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, \( \mathbb{R}^n \) 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:
\[
\begin{align*}
\dot{x}_1(t) &= -x_2(t) - x_1(t), \quad (1a) \\
\dot{x}_2(t) &= x_1(t) + ax_2(t), \quad (1b) \\
\dot{x}_3(t) &= -cx_3(t) + x_1(t)x_2(t) + b, \quad (1c) \\
y(t) &= x_1(t) + x_2(t), \quad (1d) \\
\phi(t) &= C_x x(t) + h(t), \quad \forall \ t \geq 0. \quad (1e)
\end{align*}
\]

Receiver:
\[
\begin{align*}
\dot{z}_1(t) &= -z_2(t) - z_3(t) - y(t), \quad (2a) \\
\dot{z}_2(t) &= z_1(t) + az_2(t), \quad (2b) \\
z_3(t) &= z_1(t) + y(t), \quad (2c)
\end{align*}
\]
\[ h_i(t) = \phi_i(t) - C_i z(t), \quad \forall t \geq 0, \quad (2d) \]

where \( x(t) = [x_i(t) \ x_j(t) \ x_k(t) ]^T \in \mathbb{R}^3 \) is the state vector of transmitter, \( y(t) \in \mathbb{R} \) is the output of transmitter, \( z(t) = [z_i(t) \ z_j(t) \ z_k(t) ]^T \in \mathbb{R}^3 \) is the state vector of receiver, \( h(t) \in \mathbb{R}^{q_1} \) is the information vector, \( C_h \in \mathbb{R}^{q_1} \), and \( h(t) \in \mathbb{R}^{q_1} \) is the signal recovered from \( h(t) \), with \( q \in \mathbb{N} \). 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 \( e(t) = h(t) - h(t) \) 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 \( \alpha \) such that
\[
\| e(t) \| = \| h(t) - h(t) \| \leq k \exp(-\alpha t), \quad \forall t \geq 0.
\]

In this case, the positive number \( \alpha \) 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 \( \alpha = 0.4 \).

**Proof.** Define
\[
w(t) = [w_i(t) \ w_j(t) \ w_k(t)]^T = x(t) - z(t) \in \mathbb{R}^3.
\]

Thus, from (1)-(3), one has
\[
[w_i(t)] = \begin{bmatrix} -1 & -1 & 1 \\ 0 & 1 & 0.2 \end{bmatrix} \begin{bmatrix} w_i(t) \\ w_j(t) \end{bmatrix} = A \begin{bmatrix} w_i(t) \\ w_j(t) \end{bmatrix} \quad \text{and} \quad w_k(t) = w_k(t)
\]

This implies that
\[
\begin{bmatrix} w_i(t) \\ w_j(t) \end{bmatrix} = e^{At} \begin{bmatrix} w_i(0) \\ w_j(0) \end{bmatrix} \quad \text{and} \quad w_k(t) = w_k(t), \text{ for every } t \geq 0.
\]

Hence, it results
\[
\begin{bmatrix} w_i(t) \\ w_j(t) \end{bmatrix} \leq k e^{-0.4t} \quad \text{and} \quad |w_k(t)| = |w_k(t)| \leq \begin{bmatrix} w_i(t) \\ w_j(t) \end{bmatrix} \leq k e^{-0.4t}
\]

Thus, it is easy to see that
\[
\|w(t)\| = \left( \begin{bmatrix} w_i(t) \\ w_j(t) \end{bmatrix} \right)^2 + |w_k(t)|^2 \leq 2k e^{-0.4t}, \quad \forall t \geq 0.
\]

It can be readily obtained that
\[
\|e(t)\| = \|h(t) - h(t)\| = \|\phi_i(t) - C_i z(t) - \phi_i(t) + C_i x(t)\| \leq \|C_i\| \|w(t)\| \leq \sqrt{2k_i} \|C_i\| e^{-0.4t}, \quad \forall t \geq 0.
\]

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 \( h(t) \) for the proposed secure communication (1)-(2) can be achieved with guaranteed convergence rate \( \alpha = 0.4 \).

The real message \( h(t) \), the recovered message \( h(t) \), and the error signal are depicted in Figure 2-Figure 4, respectively, which clearly indicateds that the real message \( h(t) \) is recovered 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: Recovered message of $h_1(t)$ described in in the receiver of (2).

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

REFERENCES


