International Journal of Future Generation Communication and Networking
Vol. 9, No. 7 (2016), pp. 307-316
http://dx.doi.org/10.14257/ijfgcn.2016.9.7.29

The Physical Layer Security Beamforming Method based on Large-scale Multi-antenna

Zhou Wen-gang, Li Jing, Guo Hui-ling

School of computer science and technology, ZhouKou Normal University, Henan, 466001, China
zhouwengang@zknu.edu.cn,lijing@zknu.edu.cn,guohuiling@zknu.edu.cn

Abstract

Network security with encryption and decryption technology to complete the application layer, but this technology will bring computing resources and a waste of energy, particularly in these two resources are limited wireless communication system for this problem, we use a large-scale multi-antenna technology, using beamforming algorithm in power and spectrum limited conditions, to maximize the mutual information system security, the simulation results demonstrate the ability to secure transmission algorithms can effectively improve the system.

Keywords*: Large Scale Antenna, Random Matrix, Beamforming, Secrecy Capacity*

1. Introduction

Typically used to describe the communication system performance indicators for the validity and reliability, validity refers to the performance for the time domain, frequency domain, airspace and other resources, make full use of the channel, and the reliability of the information refers to send the receiving end accurately restore performance. As technology advances, people for communication system quality requirements no longer limited to the validity and reliability, and security, the system in the face of resistance to the threat of man-made destruction or eavesdropping, when interference [1]. The wireless communication system because of its ease of communication, people get more and more attention and use. However, due to the openness of the wireless communication system physical transmission medium, and radio characteristics of the transmission channel factors, wired communication system compared to the wireless communication system more vulnerable to threats of eavesdropping and interference, the communication secure wireless communications system should be people pay more attention. Especially when it comes to the transmission of information related to national security or commercial confidentiality, security of the wireless communication system is more important than the other two indicators.

In current wireless communication systems to ensure secure communication habits means is the use of the upper layer communication protocol stack technology using authentication or cryptographic techniques to secure communications. Traditional cryptographic mechanism to get the attention of many scholars at home and abroad, has grown more perfect, but these technical problems such as symmetric key cryptosystem.

Allocation, and asymmetric cryptosystems highly computational complexity and other issues. With the increase in computing power, not only legitimate traffic double the computing power, but also increase the computing power of eavesdropping end, the traditional password mechanism can not fully guarantee the security of communications. To be clear conventional encryption mechanisms at the level of cryptographic operations are performed outside of the physical layer, the

ISSN: 2233-7857 IJFGCN

information encrypted in the physical layer is converted to the corresponding physical layer for transmission in the form of transmission, assuming physical layer error-free transmission. Due to open radio channel, broadcasting and fading resistance, error-free transmission of the physical layer of this assumption not be guaranteed. And if the physical channel is perfect, when eavesdroppers to decipher the secret key information after the communication will be a serious threat to security.

Physical layer security technology that use wireless communication in the physical layer signal format and physical characteristics of the radio channel characteristics to ensure that technology, in recent communication to become a hot spot wireless communication system security research [2-5].

The basic idea is to use the physical layer security inherent random noise and the communication channel conditions, restrict unauthorized receiver receive legitimate information. Physical layer security technology eavesdroppers do not get any limitations in terms of computing resources and network parameters. Related physical layer channel coding security technology, physical layer secret key technology, cooperative interference technology, using the channel characteristics of other technologies. Because the physical layer security technology not only can be used alone to guarantee the security of communicating, but also as a complement to traditional password mechanism to secure communications. Therefore, the study of physical layer security technology to ensure communication security is of great significance. Its an important branch of artificial noise technology in recent years has been rapid development, also has important significance.

In the system, sending and receiving end is equipped with multiple antennas can provide diversity and spatial multiplexing gain, thereby improving spectral efficiency of the system. In general, the sending and receiving end is equipped with an antenna, the higher the degree of freedom provided by the system, so that the data rate of the system and higher reliability. Thus, large-scale technology is considered the candidate for the fifth-generation radio communication system which has been more and more research. Large-scale system has the following characteristics [6-8]:

1) The base station is configured with hundreds of antennas, while service users dozens of single antenna. Users of all cells in the same frequency band, so a high spectral efficiency of the system. The system uses time division duplex transmission mode. In the uplink transmission, all users transmit the pilot to the base station, the base station estimates the channel, and then use the estimated channel uplink data detection. This system, the uplink channel and downlink channel meets reciprocity, that is, two channels are mutually transposed relationship.

2) Each antenna consumes very low power. Under ideal conditions, the total transmit power for the same power and the number of antennas each transmitting antenna is inversely proportional. Moreover, for the same transmit signal to noise ratio, the total transmit power is inversely proportional to the number of antennas.

3) Channel matrix showing unprecedented new features, and can be used random matrix theory to analyze. First, the number of antennas tends to infinity, the singular values of the channel matrix become known asymptotic distribution.

2. Related Works

2.1. Physical Layer Security Technology

For physical layer security, there are usually two ideas: First, encrypted by the secret key technology, coding, modulation, etc. to protect the security of communications; the second is the use of cooperative interference way, the

deterioration of the eavesdropper channel interference eavesdropper eavesdropping. Correspondingly, a variety of physical layer security technology.

1) Channel coding security encryption technology.

Channel coding technique that is generally used for error correction, but its role is not limited to this, can be used in public-key encryption system secret. After the study, it is multi-channel coding (error correction code), such as LDPC codes, polarization code, trellis coding, after some adaptations, may limit the capacity to achieve confidentiality, which up LDPC code applications. In general, said the capacity can be achieved secret channel coding for the security code. In addition, the space-time coding, pre-algebraic coding, spreading code technology, specially designed to be able to approach the secret channel capacity.

2) Physical layer secret key encryption technology.

The current study focused on the use of the radio channel characteristics to produce, manage and distribute keys, and a combination of specific transmission technology / systems, such as OFDM, UMB broadband system key generation method / algorithm. A problem in that, since the sender and receiver is different for the estimated channel, how to control the difference within a certain range, so that the estimation error does not affect the key. Second, the current can only be applied using the channel reciprocity in TDD systems [9-10].

3) Collaboration interference.

According to information theory, requires tapping channel capacity is less than the legal channels, in order to ensure a certain degree of secrecy capacity, secure communication becomes possible, cooperative interference is to introduce differentiated interference, deterioration eavesdropping channel, and legitimate channel quality higher than eavesdropping channel quality. Generally divided into multiple scenes and multiple antenna relay system, and the scene is divided into multiple antenna random selection, random coefficient perturbation, and from artificial noise. Here focuses on artificially noisy way to ensure secure communications physical layer issues in wireless communications, it would be artificial noise in the back way described in detail.

4) Spread spectrum and frequency hopping encryption technology.

Currently the most practical application of physical-layer encryption technology is undoubtedly expand

Encryption and frequency hopping encryption, used for high safety standards and tactical military satellite communications system, a wireless communication system. Direct Sequence Spread Spectrum need to use high-frequency pseudo-random sequence spread spectrum modulation / demodulation, spread spectrum signal to achieve; also need to use pseudo-random hopping sequences to control the carrier frequency hopping time and duration to achieve frequency hopping law pseudo randomness. And frequency-hopping spread spectrum dependent pseudo-random sequence is such that it is adapted to the natural traditional symmetric encryption password.

5) Other techniques using the channel characteristics.

Using the channel characteristics of the physical layer authentication, namely the use of certain features of the physical layer to achieve the purpose of authentication, such as radio frequency fingerprint technology; channel estimation techniques, but

in the case of phase estimation are not allowed to enhance security performance needs to further study [11-12].

Privacy is a relative concept, involving the difference in the rate of Eve and Bob. The secrecy capacity is implemented by a random encoding, where each message is associated with a plurality of code words to confuse the listener. Along with the rate of information C_S and confusion $I(X;Z)$, both the secure message and the chaotic message can be decoded by Bob, because his channel can decompose the combined message when the rate is up to $I(X;Y)$, on the other hand, all messages are equally applicable to Eve, because the decomposition of her channel is limited to $I(X;Z)$. The channel prefix of equation (1) shows another aspect of the security relativity. From the data processing inequality, the effective rate of channel prefix from $I(X;Y)$ reduced to $I(V;Y)$, and the leakage rate from $I(X;Z)$ reduced to $I(V;Z)$. However, by reducing $I(X;Z)$ the relatively possible more than $I(X;Y)$, so it needs to carefully select V, so the general situation requires to use channel prefix. For the Gauss channel, the non-fading wireless communication channel model, the input of a Gauss channel maximizes mutual information, and computes the difference between the mutual information, so the secrecy capacity is equal to the channel capacity difference between the legal link C_B and the eavesdropping link C_E. Let us suppose $C_B \geq C_E$, then

$$C_S = C_B - C_E = \frac{1}{2}\log\left(1+\frac{P}{\sigma_B^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_E^2}\right) \quad (1)$$

Confidentiality capacity is a measure of system security, initially defined as the legitimate recipient can ignore the error may be an error on the received signal is decoded, but is completely illegal eavesdropper can not be decoded when its maximum rate information . The expression is slightly different in different models eavesdropping.

Based Wyner secret eavesdropping channel capacity [13-15] is defined as the guarantee perfect secrecy (perfect secrecy) under the premise of the system up to the maximum transmission rate.

Confidential interrupt events include not only secure communication failure, including failure reliable communications. When the channel model eavesdropping channel model with Gaussian wiretap channel model, the secrecy capacity is below a given security rate, the communication will generate an interrupt, the interrupt probability; when confidential capacity above a given security rate, secure communication can get on.

After scholars, tapping in Rayleigh fading channel model, even if the average SNR legitimate receiving end of a period of time less than the average SNR eavesdropping end, there is the probability of the instantaneous received SNR is greater than the legal eavesdropping SNR exist, In other words, the system may still be able to perform secure communication.

2.2. Large Scale Antenna Research Status

Large-scale research in signal processing is mainly pre-coding and signal detection. In a single-cell large-scale systems, preclude the use of linear predictive coding can be obtained and the best dirty paper coding and close rate performance. The use of high dimension of the matrix inversion can be simplified nature, the linear pre-coding can also have a low implementation complexity. In order to reduce the power amplifier requirements, also it raised the pre-coding algorithm constant

envelope. There are some research on capacity traitor. Large-scale energy and spectral efficiency compared to single-antenna system has several orders of magnitude improvement. System and rate can be expressed as the number of antennas, the number of users, and a function of the number of resource blocks, whereby the optimum system design can be met under certain QOS criteria. For block Rayleigh fading channels, we can design the optimal space-time modulation scheme based on channel capacity. When considering a multi-cell system, compared to the ideal of independent Rayleigh fading channel, the channel response related to a more realistic propagation environment, then the channel response can be expressed as a function of the angle of arrival.

In this channel model, the performance of large-scale system is still limited to pilot pollution. And, using the channel response versus angle, beamforming may be used to send signals to particular users without interference when a limited number of base station antennas when the rate can be obtained by the analysis and the optimal number of antennas. On the other hand, by allocating the transmission power to be reduced and the time slot pilot pollution. In addition, the design and analysis of other forms of large-scale systems was also studied. For instance, frequency division duplex system analysis based on compressed sensing limited feedback and distributed power systems selection, antenna selection, pre-coding, and speed, capacity analysis.

3. Proposed Scheme

In this paper, we consider the downlink MIMO Massive system, as shown in Fig.1, the single cell BS is a transmitter, the BS is equipped with M antennas, and BS serves K users (this paper does not consider the multi-user selection problem). Each $k-th$ user is equipped with multiple antennas, and the number of receiving antennas is N_k ($k = 1, 2, 3, \mathrm{L}\ , K$). K users uniform in a radius of R in a cell, the information received by K users is in the same time - frequency resource block.

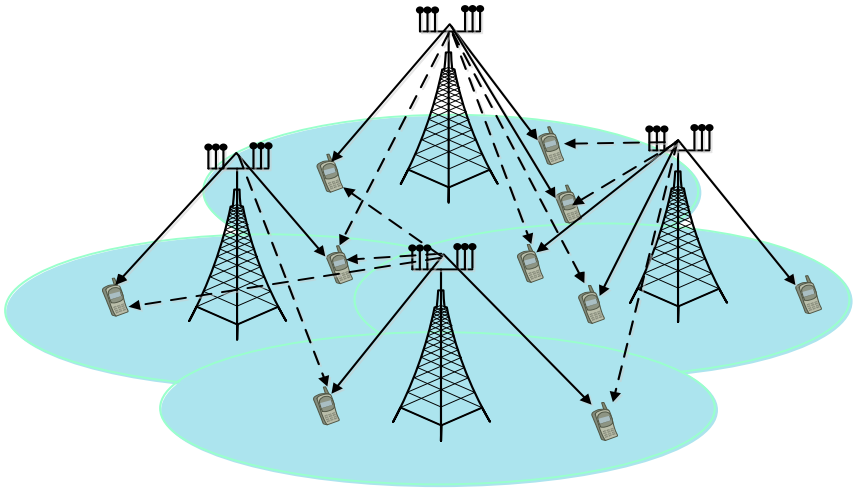

Figure 1. Large-scale Antenna MU-MIMO Network

The channel from K users to the BS can be expressed as $G = HD^{1/2}$, where, $D = diag\{\beta_1, \beta_2, \mathrm{L}\ , \beta_K\}$ is the large scale fading system matrix of the channel, mainly consider path loss and shadowing fading, $\beta_k = \phi d_k^{-\alpha} \zeta$, where ϕ is the fading constant, d_k is the distant of user k to the BS, α path loss fading index , ζ is the shadow

fading coefficient, it follows the lognormal distribution, $\lg\zeta : N\left(0,\left(\frac{\sigma_{sh}}{10}\right)^2\right)$. $H=[H_1,\mathrm{L}\ H_K]^T$,where, $H_i \in C^{N_k\times M}$, The channel is represented by a BS to a user i, where the real and imaginary parts of each element are subject to the standard normal distribution, that is, Rayleigh fading. The user i precoding matrix can be expressed as $T_i\ (i=1,\mathrm{L}\ ,\mathrm{K})$. The signals received by the user k can be expressed as

$$y_k = \sqrt{p_k}G_k T_k \mathbf{s}_k + \sum_{i=1,i\neq k}^{K}\sqrt{p_k}G_i T_k \mathbf{s}_k + \mathbf{n}_k \tag{2}$$

If there is an eavesdropper, the user's SINR is

$$SINR_E = \frac{\left|\boldsymbol{H}_E \boldsymbol{T}_1\right|^2}{\sigma^2 + \sum_{m=2}^{M}\left|\boldsymbol{H}_m \boldsymbol{T}_m\right|^2 + IT_Z} \tag{3}$$

In the optimization system, the two variables need to be determined, η_1 and η_2 respectively, which are constant in this paper.

$$\begin{aligned}
&\max_{\{T_m\}_{m=1}^{M}} \quad \log(\eta_1)+\log(\eta_2)\\
&s.t.\\
&1+SINR_1 \geq \eta_1\\
&1+SINR_E \leq 1/\eta_2\\
&SINR_m \geq \mu_m\\
&\sum_{m=1}^{M}\left\|T_m\right\| \leq P_M
\end{aligned} \tag{4}$$

In order to derive conveniently, the power of all the noise is 1, according to the optimization problem, that is (4), it can be transformed into

$$\begin{aligned}
&\max_{\{T_m\}_{m=1}^{M}} \quad \eta_1\eta_2\\
&\sum_{m=1}^{M}\left\|T_m\right\| \leq P_M\\
&1+\sum_{m=2}^{M}T_m^H \boldsymbol{H}_1 T_m \leq \frac{T_1^H \boldsymbol{H}_1 T_1}{\mu_1 - 1}\\
&1+\sum_{m=1}^{M}T_m^H \boldsymbol{H}_E T_m \leq \frac{1+\sum_{m=1}^{M}T_m^H \boldsymbol{H}_E T_m}{\mu_2}
\end{aligned} \tag{5}$$

According to this formula, the problem can be formulated as a SOCP problem. It is a non-convex optimization problem. Therefore, it is necessary to make a first order Taylor series approximation. Its iterative algorithm is:

1) Initialization T_m , μ_1, η_1 and η_2,

2) Repeated iteration with initialization values T_m , μ_1, η_1 and η_2, solving the problem (5), eventually get the optimal value values T_m , μ_1, η_1 and η_2,

3) Setting reasonable threshold, so that the algorithm will convergence, which can save the computation and time,

4) Finally, getting the precoding T_m .

4. Simulation Results and Analysis

According to [16], Tab.1 is the parameters setting.

Tab.1: Downlink Massive MIMO system parameters

Parameter	Value
Factor ϕ	1
Path loss exponent α	3.7
shadow fading standard deviation σ_{sh}	8
Noise power σ^2	$-104\left(dBm\,gHz^{-1}\right)$
Power amplifier efficiency η	0.5
Users consume power P_E	$0.01\,mW$
Each antenna circuit consume power P_C	$0.1\times10^{-3}\,mW$
Basic power consumption of BS P_0	$0.2\,mW$

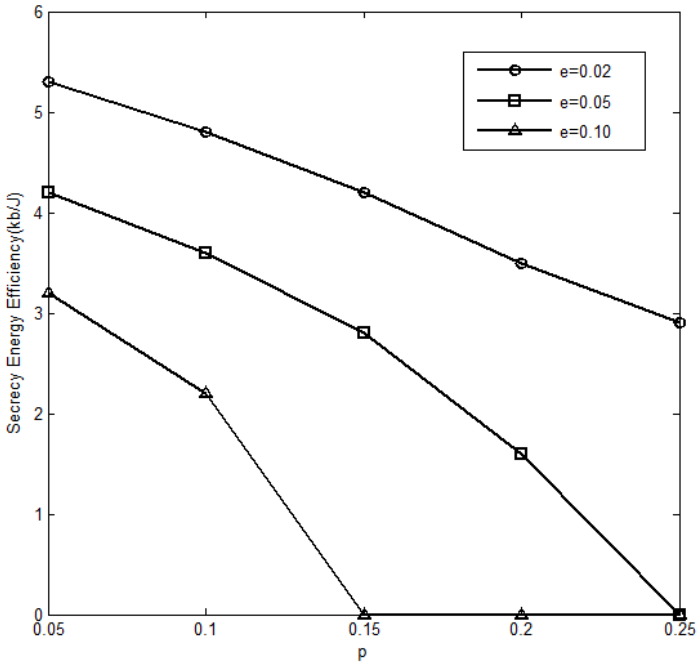

Figure 2. Secrecy Energy Efficiency

Figure 2 from the point of view of the secrecy energy efficiency, which can be seen, when η_1 is smaller, the secrecy energy efficiency is higher, and is bigger, the secrecy energy efficiency is lower, and with the increase of η_2, the secrecy energy efficiency decreases. It can be seen that the energy efficiency of the secrecy capacity is at the expense of the total transmission efficiency, as follow-up work to be discussed for this problem.

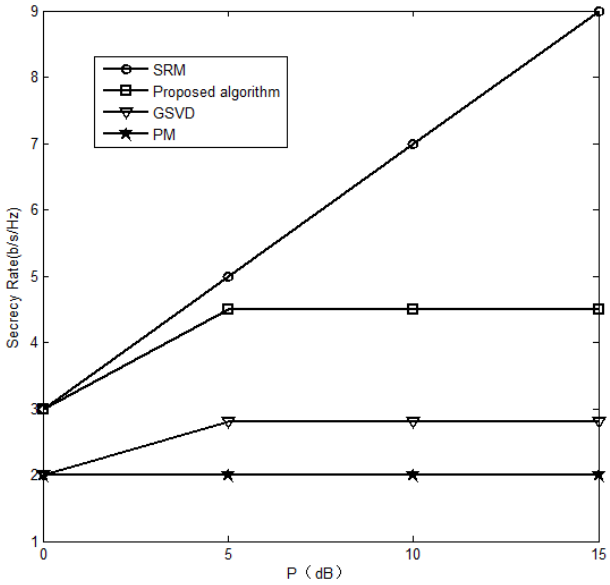

Figure 3. Maximum Mutual Information with the Transmission Power Conversion

From Figure 3, we can see that the proposed scheme has higher efficiency in the existing scheme, and it has the high secrecy capacity efficiency, which is the possibility that the numerical solution can be more close to the optimal solution, the price is the high computational complexity, in the other three schemes, the optimal solution is closed, but its secrecy capacity will not increase with transmission power.

5. Conclusion

In this paper, according to the topological structure of the fifth generation mobile communication, that is the simplest multi-user structure, with the large antenna deployment, considering the secrecy transmission energy utilization rate and the maximum secrecy capacity of the system, and the optimized solution of the system is obtained by iteration, according to the optimized solution, from the figure we can see that the proposed scheme has a great advantage in the secrecy capacity than other schemes.

Acknowledgments

This work is supported by the research projects of Henan province under Grant 162102210395, the science and technology innovation team in Colleges and universities of Henan province plan (17IRTSTHN009).

References

[1] R. Zhang, "Cooperative Multi-Cell Block Diagonalization with Per-Base-Station Power Constraints," IEEE Journal on selected areas in communications, vol. 28, no. 9, **(2010)**.
[2] ChrisT.K.Ng and Howard Huang, "Linear Precoding in Cooperative MIMO Cellular Networks with Limited Coordination Clusters," IEEE Journal on selected areas in communications, vol. 28, no. 9, **(2010)**.
[3] S. Feng, M. M. Wang, W. Yaxi, "An Efficient Power Allocation Scheme for Leakage-Based Precoding in Multi-cell Multiuser MIMO Downlink" IEEE communications letters, vol.15,no.10, **(2011)**, pp. 1053-1055.
[4] A. Papadogiannis, , Hans Jørgen Bang, David Gesbert, and Eric Hardouin, "Efficient Selective Feedback Design for Multicell Cooperative Networks," IEEE Transactions on vehicular technology, vol. 60, **(2011)**, no. 1.
[5] A. L. Anderson, , James R. Zeidler, Fellow, and Michael A. Jensen, "Reduced-Feedback Linear Precoding with Stable Performance for the Time-Varying MIMO Broadcast Channel" IEEE Journal on selected areas in communications, vol. 26, **(2010)**, no. 8.
[6] C.-C. Li and Yuan-Pei Lin, "On the Duality of MIMO Transceiver Designs With Bit Allocation," IEEE Transactions on signal processing, vol. 59, no. 8, **(2011)**, pp.3775-3787.
[7] H. Zhang, Neelesh B. Mehta, " Andreas F. Molisch, Asynchronous Interference Mitigation in Cooperative Base Station Systems," IEEE Transactions On wireless communications, vol.58,no.10, **(2008)**, pp.5233-5245.
[8] Z. Shen, Papasakellariou A., Montojo J. Overview of 3GPP LTE-advanced carrier aggregation for 4G wireless communications. IEEE Communications Magazine, vol. 50, no. 2, **(2012)**, pp. 122-130.
[9] G. Yuan, Xiang Zhang, Wenbo Wang, Yang Yang. Carrier aggregation for LTE-advanced mobile communication systems. IEEE Communications Magazine, vol. 48, no. 2, **(2010)**, pp. 88-93.
[10] K.I. Pedersen, Frederiksen F., Rosa C. Nguyen, EL; Garcia, L.G.U.; Yuanye Wang. Carrieraggregation for LTE-advanced; functionality and performance aspects. IEEE Communications Magazine, vol. 49, no. 6, **(2011)**, pp. 89-95.
[11] O. Onireti, Heliot F.,Imran M.A, "On the Energy Efficiency-Spectral Efficiency Trade-Off in the Uplink of CoMP System", IEEE Transactions on Wireless Communications, vol. 11, no. 2, **(2012)**, pp. 556-561.
[12] V. S. Annapureddy,El Gamal A. Veeravalli V. V. Degrees of Freedom of Interference Channels With CoMP Transmission and Reception. IEEE Transactions on Information Theory, vol. 58, no. 9, **(2012)**, pp. 5740-5760.
[13] U. Jang, Hyukmin Son, Jongrok Park, Sanghoon Lee. CoMP-CSB for ICI Nulling with User Selection. IEEE Transactions on Wireless Communications, vol. 10, no. 9, **(2011)**, pp. 2982-2993.
[14] F. Kaltenberger,Kountouris M.,Gesbert D., Knopp R, "On the trade-off between feedback and capacity in measured MU-MIMO channels", IEEE Transactions on Wireless Communications, vol. 8, no. 9, **(2009)**, pp. 4866-4875.
[15] J. Mao, Jinchun Gao, Yuanan Liu, Gang Xie. Simplified Semi-Orthogonal UserSelection for MU-MIMO Systems with ZFBF. IEEE Wireless Communications Letters, vol. 1, no. 1, **(2012)**, pp. 42-45.

Authors

Zhou Wen-gang received the master's degree at North China University of Technology, BeiJing, China,in 2007. He is currently an Associate Professor with School of Information Science, his current research interests include the analysis and design of Intelligent Algorithm、Cloud Computing.

Li Jing received the M.S. degree in Computer application and technology from Inner Mongolia normal university in 2008. She is a lecturer at Zhoukou Normal University. Her research interests include service computing, image processing, etc

Guo Hui-Ling received B.Eng Degree in computer application from HeNan University and the M.Eng Degree in computer science and technology from Guilin University of Technology in 2002 and 2009 respectively, She is currently researching on image processing and computer network.