SCIENCE CHINA
Information Sciences

• LETTER •

April 2020, Vol. 63 149303:1–149303:3
https://doi.org/10.1007/s11432-018-9876-6

Secure routing and transmission scheme for space-ocean broadband wireless network

Yuzhou FU[1,3], Chuan-Ao 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*

Received 29 December 2018/Revised 19 February 2019/Accepted 23 April 2019/Published online 24 September 2019

Citation Fu Y Z, Jiang C-A, Qin Y R, et al. Secure routing and transmission scheme for space-ocean broadband wireless network. Sci China Inf Sci, 2020, 63(4): 149303, https://doi.org/10.1007/s11432-018-9876-6

Dear editor,

Increase in maritime activities with exclusive economic zones leads to an increase in demands for information security in maritime communication networks. In maritime, all ships must install an automatic identification system (AIS) to ensure navigational safety, including eavesdropper ships (ESs). Therefore, the navigation information of the ships is easy for an operator to obtain via the AIS. In the study of [1], the author proposed a new AIS-based ad hoc network model and an AIS-based ad hoc routing protocol for ship-to-ship and ship-to-shore data communications. To enhance the secrecy of wireless communications, physical layer security (PLS) uses the characteristics of wireless channels [2]. A relay-aided PLS is suited for maritime networks. In [3], fountain code and relay-aided PLS techniques were found to be suitable for wireless networks. In [4], the PLS in opportunistic relay selection networks over independent and identically distributed Rayleigh fading channels was studied.

We propose a location-information-assisted secure transmission scheme in the space-ocean integrated network. The maritime network ensures security by means of routing and the satellite provides maritime broadcast services. However, with the aid of navigation information, we can use routing to avoid eavesdroppers. If interception by an eavesdropper is unavoidable, the proposed scheme can also limit the received information of eavesdroppers by using power optimization, which reduces the amount of the received encoded packets of eavesdroppers. In addition to power optimization, using multiple transmission links, the scheme can also split the raw data into pieces and transmit it. If the eavesdropper is not able to intercept all the transmission links, it cannot receive enough encoded packets to recover the message.

Model. In this study, we consider a multi-user maritime communication scenario. If two ships are close enough, then device-to-device (D2D) communications are enabled. Under the proposed scenario, one high-tower base station (HBS), multiple relay ships (RSs), and a satellite (SAT) cooperatively provide the services for maritime user ships. In particular, the SAT provides broadcast services for user ships. However, the eavesdroppers can also receive fountain packets from the SAT. Thus, the network control center (NCC) executes the transmission scheme and manages the control signals. The NCC can obtain the AIS information and decoding situation of the user ship from the AIS control center. According to the transmission scheme, the NCC selects a secure relay link to transmit signals and plans the routing of D2D communication. Afterward, the control signal of the D2D network and the AIS information can also broadcast together via SAT. More details of the system model are referenced in Appendix A.

Algorithm development. The transmission scheme can be divided into two phases: the re-

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

laying phase and the D2D phase. In the model, the relay links of HBS-RS are secured, and these communication links therefore do not need to consider security capacity. Moreover, the optimization problem of the relay is divided into two subproblems (P1 and P2). The two subproblems are solved as iterations between each other until the result of the optimization problem converges. The relay selection and power allocation are related to the communication capacity and the security capacity of the relay link. The relay network is the solution to the optimization problem below:

$$\mathrm{P1}: \max_{P_{T,i}} \sum_{i=1}^{I}\sum_{n=1}^{N} x_{i,n} R_{T,i} \tag{1}$$

$$\text{s.t. } C1: \sum_{i=1}^{I} x_{i,n} p_{T,i} \leqslant P_{T,\mathrm{th}},\ \forall n,$$

$$C2: \sum_{n=1}^{N} x_{i,n}\left(p_{T,i} \geqslant \frac{\gamma_{\mathrm{th}}^{TR}(\sigma_n + \sigma_{n_{S,i}})}{H_{T,i}}\right),\ \forall i,$$

$$C3: P_{T,R} \geqslant 0,$$

$$\mathrm{P2}: \max_{X_{i,n},P_{i,n}} \sum_{i=1}^{I}\sum_{n=1}^{N} x_{i,n} C_{i,n} \tag{2}$$

$$\text{s.t. } C4: p_{i,n} \leqslant P_{R,\mathrm{th}},\ \forall i,n,$$

$$C5: \sum_{i=1}^{I} x_{i,n} \leqslant 1,\ \forall n,$$

$$C6: x_{i,n}(C_{i,n} \geqslant C_{\mathrm{th}}^{U})\ \forall i,n,$$

$$C7: x_{i,n}(C_{i,s} \leqslant C_{\mathrm{th}}^{E})\ \forall i,n,$$

$$C8: C_{\mathrm{th}}^{U} > C_{\mathrm{th}}^{E},$$

$$C9: P_{R,U_N} \geqslant 0,$$

$$C10: x_{i,n} \in \{0,1\}\ \forall i,n.$$

In addition, to assess the security standardization of the relay link, we define a standard. According to this standard of security, if the relay link cannot ensure security, we will transmit only one part of the fountain packets or refuse to transmit fountain packet to the user-ship. In this way, the eavesdroppers cannot receive sufficient fountain packets to recover the original data. Thus, the user ship can replenish the fountain packets with the D2D optimization problem (P3):

$$\mathrm{P3}: \max_{P_{j,g}} F_{j,g} \tag{3}$$

$$F_{j,g} = C_{j,g} - \frac{\tau}{\log_2(1+\kappa m_{j,g})} p_{j,g}, \tag{4}$$

$$\text{optional user ship: } U_j = \max_{j\in U} F_{j,g}. \tag{5}$$

The definitions of the notations in the optimization problems are presented in Appendix B. After obtaining the solution to the optimization problems, the optimization problems of the relay phase are solved as iterations between the subproblems until all of the results of the subproblems converge. The solution process of the optimization problems can be seen in Appendix C. The detailed iterative procedure of the relay phase is shown in Algorithm 1.

Algorithm 1

while User matrix U is not empty **do**
  Select N user ships from U;
  Set $U = U - U^{\mathrm{sel}}$ and $x_{i,n} = 0,\ \forall i,n$;
  while $x_{i,n}$, $p_{i,n}$, $p_{T,i}$ converge, $\forall i,n$ **do**
    for $n = 1$ to N **do**
      Update $x_{i,n}$;
    end for
    while $p_{i,n}$, $p_{T,i}$ converge, $\forall i,n$ **do**
      for $i = 1$ to I **do**
        for $n = 1$ to N **do**
          Update $P_{T,i}$ and $P_{i,n}$;
        end for
      end for
    end while
  end while
  Update $C_{i,j}$;
  if $C_{i,j} \geqslant C_{\mathrm{th}}$ **then**
    $U^{\mathrm{not}} = U^{\mathrm{not}} + U_j$;
  end if
end while

In Algorithm 1, U^{sel} denotes the user ships selected from U in one relay transmission phase; C_{th} shows the security standardization of the relay link; U^{not} denotes the user ships that cannot receive sufficient fountain packets in the relay phase. Here, according to the D2D optimization problem (P3), users (U^{not}) can replenish fountain packets.

Performance evaluation. In this section, the simulation setup and simulation results are demonstrated for evaluating the proposed scheme. We choose the AFbORS algorithm in [5] as the compared scheme. More details of simulation parameters are referenced in Appendix D. The number of user ships is also a variable that ranges from 20 to 80. S denotes the number of ESs.

In Figure 1, we define a variable (D_{SAT}) to denote the number of fountain code packets by satellite broadcast. Figure 1(a) shows that the intercept probability of the proposed scheme decreases about 77% compared to that of the AFbORS scheme. In addition, better communication security performance is achieved when the number of users increases. From Figure 1(b), the recovering proportion of the proposed scheme is lower than that of the baseline scheme. If the satellite only broadcasts a small number of fountain packets, the recovering proportion for eavesdroppers is less than 0.07. Figure 1(c) shows that the proposed scheme has a higher transmission efficiency

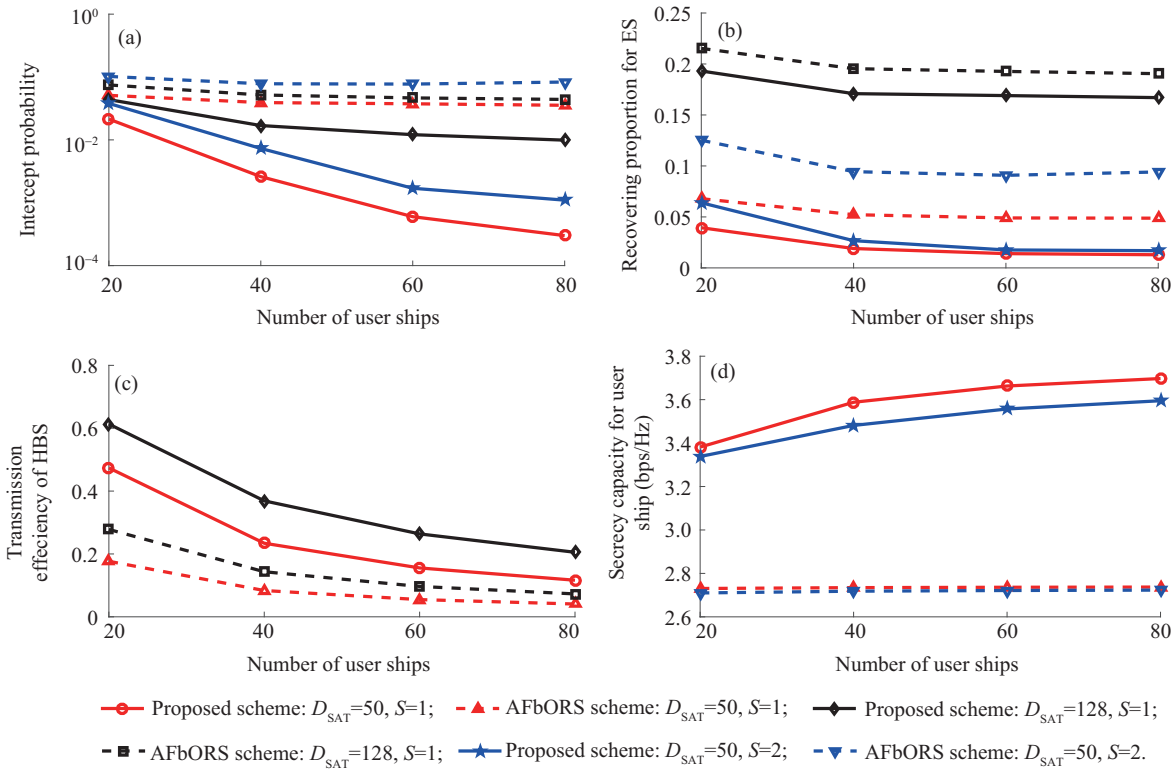

Figure 1 (Color online) (a) Intercept probability comparison between the proposed scheme and baseline schemes; (b) comparison of recovering proportion for eavesdroppers between the proposed scheme and baseline schemes; (c) transmission efficiency comparison between the proposed scheme and baseline schemes; (d) comparison of secrecy capacity for user ships between the proposed scheme and baseline schemes.

than other schemes. In the proposed scheme, the user can effectively choose to route to acquire sufficient fountain coded packets by the location information from the AIS system, which effectively improves transmission efficiency of the HBS. In Figure 1(d), the secrecy capacity of the proposed scheme achieves approximately 32% improvement compared to the baseline scheme.

Conclusion. We propose a scheme that presents a maritime wireless network transmission scheme in the integrated maritime-satellite networks. The scheme dynamically uses routing to avoid eavesdropping. According to the location information from AIS, to ensure that the eavesdropper cannot receive enough fountain packets to recover the original data, the transmitter selects multiple communication links and then optimizes the transmitting power. The simulation results show that the proposed scheme achieves better performance in both security and efficiency.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 91538203, 61871257), New Strategic Industries Development Projects of Shenzhen City (Grant No. JCYJ2017-0307145820484), Joint Research Foundation of the General Armaments Department and the Ministry of Education (Grant No. 6141A02033322), and Beijing Innovation Center for Future Chips, Tsinghua University.

Supporting information Appendixes A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Mun S M, Son J Y, Jo W R, et al. An implementation of AIS-based ad hoc routing (AAR) protocol for maritime data communication networks. In: Proceedings of the 8th International Conference on Natural Computation, Chongqing, 2012. 1007–1010
2 Hong Y W P, Lan P C, Kuo C C J. Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches. IEEE Signal Process Mag, 2013, 30: 29–40
3 Sun L, Ren P Y, Du Q H, et al. Fountain-coding aided strategy for secure cooperative transmission in industrial wireless sensor networks. IEEE Trans Ind Inf, 2016, 12: 291–300
4 Zhong B, Wu M G, Li T, et al. Physical layer security via maximal ratio combining and relay selection over Rayleigh fading channels. Sci China Inf Sci, 2016, 59: 062305
5 Zou Y L, Wang X B, Shen W M. Optimal relay selection for physical-layer security in cooperative wireless networks. IEEE J Sel Areas Commun, 2013, 31: 2099–2111