Digital Signal Processing 81 (2018) 129–137

Contents lists available at ScienceDirect

Digital Signal Processing

www.elsevier.com/locate/dsp

Energy-efficient and secure transmission scheme based on chaotic compressive sensing in underwater wireless sensor networks

Xinbin Li [a,*], Chao Wang [a], Zijun Yang [b], Lei Yan [a], Song Han [a]

[a] Institute of Electrical Engineering, Yanshan University, Qinhuangdao 066004, China
[b] Harbin power vocational technology college, Harbin 150030, China

ARTICLE INFO

Article history:
Available online 30 July 2018

Keywords:
Compressive sensing
Data encryption
Underwater wireless sensor networks
Random access

ABSTRACT

An energy-efficient and secure encryption data transmission scheme based on chaotic compressive sensing (CCS) is proposed to prolong the lifetime of underwater wireless sensor networks and guarantee the security of data. First, the scheme adopts compressive sensing (CS) by exploiting the sparsity of sensor data in the time domain. A sufficiently long interval is selected as transmission period in this step. The scheme reduces the number of transmissions in a period by sampling the data in each frame and transmitting the data at the end of a period, thereby reducing energy consumption of each sensor. Second, a CCS-based encryption algorithm is proposed to encrypt data at the end of a period to improve the security of transmission. We also provide the shortest repeat transmission strategy based on random access (RA) to deal with complex underwater transmission environments. Finally, real data examples are provided and performance analysis is conducted to illustrate the validity of the proposed scheme.

1. Introduction

Research on underwater wireless sensor networks (UWSNs) attracted considerable attention given the increasing emphasis on oceans. These networks can be applied in oceanographic data collection, field monitoring disaster prevention, and object tracking [1] [2] [3]. For example, a number of static sensors and/or vehicles over the target region can be deployed to record the temperature, salinity, or acoustic signal of objects, and monitoring can be achieved by transmitting private and critical signal to the fusion center (FC) through the acoustic channel [4] [5]. Moreover, given that the battery of the sensor device is difficult to recharge in underwater networks [6], a high-security and energy-efficient transmission scheme is key to guaranteeing the security of data transmission and improving the lifetime of UWSNs.

Most natural phenomenon can be sparsely represented on an appropriate basis [7] [8]; thus, compressive sensing (CS) allows a small number of samples to recover all required information [9] [10]. In [11] and [12], the authors demonstrated that CS can effectively compress and recover sensing data with a measurement matrix. Therefore, CS theory can be used in UWSNs to reduce the sampled data, thereby resulting in reduced energy consumption. The CS-based scheme applied in wireless sensor networks (WSNs) was widely investigated to reduce energy consumption [13] [14]. In [13], an energy-balancing scheduling algorithm based on CS was derived for WSNs. The algorithm minimizes the number of sensor nodes to reduce energy consumption. In [14], the author aimed to solve the problem of data collection in WSNs by exploiting joint routing and compressed aggregation to minimize the energy consumption of the network. In [15], a new method was proposed that integrates QR decomposition and CS; this method exploited less measurement data to reconstruct the network under the assistance of input noise. In [16] and [17], the authors proposed semi-tensor product CS to save resources in WSNs. The approach reduced the size of the measurement matrix to save storage space by breaking through the dimension match restriction of matrix multiplication and decreased the calculation amount to save calculation resources. CS has long been used to reduce energy consumption in sampling of WSNs, but it has not yet been applied in UWSNs because of the complexity of the underwater environment in limited bandwidth, time-varying multipath propagation, and high latency [18]. In [19], the author proposed a random access compressive sensing (RACS) frame-based transmission scheme for static UWSNs. The scheme exploited the sparsity of natural phenomenon in a frame. CS was used to reduce the number of sampling sensors. However, the scheme presented in [19] did not consider the time correlation of the data collected by each sensor

* Corresponding author.
E-mail addresses: lixb@ysu.edu.cn (X. Li), whc_wdc@sina.cn (C. Wang), 395110181@qq.com (Z. Yang), lyan@stumail.ysu.edu.cn (L. Yan), hansongysu@sina.cn (S. Han).

https://doi.org/10.1016/j.dsp.2018.07.006
1051-2004/© 2018 Elsevier Inc. All rights reserved.

in multiple frames to process data. Furthermore, the data transmitted from sampling sensors were in the spatial domain. Thus, the security of data transmission cannot be guaranteed if data eavesdropping exists.

To ensure security in data transmission, many algorithms were introduced to encrypt data using wave transmission [20], reversible cellular automata [21], chaotic system [22] and CS [23]. In [24], the author proposed a lightweight encryption framework by augmenting CS with wireless physical layer security. The approach eliminated the need for a separate encryption algorithm. The RSSI values of the received packets are used to generate the measurement matrix to encrypt data. An excellent encryption algorithm should have high sensitivity to the secret key in the encryption and decryption processes. In [25], the author proposed a chaotic compressive sensing (CCS)-based body-to-body network to ensure secure and energy-efficient data transmission. The networks exploit the sensitivity of chaotic systems to parameters, which have good security. However, in [24] and [25], the authors used the same measurement matrix to encrypt data; the approach resulted in a problem, wherein all encrypted data are deciphered by the measurement matrix and will be stolen if a measurement matrix is obtained by the eavesdropper.

In this study, a CCS-based data transmission scheme for UWSNs is proposed to solve the problem of secure data transmission and energy consumption. First, we exploit CS to reduce the number of sampling sensors in each frame. In contrast to the transmission of each frame in [19], each sensor is arranged to collect data in a period and encrypt and transmit the data at the end of a period. Period-based collection reduces the number of transmissions in a period, thereby reducing the energy consumption of each sensor. Second, we use CS to encrypt the data of each sensor and improve the security of data transmission by considering the sparsity of the data collected in a period. CCS can be used to ensure the relevance of the measurement matrix of each sensor to the ID of the sensors. Thus, the eavesdropper cannot steal the encrypted data from all sensors. Finally, we propose a repeat transmission strategy based on random access (RA) to achieve the shortest receiving time. The minimum number of transmissions can be obtained by ignoring the repeat packets transmitted from the same sensor during transmission. The strategy eliminates the need for a precise and synchronous transmission, which improves applicability to practical situations. In this study, we optimize the process of data collection, data encryption, and data transmission in UWSNs. This approach improves the security of data transmission and prolongs the lifetime of networks. The performance analysis and real data examples prove the excellent performance of the proposed scheme.

The main contributions of this study are summarized as follows.

(1) A periodic data collection strategy is proposed, which allows sensors to collect data with certain probability in each frame and store the data until the end of a period. The strategy avoids transmitting data in each frame, which can effectively reduce energy consumption.

(2) An ID-based CCS data encryption algorithm is proposed. A different measurement matrix is used to encrypt the data of each sensor by ensuring that the measurement matrix is correlated with the ID of each sensor. This process avoids the risk that the encrypted data of all sensors will be stolen by deciphering one of the measurement matrices. The CCS can be used to save storage space and improve the security of data transmission.

(3) A RA-based repeat transmission strategy is proposed to achieve the shortest data reception duration. By considering the collision characteristic of RA, we exploit repeat transmissions to increase the number of successfully received packets, which can be used to achieve the shortest data-receiving time. The strategy can resist the effect of variable propagation delay and clock drift on UWSNs effectively.

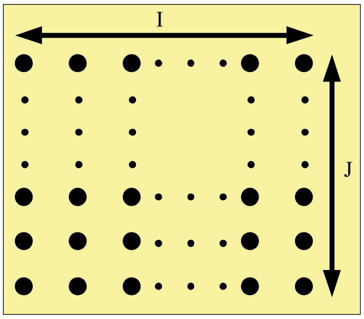

Fig. 1. The plane distribution map of sensors in target field.

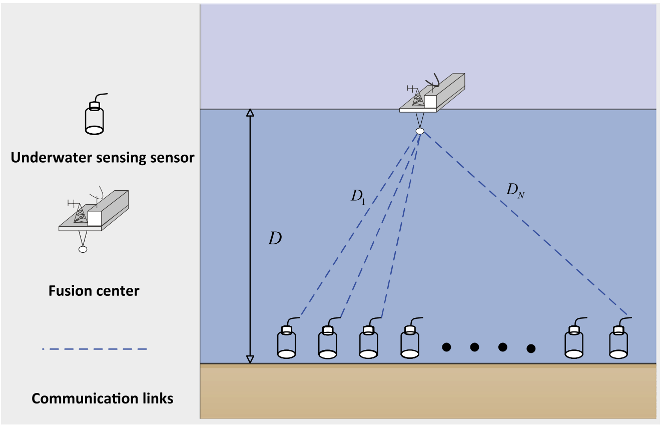

Fig. 2. The position of fusion center and sensors.

The remainder of the study is organized as follows. We introduce the network model in Section 2. We present the proposed scheme in Section 3. We provide a performance analysis of our scheme in terms of security, bandwidth, and energy consumption in Section 4. Finally, the conclusions drawn from the performance of this scheme are provided in Section 5.

2. System model

As shown in Fig. 1, a static wireless sensor network consisting of $N = IJ$ sensors is deployed at the bottom of a target field for long-term monitoring of environmental phenomenon [19]. I and J denote the number of sensors in $x-$ and $y-$ direction, respectively. Each sensor transmits its sampled data to a central node referred to as FC. The function of the FC is to receive and process data to recover the map of the field of interest.

In frame n, the sensor located at position (x_i, y_i) acquires data $u_i = u(x_i, y_i, n)$, where x_i and y_i denote the sensor's position in the two-dimensional field $i \in \{1, \dots, N\}$. Assuming that the network has bandwidth B, which is equal to the bit rate of each sensor transmitting, for given data length l, we express the duration of a packet as $T_p = l/B$. As shown in Fig. 2, D_i denotes the distance between sensor i and FC. The packet propagation delay of sensor i is expressed as $\tau_i = D_i/c$, where c is the nominal underwater velocity of sound. We consider the correlation properties of the physical process $u(x, y, n)$ to determine reasonable frame duration t. Assuming that the coherence time T_{coh} denotes the maximum duration of a slowly varying process, we consider the data collected at each sensor unchanged within T_{coh}. Therefore, sensors have to collect data at least once per T_{coh}, i.e., $t \leqslant T_{coh}$. We denote frame n as the data collected at any time $t \in [(n-1)T_{coh}, nT_{coh}]$.

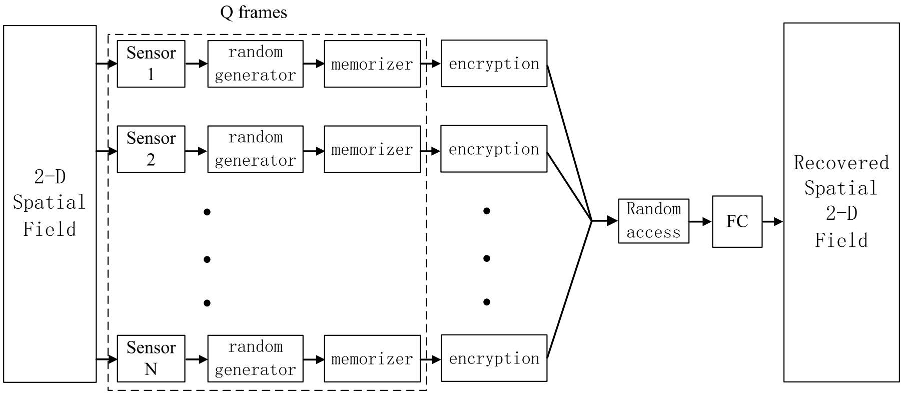

Fig. 3. The process of CCS-RA.

The sensing field can be described by a spatial matrix of sensor data as follows:

$$U=\begin{bmatrix} u_{11}(n) & u_{12}(n) & \cdots & u_{1I}(n) \\ \vdots & & & \vdots \\ u_{J1}(n) & u_{J2}(n) & \cdots & u_{JI}(n) \end{bmatrix} = \begin{bmatrix} u_1(n) & u_2(n) & \cdots & u_N(n) \end{bmatrix}^T, \quad (1)$$

where $U(n)$ is a $N \times 1$ matrix. $U(n)=\{u_1(n), u_2(n), \cdots, u_N(n)\}^T$ is defined as the data of sensors collected in frame n.

In this study, the sample in each frame is based on the fact that the signal of natural phenomenon can be modeled as a sparse component in certain domain [7]. Therefore, $U(n)$ can be represented by a few nonzero coefficients in $V(n)$, where $V(n)$ is defined as the spatial discrete Fourier transform of $U(n)$. Based on the theory of CS, if a signal has a sparse representation in certain domain, then the signal can be reconstructed with high probability from a small subset of random measurements. To reduce the energy consumption of sensors, the sparsity of natural phenomenon in a frame is exploited with only a subset of active sensors required to collect measurements during one frame. We assume that all sensors can collect data in each frame with time synchronization and are equipped with independent and identically distributed Bernoulli random generators. At the beginning of each frame, each sensor determines whether it will participate in the sensing process with a probability p. Thus a random subset of sensors is selected in the frame, and the number of active sensors M follows the Bernoulli distribution $M \sim B(N, p)$. By considering the sparsity S of natural phenomenon, we can reduce the number of required measurements in a frame from N to M.

Furthermore, given that signals in many natural phenomenons vary slowly with time, the smooth variations in each frame ensure that the signals in the time domain correlate, such that the signals collected by a sensor can be a sparse representation [8]. Assuming that the longest duration that the correlation exists is Q frames, we define Q frames as the collection period. Moreover, the sensing field in a period can be described by a space-time matrix of sensor data expressed as follows:

$$U=\begin{bmatrix} U(1) & U(2) & \cdots & U(Q) \end{bmatrix} = \begin{bmatrix} u_1(1) & u_1(2) & \cdots & u_1(Q) \\ \vdots & & & \vdots \\ u_N(1) & u_N(2) & \cdots & u_N(Q) \end{bmatrix}, \quad (2)$$

where U is a $N \times Q$ matrix. $U_i=\{u_i(1), u_i(2), \cdots, u_i(Q)\}$ is defined as the data of sensor i collected in a period.

3. CCS-based energy-efficient and secure encryption scheme for RA in wireless communication

By employing CCS to encrypt data and RA to transmit data, we propose a novel scheme referred to as chaotic compressive sensing random access (CCS-RA) to reconstruct the spatial map of natural phenomenon in the target field. The scheme can efficiently reduce energy consumption and improve the data security during transmission. The scheme eliminates the need for downlink through RA, which improves applicability to practical situations. The process of CCS-RA is as follows.

Step 1. At the beginning of each frame, sensor i determines whether or not it senses the field through an independent and identically distributed Bernoulli random generator.

Step 2. If sensor i senses the field, then it samples the measurement of interest and stores the data in a memorizer.

Step 3. At the end of a period, each sensor encrypts all of the data collected in the period, including the sensor's ID, into L bit packets using the CCS. The subsequent period starts immediately.

Step 4. All sensors transmit their packets to the FC after encryption. The transmission process of sensor i exhibits a uniformly distributed delay.

Step 5. The FC receives those packets through the RA channel. If the packets collide at the FC, then the colliding packets are discarded directly.

Step 6. After the packets are received, the FC uses the successfully received packets to reconstruct the spatial map using CS. Once the reconstruction is completed, the period is discarded and the FC waits for new packets in the subsequent period.

Fig. 3 shows the process of the scheme. The strategy of CCS-based data encryption is illustrated in Section 3.1. The transmission process based on RA and the corresponding reception strategy are presented in Section 3.2. The phenomenon reconstruction of the target field is shown in Section 3.3.

3.1. CCS-based data encryption algorithm

We propose to collect data periodically rather than transmitting in each frame by exploiting the sparsity of signals in time. Periodic collection reduces the number of data transmissions in a period, which can reduce the energy consumption of each sensor effectively.

Sparsity ensures that CS can be used to encrypt signals to improve the security of data transmission and prevent the eavesdropping of private data during transmission. However, given that an excellent encryption algorithm should be sensitive to the secret key in the encryption and decryption processes, the CCS is more secure than the traditional CS by exploiting the sensitivity of chaos. Notably, the CCS can reduce the storage space because

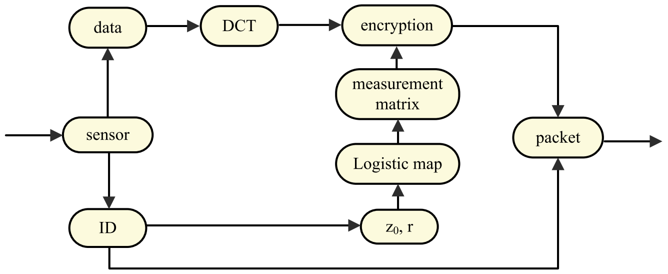

Fig. 4. The process of encryption.

it only requires the sender and receiver to preserve the matrix generation parameters as key. We also propose an ID-based CCS data encryption algorithm to prevent the eavesdropper from cracking the secret key to steal data from all sensors. Fig. 4 illustrates the process of our proposed encryption algorithm. The ID-based encryption can effectively prevent the eavesdropper from cracking the secret key of any sensor to steal all data.

The detailed steps of the proposed data encryption algorithm are as follows.

Step 1: Identify each sensor with a fixed number from 1 to N and transform the ID of each sensor into a 10 bit binary value as follows:

$$f(i) = p_{(10)}p_{(9)}p_{(8)}p_{(7)}p_{(6)}p_{(5)}p_{(4)}p_{(3)}p_{(2)}p_{(1)}, \tag{3}$$

where $f(i)$ is the ID of each sensor.

Step 2: We assume that the length of the data is Q. Given the sparsity of the data collected by a sensor in a period, U_i can be considered a sparse representation expressed as follows:

$$V_i = \Psi U_i, \tag{4}$$

where V_i is the nonzero coefficient vector of U_i in the frequency domain and Ψ is the discrete Fourier transform matrix.

Step 3: According to the ID information f_i of each sensor, we calculate the corresponding initiation value $z_0(i)$ and the chaotic parameter $r(i)$ of chaotic system, as follows:

$$z_0(i) = \frac{(f(i) \bigoplus (1111111111)_2)_{ROL=3}}{1024}, \tag{5}$$

$$r(i) = 3.57 + \frac{(f(i) \bigoplus (1010101010)_2)}{1024} \times 0.43, \tag{6}$$

where $z_0(i) \in (0,1)$ and $r(i) \in [3.57, 4]$, $i \in \{1, \cdots, N\}$; $\bigoplus$ represents the XOR operation, $(\cdot)_2$ represents the binary numbers and ROL = 3 represents the step size of the cyclic left shift.

Step 4: The chaotic sequence $x_h \in X$ generated from the output sequence produced by the logistic map can be obtained through the chaotic logistic map $z_{h+1} = rz_h(1 - z_h)$ with chaotic parameters z_0 and r. Secret key $\Phi \in \mathbb{R}^{M \times N}$ can be created column by column with X [26]. We can then obtain the measurement value vector Y_i by applying Φ to encrypt V_i.

$$x_h = 1 - 2z_{n+hd}, \tag{7}$$

$$\Phi = \sqrt{\frac{2}{M}} \begin{bmatrix} x_0 & \cdots & x_{M(N-1)} \\ x_1 & \cdots & u_{M(N-1)+1} \\ \vdots & & \vdots \\ x_{M-1} & \cdots & x_{MN-1} \end{bmatrix}, \tag{8}$$

$$Y_i = \Phi V_i, \tag{9}$$

where h is the length of X with $h = M \times N$, d is the sampling distance, and Y_i is the encrypted data of sensor i in a period.

Finally, each sensor inputs Y_i, including the sensor's ID, into a packet and transmits the packet to the FC.

3.2. RA-based transmission and reception

Given the harsh underwater environment, achieving precise transmission synchronization with a common timing reference is challenging because of variable delay. Therefore, we use the RA channel to transmit packets.

Each sensor in RA can transmit asynchronously. Each sensor is equipped with independent and identically distributed uniform random generator. Therefore, time t_i' follows a uniform distribution within $[0, T_r - T_p]$ when sensor i transmits its packet. Assuming that the propagation delay τ_i and the packet arrival time $t_i = t_i' + \tau_i$, $i \in \{1, \cdots, N\}$, we observe that t_i resembles a uniform distribution. Given the different arrival times of packets from different sensors, the possibility that packets collide at the FC is high. In this study, the approach used to handle the colliding packets is to let the FC discard them directly. The FC needs to receive a sufficient number of collision-free packets to process to ensure successful recovery. We denote the number of successfully received packets by the FC during T_r as K. Once collision is detected, the FC discards the colliding packets directly and recovers the data using the packets received successfully.

In our scheme, FC begins to collect packets at T_x and the packets that arrive after $T_x + T_r - T_p$ will not be received completed, i.e., they are not counted as received packets. Considering that a packet may collide with other received packets, we have to consider these packets when calculating collision. The event when a packet transmitted from sensor i arrives at the FC completely within duration T_r occurs with the following probability:

$$\text{prob}(T_x \leqslant t_i \leqslant T_x + T_t - T_p) = \frac{T_r - T_p}{T_r}, \tag{10}$$

where t_i denotes the arrival time of the packet transmitted from sensor i. Collision will occur if another packet transmitted from sensor j arrives at the FC in $[t_i - T_p, t_i + T_p]$. Probability is derived as follows:

$$\text{prob}(t_n - T_p \leqslant t_j \leqslant t_n + T_p) = \frac{2T_p}{T_r}. \tag{11}$$

Therefore, the probability of no collision for packet i is expressed as follows:

$$\text{prob}(\textit{collision-free}) = (1 - \frac{2T_p}{T_r})^{N-1}. \tag{12}$$

Consequently, the probability that a packet is successfully received at the FC within $[T_x, T_x + T_r]$ is derived as follows:

$$q = \frac{T_r - T_p}{T_r}(1 - \frac{2T_p}{T_r})^{N-1}. \tag{13}$$

The density function of the number of successfully received packets K can be expressed as follows:

$$P_K = prob(K = k) = B(N, q) = \binom{N}{k} q^k (1-q)^{N-k}. \tag{14}$$

Furthermore, we define the complementary cumulative distribution function of K as follows:

$$F_K = prob(K \geqslant N_s) = \sum_{k-N_s}^{\infty} P_K = 1 - \sum_{k=0}^{N_s - 1} P_K, \tag{15}$$

where N_s is the minimum number of useful packets needed to ensure successful reconstruction.

Given that the number of successfully received packets K at the FC during reception duration T_r varies because of collisions, the number of useful packets K cannot be guaranteed to be larger

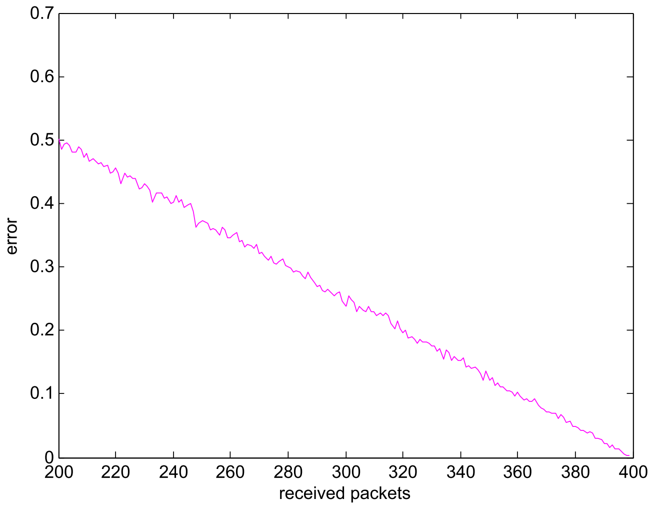

Fig. 5. The recovery error with the number of useful packets.

than N_s. Therefore, we define the minimum probability of sufficiently sensing P_s as the probability that the FC collects N_s or more correct packets. The system needs to meet the requirement that the FC collects at least N_s correct packets during T_r with probability P_s or higher, which is derived as follows:

$$prob(K \geqslant N_s) \geqslant P_s. \tag{16}$$

In this section, we propose the repeat transmission strategy to ensure the shortest data reception duration. First, we assume that all sensors will transmit their packets to the FC for reconstruction. We conclude that the required minimum number of useful packets in one transmission for a given parameter satisfies the minimum accuracy of successful recovery. Second, we let all sensors transmit their packets repeatedly to achieve high accuracy. Repeat transmission avoids the possible massive loss of data in a single transmission, which can improve the accuracy of recovery effectively. By discarding the same packet in the FC, we obtain the minimum number of transmissions for the accuracy requirement. The shortest data reception duration is determined.

We reconstruct the spatial changes with the minimum successful recovery accuracy that each sensor transmits once. Duration T_{once} can be derived by solving the following equation:

$$F_K = P_s. \tag{17}$$

We use an example to illustrate the repeat transmission strategy. For instance, when a network consists of 400 nodes, the period consists of 400 frames, packet duration is $T_p = 0.2$ s, and the coherence time of the process is $T_{coh} = 20$ s. We let the sparsity of the phenomenon be $S = 7$ for all periods to simplify the change. The collision in the RA is considered in the calculation of the minimum number of successfully received packets required for a given recovery accuracy. The relationship between recovery accuracy A and minimum number of successfully received packets K is illustrated in Fig. 5. We define $P_s = 0.9$ as the probability of sufficient sensing and $A_s = 80\%$ as the minimum requirement for successful recovery. The minimum number of useful packets corresponding to A_s is illustrated in Fig. 5, i.e., $K = 325$. The shortest reception duration T_s required for sufficient sensing can be obtained according to Eqs. (13), (14) and (15). For a given $P_s = 0.9$, FC needs to receive packets for at least $T_s \approx 880$ s to recover the field with $A = 80\%$.

The single transmission guarantees the minimum recovery accuracy in the FC. Each sensor can transmit packets many times to satisfy the high accuracy requirement. For a given T_{once}, we obtain the shortest data reception duration T_s that corresponding to required accuracy A_a, i.e., $T_s = n_s T_{once}$, where n_s is the minimum transmission number of each sensor. With the limitation of the period duration T_r, $n_s \leqslant \lfloor T/T_{once} \rfloor$.

We focus on each individual sensor to solve the minimum number of transmissions n_s. The number of same packets transmitted from a sensor is N_1 and the FC discards all repetitive packets directly. The effective number of packets transmitted by each sensor during T_s is calculated as follows:

$$N_1' = \begin{cases} 0, & N_1 = 0 \\ 1, & N_1 \geqslant 0. \end{cases} \tag{18}$$

The number of successfully received packets N' in T_{once} can be determined when T_{once} and P_s are given. We obtain the corresponding useful packets N_a for the required accuracy A_a. T_s can be expressed as follows:

$$T_s = \frac{1}{N'} \sum_{i=1}^{N_a - 1} \frac{N - i(\bmod N')}{N_a - i} T_{once}. \tag{19}$$

To illustrate the strategy, we assume that the required accuracy $A_a = 95\%$, such that we can obtain the minimum useful packets $K = 380$. For $T_{once} = 880$ s, the minimum number of transmissions required for sufficient sensing can be determined using Eq. (19), i.e., $n_s = 3$, which indicates the receive duration $T_s = 3T_{once} = 2,640$ s.

3.3. The recovery of phenomenon in target field of a period

When the packet reception process is completed, the FC begins to recover the change of phenomenon in a certain period. To this end, the FC decrypts each packet into the corresponding data that the sensor sampled first. Then, the FC reconstructs the change of phenomenon in the field in a certain period by merging all data according to the position of each sensor.

By exploiting the ID of the sensors included in the packet, the FC produces the parameters of the chaotic system and obtains the corresponding measurement matrix. Then, the FC uses the measurement matrix to decrypt the corresponding message Y_i. The decryption process at the FC can be performed by solving the following l_1-norm minimization optimization problem:

$$\min_{V_i} \|\tilde{V}_i\|_1 \quad s.t. \quad \|Y_i - \Phi\tilde{V}_i\|_2 \leqslant \varepsilon, \tag{20}$$

where ε is the bound of the noise in data. According to the theory of CS, the solution of the convex optimization problem is unique and equal to the original data if the number of observations is greater than $Q_s = CS\log Q$, where C is a small constant that is independent of Q and S. For $C = 2$, the least number of observations to recover the data collected from each sensor is $Q_s = 27$ given the expectation of sparsity in the frequency domain.

We can recover the corresponding message from $\tilde{V}_i$ to Y_i using the SL0 algorithm [27]. After all useful packets are recovered, FC merges all $\tilde{V}_i$ into $\tilde{V}$ according to the position of sensor i, where $i \in \{1, \cdots, N\}$. Finally, the change of phenomenon of target field in the period is obtained.

4. Real data example and performance analysis

In this section, we illustrate the process how our scheme reconstructs the field using a real salinity data example from Argo [28]. The data set contains long-term salinity data in latitude $+10.516$

and longitude +161.925. For a given $Q = 300$ and $T_{coh} = 20$ s, we use a 30 × 10 spatial map in random frame m to show the reconstruction performance of our scheme in Fig. 6. Fig. 6(a) is the spatial map in random frame n. Given that the number of sampled sensors in each frame $N' = 350$, the sufficient sensing probability $P_s = 0.9$ and SNR = 30 dB. The reconstructed map in frame n is shown in Fig. 6(b). The figure also shows that the main information of the field is not lost, and good similarity is observed between the original and the reconstructed spatial map.

4.1. Security analysis

A good encryption algorithm could resist various kinds of known attacks. In this section, we will assess the security analysis of the proposed encryption algorithm.

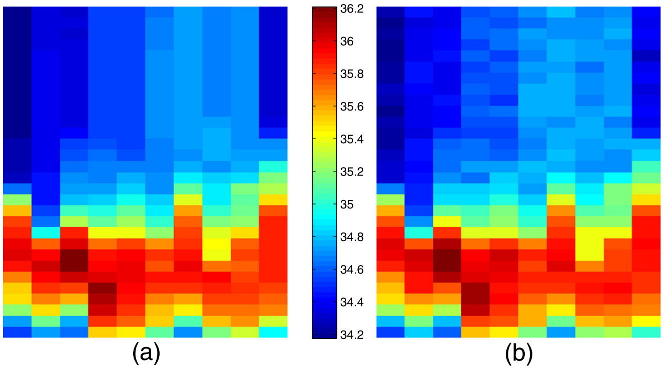

Fig. 6. The reconstruction performance of the proposed scheme with real data. (For interpretation of the colors in the figure(s), the reader is referred to the web version of this article.)

4.1.1. Key space analysis

The key space of the encryption system should be sufficiently large to resist brute force attack. In the proposed algorithm, the initial conditions and chaotic parameters of the chaotic system and the ID of each sensor constitute different secret keys of each sensor in the encryption system. Given that the floating-point precision of the initial condition is K_1, the floating-point precision of the chaotic parameters is K_2, and the ID of each sensor is K_3, the key space can be expressed as follows:

$$S = 10^{K_1+K_2} \times K_3. \tag{21}$$

The number of sensors is 300 when the maximum computation precision of K_1 is 16 and the maximum computation precision of K_2 is 15 [25]. The key space is about 3×10^{33}, which is sufficiently large to resist the brute force attacks from the eavesdropper.

4.1.2. Key sensitivity analysis

A good image encryption algorithm should have a high sensitivity to any small change of the secret key. Considering that the relationship between the initial condition of the chaotic system and the ID of each sensor, we change the parameter of the initial condition by using a small $\Delta = 10^{-16}$ to demonstrate the sensitivity of the secret key. Assuming that y is the initial condition of the sensor of ID = 100, we slightly modify y and obtain y_1. We select y as the correct parameter of the initial condition to encrypt the original data. y and y_1 are used to decrypt the encrypted data; y and y_1 are expressed as follows:

$$y = 0.2177734375, \tag{22}$$

$$y_1 = 0.2177734375000001. \tag{23}$$

The key sensitivity results of the encryption process are shown in Fig. 7. Fig. 7(a) shows the relationship between original and de-

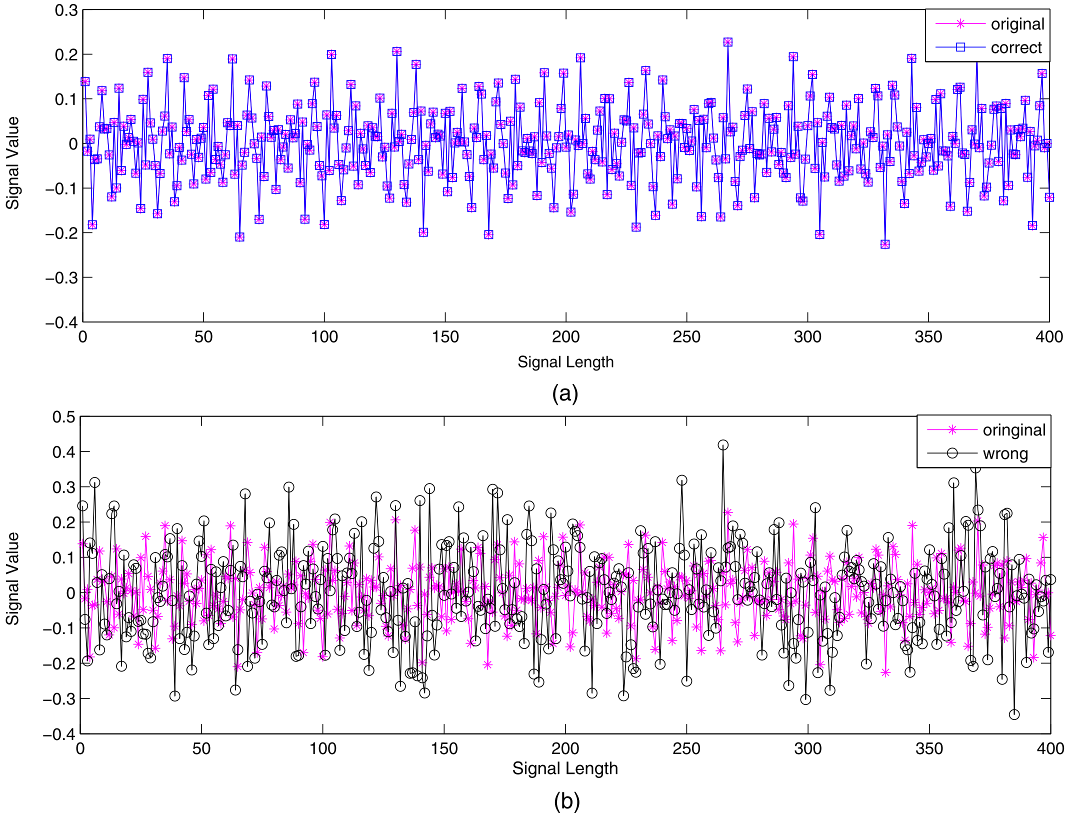

Fig. 7. The comparison between original data and decrypted data.

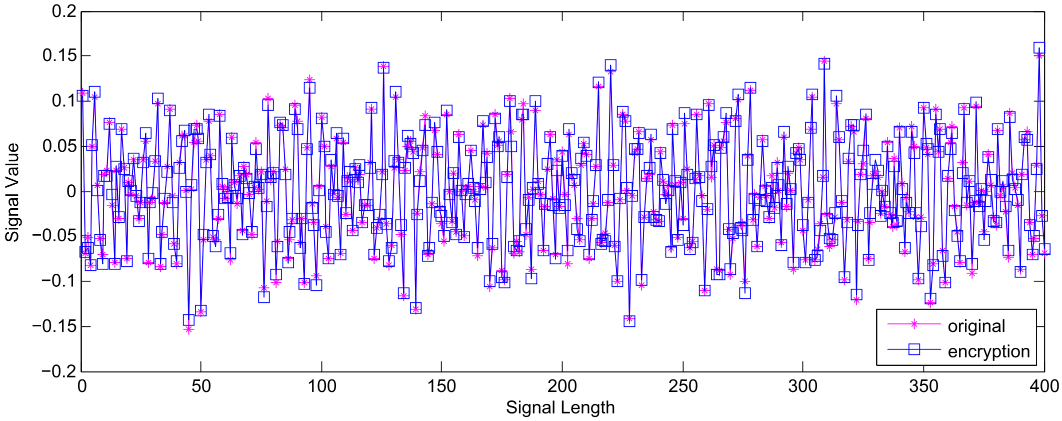

Fig. 8. The comparison between decryption data and original data with SNR = 25 dB.

cryption data with the correct initial condition y. Fig. 7(b) shows the relationship between the original and decryption data with the wrong initial condition y_1. The data in Fig. 7(a) show nearly no difference compared with the original data. Relative error is approximately in the degree of 10^{-32}. Fig. 7(b) clearly shows that nothing useful can be obtained and the relative error is as high as 100%. The experimental results show that the proposed algorithm is sensitive to the key; a small change of the matrix generation parameter in the initial condition will result in a completely different decryption result. The algorithm can prevent the eavesdropper from decrypting the data using a key similar to the secret key to decrypt the cipher data.

4.1.3. Noise attack

Given that the secure cipher data are easily affected by all kinds of noises during the transmission, the recovery accuracy of data will be reduced. Thus, a data encryption algorithm should have good robustness to resist noise attack, which is more suitable for real applications. We use white Gaussian noise to perturb the secure cipher data during transmission to test the performance. Fig. 8 shows the recovered data when SNR = 30 dB are similar to the original data. Results show that the proposed algorithm has good robustness to withstand noise attack.

4.1.4. Known-plaintext and chosen-plaintext attacks

We ensure that the initial condition of the chaotic system is correlated with the ID of each sensor to improve the capability of the proposed encryption algorithm and resist known-plaintext and chosen-plaintext attacks. The secret key of each sensor will be different because the resultant information is decided by the information of each sensor. The eavesdropper cannot obtain the useful information of the measurement matrix by encrypting special data. Therefore, the designed algorithm can resist known-plaintext and chosen-plaintext attacks.

4.2. Bandwidth analysis

Bandwidth is considerably limited in underwater acoustic networks. A low bandwidth is a critical requirement for a network scheme. In this section, we compare the bandwidth of the proposed scheme with the time-division multiple access (TDMA) transmission scheme and RACS scheme [19]. We define B_s as the minimum required bandwidth that sufficient sensing can provide and B equals the bit rate for simplicity. In TDMA scheme, this approach requires that the packets transmitted from different sensors arrive at the FC back to back. Given that the maximum collection time in a frame should be smaller than the coherence time T_{coh}, the minimum bandwidth requirement B_1 in TDMA scheme is expressed as follows:

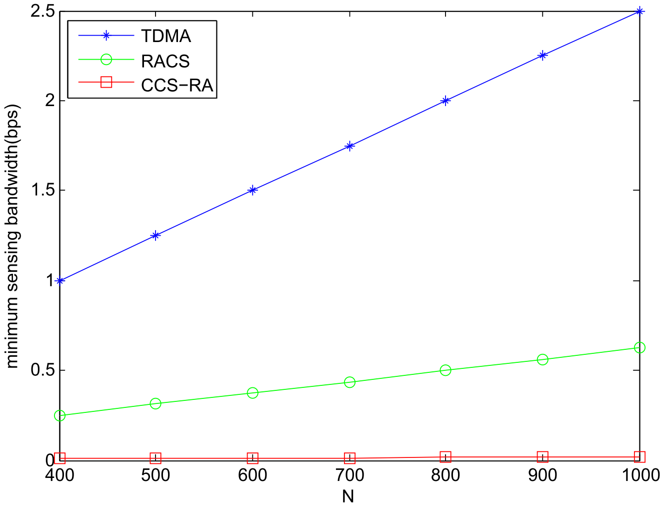

Fig. 9. The minimum bandwidth requirement with the number of sensors.

$$B_1 \geqslant \frac{NL'}{T_{coh}} = B_s, \tag{24}$$

where N is the number of all sensors and L' is the length of the data collected in a frame. With the minimum number of packets N_s' to guarantee the reconstruction in the RACS scheme, this condition results in the minimum bandwidth requirement B_2 expressed as follows:

$$B_2 \geqslant \frac{N_s' L'}{T_{coh}} = B_s. \tag{25}$$

We assume that the minimum number of useful packets that can be used to reconstruct the field by using our scheme is N_s. To ensure successful recovery, the minimum bandwidth requirement B_3 is expressed as follows:

$$B_3 \geqslant \frac{mN_s L}{T_r} = B_s, \tag{26}$$

where m is the number of transmissions. Fig. 9 shows the minimum bandwidth required for the three schemes. Given that $T_{coh} \ll T_r$, the figure illustrates that the proposed scheme could achieve the purpose using a bandwidth lower than that of TDMA and RACS, which is significant to underwater acoustic networks.

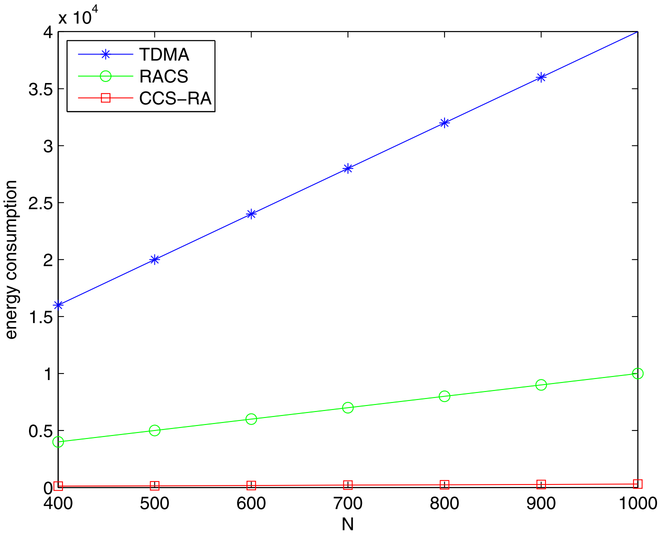

Fig. 10. The minimum energy consumption with the number of sensors.

4.3. Energy analysis

The lifetime of a network is important in underwater deployment. We analyze the total transmit energy consumption of the network for TDMA, RACS, and our scheme in this section. We let E_0 denote the energy consumption that one sensor transmits a packet to the FC. We assume that E_0 of all sensors is the same and $E_0 = 0.1$ J to simplify the calculation. From the energy consumption formula presented in [19], the total energy consumption E_1 of the conventional scheme in a period is expressed as follows:

$$E_1 = NE_0Q. \tag{27}$$

The total energy consumption E_2 of RACS in a period is expressed as follows:

$$E_2 = M'E_0Q. \tag{28}$$

M' is the number of active sensors in each period and $M' \leqslant N$. The total energy consumption E_3 of our scheme in a period is expressed as follows:

$$E_3 = mNE_0. \tag{29}$$

The comparison of the consumed energy of the three schemes is shown in Fig. 10. Our scheme ensures substantial savings compared with other cases. The energy consumption of our scheme increases slowly with the number of sensors, whereas that of other schemes increases rapidly.

5. Conclusion

This study proposes the CCS-RA scheme to achieve efficiency in energy consumption and security in data transmission by combining CCS and RA. The scheme can be adopted for large-scale sensor networks and deployed for long-term monitoring of slowly varying phenomenon. We exploit the sparsity in the spatial domain to reduce the number of sample sensors and the sparsity in the time domain to reduce the number of transmissions to reduce energy consumption. An ID-based CCS encryption algorithm is proposed to improve the security of data transmission. The encryption algorithm adopts the chaotic system to encrypt data and ensures that the parameters of the chaotic system are correlated with the ID of each sensor. This process can effectively improve the security of transmission. Furthermore, given the random collisions among packets, an RA-based repeat transmission strategy is proposed to ensure successful recovery under the shortest data-receiving time. Finally, security analysis shows that the encryption performance is excellent. Compared with a conventional TDMA scheme and the RACS scheme, the significant benefits of the proposed scheme were analyzed on the basis of bandwidth and energy consumption.

Acknowledgments

The authors thank the financial support of the Natural Science Foundation of China under Grant No. 61571387 and No. 61473247.

References

[1] S.S. Manvi, B. Manjula, Issues in underwater acoustic sensor networks, Int. J. Comput. Electr. Eng. 3 (2011) 101.

[2] A. Davis, H. Chang, Underwater wireless sensor networks, in: Oceans, 2012, 2012.

[3] J. Heidemann, W. Ye, J. Wills, A. Syed, Y. Li, Research challenges and applications for underwater sensor networking, in: Wireless Communications and Networking Conference, WCNC, 2006, 2006, pp. 228–235.

[4] Y. Zhou, Y. Fang, Y. Zhang, Securing wireless sensor networks: a survey, IEEE Commun. Surv. Tutor. 10 (2008) 6–28.

[5] I.F. Akyildiz, D. Pompili, T. Melodia, Challenges for efficient communication in underwater acoustic sensor networks, ACM SIGBED Rev. 1 (2004) 3–8.

[6] T. Rault, A. Bouabdallah, Y. Challal, Energy efficiency in wireless sensor networks: a top–down survey, Comput. Netw. 67 (2014) 104–122.

[7] U. Mitra, S. Choudhary, F. Hover, R. Hummel, Structured sparse methods for active ocean observation systems with communication constraints, IEEE Commun. Mag. 53 (2015) 88–96.

[8] B. Shahrasbi, A. Talari, N. Rahnavard TC-CSBP, Compressive sensing for time-correlated data based on belief propagation, Inf. Sci. Syst. (2011) 1–6.

[9] B. Zhang, Y. Liu, J. He, Z. Zou, An energy efficient sampling method through joint linear regression and compressive sensing, in: Fourth International Conference on Intelligent Control and Information Processing, 2013, pp. 447–450.

[10] C. Alippi, G. Anastasi, M.D. Francesco, M. Roveri, An adaptive sampling algorithm for effective energy management in wireless sensor networks with energy-hungry sensors, IEEE Trans. Instrum. Meas. 59 (2010) 335–344.

[11] R.G. Baraniuk, Compressive sensing [Lecture notes], IEEE Signal Process. Mag. 24 (2007) 118–121.

[12] E.J. Candes, M.B. Wakin, An introduction to compressive sampling, IEEE Signal Process. Mag. 25 (2) (2008) 21–30.

[13] R. Du, L. Gkatzikis, C. Fischione, M. Xiao, Energy efficient sensor activation for water distribution networks based on compressive sensing, IEEE J. Sel. Areas Commun. 33 (2015) 2997–3010.

[14] L. Xiang, J. Luo, A. Vasilakos, Compressed data aggregation for energy efficient wireless sensor networks, in: Sensor, Mesh and Ad Hoc Communications and Networks, 2011, pp. 46–54.

[15] L. Li, D. Xu, H. Peng, J. Kurths, Y. Yang, Reconstruction of complex network based on the noise via QR decomposition and compressed sensing, Sci. Rep. 7 (2017) 15036.

[16] D. Xie, H. Peng, L. Li, Y. Yang, Semi-tensor compressed sensing, Digit. Signal Process. 58 (2016) 85–92.

[17] H. Peng, Y. Tian, J. Kurths, Semitensor product compressive sensing for big data transmission in wireless sensor networks, Math. Probl. Eng. (2017) 2017.

[18] S. Han, X. Li, L. Yan, J. Xu, Z. Liu, X. Guan, Joint resource allocation in underwater acoustic communication networks: a game-based hierarchical adversarial multiplayer multiarmed bandit algorithm, Inf. Sci. (2018).

[19] F. Fazel, M. Fazel, M. Stojanovic, Random access compressed sensing for energy-efficient underwater sensor networks, IEEE J. Sel. Areas Commun. 29 (2011) 1660–1670.

[20] X. Liao, S. Lai, Q. Zhou, A novel image encryption algorithm based on self-adaptive wave transmission, Signal Process. 90 (2010) 2714–2722.

[21] X. Wang, D. Luan, A novel image encryption algorithm using chaos and reversible cellular automata, Commun. Nonlinear Sci. Numer. Simul. 18 (2013) 3075–3085.

[22] L. Xu, Z. Li, J. Li, W. Hua, A novel bit-level image encryption algorithm based on chaotic maps, Opt. Lasers Eng. 78 (2012) 17–25.

[23] X. Zhang, Y. Ren, G. Feng, Z. Qian, Compressing Encrypted Image Using Compressive Sensing, in: Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2011, pp. 222–225.

[24] R. Dautov, G.R. Tsouri, Securing while sampling in wireless body area networks with application to electrocardiography, IEEE J. Biomed. Health Inform. 20 (2014) 135–142.

[25] H. Peng, Y. Tian, J. Kurths, L. Li, Y. Yang, D. Wang, Secure and energy-efficient data transmission system based on chaotic compressive sensing in body-to-body networks, IEEE Trans. Biomed. Circuits Syst. (2017) 1–16.
[26] L. Yu, J.P. Barbot, G. Zheng, H. Sun, Compressive sensing with chaotic sequence, IEEE Signal Process. Lett. 17 (2010) 731–734.
[27] G.H. Mohimani, M. Babaiezadeh, C. Jutten, Fast sparse representation based on smoothed L0 norm, Lect. Notes Comput. Sci. 4666 (2007) 389–396.
[28] China Argo Real-time Data Center, http://www.argo.org.cn/.

Xinbin Li received his M.Sc. degree in Control Theory and Control Engineering from Yanshan University, China in 1999, and the Ph.D. degree in General and Fundamental Mechanics from Peking University, China in 2004. He is now a professor in the Institute of Electrical Engineering, Yanshan University, China. His research interests include nonlinear system and underwater acoustic networks.

Chao Wang is currently working toward his M.Sc. degree in Control Theory and Control Engineering from Yanshan University, China. His research interests include compressed sensing theory and signal processing in underwater acoustic networks.

Zijun Yang received his B.S. degree in Electrical Engineering from Harbin Institute of Electrical Technology, China in 1992. He is now an associate professor in Harbin power vocational technology college, China. His research interests include signal processing and power system.

Lei Yan is currently working toward the Ph.D. degree with the Key Lab of Industrial computer control engineering of Hebei Province, Yanshan University, China. His research interests include underwater acoustic relay networks and multi-armed bandit theory.

Song Han received his Ph.D. degree in Control Theory and Engineering from Yanshan University, China in 2018. He is now a lecturer in the Institute of Electrical Engineering, Yanshan University, China. His research interests include MAB theory and resource allocation algorithm in underwater acoustic networks.