



**ESQUEMA DE SINCRONIZAÇÃO SUBATUADO E
ROBUSTO PARA UM SISTEMA HIPERCAÓTICO
PENTADIMENSIONAL COM APLICAÇÃO EM
TELECOMUNICAÇÃO SEGURA**

VICTOR VELOSO GRACIANO

**RELATÓRIO SUBMETIDO COMO REQUISITO PARA OBTENÇÃO DO GRAU DE
ENGENHEIRO DE CONTROLE E AUTOMAÇÃO
DEPARTAMENTO DE ENGENHARIA MECATRÔNICA**

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASÍLIA

**UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA MECATRÔNICA**

**ESQUEMA DE SINCRONIZAÇÃO SUBATUADO E
ROBUSTO PARA UM SISTEMA HIPERCAÓTICO
PENTADIMENSIONAL COM APLICAÇÃO EM
TELECOMUNICAÇÃO SEGURA**

VICTOR VELOSO GRACIANO

Orientador: PROF. DR. JOSÉ ALFREDO RUIZ VARGAS

**RELATÓRIO SUBMETIDO COMO REQUISITO PARA OBTENÇÃO DO GRAU DE
ENGENHEIRO DE CONTROLE E AUTOMAÇÃO**

FICHA CATALOGRÁFICA

VICTOR VELOSO GRACIANO

Esquema De Sincronização Subatuado E Robusto Para Um Sistema Hipercaótico Pentadimensional Com Aplicação Em Telecomunicação Segura

2021xv, 61p., 201x297 mm

(ENE/FT-UnB/FT/UnB, Engenheiro de Controle e Automação, Engenharia Mecatrônica, 2021)

Relatório submetido como requisito para obtenção do grau de Engenheiro de Controle e Automação - Universidade de Brasília

Faculdade de Tecnologia - Departamento de Engenharia Mecatrônica

REFERÊNCIA BIBLIOGRÁFICA

Graciano, V. V. Esquema De Sincronização Subatuado E Robusto Para Um Sistema Hipercaótico Pentadimensional Com Aplicação Em Telecomunicação Segura. Relatório submetido como requisito para obtenção do grau de Engenheiro de Controle e Automação , Publicação FT.TG nº03, Departamento de Engenharia Mecatrônica, Universidade de Brasília, Brasília, DF, 2021. 61p.

CESSÃO DE DIREITOS

AUTOR: Victor Veloso Graciano

TÍTULO: Esquema De Sincronização Subatuado E Robusto Para Um Sistema Hipercaótico Pentadimensional Com Aplicação Em Telecomunicação Segura.

GRAU: Engenheiro de Controle e Automação ANO: 2021

É concedida à Universidade de Brasília permissão para reproduzir cópias deste relatório submetido como requisito para obtenção do grau de engenheiro de controle e automação e para emprestar ou vender tais cópias somente para propósitos acadêmicos e científicos. O autor se reserva a outros direitos de publicação e nenhuma parte deste relatório submetido como requisito para obtenção do grau de engenheiro de controle e automação pode ser reproduzida sem a autorização do autor.

Victor Veloso Graciano

UnB - Asa Norte, Brasília - DF, 70910-900

Resumo

O trabalho a seguir propõe um esquema de telecomunicação segura baseado em sincronização hipercaótica por controle subatuado projetado pela análise de Lyapunov. A implementação do canal seguro de comunicação depende da sincronização de dois sistemas pentadimensionais com dinâmica dominante idêntica, mas com condições iniciais distintas. O sistema transmissor da mensagem é dito mestre e o receptor, escravo, sendo que para realizar a sincronização projeta-se um terceiro sistema sincronizador que implementa o controle subatuado. Com a sincronização dos sistemas mestre e escravo é possível criptografar uma mensagem analógica ao adicioná-la a um dos estados do transmissor para depois decodificá-la pela subtração do sinal do mestre com o sinal do escravo. Diz-se que a mensagem é criptografada devido à natureza imprevisível do sistema hipercaótico. Em comparação com outros trabalhos da literatura atual, o trabalho proposto é mais simples por ser subatuado, ou seja, com sinal de controle de dimensão menor que a dimensão do sistemas hipercaóticos, o que possibilita implementação prática e de baixo custo com eletrônica analógica. Além disso o esquema aqui proposto é robusto pois inclui distúrbios limitados na análise de Lyapunov utilizada para projetar o controlador. Para validar o projeto simulou-se o esquema em *softwares* Matlab/Simulink.

Palavras-chave - Análise de Lyapunov, comunicação analógica segura, sincronização hipercaótica, controle não linear subatuado.

Keywords - Lyapunov analysis, analog secure communication, hyperchaotic synchronization, non-linear underactuated control.

Abstract

The following work proposes a secure communication scheme based on hyperchaotic synchronization by underactuated control designed with Lyapunov analysis. The secure communication channel depends on the synchronization of two identical 5D hyperchaotic systems with different initial conditions. The transmitter system is said to be the master and the receiver the slave such that the synchronization of them is achieved by a third system named synchronizer responsible for implementing the underactuated control law. With master and slave synchronized it is possible to encrypt an analog message by adding it to one of the states of the transmitter system in such a way that the message can be decoded by analysing the difference between master and slave signals after they have synchronized. In this configuration the message is said to be encrypted due to the unpredictable nature of hyperchaotic systems. In comparison to other works in current studies around the world, the one here proposed has the advantage of being simple since it is underactuated, i.e has a control signal with lesser dimensions than the 5D hyperchaotic system, enabling easy and cheap implementation of the practical circuits. In addition, the system is robust since limited disturbances were included in the Lyapunov analysis used to design the controller. To validate the proposed scheme the system was simulated in Matlab/Simulink.

SUMÁRIO

1	INTRODUÇÃO	1
1.1	REVISÃO DA LITERATURA	1
1.2	CONTRIBUIÇÃO	4
1.3	OBJETIVOS.....	5
1.4	ORGANIZAÇÃO DO TRABALHO.....	6
2	DEFINIÇÕES E CONCEITOS PRELIMINARES	7
2.1	SISTEMAS DINÂMICOS	7
2.2	TEORIA DA ESTABILIDADE DE LYAPUNOV	11
2.3	CAOS E HIPERCAOS	15
2.4	SINCRONIZAÇÃO CAÓTICA E COMUNICAÇÃO SEGURA	16
3	SINCRONIZAÇÃO DE UM SISTEMA HIPERCAÓTICO POR MEIO DE CONTROLE SUBTUADO PARA APLICAÇÃO EM TELECOMUNICAÇÃO SEGURA	18
3.1	FORMULAÇÃO DO PROBLEMA	19
3.2	PROVA POR ANÁLISE DE ESTABILIDADE DE LYAPUNOV	22
3.3	APLICAÇÃO EM TELECOMUNICAÇÃO SEGURA	26
4	SIMULAÇÃO <i>Matlab/Simulink</i>	27
4.1	AMBIENTE DE SIMULAÇÃO	27
4.2	PARÂMETROS DA SIMULAÇÃO	28
4.3	RESULTADOS DA SIMULAÇÃO	29
4.4	COMPARAÇÃO ENTRE SINCRONIZADORES.....	39
5	CONCLUSÕES	46
A	CÓDIGOS FONTE E DIAGRAMAS PARA SIMULAÇÃO <i>Matlab/Simulink</i>	52
A.1	DIAGRAMA DE BLOCOS <i>Simulink</i>	52
A.2	<i>PlantaMaster.m</i>	52
A.3	<i>Sinc.m</i>	53
A.4	<i>Graficos.m</i>	55
A.5	<i>GraficosMsg.m</i>	58

LISTA DE FIGURAS

2.1	Diagrama de blocos de um esquema de mascaramento caótico	17
4.1	Desempenho da sincronização dos estados $x_s(t)$ e $x_m(t)$	30
4.2	Desempenho da sincronização dos estados $y_s(t)$ e $y_m(t)$	30
4.3	Desempenho da sincronização dos estados $z_s(t)$ e $z_m(t)$	31
4.4	Desempenho da sincronização dos estados $w_s(t)$ e $w_m(t)$	31
4.5	Desempenho da sincronização dos estados $v_s(t)$ e $v_m(t)$	32
4.6	Erro de sincronização $e_1(t)$	32
4.7	Erro de sincronização $e_2(t)$	33
4.8	Erro de sincronização $e_3(t)$	33
4.9	Erro de sincronização $e_4(t)$	34
4.10	Erro de sincronização $e_5(t)$	34
4.11	Sinal mensagem $m_1(t)$ em contraste com o sinal transmitido.	35
4.12	Sinal mensagem $m_2(t)$ em contraste com o sinal transmitido.	36
4.13	Erro de recuperação da mensagem 1.....	37
4.14	Erro de recuperação da mensagem 2.....	37
4.15	Mensagem 1 recuperada em contraste com a mensagem original.	38
4.16	Mensagem 2 recuperada em contraste com a mensagem original.	38
4.17	Desempenho da sincronização dos estados $x_s(t)$ e $x_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).	40
4.18	Desempenho da sincronização dos estados $y_s(t)$ e $y_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).	40
4.19	Desempenho da sincronização dos estados $z_s(t)$ e $z_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).	41
4.20	Desempenho da sincronização dos estados $w_s(t)$ e $w_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).	41
4.21	Desempenho da sincronização dos estados $v_s(t)$ e $v_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).	42
4.22	Erro de sincronização $e_1(t)$ com lei de controle completamente atuada em con- traste com erro de sincronização para o mesmo estado com lei de controle su- batuada.	42
4.23	Erro de sincronização $e_2(t)$ com lei de controle completamente atuada em con- traste com erro de sincronização para o mesmo estado com lei de controle su- batuada.	43

4.24	Erro de sincronização $e_3(t)$ com lei de controle completamente atuada em contraste com erro de sincronização para o mesmo estado com lei de controle subatuada..	43
4.25	Erro de sincronização $e_4(t)$ com lei de controle completamente atuada em contraste com erro de sincronização para o mesmo estado com lei de controle subatuada..	44
4.26	Erro de sincronização $e_5(t)$ com lei de controle completamente atuada em contraste com erro de sincronização para o mesmo estado com lei de controle subatuada..	44
A.1	Diagrama de blocos no Simulink	52

LISTA DE SÍMBOLOS

Símbolo	Descrição
\forall	Para todo
$\ \quad \ $	Norma
\Rightarrow	Implica que
\exists	Existe
\in	Pertence a
\mathbb{R}	Conjunto dos números reais
∞	Infinito
s	"Subscrito" Escravo
m	"Subscrito" Mestre
$*$	"Sobrescrito" Ponto de equilíbrio
$-$	"Sobrescrito" Limitante superior

Capítulo 1

Introdução

1.1 Revisão da literatura

O estudo de dinâmicas visa analisar a maneira como determinados sistemas evoluem no tempo, ou seja, a partir da dinâmica de um sistema é possível analisar o comportamento futuro das variáveis que descrevem o fenômeno em estudo (STROGATZ, 2018).

Sistemas dinâmicos podem ser lineares ou não lineares a depender das relações entre suas variáveis de estado. Sistemas não lineares descrevem com maior precisão fenômenos naturais que são, na maioria das vezes, inerentemente não lineares (SLOTINE, 1991). Um exemplo de dinâmica não linear é observado no experimento do pêndulo invertido em que a aceleração angular do sistema varia de acordo com o seno da posição.

A não linearidade de alguns sistemas resulta em caos. A teoria do caos é o estudo de sistemas dinâmicos não lineares que, apesar de governados por leis determinísticas, apresentam comportamento pseudo aleatório devido a alta sensibilidade às condições iniciais (STROGATZ, 2018). Sistemas que apresentam comportamento caótico possuem dinâmica rica e variada e podem ser definidos de várias maneiras diferentes que englobam desde a medição do grau de aleatoriedade pela teoria ergódica até análises topológicas como a que propõe Robert L. Devaney (DEVANEY, 2008): Um sistema é caótico quando é topologicamente transitivo, tem resposta altamente sensível às condições iniciais e apresenta órbitas periódicas densas. Em suma um sistema é dito caótico quando possui características de imprevisibilidade, indecomponibilidade e algum elemento de regularidade, ou seja, é imprevisível devido à sensibilidade às condições iniciais, indecomponível devido à transitividade da topologia e regular por apresentar pontos periódicos densos (DEVANEY, 2008).

Acredita-se que o primeiro sistema caótico foi estudado por Isaac Newton no famoso problema dos três corpos, em que o objetivo era, a partir da velocidade e posição de três massas pontuais, determinar o movimento subsequente. O problema, que foi inspirado pela dinâmica de corpos celestiais, foi considerado de impossível resolução (STROGATZ, 2018) até que em 1890 Henri Poincaré (POINCARÉ, 1890) introduziu uma nova abordagem geométrica e qualitativa

que, ao invés de tentar explicitar as equações de movimento dos corpos, visa entender a estabilidade do sistema a longo prazo (STROGATZ, 2018). Apesar de Isaac Newton ter formulado o problema inicial, Poincaré, com sua nova abordagem, foi o primeiro a descrever um sistema determinístico que se comporta de maneira aperiódica e pseudo aleatória devido à sensibilidade dos estados às condições iniciais, ou seja, o primeiro a descrever o caos (STROGATZ, 2018).

Mesmo depois dos estudos de Poincaré a teoria do caos ainda ficou 70 anos em plano de fundo devido à grande dificuldade de se fazer à mão os cálculos iterativos necessários para a análise de sistemas caóticos. Com o advento do computador em 1950 pesquisadores, entre eles Edwards Lorenz, puderam simular sistemas com dinâmica caótica e analisar como esses evoluem no tempo. Em uma de suas simulações meteorológicas, Lorenz, tentando poupar tempo, iniciou a simulação no meio da evolução dos estados e percebeu que não obteve os mesmos resultados do que nas simulações anteriores. Lorenz ao analisar a discrepância entre as simulações percebeu que havia uma diferença de arredondamento entre as condições iniciais dos sistemas, que apesar de ínfimas, mudavam totalmente a previsão do tempo (LORENZ, 1963). A conclusão final de Lorenz é que não é possível fazer previsões meteorológicas com precisão a longo prazo devido à sensibilidade desse tipo de sistema às condições iniciais.

De acordo com o teorema de Poincaré-Bendixson, sistemas não lineares só podem apresentar comportamento caótico se tiverem dimensão superior a dois, ou seja, se possuírem pelo menos três equações de estados (WIGGINS, 1997). Existem também sistemas hipercaóticos que apresentam mais de três equações de estado e dois ou mais expoentes de Lyapunov positivos (STANKEVICH et al., 2019). No geral quanto maior a dimensão de um sistema caótico maior é o grau de imprevisibilidade e de complexidade da evolução dos estados ao longo do tempo, o que é muito útil quando se aplica esse tipo de sistema à criptografia de informações. O primeiro sistema hipercaótico foi descrito por Rössler (RÖSSLER, 1976) e mais recentemente vários outros sistemas quadridimensionais (PRAKASH et al., 2020) (SAHIN et al., 2020) e pentadimensionais (WEI; MOROZ et al., 2017) (TRIKHA; JAHANZAIB, 2020) (YU; LIU et al., 2020) apareceram na literatura. Como sistemas hipercaóticos são mais imprevisíveis e sensíveis às mudanças nas condições iniciais, são comumente utilizados em projetos de engenharia nas áreas de telecomunicação segura (KEKHA JAVAN et al., 2021) (OUANNAS et al., 2021) (TANG; MANDAL, 2021) (XIU et al., 2021), criptografia de imagens (NAIM; PACHA; SERIEF, 2021) (WEN et al., 2021) (XIAO-QING et al., 2021) e no âmbito de sistemas financeiros (GUIARTE et al., 2021) (MOUTSINGA; PINDZA; MARÉ, 2021), físicos (MAHMOUD; ABUALNAJA, 2021), biológicos (BALEANU et al., 2021) e etc.

Especificamente na área de comunicação segura os sistemas hipercaóticos são utilizados para gerar sinais pseudo-aleatórios que servem como máscara para criptografar uma mensagem sigilosa a ser transmitida em um canal suscetível à interceptação de terceiros (JOVIC, 2011). De maneira geral um sistema de comunicação segura baseado em hipercaos depende da sincronização de dois circuitos hipercaóticos: Um transmissor (mestre) e um receptor (escravo). O circuito transmissor é responsável pela criptografia da mensagem a ser enviada por um canal de comu-

nicação qualquer e o circuito escravo é responsável por recuperar a mensagem original a partir da sincronização com os estados do sistema mestre (JOVIC, 2011). O hipercaos garante que a mensagem será criptografada e os diferentes métodos de sincronização de sistemas caóticos garantem que a mensagem original possa ser recuperada pelo sistema escravo. Controle adaptativo (YANG, 2011) (GUIARTE et al., 2021) (KEKHA JAVAN et al., 2021), de modo deslizante (WEI; YOUSEFPOUR et al., 2021) (JAHANSHAHI et al., 2018) (WANG; YANG, 2021), PID (MECHERI; BOUDJEHEM; BOUDJEHEM, 2021), impulsivo (TAO YANG; CHUA, 1997) e *backstepping* (AZAR et al., 2021) são métodos comumente utilizados na literatura para atingir sincronia entre mestre e escravo.

A maioria dos esquemas de comunicação segura baseados em hipercaos encontrados na literatura utilizam um controle completamente atuado, ou seja, uma ação de controle com mesma dimensão do sistema como em (MAHMOUD; ABUALNAJA, 2021) (TIAN et al., 2021), o que torna a lei de controle demasiadamente complexa para a implementação em eletrônica analógica. Outra deficiência recorrente na literatura é a não inclusão de distúrbios (inerentes à implementação prática) na análise de Lyapunov dos sistemas, o que prejudica os esquemas em (OUANNAS et al., 2021) (TIAN et al., 2021) , por exemplo, em termos de robustez.

Motivado pelas deficiências encontradas nos trabalhos da literatura atual propõe-se um esquema de comunicação segura baseado em hipercaos a partir de um controle subatuado para que se possa implementar o circuito com componentes analógicos de baixo custo. Os circuitos mestre e escravo são baseados no sistema descrito em (WEI; MOROZ et al., 2017) que, por ser pentadimensional, apresenta maior grau de complexidade ao gerar o sinal criptografado se comparado com sistemas de menor dimensão como em (LU; WU; LÜ, 2002). Além disso o esquema a ser proposto inclui distúrbios e perturbações em sua análise e por isso é dito robusto.

1.2 Contribuição

A principal contribuição deste trabalho de conclusão de curso se concentra na proposta de um novo sistema de comunicação segura baseado em hipercaos que apresenta vantagens em vários aspectos se comparado com os esquemas presentes na literatura atual. A seguir tem-se as vantagens do sistema proposto:

- O esquema de comunicação segura é baseado em sistemas hipercaóticos pentadimensionais, que apresentam comportamento pseudo-aleatório mais acentuado que sistemas caóticos ou até hipercaóticos quadridimensionais como em (PÉREZ et al., 2020) (YU; QIAN et al., 2020). Tal característica garante um canal de comunicação mais seguro.
- O sinal de controle utilizado para sincronizar os sistemas mestre e escravo é simples e subatuado o que implica em uma implementação simples e barata do circuito a partir de componentes analógicos (Amplificadores operacionais, resistores, capacitores e multiplicadores analógicos) diferentemente do controle completamente atuado proposto em (MAHMOUD; ABUALNAJA, 2021) (WEI; YOUSEFPOUR et al., 2021) (TIAN et al., 2021) (YU; QIAN et al., 2020).
- A inclusão de distúrbios limitados na análise de estabilidade de Lyapunov para o sistema proposto é responsável pela robustez do esquema de comunicação, característica muito importante para aplicações práticas em que distúrbios e perturbações são inevitáveis. Os seguintes trabalhos são exemplos da literatura atual de esquemas que não levam em conta distúrbios (MAHMOUD; ABUALNAJA, 2021) (KEKHA JAVAN et al., 2021) (AL-SAIDI et al., 2020).

1.3 Objetivos

O seguinte trabalho de conclusão de curso tem como objetivo propor e implementar um esquema de telecomunicação segura a partir da sincronização de dois sistemas hipercaóticos pentadimensionais idênticos, mas que partem de condições iniciais distintas. Os sistemas hipercaóticos são denominados mestre e escravo e a mensagem a ser transmitida é somada aos estados do mestre para que o sinal analógico seja criptografado pela máscara caótica. Por meio de um controle subatuado sincroniza-se os sistemas mestre e escravo para que se possa decodificar a mensagem original.

O esquema deve ser simples para que se possa implementar um circuito correspondente com componentes analógicos de baixo custo e robusto para que tenha utilidade em aplicações reais. O método de sincronização escolhido (controle simples e subatuado) garante a simplicidade do esquema e a inclusão de distúrbios limitados na análise de estabilidade de Lyapunov garante a robustez necessária. Enfim será feita a validação do esquema proposto por meio de simulações nos *softwares* Matlab/Simulink.

1.4 Organização do trabalho

O trabalho está organizado nos seguinte capítulos:

- Capítulo 1: Revisão da literatura, história do estudo de sistemas caóticos, contribuições e objetivos .
- Capítulo 2: Introdução teórica para o estudo de sistemas dinâmicos não lineares e caóticos: Teoria da estabilidade de Lyapunov, sincronização caótica.
- Capítulo 3: Propõe-se uma solução ao problema de sincronização de um sistemas caóticos por meio de técnicas de controle não linear e prova-se a limitação do erro pela teoria de Lyapunov.
- Capítulo 4: Validação do esquema de telecomunicação segura por meio de *softwares* de simulação: Matlab/Simulink.
- Capítulo 5: Conclusões sobre o projeto desenvolvido nesse trabalho de conclusão de curso.

Capítulo 2

Definições e conceitos preliminares

Neste capítulo é feita uma revisão de conceitos necessários para a compreensão do trabalho proposto. As seções a seguir foram baseadas em livros conceituados da literatura (KHALIL, 2002) (IOANNOU; SUN, 2012) (SLOTINE, 1991) e introduzem tanto definições matemáticas quanto conceitos da teoria de estabilidade de Lyapunov.

2.1 Sistemas dinâmicos

No estudo de sistemas dinâmicos objetiva-se definir a evolução dos estados de um sistema físico ao longo do tempo. Para isso analisa-se o comportamento das variáveis de interesse em determinado processo a partir de equações diferenciais provenientes das relações físicas entre os componentes do sistema em questão. Uma maneira de modelar sistemas dinâmicos consiste em definir um sistema com número finito de equações diferenciais (KHALIL, 2002) como as que seguem:

$$\begin{aligned}\dot{x}_1 &= f_1(t, x_1, \dots, x_n, u_1, \dots, u_p) \\ \dot{x}_2 &= f_2(t, x_1, \dots, x_n, u_1, \dots, u_p) \\ \dot{x}_3 &= f_3(t, x_1, \dots, x_n, u_1, \dots, u_p) \\ &\vdots \\ \dot{x}_n &= f_n(t, x_1, \dots, x_n, u_1, \dots, u_p)\end{aligned}\tag{2.1}$$

em que, \dot{x}_i representa a derivada em relação ao tempo de cada uma das variáveis de estado x_i e as entradas do sistema são representadas por u_1, u_2, \dots, u_p . Reescreve-se o sistema de equações

diferenciais na forma matricial definindo:

$$x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ \vdots \\ x_n \end{bmatrix}, \quad u = \begin{bmatrix} u_1 \\ u_2 \\ u_3 \\ \vdots \\ \vdots \\ u_p \end{bmatrix}, \quad f(t, x, u) = \begin{bmatrix} f_1(t, x, u) \\ f_2(t, x, u) \\ f_3(t, x, u) \\ \vdots \\ \vdots \\ f_n(t, x, u) \end{bmatrix} \quad (2.2)$$

assim, tem-se a partir de (2.1) e (2.2):

$$\dot{x} = f(t, x, u) \quad (2.3)$$

a equação (2.3) é chamada de equação de estados em que u é o vetor de entrada e x é o vetor de estados. Em alguns casos a equação de estados vem acompanhada da equação de saída:

$$y = h(t, x, u) \quad (2.4)$$

A equação (2.4), em conjunto com a equação (2.3), representa o modelo no espaço de estados. Comumente trabalha-se com a representação não forçada da equação de estados em que a entrada u não aparece explicitamente:

$$\dot{x} = f(t, x) \quad (2.5)$$

A representação não forçada não implica que a entrada é nula, já que u pode ser uma função do tempo ou uma função dos próprios estados (realimentação de estados). Adicionalmente, se a equação de estados não forçada (2.5) independe do tempo, o sistema é dito autônomo ou invariante no tempo e pode ser representado por:

$$\dot{x} = f(x) \quad (2.6)$$

2.1.1 Ponto de equilíbrio

O estudo dos pontos de equilíbrio é de suma importância para a análise de sistemas dinâmicos, já que pontos de equilíbrio representam uma região no espaço de estados em que as trajetórias dos estados deixam de evoluir. Em outras palavras, se o sistema começa em um ponto de equilíbrio ele permanece no ponto de equilíbrio para todo tempo futuro, característica importante para a análise de estabilidade de sistemas dinâmicos. Matematicamente falando o ponto de equilíbrio representa o ponto no espaço de estados em que a derivada dos estados \dot{x} é

nula. Para o caso de um sistema invariante no tempo temos que o ponto de equilíbrio x_e pode ser determinado por:

$$\left[\frac{dx}{dt} \right]_{x=x_e} = 0 \quad (2.7)$$

2.1.2 Sistemas dinâmicos lineares

Em sistemas dinâmicos lineares as equações de estado são caracterizadas sempre por relações lineares entre as variáveis de estado, o que significa que é possível utilizar o método da superposição para analisar o comportamento do tipo de sistema em questão. No caso linear é possível escrever a equação (2.3) da seguinte forma:

$$\begin{aligned} \dot{x} &= A(t)x + B(t)u \\ y &= C(t)x + D(t)u \end{aligned} \quad (2.8)$$

em que, A é a matriz que representa a dinâmica da planta, B é a matriz de entrada, C a matriz de saída e D a matriz que representa a influência da entrada no sinal de saída do sistema.

2.1.3 Sistemas dinâmicos não lineares

Em sistemas não lineares as técnicas de análise que dependem da superposição não se aplicam, por isso não é possível fazer análise no domínio de Laplace por exemplo. Tendo em vista a versatilidade e simplicidade das técnicas de análise de sistemas lineares, um primeiro passo comum para a análise de sistemas não lineares é linearização das equações que descrevem o sistema em torno de um ponto de operação. Linearizar é útil em vários casos, mas é uma técnica que possui três desvantagens principais:

- A linearização nem sempre é possível, já que alguns sistemas dinâmicos apresentam descontinuidades no tempo em sua primeira derivada.
- O comportamento de um sistema não linear que foi linearizado só pode ser previsto localmente, já que a validade do modelo depende da proximidade da região no espaço de estados do ponto de operação escolhido para a linearização.
- O processo de linearizar um sistema consiste em desconsiderar termos de alta ordem, que podem apresentar uma dinâmica rica e útil em várias áreas do conhecimento como comunicação segura. Múltiplos pontos de equilíbrio e modos de comportamento, presença de ciclos limite e caos são exemplos de dinâmicas essencialmente não lineares que são descartadas com a técnica de linearização.

2.1.4 Escalonamento em amplitude e frequência

Para algumas aplicações é necessário que um sistema dinâmico se comporte dentro de uma faixa específica de amplitudes e frequências. Isso ocorre pois para implementar um circuito prático, por exemplo, devemos ter cuidado com a amplitude dos sinais para não saturar ou danificar os componentes e com a frequência dos sinais para que o processo ocorra na velocidade projetada.

O escalonamento na amplitude pode ser feito facilmente por uma parametrização das variáveis de estado da forma:

$$\tilde{x} = \frac{x}{r} \quad (2.9)$$

que implica em:

$$\dot{\tilde{x}} = \frac{\dot{x}}{r} \quad (2.10)$$

em que, r é um número real que representa em quantas vezes deseja-se aumentar ou diminuir amplitude do estado x . Adicionalmente deve-se parametrizar também as condições iniciais do sistema para manter o comportamento desejado.

Já o escalonamento na frequência é ainda mais simples e consiste apenas em multiplicar a equação de estados por um fator n qualquer. Se deseja-se aumentar a velocidade com que ocorre o processo, n deve ser maior que um e se o objetivo é reduzir a velocidade n deve ser menor que um. Assim como no escalonamento em amplitude também é necessário multiplicar as condições iniciais do processo pelo fator n no escalonamento na frequência para que se obtenha a mesma dinâmica.

2.2 Teoria da estabilidade de Lyapunov

Nesta seção aborda-se os conceitos introdutórios da análise de estabilidade de Lyapunov de acordo com (SLOTINE, 1991) (IOANNOU; SUN, 2012). As definições a seguir são úteis para classificar os pontos de equilíbrio de um sistema dinâmico não linear autônomo quanto sua estabilidade a partir de análises geométricas no espaço de estados. Para simplificar denota-se B_R como a região esférica definida por $\|x\| < R$ no espaço de estados e S_R a esfera propriamente dita definida por $\|x\| = R$.

2.2.1 Estabilidade

Definição 2.2.1: O ponto de equilíbrio $x = 0$ é dito estável se, para todo $R > 0$, existe um $r > 0$ em que, se $\|x(0)\| < r$ então $\|x(t)\| < R$ para todo $t > 0$.

Essencialmente estabilidade no senso de Lyapunov significa que a trajetória do sistema no espaço de estados é limitada por uma região B_R sempre que começar dentro de uma região B_r em que $r < R$. Utilizando a notação matemática temos:

$$\forall R > 0, \exists r > 0 \text{ tal que } \|x(0)\| < r \Rightarrow \forall t > 0, \|x(t)\| < R$$

2.2.2 Estabilidade assintótica e exponencial

Definição 2.2.2.1: O ponto de equilíbrio $x = 0$ é dito assintoticamente estável se é estável e adicionalmente se existe um $r > 0$ em que, se $\|x(0)\| < r$ então $\|x(t)\|$ tende a 0 para t tendendo a ∞ .

Um sistema é dito assintoticamente estável se for estável e se ao iniciar dentro da região B_r apresentar trajetórias que convergem para zero no infinito.

Definição 2.2.2.2: O ponto de equilíbrio $x = 0$ é dito exponencialmente estável se, a convergência das trajetórias do sistema para a origem ocorre em velocidade exponencial.

Vale ressaltar que estabilidade exponencial implica em estabilidade assintótica, porém o contrário não é válido.

2.2.3 Estabilidade local e global

As definições abordadas até agora assumem que o sistema terá estado inicial próximo ao ponto de equilíbrio para fazer a análise e por isso são denominadas definições de estabilidade local. Definições locais de estabilidade falham em descrever as propriedades do sistema quando as condições iniciais são distantes do ponto de equilíbrio.

Definição 2.2.3: Se um sistema é assintoticamente (ou exponencialmente) estável para qualquer estado inicial então é dito globalmente assintoticamente (ou exponencialmente) estável.

2.2.4 Análise de Lyapunov por linearização

A análise de Lyapunov por linearização assume que a estabilidade de um sistema não linear pode ser analisada localmente a partir da estabilidade do sistema linearizado. Sabe-se que linearização do sistema só é válida para as proximidades do ponto de equilíbrio e por isso diz-se que a estabilidade por linearização é local. A linearização é feita por meio da expansão em série de Taylor em torno dos pontos de equilíbrio que, no espaços de estados, consiste em encontrar o Jacobiano da matriz que representa a dinâmica dos estados avaliada no ponto de equilíbrio. Os seguintes resultados explicitam as relações entre a estabilidade do sistema não linear e a estabilidade do sistema linearizado.

Teorema 2.2.4 (Método de linearização de Lyapunov):

- Se o sistema linearizado é estritamente estável (autovalores da matriz A estritamente no semi-plano esquerdo do plano complexo) então o ponto de equilíbrio é assintoticamente estável para o sistema não linear.
- Se o sistema linearizado é instável (Ao menos um autovalor de A no semi-plano direito) então o sistema não linear é instável.
- Se o sistema linearizado é marginalmente estável (autovalores de A no semi-plano esquerdo do plano complexo, mas com ao menos um autovalor no eixo imaginário) então não é possível concluir nada sobre a estabilidade do sistema não linear que pode ser estável, assintoticamente estável ou até mesmo instável.

2.2.5 Método direto de Lyapunov

A análise de estabilidade de um sistema não linear é feita geralmente pelo método direto de Lyapunov que em sua essência parte de uma observação física: Se a energia total de um sistema é continuamente dissipada ao longo do tempo, então o sistema deve eventualmente atingir um ponto de equilíbrio. É possível então, analisar a estabilidade de um sistema dinâmico a partir da variação no tempo de uma função escalar que representa a energia total do sistema, denominada candidata de Lyapunov $V(x)$. O método direto é poderoso pois nos permite contornar as definições complexas de estabilidade, já que para fazer a análise basta definir uma candidata e analisar sua derivada no tempo $\dot{V}(x)$. A seguir temos as definições e teoremas necessários para analisar um sistema dinâmico pelo método direto de Lyapunov:

Definição 2.2.5.1: Funções $V(x)$ são ditas positivas definidas se apresentam um mínimo único na origem, ou seja, se $V(x) > 0$ para todo $x \neq 0$, $V(x)$ é dita globalmente positiva definida.

Se $x \neq 0$ implica em $V(x) > 0$ somente em uma região limitada a função é dita localmente positiva definida.

Definição 2.2.5.2: Funções $V(x)$ são ditas negativas semi-definidas se $V(x) \leq 0$. Se a função que representa a derivada da energia total do sistema for negativa semi-definida então pode-se afirmar pelo método direto de Lyapunov que o sistema é estável.

Definição 2.2.5.3: Se em uma região esférica, uma candidata $V(x)$ for positiva definida, apresentar derivadas parciais contínuas e derivada no tempo $\dot{V}(x)$ negativa semi-definida denomina-se $V(x)$ como uma função de Lyapunov.

Definição 2.2.5.4: Uma solução $x(t; x_0, t_0)$ das equações diferenciais que representam um sistema dinâmico é dita limitada se existe $\beta > 0$ tal que $x(t; x_0, t_0) < \beta$ para todo $t > t_0$.

Definição 2.2.5.5: Uma solução $x(t; x_0, t_0)$ das equações diferenciais que representam um sistema dinâmico é dita uniformemente limitada se para todo $\alpha > 0$ existe $\beta = \beta(\alpha)$ tal que, se $\|x_0\| < \alpha$ então $\|x(t; x_0, t_0)\| < \beta$ para todo $t > t_0$.

Definição 2.2.5.6: Uma solução $x(t; x_0, t_0)$ das equações diferenciais que representam um sistema dinâmico é dita uniformemente finalmente limitada (com limitante B) se existir um $B > 0$ e se para todo $\alpha \geq 0$, existir um $T = T(\alpha) > 0$ tal que $\|x_0\| < \alpha$ implica em $\|x(t; x_0, t_0)\| < B$ para todo $t > t_0 + T$

Definição 2.2.5.7: Uma função contínua $\varphi : [0, \infty) \mapsto \mathbb{R}^+$ pertence à classe \mathcal{K} se:

- $\varphi(0) = 0$
- φ é estritamente crescente em $[0, \infty)$

Definição 2.2.5.8: Uma função contínua $\varphi : [0, r) \mapsto \mathbb{R}^+$ pertence à classe \mathcal{KR} se:

- $\varphi(0) = 0$
- φ é estritamente crescente em $[0, \infty)$
- $\lim_{r \rightarrow \infty} \varphi(r) = \infty$

Teorema de Lyapunov para estabilidade local: Se, em uma região esférica B_r , existe uma função escalar $V(x)$ com primeiras derivadas parciais contínuas em que

- $V(x)$ seja positiva definida (localmente em B_r)
- $\dot{V}(x)$ seja negativa semi-definida (localmente em B_r)

então o ponto de equilíbrio na origem é estável. Se adicionalmente $\dot{V}(x)$ for localmente negativa definida ($\dot{V}(x) < 0 \forall x$ em B_r) então o ponto de equilíbrio é dito assintoticamente localmente estável.

Teorema de Lyapunov para estabilidade global: Para que o sistema seja globalmente estável é necessário expandir a região B_r para todo o espaço de estados mantendo as condições vistas no teorema local e adicionando uma condição extra para $V(x)$, que deve ser radialmente ilimitada. Então, para classificar o ponto de equilíbrio na origem como globalmente estável é necessário que

- $V(x)$ seja positiva definida para todo o espaço de estados
- $\dot{V}(x)$ seja negativa definida para todo o espaço de estados
- $V(x) \rightarrow \infty$ se $\|x\| \rightarrow \infty$

Teorema da limitação: Se existe uma função $V(x)$ com primeira derivada contínua e se existe $\varphi_1, \varphi_2 \in \mathcal{KR}$ tal que

- $\varphi_1(\|x\|) \leq V(x) \leq \varphi_2(\|x\|)$
- $\dot{V}(x) \leq 0$

a solução das equações diferenciais que representam o sistema dinâmico é dita uniformemente limitada. Adicionalmente, se existe $\varphi_3 \in \mathcal{K}$ tal que

- $\dot{V}(x) \leq -\varphi_3(\|x\|)$

a solução é dita uniformemente finalmente limitada.

2.3 Caos e Hipercaos

O estudo de sistemas não lineares impulsionou a descoberta de dinâmicas exóticas que possibilitam modelar sistemas com utilidade prática em várias áreas do conhecimento. O caos é um desses tipos de dinâmica interessante e é definido em (STROGATZ, 2018) como o comportamento aperiódico a longo termo de um sistema determinístico que apresenta grande sensibilidade às condições iniciais.

Para caracterizar sistemas dinâmicos como caóticos matematicamente é necessário analisar o quão rapidamente divergem trajetórias que começam infinitesimalmente próximas umas das outras. Assim, avalia-se a sensibilidade do sistema às condições iniciais, característica essencial para definir o caos. Suponha que $\delta(t)$ represente a distância entre as trajetórias e que δ_0 represente a distância no momento inicial t_0 , em que as trajetórias estão infinitesimalmente próximas entre si, pode-se encontrar por análises numéricas (STROGATZ, 2018) a seguinte relação:

$$\|\delta(t)\| = \|\delta_0\| e^{\lambda(t-t_0)} \quad (2.11)$$

em que λ é denominado expoente de Lyapunov. Um sistema com n dimensões apresenta igual quantidade de expoentes de Lyapunov, mas a presença de apenas um que seja positivo já caracteriza o sistema como caótico. Vale ressaltar que o teorema de Poincaré-Bendixson exclui a possibilidade de caos para sistemas com duas ou menos dimensões. Sistemas caóticos com dimensão superior ou igual a quatro são ditos hipercaóticos quando apresentam dois ou mais expoentes de Lyapunov positivos. Sistemas hipercaóticos são, por conseguinte, preferíveis quando a característica que deseja-se explorar da dinâmica de um sistema é a imprevisibilidade.

2.4 Sincronização caótica e comunicação segura

Os conceitos a seguir a respeito da sincronização de sistemas caóticos foram retirados de (JOVIC, 2011). O primeiro método para sincronizar sistemas caóticos foi desenvolvido por Pecora-Caroll (PECORA; CARROLL, 1990) e consiste basicamente de um sistema mestre e um sistema escravo, topologicamente idênticos (mesmas equações diferenciais), em que pelo menos um dos sinais do mestre está disponível para o escravo seguir. A nomenclatura mestre-escravo vem do fato de que o sistema dito escravo segue o sinal do mestre para atingir a sincronização.

Sistemas caóticos são por definição sensíveis às condições iniciais, ou seja, trajetórias que se iniciam arbitrariamente próximas umas das outras se separam exponencialmente ao longo do tempo. Essa característica torna o problema de sincronizar sistemas caóticos um desafio mesmo quando os sistemas em questão são idênticos como no método Pecora-Caroll (PC). O método utilizado para o projeto do esquema de telecomunicação proposto neste trabalho é chamado mascaramento caótico (OPPENHEIM et al., 1992), que se baseia no método PC e que foi experimentalmente demonstrado em (KOCAREV et al., 1992).

2.4.1 Mascaramento caótico

O mascaramento caótico é uma das primeiras técnicas de comunicação segura baseada em caos a aparecer na literatura. O método é inspirado pela técnica proposta por Pecora-Caroll (PC) e portanto envolve sistemas caóticos ditos mestre e escravo. As mensagens a serem transmitidas pelo canal de comunicação seguro obtido pelo método do mascaramento caótico são primariamente analógicas.

O canal de comunicação seguro no mascaramento caótico se dá pela adição da mensagem a um dos estados do sistema mestre, que por isso é denominado transmissor. O resultado dessa soma (mensagem criptografada) é então transmitido por um canal de comunicação qualquer, tendo em vista que a mensagem original se encontra misturada ao comportamento caótico e, portanto, imprevisível do sistema mestre. O diagrama a seguir ilustra um esquema de comunicação segura baseado em mascaramento caótico.

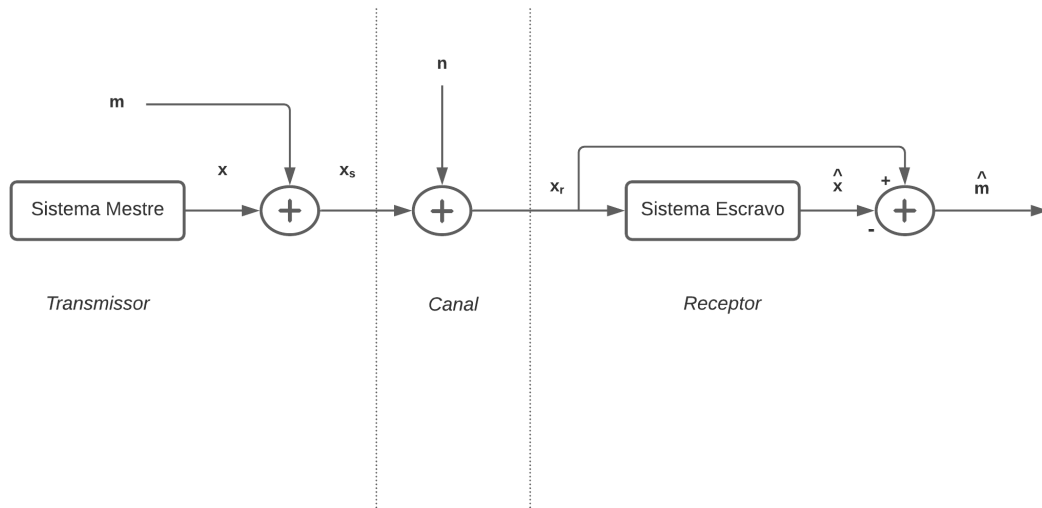


Figura 2.1: Diagrama de blocos de um esquema de mascaramento caótico

Na figura 2.1 m denota a mensagem a ser transmitida e n um ruído gaussiano decorrente das condições do canal de transmissão. Para denotar a mensagem criptografada (mensagem original somada à um dos sinais do sistema mestre) utilizou-se x_s e para denotar a mensagem afetada pelo ruído gaussiano após a transmissão utilizou-se x_r . O sistema escravo recebe então o sinal x_r e gera um sinal \hat{x} , sendo que, \hat{x} deve se aproximar de x_s após a sincronização. Para recuperar a mensagem original m basta fazer:

$$\hat{m} = x_r - \hat{x} = (m + x) - \hat{x} \approx m \quad (2.12)$$

em que, \hat{m} representa a mensagem estimada pelo esquema que converge para a mensagem original dadas as condições de sincronização.

Vale ressaltar que para que o mascaramento caótico funcione é necessário que a potência da portadora caótica (sinal do sistema mestre que serve de máscara) seja ordens de grandeza maior que a potência do sinal que representa a mensagem a ser transmitida.

Capítulo 3

Sincronização de um sistema hipercaótico por meio de controle subatuado para aplicação em telecomunicação segura

Neste capítulo aborda-se o problema de sincronizar dois sistemas hipercaóticos de modo que seja possível utilizá-los em um esquema de telecomunicação segura. O trabalho aqui proposto é uma extensão de (WEI; MOROZ et al., 2017), pois esse artigo define o sistema hipercaótico aqui utilizado como base. A sincronização é subatuada e por isso apresenta contribuições em relação a (MAHMOUD; ABUALNAJA, 2021) que atinge a sincronização com controle completamente atuado, principalmente no que diz respeito à aplicação em telecomunicação segura que depende de um controle com dimensão menor que a dimensão dos sistemas dinâmicos. Para facilitar o entendimento, dividiu-se o capítulo nas seguintes seções: Formulação do problema, Prova matemática por meio da teoria de estabilidade de Lyapunov, Aplicação em telecomunicação segura.

3.1 Formulação do problema

Considere o seguinte sistema hipercaótico que descreve a dinâmica de um dínamo de disco homopolar autoexcitante pentadimensional (WEI; MOROZ et al., 2017):

$$\begin{aligned}
 \dot{x} &= r(y - x) + w \\
 \dot{y} &= -(1 + m)y + xz - v \\
 \dot{z} &= g[1 + mx^2 - (1 + m)xy] \\
 \dot{w} &= 2(1 + m)w + xz - k_1x \\
 \dot{v} &= -mv + k_2y
 \end{aligned} \tag{3.1}$$

Os parâmetros são configurados de maneira que o comportamento do sistema seja caótico (WEI; MOROZ et al., 2017), ou seja, com $r = 8$, $m = 0.04$, $g = 140.6$, $k_1 = 34$ e $k_2 = 12$. Tendo em vista que as variáveis x, y, z, w e v representam os estados do sistema dinâmico e tomando (3.1) como base, define-se os sistemas mestre e escravo como a seguir:

Sistema mestre:

$$\begin{aligned}
 \dot{x}_m &= r(y_m - x_m) + w_m \\
 \dot{y}_m &= -(1 + m)y_m + x_m z_m - v_m \\
 \dot{z}_m &= g[1 + mx_m^2 - (1 + m)x_m y_m] \\
 \dot{w}_m &= 2(1 + m)w_m + x_m z_m - k_1 x_m \\
 \dot{v}_m &= -mv_m + k_2 y_m
 \end{aligned} \tag{3.2}$$

Sistema escravo:

$$\begin{aligned}
 \dot{x}_s &= r(y_s - x_s) + w_s + h_1(t) + u_1 \\
 \dot{y}_s &= -(1 + m)y_s + x_s z_s - v_s + h_2(t) + u_2 \\
 \dot{z}_s &= g[1 + mx_s^2 - (1 + m)x_s y_s] + h_3(t) + u_3 \\
 \dot{w}_s &= 2(1 + m)w_s + x_s z_s - k_1 x_s + h_4(t) + u_4 \\
 \dot{v}_s &= -mv_s + k_2 y_s + h_5(t) + u_5
 \end{aligned} \tag{3.3}$$

em que os estados do sistema mestre são denotados com subscrito m e os estados do sistema escravo com subscrito s . Os sinais de distúrbio são representados pelo símbolo h e estão presentes no sistema escravo para representar imprevisibilidades inerentes à situações práticas e tornar a análise robusta. Os sinais $u(t)_{1...5}$ são ações de controle responsáveis por tornar o erro de sincronização uniformemente finalmente limitado.

Hipótese 1: Assume-se que os distúrbios são limitados da seguinte maneira:

$$\begin{aligned}
|h_1(t)| &\leq \bar{h}_1 \\
|h_2(t)| &\leq \bar{h}_2 \\
|h_3(t)| &\leq \bar{h}_3 \\
|h_4(t)| &\leq \bar{h}_4 \\
|h_5(t)| &\leq \bar{h}_5
\end{aligned} \tag{3.4}$$

em que $\bar{h}_{1...5}$ são constantes positivas.

O problema se resume em sincronizar o sistema escravo e o mestre de forma a tornar possível a aplicação do esquema em telecomunicação segura. A sincronização dos sistemas dinâmicos significa que os sinais dos estados do sistema escravo seguem os sinais dos respectivos estados no sistema mestre. Vale lembrar que os sistemas em questão são hipercaóticos e por isso, muito sensíveis às condições iniciais, além de apresentarem comportamento aparentemente aleatório, o que torna a sincronização uma tarefa mais complexa.

Deseja-se por fim que a ação de controle seja capaz de tornar o erro de sincronização uniformemente finalmente limitado, assim garantindo a sincronização entre mestre e escravo. Para isso analisa-se primeiramente as equações que definem os erros de sincronização:

$$\begin{aligned}
e_1 &= x_s - x_m \\
e_2 &= y_s - y_m \\
e_3 &= z_s - z_m \\
e_4 &= w_s - w_m \\
e_5 &= v_s - v_m
\end{aligned} \tag{3.5}$$

Tomando-se a derivada, encontra-se as equações para a dinâmica dos erros de sincronização:

$$\begin{aligned}
\dot{e}_1 &= \dot{x}_s - \dot{x}_m \\
\dot{e}_2 &= \dot{y}_s - \dot{y}_m \\
\dot{e}_3 &= \dot{z}_s - \dot{z}_m \\
\dot{e}_4 &= \dot{w}_s - \dot{w}_m \\
\dot{e}_5 &= \dot{v}_s - \dot{v}_m
\end{aligned} \tag{3.6}$$

Substituindo-se as equações de (3.2) e (3.3) em (3.6), obtém-se:

$$\begin{aligned}
\dot{e}_1 &= r(y_s - x_s) + w_s + h_1(t) + u_1 - (r(y_m - x_m) + w_m) \\
\dot{e}_2 &= -(1+m)y_s + x_s z_s - v_s + h_2(t) + u_2 - (-(1+m)y_m + x_m z_m - v_m) \\
\dot{e}_3 &= g[1 + mx_s^2 - (1+m)x_s y_s] + h_3(t) + u_3 - (g[1 + mx_m^2 - (1+m)x_m y_m]) \\
\dot{e}_4 &= 2(1+m)w_s + x_s z_s - k_1 x_s + h_4(t) + u_4 - (2(1+m)w_m + x_m z_m - k_1 x_m) \\
\dot{e}_5 &= -mv_s + k_2 y_s + h_5(t) + u_5 - (-mv_m + k_2 y_m)
\end{aligned} \tag{3.7}$$

A partir das relações em (3.5) pode-se reescrever as equações de (3.6) em função dos erros de sincronização:

$$\begin{aligned}
\dot{e}_1 &= r(e_2 - e_1) + e_4 + h_1(t) + u_1 \\
\dot{e}_2 &= -(1+m)e_2 + e_1 e_3 + x_m e_3 + z_m e_1 - e_5 + h_2(t) + u_2 \\
\dot{e}_3 &= g[m(e_1^2 + 2e_1 x_m) - (1+m)(e_1 e_2 + e_1 y_m + e_2 x_m)] + h_3(t) + u_3 \\
\dot{e}_4 &= 2(1+m)e_4 + e_1 e_3 + x_m e_3 + e_1(z_m - k_1) + h_4(t) + u_4 \\
\dot{e}_5 &= -me_5 + k_2 e_2 + h_5(t) + u_5
\end{aligned} \tag{3.8}$$

Fato 1: Os estados do sistema mestre são limitados (WEI; MOROZ et al., 2017), ou seja,

$$\begin{aligned}
|x_m| &\leq \bar{X} \\
|y_m| &\leq \bar{Y} \\
|z_m| &\leq \bar{Z} \\
|w_m| &\leq \bar{W} \\
|v_m| &\leq \bar{V}
\end{aligned} \tag{3.9}$$

em que, \bar{X} , \bar{Y} , \bar{Z} , \bar{W} , \bar{V} são constantes positivas desconhecidas.

Para que o erro seja uniformemente finalmente limitado em tempo finito sugere-se os seguintes sinais para a ação de controle:

$$\begin{aligned}
u_1 &= -\psi_1 e_1 - \psi_2 e_1^3 \\
u_2 &= 0 \\
u_3 &= -\psi_3 e_3 - \psi_4 e_3^3 \\
u_4 &= -\psi_5 e_4 \\
u_5 &= 0
\end{aligned} \tag{3.10}$$

em que, $\psi_{1\dots 5} > 0$ são constantes definidas pelo usuário.

Teorema: Tendo em vista os sistemas mestre e escravo definidos em (3.2) e (3.3) e a lei de controle definida em (3.10),

se $\psi_1 > -r + \frac{1}{2}[\sigma_1 + \sigma_6(r + \bar{Z})^2 + \sigma_9(1 + \bar{Z} + k_1)^2 + \frac{2m\bar{X}}{1+m} + \bar{Y}]$, $\psi_2 > \frac{1}{2}(\sigma_8 + \frac{\sigma_7^2}{4})$, $\psi_3 > \frac{g(1+m)}{2}[\frac{\sigma_3}{g^2(1+m)^2} + \sigma_8^{-1}\frac{m^2}{(1+m)^2} + \frac{2m\bar{X}}{1+m} + \bar{Y} + \sigma_{10}\bar{X}^2]$, $\psi_4 > \frac{\sigma_7^2}{4}$ e $\psi_5 > 2(1+m) + \frac{1}{2}(\sigma_4 + \sigma_7^{-1} + \sigma_9^{-1} + \sigma_{10}^{-1})$,

Então o erro de sincronização converge em tempo finito para o conjunto compacto $\Omega = \{e \in \mathbb{R}^5 \text{ tal que } \|e\| \leq \sqrt{\frac{\beta}{\rho}}\}$,

em que $\beta = \frac{1}{2}(\bar{h}_1\sigma_1^{-1} + \bar{h}_3\sigma_3^{-1} + \bar{h}_4\sigma_4^{-1}) + \frac{1}{2}(\bar{h}_2\sigma_2^{-1} + \bar{h}_5\sigma_5^{-1}k_2^{-2})$, $\rho = \min(\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6, \rho_7)$ com $\rho_1 = \psi_1 + r - \frac{1}{2}(\sigma_1 + \sigma_6(r + \bar{Z})^2 + \sigma_9(1 + \bar{Z} + k_1)^2 + \frac{2m\bar{X}}{1+m} + \bar{Y})$, $\rho_2 = 1 + m - \frac{1}{2}(\sigma_2 + \sigma_6^{-1})$, $\rho_3 = \frac{\psi_3}{g(1+m)} - \frac{1}{2}[\frac{\sigma_3}{g^2(1+m)^2} + \sigma_8^{-1}\frac{m^2}{(1+m)^2} + \frac{2m\bar{X}}{1+m} + \bar{Y} + \sigma_{10}\bar{X}^2]$, $\rho_4 = \psi_5 - 2(1+m) - \frac{1}{2}(\sigma_4 + \sigma_7^{-1} + \sigma_9^{-1} + \sigma_{10}^{-1})$, $\rho_5 = \frac{m}{k_2} - \frac{1}{2}\sigma_5$, $\rho_6 = \psi_2 - \frac{1}{2}(\sigma_8 + \frac{\sigma_7^2}{4})$, $\rho_7 = \psi_4 - \frac{\sigma_7^2}{4}$.

3.2 Prova por análise de estabilidade de Lyapunov

Prova: Considere a seguinte candidata de Lyapunov:

$$V = \frac{1}{2} \left(e_1^2 + e_2^2 + \frac{e_3^2}{g(1+m)} + e_4^2 + \frac{e_5^2}{k_2} \right) \tag{3.11}$$

Derivando a função em (3.11), tem-se:

$$\dot{V} = e_1\dot{e}_1 + e_2\dot{e}_2 + \frac{e_3\dot{e}_3}{g(1+m)} + e_4\dot{e}_4 + \frac{e_5\dot{e}_5}{k_2} \tag{3.12}$$

Substituindo (3.8) em (3.12), obtém-se:

$$\begin{aligned}
\dot{V} = & e_1[r(e_2 - e_1) + e_4 + h_1(t) + u_1] \\
& + e_2[-(1 + m)e_2 + e_1e_3 + x_me_3 + z_me_1 - e_5 + h_2(t)] \\
& + \frac{e_3}{g(1 + m)}g[m(e_1^2 + 2e_1x_m) - (1 + m)(e_1e_2 + e_1y_m + e_2x_m) + h_3(t) + u_3] \quad (3.13) \\
& + e_4[2(1 + m)e_4 + e_1e_3 + x_me_3 + e_1(z_m - k_1) + h_4(t) + u_4] + \\
& + \frac{e_5}{k_2}(-me_5 + k_2e_2 + h_5(t))
\end{aligned}$$

Reagrupando os termos de (3.13) e substituindo os sinais de controle definidos em (3.10), temos:

$$\begin{aligned}
\dot{V} = & -e_1^2(\psi_1 + r) - e_2^2(1 + m) - e_3^2\left(\frac{\psi_3}{g(1 + m)}\right) - e_4^2[\psi_5 - 2(1 + m)] - e_5^2\left(\frac{m}{k_2}\right) \\
& + e_1h_1 + e_2h_2 + \frac{e_3h_3}{g(1 + m)} + e_4h_4 + \frac{e_5h_5}{k_2} + e_1e_2(r + z_m) + e_1e_3e_4 \quad (3.14) \\
& + e_1^2e_3\left(\frac{m}{1 + m}\right) + e_1e_4(1 + z_m - k_1) + e_1e_3\left(\frac{2mx_m}{1 + m} - y_m\right) + e_3e_4(x_1m) + \\
& - e_1^4(\psi_2) - e_3^4(\psi_4)
\end{aligned}$$

A partir das desigualdades de Young (HARDY et al., 1952), da **Hipótese 1** e do **Fato 1** é possível definir as seguintes relações:

$$\begin{aligned}
e_1 h_1 &\leq \frac{1}{2}(e_1^2 \sigma_1 + \sigma_1^{-1} \bar{h}_1^2); \\
e_2 h_2 &\leq \frac{1}{2}(e_2^2 \sigma_2 + \sigma_2^{-1} \bar{h}_2^2); \\
\frac{e_3 h_3}{g(1+m)} &\leq \frac{1}{2}\left(\frac{e_3^2 \sigma_3}{g^2(1+m)^2} + \sigma_3^{-1} \bar{h}_3^2\right); \\
e_4 h_4 &\leq \frac{1}{2}(e_4^2 \sigma_4 + \sigma_4^{-1} \bar{h}_4^2); \\
\frac{e_5 h_5}{k_2} &\leq \frac{1}{2}\left(e_5^2 \sigma_5 + \frac{\sigma_5^{-1} \bar{h}_5^2}{k_2^2}\right); \\
e_1 e_2 (r + z_m) &\leq \frac{1}{2}[\sigma_6 (r + \bar{Z})^2 e_1^2 + \sigma_6^{-1} e_2^2]; \\
e_1 e_3 e_4 &\leq \frac{1}{2}(e_1^2 e_3^2 \sigma_7 + \sigma_7^{-1} e_4^2) \leq \frac{e_4^2}{2\sigma_7} + \frac{e_1^4 \sigma_7^2}{8} + \frac{e_3^4 \sigma_7^2}{8}; \\
e_1^2 e_3 \left(\frac{m}{1+m}\right) &\leq \frac{1}{2}\left(e_1^4 \sigma_8 + \sigma_8^{-1} \frac{m^2}{(1+m)^2} e_3^2\right); \\
e_1 e_4 (1 + z_m - k_1) &\leq \frac{1}{2}[(1 + \bar{Z} + k_1)^2 e_1^2 \sigma_9 + \sigma_9^{-1} e_4^2]; \\
e_1 e_3 \left(\frac{2m x_m}{1+m} - y_m\right) &\leq \frac{1}{2}\left(\frac{2m \bar{X}}{1+m} + \bar{Y}\right)(e_1^2 + e_3^2); \\
e_3 e_4 (x_m) &\leq \frac{1}{2}(\bar{X}^2 e_3^2 \sigma_{10} + \sigma_{10}^{-1} e_4^2)
\end{aligned} \tag{3.15}$$

em que, $\sigma_{1\dots 10}$ são constantes arbitrárias e virtuais, ou seja, não fazem parte do sinal de controle e só são utilizadas para generalizar a prova matemática.

Com as relações definidas em (3.15) reescreve-se (3.14) da seguinte maneira:

$$\begin{aligned}
\dot{V} &\leq -e_1^2(\psi_1 + r) - e_2^2(1 + m) - e_3^2\left(\frac{\psi_3}{g(1+m)}\right) - e_4^2[\psi_5 - 2(1 + m)] - e_5^2\left(\frac{m}{k_2}\right) \\
&+ \frac{1}{2}(e_1^2 \sigma_1 + \sigma_1^{-1} \bar{h}_1^2) + \frac{1}{2}(e_2^2 \sigma_2 + \sigma_2^{-1} \bar{h}_2^2) + \frac{1}{2}\left(\frac{e_3^2 \sigma_3}{g^2(1+m)^2} + \sigma_3^{-1} \bar{h}_3^2\right) + \frac{1}{2}(e_4^2 \sigma_4 + \sigma_4^{-1} \bar{h}_4^2) \\
&+ \frac{1}{2}\left(e_5^2 \sigma_5 + \frac{\sigma_5^{-1} \bar{h}_5^2}{k_2^2}\right) + \frac{1}{2}[\sigma_6 (r + \bar{Z})^2 e_1^2 + \sigma_6^{-1} e_2^2] + \frac{e_4^2}{2\sigma_7} + \frac{e_1^4 \sigma_7^2}{8} + \frac{e_3^4 \sigma_7^2}{8} \\
&+ \frac{1}{2}\left(e_1^4 \sigma_8 + \sigma_8^{-1} \frac{m^2}{(1+m)^2} e_3^2\right) + \frac{1}{2}[(1 + \bar{Z} + k_1)^2 e_1^2 \sigma_9 + \sigma_9^{-1} e_4^2] + \frac{1}{2}\left(\frac{2m \bar{X}}{1+m} + \bar{Y}\right)(e_1^2 + e_3^2) \\
&+ \frac{1}{2}(\bar{X}^2 e_3^2 \sigma_{10} + \sigma_{10}^{-1} e_4^2)
\end{aligned} \tag{3.16}$$

Reagrupa-se os termos de (3.16) para encontrar:

$$\dot{V} \leq -\rho_1 e_1^2 - \rho_2 e_2^2 - \rho_3 e_3^2 - \rho_4 e_4^2 - \rho_5 e_5^2 - \rho_6 e_1^4 - \rho_7 e_3^4 + \beta \tag{3.17}$$

em que,

$$\begin{aligned}
\rho_1 &= \psi_1 + r - \frac{1}{2}[\sigma_1 + \sigma_6(r + \bar{Z})^2 + \sigma_9(1 + \bar{Z} + k_1)^2 + \frac{2m\bar{X}}{1+m} + \bar{Y}] \\
\rho_2 &= 1 + m - \frac{1}{2}(\sigma_2 + \sigma_6^{-1}) \\
\rho_3 &= \frac{\psi_3}{g(1+m)} - \frac{1}{2}[\frac{\sigma_3}{g^2(1+m)^2} + \sigma_8^{-1}\frac{m^2}{(1+m)^2} + \frac{2m\bar{X}}{1+m} + \bar{Y} + \sigma_{10}\bar{X}^2] \\
\rho_4 &= \psi_5 - 2(1+m) - \frac{1}{2}(\sigma_4 + \sigma_7^{-1} + \sigma_9^{-1} + \sigma_{10}^{-1}) \\
\rho_5 &= \frac{m}{k_2} - \frac{1}{2}\sigma_5 \\
\rho_6 &= \psi_2 - \frac{1}{2}(\sigma_8 + \frac{\sigma_7^2}{4}) \\
\rho_7 &= \psi_4 - \frac{\sigma_7^2}{4} \\
\beta_1 &= \frac{1}{2}(\bar{h}_1\sigma_1^{-1} + \bar{h}_3\sigma_3^{-1} + \bar{h}_4\sigma_4^{-1}) \\
\beta_2 &= \frac{1}{2}(\bar{h}_2\sigma_2^{-1} + \bar{h}_5\sigma_5^{-1}k_2^{-2}) \\
\beta &= \beta_1 + \beta_2
\end{aligned} \tag{3.18}$$

Ajustando-se os ganhos dos sinais de controle $\psi_{1...5}$ e as constantes virtuais $\sigma_{1...10}$ é possível que se faça $\rho_{1...7} > 0$. Assim, definindo-se $\rho = \min(\rho_1, \rho_2, \rho_3, \rho_4, \rho_5, \rho_6, \rho_7)$ reescreve-se (3.17) da seguinte forma:

$$\dot{V} \leq -\rho\|e\|^2 + \beta \tag{3.19}$$

Analisando o caso $\dot{V} \leq 0$:

$$\|e\| \geq \sqrt{\frac{\beta}{\rho}} := \theta \tag{3.20}$$

Logo, quando $\|e\| > \sqrt{\frac{\beta}{\rho}}$ tem-se $\dot{V} \leq 0$ o que implica em erro uniformemente finalmente limitado que converge para o conjunto compacto $\Omega = \{e \in \mathbb{R}^5 \mid \|e\| \leq \theta\}$. Isso ocorre pois, se $\|e\|$ sair do conjunto compacto Ω , \dot{V} será menor que zero fazendo com que a norma do erro de sincronização diminua até voltar ao conjunto residual Ω .

Comentário 1: Vale ressaltar que a sugestão para os sinais em (3.10) foi feita com base na inspeção da derivada da candidata de Lyapunov (3.16). Também é relevante o fato de que a ação de controle é subatuada, já que possui apenas três dimensões.

Comentário 2: Para poder analisar o caso em que $\dot{V} \leq 0$ deseja-se $\rho_{1...7} > 0$ e para isso é necessário introduzir diferentes ganhos, provenientes dos sinais de controle, em $\rho_1, \rho_3, \rho_4, \rho_6$

e ρ_7 , que são os que apresentam constantes negativas a serem majoradas. No caso de ρ_2 e ρ_5 é possível fixar σ_2, σ_5 e σ_6 de modo a mantê-los positivos, já que as constantes que aparecem são positivas.

Comentário 3: O conjunto Ω pode ser ajustado a partir de β , para que o erro de sincronização máximo seja reduzido. Vale ressaltar que os únicos termos em β que podem ser ajustados são as constantes virtuais σ do termo β_1 , já que essas podem ser arbitradas livremente sem que qualquer ρ assumam valores negativos (aumentando-se os ganhos ψ pode-se majorar a influência dessas constantes virtuais de β_1 no valor de $\rho_{1...7}$)

Comentário 4: Os distúrbios limitados nos estados atuados podem ser arbitrariamente reduzidos a partir do aumento dos ganhos do controlador, já que isso permite uma escolha de valores mais elevados para σ_1, σ_3 e σ_4 . O mesmo não é válido para os distúrbios nos estados subatuados, como de costume na literatura.

Comentário 5: Para modificar o tempo de convergência pode-se utilizar a técnica de escalonamento da frequência e para dimensionar os componentes de uma possível implementação dos circuitos caóticos e do controlador pode-se utilizar escalonamento da amplitude.

3.3 Aplicação em telecomunicação segura

O método utilizado neste trabalho para implementar um esquema de comunicação seguro baseado em caos é denominado mascaramento caótico e foi definido em 2.4.1.

Primeiro, adiciona-se a mensagem a um dos estados do sistema mestre fazendo com que a mensagem original se misture ao comportamento caótico do sistema. Em seguida, pode-se transmitir a mensagem criptografada por um canal qualquer, já que o hipercaos do sistema transmissor garante que a mensagem original esteja mascarada. A mensagem criptografada chega ao receptor acrescida de ruídos e perturbações inerentes ao canal de comunicação e por isso, considera-se esses distúrbios na análise. Por fim, utiliza-se o sinal de controle definido em (3.10) para atingir a sincronização entre transmissor e receptor e assim recuperar a mensagem original. A figura 2.1 ilustra o esquema composto por transmissor receptor e sincronizador.

Comentário 5: A chave da criptografia em esquemas como o aqui proposto pode ser vista como a composição dos seguintes fatores: Lei de controle e topologia do sistema caótico.

Capítulo 4

Simulação *Matlab/Simulink*

O seguinte capítulo é dedicado à simulação computacional do esquema de comunicação seguro baseado em caos proposto neste trabalho. Com o objetivo de analisar o desempenho do sincronizador projetado, simula-se a partir de *scripts Matlab* e diagramas *Simulink* o processo de transmitir, criptografar e recuperar mensagens analógicas mesmo na presença de distúrbios limitados. Os sinais gerados na simulação permitem a construção de diversos gráficos que são utilizados para analisar o erro de sincronização, as mensagens criptografadas e as mensagens recuperadas. Os arquivos com *scripts* e diagramas de simulação encontram-se no apêndice A.

As simulações foram realizadas na versão R2018a (9.4.0.813654) 64-bit (win64) do *software Matlab/Simulink* em um computador Samsung com CPU Intel Core i7-5500U, GPU NVIDIA Geforce 920M e sistema operacional Windows 10 Home. Devido à sensibilidade dos sistemas hipercaóticos, para reproduzir as simulações aqui apresentadas da melhor maneira possível é necessário reproduzir também as condições do ambiente de simulação.

4.1 Ambiente de simulação

Para simular o funcionamento do esquema de comunicação construiu-se o diagrama *Sync.mdl* no *Simulink* que contém blocos definidos por *scripts Matlab* denominados *PlantaMaster.m*, *PlantaSlave.m* e *Sinc.m*. O diagrama *Sync.mdl* consiste basicamente de uma realimentação dos estados do sistema escravo para que se possa definir os sinais dos erros de sincronização utilizados pelo sincronizador na ação de controle. Utilizou-se o método *ode113* com passo variável e tolerância de 10^{-8} para executar uma simulação com duração de vinte segundos.

O *script PlantaMaster.m* define a dinâmica do sistema transmissor e suas condições iniciais, assim como os sinais que representam as mensagens a serem transmitidas. O *script PlantaSlave.m* representa a dinâmica do sistema receptor e suas condições iniciais em conjunto com distúrbios limitados inerentes ao canal de comunicação. Já no *script Sinc.m* define-se o controlador responsável por sincronizar os sistemas transmissor e receptor, ou seja, implementa-se a

lei de controle definida em (3.10).

Para representar os distúrbios limitados utiliza-se sinais com alta densidade espectral de potência, ou seja, com componentes espectrais em várias faixas de frequência de modo a se aproximar de um sinal ruidoso. Neste trabalho utilizou-se os seguintes sinais para representar os distúrbios na simulação:

$$\begin{aligned}
h_1 &= 0.02(0.15\sin(2\pi 5t) + 0.05\cos(2\pi 12t) + 0.1(2\pi 3t) + 0.05\cos(2\pi 20t) - \\
&\quad 0.05\text{sawtooth}(2\pi 7t) + 0.22(2\pi 4t) - 0.2\cos(2\pi 9t) - 0.1\cos(2\pi 37t) + \\
&\quad 0.1\sin(2\pi 60t + \pi/17)) \\
h_2 &= 0.015(0.15\sin(2\pi 17t) + 0.15\cos(2\pi 6t) + 0.1\text{square}(2\pi 2t) + 0.15\cos(2\pi 23t) - \\
&\quad 0.05\text{sawtooth}(2\pi 9t) + 0.1\sin(2\pi 40t) - 0.1\cos(2\pi 50t) - 0.1\cos(2\pi 2t) + \\
&\quad 0.1\sin(2\pi 9t + \pi/17)) \\
h_3 &= 0.08(0.15\text{sawtooth}(2\pi 6t) + 0.15\sin(2\pi 25t) - 0.15\text{sawtooth}(2\pi 14t) - \\
&\quad 0.15\text{square}(2\pi 3t) + 0.05\cos(2\pi 2t) + 0.05\sin(2\pi 42t) + \\
&\quad 0.2\cos(2\pi 7t + \pi) + 0.1\sin(2\pi 13t)) \\
h_4 &= 0.03(0.1\sin(2\pi 17t) + 0.1\cos(2\pi 6t) + 0.13\text{square}(2\pi 2t) + \\
&\quad 0.15\cos(2\pi 23t) - 0.05\text{sawtooth}(2\pi 9t) + 0.1\sin(2\pi 40t) - \\
&\quad 0.1\cos(2\pi 50t) - 0.1\cos(2\pi 2t) + 0.1\sin(2\pi 9t + \pi/17)) \\
h_5 &= 0.04(0.08\text{sawtooth}(2\pi 8t) + 0.13\sin(2\pi 25t) - 0.11\text{sawtooth}(2\pi 14t) - \\
&\quad 0.13\text{square}(2\pi 3t) + 0.05\cos(2\pi 2t) + 0.05\sin(2\pi 40t) + \\
&\quad 0.2\cos(2\pi 7t + \pi) + 0.1\sin(2\pi 13t))
\end{aligned} \tag{4.1}$$

em que as funções *sawtooth*, *square*, *sin* e *cos* representam respectivamente ondas dente de serra, quadrada, seno e cosseno implementadas pelo *Matlab* e que possuem argumentos que definem amplitude e frequência.

4.2 Parâmetros da simulação

Os parâmetros mais importantes da simulação são os ganhos da lei de controle $\psi_{1...5}$ que podem ser ajustados no *script Sinc.m* para alcançar melhor desempenho de sincronização. Define-se $\psi_1 = \psi_2 = \psi_5 = 200$, $\psi_3 = 1000$ e $\psi_4 = 500$ a partir de métodos heurísticos, já que basta que $\psi_{1...5}$ seja grande o suficiente para majorar os termos negativos presentes em $\rho_{1...7}$ para alcançar sincronização entre mestre e escravo.

Para representar de maneira verossímil a situação de uso do esquema de comunicação definiu-se condições iniciais distintas para sistema transmissor e receptor. Em um cenário real as condições iniciais são definidas por tensões em capacitores e pela intensidade dos campos

magnéticos em indutores de uma possível implementação em eletrônica analógica no momento em que o sistema começa a evoluir, e por isso, não se pode garantir condições iniciais congruentes entre mestre e escravo. A seguir temos as condições iniciais para transmissor e receptor:

Transmissor:

$$\begin{aligned}x_m(0) &= 10.05 \\y_m(0) &= -13.5 \\z_m(0) &= -11.3 \\w_m(0) &= 10.2 \\v_m(0) &= 11.9\end{aligned}\tag{4.2}$$

Receptor:

$$\begin{aligned}x_s(0) &= -0.09 \\y_s(0) &= 0.8 \\z_s(0) &= 0.3 \\w_s(0) &= -1.5 \\v_s(0) &= -0.4\end{aligned}\tag{4.3}$$

4.3 Resultados da simulação

Nas subseções a seguir apresenta-se gráficos construídos pelos *scripts Matlab Graficos.m* e *GraficosMsg.m* que podem ser encontrados também no apêndice A e que representam os sinais mais importantes para a análise do desempenho do sincronizador projetado.

4.3.1 Sincronização dos estados do sistema escravo

As figuras a seguir, geradas pelo *script Graficos.m* demonstram a sincronização entre cada um dos estados do sistema escravo com os correspondentes estados do sistema mestre:

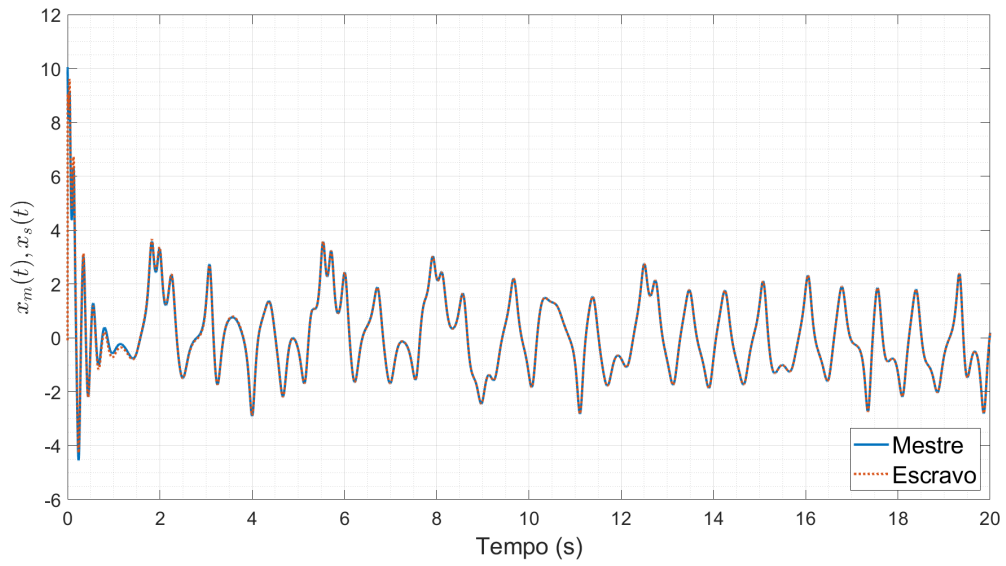


Figura 4.1: Desempenho da sincronização dos estados $x_s(t)$ e $x_m(t)$.

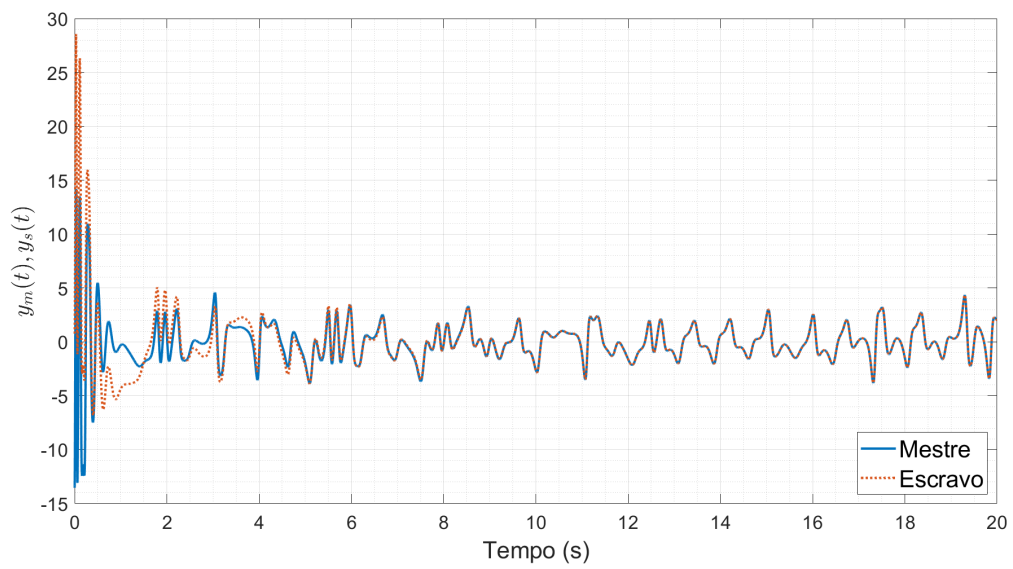


Figura 4.2: Desempenho da sincronização dos estados $y_s(t)$ e $y_m(t)$.

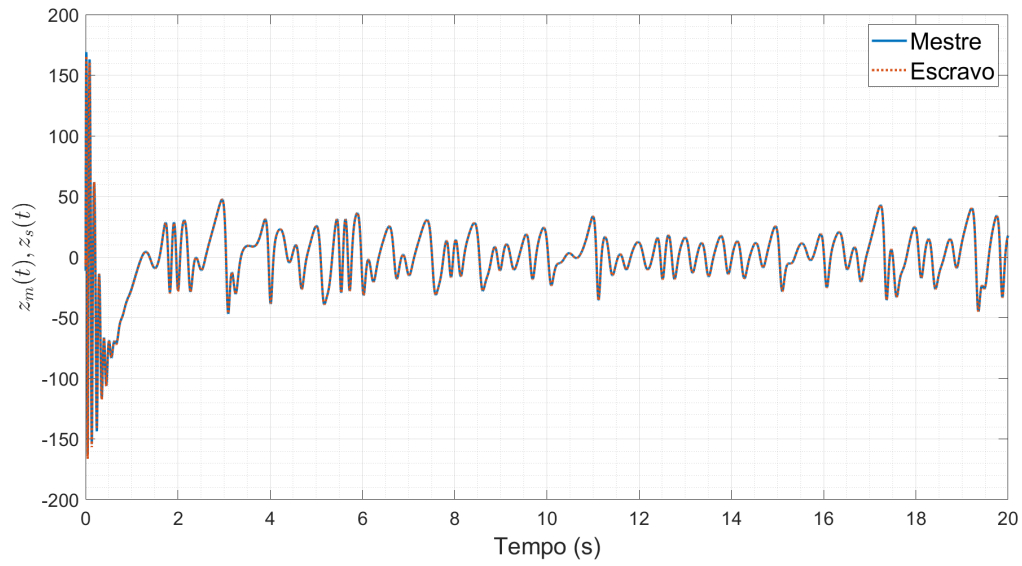


Figura 4.3: Desempenho da sincronização dos estados $z_s(t)$ e $z_m(t)$.

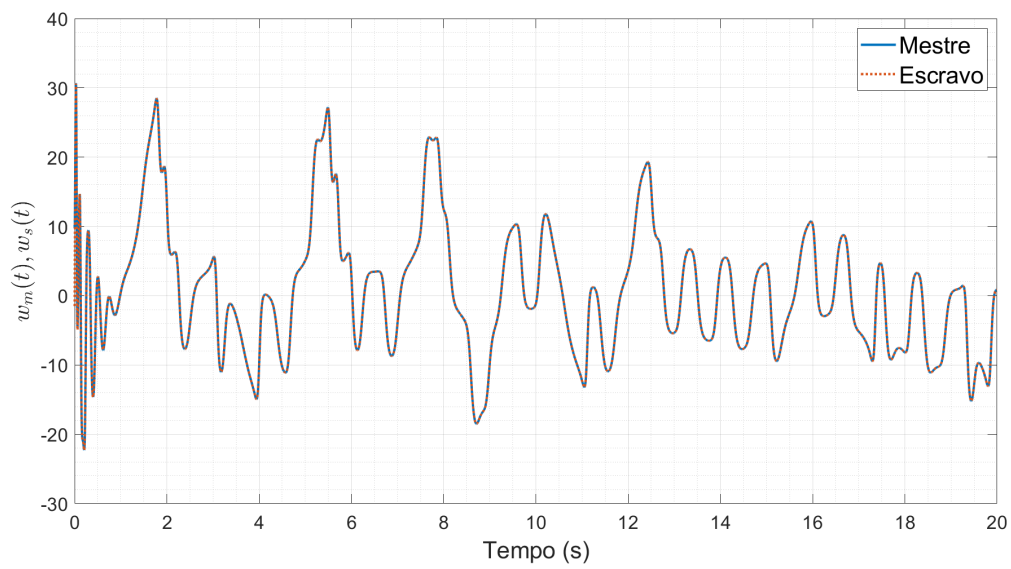


Figura 4.4: Desempenho da sincronização dos estados $w_s(t)$ e $w_m(t)$.

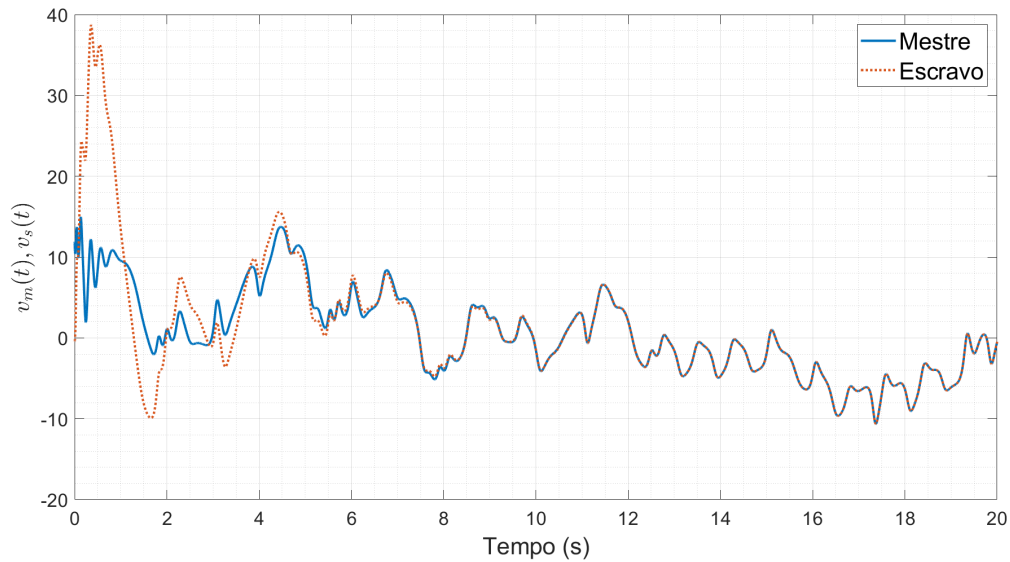


Figura 4.5: Desempenho da sincronização dos estados $v_s(t)$ e $v_m(t)$.

Pela análise dos gráficos percebe-se que a sincronização entre transmissor e receptor ocorre em tempo finito. As condições iniciais distintas fazem com que exista um transiente no começo da simulação em que os estados ainda não estão completamente sincronizados.

Analisando a diferença entre os sinais dos estados do sistema escravo e dos estados do sistema mestre é possível construir os gráficos que representam o erro de sincronização para cada estado:

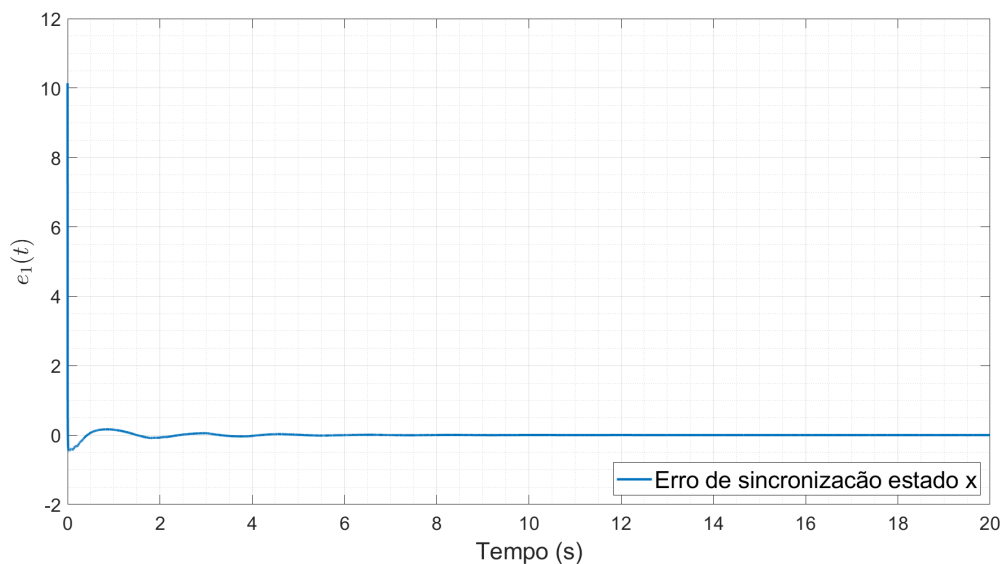


Figura 4.6: Erro de sincronização $e_1(t)$.

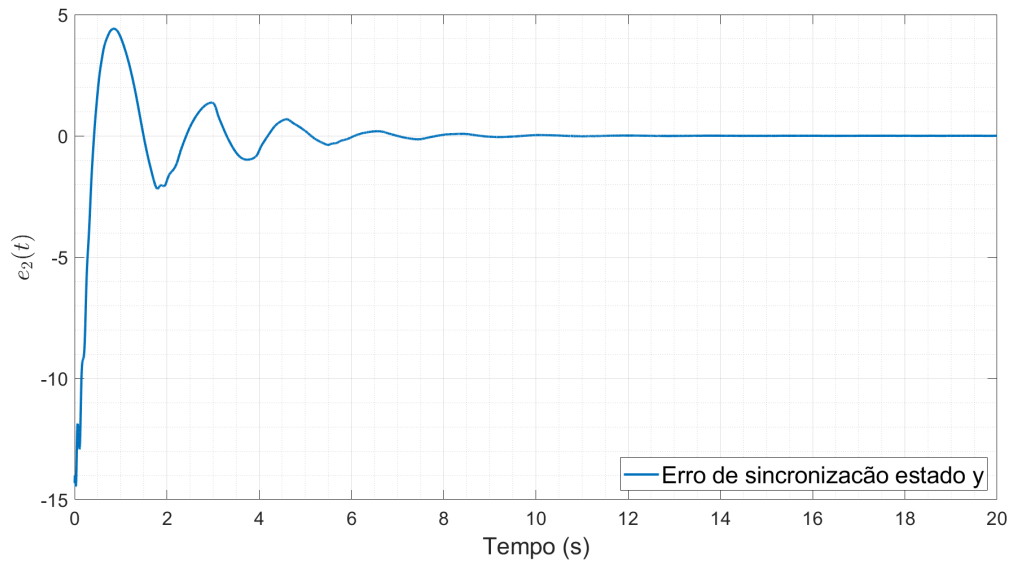


Figura 4.7: Erro de sincronização $e_2(t)$.

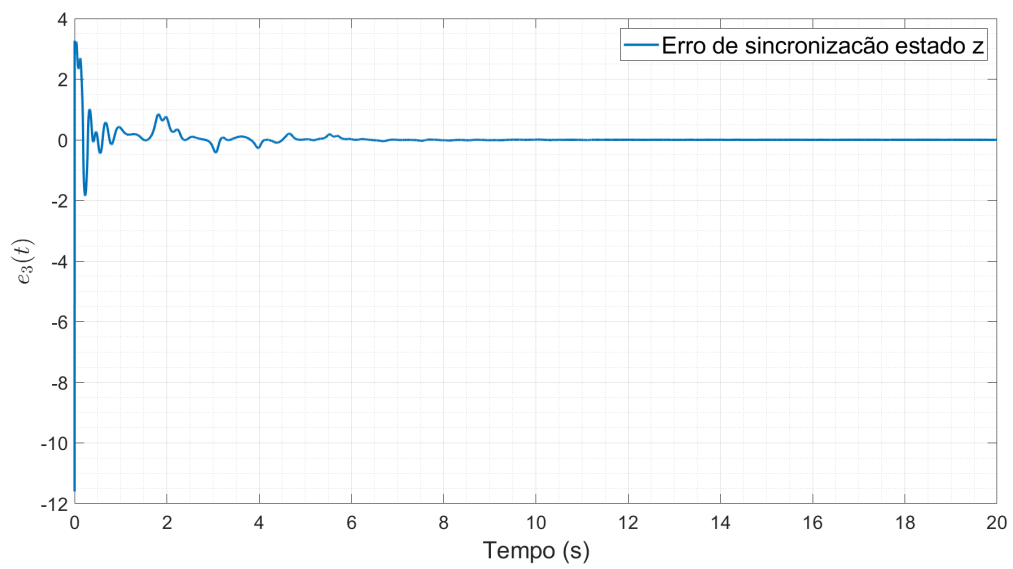


Figura 4.8: Erro de sincronização $e_3(t)$.

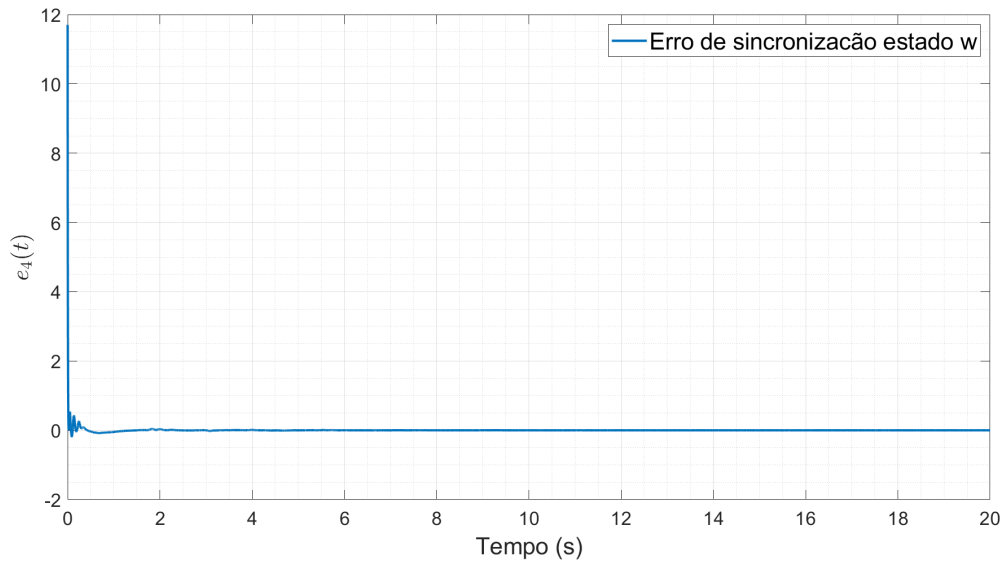


Figura 4.9: Erro de sincronização $e_4(t)$.

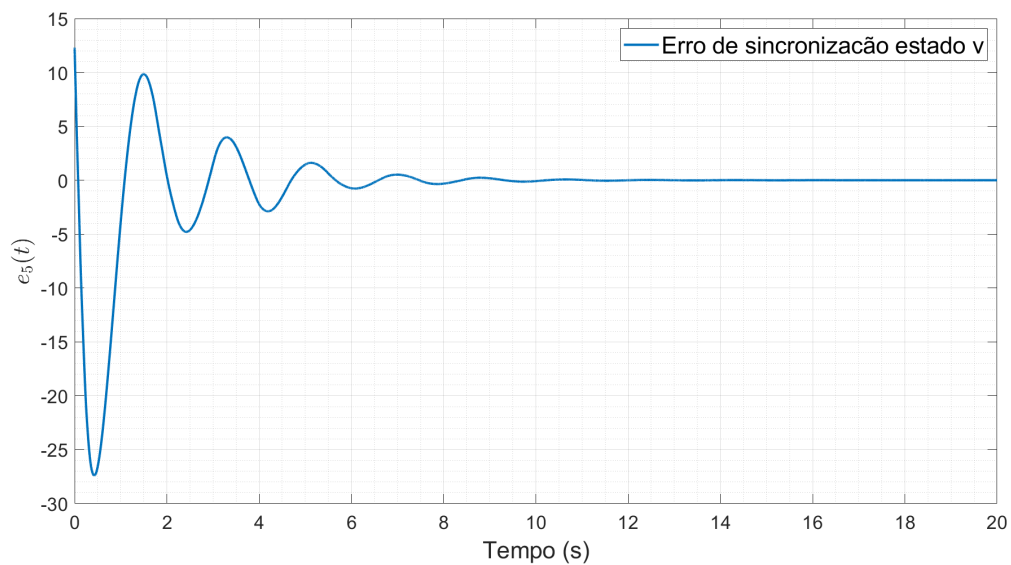


Figura 4.10: Erro de sincronização $e_5(t)$.

Pelo gráfico dos erros de sincronização pode-se afirmar que o esquema apresenta alto desempenho, já que, os referidos erros convergem para zero rapidamente para todos os estados. Isso se deve à escolha de valores elevados para os ganhos ψ do sinal de controle, como o previsto teoricamente. Vale ressaltar que o desempenho de sincronização é alto até para os estados y e v que não possuem sinal de controle.

4.3.2 Mensagens originais e criptografadas

As mensagens utilizadas para validar o esquema de comunicação em ambiente de simulação foram definidas como sinais no *PlantaMaster.m* da seguinte forma:

$$\begin{aligned} m_1 &= (0.24\sin(2\pi 0.6t) + 0.38\cos(2\pi 2t)) \\ m_2 &= (0.5\sin(2\pi 1.5t + \pi/4) + 0.26\cos(2\pi 0.6t) + 0.3\text{square}(2\pi 0.75t)) \end{aligned} \quad (4.4)$$

A mensagem denominada m_1 é adicionada ao segundo estado do sistema transmissor e a mensagem denominada m_2 ao quinto estado, de modo a serem criptografadas pelo comportamento caótico do sistema mestre e possam ser transmitidas por um canal qualquer. Para recuperar a mensagem original a partir do sinal que está sendo transmitido, basta que o sistema receptor esteja sincronizado com o sistema transmissor, já que nessas condições a mensagem original é dada pela diferença entre os sinais dos dois sistemas como na equação (2.12). Com o *script GraficosMsg.m* construiu-se gráficos que ilustram as mensagens originais em contraste com as mensagens criptografadas :

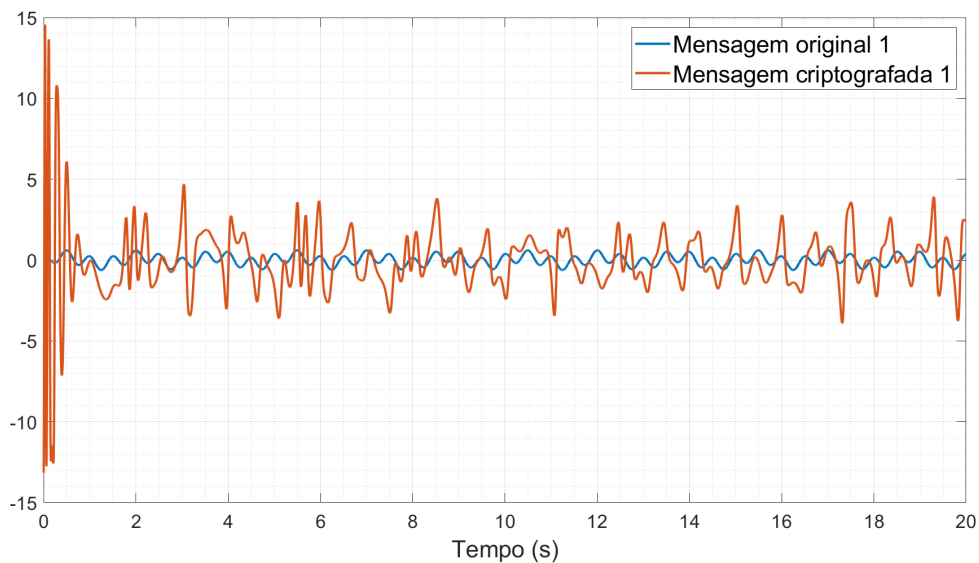


Figura 4.11: Sinal mensagem $m_1(t)$ em contraste com o sinal transmitido.

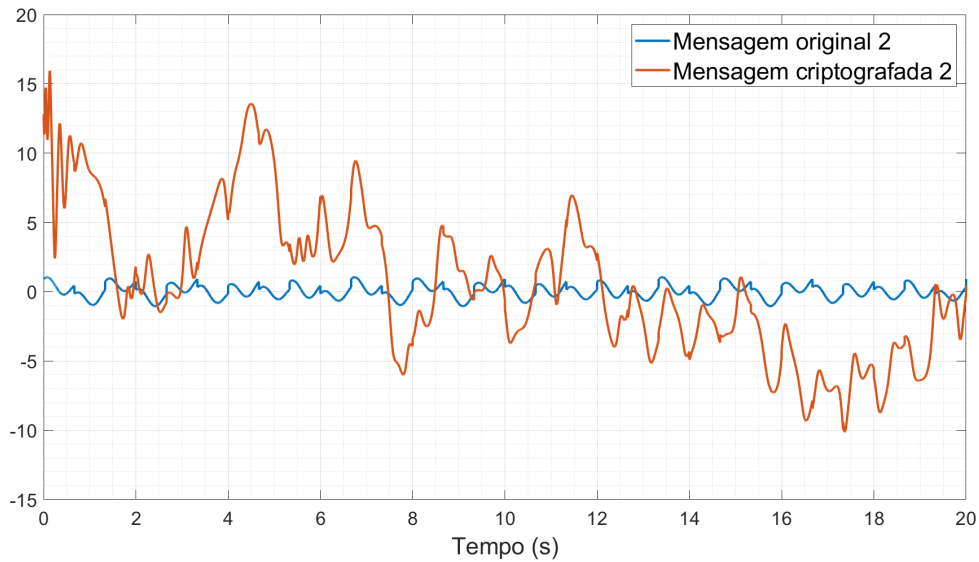


Figura 4.12: Sinal mensagem $m_2(t)$ em contraste com o sinal transmitido.

Ao comparar os sinais das mensagens originais e das mensagens transmitidas, percebe-se que o mascaramento caótico é capaz de camuflar a informação sigilosa contida na mensagem original consistentemente. Para recuperar a mensagem original é necessário conhecer a topologia dos sistemas caóticos envolvidos e o sinal de controle utilizado para a sincronização e por isso, pode-se considerar a mensagem criptografada.

4.3.3 Erro de recuperação das mensagens

De maneira análoga ao erro de sincronização, define-se o erro de recuperação da mensagem como a diferença entre mensagem original e mensagem recuperada. Os seguintes gráficos ilustram o erro de recuperação das mensagens transmitidas:

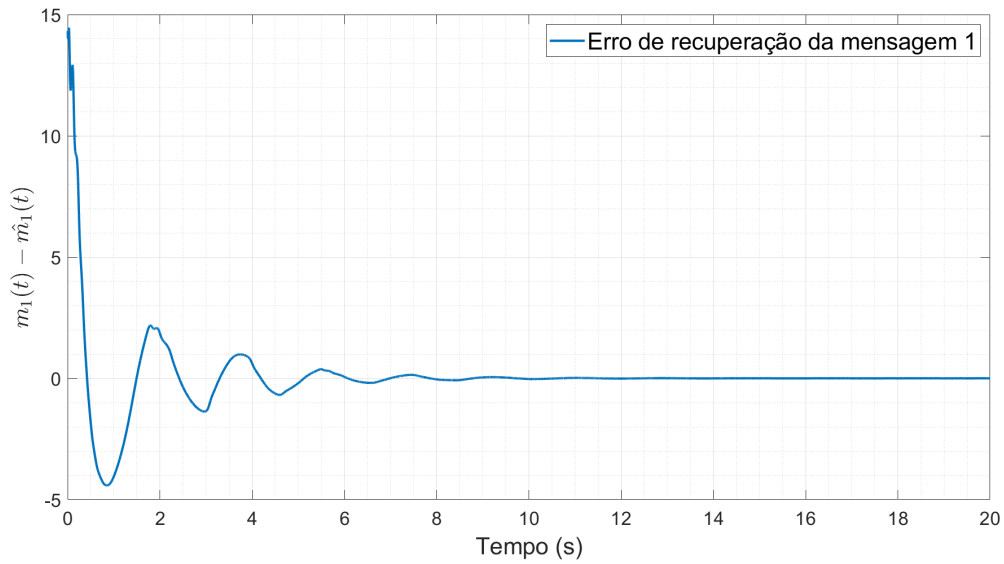


Figura 4.13: Erro de recuperação da mensagem 1.

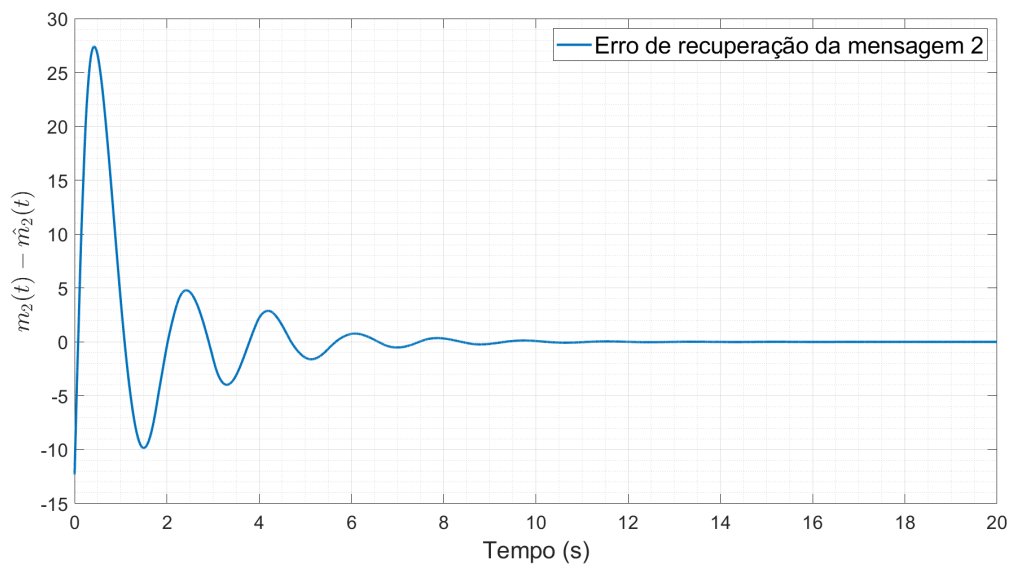


Figura 4.14: Erro de recuperação da mensagem 2.

Afim de comparar as mensagens recuperadas com as mensagens originais construiu-se os seguintes gráficos:

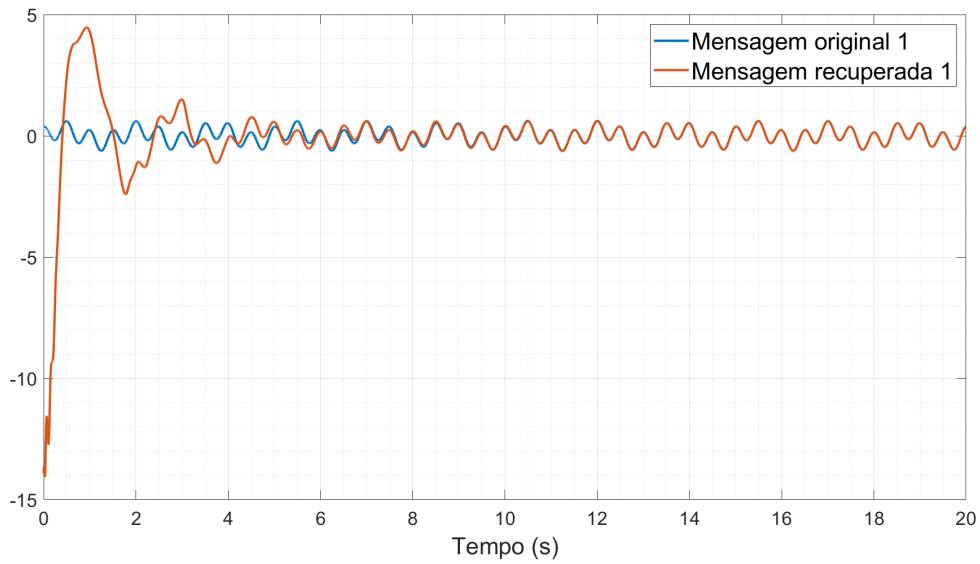


Figura 4.15: Mensagem 1 recuperada em contraste com a mensagem original.

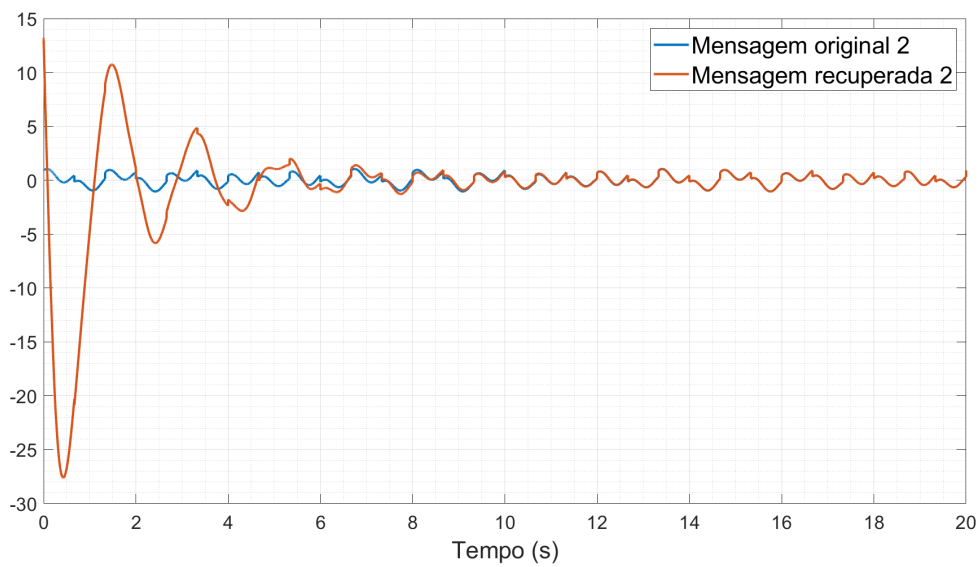


Figura 4.16: Mensagem 2 recuperada em contraste com a mensagem original.

Percebe-se pelos gráficos que a mensagem recuperada converge rapidamente para a mensagem original, o que demonstra a viabilidade do esquema de comunicação segura. Os segundos iniciais apresentam erro de recuperação da mensagem não nulo causado pelo transiente da sincronização entre transmissor e receptor.

4.4 Comparação entre sincronizadores

Para colocar em perspectiva o desempenho do sincronizador aqui proposto e para pontuar as contribuições apresentadas por este trabalho, simulou-se no mesmo ambiente descrito na seção anterior o comportamento de um outro esquema de sincronização presente na literatura (MAHMOUD; ABUALNAJA, 2021). A comparação entre as simulações é válida já que o autor de (MAHMOUD; ABUALNAJA, 2021) se baseou nos mesmos sistemas hipercaóticos pentadimensionais para projetar o sincronizador. Nas subseções a seguir apresenta-se o sincronizador proposto em (MAHMOUD; ABUALNAJA, 2021) e os gráficos que representam os sinais de interesse para a comparação de desempenho.

4.4.1 Controle completamente atuado

Em (MAHMOUD; ABUALNAJA, 2021), utiliza-se uma lei de controle completamente atuada, ou seja, uma ação de controle com dimensão igual à dos sistemas mestre e escravo:

$$\begin{aligned}u_1 &= 1(-r(e_2 - e_1)) - e_4 - ke_1 \\u_2 &= (1 + m)e_2 - x_s z_s + x_m z_m + e_5 - ke_2 \\u_3 &= -g(m(x_s^2 - x_m^2) - (1 + m)(x_s y_s - x_m y_m)) - ke_3 \\u_4 &= -2(1 + m)e_4 - x_s z_s + x_m z_m + k_1 e_2 - ke_4 \\u_5 &= me_5 - k_2 e_2 - ke_5\end{aligned}\tag{4.5}$$

em que, as constantes r, m, g, k_1, k_2 são as mesmas que definem os sistemas hipercaóticos mestre e escravo (como nas equações (3.2) e (3.3)) e $k = 2, 5$ é um parâmetro definido em (MAHMOUD; ABUALNAJA, 2021).

Note que todos os estados do sistema escravo apresentam atuação pela lei de controle em (4.5) e por isso o esquema é dito completamente atuado.

4.4.2 Sincronização pela lei de controle completamente atuada

Aproveitou-se o ambiente de simulação definido anteriormente para simular a sincronização pela lei de controle definida em (4.5). Isso significa que foram utilizadas as mesmas condições iniciais para sistemas mestre e escravo e as mesmas perturbações definidas para a simulação do esquema subatuado. Como o esperado, a única alteração feita nos scripts apresentados no apêndice A para simular a lei de controle completamente atuada diz respeito à própria lei de controle. As figuras a seguir foram construídas também com os *scripts* utilizados na seção anterior:

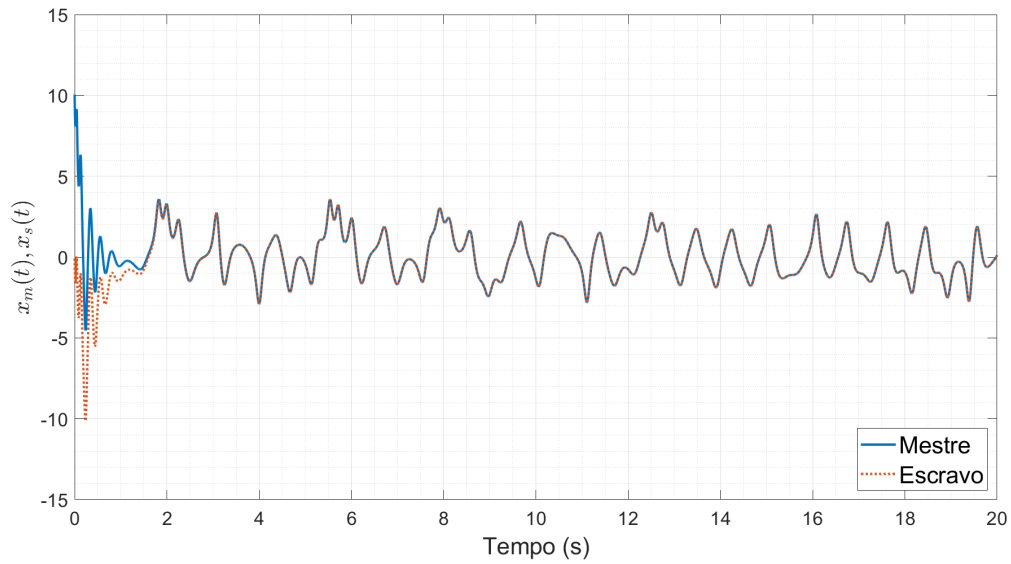


Figura 4.17: Desempenho da sincronização dos estados $x_s(t)$ e $x_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).

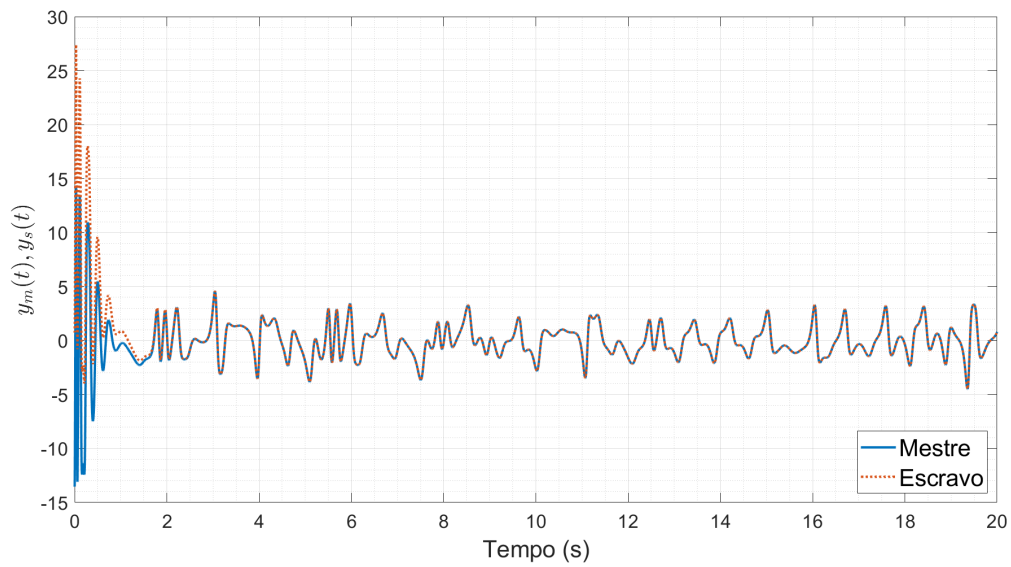


Figura 4.18: Desempenho da sincronização dos estados $y_s(t)$ e $y_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).

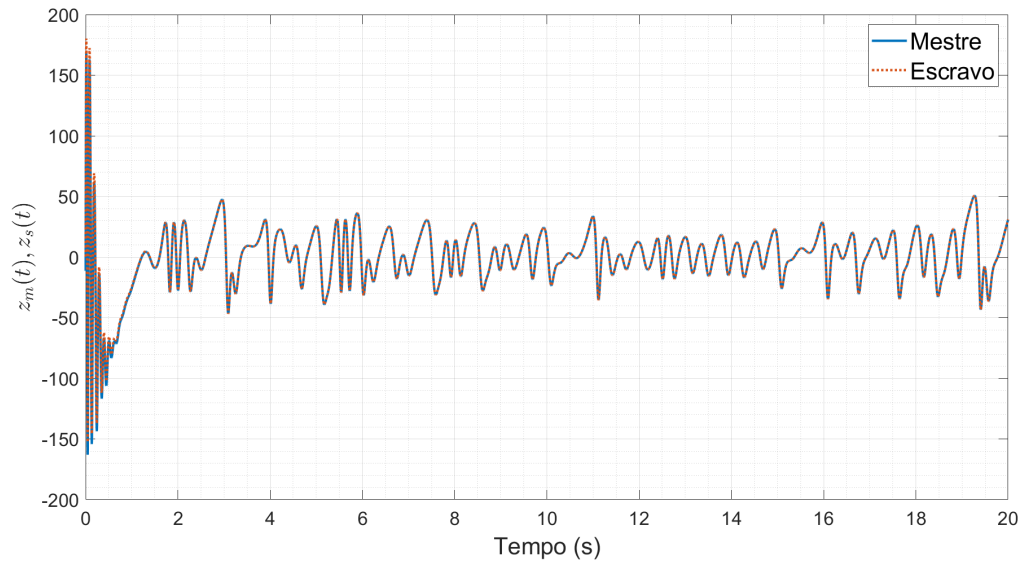


Figura 4.19: Desempenho da sincronização dos estados $z_s(t)$ e $z_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).

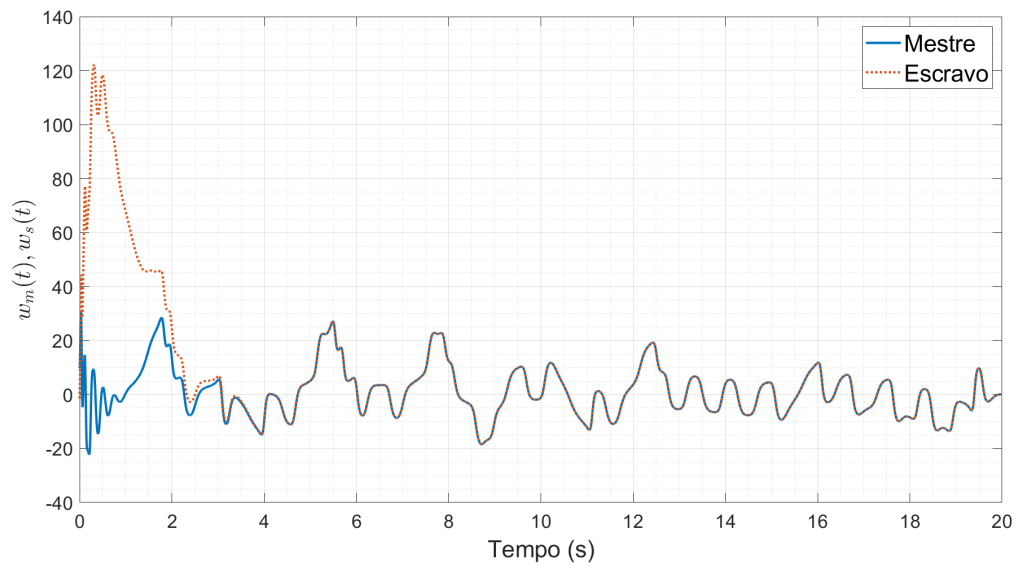


Figura 4.20: Desempenho da sincronização dos estados $w_s(t)$ e $w_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).

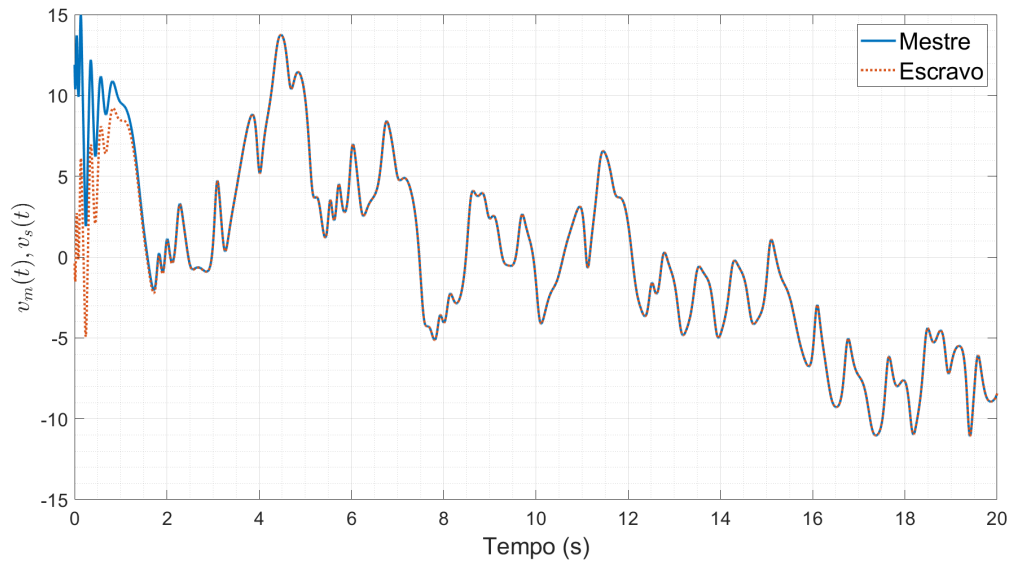


Figura 4.21: Desempenho da sincronização dos estados $v_s(t)$ e $v_m(t)$ em (MAHMOUD; ABUALNAJA, 2021).

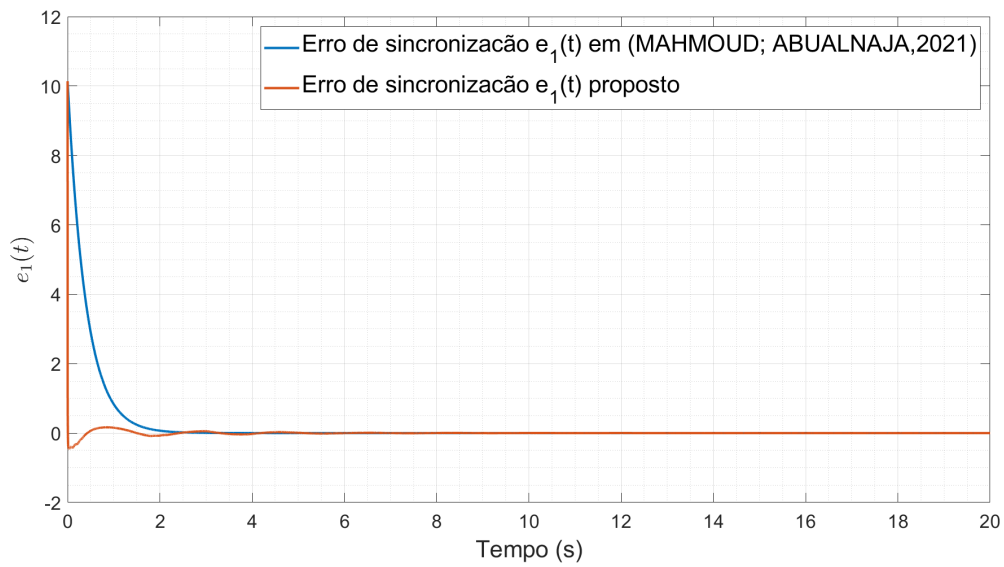


Figura 4.22: Erro de sincronização $e_1(t)$ com lei de controle completamente atuada em contraste com erro de sincronização para o mesmo estado com lei de controle subatuada.

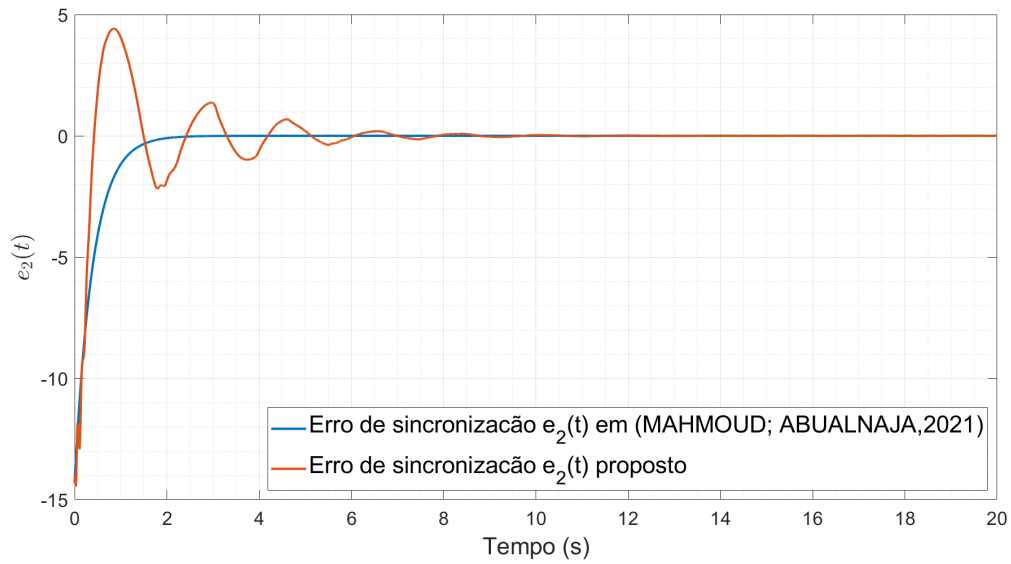


Figura 4.23: Erro de sincronização $e_2(t)$ com lei de controle completamente atuada em contraste com erro de sincronização para o mesmo estado com lei de controle subatuada..

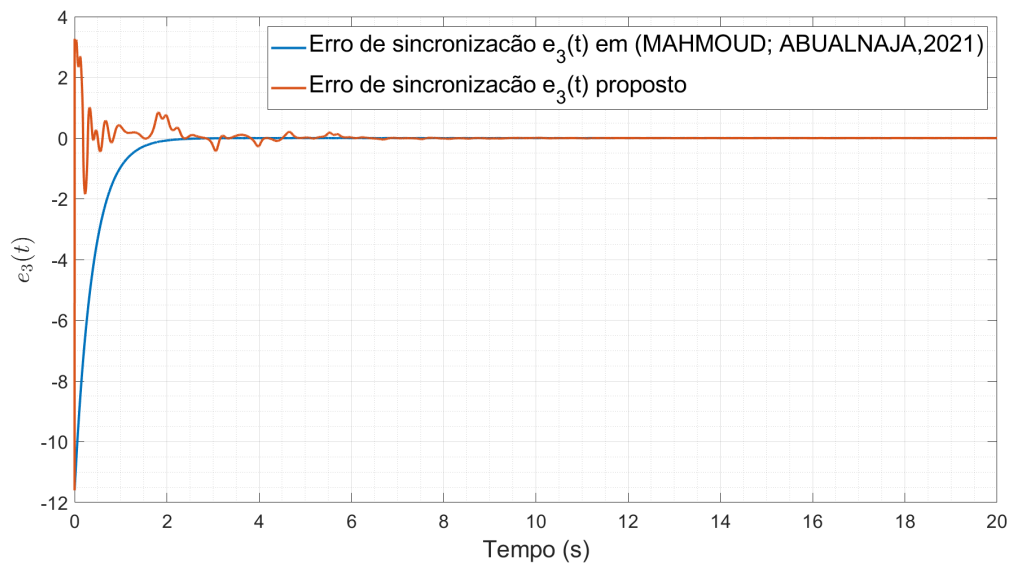


Figura 4.24: Erro de sincronização $e_3(t)$ com lei de controle completamente atuada em contraste com erro de sincronização para o mesmo estado com lei de controle subatuada..

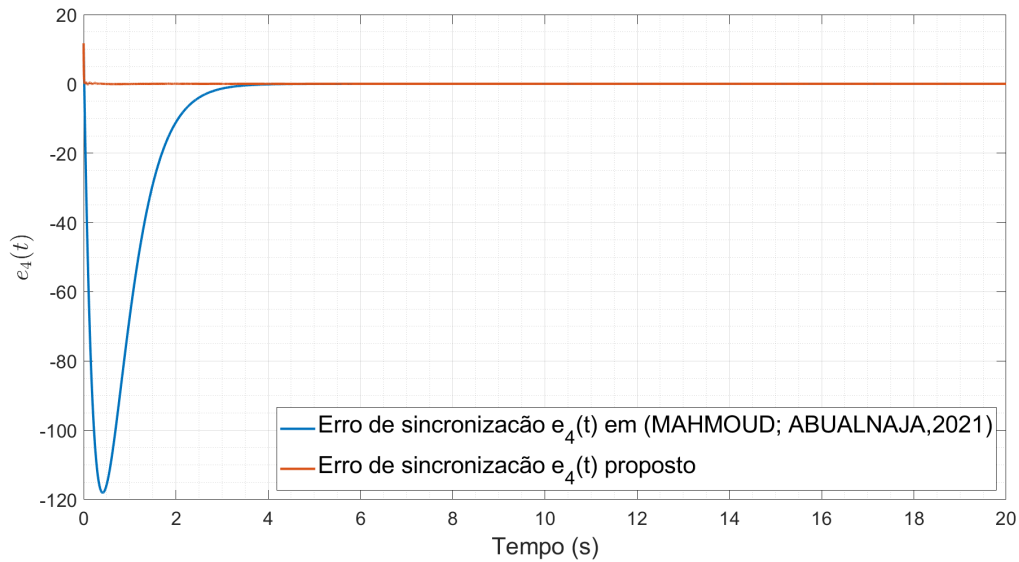


Figura 4.25: Erro de sincronização $e_4(t)$ com lei de controle completamente atuada em contraste com erro de sincronização para o mesmo estado com lei de controle subatuada..

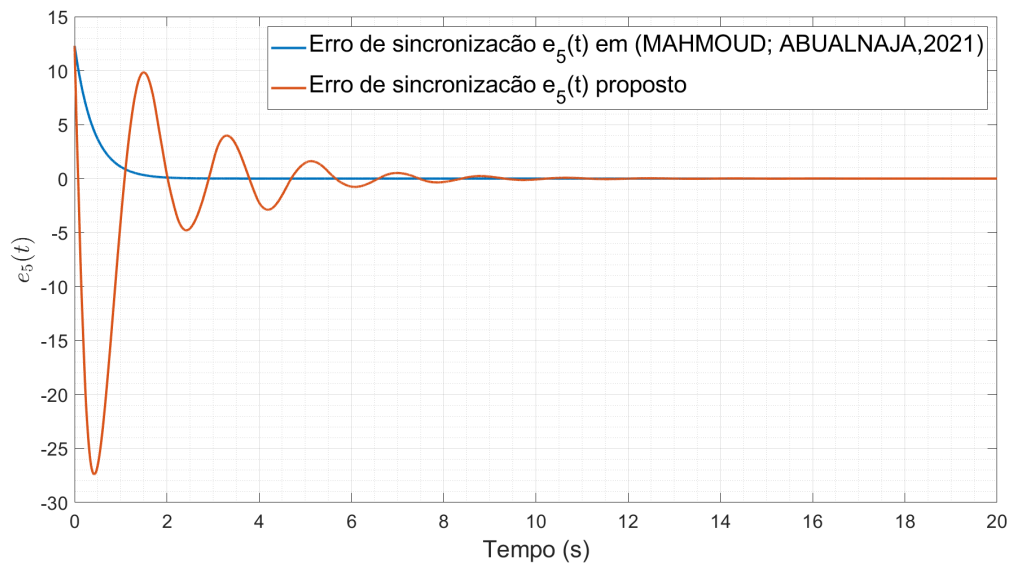


Figura 4.26: Erro de sincronização $e_5(t)$ com lei de controle completamente atuada em contraste com erro de sincronização para o mesmo estado com lei de controle subatuada..

Ao comparar as figuras acima com as obtidas na seção anterior, percebe-se que a sincronização subatuada, aqui proposta, apresenta melhor desempenho em regime transitório para os estados x , w e z que são os estados atuados. Percebe-se também que a lei de controle definida em (4.5) é mais complexa que a utilizada em (3.10) e que a última, mesmo sem ação de controle nos estados y e v , consegue atingir a sincronização completa entre mestre e escravo. Vale ressaltar que a simplicidade é um fator importante quando pretende-se montar na prática os circuitos

que compõem o esquema de telecomunicação, já que reduz-se a quantidade e a complexidade das dinâmicas a serem implementadas.

Capítulo 5

Conclusões

Neste trabalho projetou-se um esquema de telecomunicação seguro subatuado baseado em sistemas hipercaóticos de cinco dimensões. Na literatura atual, a maioria dos esquemas de sincronização são completamente atuados, e por isso, o trabalho aqui proposto se destaca ao utilizar uma lei de controle com dimensão menor que a dos sistemas mestre e escravo. Uma lei de controle subatuada é vantajosa por apresentar maior simplicidade na implementação em circuitos práticos e a transmissão de mensagens pelos estados não atuados, assim possibilitando a aplicação do sincronizador em aplicações de telecomunicação segura.

Outra contribuição importante deste trabalho é a presença de distúrbios limitados na análise de estabilidade de Lyapunov, já que assim consegue-se um esquema de telecomunicação seguro robusto e portanto aplicável, já que considera-se no projeto do sincronizador a presença de ruídos e perturbações inerentes aos canais de comunicação reais.

Para analisar o desempenho do sincronizador subatuado, simulou-se em ambiente *Matlab/Simulink* o comportamento de transmissão sincronização e recepção de duas mensagens analógicas na presença de distúrbios limitados. Os resultados da simulação são condizentes com o esperado teoricamente, ou seja, ocorre a sincronização dos estados dos sistemas mestre e escravo em tempo finito, assim como a convergência entre mensagem recuperada e mensagem original mesmo com uma ação de controle subatuada e na presença de distúrbios. Pode-se perceber pelos sinais de erro de recuperação das mensagens nas figuras 4.13 e 4.14 e, pela comparação entre mensagem original e mensagem recuperada nas figuras 4.15 e 4.16, que os resultados obtidos na simulação são os mesmos do esperado teoricamente pelo método de mascaramento caótico definido pela equação (2.12).

Como trabalhos futuros propõe-se a sincronização de sistemas hipercaóticos de alta dimensão para que a aplicação em telecomunicação segura seja ainda mais eficiente em criptografar a mensagem a ser transmitida. Para contornar a necessidade de utilizar um sistema receptor com mesma dinâmica dominante do sistema transmissor, propõe-se também como um trabalho futuro o uso de redes neurais na sincronização.

O trabalho desenvolvido aqui, é fruto dos conhecimentos adquiridos durante a realização de

outras publicações na mesma área de atuação. Como exemplos de trabalhos preliminares tem-se o trabalho (agraciado com menção honrosa) desenvolvido no 24º Congresso de Iniciação Científica da UnB (PIBIC, 2017/18) e que define um esquema de comunicação segura baseado em caos tridimensional e a publicação de artigo no 14º Simpósio Brasileiro de Automação Inteligente (SBAI, 2019) que utiliza sincronização projetiva para definir o esquema de comunicação segura.

Referências

- AZAR, A. T. et al. Backstepping control and synchronization of chaotic time delayed systems. In: BACKSTEPPING Control of Nonlinear Dynamical Systems. [S.l.]: Elsevier, 2021. p. 407–424.
- BALEANU, D. et al. Hyperchaotic behaviors, optimal control, and synchronization of a nonautonomous cardiac conduction system. *Advances in Difference Equations*, Springer, v. 2021, n. 1, p. 1–24, 2021.
- DEVANEY, R. *An introduction to chaotic dynamical systems*. [S.l.]: Westview press, 2008.
- GUIARTE, K. H. M. et al. An Adaptive Neural Identifier with Applications to Financial and Welding Systems. *International Journal of Control, Automation and Systems*, Springer, p. 1–12, 2021.
- HARDY, G. et al. *Inequalities*. [S.l.]: Cambridge University Press, 1952. (Cambridge Mathematical Library). ISBN 9780521358804.
- IOANNOU, P. A.; SUN, J. *Robust adaptive control*. [S.l.]: Courier Corporation, 2012.
- JAHANSHAHI, H. et al. Complete analysis and engineering applications of a megastable nonlinear oscillator. *International Journal of Non-Linear Mechanics*, Elsevier, v. 107, p. 126–136, 2018.
- JOVIC, B. *Synchronization Techniques for Chaotic Communication Systems*. 1. ed. [S.l.]: Springer-Verlag Berlin Heidelberg, 2011. (Signals and Communication Technology). ISBN 3642218482,9783642218484.
- KEKHA JAVAN, A. A. et al. Design of Adaptive-Robust Controller for Multi-State Synchronization of Chaotic Systems with Unknown and Time-Varying Delays and Its Application in Secure Communication. *Sensors*, Multidisciplinary Digital Publishing Institute, v. 21, n. 1, p. 254, 2021.
- KHALIL, H. K. *Nonlinear systems*. 3rd ed. [S.l.]: Prentice Hall, 2002. ISBN 0130673897,9780130673893.
- KOCAREV, L. et al. Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Chaos*, World Scientific, v. 2, n. 03, p. 709–713, 1992.
- LORENZ, E. N. Deterministic nonperiodic flow. *Journal of atmospheric sciences*, v. 20, n. 2, p. 130–141, 1963.

- LU, J.; WU, X.; LÜ, J. Synchronization of a unified chaotic system and the application in secure communication. *Physics letters A*, Elsevier, v. 305, n. 6, p. 365–370, 2002.
- MAHMOUD, E. E.; ABUALNAJA, K. M. Control and synchronization of the hyperchaotic attractor for a 5-D self-exciting homopolar disc dynamo. *Alexandria Engineering Journal*, Elsevier, v. 60, n. 1, p. 1173–1181, 2021.
- MECHERI, B.; BOUDJEHEM, D.; BOUDJEHEM, B. Fractional order PID controller for the stabilisation of chaotic systems using Takagi-Sugeno fuzzy model. *International Journal of Systems, Control and Communications*, Inderscience Publishers (IEL), v. 12, n. 1, p. 1–11, 2021.
- MOUTSINGA, C. R. B.; PINDZA, E.; MARÉ, E. Comparative performance of time spectral methods for solving hyperchaotic finance and cryptocurrency systems. *Chaos, Solitons & Fractals*, Elsevier, v. 145, p. 110770, 2021.
- NAIM, M.; PACHA, A. A.; SERIEF, C. A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem. *Advances in Space Research*, Elsevier, v. 67, n. 7, p. 2077–2103, 2021.
- OPPENHEIM, A. V. et al. Signal processing in the context of chaotic signals. In: PROC. IEEE ICASSP. [S.l.: s.n.], 1992. v. 4, p. 117–120.
- OUANNAS, A. et al. A novel secure communications scheme based on chaotic modulation, recursive encryption and chaotic masking. *Alexandria Engineering Journal*, Elsevier, v. 60, n. 1, p. 1873–1884, 2021.
- PECORA, L. M.; CARROLL, T. L. Synchronization in chaotic systems. *Physical review letters*, APS, v. 64, n. 8, p. 821, 1990.
- PÉREZ, J. C. N. et al. Secure Communication System Based on Synchronized 3D Spherical Chaotic Systems. In: IEEE. 2020 IEEE International Conference on Engineering Veracruz (ICEV). [S.l.: s.n.], 2020. p. 1–8.
- POINCARÉ, H. Sur le problème des trois corps et les équations de la dynamique. *Acta mathematica*, Springer, v. 13, n. 1, a3–a270, 1890.
- PRAKASH, P. et al. A novel simple 4-D hyperchaotic system with a saddle-point Index-2 equilibrium point and multistability: Design and FPGA-based applications. *Circuits, Systems, and Signal Processing*, Springer, p. 1–22, 2020.
- RÖSSLER, O. An equation for continuous chaos. *Physics Letters A*, v. 57, n. 5, p. 397–398, 1976. ISSN 0375-9601. DOI: [https://doi.org/10.1016/0375-9601\(76\)90101-8](https://doi.org/10.1016/0375-9601(76)90101-8). Disponível em: <<https://www.sciencedirect.com/science/article/pii/0375960176901018>>.
- SAHIN, M. E. et al. Application and modeling of a novel 4D memristive chaotic system for communication systems. *Circuits, Systems, and Signal Processing*, Springer, p. 1–30, 2020.

- AL-SAIDI, N. M. G. et al. A New Hyperchaotic Map for a Secure Communication Scheme with an Experimental Realization. *Symmetry*, v. 12, n. 11, 2020. ISSN 2073-8994. DOI: 10.3390/sym12111881. Disponível em: <<https://www.mdpi.com/2073-8994/12/11/1881>>.
- SLOTINE, L. *Applied Nonlinear Control*. [S.l.]: Englewood Cliffs, N.J: Prentice Hall, 1991.
- STANKEVICH, N. et al. Chaos and hyperchaos via secondary Neimark–Sacker bifurcation in a model of radiophysical generator. *Nonlinear dynamics*, Springer, v. 97, n. 4, p. 2355–2370, 2019.
- STROGATZ, S. H. *Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering*. [S.l.]: CRC Press, 2018.
- TANG, X.; MANDAL, S. Encrypted Physical Layer Communications Using Synchronized Hyperchaotic Maps. *IEEE Access*, IEEE, v. 9, p. 13286–13303, 2021.
- TAO YANG; CHUA, L. O. Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, v. 44, n. 10, p. 976–988, 1997. DOI: 10.1109/81.633887.
- TIAN, H. et al. Dynamic Analysis and Robust Control of a Chaotic System with Hidden Attractor. *Complexity*, Hindawi, v. 2021, 2021.
- TRIKHA, P.; JAHANZAIB, L. S. Dynamical analysis of a novel 5-d hyper-chaotic system with no equilibrium point and its application in secure communication. *Differential Geometry–Dynamical Systems*, v. 22, 2020.
- WANG, J.; YANG, C. Chaos synchronization of a finance chaotic system with an integral sliding mode controller. *Journal of Mathematics*, Hindawi, v. 2021, 2021.
- WEI, Z.; MOROZ, I. et al. Hidden hyperchaos and electronic circuit application in a 5D self-exciting homopolar disc dynamo. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, AIP Publishing LLC, v. 27, n. 3, p. 033101, 2017.
- WEI, Z.; YOUSEFPOUR, A. et al. Hopf bifurcation and synchronization of a five-dimensional self-exciting homopolar disc dynamo using a new fuzzy disturbance-observer-based terminal sliding mode control. *Journal of the Franklin Institute*, Elsevier, v. 358, n. 1, p. 814–833, 2021.
- WEN, H. et al. Security Analysis of a Color Image Encryption Algorithm Using a Fractional-Order Chaos. *Entropy*, Multidisciplinary Digital Publishing Institute, v. 23, n. 2, p. 258, 2021.
- WIGGINS, S. *Introduction to applied nonlinear dynamical systems and chaos*. 3rd. [S.l.]: Springer-Verlag Telos, 1997. ISBN 0387970037,9780387970035.
- XIAO-QING, W. et al. A Plaintext-Related Image Encryption Algorithm Based on Compressive Sensing and a Novel Hyperchaotic System. *International Journal of Bifurcation and Chaos*, World Scientific, v. 31, n. 02, p. 2150021, 2021.
- XIU, C. et al. Memristive hyperchaos secure communication based on sliding mode control. *Nonlinear Dynamics*, Springer, p. 1–17, 2021.

YANG, C.-C. Adaptive synchronization of Lü hyperchaotic system with uncertain parameters based on single-input controller. *Nonlinear Dynamics*, Springer, v. 63, n. 3, p. 447–454, 2011.

YU, F.; LIU, L. et al. Chaos-based application of a novel multistable 5D memristive hyperchaotic system with coexisting multiple attractors. *Complexity*, Hindawi, v. 2020, 2020.

YU, F.; QIAN, S. et al. A new 4D four-wing memristive hyperchaotic system: dynamical analysis, electronic circuit design, shape synchronization and secure communication. *International Journal of Bifurcation and Chaos*, World Scientific, v. 30, n. 10, p. 2050147, 2020.

Apêndice A

Códigos fonte e diagramas para simulação *Matlab/Simulink*

A.1 Diagrama de blocos *Simulink*

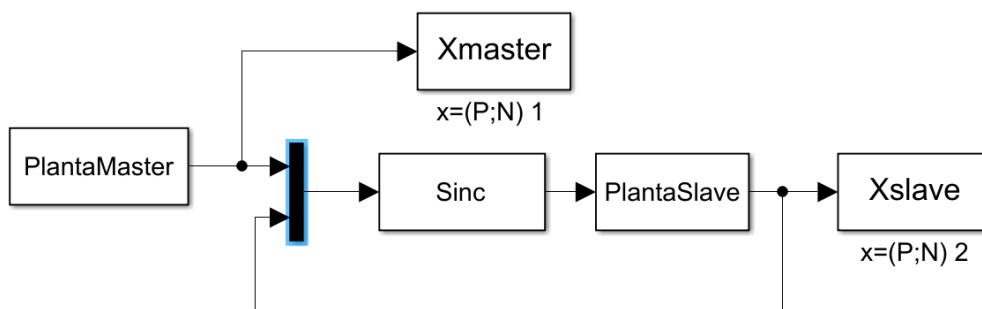


Figura A.1: Diagrama de blocos no Simulink

A.2 *PlantaMaster.m*

```
1 -]]function [sys ,x0 ,str ,ts ] = PlantaMaster(t ,x ,u ,flag )
2 %Constantes que definem o sistema hipercaotico
3 r=8;
4 m=0.04;
5 g=140.6;
6 k1=34;
7 k2=12;
8 %Mensagens a transmitir
9 msg1 = (0.24*sin(2*pi*0.6*t) + 0.38*cos(2*pi*2*t));
10 msg2 = (0.5*sin(2*pi*1.5*t + pi/4) + 0.26*cos(2*pi*0.6*t) + 0.3* square(2*pi
    *0.75*t));
11 %msg3 = 0.2*(sawtooth(2*pi*t));
12 %msg1 =0 ;
```

```

13 %msg2 =0;
14
15 switch flag ,
16
17     % Setup %
18
19 case 0,
20     sizes = simsizes;
21     sizes.NumContStates = 5; %Numero de estados continuos
22     sizes.NumDiscStates = 0; %Numero de estados discretos
23     sizes.NumOutputs = 5; %Numero de saidas
24     sizes.NumInputs = 0; %Numero de entradas
25     sizes.DirFeedthrough = 1;
26     sizes.NumSampleTimes = 1;
27     sys = simsizes(sizes);
28     x0=[10.05 -13.5 -11.3 10.2 11.9]; %Condiçoes iniciais
29     str=[];
30     ts=[0 0];
31
32     % Diretivas %
33
34 case 1, %Sistema dinamico hipercaotico
35     sys = [ r*(x(2)-x(1))+x(4);
36           -(1+m)*x(2)+x(1)*x(3)-x(5);
37           g*(1+m*x(1)*x(1)-(1+m)*x(1)*x(2));
38           2*(1+m)*x(4)+x(1)*x(3)-k1*x(1);
39           m*x(5)+k2*x(2) ];
40
41     % Saida %
42
43 case 3,
44     sys =[x(1);
45          x(2) + msg1;
46          x(3);
47          x(4);
48          x(5) + msg2];
49
50     % End %
51
52 case {2,4,9},
53     sys = [];
54 otherwise
55     error(['unhandled flag = ',num2str(flag)]);
56 end

```

A.3 *Sinc.m*

```

1 -]]function [sys ,x0 , str , ts ] = Sinc(t , x , u , flag)

```

```

2
3
4 psi1=200;
5 psi2=200;
6 psi3=1000;
7 psi4=500;
8 psi5=200;
9
10 switch flag ,
11     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
12     % Inicializacao %
13     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
14 case 0,
15
16     sizes = simsizes;
17     sizes.NumContStates = 5; %Numero de estados continuos
18     sizes.NumDiscStates = 0; %Numero de estados discretos
19     sizes.NumOutputs = 5; %Numero de saidas
20     sizes.NumInputs = 10; %Numero de entradas
21     sizes.DirFeedthrough = 1;
22     sizes.NumSampleTimes = 1;
23     sys = simsizes(sizes);
24     x0=zeros(5,1); %Condicoes iniciais
25     x0(1)=0;
26     x0(2)=0;
27     x0(3)=0;
28     x0(4)=0;
29     x0(5)=0;
30     str=[];
31     ts=[0 0];
32     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
33     % Diretivas %
34     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
35 case 1, %aqui ficariam estimadores dos pesos de uma rede neural caso
    houvesse , nesse caso nao ha
36     sys = [0;
37            0;
38            0;
39            0;
40            0];
41     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
42     % Saidas %
43     %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
44 case 3, %controlador
45     sys = [-1*(psi1*(u(6) - u(1)) + psi2*(u(6) - u(1))^3);
46            -0*(psi1*(u(7) - u(2)));
47            -1*(psi3*(u(8) - u(3)) + psi4*(u(8) - u(3))^3);
48            -1*(psi5*(u(9) - u(4)));
49            -0*(psi1*(u(10) - u(5)))]);
50     %sys = [-1*(psi1*(u(4) - u(1)))/(abs(u(4) - u(1)) + lambdazero1

```

```

    );
51     case {2,4,9},
52     sys = [];
53
54     otherwise
55     error(['unhandled flag = ', num2str(flag)]);
56 end

```

A.4 *Graficos.m*

```

1  -]]%Executando esse arquivo --> automaticamente mostra os graficos da
2  %simulacao e salva na pasta em formato png (poderia ser escolhido
3  %formato jpg tambem)
4  clc
5  fsize=20;
6
7  %Figura 1
8  fig=figure;
9  plot(t,Xmaster(:,1),t, Xslave(:,1),':','LineWidth',2);set(0,'
    DefaultAxesFontSize',16);
10 grid on
11 grid minor
12 h=legend('Mestre','Escravo','Location','southeast');
13 set(h,'FontSize',fsize);
14 set(0,'DefaultAxesFontSize',16);
15 xlabel('Tempo (s)','FontSize',fsize);
16 ylabel('$x_m(t), x_s(t)$','$','Interpreter','Latex','FontSize',fsize)
17 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
18 saveas(gcf,'FIG1.png');
19 close(fig)
20
21 %Figura 2
22 fig=figure;
23 plot(t,Xmaster(:,2),t, Xslave(:,2),':','LineWidth',2);set(0,'
    DefaultAxesFontSize',16);
24 grid on
25 grid minor
26 h=legend('Mestre','Escravo','Location','southeast');
27 set(h,'FontSize',fsize);
28 set(0,'DefaultAxesFontSize',16);
29 xlabel('Tempo (s)','FontSize',fsize);
30 ylabel('$y_m(t), y_s(t)$','$','Interpreter','Latex','FontSize',fsize)
31 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
32 saveas(gcf,'FIG2.png');
33 close(fig)
34
35 %Figura 3
36 fig=figure;

```



```

37 plot(t,Xmaster(:,3),t, Xslave(:,3),':', 'LineWidth',2);set(0,'
    DefaultAxesFontSize',16);
38 grid on
39 grid minor
40 h=legend('Mestre','Escravo','Location','northeast');
41 set(h,'FontSize',fsize);
42 set(0,'DefaultAxesFontSize',16);
43 xlabel('Tempo (s)','FontSize',fsize);
44 ylabel('$$z_{m}(t), z_{s}(t)$$','Interpreter','Latex','FontSize',fsize)
45 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
46 saveas(gcf,'FIG3.png');
47 close(fig)
48
49 %Figura 4
50 fig=figure;
51 plot(t,Xmaster(:,4),t, Xslave(:,4),':', 'LineWidth',2);set(0,'
    DefaultAxesFontSize',16);
52 grid on
53 grid minor
54 h=legend('Mestre','Escravo','Location','northeast');
55 set(h,'FontSize',fsize);
56 set(0,'DefaultAxesFontSize',16);
57 xlabel('Tempo (s)','FontSize',fsize);
58 ylabel('$$w_{m}(t), w_{s}(t)$$','Interpreter','Latex','FontSize',fsize)
59 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
60 saveas(gcf,'FIG4.png');
61 close(fig)
62
63 %Figura 5
64 fig=figure;
65 plot(t,Xmaster(:,5),t, Xslave(:,5),':', 'LineWidth',2);set(0,'
    DefaultAxesFontSize',16);
66 grid on
67 grid minor
68 h=legend('Mestre','Escravo','Location','northeast');
69 set(h,'FontSize',fsize);
70 set(0,'DefaultAxesFontSize',16);
71 xlabel('Tempo (s)','FontSize',fsize);
72 ylabel('$$v_{m}(t), v_{s}(t)$$','Interpreter','Latex','FontSize',fsize)
73 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
74 saveas(gcf,'FIG5.png');
75 close(fig)
76
77 %Figura 6
78 fig=figure;
79 plot(t,Xmaster(:,1)- Xslave(:,1), 'LineWidth',2);set(0,'DefaultAxesFontSize
    ',16);
80 grid on
81 grid minor
82 h=legend('Erro de sincronizacao estado x','Location','southeast');

```

```

83 set(h,'FontSize',fs);
84 set(0,'DefaultAxesFontSize',16);
85 xlabel('Tempo (s)','FontSize',fs);
86 ylabel('$e_{1}(t)$','Interpreter','Latex','FontSize',fs);
87 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
88 saveas(gcf,'erro1.png');
89 close(fig)
90
91 %Figura 7
92 fig=figure;
93 plot(t,Xmaster(:,2)-Xslave(:,2),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
94 grid on
95 grid minor
96 h=legend('Erro de sincronizacao estado y','Location','southeast');
97 set(h,'FontSize',fs);
98 set(0,'DefaultAxesFontSize',16);
99 xlabel('Tempo (s)','FontSize',fs);
100 ylabel('$e_{2}(t)$','Interpreter','Latex','FontSize',fs);
101 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
102 saveas(gcf,'erro2.png');
103 close(fig)
104
105 %Figura 8
106 fig=figure;
107 plot(t,Xmaster(:,3)-Xslave(:,3),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
108 grid on
109 grid minor
110 h=legend('Erro de sincronizacao estado z','Location','northeast');
111 set(h,'FontSize',fs);
112 set(0,'DefaultAxesFontSize',16);
113 xlabel('Tempo (s)','FontSize',fs);
114 ylabel('$e_{3}(t)$','Interpreter','Latex','FontSize',fs);
115 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
116 saveas(gcf,'erro3.png');
117 close(fig)
118
119 %Figura 9
120 fig=figure;
121 plot(t,Xmaster(:,4)-Xslave(:,4),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
122 grid on
123 grid minor
124 h=legend('Erro de sincronizacao estado w','Location','northeast');
125 set(h,'FontSize',fs);
126 set(0,'DefaultAxesFontSize',16);
127 xlabel('Tempo (s)','FontSize',fs);
128 ylabel('$e_{4}(t)$','Interpreter','Latex','FontSize',fs);
129 set(gcf,'units','normalized','outerposition',[0 0 1 1]);

```

```

130 saveas(gcf,'erro4.png');
131 close(fig)
132
133 %Figura 10
134 fig=figure;
135 plot(t,Xmaster(:,5)- Xslave(:,5),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
136 grid on
137 grid minor
138 h=legend('Erro de sincronizacao estado v','Location','northeast');
139 set(h,'FontSize',fsize);
140 set(0,'DefaultAxesFontSize',16);
141 xlabel('Tempo (s)','FontSize',fsize);
142 ylabel('$e_{5}(t)$','Interpreter','Latex','FontSize',fsize)
143 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
144 saveas(gcf,'erro5.png');
145 close(fig)

```

A.5 GraficosMsg.m

```

1 -]] clc
2 fsize=20;
3
4 msg1 = (0.24*sin(2*pi*0.6*t) + 0.38*cos(2*pi*2*t));
5 msg2 = (0.5*sin(2*pi*1.5*t + pi/4) + 0.26*cos(2*pi*0.6*t) + 0.3*sqrt(2*pi
   *0.75*t));
6 %msg3 = 0.2*(sawtooth(2*pi*t));
7
8
9 %Figura 11
10 fig=figure;
11 plot(t,msg1,'LineWidth',2);set(0,'DefaultAxesFontSize',16);
12 grid on
13 grid minor
14 h=legend('Mensagem original 1','Location','northeast');
15 set(h,'FontSize',fsize);
16 set(0,'DefaultAxesFontSize',16);
17 xlabel('Tempo (s)','FontSize',fsize);
18 ylabel('$msg_{1}(t)$','Interpreter','Latex','FontSize',fsize)
19 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
20 saveas(gcf,'msg1.png');
21 close(fig)
22
23 %Figura 12
24 fig=figure;
25 plot(t,msg2,'LineWidth',2);set(0,'DefaultAxesFontSize',16);
26 grid on
27 grid minor

```

```

28 h=legend('Mensagem original 2','Location','northeast');
29 set(h,'FontSize',fsize);
30 set(0,'DefaultAxesFontSize',16);
31 xlabel('Tempo (s)','FontSize',fsize);
32 ylabel('$$msg_{2}(t)$$','Interpreter','Latex','FontSize',fsize)
33 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
34 saveas(gcf,'msg2.png');
35 close(fig)
36
37 %Figura 13
38 % fig=figure;
39 % plot(t,msg3,'LineWidth',2);set(0,'DefaultAxesFontSize',16);
40 % grid on
41 % grid minor
42 % h=legend('Mensagem original 3','Location','northeast');
43 % set(h,'FontSize',fsize);
44 % set(0,'DefaultAxesFontSize',16);
45 % xlabel('Tempo (s)','FontSize',fsize);
46 % ylabel('$$msg_{3}(t)$$','Interpreter','Latex','FontSize',fsize)
47 % set(gcf,'units','normalized','outerposition',[0 0 1 1]);
48 % saveas(gcf,'msg3.png');
49 % close(fig)
50
51 %Figura 14
52 fig=figure;
53 plot(t,Xmaster(:,2)-Xslave(:,2),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
54 grid on
55 grid minor
56 h=legend('Mensagem 1 recuperada','Location','northeast');
57 set(h,'FontSize',fsize);
58 set(0,'DefaultAxesFontSize',16);
59 xlabel('Tempo (s)','FontSize',fsize);
60 ylabel('$$msg_{1}Rec(t)$$','Interpreter','Latex','FontSize',fsize)
61 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
62 saveas(gcf,'msg1Rec.png');
63 close(fig)
64
65 %Figura 15
66 fig=figure;
67 plot(t,Xmaster(:,5)-Xslave(:,5),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
68 grid on
69 grid minor
70 h=legend('Mensagem 2 recuperada','Location','northeast');
71 set(h,'FontSize',fsize);
72 set(0,'DefaultAxesFontSize',16);
73 xlabel('Tempo (s)','FontSize',fsize);
74 ylabel('$$msg_{2}Rec(t)$$','Interpreter','Latex','FontSize',fsize)
75 set(gcf,'units','normalized','outerposition',[0 0 1 1]);

```

```

76 saveas(gcf,'msg2Rec.png');
77 close(fig)
78
79 %Figura 16
80 % fig=figure;
81 % plot(t,Xmaster(:,3)- Xslave(:,3),'LineWidth',2);set(0,'
      DefaultAxesFontSize',16);
82 % grid on
83 % grid minor
84 % h=legend('Mensagem 3 recuperada','Location','northeast');
85 % set(h,'FontSize',fsize);
86 % set(0,'DefaultAxesFontSize',16);
87 % xlabel('Tempo (s)','FontSize',fsize);
88 % ylabel('$msg_{3}Rec(t)$','Interpreter','Latex','FontSize',fsize)
89 % set(gcf,'units','normalized','outerposition',[0 0 1 1]);
90 % saveas(gcf,'msg3Rec.png');
91 % close(fig)
92
93 %Figura 17
94 fig=figure;
95 plot(t,msg1-(Xmaster(:,2)- Xslave(:,2)),'LineWidth',2);set(0,'
      DefaultAxesFontSize',16);
96 grid on
97 grid minor
98 h=legend('Erro de recuperacao da mensagem 1','Location','northeast');
99 set(h,'FontSize',fsize);
100 set(0,'DefaultAxesFontSize',16);
101 xlabel('Tempo (s)','FontSize',fsize);
102 ylabel('$msg_{1}RecError(t)$','Interpreter','Latex','FontSize',fsize)
103 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
104 saveas(gcf,'msg1RecError.png');
105 close(fig)
106
107 %Figura 18
108 fig=figure;
109 plot(t,msg2-(Xmaster(:,5)- Xslave(:,5)),'LineWidth',2);set(0,'
      DefaultAxesFontSize',16);
110 grid on
111 grid minor
112 h=legend('Erro de recuperacao da mensagem 2','Location','northeast');
113 set(h,'FontSize',fsize);
114 set(0,'DefaultAxesFontSize',16);
115 xlabel('Tempo (s)','FontSize',fsize);
116 ylabel('$msg_{2}RecError(t)$','Interpreter','Latex','FontSize',fsize)
117 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
118 saveas(gcf,'msg2RecError.png');
119 close(fig)
120
121 % %Figura 19
122 % fig=figure;

```

```

123 % plot(t,msg3-(Xmaster(:,3)- Xslave(:,3)), 'LineWidth',2); set(0, '
      DefaultAxesFontSize',16);
124 % grid on
125 % grid minor
126 % h=legend('Erro de recuperacao da mensagem 3', 'Location', 'northeast');
127 % set(h, 'FontSize', fsize);
128 % set(0, 'DefaultAxesFontSize', 16);
129 % xlabel('Tempo (s)', 'FontSize', fsize);
130 % ylabel('$$msg_{3}RecError(t)$$', 'Interpreter', 'Latex', 'FontSize', fsize)
131 % set(gcf, 'units', 'normalized', 'outerposition', [0 0 1 1]);
132 % saveas(gcf, 'msg3RecError.png');
133 % close(fig)
134
135 %Figura 20
136 fig=figure;
137 plot(t, Xmaster(:,2), 'LineWidth',2); set(0, 'DefaultAxesFontSize',16);
138 grid on
139 grid minor
140 h=legend('Mensagem 1 criptografada', 'Location', 'northeast');
141 set(h, 'FontSize', fsize);
142 set(0, 'DefaultAxesFontSize', 16);
143 xlabel('Tempo (s)', 'FontSize', fsize);
144 ylabel('$$msg_{1}Cripto(t)$$', 'Interpreter', 'Latex', 'FontSize', fsize)
145 set(gcf, 'units', 'normalized', 'outerposition', [0 0 1 1]);
146 saveas(gcf, 'msg1Cripto.png');
147 close(fig)
148
149 %Figura 21
150 fig=figure;
151 plot(t, Xmaster(:,5), 'LineWidth',2); set(0, 'DefaultAxesFontSize',16);
152 grid on
153 grid minor
154 h=legend('Mensagem 2 criptografada', 'Location', 'northeast');
155 set(h, 'FontSize', fsize);
156 set(0, 'DefaultAxesFontSize', 16);
157 xlabel('Tempo (s)', 'FontSize', fsize);
158 ylabel('$$msg_{2}Cripto(t)$$', 'Interpreter', 'Latex', 'FontSize', fsize)
159 set(gcf, 'units', 'normalized', 'outerposition', [0 0 1 1]);
160 saveas(gcf, 'msg2Cripto.png');
161 close(fig)
162
163 %Figura 22
164 % fig=figure;
165 % plot(t, Xmaster(:,3), 'LineWidth',2); set(0, 'DefaultAxesFontSize',16);
166 % grid on
167 % grid minor
168 % h=legend('Mensagem 3 criptografada', 'Location', 'northeast');
169 % set(h, 'FontSize', fsize);
170 % set(0, 'DefaultAxesFontSize', 16);
171 % xlabel('Tempo (s)', 'FontSize', fsize);

```

```

172 % ylabel('$$msg_{3}Cripto(t)$$','Interpreter','Latex','FontSize',fsize)
173 % set(gcf,'units','normalized','outerposition',[0 0 1 1]);
174 % saveas(gcf,'msg3Cripto.png');
175 % close(fig)
176
177 %Figura 23
178 fig=figure;
179 plot(t,msg1,t,Xmaster(:,2),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
180 grid on
181 grid minor
182 h=legend('Mensagem original 1','Mensagem criptografada 1','Location','
        northeast');
183 set(h,'FontSize',fsize);
184 set(0,'DefaultAxesFontSize',16);
185 xlabel('Tempo (s)','FontSize',fsize);
186 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
187 saveas(gcf,'0 rig -Cripto1.png');
188 close(fig)
189
190 %Figura 24
191 fig=figure;
192 plot(t,msg2,t,Xmaster(:,5),'LineWidth',2);set(0,'DefaultAxesFontSize',16);
193 grid on
194 grid minor
195 h=legend('Mensagem original 2','Mensagem criptografada 2','Location','
        northeast');
196 set(h,'FontSize',fsize);
197 set(0,'DefaultAxesFontSize',16);
198 xlabel('Tempo (s)','FontSize',fsize);
199 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
200 saveas(gcf,'0 rig -Cripto2.png');
201 close(fig)
202
203 %Figura 25
204 % fig=figure;
205 % plot(t,msg3,t,Xmaster(:,3),'LineWidth',2);set(0,'DefaultAxesFontSize',16)
        ;
206 % grid on
207 % grid minor
208 % h=legend('Mensagem original 3','Mensagem criptografada 3','Location','
        northeast');
209 % set(h,'FontSize',fsize);
210 % set(0,'DefaultAxesFontSize',16);
211 % xlabel('Tempo (s)','FontSize',fsize);
212 % set(gcf,'units','normalized','outerposition',[0 0 1 1]);
213 % saveas(gcf,'0 rig -Cripto3.png');
214 % close(fig)
215
216 % Figura 25
217 fig=figure;

```

```

218 plot(t,msg1,t,(Xmaster(:,2)-Xslave(:,2)),'LineWidth',2);set(0,'
      DefaultAxesFontSize',16);
219 grid on
220 grid minor
221 h=legend('Mensagem original 1','Mensagem recuperada 1','Location','
      northeast');
222 set(h,'FontSize',fsize);
223 set(0,'DefaultAxesFontSize',16);
224 xlabel('Tempo (s)','FontSize',fsize);
225 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
226 saveas(gcf,'0 rig-Rec1.png');
227 close(fig)
228
229 % Figura 26
230 fig=figure;
231 plot(t,msg2,t,(Xmaster(:,5)-Xslave(:,5)),'LineWidth',2);set(0,'
      DefaultAxesFontSize',16);
232 grid on
233 grid minor
234 h=legend('Mensagem original 2','Mensagem recuperada 2','Location','
      northeast');
235 set(h,'FontSize',fsize);
236 set(0,'DefaultAxesFontSize',16);
237 xlabel('Tempo (s)','FontSize',fsize);
238 set(gcf,'units','normalized','outerposition',[0 0 1 1]);
239 saveas(gcf,'0 rig-Rec2.png');
240 close(fig)

```