Secure Communication Method of Metallurgical System Data Network based on Chaotic System Sequence Parameter Identification

Yuanyuan Ma¹, Fucai Luo², Hongfa Li³
¹Global Energy Interconnection Research Institute Co., Ltd., Nanjing, 210003, China
²State Grid Fujian Electric Power Co., Ltd., Fuzhou, 350000, China
³State Grid Fujian Electric Power Co., Ltd., Information & Telecommunication Branch, Fuzhou, 361004, China

*Corresponding author e-mail: luyl_19880922@163.com

Abstract. In the research process of chaotic system sequence parameter identification, we find that there is only one chaotic attractor in chaotic direct spread spectrum signals, which cannot satisfy the confidentiality of communications. Based on the thought of generalized synchronization of chaotic system, we proposed a chaotic secure communication method, in other words, the partial sequences of chaotic system were used for the parameter identification of chaotic system. The chaotic ant colony optimization algorithm was used for the parameter identification of partial sequences of chaotic system, so as to achieve the purpose of understanding all the information of chaotic system. The parameter space and the ant colony space were introduced into the parameter identification process. We used the space transformation function to transform the parameter space and the ant colony space. Experimental results show that using the Lorenz system numerical method can verify the feasibility of chaotic system partial sequence parameter identification and chaotic secure communication.

Keywords: Chaotic system, Sequence, Parameter identification, Secure communication

1. Introduction
Chaos is a very significant phenomenon in nonlinear dynamical systems. The chaotic phenomena shows behaviors of complexity, noise-like, unpredictability. Based on these behaviors, chaotic secure technology has received extensive attention and research [1-3]. Reference [4] realizes the parameter identification of chaotic system through the high-order adaptive sliding mode controller, which is used in the chaotic secure communication. Reference [5] uses the hybrid encryption method based on physical chaos for the image encryption, and compares and analyzes the advantages of this hybrid encryption method. Chaotic secure communication is to embed the information into the chaotic signals of transmitting system at the transmitting terminal, and the receiving terminal receives the chaotic signals containing information and extracts the information. Chaotic secure communication requires synchronization between the transmitting terminal (drive system) and the receiving terminal (response
system). The most direct way to synchronize the response system with the drive system is to identify the parameters of drive system. In recent years, the research on parameter identification of chaotic systems has attracted great attention of researchers, and a variety of effective methods for parameter identification have been proposed. We use the chaotic ant colony optimization algorithm for the parameter identification of Lorenz system.

Although the minimum relative singular value method proposed in reference [6] is not the parameter identification method for chaotic systems, it can identify the signal parameters in chaotic background, such as the frequency of sinusoidal signals. Reference [7] uses the adaptive filtering method to realize the identify the parameter identification of chaotic system, and discusses the noiseless and noise environment. Reference [8] uses adaptive sliding formwork method to realize synchronization of chaotic systems. Reference [9] uses adaptive controller to realize the parameter identification and synchronization of chaotic system. Reference [10] proposes the diffused grass algorithm, and parameters identification is carried out for several chaotic systems. Reference [11] uses the gradient descent method to realize the parameter identification and synchronization of chaotic system. The parameter identification of chaotic system calculates the corresponding unknown parameters of chaotic system based on the data sequence of chaotic system. Most of the proposed chaotic system parameter identification methods need the entire sequence of chaotic systems to achieve parameter identification.

In order to realize the communication security of parameter identification, we proposed the secure communication method based on parameter identification of chaotic system sequence. Firstly, we used the chaotic ant colony optimization algorithm to simply improve it, then introduced the ant colony space and the parameter space, so that the chaotic ant colony algorithm could not be constrained by the search range of problem. Then, after introducing the algorithm of ant colony space and parameter space, we could solve the optimization problem of any finite real number space, secondly introduced the partial sequence parameter identification of chaotic system, and proposed a chaotic secure communication method is proposed based on the identification of chaotic system parameters. Finally we carried the numerical experiments with Lorenz system, which mainly included the partial sequence parameter identification of Lorenz system and secure communication of Lorenz system verifying the feasibility of search scope. The study of sequence parameter identification and secure communication of chaotic system was guaranteed.

2. Chaotic ant Colony Optimization Algorithm
Chaos ant colony optimization algorithm is a swarm intelligence algorithm based on monomer chaotic search behavior and colonial self-organizing behavior of ant colony. Based on the improved chaotic ant colony optimization algorithm, we introduce the ant colony space and parameter space to expand the scope of application of algorithm, and the process is shown in Figure 1.

![Flowchart of ant colony space and parameter space extension algorithm](image)

**Figure 1.** Flowchart of ant colony space and parameter space extension algorithm

2.1. Ant colony Space and Parameter Space
The formula of the definition of ant colony space in chaotic ant colony optimization algorithm is:

\[
x = (x_1, x_2, \ldots, x_l), x_j \in [-10, 10], d = 1, 2, \ldots, l
\]

(1)

In this algorithm, the parameters x and l are localized which are no longer constrained by the parameter space of solution problem, and the sequence of parameter x transforms in the space of (-10,
10), and the range of sequence d is unlimited. From this we can obtain the parameter space, namely, the search space of actual problem:

\[ x' = (x'_1, x'_2, \cdots, x'_l), x'_d \in [m_d, n_d], d = 1, 2, \cdots, l \]  \hspace{1cm} (2)

The range of sequence space where the parameter space \( x' \) of the actual problem lays is \((m_d, n_d)\), and the sequence d remains unchanged. The ant colony space and the parameter space are transformed by transformation (1) and inverse transformation (2) to obtain formulas (3) and (4).

\[ x'_d = \frac{m_d + (x_d + 10)(n_d - m_d)}{100} \]  \hspace{1cm} (3)

\[ x_d = -\frac{10 + 100(x'_d - m_d)}{n_d - m_d} \]  \hspace{1cm} (4)

Formula (3) is the ant colony space transformed directly by formula (1). The formula (4) is the parameter space inversely transformed by formula (2).

2.2. Chaotic Ant Colony Optimization Algorithm based on Ant Colony Space and Parameter Space
The ant colony space and the parameter space obtained by above formulas can solve L-dimensional optimizing problems of \( p = \min f(x') \) and \( x' = (x'1, x'2, \cdots, x'l) \), and the algorithms start by:

\[ x_d(1) = 100(2 - k)h, d = 1, 2, \cdots, l \]  \hspace{1cm} (5)

We randomly generated the initial position \( x_i(1) = (x_{i1}, x_{i2}, \cdots, x_{il}) \), \( i = 1, 2, \cdots, N \) for each ant. N is the total number of ants in ant colony, which is regard as the initial possible optimal position \( q_i \), we get \( x'_i(1) \) transformed by \( x_d(1) \) as \( q'_i \), and compute the objective function \( f(x'_i(1)) \) according to the iterative equation:

\[ Y_i(k) = Y_i(k-1)^{\lambda'}, \]
\[ x_{i,d}(k) = x_{i,d}(k-1) + 100v_i \]
\[ \times e^{(1 - e^{-\beta})} \cdot \left\{ 3 - \phi_d\left[ x_{i,d}(k-1) + 100v_i \right] \right\} - 100v_i \]
\[ + \left[ q_{i,d}(k-1) - x_{i,d}(k-1) \right] e^{-(2m_k)\alpha} \]  \hspace{1cm} (6)

Calculating the next position, we get \( x_i(1) \) through the transformation (1), and calculate the objective function \( f(x_i(1)) \) and determine whether to update the optimal location \( q_i \) and \( q'_i \), and carry out the iteration in turn. Starting from the initial value, once after a certain number of iterations, all ants in ant colony will exchange the information. An optimal possible optimum position is obtained by comparing all possible optimal positions, and all ants will update the optimal information.

\[ T_d = \frac{1}{N} \sum_{i=1}^{N} t_{i,d} \]
\[ S_d = \frac{1}{N} \sum_{i=1}^{N} |x'_{i,d} - T_d| \]
\[ S_d < 1 \times 10^{-6}, d = 1, 2, \cdots, l \]
\[ |T_d(n) - T_d(n-1)| < 1 \times 10^{-5} \]
\[ d = 1, 2, \cdots, l \]  \hspace{1cm} (7)
Then we continue to search for possible optimal solutions until meeting the condition of iteration, completing the first search. The T is denoted by T (1). On the basic of the invariant possible optimal location, we carry out the second chaotic search, and get T (2) after the search, successively, when the condition is satisfied, its algorithm is over. In the chaotic ant colony optimization algorithm, the values of each parameter are m=50, n=0.2, and vi is the random number between 0 and 1.

3. Parameter Identification and Chaotic Secure Communication Method in Chaotic System Algorithm

We use partial sequence of chaotic system to identify parameters, and the remaining sequences are used in chaotic secure communication method of chaotic encryption. Because chaotic systems are extremely sensitive to initial conditions, observable sequences used for parameter identification will also be used for data correction. Using chaotic secure communication is to bury the signal in the chaotic signal. This method is simple.

3.1. Parameter Identification

For a chaotic system, there are m unknown parameters \( x_1, x_2, \ldots, x_n \), and the chaotic system includes n sequences. But we can only get n1 accurate sequence, and remaining n2 sequences cannot be obtained or cannot be obtained accurately. The purpose of parameter identification is to determine m unknown parameters of chaotic system through observable n1 sequences, so as to understand all the information of chaotic system. Firstly, the parameter identification problem is converted into the optimization problem, and then the chaotic ant colony optimization algorithm is used to solve the optimization problem, so that the parameter identification can be realized. Each sequence in observable n1 sequences is continuously sampled (by the time step \( \Delta t \)) to extract k data, we can obtain:

\[
X = \begin{bmatrix}
X_1(0)X_1(1)X_1(2)\cdots X_1(K) \\
X_2(0)X_2(1)X_2(2)\cdots X_2(K) \\
\vdots \\
X_n(0)X_n(1)X_n(2)\cdots X_n(K)
\end{bmatrix}
\]  

There are n1 groups of data. Unknown parameters \( x_1, x_2, \ldots, x_n \) and initial values of unobservable n2 sequence, \( x_{n1+1}, x_{n1+2}, \ldots, x_{n+n2} \) T constitute the parameter space \( x = (x_{n1}, x_{n1+2}, \ldots, x_{n+n2}) \). We determine the search region for each unknown parameter in parameter space. In parameter space, the n sequences can be computed by the chaotic system determined by each point with same time step, and we can get:

\[
Y = \begin{bmatrix}
Y_1(0)Y_1(1)Y_1(2)\cdots Y_1(K) \\
Y_2(0)Y_2(1)Y_2(2)\cdots Y_2(K) \\
\vdots \\
Y_n(0)Y_n(1)Y_n(2)\cdots Y_n(K)
\end{bmatrix}
\]

There are n groups of data, that is the entire sequence of chaotic systems. We can use top n1 groups of data of Y and X to define the object function:

\[
f(x) = \sum_{j=1}^{n1} \sum_{j=1}^{K} |Y_j(j) - X_j(j)|
\]

We have transformed the parameter identification problem into an optimization problem. \( G=\text{min}f(x) \) numerical experiments show that the chaotic ant colony optimization algorithm can get numerical solutions with 10.6 precision accuracy.

3.2. Chaotic Secure Communication
The chaotic secure communication process is as follows. Firstly, the information sequence \( s = (s_1, s_2, \ldots, s_n) \) is buried in the chaotic system sequence \( X = (X_1, X_2, \ldots, X_n) \) at the transmitting terminal. The receiver receives \( S = (X_1, X_2, \ldots, X_n), X_{n+1}, X_{n+2}, \ldots, X_{n+m} \). Among them, there are not accurate chaotic system sequences, and there are chaotic sequences containing information. The parameter identification method in section 3.1 is used to realize the parameter identification of partial sequence parameters in the chaotic system, fully understanding the chaotic system, so that the useful information \( s \) can be extracted from chaotic sequences.

4. Experimental Results and Analysis

The experiment mainly includes parameter identification of Lorenz system and chaotic secure communication of Lorenz system. Numerical experiments show that the chaotic ant colony optimization algorithm can obtain parameter identification results with high accuracy. Because chaotic systems are extremely sensitive to initial values, numerical experiments also show that chaotic secure communications need to correct data.

4.1. Experimental Steps

We use the chaotic ant colony optimization algorithm to identify the parameters of Lorenz system. In the numerical experiment, the total number of ant colony \( N = 1000 \). Lorenz system equation is:

\[
A = -\alpha (a - b) \\
B = rA - B - zC \\
C = -\beta z + AB
\]

(11)

Take the parameter \( a=8, b=2.5, r=30 \), the initial value \( A(0) = 2, B(0) = 1, C(0) = 1 \), the time step, \( \Delta t = 0.001 \), we obtain Lorenz system sequence \( A=A(0), A(1), A(2), \ldots, A(K) \), \( K = 600 \).

We carry out the parameter identification of Lorenz system from sequence \( A \), and the parameter space includes \( (r, B(0), C(0)) \). The search ranges respectively are \( r \in [0, 60], B(0) \in [-10, 10], C(0) \in [-10, 10] \). The chaotic ant colony optimization algorithm after 7 chaotic search and 2170 iterations gets the optimal solution \((27.99999969, 0.99999999, 0.99999958)\) that the precision accuracy is \(10^{-6}\). The parameter identification search evolution process is shown in Figure 2-Figure 4.

![Figure 2. Parameter r ant colony search evolution](image1)

![Figure 3. Initial value B (0) ant colony search evolution](image2)
The chaotic system is extremely sensitive to the initial value, we get the optimal solution with precision accuracy $10^{-6}$, which is still not the exact solution. Whether the behaviors of original system and Lorenz system determined by numerical solution are coincident is a problem that must be considered in chaotic secure communication. Because the chaotic system with $\alpha=8$, $\beta=2.5$, $r=28.99999969$ and $A'(0)=3.5$, $B'(0)=0.99999999$, $C'(0)=0.99999989$ initial value is extremely sensitive to the initial value, we get the optimal solution with precision accuracy $10^{-6}$, which is still not the exact solution. Whether the behaviors of original system and Lorenz system determined by numerical solution are coincident is a problem that must be considered in chaotic secure communication.

According to the formula, $\mathcal{E}(t)$ will suddenly become larger with the increase of $t$, when the $t=20.223$, $\mathcal{E}(t) > 10.3$, when $t=23.131$, $\mathcal{E}(t) > 0.1$.

### 4.2. Experimental Results

In the experiment, we use sine signal $s_1(t)$ and square-wave signal $s_2(t)$ which is shown in Figure 5, at the transmitting terminal, the signals $s_1(t)$ and $s_2(t)$ are buried in chaotic sequence of Lorenz system that $\alpha=8$, $\beta=2.5$, $r=28$ initial value $A'(0)=3.5$, $B'(0)=0.5$, $C'(0)=0.5$.

The receiving terminal receives the Lorenz system sequence $A'(t)$ and the chaotic sequence with signal $B'(t) + S_1(t)$, $C'(t) + s_2(t)$, as shown in Figure 6.
Figure 6. Sinusoidal signal of $B'(t) + s_1(t)$

At the receiving terminal, we use sequence $A'(t)$ and the chaotic ant colony optimization algorithm for parameter identification of $r$, $B'(0)$, $C'(0)$, so as to get the Lorenz system which is synchronized with the transmitting terminal. Thus, the receiving terminal eliminates the chaotic sequence from the sequence $B'(t) + s_1(t)$, $C'(t) + s_2(t)$, and then extracts the signal $sN 1(t)$, $sN 2(t)$, as shown in Figure 7.

Figure 7. Sinusoidal signal of $C'(t) + s_2(t)$

From Figure 7, we can see that because the chaotic system is extremely sensitive to the initial value, the signal extracted by the receiving terminal will be completely distorted after a period of time, but we can use the sequence $A'(t)$ for correct it. When the deviation $3(t)$ of sequence $A'(t)$ is higher than $10^{-3}$, we will carry out the parameter identification of partial sequence in Lorenz system again, and we can find that $B'N(t)$ and $C'N(t)$ are the sequences of Lorenz system obtained by parameter identification, and the deviation with the original Lorenz system sequence is in the range of $10^{-3}$ magnitude, so the search determined in this way is feasible. Therefore, based on the chaos sequence parameter identification, we can use the above method for the secure communication.

5. Conclusions
Using chaotic ant colony optimization algorithm for the parameter identification of chaotic system partial sequence can get results with high-precision, but the chaotic system is extremely sensitive to the initial value. The chaotic system through the parameter identification after a period of evolution will have serious deviation with the original chaotic system. Therefore, in chaotic secure communication based on the partial sequence parameter identification of chaotic systems, the chaotic system sequence $x(t)$ is not only used for the parameter identification, but also used for the correction. When the deviation of sequence $x(t)$ is too large, we need to carry out the parameter identification again. Experiments show that chaotic secure communication receiving terminal after multiple parameter identification can get useful signals which are completely consistent with the transmitting terminal. Experiments prove the sequence parameter identification of chaotic system can improve the confidentiality of communication effectively, and provide the basis for the future secure communication work in China.
Acknowledgments
This research work is funded by 2019 Industrial Internet Innovation Development Project of Ministry of Industry and Information Technology of P.R. China “Comprehensive Security Defense Platform Project for Industrial/Enterprise Networks”.

References
[1] R. Rakkiyappan, G. Velmurugan, J. Cao, Finite-time stability analysis of fractional-order complex-valued memristor-based neural networks with time delays, Nonlinear Dynamics. 78 (2014), 2823-2836.
[2] G. Velmurugan, R. Rakkiyappan, V. Vembarasan, Dissipativity and stability analysis of fractional-order complex-valued neural networks with time delay, Neural Networks. 86 (2016), 42.
[3] G. Velmurugan, R. Rakkiyappan, J. Cao, Further analysis of global \([\text{formula omitted}]\)-stability of complex-valued neural networks with unbounded time-varying delays, Neural Networks. 67 (2015), 14-27.
[4] S. Cai, P. Zhou, Z. Liu, Synchronization analysis of directed complex networks with time-delayed dynamical nodes and impulsive effects, Nonlinear Dynamics. 76 (2014), 1677-1691.
[5] G. Velmurugan, R. Rakkiyappan, J. D. Cao, Further analysis of global \(\mu\) math Container Loading Mathjax-stability of complex-valued neural networks with unbounded time-varying delays, Neural Networks. 67, 2015, 14-27.
[6] L. Zhou, C. Wang, L. Zhou, Cluster synchronization on multiple sub-networks of complex networks with nonidentical nodes via pinning control, Nonlinear Dynamics. 83 (2016), 1079-1100.
[7] N. Liu, H. An, X. Hao, The stability of the international heat pump trade pattern based on complex networks analysis, Applied Energy. 2017, 196.
[8] R. Rakkiyappan, R. Sivaranjani, G. Velmurugan, Analysis of global \(O(t-\alpha)\) stability and global asymptotical periodicity for a class of fractional-order complex-valued neural networks with time varying delays, Neural Networks. 77 (2016), 51.
[9] J. F. Donges, I. Petrova, A. Loew, How complex climate networks complement techniques for the statistical analysis of climatological data, Climate Dynamics. 45 (2015), 2407-2424.
[10] W. Xu, J. Cao, M. Xiao, A new framework for analysis on stability and bifurcation in a class of neural networks with discrete and distributed delays, IEEE Transactions on Cybernetics. 45 (2015), 2224-2236.
[11] E. R. Patchett, A. Williams, Z. Ding, A high-yield vacuum-evaporation-based R2R-compatible fabrication route for organic electronic circuits, Organic Electronics. 15 (2014), 1493-1502.