Multi-Parameter Modulation for Secure Communication via Lorenz Chaos

Yanxing Song and Xinghuo Yu
Faculty of Informatics and Communication
Central Queensland University
Rockhampton QLD 4702 Australia
Email: {y.song, x.yu}@cqu.edu.au

Abstract: In this paper, a multi-parameter modulation scheme is proposed for secure communication via Lorenz chaos using an adaptive learning mechanism. It is proved using the Lyapunov method that under the scheme, the tracking performance of the scheme can be guaranteed. It is also shown that by incorporating a low pass filter structure into the structure of the receiver, good tracking performance can be achieved when the signals to be transmitted contain noises. Simulation studies are provided to demonstrate the effectiveness of the method proposed.

1. Introduction

Secure communication via chaotic synchronization has received an increasing attention recently. One approach is by means of chaotic parameter modulation [1] [2]. Its simplest form is the chaotic switching where the message signals are assumed to be binary. The message signal(s) are used to modulate one or more parameters of the chaotic transmitter. At the receiver end, the message signal(s) are decoded through chaotic synchronization.

Various strategies for communication inspired by chaotic synchronization have been proposed. Hayes *et al.* [4], [5] demonstrated that symbolic sequences can be assigned to the chaotic waveform. Cuomo *et al.* attached a message signal to the chaotic system (transmitter) output and extracting it at the receiver end. Their method is sensitive to additive noises [6]. Parlitz and Kocarev [7] and later Yang and Chua [8] developed communication strategies based on a modulated transmitter parameter. In their methods, the chaotic system structure is used for the transmitter as well as the receiver where the parameters of the receiver are modulated for message transmission. Sobiski and Thorp [7] further considered the effectiveness of these methods in the presence of noise using the extended Kalman filter. Their approach requires that the chaotic system is near linear so that a locally linearized model can be used with the extended Kalman filter for estimation. Extension of the Kalman filter based communication techniques to other chaotic systems is difficult since most chaotic systems are highly nonlinear.

In this paper, we explore the multi parameter modulation for secure communication by making use of inherent nonlinear properties of chaotic systems so that a complete and rigorous analysis of tracking convergence and effective communication can be made without any approximation. The structure of the example chaotic system, the Lorenz chaos, is chosen for a transmitter and receiver for communication. An adaptive learning mechanism is derived which enables the receiver to retrieve the message signals sent by the transmitter. Comparing with the existing results, no approximation is required and the tracking performance is guaranteed with a rigorous analysis using the Lyapunov method. The method is verified via a simulation study.

This paper is organized as follows. Section 2 presents the main idea of multi-parameter modulation via the Lorenz chaos for communication. Section 3 shows the simulation results. Conclusion is drawn in Section 4.

2. Multi-Parameter Modulation for Secure Communication

We first present the basic idea of parameter modulation for secure communication using the Lorenz chaos. The Lorenz system is given

$$\begin{aligned} \dot{x} &= c(y-x) \\ \dot{y} &= -xz + rx - y \\ \dot{z} &= xy - bz \end{aligned} \tag{1}$$

which will be used as a master system (transmitter) to carry message signals via its parameters. A well known tailored slaver system (receiver) for synchronization is [10]

$$\begin{aligned} \dot{\tilde{x}} &= c(\tilde{y}-\tilde{x}) \\ \dot{\tilde{y}} &= -x\tilde{z} + rx - \tilde{y} \\ \dot{\tilde{z}} &= x\tilde{y} - b\tilde{z} \end{aligned} \tag{2}$$

It has been proved that the synchronization will take place between (1) and (2) [10].

Now we first choose the parameter r as a carrier for message signal transmission using the tailored receiver

structure (2). The message signal we are considering is assumed binary that is only two discrete values are available for switching. Reformulating the chaotic transmitter (1) with the extended state r yields

$$\begin{aligned}\dot{x} &= c(y-x)\\ \dot{y} &= -xz + rx - y\\ \dot{z} &= xy - bz\\ \dot{r} &= 0\end{aligned} \tag{3}$$

The slave system (receiver) is also reformulated to consist of the states $\tilde{x}, \tilde{y}, \tilde{z}$ and the extended state $\tilde{r}$, which is the signal to be retrieved:

$$\begin{aligned}\dot{\tilde{x}} &= c(\tilde{y}-\tilde{x}) - k_x e_x\\ \dot{\tilde{y}} &= -x\tilde{z} + \tilde{r}x - \tilde{y} - k_y e_y\\ \dot{\tilde{z}} &= x\tilde{y} - b\tilde{z}\\ \dot{\tilde{r}} &= f_r\end{aligned} \tag{4}$$

where the function f_r is a function for learning to be determined. Now let the errors be

$$e_x = \tilde{x} - x,\ e_y = \tilde{y} - y,\ e_z = \tilde{z} - z,\ e_r = \tilde{r} - r. \tag{5}$$

If we can find the function f_r in (4) so that the synchronization between (1) and (2) is realized, then all the states of the receiver will track the corresponding states in transmitter, and of course, $\tilde{r}$ will track r. Therefore because r is the message signal carrier, the modulation of *r* will be done.

Now we look at how to derive function f_r. Subtracting (3) from (4) yields the error dynamics

$$\begin{aligned}\dot{e}_x &= c(e_y - e_x) - k_x e_x\\ \dot{e}_y &= -xe_z - e_y + e_r x - k_y e_y\\ \dot{e}_z &= xe_y - be_z\\ \dot{e}_r &= f_r\end{aligned} \tag{6}$$

Hence the synchronization between system (3) and system (4) is equivalent to that the system (6) is asymptotically stable. We now use the Lyapunov method to derive the learning function f_r so that the system (6) is asymptotically stable.

Take the Lyapunov function

$$V(e_x, e_y, e_z, e_r) = \frac{1}{2}\left(\frac{1}{c}e_x^2 + e_y^2 + e_z^2 + \frac{1}{\gamma}e_r^2\right),$$
$$\gamma > 0, c > 0.$$

Its derivative along the error dynamics (6) is

$$\begin{aligned}\dot{V} &= \frac{1}{c}e_x\dot{e}_x + e_y\dot{e}_y + e_z\dot{e}_z + \frac{1}{\gamma}e_r\dot{e}_r\\ &= \frac{1}{c}e_x(c(e_y - e_x) - k_x e_x)\\ &\quad + e_y(-xe_z - e_y + e_r x - k_y e_y)\\ &\quad + e_z(xe_y - be_z) + \frac{1}{\gamma}e_r\dot{e}_r\\ &= e_x e_y - e_x^2 - e_y^2 + e_r e_y x - be_z^2\\ &\quad + \frac{1}{\gamma}e_r\dot{e}_r - \frac{1}{c}k_x e_x^2 - k_y e_y^2\\ &= -(e_x - \frac{1}{2}e_y)^2 - \frac{3}{4}e_y^2 - be_z^2\\ &\quad - \frac{1}{c}k_x e_x^2 - k_y e_y^2 + e_r(e_y x + \frac{1}{\gamma}\dot{e}_r)\end{aligned}$$

It is obvious that if we let

$$\dot{e}_r = -\gamma e_y x,\ \gamma > 0, \tag{7}$$

Then

$$\dot{V} = -(e_x - \frac{1}{2}e_y)^2 - \frac{3}{4}e_y^2 - be_z^2 - \frac{1}{c}k_x e_x^2 - k_y e_y^2 < 0$$

which means

$$e_x \to 0,\ e_y \to 0,\ e_z \to 0,\ e_r \to 0.$$

That means asymptotical tracking of all states including r will be realized. We now derive the function f_r. From (5) and (7), we have

$$\dot{\tilde{r}} - \dot{r} = -\gamma e_y x,$$

Hence

$$\dot{\tilde{r}} = \dot{r} - \gamma e_y x = -\gamma e_y x \tag{8}$$

since $\dot{r} = 0$ almost everywhere. Therefore

$$f_r = -\gamma e_y x \tag{9}$$

The resulting receiver for modulating r is then written as

$$\begin{aligned}\dot{\tilde{x}} &= c(\tilde{y}-\tilde{x}) - k_x e_x\\ \dot{\tilde{y}} &= -x\tilde{z} + \tilde{r}x - \tilde{y} - k_y e_y\\ \dot{\tilde{z}} &= x\tilde{y} - b\tilde{z}\\ \dot{\tilde{r}} &= -\gamma e_y x\end{aligned} \tag{10}$$

Note that the knowledge of parameter r is not required in the receiver (10). Also the adaptive learning for modulating parameter r only relies on the information of state x and the error e_y. In addition, we include the low-pass filter type of feedback $k_x e_x$ and $k_y e_y$ in the first and second equations in (6) and (9), which will in turn improve the sensitivity to possible noises in the state signals.

We now study the modulation for multiple parameters for communication. We modulate all the parameters of the Lorenz system, c, r, b, concurrently. The extended master system (transmitter) consists of the states x, y, z, r, c, b.

$$\begin{aligned}
\dot{x} &= c(y-x)\\
\dot{y} &= -xz + rx - y\\
\dot{z} &= xy - bz\\
\dot{r} &= 0\\
\dot{c} &= 0\\
\dot{b} &= 0
\end{aligned} \tag{11}$$

The slave system (receiver) consists of the states $\tilde{x}, \tilde{y}, \tilde{z}, \tilde{r}, \tilde{c}, \tilde{b}$.

$$\begin{aligned}
\dot{\tilde{x}} &= \tilde{c}(\tilde{y}-\tilde{x}) - k_x e_x\\
\dot{\tilde{y}} &= -x\tilde{z} + \tilde{r}x - \tilde{y} - k_y e_y\\
\dot{\tilde{z}} &= x\tilde{y} - \tilde{b}\tilde{z} - k_z e_z\\
\dot{\tilde{r}} &= f_r\\
\dot{\tilde{c}} &= f_c\\
\dot{\tilde{b}} &= f_b
\end{aligned} \tag{12}$$

Denoting

$$\begin{aligned}
&e_x = \tilde{x} - x, e_y = \tilde{y} - y, e_z = \tilde{z} - z,\\
&e_r = \tilde{r} - r, e_c = \tilde{c} - c, e_b = \tilde{b} - b.
\end{aligned} \tag{13}$$

If we can derive the functions f_r, f_c, f_b so that the synchronization between system (11) and (12) occurs, then the modulation will be realized. We now derive the functions f_r, f_c, f_b.

Subtracting (11) from (12) arrives at the errors dynamics

$$\begin{aligned}
\dot{e}_x &= \tilde{c}(\tilde{y}-\tilde{x}) - c(y-x) - k_x e_x\\
&= \tilde{c}\tilde{y} - cy - (\tilde{c}\tilde{x} - cx) - k_x e_x\\
&= e_c(y+e_y) + ce_y - e_c(x+e_x) - ce_x - k_x e_x
\end{aligned}$$

$$\begin{aligned}
\dot{e}_y &= -x\tilde{z} + \tilde{r}x - \tilde{y} - (-xz + rx - y) - k_y e_y\\
&= -xe_z + xe_r - e_y - k_y e_y
\end{aligned}$$

$$\begin{aligned}
\dot{e}_z &= x\tilde{y} - \tilde{b}\tilde{z} - (xy - bz) - k_z e_z\\
&= xe_y - (\tilde{b}\tilde{z} - bz) - k_z e_z\\
&= xe_y - e_b(z+e_z) - be_z - k_z e_z
\end{aligned}$$

$$\begin{aligned}
\dot{e}_r &= f_r\\
\dot{e}_c &= f_c\\
\dot{e}_b &= f_b
\end{aligned} \tag{14}$$

To design the functions f_r, f_c, f_b, we choose the Lyapunov function as

$$\begin{aligned}
&V(e_x, e_y, e_z, e_r, e_c, e_b)\\
&= \frac{1}{2}(e_x^2 + \rho e_y^2 + \rho e_z^2 + \frac{1}{\gamma}e_r^2 + \frac{1}{\theta}e_c^2 + \frac{1}{\beta}e_b^2),
\end{aligned} \tag{15}$$

where $\gamma, \theta,$ and β are learning parameters and $\gamma > 0,\ \theta > 0, \beta > 0$ and the parameter ρ satisfies $4\rho > c$. Its derivative along the dynamics (14) becomes

$$\begin{aligned}
\dot{V} &= e_x\dot{e}_x + e_y\dot{e}_y + e_z\dot{e}_z + \frac{1}{\gamma}e_r\dot{e}_r + \frac{1}{\theta}e_c\dot{e}_c + \frac{1}{\beta}e_b\dot{e}_b\\
&= e_x(e_c(y+e_y) + ce_y - e_c(x+e_x) - ce_x - k_x e_x)\\
&\quad + \rho e_y(-xe_z + xe_r - e_y - k_y e_y)\\
&\quad + \rho e_z(xe_y - e_b(z+e_z) - be_z - k_z e_z)\\
&\quad + \frac{1}{\gamma}e_r\dot{e}_r + \frac{1}{\theta}e_c\dot{e}_c + \frac{1}{\beta}e_b\dot{e}_b
\end{aligned}$$

$$\begin{aligned}
&= e_x e_c y + e_x e_c e_y + ce_y e_x - xe_x e_c - e_c e_x^2 - ce_x^2\\
&\quad - \rho xe_y e_z + \rho xe_y e_r - \rho e_y^2 + \rho xe_y e_z - \rho ze_b e_z\\
&\quad - \rho e_b e_z^2 - \rho be_z^2 + \frac{1}{\gamma}e_r\dot{e}_r + \frac{1}{\theta}e_c\dot{e}_c + \frac{1}{\beta}e_b\dot{e}_b\\
&\quad - k_x e_x^2 - \rho k_y e_y^2 - \rho k_z e_z^2
\end{aligned}$$

$$\begin{aligned}
&= ce_y e_x - ce_x^2 - \rho e_y^2 - \rho be_z^2 + e_c(\frac{1}{\theta}\dot{e}_c + ye_x\\
&\quad + e_y e_x - xe_x - e_x^2) + e_r(\frac{1}{\gamma}\dot{e}_r + \rho xe_y)\\
&\quad + e_b(\frac{1}{\beta}\dot{e}_b - \rho ze_z - \rho e_z^2) - k_x e_x^2 - \rho k_y e_y^2 - \rho k_z e_z^2
\end{aligned}$$

$$\begin{aligned}
&= -c(e_x - \frac{1}{2}e_y)^2 + \frac{1}{4}ce_y^2 - \rho e_y^2 - \rho be_z^2 + e_c(\frac{1}{\theta}\dot{e}\\
&\quad + ye_x + e_y e_x - xe_x - e_x^2) + e_r(\frac{1}{\gamma}\dot{e}_r + \rho xe_y)\\
&\quad + e_b(\frac{1}{\beta}\dot{e}_b - \rho ze_z - \rho e_z^2) - k_x e_x^2 - \rho k_y e_y^2 - \rho k_z e_z^2,
\end{aligned} \tag{16}$$

One can easily see that if the parameter error dynamics is built as follows

$$\dot{e}_r = \gamma(-\rho x e_y) = \gamma(-\rho x(\tilde{y} - y)) = \rho\gamma x(y - \tilde{y})$$
$$\dot{e}_c = \theta(x e_x + e_x^2 - y e_x - e_x e_y) = -\theta(x - \tilde{x})(\tilde{x} - \tilde{y}) \quad (17)$$
$$\dot{e}_b = \beta(\rho z e_z + \rho e_z^2) = -\beta\rho(z - \tilde{z})\tilde{z}$$

Then since $4\rho > c$

$$\dot{V} = -c(e_x - \frac{1}{2}e_y)^2 + \frac{1}{4}ce_y^2 - \rho e_y^2 - \rho b e_z^2 - k_x e_x^2$$
$$- \rho k_y e_y^2 - \rho k_z e_z^2 < -c(e_x - \frac{1}{2}e_y)^2 - \rho b e_z^2$$
$$- k_x e_x^2 - \rho k_y e_y^2 - \rho k_z e_z^2 < 0$$

Therefore the state errors system, consisting of equation (14) is asymptotically stable. That is to say

$$e_x \to 0, e_y \to 0, e_z \to 0, e_r \to 0, e_c \to 0, e_b \to 0$$

Hence the synchronization, and of course, the modulation of three parameters, can all be realized. Note that the additional terms in the first three equations of (14), namely $k_x e_x, k_y e_y, k_z e_z$, has a low pass filtering effect that is beneficial in terms of coping with high frequency oscillations in state signals. In addition, the learning parameters γ, θ, and β are introduced to adjust learning speed.

In conclusion, we arrived at the following receiver system with modulation laws for the three parameters of the Lorenz system.

$$\begin{aligned}
\dot{\tilde{x}} &= \tilde{c}(\tilde{y} - \tilde{x}) - k_x e_x \\
\dot{\tilde{y}} &= -x\tilde{z} + \tilde{r}x - \tilde{y} - k_y e_y \\
\dot{\tilde{z}} &= x\tilde{y} - \tilde{b}\tilde{z} - k_z e_z \\
\dot{\tilde{r}} &= \rho\gamma x(y - \tilde{y}) \\
\dot{\tilde{c}} &= -\theta(x - \tilde{x})(\tilde{x} - \tilde{y}) \\
\dot{\tilde{b}} &= -\rho\beta(z - \tilde{z})\tilde{z}
\end{aligned} \quad (18)$$

Note that no a priori knowledge of the transmitter parameters c, r, b is needed to be known in the receiver (18).

3. Simulation Studies

We now present the simulation studies to demonstrate the effectiveness of the modulation scheme proposed.

First, we look at the one parameter case with parameter r used for modulation. Let $c = 10, b = 8/3$, and r be changed between 28 and 32. The Lorenz system under these parameters [3] is chaotic. We also chose $k_x = 40, k_y = 60, \gamma = 8$. The white noise $\eta_x \sim N(0, 0.06)$ was added to the x channel and white noise $\eta_y \sim N(0, 0.014)$ was injected to the y channel. The simulation results are shown in Figures 1 and 2. Figure 1 shows a good tracking of $\tilde{r}$ to r. The solid line represents the modulated parameter $\tilde{r}$ and the dotted line the parameter r. Figure 2 gives the errors of the state between the transmitter and the receiver. Note that in [9], it was mentioned that there is a limitation that parameters must change in less than $\pm 5\%$ to keep a good tracking. However, there is no such a limitation in the modulation scheme presented in this paper. We will further show this point in the simulations on multi parameter modulation below.

We now present the simulation results for multi-parameter modulation via the Lorenz system. In this simulation, the parameters to be modulated concurrently were the three parameters, namely r, c, b. The original parameters for the Lorenz system were $r = 28$, $c = 10, b = 8/3$. The switching of these three parameters started at the 3rd second, 6th second and 9th second, respectively. The three parameters r, c, b were switched between 28 and 32, 10 and 13, 8/3 and 4 respectively every 9 seconds. The noises injected in x, y, z channels were white noises $\eta_x \sim N(0, 0.014)$, $\eta_y \sim N(0, 0.014)$, $\eta_z \sim N(0, 0.06)$ respectively. We chose $k_x = 60, k_y = 80, k_z = 50, \gamma = 2, \theta = 60, \beta = .5, \rho = 5$ in the simulation. Figure 3 consists of three subfigures. The dotted lines depict the parameters r, c, b switched respectively, and the solid lines show the modulated estimated parameters $\tilde{r}, \tilde{c}, \tilde{b}$ respectively. Figure 4 shows the state errors. Good performance is observed with respect to added noises.

4. Conclusion

We have proposed a multi-parameter modulation scheme for secure communication via Lorenz chaos using an adaptive learning mechanism. In comparison to the existing methods, our method provides a rigorous proof of tracking convergence hence the tracking performance is guaranteed. Novel incorporation of a low pass filter structure enables the receiver to handle the noises well. Future work will be focussed on generalize this idea to more general chaotic systems.

References

[1] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signal by chaotic synchronizations," *Int. J. Bifurcation Chaos*, vol. 2, no. 4, pp. 973-977, 1992.

[2] H. Dedieu, M. P. Kennedy, and M. Hasler, “Chaotic shift keying: Modulation and demodulation of a chaotic carrier using self-synchronization of Chua’s circuits,” *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 634-642, 1993.
[3] G. Chen and X. Dong, From Chaos to Order. *World Scientific Publishing Co*. 1998.
[4] S. Hayes, C. Grebogi, and E. Ott, "Communication with chaos," *Phys. Rev. Lett.*, vol.70, pp. 3032-3034, May 1993.
[5] S. Hayes, C. Grebogi, E. Ott, and A. Mark, "Experimental control of chaos for communication." *Phys. Rev. Lett.*, vol. 73, pp.1781-, Sept. 1994.
[6] D. R. Frey, "Chaotic digital encoding: An approach to secure communication," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 660-666, Oct. 1993.
[7] U. Parlitz and L. Kocarev, " Multichannel communication using autosynchronization,*" Int. J. Bifurcation and Chaos***,** vol.6, no. 3, pp. 581-588.
[8] Y. Tao, and L. O. Chua, " Secure communication via chaotic parameter modulation," *IEEE Trans. Circuits Syst. II*, vol.43, pp. 817-819, Sept. 1996.
[9] D. J. Sobiski and J. S. Thorp, " Chaotic communication via the extended Kalman filter." *IEEE Trans. Circuits Syst. I*, vol. 45, no. 2, pp. 194-197, Feb. 1998.
[10] L. M. Pecora, T. L. Carroll "Synchronization in chaotic systems, " *Phys. Rev. Lett.*, vol. 64, no. 8, pp. 821-824, 1990.
[11] J.-J. E. Slotine and W. Li, *Applied Nonlinear Control*, Prentice-Hall, 1991.

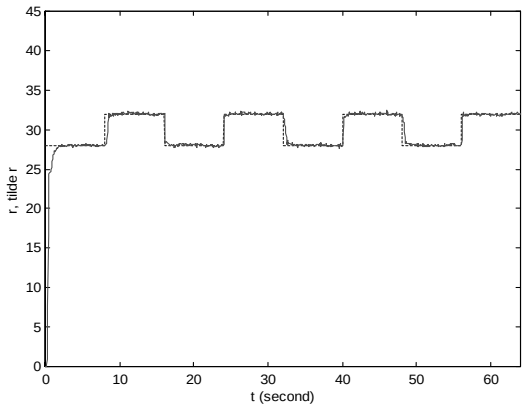

Figure 1. Modulation of parameter r

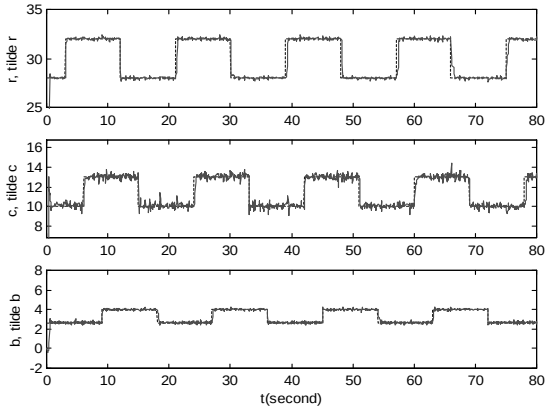

Figure 3. Modulation of three parameters

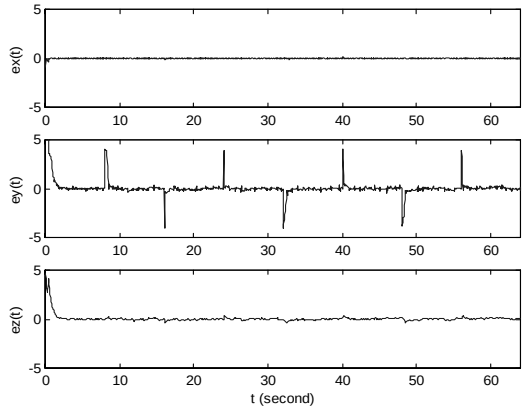

Figure 2. State errors between the receiver and transmitter

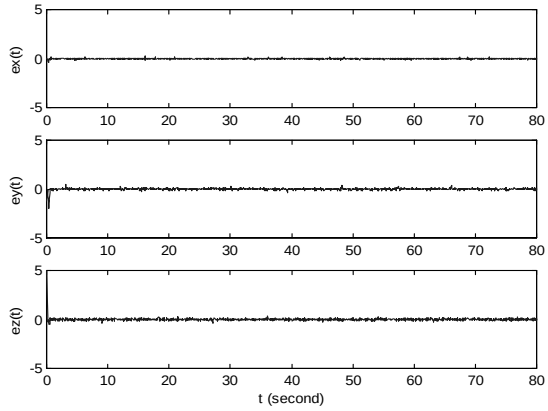

Figure 4. State errors between the receiver and transmitter