Information Security Technology of Wireless Communication Physical Layer Based on Airspace Technology

Lan Jiang

1Wuhan Polytechnic, Hubei, China, 430074

Abstract: Due to the characteristics of the broadcast function of the wireless communication network, the problem of information security has become very serious. And because the traditional upper-layer encryption technology is accompanied by the advancement of computer technology and eavesdropping technology, it has become more and more far from being able to meet the needs of modern society for information security. The multi-antenna beamforming technology in the airspace technology is a technology that can effectively increase the strength of the legal signal and suppress the eavesdropping signal. Therefore, it has become the most important technology in the physical layer security of our country and deserves our attention. Therefore, this article aims to study the wireless communication physical layer information security technology based on airspace technology. Based on the analysis of the basic theory of physical layer security, the current status of physical layer security research and the airspace physical layer security technology, the artificial noise auxiliary technology is promoted and applied to security identification. Taking the speed of maximizing the safe frequency spectrum as the design goal, an algorithm for joint optimization of information noise beam and artificial noise beam is proposed. The simulation results show that this algorithm can effectively improve the security and stability of the system, and it can also solve the eavesdropping problem.

1 Introduction

With the progress and rapid development of my country's wireless communication technology, people's daily life and work methods have been significantly improved, and a wireless communication network that can be accessed at any time has been basically completed [1-2]. However, the transmission and broadcasting nature of wireless channels makes the existing information security issues far higher than the security risks of cable TV networks [3-4]. The simplicity and convenience of wireless communication networks make today's society increasingly dependent on it, so it has established the necessity and importance of ensuring its communication security. With modern cryptography as the main theoretical basis, most of the methods that can achieve information security in the past are directly using upper-level passwords for encryption [5-6].

Traditionally, it is generally believed that one of the main goals of the upper-level secret key encryption algorithm is to ensure the transmission and security of data and information in the wireless and network, although this encryption algorithm does have better security and efficiency. However, encryption algorithms usually make the calculation data large and complex. With the continuous development and improvement of the calculation data processing speed of modern computers, coupled with many problems such as the existence of the secret key, the encryption algorithm is no longer capable. Fully meet the higher requirements of modern society for information security [7-8]. The security technology of the physical layer is to use a random feature of the wireless channel itself to realize the safe and reliable transmission of information. Because it is not a way to effectively prevent eavesdroppers from stealing information by using a neural key, but a way to fundamentally ensure the security of the information transmitted by using the inherent characteristics of the physical layer such as the decline of the neural key. Therefore, even if the current electronic computer technology has developed more mature, it will not let people fall into being cracked by the neural key, so its reliability requirements are higher, and the application prospects are broader [9-10].

Based on the analysis of the basic theory of physical layer security, the status quo of physical layer security research and the airspace physical layer security technology, this paper promotes the application of artificial noise assisting technology to wireless networks with safe recognition and recognition. Taking the speed of maximizing the safe frequency spectrum as the design goal, an algorithm for joint optimization of information noise beam and artificial noise beam is proposed. The simulation results show that this algorithm can effectively improve the security and stability of the system, and it can also solve the eavesdropping problem.
2 Research on Information Security Technology of Wireless Communication Physical Layer Based on Airspace Technology

2.1 The Basic Theory of Physical Layer Security

(1) Information security

From the perspective of information theory, since both the original message M and the code word X can be regarded as random variables, the security of the confidential system can be quantified based on the uncertainty of the information stolen by the illegal eavesdropping end [11-12]. Specifically, it is possible to reflect the security of the communication system according to the conditional entropy of the original message M sent under the condition of the known code word X, that is, the suspicion degree H(M|X) of the illegal eavesdropping terminal. When the suspicion degree H(M/X) of the message X stolen by the illegal eavesdropping terminal is equal to the uncertainty of the original message M, that is, H(M/X) = H(M), then the code word X is the same as the original message. M is statistically independent. At this time, the illegal eavesdropping terminal cannot extract any information about the original message M from the stolen code word X, so that the security model can be guaranteed to have complete security. Therefore, in order to ensure the complete security of the confidential model, the uncertainty of the encryption key K must be greater than or equal to the uncertainty of the original message, that is, H(K)≥H(M). From the perspective of the encryption algorithm, it can be ensured that every bit of information in the original message M is assigned at least one bit of encryption key, that is, unconditional and complete security can be ensured through one-time encryption, which is the security of information theory.

(2) Physical layer security

The physical layer security based on the perspective of information theory uses the physical layer characteristics of the wireless channel to achieve secure communication, rather than the complexity of the encryption algorithm to ensure communication security, and another advantage of the physical layer security technology is that it can accurately calculate leaks. This indicator can be used as an important indicator to measure the security performance of the system for the amount of information on the illegal eavesdropping terminal. Theoretically, the physical layer security technology can approach a perfect secure communication system to the limit by using a longer codeword, so the physical layer security is suitable for wireless communication scenarios.

2.2 Current Status of Physical Layer Security Research

(1) Multi-antenna eavesdropping channel

In recent years, with the development of multi-antenna technology, physical layer security technology has also obtained a broad space for development. On the one hand, multi-antenna technology provides more channel resources, making it possible to increase the difference between legal channels and eavesdropping channels in the airspace. On the other hand, multi-antenna technology can provide a richer variety of signal processing technologies, which can effectively improve the signal-to-noise ratio of the received signal at the legal receiving end while deteriorating the signal-to-noise ratio of the received signal at the illegal eavesdropping end.

(2) Relay eavesdropping channel

In wireless communication networks, channel fading will seriously affect the performance of the communication system. Channel fading will weaken the received signal at the receiving end, which not only affects the transmission distance of the signal, but also affects the normal demodulation of the received signal at the receiving end. With the development of multi-antenna technology, the cooperative relay technology through the construction of virtual MIMO achieves the function of resisting channel fading by providing spatial diversity of multiple antennas.

1) AF relay

In the AF relay forwarding process, after the relay node receives the signal sent by the sender, it does not perform any extra processing on it, but directly amplifies the received signal containing noise, and then forwards it to the legal receiving end. Since the information received by the relay node contains both original useful information and noise information, while amplifying the original useful information, the channel noise in the first transmission time slot will also be amplified accordingly, so this increases legal reception. The difficulty of demodulating the received signal at the end.

2) DF relay

In the DF relay and forwarding process, after the relay node receives the signal from the sending end, it will demodulate and encode the received signal to obtain the original signal, and then re-modulate and encode it to the legal receiving end.

3) CC relay

CC coded cooperative relay is a relay method that combines DF relay and channel coding. That is, the message sent to other users is added to the original DF relay to decode and forward the message, so that it is legal to understand the CC coding strategy. For the receiving end, it can extract its own information, but for the illegal eavesdropping end that does not understand the strategy, it will suffer more interference and limit its ability to steal information.

2.3 Airspace Physical Layer Security Technology

(1) Directional antenna technology.

The directional antenna is a kind of antenna that must have greater transmission and control power in a special direction, and has the good performance of strong signal transmission ability and wide coverage. Adjusting the main beam direction and null direction of the directional
antenna can reduce the influence of the interference source on the transmission signal to a certain extent, and achieve the goal of resisting congestion interference in the wireless communication network. Compared with the omnidirectional antenna system, the directional antenna has a great improvement in both its consumption and efficiency. At the same time, due to its higher equivalent power, the directional antenna can also make it have better shielding properties, which can promote data and information in communication are relatively safe. With the continuous maturity of directional antenna technology, its product quality and performance have been greatly improved and improved, and there are more and more application fields, but its cost and cost are relatively high. The advantages and characteristics of complex wireless communication conditions have brought certain challenges to directional antenna technology, which requires constant exploration and progress.

(2) Beamforming technology

Beamforming technology mainly refers to a directional antenna technology with movement directionality and variable frequency. Beamforming technology mainly refers to a directional antenna that uses multiple directional antenna arrays and effectively allocates various areas and other factors to achieve directional antennas. Compared with the configuration of directional antenna technology, beamforming technology requires higher energy in signal radiation and a wider transmission range. However, due to the use of multi-antenna configuration, its energy consumption is also greatly improved. The design requirements have become more stringent, and the applicable space range has become more restrictive. At present, reducing the energy efficiency, power consumption and resource utilization cost of beamforming technology has been generally regarded as a key point to promote the development and progress of space science and technology in my country.

(3) Random parameter technology.

Random parameter technology can smoothly analyze and demodulate various transmitted signals from the customer to the cable through the legal parameter receiver installed in advance for the customer and the user. Although this random parameter control technology has a good effect and effect in preventing eavesdropping or blocking interception when preventing attacks, the power consumption and hardware costs generated by it also increase, and it will cause huge signal loss. And the waste of resources, so that its further development and application difficulties are generally encountered, and we still need our relevant technical personnel to further improve and innovate.

(4) Artificial noise reduction technology

Artificial noise technology is also one of the representative methods in the physical layer security transmission. Its basic idea is to add random noise orthogonal to the legal channel into the transmitted signal to reduce the quality of the eavesdropping party's received signal without disturbing the reception of the legal receiving end. Here, "orthogonal" can be orthogonal in the mathematical sense or in the physical sense. It mainly includes the following three methods:

1) Zero-forcing artificial noise method. The transmitting end uses multiple antennas to design noise beams based on the CSI of the channel from the legal receiving end to achieve the noise signal spreading across the entire transmission space but forming a null at the legal receiving end, effectively deteriorating eavesdropping on the channel capacity while avoiding the influence of noise on the legal receiving end;

2) Noise beamforming method, under the condition that the CSI of the channel from the sender to the eavesdropper is known, the artificial noise beam is designed to be aimed at the eavesdropper, combined with the confidential signal beam aimed at the legal receiving end, to maximize the security capacity of the system;

3) The known signal interference method uses the physical orthogonal noise signal to ensure safe communication. The sending end sends a signal that is known by the legal receiving node but unknown to the eavesdropping party as interference, and the legal receiving end can eliminate this part of the interference by itself after receiving the signal.

3 Experiment

3.1 System Model

In a security cognitive wireless network, the transmission of information needs to meet two conditions at the same time: First, in order to ensure the normal communication of the main network, the interference caused by the secondary network to the main network must be less than a certain threshold; secondly, in order to ensure the security of the information transmitted on the secondary network, the information that the eavesdropping terminal can obtain must be controllable. To this end, we introduce artificial noise assistance technology into the cognitive wireless network, that is, add artificial noise to the transmitted signal at the transmitter, and jointly optimize the design of the information signal beam and the artificial noise beam to ensure the communication security of the cognitive network. Then, the transmission signal of the secondary user's transmitter can be expressed as:

\[ x = w_1s_1 + w_2s_2 \]  

In the formula, \( s_1 \) and \( s_2 \) respectively represent the information signal and artificial noise. They all obey the Gaussian distribution of zero mean unit variance, and the other

These are independent of each other, and \( w_1 \) and \( w_2 \) are their corresponding transmit beams. After channel transmission, the legal receiving end and the eavesdropping end are connected

The received signals are:

\[ y_B = h_{AB}^Hw_1s_1 + h_{AB}^Hw_2s_2 + n_B \]  

And

\[ y_B = h_{AB}^Hw_1s_1 + h_{AB}^Hw_2s_2 + n_B \]  

In addition, due to the broadcasting characteristics of the wireless channel, the primary user will also receive the transmitted signal \( x \), and the interference power caused by this signal to the primary user can be
calculated as: \( I = |h_{AB}^Hw_1|^2 + |h_{AP}^Hw_2|^2 \). The premise that the secondary user can be allowed to access the primary network is that the interference it causes to the primary user must be less than a certain threshold. Next, our job is to maximize the safe rate by jointly designing the information signal beam \( w_1 \) and the artificial noise beam \( w_2 \) to realize the communication security of the cognitive network under the two constraints of interference temperature and transmission power.

### 3.2 Improved Beam Design

Due to the high computational complexity of traditional beam design algorithms, in order to reduce the complexity, this paper proposes an improved beam design algorithm.

If artificial noise is only transmitted in the orthogonal space of the legal channel, then it will not cause any interference to the legal receiving end. In this case, the beam design can be expressed as the following optimization problem:

\[
\text{OP2.6: } \max_{w_1, w_2} \mathbb{E} \left[ 1 + |h_{AB}^Hw_1|^2 \right] - \mathbb{E} \left[ 1 + |h_{AP}^Hw_2|^2 \right] + 1 + |h_{AP}^Hw_1|^2 \right] \frac{1}{|h_{AP}^Hw_2|^2 + 1}\]

subject to C2.1, C2.2, C2.15: \( h_{AB}^Hw_1 = 0 \)

Let \( w_2 = \prod h_{AB}^Hw_3 \), where \( \prod h_{AB}^H = I - h_{AB}^H(h_{AB}^Hh_{AB})^{-1}h_{AB}^H \) is the orthogonal complement projection of \( h_{AB}^H \). Therefore, the constraint C2.15 can be eliminated to obtain the following optimization problem:

\[
\text{OP2.7} = \max_{w_1, w_2} \mathbb{E} \left[ \text{tr}(H_{AB}^Hw_1) \right]
\]

subject to C2.16: \( \text{tr}(H_{AB}^Hw_1) + \text{tr}(H_{AP}^Hw_3) \leq I_{\text{max}} \)

C2.17: \( \text{tr}(w_2) + \text{tr}\left( (\prod h_{AB}^H)^H \prod h_{AB}^H w_3 \right) \leq P_{\text{max}} \)

C2.18: \( \text{rank}(W_i) \leq 1, i \in \{1, 3\} \)

First ignore the rank constraint C2.18, then OP2.7 is a convex optimization problem, which can be solved directly by CVX. Suppose that the OP2.7 solutions when the constraint C2.18 is ignored are \( W_1^* \) and \( W_3^* \). If their ranks are both 1, then \( W_1^* \) and \( W_3^* \) can be obtained by decomposition, otherwise \( W_1^* \) and \( W_3^* \) can be obtained by approximation. Finally, the optimal beam by comparing different situations.

### 4 Discussion

In order to test the effectiveness and accuracy of the proposed improved beam design algorithm, we provide simulation results based on the following scenarios: In the three MISO channels in the system, \( h_{AB}, h_{AP} \) and \( h_{AB} \) all obey the Gaussian independent distribution. The background noise is the same. In order to simplify the calculation, the path loss from the secondary user's transmitter to the primary user and destination receiver is normalized. Some performance comparisons between traditional beam design and improved beam design are given below.

![Figure 1. Comparison of safe rates with different numbers of transmitting antennas](image-url)

As can be seen from Figure 1, the more the number of transmitting antennas, the better the security rate performance of the system. However, with the increase in the number of transmitting antennas, the improvement speed of the safety rate performance becomes slower and slower, rather than steadily increasing at a fixed speed. This shows that when the number of antennas is small, it can be obtained by increasing the number of antennas. Great performance improvement, but when the number of antennas is large enough, improving the system performance by increasing the number of antennas will not be able to obtain a very ideal effect. In addition, it can be found that as the number of antennas increases, the performance of the improved beam design algorithm...
is gradually approaching the traditional beam design algorithm, and even the same performance as the traditional beam design algorithm. Therefore, when the number of antennas is greater than 6, in order to obtain the maximum safe rate, the improved beam design algorithm may be a better choice because of its lower algorithm complexity.

| $I_{\text{max}}$ | Traditional algorithm | Improved algorithm |
|-----------------|-----------------------|---------------------|
| 10              | 6.18                  | 5.49                |
| 20              | 6.49                  | 5.99                |
| 30              | 6.65                  | 6.25                |
| 40              | 6.77                  | 6.41                |
| 50              | 6.86                  | 6.57                |
| 60              | 6.92                  | 6.64                |
| 70              | 6.98                  | 6.71                |

As shown in Table 1 and Figure 2, as the interference power limit $I_{\text{max}}$ increases, the safety rate also increases. This is because when the interference limit conditions become loose, the transmitter can use a larger transmit power to send information. But when $I_{\text{max}}$ is large enough, the safety rate will reach a stable value instead of continuing to increase. At this time, the safety awareness network is equivalent to an ordinary artificial noise-assisted multi-antenna safety network, because at this time the interference power limit is no restriction on the system.

5 Conclusions

With the further development of wireless network technology, mobile smart devices have become an inseparable and important part of people's lives. However, wireless network communication is extremely vulnerable to eavesdropping, interference and congestion by criminals, which seriously threatens the information security of users. In recent years, wireless communication physical layer information security technology has become an important protection method for wireless communication security, and airspace technology has a very significant effect on the protection of wireless networks.

References

1. Zhang Z, Long K, Vasilakos A V, et al. Full-Duplex Wireless Communications: Challenges, Solutions, and Future Research Directions[J]. Proceedings of the IEEE, 2016, 104(7):1369-1409.
2. Kuang Y, Zhu M. Characterisation of a knee-joint energy harvester powering a wireless communication sensing node[J]. Smart Materials & Structures, 2016, 25(5):055013.
3. Gan Q, Yu S, Li C, et al. Design and ARM-embedded implementation of a chaotic map-based multicast scheme for multiuser speech wireless communication[J]. International Journal of Circuit Theory & Applications, 2016, 45(11):1849-1872.
4. Bennis M, Debbah M, Poor H V. Ultrareliable and Low-Latency Wireless Communication: Tail, Risk, and Scale[J]. Proceedings of the IEEE, 2018, 106(10):1834-1853.
5. Wang H M, Zheng T X, Yuan J, et al. Physical Layer Security in Heterogeneous Cellular Networks[J]. IEEE Transactions on Communications, 2016, 64(3):1204-1219.
6. Quyen N X, Duong T Q, Vo N S, et al. Chaotic Direct-Sequence Spread-Spectrum with Variable Symbol Period: A Technique for Enhancing Physical Layer Security [J]. Computer Networks, 2016, 109(Part 1):4-12.

7. Hayder A H, Gayan B, Rafael S. Artificial Noise-Aided Physical Layer Security in Underlay Cognitive Massive MIMO Systems with Pilot Contamination [J]. Entropy, 2017, 19(7):349.

8. Hajomer A, Yang X, Hu W. Chaotic Walsh-Hadamard Transform for Physical Layer Security in OFDM-PON [J]. IEEE Photonics Technology Letters, 2017, 29(6):527-530.

9. Liu J, Liu Z, Yong Z, et al. Cooperative Jammer Placement for Physical Layer Security Enhancement [J]. IEEE Network the Magazine of Global Internetworking, 2016, 30(6):56-61.

10. Salem, Abdelhamid, Hamdi, et al. Physical Layer Security With RF Energy Harvesting in AF Multi-Antenna Relaying Networks [J]. IEEE Transactions on Communications, 2016, 64(7):3025-3038.

11. Sohrabi F, Wei Y. Hybrid Digital and Analog Beamforming Design for Large-Scale Antenna Arrays [J]. IEEE Journal of Selected Topics in Signal Processing, 2016, 10(3):501-513.

12. Chen Y, Wang F, Wan J, et al. MASS-RAB: Robust adaptive beamforming for general-rank signal models via matched spatial spectrum processing [J]. Applied Acoustics, 2016, 111(OCT.): 205-213.