SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Secure Routing and Transmission Scheme for Space-Ocean Broadband Wireless Network

Yuzhou FU[1, 3], Chuanao JIANG[2, 3], Yurong QIN[1*] & 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*

Appendix A Model

The relay network link and SAT network are main networks and work in the same carrier frequency while the D2D network works in different carrier frequency, which means that there is interference between the SAT network and the relay network. Assuming the HBS has sufficient computing capacity and frequency resource, the HBS-RS link operates in the orthogonal frequency division multiplexing (OFDM) mode and RS-user ship link operates in the frequency division multiple access (FDMA) mode, which means that there is no interference between different relay links. All RSs and user ships are assumed to be equipped with directional antennas to transmit signals and can accurately transmit signal with the help of the AIS location information. The ESs can intercept encoded packets if the ESs is within the coverage of communication signals. In addition, all ships are assumed to be equipped with omnidirectional antennas to receive signals. In this study, we assume that the ESs and user ships have the same antenna gain. The ESs are near user ships. In addition, all the ESs are non-colluding. The HBS, denoted as T, is equipped with N^{ant} directional antennas and can support N^{ant} RSs in one relay transmission phase. There are J user ships in high seas wireless network, denoted as $U = \{U_j | j = 1, 2, 3..., J\}$. $U^{sel} = \{U_n^{sel} | n = 1, 2, 3..., N\}$ denotes the user ships selected from U in one relay transmission phase. Total number of the selected users is less than N^{ant} in one relay transmission phase. $U^{not} = \{U_g^{not} | g = 1, 2..., G\}$ denotes the user ships cannot receive sufficient fountain packet in the relay phase. The RS, denoted as $R = \{R_i | i = 1, 2, 3..., I\}$ can relay the message from HBS to user ship. The ES denoted as $E = \{E_s | s = 1, 2, 3..., S\}$.

In the proposed communication scenario, the large-scale fading caused by the path loss is modeled as

$$PL(d_{t,r}) = d_{t,r}^{-\eta}, \tag{A1}$$

where η is the path loss exponent. Besides, the channel coefficients of small-scale fading remain constant during one fountain packet and change independently among different fountain packet. $d_{t,r}$ is the distance between the transmitter and the receiver. The channel coefficient is a circularly symmetric complex Gaussian random variable, namely $\mathcal{CN}(0, 1)$. Additive Gaussian white noise (AWGN) is denoted as the variance N_0. During one fountain packet, the received signal via direct transmission (DT) is expressed as

$$y_{t,r}^{DT} = \sqrt{P_t d_{t,r}^{-\eta}} h_{t,r} x + n, \tag{A2}$$

where P_t denotes the power of transmitter; $h_{t,r}$ denotes the rayleigh fading channel coefficients for the communication link between the transmitter and the receiver; n is the AWGN power; x represents a fountain packet. Consequently, the received signal-noise-ratio (SNR) of direct transmission (DT) can be defined as

$$\gamma_{t,r}^{DT} = \frac{P_t H_{t,r}}{\sigma_n}, \tag{A3}$$

where $H_{t,r} = |h_{t,r}|^2 d_{t,r}^{-\eta}$. σ_n is the AWGN power. Similarly, during one fountain packet, the received signal at relay ship R_i in amplify-and-forward (AF) mode can be given by

$$y_{T,i}^{AF} = \sqrt{P_{T,i} d_{T,i}^{-\eta}} h_{T,i} x + n + n_{S,i}. \tag{A4}$$

The received signal to interference plus noise ratio (SINR) at relay ship can be defined as

$$\gamma_{T,i}^{AF} = \frac{P_{T,i} H_{T,i}}{\sigma_n + \sigma_{n_{S,i}}}, \tag{A5}$$

* Corresponding author (email: qyr@gxu.edu.cn)

where $P_{T,i}$ denotes the power of transmitter; $d_{T,i}$ is the distance between the HBS and the R_i; $h_{T,i}$ is the small-scale gain, $n_{S,i}$ and $\sigma_{n_{S,i}}$ is the interference from the satellite. Meanwhile, the received signal at user ship U^{sel} from R_i is expressed as

$$y_{i,n}^{AF} = \sqrt{P_{i,n} d_{i,n}^{-\eta}} h_{i,n} \beta_i y_{T,i}^{AF} + n + n_{S,n},$$
$$\beta_i = \sqrt{\frac{1}{P_{T,i} H_{T,i} + \sigma_n + \sigma_{n_{S,i}}}}, \tag{A6}$$

where β_i is a scaling factor in AF mode. The $n_{S,n}$ is the interference from the satellite. Then the received SINR of U_n^{sel} and the received of E_s can be written as

$$\gamma_{i,n}^{AF} = \frac{P_{T,i} a_{T,i} P_{i,n} b_{i,n}}{P_{i,n} b_{i,n} + P_{T,i} a_{T,i} + 1}, \tag{A7}$$

$$\gamma_{i,s}^{AF} = \frac{P_{T,i} a_{T,i} P_{i,n} b_{i,s}}{P_{i,n} b_{i,s} + P_{T,i} a_{T,i} + 1}, \tag{A8}$$

where $a_{T,i} = \frac{H_{T,i}}{\sigma_n + \sigma_{S,i}}, b_{i,n} = \frac{H_{i,n}}{\sigma_n + \sigma_{i,n}}, b_{i,s} = \frac{H_{i,s}}{\sigma_n + \sigma_{i,s}}$.

The $H_{i,s}$ denotes the coefficient between E_s and R_i. If the transmission link is secure, the $H_{i,s}$ tends to zero. Based on the formula above, the link capacity and the secrecy capacity are given by

$$R_{T,i} = log_2(1 + \gamma_{T,i}^{AF}), \tag{A9}$$

$$C_{i,n} = log_2(1 + \gamma_{i,n}^{AF}) - log_2(1 + \gamma_{i,s}^{AF}), \tag{A10}$$

$$C_{j,g} = log_2(1 + \gamma_{j,g}^{DT}) - log_2(1 + \gamma_{j,s}^{DT}), \tag{A11}$$

where $R_{T,i}$ represents the link capacity between the HBS and the R_i, $C_{i,n}$ represents the secrecy capacity of relay link and $C_{j,g}$ represents the secrecy capacity of D2D link between the jth user ship and U_g^{not}.

Appendix B Algorithm Development

In the optimization problem of P1, the C1 is a transmitting power constraint for HBS, where $P_{T,th}$ is the maximum transmitting power for HBS; C2 represents the minimal power requirements for the allocated power, where γ_{th}^{TR} is minimal SINR threshold for RS; and C3 constrains the value of variables.

In the optimization problem of P2, the C4 is transmitting power constraint for RS, where $P_{R,th}$ is the maximum transmitting power threshold for RS; C5 means that the user ships can access no more than one RS; C6 represents minimal capacity requirements of user ships, where C_{th}^{U} is minimal capacity for user ships; C7 represents maximum capacity requirements of Eavesdropper, where C_{th}^{E} is maximum capacity for eavesdropper; C8 ensures that the optimized security capacity is higher than zero; C9 and C10 constrain the value of variables, where $x_{i,n} = 1$ means that the user ships (U_n^{sel}) select RS (R_i) as the relay node.

Appendix C Solving the Optimization Problem

Appendix C.1 Solving the Optimization Problem of relay Phase

The optimization problem of P2 is a non-convex and combinatorial problem. Therefore, we need to transform the original problem into a convex problem by logarithmic approximation [1]. Then the transformed problem is solved by the Lagrangian dual method. Next, based on the SCA method [2], we solve the problem with an iterative algorithm. Because the C9 also is a non-convex constraint, we relax the integer variable $x_{i,n} \in [0, 1]$ into a constant variable. We use the logarithmic approximation [1] as follow:

$$\ln(1 + \gamma_{i,n}^{AF}) \geqslant \theta_{i,n} \ln(\gamma_{i,n}^{AF}) + \beta_{i,n}. \tag{C1}$$

that is tight at $\gamma_{i,n}^{AF} = \overline{\gamma_{i,n}^{AF}}$ when the approximation constants are chosen as:

$$\theta_{i,n} = \frac{\overline{\gamma_{i,n}^{AF}}}{1 + \overline{\gamma_{i,n}^{AF}}}, \tag{C2}$$

$$\beta_{i,n} = \ln\left(1 + \overline{\gamma_{i,n}^{AF}}\right) - \frac{\overline{\gamma_{i,n}^{AF}}}{1 + \overline{\gamma_{i,n}^{AF}}} \ln\left(\overline{\gamma_{i,n}^{AF}}\right). \tag{C3}$$

By applying the logarithmic approximation and changing the variables by $\hat{\mathbf{P}}_{T,R} = \ln \mathbf{P}_{T,R}$, $\hat{\mathbf{P}}_{R,U^{sel}} = \ln \mathbf{P}_{R,U^{sel}}$, we obtain the lower bound of the objective function as follow

$$\sum_{i=1}^{I} \sum_{n=1}^{N} x_{i,n} R_{T,i} \geqslant \sum_{i=1}^{I} \sum_{n=1}^{N} x_{i,n} \hat{R}_{T,i}, \tag{C4}$$

$$\sum_{i=1}^{I} \sum_{n=1}^{N} x_{i,n} C_{i,n} \geqslant \sum_{i=1}^{I} \sum_{n=1}^{N} x_{i,n} \hat{C}_{i,n}. \tag{C5}$$

where

$$\hat{R}_{T,i} = \frac{1}{\ln 2}\left(\theta_{T,i}\ln\left(\gamma_{T,i}^{AF}\right) + \beta_{T,i}\right),$$
$$\hat{C}_{i,n} = \frac{1}{\ln 2}\left(\theta_{i,n}\ln\left(\gamma_{i,n}^{AF}\right) + \beta_{i,n}\right) - C_{th}^{E}.$$

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

$$\begin{aligned} LF1 = {} & L(\hat{R}_{T,i}, e^{\hat{P}_{T,R}}, \boldsymbol{\mu}, \boldsymbol{\omega}) \\ & - \sum_{i=1}^{I}\sum_{n=1}^{N} x_{i,n}\hat{R}_{T,i} - \sum_{n=1}^{N}\mu_n(P_{T,th} - \sum_{i=1}^{I} x_{i,n}e^{\hat{p}_{T,i}}) \\ & - \sum_{i=1}^{I}\omega_i\sum_{n=1}^{N} x_{i,n}(e^{\hat{p}_{T,i}} - \frac{\gamma_{th}^{TR}\sigma_n}{H_{T,i}}), \end{aligned} \tag{C6}$$

$$\begin{aligned} LF2 = {} & L(\hat{C}_{i,n}, X, e^{\hat{P}_{R,U^{sel}}}, \boldsymbol{\lambda}, \boldsymbol{\xi}, \boldsymbol{\varphi}, \boldsymbol{\phi}) \\ & - \sum_{i=1}^{I}\sum_{n=1}^{N} x_{i,n}\hat{C}_{i,n} - \sum_{i=1}^{I}\sum_{n=1}^{N}\lambda_{in}(P_{R,th} - e^{\hat{p}_{i,n}}) \\ & - \sum_{n=1}^{N}\xi_n(1 - \sum_{i=1}^{I} x_{i,n}) - \sum_{i=1}^{I}\sum_{n=1}^{N} x_{i,n}(\hat{C}_{i,n} - C_{th}^{U}) \\ & - \sum_{i=1}^{I}\sum_{n=1}^{N} x_{i,n}(C_{th}^{E} - \hat{C}_{i,s}), \end{aligned} \tag{C7}$$

where the parameters $\boldsymbol{\mu}, \boldsymbol{\omega}, \boldsymbol{\lambda}, \boldsymbol{\xi}, \boldsymbol{\varphi}, \boldsymbol{\phi}$ are the Lagrangian multipliers. By solving $\frac{\partial LF1}{\partial e^{\hat{P}_{T,i}}} = 0$, $\frac{\partial LF2}{\partial e^{\hat{P}_{i,n}}} = 0$ we can obtain the optimal solutions as

$$p_{T,i} = \left[\sum_{n=1}^{N}\frac{\theta_{T,i}x_{i,n}}{\ln 2\,(\mu_n - \omega_i)}\right]^{+}, \tag{C8}$$

$$\begin{aligned} p_{i,n} &= \left[\frac{x_{i,n}}{\lambda_{in}\ln 2}\{\theta_{i,n}(1+\varphi_{in})F_1 - \theta_{i,n}^{E}\phi_{in}F_2\}\right]^{+}, \\ F_1 &= \frac{p_{T,i}a_{T,i} - 1}{p_{T,i}a_{T,i}(p_{T,i}a_{T,i} + p_{i,n}b_{i,n} + 1)}, \\ F_2 &= \frac{p_{T,i}a_{T,i} - 1}{p_{T,i}a_{T,i}(p_{T,i}a_{T,i} + p_{i,n}b_{i,s} + 1)}, \end{aligned} \tag{C9}$$

$$\begin{aligned} \frac{\partial LF2}{\partial x_{i,n}} &= -\hat{C}_{i,n} + \xi_n - (\hat{C}_{i,n} - C_{th}^{U}) - (C_{th}^{E} - \hat{C}_{i,s}), \\ &\approx -\hat{C}_{i,n} + \hat{C}_{i,s}, \end{aligned} \tag{C10}$$

where the (x^{+}) is max $\{0, x\}$. The user ships tend to select the RS with the largest security capacity, the best selected RS can be expressed as

$$\begin{aligned} x_{i,n} &= 1|_{i=minz_{i,n}}, \\ z_{i,n} &= -\hat{C}_{i,n} + \hat{C}_{i,s}. \end{aligned} \tag{C11}$$

Finally, we calculate the Lagrange multipliers using the subgradient method.

$$\begin{aligned} \mu_n[t+1] &= \left[\mu_n[t] - \delta_{\mu_n}[t+1]\left(P_{T,th} - \sum_{i=1}^{I} x_{i,n}p_{T,i}\right)\right]^{+}, \\ \omega_i[t+1] &= \left[\omega_i[t] - \delta_{\omega_i}[t+1]\{\sum_{n=1}^{N} x_{i,n}(p_{T,i} - \frac{\gamma_{th}^{TR}(\sigma_n + \sigma_{n_{S,i}})}{H_{T,i}})\}\right]^{+}, \\ \lambda_{in}[t+1] &= \left[\lambda_{in}[t] - \delta_{\lambda_{in}}[t+1](P_{R,th} - p_{i,n})\right]^{+}, \\ \varphi_{in}[t+1] &= \left[\varphi_{in}[t] - \delta_{\varphi_{in}}[t+1]\{x_{i,n}(\hat{C}_{i,n} - C_{th}^{U})\}\right]^{+}, \\ \phi_{in}[t+1] &= \left[\phi_{in}[t] - \delta_{\phi_{in}}[t+1]\{x_{i,n}(C_{th}^{E} - \hat{C}_{i,s})\}\right]^{+}, \end{aligned} \tag{C12}$$

where t is the iteration step, and $\delta[t+1]$ is the step size in each iteration of subgradient method.

Appendix C.2 Solving the Optimization Problem of D2D Phase

According to the problem (P3), by solving $\frac{\partial F_{j,g}}{\partial P_{j,g}} = 0$ we can obtain the optimal solution as

$$P_{j,g}^{opt} = \underset{P_{j,g}}{\arg}\left(\frac{\partial F_{j,g}}{\partial P_{j,g}} = 0\right), \tag{C13}$$

$$\frac{\partial F_{j,g}}{\partial P_{j,g}} = \frac{\sigma_n(H_{j,g} - H_{j,s})}{\ln 2(\sigma_n + P_{j,g}H_{j,g})(\sigma_n + P_{j,g}H_{j,s})} - \frac{\tau}{\log_2(1+\kappa m_{j,g})}. \tag{C14}$$

Then, by introducing the quadratic formula and power limitation, the optimal power allocation can be expressed as

$$P_{j,g}^{opt} = \frac{\sqrt{(\sigma_n H_{j,g} - \sigma_n H_{j,s})^2 + \frac{4\sigma_n H_{j,g} H_{j,s}\log_2(1+\kappa m_{j,g})(H_{j,g}-H_{j,s})}{\tau \ln 2}}}{2H_{j,g}H_{j,s}} - \frac{\sigma_n(H_{j,g}+H_{j,s})}{2H_{j,g}H_{j,s}}. \tag{C15}$$

$$P_{j,g}^{opt} = \begin{cases} P_{j,g}^{opt}, & \text{if } P_{j,g}^{opt} \in (0, P_{U,th}]; \\ P_{U,th}, & \text{if } P_{j,g}^{opt} > P_{U,th}; \\ 0, & \text{if } P_{j,g}^{opt} \leqslant 0. \end{cases} \tag{C16}$$

We define a variable $\overline{g} = \frac{\log_2(1+\kappa m_{j,g})(H_{j,g}-H_{j,s})}{\ln 2}$, and prove the equations easily as follow:

$$\frac{\partial P_{j,g}^{opt}}{\partial \overline{g}} > 0, \tag{C17}$$

$$P_{j,g}^{opt} > 0|_{\log_2(1+\kappa m_{j,g})(H_{j,g}-H_{j,s}) > \sigma_n \tau \ln 2}. \tag{C18}$$

The $m_{j,g}$ is a constant, with the increasing of the $\log_2(1+\kappa m_{j,g})(H_{j,g}-H_{j,s})$, the $P_{j,g}^{opt}$ also increases. The $H_{j,g}-H_{j,s}$ is security gain of communication link, and the $\log_2(1+\kappa m_{j,g})$ is gain of fountain package. The higher the gain of security and fountain package are, the larger the optimal power $P_{j,g}^{opt}$ is. The U_j cannot be selected, if the $P_{j,g}^{opt}$ is less than zero. Therefore, the $\log_2(1+\kappa m_{j,g})(H_{j,g}-H_{j,s})$ must be higher than the threshold value ($\sigma_n \tau \ln 2$). We can draw a conclusion about the threshold value that if the user ship has more missing fountain packets, the threshold value is lower. The user ship with lower threshold value is more likely to be selected, which is also an important criterion to select optimal user ship.

Appendix D Performance Evaluation

The relay node that maximizes the secrecy capacity of AF relaying transmission is viewed as the optimal relay. The carrier frequency of relay network and D2D network are set as 2.5 GHz and 1.89 GHz. The bandwidth B is 10 MHz. The AWGN power is defined as $\sigma_n = BN_0$, where N_0 is the AWGN spectral efficiency, and $N_0 = -174dBm/Hz$. The maritime satellite is assumed to be on the geosynchronous orbit of $36,000km$, and the parameters of the satellite is defined referring to [3]. We set $P_{T,th} = 49dBm$, $P_{R,th} = 43dBm$ and $P_{U,th} = 41dBm$. The path loss exponent η of maritime channel is defined referring to [4], and the path loss exponent of satellite channel is 2. The number of directive antennas equipped in HBS N^{ant} is set to 3. We emulate transmission 10^4 times. Moreover, the total number of data packets denoted as K, which is assumed to be 128. The fountain code selects LT codes [5]. The packet error rate (PER) can be defined as [6]:

$$FER_n(\boldsymbol{\gamma}) = \begin{cases} 1, & \text{if } 0 < \boldsymbol{\gamma} < \boldsymbol{\gamma}_{pn}; \\ a_n exp(-g_n \boldsymbol{\gamma}), & \text{if } \boldsymbol{\gamma} \geqslant \boldsymbol{\gamma}_{pn}. \end{cases} \tag{D1}$$

where $\boldsymbol{\gamma}$ is received SNR and n denotes mode index. By referring to the fitting parameters in [7], the fitting parameters are listed as follows:

$$\begin{aligned} a_n &= 50.1222, \\ g_n &= 0.6644, \\ \boldsymbol{\gamma}_{pn} &= 7.7021. \end{aligned} \tag{D2}$$

In addition, we define four performance indexes to evaluate the performance of the proposed scheme.

Appendix D.1 Intercept probability for ES

we define the M_{eve} as the number of data packets which are successfully decoded when all transmissions are complete. If M_{eve} equals to K, the eavesdroppers successfully intercept all messages. Otherwise, the intercept is failed. Hence, the intercept probability is the ratio between the number of successful eavesdropping times and the total number of transmissions.

Appendix D.2 Recovering proportion for ES

this index is defined as the mean value of $M_{eavesdropper} \setminus K$ when the preset value numbers of transmission time are reached.

Appendix D.3 Transmission efficiency of HBS

this index is defined as the mean value of $K(1+\boldsymbol{\sigma})N^{ant} \setminus D_{HBS}$ when the preset value numbers of transmission time are reached, in which D_{HBS} denotes the number of fountain packets in average, in one relay phase. The $\boldsymbol{\sigma}$ is decoding overhead.

Appendix D.4 Secrecy capacity for user ship

this index is defined as the mean value of secrecy capacity in one transport process.

References

1 Papandriopoulos J, Evans J S. SCALE: A Low-Complexity Distributed Protocol for Spectrum Balancing in Multiuser DSL Networks. IEEE Transactions on Information Theory, 2009, 55:3711-3724

2 B R Marks, G P Wright. A general inner approximation algorithm for nonconvex mathematical programs. Operations Research, 1978, 26:681-683

3 D Christopoulos, S Chatzinotas, B Ottersten. Ulticast Multigroup Precoding and User Scheduling for Frame-Based Satellite Communications. IEEE Transactions on Wireless Communications, 2015, 146:4695-4707

4 Li jun Z, Hong Guang W, Rui Z et al. Radio wave propagation characteristics measurement and modeling over the sea. In: Proceedings of 2014 URSI General Assembly and Scientific Symposium (URSI GASS), Beijing, 2014.1-4

5 M Luby. LT Codes. In: Proceedings of The 43rd Annual IEEE Symposium on Foundations of Computer Science, Vancouver, BC, 2002. 271-282

6 Liu Q, Zhou S, Giannakis G B. Queuing with adaptive modulation and coding over wireless links: cross-Layer analysis and design. IEEE Transactions on Wireless Communications, 2005, 4:1142-1153

7 Qinghe D, Ying X, Wanyu L, et al. Security Enhancement for Multicast over Internet of Things by Dynamically Constructed Fountain Codes. Wireless Communications and Mobile Computing, 2018, 2018:1-11