Secure Access and Routing Scheme for Maritime Communication Network

Yuzhou Fu[1,3], Chuanao Jiang[2,3], Yurong Qin[1], and Liuguo Yin[2,3(✉)]

[1] School of Computer and Electronics Information, Guangxi University, Nanning 530004, China
[2] School of Information Science and Technology, Tsinghua University, Beijing 100084, China
[3] Key Laboratory of EDA, Research Institute of Tsinghua University in Shenzhen, Shenzhen 518057, China
yinlg@tsinghua.edu.cn

Abstract. This paper proposes a transmission scheme to ensure the maritime communication security, which includes access rules, routing selection scheme, and power allocation mechanisms. The access rules and the routing selection utilize the automatic identification system (AIS) information to choose the secure access points and routing links to prevent eavesdropping, and the power allocation limits the leaked information by means of reducing the received signal power of the eavesdroppers. The simulation results show that the intercept probability of the proposed scheme decreases by about ten to the negative two power compared with that of the contrastive scheme, and the recovering proportion for eavesdropper is less than 0.2. In addition to above, the secrecy capacity of the proposed scheme achieves about 6.8% improvement compared with the baseline scheme.

Keywords: Security · Access rules · Routing · Maritime Communication Network · Cooperative communication

1 Introduction

With the increase of maritime economic activities, the security of maritime communication network (MCN) is becoming increasingly important. Nowadays, the MCN mainly depends on the satellite and shore-based station, which cannot satisfy the increasing communication need. There have been some researches about

This work was supported by the National Natural Science Foundation of China (91538203 and 61871257), the new strategic industries development projects of Shenzhen City (JCYJ20170307145820484), the Joint Research Foundation of the General Armaments Department and the Ministry of Education (6141A02033322), and the Beijing Innovation Center for Future Chips, Tsinghua University.

S. Han et al. (Eds.): AICON 2019, LNICST 287, pp. 115–126, 2019.
https://doi.org/10.1007/978-3-030-22971-9_10

the high-speed and long-distance MCN, which mostly depend on the relay networks [1–3]. However, these schemes cannot effectively prevent the eavesdropping. Therefore, an effective transmission scheme for the maritime scenario is in urge need.

In the MCN, all the ships are mandatory to install AIS. Therefore, the location information of the ships is easy to obtain for the operators via the AIS. In the MCN, the shipborne base stations are used to provide access points for the user ships. In addition, the device-to-device (D2D) communication is enabled among the users in the scenario [4], which constitutes a flexible relay network. The physical layer security (PLS) enhances the secrecy of wireless communications by the characteristics of wireless channels, without using complex encryption/decryption algorithms [5]. Therefore, the relay-aided PLS is suited for MCN. In [6], the authors used relay selection technique to enhance the communication security and the formula of the intercept probability of the multi-relay network was derived. In [7], the technique of fountain code and relay-aided PLS were used in the wireless sensor networks. Also, the secrecy outage probability (SOP) of the DF relay network with joint multiple users and full-duplex (FD) relays was examined in [8]. In the literature [9], the author considered PLS of D2D communications and developed a Stackelberg game framework to analyze the communication rate of cellular users and secrecy rate of D2D links.

In this paper, we present a location information assisted secure access and routing scheme in the MCN, the MCN ensures the security by means of selecting the access point and the routing. To compensate high path loss in maritime network, the technique of directional antennas, narrow beam and LDPC code [10,11] are employed. With the aid of location information, the shipborne base stations can provide the secure wideband access for the user ships. If intercepting by the eavesdropper is unavoidable, the user ship can send a random sequence to shipborne base stations by D2D communication. And then, the shipborne base station uses these random sequences as the keys to encrypt original data by means of simple XOR operation. After the shipborne base station encoding the original data, the encoded data are transmitted back to the user ship. With the aid of location information and D2D communications, the eavesdropper can hardly intercept sufficient data to recover the original data. In addition to the aforementioned method, the proposed scheme can also limit the received information of eavesdroppers by power optimization, which reduces the amount of the received data packets of eavesdroppers.

The rest of this paper is organized as follows. In Sect. 2, the system model and the problem formulation are presented. Section 3 introduces the proposed transmission scheme as well as the resource allocation process in detail. Then Sect. 4 presents the simulation setup and simulation results among the proposed scheme. Finally, conclusions are drawn in Sect. 5.

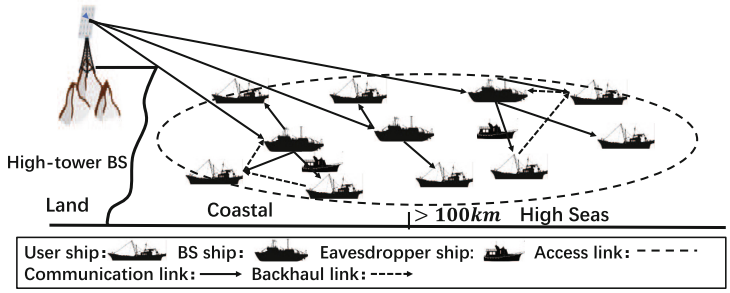

Fig. 1. Maritime Communications Network (MCN) Architecture

2 System Model and Problem Formulation

2.1 System Model

As shown in Fig. 1, the proposed scenario includes one high-tower base station (HBS), shipborne base stations (SBSs), user ships (USs) and eavesdropper ships (ESs). The HBS provides down-link transmission for the SBS. In maritime, the maritime satellite can provide the backhaul for the SBS and is connected to the HBS, so the SBSs can connect to the HBS through the satellite. The satellite backhaul can transmit the secret key to ensure security of the down-link data. Therefore, we assume that the down-link is secure. If two USs are close enough, they can communicate with each other by D2D communication. All the ESs are close to the USs. The SBS is denoted as $B = \{B_i | i = 1, 2, 3..., I\}$ and is equipped with N directional antennas to forward data to user ships. The USs denoted as $U = \{U_j | j = 1, 2, 3..., J\}$ are equipped with one directional antenna. The ESs denoted as $E = \{E_s | s = 1, 2, 3..., S\}$ are equipped with one omnidirectional antenna. The SBSs and USs can accurately receive the signal by directional antenna with the help of the AIS location information. Therefore, we assume that the interference is not considered in this paper. In this paper, we assume that the ES and the US have same antenna gain.

In the MCN scenario, the large-scale fading caused by the two-ray reflection model is modeled as [12]

$$L_{i,j} = \left(\frac{\lambda}{4\pi d_{i,j}}\right)^2 \left[2sin\left(\frac{2\pi h_i h_j}{\lambda d_{i,j}}\right)\right]. \tag{1}$$

where λ is the carrier frequency wavelength, h_i and h_j represent the heights of transmitter and receiver, and $d_{i,j}$ is the distance between transmitter and receiver. Besides, the channel coefficients of small-scale fading remain constant during one data packet and change independently among different data packet. The channel coefficient is a circularly symmetric complex Gaussian random variable, namely $\mathcal{CN}(0, 1)$. Therefore, the received signal can be written as:

$$y_{i,j} = \sqrt{p_{i,j} L_{i,j}} h_{i,j} s_k + n_{i,j}. \tag{2}$$

where $n_{i,j}$ is the additive white Gaussian noise (AWGN); s_k is the k th data symbol of stream and $p_{i,j}$ is the power of transmitter; The $h_{i,j}$ is channel coefficient. Then the signal noise ratio (SNR) of received is given by:

$$SNR_{i,j} = \frac{p_{i,j}H_{i,j}}{\sigma_{n_{i,j}}}. \tag{3}$$

where $H_{i,j} = L_{i,j}|h_{i,j}|^2$. In addition to this, the security capacity is given by:

$$C_{i,j} = log_2(1 + SNR_{i,j}) - log_2(1 + SNR_{i,s}). \tag{4}$$

2.2 Problem Formulation

The problem formulation can be divided into two parts: the user ships access (USsA) phase and the User ships backhaul (USsB) phase. In the USsA phase, the user association and power allocation are related to the channel gain and the security capacity. In addition, we define some threshold values to determine the security of USsA link. If the USsA link cannot ensure security, we will encode the data of the SBS in the USsB phase. The optimization problems are formulated as:

$$USsA(P1): \max_{\mathbf{X},\boldsymbol{P}_{I,J}} \sum_{i=1}^{I}\sum_{j=1}^{J} x_{i,j}C_{i,j}. \tag{5}$$

$$P1C1: \sum_{j=1}^{J} x_{i,j}p_{i,j} \le P_{B,th}, \forall i, \qquad P1C2: \sum_{j=1}^{J} x_{i,j} \le N, \forall i,$$

$$P1C3: \sum_{i=1}^{I} x_{i,j} \le 1, \forall j, \qquad P1C4: x_{i,j}\left(\frac{p_{i,j}H_{i,s}}{\sigma_{n_{i,s}}} \le \gamma_{th}^{E}\right), \forall i, j,$$

$$P1C5: x_{i,j}(C_{i,j} \ge C_{th}), \forall i, j, \quad P1C6: x_{i,j} \in \{0, 1\}, \forall i, j, \quad P1C7: \boldsymbol{P}_{I,J} \ge 0.$$

where P1C1 is the maximum transmission power constraint for the SBS. P1C2 represents the maximum downlink data stream constraint for SBS; P1C3 means that the users can access no more than one SBS; P1C4 presents maximum SNR of ES, where γ_{th}^{E} is maximum SNR for Eve; P1C5 is the minimum security capacity constraint for the SBS; P1C6 and P1C7 constrain the value of variables, where $x_{i,j} = 1$ means that the user ship (U_j) selects BS (B_i) as the access point.

$$USsB(P2): \max_{\mathbf{X},\boldsymbol{P}_{J,M},\boldsymbol{P}_{M,I}} \sum_{i=1}^{I}\sum_{\substack{m=1 \\ m \ne j}}^{J} Q_{m,i} \tag{6}$$

$$Q_{m,i} = \min\left\{x_{m,i}C_{m,i}, x_{m,i}C_{j,m}\right\}. \tag{7}$$

$$P2C1: \sum_{i=1}^{I}\sum_{\substack{m=1\\m\neq j}}^{J} x_{m,i}p_{j,m} \leq P_{U,th}, \qquad P2C2: \sum_{i=1}^{I}\sum_{\substack{m=1\\m\neq j}}^{J} x_{m,i}p_{m,i} \leq P_{U,th},$$

$$P2C3: \sum_{i=1}^{I} x_{m,i} \leq 1, \forall m, \qquad P2C4: \sum_{\substack{m=1\\m\neq j}}^{J} x_{m,i} \leq 1, \forall j,$$

$$P2C5: x_{m,i}C_{m,i} \geq Q_{m,i}\forall m, i, \qquad P2C6: x_{m,i}C_{j,m} \geq Q_{m,i}\forall m, i,$$

$$P2C7: x_{m,i}\left(\frac{p_{j,m}H_{j,s}}{\sigma_{n_{j,s}}} \leq \gamma_{th}^{E}\right), \forall i, m, \qquad P2C8: x_{m,i}\left(\frac{p_{m,i}H_{m,s}}{\sigma_{n_{m,s}}} \leq \gamma_{th}^{E}\right), \forall i, m,$$

$$P2C9: x_{m,i} \in \{0,1\}\forall m, i, \qquad P2C10: \boldsymbol{P}_{J,M} \geq 0, \boldsymbol{P}_{M,I} \geq 0.$$

where P2C1 and P2C2 are the maximum transmission power constraint for the user ship; P2C3 and P2C4 mean that the users can select no more than one user ship to backhaul; P2C5 and P2C6 are the minimum security capacity constraint for the D2D link; P2C7 and P2C8 present maximum SNR of ES, where γ_{th}^{E} is maximum SNR for Eve; P2C9 and P2C10 constrain the value of variables.

3 Algorithm Development

In the previous section, we know that the problem (5) and (6) are non-convex. Therefore, We should transform the non-convex problem into a series of convex subproblems with logarithmic approximation [13], and then we use the Lagrangian dual method to solve. Finally, we can get the original problem solution by the successive convex approximation (SCA) approach proposed in [14]. We will make use of the following lower bound:

$$\theta\log_2(SNR) + \beta \geq \log_2(1+SNR). \tag{8}$$

that is tight at $SNR = \overline{SNR}$ when the approximation constants are chosen as

$$\theta = \frac{\overline{SNR}}{1+\overline{SNR}}. \tag{9}$$

$$\beta = \ln\left(1+\overline{SNR}\right) - \frac{\overline{SNR}}{1+\overline{SNR}}\ln\left(\overline{SNR}\right). \tag{10}$$

By applying the logarithmic approximation and changing the variables by $\hat{\mathbf{P}}_{I,J} = \ln \mathbf{P}_{I,J}$, $\hat{\mathbf{P}}_{J,M} = \ln \mathbf{P}_{J,M}$, $\hat{\mathbf{P}}_{M,I} = \ln \mathbf{P}_{M,I}$. The lower bound of the objective function is obtained as follows:

$$C_{i,j} \geq \hat{C}_{i,j} = \frac{1}{\ln 2} \left(\theta_{i,j} \ln \left(SNR_{i,j}\right) + \beta_{i,j}\right) - \log_2 \left(1 + \gamma_{th}^{E}\right). \tag{11}$$

$$Q_{m,i} \geq \hat{Q}_{m,i} = \min \left\{ x_{m,i} \hat{C}_{m,i}, x_{m,i} \hat{C}_{j,m} \right\}. \tag{12}$$

For solving the aforementioned questions, we introduce the Lagrangian dual method. The Lagrangian functions are given as

$$\begin{aligned}
&L_{P1}(e^{\hat{\mathbf{P}}_{I,J}}, X, \mu, \kappa, \zeta, \omega, \tau) \\
&= -\sum_{i=1}^{I}\sum_{j=1}^{J} x_{i,j}\hat{C}_{i,j} - \sum_{i=1}^{I} \mu_i (P_{B,th} - \sum_{j=1}^{J} x_{i,j} e^{\hat{p}_{i,j}}) \\
&\quad - \sum_{i=1}^{I} \kappa_i (N - \sum_{j=1}^{J} x_{i,j}) - \sum_{j=1}^{J} \zeta_j (1 - \sum_{i=1}^{I} x_{i,j}) \\
&\quad - \sum_{i=1}^{I}\sum_{j=1}^{J} \omega_{i,j} x_{i,j} \left(\gamma_{th}^{E} - \frac{e^{\hat{p}_{i,j}} H_{i,s}}{\sigma_{n_{i,s}}}\right) \\
&\quad - \sum_{i=1}^{I}\sum_{j=1}^{J} \tau_{i,j} x_{i,j} (\hat{C}_{i,j} - C_{th}).
\end{aligned} \tag{13}$$

$$\begin{aligned}
&L_{P2}(e^{\hat{\mathbf{P}}_{J,M}}, e^{\hat{\mathbf{P}}_{M,I}}, X, \lambda, \eta, \epsilon, \rho, \varphi, \phi, \xi, \partial) \\
&= -\sum_{i=1}^{I} \sum_{\substack{m=1 \\ m \neq j}}^{J} \hat{Q}_{m,i} - \lambda \left(P_{U,th} - \sum_{i=1}^{I} \sum_{\substack{m=1 \\ m \neq j}}^{J} x_{m,i} e^{\hat{p}_{j,m}} \right) - \eta \left(P_{U,th} - \sum_{i=1}^{I} \sum_{\substack{m=1 \\ m \neq j}}^{J} x_{m,i} e^{\hat{p}_{m,i}} \right) \\
&- \sum_{\substack{m=1 \\ m \neq j}}^{J} \epsilon_m (1 - \sum_{i=1}^{I} x_{m,i}) - \sum_{i=1}^{I} \rho_j (1 - \sum_{\substack{m=1 \\ m \neq j}}^{J} x_{m,i}) \\
&- \sum_{i=1}^{I} \sum_{\substack{m=1 \\ m \neq j}}^{J} \varphi_{m,i} (x_{m,i} \hat{C}_{m,i} - \hat{Q}_{m,i}) - \sum_{i=1}^{I} \sum_{\substack{m=1 \\ m \neq j}}^{J} \phi_{m,i} (x_{m,i} \hat{C}_{j,m} - \hat{Q}_{m,i}) \\
&- \sum_{i=1}^{I} \sum_{\substack{m=1 \\ m \neq j}}^{J} \xi_{m,i} x_{m,i} \left(\gamma_{th}^{E} - \frac{e^{\hat{p}_{j,m}} H_{j,s}}{\sigma_{n_{j,s}}} \right) - \sum_{i=1}^{I} \sum_{\substack{m=1 \\ m \neq j}}^{J} \partial_{m,i} x_{m,i} \left(\gamma_{th}^{E} - \frac{e^{\hat{p}_{m,i}} H_{m,s}}{\sigma_{n_{m,s}}} \right).
\end{aligned} \tag{14}$$

where the parameters $\mu, \delta, \zeta, \omega, \tau, \lambda, \eta, \epsilon, \rho, \varphi, \phi, \xi, \partial$ are the Lagrangian multipliers. By solving $\frac{\partial L_{P1}}{\partial e^{\hat{p}_{i,j}}} = 0$, $\frac{\partial L_{P1}}{\partial x_{i,j}} = 0$, $\frac{\partial L_{P2}}{\partial e^{\hat{p}_{j,m}}} = 0$, $\frac{\partial L_{P2}}{\partial e^{\hat{p}_{m,i}}} = 0$, $\frac{\partial L_{P2}}{\partial x_{m,i}} = 0$, we can obtain the optimal solutions as

$$p_{i,j} = \left[\frac{\theta_{i,j} x_{i,j} (1 + \tau_{i,j})}{\ln 2 \left(\mu_i + \frac{\omega_{i,j} H_{i,s}}{\sigma_{n_{i,s}}} \right)} \right]^{+}. \tag{15}$$

$$x_{i,j} = 1|_{i,j=\max \tau_{i,j}\hat{C}_{i,j}}. \tag{16}$$

$$p_{j,m} = \left[\sum_{i=1}^{I} \frac{\theta_{m,i}\varphi_{m,i}x_{m,i}}{\ln 2\left(\lambda + \frac{\xi_{j,m}H_{j,s}}{\sigma_{n_{j,s}}}\right)}\right]^{+}. \tag{17}$$

$$p_{m,i} = \left[\frac{\theta_{m,i}\phi_{m,i}x_{m,i}}{\ln 2\left(\eta + \frac{\partial_{m,i}H_{m,s}}{\sigma_{n_{m,s}}}\right)}\right]^{+}. \tag{18}$$

$$x_{m,i} = 1|_{m,i=\max \min\left\{\varphi_{j,m}\hat{C}_{j,m},\phi_{m,i}\hat{C}_{m,i}\right\}}. \tag{19}$$

Where (x^{+}) is min $\{0, x\}$. Note that the user ships tend to access the SBS and select user ship with the largest security link rate. While the USsB phase should consider two links of security rate. Finally, we calculate the Lagrange multipliers using the subgradient method.

$$\mu_i[t+1] = \left[\mu_i[t] - \delta_{\mu_i}[t+1]\left(P_{B,th} - \sum_{j=1}^{J} x_{i,j}e^{\hat{p}_{i,j}}\right)\right]^{+},$$

$$\omega_{i,j}[t+1] = \left[\omega_{i,j}[t] - \delta_{\omega_{i,j}}[t+1]\left\{x_{i,j}\left(\gamma_{th}^{E} - \frac{p_{i,j}H_{i,s}}{\sigma_{n_{i,s}}}\right)\right\}\right]^{+},$$

$$\tau_{i,j}[t+1] = \left[\tau_{i,j}[t] - \delta_{\tau_{i,j}}[t+1]\left\{x_{i,j}(C_{i,j} - C_{th})\right\}\right]^{+},$$

$$\lambda[t+1] = \left[\lambda[t] - \delta_{\lambda}[t+1]\left(P_{U,th} - \sum_{i=1}^{I}\sum_{\substack{m=1\\m\neq j}}^{J} x_{m,i}p_{j,m}\right)\right]^{+},$$

$$\eta[t+1] = \left[\eta[t] - \delta_{\eta}[t+1]\left(P_{U,th} - \sum_{i=1}^{I}\sum_{\substack{m=1\\m\neq j}}^{J} x_{m,i}p_{m,i}\right)\right]^{+},$$

$$\varphi_{m,i}[t+1] = \left[\varphi_{m,i}[t] - \delta_{\varphi_{m,i}}[t+1]\left(x_{m,i}C_{m,i} - Q_{m,i}\right)\right]^{+},$$

$$\phi_{m,i}[t+1] = \left[\phi_{m,i}[t] - \delta_{\phi_{m,i}}[t+1]\left(x_{m,i}C_{j,m} - Q_{m,i}\right)\right]^{+},$$

$$\xi_{m,i}[t+1] = \left[\xi_{m,i}[t] - \delta_{\xi_{m,i}}[t+1]\left\{x_{m,i}\left(\gamma_{th}^{E} - \frac{p_{j,m}H_{j,s}}{\sigma_{n_{j,s}}}\right)\right\}\right]^{+},$$

$$\partial_{m,i}[t+1] = \left[\partial_{m,i}[t] - \delta_{\partial_{m,i}}[t+1]\left\{x_{m,i}\left(\gamma_{th}^{E} - \frac{p_{m,i}H_{m,s}}{\sigma_{n_{m,s}}}\right)\right\}\right]^{+}. \tag{20}$$

In the Algorithm 1, we defined a threshold value (C_{th}^{Min}). If the security capacity of SBS link is less than threshold value, the SBS link is not security. Therefore, we use Algorithm 2 to replan route. And then, the Algorithm 1 will be performed based on the access scheme of algorithm 2 until the results converge.

Algorithm 1

Input: the user set U
while U is not empty **do**
  Initialize: $t = 1, \theta_{i,j} = 1, \beta_{i,j} = 0, p_{i,j} = 1, \forall i, j.\ \mu, \omega, \tau \geq 0$
  while $x_{i,j}, p_{i,j}$ converge and $C_{i,j} \geq C_{th}^{Min}, \forall i, j$ **do**
    Update $x_{i,j}, H_{i,s}$ calculated by (16) and Algorithm 2
    while $p_{i,j}$ converge,$\forall i, j$ **do**
      for $i = 1$ to I **do**
        for $j = 1$ to J **do**
          Update $p_{i,j}$ calculated by (15)
        end for
      end for
      Update μ, ω, τ calculated by (20) and $t = t + 1$
    end while
    for $i = 1$ to I **do**
      for $j = 1$ to J **do**
        Update $\theta_{i,j}, \beta_{i,j}$ calculated by (9) and (10)
      end for
    end for
    Update $C_{i,j}$ calculated by (4)
    if $C_{i,j} \leq C_{th}^{Min}$ **then**
      Loading the **Algorithm** 2
    end if
  end while
  Set: $U = U - U_j$
end while

4 Performance Evaluation

In this section, the simulation setup and simulation results are presented for evaluating the performance of proposed scheme. We choose the DFbORS scheme in [6] as the compared scheme, and the power of SBS is equal allocated. The carrier frequency is set as 2 GHz and the available bandwidth B is 10 MHz. The AWGN power is defined as $\sigma_n = BN_0$, where N_0 is the AWGN spectral efficiency, and $N_0 = -174$ dBm/Hz. We set $P_{B,th} = 43$ dBm and $P_{U,th} = 40$ dBm. The heights of SBS antennas, user ship antennas and ES antennas are 30 m, 15 m and 15 m respectively. The maximum data streams of SBS number N is set to 6. The number of user ships is also a variable which ranges from 20 to 80. The number of ESs is set to 3. We emulate the transmission for 10^5 times. Moreover, the total number of data packets is denoted as K, which is assumed to be 128. If the eavesdropper are successfully recovering 80% of original data in one transmission time, the total confidential file is successfully intercepted by ES. The packet error rate (PER) can be defined as [15]:

$$FER_n(\boldsymbol{\gamma}) = \begin{cases} 1, & \text{if } 0 < \boldsymbol{\gamma} < \boldsymbol{\gamma}_{pn}; \\ a_n exp(-g_n \boldsymbol{\gamma}), & \text{if } \boldsymbol{\gamma} \geq \boldsymbol{\gamma}_{pn}. \end{cases} \tag{21}$$

Algorithm 2

Initialize: $t = 1, \theta_{j,m} = \theta_{m,i} = 1, \beta_{j,m} = \beta_{m,i} = 0, p_{j,m} = p_{m,i} = 1, \forall m, i.\ \lambda, \eta, \varphi, \phi, \xi, \partial \geq 0$
while $x_{m,i}, p_{j,m}, p_{m,i}$ converge, $\forall i, j$ **do**
  Update $x_{m,i}$ calculated by (19)
  while $p_{j,m}, p_{m,i}$ converge,$\forall m, i, j$ **do**
    for $m = 1$ to J **do**
      Update $p_{j,m}$ calculated by (17)
      for $i = 1$ to I **do**
        Update $p_{m,i}$ calculated by (18)
      end for
    end for
    Update $\lambda, \eta, \varphi, \phi, \xi, \partial$ and $t = t + 1$ calculated by (20)
  end while
  for $m = 1$ to J **do**
    Update $\theta_{j,m}, \beta_{j,m}$ calculated by (9) and (10)
    for $i = 1$ to I **do**
      Update $\theta_{m,i}, \beta_{m,i}$ calculated by (9) and (10)
    end for
  end for
end while
Update $x_{i,j} = 1$ and $H_{i,s} = 0$

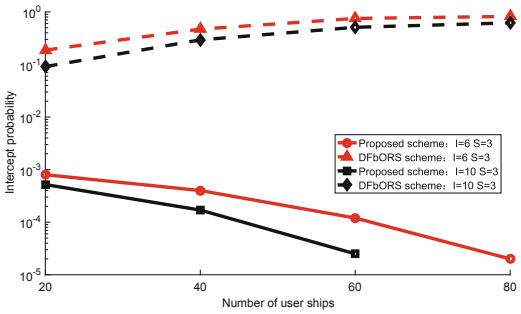

Fig. 2. Comparison of intercept probability between the proposed scheme and the baseline scheme, where the number of user ships varies from 20 to 80.

Where $\boldsymbol{\gamma}$ is received SNR and n denotes mode index. The fitting parameters of different transmission modes can be found in [16]. The fitting parameters are listed as follows [16]:

$$\begin{aligned} a_n &= 50.1222, \\ g_n &= 0.6644, \\ \boldsymbol{\gamma}_{pn} &= 7.7021. \end{aligned} \tag{22}$$

In the simulation, we set a situation, namely different number of SBSs. In Fig. 2, the intercept probabilities of the proposed scheme decline with the

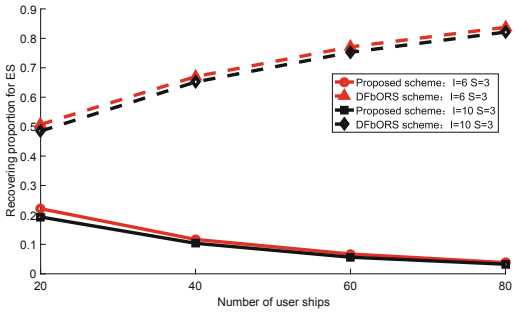

Fig. 3. Comparison of recovering proportion for Eve between the proposed scheme and the baseline scheme, where the number of user ships varies from 20 to 80.

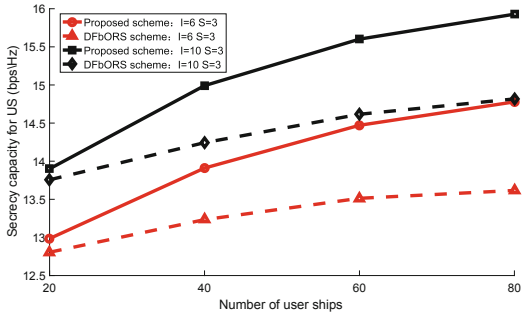

Fig. 4. Comparison of secrecy capacity for user ship between the proposed scheme and the baseline scheme, where the number of user ships varies from 20 to 80.

increase of the number of user ships, while the intercept probabilities of the DFbORS scheme are increasing. In this situation (namely, $I = 10, S = 3$), the intercept probability of the proposed scheme is less than ten to the negative five power if the number of user ships is more than 60. With the increase of the number of user ships, the proposed scheme can be more flexible to select routing with D2D communication. While, the contrastive scheme is opposite. The intercept probability of the proposed scheme at least decreases by about ten to the negative two power compared with that of the DFbORS scheme. Hence, the proposed scheme achieves a better communication security than the DFbORS scheme. From Fig. 3, the recovering probability of the proposed scheme is lower than the baseline scheme. The recovering probability for EB is less than 0.2, because the eavesdropper can receive sufficient original data and the random sequences. In Fig. 4, the secrecy capacity of the proposed scheme achieves about 6.8% improvement compared with the baseline scheme. Namely, the proposed scheme can securely transmit more data in one transmission process.

5 Conclusions

This paper proposes an access and routing transmission scheme in the maritime communication networks. According to the location information from AIS, the scheme can select access point and routing flexibly to avoid eavesdropping. In addition, the power allocation can limit the leaked information by means of reducing the received signal power of the eavesdroppers. The simulation results show that the proposed scheme achieves a better performance in security. The proposed scheme can at least decrease intercept probability by about ten to the negative two power compared with the contrastive scheme, and the recovering proportion for EB is less than 0.2. The secrecy capacity of the proposed scheme achieves about 6.8% improvement compared with the baseline scheme. Namely, the proposed scheme can securely transmit more data in one transmission process. In conclusion, the proposed scheme can securely transmit more data in one transmission process.

References

1. Li, Y.: Efficient coastal communications with sparse network coding. IEEE Netw. **32**(4), 122–128 (2018)
2. Rao, S.N., Raj, D., Parthasarathy, V.: A novel solution for high speed internet over the oceans. In: Proceedings of IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops, Honolulu, pp. 906–912 (2018)
3. Singh, D., Kimbahune, S., Singh, V.V.: Mobile signal extension in deep sea - towards a safe and sustainable fisheries. In: Proceeding of 2016 ITU Kaleidoscope: ICTs for a Sustainable World, Bangkok, pp. 1–8 (2016)
4. Liu, J.: Device-to-device communication in LTE-advanced networks. A survey. IEEE Commun. Surv. Tutorials **17**(4), 1923–1940 (2015)
5. Hong, Y.W.P.: Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches. IEEE Signal Process. Mag. **30**(5), 29–40 (2013)
6. Zou, Y.: Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J. Sel. Areas Commun. **31**(10), 2099–2111 (2013)
7. Sun, L.: Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks. IEEE Trans. Ind. Inf. **12**(1), 291–300 (2016)
8. Feng, Y., Yang, D.Z., Yan, S.: Physical layer security enhancement in multi-user multi-full-duplex-relay networks. In: Proceedings of 2017 IEEE International Conference on Communications, Paris, pp. 1–7 (2017)
9. Luo, Y., Cui, L., Yang, Y.: Power control and channel access for physical-layer security of D2D underlay communication. In: 2015 International Conference on Wireless Communications and Signal Processing, Nanjing, pp. 1–5 (2015)
10. Chen, Z.: CodeHop: physical layer error correction and encryption with LDPC-based code hopping. Sci. China Inf. Sci. **59**, 102309:1C–102309:15 (2016)
11. Ping, W.: An efficient helicopter-satellite communication scheme based on check-hybrid LDPC coding. Tsinghua Science and Technology **10**(26599), TST.9010038 (2018)
12. Zhao, Y., Ren, J., Chi, X.: Maritime mobile channel transmission model based on ITM. In: 2nd International Symposium on Computer, Communication, Control and Automation. Atlantis Press (2013)

13. Papandriopoulos, J., Evans, J.S.: SCALE: a low-complexity distributed protocol for spectrum balancing in multiuser DSL networks. IEEE Trans. Inf. Theor. **55**(8), 3711–3724 (2009)
14. Marks, B.R.: A general inner approximation algorithm for nonconvex mathematical programs. Oper. Res. **26**(4), 681–683 (1978)
15. Liu, Q.: Queuing with adaptive modulation and coding over wireless links: cross-Layer analysis and design. IEEE Trans. Wireless Commun. **4**(3), 1142–1153 (2005)
16. Qinghe, D., Ying, X., Wanyu, L., et al.: Security enhancement for multicast over internet of things by dynamically constructed fountain codes. Wireless Commun. Mob. Comput. **2018**, 1–11 (2018)