An overview of UAV communication technologies

Anyi She

College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, China

*Corresponding author: b21012318@njupt.edu.cn

Abstract. Recently, Unmanned Aerial Vehicle (UAV) as a flexible platform has received extensive attention from scholars at home and abroad. Compared with terrestrial communication, UAV has the unique advantages of high flexibility, wide coverage and no influence of terrain. In this paper, two aspects of UAV outage probability and covert communication are discussed and two system models are established, respectively. In the first aspect, the outage probability expression is calculated using the output SNR, and then the relay drone's best position is solved in order to minimum outage probability. In the second aspect, in the case of the presence of listener and eavesdropper in the system, the detection performance of the listener is discussed, and then the secure concealment rate of the system is analyzed.

Keywords: UAV; SNR; outage probability; detection performance; secure concealment rate.

1. Introduction

Nowadays, the proliferation of IoT has caused a spike in the usage of mobile data over 5G wireless networks. Recent studies suggest that by 2028, global mobile traffic will reach 1 ZB, which will put a huge capacity demand on existing infrastructure communication facilities, as well as increase the investment and operational costs for telecom operators. At the same time, the deployment of terrestrial infrastructures is economically unfeasible and hazardous in unexpected or emergency situations due to high operational expenses and a complex and volatile environment. UAV communications, as an important complement to traditional communication methods, are able to perform in harsh environments, and the high altitude advantage of UAVs over traditional terrestrial communication systems offers the possibility of establishing line-of-sight (LoS) transmission links, which will significantly improve wireless communication performance [1].

But using drones also presents new difficulties for communications security. The open nature of the wireless channel makes drones susceptible to eavesdropping and attacks by malicious users when communicating with ground nodes [2]. Specifically, on the one hand, transmission over a wireless LoS channel may be intercepted by some unwanted receivers, thus risking information leakage. On the other hand, UAV wireless transceivers are susceptible to malicious jamming strikes. The security paradigm for protecting the confidentiality of wireless communications in existing communication networks remains unclear. How to secure wireless data transmission is one of the important issues facing any wireless communication system.

Under the guidance of the basic theoretical research on UAV communication, the research on UAV communication is slowly unfolding. In the literature [3], multiple UAVs are considered for inter communication, which focuses on the trajectory control of UAVs. In the literature [4], in order to improve the physical layer security of terrestrial communication networks, a drone-based relaying scheme is proposed. In the literature [5], noise is used as a mask signal to together maximize the transmission power of the UAV and the altitude at which it is located to improve the communication performance in light of the circumstance that the channel state information (CSI), the covertness constraint and the maximum transmission power constraint is known.

In this paper, the author presents an overview of UAV communication technologies based on two aspects: outage probability and covert communication, and based on the current state of research to make a deeper derivation.

2. Analysis based on outage probability

2.1. System model

The UAV relay transmission system, as seen in Fig. 1, comprises an observation UAV (O), a relay UAV (R), and a base station (S), supposing that every node is configured with just one antenna. The observation UAV, the relay UAV, and the base station can communicate with each other, and every UAV has a radio transmitter and transceiver installed. The base station position remains static, while the observation drone scans a circular region. The collected information is transmitted in real time to the base station via the relay drone. d shows the separation between the base station and the relay drone, D shows the separation between the observation drone and the base station, and r denotes the radius of the circular region for observation.

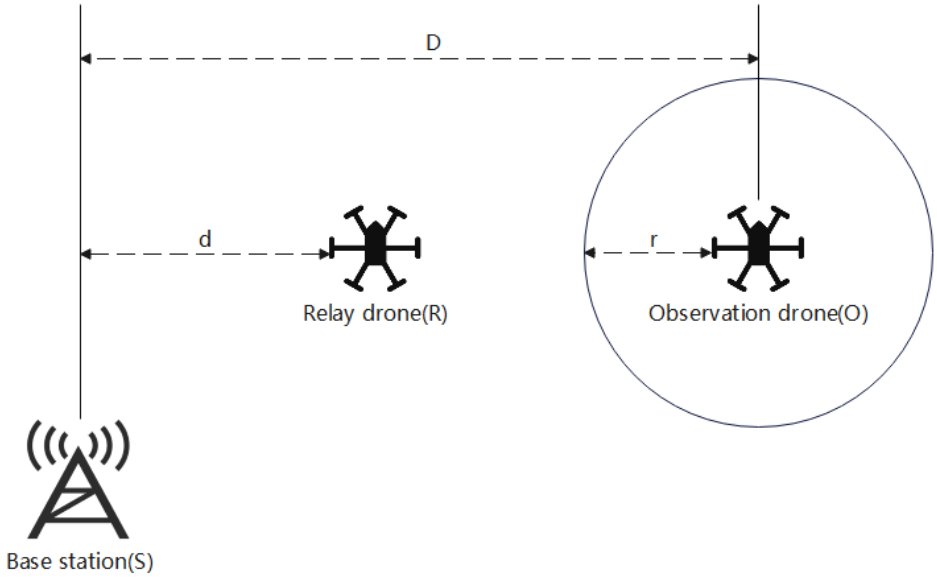


Fig. 1 Drone relay transmission system

2.1.1. Channel model

When modeling S- R and R- O links, in addition to considering wireless channel fading, the effects of practical parameters such as radio wave propagation loss are also considered. One way to represent the channel model is as:

$$F_i = L_i g_i (i = SR, RO) \tag{1}$$

In Eq. (1), F_i denotes the channel response of S-R link or R-O link, g_i denotes the small-scale fading of the channel, and L_i denotes the pass loss of the channel, whose expression is:

$$L_i = \frac{C\sqrt{G_t G_r}}{4\pi f d} (i = SR, RO) \tag{2}$$

In Eq. (2), C is the velocity that light travels, f is the frequency of operation, d is the length for transmission, G_t and G_r denote the antenna gain of the transmitter and receiver, respectively. Assuming that the S- R and R- O channel fading $|g_i|^2$ obeys the Rayleigh distribution, whose Probability Density Function (PDF) can be given as:

$$f_{|g_i|^2}(x) = \frac{1}{2p_{\gamma_i,d}\bar{\gamma}_i} \exp\left(-\frac{x}{2p_{\gamma_i,d}\bar{\gamma}_i}\right), x \geq 0 \tag{3}$$

In Eq. (3), $p_{\gamma_i,d}$ denotes the average power in a particular time slot, and $\overline{\gamma_i}$ is the mean signal-to-noise ratio (SNR) of the output in a particular time slot.

2.1.2. Signal model

The entire information transfer process is split into two phases. Phase one involves S sending out a signal satisfying $E[|x_S(t)|^2]=1$ to the relay drone R. The received signal of R is:

$$y_R(t)=\sqrt{P_R}\,g_{SR}x_S(t)+n_0(t) \tag{4}$$

In Eq. (4), P_R denotes the average power of the relay drone R, and $n_0(t)$ denotes the Additive White Gaussian Noise (AWGN) with mean 0 and variance σ^2. The output SNR at R can be obtained using Eq. (4) as:

$$\gamma_R=P_R\|g_{SR}\|_F^2/\sigma^2=\overline{\gamma_{SR}}\|g_{SR}\|_F^2 \tag{5}$$

In Eq. (5), $\overline{\gamma_{SR}}$ is the average SNR of the S-R channel, which is expressed as:

$$\overline{\gamma_{SR}}=P_R/\sigma^2=P_tL_{SR}^2/\sigma^2=\left(\frac{C}{4\pi fd}\right)^2\frac{G_tG_rP_s}{\sigma^2} \tag{6}$$

In Eq. (6), P_s is the power of source node S that is transmitted.

The relay drone R transmits the recoded signal $x_R(t)$ to the observation drone O in the second phase after first decoding the signal $y_R(t)$ it got. The signal received by O from the relay drone R can be expressed as:

$$y_O(t)=\sqrt{P_O}\,g_{RO}x_R(t)+n_0(t) \tag{7}$$

In Eq. (7), P_O denotes the average power of the observation drone O. Similar to the first stage, the output SNR at O can be expressed as:

$$\gamma_O=P_O\|g_{RO}\|_F^2/\sigma^2=\overline{\gamma_{RO}}\|g_{RO}\|_F^2 \tag{8}$$

In Eq. (8), $\overline{\gamma_{RO}}$ denotes the average SNR of the observation drone. It can be expressed as:

$$\overline{\gamma_{RO}}=\left(\frac{C}{4\pi f(D-d-r)}\right)^2\frac{G_tG_rP_s}{\sigma^2}(1-A) \tag{9}$$

In Eq. (9), A denotes the attenuation rate which is the presence of obstacles makes the transmission signal lossy [6].

In summary, the output SNR of the whole system is

$$\gamma=\min(\gamma_R,\gamma_O) \tag{10}$$

2.2. Outage probability

Outage probability (OP) is an important measure of the quality of service (QoS) for wireless communications. Typically, it is described as the likelihood that the signal output SNR will go beneath a specific threshold value Λ, which is:

$$P_{out}=Pr\{\gamma\leqslant\Lambda\}=F_\gamma(\Lambda) \tag{11}$$

According to Eq. (10) and Eq. (11), OP can be further expressed as:

$$\begin{aligned} P_{out} &= Pr\{\gamma \leqslant \Lambda\} \\ &= Pr\{\min(\gamma_R, \gamma_O) \leqslant \Lambda\} \\ &= 1 - Pr\{\min(\gamma_R, \gamma_O) > \Lambda\} \\ &= 1 - Pr\{\gamma_R > \Lambda\} Pr\{\gamma_O > \Lambda\} \end{aligned} \tag{12}$$

From Eq. (3), the PDF of γ_i is given as:

$$f_{\gamma_i}(x) = \frac{1}{=}{\gamma_i} \exp\left(-\frac{x}{=}{\gamma_i}\right), x > 0 \tag{13}$$

Further from Eq. (13), the probability distribution function of γ_i is given as:

$$F_{\gamma_i}(\Lambda) = \int_0^{\Lambda} f_{\gamma_i}(x)dx = 1 - \exp\left(-\frac{\Lambda}{=}{\gamma_i}\right) \tag{14}$$

Thus, $Pr\{\gamma_i > \Lambda\}$ can be express as:

$$Pr\{\gamma_i > \Lambda\} = 1 - F_{\gamma_i}(\Lambda) = \exp\left(-\frac{\Lambda}{=}{\gamma_i}\right) \tag{15}$$

Substituting Eq. (15) into Eq. (12) results in:

$$P_{out} = 1 - \exp\left(-\frac{\Lambda}{=}{\gamma_{SR}}\right) \exp\left(-\frac{\Lambda}{=}{\gamma_{RO}}\right) \tag{16}$$

2.3. Optimal relay drone position selection

To ensure that the relay drone is positioned optimally, it boils down to an optimization problem. The optimal position of the drone is obtained by getting the minimum value of P_{out}. Substituting Eq. (6) and Eq. (9) into Eq. (16) and making its derivative with respect to d equal to 0, the relationship between D, d, r can be obtained, which is the optimal position of the relay drone. In practice, a reasonable setting of D and r values in order to determine the optimal position of the relay drone.

$$d = \frac{D + r}{2 - A} \tag{17}$$

3. Analysis based on covert communication

3.1. System model

The UAV system for clandestine communication, as seen in Fig. 2, has a UAV S providing services to a legitimate user U in the ground coverage area. A listener L exists to detect the communication between UAV S and user U, and an eavesdropper E attempts to steal the transmission signal between UAV S and user U. The signal transmission needs to resist both the threat of information eavesdropping by the eavesdropper E and listening by the listener L in order to realize the wireless covert transmission of information. Assuming that L and E are independent of each other, and user U, listener L and eavesdropper E are equipped with a single antenna.

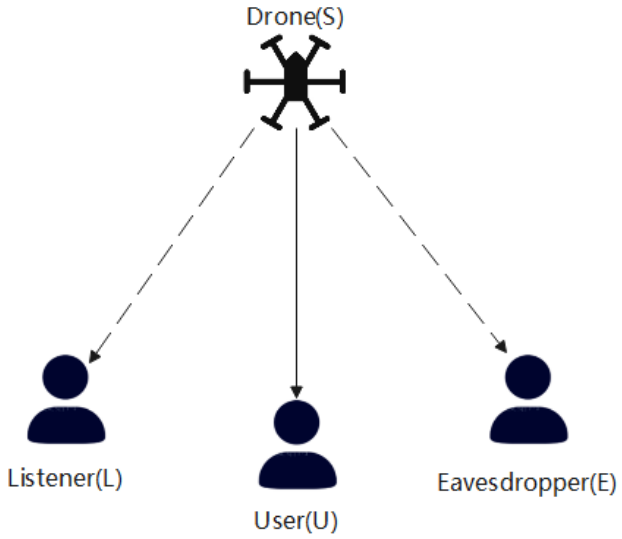


Fig. 2 Drone clandestine communication system

To degrade the performance of E and at the same time confuse the detection of L for better communication signaling, an interfering signal is added to the message received by the user U. A communication time slot can be described as a temporal interval during which a message is transmitted from S to U. Each time slot contains k symbol periods, assuming that k is sufficiently large, which is $k \gg 1$. In each communication time slot, the channel coefficients are kept constant, and independently varied in another communication time slot fading the wireless channel [7].

The valid signal sent by the UAV S to the legitimate user U is x_s and the interfering signal sandwiched between the signals is x_n, which satisfy $E\left[|x_s(i)|^2\right]=1$ and $E\left[|x_n(i)|^2\right]=1$ respectively. Then the signal received by the legitimate user U can be expressed as:

$$y_U(i)=\sqrt{P_s}\,g_{SU}x_s(i)+\sqrt{P_n}\,g_{SU}x_n(i)+n_0(i) \tag{18}$$

In Eq. (18), P_s denotes the power allocated by the UAV S to the valid signal x_s, and $g_{Si}(i=L,U,E)$ denotes the channel fading vector, which can be expressed as $g_{Si}=\frac{h_{Si}}{\sqrt{V(d_i)}}$, where h_{Si} is a random vector obeying a Rice distribution and $V(d_i)$ is the path loss [8]. P_n denotes the power assigned to the interfering signal x_n, whose probability obeys a uniform distribution between $[0,P_n^{\max}]$, where $P_n^{\max}$ is the maximum power assigned to the interfering signal x_n, then its PDF is:

$$f_{P_n}(x)=\begin{cases}\frac{1}{P_n^{\max}}, 0\leqslant x\leqslant P_n^{\max}\\ 0, the\ rest\end{cases} \tag{19}$$

Similarly, the signal that the eavesdropper E got is:

$$y_E(i)=\sqrt{P_s}\,g_{SE}x_s(i)+\sqrt{P_n}\,g_{SE}x_n(i)+n_0(i) \tag{20}$$

In order to determine whether the drone S is transmitting information, the detection by the listener L requires the following two assumptions:

$$y_L(i)=\begin{cases}\sqrt{P_n}\,g_{SL}x_n(i)+n_0(i), H_0\\ \sqrt{P_s}\,g_{SL}x_s(i)+\sqrt{P_n}\,g_{SL}x_n(i)+n_0(i), H_1\end{cases} \tag{21}$$

In Eq. (21), H_0 means that L receives only noise and H_1 means that L observes a superposition of the valid signal and noise. Assume that L uses the energy detection method, which is a non-coherent blind detection method based on signal energy. Assuming that the test statistic is the average received power within each block, the judgment criterion for L can be expressed as [9]:

$$\Gamma = \begin{cases} \frac{1}{k}\sum_{i=1}^{k}|y_L(i)|^2 < \nu, \lambda_0 \\ \frac{1}{k}\sum_{i=1}^{k}|y_L(i)|^2 > \nu, \lambda_1 \end{cases} \tag{22}$$

In Eq. (22), ν denotes the judgment threshold set by L, and λ_0 and λ_1 denote the judgment on hypotheses H_0 and H_1 respectively. λ_0 denotes that L judges that S sends a valid signal, and λ_1 denotes that L judges that S does not send a valid signal. Thus, the false alarm rate α and the miss alarm rate β of detection judgment can be expressed as:

$$\begin{aligned} \alpha &= P(\lambda_1|H_0) = P(\Gamma > \nu|H_0) \\ \beta &= P(\lambda_0|H_1) = P(\Gamma < \nu|H_1) \end{aligned} \tag{23}$$

Assume that $P(H_0) = P(H_1) = 0.5$. Let $\theta = \alpha + \beta$. Obviously $0 \leqslant \theta \leqslant 1$, and the smaller θ is, the lower probability of detection error and the higher the detection performance of L is. When $\theta = 0$, L can detect the communication accurately; when $\theta = 1$, L's detection is completely random and unconvincing.

3.2. Performance Analysis of Listener Detection

Assume that the signal samples collected by L tend to infinity, which is $k \to \infty$. The average power of L under the assumption H_0 is [10]:

$$P_L(H_0) = \lim_{k\to\infty}\frac{1}{k}\sum_{i=1}^{k}|y_L(i)|^2 = \lim_{k\to\infty}\left(P_n|g_{SL}|^2 + \sigma^2\right)\frac{\chi_{2k}^2}{k} \tag{24}$$

In Eq. (24), χ_{2k}^2 is a random variable that obeys a chi-square distribution and has 2k degrees of freedom. According to the law of large numbers, when $k \to \infty$, $\frac{\chi_{2k}^2}{k}$ converges to 1. Thus, Eq. (24) can be changed to:

$$P_L(H_0) = P_n|g_{SL}|^2 + \sigma^2 \tag{25}$$

Therefore, when P_n obeys a uniform distribution between $[0, P_n^{\max}]$, the false alarm probability α can be expressed as:

$$\begin{aligned} \alpha &= P(\Gamma > \nu|H_0) = P\left(P_n|g_{SL}|^2 + \sigma^2 \geqslant \nu\right) = P\left(P_n \geqslant \frac{\nu - \sigma^2}{|g_{SL}|^2}\right) \\ &= \begin{cases} 1, \nu \leqslant \sigma^2 \\ 1 - \frac{\nu - \sigma^2}{|g_{SL}|^2 P_n^{\max}}, \sigma^2 < \nu < \tau_1 \\ 0, \nu \geqslant \tau_1 \end{cases} \end{aligned} \tag{26}$$

In Eq. (26), $\tau_1 = |g_{SL}|^2 P_n^{\max} + \sigma^2$. Similarly, the missed detection probability β can be expressed as:

$$\beta = P(\Gamma < \nu | H_1) = P\left((P_s + P_n)\left|g_{SL}\right|^2 + \sigma^2 \leqslant \nu\right) = P\left(P_n \leqslant \frac{\nu - \sigma^2}{\left|g_{SL}\right|^2} - P_s\right)$$

$$= \begin{cases} 0, \ \nu \leqslant \tau_2 \\ \frac{\nu - \tau_2}{\left|g_{SL}\right|^2 P_n^{\max}}, \tau_2 < \nu < \tau_1 + \tau_2 - \sigma^2 \\ 1, \nu \geqslant \tau_1 + \tau_2 - \sigma^2 \end{cases} \tag{27}$$

In Eq. (27), $\tau_2 = \left|g_{SL}\right|^2 P_s + \sigma^2$.

The listener L can set the ideal cutoff point ν to reduce the likelihood of its detection mistake. However, since the sizes of τ_1 and τ_2 are unknown, the optimal threshold ν needs to be discussed in classification, which ultimately results in the expression for the detection error probability θ as:

$$\theta = \begin{cases} 1, \nu \leqslant \sigma^2 \ or \ \nu \geqslant \tau_1 + \tau_2 - \sigma^2 \\ 1 - \frac{\nu - \sigma^2}{\left|g_{SL}\right|^2 P_n^{\max}}, \sigma^2 < \nu \leqslant \tau_2 \\ 1 - \frac{P_s}{P_n^{\max}}, \tau_2 < \nu \leqslant \tau_1 \\ \frac{\nu - \tau_2}{\left|g_{SL}\right|^2 P_n^{\max}}, \tau_1 < \nu \leqslant \tau_1 + \tau_2 - \sigma^2 \end{cases} \tag{28}$$

The approximate image of θ is:

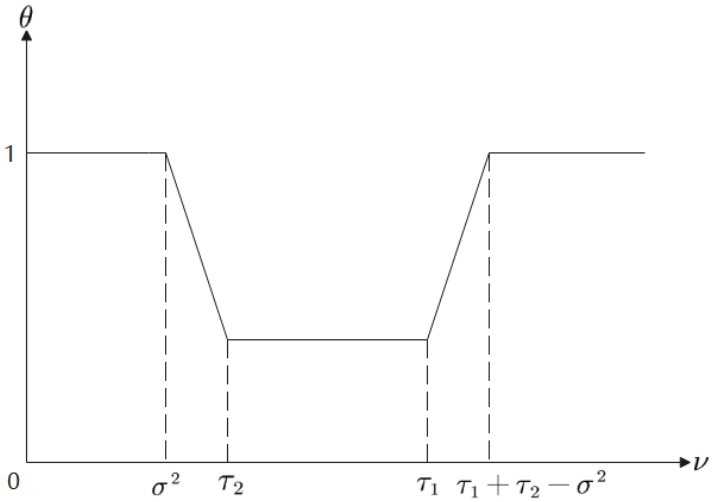


Fig. 3 The approximate image of θ

According to Fig. 3, when $\tau_2 \leqslant \nu \leqslant \tau_1$, the minimum probability of detection error $\theta = 1 - \frac{P_s}{P_n^{\max}}$. Thus, the larger $P_n^{\max}$ is, the larger θ is, which shows that adding interfering noise power increases the probability of detection error, and it has an important impact on the covert communication performance.

3.3. System security concealment rate

Due to the existence of eavesdropper E and listener L, the system needs to sacrifice part of the performance to ensure the security of the message. The safety performance of the whole communication system can be measured by the system achievable safety rate, which can be expressed as:

$$R_s = \log_2(1+\gamma_U) - \log_2(1+\gamma_E) \tag{29}$$

In Eq. (29), γ_U and γ_E are the letter-drying ratios of U and E, respectively. The goal of guaranteeing communication steganography is that, regardless of the strategy employed by L, for any given constant $\varepsilon \in [0,\ 1]$, there is always $\theta \geqslant 1-\varepsilon$. Thus, the security concealment rate of the system can be expressed as:

$$\begin{aligned} &\max\ R_c = P(H_1)R_s \\ &s.t.\ \ \theta \geqslant 1-\varepsilon \\ &\quad P_s + P_n = P \end{aligned} \tag{30}$$

Using the golden section method for simplification, equation (30) can be changed to:

$$\begin{aligned} &\min\ -R_c \\ &s.t.\ \ P_s \leqslant \varepsilon P_n^{\max} \end{aligned} \tag{31}$$

In practice, the optimal allocation ratio of P_s and P_n in the system can be derived by solving Eq. (30) to achieve the maximum system concealment rate.

4. Conclusion

In this paper, the author conducts a preliminary study on UAV communication technology, mainly focusing on the two aspects of outage probability and covert communication, and derive the optimal position determination method for relay UAVs and the maximum safe covert rate of the system, respectively. Although this paper has achieved some preliminary research results, with the advance of UAV communication technology, the problems in the field of UAV communication still need more in-depth research.

References

[1] Jiang, Xu and Chen, Xinying and Tang, Jie and Zhao, Nan and Zhang, Xiu Yin and Niyato, Dusit and Wong, Kai-Kit. Covert Communication in UAV-Assisted Air-Ground Networks[J]. IEEE Wireless Communications, 2021, 28(4): 190-197.

[2] Wyner A D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[3] Fadlullah Z M, Takaishi D, Nishiyama H, et al.A Dynamic Trajectory Control Algorithm for Improving the Communication Throughput and Delay in UAV- aided Networks[J]. IEEE Network,2016,30(1):100-105.

[4] Wang Q, Chen Z, Mei W, et al. Improving physical layer security using UAV-enabled mobile relaying[J]. IEEE Wireless Communications Letters, 2017, 6(3): 310-313.

[5] Yan, Shihao and Hanly, Stephen V. and Collings, Iain B. and Goeckel, Dennis L. Hiding Unmanned Aerial Vehicles for Wireless Transmissions by Covert Communications [C]. ICC 2019-2019 IEEE International Conference on Communications (ICC). IEEE, 2019: 1-6.

[6] Abualhaol I Y, Matalgah M W. Performance analysis of cooperative multi- carrier relay- based UAV networks over generalized fading channels[J].International Journal of Communication Systems,2011,24(8):1049- 1064

[7] Hu J, Yan S, Zhou X, et al. Covert communication achieved by a greedy relay in wireless networks[J]. IEEE Trans. on Wireless Communications, 2018, 17(7): 4766-4779.

[8] DAN Zhenlei, WU Xuewen, OUYANG Jian, etc. Outage performance analysis for multi-UAV relay systems with threshold-based DF protocol [J]. Telecommunications Science, 2020, 36(8): 103-111.

[9] Shahzad K. Relaying via cooperative famming in covert wireless communications[C]. 12th International Conference on Signal Processing and Communication Systems (ICSPCS), 2018: 1-6.

[10] LIN Yuda, JIN Liang, ZHOU You, etc. Performance analysis of covert wireless communication based on beam forming with noise uncertainty [J]. Journal on Communications, 2020, 41(7): 49-58.