Secure Transmission Strategy of Power Communication Based on Sensor-to-Computation Linkage

Bin Li[1], Linghui Kong[1], Xiangyi Zhang[1], Bochuo Kou[1], Hui Yu[1], and Bowen Liu[1]

[1]State Grid Beijing Urban District Power Supply Company

December 8, 2022

Abstract

The automatic collection of power grid situation information and the real-time multimedia interaction between the front and back end of the accident handling have generated massive power grid data. Wireless communication provides a convenient channel for grid terminal access and data transmission, but the bandwidth of wireless communication is limited, and its broadcasting nature makes information easy to be monitored by illegal eavesdroppers in the transmission process. In order to realize reliable, secure and real-time transmission of power grid data, an intelligent security transmission strategy based on sense-transfer linkage is proposed. The optimization problem is constructed with maximum system security capacity as the goal, interruption probability and interception probability as constraints, and a low complexity algorithm is designed to obtain the sub-optimal solution of the problem. Finally, simulation results verify the effectiveness of the proposed scheme in ensuring communication security, stability and real-time performance.

Received: Added at production | Revised: Added at production | Accepted: Added at production

DOI: xxx/xxxx

ARTICLE TYPE

Secure Transmission Strategy of Power Communication Based on Sensor-to-Computation Linkage

Bin Li* | Linghui Kong | Xiangyi Zhang | Bochuo Kou | Hui Yu | Bowen Liu

State Grid Beijing Urban District Power Supply Company, Beijing, China

Correspondence
*Corresponding author name. 41 Qianmen West Dajie, Beijing, China. Email: 19801116781@163.com

Present Address
41 Qianmen West Dajie, Beijing, China

Summary

The automatic collection of power grid situation information and the real-time multimedia interaction between the front and back end of the accident handling have generated massive power grid data. Wireless communication provides a convenient channel for grid terminal access and data transmission, but the bandwidth of wireless communication is limited, and its broadcasting nature makes information easy to be monitored by illegal eavesdroppers in the transmission process. In order to realize reliable, secure and real-time transmission of power grid data, an intelligent security transmission strategy based on sense-transfer linkage is proposed. The optimization problem is constructed with maximum system security capacity as the goal, interruption probability and interception probability as constraints, and a low complexity algorithm is designed to obtain the sub-optimal solution of the problem. Finally, simulation results verify the effectiveness of the proposed scheme in ensuring communication security, stability and real-time performance.

KEYWORDS:
secure transmission strategy, sensor-to-computation linkage, security capacity, interruption probability, power communication

1 | INTRODUCTION

The automatic collection of power grid situation information and the real-time multimedia interaction between the front and back ends of the accident disposal have produced massive power grid data [1]. With the development of power communication, wireless communication provides a convenient channel for the access of power grid terminals and the transmission of data, but the bandwidth of wireless communication is limited, and its broadcast nature makes the information easily monitored by illegal eavesdroppers in the transmission process. In order to achieve reliable, secure and real-time transmission of power grid data, it is necessary to propose an intelligent secure transmission strategy.

In recent years, many scholars have studied the impact of antenna correlation on physical layer security technology in wireless communications. In Reference [2], the author modeled the channel gain between the multiple antennas at the base station as a spatially arbitrary correlated Rayleigh random variable, and studied the relationship between the security performance of the system and the correlation coefficient when the base station transmits signals using Maximum Ratio Transmission (MRT) technology. The pros and cons of the correlation pair system are related to the SNR of the main channel. In the process of wireless transmission, the security problem that information is illegally eavesdropped by malicious users often occurs [3-4]. Considering the presence of eavesdropping users [5-6], based on the MIMO system in which the main channel and the eavesdropping channel are correlated at the same time, the author proposes that when the signal-to-noise ratio of the main channel is at a medium or high

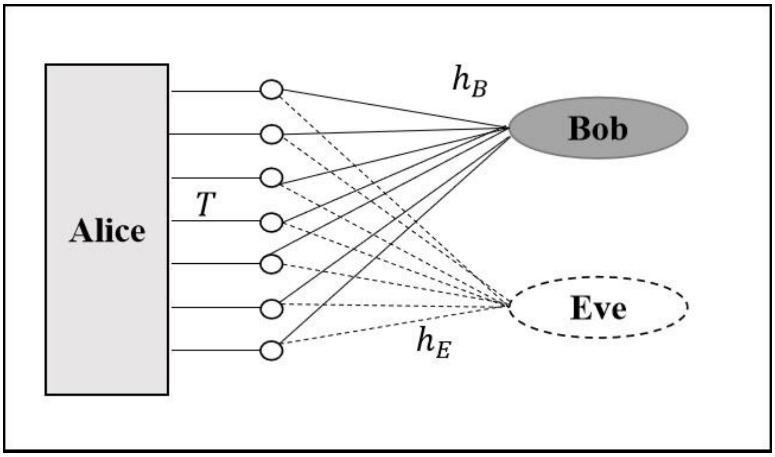

Figure 1 System Model.

level, the antenna correlation damages the security performance of the system, and then the channel security will be improved by reducing the signal-to-noise ratio of the main channel. However, the influence of the correlation between the main channel and the wiretap channel on the system is not considered in the above literatures, and this correlation model is called wiretap channel correlation in this paper. In actual transmission, this related scenario occurs when the eavesdropper is near the legitimate receiving user or in the radio path of the receiver signal [7]. In recent years, more and more people begin to pay attention to the correlation between the main channel and the wiretap channel in the research of physical layer security [8-10]. The wiretap channel correlation was studied earlier in reference [8]. Through the analysis of the multi-input single-output wiretap channel using the transmit antenna selection (TAS) technology, the author obtained that when the signal to noise ratio of the main channel is at a higher level than that of the eavesdropper channel, the correlation of the eavesdropper channel will improve the security performance of the system. Subsequently, the authors obtained the same conclusion by studying the Rayleigh [9] and Nagakami-m channels [10] using transmit antenna selection/maximum ratio combining techniques in combination. In references [11-13], the authors also studied the optimal power allocation problem of the artificial noise technique at the transmitter when the wiretap channel is correlated. Compared with the traditional diversity scheme, MRT can not only provide diversity gain, but also have antenna array gain, so as to obtain a larger received signal-to-noise ratio and reduce the impact of multipath fading and co-channel interference, but there is no report on the security performance of MRT technology in wiretap channel related scenarios.

This paper mainly considers the security performance of the system when the transmitter uses MRT technology in the wiretap channel correlation scenario, and analyzes the impact of wiretap channel correlation on the system security performance from the perspective of security outage probability and average security capacity. Finally, an optimal power allocation method is proposed to maximize the secrecy rate while satisfying the security outage constraint, which allocates the total power to the legitimate transmitter, the active eavesdropper and the passive eavesdropper optimally, so as to maximize the secrecy rate.

2 | SYSTEM MODEL & PROBLEM FORMULATION

2.1 | System model

The system model is shown in Fig. 1. In this paper, we consider the downlink of the flat Rayleigh fading channel, where the base station (Alice) is configured with T antennas and transmits information using MRT, and the legitimate receiver (Bob) has only one antenna. An eavesdropper (Eve) with a single antenna can only receive information passively and both Bob and Eve are far away from Alice. It is assumed that Alice can obtain all the channel state information (CSI) with Bob. h_B , h_E represent the channel parameter matrices between Alice, Bob and Eve's link, respectively. The channel coefficients of each channel are independently distributed.

It is assumed that there is a certain correlation between the main channel and the wiretap channel, and the correlation coefficient is ρ, which satisfies $0 \leq \rho \leq 1$. According to the Rayleigh fading channel model, in the multipath channel environment with rich scattering, when the number of scatterers tends to infinity, the correlation function of the channel characteristic parameters is the first kind of zero-order Bessel function, which is $\rho = J_0\left(2pf_m t\right)$. Here, $J_0()$ denotes the zero-order Bessel function of the first kind. f_m is the Doppler frequency shift, which is generally considered to be inversely proportional to the coherence time of the channel. The coherence time satisfies $T_c = 1\big/f_m$. In the channel model of this paper, the channel temporal correlation is equivalent to the spatial correlation. For example, when Eve is near Bob, the correlation coefficient can be expressed as $\rho = J_0\left(2p\Delta d\right), \Delta d = D/l$. Here, l represents the wavelength of the carrier wave used for signal transmission, and D represents the distance between the eavesdropper and the legitimate receiver. Therefore, the channel parameters of the wiretap channel h_E can be calculated as follows.

$$h_E = \rho h_B + \sqrt{1-\rho^2}h_e \tag{1}$$

Here, h_B and h_E are independent and identically distributed Rayleigh channels. $\rho = 0$ indicates that the channels between the main channel and the wiretap channel are independent. $\rho = 1$ represents a full correlation between that main channel and the wiretap channel. Maximum transmit weight vector $w = \left(w_1, w_2, ..., w_T\right)^T$ can be calculated by $w = h_B^H\big/\left\|h_B\right\|_F$. Therefore, the received signals of Bob and Eve can be computes follows.

$$y_B = \sqrt{P}h_B wx + n_B \tag{2}$$

$$y_E = \sqrt{P}h_E wx + n_E \tag{3}$$

Here, n_B and n_E represent the complex Gaussian white noise of the main channel and the wiretap channel respectively, and their variances are σ_b^2, σ_e^2. P represents the transmit power of the signal. According to [14], The cumulative distribution function of the γ_B and the probability density function of γ_E can be expressed as follows.

$$F_{\gamma_B}(x) = 1 - \exp\left(-\frac{x}{\gamma_B}\right)\sum_{m=0}^{T-1}\frac{1}{m!}\left(\frac{x}{\gamma_B}\right)^m \tag{4}$$

$$f_{\gamma_E}(x) = \frac{1}{\bar{\gamma}_E^T}\sum_{i=0}^{T-1}\begin{pmatrix} T-1 \\ i \end{pmatrix}\frac{\left(\rho^2\right)^{T-i+1}\left[\sqrt{\gamma_E}\left(1-\rho^2\right)\right]^i}{(T-i-1)!}x^{T-i-1}\exp\left(-\frac{x}{\gamma_E}\right) \tag{5}$$

Here, γ_B and γ_E denote the instantaneous received SNR of Bob and Eve, respectively, satisfying $\gamma_B = \bar{\gamma}_B\left\|h_B w\right\|_F^2$ and $\gamma_E = \bar{\gamma}_E\left\|h_E w\right\|_F^2$. $\bar{\gamma}_B$ and $\bar{\gamma}_E$ represent the average signal-to-noise ratio of the main channel and the wiretap channel, respectively.

2.2 | Problem Formulation

In order to ensure the quality of communication, the security outage probability should be less than the threshold. Therefore, to maximize the secrecy rate under reliability and security requirements, we formulate the optimization problem as follows, i.e., to maximize the system capacity subject to the outage probability constraint.

$$\max_{P} \mathrm{C}_s \tag{6}$$

$$P_{out}^{\infty}\left(R_s\right) < \delta \tag{7}$$

$$0 \leq R_s \leq R_b \tag{8}$$

$$0 \leq P \leq P_{\max} \tag{9}$$

Here, C_s denotes the system privacy capacity. R_s is the transmission rate threshold. $P_{out}^{\infty}\left(R_s\right)$ represents the outage probability. δ denotes the outage probability threshold. $P_{\max}$ represents the maximum transmit power.

3 | OPTIMAL POWER ALLOCATION STRATEGY

3.1 | Example for another second level head

The security outage probability is an important indicator for analyzing the security performance of wireless systems. The security outage probability is defined as the probability of the secrecy capacity C_s under secure transmission rate threshold R_s. Here, R_s is related to the estimation of Eve's channel state information by Alice. The outage probability can be expressed as follows.

$$P_{out}\left(R_s\right) = \Pr\left(C_s < R_s \left|\gamma_B > \gamma_E\right.\right) \Pr\left(\gamma_B > \gamma_E\right) + \Pr\left(\gamma_B < \gamma_E\right) \tag{10}$$

$$P_{out}\left(R_s\right) = \int\limits_0^{\infty} \int\limits_0^{\Lambda\left(1+\gamma_E\right)-1} f_{\gamma_E}\left(\gamma_E\right) f_{\gamma_B}\left(\gamma_B\right) d\gamma_E d\gamma_B = \int\limits_0^{\infty} f_{\gamma_E}(x) F_{\gamma_B}\left(\Lambda\left(1+x\right)-1\right) dx \tag{11}$$

Here, $\Lambda = 2^{R_s}$. With the help of literature [14-15], we can obtain an approximate expression for the outage probability, as shown in Eq. (12).

$$\begin{gathered} P_{out}\left(R_s\right) = 1- \\ \exp\left(\tfrac{-(\Lambda-1)}{\left(\bar{\gamma}_B-\Lambda\bar{\gamma}_E\rho^2\right)}\right) \sum_{m=0}^{T-1} \sum_{i=0}^{T-1} \sum_{k=0}^{m} \begin{pmatrix} T-1 \\ i \end{pmatrix} \begin{pmatrix} m \\ k \end{pmatrix} \tfrac{(\Lambda-1)^{m-k}\left(\Lambda\bar{\gamma}_E\left(1-\rho^2\right)\right)^k \left(\rho^2\right)^{T-1-i} \left(1-\rho^2\right)^i}{\left(\bar{\gamma}_B-\Lambda\bar{\gamma}_E\rho^2\right)^m m!(T-i-1)!} \left(\tfrac{\left(\bar{\gamma}_B-\bar{\gamma}_E\rho^2\right)}{\bar{\gamma}_B-2\Lambda\bar{\gamma}_E\rho^2-\Lambda\bar{\gamma}_E}\right)^{T-i+m} \\ \times\Gamma\left(T-i-1+m\right) \end{gathered} \tag{12}$$

Here, $\Gamma\,()$ represents the Gamm function.

The safety capacity can be defined as shown in Eq. (13).

$$C_s = \begin{cases} R_B - R_E, \ \gamma_B > \gamma_E \\ 0, \ \gamma_B \le \gamma_E \end{cases} \tag{13}$$

Here, $R_B = \log\left(1+\gamma_B\right)$ indicates the instantaneous transmission rate of the main channel. $R_E = \log\left(1+\gamma_E\right)$ represents the instantaneous transmission rate of the wiretap channel. $C_s \ge R_s$ can guarantee the secure communication. Otherwise, Eve may steal the information. Since the channel capacity is a random variable, here we consider the ergodic capacity, i.e., the average secrecy capacity, which implies that Alice can transmit at an arbitrary rate bounded by the average secrecy capacity. According to the conventional literature, the average safety capacity can be expressed as follows.

$$\bar{C}_s = \int\limits_0^{\infty}\int\limits_0^{\infty} C_s f_{\gamma_B}(x) f_{\gamma_E}(x)\, dx dy = \int\limits_0^{\infty}\int\limits_0^{\infty} \left[C_s f_{\gamma_E}(y)\, dy\right] f_{\gamma_B}(x)\, dx \tag{14}$$

Combining with the Eq. (15), we can obtain the expression as follows.

$$C_s = \int\limits_0^{x} \left(R_B - R_E\right) f_{\gamma_E}(y)\, dy = \frac{1}{\ln 2} \int\limits_0^{x} \frac{F_{\gamma_E}(y)}{1+y} dy \tag{15}$$

$$\bar{C}_s = \frac{1}{\ln 2} \int\limits_0^{\infty} \frac{F_{\gamma_E}(x)}{1+x} \left[1 - F_{\gamma_B}(x)\right] dx \tag{16}$$

According to the integral solution formula, we can obtain the closed-form expression of the average secure capacity, as shown in Eq. (17).

$$\bar{C}_s = \frac{1}{\ln 2} \sum_{m=0}^{T-1} \frac{1}{m!} \left[\begin{array}{l} (-1)^{m-1} \exp\left(\frac{1}{\bar{\gamma}_B}\right) Ei\left(-\frac{1}{\bar{\gamma}_B}\right) \\ + \sum_{k=0}^{m} k!(-1)^{m-k} \left(\frac{1}{\bar{\gamma}_B}\right)^{-k} \end{array} \right] - \frac{1}{\ln 2} \sum_{n=0}^{T-1} \sum_{i=0}^{T-1-n} \sum_{m=0}^{T-1} \frac{\left((\rho^2)^{T-1-n}(1-\rho^2)^n\right)}{i!m!\bar{\gamma}_E^{-i}\bar{\gamma}_B^{-m}} \times \left[\begin{array}{l} (-1)^{i+m-1} \exp\left(\frac{1}{\bar{\gamma}_B} + \frac{1}{\bar{\gamma}_E}\right) Ei\left(-\frac{1}{\bar{\gamma}_B} - \frac{1}{\bar{\gamma}_E}\right) \\ + \sum_{q=0}^{i+m} q!(-1)^{i+m-q} \left(\frac{1}{\bar{\gamma}_B} + \frac{1}{\bar{\gamma}_E}\right)^{-q} \end{array} \right] \tag{17}$$

Here, $Ei\,()$ represents an exponential integral function.

In order to better understand the impact of correlation factors on the system performance at high SNR, we discussed the security outage probability of the system when $\bar{\gamma}_B, \bar{\gamma}_E \rightarrow \infty$. Referring to [15], we perform a Taylor expansion of the Eq. (4) and take the first term in the expansion to non-zero order to obtain the expression of its asymptotic distribution function, which is shown in Eq. (18).

$$F_{\gamma_B}^{\infty} = \frac{1}{T!} \left(\frac{x}{\bar{\gamma}_B}\right)^T + O\left(\left(\frac{x}{\bar{\gamma}_B}\right)^T\right) \tag{18}$$

Here, $O\,()$ is defined as a higher order infinitesimal. According to the Eq. (10), we calculate the expression of the system safety outage probability as shown in the Eq. (19).

$$P_{out}^{\infty}\left(R_s\right) = \varphi\left(\bar{\gamma}_B - \Lambda\bar{\gamma}_E\rho^2\right)^{-G_d} \tag{19}$$

Here, $\varphi = \sum_{i=0}^{T-1} \sum_{k=0}^{T} \binom{T-1}{i} \binom{T}{k} \frac{\left(\Lambda\bar{\gamma}_E\left(1-\rho^2\right)\right)^k (\Lambda-1)^{T-k} \Gamma(T-i+k)}{T!\Gamma(T-i)}$, $G_d = T$ represents the safe diversity order.

Based on the above, we propose the optimal power allocation algorithm as follows.

Algorithm 1 Optimal Power Allocation Algorithm

```
Input: channel information, maximum transmission power
Output: Optimal power allocation
Initialization: Initialize the initial transmit power
Calculate the power interval $[p_1, p_2]$ meeting the outage probability constraint according to the Eq. (8).
The power that maximizes the capacity $p^*$ is calculated according to the Eq. (13).
If $p^*$ located in the interval $[p_1, p_2]$ Then the optimal power allocation is $p^*$.
If $p^*$ located in the interval $[p_1, p_2]$'s left side, then the optimal power allocation is $p_2$.
If $p^*$ located in the interval $[p_1, p_2]$'s right side, then the optimal power allocation is $p_1$.
Return the optimal power distribution.
```

4 | SIMULATION ANALYSIS

In this section, the influence of wiretap channel correlation on the security performance of wireless communication system using MRT is analyzed by numerical simulation and verified by Monte Carlo simulation. Since we do not delve into how to set the secrecy rate threshold, is assumed in the following simulation.

Fig. 2 shows the average signal-to-noise ratio of the security outage probability $\bar{\gamma}_B$ with the main channel. Set $\bar{\gamma}_E = 0$ in the simulation. From the figure, it can be found that when $\bar{\gamma}_B$ locates lower levels, the safety performance of the system deteriorates significantly. In addition, the stronger the correlation is, the more serious the safety performance of the system deteriorates. With $\bar{\gamma}_B$ gradually rising to the medium and high level, we can find that the stronger the correlation, the faster the security performance of the channel. When $\bar{\gamma}_B$ is larger, the approximate curve of the security outage probability can be consistent with the theoretical curve, which verifies the correctness of the optimal power allocation.

Fig. 3 shows the relationship between the security outage probability and the correlation coefficient under different channel conditions when the number of antennas at the transmitter is T = 2. The two curves in the upper part of the figure indicate that

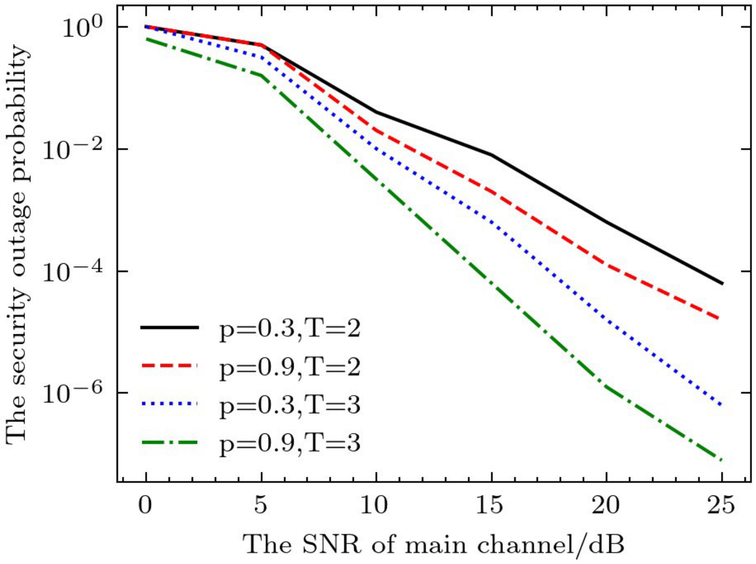

Figure 2 The SNR of main channel vs the security outage probability.

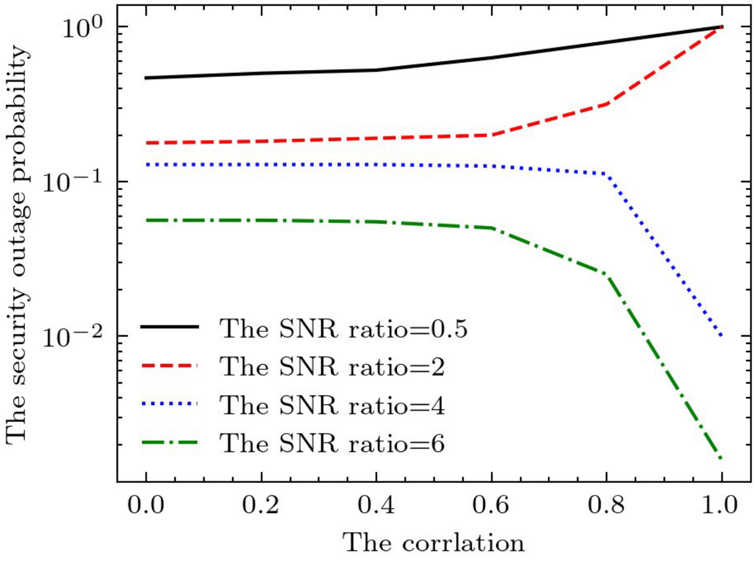

Figure 3 The correlation vs the security outage probability.

the signal-to-noise ratio of the main channel is at a medium or low level. It can be seen that when the main signal-to-noise ratio is low, the stronger the correlation is, the worse the security performance of the system is. The lower two curves represent the case when the main channel signal-to-noise ratio is at a high level, but when the correlation is weak. There is still a slight increase in the safety outage probability, however, when the correlation coefficient is greater than 0. 6, the safe outage probability decreases obviously with the increase of the correlation, and the system reliability is improved.

As shown in Fig. 4, assuming that the number of transmissions T = 3 and the signal-to-noise ratio of the wiretap channel, the relationship between the average secrecy capacity and the signal-to-noise ratio of the main channel is numerically simulated for different correlation coefficients. It can be found that the higher the correlation is, the lower the average channel security capacity is. The average safety capacity will be improved by improving the signal-to-noise ratio of the main channel.

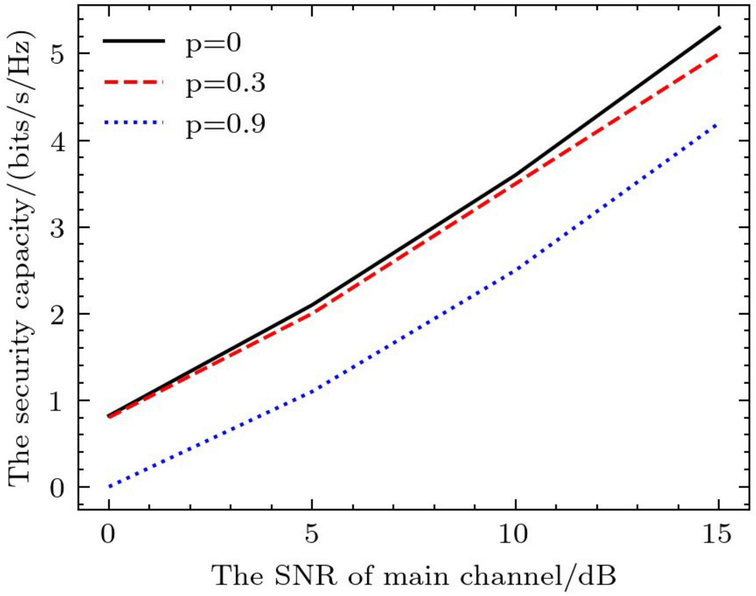

Figure 4 The SNR of main channel vs the security capacity.

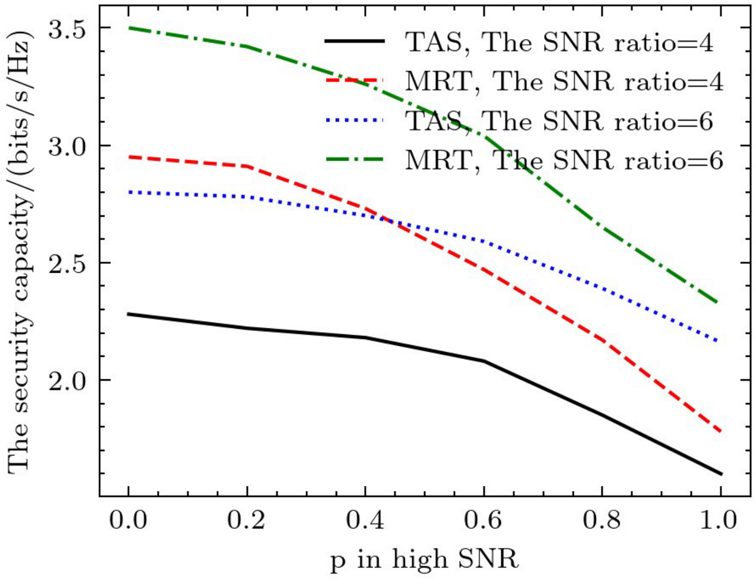

Figure 5 The correlation in high SNR vs the security capacity.

Fig. 5 simulates the relationship between the correlation coefficient and the average security capacity when the base station transmits signals using MRT and TAS respectively. Similar to the rule in Fig. 4, the stronger the correlation of the channel is, the lower the value of the average security capacity is. By comparing the two transmission technologies, we find that with the increase of correlation strength, the advantage of MRT over TAS technology in the ability to improve the average security capacity gradually decreases.

5 | CONCLUSION

In the case of wiretap channel correlation, the relationship between the performance of MISO system with MRT and the channel correlation strength is studied from the perspective of physical layer security. The closed-form expressions of the secrecy outage probability and the average secrecy capacity are derived, and the asymptotic performance analysis of the secrecy outage probability in this scenario is given, which provides theoretical guidance for future beamforming technology research in such scenarios. The simulation results show that, for the SOP performance, when the quality of the main channel is poor, the higher the correlation degree is, the worse the security performance is, and when the quality of the main channel is higher than that of the wiretap channel, the weak correlation has little effect on the security outage probability, but the strong correlation is beneficial to the SOP performance of the system. From the perspective of average security capacity, the correlation damages the security performance of the system, and the advantage of MRT over TAS becomes smaller as the channel correlation strength increases.

Financial disclosure

None reported.

Conflict of interest

The authors declare no potential conflict of interests.

References

1. T. Choi et al., "Experimental Investigation of Frequency Domain Channel Extrapolation in Massive MIMO Systems for Zero-Feedback FDD," in IEEE Transactions on Wireless Communications, vol. 20, no. 1, pp. 710-725, Jan. 2021.

2. C. Li, S. De Bast, E. Tanghe, S. Pollin and W. Joseph, "Toward Fine-Grained Indoor Localization Based on Massive MIMO-OFDM System: Experiment and Analysis," in IEEE Sensors Journal, vol. 22, no. 6, pp. 5318-5328, 15 March15, 2022.

3. B. Ji, Y. Li, D. Cao, C. Li, S. Mumtaz and D. Wang, "Secrecy Performance Analysis of UAV Assisted Relay Transmission for Cognitive Network With Energy Harvesting," in IEEE Transactions on Vehicular Technology, vol. 69, no. 7, pp. 7404-7415, July 2020.

4. L. Zhouhong, X. Tian, D. Lijuan and T. Xingtao, "Research on Capacity Selection of Multiple Distributed Generations Connected to Microgrid," 2018 China International Conference on Electricity Distribution (CICED), 2018, pp. 2131-2136.

5. N. S. Ferdinand, D. B. da Costa and M. Latva-aho, "Physical Layer Security in MIMO OSTBC Line-of-Sight Wiretap Channels with Arbitrary Transmit/Receive Antenna Correlation," in IEEE Wireless Communications Letters, vol. 2, no. 5, pp. 467-470, October 2013.

6. Rung-Hung Gau, "Performance analysis of multicast key backbone for secure group communications," in IEEE Communications Letters, vol. 10, no. 7, pp. 555-557, July 2006.

7. L. Wei, Y. Chen, D. Zheng and B. Jiao, "Secure performance analysis and optimization for FD-NOMA vehicular communications," in China Communications, vol. 17, no. 11, pp. 29-41, Nov. 2020.

8. X. Sun, J. Wang, W. Xu and C. Zhao, "Performance of Secure Communications Over Correlated Fading Channels," in IEEE Signal Processing Letters, vol. 19, no. 8, pp. 479-482, Aug. 2012.

9. X. Liu and M. Nie, "Quantum Secure Direct Communication Protocol Based on Entangled State and Quantum State," 2012 International Conference on Industrial Control and Electronics Engineering, 2012, pp. 828-831.

10. J. You, Z. Zhong, G. Wang and B. Ai, "Security and Reliability Performance Analysis for Cloud Radio Access Networks With Channel Estimation Errors," in IEEE Access, vol. 2, pp. 1348-1358, 2014.

11. D. Do, A. Le and S. Mumtaz, "Secure Performance Analysis of RIS-aided Wireless Communication Systems," 2021 IEEE Global Communications Conference (GLOBECOM), 2021, pp. 01-06.

12. A. Festag, P. Papadimitratos and T. Tielert, "Design and Performance of Secure Geocast for Vehicular Communication," in IEEE Transactions on Vehicular Technology, vol. 59, no. 5, pp. 2456-2471, Jun 2010.

13. J. -Y. Wang, Y. Qiu, S. -H. Lin, J. -B. Wang, Q. Wang and B. Zhang, "Performance Analysis and Improvement for Secure VLC With SLIPT and Random Terminals," in IEEE Access, vol. 8, pp. 73645-73658, 2020.

14. M. P. Anastasopoulos, D. K. Petraki and H. -H. Chen, "Secure communications in local multipoint distribution service (LMDS) networks," in IEEE Transactions on Wireless Communications, vol. 8, no. 11, pp. 5400-5403, November 2009.

15. Q. Chen, Y. Fan, M. Cheng and X. Gao, "Secure Spread Spectrum Communication Using Super-Orthogonal Optical Chaos Signals," in IEEE Photonics Journal, vol. 14, no. 4, pp. 1-6, Aug. 2022.

AUTHOR BIOGRAPHY

Bin Li. Bin Li received the B.E. and M.E. degrees in Electrical Engineering and Automation from Tianjin University, Tianjing, China,in 2002, and 2005. He is currently a Senior Engineer in State Grid Beijing Urban District Power Supply Company. His research interests include power system transient stability assessment, Power flow analysis, and distribution network planning.

Linghui Kong. Linghui Kong received the B.E. degree in Electrical Engineering and Automation from North China Electric Power University, Beijing, China, in 2007, received the M.E. degree in project management from North China Electric Power University, Beijing, China, in 2016. She is currently a Senior Engineer in State Grid Beijing Urban District Power Supply Company. Her research interests include power system operation and power market.

Xiangyi Zhang. Xiangyi Zhang Graduated from Electrical Engineering of North China Electric Power University and started working in 1997. He is currently a Senior Engineer in State Grid Beijing Urban District Power Supply Company, mainly engaged in power supply and power quality management. He has published lots papers in the issue of Electrical Technology (Including English EI journals).research interests include the transmission of electric power and energy conservation and loss reduction of power grid.

Bochuo Kou. Bochuo Kou received the B.E. degree in Electrical Engineering and Automation and M.E. degree in electrical engineering from North China Electric Power University, Baoding, Hebei Province, China. He is currently a Engineer in State Grid Beijing Urban District Power Supply Company. His research interests include power system protection and control, power system reliability, and risk assessment.

Hui Yu. Hui Yu received the B.E. degree in Electrical Engineering and Automation from Tianjin University, Tianjing, China, in 2003, received the M.S. degree in Electrical and Electronics Engineering from the Huazhong University of Science and Technology, Wuhan China, in 2006. He is currently a Senior Engineer in State Grid Beijing Urban District Power Supply Company. His research interests include power systems, disrtibution network planning and automation, and smart grids.

Bowen Liu. Bowen Liu received the B.E. degree in Communication Engineering from North China Electric Power University, Beijing, China,in 2011, received the M.E. degree in Electrical Engineering from Northeast Electric Power University, Changchun, China, in 2016. He is currently an Engineer in State Grid Beijing Urban District Power Supply Company. His research interests include distribution automation system, smart power distribution network and digital power grid.

□