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.

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, $\mathbb{R}^n$ denotes the n-dimensional Euclidean space, $\|x\| = \sqrt{x^T x}$ 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:

$$\begin{align*}
x_1(t) &= a_x x_1(t) x_3(t), \quad (1a) \\
x_2(t) &= a_x x_1(t) + a_y x_2(t), \quad (1b) \\
x_3(t) &= a_4 x_1(t) x_2(t), \quad (1c) \\
y(t) &= a_y x_1(t) + a_y x_2(t), \quad (1d) \\
\phi(t) &= C_{\omega} x(t) + m(t), \quad \forall t \geq 0. \quad (1e)
\end{align*}$$
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
\[
\|e(t)\| := \|m_2(t) - m_1(t)\| \leq k \exp(-\alpha t), \quad \forall t \geq 0.
\]
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 \( \alpha = 1 + \frac{a_2}{a_6} \).

Proof. Define
\[
w(t) = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} x_1 - z_1 \\ x_2 - z_2 \end{bmatrix} \in \mathbb{R}^2.
\]
Thus, from (1)-(3), one has
\[
\dot{w}(t) = \begin{bmatrix} a_2 x_1(t) + a_3 x_2(t) + \left( \frac{a_2 a_3}{a_6} - a_3 \right) z_2(t) \\ - \frac{a_2}{a_6} y(t) \end{bmatrix} = a_2 x_1(t) + a_3 x_2(t) + \left( \frac{a_2 a_3}{a_6} - a_3 \right) z_2(t) - \frac{a_2}{a_6} \left[ a_1 x_1(t) + a_3 x_2(t) \right]
\]
\[
= \begin{bmatrix} \frac{a_2}{a_6} + a_3 \end{bmatrix} x_1(t) + \left( \frac{a_2 a_3}{a_6} - a_3 \right) z_2(t)
\]
\[
= \begin{bmatrix} - \frac{a_2}{a_6} \end{bmatrix} x_2(t) - z_2(t)
\]
\[
= \begin{bmatrix} \frac{a_2 a_3}{a_6} + a_3 \end{bmatrix} x_1(t) + \left( \frac{a_2 a_3}{a_6} - a_3 \right) z_2(t)
\]
\[
= \begin{bmatrix} - \frac{a_2}{a_6} \end{bmatrix} w_1(t) + \left( \alpha \right) w_2(t)
\]
\[
= \begin{bmatrix} \frac{a_2}{a_6} + \frac{a_2}{a_6} \end{bmatrix} w_2(t)
\]
\[
\dot{w}_1(t) = \frac{a_2}{a_6} w_2(t) \exp \left[ -\frac{a_2}{a_6} (t) \right], \quad \forall t \geq 0.
\]

Hence, from (3)-(5), it results
\[
\|w(t)\| = \sqrt{w_1^2(t) + w_2^2(t)} \leq \sqrt{\frac{a_2^2 + a_2^2}{a_6^2} |w_2(0)|} \exp \left[ -\frac{a_2}{a_6} (t) \right], \quad \forall t \geq 0.
\]

Thus, it can be readily obtained that
\[
\|e(t)\| = \|m_2(t) - m_1(t)\| \leq \|w(t)\| \leq \sqrt{\frac{a_2^2 + a_2^2}{a_6^2} |w_2(0)|} \|C_m\| \exp \left[ -\frac{a_2}{a_6} (t) \right], \quad \forall t \geq 0,
\]
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 $a_{s} = a_{r} = 1$ and $C_{m} = [I \ -I]$. By Theorem 1, the synchronization of signals $m_{r}(t)$ and $m_{s}(t)$ for the proposed secure communication (1)-(2) can be achieved with guaranteed convergence rate of $\alpha = 2$. The real message $m_{r}(t)$, the recovered message $m_{s}(t)$, and the error signal are depicted in Figure 2-Figure 4, respectively, which clearly indicates that the real message $m_{r}(t)$ 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.
REFERENCES