International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal | www.ijtsrd.com

ISSN No: 2456 - 6470 | Volume - 3 | Issue – 1 | Nov – Dec 2018

A Novel Design Architecture of Secure Communication System with Reduced-Order Linear Receiver

Yeong-Jeu Sun
Professor, Department of Electrical Engineering, I-Shou University, Kaohsiung, Taiwan

ABSTRACT

In this paper, a new concept about secure communication system is introduced and a novel secure communication design with reduced-order linear receiver is developed to guarantee the global exponential stability of the resulting error signals. Besides, the guaranteed exponential convergence rate of the proposed secure communication system can be correctly calculated. Finally, some numerical simulations are given to demonstrate the feasibility and effectiveness of the obtained results.

Key Words: *Chaotic system, secure communication system, reduced-order linear receiver*

1. INTRODUCTION

As we know, because chaotic system is highly sensitive to initial value, the output behaves like a random signal. Frequently, chaos in many dynamic systems is an origin of the generation of oscillation and an origin of instability. Several kinds of chaotic systems have been widely applied in various applications such as secure communication, master-slave chaotic systems, image encryption, biological systems, chemical reactions, system identification, and ecological systems; see, for instance, [1-3] and the references therein.

In recent years, numerous secure communications have been extensively explored; see, for example, [4-12] and the references therein. Generally speaking, a secure communication is composed of transmitter and receiver and reduced-order linear receiver has the merits of low price and easy implementation. Therefore, searching a lower-dimensional reduced-order linear receiver for the secure chaotic communication system constitutes an important area for practical control design.

In this paper, we will propose a new idea about secure communication system and a novel design of secure communication system with reduced-order linear receiver will be developed to guarantee that the resulting error signals can converge to zero in some exponential convergence rate. Meanwhile, the guaranteed exponential convergence rate of the proposed chaotic secure communication system can be accurately estimated. Finally, some numerical simulations are proposed to exhibit the capability and feasibility of the main results.

This paper is organized as follows. The problem formulation and main results are presented in Section 2. Several numerical simulations are given in Section 3 to illustrate the main result. Finally, conclusion remarks are drawn in Section 4. Throughout this paper, $\Re^n$ denotes the n-dimensional Euclidean space, $\|x\| := \sqrt{x^T \cdot x}$ denotes the Euclidean norm of the column vector x, and $|a|$ denotes the absolute value of a real number a.

2. PROBLEM FORMULATION AND MAIN RESULTS

In this paper, we develop the following new secure communication system with simple reduced-order linear receiver and its block diagram is shown in Figure 1.

Transmitter:

$$\dot{x}_1(t) = a_1 x_2(t) x_3(t), \tag{1a}$$

$$\dot{x}_2(t) = a_2 x_1(t) + a_3 x_2(t), \tag{1b}$$

$$\dot{x}_3(t) = a_4 + a_5 x_1(t) x_2(t), \tag{1c}$$

$$y(t) = a_6 x_1(t) + a_7 x_2(t), \tag{1d}$$

$$\phi_m(t) = C_m x(t) + m_1(t), \quad \forall\, t \ge 0. \tag{1e}$$

Receiver:

$$z_1(t) = -\frac{a_7}{a_6} z_2(t) + \frac{1}{a_6} y(t), \qquad (2a)$$

$$\dot{z}_2(t) = -\left(\frac{a_2 a_7}{a_6} - a_3\right) z_2(t) + \frac{a_2}{a_6} y(t), \qquad (2b)$$

$$m_2(t) = \phi_m(t) - C_m z(t), \quad \forall\, t \geq 0, \qquad (2c)$$

where $x(t) := [x_1(t) \quad x_2(t)]^T \in \Re^2$ is the partial state vector of transmitter, $y(t) \in \Re$ is the output of transmitter, $z(t) := [z_1(t) \quad z_2(t)]^T \in \Re^2$ is the state vector of receiver, $m_1(t) \in \Re^{q \times 1}$ is the information vector, $C_m \in \Re^{q \times 2}$, and $m_2(t) \in \Re^{q \times 1}$ is the signal recovered from $m_1(t)$, with $q \in N$. It is noted that the chaotic Sprott B system is the special case of the system (1) with $a_1 = a_2 = a_3 = -a_3 = -a_5 = 1$. In the sequel, we adopt the same parameters of the chaotic Sprott B system with $a_6 a_7 > 0$. Apparently, a good secure communication system means that we can recover the message $m_1(t)$ in the receiver system; i.e., the error vector $e(t) := m_2(t) - m_1(t)$ can converge to zero in some sense.

Before presenting the main result, let us introduce a definition which will be used in the main theorem.

Definition 1: The system (1) with (2) is called secure communication system with exponential convergence type if there are positive numbers k and α such that $\|e(t)\| := \|m_2(t) - m_1(t)\| \leq k \exp(-\alpha t), \quad \forall\, t \geq 0$.

In this case, the positive number α is called the exponential convergence rate.

Now we present the main results for secure communication system of (1) with (2).

Theorem 1: The system (1) with (2) is a secure communication system with exponential convergence type. Besides, the guaranteed exponential convergence rate is given by $\alpha = 1 + \frac{a_7}{a_6}$.

Proof. Define

$$w(t) = [w_1 \quad w_2]^T = [x_1 - z_1 \quad x_2 - z_2]^T \in \Re^2 . (3)$$

Thus, from (1)-(3), one has

$$\begin{aligned} \dot{w}_2(t) &= \dot{x}_2(t) - \dot{z}_2(t) \\ &= a_2 x_1(t) + a_3 x_2(t) + \left(\frac{a_2 a_7}{a_6} - a_3\right) z_{12}(t) \\ &\quad - \frac{a_2}{a_6} y(t) \\ &= a_2 x_1(t) + a_3 x_2(t) + \left(\frac{a_2 a_7}{a_6} - a_3\right) z_2(t) \\ &\quad - \frac{a_2}{a_6}\left[a_6 x_1(t) + a_7 x_2(t)\right] \\ &= \left(-\frac{a_2 a_7}{a_6} + a_3\right) x_2(t) + \left(\frac{a_2 a_7}{a_6} - a_3\right) z_2(t) \\ &= -\left(\frac{a_2 a_7}{a_6} - a_3\right)\left[x_2(t) - z_2(t)\right] \\ &= \left(-\frac{a_2 a_7}{a_6} + a_3\right) x_2(t) + \left(\frac{a_2 a_7}{a_6} - a_3\right) z_2(t) \\ &= -\left(\frac{a_2 a_7}{a_6} - a_3\right) w_2(t) \\ &= -\left(\frac{a_7}{a_6} + 1\right) w_2(t). \end{aligned}$$

This implies that

$$w_2(t) = w_2(0) \cdot \exp\left[-\left(\frac{a_7}{a_6} + 1\right) t\right]. \qquad (4)$$

From (1)-(4), it is easy to see that

$$\begin{aligned} w_1(t) &= x_1(t) - z_1(t) \\ &= \left[\frac{1}{a_6} y(t) - \frac{a_7}{a_6} x_2(t)\right] \\ &\quad - \left[-\frac{a_7}{a_6} z_2(t) + \frac{1}{a_6} y(t)\right] \\ &= -\frac{a_7}{a_6}\left[x_2(t) - z_2(t)\right] \\ &= -\frac{a_7}{a_6} w_2(t) \\ &= -\frac{a_7 w_2(0)}{a_6} \cdot \exp\left[-\left(\frac{a_7}{a_6} + 1\right) t\right]. \qquad (5) \end{aligned}$$

Hence, from (3)-(5), it results

$$\begin{aligned} \|w(t)\| &= \sqrt{w_1^2(t) + w_2^2(t)} \\ &\leq \sqrt{\frac{a_6^2 + a_7^2}{a_6^2}} \cdot |w_2(0)| \\ &\quad \cdot \exp\left[-\left(\frac{a_7}{a_6} + 1\right) t\right], \quad \forall\, t \geq 0. \qquad (6) \end{aligned}$$

Thus, it can be readily obtained that

$$\begin{aligned} \|e(t)\| &= \|m_2(t) - m_1(t)\| \\ &= \|\phi_m(t) - C_m z(t) - \phi_m(t) + C_m x(t)\| \\ &\leq \|C_m\| \cdot \|w(t)\| \\ &\leq \sqrt{\frac{a_6^2 + a_7^2}{a_6^2}} \cdot |w_2(0)| \cdot \|C_m\| \\ &\quad \cdot \exp\left[-\left(\frac{a_7}{a_6} + 1\right) t\right], \ \forall\, t \geq 0, \end{aligned}$$

in view of (1), (2), and (6). This completes the proof.

Remark 1: It should be emphasized that the proposed receiver of (2) is linear and with lower dimensions than that of the transmitter. Consequently, the proposed receiver of (2) has the superiorities of low price and easy implementation by electronic circuit.

3. NUMERICAL SIMULATIONS

Consider the novel secure communication system of (1)-(2) with $a_6 = a_7 = 1$ and $C_m = [1 \ \ -1]$. By Theorem 1, the synchronization of signals $m_1(t)$ and $m_2(t)$ for the proposed secure communication (1)-(2) can be achieved with guaranteed convergence rate of $\alpha = 2$. The real message $m_1(t)$, the recovered message $m_2(t)$, and the error signal are depicted in Figure 2-Figure 4, respectively, which clearly indicates that the real message $m_1(t)$ is recovered after 3 seconds.

4. CONCLUSION

In this paper, a new concept about secure communication system has been introduced and a novel secure communication design with reduced-order linear receiver has been developed to guarantee the global exponential stability of the resulting error signals. Meanwhile, the guaranteed exponential convergence rate of the proposed secure communication system can be correctly calculated. Finally, some numerical simulations have been offered to show the feasibility and effectiveness of the obtained results.

ACKNOWLEDGEMENT

The author thanks the Ministry of Science and Technology of Republic of China for supporting this work under grants MOST 106-2221-E-214-007, MOST 106-2813-C-214-025-E, and MOST 107-2221-E-214-030. Besides, the author is grateful to Chair Professor Jer-Guang Hsieh for the useful comments.

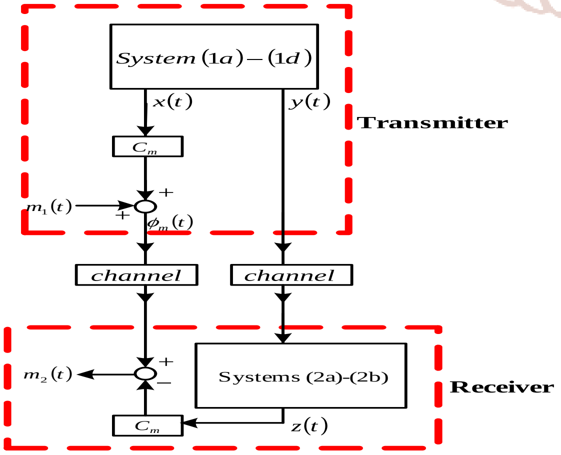

Figure 1: Secure-communication scheme ($m_1(t)$ is the information vector and $m_2(t)$ is the recovered vector).

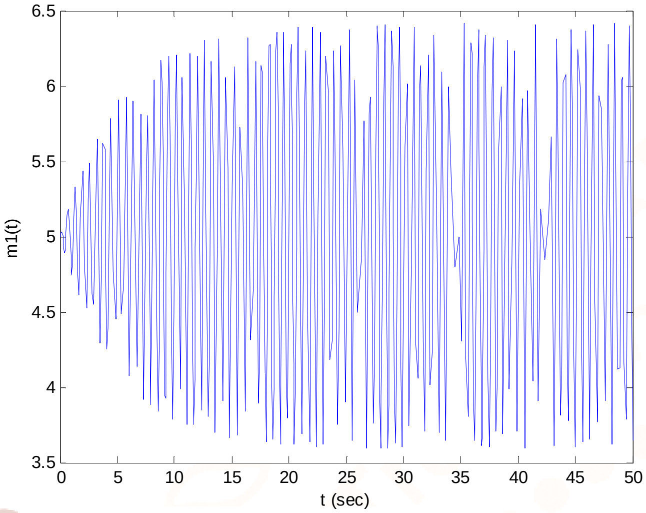

Figure 2: Real message of $m_1(t)$ described in the transmitter of (1).

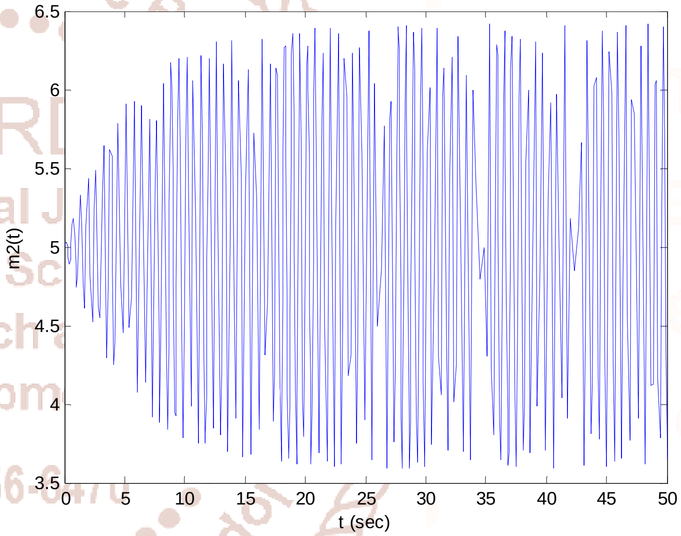

Figure 3: Recoverd message of $m_2(t)$ described in the receiver of (2).

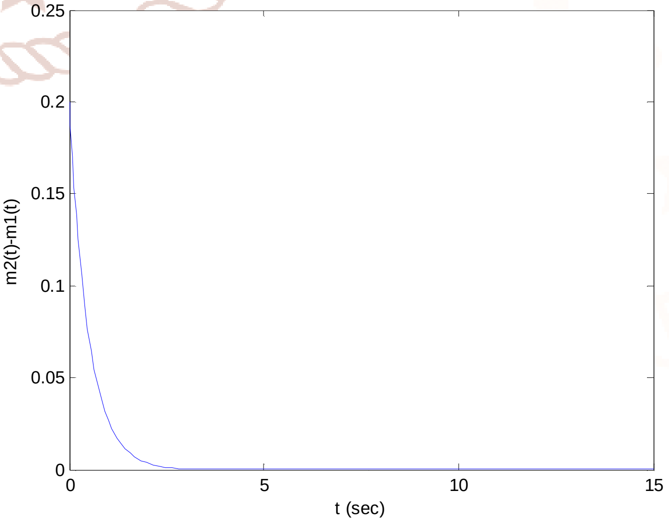

Figure 4: Error signal of $m_2(t) - m_1(t)$.

REFERENCES

1. Y.J. Xian, C . Xia, T.T. Guo, K.R. Fu, and C.B. Xu, “Dynamical analysis and FPGA implementation of a large range chaotic system with coexisting attractors,” Results in Physics, vol. 11, pp. 368-376, 2018.
2. L. Xiong, S. Zhang, Y. Zeng, and B. Liu, “Dynamics of a new composite four-Scroll chaotic system,” Chinese Journal of Physics, vol. 56, pp. 2381-2394, 2018.
3. Y.Wang and H. Yu, “Fuzzy synchronization of chaotic systems via intermittent control,” Chaos, Solitons & Fractals, vol. 106, pp. 154-160, 2018.
4. A.A. Zaher, “Duffing oscillators for secure communication,” Computers & Electrical Engineering, vol. 71, pp. 77-92, 2018.
5. S. Çiçek, U.E. Kocamaz, and Y. Uyaroğlu, “Secure communication with a chaotic system owning logic element,” AEU-International Journal of Electronics and Communications, vol. 88, pp. 52-62, 2018.
6. J. Hua, L. Chai, D. Xiong, and W. Wang, “A novel method of realizing stochastic chaotic secure communication by synchrosqueezed wavelet transform,” Digital Signal Processing, vol. 82, pp. 194-202, 2018.
7. Z. Sun, L. Si, Z. Shang, and J. Lei, “Finite-time synchronization of chaotic PMSM systems for secure communication and parameters identification,” Optik, vol. 157, pp. 43-55, 2018.
8. P. Vijayakumar, V. Chang, L.J. Deborah, and B.R Kshatriya, “Key management and key distribution for secure group communication in mobile and cloud network,” Future Generation Computer Systems, vol. 84, pp. 123-125, 2018.
9. N. Vafamand, S. Khorshidi, and A. Khayatian, “Secure communication for non-ideal channel via robust TS fuzzy observer-based hyperchaotic synchronization,” Chaos, Solitons & Fractals, vol. 112, pp. 116-124, 2018.
10. L. Wang and X. Liu, “Secure cooperative communication scheme for vehicular heterogeneous networks,” Vehicular Communications, vol. 11, pp. 46-56, 2018.
11. D. Chang, Z. Li, M. Wang, and Y. Zeng, “A novel digital programmable multi-scroll chaotic system and its application in FPGA-based audio secure communication,” AEU-International Journal of Electronics and Communications, vol. 88, pp. 20-29, 2018.
12. A. A. Saad, S. Ahmad, S. Azzam, and A. A. Nedaa, “Securing robot communication using packet encryption distribution,” Network Security, vol. 2018, pp. 8-14, 2018.