Research on Physical Layer Encryption Technology of HST 5G communication system with spatial permutation modulation

Lingzhi Yi
Xiangtan University
Peng Jiang (jp_462600@163.com)
Xiangtan University https://orcid.org/0000-0001-7499-1001
Huan Liao
Xiangtan University
Chaodong Fan
Xiangtan University
Wang Li
The State Key Laboratory of Heavy Duty AC Drive Electric Locomotive Systems Integration,Zhuzhou,Hunan,China
Xiaodong Feng
Xiangtan University

Research Article

Keywords: 5G-R scenarios, Physical layer encryption, Massive MIMO, HASPM, HST differentiated communication system

Posted Date: May 28th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-188825/v1

Research on Physical Layer Encryption Technology of HST 5G communication system with spatial permutation modulation

Lingzhi YI,[1,2] Peng JIANG,[1] Huan LIAO,[1] Chaodong FAN,[1,2] Wang LI,[3] and Xiaodong FENG[1]

[1] College of Automation and electronic information, Xiangtan University. Hunan Province Engineering Research Center for Multi-Energy Collaborative Control Technology, Xiangtan, Hunan 411105, China

[2] Hunan Province Cooperative Innovation Center for Wind Power Equipment and Energy Conversion, Xiangtan, Hunan 411100, China

[3] The State Key Laboratory of Heavy Duty AC Drive Electric Locomotive Systems Integration, 412001, China

Correspondence should be addressed to Peng JIANG; jp_462600@163.com

Abstract

In high-speed train (HST) communication, the application of 5G technology is of great importance. The massive multi-input multi-output (massive MIMO) technology in HST communication has advantages, but there are problems of inter-channel interference and multiple antennas synchronization. Spatial modulation has been widely used as a technology to solve this problem. In order to ensure the security of the HST wireless communication system, a hyperchaotic antenna-index spatial permutation modulation (HASPM) is proposed by combining chaos theory on the basis of spatial modulation technology. Aiming at the problem of reduced spectrum efficiency in traditional encryption algorithms due to pre-shared keys, channel information and noise interference, the proposed HASPM physical layer encryption scheme can improve above shortcomings on the basis of secure communication. The multipath fading effect is reduced, the bit error rate (BER) performance is greatly improved, and the system security and reliability are thus guaranteed. The evaluation results of calculation analysis and simulation on the scheme verified the feasibility and effectiveness of the proposed scheme.

Index Terms—5G-R scenarios, Physical layer encryption, Massive MIMO, HASPM, HST differentiated communication system

1 Introduction

HST communication is one of the most important usage scenarios of 5G wireless communication, which defines the physical layer of the mobile communication network beyond the fourth-generation technology [1]. With the rapid development of HST and the continuous improvement of speed, the wireless transmission of train operation control signals with low delay and high reliability has become more and more important. 5G-R is based on 5G mobile communication and develops specific applications for railway scenes on dedicated frequency bands for railway communication [2]. Table 1 shows the comparison between 5G-R and existing railway communication methods. GSM-R is limited by the limitations of 2G technology narrowband communication, and its transmission rate and delay performance are unsatisfactory [3]. LTE-R uses two physical layer technologies, orthogonal frequency division multiplexing (OFDM) and multiple input multiple output (MIMO). OFDM can

Table 1: Comparison of 5G-R and existing railway communication.

	GSM-R	LTE-R	5G-R
frequency	150MHz,450MHz	450MHz	900MHz
rate	9.6kbits/s	100Mb/s	1Gb/s
dely	400ms	<100ms	1-5ms
network architecture	BTS-BSC	Full IP	SBA
specific techniques	GSMK, TDMA	OFDM, MIMO	CP-OFDM, massive MIMO, Network Slicing

independently process signals in each sub-channel to eliminate interference to the maximum extent. MIMO can generate multiple parallel independent channels to increase the data transmission rate of LTE-R without increasing bandwidth [4]. However, neither of these two methods can provide massive user connections, extensive signal coverage, and real-time video surveillance technologies to meet the requirements of intelligent railway dispatching and safety assurance. In addition to its excellent rate and delay performance, 5G-R can also use cyclic prefix orthogonal frequency division multiplexing (CP-OFDM) for modulation, use massive MIMO technology to increase the number of channels, and use network slicing to meet different scenarios Differentiated communication requirements [5]. Massive MIMO and millimeter wave technologies have been considered for application in HST communication systems due to their technical prospects.

The Massive MIMO base station antenna array is equipped with an order of magnitude more antennas than existing systems, so it has all the advantages of traditional multi-input and multi-output systems, as well as simpler precoding and detection schemes [6]. However, the openness of wireless communications makes the system more vulnerable to attacks such as jamming and eavesdropping. In the traditional communication system, eavesdroppers can easily receive the upper ciphertext, and can use a large number of ciphertext to obtain the key data that determines the system security [7]. Physical layer encryption uses the physical characteristics of wireless communication system to achieve secure communication, which can greatly improve the security level of the system.

A classic three-terminal eavesdropping model (Alice-Bob-Eve model) for physical layer security was proposed in [8], including a transmitter (Alice), a legitimate receiver (Bob) and an eavesdropper (Eve). Massive MIMO can use multiple transmitting antennas to enhance the confidentiality of communication system, so its combination with communication encryption is natural [9]. The concepts of eavesdropping channel and confidentiality have promoted the research of physical layer security of wireless communication systems [10,11]. There have been a number of phased progress in the study of wireless system security performance [12-16]. Literature [17] and [18] gave a general representation method for the channel security capability of multi-antenna eavesdropping under the constraint of the input matrix. A suboptimal beamforming scheme based on Markov bound was proposed in [19]. In this scheme, transmitter must know the prior knowledge of the receiver channel. The physical layer security of the massive MIMO system is configured when the eavesdropper has a large number of antennas in [20]. This scheme requires a minimum level of noise. To improve the physical layer security of the channel under the classical eavesdropping model, transmission antenna selection scheme is analyzed in [21]. The security of the physical layer for new generation of wireless communication systems was further discussed in

[22]. In a secure multi-antenna system, sends noise to the empty space of the receiving end to confuse Eve, but this method does not guarantee the absolute security of communication channel.

This article proposes a physical layer encryption scheme for Massive MIMO system based on spatial permutation modulation (SPM). A space-modulated multi-antenna transmission scheme is proposed in [23] The activation state of the signal transmitting antenna creates a new modulation dimension. To break through the limitation of the number of transmitting antennas in traditional SM scheme, a joint mapping spatial modulation scheme was proposed in [24] and [25]. MIMO systems show better confidentiality than single-antenna systems in [26]. SPM scheme was proposed in [27], which modulates data bits into permutation vectors, and the antennas are activated according to the vectors in continuous time. This article applies SPM technology to wireless communication encryption. In order to further improve the security, chaos theory is applied to key extraction, a key generation algorithm is designed, and keys are used to protect antennas combination and mapping modes antenna combination and mapping modes (ACMM) and interfere with spatial constellation. Finally, HASPM method is proposed for information encryption and modulation.

The main contributions of the paper are as follows.

1) A new HASPM is proposed for spatial modulation scheme for massive MIMO wireless communication. This scheme uses the antenna sequence generated by hyperchaotic mapping to encrypt the spatial modulation information.
2) Using SPM technology, compared with traditional physical layer security solutions, the system can be designed with mature discrete mathematics domain knowledge, and it has high compatibility, reliability and flexibility.
3) The chaos theory is applied to key generation, and a new key generation algorithm is proposed to further improve the security of the physical layer encryption system.
4) Carry out theoretical research on the proposed scheme, analyze its complexity, randomness and reliability, and perform simulation to illustrate the advantages of the scheme.

The rest of the paper is organized as follows. The second section introduces the 5G-R scenario massive MIMO technology and SPM model, and briefly describes the main ideas of the proposed scheme. The third section introduces the HASPM scheme in detail from three aspects: key generation, spatial modulation and signal reception. The fourth section gives the superiority analysis and simulation results. The fifth section summarizes the paper.

2 5G-R scenarios and SPM scheme

2.1 5G-R scenarios

As shown in the figure1, according to different communication scenarios, the railway wireless communication system can be divided into four types: T2I communication, T2T communication, intra-carriage communication and intra-station communication. T2I communication system and T2T communication system play a decisive role in train safety, so we discuss these two communication scenarios.

For T2I communication, real-time image and video services are urgently needed in the next generation HST wireless communication system, so it is necessary to discuss the application of 5G in T2I communication. As a heterogeneous integrated network, 5G can realize the backward compatibility of wireless communication technology, so it can support all existing railway services and lay the foundation for the practical application of 5G-R. Compared with traditional MIMO, massive MIMO can provide more degrees of freedom wireless

Table 2: HST communication technology comparison.

	Advantages	Drawbacks
Satellite	Existing infrastructure	Limited throughput, Obstacles influence
LTE/5G	Upgradable Infrastructure，Low cost	Coverage problem
WiFi	Average throughput, Seamless Communications	High costs
Radio on Fiber	Low cost base station, Seamless Communications	High costs
Optical Wireless	High throughput，Seamless Communications	Heavy infrastructure Atmosphere influence High costs

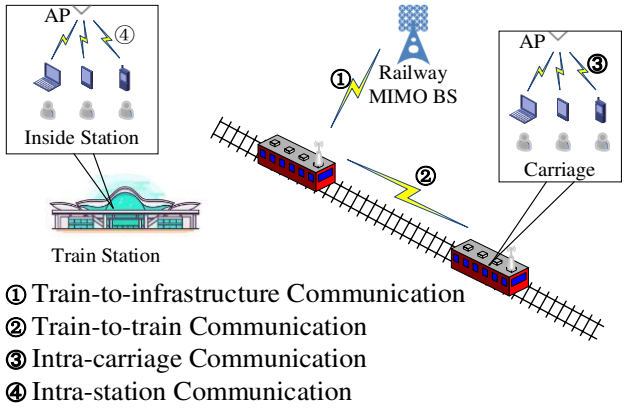


Figure 1: MIMO railway wireless communication.

The railway wireless communication system consists of train-to-infrastructure communication (T2I communication), train-to-train communication (T2T communication), intra-carriage communication and intra-station communication.

channel and support higher data rate [28]. Therefore, it can also significantly improve spectrum efficiency and energy efficiency in addition to the advantages of traditional MIMO [29], and can simplify the access control layer design and further reduce the system delay, it can be seen that massive MIMO can significantly improve the transmission performance of 5G-R. 5G-R will provide emerging railway services beyond existing railway technologies, such as real-time video surveillance and train multimedia dispatch. HST is considered as a typical application scenario for 5G due to its short time delay, real-time video monitoring and a large number of sensing requirements for railway internet of things sensors.

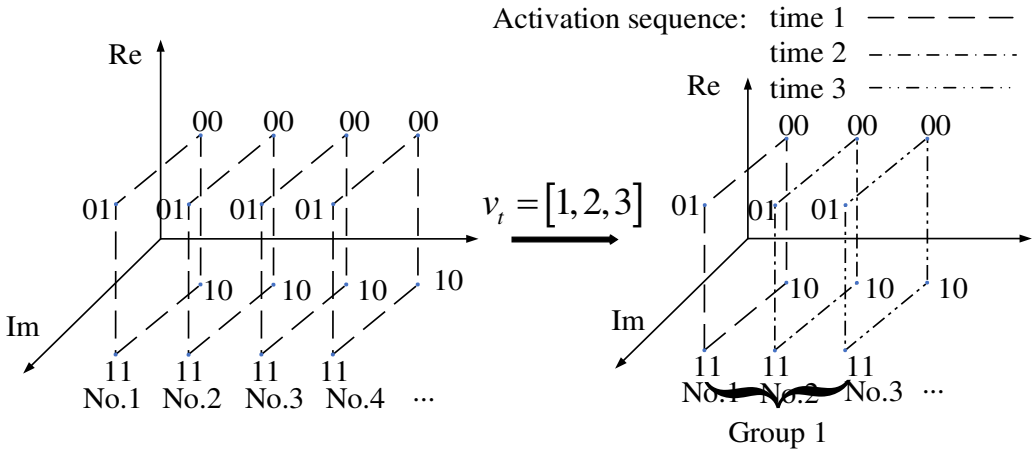
T2T communication can provide emergency communication between trains when the T2I communication network is interrupted. As the train speed continues to increase and the distance between the workshops continues to decrease, the available braking time of the train is greatly reduced. Therefore, there are higher requirements for transmission rate and network delay. 5G applies network layering technology, allowing devices to communicate directly without involving infrastructure. Network layering technology for 5G applications allows devices to communicate directly without involving infrastructure. The characteristics of high speed and low latency enable it to meet the requirements of T2T communication.

In order to intuitively show the advantages and development prospects of 5G-R scenarios, compare it with the existing HST communication technology in table 2, and summarize the advantages and disadvantages of various technologies. In addition to its advantages in transmission rate and delay, 5G technology also has the advantages of convenient upgrade and low cost. Therefore, HST communication will focus on LTE-R and 5G-R in the future.

As shown in Figure 2, the integrated cab can implement T2T communication and T2I communication. On this basis, MEC paradigm is applied to the existing train control system, and TDAP is constructed for on-site analysis of train data. The functions of the four parts are as follows.

2.2 SPM scheme

In classic communication-eavesdropping



(a)SM in massive MIMO system (b)SPM in massive MIMO system

Figure 2: The proposed SPM scheme compared with traditional scheme.

model, the transmitter and the corresponding legitimate receiver communicate in the presence of passive eavesdropping. The number of antennas for the transmitter, receiver and eavesdropper in the model are N_t, N_r and N_d, respectively. For the party receiving the signal, Both Bob and Eve have a massive MIMO antenna array, and the number of antennas of the latter is not less than that of the former.

In the encryption technology of the wireless communication system model, ACMM is stored in the antenna index, which is compared with ACMM according to book, and the spatial modulation is realized by SPM scheme in the information bit. SPM scheme selects appropriate phase vectors, activates transmitting antennas corresponding to the vectors in a continuous time to disperse the space signal as shown in figure2.

In consideration of system security, the proposed system scheme adopts three-level encryption, which respectively correspond to the keys $K1$, $K2$, and $K3$ generated by hyperchaotic Henon mapping. The first level of encryption is to use $K1$ to select the appropriate ACMM in the book. The second level of encryption uses $K2$ to disrupt the correspondence between ACMM and the memory address in the book. The third level of encryption is to use SPM for three-dimensional modulation. Bob can decrypt the information by combining the keys and performing reverse operations in corresponding order.

Different transmitting antennas carry out signal propagation with different gains, the SPM receiver can thus detect the data symbols by identifying the most-likely combination of the fading gain and constellation symbol.

3 HASPM encryption scheme

3.1 Hyperchaotic Henon key generation algorithm

5G-R scenario wireless channel has many inherent properties at the physical layer, such as randomness, reciprocity, and location specificity. these properties make it possible to extract keys from channel's properties. As shown in the figure 3, the process of extracting keys from channel state information can be roughly divided into channel detection, measurement quantification, information adjustment and privacy amplification. Channel measurement is a method for Alice and Bob to collect channel measurement values. Channel state information is obtained by alternately transmitting signals and evaluating them. Since the channels are reciprocal, the difference between measured values observed by both parties is very small. Measurement quantization is to quantize the result measured in the previous step into a vector and convert it into the form of data encoding, and

then the preliminary keys can be obtained. Since the complete consistency of the channel measurement between two parties cannot be guaranteed, errors often occur during the measurement process, and the obtained preliminary keys cannot match each other. Therefore, information coordination is required. Information exchange through a common channel and key synchronization is achieved through coding error correction, ensuring that the keys generated respectively are the same. Privacy amplification is a method to eliminate the correlation between parts of information for

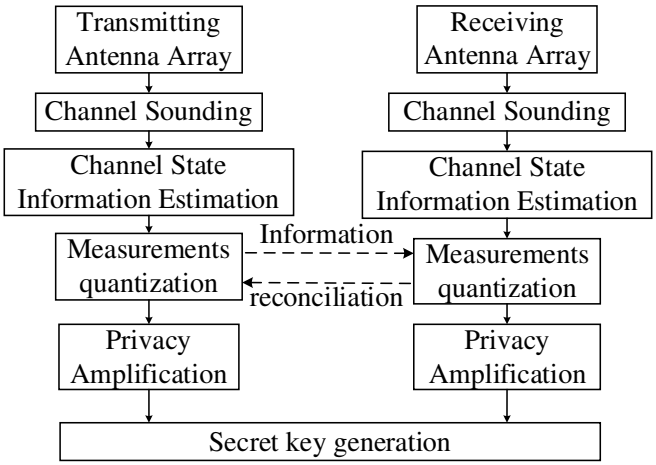


Figure 3: The process of extracting key from channel state information (CSI).

the key intercepted by the opponent.

To ensure the security of generating keys based on channel information, it is necessary to perform high-dimensional mapping on keys extracted from channel information, chaotic systems have the characteristics of randomness, unpredictability, and high sensitivity to initial values and system parameters. In this paper, the generalized Henon chaotic mapping is selected. It has two positive Lyapunov exponents, it is thus called a hyperchaotic map. Compared with Lorenz chaotic and chen chaotic, Lyapunov exponents of hyperchaotic Henon mapping are not the largest, but only it has two positive Lyapunov exponents, which shows that it has good randomness compared to the other two chaotic systems. In addition, Henon mapping only needs two multiplications for each iteration, while Lorenz mapping needs to solve a set of differential equations. Therefore, hyperchaotic Henon mapping can generate keys faster and ensure the encryption rate. The mathematical expression is as follows.

$$\begin{cases} \dot{u} = m - v^2 + nw \\ \dot{v} = u \\ \dot{w} = v \end{cases} \tag{1}$$

where m, n are system parameters. u, v, and w are variables.

When the parameters meet the conditions $1.54<m<2, 0<|n|<1$, mapping is in a hyperchaotic state. When two parameter values are m=1.65 and n=0.15, two largest Lyapunov exponents of the chaotic system are 0.689 and 0.693.

Keys extracted from the wireless channel is used as the initial value of the chaotic system to carry out the operation to generate a new chaotic sequence, and then use an appropriate quantization method to quantize the disordered sequence into a binary sequence, and three binary sequences respectively constitute the key $K1$, $K2$, $K3$.

3.2 Antenna mapping and spatial permutation modulation

The SPM scheme selects appropriate phase vectors, activates transmitting antennas corresponding to the vectors in a continuous time to disperse the space signal, and changes the antenna activation sequence from original simultaneous activation at the same time and different positions to sequential activation at different moments and different positions determined by the vectors. For example, when two antennas are activated at two consecutive times, in addition to the information conveyed by the quadrature amplitude modulation (QAM) signal, space modulation transmitters use permutation sets composed of permutation vectors for modulation. Bit '0' indicates that the selection is vector $[1,2]^T$, where the order of antenna activation is that the first antenna is

Table 3: Examples of permutation sets with various F and $d_{\min}$.

p	F	$d_{\min}$	$A_{Nt,p}(F,d_{\min})$
2	4	2	$[1,4]^T$,$[4,1]^T$,$[2,3]^T$,$[3,2]^T$
3	4	3	$[1,2,4]^T$,$[3,4,2]^T$,$[2,3,1]^T$,$[4,1,2]^T$
	8	2	$[1,2,3]^T$,$[1,4,2]^T$,$[2,1,3]^T$,$[2,3,4]^T$ $[3,1,4]^T$,$[3,2,1]^T$,$[4,1,2]^T$,$[4,3,1]^T$
4	4	4	$[1,2,3,4]^T$,$[2,1,4,3]^T$,$[3,4,1,2]^T$,$[4,3,2,1]^T$
	8	3	$[1,2,3,4]^T$,$[1,4,2,3]^T$,$[1,3,4,2]^T$,$[2,1,4,3]^T$ $[2,3,1,4]^T$,$[2,4,3,1]^T$,$[3,2,4,1]^T$,$[4,1,3,2]^T$

activated at time 1 and the second antenna is activated at time 2, bit '1' indicates that the selection is vector $[2,1]^T$, and antenna activation order is that first antenna is activated at time 2 and second antenna is activated at time 1. In the process of vector replacement, the number of repeated transmissions of the QAM signal is minimum Hamming distance between vectors to obtain the complexity of the QAM signals and vectors.

As mentioned earlier, the number of transmitting antennas is N_t. In the process of spatial modulation using permutation vectors, assuming that there are p elements that need to be arranged, then $A_{Nt,p}$ is a set of all p elements arranged in the N_t space. For example, the representation of the permutation set $A_{3,1}$ and $A_{3,2}$ are as follows.

$$A_{3,1} = \{[1],[2],[3]\}$$
$$A_{3,2} = \left\{\begin{bmatrix}1\\2\end{bmatrix},\begin{bmatrix}1\\3\end{bmatrix},\begin{bmatrix}2\\1\end{bmatrix},\begin{bmatrix}2\\3\end{bmatrix},\begin{bmatrix}3\\1\end{bmatrix},\begin{bmatrix}3\\2\end{bmatrix}\right\} \quad (2)$$

In order to obtain keys through permutation vectors to facilitate the spatial modulation of the information, permutation vectors representing the constellation are corresponding to binary digital codes, and F permutation vectors with smallest Hamming distance $d_{\min}$ are selected from $A_{Nt,p}$ and combined into a permutation set subset $A_{Nt,p}(F,d_{\min})$. SPM spatial signal is generated from specific permutation vectors selected from the subset $A_{Nt,p}(F,d_{\min})$ according to data bits.

Table 3 shows permutation sets in different situations. Compared to the number of modulated bits $\lfloor \log_2 N_t \rfloor$ of SM spatial signal, the number of modulated bits of SPM spatial signal has a logarithmic relationship with the dimension of the permutation vector used, that is $\lfloor \log_2 F \rfloor$. The more permutation vectors contained in $A_{Nt,p}(F,d_{\min})$, the more bits can be modulated by reducing the Hamming distance. Therefore, bit error rate performance and modulation rate can be balanced by adjusting F and $d_{\min}$. When transmitter is equipped with more antennas, the number of permutation vectors that meet conditions will also increase, so SPM can be easily applied to a massive MIMO system.

For the selection of the permutation vector set, first define all permutation vectors that meet conditions as a candidate pool. Define other vectors whose Hamming distance from the permutation vector is less than $d_{\min}$ as its neighbors. The permutation vector with fewest neighbors is selected, and its neighbors are removed from the candidate pool. If the number of permutation vectors in the expected permutation set is more than F, increase $d_{\min}$ and perform repeated screening until a permutation set that meets requirements is selected.

In practical applications, according to scenarios and user requirements, corresponding replacement subsets will be pre-arranged in transmitting and receiving antennas. SPM modulates v bit information contained in keys into a replacement vector $\vec{v} = [v_1, v_2, \ldots, v_t]^T \in A_{Nt,p}(F,d_{\min})$, so that each antenna is activated at the corresponding time.

Figure 4 shows the flow chart of the HASPM scheme, which is divided into four steps and introduced later.

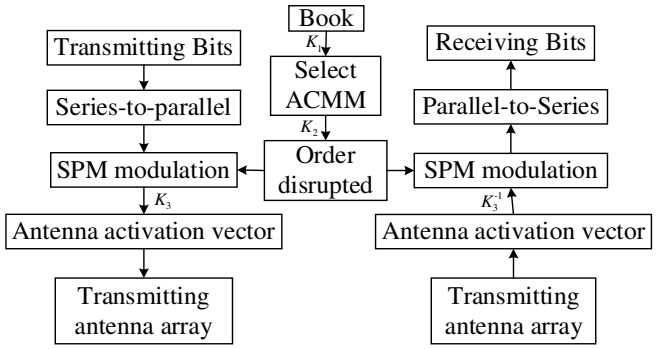


Figure 4: Flow chart of HASPM scheme.

First, the keys $K1$, $K2$, and $K3$ generated by the algorithm are used to select the applicable ACMM from the book and disrupt the relationship between the ACMM and the address storage, and finally perform space replacement modulation on it.

Secondly, the correspondence between ACMM and address storage can be established by the selection of the key $K1$, and each ACMM has a different address storage corresponding to it. The number of transmitting antennas is N_t, and the number of different antenna combinations is as follows.

$$\frac{C_{N_t}^3 C_{N_t-3}^3 \cdots C_3^3}{A_{N_t/3}^{N_t/3}} = 6^{\frac{N_t}{3}} \frac{(N_t)!}{(N_t/3)!} = N_{tc} \qquad (3)$$

Since the transmitting antenna is a group of three, N_t must be a multiple of three. When the modulation order is L, the number of different mapping modes on the three antennas is (3L)!. So the book is composed of N_{tc}(3L)! different ACMMs stored in the same number of storage addresses. The key $K2$ is used to disrupt the previously described relationship between the ACMM and the storage address. This operation makes it extremely difficult to obtain the correct corresponding relationship and prevents eavesdropper from intercepting the correct ACMM. At the same time, this operation ensures that the length of the binary sequence composing $K1$ does not exceed $\log_2(N_{tc}(3L)!)$. By using the key $K2$ for corresponding address interference, the key space is increased to N_{tc}(3L)!, and the security of the system is further improved.

In actual applications, usually only part of the book is used instead of the entire content to reduce the complexity of the system caused by the correspondence, but for eavesdropper, without knowing which part of the content is used, they can only try to search the entire space increases the difficulty of interception.

Then, after determining the relationship between the ACMM and the storage address, the information stream to be transmitted needs to be mapped to the activated antenna, and the antenna activation needs to be spatially modulated. The HASPM scheme proposed in this paper uses SPM to spatially modulate information bits. The traditional modulation technology only maps a certain number of bit streams to constellation punctuations, and transmits information through different antennas. The modulation type is easily intercepted and therefore leads to information leakage. Different from the traditional modulation strategy, the proposed HASPM scheme combines chaos theory and applies the physical layer-based SPM method to modulate partially activated antennas. The antenna activation sequence determined by key $K3$ will be used for SPM of information to realize the whole process from modulation to transmission. In the process of information transmission, rather than all antennas being activated, this solution thus has better energy efficiency. The information bit is a group of three bits and is mapped to a signal. The first bit selects the transmitting antenna to be activated, and the second two bits select the position of the constellation punctuation on the antenna. The transmitting antennas are divided into group $N_t/3$ by ACMM, and each group has three antennas. ACMM determines the constellation plot of each group. When a different ACMM is used, the activated antenna and the selected modulation type will change accordingly. For eavesdropper, it becomes more difficult to obtain the correct constellation diagram and modulation method, thus ensuring the security of information

transmission.

Finally, the information is transmitted through the wireless network and demodulated after being received at the receiving end. The received signal is detected by the detection algorithm, and then the decryption operation opposite to the encryption operation is performed to obtain the original information.

3.3 Minimum mean square channel estimation decoding

After receiving the coded and modulated signal, the signal receiving antenna must decode the received information to obtain the original correct signal. To perform the decoding operation, the serial number and constellation punctuation of the activated antenna at the transmitting end must be obtained in advance. Because different transmitting antennas use different gains for signal propagation, the signal receiver can detect data information according to the combination of attenuation gain and constellation signal. Then use the minimum mean square error estimation monitoring scheme to decode the constellation symbols. The signal received by the energy detection method decision device is as follows.

$$P_i = K \bullet S_i + E_i \tag{4}$$

where i is the antenna serial number, P_{i} is the constellation punctuation of the antenna transmission, K is the channel gain, E_{i} is the channel noise, and S_{i} is the activation state of the antenna.

Since the transmitting antenna and the receiving antenna have already performed wireless channel information detection and exchange during the key generation phase, the channel state information is known, and the data detection operation can be performed when the antenna is in the active state. Considering that the frequency selection channel signal model should be more accurately expressed as follows.

$$P_i = K_i \bullet S_i + E_i \tag{5}$$

Where K_{i} is the gain of the i-th antenna. In order to detect the activated antennas, N antennas are selected according to the channel signal energy. Using the introduced energy detection method, the serial numbers of N activated antennas can be known. The next step is to use the minimum variance estimation detection method to decode the constellation of the activated antenna, and then perform the opposite operation to the original information encrypted by the transmitting antenna to obtain the correct information.

4 Performance analysis and simulation

Theoretical analysis and simulation experiment were used to verify the feasibility and advantages of the proposed scheme in this section. The channel information is fully known to the transmitter and receiver, so the keys can be properly synchronized. In this paper, the key is generated by hyperchaotic Henon mapping, and the spatial modulation is carried out by HASPM scheme.

4.1 Complexity analysis

The security of the ACMM mapping process depends on two encryption processes corresponding to the three keys. Process 1 is that $K1$ selects an ACMM, whose opposite relationship with memory address is disorganized by $K2$. Process 2 is that $K3$ transforms the spatial distribution of information into the temporal distribution.

In first process, the main calculation of decrypting intercepted information focuses on finding the selected ACMM. For Eve without a key to get the original information, every ACMM in the book should be tried, so the computational complexity is $N_{\mathrm{tc}}(3\mathrm{L})!$. Bob can obtain the correct mapping mode according to the received key and directly obtain the correct ACMM. Table 4 shows the comparison of the calculation amount of the legitimate receiver and the

Table 4: The Computation Complexity Comparison.

N_t	3	3	6	6	9	9
L	2	3	2	3	2	3
Bob	1	1	1	1	1	1
Eve	2.59×10^4	1.31×10^7	9.33×10^6	6.72×10^8	9.41×10^9	4.74×10^{12}

eavesdropper during decryption. The calculation amount required for the decryption operation is calculated under different combinations of the number of transmitting antennas and the modulation order. The unit is the number of addressing operations. N_t represents the number of transmitting antennas, and L represents the modulation order.

For Eve, in the case of the same modulation order and different antenna numbers, the amount of calculation increases by 2-3 orders of magnitude with the double increase of the number of antennas, and the amount of calculation increases sharply with the increase of the multiple of antennas. In the case of the same number of antennas and different modulation orders, every time the modulation order increases by 1, the amount of calculation will increase by 2-3 orders of magnitude. It can be seen that the amount of calculation of Eve increases drastically with the increase of the modulation order and the number of transmitting antennas, but Bob only needs to use the key to perform addressing operations to obtain the correct original information.

In second process, Constellation punctuation completes the conversion of information from space to time after the key $K3$ modulation. The constellation punctuation of quadrature phase shift keying (QPSK) modulation is four points on the quadrant angle bisector with a distance of 1 from the origin. If Eve can intercept the complete spatially modulated signal, then its BER is as follows.

$$Pser = \sum_{i=1}^{Nt} \frac{1}{Nt} \Pr\left(\frac{\pi}{4} < \angle K3 < \frac{7\pi}{4}\right) = \frac{3}{4} \quad (6)$$

where P_r is the probability of the original signal rotating to other quadrants.

Analysis shows that the combination of the two encryption processes can effectively prevent the original information from being intercepted. Eve cannot identify the modulation type through higher order statistics, which is the most widely used modulation classification method. In addition, the security of the encryption algorithm also depends on the randomness and consistency of the key.

4.2 Random analysis

Regarding the security of wireless communication, the key used for communication must have enough randomness to ensure the irregularity of cracking the key. The most commonly used test in the world is fifteen different test indicators designed by the National Institute of Standards and Technology (NIST), including frequency test, test operation, and entropy test. The standard suite uses a specific test algorithm to obtain a value between 0 and 1 indicating the degree of difference by comparing the measurement results of the sequence to be tested and the degree of difference between the ideal sequence. The test will only be performed when this value is greater than the significance level a=0.01. After repeated test statistics and calculations, the results shown in Table 5 can be obtained. It can be seen from the table that the test values are significantly higher than the significance level, and 8 items of test values exceed 0.5, so the key stream sequence generated by the super chaotic mapping has enough randomness, and the hyperchaotic Henon algorithm is safe.

The ZUC algorithm is a candidate algorithm recommended by the international organization 3GPP as the third set of international encryption

and integrity standards for 4G wireless communications. Adding the ZUC algorithm to the NIST test comparison, it can be seen that the test value of the algorithm proposed is higher than the ZUC algorithm in most test items, there is even a huge lead in four tests (Serial, Longest Runs of ones, Approximate Entropy and Fast Fourier Transform). It shows that hyperchaotic Henon algorithm has obvious advantages over traditional encryption algorithms.

Table 5: NIST Random Test Result.

Item	Henon	ZUC
Frequency	0.3458	0.4729
Universal	0.4757	0.3388
Block Frequency	0.7452	0.6664
Linear Complexity	0.4675	0.4549
Runs	0.3158	0.3021
Serial	0.8544	0.1072
Rank	0.0585	0.5794
Cumulative Sums	0.3321	0.4949
FFT	0.7048	0.1194
Random Excursions	0.4126	0.1359
Random Excursions Variant	0.7459	0.4291
Overlapping Template	0.9462	0.7399
Non-Overlapping Template	0.6278	0.5084
Longest Runs of ones	0.9246	0.1073
Approximate Entropy	0.9145	0.1122

4.3 Reliability analysis

In the HASPM scheme, only one antenna per group is activated at the same time, which reduces the effect of multipath fading and greatly improves the BER performance. The space diversity order (sdo) in the case of the transmitting antenna and the receiving antenna are respectively N_t and N_r are expressed as follows.

$$N_{sdo} = N_r - N_t + 1 \tag{7}$$

In a traditional 36×36 MIMO system, N_{sdo}=1. In the same situation when using the HASPM scheme, each group of transmitting antennas only activates one antenna at a time, and the receiving antennas are all activated, so N_{sdo}=25. As N_{sdo} increases in wireless communication, its multipath fading effect decreases, so with the same SNR, BER decreases as N_{sdo} increases. Moreover, in massive MIMO system, the number of receiving antennas increases, and the interference between the transmitting antennas is reduced, the receiving antennas can thus receive signals more effectively.

The figure 5 shows the comparison between the HASPM scheme and the traditional digital modulation method QPSK when the number of antennas, coding algorithms, and decoding algorithms are the same.

It can be seen from the figure that Eve's BER is always maintained at about 0.5 with different

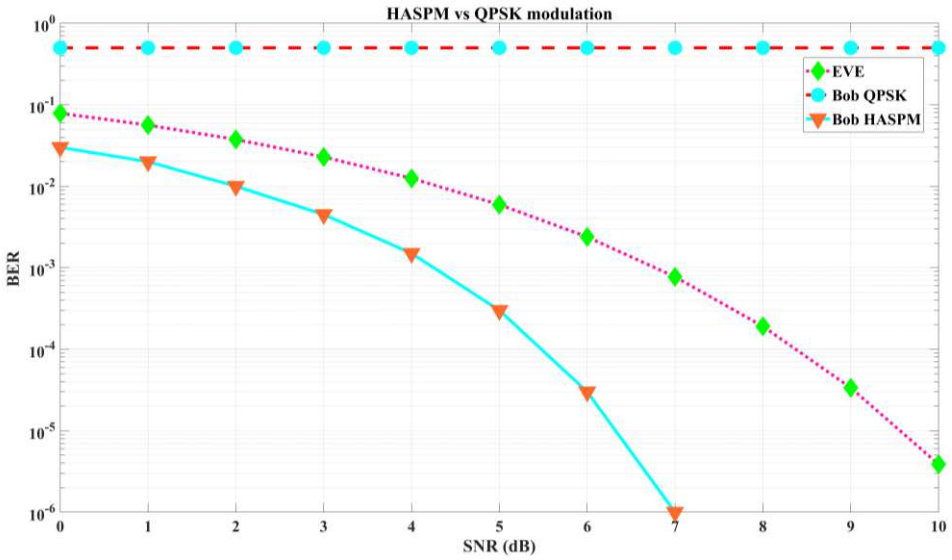


Figure 5: BER Comparison of HASPM and traditional QPSK.

received signal-noise ratio (SNR), the BER remains high. It is impossible to decode the intercepted information to obtain the correct Communication information. On the other hand, compared with QPSK digital modulation, the Bob's BER performance of proposed scheme is much better. When the modulation type is QPSK and the bit error rate is 10^{-2} and 10^{-4}, the performance gain is 2dB and 3.3dB respectively. From the curve trend, the BER improves more obviously as the SNR increases.

5 Conclusions

In this paper, we proposed a new physical layer encryption scheme HASPM, which uses hyperchaotic mapping and spatial permutation modulation are used to prevent eavesdropping by eavesdropper with large-scale receiving antennas and improve the security of massive MIMO system. First, the proposed scheme uses hyperchaotic Henon mapping to generate keys, encrypts the correspondence between ACMM and storage address and the modulation method, and improves the security of the communication system. Secondly, only one antenna in each group is activated at a time on the transmitting antenna side, the multipath fading effect is thus reduced and the problem of mutual interference of transmitted signals among different channels is solved. Finally, the complexity, randomness, and reliability of the system are verified. The huge number of antenna combination modes and modulation methods make it impossible for eavesdropper to obtain the original information they strive for even if they have a sufficient number of receiving antennas. The receiver can decode the signal according to the key and easily receive and decode the original information. Therefore, the key and channel information are transmitted and exchanged when the information is transmitted, and do not need to be shared in advance. The physical layer security encryption is realized with a more concise calculation.

Compared with the traditional massive MIMO modulation scheme, the multipath fading effect is reduced, the BER performance is greatly improved, and the system security and reliability are thus guaranteed. Theoretical analysis and experimental results also show the proposed solution can further improve the security of the wireless communication system compared with the traditional MIMO physical layer security solution. In general, the scheme proposed in this paper has a good guarantee in terms of complexity and security, improves the security of the wireless communication system, and in terms of information transmission, it can reduce channel interference and improve the BER performance.

References

[1] T. Levanen, J. Talvitie, R. Wichman, et al., "Location-aware 5G communications and Doppler compensation for high-speed train networks," 2017 European Conference on Networks and Communications, Oulu, pp. 1-6, 2017.

[2] R. Chen, W. Long, G. Mao and C. Li, "Development Trends of Mobile Communication Systems for Railways," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3131-3141, 2018.

[3] J. Zhao, Y. Liu, C. Wang, L. Xiong and L. Fan, "High-speed based adaptive beamforming handover scheme in LTE-R," IET Communications, vol. 12, no. 10, pp. 1215-1222, 26 6, 2018.

[4] J. Yang, Bo Ai, Sana Salous, et al., "An Efficient MIMO Channel Model for LTE-R Network in High-Speed Train Environment," IEEE Transactions on Vehicular Technology, vol. 68, no. 4, pp. 3189-3200, 2019.

[5] C. Wang, J. Bian, J. Sun, W. Zhang and M. Zhang, "A Survey of 5G Channel Measurements and Models," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3142-3168, 2018.

[6] M. Pappa, C. Ramesh and M. N. Kumar, "Performance comparison of massive MIMO and conventional MIMO using channel parameters," 2017 International Conference on Wireless Communications, Signal Processing and Networking,

Chennai, 2017, pp. 1808-1812.

[7] A. Mukherjee, S. A. A. Fakoorian, J. Huang and A. L. Swindlehurst, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey," in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1550-1573, 2014.

[8] A. D. Wyner, "The wire-tap channel," The Bell System Technical Journal, vol. 54, no. 8, pp. 1355-1387, 1975.

[9] J. Zhu, R. Schober and V. K. Bhargava, "Secure Transmission in Multicell Massive MIMO Systems," IEEE Transactions on Wireless Communications, vol. 13, no. 9, pp. 4766-4781, 2014.

[10] H. Q. Ngo, E. G. Larsson and T. L. Marzetta, "Energy and Spectral Efficiency of Very Large Multiuser MIMO Systems," IEEE Transactions on Communications, vol. 61, no. 4, pp. 1436-1449, 2013.

[11] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 339-348, 1978.

[12] E. G. Larsson, O. Edfors, F. Tufvesson and T. L. Marzetta, "Massive MIMO for next generation wireless systems," IEEE Communications Magazine, vol. 52, no. 2, pp. 186-195, 2014.

[13] T. Amin, D. B. Rawat and M. Song, "Performance Analysis of Secondary Users in the Presence of Attackers in Cognitive Radio Networks," 2015 IEEE Global Communications Conference (GLOBECOM), San Diego, CA, pp. 1-7, 2015.

[14] Q. Xu, P. Ren, H. Song and Q. Du, "Security Enhancement for IoT Communications Exposed to Eavesdroppers With Uncertain Locations," IEEE Access, vol. 4, pp. 2840-2853, 2016.

[15] R. K. Sharma and D. B. Rawat, "Advances on Security Threats and Countermeasures for Cognitive Radio Networks: A Survey," IEEE Communications Surveys & Tutorials, vol. 17, no. 2, pp. 1023-1043, 2015.

[16] Q. Xu, P. Ren, H. Song and Q. Du, "Security-Aware Waveforms for Enhancing Wireless Communications Privacy in Cyber-Physical Systems via Multipath Receptions," IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1924-1933, 2017.

[17] T. Liu and S. Shamai, "A Note on the Secrecy Capacity of the Multiple-Antenna Wiretap Channel," IEEE Transactions on Information Theory, vol. 55, no. 6, pp. 2547-2553, 2009.

[18] F. Oggier and B. Hassibi, "The Secrecy Capacity of the MIMO Wiretap Channel," IEEE Transactions on Information Theory, vol. 57, no. 8, pp. 4961-4972, 2011.

[19] S. Gerbracht, C. Scheunert and E. A. Jorswieck, "Secrecy Outage in MISO Systems With Partial Channel Information," IEEE Transactions on Information Forensics and Security, vol. 7, no. 2, pp. 704-716, 2012.

[20] J. Zhu, R. Schober and V. K. Bhargava, "Secure Transmission in Multicell Massive MIMO Systems," IEEE Transactions on Wireless Communications, vol. 13, no. 9, pp. 4766-4781, 2014.

[21] N. Yang, P. L. Yeoh, M. Elkashlan, R. Schober and I. B. Collings, "Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels," IEEE Transactions on Communications, vol. 61, no. 1, pp. 144-154, 2013.

[22] Y. Liu, H. Chen and L. Wang, "Physical Layer Security for Next Generation Wireless Networks: Theories, Technologies, and Challenges," IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 347-376, 2017.

[23] Y. A. Chau and Shi-Hong Yu, "Space modulation on wireless fading channels," IEEE 54th Vehicular Technology Conference. VTC Fall 2001. Proceedings (Cat. No.01CH37211), Atlantic City, NJ, USA, vol.3, pp. 1668-1671 2001.

[24] S. Guo, H. Zhang, S. Jin and P. Zhang, "Spatial Modulation via 3-D Mapping," IEEE Communications Letters, vol. 20, no. 6, pp. 1096-1099, 2016.

[25] S. Guo, H. Zhang, P. Zhang, D. Wu and D. Yuan, "Generalized 3-D Constellation Design for Spatial Modulation," IEEE Transactions on Communications, vol. 65, no. 8, pp. 3316-3327, 2017.

[26] S. Sinanovic, M. Di Renzo and H. Haas, "Secrecy Rate of Time Switched Transmit Diversity System," 2011 IEEE 73rd Vehicular Technology Conference (VTC Spring), Yokohama, pp. 1-5, 2011.

[27] I. Lai, J. Shih, C. lee, et al., "Spatial Permutation

Modulation for Multiple-Input Multiple-Output (MIMO) Systems," IEEE Access, vol. 7, pp. 68206-68218, 2019.

[28] F. Boccardi, R. W. Heath, A. Lozano, T. L. Marzetta and P. Popovski, "Five disruptive technology directions for 5G," IEEE Communications Magazine, vol. 52, no. 2, pp. 74-80, 2014.

[29] C. Wang, F. Haider, X. Gao, et al., "Cellular architecture and key technologies for 5G wireless communication networks," IEEE Communications Magazine, vol. 52, no. 2, pp. 122-130, 2014.