

Acoplamento de osciladores eletrônicos caóticos para comunicação segura

Orientador: Marcos Oriá

Co-orientador: Weliton Martins

1. Introdução

Comunicação segura é um imperativo para envio de dados entre partes evitando-se o conhecimento do conteúdo por terceiros [1]. Desta forma o desenvolvimento e aplicação de técnicas originais de comunicação segura e de criptografia são urgentes para se fazer face às necessidades de canais privados de comunicação entre agentes governamentais, econômicos, industriais e comerciais, mas também para o uso social nos diversos meios de comunicação entre máquinas e/ou pessoas. Criptografia baseada em sistemas cuja dinâmica é não-linear é uma opção que tem sido investigada nos últimos anos, onde se explora comportamentos não-lineares de sistemas como novas alternativas para comunicação segura [2].

Após o estabelecimento de técnicas de estudo de caos e a constatação da forte dependência da evolução do estado do sistema com suas condições iniciais, permitindo a geração de comportamentos pseudo-aleatórios com características estatísticas similares a de criptosistemas, sugeriam o uso do caos como técnica criptográfica. Ou seja, embora determinísticos, sinais caóticos tem propriedades quase-randômicas [3] e no final dos anos 1980 foram propostas técnicas criptográficas baseadas em caos [4]. Logo após a demonstração da sincronização de sistemas caóticos [5], osciladores caóticos acoplados passaram a ser testados para o envio de mensagens escondidas no sinal caótico de um dos osciladores [6]. A sincronização da parte do sinal caótico porém determinístico, pelo receptor, permite se extrair a mensagem enviada. Demonstração do emprego dessa técnica em uma rede comercial permitiu validar o potencial de emprego prático de comunicação secreta com caos [7], no que pese as discussões do nível de segurança daquela técnica em particular.

Temos utilizado osciladores eletrônicos não-lineares para estudos de sincronização e dessincronização entres sistemas caóticos analisando a topologia do espaço de fase do sistema não-linear, o que permite determinar as condições para ocorrência de eventos de sincronização e de dessincronização [8-11]. Nesse último caso, analisando a estatística de eventos de dessincronização, demonstramos a capacidade de previsão de certos eventos extremos e o seu controle [12].

Nesse projeto para uma dissertação de mestrado serão construídos osciladores autônomos, para os quais serão determinados regimes de sincronização e montado um protótipo para comunicação com caos.

2. Objetivos

2.1 Geral

Aprofundar a *expertise* no uso de sistemas não-lineares como técnica de comunicação segura, desenvolvendo novas técnicas de uso de osciladores caóticos em comunicação;

Desenvolver novas estratégias e dispositivos para envio de mensagens escondidas ou encriptadas em sinais caóticos;

Aplicar técnicas de análise dos eventos de dessincronização como ferramenta de estudo de sistemas complexos, no que tange a ocorrência de eventos extremos nesses sistemas.

2.1 Específicos

Os objetivos específicos desse projeto visam o treinamento de um estudante a nível de mestrado, com as seguinte metas, além dos cursos de formação avançada:

- construção de protótipos de sistemas eletrônicos para sincronização de caos e sua caracterização experimental;
- construção de modelo linearizado para as equações não-lineares dos sistemas estudados, para se obter condições de sincronização a partir de medidas de expoentes de Lyapunov para os osciladores autônomos;
- realização de simulações numéricas dos sistemas não-lineares que descrevem os osciladores experimentais e comparação com as medidas experimentais. Análise dos resultados;
- demonstração de protótipo de um sistema de osciladores cóticos acoplados para comunicação segura.

3. Metodologia

Sistemas não-lineares, com comportamento caótico tem sido estudados desde o final do século XIX, tendo ganhando grande impulso a partir dos anos 1970, com o advento de computadores, ferramenta imprescindível para o estudo aprofundado de comportamentos caóticos [13]. Comunicação com caos foi demonstrada em anos recentes com circuitos eletrônicos [14], assim como em frequências óticas, utilizando lasers [7,15], pela vantagem evidente da faixa de frequência a ser explorada. A possibilidade de sincronização de osciladores caóticos está na base de diversas técnicas de comunicação com caos, onde a informação pode ser mascarada no sinal caótico transmitido. Nesse projeto desenvolveremos um protótipo de osciladores caóticos sincronizados usando circuitos eletrônicos não-lineares. Estudaremos a sincronização de sinais caóticos e faremos a demonstração do seu uso em comunicação segura.

O estudo sistemático de sincronização de osciladores não-lineares foi realizada em diversas configurações entre osciladores idênticos e não-idênticos, acoplamento uni- ou bi-, ou mesmo multi-direcional, resultando na existência de diferentes regimes de sincronização, como completo, de fase, incompleto, atrasado, ou generalizado, onde os sinais dos dois osciladores estão associados por uma função bem definida. Nesse projeto limitaremos nossas investigações ao acoplamento de dois circuitos, descritos por equações diferenciais quase-idênticas de primeira ordem, com acoplamento linear. Pequenas diferenças nos valores dos componentes dos circuitos, assim como o ruído intrínseco serão incluídos nos modelos. Nesse regime de operação usaremos ferramentas de análise de comportamento não linear como os expoentes de Lyapunov e correlações, que permitem determinar condições de acoplamento completo ou intermitente [16].

Circuitos que implementam as equações do tipo Lorenz [17], Rossler [18], Chua [19], van der Pol [20], hipercaos [21], são bem conhecidos e sua implementação é relativamente bem estabelecida na literatura, mesmo com componentes analógicos, visto a possibilidade de se usar elementos derivadores e integradores. De fato, sistemas não-lineares com três variáveis independentes, que permitem a geração de caos, podem de forma geral serem implementados por 'calculadoras' analógicas realizadas por circuitos eletrônicos. Opções com circuitos integrados também tem sido explorados. Concretamente construiremos nesse projeto circuitos autônomos, do tipo Chua [22] modificado, cuja não-linearidade é assegurada pela resposta linear-por-partes de diodos contra-paralelos [16] e que oscila de forma autônoma graças a um resistor 'negativo' [23].

Como demonstrado em trabalhos anteriores, onde usamos sistemas acoplados em regime intermitente [8-12] o uso de osciladores caóticos acoplados é uma potente ferramenta para estudo de categorias estatísticas, particularmente as distribuições anômalas. Desta forma exploraremos outras configurações possíveis de acoplamento que incluem o uso de osciladores autônomos e diferentes tipos de acoplamento, seja unidirecional, bi-direcional, ou mesmo envolvendo um maior número de osciladores. Possíveis desdobramentos desses trabalhos se dará através do uso de configurações em rede de circuitos quase-idênticos, ou osciladores óticos. Esses desdobramentos dependerão do desenvolvimento dos objetivos específicos desse projeto, no período da preparação de uma dissertação de mestrado.

Para descrever os resultados da dinâmica não-linear de osciladores caóticos, assim como obter medidas estatísticas dos eventos de dessincronização, rotinas numéricas têm sido desenvolvidas em nosso laboratório. Elas estão sendo frequentemente adaptadas, buscando-se descrever, de forma realista, novas configurações a serem implementadas. Parte desse projeto consistirá na implementação de rotinas numéricas e análise comparativa das simulações com resultados experimentais, assim como usaremos simulações numéricas em testes para se avaliar novas configurações antes de sua implementação em laboratório. Portanto, simulações dos comportamentos oscilatórios dos circuitos não lineares, assim como o acoplamento entre circuitos equivalentes será feita em rotinas numéricas em Python. Ademais a utilização de softwares dedicados para simular circuitos eletrônicos, tipo Multisim, poderá ser usada para validar resultados obtidos com os circuitos reais em laboratório.

De forma geral o estudo do comportamento estatístico de eventos de sincronização também permite estender a aplicabilidade desses sistemas em estudos para se identificar comportamentos universais em sistemas complexos. Ou seja, lidar com sistemas dinâmicos não-lineares é uma opção realista quando vislumbramos a compreensão de sistemas complexos, sejam eles grandes ou pequenos, com muitos ou poucos corpos e/ou variáveis. De fato, além de sistemas físicos e químicos que abordaremos em nossos laboratórios, sistemas biológicos, populações, assim como redes de computadores, transações financeiras, logística e problemas de infraestrutura urbana, são exemplos de sistemas com marcada natureza não-linear na sua dinâmica temporal. Algumas das propriedades, características e comportamentos desses sistemas podem ser comuns, dada a universalidade de descrições matemáticas. Em outros termos, a relativa simplicidade de implementação de sistemas não-lineares em laboratório, que embora descritos por poucas equações de primeira ordem, resultam em sinais surpreendentemente complexos, e servem de 'bancada de teste', em laboratório, permitindo a análise das propriedades, características e comportamentos que eventualmente podem ser estendidos para outros sistemas complexos de difícil experimentação, dada a universalidade de descrições matemáticas.

4. Resultados Esperados

Nesse projeto implementaremos técnicas efetivas de utilização de osciladores caóticos em circuitos eletrônicos de relativamente baixa frequência visando o domínio da técnica de comunicações seguras onde a informação pode ser escondida no sinal caótico e recuperado pelo receptor, usando canais públicos, através da sincronização do oscilador local com o sinal transmitido.

O principal resultado desse projeto é a formação qualificada de um estudante de pós-graduação, quantificado por uma dissertação de mestrado;

Relatórios técnicos, apresentações em encontros tecnológicos e científicos, assim como a redação de artigos detalharão os resultados obtidos;

Um protótipo de osciladores caóticos acoplados para comunicação segura será produzido.

5. Aderência aos critérios de Priorização

Este Projeto será desenvolvido no Campus das Engenharias, da UFRPE, situado no Cabo de Santo Agostinho, no Programa de Pós-graduação em Engenharia Física. Assim como os cursos de graduação da Unidade Acadêmica do Cabo, esse programa de pós-graduação visa aprofundar relações técnico-científicas com o polo industrial de Suape, assim como com laboratórios do Porto Digital, onde parcerias de cooperação estão sendo implementadas.

Explicitamente os temas estratégicos para o desenvolvimento do Estado relacionados com o Desenvolvimento de Arranjos Produtivos Locais (APLs) são dois:

Metalmecânico De Suape

Porto Digital

O projeto está vinculado ao programa de pós-graduação em Engenharia Física, sediado na UACSA-UFRPE, pertencente à grande área de Materiais da CAPES.

Considerando que o Parque Tecnológico de Pernamubuco envolve empresas com sofisticados procedimentos tecnológicos, particularmente na região portuária de Suape, onde nossa instituição acadêmica está inserida, entendemos que a subvenção desse projeto se justifica no esforço de geração de conhecimento tecnológico no Estado, que beneficiem empresa de prestação de serviços de alta conteúdo tecnológico.

Atendemos aos critérios de priorização, de acordo com o Edital:

I. Reserva de bolsas para Cursos Novos

II. Apoio diferenciado à pós-graduação em Engenharias

6. Cronograma de Atividades

Atividades	1º Semestre	2º Semestre	3º Semestre	4º Semestre
Revisão e atualização bibliográfica	X	X	X	X
Disciplinas do Programa	X	X		
Montagem experimental de circuitos caóticos e/ou osciladores óticos	X	X	X	
Modelos para os osciladores acoplados. Simulações numéricos.	X	X	X	
Aquisição de dados e análise de resultados.		X	X	X
Comparação para adaptação/ajuste do modelo teórico.		X	X	X
Elaboração de artigos, trabalho para Conferência, etc			X	X
Redação da Dissertação			X	X
Defesa da Dissertação				X

7. Referências Bibliográficas

[1] - A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, (1996).

- [2] - S. Boccaletti, J. Kurths, G. Osipov, D. Valladares, and C. Zhou, "The synchronization of chaotic systems," *Phys. Rep.* **366**, 1 (2002).
- [3] - Atsushi Uchida et al. "Fast physical random bit generation with chaotic semiconductor lasers" *Nature Photonics*, **2**, 728 (2008).
- [4] - V. S. Afraimovich, N. N. Verichev, and M. I. Rabinovich, "Stochastic synchronization of oscillations in dissipative systems," *Radiophys. Quantum Electron.* **29**, 795 (1986).
- [5] - L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems". *Phys. Rev. Lett.* **64**, 821 (1990).
- [6] - K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications" *Phys. Rev. Lett.* **71**, 65 (1993).
- [7] - Apostolos Argyris et al. "Chaos-based communications at high bit rates using commercial fibre-optic links" *Nature* **438**, 343 (2005).
- [8] - Gilson F. de Oliveira Jr., Hugo L. D. de S Cavalcante, Orlando di Lorenzo, Martine Chevrollier, T. P. de Silans, and Marcos Oriá. "Tunable power law in the desynchronization events of coupled chaotic electronic circuits" *Chaos*, **24**, 013105 (2014).
- [9] - Gilson F. de Oliveira Jr., Martine Chevrollier, T. P. de Silans, Marcos Oriá and Hugo L. D. de Souza Cavalcante. "Trajectory-probed instability and statistics of desynchronization events in coupled chaotic systems". *Chaos* **25**, 113107 (2015).
- [10] - Gilson F. de Oliveira, Jr., Orlando Di Lorenzo, T P de Silans, Martine Chevrollier, Marcos Oriá and Hugo L. D. de Souza Cavalcante. "Local instability driving extreme events in a pair of coupled chaotic electronic circuits" *Phys. Rev. E* **93**, 062209 (2016).
- [11] - Gilson F. de Oliveira. "Estatística do dessincronismo intermitente entre circuitos elétricos caóticos" Tese de doutorado-UFPB (2016).
- [12] - Hugo Cavalcante, Marcos Oriá, Didier Sornette, Edward Ott, and Daniel J. Gauthier. "Predictability and Suppression of Extreme Events in a Chaotic System" *Phys. Rev. Lett.* **111**, 198701 (2013).
- [13] - Steven H. Strogatz. *Nonlinear Dynamics and Chaos*. Perseus Books, (1994).
- [14] - L. M. Pecora and T. L. Carroll, *Phys. Rev. A* **44**, 2374 (1991); W. L. Ditto and L. M. Pecora, *Sci. Am.* **269**, 62 (1993); K. M. Cuomo and A. V. Oppenheim, *Phys. Rev. Lett.* **71**, 65 (1993); K. M. Cuomo and A. V. Oppenheim, S. H. Strogatz, *IEEE Trans. Circ. Syst.* **40**, 626 (1993); U. Partitz, et al. *Phys. Rev. E* **53**, 4351 (1996).
- [15] - G. D. VanWiggeren and R. Roy, "Communication with Chaotic Lasers". *Science* **279**, 1198 (1998).
- [16] - D. J. Gauthier and J. C. Bienfang. "Intermittent Loss of Synchronization in Coupled Chaotic Oscillators: Toward a New Criterion for High-Quality Synchronization". *Phys. Rev. Lett.* **77**, 1751 (1996).
- [17] - Chen, Hsin-Chieh, Ben-Yi Liao, and Yi-You Hou. "Hardware implementation of Lorenz circuit systems for secure chaotic communication applications." *Sensors* **13**, 2494 (2013).
- [18] - K. M. Ibrahim et al. "Chaotic behaviour of the Rossler model and its analysis by using bifurcations of limit cycles and chaotic attractors" *J. Phys.: Conf. Ser.* **1003** 012099 (2018).
- [19] - L. Kocarev et al. "Experimental demonstration of secure communications via chaotic synchronization". *Inter. J. of Bifurc. and Chaos* **2**, 709 (1992).
- [20] - Y. Lu, X. Huang, S. He, D. Wang, and B. Zhang. "Memristor Based van der Pol oscillation circuit". *Inter. J. of Bifurc. and Chaos* **24**, 1450154 (2014).
- [21] - Z. Wei, et al. "Hidden hyperchaos and electronic circuit application in a 5D self-exciting homopolar disc dynamo." *Chaos* **27**, 033101 (2017).
- [22] - M. P. Kennedy, "Three Steps to Chaos" part I. *IEEE Trans. Circuits and Syst.* **40**, 641 (1993); _ part II, **40**, 657 (1993).
- [23] - M. Shinriki, M. Yamamoto, and S. Mori, "Multimode Oscillations in a Modified Van Der Pol Oscillator Containing a Positive Nonlinear Conductance" *Proc. IEEE* **69**, 394 (1981).