Multistage Synchronous Secure Communication Method

Wei SUN¹, Jun HE¹, Lei QUAN²

¹. Science and Technology on Complex Electronic System Simulation Labratory, University of Aerospace Engineering, Beijing, 101416, China
². Naval Academy of Armament, Beijing, 100161, China

Based on Time-delayed Hyperchaotic System
Email: sunwei0326@163.com

Abstract. To solve the security of data transmission in network, a secure communication method based on time-delayed hyperchaotic synchronization is presented. By selecting the typical hyperchaotic system, the communication system synchronization scheme is designed to realize the recovery of the encrypted signal, and the security performance of the method is analyzed by simulation. The simulation results show that the synchronization method has the characteristics of high security and is easy to implement.

1. Introduction

Hyperchaotic systems are at least four-dimensional nonlinear complex systems. Such systems abound in nature and in laboratories, such as plasma systems in controlled devices, complex fluid systems, Dolo microwave systems, and Josephson junctions. Compared with the study of chaos synchronization, the study of hyperchaotic synchronization is not particularly deep[1,2]. Hyperchaotic motion is similar to chaotic motion, and a variety of instability coexist in a system. However, the hyperchaotic attractor has two or more positive Lyapunov exponents, which have the characteristics of multi-directional exponential divergence, Highly tangled complex form. Due to the limitations of mathematical methods, it is very difficult to solve hyperchaotic systems. In fact, the control of a variety of instability in the plasma in the technical requirements are very high. Usually an unstable system is controlled, and another instability comes out. So that the control of hyperchaotic system is extremely hard. Therefore, the difficulty of the stability control of hyperchaotic attractors is much greater than that of chaotic attractors.

At present, most of the chaotic communication systems adopt a simple chaotic system with only one positive Lyapunov exponent. There are still some problems in the security of such chaotic communication systems. The hyperchaotic system with multiple positive Lyapunov exponents is no longer a one-dimensional curve with ordinary chaos of only one positive Lyapunov exponent under the appropriate regression mapping, but a high-dimensional attractor, the modulated signal and the original chaos Signal is mixed and indistinguishable. It is difficult to decipher, and hyperchaotic attractors have multi-directional, can be used as a carrier of multiple chaotic signals to transmit information, can be more efficient coding, thereby increasing the communication rate and increase the amount of communication information and improve communication System of confidentiality.

The hyperchaotic system is an infinite dimensional system. The hyperchaos generated by such a system can have multiple positive Lyapunov exponents, so the system can produce complex time series, and the number of positive Lyapunov exponents of the system is no longer affected by the
system dimension Number of restrictions. This feature of the time-delayed hyperchaotic system makes it particularly suitable for secure communication. In this paper, a typical time-delayed hyperchaotic system is selected to realize multistage synchronous secure communication and security analysis is carried out.

2. Selection of Chaotic System

It is well known that the structure of hyperchaotic systems is very complex. But when a simple delayed feedback is introduced, it is easy to convert a low-dimensional chaotic system into a hyperchaotic system. The introduction of this delayed feedback term avoids the shortcomings that the system structure is too complex because of the realization of hyperchaos [3]. Therefore, the Markey-Glass time-delayed hyperchaotic system is chosen in this design, which is a typical time-delayed hyperchaotic system.

Markey-Glass time-delayed hyperchaotic system equations are described as follows:

\[ \dot{x} = \frac{ax(t - \tau)}{1 + x^3(t - \tau)} - cx \]  

Which \( x \in \mathbb{R} \) is the state of the system variables, \( a, b, c \) is the system parameters. When \( a = 0.2, b = 10, c = 1, \tau = 17 \), the system has five positive Lyapunov exponents, so the system is hyperchaotic and has complex dynamical behavior. The system state variables \( x \) changes over time as shown in Figure 1.

![Figure 1 Status Variable](image.png)

3. Selection of Synchronization Scheme

The multistage chaotic synchronization secure communication system is selected as the realization method. At the transmitting end, the chaotic signal is first synthesized with the useful signal, and then the synthesized chaotic signal is applied to another chaotic system. At the receiving end, the chaotic signal transmitted by the channel is recovered by the same chaotic system with the same structure as the transmitter out of the original signal. Obviously, because the useful signal directly acts on the chaotic system, and in the receiver must go through the secondary demodulation to restore the useful signal, taking into account the chaotic signal on the initial value of the sensitive dependence, the system in terms of safety performance is superior to the original synchronization masked communication system. In addition, the combination of useful signal and chaotic system makes the effective bandwidth of the system greatly wider than the original synchronization masking communication system.
4. Design Process

The first step is to design the sending side of the communication system.

Figure 3 shows the structure of the sender. The chaotic system with the same structure as the system (1) is used as the main chaotic system at the transmitter of the communication system. The structure of the second order subsystem is the same as that of the main chaotic system

\[
\dot{x}_i = \frac{ax_i(t-\tau)}{1+x_i^2(t-\tau)} - cx_i \quad (i = 1, 2)
\]  

(2)

At first, the hyperchaotic system and the useful signal are synthesized; signal synthesis can be used in a variety of ways. For convenience, a superimposed synthesis is selected in the program, and the synthesis of the signal is expressed as

\[
\dot{x}_i = \frac{ax_i(t-\tau)}{1+x_i^2(t-\tau)} - cx_i + h(t)
\]

(3)

The selected useful signal is \( h(t) = \sin(0.05t) \). A part of the (1) is selected to be acted on the second order chaotic as subsystem. The selected signal is \( H_i(t) = \frac{ax_i(t-\tau)}{1+x_i^2(t-\tau)} + h(t) \). The second level subsystem can be described as follows:

\[
\dot{x}_i(t) = \frac{ax_i(t-\tau)}{1+x_i^2(t-\tau)} - cx_i(t) + H_i(t)
\]

(4)

and it is acted as a signal to be transmitted in the channel.

The second step is to design the receiving end of the communication system.
Figure 4 Structural Design of Receiver on Chaotic Communication System

Figure 4 shows the structure of the receiver. At the receiving end, the hyperchaotic system and the system (1) have the same structure. The signal $H_1(t)$ transmitted in the channel can be recovered as $H_1'(t)$ by the demodulation of the first-level hyperchaotic system, and then the second stage demodulation can be recovered to the useful signal $h'(t)$.

The third step, to simulate and verify the rationality of the program.

The computer simulation of the designed communication system is carried out. In the simulation, the hyperchaotic system takes the parameter $a = 0.2, b = 10, c = 1, r = 17$ and assumes the information signal to $h(t) = \sin(0.05t)$. The simulation results are shown in Figure 5.

(a) Information Signal  
(b) Mixed Signal  
(c) Transmitted Signal  
(d) Restored Signal  
(e) Error Signal  
(f) Phase Diagrams

Figure 5 Designed Chaotic Secure Communication System
As can be seen from Figure 5 and Figure 6:
(1) The multistage synchronous secure communication scheme based on time-delayed hyperchaotic system can improve the security performance more effectively than the single-level method, and it is not easy to be cracked by the attacker.
(2) It can be better to restore the information signal.
(3) The error of the recovered signal and the transmitted information signal is in the order of magnitude $10^{-16}$, which is small, and what can be seen through this program is that it can be a very good realization of hyperchaotic system of confidential communications.

5. Security Discussion
Assuming that the illegal stealer has stolen the signal $H_x(t)$ transmitted in the channel, and the stealer knows the structure of the chaotic communication system used, but does not know the exact parameters of the system. Assuming that the system parameters obtained by the stealer are $a + \Delta a, b + \Delta b, c + \Delta c, \tau + \Delta \tau$ and $\Delta a = \Delta b = \Delta c = 0.0002$, $\Delta \tau = 0.1$, the error of the signal deciphered by the stealer through this inaccurate parameter and the actual transmitted information signal is shown in Figure 7.

By analyzing the security of the time-delayed hyperchaotic synchronization secure communication system, it can be seen that the illegal stealer cannot get the information signal which is actually transmitted through the inaccurate parameters. So this communication system has a very good security.

6. Conclusion
Based on the study of hyperchaotic system synchronization, the application in secure communication is studied. Firstly, the hyperchaotic synchronization and chaotic synchronization secure communication are briefly introduced. Then, the hyperchaotic synchronization scheme based on the state observer method is studied, and the simulation and robustness analysis are carried out. Finally,
the multistage synchronous secure communication scheme of time-delayed hyperchaotic system is analyzed, and the security discussion is also discussed.

References
[1] En Zou, Xiangfei Lee, Jianguo Chen. Chaos Control and Its Application. National Defense University of Science and Technology Press, 2002.
[2] Jinqing Fang, Geng Zhao, Xiaoshu Luo. Advances of Application Research in Chaotic Secure Communication, Journal of GuangXi Normal University, vol.20, 2002:6-18
[3] Kuang Jinyu, Pei Liqing, Tang Xiujuan, Huang Ronghuai. A Multistage Chaotic Synchronized System for Secure Communications. ACTA Electronica Sinica, vol.27, No.6, June 1999:23-26
[4] Bruce Schneier. Applied Cryptography. Wu Shizhong, Beijing, Machinery Industry Press. 2000: 340-356
[5] Short K M. Steps toward to unmasking secure communications. Int. J. Bifurcation and Chaos, 1994, 4(4):959-977
[6] J. Mendoza-Camargo et al. On the parameters identification of the Duffing's system by means of a reduced order observer. Physics Letters A 331, 2004: 316-324
[7] M. Brucoli, L. Carnimeo, L. Grassi. A method for the synchronization of hyperchaotic circuit. Int. J. Bifurcation and chaos, 1996, 6(9):1673-1681