Localização Espacial Através de Pistas Auditivas: Um Estudo Comparativo entre Diferentes Tipos de Som

Bolsista: Alyson Matheus de Carvalho Souza (UFRN)
Orientador: Jauvane Cavalcante de Oliveira (LNCC/NCT)
Co-Orientador: Selan Rodrigues dos Santos (UFRN)

Resumo

A maioria dos sistemas de RV se preocupam em enfatizar o sentido da visão, deixando de lado, na maior parte dos casos, a audição. Nesse projeto procuramos estudar os diferentes tipos de som que podem ser explorados e seus impactos em uma aplicação de RV. Através de um ambiente sem pistas visuais, testaremos a capacidade dos usuários de se orientar e encontrar objetos apenas a partir dos sons que eles emitem. Isso deverá ser feito utilizando sistemas de som surround, stereo e mono, assim como alto-falantes e fones de ouvido. O projeto visa fazer um estudo comparativo entre essas variáveis.

Objetivos

O projeto tem como objetivo realizar testes com usuários em 6 situações diferentes. Som mono, a partir de alto-falantes; som stereo a partir de alto-falantes; som surround a partir de alto-falantes; som mono a partir de fones de ouvido; som stereo a partir de fones de ouvido e som surround a partir de fones de ouvido. Configuraremos experimentos para testar a capacidade do usuário de identificar fontes que estão emitindo sons específicos utilizando cada uma das situações anteriormente citadas. Depois, há a necessidade de um estudo comparativo sobre os resultados obtidos a cerca dos experimentos realizados.
O projeto também teve como objetivo o estudo dos diferentes tipos de áudio, assim como dos diferentes dispositivos que podem ser utilizados na emissão dos mesmos. Esse estudo foi feito com objetivo de gerar definições claras do que seria o som surround, o som stereo, o som mono e até mesmo o som 3D, ou som espacializado. Já na parte dos dispositivos de áudio, foram estudados os fones de ouvido e também as diversas configurações de som, desde o som mono emitido através de um único alto-falante até o som Surround 10.2, que se utiliza de 12 alto-falantes para garantir o efeito desejado.
O objetivo final do projeto é comprovar ou não a hipótese levantada de que quanto mais elaborado o som, melhor será a orientação do usuário dentro do ambiente virtual.

Desenvolvimento do Projeto

O projeto foi desenvolvido em diferentes fases de trabalho, fazendo com que cada parte fosse estudada de uma vez. As partes desenvolvidas e as que ainda devem ser feitas são as seguintes:

Estudo das diferentes técnicas sonoras: Nessa parte do trabalho, foi feito o estudo acima citado das diferentes técnicas disponíveis, assim como suas vantagens, desvantagens e meios de implementação. Também foi feito um estudo para saber se seria possível ou não, na questão de equipamentos, se utilizar das técnicas para fazer o estudo comparativo.

Estudo das tecnologias disponíveis para a geração do programa de teste: Nessa parte foram estudadas algumas tecnologias para a geração de um programa que trabalhasse com áudio

surround, stereo e mono. O Unity terminou sendo a plataforma escolhida. Foram feitos estudos sobre as funcionalidades do Unity em relação a áudio e também quão longe poderíamos ir utilizando-se deste programa.

Desenvolvimento do programa de testes: Nessa fase do projeto foi desenvolvido o programa de teste. O programa consiste em varias caixas identicas, distribuidas atraves de um cenário, cada uma emitindo um instrumento diferente da mesma música. O programa coloca o usuário no centro do quadrado formado por essas caixas e emite mensagens indicando qual instrumento ele quer que o usuário encontre. Com isso, o usuário deve se utilizar das pistas sonoras para encontrar a caixa correta e a selecionar, utilizando o sistema WASD + Mouse e a barra de espaço para seleção.
Testes com Usuário: Nessa fase final do projeto, os testes com usuário serão feitos. Essa parte ainda não foi concluída, mas está agendada para ser até o final do mês. Os testes indicarão qual dos esquemas será mais eficiente para ajudar o usuário a se orientar através das pistas sonoras. Realizaremos estes submetendo os participantes a uma mesma tarefa em três configurações diferentes. Os participantes serão divididos em dois grupos. O primeiro grupo testará os 3 tipos de som utilizando fones de ouvido, já o segundo, utilizará o mesmo esquema, porém, com alto-falantes. Após a conclusão do experimento, os participantes serão submetidos a um questionário subjetivo para avaliar a participação do participante no experimento. O experimento também irá colher dados como o tempo, a distancia percorrida e a taxa de acertos até a conclusão do experimento. Após colhermos os dados do experimento, será realizada uma analise estatística deles para assim podermos chegar a conclusões sobre a hipótese levantada. Buscaremos descobrir, dentro de cada grupo, qual configuração se mostrou mais eficiente, ou mesmo se não houve diferença entre os resultados apresentados, em relação a tempo, taxa de acerto e também distancia percorrida. Também faremos comparações entre os grupos, para tentarmos encontrar alguma diferença significativa entre o fone de ouvido e os alto-falantes, na questão performance.

Conclusões

Como foi dito, a parte final do projeto, que envolve os testes com o usuário ainda não foi executada. Apenas após essa fase seremos capazes de concluir se houve ou não corretude na hipótese levantada. Mesmo assim, com o estudo que já foi realizado foi possível ver as diferenças que existem entre os variados tipos de som. As diferenças entre mono, stereo, surround e som espacializado são notáveis e devem sempre ser levadas em conta na hora de escolher qual utilizar em um sistema de RV.

Sistema da Informação Sistema de Monitoramento de Gerência e de Segurança - SiMGeS

Bolsista: Carlos Leonardo Souza Cardozo (Universidade Estácio de Sá)
Orientador: Luis Rodrigo de Oliveira Gonçalves (LNCC/MCT)

Resumo

Desenvolvimento do Portal MHOLline: Sistema Computacional para Modelagem Comparativa em Genômica Estrutural

Bolsista: Damásio Antonio Alves Ferreira (ISTCC-P)
Orientador: Laurent E. Dardenne (LNCC/MCT)
Co-Orientadora: Priscila V. Z. Caprilles Goliatt (Doutorado/LNCC)

Resumo
O aumento contínuo do número de projetos de sequenciamento de genomas juntamente com as limitações na predição experimental de estruturas protéicas, têm sido apontados como principais motivos para a busca de métodos teóricos capazes de predizer a estrutura tridimensional (3D) de proteínas em grande escala. A partir desta necessidade, ferramentas como o MHOLline, um *workflow* para a predição de estruturas de proteínas em grande escala, são de alta relevância, pois possibilitam o fácil acesso e uso integrado de ferramentas voltadas para a modelagem comparativa.

A primeira versão do MHOLline foi desenvolvida e lançada juntamente com a elaboração da tese de doutorade de Shaila C. S. Rössle no ano de 2004, pela Universidade Federal do Rio de Janeiro, constando apenas de um conjunto de código executáveis via linha de comando. Neste presente trabalho, visamos dar continuidade ao desenvolvimento do MHOLline de maneira que o mesmo viesse a ser amplamente utilizado pela comunidade cientifica, de forma que os usuário pudessem remotamente iniciar os seus processos e recuperar os resultados gerados de forma simples.

Nas etapas deste projeto, foram desenvolvidas as interfaces gráficas (mholweb) do portal MHOLline (disponível em: http://www.mholline.lncc.br), um banco de dados (mholdb) para gerenciamento de resultados, os códigos de execução do *workflow* (mholline) e uma interface de administração do sistema para gerenciamento de contas de usuários, atualizações e *backups* do sistema, e acompanhamento estatístico do *workflow*. O MHOLline foi aprimorado, melhorando as formas de acesso aos programas que já faziam parte deste processo, e integrando novas ferramentas como o ECNGet.

Neste último ano, o portal MHOLline vem sendo usado por grupos de pesquisa das regiões Norte, Nordeste e Sudeste do Brasil, sempre apresentando bom desempenho, e já analisou mais de 60.000 sequências protéicas. Os próximos passos para este trabalho são: desenvolver um aplicativo de instalação automatizada do MHOLine e realizar a paralelização do código fonte para a sua instalação no cluster do Laboratório Nacional de Computação Científica (LNCC/MCT).

Algoritmo Quântico com Espaço de Dados Polinomial para o Problema do Subgrupo Oculto sobre Grupos Metacíclicos

Bolsista: Daniel Gaspar Gonçalves de Souza (UCP)
Orientador: Renato Portugal (LNCC/MCT)
Co-Orientador: Demerson Nunes Gonçalves (Bolsista PCI/LNCC)

Resumo

O Problema do Subgrupo Oculto (PSO) consiste em determinar um subgrupo H de um grupo finito G oculto por um função que é constante nas classes laterais de H e distinta nas diferentes classes laterais. Para ser eficiente, um algoritmo para o PSO tem que ser polilogaritmo na ordem de G. É conhecido que se o grupo G é abeliano então o PSO pode ser eficientemente resolvido por um computador quântico, enquanto, nenhuma solução geral é conhecida para o caso de grupos não-abelianos [1].

Neste trabalho, nós apresentamos um algoritmo quântico em tempo sub-exponencial com espaço de dados polinomial para o PSO sobre o grupo $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$, onde p, q são números primos distintos e r, s inteiros positivos arbitrários. Usando a classificação dos subgrupos de $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$, nós simplificamos o PSO ao problema de encontrar subgrupos cíclicos da forma $\langle x^a y^{q^j} \rangle$, onde $a \in \mathbb{Z}_{p^r}$, $x = (1,0)$, $y = (0,1)$ e j um inteiro positivo $0 \leq j \leq s$ conhecido. Existem $O(p^r)$ subgrupos desta forma, assim, uma busca exaustiva do valor de a é ineficiente.

Fazendo uso da transformada de Fourier abeliana e combinando as idéias apresentadas em Kuperberg [3] e Regev [4] para o PSO no grupo diedral, obtemos um procedimento quântico que gera estados

$$|0\rangle + e^{\frac{2\pi i a^\gamma ak}{p^r}}|1\rangle,$$

onde $0 \leq \gamma \leq \lceil \log p^r \rceil$ e $k \in \mathbb{Z}_{p^r}$ é um número uniformemente randômico. Agora, utilizamos um certo procedimento de medida e combinação. Este procedimento utiliza $l+4$ estados da forma $|0\rangle + e^{\frac{2\pi i a^\gamma ak}{p^r}}|1\rangle$, onde $l = O\left(\left\lceil \sqrt{\log p^r - 1} \right\rceil\right)$, e retorna um novo estado $|0\rangle + e^{\frac{2\pi i a^\gamma ab}{p^r}}|1\rangle$, onde os l bits mais significativos de b são iguais a zero.

Executando esta rotina l vezes, obtemos com probabilidade constante um estado da forma

$$|\psi_1^{2^\gamma a p^r}\rangle := |0\rangle + e^{\frac{2\pi i a^\gamma a}{p^r}}|1\rangle.$$

Agora, aplicando a transformada de Fourier inversa ao conjunto de estados quânticos $\{|\psi_1^{2^\gamma a p^r}\rangle, \gamma = 0 \ldots, \lceil \log p^r \rceil\}$, obtemos o valor de a com alta probabilidade.

Abstract

In this paper we present a quantum algorithm with time complexity $2^{O(\sqrt{r \log p})}$ and polynomial space that solves the hidden subgroup problem (HSP) on the semidirect product

of cyclic groups $\mathbb{Z}_{p^r} \rtimes \mathbb{Z}_{q^s}$, where p, q are any odd prime numbers and r, s are any positive integers. Our approach uses the ideas behind Kuperberg and Regev's algorithm for the dihedral groups with a reduction procedure to cyclic subgroups present in some algorithms in the literature. As far as we know, this is the first subexponential-time quantum algorithm with polynomial space for the HSP in this class of groups.

Referências

[1] C. Lomont, "Hidden Subgroup Problem - Review and Open Problems", *ArqXiv preprint quant-ph/0411037*, 2004.

[2] D. N. Gonçalves, R. Portugal, C.M.M. Cosme, "Solutions to the Hidden Subgroup Problem on some Metacyclic Groups", *Theory of Quantum Computation, Communication and Criptography. Waterloo. Publicação: Lecture Notes in Computer Science (LNCS)*, V. 5906, 2009.

[3] G. Kuperberg, "A subexponential-time quantum algorithm for the dihedral hidden subgroup problem", *arXiv:quant-ph/0302112v2*, 2004.

[4] O. Regev, "A Subexponential Time Algorithm for the Dihedral Hidden Subgroup Problem with Polynomial Space", *arXiv:quant-ph/0406151v1*, 2004.

Aplicações de Maple em Geometria Analítica

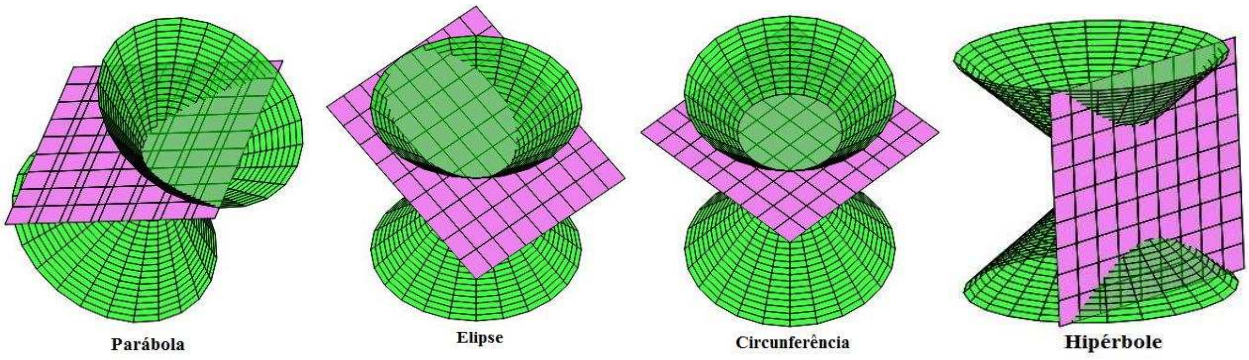
Bolsista: Débora Carolina Kreischer (CEDERJ-UFF)
Orientador: Renato Portugal (LNCC/MCT)

Resumo

Este resumo tem como objetivo apresentar as seguintes curvas no plano, chamadas de *secções cônicas* ou simplesmente *cônicas*: *parábola, elipse, circunferência* e *hipérbole.*

Para isto, foi utilizado o software de computação algébrica *Maple*, que permite a manipulação das cônicas, isto é, através de linhas de comando onde é possível definir cada cônica através de seus elementos, de acordo com a sintaxe de cada comando, além de desenhá-las com bastante precisão. No Maple existem *pacotes*, que são agrupamentos de comandos com fins específicos. No caso das cônicas, foi utilizado o pacote *geometry*, que define diversos objetos geométricos no plano. Para carregá-lo, basta inserir no Maple o comando > with(geometry);.

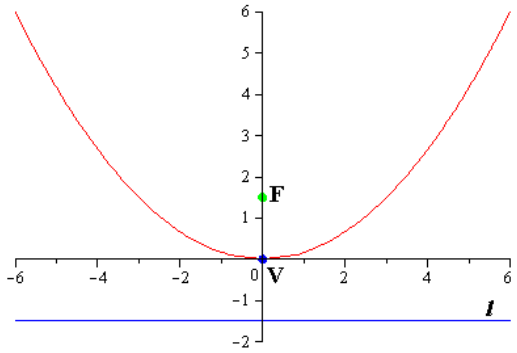
Uma secção cônica é uma curva que resulta da intersecção entre um plano e um duplo cone circular reto, sendo que esse plano não passa pelo vértice do cone. As figuras abaixo ajudam a visualizar tais curvas:



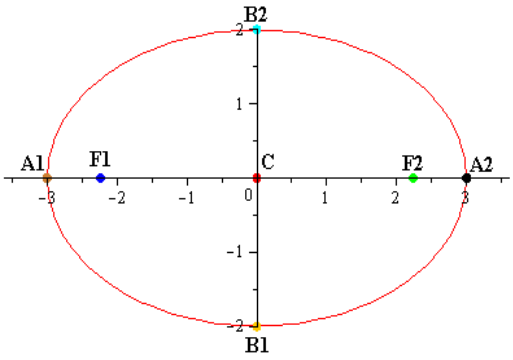
Na área da Geometria Analítica, as cônicas são definidas como lugares geométricos no plano. Isto significa descrever o conjunto dos pontos do plano que satisfazem uma propriedade específica, dependendo apenas do conceito de distância entre pontos ou entre retas e pontos, a saber, respectivamente:

$d(A,B)=\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}$, onde $A=(x_1,y_1)$ e $B=(x_2,y_2)$, e $d(P,r)=\dfrac{|ax_p+by_p+c|}{\sqrt{a^2+b^2}}$, onde *a*, *b* e *c* são os coeficientes da equação da reta *r* dada na forma geral $ax+by+c=0$ e $P=(x_p,y_p)$. Dessa forma, pode-se obter a definição de cada cônica:

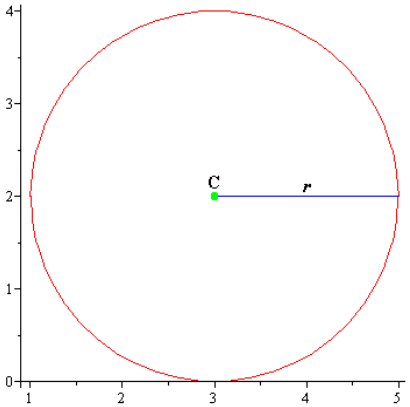
Parábola: é o lugar geométrico dos pontos *P* do plano equidistantes da reta *l* (diretriz) e do ponto *F* (foco). Em termos matemáticos, $Parábola = \{P \mid d(P,F) = d(P,l)\}$.



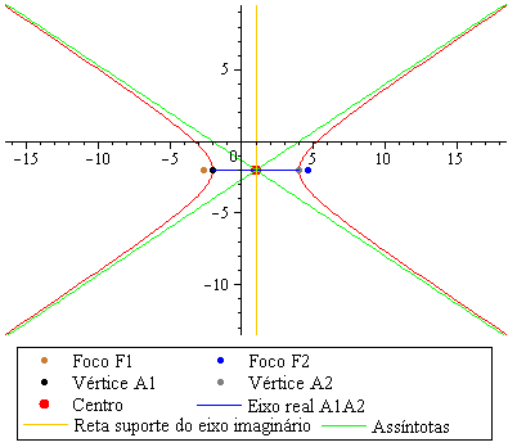
Elipse: é o lugar geométrico dos pontos do plano cuja soma das distâncias aos pontos *F1* e *F2* (focos) é constante. Escrevendo essa constante como *2a*, temos:
$Elipse = \{P \mid d(P,F1) + d(P,F2) = 2a\}$.



Circunferência: é o lugar geométrico dos pontos do plano cuja distância ao ponto *C* (centro) é *r* (raio). Em termos matemáticos, $Circunferência = \{P \mid d(P,C) = r\}$.



Hipérbole: é o lugar geométrico dos pontos do plano cujo valor absoluto da diferença das distâncias aos pontos *F1* e *F2* (focos) é uma constante positiva menor do que a distância entre os focos. Escrevendo essa constante como *2a*, temos: $Hipérbole = \{P \mid |d(P,F1) - d(P,F2)| = 2a\}$.



Para definir no Maple cada cônica, utilizam-se os comandos listados abaixo:

Parábola:
> parabola(p,['focus'=fou,'vertex'=ver,n);
> parabola(p,['directrix'=dir,'focus'=fou,n);
> parabola(p,eqn,n);

Elipse:
> ellipse(e,['foci'=foi,'MajorAxis'=lma,n);
> ellipse(e,['foci'=foi,'MinorAxis'=lmi,n);
> ellipse(e,['foci'=foi,'MajorAxis'=ep1,'MinorAxis'=ep2,n);
> ellipse(e,['directrix'=dir,'focus'=fou,'eccentricity'=ecc],n);
> ellipse(e,eqn,n);

Circunferência:
> circle(c,[P,rad],n,'centername'=m);
> circle(c,eqn,n,'centername'=m);

Hipérbole:
> hyperbola(h,['foci'=foi,'vertices'=ver,n);
> hyperbola(h,['foci'=foi,'distancev'=disv,n);
> hyperbola(h,['vertices'=ver,'distancef'=disf,n);
> hyperbola(h,['directrix'=dir,'focus'=fou,'eccentricity'=ecc],n);
> hyperbola(h,eqn,n);

Para desenhar cada cônica, usa-se o comando > draw(nome atribuído a cônica); e para mostrar os detalhes de uma determinada cônica, utiliza-se o comando > detail(nome atribuído a cônica);.

Durante o período de estudos, foi elaborada uma apostila didática sobre as cônicas. A mesma foi apresentada no momento da apresentação do poster e distribuída no formato pdf.

Integral de Itō e seu Poder de Aplicação

Bolsista: Diego dos Reis Oliveira (UCP)
Orientador: Jack Baczynski (LNCC/MCT)

Resumo

A partir da caracterização dos *processos estocásticos*, é apresentada a integração dos processos estocásticos fixando-se uma dada realização, isto é, uma dada trajetória. Isto implica o estabelecimento da integral de uma função f(t) em relação a outra g(t), o que impõe condições não satisfeitas pela *integral de Riemann* tradicional; é estabelecida então a *integral de Riemann-Stieltjes*, com base nas chamadas *somas de Riemann-Stieltjes*. E, embora não possa ser obtida a integração da trajetória de certos processos estocásticos tais como o *movimento browniano*, o limite no *espaço de funções* L^2 da soma de Riemann-Stieltjes das variáveis aleatórias do processo propicia o caminho para a obtenção de uma integral.

No trabalho são enunciadas três das grandes contribuições do matemático japonês *Kiyoshi Itō* (伊藤 清; 1915 –2008) para o estabelecimento da área do *cálculo estocástico*: a *integral estocástica de Itō*, a *partição* e o *lema de Itō*. Esse último lema fornece, para o cálculo estocástico, uma regra análoga à *regra da cadeia* no cálculo tradicional.

São citadas as *difusões* e as *equações diferenciais parciais estocásticas* como ferramentas teóricas com um vasto campo de aplicação, por exemplo a matemática financeira, e que motivam um estudo aprofundado do cálculo estocástico.

Desenvolvimento de Software em MatLab para Otimização estrutural utilizando Derivada Topológica

Bolsista: Diego Esteves Campeão (UCP)
Orientador: Antonio André Novotny (LNCC/MCT)

Resumo

O trabalho que vem sendo desenvolvido nos últimos anos teve por objetivo o desenvolvimento teórico de um método de otimização para o problema de flexão elástica de placas de Kirchhoff baseado no conceito de Derivada Topológica. O presente trabalho consiste na implementação computacional da teoria para a obtenção de resultados numéricos utilizando o programa MatLab. Além da implementação do elemento finito de placa em MatLab o trabalho tem por objetivo o desenvolvimento de uma interface gráfica para um programa de otimização para os problemas de elasticidade, transferência de calor e, futuramente, placas de Kirchhoff.

Modelo Binomial de Não-Arbitragem para a Precificação de Ativos Financeiros

Bolsista: Estevão Rosalino Junior (UFRRJ)
Orientador: Jack Baczynski (LNCC/MCT)

Resumo

Este trabalho tem como objetivo apresentar o ***Modelo Binomial de Não-Arbitragem Para a Precificação de Ativos Financeiros***, que preserva todos os aspectos da teoria dos casos multi-períodos e a tempo contínuo. É um assunto introdutório ao estudo do cálculo estocástico aplicado à finanças.

Começa-se com um breve histórico sobre a aplicação do cálculo estocástico em finanças, que passa por nomes importantes na evolução deste estudo, tais como *Fischer Black* e *Myron Scholes*. Toma-se a construção do modelo, sendo necessária a apresentação dos conceitos de ***Arbitragem*** e ***Derivativos***, chegando-se então a precificação de um derivativo a partir da sua replicação em uma negociação no mercado de ações (*stock market*) e no mercado monetário (*money market*). A partir deste método, encontramos o preço justo para um derivativo. Este preço faz com que o derivativo seja uma estratégia de negociação sem arbitragem, o que constitui uma característica fundamental para um mercado eficiente.

Programando Aplicativos com Cuda/C++ e PyCuda/Python

Bolsista: Fabricio Gomes Vilasbôas (ISTCC-P)
Orientador: Paulo Roberto Godoy Bordoni (SAAFRH)

Resumo

Este trabalho propõe apresentar um algoritmo que possa, de forma eficiente, achar as raízes de qualquer polinômio, e para tal, utilizamos placas GP-GPU para obter mais velocidade no processo.
GP-GPU, General Purpose Graphic Processing Unit, estão vindo com grande força quando se diz respeito a processamento de auto desempenho, por possuírem vários processadores que podem ser utilizados para cálculos matemáticos. Para o desenvolvimento deste algoritmo fizemos uso de placas GTX 285 e Tesla C1060 ambas da fabricante Nvidia.
Tomamos como base o Algoritmo da Bissecção e desenvolvemos um algoritmo que intitulamos de Algoritmo da "plurissecção", por que ele divide o espaço de busca no número máximo de threads que possa ser utilizado pela GP-GPU.
O funcionamento do algoritmo é da seguinte forma:

1. Determina-se um espaço de busca, por exemplo, determinado entre o ponto 'a' e o ponto 'b';
2. O Δx é dado pela razão entre a diferença entre 'b' e 'a' e o número máximo de threads suportado pela GP-GPU, onde Δx é a distância entre os pontos no intervalo 'ab';
3. Calcula-se, então, o valor da função em cada ponto e é retornado, apenas, o sinal daquele valor;
4. E por fim é visto onde muda o sinal e assim o valor de onde a função torna-se 0.

Um exemplo:
A função dada é $f(x)=x - 3$, sabendo, assim, que sua raiz é exatamente no ponto $x = 3$.

1. Pega-se o intervalo entre -4 e 4 sendo $a = -4$ e $b = 4$;
2. Δx é dado por (b - a) / número total de threads, que nesse caso será de 8, então, (4 - (-4)) / 8, tornando, assim, $\Delta x = 1$;
3. Tomando o $\Delta x = 1$, calcula-se o valor da função em cada ponto, dado que o primeiro ponto é o ponto $x = a$ e o último é o $x = b$, sendo que o intervalo entre os ponto é dado por $x = \Delta x + x$;
4. Faz-se, por fim, uma inspeção de todos os valores retornados para achar onde mudou o sinal.

Com a utilização conseguimos obter um ganho de 36 vezes em relação ao mesmo algoritmo serial.

Desenvolvimento de Cenários X3D para Ambientes Virtuais Colaborativos

Bolsista: Graziele Weinchutz Kapps (ISTCC-P)
Orientador: Jauvane C. de Oliveira (LNCC/MCT)

Resumo

Ambientes Virtuais Colaborativos(AVCs) tem sido, historicamente, aplicados a diversas áreas do conhecimento, tais como treinamento, engenharia de software, design e engenharia, medicina, simulação militar de combate para treinamento de tropas etc. Tais aplicações, se imersivas, podem incluir um nível a mais de realismo em uma simulação, permitindo que o usuário tenha uma experiência similar àquela que o mesmo teria em similar situação no mundo real.

Uma tecnologia emergente para a criação de mundos virtuais para ambientes colaborativos e imersivos é o *Extensive 3D Graphics* (X3D) padronizado pelo comitê ISO. O laboratório ACiMA possui um ambiente imersivo CAVE no qual funciona um sistema para renderização de cenários em X3D através do *framework* InstantReality.

Pode-se notar que o desenvolvimento de um Ambiente Virtual Colaborativo não é uma tarefa trivial. Um AVC necessita controlar diversos dispositivos de realidade virtual, tais como luvas de dados, phantoms, sistemas de posicionamento, bem como renderização 3D; simulação de leis da física, incluindo tratamento de colisão, distribuição e filtragem de informação e compensação pela inconsistência de uma rede tal como a Internet.

O desenvolvimento de um cenário coerente que trate dos diversos dispositivos e tecnologias envolvidos em ambientes imersivos e colaborativos não é uma tarefa simples. A fluência em X3D pode ser uma maneira de contornar o problema numa fase inicial de desenvolvimento de AVC e ambientes imersivos.

Ambientes Virtuais Colaborativos têm se mostrado de grande valia para a simulação de uma grande variedade de situações das mais variadas áreas do conhecimento. A finalidade deste projeto de iniciação foi desenvolver cenários complexos para ambientes virtuais colaborativos e/ou imersivos usando X3D e Java usando o *framework* InstantReality. As características destes cenários incluem módulos, tais como:

- Definição de objetos geométricos virtuais;
- Coordenação da interação do usuário com o cenário;
- Controle de alto e baixo nível de dispositivos, como navegadores 3D, joystick e tracker;
- Desenvolvimento de menus em X3D;
- Desenvolvimento de modelos focados na área de petróleo e gás natural, conforme necessidades do Laboratório ACiMA.

O Código Quantico de Shor Para Correção de Erros

Bolsista: Guilherme de Oliveira Ferreira (ISTCC-P)
Orientador: Renato Portugal (LNCC/MCT)
Co-Orientador: Demerson Golçalves (Bolsista PCI/LNCC)

Resumo

As primeiras técnicas eficientes para correção de erro quântica foram desenvolvidas em 1996, por Peter Shor, e simultaneamente por Andrew Steane. Até então, alguns cientistas consideravam a computação quântica como impraticável, atualmente, é considerada extremamente difícil.

Para proteger estados quânticos, da ação de ruidos, seria interessante que houvessem códigos semelhantes aos códigos corretores de erro classicos, como o código de repetição, porém, existem algumas restrições que a computação quântica impõe, como por exemplo, a não clonagem. Sabe-se que não é possível clonar um estado quântico, o que impossibilita a implementação do código de repetição quanticamente, por isso, deve-se pensar em maneiras alternativas de implementar estes códigos.

O código de Shor para correção de erro baseia-se no código corretor de erro clássico, onde a idéia principal é codificar a informação adicionando suficiente redundância de forma que a informação original possa ser recuperada após a ação do ruído. O código é uma combinação de dois códigos corretores distintos: O código de três q-bits para inversão de bit e o código de três q-bits para inversão de fase.

O Código de três q-bits para inversão de bit

Suponha que q-bits sejam enviados por um canal que, com probabilidade *p*, leva o estado $|\psi\rangle$ para o estado $X|\psi\rangle$ onde *X* é uma das matrizes de Pauli. Pode-se proteger q-bits da ação deste ruido, como será mostrado a seguir.

Suponha que um estado inicial $a|0\rangle + b|1\rangle$ possa ser perfeitamente codificado como $a|000\rangle + b|111\rangle$, e que cada um dos q-bits é enviado por uma cópia independente do canal de inversão de bit . Suponha também que a inversão ocorra em no máximo um q-bit. Neste caso existe um procedimento simples para correção de erro que consiste em duas etapas:

1 – Detecção do erro:

São realizadas medidas que detectam erros, se houver, sobre o estado. O resultado destas medidas é chamado *síndrome de erro*.

Utiliza-se duas medidas Z_1Z_2 e Z_2Z_3 definidas como:

$$Z_1Z_2 = Z \otimes Z \otimes I, Z_2Z_3 = I \otimes Z \otimes Z.$$

Cada um destes observáveis possui autovalores +1 e -1, logo, uma medida sobre um estado com estes observáveis resultará em +1 ou -1.

A medida Z_1Z_2 pode ser vista como uma comparação entre o primeiro e o segundo q-bit com resultado +1 se os bits forem iguais e -1 se forem diferentes, da mesma forma, a medida Z_2Z_3 pode ser vista como uma comparação entre o segundo e o terceiro q-bit.

Note que, existem quatro medidas de síndrome possíveis, mostradas forma (Z_1Z_2, Z_2Z_3): (1, 1) – sem erros, (-1, 1) – erro no primeiro bit, (-1, -1) – erro no segundo bit, (1, -1) – erro no terceiro bit.

É importante ressaltar que nenhuma das medidas descritas acima fornece informações sobre as amplitudes *a* e *b* do estado quântico e, portanto, não destroem a superposição do estado que estão tentando proteger.

2 – Recuperação:

O estado original é recuperado aplicando-se novamente a porta *X* no bit invertido. É fácil ver que este procedimento irá funcionar para cada um dos casos mostrados anteriormente.

Código de três q-bits para inversão de fase

O canal de inversão de fase, representado pela matriz de Pauli *Z*, atua sobre estados quânticos da seguinte forma: seja um estado qualquer definido por $a|0\rangle + b|1\rangle$, a ação do ruído após o estado passar pelo canal é definida por $Z(a|0\rangle + b|1\rangle) = a|0\rangle - b|1\rangle$.

Para proteger a informação quântica deste tipo de ruído, pode-se transformar o canal de inversão de fase em um canal de inversão de bits. Para isto, suponha que se trabalhe nas bases $|+\rangle$ e $|-\rangle$. Perceba que em relação a esta base, o operador *Z* leva o estado $|+\rangle$ para $|-\rangle$ e vice versa. Note também, que com relação a esta base, o operador *Z* atua exatamente como o operador *X*, mas com relação aos rótulos + e -.

Pode-se agora aplicar operações semelhantes àquelas utilizadas para o código de três q-bits para inversão de bit para proteger o estado da inversão de fase.

1 - Codificação:

É realizada em duas etapas, primeiro, o estado é codificado exatamente como foi feito para o canal de inversão de bit, em seguida aplica-se a porta Hadamard a cada um dos bits. Por fim, cada um dos três q-bits é enviado por uma copia independente do canal de inversão de fase.

2 – Detecção:

Da mesma forma que foi feito para o código de inversão de bits, pode-se utilizar os observáveis Z_1Z_2 e Z_2Z_3, porém, conjudados por operadores Hadamard:

$$Z_1Z_2 \rightarrow H^{\otimes 3}Z_1Z_2H^{\otimes 3}, Z_2Z_3 \rightarrow H^{\otimes 3}Z_2Z_3H^{\otimes 3}$$

Estas medidas devem ser interpretadas de forma semelhante ao que foi feito para o canal de inversão de bit. Assim, a primeira medida deve ser considerada como uma comparação entre as fases dos dois primeiros q-bits, e a segunda, uma comparação entre o segundo e o terceiro q-bit.

Note que estes operadores também possuem autovalores +1 e -1, logo os resultados das medidas são os mesmos mostrados para o caso de inversão de bit. Note também que após a aplicação das portas Hadamard o problema é reduzido ao caso de inversão de bits que foi mostrado no tópico anterior deste trabalho.

3 – Recuperação:

É facil ver que os canais de inversão de bit e de fase possuem as mesmas características e que, portanto, o procedimento de correção consiste em aplicar o operador *X H X*, ou seja, *X* conjugado por portas Hadamard, no bit alterado.

O Código de Shor

O código de Shor é formado pela concatenação dos dois códigos corretores mostrados acima, logo, é capaz de proteger um q-bit da ação de um erro por alteração de bit ou de fase, inclusive se ambos ocorrerem em um mesmo q-bit.

Primeiramente, um estado quântico $|\psi_0\rangle = a|0\rangle + b|1\rangle$ é codificado utilizando o código de inversão de fase, i.e, $|\psi_0\rangle \rightarrow |\psi_1\rangle = a|+++\rangle + b|---\rangle$, em seguida cada um dos q-bis é codificado com o código de inversão de bit. O resultado é um estado com 9 q-bits:

$$|\psi_2\rangle = \left[\frac{a}{\sqrt{2}}(|000\rangle + |111\rangle) + \frac{b}{\sqrt{2}}(|000\rangle - |111\rangle)\right]^{\otimes 3}$$

Repare que o estado acima pode ser dividido em três blocos de três q-bits cada.

Codificando o estado desta maneira, o código é capaz de detectar e corrigir erros de inversão em qualquer dos nove q-bits, isto é feito utilizando as mesmas medidas Z_1Z_2 e Z_2Z_3 descritas anteriormente para o código de inversão de bit. Note também, que uma vez que o código de inversão de bits atua sobre os três blocos de forma independente, é capaz de detectar e corrigir mais de uma inversão de bit, desde que os bits estejam em blocos separados, como por exemplo, se os bits 1 e 5 forem invertidos.

Para o caso de inversão de fase, utiliza-se, também, os mesmos operadores de medida descritos para o código de inversão de fase, estes atuam sobre os três blocos comparando suas fases. Note que uma inversão de fase em qualquer bit de um bloco inverte a fase de todo o bloco de bits. As medidas de correção são as mesmas para o codigo de inversão de fase com três q-bits, uma vez detectado um erro, pode-se inverter a fase do bloco novamente.

É importante ressaltar, que o código de Shor protege um estado quântico de um erro arbitrário, porém, para esta demonstração é necessário uma abordagem mais profunda de alguns conceitos como o formalismo estabilizador, por isso, deixamos esta discução para um trabalho futuro onde possamos dar maior enfâse ao assunto e torna-lo mais claro.

Referências

[1] LIMA, Elon Lages. Álgebra Linear. 7. Ed. Rio de Janeiro: IMPA, 2008.
[2] NICHOLSON, Keith W., Álgebra Linear.2.ED.São Paulo:McGraw-Hill, 2006.
[3] NIELSEN, Michael A., CHUANG, Iassc L. Computação Quântica e Informação Quântica. 1. Ed. Porto Alegre: Bookman, 2005.

[4] PORTUGAL, Renato, LAVOR, C.,CARVALHO,Luiz M., MACULAN, Nelson Uma Introdução aos Algoritmos Quânticos
[5] LAVOR, Carlile Campos, Uma Introdução à Teoria de Códigos, São Carlos, SP: SBMAC, 2006.

Algoritmos Quânticos de Busca

Bolssita: Jorge Luiz Ferreira da Silva Junior
Orientador: Renato Portugal (LNCC)
Co-Orientador: Demerson Nunes Gonçalves (Bolsista PCI/LNCC)

Resumo

Existem duas classes importantes de algoritmos quânticos que oferecem ganho de eficiência em relação aos seus equivalentes clássicos. A primeira é formada por algoritmos para o Problema do Subgrupo Oculto (PSO). Dado um grupo finito *G* e uma função *f* que é constante nas classes laterais de um subgrupo *H* de *G* e distinta em cada classe lateral, o PSO é o problema de determinar um conjunto gerador para *H*, a partir de informações obtidas da função *f*. A maioria dos algoritmos quânticos para o PSO em tempo polinomial faz uso da transformada de Fourier quântica em grupos. O exemplo mais conhecido desta classe de algoritmos é o algoritmo de Shor para fatoração de inteiros grandes e cálculo de logaritmo discreto [2]. Este algoritmo apresenta ganho de eficiência exponencial sobre o melhor algoritmo clássico conhecido.

A segunda classe de algoritmos que apresenta vantagens sobre os algoritmos tradicionais é representada por algoritmos quânticos de busca. Estes foram primeiramente estudados por Grover [3,4]. O princípio básico desses algoritmos consiste em resolver o seguinte problema: dado um espaço de busca de dimensão *N*, e nenhum conhecimento prévio sobre a estrutura dos elementos no espaço, o objetivo é encontrar um elemento desse espaço que satisfaça uma propriedade requerida. Em quanto tempo tal elemento pode ser encontrado? Classicamente, esse problema requer aproximadamente *N* operações, contudo, um algoritmo quântico de busca pode encontrar tal elemento perfazendo cerca de √N operações.

Neste trabalho, nós estudamos a classe de algoritmos quânticos de busca, mais especificamente, o algoritmo de Grover para busca de um elemento marcado numa lista não ordenada. O algoritmo não apresenta um ganho de eficiência exponencial em contraste com aqueles baseados na transformada de Fourier, mesmo assim, o seu estudo desperta interesse da comunidade científica devido a importantes aplicações como na aceleração nas soluções de problemas NP-completos. O que segue é uma descrição resumida do algoritmo.

O problema da busca consiste em localizar um elemento $|i_0\rangle$ em um banco de dados não ordenado. Classicamente, teríamos uma média de N/2 tentativas ou N tentativas no pior caso. Utilizando o algoritmo quântico de Grover a busca pode ser reduzida para √N tentativas. O algoritmo utiliza dois registradores: o primeiro, com n q-bits, inicializado no estado $|0...0\rangle$ e o segundo, com 1 q-bit, inicializado no estado $|1\rangle$. Vamos representar matematicamente o problema como uma busca sobre a lista {0,1,...,N-1}, onde $N = 2^n$ para algum número natural n, e f uma função

$$f : \{0, 1, ..., N - 1\} \rightarrow \{0, 1\}$$

definida por

$$f = \begin{cases} 1, se\ i = i_0 \\ 0, se\ i \neq i_0 \end{cases}$$

responsável por marcar o elemento procurado i_0.

Agora, façamos o seguitnte:

Passo 1 - Para inicializar o algoritmo, vamos aplicar o operador $H^{\otimes n}$ em cada q-bit do primeiro registrador, denominando esta superposição $|\psi\rangle$. Em seguida vamos aplicar H sobre o estado inicial do primeiro registrador, o novo estado será denomidao de $|-\rangle$.

Passo 2 - Agora vamos imaginar um operador unitario U_f que transforme $|i\rangle$ *em* $|f(1)\rangle$, onde $|i\rangle$ é o estado de n q-bits do primeiro registrador. Aplicando o operador U_f nos registradores observamos que há uma alteração no estado do segundo registrador quando o primeiro registrador representa o elemento procurado.

$$U_f(|i\rangle|0\rangle) = \begin{cases} |i\rangle|1\rangle, se\ i = i_0 \\ |i\rangle|0\rangle, se\ i \neq i_0 \end{cases}$$

Analogamente

$$U_f(|i\rangle|1\rangle) = \begin{cases} |i\rangle|0\rangle, se\ i = i_0 \\ |i\rangle|1\rangle, se\ i \neq i_0 \end{cases}.$$

Por simplicidade, podemos descrever as duas equações anteriores como:

$$U_f(|i\rangle|j\rangle) = |i\rangle|j \oplus f(i)\rangle),$$

onde $|i\rangle$ é o estado de n-qbits do primeiro registrador, e $|j\rangle$ é o estado de 1 q-bit do segundo registrador. Para que o operador U_f proporcione um ganho satisfatório temos que aplicá-lo em estados superpostos, caso contrário não haveria ganho em relação ao algoritmo clássico.

Passo 3 - Vamos aplicar o operador U_f sobre o estado $|\psi\rangle|-\rangle$, que irá gerar um novo estado $|\psi_1\rangle$.

Com a aplicação deste último passo, a função f foi avaliada em todos os pontos com uma única aplicação de U_f. Com isso, o estado associado ao elemento procurado será o único que terá sua amplitude alterada, porém o estado do segundo registrador permanece inalterado.

Se realizássemos uma medida do primeiro registrador neste momento, a probabilidade de se obter $|i_0\rangle$ seria $\left|\frac{-1}{\sqrt{N}}\right|^2 = \frac{1}{N}$, que é uma probabilidade muito baixa.

Ao realizarmos uma melhor análise da aplicação do operador U_f sobre o estado $|\psi\rangle|-\rangle$, veremos que ao refletirmos $|\psi_1\rangle$ em relação a $|\psi\rangle$ a amplitude de $|i_0\rangle$ será aumentada em relação a $|\psi\rangle$. Esta reflexão é produzida pelo operador $2|\psi\rangle\langle\psi| - \mathbf{I}$, que pode ser encontrado pela soma vetorial da projeção de $|\psi_1\rangle$ sobre $|\psi\rangle$ com $|\psi_1\rangle$.

Passo 4 - Vamos aplicar o operador $2|\psi\rangle\langle\psi| - I$ sobre o estado $|\psi_1\rangle$. Esta aplicação irá gerar um novo estado $|\psi_G\rangle$.

Vamos chamar a aplicação desses dois últimos operadores de operador de Grover G, isto é:

$$G = ((2|\psi\rangle\langle\psi| - I) \otimes I)U_f.$$

Após a primeira aplicação do operador G a amplitude de $|i_0\rangle$ cresce aproximadamente

três vezes em relação a sua amplitude no estado $|\psi\rangle$, para N grande:

$$\left(\frac{N-4}{N}\right)\left(\frac{1}{\sqrt{N}}\right)+\frac{2}{\sqrt{N}}=\left(\frac{3N-4}{N\sqrt{N}}\right)\simeq\frac{3}{\sqrt{N}}.$$

Passo 5 – Agora note que o número de vezes k para qual o operador G deve ser aplicado em $|\psi\rangle$, fazendo com que o estado $G^k|\psi\rangle$ torne-se mais próximo do estado $|i_0\rangle$ é dado pela equação:

$$\text{acos}(\langle\psi|i_0\rangle) = k\theta.$$

Isolando k, temos:

$$k=\frac{acos\left(\frac{1}{\sqrt{N}}\right)}{acos\left(\frac{N-2}{N}\right)}.$$

Para sabermos a ordem de grandeza de k, vamos comparar N com k. Calculando os limites, temos:

$$\lim_{N\to\infty}\frac{k}{N}=0,$$

Ou seja, k é menor do que N, para valores grandes de N.

$$\lim_{N\to\infty}\frac{k}{\log_2(N)}=\infty.$$

Neste caso, k é maior do que $\log_2(N)$, para valores grandes de N. Tentando um valor médio, obtemos:

$$\lim_{N\to\infty}\frac{k}{\sqrt{N}}=\frac{\pi}{4}.$$

Ou seja, para valores grandes de N, o número de vezes que o operador G deve ser aplicado é $\sqrt{N}$ vezes. Assim concluímos o Algoritmo de Grover.

Conclusão

Neste trabalho, apresentamos um algoritmo quântico com ganho de eficiência quadrático em relação ao melhor algoritmo clássico conhecido para o problema de busca de um elemento marcado em uma lista não ordenada. Este trabalho é o resultado de um ano de trabalho no projeto de iniciação científica orientado pelos professores Dr. Demerson Nunes Gonçalves da Universidade Católica de Petrópolis e o prof. Dr. Renato Portugal do LNCC. Para o entendimento desse algoritmo foi necessário um estado preliminar de alguns conceitos básicos sobre álgebra linear e computação quântica.

Referências

[1] Axler, Sheldon, Linear Algebra Done Right. 2. Ed. San Francisco: Springer, 1997, San Francisco State University.

[2] C. Lomont, "Hidden Subgroup Problem - Review and Open Problems", *ArqXiv preprint quant-ph/0411037*, 2004.

[3] Grover L.K.: A fast quantum mechanical algorithm for database search, Proceedings, 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212.

[4] Grover L.K.: From Schrödinger's equation to quantum search algorithm, American Journal of Physics, 69(7): 769-777, 2001. Pedagogical review of the algorithm and its history.

[5] LAVOR, C., MANSUR, L.R.U., PORTUGAL,R., Grover's Algorithm: Quantum Database Search

[6] LIMA, Elon Lages. Álgebra Linear. 7. Ed. Rio de Janeiro: IMPA, 2008.

[7] NICHOLSON, Keith W., Álgebra Linear.2.ED. São Paulo:McGraw-Hill, 2006.

[8] NIELSEN, Michael A., CHUANG, Iassc L. Computação Quântica e Informação Quântica. 1. Ed. Porto Alegre: Bookman, 2005.

[9] PORTUGAL, Renato, LAVOR, C.,CARVALHO,Luiz M., MACULAN, Nelson Uma Introdução aos Algoritmos Quânticos.

Construção de Bibliotecas de Fragmentos para a Predição de Estruturas de Proteínas

Bolsista: Karina Baptista dos Santos (ISTCC-P)
Orientador: Laurent E. Dardenne (LNCC/MCT)
Co-Orientador: Fabio Lima Custódio (Bolsista PCI/LNCC)

Resumo

O uso de bibliotecas de fragmentos em métodos de predição de estrutura de proteínas tem demonstrado um grande potencial para obtenção de resultados com um bom nível de acurácia. Isso porque os fragmentos - pequenos segmentos retirados de proteínas cujas estruturas são conhecidas, carregam relações estruturais importantes e seu uso reduz o espaço de configurações a ser investigado. O que permite que sequências mais longas tenham suas estruturas preditas, contornando uma das maiores limitações dos métodos de predição ab initio. Em geral uma biblioteca é construída por similaridade entre a sequência de aminoácidos dos fragmentos e uma determinada posição na sequência alvo. Outros critérios também podem ser utilizados, como por exemplo, a estrutura secundária da sequência alvo.

Um programa gerador de bibliotecas de fragmentos deve ser customizado, ou seja, deve possuir opções capazes de torná-lo flexível e automatizado, visando fornecer uma maior praticidade ao seu usuário. O uso de uma interface gráfica para esse programa, na forma de um portal interativo, é uma opção vantajosa para alcançar essa praticidade. Isso porque torna desnecessária a instalação local do programa e a criação do banco de dados com as geometrias que serão usadas na construção dos fragmentos, um processo bastante demorado.

O objetivo deste trabalho foi o desenvolvimento de um programa gerador de bibliotecas de fragmentos, com um portal interativo na internet atuando como interface, chamado ProFrager que apresenta maior flexibilidade na escolha de opções para geração dos fragmentos em comparação com outros portais que oferecem um serviço semelhante.

O ProFrager cria as bibliotecas de fragmentos para as sequências de proteínas a partir de um banco de dados de estruturas protéicas extraído do PDB (Protein Data Bank) e é capaz de gerar bibliotecas com fragmentos de qualquer comprimento selecionado pelo usuário. Também é possível determinar o número de fragmentos por posição. O ProFrager tem como diferencial oferecer ao usuário opções avançadas para a criação das bibliotecas. Pode-se determinar o score mínimo que um fragmento precisa obter para ser incluído na biblioteca e também optar por criar fragmentos apenas de estruturas homólogas à sequência alvo ou, ainda, apenas de não-homólogas. Os fragmentos podem ser criados usando apenas o critério de similaridade de sequência ou, além desse, informações prévias a respeito da sequência alvo, como predição de sua estrutura secundária.

Análise Arquitetural de Sistemas de Teleatendimento Médico Emergencial

Bolsista: Luiz Felipe do Amaral Marchese da Silva (Universidade Estácio de Sá)
Orientador: Antônio Tadeu Azevedo Gomes (LNCC/MCT)
Co-orientador: Artur Ziviani (LNCC/MCT)

Resumo

O sistema AToMS (AMI Teleconsultation & Monitoring System) [1] é um sistema de telemedicina que oferece um serviço de suporte remoto à decisão no tratamento terapêutico quanto ao uso de trombolíticos em pacientes com Infarto Agudo do Miocárdio (IAM). Esse sistema leva, através de tecnologias de comunicação sem fio, o conhecimento de um especialista até o local onde o paciente com IAM recebe seu primeiro atendimento por uma equipe de emergência. Por fim, o uso de tecnologia sem fio permite que um paciente seja monitorado continuamente durante a sua remoção para uma unidade coronariana. Este trabalho teve por objetivo aplicar técnicas de análise arquitetural com o intuito de identificar as partes do sistema AToMS que demandam modificações em sua estrutura (e, consequentemente, em seu código) para torná-lo mais facilmente adaptável a novas tecnologias de interconexão dos componentes do sistema. A partir dessa análise, foi proposta uma arquitetura alternativa, bem como a reimplementação (em princípio, parcial) do sistema, com vistas a refletir essa nova arquitetura.

Foi usado o método SAAM [2] para avaliar a modificação na parte que se diz respeito à troca do mecanismo de interconexão, que no sistema AToMS é implementado por meio de Web Services [3]. A constatação da avaliação é que, embora esse sistema siga um estilo arquitetural em camadas, seus componentes são altamente acoplados aos detalhes de implementação de Web Services, o que dificulta a modificação para outras tecnologias de interconexão. Assim, um protótipo de uma nova versão do sistema foi implementado que permite a troca do mecanismo de interconexão, e testes foram feitos com a troca de Web Services por XMPP [4], com resultados satisfatórios.

Referências

[1] Malinoski, Iuri. ; Viçoso, R. P.; Correa, B. S. P. M.; Gomes, A. T. A. ; Ziviani, A. . Suporte Remoto ao Atendimento Médico Emergencial via Dispositivos Móveis. In: Workshop de Informática Médica (WIM), 2009, Bento Gonçalves, RS - Brasil. Anais do IX Workshop de Informática Médica, 2009.

[2] Bass, L., Clements, P., Kazman, R. Software Architecture in Practice. Addison-Wesley, 1998

[3] W3C Consortium. Web Services Activity. http://www.w3.org/2002/ws/

[4] Jabber Software Foundation. Extensible Messaging and Presence Protocol (XMPP): Core. Internet standards track: RFC 3920. http://xmpp.org/rfcs/rfc3920.html

Comunicação de Dados em Ambientes Colaborativos

Bolsista: Matheus Otoni Amorim Silva (ISTCC-P)
Orientador: Jauvane C. de Oliveira (LNCC/MCT)

Resumo

Ambientes Virtuais Colaborativos (AVCs) permitem que usuários localizados em posições geográficas distintas colaborem através de uma simulação de um mundo sintético controlado por computadores, utilizando uma infra-estrutura de comunicação tal como a Internet.

AVCs tem sido, historicamente, aplicados a diversas áreas do conhecimento, tais como treinamento, engenharia de software, design e engenharia, medicina, simulação militar de ombate para treinamento de tropas etc. Tais aplicações, se imersivas, podem incluir um nível a mais de realismo em uma simulação, permitindo que o usuário tenha uma experiência similar àquela que o mesmo teria em similar situação no mundo real.

O laboratório ACiMA possui um ambiente imersivo CAVE no qual é usado um *framework* InstantReality que renderiza ambientes virtuais X3D. O desenvolvimento de um Ambiente Virtual Colaborativo não é uma tarefa trivial. Um AVC necessita controlar diversos tipos de dispositivos de realidade virtual, tais como datagloves, phantons, sistemas de posicionamento (trackers), renderização 3D, som 3D, simulação de leis da física, tratamento de colisão entre objetos no mundo virtual, comunicação via rede, etc.

O objetivo desse projeto foi desenvolver mundos virtuais usando X3D os quais podem ser utilizado no CAVE do laboratório ou distribuídos pela internet. O trabalho consistiu na criação de objetos virtuais geométricos, modelagem das interação do usuário com o cenário e desenvolvimento de cenários temáticos para área de petróleo e militares.

Controle e Modelagem Estocástica

Bolsista: Paulo Cesar Silva de Araújo (UFRRJ)
Orientador: Jack Baczynski (LNCC/MCT)

Resumo

Apresentaremos modelos matemáticos que simulam sistemas físicos para fins de otimização e controle. Inicialmente, apresentamos, como motivação, algumas situações de aplicação do modelo, determinístico e estocástico, para então abordar a questão de otimização. Feito isso, exibiremos a estrutura do problema e na seqüência um método de otimização.

Mostraremos o Princípio de Bellman e a equação de Programação dinâmica para o caso do problema de regulador linear determinístico com observações perfeitas.

Predição de Estruturas de Proteínas por Primeiros Princípios em Ambientes de Computação de Alto Desempenho

Bolsista: Paulo Roberto Teixeira Werdt (ISTCC-P)
Orientador: Laurent Emmanuel Dardenne(LNCC/MCT)
Co-Orientador: Fabio Lima Custódio(Bolsista PCI/LNCC)

ProtR-3D: ferramenta *web* para alinhamento estrutural de proteínas

Bolsista: Ranulfo Oliveira Souza (ISTCC-P)
Orientador: Laurent E. Dardenne (LNCC/MCT)
Co-Orientadora: Priscila V. Z. Capriles Goliatt (Doutorado/LNCC)

Resumo

Com o crescente interesse em analisar comparativamente estruturas tridimensionais (3D) de proteínas de diversos organismos biológicos, surge a necessidade de avaliar o quão estas estruturas são semelhantes entre si para apontar o grau de relação evolutiva entre as mesmas. Uma das formas de se realizar essa comparação é através da técnica de sobreposição de estruturas protéicas e do cálculo da distância entre seus átomos retornando o desvio médio quadrático (RMSD). Quanto menor o RMSD maior a similaridade estrutural entre as proteínas envolvidas na análise. Para que o RMSD apresente um resultado mais preciso (próximo de zero), antes temos que obter a melhor matriz de rotação composta pelas coordenadas tridimensionais dos átomos da proteína que será alinhada, e esta matriz é estabelecida através do método de Kabsch [1, 2].

Neste trabalho, foi desenvolvido um programa na linguagem C++, intitulado ProtR-3D, que usa uma biblioteca desenvolvida na linguagem C para estabelecer o cálculo do RMSD, bem como o algoritmo Kabsch para minizar o RMSD. Este programa exige como entrada arquivos texto no formato PDB (*Protein Data Bank*), formato este que contém informações estruturais (coordenadas cartesianas) sobre determinada proteína. O programa foi desenvolvido adequando-se às necessidades de seus usuários, para isso, vale ressaltar que o programa realiza os seguintes tipos de alinhamento: (i) de todo o esqueleto da proteína; (ii) apenas dos carbonos alfa; (iii) de toda a extensão da proteína que compreende as opções (i) e (ii); (iv) de parte da proteína, limitando-se à um intervalo de átomos descriminados pelo usuário. Além disto, caso haja átomos na proteína de referência que não exista nas demais proteínas submetidas, o programa irá tratar esses átomos da proteína de referência, garantindo assim, que o número de átomos para ambos sejam iguais, obedecendo os requisitos para o sucesso do cálculo do RMSD. Após processar os arquivos, montar os vetores de coordenadas tridimensionais e de realizar o melhor alinhamento das mesmas, o programa ProtR-3D retorna, além dos valores de RMSD entre a primeira proteína e as demais, um arquivo no formato PDB resultante contendo as informações tridimensionais dessas proteínas alinhadas.

Visando a praticidade e aplicabilidade deste programa para a comunidade acadêmica e científica, foi desenvolvido um sistema *web* na linguagem PHP, através do qual usuários remotos podem se conectar e acessar todas as funcionalidades deste programa. Além do programa ProtR-3D, o sistema *web* conta também com o Jmol [3], um aplicativo para visualização de estruturas químicas 3D. O Jmol é *open-source*, foi desenvolvido em linguagem Java, e oferece uma melhor interatividade entre o usuário e o arquivo PDB resultante. O sistema já se encontra operacional e está disponível na página do Grupo de Modelagem Molecular em Sistemas Biológicos do Laboratório Nacional de Computação Científica (GMMSB/LNCC) atráves do link: http://www.gmmsb.lncc.br/index.php?pg=16.

Referências

[1] Kabsch, W.. A solution for the best rotation to relate two sets of vectors. *Acta Cryst.* (1976).
[2] Kabsch, W.. A discussion of the solution for the best rotation to relate two sets of vectors. *Acta Cryst.* (1978).
[3] Jmol: An open-source Java viewer for chemical structures in 3D. Disponível em: http://www.jmol.org/

Controle Dinâmico de Câmera em Ambientes de Mesa para Ampliar Imersão

Bolsista: Rivaldo Rodrigues Machado Júnior (UFRN)

Orientador: Jauvane Cavalcante Oliveira(LNCC/MCT)

Co-Orientador: Selan Rodrigues dos Santos(UFRN)

Resumo

Várias aplicações de realidade virtual (RV) envolvem a interação com ambientes virtuais (AV) tridimensionais nos quais a navegação é uma atividade fundamental. A navegação está diretamente relacionada ao controle que o usuário tem sobre a câmera (ou observador) virtual e seu posicionamento dentro do AV. Estudos mostram que a disponibilização de mecanismos de navegação intuitivos e que aproximam a forma natural de interação no mundo real contribuem para (i.e. AVs cuja representação visual é exibida apenas através um monitor regular). A navegação assistida é um destes mecanismos e pode vir a auxiliar o usuário na tarefa de atingir seus objetivos e realizar determinadas tarefas dentro do domínio da aplicação do AV, como por exemplo localizar recursos de interesses ou determinar rotas de navegação entre lugares de interesse.
Este projeto propõem o estudo e o desenvolvimento de um mecanismo de navegação assistida denominado de Câmera de Interesse, cujo objetivo é direcionar o usuário aos pontos de interesses, determinados por um conjunto de regras previamente estabelecidas pelo usuário e/ou aplicação.

Objetivos

O projeto teve por objetivo a implementação de módulos computacionais que visam implementar a idéia de uma Câmera de Interesse. De uma maneira geral, a Câmera de Interesse funciona da seguinte forma: Dados um AV e um conjunto de entidades de interesse, a câmera deve guiar o avatar pelo melhor caminho no AV até uma entidade de interesse especificada. Para tanto, fazemos uso de uma câmera em terceira pessoa que se posiciona automaticamente no AV de forma a indicar a todo instante e de forma não ambígua o caminho relativo a ser tomado, para um dado objetivo específico.

Para alcançar os objetivos supracitados, se faz necessário alcançar as seguintes metas específicas:

- Desenvolver o módulo de pré-processamento do cenário, capaz de gerar um grafo de suporte ao mecanismo da Câmera de Interesse, possibilitando assim o planejamento de caminho necessário.
- Desenvolver e aplicar técnicas de planejamento de deslocamento de forma a controlar, de forma automática, a movimentação da câmera de interesse dentro do ambiente virtual, levando-se em considerações as restrições de movimento e deslocamento dentro do ambiente virtual.
- Realizar testes empíricos comparando a navegação convencional com a navegação assistida pela Câmera de Interesse. Espera-se coletar evidência para corroborar ou mesmo aprimorar a idéia de Câmera de Interesse com bases em uma série de testes envolvendo usuários de vários backgrounds tecnológicos.

Desenvolvimento

Para alcançarmos os objetivos propostos pelo trabalho, seguimos as metas estabelecidas.

Módulo de Pré-Processamento

O módulo de pré-processamento examina um ambiente virtual e gera um grafo de navegação entre suas regiões livres. Uma característica deste tipo de grafo é que entre quaisquer dois pontos, sempre há um caminho alcançável pelo avatar. Para a geração do grafo, criamos um algoritmo de computação de roadmap probabilístico baseado em \cite{roadmap} adaptado às nossas necessidades, com a propriedade de não conectar nós entre os quais já haja um caminho que os conecte. Nossa implementação resultou em grafos menos densos, e mais rapidez na sua computação.

Módulo de Movimentação

O módulo de movimentação foi implementado conforme suas especificações. O algoritmo desenvolvido recebe como entrada a câmera, o objeto de interesse, o avatar, o roadmap precomputado e retorna a posição de destino da câmera a qualquer instante. Internamente, ele mapeia o objetivo de interesse e o avatar para as posições mais próximas do roadmap. Uma vez feito isso, traça-se a rota entre os dois pontos. Por fim, encontra-se a última posição visível do caminho, chamada de destino relativo. O destino relativo e a posição do avatar são então usados para se calcular a posiçaõ final da câmera, que deve garantir a visibilidade de ambos e se posicionar de modo a focar o destino relativo. Este processo, repetido em intervalos de tempo regulares, garante a navegabilidade proposta.

Especial cuidado tem de ser tomado com relação à oclusão, quando um objeto obstrui a visão do avatar. Tal evento tipicamente deixa os usuários confusos e perdidos dentro do AV. Implementamos uma estratégia de resolução de oclusão simples e efetiva, que translada a câmera para o ponto mais próximo de sua posição original que não está ocludido. Isto é feito deslocando-se longitudenalmente a câmera ao longo do raio que conecta o avatar e o destino relativo, de modo a aproximar a câmera do avatar.

Experimentos

Os experimentos comparativos foram conduzidos com 27 estudantes da UFRN. No experimento, comparamos o tempo para se encontrar um grupo de objetos dentro de um AV relativamente complexo para três métodos de navegação: a Câmera de Interesse, o método da Bússola e navegação com Mapas. A bússola apenas ponta para o destino final, enquanto que a navegação por mapas exige que o usuário saiba se localizar no AV em relação ao mapa. Nossa hipótese principal era de que nosso método fosse mais rápido que ambos os outros.

Resultados

Os resultados mostraram que a câmera de interesse foi mais rápida na grande maioria dos casos, e ainda indicaram possíveis caminhos para se otimizar o método.

Conclusões

Entendemos que o nosso método contribui para com o conhecimento existente na área de navegação em AVs. Nossos resultados mostraram que o método é plausível, justificável e eficiente, e constitui uma nova abordagem na área de trabalhos sobre navegação assistida.

Referências

[1] B. Salomon, M. Garber, M. C. Lin, and D. Manocha. Interactive navigation in complex environments using path planning.

Sistema de Monitoramento de Gerência e de Segurança - SiMGeS

Bolsista: Suzana Mattos da Costa (Universidade Estácio de Sá)
Orientador: Luis Rodrigo de Oliveira Gonçalves (LNCC/MCT)

Resumo

SiMGeS (Sistema de Monitoramento de Gerência e de Segurança)consiste em uma ferramentapara monitoramento da rede. O Sistema principal irá rodar em um servidor Apache, sendo possível acessar ferramentas de gerência com um navegador web.

O Sistema trará informações da rede tais como: quantos computadores estão online, e offline (dado que os offline têm de passar antes pelos oletores, assim ficando guardadas as informações no banco), sistema operacional em cada máquina na rede, uso de largura de banda disponível, tipos e quantidades de protocolos que passam na rede e criação de gráficos a partir dos dados coletados. Além de auxiliar na parte administrativa. SiMGeS também trás a idéia de uma ferramenta com baixo custo de desenvolvimento em software, pois utiliza softwares livres.

Introdução

Visto o rápido crescimento da estrutura de comunicação, tanto a nível de recursos e usuários, faz-se necessário o desenvolvimento de pesquisas sobre as melhores práticas de gerência e de monitoramento deste ambiente, de forma a prover um melhor nível de utilização dos recursos.

Entretanto deve-se focar em atividades que levem a implementação de trabalhos práticos, que possam ser utilizados no dia a dia da equipe de Técnicos e Tecnologias destas instituições.

Esta nova geração de ferramentas deve se basear em técnicas que permitam sua utilização e configuração de forma intuitiva, bem como permita a extração de informações de cunho técnico e administrativo. As aplicações além de analisarem a estrutura de comunicação devem ser capazes de apontar possíveis pontos críticos e sempre que possível indicar caminhos que levem a evitar os mais variados tipos de incidentes. Indo de encontro a estas necessidades surgiu a proposta do desenvolvimento da ferramenta SiMGeS – Sistema de Monitoramento de Gerência e de Segurança – que está sendo implantada pelo CSR na infra-estrutura do LNCC (Laboratório Nacional de Computação Cientifica). Com a implementação deste plano de trabalho pretende-se aprimorar e implementar várias das funcionalidades da SiMGeS.

Atualmente, esta sendo implementado e implantado no LNCC, junto à CSR um conjunto de ferramentas que serão utilizadas na gerência e administração de toda a estrutura de rede da instituição. Este processo requer a pesquisa sobre as melhores práticas a serem aplicadas, bem como sobre quais ferramentas serão utilizadas. Findo o processo de análise e pesquisa inicial, pretende-se iniciar a implementação de parte do que será o NOC – Network Operation Center do LNCC.

No presente momento, já se encontra ativo um grupo de sondas que estão coletando várias informações sobre a rede, seus ativos e os dados que nela trafegam. Visando complementar o funcionamento destas sondas pretende-se realizar desenvolver um método que facilite e acelere o seu funcionamento, assim como a construção de uma ferramenta que permita o seu controle de forma remota.

Logo, este projeto propõe basicamente: (i) a remodelagem de repositório de dados, onde são armazenadas as informações utilizadas pelas sondas, (ii) a implementação da interface de gerência remota das sondas, (iii) a implementação de uma interface através de gráficos e mapas de rede poderão ser gerados, (iv) a pesquisa de métodos através dos quais seja possível obter dados que serão utilizados na construção de uma vasta gama de relatórios administrativos e técnicos, os quais fornecerão a base para a tomada de decisão quanto ao funcionamento do ambiente, assim como pela detecção de possíveis incidentes.

O principal objetivo deste projeto é o desenvolvimento do protótipo de uma ferramenta que facilitará o monitoramento e a gerência da estrutura de rede deste laboratório. O Presente projeto integra-se aos esforços dos Tecnologistas do LNCC em intensificar as pesquisas na área de Gerência de Redes e Segurança da Informação. O desenvolvimento de recursos para verificação do nível de utilização do ambiente computacional de forma automática e eficiente permitirá uma maior confiança quanto disponibilidade do sistema suportado pelo LNCC e seus parceiros.

Monitoramento de Redes – SiMGeS

Minha participação no projeto SiMGeS consiste na criação de sondas para o monitoramento do tráfego de redes.

O monitoramento de redes consiste basicamente na coleta de dados, detecção e correção de falhas em um tempo mínimo, e em estabelecer procedimentos para a previsão futura.

O monitoramento permanente nos permite obter altos índices de segurança, mas para isto são necessárias ferramentas que nos permitam acompanhar o desempenho de equipamento, sistemas e links e todos os demais dispositivos sujeitos as falhas, manipulações ou a acessos indevidos.

A coleta de dados é o primeiro passo do processo de monitoramento, todavia a transformações de dados em informações úteis, em geral, requer o processamento estatístico destes dados, sua comparação com indicadores históricos e sua apresentação em um formato que permita sua análise.

Monitorar links de dados nos permite não apenas uma avaliação do tráfego em si, mas também nos oferece informações sobre sua forma de utilização, horários de pico, perfis de aplicativos e usuários.

O dimensionamento de servidores e links têm sido apontados como os principais problemas em infraestrutura em TI, o monitoramento de equipamento e sistemas permite ir além da função reativa, possibilitando a análise e o planejamento de longo prazo de upgrades de hardware e software de forma a evitar gargalos na infraestrutura.

Estágio Atual do Projeto – SiMGes

No momento estamos trabalhando com a ferramenta de monitoramento Tcpdump, já foram criadas quatro sondas para coletagem dos protocolos IP, ARP, Ipv6 e STP, para podermos monitorar o tráfego da rede, obtendo os principais protocolos que passam por ela, horários de maior tráfego, criação de broadcast e possíveis pontos e horários de "picos".
As quatro sondas para coletagem de dados foram criadas na linguagem Shell script, e postadas no banco de dados mysql através de scripts feitos na linguagem de programação python.

As sondas estão instaladas em uma bridge localizada no LAB 1 do LNCC, onde são executados os testes com o SiMGeS, lá temos uma rede de testes e simulações e posteriormente começarão as coletas de teste junto a toda rede do LNCC.

Há criação do front end será feito com o framework Django, onde depois de coletadas e inseridas as informações no banco de dados, mostraremos resumos e gráficos dos dados coletados.

Haverá a inserção de novas ferramentas de monitoramento de redes, como ,Ntop, Nagios, Ettercap entre outras, com o objetivo de implementar novas funcionalidades ao SiMGeS.

Ferramentas Utilizados no Projeto SiMGeS

Foram utilizadas ferramentas de menor custo possível, Sistema Operacional Linux e ferramentas que são disponíveis de graça para ele, como servidor Apache2, linguagem Shell script, linguagem Python (atualmente vem com o SO) , banco de dados MySQL, Framework Django, coletas da rede via SNMP e Tcpdump e Jude para os diagramas UML.

Tcpdump

O Tcpdump é uma ferramenta de monitoramento de redes de computadores, utilizada para monitorar os pacotes que trafegam na rede (Sniffer). Ela seleciona e retorna para análise os cabeçalhos dos pacotes que passam pela interface de rede.

O Tcpdump funciona na maioria dos sistemas operativos UNIX: Linux, Solaris, BSD, Mac VOS X, HP-UX e AIX entre outros. Nesses sistemas, tcpdump faz uso da biblioteca libpcap para capturar os pacotes que circulam pela rede.Existe uma adaptação de tcpdump para os sistemas Windows que se chama WinDump e que faz uso da biblioteca Winpcap.

Em UNIX e outros sistemas operativos por motivos de segurança é necessário ter os privilégios do root para utilizar tcpdump.

Instalação em sistemas baseados em Debian:

login como super usuário (root) – su

apt-get install tcpdump

Em seu modo de utilização mais simples, o tcpdump não precisa de nenhum parâmetro para ser utilizado.

Estando logado como root (O tcpdump utiliza-se de sua interface em promiscuous mode), digite no terminal: tcpdump:

A saída será parecida com o exemplo abaixo:

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes22:30:36.319613 IP

workstation.mshome.net.33810 > servidor.mshome.net.domain: 44128+ A? mail.google.com.

(33)

22:30:36.350612 IP workstation.mshome.net.50163 > servidor.mshome.net.domain: 5369+ PTR? 1.0.168.192.in-addr.arpa. (42)

22:30:36.353572 IP servidor.mshome.net.domain > workstation.mshome.net.36283: 17390-1/0/0 (104)

22:30:36.612322 IP servidor.mshome.net.domain > workstation.mshome.net.33810: 44128 5/0/0 CNAME[|domain]

Encerrando o sniffer (Ctrl + C):

77 packets captured

77 packets received by filter

0 packets dropped by kernel

Analisando os principais campos da saída acima (Os campos são separados por espaços):

• Timestamp=Horário de captura do pacote.

• Tipo (Protocolo) do pacote capturado.

• Endereço e porta de origem do pacote.

• Sinal indicador do sentido do pacote.

• Endereço e porta de destino do pacote.

Parâmetros básicos do Tcpdump

O Tcpdump tem os seguintes parâmetros:

-A: Imprime a cada pacote em código ASCII.

-c: Termina a execução após receber “n” pacotes.

-i: Recebe como parâmetro a interface ou o número associado a ela. Se especificado “any” captura de todas as interfaces, porém sem ser em modo promíscuo.

-D: Exibe a lista de interfaces disponíveis.

-n: Não converte endereços em nomes.

-r: Lê os pacotes a partir de um arquivo.

-s: Define o tamanho de cada pacote a ser capturado.

-t: Não imprime a hora de captura dos pacotes.

-v: Exibe a saída com mais detalhes.

-vv: Exibe a saída com mais detalhes ainda.

-vvv: Exibe a saída com informações ainda mais detalhadas.

-w: Escreve os pacotes em um arquivo que pode ser lido posteriormente com a opção -r.

-x: Exibe o conteúdo do pacote no formato hexadecimal.

-X: Exibe o conteúdo do pacote nos formatos hexadecimal e código ASCII.

src: Direcção e porta de origem.

dst: Direcção e porta de destino.

flags: Exibe as flags do cabeçalho TCP.

dataseq: Número de sequência do primeiro byte de dados neste segmento TCP. O formato é primeiro:último (n).

ack: Indica o número seguinte de sequência que se espera receber.

window: Tamanho da janela de recepção.

urgent: Existem dados urgentes.

options: Indica a existência de opções. Vão entre «"...»".

Exemplos:

Conexões de origem podem ser monitoradas utilizando o parâmetro src host, um exemplo simples seria monitorarmos o tráfego que vem de 192.168.0.9 para nosso computador, com o ip 192.168.0.2, com o comando abaixo:

tcpdump -i eth0 src host 192.168.0.9

Se quisermos monitorar as conexões especificando um host de destino, poderíamos fazê-lo com o parâmetro dst host, com o caomando abaixo coletamos todo o tráfego do host 192.168.0.2 com 192.168.0.1, no caso, 192.168.0.1 é nosso gateway.

tcpdump -i eth0 dst host 192.168.0.1

Com tcpdump também podemos especificar exceções com o parâmetro not host, por exemplo, em nosso servidor queremos ver todo o tráfego que se passa em sua interface, exceto o de 192.168.0.8:

tcpdump -i eth0 not host 192.168.0.9

No tcpdump podemos também especificar portas de origem e destino com os comandos src port e dst port, um exemplo seria monitorarmos o tráfego destinado à porta 80 (http), com o comando abaixo:

tcpdump -i eth0 dst port 80

Para verificarmos o tráfego da porta de origem 32881:

tcpdump -i eth0 src port 32881

Faz a captura de 30 pacotes do host 192.168.0.110 na interface eth0 sem resolver nomes com tamanho máximo de pacote de 1500 bytes exibindo o conteúdo dos pacotes nos formatos ASCII e Hexadecimal:

tcpdump -n -i eth0 -s 1500 -X host 192.168.0.110 -c 30

Analisa o tráfego da interface eth2 e coleta os dados de pacotes com até 1500 bytes referentes à rede de destino 192.168.0.0 exceto o que se refere ao host 192.168.0.114 e a porta 22(ssh) com o máximo de detalhes sem exibir o timestamp e os grava no arquivo dump.log:

tcpdump -i eth2 -t -vvv -s 1500 -A dst net 192.168 and not host 192.168.0.114 and not port ssh -w dump.log

Esses são apenas alguns exemplos básicos do Tcpdump, e do que podemos coletar com ele.

Python

Python é uma linguagem de programação de alto nível (linguagem com um nível de abstração relativamente elevado, longe do código de máquina e mais próximo à linguagem humana), interpretada, imperativa, orientada a objetos, de tipagem dinâmica e forte.

Atualmente possui um modelo de desenvolvimento comunitário, aberto e gerenciado pela organização sem fins lucrativos Python Software Foundation. Apesar de várias partes da linguagem possuírem padrões e especificações formais, a linguagem como um todo não é formalmente especificada. O padrão de facto é a implementação CPython.

A linguagem foi pensada e estruturada para o ensino de programação, então ela teria que conter uma compreensão simples da estrutura para o fácil aprendizado e é isso que o Python apresenta, priorizando a legibilidade do código sobre a velocidade ou expressividade. Combina uma sintaxe concisa e clara com os recursos poderosos de sua biblioteca padrão e por módulos e frameworks desenvolvidos por terceiros.

Python no SiMGeS

A escolha da linguagem de programação Python para o SiMGeS, se deu por se tratar de uma linguagem de programação de alto nível, rápida, concisa, de fácil interaç atendendo nossas necessidades.

Framework Django

Django é um framework(framework é o conjunto de classes implementadas em uma linguagem específica, usadas para auxiliar o desenvolvimento de software) para desenvolvimento rápido para web, escrito em Python, que utiliza o padrão MVC (model-view-controller).Django utiliza o princípio DRY (Don't Repeat Yourself), onde faz com que o desenvolvedor aproveite ao máximo o código já feito, evitando a repetição.

Funcionamento do Django:

O django funciona da seguinte maneira:

1. Você entre em um navador de páginas da internet e digita o endereço do seu site.
2. O site é feito em Django, usando a linguagem Python;
3. Através do Django, seu site acessa o Banco de Dados (no caso do sistema SiMGes estamos usando o Mysql) e em arquivos locais e retorna para o seu navegador a página com funcionalidades em geral;

Framework Django no SiMGeS

Usaremos o Framework Django para criação do front end do SiMGeS, onde constará relatórios dos dados coletados (dando ao usuário opções de relatórios por hora, dia, semana e mês), e gráficos do tráfego da rede.

Mysql

O MySQL é um sistema de gerenciamento de banco de dados (SGBD), que utiliza a linguagem SQL (Linguagem de Consulta Estruturada, do inglês Structured Query Language) como interface. É atualmente um dos bancos de dados mais populares.

Características

• Portabilidade (suporta praticamente qualquer plataforma atual);

• Compatibilidade (existem drivers ODBC, JDBC e .NET e módulos de interface para diversas linguagens de programação, como Delphi, Java, C/C++,Visual Basic, Python, Perl, PHP, ASP e Ruby)

• Excelente desempenho e estabilidade;

• Pouco exigente quanto a recursos de hardware;

• É um Software Livre com base na GPL;

Mysql no SiMGeS

Escolhemos o banco de dados Mysql por ele ser o que melhor atende nossas necessidades, por sua grande portabilidade e compatibilidade, ser um dos bancos de dados mais utilizados naatualidade e ser de fácil domínio.

Conclusão

O sistema coleta as informações na rede usando a ferramenta de monitoramento de rede Tcpdump armazenando as informações mais necessárias no banco de dados, para uma análise posterior, como protocolos mais usados, horários de maior funcionamentouso, geração de Broadcast.

Podendo assim fazer tomada de decisões mais precisas e melhores. Agilidade e precisão de possíveis problemas na rede é um dos principais ganhos fazendo esse tipo de coletas, sendo muito útil em ambientes de grande porte.

Implementação e inclusão do Serviço MyProxyna grade VCG e no Portal de Submissão

Bolsista: Victor D. Oliveira (Universidade Estácio de Sá)
Orientador: Bruno Richard Schulze (LNCC/MCT)
Co-Orientador: Antonio Roberto Mury (Bolsista CNPq/Visistante)

Resumo

A garantia da segurança em um ambiente de grade computacional é uma tarefa complexa. A necessidade de fornecer direitos de uso dos recursos da grade e gerar um certificado para seus usuários é mais complexa ainda sendo vários os procedimntos para obter o direito de acesso. Neste caso o MyProxy se apresenta como uma excelente ferramenta, que tem como função fornecer certificados com tempo de vida relativamente curto para os usuários, possibilitando um maior controle.

O MyProxy é um software de código aberto para gerenciamento da infraestrutura de chaves públicas padrão X509. Combina um repositório de credenciais online comum a autoridade certificadora (CA) que permite que os usuários obtenham facilmente credenciais quando e onde necessitam. Com isso não há a necessidade do usuário transportar seu certificado e a sua chave privada por toda rede.

O trabalho abaixo apresenta o uso do MyProxy em um ambiente de grade computacional com a finalidade de prover um serviço de autenticação mais seguro e amigável ao usuário.

Processo de Geração e uso de Certificado

Quando um usuário deseja utilizar a grade computacional é necessário que se emita um certificado de uso, estes certificados devem ser compatíveis com os da Autoridade Certificadora da grade, em especial o Globus Toolkit [1] e o MyProxy [2].

Apartir das versões mais recentes do Globus Toolkit, o MyProxy [3] foi incluído como parte do pacote de instalação, porém permanece ainda por parte dos administradores do ambiente, a responsabilidade de configurar e implementar o serviço de acordo com a arquitetura e necessidades específicas.

Para que possa gerenciar os certificados é necessária a configuração do seu servidor e serviços. Para o caso específico da Grade VCG foram implementados um conjunto de regras que determinam a forma com que o usuário será capaz de acessar os serviços disponíveis[4].

Entre os serviços implementados destacam-se a possibilidade da geração e renovação dos certificados, possibilitando aos usuários o direito de uso dos recursos da grade. Esse serviço foi implementado no portal por meio do uso da ferramenta o Java Cog Kit [5] que cria um ambiente para execução dos serviços: GSI, Grid FTP, GRAM e My Proxy, sendo esse último utilizado nesse projeto.

A implementação acima permitiu que o gerenciamento dos certificados fosse facilitado, tornando-o transparente, rápido e de fácil uso por parte de seus usuários

Implementação

Como resultado, três formas de colocar em prática o serviço de certificado são hoje possíveis na grade e no portal VCG.

Armazenamento do Certificado – Depois de obter um certificado da Autoridade Certificadora (CA), o usuário pode armazenar a credencial obtida no serviço de proxy. O certificado fica disponível, por padrão, para uso no repositório MyProxy por um período de 7 dias, podendo estes ser prolongado em função das necessidades (Figura1).

Figura 1 - Armazenamento e Recuperação dos Certificados

Geração do Certificado pelo MyProxy –Outra maneira, é utilizara Autoridade Certificadorado MyProxy. Nesse caso, o MyProxy CA pode criar certificados sob demanda. Em outras palavras, o usuário poderá utilizar os recursos da grade sem a necessidade de um certificado gerado pela CA da grade, utilizando o certificado gerado diretamente pelo MyProxy, dispensando assim o armazenamento do certificado na máquina do usuário. O usuário autentica-se junto ao servidordo MyProxy e o mesmo devolve um certificado correspondente (Figura2).

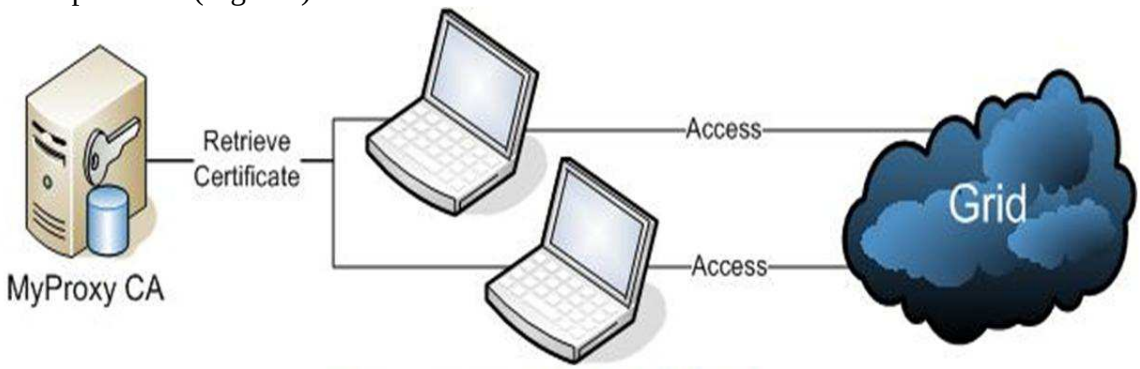


Figura 2 – Geração do certificado pelo MyProxy CA

Certificado de Curto Prazo –A terceira e última maneira, foi a implementação do serviço de obter credenciais de curta duração no portal de submissão GT -VCG. O usuário ao entrar como seu login e a sua senha no portal recebe o Proxy gerado pelo MyProxy, o que permite o uso dos recursos da grade, sem a necessidade do armazenamento dos certificados e as chaves no portal, isto é possível porque ele busca os certificados dos usuários diretamente do seu repositório (Repositóriodo MyProxy). Esse serviço foi totalmente customizado para uso na grade (Figura3).

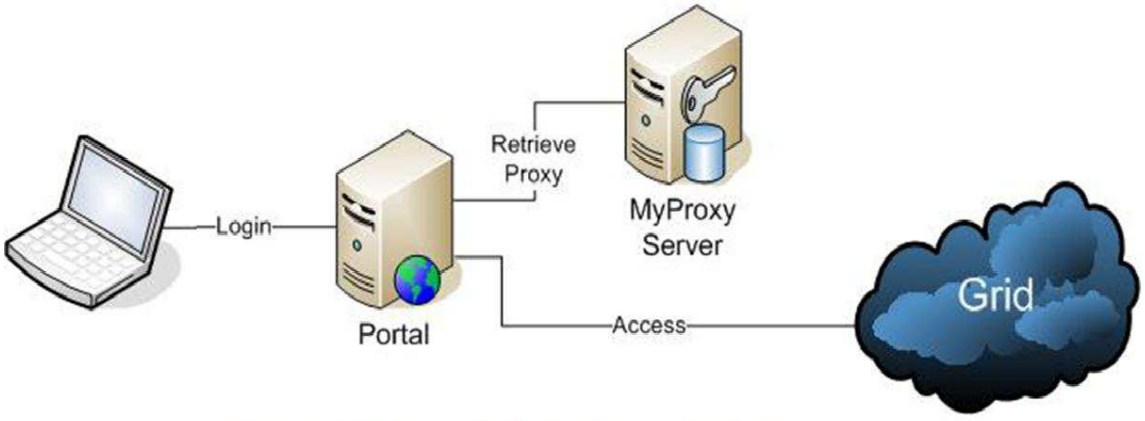


Figura 3 – Fornecimento certificado curta duração no Portal VCG

Conclusões

Concluímos que o My Proxy se apresenta como uma ferramenta ideal para a Implantação de um serviço de autenticação de usuários em um ambiente de grade. A propriedade de gerar certificados de curta duração garante um nível de segurança maior do que credenciais manipuladas por tempo indeterminado. Além disso, ele torna o processo de criação de credenciais mais rápido e fácil para os usuários, que podem requisitar um proxy para utilização dos recursos da grade independentemente de onde estiverem.

Referências Bibliográficas

[1]TheGlobusAlliance.Disponívelem:http://www.globus.org/.Acessoem:14junhode2010.
[2]CredentialManagementService.Disponívelem:http://grid.ncsa.illinois.edu/.Acessoem:11junhode2010.
[3]JavaCogKit.DisponívelemhttP://www.cogkit.org/.Acessoem:17junhode2010.
[4]LICHT,Fábio.FornecimentoAutomatizadodeCertificadosdeCurtaDuraçãoParaDispositivosMóveisemGradesComputacionais.RiodeJaneiro,RJ:IME,2006.TesedeMestrado.
[5]MyProxy–Globus.DisponívelemhttP://dev.globus.org/wiki/MyProxy.Acessoem:15junhode2010.