IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 19 June 2022, accepted 14 July 2022, date of publication 19 July 2022, date of current version 4 August 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3192400

METHODS

A Method for Underwater Acoustic Key Detection Based on OFDM Pilot Sequences

XINYU LI, GANG XIN, BIN WANG, AND YAN HUANG
PLA Strategic Support Force Information Engineering University, Zhengzhou 450001, China
Corresponding author: Bin Wang (commutech@163.com)

ABSTRACT The traditional physical layer key generation technology uses channel temporal variation, reciprocity, and spatial decorrelation to realize key distribution and fast update. However, due to the complex, time-varying and time-delayed features, the underwater acoustic channel environment often changes during channel detection, resulting in impaired channel reciprocity. To solve this problem, this paper proposes an orthogonal frequency division multiplexing pilot structure based on the features of underwater acoustic time-varying multipath channel. The structure can complete key detection when channel reciprocity is impaired, promotes the consistency of observation sequences, and reduces the key disagreement rate. The theoretical deduction proves the validity of the proposed method under an underwater acoustic multipath time-varying channel. Also, the simulation results verify the feasibility of the proposed method.

INDEX TERMS Physical layer security, channel detection, orthogonal frequency division multiplexing.

I. INTRODUCTION

Physical-layer key generation is a security technology that directly uses channel features as a random source to generate keys. With the advantages of no key distribution, high security, and fast key update, it exploits the reciprocity of wireless channels to generate random keys, uses the spatial decorrelation to ensure the security, and utilizes the channel temporal variation to ensure the rapid update [1]–[3]. Physical-layer key generation usually includes channel detection, feature extraction, quantization, key negotiation, and privacy amplification. It can effectively solve the problems of difficult key distribution and easy loss of cryptographic equipment in underwater acoustic (UWA) secure communication. In recent years, the physical-layer key generation has attracted extensive attention in academia and has broad prospects.

The physical-layer key generation technology of radio communication has evolved fast, e.g., wireless local area networks [4]–[5], wireless sensor networks [6] and RIS [7]. Because of the reciprocity, decorrelation and time-varying features of UWA channels, the idea of physical-layer key generation has been extended to the UWA field. In 2016, Luo proposed to realize physical-layer key generation by using the UWA received signal strength (RSS) as the random source, systematically studied the feasibility of applying the physical layer key generation technology to the UWA environment, and proposed to use orthogonal frequency division multiplexing (OFDM) to promote the key generation rate and use smoothing filter to enhance the reciprocity of detection sequences [8]. However, it only introduced the traditional radio key generation technology into the UWA field, without utilizing the features of the UWA channel; Then, the UWA physical-layer key generation system was built in [9]–[12], and the feasibility of the system was verified through field experiments. The works briefly discussed the features of the UWA channel suitable for key generation, but they did not discuss the problem of impaired reciprocity caused by the large delay of the UWA channel in time-division half-duplex systems; By exploring the application of the UWA physical-layer key, the underwater covert communication was completed in 2019 [13]. However, it did not fully consider the features of the UWA channel, and the range of communication was only 60 meters in the field experiment, which is difficult to satisfy actual needs. In a word, the research on the UWA key generation technology is still preliminary with many problems to be solved.

The associate editor coordinating the review of this manuscript and approving it for publication was Jie Tang.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

The first step of UWA key generation is channel detection. In this step, legitimate users can obtain the observation sequence that can extract the channel features and generate the same key. UWA communication is mainly half-duplex. The reciprocity of a half-duplex communication channel will be affected by transmission delay, system delay, device fingerprint, and noise. Due to the slow propagation rate of underwater sound, the influence of transmission delay on reciprocity is more obvious.

Assuming that the sound speed is 1500 m/s and the communication distance is 1 km, it takes about 1.3 seconds to complete the two-way transmission of half-duplex communication. Meanwhile, the time-varying channel will damage the channel reciprocity, due to the relative movement, the change in the hydrological environment and other factors. When channel features are used as the random source to extract observation sequences, the time-varying random source will reduce the correlation of the observation sequences and affect the subsequent steps such as feature extraction and quantization. To solve this problem, the local pilot auxiliary wait protocol (LPAWP) was proposed [14], which provides a new idea to solve the impaired reciprocity problem in time-division half-duplex systems. However, this method assumes that the channel is flat fading. In fact, both frequency selective fading and time selective fading of UWA channels have impact on channel detection. The frequency selective fading makes it difficult for LPAWP to obtain low key disagreement rate (KDR). While, for the time selective fading caused by relative movement, a communication scenario with low speed is considered and the suitable detection signal length can be selected to attenuate the effect of time selective fading on channel detection. Therefore, this paper mainly discusses the UWA channel frequency selective fading and the impaired channel reciprocity due to environmental changes caused by relative movement.

Inspired by [14], this paper designs a key detection method based on the OFDM pilot for the UWA channel by fully considering the time-varying and frequency selective fading characteristics of the UWA channel. Then, the applicable conditions are demonstrated, and the applicability is verified through simulation experiments.

II. KEY DETECTION IN UWA PHYSICAL LAYER BASED ON OFDM PILOT

A. SIGNAL MODEL

OFDM utilizes orthogonal subcarriers to carry different data to complete information transmission, which has the advantages of immunity to frequency selective fading, high spectrum efficiency, simple system implementation and easy channel estimation [15]. When it is applied to physical-layer key generation, OFDM channel frequency response (CFR) has rich characteristic information to estimate, which contributes to high KDR.

Based on the advantages, OFDM modulation is used as the detection signal in this study. Because of orthogonal

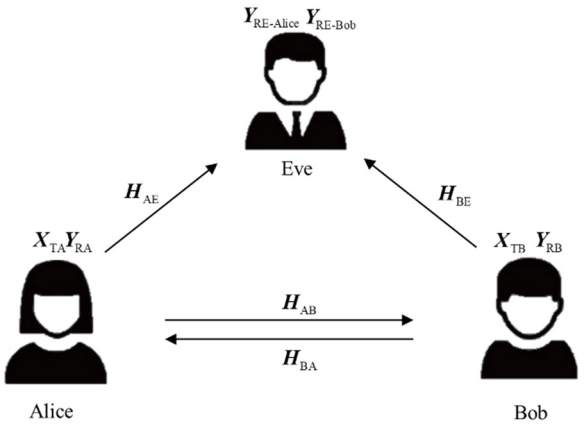


FIGURE 1. The typical scene of physical layer key generation.

subcarriers, an OFDM symbol containing N subcarriers can be given as [16]

$$\mathbf{X} = \begin{bmatrix} X(1) & 0 & \cdots & 0 \\ 0 & X(2) & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & X(N) \end{bmatrix}, \tag{1}$$

where $X(k)$ is complex data on the k-th subcarrier. Assuming that the CFR is $H(k)$ and the noise is $W(k)$ on the k-th subcarrier, the received OFDM symbol is given as, (2), shown at the bottom of the next page, where $\boldsymbol{H}$ is channel vector (i.e., $\boldsymbol{H} = [H(1), H(2), \ldots, H(N)]^{\mathrm{T}}$) and $\mathbf{W}$ is Gaussian noise vector (i.e., $\boldsymbol{W} = [W(1), W(2), \ldots, W(N)]^{\mathrm{T}}$). The channel $\boldsymbol{H}$ is frequency selective fading channel in this paper. And when Doppler exists, the frequency offset f_{d} is considered. The channel $\boldsymbol{H}$ can be expressed as

$$\mathbf{H} = \begin{bmatrix} H(1) \\ H(2) \\ \vdots \\ H(N) \end{bmatrix} = \begin{bmatrix} \tilde{H}(1) f_{\mathrm{d}}(1) \\ \tilde{H}(2) f_{\mathrm{d}}(2) \\ \vdots \\ \tilde{H}(N) f_{\mathrm{d}}(N) \end{bmatrix}. \tag{3}$$

The received symbol $Y(k)$ on the k-th subcarrier is given as

$$Y(k) = X(k) H(k) + W(k), k = 1, 2, \ldots, N. \tag{4}$$

B. CHANNEL DETECTION METHOD

1) BASIC PRINCIPLE OF KEY DETECTION IN UWA PHYSICAL LAYER KEY GENERATION

As illustrated in Fig. 1, Alice and Bob are the legitimate users who want to perform key generation using the UWA channel, and Eve is an eavesdropper.

Alice and Bob send detection signals $\boldsymbol{X}_{\mathbf{TA}}$ and $\boldsymbol{X}_{\mathbf{TB}}$ respectively, and they use the received signals $\mathbf{Y}_{\mathbf{RA}}$ and $\boldsymbol{Y}_{\mathbf{RB}}$ to generate observation sequences that can characterize the randomness of $\boldsymbol{H}_{\mathbf{AB}}$ and $\boldsymbol{H}_{\boldsymbol{BA}}$. The passive eavesdropper Eve does not send signals but only generates observation sequences by using the received signals $\boldsymbol{Y}_{\mathbf{RE-Alice}}$ and

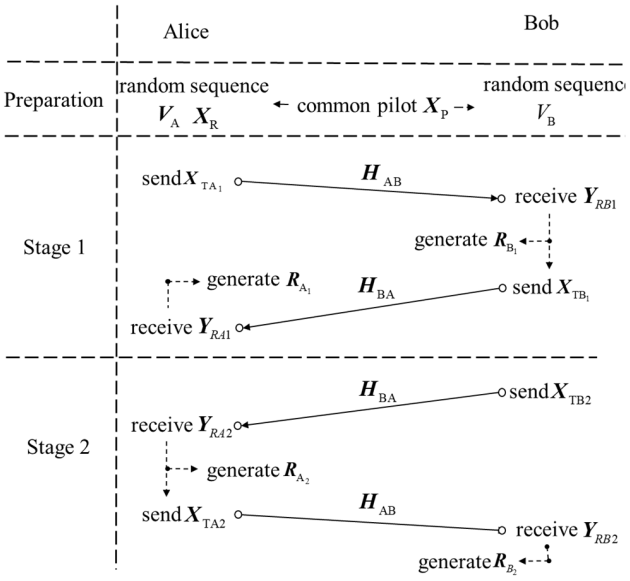


FIGURE 2. The process of physical layer key detection.

$\boldsymbol{Y}_{\mathbf{RE-Bob}}$, which can characterize the randomness of $\boldsymbol{H}_{\mathbf{AE}}$ and $\boldsymbol{H}_{\mathbf{BE}}$.

When the UWA channel reciprocity between Alice and Bob is damaged, i.e., the consistency between $\boldsymbol{H}_{\mathbf{AB}}$ and $\boldsymbol{H}_{\mathbf{BA}}$ is low, LPAWP is proposed. By using different OFDM subcarriers to carry different pilots, legitimate users extract keys from two random sources of positive and negative channels through information interaction.

As shown in Fig. 2, Alice generates random sequences $\boldsymbol{V}_{\mathbf{A}}$ and $\boldsymbol{X}_{\mathbf{R}}$, and Bob generates random sequences $\boldsymbol{V}_{\mathbf{B}}$. The common pilot sequence $\boldsymbol{X}_{\mathbf{P}}$ is pre-stored by Alice and Bob. In stage 1, Alice sends $\boldsymbol{X}_{\mathbf{TA}_1}$ for channel detection. After receiving $\boldsymbol{Y}_{\mathbf{RB}_1}$, Bob sends $\boldsymbol{X}_{\mathbf{TB}_1}$ containing the information of$\boldsymbol{H}_{\mathbf{AB}}$. Then, Alice can receive $\boldsymbol{Y}_{\mathbf{RA}_1}$.Through $\boldsymbol{Y}_{\mathbf{RA}_1}$ and $\boldsymbol{Y}_{\mathbf{RB}_1}$, Alice and Bob can obtain the channel observation sequences $\boldsymbol{R}_{\mathbf{A}_1}$ and $\boldsymbol{R}_{\mathbf{B}_1}$ respectively, both of which contain random source $\boldsymbol{H}_{\mathbf{AB}}$. At this time, stage 1 of channel detection ends. In stage 2, Bob sends $\boldsymbol{X}_{\mathbf{TB}_2}$. After receiving $\boldsymbol{Y}_{\mathbf{RA}_2}$, Alice sends $\boldsymbol{X}_{\mathbf{TA}_1}$ containing information of $\boldsymbol{H}_{\mathbf{BA}}$. Then Bob can receive $\boldsymbol{Y}_{\mathbf{RB}_2}$. Through $\boldsymbol{Y}_{\mathbf{RA}_2}$ and $\boldsymbol{Y}_{\mathbf{RB}_2}$, Alice and Bob can obtain the channel observation sequences $\boldsymbol{R}_{\mathbf{A}_2}$ and $\boldsymbol{R}_{\mathbf{B}_2}$ respectively, both of which contain random source $\boldsymbol{H}_{\mathbf{BA}}$. Stage 2 of channel detection ends. After two stages, the observation sequences are generated by using both $\boldsymbol{H}_{\mathbf{AB}}$ and $\boldsymbol{H}_{\mathbf{BA}}$, which can generate the consistent key.

Stage 2 is similar to stage 1, so this paper only discusses the details of stage 1 without losing generality. By placing pilot sequences and different random sequences on odd and even OFDM subcarriers, LPAWP realizes channel detection and information exchange. In high signal-to-noise ratio (SNR) cases, the observed value on the k-th subcarrier obtained by Alice is given as [14]

$$R_{\mathrm{A}_1}(k) = H_{\mathrm{AB}}(2k-1)\frac{H_{\mathrm{BA}}(2k)}{H_{\mathrm{BA}}(2k-1)}V_{\mathrm{A}}(k), \quad k = 1, 2, \ldots, \frac{N}{2}. \tag{5}$$

The observed value on the k-th subcarrier obtained by Bob is given as

$$R_{\mathrm{B}_1}(k) = H_{\mathrm{AB}}(2k)V_{\mathrm{A}}(k), k = 1, 2, \ldots, \frac{N}{2} \tag{6}$$

where $H(k)$ is the CFR of the forward channel on the k-th subcarrier, $V(k)$ is the random value generated on the k-th subcarrier, and $R(k)$ is the observed value on the k-th subcarrier, which can be used to generate keys. Under a small spacing of adjacent subcarriers and a large channel coherence, the constraint condition can be given as

$$H(2j) \approx H(2j-1), j = 1, 2, \ldots, \frac{N}{2} \tag{7}$$

According to (7), (5) can be rewritten as

$$R_{\mathrm{A}_1}(k) = H_{\mathrm{AB}}(2k-1)V_{\mathrm{A}}(k), k = 1, 2, \ldots, \frac{N}{2} \tag{8}$$

The key detection consistency can be expressed by mean square error (MSE) (i.e., $E\{(\boldsymbol{R}_A - \boldsymbol{R}_B)^H \bullet (\boldsymbol{R}_A - \boldsymbol{R}_B)\}$). At high SNR cases, the MSE between $\boldsymbol{R}_{\mathrm{A}}$ and $\boldsymbol{R}_{\mathrm{A}}$ can be expressed as, (9), shown at the bottom of the next page.

(9) is equal to 0 if and only if the coherence of adjacent subcarriers is large. That is, when (7) is satisfied, the results of key detection are consistent. However, the correlation bandwidth of the UWA channel is very narrow, which is prone to frequency selective fading. It is difficult to guarantee that the channel response of adjacent frequencies is consistent, and the MSE of the observed sequences will be affected by the channel.

2) CHANNEL DETECTION BASED ON OFDM PILOT DESIGN

Considering the frequency selective fading and impaired reciprocity, the OFDM pilot structure for sequence detection is optimized during channel detection. The algorithm flow is similar to that shown in Fig. 2, but the content of detection

$$\boldsymbol{Y} = \begin{bmatrix} Y(1) \\ Y(2) \\ \vdots \\ Y(N) \end{bmatrix} = \begin{bmatrix} X(1) & 0 & \cdots & 0 \\ 0 & X(2) & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & X(N) \end{bmatrix} \begin{bmatrix} H(1) \\ H(2) \\ \vdots \\ H(N) \end{bmatrix} + \begin{bmatrix} W(1) \\ W(2) \\ \vdots \\ W(N) \end{bmatrix}, \\ = \boldsymbol{X}\boldsymbol{H} + \boldsymbol{W} \tag{2}$$

X_{TA_1}

$X_R(1)$	$V_A(1)X_P(1)$
$X_R(2)$	$V_A(2)X_P(2)$
…	…
$X_R(k)$	$V_A(k)X_P(k)$
…	…
$X_R(N)$	$V_A(N)X_P(N)$

X_{TB_1}

$V_B(1)H_{AB}(1,1)X_R(1)$	$V_B(1)X_P(1)$
$V_B(2)H_{AB}(2,1)X_R(2)$	$V_B(2)X_P(2)$
…	…
$V_B(k)H_{AB}(k,1)X_R(k)$	$V_B(k)X_P(k)$
…	…
$V_B(N)H_{AB}(N,1)X_R(N)$	$V_B(N)X_P(N)$

FIGURE 3. The pilot structures of OFDM sequences.

sequences differs. In this paper, n OFDM symbols are used to realize information exchange. The simplified UWA channel model is used for theoretical derivation. When cyclic prefix (CP) is used, we can assume no inter symbol interference (ISI) between OFDM blocks. And (4) can be extended to, (10), as shown at the bottom of the page, where $Y(k,i)$ is the receive symbol, $X(k,i)$ is the transmit symbol, $H(k,i)$ is the CFR, and $W(k,i)$ is the Gaussian noise on the i-th OFDM symbol of the k-th subcarrier. The pilot structures of the transmitted OFDM pilot symbol $\mathbf{X}_{\mathrm{TA}_1}$ and $\mathbf{X}_{\mathrm{TB}_1}$ are shown in Fig. 3.

On the k-th subcarrier, channel detection can be divided into four steps:

Step 1: The phase of preparation.

Alice generates local pilot symbols $V_{\mathrm{A}}(k)$ and $X_{\mathrm{R}}(k)$, and Bob generates local pilot symbol $V_{\mathrm{B}}(k)$. The common pilot symbol $X_{\mathrm{P}}(k)$ is stored in Alice and Bob in advance. $V_{\mathrm{A}}(k)$, $X_{\mathrm{R}}(k)$, $V_{\mathrm{B}}(k)$ and $X_{\mathrm{P}}(k)$ are OFDM pilot symbols on the k-th subcarrier. Before each round of detection, the local pilot symbols are generated randomly. So, they cannot be obtained by Eve.

Step 2: The phase of Alice's sending.

Alice sends the pilot sequences $\boldsymbol{X}_{\mathrm{TA}_1}$ that are composed of two OFDM symbols. $\boldsymbol{X}_{\mathrm{TA}_1}$ can be written as

$$\mathbf{X}_{\mathrm{TA}_1} = \begin{cases} X_{\mathrm{TA}_1}(k,1) = X_{\mathrm{R}}(k), i = 1 \\ X_{\mathrm{TA}_1}(k,2) = V_{\mathrm{P}}(k)X_{\mathrm{P}}(k), i = 2 \\ k = 1,2,\ldots,N. \end{cases}, \quad (11)$$

Step 3: The phase of Bob's receiving, processing and sending.

Bob receives $\boldsymbol{Y}_{\mathrm{RB}_1}$, which can be given as

$$\boldsymbol{Y}_{\mathrm{RB}_1} = \begin{cases} Y_{\mathrm{RB}_1}(k,1) = H_{\mathrm{AB}}(k,1)X_{\mathrm{TA}_1}(k,1) + W_{\mathrm{B}}(k,1) \\ \quad = H_{\mathrm{AB}}(k,1)X_{\mathrm{R}}(k) + W_{\mathrm{B}}(k,1), i = 1 \\ Y_{\mathrm{RB}_1}(k,2) = H_{\mathrm{AB}}(k,2)X_{\mathrm{TA}_1}(k,2) + W_{\mathrm{B}}(k,2) \\ \quad = H_{\mathrm{AB}}(k,2)V_{\mathrm{A}}(k)X_{\mathrm{P}}(k) + W_{\mathrm{B}}(k,2), i = 2 \end{cases}, \quad k = 1,2,\ldots,N \quad (12)$$

where $W_{\mathrm{B}}(k,i)$ is the local Gaussian noise at Bob. With $Y_{\mathrm{RB}_1}(k,2)$ and $X_{\mathrm{P}}(k)$, The observation symbol of Bob can be obtained by

$$R_{\mathrm{B}_1}(k) = \frac{Y_{\mathrm{RB}_1}(k,2)}{X_{\mathrm{P}}(k)} = \frac{H_{\mathrm{AB}}(k,2)V_{\mathrm{A}}(k)X_{\mathrm{P}}(k) + W_{\mathrm{B}}(k,2)}{X_{\mathrm{P}}(k)}, \quad k = 1,2,\ldots,N \quad (13)$$

At high SNR cases, (13) can be approximately expressed as

$$R_{\mathrm{B}_1}(k) \approx H_{\mathrm{AB}}(k,2)V_{\mathrm{A}}(k), k = 1,2,\ldots,N. \quad (14)$$

Then Bob sends pilot sequences $\boldsymbol{X}_{\mathrm{TB}_1}$ containing $Y_{\mathrm{RB}_1}(k,1)$ and $V_{\mathrm{B}}(k)$, which can be written as, (15), shown at the bottom of the next page.

Step 4: The phase of Alice's receiving and processing.

Alice receives $\boldsymbol{Y}_{\mathrm{RA}_1}$, which can be given as

$$\boldsymbol{Y}_{\mathrm{RA}_1} = \begin{cases} Y_{\mathrm{RA}_1}(k,1) = H_{\mathrm{BA}}(k,1)X_{\mathrm{TB}_1}(k,1) + W_{\mathrm{A}}(k,1) \\ = H_{\mathrm{BA}}(k,1)V_{\mathrm{B}}(k)(H_{\mathrm{AB}}(k,1)X_{\mathrm{R}}(k) \\ +W_{\mathrm{B}}(k,1)) + W_{\mathrm{A}}(k,1), i = 1 \\ Y_{\mathrm{RA}_1}(k,2) = H_{\mathrm{BA}}(k,2)X_{\mathrm{TB}_1}(k,2) + W_{\mathrm{A}}(k,2) \\ = H_{\mathrm{BA}}(k,2)V_{\mathrm{B}}(k)X_{\mathrm{P}}(k) + W_{\mathrm{A}}(k,2), i = 2 \end{cases} \quad k = 1,2,\ldots,N, \quad (16)$$

where $W_{\mathrm{A}}(k,i)$ is the local Gaussian noise at Alice. With $V_{\mathrm{A}}(k)$, $X_{\mathrm{R}}(k)$ and $X_{\mathrm{P}}(k)$, the observation symbol of Alice

$$\begin{aligned} \mathrm{MSE} &= E\{(\boldsymbol{R}_A - \boldsymbol{R}_B)^H(\boldsymbol{R}_A - \boldsymbol{R}_B)\} \\ &= \frac{2}{N}\sum_{k=1}^{\frac{N}{2}} \begin{bmatrix} (H_{AB}(2k) - H_{AB}(2k-1)\frac{H_{BA}(2k)}{H_{BA}(2k-1)})^*(H_{AB}(2k) \\ -H_{AB}(2k-1)\frac{H_{BA}(2k)}{H_{BA}(2k-1)}) \end{bmatrix} \end{aligned} \quad (9)$$

$$\begin{bmatrix} Y(k,1) \\ Y(k,2) \\ \cdots \\ Y(k,i) \\ \cdots \\ Y(k,n) \end{bmatrix} = \begin{bmatrix} H(k,1) & 0 & \cdots & 0 \\ 0 & H(k,2) & \cdots & 0 \\ & & \ddots & \\ \vdots & \vdots & H(k,i) & \vdots \\ & & & \ddots \ 0 \\ 0 & 0 & \cdots & 0 \ H(k,n) \end{bmatrix} \begin{bmatrix} X(k,1) \\ X(k,2) \\ \cdots \\ X(k,i) \\ \cdots \\ X(k,n) \end{bmatrix} + \begin{bmatrix} W(k,1) \\ W(k,2) \\ \cdots \\ W(k,i) \\ \cdots \\ W(k,n) \end{bmatrix}, \quad (10)$$

can be obtained by

$$R_{A_1}(k) = \frac{Y_{RA_1}(k,1)X_P(k)V_A(k)}{Y_{RA_1}(k,2)X_R(k)} = \frac{(H_{BA}(k,1)V_B(k)(H_{AB}(k,1)X_R(k)+W_B(k,1)) + W_A(k,1))X_P(k)V_A(k)}{(H_{BA}(k,2)V_B(k)X_P(k)+W_A(k,2))X_R(k)}, \quad k = 1,2,\ldots,N \tag{17}$$

At high SNR cases, (17) can be approximately expressed as

$$R_{A_1}(k) \approx \frac{H_{BA}(k,1)V_B(k)H_{AB}(k,1)X_R(k)X_P(k)V_A(k)}{H_{BA}(k,2)V_B(k)X_P(k)X_R(k)} = \frac{H_{BA}(k,1)H_{AB}(k,1)V_A(k)}{H_{BA}(k,2)}, k = 1,2,\ldots,N \tag{18}$$

In the slow time-varying channel, the impulse response of adjacent OFDM symbols is approximately consistent. That is:

$$\begin{aligned} H_{AB}(k,1) &= H_{AB}(k,2) \\ H_{BA}(k,1) &= H_{BA}(k,2), k = 1,2,\ldots,N. \end{aligned} \tag{19}$$

Then, (18) can be written as

$$R_{A_1}(k) = \frac{H_{BA}(k,1)H_{AB}(k,1)V_A(k)}{H_{BA}(k,2)} = H_{AB}(k,1)V_A(k), k = 1,2,\ldots,N \tag{20}$$

According to (14), (19), and (20), the relationship is given as

$$R_{A_1}(k) \approx R_{B_1}(k), k = 1,2,\ldots,N. \tag{21}$$

At this time, stage 1 of detection is completed, and Alice and Bob obtain $\boldsymbol{R}_{A_1}$ and $\boldsymbol{R}_{B_1}$ respectively. Under high SNR and a slow time-varying channel, the consistency of the observed sequences analyzed by MSE is given as, (22), shown at the bottom of the next page.

(22) indicates that the observation sequences $\boldsymbol{R}_{A_1}$ and $\boldsymbol{R}_{B_1}$ containing the random source $\boldsymbol{H}_{AB}$ are consistent. Similarly, consistent observation sequences $\boldsymbol{R}_{A_2}$ and $\boldsymbol{R}_{B_2}$ containing random source $\boldsymbol{H}_{BA}$ can be obtained in stage 2.

To complete detection, two OFDM symbols are used as pilot sequences in this paper. While, the reliability of communication is affected by ISI caused by UWA multipath delay characteristics during actual communication.

The cyclic prefix is often inserted between OFDM symbols as the protection interval to eliminate the ISI [17], and the length of the CP T_G is set to be greater than the maximum delay spread T_L of the channel. At this time, the multipath interference of the previous OFDM symbol to the next OFDM symbol will be limited within the protection interval, which will no longer affect the demodulation of the next OFDM symbol and avoid ISI. The transmission pilot structures are shown in Fig. 4.

X_{TA_1}

CP	$X_B(1)$	CP	$V_A(1)X_P(1)$
CP	$X_B(2)$	CP	$V_A(2)X_P(2)$
...	...	...	...
CP	$X_B(k)$	CP	$V_A(k)X_P(k)$
...	...	...	...
CP	$X_B(N)$	CP	$V_A(N)X_P(N)$

X_{TB_1}

CP	$V_B(1)H_{AB}(1,1)X_R(1)$	CP	$V_B(1)X_P(1)$
CP	$V_B(2)H_{AB}(2,1)X_R(2)$	CP	$V_B(2)X_P(2)$
...	...	...	...
	$V_B(k)H_{AB}(k,1)X_R(k)$		$V_B(k)X_P(k)$
...	...	...	...
CP	$V_B(N)H_{AB}(N,1)X_R(N)$	CP	$V_B(N)X_P(N)$

FIGURE 4. The Pilot structures with CP of OFDM sequences.

In step 4, the slow time-varying channel is assumed. (The time-varying characteristic can be described as the channel coherence time.) When the length of a pilot signal T_S is less than the channel coherence time $T_{\texttt{coherent}}$, the channel can be considered as a slow time-varying channel. At this time, the impulse responses of adjacent OFDM symbol channels are approximately equality.

To sum up, legitimate users can use the same random source to generate observation sequences and complete channel detection through transmitting OFDM pilot sequences containing CP in a slow time-varying multipath channel, even if the channel reciprocity is damaged.

C. SAFETY ANALYSIS

In a typical physical-layer key generation scenario, a passive eavesdropper is assumed, who eavesdrops on the key generation process and knows the channel detection method and common pilot sequence $X_P(k)$. Eve does not send active detection signals but only conducts passive eavesdropping. The legitimate users cannot know any information about Eve. In this case, two situations are discussed. Eve is far away from both sides, and Eve is close to one side.

When Eve is far away from both sides of legitimate users and the channel environment is inconsistent with the channel between Alice and Bob, that is, (23), as shown at the bottom of the next page, where $H_{AE}(k,i)$, $H_{BE}(k,i)$ is the CFR of the channel from Alice to Eve and Bob to Eve on the i-th OFDM symbol of the k-th subcarrier respectively. The receive sequences of Eve on k subcarrier can be given as, (24) and (25), shown at the bottom of the next page, where $Y_{\text{RE-Alice}_1}(k,i)$ is the receive value obtained by Eve from Alice, $Y_{\text{RE-Bob}_1}(k,i)$ is receive value obtained by Eve from Bob, and $W_E(k,i)$ is the Gaussian noise on the i-th OFDM symbol of the k-th subcarrier.

Due to $H_{AB}(k,i) \neq H_{AE}(k,i)$, Eve cannot obtain the expected observation sequences using (24), even if $X_P(k)$ is known. Meanwhile, Eve cannot obtain randomly generated

$$\boldsymbol{X}_{TB_1} = \begin{cases} X_{TB_1}(k,1) = V_B(k)Y_{RB_1}(k,1) \\ = V_B(k)(H_{AB}(k,1)X_R(k)+W_B(k,1)), & i = 1 \\ X_{TB_1}(k,2) = V_B(k)X_P(k), i = 2, & k = 1,2,\ldots,N \end{cases} \tag{15}$$

pilot sequences $V_{\mathrm{A}}(k)$ and $X_{\mathrm{R}}(k)$, so the expected observation sequences cannot be obtained using (25). Similarly, in stage 2, Eve cannot obtain the expected observation sequence as well. Therefore, the proposed method in this paper can ensure the security when Eve is far away from both sides of legitimate users

When Eve approaches Alice, the channel impulse responses from Bob to Alice and from Bob to Eve are similar (i.e.,$H_{\mathrm{BE}}(k,i) \approx H_{\mathrm{BA}}(k,i)$). In stage 1, (25) can be expressed as, (26), shown at the bottom of the next page.

Without $X_{\mathrm{R}}(k)$ and $V_{\mathrm{A}}(k)$ generated randomly by Alice, Eve is still unable to obtain the expected observation sequences, which can ensure communication security.

When Eve approaches Bob, the channel impulse responses form Alice to Bob and from Alice to Eve are similar (i.e.,$H_{\mathrm{AE}}(k,i) \approx H_{\mathrm{AB}}(k,i)$). In stage 1, (24) can be expressed as, (27), shown at the bottom of the next page.

Utilizing $X_{\mathrm{P}}(k)$, Eve can obtain the expected observation sequences $H_{\mathrm{AB}}(k,i)\,V_{\mathrm{A}}(k)$ in stage 1. However, in stage 2, the receive sequences of Eve can be given as, (28) and (29), shown at the bottom of the next page.

Without $X_{\mathrm{R}}(k)$ and $V_{\mathrm{B}}(k)$ generated randomly by Bob, Eve is still unable to obtain the expected observation sequences, which can ensure communication security.

To sum up, when Eve is far away from both legitimate users or close to either user, Eve cannot obtain the expected observation value $H_{\mathrm{AB}}(k,i)V_{\mathrm{A}}(k)$ and $H_{\mathrm{BA}}(k,i)V_{\mathrm{B}}(k)$ at the two stages of key generation. Thus, the detection method proposed in this paper can ensure that the eavesdropper cannot obtain all the observation sequences and guarantee the safety of the detection process.

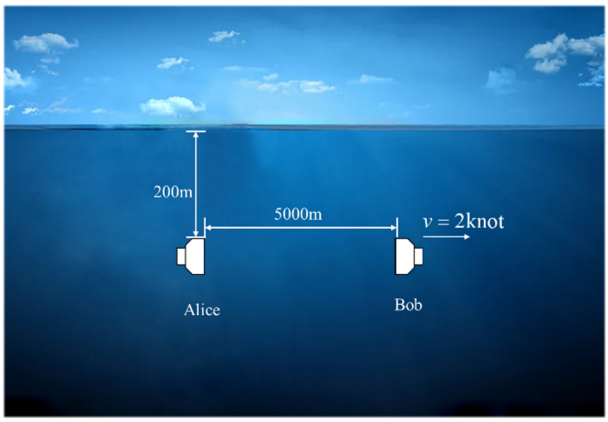


FIGURE 5. The simulation environment.

III. SIMULATION AND ANALYSIS

To verify the performance of our method, the MSE of the channel observation sequences and KDR are analyzed, and our method is compared with LPAWP at a high SNR. In addition, the effect of the channel detection method is mainly considered, so key negotiation and key enhancement are not discussed. Besides, when the KDR is verified, the single-bit quantization without protection interval is used to quantize the observation sequences.

A. SIMULATION TO CHANNEL

In Fig. 5, Alice and Bob are transceivers with a distance of 5 km and 200 m underwater. Alice remains stationary and Bob moves away from Alice at a speed of 2 knots.

$$\begin{aligned}\mathrm{MSE} &= E\{(\boldsymbol{R}_{\mathrm{A}_1} - \boldsymbol{R}_{B_1})^H \cdot (\boldsymbol{R}_{A_1} - \boldsymbol{R}_{B_1})\} \\ &= \frac{1}{N}\sum_{k=1}^{N}\begin{bmatrix}(H_{\mathrm{AB}}(k,1)V_{\mathrm{A}}(k) - H_{\mathrm{AB}}(k,2)V_{\mathrm{A}}(k))^H (H_{\mathrm{AB}}(k,1)V_{\mathrm{A}} \\ -H_{\mathrm{AB}}(k,2)V_{\mathrm{A}}(k))\end{bmatrix} \\ &= 0\end{aligned} \tag{22}$$

$$\begin{cases} H_{\mathrm{AB}}(k,i) \neq H_{\mathrm{AE}}(k,i) \\ H_{\mathrm{BA}}(k,i) \neq H_{\mathrm{BE}}(k,i), \end{cases} \quad k = 1,2,\cdots,N, i = 1,2,\cdots,M, \tag{23}$$

$$\boldsymbol{Y}_{\mathrm{RE\text{-}Alice_1}} = \begin{cases} Y_{\mathrm{RE\text{-}Alice_1}}(k,1) = H_{\mathrm{AE}}(k,1)X_{\mathrm{R}}(k) \\ +W_{\mathrm{E}}(k,1), i = 1 \\ Y_{\mathrm{RE\text{-}Alice_1}}(k,2) = H_{\mathrm{AE}}(k,2)V_{\mathrm{A}}(k)X_{\mathrm{P}}(k) \\ +W_{\mathrm{E}}(k,2), i = 2 \end{cases}, k = 1,2,\cdots,N, \tag{24}$$

$$\boldsymbol{Y}_{\mathrm{RE\text{-}Bob_1}} = \begin{cases} Y_{\mathrm{RE\text{-}Bob_1}}(k,1) = H_{\mathrm{BE}}(k,1)V_{\mathrm{B}}(k)H_{\mathrm{AE}}(k,1)X_{\mathrm{R}}(k) \\ +W_{\mathrm{E}}(k,1), i = 1 \\ Y_{\mathrm{RE\text{-}Bob_1}}(k,2) = H_{\mathrm{BE}}(k,2)V_{\mathrm{B}}(k)X_{\mathrm{R}}(k) \\ +W_{\mathrm{E}}(k,2), i = 2 \end{cases}, k = 1,2,\cdots,N, \tag{25}$$

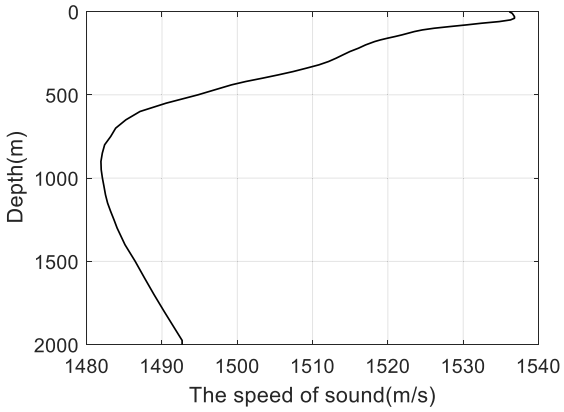


FIGURE 6. Sound velocity profile.

TABLE 1. Simulation parameters.

	Alice to Bob	Bob to Alice
emitter depth	200 m	
receiver depth	200 m	
distance	3000 m	3002 m
relative velocity	2 knots	

Bellhop, a typical UWA channel simulation software, is used to generate the channel impulse response from Alice to Bob and from Bob to Alice respectively [18]. The area of legitimate users is set to (115.5°E, 19.5°N), and the Argo database is employed to obtain the sound velocity profile and ocean depth [19]. The sound velocity profile is shown in Fig. 6.

Other simulation parameters are presented in Table 1. When the relative speed of users is 2 knots (about 1 m/s) and the carrier frequency of the pilot is 10 Hz, the channel coherence time is about:

$$T_{\text{coherent}} \approx \frac{1}{f_{\text{d}}} = \frac{1}{\Delta f_{\text{c}}} = \frac{\text{c}}{v f_{\text{c}}} \approx 0.15\ s, \tag{30}$$

where f_{d} is the maximum Doppler frequency offset; Δ is the Doppler factor; v is the relative velocity of users; c is the sound velocity and it is 1517 m/s according to Fig. 6.

The existing relative motion, not only Doppler interference but also different communication distances need to be considered when simulating the channel from Alice to Bob and the channel from Bob to Alice. In stage 1, the distance between the two users is 3000 m. It takes about 2 s to complete one-way channel detection from Alice sending the pilot sequences to Bob receiving the pilot sequences. Due to the back movement, when Bob sends the pilot sequences, the distance between the two users becomes 3002 m, and the channel parameters change.

Fig. 7 shows the channel amplitude-frequency responses of positive channel and negative channel, and the correlation function between positive channel and negative channel is shown in Fig. 8. Fig. 7 indicates that even if the communication distance changes slightly, the CFR may change greatly. Fig. 8 indicates that the correlation between the positive channel and negative channels is not high and the maximum correlation peak is less than 0.35, which causes the traditional physical-layer key generation method difficult to apply.

Fig. 9 shows the channel fading from the 40-th OFDM subcarrier to the 88-th OFDM subcarrier. It indicates that the UWA channel has obvious frequency selective fading.

$$\boldsymbol{Y}_{\text{RE-Bob}_1} = \begin{cases} Y_{\text{RE-Bob}_1}(k,1) = \\ H_{\text{BA}}(k,1)V_{\text{B}}(k)H_{\text{AE}}(k,1)X_{\text{R}}(k) \\ +W_{\text{E}}(k,1), i=1 \\ Y_{\text{RE-Bob}_1}(k,2) = H_{\text{BA}}(k,2)V_{\text{B}}(k)X_{\text{R}}(k) \\ +W_{\text{E}}(k,2), i=2 \end{cases} , k = 1, 2, \cdots, N. \tag{26}$$

$$\boldsymbol{Y}_{\text{RE-Alice}_1} = \begin{cases} Y_{\text{RE-Alice}_1}(k,1) = H_{\text{AB}}(k,1)X_{\text{R}}(k) \\ +W_{\text{E}}(k,1), i=1 \\ Y_{\text{RE-Alice}_1}(k,2) = H_{\text{AB}}(k,2)V_{\text{A}}(k)X_{\text{P}}(k) \\ +W_{\text{E}}(k,2), i=2 \end{cases} , k = 1, 2, \cdots, N. \tag{27}$$

$$\boldsymbol{Y}_{\text{RE-Bob}_2} = \begin{cases} Y_{\text{RE-Bob}_2}(k,1) = H_{\text{BE}}(k,1)X_{\text{R}}(k) \\ +W_{\text{E}}(k,1), i=1 \\ Y_{\text{RE-Bob}_2}(k,2) = H_{\text{BE}}(k,2)V_{B}(k)X_{\text{P}}(k) \\ +W_{\text{E}}(k,2), i=2 \end{cases} , k = 1, 2, \cdots, N, \tag{28}$$

$$\boldsymbol{Y}_{\text{RE-Alice}_2} = \begin{cases} Y_{\text{RE-Alice}_2} = H_{\text{AB}}(k,1)V_{\text{B}}(k)H_{\text{BE}}(k,1)X_{\text{R}}(k) \\ +W_{\text{E}}(k,1), i=1 \\ Y_{\text{RE-Alice}_2} = H_{\text{AB}}(k,2)V_{\text{B}}(k)X_{\text{R}}(k) \\ +W_{\text{E}}(k,2), i=2 \end{cases} , k = 1, 2, \cdots, N. \tag{29}$$

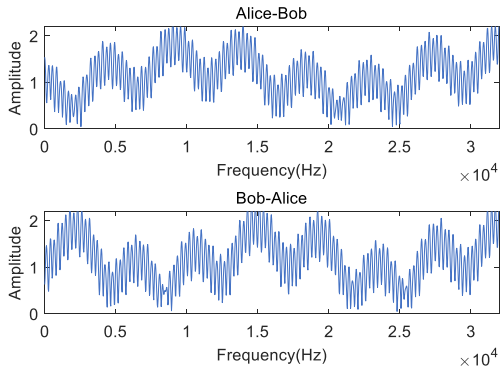


FIGURE 7. Channel amplitude-frequency response.

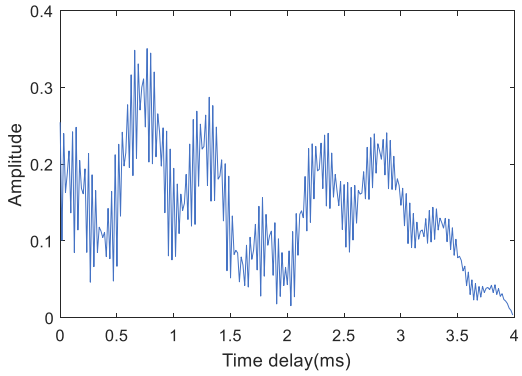


FIGURE 8. Bidirectional channel correlation coefficient.

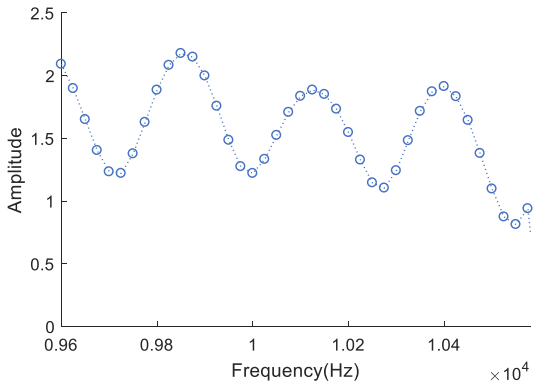


FIGURE 9. Partial channel amplitude-frequency response of Alice-Bob.

Meanwhile, the fading experienced by adjacent subcarriers is obviously different, which is difficult to meet the channel constraints of LPAWP. By contrast, the method proposed in this paper is not limited by this channel constraint, and it can obtain better performance in frequency selective fading channels in theory.

B. SIMULATION TO DETECTION METHOD

In this section, the MSE of channel observation sequences and the KDR are simulated respectively, and they are compared with those of LPAWP. For the method proposed in this paper, two-stage channel detection can generate 256-bit keys, and 5000 Monte Carlo experiments are conducted to generate 1280000-bit keys. For LPAWP, two-stage channel detection can generate 128-bit keys, and 10000 Monte Carlo experiments are conducted to generate 1280000-bit keys.

TABLE 2. Modulation parameters of OFDM.

Parameter	Quantity
sampling rate	64 kHz
carrier frequency	10 kHz
subcarrier spacing	25 Hz
number of OFDM subcarriers	128
length of CP	20 ms
length of detection signal	120 ms

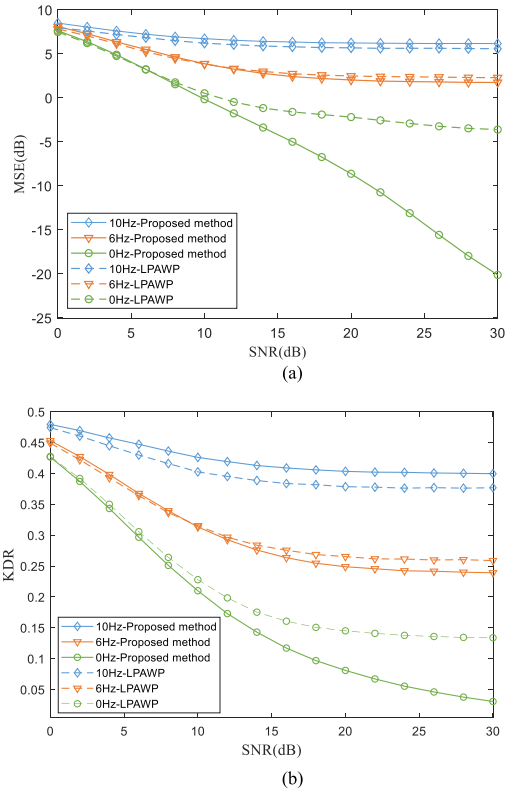


FIGURE 10. Doppler effect on detection methods.

In the preparation phase, random 01 sequences are generated and pilot sequences are generated through PSK mapping, and OFDM modulation using 01 sequences. The parameters of OFDM modulation are presented in Table 2.

1) DOPPLER EFFECT ON CHANNEL DETECTION

The relative motion of users' Doppler interference and the location change of both sides will further cause the change in the channel environment. Fig. 10 compares the MSE and the KDR of observation sequences when the maximum Doppler frequency offset of the received pilot sequences is 0 Hz, 6 Hz, and 10 Hz, respectively.

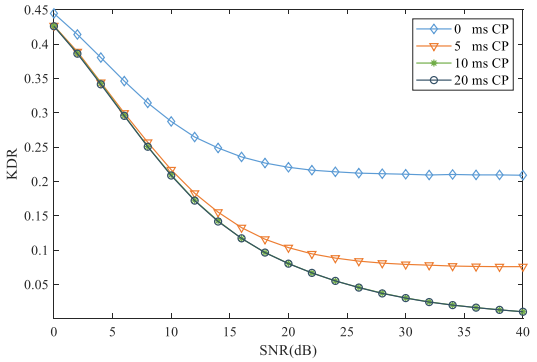


FIGURE 11. CP effect on KDR.

The experiments show that the Doppler frequency shift has a great impact on the method proposed in this paper, and the higher the frequency offset, the worse the correlation between the observation sequences generated by legitimate users, and the lower the KDR.

Because of longer pilot sequences, this paper requires a longer channel coherence time to complete channel detection. Therefore, our method has a weaker anti-Doppler frequency shift ability than LPAWP, and the performance is similar when the Doppler frequency shift is 6 Hz and 10 Hz. However, our method is obviously better than LPAWP, with Doppler compensation or small Doppler frequency shift, because it does not need to meet the constraint that adjacent subcarriers experience the same fading.

2) CP EFFECT ON CHANNEL DETECTION

For OFDM communication system, the length of CP has a great impact on system performance. When the CP length is less than the maximum delay, the ISI will appear which will seriously affect the performance. In this paper, the maximum delay of forward channel and reverse channel is about 6 ms, and the length of an OFDM symbol (without CP) is 40 ms. We discuss the KDR when the CP length is 0 ms, 5 ms, 10 ms, and 20 ms, respectively.

Fig. 11 indicates that even at high SNR, the KDR in the case of 0 ms CP is still higher than 0.2, which is affected seriously by ISI. In the case of 5 ms CP, the CP length is still less than the maximum delay (6 ms), and ISI will be generated, which will affect the KDR. When CP length is 10ms or 20ms, the CP length is greater than the maximum delay, which can resist ISI between OFDM symbols, so their performances are similar.

Experiments show that a long CP is needed to remove ISI. However, the redundant CP does not improve performance significantly, which even causes a waste of spectrum resources. Therefore, the appropriate CP length should be selected to balance the performance and spectrum resources in practical application.

IV. CONCLUSION

This work studied the problem of physical-layer key generation for the UWA environment, with a focus on the impaired reciprocity and frequency selective fading, at the low speed robust underwater acoustic communication scenario. Especially, for the time-division half-duplex system, due to the relative motion, the channel environment between both sides changes greatly in a short time. This reduces of the correlation between the forward channel and the reverse channel, and directly affects the consistency of the channel detection results on both sides. In this paper, a key detection method based on OFDM pilot structure is proposed for an UWA time-varying multipath channel. It solves the problem of impaired reciprocity and obtains a low KDR. In a channel with high SNR and frequency selective fading, the simulation results simulation results show that the KDR is lower than 0.05.

REFERENCES

[1] K. Huang, L. Jin, Y. Chen, Y. Lou, Y. Zhou, K. Ma, X. Xu, Z. Zhong, and S. Zhang, "Development of wireless physical layer key generation technology and new challenges," *J. Electron. Inf. Technol.*, vol. 42, no. 10, pp. 2330–2341, 2020, doi: 10.11999/JEIT200002.

[2] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015, doi: 10.1109/MCOM.2015.7120014.

[3] L. Jin, X. Hu, Y. Lou, Z. Zhong, X. Sun, H. Wang, and J. Wu, "Introduction to wireless endogenous security and safety: Problems, attributes, structures and functions," *China Commun.*, vol. 18, no. 9, pp. 88–99, Sep. 2021, doi: 10.36227/techrxiv.14125346.v1.

[4] J. Zhang, R. Woods, A. Marshall, and T. Q. Duong, "Verification of key generation from individual OFDM subcarrier's channel response," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[5] R. Guillaume, F. Winzer, A. Czylwik, C. T. Zenger, and C. Paar, "Bringing PHY-based key generation into the field: An evaluation for practical scenarios," in *Proc. IEEE 82nd Veh. Technol. Conf. (VTC-Fall)*, Boston, MA, USA, Sep. 2015, pp. 1–5.

[6] R. Cavallari, F. Martelli, R. Rosini, C. Buratti, and R. Verdone, "A survey on wireless body area networks: Technologies and design challenges," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 3, pp. 1635–1657, Aug. 2014.

[7] L. Jin, X. Wang, Y. Lou, and X. Xu, "Achieving one-time pad via endogenous secret keys in wireless communication," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Aug. 2020, pp. 1092–1097.

[8] Y. Luo, L. Pu, Z. Peng, and Z. Shi, "RSS-based secret key generation in underwater acoustic networks: Advantages, challenges, and performance improvements," *IEEE Commun. Mag.*, vol. 54, no. 2, pp. 32–38, Feb. 2016, doi: 10.1109/MCOM.2016.7402258.

[9] A. Petroni, S. Pergoloni, H. L. Ko, T. H. Im, Y. H. Cho, R. Cusani, G. Scarano, and M. Biagi, "Channel reciprocity analysis for bi-directional shallow water acoustic communications," in *Proc. OCEANS*, Anchorage, AK, USA, Sep. 2017, pp. 1–5.

[10] K. Pelekanakis, C. M. G. Gussen, R. Petroccia, and J. Alves, "Robust channel parameters for crypto key generation in underwater acoustic systems," in *Proc. OCEANS MTS/IEEE SEATTLE*, Seattle, WA, USA, Oct. 2019, pp. 1–7, doi: 10.23919/OCEANS40490.2019.8962548.

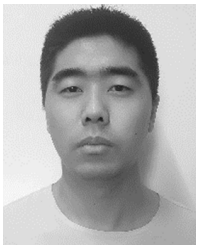
[11] K. Pelekanakis, S. A. Yildirim, G. Sklivanitis, R. Petroccia, J. Alves, and D. Pados, "Physical layer security against an informed eavesdropper in underwater acoustic channels: Feature extraction and quantization," in *Proc. 5th Underwater Commun. Netw. Conf. (UComms)*, Lerici, Italy, Aug. 2021, pp. 1–5, doi: 10.1109/UComms50339.2021.9598102.

[12] G. Sklivanitis, K. Pelekanakis, S. A. Yildirim, R. Petroccia, J. Alves, and D. A. Pados, "Physical layer security against an informed eavesdropper in underwater acoustic channels: Reconciliation and privacy amplification," in *Proc. 5th Underwater Commun. Netw. Conf. (UComms)*, Lerici, Italy, Aug. 2021, pp. 1–5, doi: 10.1109/UComms50339.2021.9598159.

[13] J. K. LIU, Y. Z. Dong, and G. Q. Zhang, "Key generation technology based on underwater acoustic channel estimation in covert communication," *J. Appl. Acoust.*, vol. 38, no. 4, pp. 681–687, 2019, doi: 10.11684/j.issn.1000-310X.2019.04.027.

[14] J. M. Liu, Z. W. Shen, Q. Q. Han, and J. W. Liu, "Underwater acoustic communication physical layer key generation scheme," *J. Commun.*, vol. 40, no. 2, pp. 111–117, 2019, doi: 10.11959/j.issn.1000-436x.2019027.

[15] S. Sarowa, H. Singh, S. Agrawal, and B. S. Sohi, "A novel energy-efficient ICI cancellation technique for bandwidth improvements through cyclic prefix reuse in an OFDM system," *Frontiers Inf. Technol. Electron. Eng.*, vol. 18, no. 11, pp. 1892–1899, Nov. 2017.
[16] Y. S. Cho, J. Kim, W. Y. Yang, and C. G. Kang, *MIMO-OFDM Wireless Communications With MATLAB*. Hoboken, NJ, USA: Wiley, 2010, pp. 101–162.
[17] Z. Wang-Xing, W. Qun, and C. Zhang-Xin, "Novel restructuring method for CP-based LS channel estimation in OFDM system," *J. Commun.*, vol. 34, no. 3, pp. 175–182, 2013, doi: 10.3969/j.issn.1000-436x.2013.03.023.
[18] M. B. Porter and H. P. Bucker, "Gaussian beam tracing for computing ocean acoustic fields," *J. Acoust. Soc. Amer.*, vol. 82, no. 4, pp. 1349–1359, Oct. 1987, doi: 10.1121/1.395269.
[19] Argo. (Nov. 10, 2021). *Argo Float Data and Metadata from Global Data Assembly Centre*. [Online]. Available: http://doi.org/10.17882/42182.



XINYU LI was born in 1997. He received the B.S. degree from Information Engineering University, in 2020, where he is currently pursuing the master's degree. His research interest includes underwater acoustic communication secure.

GANG XIN received the M.S. degree from the National Digital Switching System Engineering and Technological Research Center (NDSC), in 2004. His research interests include channel coding and information theory.

BIN WANG received the Ph.D. degree from Information Engineering University, in 2007. She is currently an Associate Professor with the School. Her research interests include underwater acoustic communication signal processing and blind channel equalization.

YAN HUANG received the M.S. degree from Information Engineering University, in 2007. He is currently a Professor with the School. His research interest includes communication signal analysis and processing.