covert communication. The research work has important scientific and theoretical significance and practical application value. In terms of scientific theories, the research results fully reveal the mechanism of IRS and MIMO combined for covert communication, explore a novel and effective theoretical method for covert communication. The research results are expected to break the limitations of the traditional airspace-adapted covert communication framework and lead to the formation of a new paradigm of airspace-oriented intelligent and controllable covert communication research. In terms of practical applications, the research results will have a positive impact and promote the popularization of covert communication applications in civil, military and national defence security areas by systematically and thoroughly examining covert communication scenarios and problems of different levels of complexity and formulating practical covert communication technology.

3. Performance of IRS-based MIMO covert communication system

3.1. System Model

Consider the IRS-based MIMO covert communication system shown in Fig.2, where Alice, Bob, and Willie are respectively configured with N_A, N_B, N_W antennas and the IRS equipped with M_I reflector units. Assume the direct and reflected paths of Alice to Bob and Willie exist, and the received signals of Bob and Willie at a certain time can be expressed uniformly as:

$$\mathbf{y}_s[n] = \begin{cases} \mathbf{n}_s[n], & \mathcal{H}_0 \\ (\mathbf{H}_{AS} + \mathbf{H}_{IS}\mathbf{Q}\mathbf{H}_{AI})x[n] + n_s[n], & \mathcal{H}_1 \end{cases} \tag{1}$$

with

$$S \in \{B, W\} \tag{2}$$

where $x[n]$ represents Alice's transmitted signal, $n_B(n_W)$ represents Bob's (Willie's) noise, and $H_{p,q}$ represents the channel matrix between nodes p and q, where $p, q \in \{A, B, W, I\}$, $Q = diag\left(e^{\theta_1}, e^{\theta_2}, \cdots, e^{\theta_{MI}}\right)$ represents the IRS phase shift matrix, where $\theta_i \in (0, 2\pi]$ denotes the phase shift of the reflecting cell. $\mathcal{H}_0$ is the null hypothesis, representing that Alice is not sending a message, while $\mathcal{H}_1$ is the alternative hypothesis, representing that Alice is sending.

3.2. Concealed Detection Issues

Detecting whether Alice is sending a message is a binary hypothesis testing problem, i.e. Willie needs to determine which hypothesis holds between $\mathcal{H}_0$ and $\mathcal{H}_1$. Considering that Willie's listening time is synchronised with Alice's transmission time, Willie uses energy detection and analyses a large number of signal observation samples for binary hypothesis testing. Considering that Alice transmits a Gaussian signal, and Willie's average received power can be expressed as,

$$\hat{P}_W = \begin{cases} \sigma_W^2, & \mathcal{H}_0 \\ P_W + \sigma_W^2, & \mathcal{H}_1 \end{cases} \tag{3}$$

where $P_W \triangleq \operatorname{tr}\left((\mathbf{H}_{AW} + \mathbf{H}_{IW}\mathbf{Q}\mathbf{H}_{AI})\,\mathbf{R}\,(\mathbf{H}_{AW} + \mathbf{H}_{IW}\mathbf{Q}\mathbf{H}_{AI})^H\right)$ denotes the signal power from Alice, $\mathbf{R} \triangleq \mathbb{E}\left[xx^H\right]$ denotes the MIMO signal covariance matrix, and σ_w^2 denotes Willie's noise power.

Willie sets the detection threshold to λ. If $\hat{P}_W \leq \lambda$, we can consider $\mathcal{H}_0$ holds, and vice versa for $\mathcal{H}_1$. Consider $\mathcal{H}_0$ and $\mathcal{H}_1$ with equal prior probabilities, i.e., $\mathbb{P}\{\mathcal{H}_0\} = \mathbb{P}\{\mathcal{H}_1\} = 0.5$, and the detection error probability can be defined as $\xi \triangleq P_{FA} + P_{MD}$ where $P_{FA} \triangleq \mathbb{P}\left\{\hat{P}_W > \lambda | \mathcal{H}_0\right\} = \mathbb{P}\left\{\sigma_w^2 > \lambda\right\}$ and $P_{MD} \triangleq \mathbb{P}\left\{\hat{P}_W \leq \lambda | \mathcal{H}_1\right\} = \mathbb{P}\left\{P_w + \sigma_w^2 \leq \lambda\right\}$ represent the probability of a false alarm and the probability of missed detection, respectively. Considering the uncertainty of the noise at Willie due to the change in the electromagnetic environment, the probability of false alarm and the probability of missed detection are based on bounded uncertainty. Based on the bounded uncertainty model, the probability density function of the noise power σ_w^2 is expressed as,

$$f_{\sigma_w^2}(x) = \begin{cases} \frac{1}{2\ln(\rho)x}, & \frac{\tilde{\sigma}_W^2}{\rho} \leq x < \rho\tilde{\sigma}_W^2 \\ 0, & \text{otherwise} \end{cases} \tag{4}$$

where $\rho \geq 1$ is the noise uncertainty coefficient. It is important to note that this noise uncertainty will have an important impact on the analysis of detection performance and the subsequent optimisation of parameters.

In this study, the concealment rate is used as the core metric. According to (1), the concealment rate Ω can be expressed as,

$$\Omega \triangleq \log_2\left|\mathbf{I}_{N_n} + (\mathbf{H}_{AB} + \mathbf{H}_{IB}\mathbf{Q}\mathbf{H}_{AI})\,\mathbf{R}\,(\mathbf{H}_{AB} + \mathbf{H}_{IB}\mathbf{Q}\mathbf{H}_{AB})^H / \sigma_B^2\right|. \tag{5}$$

This study proposes to jointly design the MIMO signal covariance matrix $\mathbf{R}$ and the IRS phase shift matrix $\mathbf{Q}$. The basic idea is to tailor the design to different levels of CSI knowledge and to make the best use of the already available information.

3.3. Global CSI known

Consider the problem of maximizing the concealed rate when Alice's global CSI is known, which is described as,

$$\max_{\mathbf{R},\mathbf{Q}} \Omega \tag{6}$$

$$\text{s.t. } \operatorname{tr}(\mathbf{R}) \leq P_A, \mathbf{R} \geq 0, \tag{6a}$$

$$\xi \geq 1 - \epsilon, \tag{6b}$$

$$\left|\mathbf{Q}_{i,i}\right| = 1, i = 1, 2, \cdots, M_I. \tag{6c}$$

Constraint (6a) indicates that the Alice transmit power cannot exceed P, (6b) represents the concealed constraint that the detection error probability ξ cannot fall below the threshold $1-\epsilon$, and (6c) represents the unit modulus constraint on the IRS reflection phase shift coefficient.

To solve the above optimization problem, the detection error probability ξ needs to be expressed analytically. Combined with the noise uncertainty model of equation (4), the detection error probability $\xi(\lambda)$ under the given detection threshold λ can be calculated as,

$$\begin{aligned}\xi(\lambda) &= \mathbb{P}\left\{\sigma_W^2 > \lambda\right\} + \mathbb{P}\left\{P_W + \sigma_W^2 < \lambda\right\} \\ &= 1 - \mathbb{P}\left\{\lambda - P_W < \sigma_W^2 < \lambda\right\} \\ &= 1 - \int_{\max\left(\lambda - P_W, \tilde{\sigma}_W^2/P\right)}^{\min\left(\lambda, \rho\tilde{\sigma}_W^2\right)} f_{\sigma_W^2}(x)dx\end{aligned} \tag{7}$$

Consider the robust design and assume that Willie can always use the optimal detection threshold λ^* to obtain the minimum detection error probability $\xi^* = \xi(\lambda)$. We can obtain the closed-form expression of the optimal detection threshold λ^* and the minimum detection error probability ξ^* by taking the derivative of equation (7) to λ. We can observe that ξ^* is a monotone decreasing function of Willie's signal receiving power P_W. Therefore, the hidden constraint (6b) can be transformed into the following constraint on P_W,

$$\begin{aligned}\xi &\geq 1 - \epsilon \Rightarrow P_W \\ &= \mathrm{tr}\left(\left(\mathbf{H}_{AW} + \mathbf{H}_{IW}\mathbf{Q}\mathbf{H}_{AI}\right)\mathbf{R}\left(\mathbf{H}_{AW} + \mathbf{H}_{IW}\mathbf{Q}\mathbf{H}_{AI}\right)^H\right) \\ &\leq \kappa \triangleq \xi^{-1}(1 - \epsilon),\end{aligned} \tag{8}$$

where κ is equal to $(1-\epsilon)$, representing the maximum allowable signal power leaked to Willie.

As the optimization variables $\mathbf{R}$ and $\mathbf{Q}$ present a complex coupling relationship in the objective function (6) and hidden constraint (6b), we can adopt the idea of alternate optimization to design $\mathbf{R}$ and $\mathbf{Q}$. First, fix $\mathbf{Q}$, and we can find that the original problem degenerates into a convex problem about $\mathbf{R}$, and the closed-form solution of the optimal $\mathbf{R}$ can be derived. Then, given $\mathbf{R}$, the optimization problem about $\mathbf{Q}$ is a typical nonconvex problem due to the existence of the constraint (6c) on the unit modulus of the elements in $\mathbf{Q}$. In this case, optimization methods such as maximizing the lower bound of the objective function or using continuous convex approximation can be used to solve the subproblem. The optimal $\mathbf{R}^*$ and $\mathbf{Q}^*$can be obtained through the iterative solution of the above two subproblems.

Fig. 3-5 show the results of secrecy outage probability with federate learning, where the transmit power P varies from 0dB to 20dB. In particular, Fig. 3 is associated with one IRS unit, where the detailed numerical data in given in Table 1; Fig. 4 is associated with two IRS units, where the detailed numerical data in given in Table 2; Fig. 5 is associated with three IRS units, where the detailed numerical data in given in Table 3. From the three figures and tables, one can see that proposed scheme is better than the zero-forcing (ZF) and maximal ratio combing (MRC) schemes, as it can efficiently exploit the spatio-temporal resources provided by multiple antennas and IRS units, through the federated learning.

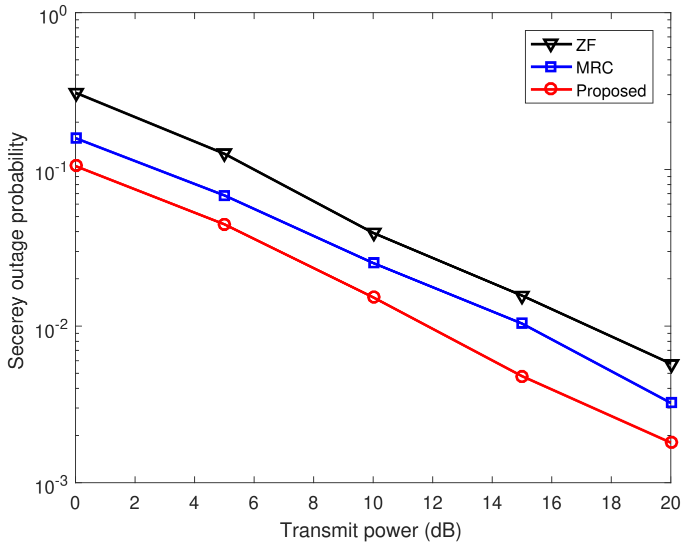

Figure 3. SOP of the considered system with $M_I = 1$.

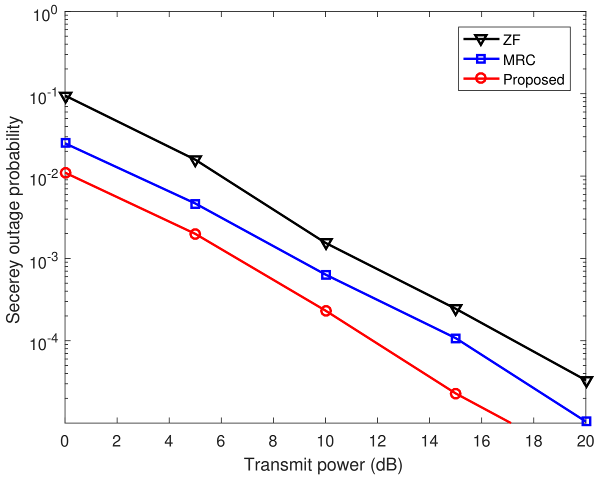

Figure 4. SOP of the considered system with $M_I = 2$.

4. Conclusions

To reveal the system design and optimization on the convert communication with the deep incorporation of IRS, this paper firstly gave a comprehensive literature

Table 1 Data of SOP with $M_I = 1$.

P (dB)	0	5	10	15	20
ZF	3.08e-01	1.26e-01	3.93e-02	1.56e-02	5.76e-03
MRC	1.58e-01	6.82e-02	2.52e-02	1.04e-02	3.23e-03
Proposed	1.05e-01	4.46e-02	1.53e-02	4.79e-03	1.80e-03

Table 2 Data of SOP with $M_I = 2$.

P (dB)	0	5	10	15	20
ZF	9.51e-02	1.58e-02	1.55e-03	2.45e-04	3.32e-05
MRC	2.50e-02	4.65e-03	6.37e-04	1.08e-04	1.04e-05
Proposed	1.10e-02	1.99e-03	2.33e-04	2.29e-05	3.25e-06

Table 3 Data of SOP with $M_I = 3$.

P (dB)	0	5	10	15	20
ZF	2.93e-02	1.99e-03	6.08e-05	3.83e-06	1.91e-07
MRC	3.95e-03	3.17e-04	1.61e-05	1.12e-06	3.37e-08
Proposed	1.15e-03	8.87e-05	3.55e-06	1.10e-07	5.86e-09

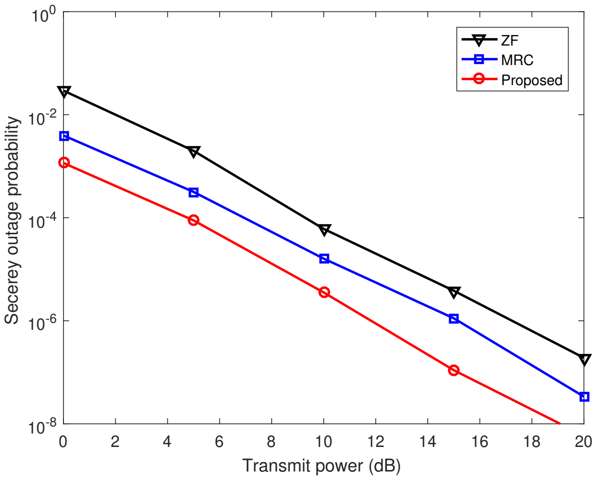

Figure 5. SOP of the considered system with $M_I = 3$.

review on the secure communication with the aid of federated learning, and then listed some key challenges on the secure communication in poor channel state. In further, this paper provided some solutions to the challenges on the secure communication, where some results were provided to show the advantages coming from the IRS technology. The research results in this paper can provide some important theoretical and practical guidance for the system design and optimization on the future network and security.

4.1. Acknowledgements

The work in this paper was supported by the NSFC with grant number 61871235.

4.2. Copyright

References

[1] J. Lu, S. Lai, J. Xia, M. Tang, C. Fan, J. Ou, and D. Fan, "Performance analysis for irs-assisted mec networks with unit selection," *Physical Communication*, vol. 55, p. 101869, 2022.

[2] L. Zhang, S. Lai, J. Xia, C. Gao, D. Fan, and J. Ou, "Deep reinforcement learning based irs-assisted mobile edge computing under physical-layer security," *Physical Communication*, p. 101896, 2022.

[3] Y. Wu, J. Xia, C. Gao, J. Ou, C. Fan, J. Ou, and D. Fan, "Task offloading for vehicular edge computing with imperfect csi: A deep reinforcement approach," *Physical Communication*, vol. 55, p. 101867, 2022.

[4] X. Hu, C. Zhong, Y. Zhu, X. Chen, and Z. Zhang, "Programmable metasurface-based multicast systems: Design and analysis," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 8, pp. 1763–1776, 2020.

[5] X. Hu, J. Wang, and C. Zhong, "Statistical CSI based design for intelligent reflecting surface assisted MISO systems," *Science China: Information Science*, vol. 63, no. 12, p. 222303, 2020.

[6] D. Cai, P. Fan, Q. Zou, Y. Xu, Z. Ding, and Z. Liu, "Active device detection and performance analysis of massive non-orthogonal transmissions in cellular internet of things," *Science China information sciences*, vol. 5, no. 8, pp. 182 301:1–182 301:18, 2022.

[7] B. Wang, F. Gao, S. Jin, H. Lin, and G. Y. Li, "Spatial- and frequency-wideband effects in millimeter-wave massive MIMO systems," *IEEE Trans. Signal Processing*, vol. 66, no. 13, pp. 3393–3406, 2018.

[8] H. Ren, T. Huang, and H. Yan, "Adversarial examples: attacks and defenses in the physical world," *International Journal of Machine Learning and Cybernetics*, vol. 12, no. 11, pp. 3325–3336, 2021.

[9] K. Mo, W. Tang, J. Li, and X. Yuan, “Attacking deep reinforcement learning with decoupled adversarial policy,” *IEEE Transactions on Dependable and Secure Computing*, 2022.

[10] H. Yan, L. Hu, X. Xiang, Z. Liu, and X. Yuan, “Ppcl: Privacy-preserving collaborative learning for mitigating indirect information leakage,” *Information Sciences*, vol. 548, pp. 423–437, 2021.

[11] S. Sheikhzadeh, M. Pourghasemian, M. R. Javan, N. Mokari, and E. A. Jorswieck, “Ai-based secure NOMA and cognitive radio-enabled green communications: Channel state information and battery value uncertainties,” *IEEE Trans. Green Commun. Netw.*, vol. 6, no. 2, pp. 1037–1054, 2022. [Online]. Available: https://doi.org/10.1109/TGCN.2021.3135479

[12] X. Liu, C. Li, S. S. Ge, and D. Li, “Time-synchronized control of chaotic systems in secure communication,” *IEEE Trans. Circuits Syst. I Regul. Pap.*, vol. 69, no. 9, pp. 3748–3761, 2022. [Online]. Available: https://doi.org/10.1109/TCSI.2022.3175713

[13] Z. Cao, X. Ji, J. Wang, W. Wang, K. Cumanan, Z. Ding, and O. A. Dobre, “Artificial noise aided secure communications for cooperative NOMA networks,” *IEEE Trans. Cogn. Commun. Netw.*, vol. 8, no. 2, pp. 946–963, 2022. [Online]. Available: https://doi.org/10.1109/TCCN.2021.3130979

[14] G. Sun, J. Li, A. Wang, Q. Wu, Z. Sun, and Y. Liu, “Secure and energy-efficient UAV relay communications exploiting collaborative beamforming,” *IEEE Trans. Commun.*, vol. 70, no. 8, pp. 5401–5416, 2022. [Online]. Available: https://doi.org/10.1109/TCOMM.2022.3184160

[15] L. Xiao, H. Li, S. Yu, Y. Zhang, L. Wang, and S. Ma, “Reinforcement learning based network coding for drone-aided secure wireless communications,” *IEEE Trans. Commun.*, vol. 70, no. 9, pp. 5975–5988, 2022. [Online]. Available: https://doi.org/10.1109/TCOMM.2022.3194074

[16] M. Stute, F. Kohnhäuser, L. Baumgärtner, L. Almon, M. Hollick, S. Katzenbeisser, and B. Freisleben, “RESCUE: A resilient and secure device-to-device communication framework for emergencies,” *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 3, pp. 1722–1734, 2022. [Online]. Available: https://doi.org/10.1109/TDSC.2020.3036224