Modelo para Criação de Apresentações do LabEPI

Para defesas de TCC e Apresentações de Trabalhos

Nome Completo do Aluno ou Autor(es)

Orientador: Prof. Dr. Nome Completo do Orientador

(Defesa de Trabalho de Conclusão de Curso)

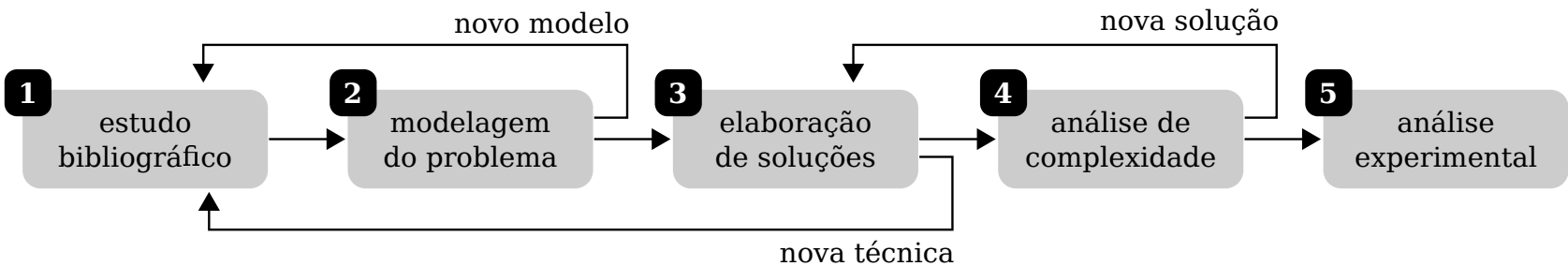
Universidade Federal do Rio Grande do Norte – UFRN
Centro de Ensino Superior do Seridó – CERES
Departamento de Ciências Exatas e Aplicadas – DCEA
Bacharelado em Sistemas de Informação – BSI

Laboratório de Elementos do Processamento da Informação – LabEPI

4 de janeiro de 2015

Problema

Projeto de Sistemas de Monitoramento de Redes de Computadores



Trabalhos relacionados

Observabilidade

- Cáceres et al. (1999)
  - modelo *multicast*
- Ji & Elwalid (2002)
  - escalabilidade da quantidade de medições
- Chen et al. (2007)
  - quantidade de nós monitores da ordem de $O(n \log n)$, monitoramento de *links*
- Gopalan & Ramasubramanian (2012)
  - localização dos nós observadores

Visualização

- Yee et al. (2001)
  - visualização radial interativa
- Bachmaier (2007)
  - planaridade radial
- Diehl et al. (2010)
  - tempo de resposta similares
- Burch et al. (2011)
  - tempo de resposta no centro da visualização

Proposta

O problema da escolha dos observadores

Dado que a topologia da rede é conhecida, como escolher de forma ótima, dentre os nós acessíveis na topologia, aqueles que desempenharão o papel de observadores?

Utilização da teoria de representação de redes como sistemas lineares para explorar o conceito de observabilidade.

Proposta

O problema da apresentação da informação

Dado um conjunto de predicados, como é possível apresenta-los de forma eficiente, escalável e eficaz, considerando a utilização do fator visual e da ampliação da cognição que ela proporciona?

Minimização do tempo e da quantidade de recursos necessários para apresentação dos predicados por meio da visualização por disposição radial.

Organização

- Observabilidade
  - Conceitos: estrutural e funcional
  - Premissas
  - Modelo
  - Resultados teóricos
  - Experimentos
- Visualização
  - Conceitos
  - Premissas
  - Modelo
  - Resultados teóricos
  - Experimentos
- Considerações finais

Observabilidade

Observabilidade estrutural

Conjunto de nós para os quais a leitura dos estados permitem a inferência do estado de todos os outros nós da rede.

Observabilidade funcional

Conjunto de nós cuja quantidade de informação que trafega por eles consiste em um fator predefinido da totalidade do tráfego que se propaga na rede.

Busca-se a minimização desses conjuntos para atender os requisitos de escalabilidade.

Observabilidade estrutural

Invariância topológica

Considera-se que a topologia da rede não muda com o tempo. Essa propriedade é denominada invariância topológica restrita.

Evolução discreta de estado

A transição de estado do sistema ocorre de forma síncrona, para cada nó da rede, e discreta, em instantes bem definidos.

Observabilidade funcional

Conservação da informação

A probabilidade de haver perda de informação na rede durante o processo de propagação é nula.

Atingibilidade

A probabilidade de que uma informação partindo de um nó qualquer da rede atinja qualquer outro nó da rede é sempre positiva.

Observabilidade funcional

Processo markoviano

Um processo de Markov é uma descrição de um sistema cujo estado $\mathbf{x}(t)$ evolui da seguinte forma:

$$\mathbf{x}(t+1) = \mathbf{P}\mathbf{x}(t),$$

onde $\mathbf{P}$ é uma matriz estocástica de transição de estado definida como

$$\mathbf{P} = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{bmatrix},$$

onde p_{ij} descreve a probabilidade de ocorrência no estado $x_i(t+1)$ dada uma ocorrência precedente em $x_j(t)$.

Visualização

Teorema (Tempo de execução esperado do algoritmo)

O tempo esperado de execução necessário para se calcular o raio base mínimo para visualização por disposição radial expressiva é da ordem de $\Theta(n)$, ou seja, linear e proporcional a quantidade de nós. □

Teorema (Escalabilidade da visualização)

A quantidade de nós n em uma visualização por disposição radial expressiva mínima com área A é dada pela relação assintótica $n \in \Theta(A^{\alpha})$, onde $1/2 \leq \alpha \leq 1$. Sendo que, para $\alpha = 1/2$, caracteriza-se o pior caso de escalabilidade, e para $\alpha = 1$, o melhor caso. □

Conclusões

Observabilidade

métrica	observabilidade estrutural $\lvert O_e^o \rvert$	observabilidade funcional $\lvert O_c^o \rvert$
densidade	inversa	direta
grau médio	inferior	superior
diâmetro	inversa	direta
eficiência	direta	inversa
agrupamento	direta	inversa

Visualização

métrica	raio total para $m = 1$	raio total para $m = 2$
diâmetro	direta	invariante
eficiência	direta	direta

Contribuições

Observabilidade

- Demonstração da possíbilidade de inferência do estade da rede a partir do monitoramento de um subconjunto de nós;
- Algoritmos de tempo linear para definição dos conjuntos observadores mínimos;
- Observações com base em experimentos que relacionam métricas da rede com a quantidade mínima de nós observadores;

Visualização

- Minimização do espaço necessário para representação expressiva pela disposição radial;
- Algoritmo de tempo linear para otimização da visualização;
- Demonstração dos limites teóricos de escalabilidade;
- Observações com base em experimentos que relacionam métricas da rede com a escalabilidade da visualização.

Produção

Capítulos de livros

- Medeiros, J.P.S.; Borges Neto, J.B.; Brito Júnior, A.M.; Pires, P.S.M. **Learning Remote Computer Fingerprinting**, Computational Intelligence in Digital Forensics, Springer, Intelligent Systems Reference Library, ISSN 1868-4394, 2014 (aceito para publicação).
- Medeiros, J.P.S.; Borges Neto, J.B.; Queiroz, G.S.D.; Pires, P.S.M. **Intelligent Remote Operating System Detection**, Case Studies in Secure Computing, Achievements and Trends, CRC Press, Taylor and Francis, 2014 (aceito para publicação).

Periódicos

- Medeiros, J.P.S.; Santos, S.R.; Brito Júnior, A.M.; Pires, P.S.M. **Advances in Network Topology Security Visualisation**, International Journal of System of Systems Engineering (IJSSE), ISSN 1748-0671, Inderscience, volume 1, number 4, pages 387-400, 2009.
- Medeiros, J.P.S.; Brito Júnior, A.M.; Pires, P.S.M. **Using Intelligent Techniques to Extend the Applicability of Operating System Fingerprint Databases**, Journal of Information Assurance and Security (JIAS), ISSN 1554-1010, volume 5, issue 4, pages 554-560, 2010.
- Medeiros, J.P.S.; Pires, P.S.M. **On the Scalability Bounds of Radial Layout for the Visualization of Scale-free Networks**, Applicable Algebra in Engineering, Communication and Computing (AAECC), ISSN 0938-1279, Springer, 2013 (submetido para revisão).

Produção

Conferências

- Medeiros, J.P.S.; Brito Júnior, A.M.; Pires, P.S.M. **A New Method for Recognizing Operating Systems of Automation Devices**, 14th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), 2009. Proceedings of ETFA 2009, ISSN 1946-0759, pages 1-4, ISBN 978-1-4244-2727-7, 2009.
- Medeiros, J.P.S.; Brito Júnior, A.M.; Pires, P.S.M. **A Data Mining Based Analysis of Nmap Operating System Fingerprint Database**, 2nd International Workshop on Computational Intelligence in Security for Information Systems (CISIS), 2009. Advances in Soft Computing, ISSN 1867-5662, volume 63, pages 1-8, Springer, 2009.
- Medeiros, J.P.S.; Brito Júnior, A.M.; Pires, P.S.M. **An Effective TCP/IP Fingerprinting Technique Based on Strange Attractors Classification**, 2nd International Workshop on Autonomous and Spontaneous Security (SETOP), 2009. Lecture Notes in Computer Science (LNCS), ISSN 0302-9743, volume 5939, pages 208-221, Springer, 2010.
- Medeiros, J.P.S.; Brito Júnior, A.M.; Pires, P.S.M. **A Qualitative Survey of Active TCP/IP Fingerprinting Tools and Techniques for Operating Systems Identification**, 4th International Workshop on Computational Intelligence in Security for Information Systems (CISIS), 2011. Lecture Notes in Computer Science (LNCS), ISSN 0302-9743, volume 6694, pages 68-75, Springer, 2011.
- Medeiros, J.P.S.; Pires, P.S.M. **Optimal Visualization of Complex Networks Using Radial Layout**, Perspectives and Challenges in Statistical Physics and Complex Systems for the Next Decade: A Conference in Honor of Eugene Stanley and Liacir Lucena, Book of Abstracts, page 37, 2011.

Trabalhos futuros

Observabilidade

- Estudo da validade do modelo considerando premissas menos restritivas;
- Projetar um sistema de monitoramento como prova de conceito;
- Estudar mecanismos de ajuste da matriz de transição de estrados para o caso variante no tempo;
- Estudar projeto de topologias menos sucetíveis à ataques distriuídos.

Visualização

- Extensão do modelo para utilização de técnicas de distorção;
- Verificar demais propriedades da rede relacionadas à escalabilidade.