TEKNOLOJİ, Yıl 6, (2003), Sayı 3-4, 1-6

TEKNOLOJİ

AN ADAPTIVE OBSERVER FOR CRYPTOSYSTEMS BASED ON THE LORENZ CHAOTIC OSCILLATOR

Ata SEVİNÇ
Kırıkkale University, Department of Electrical and Electronic Engineering, 71450 Kırıkkale, Turkey

ABSTRACT

An adaptive observer design technique proposed for nonlinear systems has been successfully applied to the Lorenz chaotic system which is used in cryptosystems. This observer does not use direct feedback but the adaptation scheme uses the feedback. One of the system parameters is assumed to be unknown and only one of the state variables, which is transmitted in the communication system, is assumed to be accessible. It is possible to transmit two different information signals over the same chaotic signal securely using this adaptive observer.

Keywords: Adaptive observers, nonlinear observers, Lorenz chaotic oscillator, parameter estimation, crypto systems.

ÖZET

Doğrusal olmayan sistemler için önerilmiş bir adaptif gözleyici tasarım tekniği, kripto sistemlerinde kullanılan Lorenz kaotik sistemine başarıyla uygulanmıştır. Bu gözleyici doğrudan doğruya geribesleme kullanmaz; geribeslemeyi sadece adaptasyon algoritması kullanır. Sistem parametrelerinden bir tanesinin bilinmediği ve durum değişkenlerinden sadece birinin erişilebilir olduğu kabul edilmiştir. Haberleşme sisteminde karşı tarafa bu değişken gönderilmektedir. Bu adaptif gözleyici kullanılarak, iki ayrı bilgi sinyalinin aynı kaotik sinyal üzerinden güvenli bir şekilde gönderilmesi mümkündür.

Anahtar Kelimeler: Adaptif gözleyiciler, lineer olmayan gözleyiciler, Lorenz Kaotik sistemi, parametrik tahmin, kripto sistemleri.

1. INTRODUCTION

Lorenz chaotic system, which was proposed 40 years ago as a model for two-dimensional fluid convection, is given by

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} \sigma(x_2 - x_1) \\ rx_1 - x_2 - x_1 x_3 \\ -bx_3 + x_1 x_2 \end{bmatrix} \tag{1}$$

where σ, r and b are system parameters, and x_1, x_2 and x_3 are state variables [1,2]. This system produces broadband chaotic oscillations. The Lorenz chaotic system is used in secure communications since these oscillations are noise-like and depend on the initial conditions and system parameters, which are difficult to estimate. In such systems, the information signal with very small amplitude is added to one of the chaotic signals produced by the chaotic oscillator and the mixed signal is transmitted. The receiver estimates first the chaotic signal as it was before mixing with the information signal using an observer providing synchronization between the transmitter and the receiver. Then, the difference between this chaotic signal

and the received signal gives the small-amplitude information signal [3]. A simplified block diagram of such a system is given in Figure 1, where $m(t)$ is the information signal.

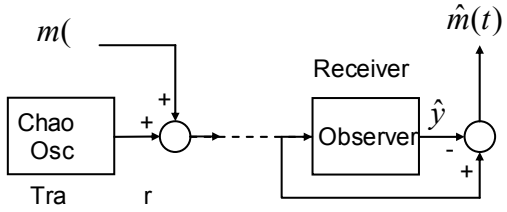

Figure 1: Use of chaotic oscillator in secure communications.

Some of popular observers used in secure communications based on the Lorenz chaotic oscillator are the extended Kalman filter, Thau observer, state dependent Riccati equation, high-gain observer and covariance upper bound assignment [4].

Even though the feedback is essential for observers, an observer design technique without using the direct feedback has been recently proposed [5,6]. Convergence of the state estimations with such an observer, which is called a *natural observer*, is achieved using a parameter adaptation scheme. In this paper, this technique has been applied to the Lorenz chaotic system successfully. The main advantages of this observer over the other observers applied to the Lorenz chaotic system are it is adaptive and very simple. Since the observer does not use the feedback directly, it is quite robust to the measurement noise. Moreover, with such an adaptive system, it is possible to send two different information signals over the same chaotic signal.

2. AN ADAPTIVE NATURAL OBSERVER DESIGN FOR THE LORENZ CHAOTIC OSCILLATOR

Natural observers are designed in the same structure as the actual system and can be used for many nonlinear systems with bounded-input bounded-state (*bibs*) stability [56]. The system (1) is also *bibs* stable [7] and a natural observer can be designed assuming only one of the state variables is accessible. In this paper, the accessible chaotic signal is chosen as

$$y = x_2 \tag{2}$$

and r is assumed to be the parameter to be estimated. Then the natural observer, which is in the same form as system (1)-(2), is given by

$$\begin{bmatrix} \dot{\hat{x}}_1 \\ \dot{\hat{x}}_2 \\ \dot{\hat{x}}_3 \end{bmatrix} = \begin{bmatrix} \sigma(\hat{x}_2 - \hat{x}_1) \\ \hat{r}\hat{x}_1 - \hat{x}_2 - \hat{x}_1\hat{x}_3 \\ -b\hat{x}_3 + \hat{x}_1\hat{x}_2 \end{bmatrix}, \quad \hat{y} = \hat{x}_2 \tag{3}$$

where a hat ($\hat{}$) symbol associates the symbols of the quantities to be estimated.

The convergence between the observer, (3), which does not use any feedback directly, and the actual system, (1)-(2), is achieved controlling the observer with $\hat{r}$ using the feedback as if $\hat{r}$ is an input. By this way, $\hat{r}$ will be estimation of r and the observer will use the feedback indirectly. Since (1) is *bibs* stable, (3) will also be *bibs* stable for certain ranges of $\hat{r}$.

The correction term for the parameter adaptation will be the estimation error of the only measured state

$$e = \hat{x}_2 - x_2 \tag{4}$$

Since $\hat{r}$ explicitly appears in the first derivative of e, a first order differential equation of e can be established as

$$\dot{e} + \alpha e = d - (-\hat{x}_2)\hat{r} \tag{5}$$

where α is an arbitrary positive constant and d summarises all the other terms not including $\hat{r}$ explicitly in the right hand side of (5). Because the system (1)-(2) is observable, asymptotic convergence of e to zero means all the estimated terms converge to the corresponding values in the actual system. If $\hat{r}$ is changed in such a way that $(-\hat{x}_2)\hat{r}$ follows d, then e goes to zero as the right hand side of (5) becomes zero. In order that $(-\hat{x}_2)\hat{r}$ follows d, a closed loop integral control is proposed as shown in Figure 2.

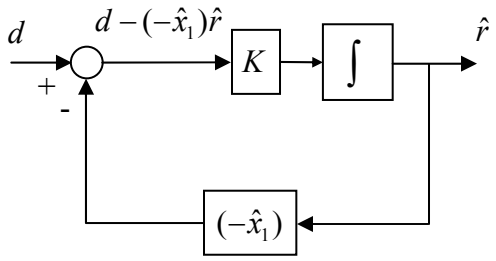

Figure 2: Closed-loop integral control for $(-\hat{x}_2)\hat{r}$ to follow d.

Under the assumption that d and $(-\hat{x}_2)$ change slowly with respect to the adaptation, assigning the sign of the gain K as

$$\text{sign}(K) = \text{sign}\left(\hat{x}_1 - \hat{x}_2\right) \tag{6}$$

implies that $(-\hat{x}_2)\hat{r}$ follows d with a small error. In order to apply this control while d is unknown, $d - (-\hat{x}_2)\hat{r}$ is replaced with $\dot{e} + \alpha e$ due to (5) as shown in Figure 3..

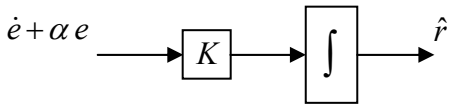

Figure 3: Simplification of Figure 2.

This means r is estimated with a PI adaptation algorithm as

$$\hat{r} = K_p e + \int K_i e dt \tag{7}$$

where K_p and K_i correspond to K and $K\alpha$ respectively.

Actually, d and $(-\hat{x}_2)$ are not slow-varying and a small error between $(-\hat{x}_2)\hat{r}$ and d does not allow all the observer variables to converge to the actual system values. However, this d is not an ordinary signal but a function of the observer and actual system states such that its difference with $(-\hat{x}_2)\hat{r}$ decreases as the observer variables converge to the actual values. For suitable absolute values of K_p and K_i gains, this decrease reduces e further due to (5) and in turn both $\hat{r}$ and the observer states converge to the corresponding values in the actual system. Suitable absolute values of K_p and K_i gains are found with trial-errors in simulation. In this context, this method can be regarded as an empirical method in some respects; however, this method is still very useful since some suitable gains can be found simply with a few trials.

To guarantee the boundedness of the observer states, $\hat{r}$ can be limited within quite a large range as $\left[r_{\min}, r_{\max}\right]$. In order to prevent jumps in $\hat{r}$ due to the proportional term in (7) when K_p and K_i change sign, the integral term in (7) is re-initiated at these instants as

$$\xi^+ = \hat{r}^- - K_p^+ e^- \tag{8}$$

where K_p^+ is the new value of K_p, ξ^- and ξ^+ are the integral values just before and after the sign change, and $\hat{r}^-$ and e^- are the values of $\hat{r}$ and e just before the sign change respectively.

It is possible to send two different information signals, $m_1(t)$ and $m_2(t)$, over the same chaotic signal. For this purpose, whilst directly adding a small-amplitude $m_1(t)$ signal to the transmitted chaotic signal as in the existing methods, the parameter to be estimated is changed according to a low-frequency $m_2(t)$ signal. The proposed use of the Lorenz chaotic oscillator is shown in Figure 4, where $f(.)$ is a calibrating function for r according to the value of $m_2(t)$. On the receiver side, inverse of this function is used to convert the estimation of r to the estimated value of the low frequency information signal, $m_2(t)$. The Lorenz chaotic oscillators on both sides are of the identical form with different initial values. The one on the receiver side acts as a natural observer.

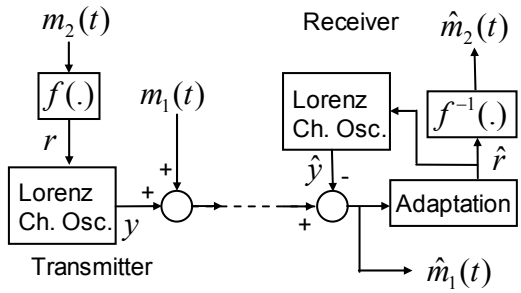

Figure 4: Proposed use of the chaotic oscillator in secure communications.

3. SIMULATION RESULTS

The Lorenz chaotic system (1)-(2), the observer (3) and the adaptation scheme (7) have been simulated with $1ms$ of time steps using the Euler method. The parameters are assigned as $\sigma = 10$, $r = 100$ and $b = 8/3$ in the beginning, then in order to see the performance of the adaptation better, r is changed as $r = 50$ for $6s \le t < 10s$ and $r = 120$ for $t \ge 10s$. Absolute values of the adaptation gains are selected as $|K_p| = 1$ and $|K_i| = 100$, the initial conditions are assigned as $x_1 = x_2 = x_3 = 1$ for the actual system, $\hat{x}_1 = 0.1$, $\hat{x}_2 = \hat{x}_3 = 0$ for the observer and zero for the integral in (7). The results are shown in Figures 5-8.

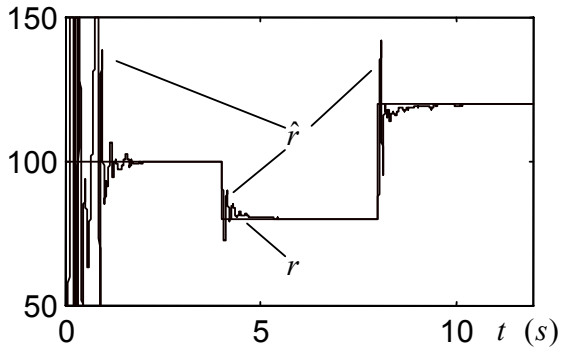

Figure 5: Change and estimation of r.

As seen in Figure 5, $\hat{r}$ converges to r quickly after some oscillations. Meanwhile, the observer states also converge to the actual system states as seen in Figures 6-8. Once the convergence is achieved, there is not a remarkable transient error seen in state estimations even when r changes suddenly and all the estimations converge to the actual values quickly after the sudden changes in r.

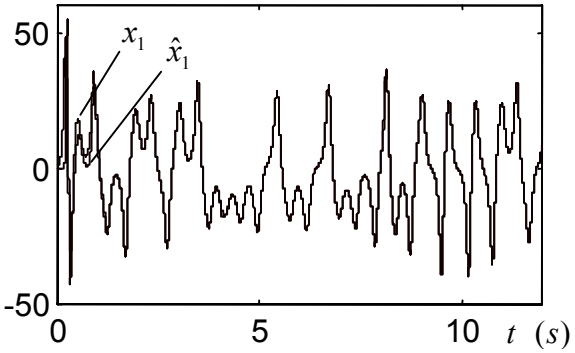

Figure 6: x_1 and its estimation.

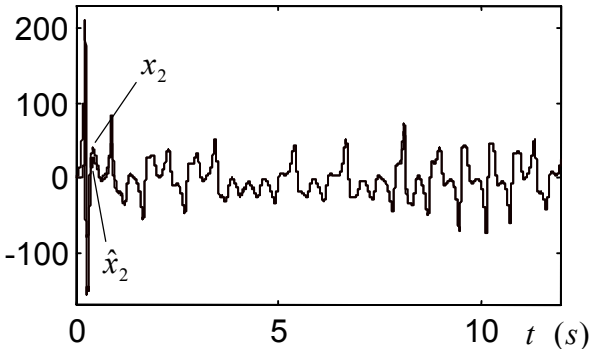

Figure 7: x_2 and its estimation.

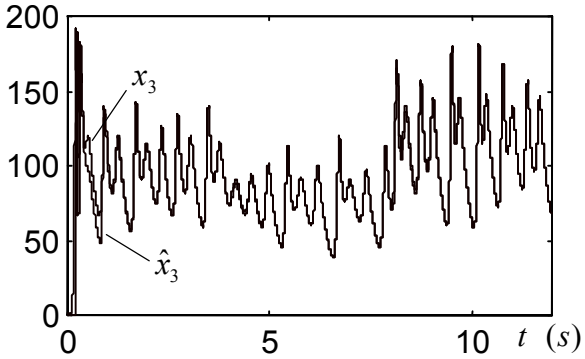

Figure 8: x_3 and its estimation.

4. CONCLUSIONS AND FUTURE WORK

An adaptive observer has been developed for the Lorenz chaotic system, which is used in secure communications with its observer. Even though the adaptation gains are found with trial-error in simulations for this adaptive observer, its implementation is very simple and useful. When this observer is used in cryptosystems, an extra information signal can be transmitted changing the parameter to be estimated. However, this signal can be slow-varying. The proposed adaptation scheme is in the proportional-integral form. Since the proportional gain is relatively small, the adaptation is quite insensitive to the noise. If the adaptation algorithm is improved such that a more suitable feedback signal is used to get rid of the proportional term, the measurement noise will be double filtered by the adaptation and the same observer. This will be considered as a future work in order to obtain a more noise-insensitive adaptive observer.

REFERENCES

1. Lorenz, E.N., "Deterministic Nonperiodic Flow", **Journal of the Athmosferic Sciences**, Vol. 20, 130-141, 1963.
2. González, O.A., Han, G., de Gyvez, J.P., and Edgar, "CMOS Cryptosystem Using a Lorenz Chaotic Oscillator", *Proceedings* **of the IEEE International Symposium on Circuits and Systems, ISCAS '99**, Vol. 5, 442-445, 1999.
3. Cuomo, K.M., Oppenheim, A.V. and Strogatz, S.H., "Synchronization of Lorenz-Based Chaotic Circuits with Applications to Communications", **IEEE Trans. Circuits and Systems-II: Analog and Digital Signal Processing**, Vol. 40, No 10, 626-633, 1993.
4. Amirazodi, J., Yaz, E.E., Azemi, A. and Yaz, Y.I., "Nonlinear Observer Performance in Chaotic Synchronization with Application to Secure Communication", **IEEE Int. Conference on Control Applications**, Glasgow-UK, 76-81, 2002.
5. Sevinç, A., "Speed Sensorless Control of Induction Motors", **PhD Thesis,** University of Bristol, Dept. of Electrical and Electronic Eng., 2001.
6. Bowes, S.R., Sevinç, A. and Holliday, D. "New Natural Observer Applied to Speed Sensorless DC Servo and Induction Motors" (sent **IEEE Trans. on Industrial Electronics** and still under review), 2003.
7. Pecora, L.M. and Carroll, T.L., "Synchronization in chaotic systems", **Phys. Rev. Lett**., Vol. 64, 821-824, Feb. 1990.