IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, December 2022
Impact Factor: 6.252

New Design of Secure Communication System Based on Dynamic Linear Receiver

Yeong-Jeu Sun[1], Feng-Yi Sung[2], Xiang-Yu Wang[3]
Professor, Department of Electrical Engineering[1]
Students, Department of Electrical Engineering [2,3]
I-Shou University, Kaohsiung, Taiwan

Abstract: *In this paper, the design issues of the chaotic secure communication system will be scientifically explored. Based on time-domain analysis, a new secure communication system with dynamic linear receivers will be constructed. This secure communication system can not only make the error signal close to zero, but also can correctly calculate its exponential convergence rate. Finally, several numerical simulation results are proposed to illustrate the practicability and correctness of the main results.*

Keywords: Secure communication system, Dynamic linear receiver, Moore-Spiegel chaotic oscillator, Exponential convergence rate

I. INTRODUCTION

In recent years, various types of secure communication systems have been extensively investigated and proposed by experts and scholars; see, for instance, [1]-[8] and the references therein. Due to the highly unpredictability of chaotic signals, the security communication system with chaos theory can be said to be the leader of the security communication system.

It is well known that dynamic linear receivers have the advantages of easy hardware implementation and low cost. How to design a secure communication system with a dynamic linear receiver has always been a subject that experts in communication security systems are eager to overcome.

Based on the above reasons, this paper intends to design a chaotic secure communication system with a dynamic linear receiver. Besides, time-domain analysis method is also used to verify the convergence of the error signal, and at the same time, the exponential convergence rate is also calculated rigorously. Throughout this paper, $\|x\| := \sqrt{x^T \cdot x}$ denotes the Euclidean norm of the column vector x and $|a|$ denotes the absolute value of a real number a.

II. PROBLEM FORMULATION AND MAIN RESULTS

In this paper, we propose the following secure communication system with dynamic linear receiver and its architectural diagram is shown in Fig. 1.

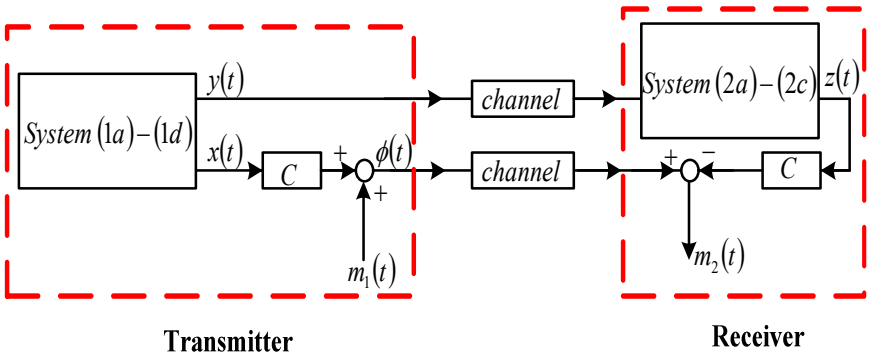

Fig. 1 Architectural diagram of secure communication system ($m_1(t)$ is the sending signal and $m_2(t)$ is the receiving signal).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, December 2022
Impact Factor: 6.252

2.1 Transmitter

$$\dot{x}_1 = x_2 \tag{1a}$$

$$\dot{x}_2 = x_3 \tag{1b}$$

$$\dot{x}_3 = ax_1 + bx_2 + cx_3 + dx_1^2 x_2, \quad \forall\, t \geq 0 \tag{1c}$$

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

$$\phi(t) = Cx(t) + m_1(t), \quad \forall\, t \geq 0. \tag{1e}$$

2.2 Receiver

$$\dot{z}_1(t) = \frac{-\alpha}{\beta} z_1(t) + \frac{1}{\beta} y(t), \tag{2a}$$

$$z_2(t) = \frac{-\alpha}{\beta} z_1(t) + \frac{1}{\beta} y(t), \tag{2b}$$

$$z_3(t) = \frac{-\alpha}{\beta} z_2(t) + \frac{1}{\beta} \dot{y}(t), \tag{2c}$$

$$m_2(t) = \phi(t) - Cz(t), \quad \forall\, t \geq 0, \tag{2d}$$

where $x(t) := [x_1(t) \quad x_2(t) \quad x_3(t)]^T \in \Re^{3\times 1}$ is the state vector of transmitter, $y(t) \in \Re$ is the output of transmitter, $z(t) := [z_1(t) \quad z_2(t) \quad z_3(t)]^T \in \Re^{3\times 1}$ is the state vector of receiver, $m_1(t)$ is the sending signal, and $m_2(t)$ is the receiving signal. In addition, parameters α, β and nonzero matrix $C \in \Re^{1\times 3}$ can be designed arbitrarily with $\alpha\beta > 0$. It is noted that the Moore-Spiegel chaotic oscillator is the special case of the system (1) with $a = -6, b = 14, c = -1$, and $d = -20$. Apparently, a high-quality secure communication system means that we can recover the sending signal $m_1(t)$ in the receiver system; i.e., the error vector $e(t) := m_2(t) - m_1(t)$ can approach zero.

The definition of exponential secure communication system is as follows.

Definition 1: If there are positive numbers k and γ satisfying the inequality

$$|e(t)| := |m_2(t) - m_1(t)| \leq k \exp(-\gamma t), \quad \forall\, t \geq 0,$$

system (1) with (2) is called exponential secure communication system. In this case, the positive number γ is called the exponential convergence rate.

Now we present the main results.

Theorem 1: The system (1) with (2) is an exponential secure communication system. Besides, the guaranted exponential convergence rate is given by $\gamma = \frac{\alpha}{\beta}$.

Proof. Let us define

$$w(t) = [w_1(t) \quad w_2(t) \quad w_3(t)]^T = x(t) - z(t) \in \Re^3. \tag{3}$$

Thus, from (1)-(3), it can be readily obtain that

$$\begin{cases} \dot{w}_1(t) = \dfrac{-\alpha}{\beta} w_1(t), \\ w_2(t) = \dfrac{-\alpha}{\beta} w_1(t), \\ w_3(t) = \dfrac{-\alpha}{\beta} w_2(t), \quad \forall\, t \geq 0. \end{cases}$$

It follows that

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, December 2022
Impact Factor: 6.252

$$\begin{cases} w_1(t) = e^{\frac{-\alpha}{\beta}t} w_1(0), \\ w_2(t) = \dfrac{-\alpha}{\beta} \cdot e^{\frac{-\alpha}{\beta}t} w_1(0), \\ w_3(t) = \left(\dfrac{\alpha}{\beta}\right)^2 \cdot e^{\frac{-\alpha}{\beta}t} w_1(0), \quad \forall\, t \geq 0. \end{cases}$$

Thus, one has

$$\|w(t)\| \leq \sqrt{1+\left(\frac{\alpha}{\beta}\right)^2+\left(\frac{\alpha}{\beta}\right)^4} \cdot |w_1(0)| \cdot e^{\frac{-\alpha}{\beta}t}, \quad \forall\, t \geq 0. \qquad (4)$$

It is easy to see that

$$\begin{aligned} |e(t)| &= |m_2(t) - m_1(t)| \\ &= |\phi(t) - Cz(t) - \phi(t) + Cx(t)| \\ &\leq \|C\| \cdot \|w(t)\| \\ &\leq \sqrt{1+\left(\frac{\alpha}{\beta}\right)^2+\left(\frac{\alpha}{\beta}\right)^4} \cdot \|C\| \cdot |w_1(0)| \cdot e^{\frac{-\alpha}{\beta}t}, \quad \forall\, t \geq 0, \end{aligned}$$

in view of (1e), (2d), and (4). This completes the proof.

Remark 1: It is worth mentioning that the dynamic linear receiver of (2) has the dual advantages of easy hardware implementation and low cost.

III. NUMERICAL SIMULATIONS

Consider the new secure communication system of (1)-(2) with $(a,b,c,d) = (-6{,}14{,}-1{,}-20)$, $(\alpha,\beta) = (1{,}0.1)$, and $C = [4 \quad 1 \quad 0]$. By Theorem 1, the signals $m_1(t)$ and $m_2(t)$ can achieve global exponential synchronization.

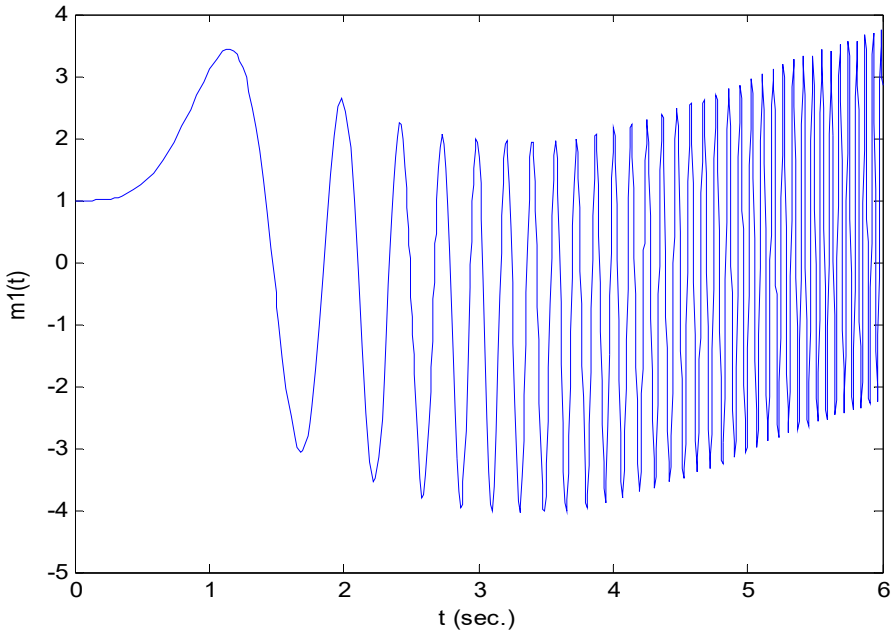

Fig. 2. Sending signal of $m_1(t)$ described in the transmitter of (1).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, December 2022
Impact Factor: 6.252

Moreover, the guaranteed exponential converence rate is given by $\gamma = 10$. The sending signal $m_1(t)$, the receiving signal $m_2(t)$, and the error signal are shown in Fig.2-Fig. 4, respectively. It can be clearly seen that the two signals of $m_1(t)$ and $m_2(t)$ can reach the goal of synchronization after about 0.8 seconds.

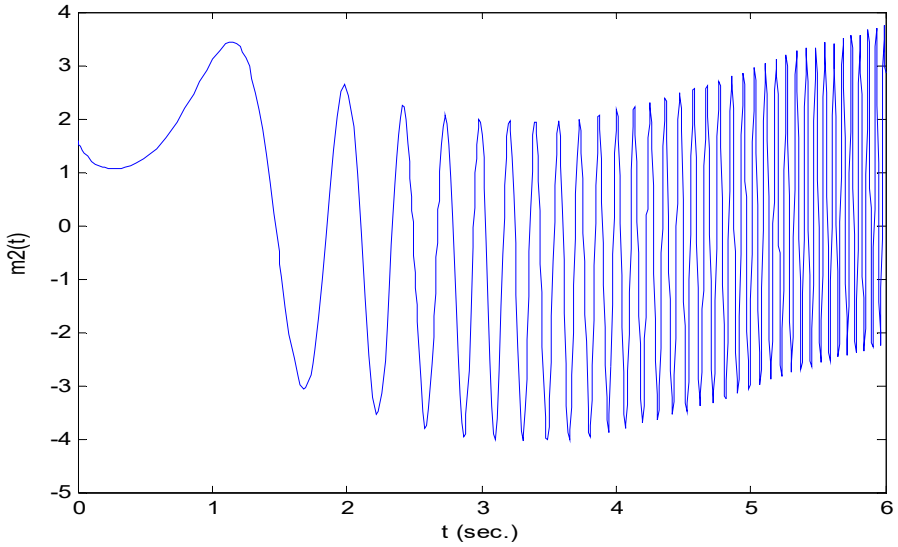

Fig. 3. Receiving signal of $m_2(t)$ described in in the receiver of (2).

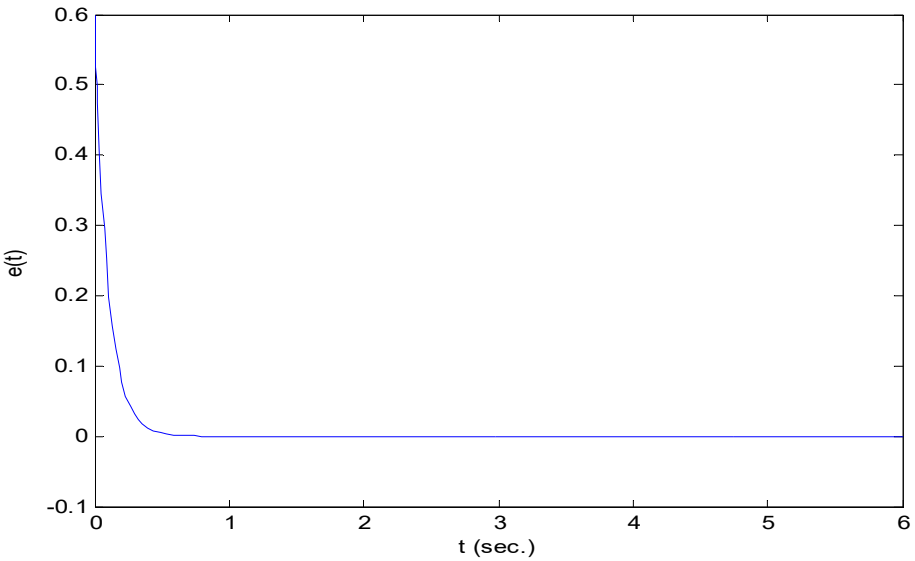

Fig. 4. Error signal of $e(t) := m_2(t) - m_1(t)$.

IV. CONCLUSION

In this paper, the design issue of the chaotic secure communication system has been scientifically explored. Based on time-domain analysis, a new secure communication system with dynamic linear receivers has been developed. This secure communication system can not only make the error signal close to zero, but also can correctly calculate its exponential convergence rate. Finally, several numerical simulation results have been proposed to illustrate the practicability and correctness of the main results.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 2, December 2022
Impact Factor: 6.252

V. ACKNOWLEDGMENT

The authors thank the Ministry of Science and Technology of Republic of China for supporting this work under grants MOST 107-2221-E-214-030 and MOST 109-2221-E-214-014.

REFERENCES

[1]. S.A. Gebereselassie and B.K. Roy, "A new secure speech communication scheme based on hyperchaotic masking and modulation," IFAC, vol. 55, no. 1, pp. 914-919, 2022.

[2]. Y.J. Sun, C.M. Chuang, and T.C. Chang, "Design of chaotic secure communication system based on laser dynamic model," International Journal of Trend in Scientific Research and Development, Vol. 6, No. 7, pp. 370-373, 2022.

[3]. K. Babanli and R.O. Kabaoğlu, "Fuzzy modeling of desired chaotic behavior in secure communication systems," Information Sciences, vol. 594, pp. 217-232, 2022.

[4]. Y.J. Sun, "New design architecture of chaotic secure communication system combined with linear receiver," International Journal of Trend in Scientific Research and Development, vol. 5, no. 1, pp. 1394-1396, 2020.

[5]. F. Zhu, F. Wang, and L. Ye, "Artificial switched chaotic system used as transmitter in chaos-based secure communication," Journal of the Franklin Institute, vol. 357, no. 15, pp. 10997-11020, 2020.

[6]. Y.J. Sun, "A novel design of secure communication system with linear receiver," Journal of Multidisciplinary Engineering Sciences and Technology, vol. 4, no. 10, pp. 8451-8453, 2017.

[7]. C. Zhao, X. Liu, and Q. Zhong, "Secure consensus of multi-agent systems with redundant signal and communication interference via distributed dynamic event-triggered control," ISA Transactions, vol. 112, pp. 89-98, 2020.

[8]. Y.J. Sun, "A novel design architecture of secure communication system with reduced-order linear receiver," International Journal of Trend in Scientific Research and Development, vol. 3, no. 1, pp. 1154-1157, 2018.