two forms.

A. Optimization Under Accurate W2A-Link SNR

Consider the optimization under accurate snr_B, which serves as a performance limit on a more realistic case where Alice estimates snr_B based on the W2A-A2W link correlation. The optimization problem with respect to the superposition parameter is formulated as

$$\begin{array}{ll} \max & \rho_B \\ \text{s.t.} & P_e\left(snr_B, \rho_B\right) \leq th \end{array}, \tag{26}$$

where th is the threshold of Bob's SER. The expressions of demodulation SER P_e for 4-PAM and 8-PAM signals are given by (3) and (4) with $\rho = \rho' = \rho_B$. Since P_e increases with ρ_B when $\rho_B \geq 2$ for 4-PAM signal and $\rho_B \geq 4$ for 8-PAM signal, the constraint in (26) must hold with equality for the optimal solution, i.e.,

$$P_e\left(snr_B, \rho_B\right) = th, \tag{27}$$

so we have

$$\rho_B = g\left(th, snr_B\right), \tag{28}$$

where g is mapping function derived from P_e. It is implied that the value of superposition parameter ρ_B is selected according to the SNR of Alice-Bob channel and SER threshold.

B. Optimization Under Estimated W2A-Link SNR

In a more general case, Alice estimates W2A-link SNR snr_B based on the A2W link with estimation error. The SNR estimation error (in dB) can be expressed as

$$\eta = {snr_B}^{dB} - {\hat{snr}_B}^{dB} = 20\log\left(\frac{h_B}{\hat{h}_B}\right), \tag{29}$$

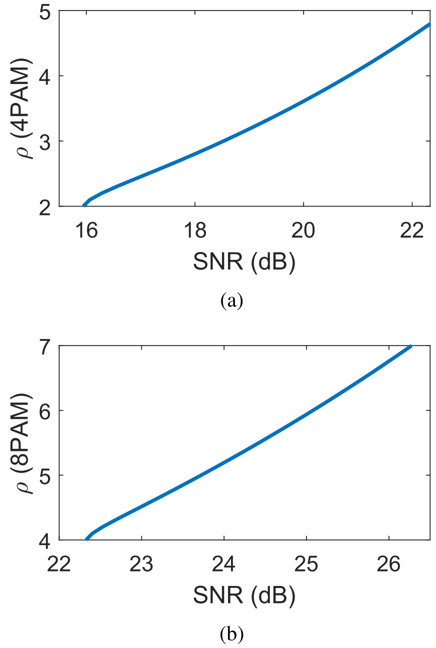
where $\hat{snr}_B$ is the W2A-link SNR estimated by Alice, and η is a random variable on interval $[-\tau_1, \tau_2]$.

Alice selects superposition parameter according to estimated $\hat{snr}_B$, and the optimization problem can be written as

$$\begin{array}{ll} \max & \hat{\rho}_B \\ \text{s.t.} & P_e\left({snr_B}^{dB}, \hat{\rho}_B, \rho_B\right) \leq th, \\ & \forall {snr_B}^{dB} \in \left[{\hat{snr}_B}^{dB} - \tau_1, {\hat{snr}_B}^{dB} + \tau_2\right], \end{array} \tag{30}$$

where $\hat{\rho}_B$ is the superposition parameter selected by Alice, and ρ_B is selected by Bob satisfying $\rho_B = g(th, snr_B)$ according to (27). P_e denotes Bob's SER when Alice modulates the symbols with superposition parameter $\hat{\rho}_B$ and Bob demodulates the symbols with ρ_B, which is given by (3) and (4) with $\rho = \hat{\rho}_B$ and $\rho' = \rho_B$. The robust optimization problem can be solved using Matlab toolbox.

In addition, for intelligent attack, there is no explicit expression for Eve's SER using K-means clustering and EM algorithm. From the following simulation results in Fig. 16, Eve's SER increases with the superposition parameter selected by Alice under the same modulation order, since the minimum distance $2\sqrt{\frac{E_s}{\rho^2 + \frac{1}{3} \times 2^{2m-2} - \frac{1}{3}}}$ between constellation points of modulation type (m,ρ) decreases with ρ. Lager superposition parameters lead to shorter constellation distances and larger classification errors for Eve. Therefore, the selection strategy is the same as that given by (30). For post-processing attack, the entropy of potential set is not sensitive to the superposition parameter of transmitted symbols in (15), but the entropy depends on the number of modulation types (m,ρ). The strategy in (30) varies the modulation type based on the Bob's SNR, which maximizes the Eve's entropy.



(a)

(b)

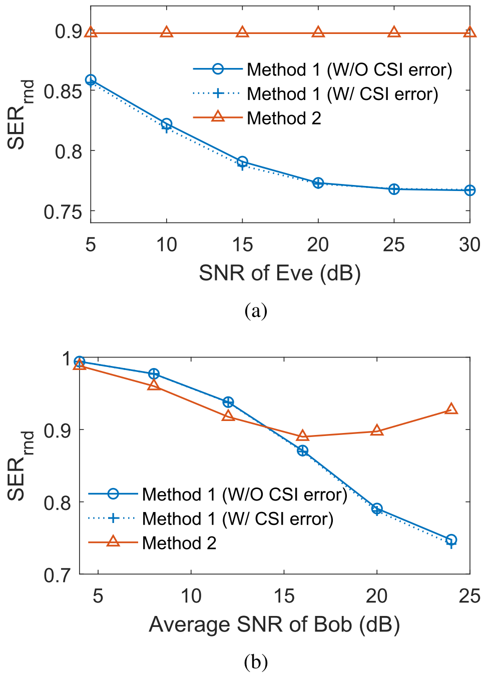
Fig. 10. The superposition parameters versus SNR of Alice-Bob channel (a) for 4-PAM signal and (b) for 8-PAM signal.

TABLE I
SELECTION OF MODULATION TYPE

SNR range (dB)	m	ρ
$[8.47, 15.94)$	1	–
$[15.94, 16.06)$	2	2
$[16.06, 16.28)$	2	2.1
$[16.28, 16.55)$	2	2.2
⋮	⋮	⋮
$[22.16, 22.33)$	2	4.7
$[22.33, 22.40)$	3	4
$[22.40, 22.53)$	3	4.1
$[22.53, 22.67)$	3	4.2
⋮	⋮	⋮
$[26.16, 26.28)$	3	6.9
$[26.28, -)$	3	7

VI. Simulation Results and Discussions

In this section, we evaluate the performance of the proposed scheme under different types of attacks. We consider modulation orders $\{2, 4, 8\}$, corresponding to $m = 1, 2, 3$. Bob's SER threshold is set to FEC threshold 3.8×10^{-3}, and the relation between superposition parameter ρ_B and accurate Bob's SNR snr_B of W2A link is shown in Fig. 10 according (27). The mapping relationship between discrete ρ_B and snr_B is shown in Table I.



(a)

(b)

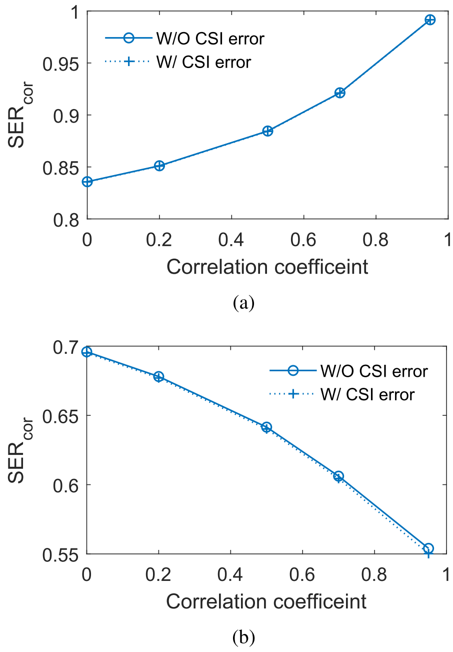
Fig. 11. The SER versus (a) SNR of Eve (average SNR of Bob is 20 dB) and (b) average SNR of Bob (SNR of Eve is 15 dB).

A. Channel Parameter Setting

In Section II-C, we experimentally measure the W2A and A2W link gains when Alice and Bob are located at (0, 0, -0.2) m and (0, 0, 0.7) m, respectively. The W2A link gain can be estimated from the A2W link gain based on correlation and 92% of relative estimation errors $(h_B - \hat{h}_B)/h_B$ are within 0.05. According to (29), the SNR estimation error range for Alice is set to $[\tau_1, \tau_2] = [-0.42, 0.45]$ dB. The lognormal distribution parameters of fitting Bob's channel gain are $u_1 = -5.21$ and $\sigma_1 = 0.59$ from the experimental results, and thus Bob's SNR snr_B follows the lognormal distribution with parameters (u, σ) in (6). We adopt average SNR of Bob ($\mathbb{E}(snr_B) = e^{u+\frac{1}{2}\sigma^2}$) to represent different channel conditions in the subsequent parts. The lognormal distribution parameters of Eve's channel gain are shown in Fig. 7(b) when Eve is located at (0.3 m, 0 m, 1.19 m) and (0.3 m, 0 m, 0.62 m). The measured link gain values are adopted to evaluate the SER of Alice-Eve link in Section VI-B to Section VI-F. In Section VI-G, limited by the size of the laboratory space, we investigate Eve's eavesdropping performance at more distant locations by adopting the theoretical model of channel gain in previous work [8].

B. Random Attack

Fig. 11(a) compares the SERs (cf., (5) and (7)) of the two random attack methods when the Bob's average SNR is 20 dB. For the first method, it is seen that the SERs decrease from 0.86 to 0.77 as Eve's SNR increases from 5 dB to 30 dB, and drop slightly under CSI estimation error. Since the second method randomly chooses modulation order and constellation point index, the SER performance is independent of Eve's SNR and remains at 0.90. Fig. 11(b) shows the SER versus Bob's



(a)

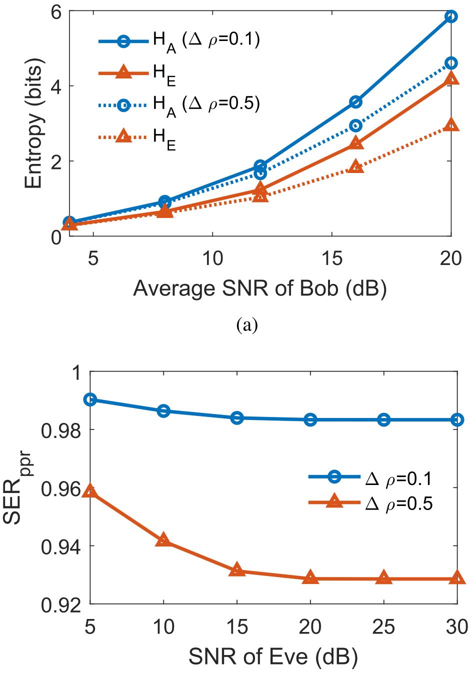
(b)

Fig. 12. The SER versus correlation coefficients when Eve is (a) at (0.3, 0, 1.19) m and (b) at (0.3, 0, 0.62) m.

average SNR when Eve's SNR is fixed at 15 dB. It is seen that when Bob's average SNR is low, there is a large probability that Alice does not transmit signal, such that the SERs of these two methods are close to 1. As Bob's average SNR increases, the probability of transmitting 2-PAM signal increases and the SER decreases for both methods. When Bob's average SNR keeps increasing, the SER of the second method begins to increase due to the lower probability of detecting 8-PAM symbols correctly. The SER of the first method without CSI estimation error drops to 0.74 as Bob's average SNR increases to 24 dB, since the probability that Bob and Eve select the same modulation type increases.

C. Correlated Attack

As in the previous section, we assume that Bob is at (0, 0, 0.7) m and Bob's average SNR is 20 dB. Fig. 12(a) shows the SER (cf., (9)) versus correlation coefficient between Alice-Bob channel and Alice-Eve channel. When Eve is located at (0.3, 0, 1.19) m away from Bob, the difference between Bob's and Eve's SNR values is large due to different link attenuation. It is seen that the SER increases with correlation coefficient and is beyond 0.84 for all correlation coefficients. The correlation coefficient is essentially a normalized measurement of the covariance after removing the mean SNRs of the two links, which reflects the increasing/decreasing trend correlation across the mean SNRs. Under large correlation coefficient, the SNRs of Alice-Bob channel and Alice-Eve channel will increase/decrease simultaneously across their mean SNRs, but the SNR values do not overlap under large difference in mean SNRs. Therefore, the modulation order and superposition parameter selected by Eve will be different from those for Bob in most cases. In addition, the SER without CSI error is identical to the SER with CSI error, since the detection error mainly comes from different modulation orders selected by Alice and Eve, and the difference of superposition parameters caused by CSI estimation error has little impact. In Fig. 12(b), when Eve is close enough to Bob (0.3, 0, 0.62) m, the SNR difference gets smaller. As the correlation coefficient increases, there is a high probability that Eve's SNR value is close to Bob's. Therefore, the probability of Eve choosing the correct modulation type increases and the SER decreases from 0.70 to 0.55. However, this is an unrealistic scenario as a passive eavesdropper can be detected if it is close to a legitimate receiver.



(a)

(b)

Fig. 13. (a) The entropy versus average SNR of Bob and (b) the SER versus Eve's SNR (average SNR of Bob is 20 dB).

D. Post-Processing Attack

Fig. 13(a) shows the entropies of Alice and Eve (cf., (14) and (15)) versus Bob's average SNR. It is seen that as Bob's average SNR increases to 20 dB, the number N_t of modulation types transmitted by Alice increases, and the entropies of Alice and Eve for $\Delta\rho = 0.1$ increase to 5.85 bits and 4.17 bits, respectively. If we change $\Delta\rho = 0.5$, the entropies of Alice and Eve increase to 4.61 bits and 2.93 bits, respectively. Smaller step size increases the variety of superposition parameters and increases the uncertainty of transmitted symbols, resulting in higher complexity of successful cracking for Eve. In Fig. 13(b), when symbol $(m^* = 2, \rho^* = 3, k^* = 3)$ is transmitted, the SER (cf., (16)) for $\Delta\rho = 0.1$ decreases from 0.99 to 0.98, and the SER for $\Delta\rho = 0.5$ decreases from 0.96 to 0.93 as Eve's SNR increases from 5 dB to 30 dB. The reason is that a higher SNR leads to an increase of the probability that transmitted symbol is in the potential set. Smaller step size of superposition parameters leads to a larger potential set, and further leads to a higher SER.

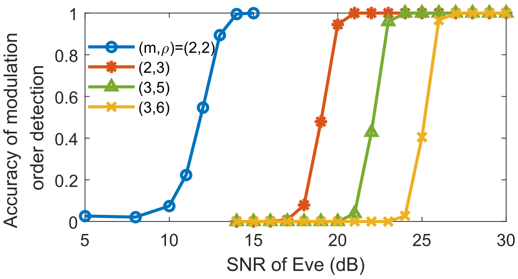
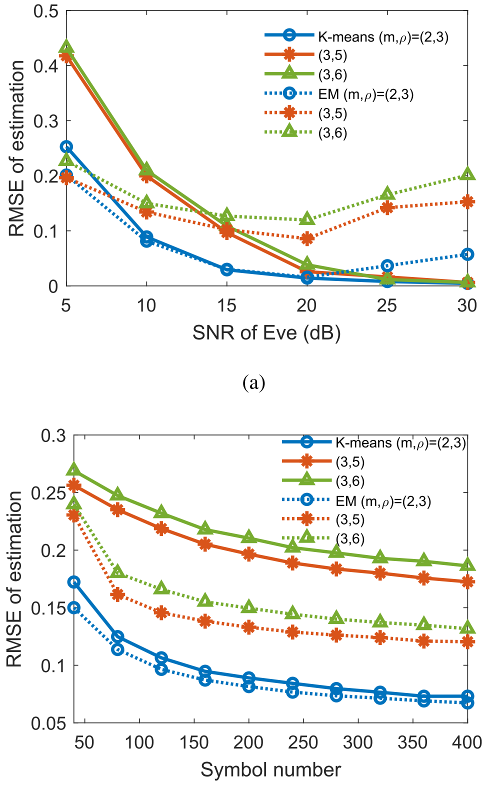


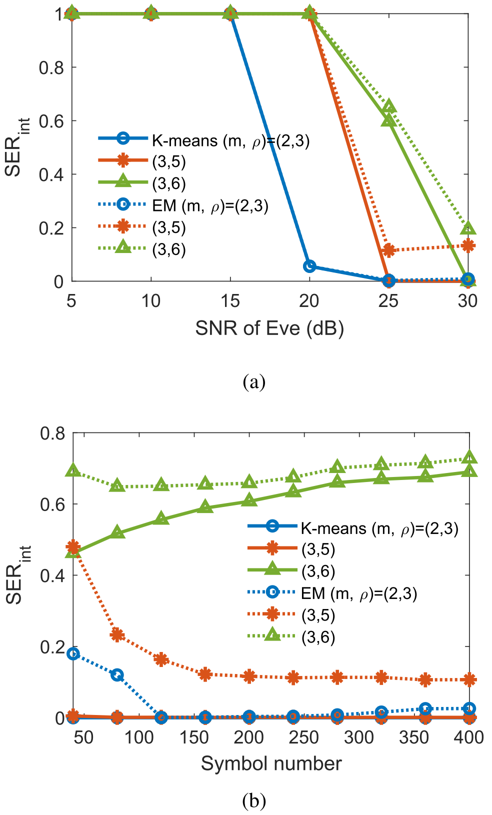
Fig. 14. The accuracy of modulation order detection versus Eve's SNR (symbol number is 200).



(a)

(b)

Fig. 15. The RMSE of estimation of constellation locations versus (a) SNR of Eve (symbol number is 200) and (b) symbol number (SNR of Eve is 10 dB).



(a)

(b)

Fig. 16. The SER versus (a) SNR of Eve (symbol number is 200) and (b) symbol number (SNR of Eve is 25 dB).

E. Intelligent Attack

Eve calculates Silhouette scores of different modulation orders (i.e., clustering numbers) to select the optimal value of the modulation order. The accuracy of modulation order detection is shown in Fig. 14. For equally spaced 4-PAM signal ($m = 2$, $\rho = 2$), Eve's SNR needs to be over 15 dB to achieve 100% accuracy of modulation order detection. As the modulation order and superposition parameter increase, Eve's SNR increases to 21 dB ($m = 2, \rho = 3$), 24 dB ($m = 3, \rho = 5$) and 28 dB ($m = 3$, $\rho = 6$) to achieve 100% accuracy of modulation order detection. The high SNR requirement for Eve implies low probability of successful demodulation in realistic scenarios.

In Fig. 15, we compare the estimation performance of constellation locations of K-means clustering and EM algorithm after the modulation order (clustering number) is correctly identified. For K-means clustering in Fig. 15(a), after running 10^4 times, the root mean square error (RMSE) for different modulation types (m, ρ) decreases to 6.31×10^{-3} as Eve's SNR increases to 30 dB. The RMSE of constellation estimation of EM algorithm is lower than that of K-means clustering in low SNR regime, but higher than that of K-means clustering in high SNR regime. Since EM algorithm has more initialization parameters than K-means clustering and is more sensitive to initialization, it is inferior to K-means in high SNR regime. Fig. 15(b) shows that the RMSE of constellation point estimation decreases with the collected symbol number (from 40 to 400), and tends to a stable value. Larger modulation order and superposition parameter yield higher stable value of RMSE.

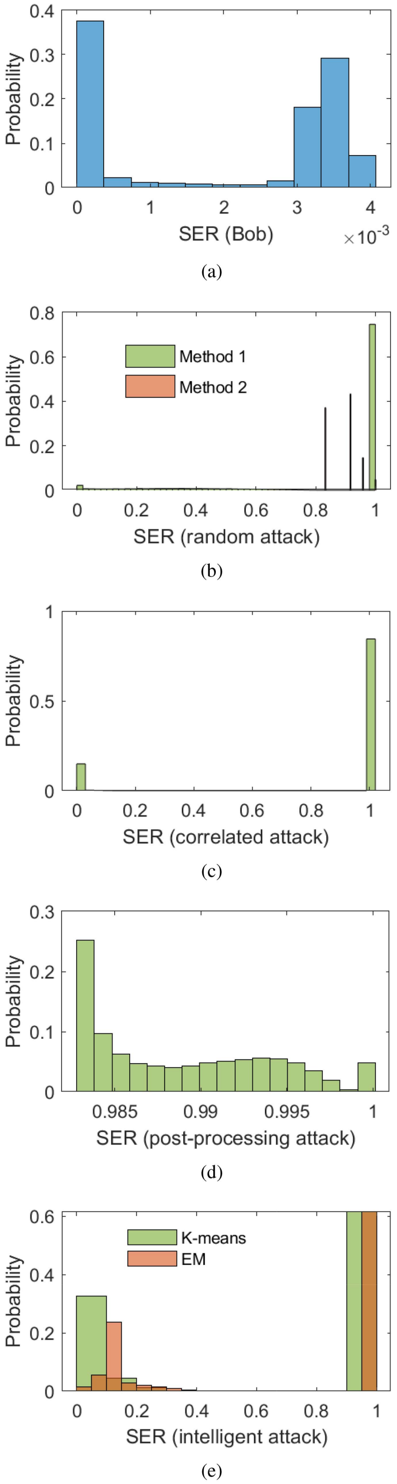
After modulation order detection and constellation location estimation, the SER performance SER_{int} is shown in Fig. 16. The SER of K-means for all three modulation types decreases to 8.40×10^{-3} when Eve's SNR increases to 30 dB, as shown in Fig. 16(a). In the low SNR regime, the low accuracy of modulation order detection results in SER of 1. The SER of EM algorithm is close to that of K-means algorithm when $(m, \rho) = (2, 3)$. However, for the other two modulation types, the SER of EM algorithm is higher than that of K-means algorithm in high SNR regime. It is seen from Fig. 16(b) that under Eve's SNR of 25 dB, the SER of K-means for $(m, \rho) = (3, 6)$ increases from 0.48 to 0.69 as the symbol number increases from 40 to 400. Since higher superposition parameter yields smaller distance of constellation points, which may further lead to the increase in the probability of near-constellation points being classified into one cluster, and the error probability of modulation order detection increases. For $(m, \rho) = (2, 3)$ and $(m, \rho) = (3, 5)$, as the number of symbols increases, SERs of K-means gradually reach steady value 0. It indicates that higher Eve's SNR leads to an increase in the successful demodulation probability for symbols with low superposition parameters.

F. Distributions of SER

Note that SER varies with the channel gain of each coherent time. In this subsection, we investigate the distributions of SER. Assume that Alice, Bob and Eve are located at (0, 0, -0.2) m, (0, 0, 0.7) m and (0.3, 0, 1.19) m, respectively. Assume that the average SNR of Bob is 20 dB. The SER is calculated for each frame of length 1000 within coherent time interval (2 ms), and 10^4 frames are adopted to investigate the distributions of SER.

The distributions of SER for Bob and Eve are shown in Fig. 17. For random, correlated and post-processing attacks, the SER is mostly distributed near 1 due to the incorrect selection of modulation parameters. For intelligent attack in Fig. 17(e), there exists a certain proportion of low SER since the clustering performance is significantly improved at high Eve's SNR as shown in Fig. 16(a).

The proportions of Eve's SER higher than Bob are 0.99 (random attack, method 1), 1 (random attack, method 2), 0.96 (correlated attack), 1 (post-processing attack), 0.89 (intelligent attack, K-means) and 0.99 (intelligent attack, EM), respectively. Such results imply that under W2A surface fluctuation, there is a large possibility that Eve has a higher SER than Bob in each frame. Higher decoding failure of Eve can be predicted if proper channel codes are adopted for Alice-Bob channel, which is beyond the communication capability of Alice-Eve link.



(a)

(b)

(c)

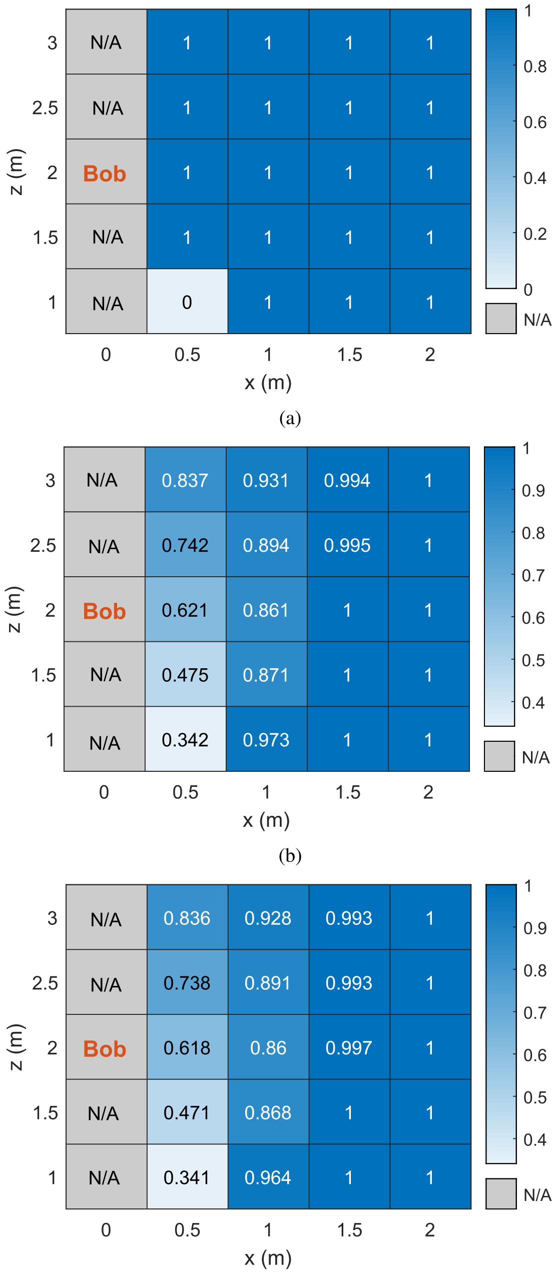
(d)

(e)

Fig. 17. The distributions of SER for (a) Bob, (b) random attack, (c) correlated attack, (d) post-processing attack and (e) intelligent attack.

G. Insecure Region

To investigate the insecure region, we adopt the theoretical model of channel gain in previous work [8] to calculate Eve's SER in different positions, where the statistical properties of link gains can match those from real measurements. Assume that Eve adopts K-means algorithm of intelligent attack to demodulate symbols, since it yields the smallest probability that Eve has a higher SER than Bob as shown in Section VI-F. Assume that Alice and Bob are located at (0, 0, -0.2) m and (0, 0, 2) m, respectively. In Fig. 18, we fix Eve's y-coordinate at 0 m and vary the x-coordinate and z-coordinate. Note that x-coordinate cannot be 0 since eavesdropper cannot block Bob's light path. When the water surface is calm as shown in Fig. 18(a), the channel gain and SNR do not vary with time. There is only one position (0.5, 0, 1) m where Eve's SER is lower than Bob's, since Eve is much closer to Alice than Bob and receives more optical power. In Fig. 18(b), for wave slope statistics in laboratory environment following truncated logistic distribution with parameter $\sigma_w = 6.7$ degrees in [8], the probability of Eve's SER higher than Bob's exceeds 0.99 in the positions with x-coordinate larger than 1.5 m. It is seen that the insecure region ($x < 1$ m and $z < 2$ m) is between Alice and Bob with small horizontal distance, but eavesdropping operation is unrealistic in such region. In Fig. 18(c), when wave intensity increases (truncated logistic distribution with parameter $\sigma_w = 10$ degrees), the probability of Eve's SER higher than Bob's at the same position decreases slightly compared with Fig. 18(b). Greater wave intensity increases the probability of Eve's channel gain higher than Bob's,



(a)

(b)

(c)

Fig. 18. The probabilities of Eve's SER higher than Bob's versus Eve's positions (Bob is at (0, 0, 2) m) for (a) calm surface, (b) wave surface (truncated logistic distribution $\sigma_w = 6.7$ degrees) and (c) wave surface (truncated logistic distribution $\sigma_w = 10$ degrees).

and decreases the probability of Eve's SER higher than Bob's. It is shown that the insecure region is also between Alice and Bob with small horizontal distance.

VII. Conclusion

In this work, we have investigated a PLS scheme for W2A-VLC systems. Based on high correlation between the W2A and A2W link gains verified by ray tracing simulation and experiment, the proposed scheme selects the modulation order and superposition parameter between the legitimate transceiver. Four attack types have been considered to investigate the security performance of the proposed scheme. Based on the link gains from real measurements, the SERs have been analyzed for both random and correlated attacks. It is shown that Eve's SER under random attack exceeds 0.77 when Eve's SNR varies from 5 dB to 30 dB, and under correlated attack Eve's SER decreases only for a high correlation coefficient when Eve is close enough to Bob. In addition, the entropy of potential set under post-processing attack has been derived, demonstrating that the complexity of successful cracking increases with the number of modulation types. For intelligent attack, the K-means clustering and EM algorithm are adopted to identify the modulation type, where a larger modulation order and superposition parameter lead to larger RMSE due to small distance of adjacent constellation points. The distributions of Eve' SER show that the probability of Eve's SER higher than Bob's is higher than 0.9 for other types of attacks, except for K-means-based intelligent attack with probability 0.89. In addition, the probability of Eve's SER higher than Bob's under K-means-based intelligent attack is investigated for different Eve's positions. It is shown that insecure region where such probability is lower than 0.5 under wavy water surface is enlarged compared to calm surface. Such region is only located between Alice and Bob with small horizontal distance, which is unrealistic for eavesdropping operation. Greater wave intensity increases the probability of Eve's channel gain higher than Bob's, and decreases the probability of Eve's SER higher than Bob's. Analytical and simulation results demonstrate a significant improvement in secrecy performance of W2A-VLC.

Appendix A
Proof of Theorem 1

The partial derivative of P_s with respect to ρ_B for 4-PAM signal is given by

$$\frac{\partial P_s}{\rho_B} = \frac{\sqrt{snr_E}}{\sqrt{\left(1+{\rho_B}^2\right)^5}} \exp\left(-\frac{\left(2-2\rho_B+{\rho_B}^2\right) snr_E}{2\left(1+{\rho_B}^2\right)}\right) \times \left(1+{\rho_B}^2\right)\left(\frac{1+\rho_B}{2\sqrt{2\pi}}\exp\left(\frac{snr_E}{2+2{\rho_B}^2}\right) - \frac{\rho_B}{\sqrt{2\pi}}\exp\left(\frac{\left(\rho_B-1\right)^2 snr_E}{2+2{\rho_B}^2}\right)\right). \tag{31}$$

Since $\frac{1+\rho_B}{2} < \rho_B$ and $(\rho_B - 1)^2 \geq 1$ for $\rho_B \geq 2$, we have $\frac{\partial P_s}{\partial \rho_B} \leq 0$ for $\rho_B \geq 2$. The partial derivative of P_s with respect to ρ_B for 8-PAM signal is derived as

$$\frac{\partial P_s}{\rho_B} = \frac{\sqrt{snr_E}}{4\sqrt{2\pi\left(5+{\rho_B}^2\right)^3}} \exp\left(-\frac{\left(10-6\rho_B+{\rho_B}^2\right) snr_E}{2\left(5+{\rho_B}^2\right)}\right) \times \left(-6\rho_B\exp\left(\frac{\left(\rho_B-3\right)^2 snr_E}{2\left(5+{\rho_B}^2\right)}\right) + \left(5+3\rho_B\right)\exp\left(\frac{snr_E}{2\left(5+{\rho_B}^2\right)}\right)\right). \tag{32}$$

Since $6\rho_B > 5 + 3\rho_B$ and $(\rho_B - 3)^2 \geq 1$ for $\rho_B \geq 4$, we have $\frac{\partial P_s}{\partial \rho_B} \leq 0$ for $\rho_B \geq 4$. In summary, we have proved that the probability P_s of correct demodulation decreases monotonically with ρ_B when $\rho_B \geq 2$ for 4-PAM and $\rho_B \geq 4$ for 8-PAM.

References

[1] H. Luo, J. Wang, F. Bu, R. Ruby, K. Wu, and Z. Guo, "Recent progress of air/water cross-boundary communications for underwater sensor networks: A review," *IEEE Sensors J.*, vol. 22, no. 9, pp. 8360–8382, May 2022.

[2] F. Tonolini and F. Adib, "Networking across boundaries: Enabling wireless communication through the water-air interface," in *Proc. Conf. ACM Special Int. Group Data Commun.*, 2018, pp. 117–131.

[3] X. Sun et al., "Field demonstrations of wide-beam optical communications through water–air interface," *IEEE Access*, vol. 8, pp. 160480–160489, Sep. 2020.

[4] T. Lin, N. Huang, C. Gong, J. Luo, and Z. Xu, "Preliminary characterization of coverage for water-to-air visible light communication through wavy water surface," *IEEE Photon. J.*, vol. 13, no. 1, pp. 1–13, Jan. 2021.

[5] J. A. Simpson, B. L. Hughes, and J. F. Muth, "Smart transmitters and receivers for underwater free-space optical communication," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 5, pp. 964–974, Jun. 2012.

[6] Z. Xu, W. Liu, Z. Wang, and L. Hanzo, "Petahertz communication: Harmonizing optical spectra for wireless communications," *Digit. Commun. Netw.*, vol. 7, no. 4, pp. 605–614, Aug. 2021.

[7] M. Obeed, A. M. Salhab, M.-S. Alouini, and S. A. Zummo, "Survey on physical layer security in optical wireless communication systems," in *Proc. IEEE 7th Int. Conf. Commun. Netw.*, 2018, pp. 1–5.

[8] Q. Hu, C. Gong, T. Lin, J. Luo, and Z. Xu, "Secrecy performance analysis for water-to-air visible light communication," *J. Lightw. Technol.*, vol. 40, no. 14, pp. 4607–4620, Apr. 2022.

[9] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, Nov. 2015.

[10] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor, "On the throughput of secure hybrid-ARQ protocols for Gaussian block-fading channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1575–1591, Apr. 2009.

[11] J. M. Hamamreh and H. Arslan, "Joint PHY/MAC layer security design using ARQ with MRC and null-space independent PAPR-aware artificial noise in SISO systems," *IEEE Trans. Wireless Commun.*, vol. 17, no. 9, pp. 6190–6204, Jul. 2018.

[12] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surv. Tuts.*, vol. 21, no. 2, pp. 1773–1828, Oct. 2018.

[13] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[14] S. N. Premnath et al., "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, Mar. 2012.

[15] H. Zhang, Z. Ji, H. Wang, and W. Wu, "Survey on quantum information security," *China Commun.*, vol. 16, no. 10, pp. 1–36, Oct. 2019.

[16] A. Mostafa and L. Lampe, "Physical-layer security for indoor visible light communications," in *Proc. IEEE Int. Conf. Commun.*, 2014, pp. 3342–3347.

[17] S. Cho, G. Chen, and J. P. Coon, "Securing visible light communication systems by beamforming in the presence of randomly distributed eavesdroppers," *IEEE Trans. Wireless Commun.*, vol. 17, no. 5, pp. 2918–2931, May 2018.

[18] A. Mostafa and L. Lampe, "Securing visible light communications via friendly jamming," in *Proc. IEEE Globecom Workshops*, 2014, pp. 524–529.

[19] S. Cho, G. Chen, and J. P. Coon, "Cooperative beamforming and jamming for secure VLC system in the presence of active and passive eavesdroppers," *IEEE Trans. Green Commun. Netw.*, vol. 5, no. 4, pp. 1988–1998, Dec. 2021.

[20] J. M. Hamamreh, E. Basar, and H. Arslan, "OFDM-subcarrier index selection for enhancing security and reliability of 5G URLLC services," *IEEE Access*, vol. 5, pp. 25863–25875, Nov. 2017.

[21] A. Mukherjee and A. L. Swindlehurst, "Robust beamforming for security in MIMO wiretap channels with imperfect CSI," *IEEE Trans. Signal Process.*, vol. 59, no. 1, pp. 351–361, Jan. 2010.

[22] Y. Shi, M. Badi, D. Rajan, and J. Camp, "Channel reciprocity analysis and feedback mechanism design for mobile beamforming systems," *IEEE Trans. Veh. Technol.*, vol. 70, no. 6, pp. 6029–6043, May 2021.

[23] M. Xiu, L. Li, Y. Wang, L. Wang, and W. Hou, "Pierson-Moscowitz spectrum simulation based on the rough sea surface," *J. Phys.: Conf. Ser.*, vol. 1971, no. 1, pp. 012050–012056, 2021.

[24] M. G. Solonenko and C. D. Mobley, "Inherent optical properties of jerlov water types," *Appl. Opt.*, vol. 54, no. 17, pp. 5392–5401, 2015.

[25] P. A. Hoeher and T. Wo, "Superposition modulation: Myths and facts," *IEEE Commun. Mag.*, vol. 49, no. 12, pp. 110–116, Dec. 2011.

[26] S. Althunibat, V. Sucasas, and J. Rodriguez, "A physical-layer security scheme by phase-based adaptive modulation," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 9931–9942, Nov. 2017.

[27] Z. Zhu and A. K. Nandi, *Automatic Modulation Classification: Principles, Algorithms and Applications*. Hoboken, NJ, USA: Wiley Inc., 2015.

[28] P. J. Rousseeuw, "Silhouettes: A graphical aid to the interpretation and validation of cluster analysis," *J. Comput. Appl. Math.*, vol. 20, pp. 53–65, Nov. 1987.

[29] V.-E. Neagoe and V. Chirila-Berbentea, "Improved Gaussian mixture model with expectation-maximization for clustering of remote sensing imagery," in *Proc. IEEE Int. Geosci. Remote Sens. Symp.*, 2016, pp. 3063–3065.

Qingqing Hu received the B.S. degree from the Dalian University of Technology, Dalian, China, in 2016, the M.S. degree in 2019 from the University of Science and Technology of China, Hefei, China, where she is currently working toward the Ph.D. degree. Her research interests include physical layer security, signal processing, and visible light communication.

Nuo Huang received the B.S. degree in electronics and information engineering from the Huazhong University of Science and Technology, Wuhan, China, in 2012, and the Ph.D. degree in information and communication engineering from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in 2019. He is currently a Research Associate with the Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei, China. From December 2015 to June 2017, he was a Visiting Student with the Department of Electrical Engineering, Columbia University, New York, NY, USA. He was selected by the National Postdoctoral Program for Innovative Talents in 2019. His research interests include resource allocation and transceiver design in (optical) wireless communications.

Chen Gong (Senior Member, IEEE) received the B.S. degree in electrical engineering and mathematics (minor) from Shanghai Jiaotong University, Shanghai, China, in 2005, the M.S. degree in electrical engineering from Tsinghua University, Beijing, China, in 2008, and the Ph.D. degree from Columbia University, New York City, NY, USA, in 2012. From 2012 to 2013, he was a Senior Systems Engineer with the Qualcomm Research, San Diego, CA, USA. He is currently a Faculty Member with the University of Science and Technology of China, Hefei, China. His research interests include wireless communications, optical wireless communications, and signal processing. He was the recipient of the Hongkong Qiushi Outstanding Young Researcher Award in 2016.