A Novel Design Of Secure Communication System With Linear Receiver

Yeong-Jeu Sun
Department of Electrical Engineering,
I-Shou University, Kaohsiung, Taiwan 840, R.O.C.
Email: yjsun@isu.edu.tw; Fax: 886-7-6577205

***Abstract*—In this paper, a new concept about secure communication system is firstly introduced and a novel secure communication design with 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.**

Keywords—Chaotic system; secure communication system; linear receiver

I. INTRODUCTION

It is well-known that since chaotic system is exceedingly sensitive to initial conditions and the output behaves like a random signal, several kinds of chaotic systems have been widely applied in various applications such as secure communication, image encryption, master-slave chaotic systems, chemical reactions, ecological systems, biological systems, and system identification; see, for instance, [1]-[3] and the references therein.

Over the past decade, numerous secure communications have been extensively explored; see, for example, [3-6] and the references therein. Generally speaking, a secure communication is composed of transmitter and receiver. In particular, linear receiver has the advantages of low price and easy implementation. Therefore, searching a lower-dimensional linear receiver for the secure chaotic communication system constitutes an important area for practical control design.

In this paper, we will firstly propose a new concept about secure communication system and A novel design of secure communication system with linear receiver will be developed to guarantee that the resulting error signals can converge to zero in some exponential convergence rate. Furthermore, the guaranteed exponential convergence rate of the proposed chaotic secure communication system can be accurately estimated. Finally, some numerical simulations are given 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 II. Several numerical simulations are given in Section III to illustrate the main result. Finally, conclusions are made in Section IV. 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*.

II. PROBLEM FORMULATION AND MAIN RESULTS

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

Transmitter:

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

$$\dot{x}_2(t) = x_1(t) + ax_2(t), \tag{1b}$$

$$\dot{x}_3(t) = -cx_3(t) + x_1(t)x_3(t) + b, \tag{1c}$$

$$y(t) = -x_1(t) + x_3(t), \tag{1d}$$

$$\phi_h(t) = C_h x(t) + h(t), \quad \forall\, t \geq 0. \tag{1e}$$

Receiver:

$$\dot{z}_1(t) = -z_1(t) - z_2(t) - y(t), \tag{2a}$$

$$\dot{z}_2(t) = z_1(t) + az_2(t), \tag{2b}$$

$$z_3(t) = z_1(t) + y(t), \tag{2c}$$

$$h_1(t)=\phi_h(t)-C_h z(t), \quad \forall\, t\geq 0, \tag{2d}$$

where $x(t):=[x_1(t) \quad x_2(t) \quad x_3(t)]^T \in\Re^3$ is the state vector of transmitter, $y(t)\in\Re$ is the output of transmitter, $z(t):=[z_1(t) \quad z_2(t) \quad z_3(t)]^T \in\Re^3$ is the state vector of receiver, $h(t)\in\Re^{q\times 1}$ is the information vector, $C_h\in\Re^{q\times 3}$, and $h_1(t)\in\Re^{q\times 1}$ is the signal recovered from $h(t)$, with $q\in N$. It is noted that the Rossler chaotic system is the special case of the system (1) with $a=0.2, b=0.2, c=5.7$. In the sequel, we adopt the same parameters of the Rossler chaotic system. Undoubtedly, a good secure communication system means that we can recover the message $h(t)$ in the receiver system; i.e., the error vector $e(t):=h_1(t)-h(t)$ 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

$$\|e(t)\|:=\|h_1(t)-h(t)\|\leq k\exp(-\alpha t), \quad \forall\, t\geq 0.$$

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 guaranted exponential convergence rate is given by $\alpha=0.4$.

Proof. 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), one has

$$\begin{bmatrix}\dot{w}_1(t)\\ \dot{w}_2(t)\end{bmatrix}=\begin{bmatrix}-1 & -1\\ 1 & 0.2\end{bmatrix}\begin{bmatrix}w_1(t)\\ w_2(t)\end{bmatrix}:=A\begin{bmatrix}w_1(t)\\ w_2(t)\end{bmatrix} \text{ and } w_3(t)=w_1(t)$$

This implies that

$$\begin{bmatrix}w_1(t)\\ w_2(t)\end{bmatrix}=e^{At}\begin{bmatrix}w_1(0)\\ w_2(0)\end{bmatrix} \text{ and } w_3(t)=w_1(t), \text{ for every } t\geq 0.$$

Hence, it results

$$\left\|\begin{bmatrix}w_1(t)\\ w_2(t)\end{bmatrix}\right\|\leq k_1 e^{-0.4t} \text{ and } |w_3(t)|=|w_1(t)|\leq\left\|\begin{bmatrix}w_1(t)\\ w_2(t)\end{bmatrix}\right\|\leq k_1 e^{-0.4t}$$

Thus, it is easy to see that

$$\begin{aligned}\|w(t)\|&=\sqrt{\left\|\begin{bmatrix}w_1(t)\\ w_2(t)\end{bmatrix}\right\|^2+|w_3(t)|^2} \\ &\leq\sqrt{2k_1^2 e^{-0.8t}}=\sqrt{2}k_1 e^{-0.4t}, \quad \forall\, t\geq 0.\end{aligned} \tag{4}$$

It can be readily obtained that

$$\begin{aligned}\|e(t)\|&=\|h_1(t)-h(t)\| \\ &=\|\phi_h(t)-C_h z(t)-\phi_h(t)+C_h x(t)\| \\ &\leq\|C_h\|\cdot\|w(t)\| \\ &\leq\sqrt{2}k_1\cdot\|C_h\|e^{-0.4t}, \quad \forall\, t\geq 0,\end{aligned}$$

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

Remark 1: It should be pointed out that the proposed receiver of (2) is linear and has the advantages of low price and easy implementation by electronic circuit.

III. Numerical Simulations

Consider the novel secure communication system of (1)-(2) with $C_h=[1 \quad -1 \quad 0]$. By Theorem 1, the synchronization of signals $h(t)$ and $h_1(t)$ for the proposed secure communication (1)-(2) can be achieved with guaranteed converence rate $\alpha=0.4$. The real message $h(t)$, the recoverd message $h_1(t)$, and the error signal are depicted in Figure 2-Figure 4, respectively, which clearly indicateds that the real message $h(t)$ is recoved after 15 seconds.

Conclusions

In this paper, a new concept about secure communication system has been firstly introduced and a novel secure communication design with 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.

Acknowledgments

The author thanks the Ministry of Science and Technology of Republic of China for supporting this work under grants MOST 105-2221-E-214-025, MOST 106-2221-E-214-007, and MOST 106-2813-C-214-025-E.

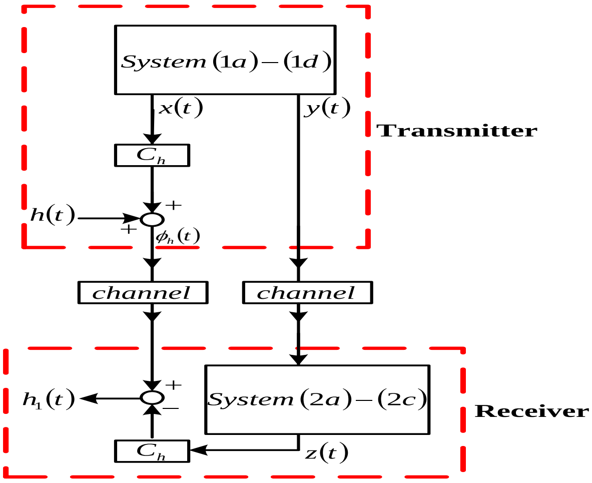

Figure 1: Secure-communication scheme ($h(t)$ is the information vector and $h_1(t)$ is the recovered vector).

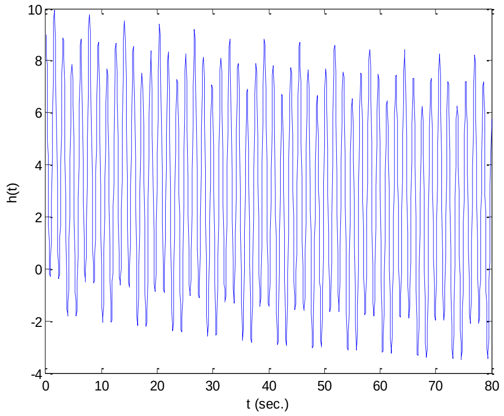

Figure 2: Real message of $h(t)$ described in the transmitter of (1).

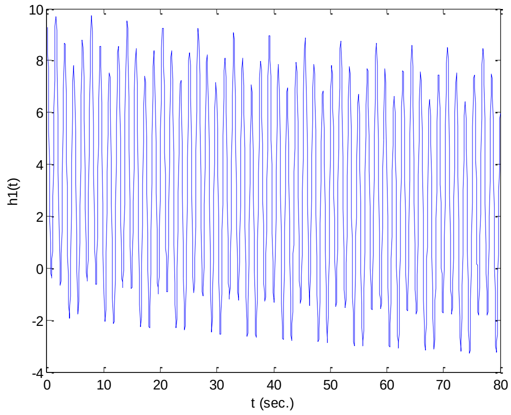

Figure 3: Recoverd message of $h_1(t)$ described in in the receiver of (2).

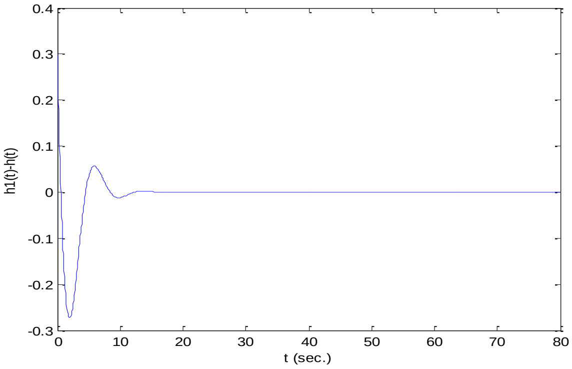

Figure 4: Error signal of $h_1(t)-h(t)$.

REFERENCES

[1] S He, K Sun and H Wang, “Multivariate permutation entropy and its application for complexity analysis of chaotic systems,” Physica A: Statistical Mechanics and its Applications, vol 461: 812-823, 2016.

[2] D S Laiphrakpam and M S Khumanthem, “Cryptanalysis of symmetric key image encryption using chaotic Rossler system,” Optik-International Journal for Light and Electron Optics, vol 135: 200-209, 2017.

[3] B Wang, S M Zhong and X C Dong, “On the novel chaotic secure communication scheme design,” Communications in Nonlinear Science and Numerical Simulation, vol 39: 108-117, 2016.

[4] S Raza, T Helgason, P Papadimitratos and T Voigt, “End-to-end secure communication architecture for the cloud-connected Internet of Things,” Future Generation Computer Systems, vol 77: 40-51, 2017.

[5] Y Allouche, E M. Arkin, Y Cassuto, A Efrat and M Segal, “Secure communication through jammers jointly optimized in geography and time,” Pervasive and Mobile Computing, vol 41: 83-105, 2017.

[6] G Xu, J Xu, C Xiu, F Liu and Y Zang, “Secure communication based on the synchronous control of hysteretic chaotic neuron,” Neurocomputing, vol 227: 108-112, 2017.