UNIVERSIDADE FEDERAL DE GOIÁS
PROGRAMA DE PÓS-GRADUAÇÃO EM
ENGENHARIA ELÉTRICA
E DE COMPUTAÇÃO

CORINDA: QUEBRANDO HASHES DE SENHAS CONCORRENTEMENTE COM A LINGUAGEM DE PROGRAMAÇÃO GO

Bernardo Araujo Rodrigues

[UFG] & [EMC]
[Goiânia - Goiás - Brasil]
23 de janeiro de 2018

UNIVERSIDADE FEDERAL DE GOIÁS
PROGRAMA DE PÓS-GRADUAÇÃO EM
ENGENHARIA ELÉTRICA
E DE COMPUTAÇÃO

CORINDA: QUEBRANDO HASHES DE SENHAS CONCORRENTEMENTE COM A LINGUAGEM DE PROGRAMAÇÃO GO

Bernardo Araujo Rodrigues

Dissertação apresentada a Banca Examinadora como exigência parcial para a obtenção do título de Mestre em Engenharia Elétrica e de Computação pela Universidade Federal de Goiás (UFG), Escola de Engenharia Elétrica, Mecânica e de Computação (EMC), sob a orientação do Prof. Dr. Wesley Pacheco Calixto.

[UFG] & [EMC]
[Goiânia - Goiás - Brasil]
23 de janeiro de 2018

Dados Internacionais de Catalogação na Publicação (CIP)
Sistemas da Bibliotecas da UFG, GO - Brasil

C331s Rodrigues, Bernardo Araujo, 31/07/90.
Corinda: Quebrando *Hashes* de Senhas Concorrentemente com a Linguagem de Programao Go [manuscrito]/ Bernardo Araujo Rodrigues. – [Goiânia - Goiás - Brasil]: [UFG] & [EMC], 23 de janeiro de 2018.
38 f. : il.

Orientador: Wesley Pacheco Calixto - UFG

Dissertação - Universidade Federal de Goiás - UFG, Escola de Engenharia Elétrica, Mecânica e de Computação - EMC

Inclui bibliografia.

1.Senhas - Teses. 2.*Hashes* - Teses. 3.Segurança da Informação - Teses. I. Calixto, Wesley Pacheco; II. Universidade Federal de Goiás. Programa de Pós-Graduação em Engenharia Elétrica e de Computação. III. Corinda: Quebrando *Hashes* de Senhas Concorrentemente com a Linguagem de Programao Go

CDU 000.0.000:000.0

"Escreva aqui a epígrafe."

Escreva aqui o nome do autor da epígrafe

A todas as pessoas que me acolheram de alguma forma. Entes e amigos queridos que acreditaram em mim. A eles dedico este nosso trabalho.

AGRADECIMENTOS

AgradeÃ§o ao orientador e amigo Wesley Pacheco Calixto, por sua dedicaÃ§Ã£o e compreensÃ£o. Por ter acreditado em mim desde o inÃcio, e ter permitido que eu seguisse o caminho onde pude florescer.

Aos colegas do NExT (Nucleo de Estudos Experimentais e Tecnologicos), pelo companheirismo, dedicaÃ§ao e amizade.

A minha famÃlia, pelo amor e incentivo incondicional, seja em momentos de dificuldade ou de alegria.

Aos colegas de trabalho e amigos da Data Traffic, pela compreensÃ£o, incentivo, e risadas.

A CAPES pelo aporte para o desenvolvimento deste trabalho.

RESUMO

Escreva aqui o resumo do seu trabalho...

CORINDA: CRACKING PASSWORD HASHES WITH GO PROGRAMMING LANGUAGE

ABSTRACT

Write here the abstract of your work ...

SUMÁRIO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE TABELAS

Pág.

LISTA DE SÍMBOLOS

Coloque seus símbolos aqui conforme exemplo:

N_m	–	Horizonte do modelo
N_u	–	Horizonte de controle
N_y	–	Horizonte de predição
α	–	Taxa de amortecimento da referência
ω	–	Trajetória referência

LISTA DE ABREVIATURAS E SIGLAS

Coloque suas abreviaturas aqui conforme exemplo.

AG	–	Algoritmo Genético
CA	–	Corrente Alternada
CC	–	Corrente Contínua
CMD	–	Controle por Matriz Dinâmica
CPBM	–	Controle Preditivo Baseado em Modelos
CPBML	–	Controle Preditivo Baseado em Modelo Linear
CPBMNL	–	Controle Preditivo Baseado em Modelo Não Linear
CPPNL	–	Controle Preditivo Prático Não Linear
CPG	–	Controle Preditivo Generalizado
IAE	–	Integral do valor absoluto do erro
ISE	–	Integral do erro quadrático
ITAE	–	Integral do valor absoluto do erro multiplicado pelo tempo
MCC	–	Motor de Corrente Contínua
MIMO	–	Sistemas Multivariáveis
PID	–	Proporcional, Integral e Derivativo
SISO	–	Sistemas Monovariáveis

CAPÍTULO 1

INTRODUÇÃO (xx/xx/2017)

- Frase introdutória
- Estado da arte
- Justificativa
- Hipótese
- Objetivos
- Estrutura do trabalho

CAPÍTULO 2

CONTROLE MODERNO (xx/xx/2017)

2.1 Controle clássico e moderno

Aqui você deve escrever umas 15 linhas ou mais sobre a diferença entre controles clássicos e controle moderno. Termine citando os controladores por modos deslizantes e o preditivo.

2.2 Controle por modos deslizantes

Aqui você deve falar do controle por modos deslizantes.

2.2.1 Sintonia do controlador por modos deslizantes

Aqui você deve dar ênfase nas variáveis manipuladas do controle por modos deslizantes.

2.3 Controle preditivo baseado em modelos

Aqui você deve falar do controle preditivo baseado em modelos.

2.3.1 Sintonia do controlador preditivo baseado em modelos

Aqui você deve dar ênfase nas variáveis manipuladas do controle preditivo baseado em modelos.

2.4 Considerações

Veja as Figura 2.1 e Figura 2.2, que servem de exemplo para inserção figuras.

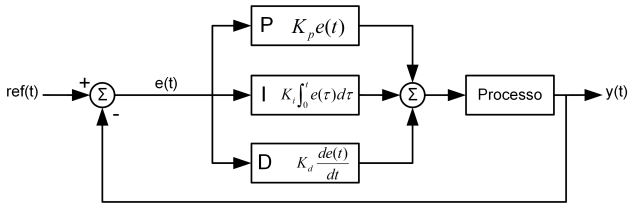

Figura 2.1 - Partes construtivas do motor de corrente contínua.

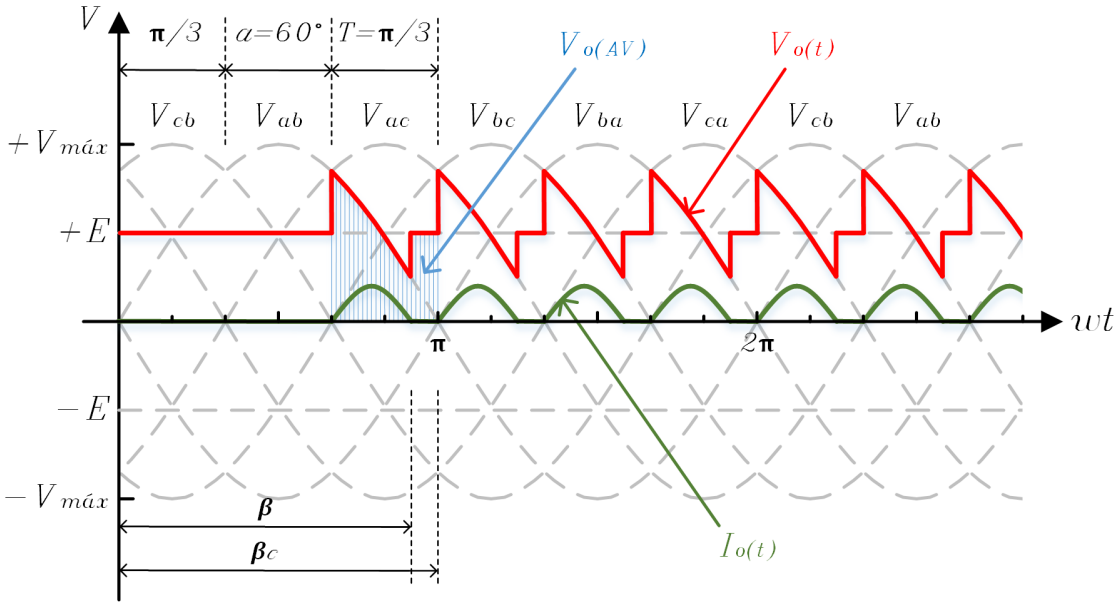

Figura 2.2 - Ligações de máquinas CC: (a) excitação independente, (b) em derivação, (c) em série, (d) composta.

CAPÍTULO 3

SISTEMA, MODELO E OTIMIZAÇÃO (xx/xx/2017)

3.1 Sistema

Aqui você deve definir o que é sistema. Pode utilizar o livro do Medina e outros.

3.2 Modelo

Aqui você deve definir o que é modelo. Pode utilizar o livro do Medina e outros.

3.2.1 Construção da modelagem do motor de corrente contínua

Aqui você deve falar somente o necessário para que seu leitor entenda o que é o modelo do motor de corrente contínua, dado as expressões que o define.

3.3 Processo de otimização

Aqui você deve falar sucintamente sobre o processo de otimização. Pegue o material comigo.

3.3.1 Otimização aplicada ao controle do motor de corrente contínua

Aqui você fala do trabalho do Márcio, Douglas e Rafael, descrevendo o que eles fizeram como processo de otimização.

3.4 Considerações

Veja as expressões (3.1) e (3.2), que servem de exemplo de como inserir expressões matemática.

$$v_a(t) = R_a \cdot i_a(t) + L_a \frac{di_a(t)}{dt} + e_g(t) \tag{3.1}$$

$$v_f(t) = R_f \cdot i_f(t) + L_f \frac{di_f(t)}{dt} \tag{3.2}$$

CAPÍTULO 4

METODOLOGIA (xx/xx/2017)

4.1 Construção e configuração do sistema

4.2 Modelagem e simulação

4.3 Aplicação do processo de otimização na sintonia dos controladores

4.4 Análise de desempenho entre os controladores

4.5 Considerações

CAPÍTULO 5

RESULTADOS (xx/xx/2018)

Se qualificação, **RESULTADOS PRELIMINARES**. Se defesa final, apenas **RESULTADOS**.

Na mesma sequência da metodologia.

5.1 Construção da bancada e do modelo

5.2 Resultado de simulação

5.2.1 Otimização aplicada na sintonia dos controladores

5.3 Resultado de bancada

5.4 Comentários

Veja as Tabela 5.4 e Tabela 5.2, que servem de exemplo de como inserir tabela. Caso necessário, baixe o aplicativa *La Table* para lhe auxiliar na formatação de tabelas.

Tabela 5.1 - Parâmetros da expressão NARMAX do modelo do sistema.

Parâmetro	**Valores**
n_y	$\begin{bmatrix}1\end{bmatrix}$
n_u	$\begin{bmatrix}1\end{bmatrix}$
t_d	$\begin{bmatrix}1\end{bmatrix}$
P	$\begin{bmatrix} 0.0011 & -0.0032 \\ 3.97 \cdot 10^{-6} & 0.0872 \end{bmatrix}$
L'	$\begin{bmatrix}928.9889 & 14.3086\end{bmatrix}$
d	$\begin{bmatrix}1338.6041\end{bmatrix}$
Q	$\begin{bmatrix} 0.0011 & -0.0032 \\ 3.97 \cdot 10^{-6} & 0.0872 \end{bmatrix}$
A	$\begin{bmatrix}-248.3902 & -39.8336 & 27.1611 & 12.6842 & 28.3081\end{bmatrix}$
B	$\begin{bmatrix} -2.0417 & 4.9036 & 3.2205 & 4.0505 & 5.7625 \\ 0.9853 & 1.0024 & -0.9176 & -0.8418 & 0.4071 \end{bmatrix}$
C	$\begin{bmatrix}8.9914 & -8.2400 & -6.0503 & -4.3234 & -1.7206\end{bmatrix}$

Tabela 5.2 - Parâmetros otimizados para o controlador PID.

Parâmetro	K_P	K_I	K_D
Valores	$0,01241$	$0,000002$	$0,00641$

CAPÍTULO 6

CONCLUSÃO (xx/xx/2018)

Se qualificação, **CONCLUSÃO PARCIAL**. Se defesa final, apenas **CONCLUSÃO**.

6.1 Contribuições do Trabalho

As contribuições podem assim ser descritas:

Artigos em revista:

Artigos em congresso:

Se qualificação:

6.2 Continuação do trabalho

Se defesa final:

6.3 Sugestões para Trabalhos Futuros

REFERÊNCIAS BIBLIOGRÁFICAS

GLOSSÁRIO

Condutivímetro - é um medidor digital portátil que mensura a condutividade elétrica do solo diretamente "*in loco*".

Data Logger - é um coletor de dados também chamado de datalogger ou gravador de dados. É um dispositivo eletrônico que registra os dados ao longo do tempo ou em relação a uma localização, construído com sensores externos. São baseados em um processador digital com memórias internas para armazenamento de dados. São de uso geral para uma gama de aplicações em dispositivos de medição específicos, podem ser programáveis.

GPS - é um sistema de navegação por satélite que fornece a um aparelho receptor móvel a posição do mesmo, assim como informação horária, sob todas quaisquer condições atmosféricas, a qualquer momento e em qualquer lugar na Terra, desde que o receptor se encontre no campo de visão de quatro satélites GPS.

Neossolo Regolítico - são tipos de solos que apresentam textura arenosa e baixa capacidade de adsorção de nutrientes, quando comparado com solos argilosos, possui baixo teor de matéria orgânica e nitrogênio que diminuem, após alguns anos de uso agrícola.

Nitossolo Vermelho - são solos minerais, não-hidromórficos, apresentando cor vermelho-escura tendendo à arroxeada. São derivados do intemperismo de rochas básicas e ultrabásicas, ricas em minerais ferromagnesianos. Uma característica peculiar é que esses solos, como os Latossolos Roxos, apresentam materiais que são atraídos pelo imã. Seus teores de ferro ($Fe2O3$) são elevados (superiores a 15%).

Plintossolo Pétrico Concrecionário - são solos que ocorrem em áreas baixas e nas bordas das chapadas, constituindo geralmente por solos pobres em nutrientes. A origem de concreções ferruginosas nos solos tem sido atribuída, de forma generalizada, às condições de variações sazonais do lençol freático. Este, inicialmente elevado, propicia a redução do ferro com a sua retirada parcial do sistema, mobilização, transporte e concentração. Posteriormente, em épocas secas, a oxidação forma plintitas constituídas por mistura de argila pobre em C orgânico e rica em ferro e alumínio, segregada sob a forma de manchas vermelhas, que com a retirada do lençol freático, apresentam endurecimento constituindo concreções ferruginosas ou petroplintitas.

PVC - é feito a partir de repetidos processos de polimerização que convertem hidrocarbonetos, contidos em materiais como o petróleo, em um único composto chamado polímero. O vinil é formado basicamente por etileno e cloro. Por

uma reação química, o etileno e o cloro combinam-se formando o dicloreto de etileno, que por sua vez é transformado em um gás chamado *VCM* (Vinyl chloride monomer, em português cloreto de vinila). O passo final é a polimerização, que converte o monómero num polímero de vinil, que é o *PVC*, ou simplesmente vinil, contém, em peso, 57% de cloro (derivado do cloreto de sódio - sal de cozinha) e 43% de eteno (derivado do petróleo).

TC scan - é uma tomografia computadorizada (*TC*), originalmente apelidada tomografia axial computadorizada (*TAC*), é um exame complementar de diagnóstico por imagens tridimensionais, que consiste numa representação de uma secção ou fatia do estudo. É obtida através do processamento por computador de informação recolhida após expor o objeto estudado a uma sucessão de raios X. Seu método principal é estudar a atenuação de um feixe de raios X durante seu trajeto através de um segmento do objeto estudado; no entanto, ela se distingue da radiografia convencional em diversos elementos.