SINCRONIZAÇÃO CAÓTICA APLICADA À COMUNICAÇÃO SEGURA VIA CONTROLE POR MODOS DESLIZANTES

Victor Hugo Pereira Rodrigues*, Tiago Roux Oliveira*

*Departamento de Engenharia Eletrônica e Telecomunicações — Faculdade de Engenharia
Universidade do Estado do Rio de Janeiro — Rua São Francisco Xavier 524, sala 5001E — 20559-900

Emails: rodrigues.vhp@gmail.com, tiagoroux@uerj.br

Abstract— In this paper, we have assumed that the parameters of a unified chaotic system are time-varying, uncertain and only the output variable is available for feedback. Due to its robustness to parametric uncertainties and fast transient responses, a sliding mode control strategy is introduced to globally synchronize two of these chaotic systems, i.e., the initial conditions of master (transmitter) and slave (receiver) systems are arbitrary. This result also allow us to solve the problem of secure communications, where the proposed formulation based on norm observers and time-varying cryptographic keys increases the security level of the approach. Simulation results illustrate fast synchronization and less vulnerability properties of the new communication scheme.

Keywords— Chaos Systems; Sliding Mode Control; Output-feedback; Norm Observers; Global Synchronization; Secure Communication.

Resumo— Neste artigo, foi assumido que os parâmetros do sistema caótico unificado são variantes em relação ao tempo, incertos e apenas a saída está disponível para a realimentação. Devido a sua robustez às incertezas paramétricas e rápida resposta transiente, uma estratégia de controle por modos deslizantes é introduzida para sincronizar globalmente dois destes sistemas, isto é, as condições iniciais do sistema mestre (transmissor) e escravo (receptor) são arbitrárias. Este resultado também permite que se resolva o problema de comunicação segura, onde a formulação proposta baseada em observadores da norma e chave criptográfica variante aumenta o nível de segurança da abordagem. Resultados de simulações ilustram a rápida sincronização e as propriedades menos vulneráveis do novo esquema de comunicação.

Palavras-chave— Sistemas Caóticos; Controle por Modo Deslizante; Realimentação de Saída; Observadores da Norma; Sincronização Global; Comunicação Segura.

1 Introdução

O primeiro modelo matemático de um sistema caótico foi proposto por (Lorenz, 1963), representando uma simplificação das equações diferencias parciais de (Saltzman, 1962). Depois de trabalho pioneiro de (Ott et al., 1990), o controle de sistemas caóticos tem sido intensivamente estudado.

Por outro lado, a sincronização de dois sistemas caóticos foi proposta em (Pecora and Carroll, 1990) e dai por diante vários trabalhos lidando com sua aplicação à comunicação foram introduzidas.

Em (Pecora and Carroll, 1990), uma implementação de um circuito para o sistema caótico de Lorenz é descrita com aplicação à comunicação. No entanto, este circuito é criado considerando que os sistemas são acoplados, isto é, uma das variáveis de estado do escravo é exatamente a mesma do sistema mestre. Em (Cuomo and Oppenheim, 1993), duas abordagens para mascaração e modulação são aplicadas à comunicação. Ambas usando a propriedade de acoplamento mencionada acima.

Em (Yang and Chua, 1997), uma aplicação de uma sincronização caótica impulsiva para comunicação segura é apresentada. O esquema caótico de comunicação segura lida com a combinação de métodos criptográficos convencionais e uma técnica de sincronização impulsiva. Em (Liao and Tsai, 2000), um esquema de sincronização adaptativa com aplicação à comunicação segura também é proposta. O processo pode ser dividido em duas fases: a fase de adaptação, onde os distúrbios do transmissor caótico são estimados; e a fase de comunicação, com a informação sendo transmitida e então recuperada com base nos parâmetros estimados.

Até o momento, a sincronização é um importante passo para todas as metodologias discutidas acima. Em geral, são realizadas assumindo sistemas caóticos com parâmetros constantes, tal como o atrator de Lorenz ou o circuito de Chua, restringindo a forma da chave na concepção criptográfica e, consequentemente, aumentando o nível de vulnerabilidade do sistema de comunicação.

O sistema caótico unificado foi introduzido por (Lü et al., 2002). Este sistema surge como uma alternativa para obter uma melhor chave criptográfica, criando uma ponte entre os atratores de Lorenz e Chen (Chen and Ueta, 1999) via um parâmetro de projeto α. Neste artigo, o problema de sincronização é tratado considerando um sistema caótico unificado com uma contínua, variante e periódica função de chaveamento $\alpha(t)$ proposta por (Jun-An and Xiaoqun, 2003).

Em (Jun-An and Xiaoqun, 2003), métodos de controle são desenvolvidos para estabilizar e sincronizar sistemas caóticos. No entanto, são projetados assumindo realimentação de estado e o conhecimento exato de todos os parâmetros do sistema. Em (Zhang et al., 2005), a teoria de con-

trole impulsivo é usada para estabilizar e sincronizar sistemas caóticos na presença de atraso assumindo de novo o mensuramento por completo do estado. A mesma suposição é considerada em (Li et al., 2008), onde um controlador por modo deslizante com intervalo fuzzy de tipo-2 é proposto para controlar um sistema caótico unificado variante com parâmetro de chaveamento $\alpha(t)$ variando dentro do intervalo $[0, 1]$.

A contribuição deste artigo é a proposta de uma nova estratégia de sincronização do sistema caótico unificado com parâmetros variantes e chaveamento periódico contínuo via controle por modos deslizantes (Utkin, 1978). Para este fim, foi assumido que todos os parâmetros dos sistemas metre e escravo são incertos. Em vez da aplicação de observadores padrão, foi assumido o uso de observadores da norma para o vetor de estado imensurado na estrutura de realimentação de saída, já que eles são mais robustos às incertezas, dando limitantes superiores para a norma do estado. Então, o controlador projetado é aplicado ao cenário de comunicação segura, onde a rápida sincronização e uma criptografia mais robusta são os principais ingredientes da receita proposta.

2 Notação e Terminologia

As seguintes notações e conceitos básicos são empregados ao longo do texto. A norma Euclidiana de um vetor x e a correspondente norma induzida de uma matriz A são denotadas por $|x|$ e $|A|$, respectivamente. Aqui, adotou-se a definição de (Filippov, 1964) para a solução de equações diferenciais com lado direito descontínuo. O conceito de estabilidade ISS (Input-to-State-Stability), assim como as definições de funções de classe $\mathcal{K}$ e $\mathcal{K}_\infty$ encontram-se de acordo com (Khalil, 2002):

Definição 1: *Uma função contínua* $\alpha : [0, a) \to [0, \infty)$ *é dita pertencer à classe* $\mathcal{K}$ *se ela for estritamente crescente e* $\alpha(0) = 0$. *Ela é dita pertencer à classe* $\mathcal{K}_\infty$ *se* $\alpha = \infty$ *e* $\alpha(r) \to \infty$ *com* $r \to \infty$.

Definição 2: *Uma função contínua* $\beta : [0, a) \times [0, \infty) \to [0, \infty)$ *é dita pertencer à uma classe* $\mathcal{KL}$ *se, para cada* s *fixo, o mapeamento* $\beta(r, s)$ *pertencer à classe* $\mathcal{K}$ *com respeito a* r *e, para cada* r *fixo, o mapeamento* $\beta(r, s)$ *é decrescente com respeito a* s *e* $\beta(r, s) \to 0$ *com* $s \to \infty$.

Definição 3: *Considere o sistema* $\dot{x} = f(x)$, *onde* $x \in \mathbb{R}^n$. *Seja* $\overline{x}$ *um ponto de equilíbrio deste sistema e considere* $V : U \to \mathbb{R}$ *ser uma função* C^1 *definida em alguma vizinhança* U *de* $\overline{x}$ *tal que*

$$(i) V(\overline{x}) = 0 \text{ e } V(\overline{x}) > 0 \text{ se } x \neq \overline{x}\,.$$
$$(ii) \dot{V} < 0 \text{ em } U - \{\overline{x}\}\,.$$

Então, $\overline{x}$ *é assintoticamente estável.*

A definição 3 se refere V como uma função de Lyapunov. Se U pode ser escolhido para todo $\mathbb{R}^n$, então $\overline{x}$ é dito ser *globalmente assintoticamente estável, i.e.,* $|x(t) - \bar{x}| \leq \beta(|x(0)|, t)$, $\forall t \geq 0$ *e* $\forall x(0)$, *onde* $\beta(|x(0)|, t) \in \mathcal{KL}$.

Definição 4: *Considere o sistema* $\dot{x} = f(t, x, u)$, *onde* $f : [0, \infty) \times \mathbb{R}^n \times \mathbb{R} \to \mathbb{R}^n$ *é contínuo por partes em* t *e localmente Lipschitz em* x *e* u. *O sistema é dito ser input-to-state stable (ISS) se existe uma função* β *de classe* $\mathcal{KL}$ *e uma função* γ *de classe* $\mathcal{K}$ *tal que para qualquer estado inicial* $x(t_0)$ *e qualquer entrada limitada* $u(t)$, *a solução* $x(t)$ *existe para todo* $t \geq t_0$ *e satisfaz*

$$|x(t)| \leq \beta(|x(t_0)|, t - t_0) + \gamma\left(\sup_{t_0 \leq \tau \leq t} |u(\tau)|\right).$$

Se na Definição 4 a função de classe $\mathcal{KL}$ é uma exponencial, então a estabilidade ISS é do tipo exponencial.

3 O Sistema Caótico Unificado com Chaveamento Contínuo e Periódico

Como em (Jun-An and Xiaoqun, 2003), o sistema caótico unificado com chaveamento entre os sistemas de Lorenz e Chen é dado por:

$$\begin{aligned}\dot{x}_1 &= (25\sin^2\omega t + 10)(-x_1 + x_2)\,,\\ \dot{x}_2 &= (28 - 35\sin^2\omega t)x_1 - x_1x_3 + (29\sin^2\omega t - 1)x_2\,,\\ \dot{x}_3 &= -\frac{(8 + \sin^2\omega t)}{3}x_3 + x_1x_2\,,\end{aligned} \tag{1}$$

onde o vetor de estado é definido por $x = [x_1\ x_2\ x_3]^T \in \mathbb{R}^3$, ω é um parâmetro ajustável e o termo

$$\alpha(t) = \sin^2\omega t \tag{2}$$

é a função de chaveamento periódico (Jun-An and Xiaoqun, 2003). Este sistema é um paradigma, já que ele captura vários aspectos da dinâmica caótica. Na Figura 1, as trajetórias do sistema no espaço de estado são mostradas. Neste caso, as condições iniciais eram $x_1(0) = x_3(0) = 1$, $x_2(0) = 0$ e a frequência $\omega = 2\pi/30\ rad/s$.

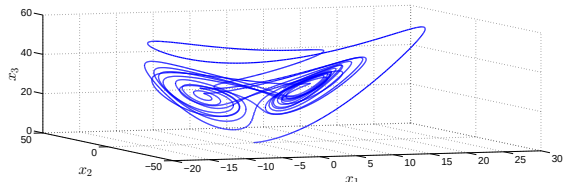

Figura 1: Sistema caótico unificado com chaveamento contínuo.

Os objetivos deste artigo são dois:

- sincronizar globalmente dois sistemas caóticos variantes de uma maneira mais rápida e robusta;
- aplicar o resultado da sincronização para obter um esquema de comunicação segura;

usando apenas realimentação de saída via observadores da norma e explorando propriedades ISS dos sistemas não-lineares considerados. Para este fim, uma lei de controle por modos deslizantes é adotada para garantir propriedades de robustez com respeito às incertezas paramétricas e capacidade de rejeição de perturbações.

4 Observadores da Norma

Os observadores da norma são aplicados para estimar limitantes superiores para a norma do vetor de estado de um sistema usando valores de limitantes inferiores e superiores dos parâmetros do sistema. Essa estimativa estará sempre acima da norma do estado observado exceto por um termo exponencial decrescente que está relacionado com o termo transitório devido a condições iniciais. Em (Oliveira et al., 2010), foi desenvolvido um método baseado em (M. Krichman and Wang, 2001) para o projeto dos observadores da norma. Este método pode ser diretamente aplicado às equações dinâmicas de x_1 e x_3 do sistema (1). Uma descrição matemática rigorosa pode ser encontrada nas referências citadas. No que segue, será descrita a uma breve introdução dos resultados principais.

Seja um sistema não-linear genérico:

$$\dot{x} = f(x, y) \tag{3}$$

onde $y \in \mathbb{R}$ é encarada como uma entrada do sistema e $x \in \mathbb{R}^n$ é o estado não mensurado. A função incerta f é localmente Lipschitz contínua nos seus argumentos.

Definição 5 *Um observador da norma para o subsistema (3) é um sistema dinâmico SISO de primeira ordem da forma:*

$$\dot{\hat{x}} = -\lambda\hat{x} + \varphi(|y|), \tag{4}$$

com entrada $\varphi(|y|) \in \mathcal{K}$, saída $\hat{x}$ e $\lambda > 0$ sendo uma constante apropriada, tal que para qualquer condição inicial $x(0)$ e $\hat{x}(0)$, o estado x de (3) satisfaz

$$|x(t)| \leq |\hat{x}(t)| + \bar{k}(|\hat{x}(0)| + |x(0)|)e^{-\lambda t}, \quad \forall t \geq 0 \tag{5}$$

com alguma constante $\bar{k} > 0$.

Sabe-se que se o sistema (3) é ISS com respeito a y, então ele admite tal observador da norma e então pode-se concluir que a planta é de fase mínima.

Por inspeção direta do sistema (1) é fácil notar que a dinâmica que governa x_1 é ISS em relação a x_2 e que a dinâmica de x_3 é ISS com relação a função x_1x_2. Assim sendo, ao considerar a saída do sistema como

$$y := x_2\,, \tag{6}$$

os observadores da norma para x_1 e x_3 podem ser projetados e uma lei de controle usando apenas em realimentação de saída pode ser obtida.

Em (Rodrigues and Oliveira, 2013), a técnica dos observadores da norma foi usada para estabilizar o sistema de Lorenz. Aqui, a metodologia é analisar os casos limites do sistema unificado e, então escolher os parâmetros dos observadores da norma que atendam a ambos os casos ou o pior caso, em outras palavras, quando $\sin^2\omega t = 0$ (Lorenz) ou $\sin^2\omega t = 1$ (Chen).

Lema 1: *Se $y = x_2$ é escolhida como a saída do sistema (1), observadores da norma para x_1 e x_3 podem ser dados por*

$$\dot{\hat{x}}_1 = -\underline{\sigma}\hat{x}_1 + \overline{\sigma}|y| \tag{7}$$

$$\dot{\hat{x}}_3 = -\underline{b}\hat{x}_3 + \overline{b}|\hat{x}_1 y|\,, \tag{8}$$

onde os parâmetros devem satisfazer $0 < \underline{\sigma} < 10$, $\overline{\sigma} > 35$, $0 < \underline{b} < \frac{8}{3}$ e $\overline{b} > 1$. Então, a norma de $\hat{x}_1$ e $\hat{x}_3$ são limitantes superiores de $|x_1|$ e $|x_3|$, respectivamente, de acordo com a inequação (5), i.e., exceto por um termo exponencial decrescente.
Prova: *Suponha que $\sin^2\omega t = 0$ em (1), então o sistema é o atrator de Lorenz dado por*

$$\begin{aligned} \dot{x}_1 &= 10(-x_1 + x_2) \\ \dot{x}_2 &= 28x_1 - x_1x_3 - x_2 \\ \dot{x}_3 &= -\frac{8}{3}x_3 + x_1x_2\,. \end{aligned} \tag{9}$$

Se o sistema (1) tem $\sin^2\omega t = 1$, então ele corresponde ao atrator de Chen dado como segue

$$\begin{aligned} \dot{x}_1 &= 35(-x_1 + x_2) \\ \dot{x}_2 &= -7x_1 - x_1x_3 + 28x_2 \\ \dot{x}_3 &= -3x_3 + x_1x_2\,. \end{aligned} \tag{10}$$

Analisando a resposta impulsiva dos subsistemas x_1 e x_3 em (9)–(10), quando y e x_1y são considerados como os sinais de entrada, então os parâmetros dos observadores da norma devem ser escolhidos tal forma que a norma de $\hat{x}_1$ e $\hat{x}_3$ são maiores do que as normas de x_1 e x_3, não importando os valores instantâneos assumidos pelos parâmetros do sistema (1). Esta condição é garantida se $0 < \underline{\sigma} < 10$, $\overline{\sigma} > 35$, $0 < \underline{b} < \frac{8}{3}$ e $\overline{b} > 1$. ▷

5 Sincronização via Realimentação de Saída

Nesta seção, uma nova estratégia para sincronizar dois sistemas caóticos unificados com chaveamento periódico e a mesma frequência é proposto. É considerado que apenas uma variável de estado de cada sistema (mestre e escravo) está disponível, então observadores da norma são construídos para agir de tal forma que as propriedades de estabilidade global do sistema do erro seja preservada.

Suponha o sistema mestre como em (1) sem qualquer ação de controle e observadores da norma

dados por (7)–(8). Por outro lado, o sistema escravo é

$$\begin{aligned}\dot{w}_1 &= (25\sin^2\omega t + 10)(-w_1 + w_2)\\ \dot{w}_2 &= (28–35\sin^2\omega t)w_1 – w_1 w_3 + (29\sin^2\omega t – 1)w_2 + u\\ \dot{w}_3 &= -\frac{(8+\sin^2\omega t)}{3}w_3 + w_1 w_2\end{aligned} \tag{11}$$

onde u é a entrada de controle e $w = [w_1\ w_2\ w_3]^T \in \mathbb{R}^3$ é o estado imensurável.

Na Figura 2, os sistemas (1) e (11) são simulados como $u = 0$, $\omega = 2\pi/30\ rad/s$ e condições iniciais $x_1(0) = x_3(0) = 1$, $w_1(0) = w_3(0) = -1$ e $x_2(0) = w_2(0) = 0$.

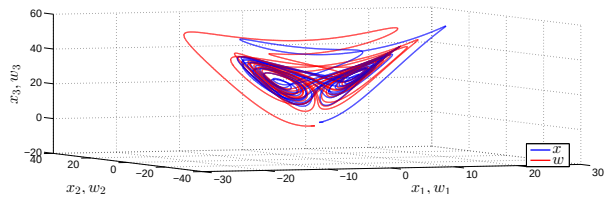

Figura 2: Trajetórias de estado x e w sem ação de controle.

Considere que

$$z := w_2 \tag{12}$$

é a saída mensurada do sistema (11), então, usando o Lema 1, os seguintes observadores da norma podem ser obtidos para w_1 e w_3:

$$\dot{\hat{w}}_1 = -\underline{\sigma}\hat{w}_1 + \overline{\sigma}|z| \tag{13}$$

$$\dot{\hat{w}}_3 = -\underline{b}\hat{w}_3 + \overline{b}|\hat{w}_1 z|\,. \tag{14}$$

O vetor erro é dado por $e := w - x$, e a dinâmica do erro pode ser escrita como:

$$\begin{aligned}\dot{e}_1 &= (25\sin^2\omega t + 10)(-e_1 + e_2)\\ \dot{e}_2 &= (28–35\sin^2\omega t)e_1 – w_3 e_1 – x_1 e_3 + (29\sin^2\omega t – 1)e_2 + u\\ \dot{e}_3 &= -\frac{(8+\sin^2\omega t)}{3}e_3 + w_2 e_1 + x_1 e_2\,.\end{aligned} \tag{15}$$

Observação 1: *Pelo Lema 1, a equação dinâmica do observador da norma para $e_1 = w_1 - x_1$ é dado por*

$$\dot{\hat{e}}_1 = -\underline{\sigma}\hat{e}_1 + \overline{\sigma}|e_2|\,, \tag{16}$$

com $e_2 = z - y$, onde y é a saída do mestre em (6) e z é a saída do escravo em (12).

A seguir, o controlador por modos deslizantes via realimentação de saída para a sincronização é apresentado.

Teorema 1: *Se o controlador por modo deslizante via realimentação de saída u é dado por*

$$u = -[\overline{D} + \delta]sgn(e_2) \tag{17}$$

$$\overline{D} = |\overline{r}\hat{e}_1| + |\hat{x}_1\hat{x}_3 - \hat{w}_1\hat{w}_3| + |\overline{r}e_2|\,, \tag{18}$$

onde δ é uma constante qualquer arbitrariamente pequena, $\overline{r} \geq 28$, $e_2 = z - y$ é a saída mensurada do erro. Os sinais $\hat{x}_1$, $\hat{x}_3$, $\hat{w}_1$, $\hat{w}_3$ e $\hat{e}_1$ são os estados dos observadores da norma projetados pelas saídas do mestre e do escravo y e z, respectivamente. Então, o ponto de equilíbrio $(e_1, e_2, e_3) = (0, 0, 0)$ do sistema do erro (15) é globalmente assintoticamente convergente e todos os sinais do sistema em malha fechada são uniformemente limitados.

Prova: *Considere a seguinte função de Lyapunov candidata*

$$V = \frac{1}{2}{e_2}^2$$

onde a taxa de variação de V é $\dot{V} = e_2\dot{e}_2$. Então, pode-se concluir que $\dot{V} < 0$ se $e_2\dot{e}_2 < 0$. De acordo com o Lema 1:

$$\overline{D} \geq |D| = |(28–35\alpha(t))e_1 – w_3 e_1 – x_1 e_3 + (29\alpha(t)–1)e_2|,$$

que é válido depois de um transitório inicial e $\alpha(t)$ definido por (2). Então, usando o controlador por modo deslizante (17)–(18), pode-se concluir que

$$\begin{aligned}\dot{V} &= e_2\dot{e}_2\\ &= e_2[(28–35\alpha(t))e_1 – w_3 e_1 – x_1 e_3 + (29\alpha(t)–1)e_2 + u]\\ &= e_2[(28–35\alpha(t))e_1 – w_3 w_1 + x_1 x_3 + (29\alpha(t)–1)e_2 + u]\\ &\leq e_2[|D| - (\overline{D} + \delta)sgn(e_2)]\\ &\leq (|D| - \overline{D} - \delta)|e_2|\\ &\leq (\overline{D} - \overline{D} - \delta)|e_2|\\ &\leq -\delta|e_2|\,.\end{aligned} \tag{19}$$

A inequação (19) garante que um modo deslizante ideal ocorra em tempo finito na superfície $e_2 \equiv 0$ para o sistema (15) com qualquer constante arbitrariamente pequena $\delta > 0$ (Utkin et al., 1999). Além disso, de acordo com Definição 4, a dinâmica de e_1, e_3 e $\hat{e}_1$ são ISS com respeito a e_2. Então, o vetor de estado por completo tende globalmente exponencialmente a zero.

Como as equações dinâmicas de $\hat{x}_1$, $\hat{x}_3$, $\hat{w}_1$, $\hat{w}_3$ são guiadas por y ou z, que estão confinados dentro de um conjunto compacto do espaço de estado correspondendo ao atrator caótico, então, aqueles sinais também devem ser uniformente limitados. ▷

Na Figura 3, um diagrama de blocos com o esquema de sincronização é mostrado. As saídas dos sistemas mestre e escravo (y e z) são entradas dos observadores da norma que são usadas no projeto do controlador.

6 Aplicação à Comunicação Segura

Nesta seção, um novo esquema para comunicação segura é desenvolvido. A vantagem deste método é o total desacoplamento dos sistemas dinâmicos transmissor (mestre) e receptor (escravo) e a redução no número de sensores. Na referida literatura,

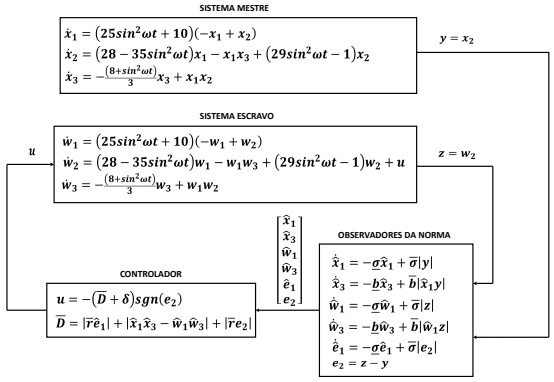

Figura 3: Diagrama de blocos: esquema de sincronização.

grande parte dos casos considera que o sistema escravo tem uma variável de estado em comum com o sistema mestre e então a mensagem transmitida pode ser facilmente recuperada, incluindo intrusos. Aqui, a mensagem transmitida é construída com uma função caótica e uma codificação binária que juntas formam a mensagem caótica. Além disso, os sinais de saída y e z são utilizados para obter a sincronização.

Para a sincronização, o controlador é projetado usando apenas realimentação de saída e, quando os dois sistemas estão completamente sincronizados, o receptor é capaz de recuperar a mensagem binária original usando a mensagem caótica e apenas as variáveis de estado do escravo. Vale a pena mencionar que o transmissor envia dois sinais para o receptor: um sinal de saída usado para a sincronização e a mensagem caotificada. Para recuperar a mensagem original, o receptor deve estar sincronizado com o transmissor tal que seus estados sejam os mesmo depois de um período transiente. Note que o tempo gasto para a sincronização deve ser tão curto quanto possível, i.e., a fase transitória deve ser reduzida pelo uso do proposto esquema de controle por modo deslizante.

Quando um sistema caótico unificado é usado na comunicação segura, o parâmetro $\alpha(t)$ é visto como uma chave criptográfica que é conhecida pelo transmissor e pelo receptor. Neste artigo, tal parâmetro é variante com relação ao tempo e então a chave criptográfica pode ter um sinal ricamente relacionado com sua frequência. Este fato impõe ao intruso um novo desafio, uma chave criptográfica variante no tempo. Uma outra vantagem deste método é que o projetista tem mais possibilidades para criar o sinal caótico que mascara a mensagem binária. Então, os principais aspectos da abordagem proposta são:

- Não há uso do vetor de estado do mestre durante a transmissão;
- Sincronização é alcançada usando apenas os sinais de saída do mestre e do escravo;
- "Caotificação da mensagem (recuperação)" como uma nova função de saída do estado sistema do mestre (escravo);
- Uma chave criptográfica variante no tempo.

Seja $\Phi : \mathbb{R}^3 \to \mathbb{R}$ qualquer função não-linear contínua usada para caotificação da mensagem de interesse. Matematicamente, não há restrições quanto ao projeto desta função, *a priori*.

Considere que a mensagem transmitida é

$$m_t(t) = \Phi(x(t)) + m(t)\,, \tag{20}$$

onde $\Phi(x(t))$ é a função de caotificação, formada pelo estado do mestre e m, que é a mensagem binária sendo mascarada. Se os sistemas estão sincronizados, o sistema escravo pode recuperar a mensagem original com seu próprio estado usando uma função de recuperação $\Phi(w(t))$. Então, a mensagem gerada pelo receptor é

$$m_r(t) = m_t(t) - \Phi(w(t)) \tag{21}$$

e $m_r(t)$ é igual a $m(t)$, que é a mensagem de interesse.

Sem perda de generalidade, a função caótica para a comunicação segura, foi escolhida como a combinação linear das variáveis de estado do mestre, i.e.,

$$\Phi(x(t)) = x_1(t) + x_2(t) + x_3(t) \tag{22}$$

e

$$\Phi(w(t)) = w_1(t) + w_2(t) + w_3(t)\,, \tag{23}$$

para a função de recuperação. Funções mais complexas incluindo não-linearidades podem ser usadas.

Na próxima seção, alguns resultados de simulações são apresentados para mostrar a efetividade da estratégia proposta.

Para ilustrar a sincronização aplicada à comunicação segura, um diagrama de blocos do esquema proposto é mostrado na Figura 4.

7 Simulações

Nas seguintes simulações os parâmetros de controle foram escolhidos como: $\underline{\sigma} = 5$, $\overline{\sigma} = 52.5$, $\underline{b} = 4/3$, $\overline{b} = 1.5$, $\overline{r} = 42$, $\omega = 2\pi/30$ rad/s e $\delta = 0.001$. As condições iniciais foram: $x_1(0) = x_3(0) = 1$, $x_2(0) = w_2(0) = \hat{x}_1(0) = \hat{x}_3(0) = \hat{w}_1(0) = \hat{w}_3(0) = \hat{e}_1(0) = 0$ e $w_1(0) = w_3(0) = -1$.

Na Figura 5, o sinal de controle (17)–(18) aplicado ao problema de sincronização é apresentado. O sistema do erro (15) é estabilizado na origem e, então, o sistema mestre (1) e o escravo (11) estão sincronizados (ver Figura 6).

A mensagem binária m que será mascarada no dispositivo transmissor é mostrada na Figura 7. Depois da caotificação, a mensagem transmitida m_t na Figura 8 não tem nenhuma similaridade com a original m. A mensagem que é recuperada

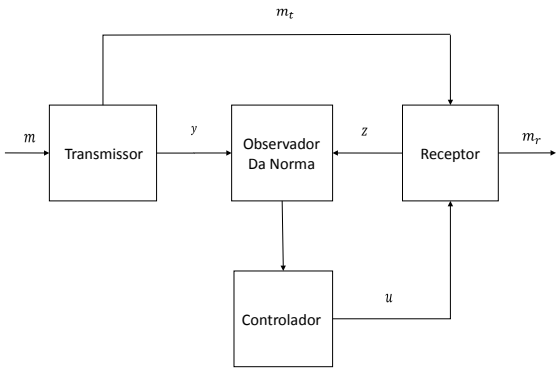

Figura 4: Diagrama de blocos: esquema de comunicação segura.

no receptor (m_r) é mostrada na Figura 9. Note que, até que os sistemas mestre e escravo estejam completamente sincronizados, m e m_r são bem diferentes.

Se a frequência de $\alpha(t) = \sin^2 \omega t$ nos dois sistemas forem diferentes, a mensagem original não poderá ser recuperada como é apresentado na Figura 10. Neste caso, a mensagem resultante é plotada quando a frequência ω da chave do transmissor foi 2 vezes mais lenta do que a do receptor. Mesmo se um intruso tiver descoberto a função de caotificação (22), a chave criptográfica $\alpha(t)$ deve ser exatamente implementada para que a mensagem original seja recuperada, o que garante um nível adicional de segurança ao sistema de comunicação.

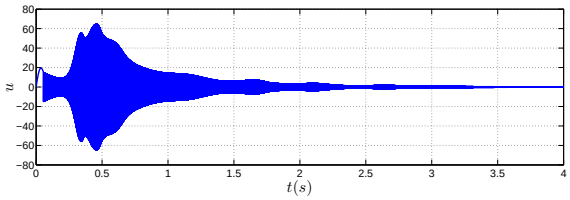

Figura 5: Sinal de controle na sincronização.

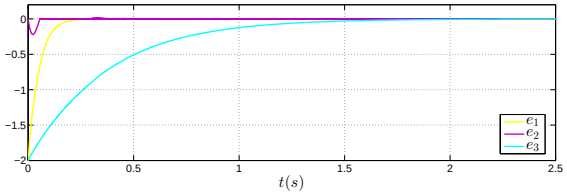

Figura 6: erros de sincronização.

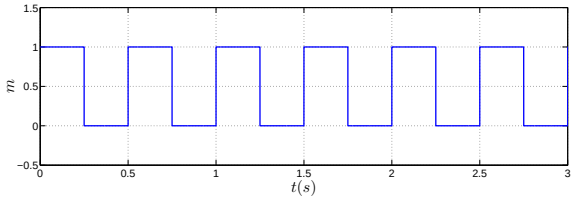

Figura 7: Mensagem original.

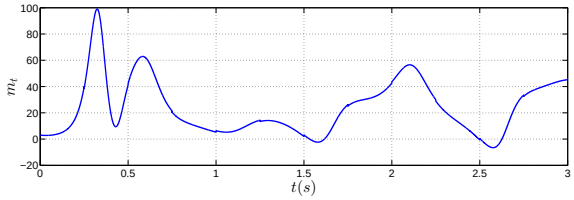

Figura 8: Mensagem transmitida.

8 Conclusões

Explorando as características ISS do sistema caótico unificado, foi proposta uma lei de controle baseada em modos deslizantes e observadores da norma para o problema de sincronização. Foi demostrada a estabilidade global do sistema do erro usando apenas realimentação de saída, mesmo considerando que os parâmetros do sistema caótico eram incertos e variantes no tempo. O controlador por modo deslizante proposto parece ser uma atrativa metodologia para a rápida sincronização devido a sua boa resposta transiente, sendo robusto à incertezas paramétricas e distúrbios. A aplicação da sincronização à sistemas de comunicação segura muito bem avaliada. Uma interessante vantagem do método é obter uma melhor chave criptográfica usando um número reduzido de sensores (sinais de saída). Em trabalhos futuros pretende-se avaliar a influencia do ruído no canal de comunicação na obtenção da mensagem criptografada e realizar comparações com outras técnicas conhecidas na literatura.

Referências

Chen, G. and Ueta, T. (1999). Yet another chaotic attractor., **9**(7): 1465–1466.

Cuomo, K. M. and Oppenheim, A. V. (1993). Circuit implementation of synchronized chaos with applications to communications., **71**: 65–68.

Filippov, A. F. (1964). Differential equations with discontinuous right-hand side., **42**(2): 199–231.

Jun-An, L. and Xiaoqun, W. (2003). A unified chaotic system with continuous periodic switch., **20**: 245–251.

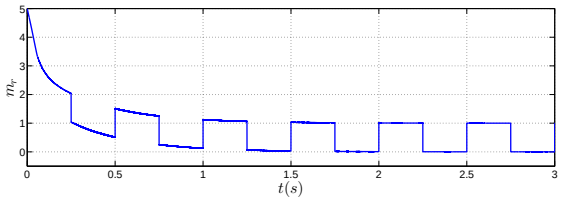

Figura 9: Mensagem recuperada.

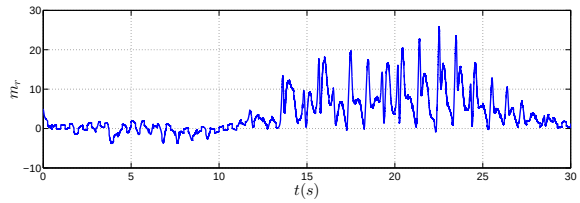

Figura 10: Erro na mensagem recuperada.

Khalil, H. K. (2002). *Nonlinear Systems*, Pretice Hall.

Li, T.-H. S., Hsiao, M.-Y., Lee, J.-Z. and Tsai, S.-H. (2008). Interval type 2 fuzzy sliding-mode control of a unified chaotic system., **96**: 1–4.

Liao, T.-L. and Tsai, S.-H. (2000). Adaptive synchronization of chaotic systems and its application to secure communications., **11**: 1387–1396.

Lorenz, E. N. (1963). Deterministic nonperiodic flow., **20**(2): 130–141.

Lü, J. H., Chen, G. R. and Celikovsky, S. (2002). Bridge the gap between the Lorenz system and the Chen system., **12**(12): 2917–2926.

M. Krichman, E. D. S. and Wang, Y. (2001). Input-output-to-state stability., **39**(6): 1874–1928.

Oliveira, T. R., Peixoto, A. J. and Hsu, L. (2010). Sliding mode control of uncertain multivariable nonlinear systems with unknown control direction via switching and monitoring function., **55**: 1028–1034.

Ott, E., Grebogi, C. and Yorke, J. A. (1990). Controlling chaos., **64**(11): 1196–1199.

Pecora, L. M. and Carroll, T. L. (1990). Synchronization in chaotic systems., **64**(8): 821–824.

Rodrigues, V. H. P. and Oliveira, T. R. (2013). Estabilização global do sistema caótico de lorenz através do controle por modos deslizantes via observadores da norma., XII Conferência Brasileira de Dinâmica, Controle e Aplicações (DINCON'2013).

Saltzman, B. (1962). Finite amplitude free convection as an initial value problem-i., **19**(4): 329–341.

Utkin, V. I. (1978). *Sliding Modes And Their Application In Variable Structure Systems.*, Mir Publishers.

Utkin, V. I., Guldner, J. and Shi, J. (1999). *Sliding Mode Control in Electromechanical Systems.*, Taylor & Francis.

Yang, T. and Chua, L. O. (1997). Impulsive stabilization for control and synchronization of chaotic systems: Theory and application to secure communication., **44**(10): 976–988.

Zhang, X., Liao, X. and Li, C. (2005). Impulsive control, complete and lag synchronization of unified chaotic system with continuous periodic switch., **26**: 845–854.